SANS | GIAC CERTIFICATIONS

85+ hands-on courses

150+ extraordinary, SANS-certified instructors

40+ certifications

The proven industry standard for cybersecurity training, certifications, degrees, and research

REAL EXPERTISE.
REAL SKILLS.
REAL PROTECTION.

"The real value of this training lies at the intersection of quality content and delivery by a subject-matter expert actively working in the field, making it incredibly relevant and immediately applicable to my job."

—P. Watson

The SANS Promise:

You will be able to use the skills you've learned in our training and programs immediately in your work.

About SANS

SANS is the world's largest and most trusted provider of cyber security training. Founded in 1989, SANS operates globally and has over 200,000 alumni.

For over thirty years, we have worked with many of the world's more prominent companies, military organisations, and governments.

Technology may have changed in that time, but our core mission has remained constant: to protect people and assets through sharing cutting-edge cyber-security skills and knowledge.

Strength from people
SANS Instructors are, first and foremost, industry professionals with a wealth of real-world experience – experience that they bring into the classroom.

Across our roster of Instructors are many active security practitioners who work for high profile organisations. The list includes red team leaders, information warfare officers, technical directors, CISOs, and research fellows.

Along with respected technical credentials, SANS Instructors are also expert teachers. Their passion for their subject shines through, making the SANS classroom efficient and effective.

Cutting edge training
Cybercrime evolves constantly. SANS prepares students to meet today's dominant threats and tomorrow's challenges.

We do this through constantly updating and rewriting our courses and support material.
This process is steered by an expert panel that draws on the global community's consensus regarding best practice.

Focussed training
SANS training is job and skill-specific. We offer more than 70 courses, designed to align with dominant security team roles, duties, and disciplines.

The SANS Curriculum spans Digital Forensics, Audit, Management, Offensive Operations, ICS, Secure Software Development and more (see pages 14-19). Each curriculum offers a progression of courses that can take practitioners from a subject's foundations right up to specialist skills and knowledge.

Our training is designed to be practical; students are immersed in hands-on lab exercises built to let them rehearse, hone and perfect what they've learned.

The SANS Promise
At the heart of everything we do is the SANS Promise: Students will be able to deploy the new skills they've learned immediately.

The global community
SANS Institute is a prominent member of the global cybersecurity community. We operate the Internet Storm Centre – the internet's early warning system.

SANS also develops, maintains, and publishes a large collection of research papers about many aspects of information security. These papers are made available for free.

The GIAC Advantage
GIAC validates the skills of information security professionals, proving that those certified have the technical knowledge necessary to work in key areas of cyber security.

GIAC certifications are respected globally because they measure specific skill and knowledge areas. GIAC offers the only cyber security certifications that cover advanced technical subject areas.

There are over 40 specialised GIAC certifications. Several GIAC certifications are accepted under the ANSI/ISO/IEC 17024 Personnel Certification programme.

Many SANS training courses align with GIAC certifications. As such, SANS Training is an ideal preparation for a GIAC certification attempt.

Why SANS is the best training and educational investment
SANS' immersion training is intensive and hands-on and our courseware is unrivalled in the industry.

SANS Instructors and course authors are leading industry experts and practitioners. Their real-world experience informs their teaching and SANS' training content.

SANS training strengthens a student's ability to achieve a GIAC certification, with both SANS and GIAC placing an emphasis on learning practical skills.

How to register for SANS training
SANS runs training events both online and In-Person globally. In-Person training runs across an intensive 5/6 days. For Online Training you have the choice of either taking your course at your own pace through SANS OnDemand over the course of 4 months, or through SANS Live Online which offers live-streamed instructor-led training across 1 or 2 weeks. With SANS Online Training, you can experience all the features you love about SANS classroom-based training events, without the need to travel. Enjoy live, Instructor-led training with courses available across multiple time zones or train at your own pace, anytime, anywhere with pre-recorded sessions.

Find your course, choose your training modality and enjoy everything the SANS training experience has to offer.

Students should register online by visiting **www.sans.org**

Contact SANS
UK, Mainland Europe and Nordics:
+44 203 384 3470
Middle East & Africa: +971 04 431 0761
Australia: +61 2 6174 4581
India: +91 974 1900 324
Japan: +81 3 3242 6276
Singapore: +65 8612 5278 / +65 3165 66 81

Or you can email us at
emea@sans.org (for UK, Mainland Europe & Nordics),
mea@sans.org (for Middle East & Africa)
asiapacific@sans.org (for Asia Pacific)

Course Contents

TRAIN & CERTIFY – INVEST IN YOUR FUTURE

63% **of organizations were breached in the past year.***

** Forrester The 2021 State of Enterprise Breaches*

Cybersecurity skills continue to be in high demand as organizations are challenged to get past the skills gap in their search for infosec talent. As cyber threats and attacks increase in number and sophistication, there's a growing global incentive to focus on educating, empowering, and evolving the workforce to reduce cyber risk.

People are truly the most critical line of defense against threats, and it's essential to provide them with the practical skills required to best defend your organization. From improving security awareness across enterprises to building high-performing cybersecurity teams, SANS has training, certifications, and resources to help reduce risk to your organization.

- **Enhance awareness culture and cybersecurity readiness**
- **Reduce the time to detect an intrusion, respond to it, and restore operations**
- **Fortify your organization's security posture**
- **Solve complex cybersecurity problems using advanced tools**
- **Improve your ability to identify and remediate vulnerabilities**
- **Mitigate risk and impact to your organization**

Your best cyber defense requires **everyone** in your organization to be threat-aware and cyber-ready. **Only SANS** delivers the security training, certification, and awareness programs that **transform your people into your protection**.

SANS builds experts who outsmart cyber threats.

Real Expertise
Master practitioners who turn their knowledge into your expertise.

Real Skills
The real-world skills you need to protect your business in real time.

Real Protection
Employees empowered to keep your organization secure.

GIAC
The Highest Standard in Cybersecurity Certification

CYBERLIVE

Introducing CyberLive

Raising the bar even higher on GIAC Certifications

CyberLive brings real-world, virtual machine testing directly to cybersecurity practitioners, helping them prove their skills, abilities, and understanding. All in real-time.

Learn more at **giac.org/cyberlive**

"Increasingly, the hands-on portion is important to measure the abilities of cyber professionals."

– Ben Boyle
GXPN, GDAT, GWAPT

GIAC develops and administers premier, professional cybersecurity certifications. Each certification aligns with SANS training and ensures mastery in critical, specialized InfoSec domains – providing the highest, most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world.

Learn more at GIAC.ORG

GIAC
CERTIFICATIONS

What's New at SANS?

SANS course authors develop the most up-to-date and relevant content available.

Offensive Operations

SEC446: Hardware Assisted Hacking

Tightly packed with tips, techniques, and hands-on procedures, this course teaches the foundations of both hardware theory and hardware practice, as well as how they relate to hardware and software security.

SEC565: Red Team Operations and Adversary Emulation

This course prepares operators to emulate adversaries and threats in a professional manner to test a target organization's people, processes, and technology from a holistic perspective.

SEC568: Combating Supply Chain Attacks with Product Security Testing

This course is a practical on-ramp into the world of product security testing and risk analysis for introducing desktop, mobile, proprietary protocols, and hardware devices into your environment.

SEC598: Security Automation for Offense, Defense, and Cloud

Learn how to break down an organization's security issues and define solutions to locally automate secure configurations, set a desired state configuration, deploy infrastructure as code in different environments, and detect and respond to security incidents in an automated manner.

SEC670: Red Teaming Tools - Developing Windows Implants, Shellcode, Command and Control

Learn the essential building blocks for developing custom offensive tools through required programming, APIs used, and mitigations for techniques.

Cybersecurity Leadership

MGT553: Cyber Incident Management

Go beyond technical analysis and response activities and learn how to effectively manage and lead people and processes for cyber incidents.

Cyber Defense & Blue Team Ops

SEC673: Advanced Information Security Automation with Python

This course will teach you the advanced programming concepts you need to make your code faster, more efficient, and easier to develop and maintain. You will learn how to automate common networking and desktop applications using Python objects.

Cloud Security

SEC388: Introduction to Cloud Computing and Security

This course is designed for those in a decision-making or hands-on role whose organization is either planning to move to or already operating in the cloud.

SEC549: Enterprise Cloud Security Architecture

Learn how to design and build an enterprise cloud security architecture in cloud-first and hybrid environments.

ICS Security

ICS418: ICS Security Essentials for Managers

This course will help you learn to manage the people, processes, and technologies necessary to create and sustain lasting ICS cyber risk programs while promoting a culture of safety, reliability, and security.

Cyber Ranges

New Netwars Core Version 8!

SANS Netwars Core Version 8 is a new and exciting Cyber Range from SANS. Featuring AWS cloud content and more, it has fun, story-driven challenges to keep you engaged in learning and practicing your essential cybersecurity skills. We've also eliminated the need to download large VM files locally — 100% browser-based challenges!

DFIR & Threat Hunting

FOR528: Ransomware for Incident Responders

This course uses deftly devised, real-world attacks and their subsequent forensic artifacts to provide the analyst with everything needed to respond to ransomware incidents.

FOR532: Enterprise Memory Forensics In-Depth

This course focuses on memory forensics from acquisition to detailed analysis, from analyzing one machine to many machines all at once. It covers Windows, Mac, and Linux memory forensics as well as cloud memory acquisition.

FOR589: Cybercrime Intelligence

Learn to hunt for Criminal Intelligence (CRIMINT) on the Dark Web and analyze criminal "on-chain" financial transactions using Blockchain Intelligence (BLOCKINT) tools, as well as how to identify, analyze, and extract cryptocurrency artifacts from criminal devices in computer and mobile forensics investigations.

FOR577: LINUX Incident Response & Analysis

Linux powers a vast range of business-critical systems across the globe. From webservers to database platforms, to network hardware to security appliances, Linux can often be found "under the hood" making sure the system just keeps working. This course gives incident responders and forensic investigators the knowledge they need to understand how the systems work, how attackers compromise environments and how to respond and investigate in an effective manner.

SANS OnDemand

OnDemand 2.0

The new SANS OnDemand experience offers ultimate flexibility and is packed with enhanced features to build your cybersecurity skills at your own pace. Take it for a test drive with one of our free course demos.
www.sans.org/course-preview

GIAC Certifications

GIAC iOS and MacOS Examiner (GIME)

The GIME certification validates a practitioner's knowledge of Mac and iOS computer forensic analysis and incident response skills. GIME-certified professionals are well-versed in traditional investigations as well as intrusion analysis scenarios for compromised Apple devices.

GIAC Cloud Forensics Responder (GCFR)

The GCFR certification validates a practitioner's ability to track and respond to incidents across the three major cloud providers. GCFR-certified professionals are well-versed in the log collection and interpretation skills needed to manage rapidly changing enterprise cloud environments.

GIAC Cloud Threat Detection (GCTD)

The GCTD certification validates a practitioner's ability to detect and investigate suspicious activity in cloud infrastructure. GCTD-certified professionals are experienced in cyber threat intelligence, secure cloud configuration, and other practices needed to defend cloud solutions and services.

Cyber Live

The New Mark of Hands-On Cybersecurity Skills

Cybersecurity professionals need discipline-specific certifications and practical testing that validate their knowledge and hands-on skills. GIAC recognized this industry-wide need and developed CyberLive—hands-on, real-world practical testing—to fill the gaps in the market.

sans.org/mlp/new-sans-courses

SANS INSTITUTE

The most trusted resource for information security training, cybersecurity certifications, and research.

The Highest Standard in Cybersecurity Education

Our instructors are experienced practitioners who also excel in mentoring others. They are respected leaders in cyber who share research, tools, and incident analysis with the world, and bring practical, collaborative expertise to our community. Along with our students and community contributors, these dynamic instructors make SANS the engaging, high-quality educational organization that it is.

"I have taken numerous courses over my career and many were online. Nothing, including expensive college-level courses, were on the same level as SANS training. It's dense, rich, and immediately applicable. If the student takes what they have learned into their workplace, they will immediately be able to distinguish themselves. I'm already looking forward to my next SANS training opportunity, and I highly recommend it to others."
—Dave Brock, **Lytx Inc.**

150+
extraordinary SANS-certified instructors

Multiple Training Formats

Find the option that best fits your schedule, budget, and preferred learning style.

OnDemand
Train anywhere and anytime with four months of online access. Receive training from the same top-notch SANS instructors who teach at our live training events – bringing the true SANS experience right to you. Enjoy access to repeatable hands-on labs and premium live subject-matter-expert support.

Live Online
Avoid travel and attend scheduled live interactive streaming sessions direct from your SANS instructor, featuring many of the activities that SANS students love at In-Person training events.

In-Person
Experience SANS courses taught by world-renowned faculty in select locations, featuring hands-on labs to practice your skills in a focused, immersive environment without distractions, plus opportunities to network with fellow cybersecurity professionals.

Private Courses
Train with your colleagues at your organization's location and freely discuss issues and objectives specific to your environment.

Summits
Take part in one or two-day special SANS events featuring expert presentations covering a single topic of interest to the cybersecurity community.

Ranges
Prepare for real-world IT and cybersecurity roles with interactive learning scenarios that build skills which can be applied immediately on the job.

If you're new to SANS or unsure of the subject area or skill level to select for your next training course, SANS offers free one-hour course previews via our OnDemand platform.
Preview our courses at sans.org/demo

Technology, Attackers, and Cyber Defense Techniques Change Rapidly – Sometimes in Days

Our courses, labs, content, and certifications deliver on the most advanced teaching techniques, labs, content, and certifications that are TRUSTED by organizations worldwide.

- **EXPERTS:** Trained by experts who undergo years of training and teaching mastery. Only the best of the best are invited to teach.
- **CONTENT:** Technology, attacker techniques, and defensive capabilities are changing rapidly. SANS course content is continually updated.
- **SKILLS:** Real-world labs are architected, engineered, written, and tested – continuously.
- **TRAINING VALIDATION:** GIAC certifications keep pace with continually emerging content and skills, ensuring for employers that their people can perform in the latest threat environment.

"SANS is trusted. SANS delivers. SANS never accepts anything less than the best techniques, capabilities, and instructors worldwide. It takes a lot for SANS to maintain the 'Most Trusted Source of Cyber Security Training, Certification, and Research' worldwide. We won't lie. It is hard. We deliver that promise. We know your organization depends on it and we take our jobs seriously. And we love knowing what we do matters."

—Rob Lee, Chief Curriculum Director at SANS

The SANS Promise

You will be able to use the skills you've learned in our training and programs immediately in your work.

137,000+
GIAC Certifications Issued

30+
Countries Featuring SANS Training Events

40,000+
SANS Students Per Year

85+
Cybersecurity Courses

40+
GIAC Certifications

150+
Certified Instructors

NICE Framework

The NICE framework provides a common language to speak about cyber roles, jobs and tasks/skills/knowledge (TSKs) in cybersecurity. The U.S. Department of Commerce created this framework to enable workforce continuity.

Use this as a blueprint to organize cybersecurity work into Categories, Specialty Areas, Work Roles Tasks, and Knowledge, Skills and Abilities (KSAs). **www.nist.gov/itl/applied-cybersecurity/nice**

Analyze (AN)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Threat Analysis (TWA)	Threat/Warning Analyst	FOR578 (GCTI) FOR589 SEC504 (GCIH) FOR610 (GREM) FOR532 FOR710 FOR572 (GNFA) FOR577
Exploitation Analysis (EXP)	Exploitation Analyst	SEC560 (GPEN) SEC661 SEC660 (GXPN) SEC542 (GWAPT) SEC760
All-Source Analysis (ASA)	All-Source Analyst	FOR578 (GCTI) FOR589 SEC504 (GCIH) FOR509 FOR532 FOR577
	Mission Assessment Specialist	SEC504 (GCIH) FOR578 (GCTI) SEC560 (GPEN) FOR532 SEC588 (GCPN) FOR589
Targets (TGT)	Target Developer	SEC560 (GPEN) SEC699 SEC542 (GWAPT) FOR509 (GCFR) SEC565 FOR518 (GIME) SEC588 (GCPN) FOR532 SEC660 (GXPN) FOR585 (GASF) SEC760 FOR589 SEC661 FOR572 (GNFA) SEC599 (GDAT)
	Target Network Analyst	FOR578 (GCTI) FOR589 SEC504 (GCIH) FOR572 (GNFA) SEC560 (GPEN) FOR532

Collect and Operate (CO)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Collection Operations (CLO)	All Source-Collection Manager	FOR498 (GBFA) FOR532 FOR578 (GCTI) FOR589 FOR508 (GCFA) FOR608 FOR509 (GCFR) FOR577 FOR518 (GIME)
	All Source-Collection Requirements Manager	FOR498 (GBFA) FOR532 FOR578 (GCTI) FOR589 FOR508 (GCFA) FOR509 (GCFR)
Cyber Operational Planning (OPL)	Cyber Intel Planner	FOR532 SEC504 (GCIH) FOR589 FOR578 (GCTI)
	Cyber Ops Planner	SEC565 SEC699 SEC560 (GPEN) SEC599 (GDAT) SEC542 (GWAPT) SEC467 SEC588 (GCPN) SEC556 SEC660 (GXPN) FOR577
	Partner Integration Planner	SEC565, SEC699 FOR589 SEC599 (GDAT) FOR578 (GCTI) FOR532
Cyber Operations (OPS)	Cyber Operator	FOR508 (GCFA) SEC560 (GPEN) FOR528 SEC660 (GXPN) FOR532 SEC556 FOR572 (GNFA) SEC467 FOR578 (GCTI) SEC573 (GPYC) FOR589 FOR577 FOR608

Industrial Control Systems (NICE 2020)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Operations Technology Engineering	Process Control Engineer/Instrument & Control Engineer	ICS410 (GICSP) ICS612
	ICS/SCADA Security Engineer	ICS410 (GICSP) ICS515 (GRID) ICS418
	ICS/OT Systems Engineer	ICS410 (GICSP) ICS515 (GRID) ICS418 ICS612
OT Security Operations Center	OT SOC Operator	ICS410 (GICSP) ICS418 ICS515 (GRID)

Oversee and Govern (OV)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	LDR523 SEC403 SEC402
	Privacy Officer/ Privacy Compliance Manager	SEC301 (GISF) ICS456 (GCIP) LDR512 (GSLC) SEC504 (GCIH)
Training, Education and Awareness (TEA)	Cyber Instructional Curriculum Developer	SEC401 (GSEC) LDR521 LDR433 (SSAP) SEC504 (GCIH)
	Cyber Instructor	SEC401 (GSEC), SEC501 (GCED), SEC504 (GCIH), SEC403, SEC402
	Security Awareness & Communications Manager	LDR433 (SSAP) SEC402 LDR512 (GSLC) SEC403 LDR521
Cybersecurity Management (MGT)	Information Systems Security Manager	LDR512 (GSLC) LDR551 (GSOM) LDR514 (GSTRT) SEC504 (GCIH) LDR520 SEC488 (GCLD) LDR521
	Communications Security (COMSEC) Manager	SEC301 (GISF) LDR512 (GSLC)
Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	LDR512 (GSLC) LDR514 (GSTRT) LDR521
	Cyber Policy and Strategy Planner	LDR512 (GSLC) LDR514 (GSTRT) LDR521
Executive Cyber Leadership (EXL)	Executive Cyber Leadership	LDR512 (GSLC) LDR514 (GSTRT) LDR521
Program/Project Management (PMA) and Acquisition	Program Manager	LDR512 (GSLC) LDR520 LDR514 (GSTRT) LDR521
	IT Project Manager	LDR512 (GSLC) LDR520 MGT525 (GCPM) LDR521 LDR514 (GSTRT)
	Product Support Manager	LDR512 (GSLC) MGT525 (GCPM)
	IT Investment/ Portfolio Manager	SEC401 (GSEC) LDR512 (GSLC) SEC504 (GCIH)
	IT Program Auditor	AUD507 (GSNA) SEC402 SEC460 (GEVA) SEC403

Securely Provision (SP)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Risk Management (RSK)	Authorizing Official/ Designating Representative	SEC301 (GISF) SEC402 LDR512 (GSLC) SEC403 LDR415
	Security Control Assessor	SEC460 (GEVA) SEC401 (GSEC) AUD507 (GSNA) SEC510 (GCPS) SEC560 (GPEN) SEC566 (GCCC) SEC542 (GWAPT) MGT516 SEC588 (GCPN)
Software Development (DEV)	Software Developer	SEC522 (GWEB) SEC542 (GWAPT) SEC540 (GCSA) SEC549
	Secure Software Assessor	SEC542 (GWAPT) SEC540 (GCSA) SEC510 (GCPS) SEC573 (GPYC) SEC522 (GWEB) SEC549
Systems Architecture (ARC)	Enterprise Architect	SEC530 (GDSA) SEC540 (GCSA) SEC510 (GPCS)
	Security Architect	SEC488 (GCLD) SEC530 (GDSA) SEC511 (GMON) SEC510 (GPCS)
Technology R&D (TRD)	Research & Development Specialist	SEC568 SEC522 (GWEB) SEC573 (GPYC) SEC510 (GPCS) SEC540 (GCSA)
Systems Requirements Planning (SRP)	Systems Requirements Planner	MGT525 (GCPM) SEC402 SEC403
Test and Evaluation (TST)	System Testing & Evaluation Specialist	SEC460 (GEVA) SEC556 SEC568 AUD507 (GSNA), SEC560 (GPEN) SEC402 SEC588 (GCPN) SEC403 SEC542 (GWAPT)
Systems Development (SYS)	Information Systems Security Developer	SEC540 (GCSA) SEC510 (GPCS) SEC522 (GWEB) SEC542 (GWAPT)
	Systems Developer	SEC540 (GCSA) SEC542 (GWAPT) SEC522 (GWEB)

Investigate (IN)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Cyber Investigation (INV)	Cyber Crime Investigator	FOR498 (GBFA) FOR608 FOR308 FOR585 (GASF) FOR500 (GCFE) FOR518 (GIME), FOR508 (GCFA) FOR578 (GCTI) FOR528 FOR589 FOR532 FOR610 (GREM) FOR572 (GNFA) FOR710 FOR509 (GCFR)
Digital Forensics (FOR)	Law Enforcement/ CounterIntelligence Forensics Analyst	FOR308 FOR509 (GCFR) FOR508 (GCFA) FOR518 (GIME) FOR528 FOR589 FOR532 FOR608 FOR498 (GBFA) FOR710 FOR572 (GNFA) FOR308 FOR610 (GREM) SEC573 (GPYC) FOR578 (GCTI)
	Cyber Defense Forensics Analyst	FOR500 (GCFE) FOR608 FOR308 FOR518 (GIME) FOR498 (GBFA) FOR572 (GNFA) FOR508 (GCFA), FOR585 (GASF) FOR509 (GCFR) FOR610 (GREM) FOR528 FOR710 FOR532 SEC573 (GPYC) FOR589

Protect and Defend (PR)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst	SEC401 (GSEC) SEC586 SEC450 (GSOC) FOR532 SEC504 (GCIH) FOR578 (GCTI) SEC501 (GCED) FOR589 SEC503 (GCIA) FOR610 (GREM) SEC511 (GMON) FOR710 SEC573 (GPYC) SEC541 (GCTD)
Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	SEC568 SEC511 (GMON) SEC401 (GSEC) SEC586 SEC450 (GSOC) SEC460 (GEVA) SEC501 (GCED)
Incident Response (CIR)	Cyber Defense Incident Responder	SEC504 (GCIH) FOR532 FOR508 (GCFA) FOR589 FOR572 (GNFA) FOR710 FOR509 (GCFR) ICS515 (GRID) FOR608 SEC541 (GCTD) FOR610 (GREM) SEC586 FOR518 (GIME) FOR532 FOR528 FOR577 FOR578 (GCTI)
Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	SEC460 (GEVA) SEC556 SEC542 (GWAPT) SEC660 (GXPN) SEC588 (GCPN) LDR516 SEC560 (GPEN)
	Pen Tester	SEC560 (GPEN) SEC588 (GCPN) SEC542 (GWAPT) SEC660 (GXPN) SEC556 SEC467
	Adversary Emulation Specialist/Red Teamer	SEC565 SEC504 (GCIH) SEC599 (GDAT) SEC556 SEC699 SEC660 (GXPN) SEC670 SEC760

Operate and Maintain (OM)

NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)
Data Administration (DTA)	Database Administrator	SEC401 (GSEC) FOR498 (GBFA) FOR308
	Data Analyst	SEC401 (GSEC) FOR498 (GBFA) SEC573 (GPYC) FOR585 (GASF) FOR578 (GCTI) FOR518 GIME) SEC595 FOR308
Knowledge Management (KMG)	Knowledge Manager	SEC301 (GISF) FOR498 (GBFA) SEC402 FOR585 (GASF) SEC403 FOR518 GIME) FOR308
Customer Service and Technical Support (STS)	Technical Support Specialist	SEC401 (GSEC) SEC505 (GCWN) SEC504 (GCIH)
Network Services (NET)	Network Operations Specialist	SEC401 (GSEC) SEC501 (GCED) SEC555 (GCDA)
Systems Administration (ADM)	System Administrator	SEC401 (GSEC) FOR308 SEC505 (GCWN) FOR498 (GBFA) SEC586
Systems Analysis (ANA)	Systems Security Analyst	SEC401 (GSEC) SEC586 SEC488 (GCLD) FOR308 SEC504 (GCIH) FOR585 (GASF) AUD507 (GSNA) FOR518 GIME) SEC505 (GCWN)

SANS Training Roadmap

Topic | Course Code | GIAC Certification

Essentials — ICS410 **ICS/SCADA Security Essentials** | GICSP — Course Title

Baseline Skills

NEW TO CYBERSECURITY | COMPUTERS, TECHNOLOGY, AND SECURITY

COMPUTER & IT FUNDAMENTALS	SEC275 **Foundations: Computers, Technology & Security** | GFACT
CYBERSECURITY FUNDAMENTALS	SEC301 **Introduction to Cyber Security** | GISF

These entry-level courses cover a wide spectrum of security topics and are liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes these course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management.

CORE TECHNIQUES | PREVENT, DEFEND, MAINTAIN

Every Security Professional Should Know

SECURITY ESSENTIALS	SEC401 **Security Essentials: Network, Endpoint, and Cloud** | GSEC

Whether you are new to information security or a seasoned practitioner with a specialized focus, SEC401 will provide the essential information security skills and techniques you need to protect and secure your critical information and technology assets, whether on-premise or in the cloud.

BLUE TEAM	SEC450 **Blue Team Fundamentals: Security Operations and Analysis** | GSOC
ATTACKER TECHNIQUES	SEC504 **Hacker Tools, Techniques, and Incident Handling** | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense in depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

TECHNICAL TRAINING FROM SANS SECURITY AWARENESS

Security Essentials for IT Administrators

Protecting your organization from cyber threats requires continuous investment in skills development to stay ahead of any emerging threats. This short-form computer-based training provides technical teams with a deep understanding of evolving security concepts with a learning progression suited to their skillset.

FORENSICS ESSENTIALS

Every Forensics and Incident Response Professional Should Know

FORENSICS ESSENTIALS	FOR308 **Digital Forensics Essentials**
BATTLEFIELD FORENSICS & DATA ACQUISITION	FOR498 **Battlefield Forensics & Data Acquisition** | GBFA

CLOUD SECURITY ESSENTIALS

Every Cloud Security Professional Should Know

ESSENTIALS	SEC488 **Cloud Security Essentials** | GCLD

If you are new to cybersecurity or looking to up-skill, cloud security essentials is a requirement for today's organizations. This course provides the basic knowledge required to introduce students to the cloud security industry, as well as in-depth, hands-on practice in labs.

CLOUD FUNDAMENTALS

Built for professionals who need to be conversant in basic cloud security concepts, principles, and terms, but who are not responsible for hands-on cloud activities.

INTRODUCTION	SEC388 **Intro to Cloud Computing and Security**

TECHNICAL TRAINING FROM SANS SECURITY AWARENESS

Developer Secure Code Training

Educate everyone involved in the software development process including developers, architects, managers, testers, business owners, and partners with role-focused training that ensures your team can properly build defensible applications from the start.

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Professional Should Know

ESSENTIALS	ICS410 **ICS/SCADA Security Essentials** | GICSP

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Manager Should Know

ESSENTIALS	ICS418 **ICS Security Essentials for Managers**

FOUNDATIONAL LEADERSHIP

Every Cybersecurity Manager Should Know

CISSP® TRAINING	LDR414 **SANS Training Program for CISSP® Certification** | GISP
SECURITY AWARENESS	LDR433 **Managing Human Risk** | SSAP

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those leaders will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

CYBER RANGES

CTF & TRIVIA	Bootup CTF
SKILLS ASSESSMENT & PRACTICAL APPLICATION	NetWars Core

These cyber range offerings cover the broadest range of topics and are meant for all InfoSec professionals at all levels.

Focused Job Roles

DESIGN, DETECTION, AND DEFENSIVE CONTROLS

Focused Cyber Defense Skills

ADVANCED GENERALIST	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
MONITORING & OPERATIONS	SEC511 **Continuous Monitoring and Security Operations** | GMON
SECURITY ARCHITECTURE	SEC530 **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise** | GDSA

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Open-Source Intelligence

OSINT	SEC497 **Practical Open-Source Intelligence (OSINT)** | GOSI

OFFENSIVE OPERATIONS | VULNERABILITY ANALYSIS, PENETRATION TESTING

Every Offensive Professional Should Know

NETWORK PEN TESTING	SEC560 **Enterprise Penetration Testing** | GPEN
WEB APPS	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT
VULNERABILITY ASSESSMENT	SEC460 **Enterprise and Cloud | Threat and Vulnerability Assessment** | GEVA

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of Red Team/Blue Team deployments is that finding vulnerabilities requires different ways of thinking and different tools. Offensive skills are essential for cybersecurity professionals to improve their defenses.

INCIDENT RESPONSE & THREAT HUNTING | HOST & NETWORK FORENSICS

Every Forensics and Incident Response Professional Should Know

ENDPOINT FORENSICS	FOR500 **Windows Forensic Analysis** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA FOR532 **Enterprise Memory Forensics In-Depth** FOR577: **LINUX Incident Response & Analysis** FOR608 **Enterprise-Class Incident Response & Threat Hunting**
NETWORK FORENSICS	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA

Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

CORE CLOUD SECURITY

Preparation for More Focused Job Functions

PUBLIC CLOUD	SEC510 **Public Cloud Security: AWS, Azure, and GCP** | GPCS
AUTOMATION & DEVSECOPS	SEC540 **Cloud Security and DevSecOps Automation** | GCSA
MONITORING & DETECTION	SEC541 **Cloud Security Attacker Techniques, Monitoring & Threat Detection** | GCTD
ARCHITECTURE	SEC549 **Enterprise Cloud Security Architecture**

With the massive global shift to the cloud, it becomes more critical for every organization to have experts who understand the security risks and benefits that come with public cloud use, how to navigate and take full advantage of multicloud environments, and how to incorporate security from the start of all development projects.

INDUSTRIAL CONTROL SYSTEMS SECURITY

Every ICS Security Professional Should Know

ICS DEFENSE & RESPONSE	ICS515 **ICS Visibility, Detection, and Response** | GRID
ICS ADVANCED SECURITY	ICS612 **ICS Cybersecurity In-Depth**
NERC Protection	
NERC SECURITY ESSENTIALS	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

CORE LEADERSHIP

Transformational Cybersecurity Leader

TECHNOLOGY LEADERSHIP	LDR512 **Security Leadership Essentials for Managers** | GSLC
SECURITY STRATEGY	LDR514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
SECURITY CULTURE	LDR521 **Leading Cybersecurity Change: Building a Security-Based Culture**

Operational Cybersecurity Executive

VULNERABILITY MANAGEMENT	LDR516 **Building and Leading Vulnerability Management Programs**
SOC	LDR551 **Building and Leading Security Operations Centers** | GSOM
FRAMEWORKS & CONTROLS	SEC566 **Implementing and Auditing Security Frameworks & Controls** | GCCC

CYBER RANGES

CYBER DEFENSE	NetWars Cyber Defense
DIGITAL FORENSICS & INCIDENT RESPONSE	NetWars DFIR
INDUSTRIAL CONTROL SYSTEMS	NetWars ICS
POWER GENERATION AND DISTRIBUTION	NetWars GRID

SANS offers specialized versions of NetWars for more specific job roles. These cyber ranges dive deeper into the respective topics and help advance your career with situation-based challenges and scenarios rooted in real-life events.

Specific Skills, Specialized Roles

ADVANCED CYBER DEFENSE | HARDEN SPECIFIC DEFENSES

Platform-Focused

WINDOWS/ POWERSHELL	SEC505 **Securing Windows and PowerShell Automation** | GCWN

Topic-Focused

TRAFFIC ANALYSIS	SEC503 **Network Monitoring and Threat Detection In-Depth** | GCIA
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA
POWERSHELL	SEC586 **Security Automation with PowerShell**
PYTHON CODING	SEC573 **Automating Information Security with Python** | GPYC SEC673 **Advanced Information Security Automation with Python**
DATA SCIENCE	SEC595 **Applied Data Science and Machine Learning for Cybersecurity Professionals**

Open-Source Intelligence

OSINT	SEC587 **Advanced Open-Source Intelligence (OSINT) Gathering & Analysis**

SPECIALIZED OFFENSIVE OPERATIONS | FOCUSED TECHNIQUES & AREAS

Network, Web, and Cloud

EXPLOIT DEVELOPMENT	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN SEC661 **ARM Exploit Development** SEC760 **Advanced Exploit Development for Penetration Testers**
CLOUD PEN TEST	SEC588 **Cloud Penetration Testing** | GCPN

Specialized Penetration Testing

SOCIAL ENGINEERING	SEC467 **Social Engineering for Security Professionals**
BLOCKCHAIN	SEC554 **Blockchain and Smart Contract Security**
RED TEAM	SEC565 **Red Team Operations and Adversary Emulation** SEC670 **Red Teaming Tools - Developing Windows Implants, Shellcode, Command and Control**
MOBILE	SEC575 **iOS and Android Application Security Analysis and Penetration Testing** | GMOB
PRODUCT SECURITY	SEC568 **Combating Supply Chain Attacks with Product Security Testing**
PEN TEST	SEC580 **Metasploit for Enterprise Penetration Testing**
WIRELESS	SEC556 **IoT Penetration Testing** SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN

Purple Team

ADVERSARY EMULATION	SEC598 **Security Automation for Offense, Defense, and Cloud** SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT SEC699 **Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection**

DIGITAL FORENSICS, MALWARE ANALYSIS, & THREAT INTELLIGENCE | SPECIALIZED INVESTIGATIVE SKILLS

Specialization

CLOUD FORENSICS	FOR509 **Enterprise Cloud Forensics & Incident Response** | GCFR
RANSOMWARE	FOR528 **Ransomware for Incident Responders**
MALWARE ANALYSIS	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM FOR710 **Reverse-Engineering Malware: Advanced Code Analysis**

Threat Intelligence

CYBER THREAT INTELLIGENCE	FOR578 **Cyber Threat Intelligence** | GCTI FOR589 **Cybercrime Intelligence**

Digital Forensics & Media Exploitation

SMARTPHONES	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
MAC FORENSICS	FOR518 **Mac and iOS Forensic Analysis and Incident Response** | GIME
LINUX FORENSICS	FOR577 **Linux Incident Response & Analysis**

SPECIALIZATION IN CLOUD SECURITY

Specialization for Advanced Skills & Roles

APPLICATION SECURITY	SEC522 **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB
CLOUD PEN TEST	SEC588 **Cloud Penetration Testing** | GCPN
CLOUD FORENSICS	FOR509 **Enterprise Cloud Forensics and Incident Response** | GCFR
DESIGN & IMPLEMENTATION	MGT520 **Leading Cloud Security Design and Implementation**

Learning how to convert traditional cybersecurity skills into the nuances of cloud security is a necessity for proper monitoring, detection, testing, and defense.

TECHNICAL TRAINING FROM SANS SECURITY AWARENESS

ICS Engineer Training

Help protect critical systems by reinforcing the behavior your engineers, system operators and others who interact with ICS environments require to prevent, identify and respond to cyber incidents.

LEADERSHIP SPECIALIZATIONS

Management Specialization

AUDIT & MONITOR	AUD507 **Auditing Systems, Applications, and the Cloud** | GSNA
DESIGN & IMPLEMENTATION	LDR520 **Leading Cloud Security Design and Implementation**
LAW, DATA PRIVACY, & IP	LDR523 **Cybersecurity Law, Data Privacy, & Intellectual Property**
PROJECT MANAGEMENT	MGT525 **Managing Cybersecurity Initiatives & Effective Communication** | GCPM
INCIDENT RESPONSE	LDR553 **Cyber Incident Management**

MANAGE HUMAN RISK WITH TRAINING FROM SANS SECURITY AWARENESS

EndUser Awareness Training

Computer-based end-user training is built from a curated selection of the most pressing risk and compliance topics to address employee security behaviors. This engaging, modular, and multilingual suite of content reduces training fatigue and increases comprehension by tailoring your security awareness training program to the role- and industry-based issues relevant to your organization.

SANS CURRICULUM FOCUS AREA

NEW2CYBER
Cybersecurity and IT Essentials

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of skills to understand how attackers operate, implement defense in depth, and respond to incidents to mitigate risks and properly secure systems.

To be secure, you should set a high bar for the baseline set of skills in your organization. SANS New2Cyber courses will teach you to:

- Adopt techniques that focus on high-priority security problems within your organization
- Build a solid foundation of core policies and practices to enable you and your security teams to practice proper incident response
- Deploy a toolbox of strategies and techniques to help defend an enterprise from every angle
- Identify the latest attack vectors and implement controls to prevent and detect them
- Use strategies and tools to detect attacks
- Develop effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand
- Implement a comprehensive security program focused on preventing, detecting, and responding to attacks
- Build an internal security roadmap that can scale today and into the future

Enhance your training with:

- Cyber Defense Netwars **sans.org/netwars**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs **sans.edu**
- Free Resources **sans.org/free**

"This training has given me a great overview of everything security related...showing you such a broad amount of information that you will use to determine security issues you may not have considered before."

—Frank Perrilli, **IESO**

New2Cyber Job Roles:

- Security Analyst
- Digital Forensic Analyst
- Security Engineer
- Technical Manager
- Auditor

SEC275: Foundations: Computers, Technology, & Security

6 Day Program	38 CPEs	Laptop Required

What You Will Learn

The course provides exactly what you need to go from zero technical and security knowledge to a level of sufficient theoretical understanding and applied practical skills that will enable you to speak the same language as industry professionals. Students will develop fundamental skills and knowledge in key IT subject areas such as:

- Computer Components & Concepts
- Operating Systems & Virtualization
- Linux
- The Web
- Networking Fundamentals
- Servers and Services
- Practical Programming Concepts
- Structured Query Language – SQL
  - Basic statements
  - MySQL Joins
  - Operators
  - Database Administration
- Windows Foundations
- Advanced Computer Hardware
- Security Concepts
- Offensive Security Concepts
- Network and Computer Infiltration

What is included with SANS Foundations?

- Over 120 hours of curated content
- Hands-on labs experience
- Quizzes to consolidate learning outcomes
- Training by world-renowned experts
- Engaging 4K video content Proctored final exam delivered by GIAC

SANS Foundations is the best course available to learn the core knowledge and develop practical skills in computers, technology, and security foundations that are needed to kickstart a career in cybersecurity. The course features a comprehensive variety of innovative, hands-on labs, and practical exercises that go far beyond what is offered in any other foundational course in cybersecurity. These labs are developed by leading subject-matter experts, drawing on the latest technology, techniques, and concepts in cybersecurity.

The course provides students with the practical learning and key skills to empower future cybersecurity learning and professional development.

Author Statement

"Cybersecurity is an exciting and fast-growing field, and it must be at a time when the global talent shortage continues to grow, and both the number of threats and malicious actors continues to rise. While job roles in application security, reverse malware engineering, and threat hunting may sound enticing, practitioners in these roles all had to start by learning the basics. There are essential computing and technology skills that all successful cybersecurity professionals first learn that serve as the baseline for careers and future education in the field. SANS Foundations serves as the launch of an IT education and career or can fill in the gaps by introducing students to these fundamentals.

"By providing students with minimal technology proficiency and the ability to recognize key terms and develop competencies with tools and systems in a comfortable atmosphere, they are prepared for future skills development. Whether you are a career seeker, self-driven learner, or in an immersive training program, SANS Foundations will provide you with the core IT and computer knowledge and abilities integral to a future career in cybersecurity.

"SANS Foundations teaches students a broad array of fundamental knowledge in areas such as computer hardware, networking, Linux, operating systems, data storage, and much more. The skills gained are applicable to everyone in an IT, computing, or security role. Practical skills are key to success in cybersecurity, and thus there are over 100 labs and hands-on exercises in the course to kickstart your cybersecurity journey. The course will set you up for entering the workforce and be ready to continue learning in more advanced, technical areas across cybersecurity."

—James Lyne, SANS Chief Technology Officer

"Great content and learning, very positive. Really a great way to step into cybersecurity and build skills day to day."

"The labs were a great way to practice and learn the new commands, I loved them. Another great tool were the videos with execution examples."

Certification: GIAC Foundational Cybersecurity Technologies (GFACT)
giac.org/gfact

FOR308: Digital Forensics Essentials

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Effectively use digital forensics methodologies
- Ask the right questions in relation to digital evidence
- Understand how to conduct digital forensics engagements compliant with acceptable practice standards
- Develop and maintain a digital forensics capacity
- Understand incident response processes and procedures and when to call on the team
- Describe potential data recovery options in relation to deleted data
- Identify when digital forensics may be useful and understand how to escalate to an investigator
- If required, use the results of your digital forensics in court

Course Topics

- Introduction to digital investigation and evidence
- Where to find digital evidence
- Digital forensics principles
- Digital forensics and incident response processes
- Digital forensics acquisition
- Digital forensics examination and analysis
- Presenting your findings
- Understanding digital forensic reports
- Challenges in digital forensics
- Building and developing digital forensics capacity
- Legality of digital evidence
- How to testify in court

More than half of jobs in the modern world use a computer. The vast majority of people aged 18-30 are 'digitally fluent'; accustomed to using smartphones, smart TVs, tablets and home assistants, in addition to laptops and computers, simply as part of everyday life. Yet, how many of these users actually understand what's going on under the hood? Do you know what your computer or smartphone can tell someone about you? Do you know how easy it might be for someone to access and exploit that data? Are you fed up with not understanding what technical people are talking about when it comes to computers and files, data and metadata? Do you know what actually happens when a file is deleted? Do you want to know more about Digital Forensics and Incident Response? If you answered 'yes' to any of the above, this course is for you. This is an introductory course aimed at people from non-technical backgrounds, to give an understanding, in layman's terms, of how files are stored on a computer or smartphone. It explains what Digital Forensics and Incident Response are and the art of the possible when professionals in these fields are given possession of a device.

This course is intended to be a starting point in the SANS catalogue and provide a grounding in knowledge, from which other, more in-depth, courses will expand.

IT'S NOT JUST ABOUT USING TOOLS AND PUSHING BUTTONS

Digital forensics has evolved from methods and techniques that were used by detectives in the 1990's to get digital evidence from computers, into a complex and comprehensive discipline. The sheer volume of digital devices and data that we could use in investigative ways meant that digital forensics was no longer just being used by police detectives. It was now being used as a full forensic science. It was being used in civil legal processes. It was being used in the military and intelligence services to gather intelligence and actionable data. It was being used to identify how people use and mis-use devices. It was being used to identify how information systems and networks were being compromised and how to better protect them. And that is just some of the current uses of digital forensics.

However digital forensics and incident response are still largely misunderstood outside of a very small and niche community, despite their uses in the much broader commercial, information security, legal, military, intelligence and law enforcement communities.

Many digital forensics and incident response courses focus on the techniques and methods used in these fields, which often do not address the core principles: what digital forensics and incident response are and how to actually make use of digital investigations and digital evidence. This course provides that. It serves to educate the users and potential users of digital forensics and incident response teams, so that they better understand what these teams do and how their services can be better leveraged. Such users include executives, managers, regulators, legal practitioners, military and intelligence operators and investigators. In addition, not only does this course serve as a foundation for prospective digital forensics practitioners and incident responders, but it also fills in the gaps in fundamental understanding for existing digital forensics practitioners who are looking to take their capabilities to a whole new level.

"FOR308 is packed with technical information and covers aspects necessary for those taking their first steps in the digital forensics as well as those who think about leading teams in the field. An overall good balance of theory to practice, delivered in a very professional manner."

— Wiktor Kardacki, **6point5**

SEC301: Introduction to Cyber Security

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) for prioritization of critical security resources
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand how a computer works
- Understand computer network basics
- Have a fundamental grasp of any number of technical acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS, and the list goes on.
- Utilize built-in Windows tools to see your network settings
- Recognize and be able to discuss various security technologies, including anti-malware, firewalls, intrusion detection systems, sniffers, ethical hacking, active defense, and threat hunting.
- Understand wireless technologies including WiFi, Bluetooth, mobile phones and the Internet of Things (IoT)
- Explain a variety of frequent attacks such as social engineering, drive-by downloads, watering hole attacks, lateral movement, and other attacks
- Understand different types of malware
- Understand browser security and the privacy issues associated with web browsing
- Explain system hardening
- Discuss system patching
- Understand virtual machines and cloud computing
- Understand backups and create a backup plan for your personal life that virtually guarantees you never have to pay ransom to access your data

To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to cybersecurity and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in cybersecurity and need formal training and certification?

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301.

This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You'll learn fundamentals of cybersecurity that will serve as the foundation of your security skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next SANS course in this progression, SEC401: Security Essentials Bootcamp Style. It also delivers on the SANS promise: You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.

"SEC301 is an extremely valuable course, even for someone with 12 years of IT experience!"

— Brian Pfau, **Banfield Pet Hospital**

"SEC301 is a great class for the individual who wants to learn an extensive amount of material in one week."

— **Steven Chovanec**, Discover Financial Services

Certification: GIAC Information Security Fundamentals (GISF)
giac.org/gisf

SEC388: Introduction to Cloud Computing and Security

3 Day Program	18 CPEs	Laptop Required

You Will Be Able To

- Make sense of different cloud-based services
- Understand and analyze risk in the cloud
- Interact with Azure and AWS environments using a browser and command line tools
- Change behavior and build a security-aware culture
- Deploy and integrate cloud services in AWS and Azure
- Get up to speed quickly on cloud security issues and terminology
- Detect and effectively respond to a simulated cloud breach
- Speak the same language as technical security professionals
- Learn how to automate common tasks using cloud shells
- Defend cloud services from attacks
- Track, audit and manage budgeting in your cloud environments

"Serge is the best instructor I've ever had! He's so knowledgeable and has a great teaching style. Very relatable and helps when people have questions."

—Seth J., SEC542 student

Ground School for Cloud Security

The purpose of SEC388 is to learn the fundamentals of cloud computing and security. We do this by introducing, and eventually immersing, you in both AWS and Azure; by doing so, we are able to expose you to important concepts, services, and the intricacies of each vendor's platform. This course provides you with the knowledge you need to confidently speak to modern cybersecurity security issues brought on by the cloud, and become well versed with applicable terminology. You won't just learn about cloud security, you will learn the "how" and the "what" behind the critical cloud security topics impacting businesses today.

Business Takeaways

This course will help your organization:

- Develop professionals – technical or managerial – that know how to use AWS and Azure services
- Anticipate what cloud security threats are applicable to your business
- Learn how to mitigate threats
- Create a culture where security empowers the business to succeed

Hands-On Training

All labs in SEC388 are focused on Azure and AWS and involve directly interacting with each cloud service provider. Students will use a browser to access each cloud environment to gain familiarity with cloud computing concepts. During labs, students will implement cloud services, deploy a cloud-based website, and perform essential security tasks in order to become accustomed to cloud computing and cloud security. The total time committed to labs is about 37% of the course.

Author Statement

"Cloud computing is not new and the adoption of the cloud by organizations continues to grow at an astounding rate. Due to this, many people are finding themselves in the position where it clearly makes sense to learn more about cloud computing. Interestingly, this rise in cloud computing has brought forth a rise in cloud-related breaches – and it makes perfect sense why. As we see with any new frontier in computer science, what's old is new again, and many of the mistakes of the past, are being revived in today's modern world of cloud computing. It is critically important to develop the skills and knowledge needed to positively influence cloud security in every capacity we can influence. Regardless of your background, SEC388's entry-level approach and focus on cloud computing and security will help you prepare for a rewarding career, just as it will help level-up your skills as an accomplished professional, ultimately preparing you for success in a world of cloud computing."

—Serge Borso

SEC401: Security Essentials - Network, Endpoint, and Cloud

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Understand the core areas of cybersecurity and how to create a security program that is built on a foundation of Detection, Response, and Prevention
- Apply practical tips and tricks that focus on addressing high-priority security problems within your organization and doing the right things that lead to security solutions that work
- Understand how adversaries adapt tactics and techniques, and importantly how to adapt your defense accordingly
- Know what ransomware is and how to better defend against it
- Leverage a defensible network architecture (VLANs, NAC, and 802.1x) based on advanced persistent threat indicators of compromise
- Understand the Identity and Access Management (IAM) methodology, including aspects of strong authentication (Multi-Factor Authentication)
- Leverage the strengths and differences among the top three cloud providers (Amazon, Microsoft, and Google), including the concepts of multi-cloud
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, configure the system to be more secure (realistic and practical application of a capable vulnerability management program)
- Sniff network communication protocols to determine the content of network communication (including access credentials) using tools such as tcpdump and Wireshark
- Use Windows, Linux, and macOS command line tools to analyze a system looking for high-risk indicators of compromise, as well as the concepts of basic scripting for the automation of continuous monitoring
- Build a network visibility map that can be used to validate the attack surface and determine the best methodology to reduce the attack surface through hardening and configuration management
- Know why some organizations win and some lose when it comes to security, and most importantly, how to be on the winning side

This course will show you the most effective steps to prevent attacks and detect adversaries with actionable techniques that can be used as soon as you get back to work. You'll learn tips and tricks designed to help you win the battle against the wide range of cyber adversaries that want to harm your environment.

Organizations are going to be targeted, so they must be prepared for eventual compromise. Today more than ever before, TIMELY detection and response is critical. The longer an adversary is present in your environment, the more devastating and damaging the impact becomes. The most important question in information security may well be, "How quickly can we detect, respond, and REMEDIATE an adversary?"

Information security is all about making sure you focus on the right areas of defense, especially as applied to the uniqueness of YOUR organization. In SEC401 you will learn the language and underlying workings of computer and information security, and how best to apply them to your unique needs. You will gain the essential and effective security knowledge you will need if you are given the responsibility to secure systems and/or organizations.

Whether you are new to information security or a seasoned practitioner with a specialized focus, SEC401 will provide the essential information security skills and techniques you need to protect and secure your organization's critical information and technology assets, whether on-premise or in the cloud. SEC401 will also show you how to directly apply the concepts learned into a winning defensive strategy, all in the terms of the modern adversary. This is how we fight; this is how we win!

Is SEC401: Security Essentials: Network, Endpoint, and Cloud the right course for you?

Ask yourself the following questions:

- Do you fully understand why some organizations become compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you understand the effectiveness of each security control and are you certain that they are all configured correctly?
- Are the proper security metrics set up and communicated to your executives to help drive the best security decisions?

SEC401 provides the information security knowledge necessary to help you answer these questions, delivered in a bootcamp-style format and reinforced with hands-on labs.

SEC401 can be taken in Japanese language with Japanese textbooks.

"SEC401 gives you a fantastic knowledge base to build on, and I would say it's essential for anyone working in cybersecurity."

— Thomas Wilson, **Agile Systems**

Certification: GIAC Security Essentials (GSEC)
giac.org/gsec

SEC402: Cybersecurity Writing: Hack the Reader

2 Day Course	12 CPEs	Laptop Not Needed

You Will Be Able To

- Uncover the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing
- Make these elements part of your arsenal through hands-on exercises that draw upon common security scenarios
- Learn the key topics you need to address in security reports and other written communications
- Understand how to pick the best words, structure, look, and tone
- Begin improving your skills at once by spotting and fixing weaknesses in security samples
- Receive practical checklists to ensure you'll write clearly and effectively right away

Who Should Attend

If your cybersecurity job involves writing emails, reports, proposals, or other content, you'll find this course indispensable, whether you are:

- A manager or an individual team member
- A consultant or an internally-focused employee
- An expert or a beginner
- A defender or an attacker
- An earthling or an alien

You get the idea—the course is for all cybersecurity professionals who want to improve their written communications and boost their careers.

NICE Framework Work Roles

- Authorizing Official/Designating Representative (OPM 611)
- Systems Requirements Planner (OPM 641)
- System Testing and Evaluation Specialist (OPM 671)
- Knowledge Manager (OPM 431)
- Cyber Legal Advisor (OPM 731)
- Cyber Instructor (OPM 712)
- Security Awareness & Communications Manager (OPM 712)
- IT Program Auditor (OPM 805)

Want to write better? Learn to hack the reader! Discover how to find an opening, break down your readers' defenses, and capture their attention to deliver your message--even if they're too busy or indifferent to others' writing. This unique course, built exclusively for cybersecurity professionals, will strengthen your writing skills and boost your security career.

You will:

- Uncover the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing.
- Make these elements part of your arsenal through hands-on exercises that draw upon common security scenarios.
- Learn the key topics you need to address in security reports and other written communications.
- Understand how to pick the best words, structure, look, and tone.
- Begin improving your skills at once by spotting and fixing weaknesses in security samples.
- Receive practical checklists to ensure you'll write clearly and effectively right away.

This isn't your normal writing course:

- The course builds upon the author's two decades of cybersecurity experience. You'll learn from examples relevant to security professionals, whether they're experts or beginners, managers or individual team members.
- The course focuses on common writing problems you'll learn to avoid, instead of presenting tedious grammar rules or theoretical explanations. You'll advance your writing by reviewing and improving real-world cybersecurity samples.

Master the writing secrets that'll make you stand out in the eyes of your peers, colleagues, managers, and clients. Learn to communicate your insights, requests, and recommendations persuasively and professionally. Make your cybersecurity writing remarkable.

Author Statement

How can you stand out from other cybersecurity professionals with similar technical skills? How can you get your managers, clients, and colleagues to notice your contribution, accept your advice, and appreciate your input? Write better!

Here's an uncommon opportunity to improve your writing skills without sitting through tedious lectures or writing irrelevant essays. You'll make your writing remarkable by learning how to avoid common mistakes, working on real-world exercises to spot and correct cybersecurity writing problems. You'll write clearly and effectively right away with the help of practical checklists.

This course captures my experience of writing in cybersecurity for over two decades and incorporates insights from other members of the community. It's a course I wish I could have attended when I needed to improve my own writing skills. It's a course I know will help you propel your own cybersecurity career.

—Lenny Zeltser

"Outstanding course. It provides a writing framework/rubric to evaluate and guide future writing."

—Jordan Whitley, **New York Life**

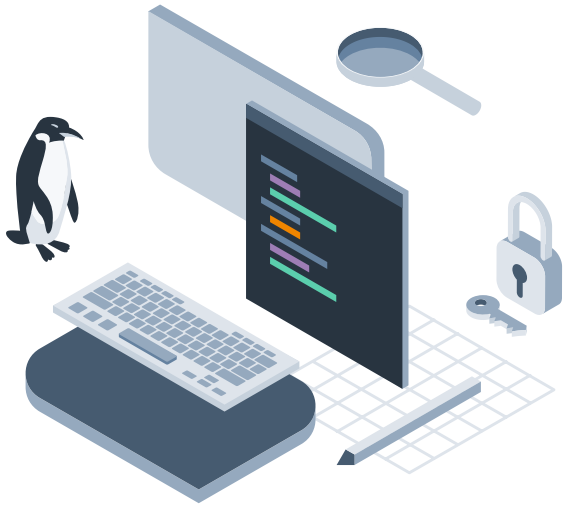
SANS Foundations

Computers, Technology and Security

SANS Foundations is the best single course available to learn core knowledge and develop practical skills in computers, technology, and security fundamentals that are needed to kickstart a career in cybersecurity.

What is included with SANS Foundations?

- Over 120 hours of curated content
- Hands-on labs experience
- Quizzes to consolidate learning outcomes
- Training by world-renowned experts
- Engaging 4K video content
- Proctored final exam delivered by GIAC



What will Students learn in this course?

The course provides students with exactly what they need to go from zero technical and security knowledge to a level of sufficient theoretical understanding and applied practical skills that will enable them to speak the same language as industry professionals. Students will develop fundamental skills and knowledge in key IT subject areas such as Linux, programming, networking, computer hardware, operating systems, encryption, basic security concepts, and more!

Who should take this course?

This course is designed for:

- Career changers
- Online self-driven learners seeking new skills
- College and university students
- Business professionals without a deep cybersecurity background
- New hires in IT/cybersecurity
- Participants in reskilling programs

For more information visit
www.sans-foundations.com
or email
foundations@sans.org

> I think the biggest value add for SANS Foundations was simply how comprehensive it was. It covered a lot of topics, but each was covered in enough depth for a better handle on the basics without being overwhelming.
>
> - U.S. government federal law enforcement professional

SANS CURRICULUM FOCUS AREA

Cyber Defense & Blue Team Operations

The term Blue Team comes from the world of military exercises, during which the Red Team plays the role of the adversary and the Blue Team acts as the friendly force defending itself from Red Team cyber-attacks.

In cybersecurity, the Blue Team's focus is on defending the organization from cyber-attacks. Blue Teams develop and implement multiple security controls in a layered defense-in-depth strategy, verify their effectiveness, and continuously monitor and improve defenses.

Cyber Defense and Blue Team Ops courses will teach you to:

- Deploy tools and techniques needed to defend your networks with insight and awareness
- Implement a modern security design that allows you to protect your assets and defend against threats
- Establish and maintain a holistic and layered approach to security
- Detect intrusions and analyze network traffic
- Apply a proactive approach to Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM)
- Use methods and processes to enhance existing logging solutions
- Apply technical security principles and controls for the cloud

Enhance your training with:

- Cyber Defense Netwars **sans.org/netwars**
- SANS Summits: Blue Team and Open-Source Intelligence **sans.org/summit**
- Free Resources: Podcasts, webcasts, live stream video discussions, blogs and more **sans.org/cyber-defense**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a Graduate Certificate in Cyber Defense Operations **sans.edu**

"Using the techniques from this class, I will immediately be able to improve our logging and detection capabilities."

—Kendon Emmons, **Dart Container**

Cyber Defense & Blue Team Ops Job Roles:

- SOC Analyst/Manager
- Intrusion Detection Engineer, Threat Hunter
- Security and Network Engineers/Architect
- Investigator/OSINT Analyst
- Endpoint/Server System Administrators
- Automation and DevSecOps
- Incident Responders
- Cyber Threat Intelligence Analysts

SEC450: Blue Team Fundamentals: Security Operations and Analysis

6 Day Program	36 CPEs	Laptop Required

Business Takeaways

This course will help your organization:

- Make the most of security telemetry including endpoint, network, and cloud-based sensors
- Reduce false positives to a minimum
- Quickly and accurately triage security incidents
- Improve the effectiveness, efficiency, and success of your SOC

Why Choose SANS SEC450 Over the Competition?

Unmatched in the industry with its volume and depth, SEC450 includes:

- Nearly 1000 pages of instructional content with extensive notes and documentation
- 15 hands-on exercises putting real SOC tools and situations in front of students to emphasize lessons and a 400+ page in-depth instructional exercise workbook to go with them
- Full lab walkthrough videos, recorded and explained step by step by the course author
- A custom course Linux virtual machine filled with SOC tools
- A full day capture-the-flag contest experience with 75 challenges where students will apply their learning and put their skills to the test!
- Continuously updated material to cover the newest attackers and techniques

This depth of material makes SEC450 and the GSOC certification a cyber security analyst training class like no other, covering techniques, mindset, and tools at a level unmatched by other offerings. Whether you're taking SEC450 yourself or including it in your analyst training plan, we'd love to have you and your org join the growing list of alumni and GSOC certified security analysts helping to halt the flow of disruptive cyberattacks!

If you're looking for the gold standard in cyber security analyst training, you've found it! SANS SEC450 and the accompanying GIAC GSOC certification are the premier pair for anyone looking for a comprehensive security operations training course and certification. Check out the extensive syllabus and description below for a detailed run down of course content and don't miss the free demo available by clicking the "Course Demo" button!

Designed for teams of all types, SEC450 will get you hands-on with the tools and techniques required to stop advanced cyberattacks! Whether you are a part of a full SOC in a large organization, a small security ops group, or an MSSP responsible for protecting customers, SEC450 will teach you and your team the critical skills for understanding how to defend a modern organization.

Designed By Security Analysts, For Security Analysts

SEC450 is authored, designed, and advised by a group of veteran SOC analysts and managers to be a one-stop shop for all the essential techniques, tools, and data your team will need to be effective, including:

- **Security Data Collection –** How to make the most of security telemetry including endpoint, network, and cloud-based sensors
- **Automation –** How to identify the best opportunities for SOAR platform and other script-based automation
- **Efficient Security Process –** How to keep your security operations tempo on track with in-depth discussions on what a SOC or security operations team should be doing at every step from data generation to detection, triage, analysis, and incident response
- **Quality Triage and Analysis –** How to quickly identify and separate typical commodity attack alerts from high-risk, high-impact advanced attacks, and how to do careful, thorough, and cognitive-bias free security incident analysis
- **False Positive Reduction –** Detailed explanations, processes, and techniques to reduce false positives to a minimum
- **SOC Tools –** Includes hands-on exercises
- Burnout and Turnover Reduction – Informed with both scientific research and years of personal experience, this class teaches what causes cyber security analyst burnout and how you and your team can avoid it by understanding the causes and factors that lead to burnout. This class will help you build a long-term sustainable cyber defense career so you and your team can deliver the best every day!
- **Certification –** The ability to add on the GIAC GSOC certification that encourages students to retain the material over the long term, and helps you objectively demonstrate you and your team's level of skill

SEC450 takes the approach of not just teaching what to do, but also why these techniques work and encourages students to ask the critical question "How can we objectively measure that security is improving?" And unlike shorter security analyst training courses, SEC450 has the time to cover the deeper reasoning and principles behind successful cyber defense strategies, ensuring students can apply the concepts even beyond the class material to take their defensive skills and thinking to the next level. Don't just take our word for it, ask any of the course alumni! SEC450 instructors repeatedly see the long lists of improvement ideas students finish the class with, eager to bring them back to their organizations.

Certification: GIAC Security Operations Certified (GSOC)
giac.org/gsoc

SEC497: Practical Open-Source Intelligence (OSINT)

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform a variety of OSINT investigations while practicing good OPSEC
- Create sock puppet accounts
- Locate information on the internet, including some hard-to-find and deleted information
- Locate individuals online and examine their online presence
- Understand and effectively search the dark web
- Create an accurate report of the online infrastructure for cyber defense, merger and acquisition analysis, pen testing, and other critical areas for an organization.
- Use methods that can often reveal who owns a website as well as the other websites that they own or operate
- Understand the different types of breach data available and how they can be used for offensive and defensive purposes
- Effectively gather and utilize social media data
- Understand and use facial recognition and facial comparison engines
- Quickly and easily triage large datasets to learn what they contain
- Identify malicious documents and documents designed to give away your location

Business Takeaways

- Improve the effectiveness, efficiency, and success of OSINT investigations
- Build an OSINT team that can perform a variety of OSINT investigations while practicing good OPSEC
- Create accurate reporting of your organization's online infrastructure
- Understand how breach data can be used for offensive and defensive purposes

SEC497 is a comprehensive training course on Open-Source Intelligence (OSINT) written by an industry professional with over two decades of experience. The course is designed to teach you the most important skills, tools, and methods needed to launch or further refine your investigation skills. SEC497 will provide actionable information to students throughout the OSINT world, including intelligence analysts, law enforcement officials, cyber threat intelligence and cyber defenders, pen testers, investigators, and anyone else who wants to improve their OSINT skills. There is something for everyone, from newcomers to experienced practitioners.

SEC497 focuses on practical techniques that are useful day in and day out. This course is constructed to be accessible for those new to OSINT while providing experienced practitioners with tried-and-true tools that they can add to their arsenal to solve real-world problems. The course has a strong focus on understanding how systems work to facilitate informed decisions, and includes hands-on exercises based on actual scenarios from the government and private sectors. We will discuss cutting-edge research and outlier techniques and not only talk about what is possible, we will practice doing it! Dive into the course syllabus below for a detailed breakdown of the topics covered.

Course Author Statement

"When I started the first open-source intelligence (OSINT) unit for my organization over a decade ago, I was told we had no budget for tools, equipment, or training. I used to joke that one nice thing about not having a budget was that it made many of my decisions very easy. If there was something I needed, I either built it myself or did without.

"Coming from that background forces you to understand how things work and what truly matters. In addition to performing countless OSINT investigations, I've traveled across the world for over a decade teaching operational security (OPSEC) and OSINT to various government agencies and consulted with numerous private companies, ranging from small start-ups to Fortune 100 enterprises. I have helped hunt down international fugitives, identified online infrastructure for a merger and acquisitions due diligence report, and handled numerous tasks in between. This course allows me me share my experience with what works, what does not work, and how we can achieve our goals with minimal effort and cost."

—Matt Edmondson

"The module on dealing with large data sets was very helpful. Getting a deep understanding on the challenges large data sets pose and how to work around them is very helpful and practical."

—Jamal Gumbs

Certification: GIAC Open Source Intelligence Certification(GOSI)
giac.org/gosi

SEC501: Advanced Security Essentials - Enterprise Defender

6 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Build a defensible network architecture by auditing router configurations, launching successful attacks against them, hardening devices to withstand those same attacks, and using active defense tools to detect an attack and generate an alert
- Perform detailed analysis of traffic using various sniffers and protocol analyzers, and automate attack detection by creating and testing new rules for detection systems
- Identify and track attacks and anomalies in network packets
- Use various tools to assess systems and web applications for known vulnerabilities, and exploit those vulnerabilities using penetration testing frameworks and toolsets
- Analyze Windows systems during an incident to identify signs of a compromise
- Find, identify, analyze, and clean up malware such as Ransomware using a variety of techniques, including monitoring the malware as it executes and manually reversing its code to discover its secrets

Business Takeaways

- Improve the effectiveness, efficiency, and success of cybersecurity initiatives
- Build defensible networks that minimize the impact of attacks
- Identify your organization's exposure points to ultimately prioritize and fix the vulnerabilities, increasing the organization's overall security

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and appropriately respond to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of where it resides or what paths it travels.

The primary way to PREVENT attacks begins with assuring that your network devices are optimally configured to thwart your adversary. This is done by auditing against established security benchmarks, hardening devices to reduce their attack surface, and validating their increased resilience against attack. Prevention continues with securing hostname resolution (an obvious adversary target for establishing a Machine-in-the-Middle position) and goes even further with securing and defending cloud infrastructure (both public and private) against compromise.

Enterprises need to be able to DETECT attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, monitoring for indications of compromise, and employing active defense techniques to provide early warning of an attack. Of course, despite an enterprise's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Performing penetration testing and vulnerability analysis against your enterprise to identify problems and issues before a compromise occurs is an excellent way to reduce overall organizational risk.

Once an attack is identified, you must quickly and effectively RESPOND, activating your incident response team to collect the forensic artifacts needed to identify the tactics, techniques, and procedures being used by your adversaries. With this information you can contain their activities, ensure that you have scoped out all systems where they have had an impact, and eventually eradicate them from the network. This can be followed by recovery and remediation to PREVENT their return. Lessons learned through understanding how the network was compromised can then be fed back into more preventive and detective measures, completing the security lifecycle.

It costs enterprises worldwide billions of dollars annually to respond to malware, and particularly Ransomware, attacks. So it is increasingly necessary to understand how such software behaves. Ransomware spreads very quickly and is not stealthy; as soon as your data become inaccessible and your systems unstable, it is clear something is amiss. Beyond detection and response, when prevention has failed, understanding the nature of malware, its functional requirements, and how it achieves its goals is critical to being able to rapidly reduce the damage it can cause and the costs of eradicating it.

Business Takeaways

- Improve the effectiveness, efficiency, and success of cybersecurity initiatives
- Build defensible networks that minimize the impact of attacks
- Identify your organization's exposure points to ultimately prioritize and fix the vulnerabilities, increasing the organization's overall security

Certification: GIAC Certified Enterprise Defender (GCED)
giac.org/gced

SEC503: Network Monitoring and Threat Detection In-Depth

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Configure and run Snort and Suricata
- Create and write effective and efficient Snort, Suricata and FirePOWER rules
- Configure and run open-source Zeek to provide a hybrid traffic analysis framework
- Create automated threat hunting correlation scripts in Zeek
- Understand TCP/IP component layers to identify normal and abnormal traffic for threat identification
- Use traffic analysis tools to identify signs of a compromise or active threat
- Perform network forensics to investigate traffic to identify TTPs and find active threats
- Carve out files and other types of content from network traffic to reconstruct events
- Create BPF filters to selectively examine a particular traffic trait at scale
- Craft packets with Scapy
- Use NetFlow/IPFIX tools to find network behavior anomalies and potential threats
- Use your knowledge of network architecture and hardware to customize placement of network monitoring sensors and sniff traffic off the wire

SEC503 is the most important course that you will take in your information security career – past students describe it as the most difficult but most rewarding course they've ever taken. If you want to be able to perform effective threat hunting to find zero-day activities on your network before public disclosure, this is definitely the course for you.SEC503 is not for people looking to understand alerts generated by an out-of-the-box network monitoring tool; rather, it is for those who want to deeply understand what is happening on their network today, and who suspect that there are very serious things happening right now that none of their tools are telling them about.

What sets SEC503 apart from any other course in this space is that we take a bottom-up approach to teaching network monitoring and network forensics, which leads naturally to effective threat hunting. Rather than starting with a tool and teaching you how to use it in different situations, this course teaches you how and why TCP/IP protocols work the way they do. The first two sections present what we call "Packets as a Second Language," then we move to presenting common application protocols and a general approach to researching and understanding new protocols. Throughout the discussion, direct application of this knowledge is made to identify both zero-day and known threats.

With this deep understanding of how network protocols work, we turn our attention to the most important and widely used automated threat detection and mitigation tools in the industry. You will you learn how to develop efficient detection capabilities with these tools, and you'll come to understand what existing rules are doing and identify whether they are useful. The result is that you will leave this course with a clear understanding of how to instrument your network and perform detailed threat hunting, incident analysis, network forensics, and reconstruction.

What makes SEC503 as important as we believe it is (and students tell us it is) is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today. Preserving the security of your network in today's threat environment is more challenging than ever, especially as you migrate more and more services into the cloud. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable.

Some of the specific technical knowledge and hands-on training in SEC503 covers the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, enabling you to intelligently examine network traffic for signs of compromise or zero-day threat. You will get plenty of practice learning to master a variety of tools, including tcpdump, Wireshark, Snort, Suricata, Zeek, tshark, SiLK, and NetFlow/IPFIX. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution, and evening Bootcamp sessions force you to apply the theory learned during the day to real-world problems immediately. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

SEC503 is most appropriate for students who monitor, defend, and conduct threat hunting on their network, including security analysts and those who work in Security Operations Centers, although red team members often tell us that the course also ups their game, especially when it comes to avoiding detection.

Certification: GIAC Certified Intrusion Analyst (GCIA)
giac.org/gcia

SEC505: Securing Windows and PowerShell Automation

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Write PowerShell scripts for security automation
- Execute PowerShell scripts on remote systems
- Harden PowerShell itself against abuse, and enable transcription logging for your SIEM
- Use PowerShell to access the WMI service for remote command execution, searching event logs, reconnaissance, and more
- Use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds (assume breach)
- Block the lateral movement of hackers and ransomware using Windows Firewall, IPsec, DNS sinkholes, admin credential protections, and more
- Prevent exploitation using AppLocker and other Windows OS hardening techniques in a scalable way with PowerShell
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root
- Configure mitigations against pass-the-hash attacks, Kerberos Golden Tickets, Remote Desktop Protocol (RDP) man-in-the-middle attacks, Security Access Token abuse, and other attacks discussed in SEC504 and other SANS hacking courses
- Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certificate Authentications (CAs)
- Harden essential protocols against exploitation, such as SSL, RDP, DNS, PowerShell Remoting, and SMB

WINDOWS SECURITY AUTOMATION MEANS POWERSHELL

In this course you will learn how to:

- Write PowerShell scripts for Windows and Active Directory security automation
- Safely run PowerShell scripts on thousands of hosts over the network
- Defend against PowerShell malware such as ransomware
- Harden Windows Server and Windows 10 against skilled attackers

In particular, we will use PowerShell to secure Windows against many of the attacks described in the MITRE ATT&CK matrix, especially stolen administrative credentials, ransomware, hacker lateral movement inside the LAN, and insecure Windows protocols, like RDP and SMB.

You will leave this course ready to start writing your own PowerShell scripts to help secure your Windows environment. It's easy to find Windows security checklists, but how do you automate those changes across thousands of machines? How do you safely run scripts on many remote boxes? In this course you will learn not just Windows and Active Directory security, but how to manage security using PowerShell.

DON'T JUST LEARN POWERSHELL SYNTAX, LEARN HOW TO LEVERAGE POWERSHELL AS A FORCE MULTIPLIER FOR WINDOWS SECURITY

There is another reason why PowerShell has become popular: PowerShell is just plain fun! You will be surprised at how much you can accomplish with PowerShell in a short period of time – it's much more than just a scripting language, and you don't have to be a coding guru to get going.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for IT people with PowerShell skills. You don't have to know any PowerShell to attend this course, we will learn it together during the labs.

You can learn basic PowerShell syntax on YouTube for free, but this course goes far beyond syntax. In this course we will learn how to use PowerShell as a platform for managing security, as a "force multiplier" for the Blue Team, and as a rocket booster for your Windows IT career.

WE WILL WRITE A POWERSHELL RANSOMWARE SCRIPT AND DEFEND AGAINST IT

Unfortunately, PowerShell is being abused by hackers and malware authors, so in the last section of the course, we will write our own ransomware script to see how to defend against scripts like it.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security at the same time.

The course author, Jason Fossen, is a SANS Institute Fellow and has been writing and teaching for SANS since 1998. In fact, SEC505 has had at least one day of PowerShell for more than 10 years, and now PowerShell is the centerpiece of the course.

"In SEC505, real-life solutions are offered by someone who understands the roadblocks in the way. This is information I could implement tomorrow and make my network more secure."

— Mary Becken, **Egan Company**

Certification: GIAC Certified Windows Security Administrator (GCWN)
giac.org/gcwn

SEC511: Continuous Monitoring and Security Operations

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Centers (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring
- Determine requisite monitoring capabilities for a SOC environment

While the above list briefly outlines the knowledge and skills you will learn, it barely scratches the surface of what this course has to offer. Hands-on labs throughout the course will reinforce key concepts and principles, as well as teach you how to use scripting to automate continuous monitoring. We look forward to seeing you soon!

Analyze Threats. Detect Anomalies. Stop Intrusions.

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. SEC511 will teach you how to strengthen your skills to undertake that proactive approach.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and section five of this course will greatly increase your understanding and enhance your skills in implementing CM using the NIST framework.

SANS is uniquely qualified to offer this course. Course authors Eric Conrad (GSE #13) and Seth Misenar (GSE #28) hold the distinguished GIAC Security Expert Certification, and both are experienced, real-world, practitioners who apply the concepts and techniques they teach in this course on a daily basis. SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final section features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. The competition has been designed to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

With your training journey now complete and your skills enhanced and honed, it is time to go back to work and deliver on the SANS promise that you will be able to apply what you learn in this course the day you return to the office.

Certification: GIAC Continuous Monitoring Certification (GMON)
giac.org/gmon

SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Analyze a security architecture for deficiencies
- Discover data, applications, assets and services, and assess compliance state
- Implement technologies for enhanced prevention, detection, and response capabilities
- Comprehend deficiencies in security solutions and understand how to tune and operate them
- Understand the impact of 'encrypt all' strategies
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing technologies
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program
- Design and Implement Zero Trust strategies leveraging current technologies and investment

SEC530 is designed to help students establish and maintain a holistic and layered approach to security, while taking them on a journey towards a realistic 'less trust' implementation, based on Zero Trust principles, pillars and capabilities. Effective security requires a balance between detection, prevention, and response capabilities, but such a balance demands that controls be implemented on the network, directly on endpoints, and within cloud environments. The strengths and weaknesses of one solution complement another solution through strategic placement, implementation, and continuous fine-tuning.

To address these issues, this course focuses on combining strategic concepts of infrastructure and tool placement while also diving into their technical application. We will discuss and identify what solutions are available and how to apply them successfully to reduce attack surface and implement adaptive trust. Most importantly, we'll evaluate the strengths and weaknesses of various solutions and how to layer them cohesively to achieve a defensible security architecture.

SEC530 is a practical class, focused on teaching effective tactics and tools to architect and engineer for disruption, early warning detection, and response to most prevalent attacks, based on the experience of the authors, highly experienced practitioners with an extensive career in cyberdefense. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, next-gen firewalls, IDS, IPS, WAF, SIEM, sandboxes, encryption, PKI and proxies, among others. Students will learn how to assess, re-configure and validate these technologies to significantly improve their organizations' prevention, detection and response capabilities, augment visibility, reduce attack surface, and even anticipate attacks in innovative ways. The course will also delve into some of the latest technologies and their capabilities, strengths, and weaknesses. You will come away with recommendations and suggestions that will aid in building a robust security infrastructure, layer by layer, across hybrid environments, as you embark on a journey towards Zero Trust.

While this is not a monitoring course, it will dovetail nicely with continuous security monitoring, ensuring that your security architecture not only supports prevention but also provides the critical logs that can be fed into behavioral detection and analytics systems, like UEBA or Security Information and Event Management (SIEM), in a Security Operations Center (SOC).

Multiple hands-on labs conducted daily will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

Business Takeaways

- Identify and comprehend deficiencies in security solutions
- Design and Implement Zero Trust strategies leveraging current technologies and investment
- Maximize existing investment in security architecture by reconfiguring existing technologies
- Layer defenses to increase protection time while increasing the likelihood of detection
- Improved prevention, detection, and response capabilities
- Reduced attack surface

"SEC530 provided an excellent understanding of application attacks and how to protect against them."

— Shayne Douglass, **AMEWAS Inc.**

Certification: GIAC Defensible Security Architecture (GDSA)
giac.org/gdsa

SEC555: SIEM with Tactical Analytics

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Deploy the SANS SOF-ELK VM in production environments
- Demonstrate ways most SIEMs commonly lag current open source solutions (e.g. SOF-ELK)
- Bring students up to speed on SIEM use, architecture, and best practices
- Know what type of data sources to collect logs from
- Deploy a scalable logs solution with multiple ways to retrieve logs
- Operationalize ordinary logs into tactical data
- Develop methods to handle billions of logs from many disparate data sources
- Understand best practice methods for collecting logs
- Dig into log manipulation techniques challenging many SIEM solutions
- Build out graphs and tables that can be used to detect adversary activities and abnormalities
- Combine data into active dashboards that make analyst review more tactical
- Utilize adversary techniques against them by using frequency analysis in large data sets
- Develop baselines of network activity based on users and devices
- Develop baselines of Windows systems with the ability to detect changes from the baseline
- Apply multiple forms of analysis such as long tail analysis to find abnormalities
- Correlate and combine multiple data sources to achieve more complete understanding
- Provide context to standard alerts to help understand and prioritize them
- Use log data to establish security control effectiveness
- Implement log alerts that create virtual tripwires for early breach detection
- Understand how to handle container monitoring and log collection
- Baseline and find unauthorized changes in cloud environments
- Integrate and write custom scripts against a SIEM

Business Takeaways

- Use log data to establish security control effectiveness
- Combine data into active dashboards that make analyst review more tactical
- Simplify the handling and filtering of the large amount of data generated by both servers and workstations
- Apply large data analysis techniques to sift through massive ammounts of endpoint data
- Quickly detect and respond to the adversary

Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of those sources for proper analysis. This class is designed to provide students with the training, methods, and processes to enhance existing logging solutions. The class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Information and Event Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a "Big Data" problem but rather a "Data Analysis" problem. Let's face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the "appropriate" use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, how to start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

"This course uses real-world events and hands-on training to allow me to immediately improve my organization's security stance. Day one back in the office I was implementing what I learned."

— Frank Giachino, **Bechtel**

Certification: GIAC Certified Detection Analyst (GCDA)
giac.org/gcda

SEC573: Automating Information Security with Python

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Leverage Python to perform routine tasks quickly and efficiently
- Automate log analysis and packet analysis with file operations, regular expressions, and analysis modules to find evil
- Develop forensics tools to carve binary data and extract new artifacts
- Read data from databases and the Windows Registry
- Interact with websites to collect intelligence
- Develop UDP and TCP client and server applications
- Automate system processes and process their output

Python is a simple, user-friendly language that is designed to make it quick and easy to automate the tasks performed by security professionals. Whether you are new to coding or have been coding for years, SANS SEC573: Automating Information Security with Python will have you creating programs that make your job easier and your work more efficient. This self-paced course starts from the very beginning, assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced course material.

All security professionals, including penetration testers, forensics analysts, network defenders, security administrators, and incident responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold...or you can write a tool yourself.

Or perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

If you are a penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool.

SEC573 is designed to give you the skills you need to tweak, customize, or outright develop your own tools. We put you on the path to create your own tools, empowering you to better automate the daily routine of today's information security professional and achieve more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

Business Takeaways

This course will help your organization:

- Automate system processes and process their input quickly and efficiently
- Create programs that increase efficiency and productivity
- Develop tools to provide the vital defenses our organizations need

"SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs."

— Caleb Jaren, **Microsoft**

Certification: GIAC Python Coder (GPYC)
giac.org/gpyc

SEC586: Blue Team Operations: Defensive PowerShell

6 Day Program	36 CPEs	Laptop Required

Author Statement

"My Information Security experience has taught me that human analysis is a critical attribute of effective cyber defense. Yet, the very people who are critical to preventing, discovering, and responding to threats are often bogged down with manual work that, while it needs to be done, is done at the expense of more advanced efforts. At the same time, we're facing a critical personnel and skills shortage in Information Security, and many organizations are struggling to fill open positions.

The immediate answer to these problems is automation. PowerShell is a cross-platform automation engine that is uniquely positioned for this task. Blue Teams can transform their everyday operations by automating wherever possible. System auditing and hardening tasks can be streamlined via configuration as code and substantial automation, leaving room for professionals to interpret reporting and work on higher-level tasks. Detection and response tasks can also be significantly improved. Data aggregation and analysis can be performed automatically, leaving analysts with pre-filtered data of interest to aid in detection. For response, a pre-built toolkit can enable near real-time response actions such as quarantining systems on the network, interrogating suspicious hosts for more information, capturing artifacts for forensic analysis, or even automatically remediating common issues.

SEC586 is designed to help teams raise the bar and spend time on what will provide the most value to their organizations. Deep automation alongside capable professionals flips the script and makes organizations a dangerous target for their adversaries."

—Josh Johnson

Prerequisites

- Basic understanding of programming concepts
- Basic understanding of information security principles

Effective Blue Teams work to harden infrastructure, minimize time to detection, and enable real-time response to keep pace with modern adversaries. Automation is a key component to facilitate these capabilities, and PowerShell can be the glue that holds together and enables the orchestration of this process across disparate systems and platforms to effectively act as a force multiplier for Blue Teams. This course will enable Information Security professionals to leverage PowerShell to build tooling that hardens systems, hunts for threats, and responds to attacks immediately upon discovery.

PowerShell is uniquely positioned for this task of enabling Blue Teams. It acts as an automation toolset that functions across platforms and it is built on top of the .NET framework for nearly limitless extensibility. SEC586 maximizes the use of PowerShell in an approach based specifically on Blue Team use cases.

Students will learn:

- PowerShell scripting fundamentals from the ground up in terms of PowerShell's capabilities as a defensive toolset
- Ways to maximize performance of code across dozens, hundreds, or thousands of systems
- Modern hardening techniques using Infrastructure-as-Code principles
- How to integrate disparate systems for multi-platform orchestration
- PowerShell-based detection techniques ranging from Event Tracing for Windows to baseline deviation and deception
- Response techniques leveraging PowerShell-based automation

This course is meant to be accessible to beginners who are new to the PowerShell scripting language as well as to seasoned veterans looking to round out their skillset. Language fundamentals are covered in-depth, with hands-on labs to enable beginning students to become comfortable with the platform. For skilled PowerShell users who already know the basics, the material is meant to solidify knowledge of the underlying mechanics while providing additional challenges to further this understanding.

The PowerPlay platform built into the lab environment enables practical, hands-on drilling of concepts to ensure understanding, promote creativity, and provide a challenging environment for anyone to build on their existing skillset. PowerPlay consists of challenges and questions mapping back to and extending the course material.

Between the course material and the PowerPlay bonus environment, SEC586 students will leave the course well equipped with the skills to automate everyday cyber defense tasks. You will return to work ready to implement a new set of skills to harden your systems and accelerate your capabilities to more immediately detect and respond to threats.

SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Take a dive more in-depth into finding, collecting, and analyzing information found on the internet
- Debug, understand, alter, and create your own OSINT-focused Python scripts
- Move and pivot around safely on the Dark Web
- Perform financial OSINT investigations

"This would be a valuable course for any cybersecurity professional. The subjects and tools in this class are invaluable. I have not seen navigating the Dark Web being taught anywhere else."

—Mark Styron

SANS SEC587 is an advanced Open-Source Intelligence (OSINT) course for those who already know the foundations of OSINT. The goal is to provide students with more in-depth and technical OSINT knowledge. Students will learn OSINT skills and techniques that law enforcement, intelligence analysts, private investigators, journalists, penetration testers and network defenders use in their investigations.

Open-source intelligence collection and analysis techniques are increasingly useful in a world where more and more information is added to the internet every day. With billions of internet users sharing information on themselves, their organizations, and people and events they have knowledge of, the internet is a resource-rich environment for intelligence collection. SEC587 is designed to teach you how to efficiently utilize this wealth of information for your own investigations.

SEC587 will take your OSINT collection and analysis abilities to the next level, whether you are involved in intelligence analysis, criminal and fraud investigations, or just curious about how to find out more about anything! SEC587 is replete with hands-on exercises, real-world scenarios, and interaction with live internet and dark web data sources.

This course is also blended with all the fundamentals an OSINT analyst will need to learn and understand and apply basic coding in languages such as Python, JSON, and shell utilities as well as interacting with APIs for automating your OSINT processes.

SEC587 students will learn effective OSINT methods and techniques including:

- Structured intelligence analysis
- Rating the reliability of information and its sources
- Researching sensitive and secretive groups
- Practical and Advanced Image and video analysis and verification
- Dark web and criminal underground investigations.
- Operational Security (OPSEC) for OSINT
- Fact-checking and analysis of disinformation and misinformation
- Knowing cryptocurrency fundamentals and tracking
- Using basic coding to facilitate information collection and analysis
- Interacting with APIs for data collection and filtering
- Conducting internet monitoring
- Automation techniques to support OSINT processes

"Having a broad coverage over multiple areas of OSINT is really helpful to reinforce the fundamentals and understand the diverse applications of an open source investigator's skills."

—Dan Black

SEC595: Applied Data Science and Machine Learning for Cybersecurity Professionals

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Apply statistical models to real world problems in meaningful ways
- Generate visualizations of your data
- Perform mathematics-based threat hunting on your network
- Understand and apply unsupervised learning/clustering methods
- Build deep learning Neural Networks
- Build and understand convolutional Neural Networks
- Understand and build genetic search algorithms
- Build AI anomaly detection tools
- Model information security problems in useful ways
- Build useful visualization dashboards
- Solve problems with Neural Networks

Business Takeaways

- Generate useful visualization dashboards
- Solve problems with Neural Networks
- Improve the effectiveness, efficiency, and success of cybersecurity initiatives
- Build custom machine learning solutions for your organization's specific needs

Data Science, Artificial Intelligence, and Machine Learning aren't just the current buzzwords, they are fast becoming one of the primary tools in our information security arsenal. The problem is that, unless you have a degree in mathematics or data science, you're likely at the mercy of the vendors. This course completely demystifies machine learning and data science. More than 70% of the time in class is spent solving machine learning and data science problems hands-on rather than just talking about them.

Unlike other courses in this space, this course is squarely centered on solving information security problems. Where other courses tend to be at the extremes, teaching almost all theory or solving trivial problems that don't translate into the real world, this course strikes a balance. We cover only the theory and math fundamentals that you absolutely must know, and only in so far as they apply to the techniques that we then put into practice. The course progressively introduces and applies various statistic, probabilistic, or mathematic tools (in their applied form), allowing you to leave with the ability to use those tools. The hands-on projects covered were selected to provide you a broad base from which to build your own machine learning solutions.

Major topics covered include:

- Data acquisition from SQL, NoSQL document stores, web scraping, and other common sources
- Data exploration and visualization
- Descriptive statistics
- Inferential statistics and probability
- Bayesian inference
- Unsupervised learning and clustering
- Deep learning neural networks
- Autoencoders
- Loss functions
- Convolutional networks
- Embedding layers

Author Statement

"AI and machine learning are everywhere. How do the vendor solutions work? Is this really black magic? I wrote this course to fill an enormous knowledge gap in our field. I believe that if you are going to use a tool, you should understand how that tool works. If you don't, you don't really know what the results mean or why you are getting them. This course provides you a crash-course in statistics, mathematics, Python, and machine learning, taking you from zero to...I'm reluctant to promise 'Hero...' Let's say competent who-can-solve-real-problems-today person!"

—David Hoelzer

SANS SECURITY AWARENESS

Trust SANS to Bring Security Awareness to Your Workforce

SANS is the most trusted and largest source for information security training and security certification in the world—leverage our best-in-class Security Awareness solutions to transform your organization's ability to measure and manage human risk.

Expertly-created comprehensive training builds a powerful program that embodies organizational needs and learning levels.

Cyber Risk Insight Suite™
- Culture Assessment
- Knowledge Assessment
- Behavioral Assessment

EndUser Training

Phishing Platform

Specialized Training
- Developer Training
- ICS Engineering Training
- NERC CIP Training
- Healthcare Training

Thousands of Clients. Millions of Learners. One Mission.

Reach out for a demo!

Visit **sans.org/security-awareness-training/** email **SSAInfo@sans.org**

SANS CURRICULUM FOCUS AREA

Offensive Operations

Organizations rely on offensive tactics to discover and understand their system vulnerabilities so that they can fix known issues before bad guys attack.

As adversaries evolve and attacks become more sophisticated, pen testers and Red Teams need to emulate current real-world attack techniques, discover issues, and properly report those findings in order to deliver significant value to the security team.

SANS Offensive Operations courses will teach you to:

- Emulate today's most powerful and common attacks
- Discover vulnerabilities in target systems
- Exploit vulnerabilities under controlled circumstances
- Apply technical excellence to determine and document risk and potential business impact
- Conduct professional and safe testing according to a carefully designed scope and rules of engagement
- Help an organization with its goal of properly prioritizing resources

Enhance your training with:

- Core Netwars
  sans.org/netwars
- SANS Summit: HackFest
  sans.org/summit
- Free Resources:
  Webcasts, blogs, research, and other features like Slingshot linux distribution
  sans.org/offensive-operations
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a Graduate Certificate in Pen Testing & Ethical Hacking
  sans.edu

"In one week, my instructor built a bridge from typical vulnerability scanning to the true art of penetration testing. Thank you SANS for making myself and my company much more capable in information security."

—Mike Dozier, **Savannah River Nuclear Solutions**

Offensive Operations Job Roles:

- System/Network Penetration Tester
- Application Penetration Tester
- Incident Handler
- Vulnerability Researcher
- Exploit Developer
- Red Teamer
- Mobile Security Manager

SEC460: Enterprise and Cloud Vulnerability Assessment

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform end-to-end vulnerability assessments
- Develop customized vulnerability discovery, management, and remediation plans
- Conduct threat intelligence gathering and analysis to create a tailored cybersecurity plan that integrates various attack and vulnerability modeling frameworks
- Implement a proven testing methodology using industry-leading tactics and techniques
- Adapt information security approaches to target real-world enterprise challenges
- Configure and manage vulnerability assessment tools to limit risk added to the environment by the tester
- Operate enumeration tools like Nmap, Masscan, Recon-ng, and WMI to identify network nodes, services, configurations, and vulnerabilities that an attacker could use as an opportunity for exploitation
- Conduct infrastructure vulnerability enumeration at scale across numerous network segments, in spite of divergent network infrastructure and nonstandard configurations
- Conduct web application vulnerability enumeration in enterprise environments while solving complex challenges resulting from scale
- Perform manual discovery and validation of cybersecurity vulnerabilities that can be extended to custom and unique applications and systems
- Manage large vulnerability datasets and perform risk calculation and scoring against organization-specific risks
- Implement vulnerability triage and prioritize mitigation

Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organizations must become more effective at mitigating their information security risks at the enterprise scale. SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise. The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from mid-sized to large organizations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools and a proven testing methodology.

SEC460 takes you beyond the checklist, giving you a tour of the attackers' perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasizes this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions.

We wrap up the first five sections of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day against an enterprise-grade cyber range with numerous target systems for you to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your organization.

"SEC460 has provided me the knowledge to build a great Vulnerability Management/Vulnerability Assessment Program that vendor courses couldn't provide."

— Eric Osmus, **ConocoPhillips Company**

Certification: GIAC Enterprise Vulnerability Assessor (GEVA)
giac.org/geva

SEC467: Social Engineering for Security Professionals

2 Day Course	12 CPEs	Laptop Required

You Will Learn

- The psychological underpinnings of social engineering
- How to successfully execute your first social engineering test in your company or as a consultant
- Social engineering knowledge to develop new variations of attacks or increase your snare rate
- How to manage some of the ethical and risk challenges associated with social engineering engagements
- How to enhance other penetration testing disciplines by understanding human behavior and how to exploit it

Who Should Attend

- Penetration testers looking to increase their testing breadth and effectiveness
- Security defenders looking to enhance their understanding of attack techniques to improve their defenses
- Staff responsible for security awareness and education campaigns who want to understand how cyber criminals persuade their way through their defenses

Author Statement

"Social engineering has always been a critical part of the cyber criminals' toolkit and has been at the core of innumerable attacks over the years. Organizations are taking significant interest in social engineering as a part of penetration testing, yet many penetration testers do not have social engineering skills in their attack toolkit. We are passionate about changing that and opening up a new set of attack possibilities. That being said, this is an area filled with ethical challenges, risks, and even legal landmines. So we've done our best to share our experiences in the course in a way that enables people to reap the benefits of our experiences without enduring the pitfalls we have dealt with over the years."

—Dave Shackleford and James Leyte-Vidal

Social engineering is an amazingly effective technique that has one important advantage over many other attacks, it allows adversaries or testers to bypass many of the technological controls in an environment by enabling them to act as, or with the assistance of, a trusted insider.

Any organization that employs humans is subject to risk. Social engineering allows the adversary to achieve a foothold in environments where technical controls may have made gaining such a foothold very difficult. Successful social engineering utilizes psychological principles and technical techniques to measure your success, manage the associated risk, and prepare an organization for social engineering attacks.

SEC467: Social Engineering for Security Professionals provides the blend of knowledge required to add social engineering skills to your penetration testing portfolio. The course provides tools and techniques for testers to identify flaws in their environments that are vulnerable to social engineering attacks. Defenders taking this course will note common tools and techniques that will enable them to prepare responses and countermeasures within their organizations. SEC467 covers the principles of persuasion and the psychological foundations required to craft effective attacks. It then bolsters that information with numerous examples of what works, drawing on the experiences of both cyber criminals as well as the course authors. You will learn how to perform recon on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You will also learn how to conduct pretexting exercises. We'll wrap up the course with a fun Capture-the-Human exercise to put what you have learned into practice. This is the perfect course to open up new attack possibilities, better understand the human vulnerability in attacks, and practice snares that have proven themselves in tests time and time again.

Section Descriptions

SECTION 1: Social Engineering Fundamentals, Recon, and Phishing

Section one of the course introduces you to key social engineering concepts, the goals of social engineering, and a myriad of reconnaissance tools to help prepare you for successful campaigns. We complete the section with exercises centered around the most popular and scalable form of social engineering: phishing. Each exercise includes how to execute the attack, what works and what doesn't, and how to report on the attack to help the organization improve its defenses.

TOPICS: Psychology of Social Engineering; Targeting and Recon; Secure and Convincing Phishing; Tracking Clicks; Secure Phishing Forms

SECTION 2: Media Drops and Payloads, Pretexting, Physical Testing, and Reporting

Section 2 builds on the principles covered in the previous section to focus heavily on payloads for your social engineering engagements. We will cover how to avoid detection, limit the risk of your payloads causing issues, and build a bespoke payload that works and looks the part of your selected snare. We will then introduce another powerful skill with pretexting and cover how it can be combined to get payloads running. We end the section with a Capture-the-Human exercise in which students can apply their newly found skills and with a look at the top do s and don ts in an engagement.

TOPICS: USB and Media Drops; Building a Payload; Clicks That Work; Successful Pretexting; Tailgating and Physical Access; Social Engineering Reports; Social Engineering: Where It All Fits; Risky Business

SEC504: Hacker Tools, Techniques, and Incident Handling

6 Day Program | 38 CPEs | Laptop Required

You Will Learn

- How to apply a dynamic approach to incident response
- How to identify threats using host, network, and log analysis
- Best practices for effective cloud incident response
- Cyber investigation processes using live analysis, network insight, and memory forensics
- Defense spotlight strategies to protect critical assets
- Attacker techniques to evade endpoint detection tools
- How attackers exploit complex cloud vulnerabilities
- Attacker steps for internal discovery and lateral movement after an initial compromise
- The most effective attacks to bypass system access controls
- The crafty techniques attackers use, and how to stop them

The goal of modern cloud and on-premises systems is to prevent compromise, but the reality is that detection and response are critical. Keeping your organization out of the breach headlines depends on how well incidents are handled to minimize loss to the company.

In SEC504, you will learn how to apply a dynamic approach to incident response. Using indicators of compromise, you will practice the steps to effectively respond to breaches affecting Windows, Linux, and cloud platforms. You will be able to take the skills and hands-on experience gained in the course back to the office and apply them immediately.

A big focus in SEC504 is applying what you learn with hands-on exercises: 50% of the course is hands-on where you will attack, defend, and assess the damage done by threat actors. You will work with complex network environments, real-world host platforms and applications, and complex data sets that mirror the kind of work you may be asked to do. You never lose access to the lab exercises, and they can be repeated as often as you like. All lab exercises come with detailed walkthrough video content to help reinforce the learning concepts in the course.

Understanding the steps to effectively conduct incident response is only one part of the equation. To fully grasp the actions attackers take against an organization, from initial compromise to internal network pivoting, you also need to understand their tools and techniques. In the hands-on environment provided by SEC504, you ll use the tools of the attackers themselves in order to understand how they are applied and the artifacts the attackers leave behind. By getting into the mindset of attackers, you will learn how they apply their trade against your organization, and you ll be able to use that insight to anticipate their moves and build better defenses.

SEC504 can be taken in Japanese language with Japanese textbooks.

Author Statement

"Attacker tools and techniques have changed, and we need to change our incident response techniques to match. Since I took over as author of SEC504 in 2019, I have rewritten the entire course to give you the skills you need to succeed at incident response. Whether the attacks are Windows-focused or involve attacking critical database platforms or exploiting cloud vulnerabilities, you'll be prepared to effectively identify the attack, minimize the impact, and respond efficiently. With your knowledge of hacker tools and techniques, and by using defense skills that dramatically improve security, you will be ready to become the subject-matter expert your organization needs to meet today's cyber threats."

—Joshua Wright

"SEC504 is a great class overall that is perfect for pen testers and defenders alike. It has greatly helped me understand how attackers think, how they gather information, and how they maintain and gain control of systems."

—Evan Brunk, **Acuity Insurance**

"Great content! As a developer it is extremely useful to understand exploits and how better coding practices help your security position."

—Alex Colclough, **Clayton Homes**

Certification: GIAC Certified Incident Handler (GCIH)
giac.org/gcih

SEC542: Web App Penetration Testing and Ethical Hacking

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Apply OWASP's methodology to your web application penetration tests to ensure they are consistent, reproducible, rigorous, and under quality control
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization
- Understand and exploit insecure deserialization vulnerabilities with ysoserial and similar tools
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks with ZAP, BurP'S Intruder and ffuf
- Explain the impact of exploitation of web application flaws
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and BurpSuite Pro to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Manually discover and exploit Server-Side Request Forgery (SSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Use the Nuclei tool to perform scans of target web sites/servers
- Perform two complete web penetration tests, one during the five sections of course instruction, and the other during the Capture-the-Flag exercise

"Every day of SEC542 gives you invaluable information from real-world testing you cannot find in a book."

—David Fava, **The Boeing Company**

Web applications play a vital role in every modern organization. But, if your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

SEC542 helps students move beyond push-button scanning to professional, thorough, high-value web application penetration testing.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the business impact should attackers exploit discovered vulnerabilities.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 gives novice students the information and skills to become expert penetration testers with practice, and fills in all the foundational gaps for individuals with some penetration testing background.

Students will come to understand common web application flaws, as well as how to identify and exploit them with the intent of demonstrating the potential business impact. Along the way, students follow a field-tested and repeatable process to consistently find flaws. Information security professionals often struggle with helping their organizations understand risk in terms relatable to business. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help students demonstrate the true impact of web application flaws not only through exploitation but also through proper documenting and reporting.

SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to walking students through a web app penetration using more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS Netwars cyber range. This Capture-the-Flag event groups students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned throughout the course.

Business Takeaways:

- Apply a repeatable methodology to deliver high-value penetration tests
- Discover and exploit key web application flaws
- Explain the potential impact of web application vulnerabilities
- Convey the importance of web application security to an overall security posture
- Wield key web application attack tools more efficiently
- Write web application penetration test reports

Certification: GIAC Web Application Penetration Tester (GWAPT)
giac.org/gwapt

SEC554: Blockchain and Smart Contract Security

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Compile and deploy smart contracts
- Exploit vulnerable smart contracts, nodes, and private keys
- Run automated security scans on smart contracts
- Use the latest blockchain tools for development, security, auditing, and exploiting
- Trace and discover blockchain transaction information
- Set up and protect a cryptocurrency wallet
- Crack partially exposed mnemonics keys
- Send transactions to blockchain
- Set up a local ethereum blockchain for testing
- Join a cryptocurrency mining pool, or create your own mining node
- Run static analysis on EVM bytecode
- Interact with cryptocurrency on main and test networks
- Investigate, install, and prevent crypto-jacking malware
- Protect and defend against privacy attacks on blockchain

"SEC554 gives an excellent education on the next big technological revolution, taught by the folks on the front lines."

—Ravi Danesh, **BMO Financial Group**

In 2008, an anonymous author, under the pseudonym Satoshi Nakamoto, published a white paper outlining a public transaction ledger for a decentralized peer-to-peer payment system entitled Bitcoin: A Peer-to-Peer Electronic Cash System, which is regarded as the "birth" of blockchain. Since then, the use of blockchain has evolved beyond its original implementation as a cryptocurrency. It has gained momentum in recent years, being adopted by some of the largest organizations in the world, including IBM, Amazon, PayPal, Mastercard, and Walmart. However, due to the relative newness of blockchain compared to more understood and traditional technologies, its use is still hindered by speculation, confusion, uncertainty, and risk.

In SEC554: Blockchain and Smart Contract Security, you will become familiar with essential topics of blockchain and smart contract technology, including its history, design principles, architecture, business use cases, regulatory environment, and technical specifications. The course takes a detailed look at the mechanics behind the cryptography and the transactions that make blockchain work. It provides exercises that will teach you how to use tools to deploy, audit, scan, and exploit blockchain and smart contract assets. Hands-on labs and exercises will enable you to interact with various blockchain implementations, such as ethereum and bitcoin, and you'll be provided with resources to take with you to further explore.

There have already been widespread security breaches, fraud, and hacks on blockchain platforms, resulting in billions of dollars in losses. These issues, along with growing scrutiny by government agencies to find malicious users abusing the technology, is tarnishing blockchain's reputation. SEC554 approaches blockchain and smart contracts from an offensive perspective to inform students what vulnerabilities exist, how they are exploited, and how to defend against attacks that are currently leveraged today. Some of the skills and techniques you will learn are:

- How to interact with and get data from public blockchains
- How to exploit several types of smart contract vulnerabilities
- How to test and exploit weak cryptography/entropy
- How to discover and re-create private keys
- What cryptojackers do and how to trace and track movements on blockchain
- How to combat non-technical or social engineering types of attacks that adversaries use to access and steal from victims

We can see the many solutions blockchain technology can provide as a payment system, but as the technology is increasingly adopted, its attack surface will continue to grow. While there are some educational resources available for blockchain, there is relatively little educational content around blockchain security. No other training provides the comprehensive level of blockchain testing, exercises and knowledge that is delivered in SEC554.

Author Statement

"Blockchain is a revolutionary solution that solves multiple issues inherent in the social, economic, and technological challenges we face today. Decentralization and self-sovereignty are not just concepts, but fundamental ideals that should be made available and accessible for all to benefit from. But those processes need to be carried out responsibly and securely. In order to drive adoption, security must be a priority for all developers, users, or speculators interacting with blockchains or smart contracts. I've always thought the best way to protect something is to learn how to break it."
—Steven Walbroehl

SEC556: IoT Penetration Testing

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Assess IoT network-facing controls, web applications, and API endpoints with an IoT focus
- Examine hardware to discover functionality and find interaction points and use them to obtain data from the hardware
- Uncover firmware from hardware and other means, and explore it for secrets and implementation failures
- Sniff, interact with, and manipulate WiFi, LoRA, and Zigbee wireless technologies and understand security failures in implementation
- Interact with Bluetooth Low Energy (BLE) for device manipulation
- Automate recovery of unknown radio protocols to perform replay attacks and additional analysis

You Will Receive With This Course

- BusPirate 3.6a and cable
- SPI Flash integrated circuit
- Solderless breadboard
- HackRF One with antenna
- HackRF ANT500 antenna
- USB Logic analyzer
- Dupont wires
- RaspberryPi 4 8G Vilros Kit (32 Gig SD card) (Note: this comes with a U.S. plug, so international students will need to bring an adapter)
- USB wireless adapter
- TP-Link Bluetooth Low Energy USB adapter
- 433Mhz IoT remote-controlled outlet (110/120V only, EU and APAC students will need to bring a voltage converter)
- A pair of CC2531 custom-flashed USB Zigbee adapters
- USB 3.0 4-port hub
- Ethernet cable
- Custom Slingshot Linux Virtual Machine
- Custom Raspberry Pi image (PIoT.01)

A growing trend in recent years has seen small-form factor computing devices increasingly accessing networks to provide connectivity to what typically used to be disconnected devices. While we can debate if your home appliances truly need Internet access, there is no debate that the Internet of Things (IoT) is here to stay. It allows for deeper connectivity of many devices that are indeed useful, with great benefits to homes and enterprises alike.

Unfortunately, with this proliferation of connected technology, many of these devices do not consider or only minimally consider security in the design process. While we have seen this behavior in other types of testing as well, IoT is different because it utilizes and mixes together many different technology stacks such as custom Operating System builds, web and API interfaces, various networking protocols (e.g., Zigbee, LoRA, Bluetooth/BLE, WiFi), and proprietary wireless. This wide range of diverse, poorly secured technology makes for a desirable pivot point into networks, opportunities for modification of user data, network traffic manipulation, and more.

SEC556 will familiarize you with common interfaces in IoT devices and recommend a process along with the Internet of Things Attack (IoTA) testing framework to evaluate these devices within many layers of the Open Systems Interconnection (OSI) model. From firmware and network protocol analysis to hardware implementation issues and all the way to application flaws, we will give you the tools and hands-on techniques to evaluate the ever-expanding range of IoT devices. The course approach facilitates examining the IoT ecosystem across many different verticals, from automotive technology to healthcare, manufacturing, and industrial control systems. In all cases, the methodology is the same but the risk model is different.

Once we have been empowered to understand each individual challenge, we can understand the need for more secure development and implementation practices with IoT devices.

Authors Statement

"It has been amazing to watch the progression and widespread adoption of what we now know as the Internet of Things in both our homes and enterprises whether you realize it or not! However, while IoT-enabled technologies have arguably made our lives better by improving conveniences and our ability to obtain more accurate data about our environment, we unknowingly increase our attack surface through their use."

"In other words, the benefits often come at a cost, in many cases because of lackluster development practices by many IoT manufacturers that fail to consider the entirety of the attack surface of their device ecosystem. This failure is largely seen as financial; baking security in from the start is an expense that reduces the already low profit margins on IoT devices. Delays from adopting enhanced security measures can prevent a timely push to market, further compounding profit-per-device issues.

"With the increased adoption of IoT, attackers have also focused their efforts on IoT platforms. Techniques and tool capabilities have become exponentially more sophisticated, and they are often used for "good" to unlock additional features and capabilities. However, less-ethical attackers have gained the same sophistication with their toolsets, giving them the upper hand in exploiting the technology we rely on for critical tasks. The IoT adoption rate, in combination with the sophistication of attackers, paints a grave picture for the future of IoT and the networks IoT devices are connected to unless we begin now to improve the security of all facets of the IoT ecosystem.

"We are very excited to deliver interactive, hands-on labs and a suite of hardware and software tools to equip IoT analysts and developers with practical skills, methodologies, and thought processes that they can bring back to their organizations and apply on day one. The skills you will build in this class will be valuable for today's IoT technology and serve as a foundation for tomorrow's advancements, regardless of your vertical, application, or data."

–Larry Pesce, James Leyte-Vidal, and Steven Walbroehl

SEC560: Enterprise Penetration Testing

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Properly plan and prepare for an enterprise penetration test
- Perform detailed reconnaissance to aid in social engineering, phishing, and making well-informed attack decisions
- Scan target networks using best-of-breed tools to identify systems and targets that other tools and techniques may have missed
- Perform safe and effective password guessing to gain initial access to the target environment, or to move deeper into the network
- Exploit target systems in multiple ways to gain access and measure real business risk
- Execute extensive post-exploitation to move further into the network
- Use Privilege Escalation techniques to elevate access on Windows or Linux systems, or even the Microsoft Windows Domain
- Perform internal reconnaissance and situational awareness tasks to identify additional targets and attack paths
- Execute lateral movement and pivoting to further extend access to the organization and identify risks missed by surface scans
- Crack passwords using modern tools and techniques to extend or escalate access
- Use multiple Command and Control (C2, C&C) frameworks to manage and pillage compromised hosts
- Attack the Microsoft Windows domain used by most organizations
- Execute multiple Kerberos attacks, including Kerberoasting, Golden Ticket, and Silver Ticket attacks
- Conduct Azure reconnaissance
- Azure AD password spraying attacks
- Execute commands in Azure using compromised credentials
- Develop and deliver high-quality reports

As a cybersecurity professional, you have a unique responsibility to identify and understand your organization s vulnerabilities and work diligently to mitigate them before the bad actors pounce. Are you ready? SEC560, the flagship SANS course for penetration testing, fully equips you to take this task head-on.

In SEC560, you will learn how to plan, prepare, and execute a penetration test in a modern enterprise. Using the latest penetration testing tools, you will undertake extensive hands-on lab exercises to learn the methodology of experienced attackers and practice your skills. You'll then be able to take what you've learned in this course back to your office and apply it immediately.

This course is designed to strengthen penetration testers and further add to their skillset. The course is also designed to train system administrators, defenders, and others in security to understand the mindset and methodology of a modern attacker. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. Both the offensive teams and defenders have the same goal: keep the real bad guys out.

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test, and at the end of the course you'll do just that. After building your skills in comprehensive and challenging labs, the course culminates with a final real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.

Author Statement

"All security professionals need to understand modern attack tactics and principles. As a defender, incident responder, or forensic analyst, it is important to understand the latest attacks and the mindset of the attacker. In this course, penetration testers, red teamers, and other offensive security professionals will learn tools and techniques to increase the impact and effectiveness of their work. As the lead author for this course, I'm proud to bring my years of security experience (both offensive and defensive) as well as network/system administration experience to the course. We aim to provide a valuable, high-impact penetration testing course designed to teach experienced pen testers new tips, help prepare new penetration testers, and provide background to anyone dealing with penetration testers, Red Teams, or even malicious attackers. I personally enjoy teaching this course and sharing my experience and real-life examples with you."
—Tim Medin

"I think if you genuinely want to learn how exploitation techniques work and how to properly think like a hacker, it would be silly not to attend SEC560."

—Marc Hamilton, **McAfee**

Certification: GIAC Penetration Tester (GPEN)
giac.org/gpen

SEC565: Red Team Operations and Adversary Emulation

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Consume threat intelligence and plan a Red Team engagement
- Set up the required infrastructure to have a successful operation taking into account operational security
- Create weaponization that will allow you to infiltrate an organization
- Enumerate and extract valuable data required to achieve your objectives using automated tooling, but also manually, if required
- Move laterally and persist in a corporate network
- Elevate privileges using a variety of attack vectors and misconfigurations that you will now be able to identify
- Report your findings in a meaningful way to bring maximum value to your client

Prerequisites

The concepts and exercises in this course are built on the fundamentals of offensive security. An understanding of general penetration testing concepts and tools is encouraged, and a background in security fundamentals will provide a solid foundation upon which to build Red Team concepts.

Many of the Red Team concepts taught in this course are suitable for anyone in the security community. Both technical staff as well as management personnel will be able to gain a deeper understanding of Red Team exercises and adversary emulations.

Penetration testing is effective at enumerating vulnerabilities, but less effective in addressing personnel and processes on the defense side. This can leave Blue Teams or defenders without sufficient knowledge of what offensive input to improve, in turn leaving organizations stuck in a cyclical process of just focusing on vulnerabilities in systems rather than on maturing defenders to effectively detect and respond to attacks.

In SEC565, students will learn how to plan and execute end-to-end Red Teaming engagements that leverage adversary emulation, including the skills to organize a Red Team, consume threat intelligence to map against adversary tactics, techniques, and procedures (TTPs), emulate those TTPs, report and analyze the results of the Red Team engagement, and ultimately improve the overall security posture of the organization. As part of the course, students will perform an adversary emulation against a target organization modeled on an enterprise environment, including Active Directory, intelligence-rich emails, file servers, and endpoints running in Windows and Linux.

SEC565 features six intensive course sections. We will start by consuming cyber threat intelligence to identify and document an adversary that has the intent, opportunity, and capability to attack the target organization. Using this strong threat intelligence and proper planning, students will follow the Unified Kill Chain and multiple TTPs mapped to MITRE® ATT&CK™(Adversarial Tactics, Techniques, and Common Knowledge) during execution. During three course sections, students will be immersed in deeply technical Red Team tradecraft ranging from establishing resilient and advanced attack infrastructure to abusing Active Directory. After gaining initial access, students will thoroughly analyze each system, pilfer technical data and target intelligence, and then move laterally, escalating privileges, laying down persistence, and collecting and exfiltrating critically impactful sensitive data. The course concludes with an exercise analyzing the Blue Team response, reporting, and remediation planning and retesting.

In SEC565, you will learn how to show the value that Red Teaming and adversary emulations bring to an organization. The main job of a Red Team is to make a Blue Team better. Offense informs defense and defense informs offense. SEC565 develops Red Team operators capable of planning and executing consistent and repeatable engagements that are focused on training and on measuring the effectiveness of the people, processes, and technology used to defend environments.

You Will Learn How To:

- Use threat intelligence to study adversaries for emulation
- Build an adversary emulation plan
- Map actions to MITRE® ATT&CK™ to aid in communicating with the Blue Team
- Establish resilient, advanced C2 infrastructure
- Maintain operational security throughout an engagement
- Leverage initial access to elevate and propagate through a network
- Enumerate and attack Active Directory
- Collect and exfiltrate sensitive data in a safe manner
- Close an engagement, deliver value, and plan for retesting

SEC575: Mobile Device Security and Ethical Hacking

6 Day Program	36 CPEs	Laptop Required

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

Author Statement

The first iPhone was released in 2007, and it is considered by many to be the starting point of the smartphone era. Over the past decade, we have seen smartphones grow from rather simplistic into incredibly powerful devices with advanced features such as biometrics, facial recognition, GPS, hardware-backed encryption, and beautiful high-definition screens. While many different smartphone platforms have been developed over the years, it is quite obvious that Android and iOS have come out victorious.

While smartphones provide a solid experience right out of the box, the app ecosystem is probably the most powerful aspect of any mobile operating system. Both the Google Play and Apple App stores have countless applications that increase the usefulness of their platforms and include everything from games to financial apps, navigation, movies, music, and other offerings.

However, many smartphones also contain an incredible amount of data about both the personal and professional lives of people. Keeping those data secure should be a primary concern for both the operating system and the mobile application developer. Yet, many companies today have implemented a bring-your-own-device policy that allows smartphones onto their network. These devices are often not managed and thus bring a new set of security threats to the company.

This course will teach you about all the different aspects of mobile security, both at a high level and down into the nitty-gritty details. You will learn how to analyze mobile applications, attack smartphone devices on the network, man-in-the-middle either yourself or others, and root/jailbreak your device. You will also learn what kind of malware may pose a threat to your company and your employees.

Mobile security is a lot of fun, and I hope you will join us for this course so that we can share our enthusiasm with you!

Imagine an attack surface that is spread across your organization and in the hands of every user. It moves regularly from place to place, stores highly sensitive and critical data, and sports numerous, different wireless technologies all ripe for attack. Unfortunately, such a surface already exists today: mobile devices. These devices constitute the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

SEC575: Mobile Device Security and Ethical Hacking is designed to give you the skills to understand the security strengths and weaknesses of Apple iOS and Android devices, including Android 12 and iOS 15. Mobile devices are no longer a convenience technology. They are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores across the world. Users rely on mobile devices today more than ever before and the bad guys do too. SEC575 examines the full gamut of these devices.

Learn How to Pen Test the Biggest Attack Surface in Your Entire Organization

With the skills you acquire in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption and manipulate apps to circumvent client-side security techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll learn how to bypass locked screens to exploit lost or stolen devices.

Corellium for Android and iOS Emulation

Throughout the course, students will use the innovative Corellium platform to experience iOS and Android penetration testing in a realistic environment. Corellium allows users to create virtualized iOS and Android devices with full root access even on the latest versions. By using this platform, SEC575 students can immediately test their skills right in their own browser, while still having full SSH/ADB capabilities and access to a range of powerful tools.

Take a Deep Dive into Evaluating Mobile Apps and Operating Systems and Their Associated Infrastructure

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review ways to effectively communicate threats to key stakeholders. You'll learn how to use industry standards such as the OWASP Mobile Application Security Verification Standard (MASVS) to assess an application and understand all the risks so that you can characterize threats for managers and decision-makers.

Your Mobile Devices Are Going to Come Under Attack: Help Your Organization Prepare for the Onslaught

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure to attackers of enterprise secrets, intellectual property, and personally identifiable information assets. Further complicating matters, there simply are not enough professionals with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as someone prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test. These are all critical skills to protect and defend mobile device deployments.

Certification: GIAC Mobile Device Security Analyst (GMOB)
giac.org/gmob

SEC580: Metasploit for Enterprise Penetration Testing

2 Day Course	12 CPEs	Laptop Required

Who Should Attend

- IT security engineers
- Penetration testers
- Security consultants
- Vulnerability assessment personnel
- Vulnerability management personnel
- Network security analysts
- Auditors
- General security engineers
- Security researchers

"SEC580 is the best course available on the planet for in-depth knowledge of Metasploit."

— Tom Reeves, **Northrup Grumman**

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of these tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers confirm vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

SEC580 will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, and according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, anti-virus evasion, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created to exploit and analyze security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

Author Statement

"Metasploit is the most popular free exploitation tool available today. It is in widespread u penetration testers, vulnerability assessment personnel, auditors, and real-world threat a However, most of its users rely on and understand only about 10 percent of its functionali not realizing the immensely useful other features that Metasploit offers. This course will e students to master the 10 percent they currently rely on (applying it in a more comprehen safe manner), while unlocking the other 90 percent of features they can then apply to mal tests more effective. By attending this course, students will learn how to make a free tool the power of many much more costly commercial tools."

— Jeff McJunkin

SEC588: Cloud Penetration Testing

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Conduct cloud-based penetration tests
- Assess cloud environments and bring value back to the business by locating vulnerabilities
- Understand first-hand how cloud environments are constructed and how to scale factors into the gathering of evidence
- Assess security risks in Amazon and Microsoft Azure environments, the two largest cloud platforms in the market today
- Immediately apply what you have learned to your work

Aim Your Arrows To The Sky And Penetrate The Cloud

You have been asked to perform a penetration test, security assessment, maybe an Attacker Simulation or a red team exercise. The environment in question is mainly cloud-focused. It could be entirely cloud-native for the service provider or Kubernetes-based. Perhaps the environment in question is even multi-cloud, having assets in both Amazon and Azure. What if you have to assess Azure Active Directory, Amazon Web Services (AWS) workloads, serverless functions, or Kubernetes? SEC588: Cloud Penetration Testing will teach you the latest penetration testing techniques focused on the cloud and how to assess cloud environments.

Computing workloads have been moving to the cloud for years. Analysts predict that most, if not all, companies will have soon have workloads in public and other cloud environments. While organizations that start in a cloud-first environment may eventually move to a hybrid cloud and local data center solution, cloud usage will not decrease significantly. So when assessing risks to an organization going forward, we need to be prepared to evaluate the security of cloud-delivered services.

The most commonly asked questions regarding cloud security when it comes to penetration testing are: Do I need to train specifically for engagements that are cloud-specific? and Can I accomplish my objectives with other pen test training and apply it to the cloud? In cloud-service-provider environments, penetration testers will not encounter a traditional data center design, there will be new attack surface areas in the service (control) planes of these environments. Learning how such an environment is designed and how you as a tester can assess what is in it is a niche skill set that must be honed. What we rely on to be true in a classical data center environment such as who owns the Operating System and the infrastructure and how the applications are running will likely be very different. Applications, services, and data will be hosted on a shared hosting environment unique to each cloud provider.

SEC588: Cloud Penetration Testing draws from many skill sets required to assess a cloud environment properly. If you are a penetration tester, the course will provide a pathway to understanding how to take your skills into cloud environments. If you are a cloud-security-focused defender or architect, the course will show you how the attackers are abusing cloud infrastructure to gain a foothold in your environments.

The course dives into topics of classic cloud Virtual Machines, buckets, and other new issues that appear in cloud-like microservices, in-memory data stores, files in the cloud, serverless functions, Kubernetes meshes, and containers. It also covers Azure and AWS penetration testing, which is particularly important given that AWS and Microsoft account for more than half of the market. The goal is not to demonstrate these technologies but to teach you how to assess and report on the actual risk your organization could face if these services are left insecure.

"SANS course SEC588 taught me more than I expected. With the rapid development of new technologies offered by cloud providers, SEC588 has given me an important framework for cloud pen testing."

—Jonus Gerrits, **Phillips 66**

"This emerging course perfectly complements the change in the direction of red team engagement scopes."

—Kyle Spaziani, **Sanofi**

Certification: GIAC Cloud Penetration Tester (GCPN)
giac.org/gcpn

SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Understand how recent high-profile attacks were delivered and how they could have been stopped
- Implement security controls throughout the different phases of the Cyber Kill Chain and the MITRE ATT&CK framework to prevent, detect, and respond to attacks

Topics To Be Addressed

- Leveraging MITRE ATT&CK as a "common language" in the organization
- Building your own Cuckoo sandbox solution to analyze payloads
- Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlighting key bypass strategies for script controls (unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

You just got hired to help our virtual organization "SYNCTECHLABS" build out a cybersecurity capability. On your first day, your manager tells you: "We looked at some recent cybersecurity trend reports and we feel like we've lost the plot. Advanced persistent threats, ransomware, denial of service...We're not even sure where to start!"

Cyber threats are on the rise: ransomware tactics are affecting small, mid-size, and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses will arm you with the knowledge and expertise you need to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries.

Course authors Stephen Sims and Erik Van Buggenhout (both certified as GIAC Security Experts) are hands-on practitioners who have built a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked the question: "How do I prevent or detect this type of attack?" Well, this is it! SEC599 gives students real-world examples of how to prevent attacks. The course features more than 20 labs plus a full-day Defend-the-Flag exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment.

Our six-part journey will start off with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce formal descriptions of adversary behavior such as the Cyber Kill Chain and the MITRE ATT&CK framework. In order to understand how attacks work, you will also compromise our virtual organization "SYNCTECHLABS" in section one exercises.

In sections two through five, we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. The topics to be addressed include:

- Leveraging MITRE ATT&CK as a "common language" in the organization
- Building your own Cuckoo sandbox solution to analyze payloads
- Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlighting key bypass strategies for script controls (Unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

SEC599 will finish with a bang. During the Defend-the-Flag Challenge on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren't slowing down, so what are you waiting for?

Certification: GIAC Defending Advanced Threats (GDAT)
giac.org/gdat

SEC617: Wireless Penetration Testing and Ethical Hacking

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless devices to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks
- Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones
- Implement a WPA2 Enterprise penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilize Scapy to force custom packets to manipulate wireless networks in new ways, quickly building custom attack tools to meet specific penetration test requirements
- Identify WiFi attacks using network packet captures traces and freely available analysis tools
- Identify and exploit shortcomings in the security of proximity key card systems
- Decode proprietary radio signals using Software-Defined Radio
- Mount a penetration test against numerous standards-based or proprietary wireless technologies

"SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks."

— Garret Picchioni, **Salesforce**

"I have a better understanding of the technologies and protocols in use and can now perform more accurate risk assessments."

— Shawn Pray, **Accenture**

This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers.

The authors of SEC617, as penetration testers themselves, know that many organizations overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now commonplace in executive suites, financial departments, government offices, manufacturing production lines, retail networks, medical devices, and air traffic control systems. Given the known risks of insecure wireless technologies and the attacks used against them, SEC617 was designed to help people build the vital skills needed to identify, evaluate, assess, and defend against these threats. These skills are 'must-have' for any high-performing security organization.

For many analysts, "wireless" was once synonymous with "Wi-Fi," the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning – not only encompassing the security of Wi-Fi systems, but also the security of Bluetooth, Zigbee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of Wi-Fi networks and identify the Wi-Fi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern Wi-Fi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in Wi-Fi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking Wi-Fi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android Wi-Fi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device's security for use within your organization.

Beyond analyzing Wi-Fi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilized in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of Zigbee and Z-Wave wireless systems used for automation, control, and smart home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises to exploit the same kinds of flaws discovered in mass transit smart card systems, hotel guest room access systems, and more.

In addition to standards-based wireless systems, we also dig deeper into the radio spectrum using software-defined radio (SDR) systems to scour for signals. Using SDR, you will gain new insight into how widely pervasive wireless systems are deployed. With your skills in identifying, decoding, and evaluating the data these systems transmit, you will be able to spot vulnerabilities even in custom wireless infrastructures.

Certification: GIAC Assessing and Auditing Wireless Networks (GAWN)
giac.org/gawn

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Perform fuzz testing to enhance your company's SDL process
- Exploit network devices and assess network application protocols
- Escape from restricted environments on Linux and Windows
- Test cryptographic implementations
- Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
- Develop more accurate quantitative and qualitative risk assessments through validation
- Demonstrate the needs and effects of leveraging modern exploit mitigation controls
- Reverse-engineer vulnerable code to write custom exploits

This course is designed as a logical progression point for those who have completed SEC560: Network Penetration Testing and Ethical Hacking, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of section one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Section two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the section is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Section three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Sections four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course section is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

Among the biggest benefits of SEC660 is the expert-level hands-on guidance provided through the labs and the additional time allotted each evening to reinforce daytime material and master the exercises.

"SEC660 is the right balance between theory and practice; it's hands-on, not too hard, but also not too easy."

— Anton Ebertzeder, **Siemens AG**

Certification: GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
giac.org/gxpn

SEC661: ARM Exploit Development

2 Day Course	12 CPEs	Laptop Required

You Will Learn:

- Techniques for running ARM in an emulated environment
- The fundamentals of ARM assembly
- How to write ARM exploits to leverage stack-based buffer overflows
- Exploit mitigations and common workarounds
- How to work with ARM shellcode
- Return Oriented Programming (ROP)
- How to exploit IoT devices in ARM
- 64-bit ARM exploit development

Prerequisites:

- Familiarity with some type of assembly language is recommended. We will cover some of the basics in class, but any assembly experience would be a great head start.
- Working knowledge of the C programming language
- Familiarity with the Linux operating system, including navigating the file system and running basic commands, as well as using a console-based editor such as vim or nano.
- Ability to edit and run basic Python scripts

The Internet of Things (IoT) has taken over. Everywhere we look we see more systems coming online, from routers to refrigerators. But as these systems become more and more integrated into our home and business networks, how does their security posture keep up with their increasing popularity? The Advanced Reduced instruction set computing Machines architecture (ARM) introduced a new family of computer processors that provide a robust platform that is ideal for running a wide variety of small, specialized systems.

Unfortunately, the rapid expansion of new devices coming to market, along with accelerated development lifecycles, mean that security is often an afterthought. The security posture of many IoT devices is further restricted due to hardware limitations and the need to maintain low production costs.

Now more than ever, there is a demand for highly skilled security professionals who understand IoT vulnerabilities and ARM exploitation. However, the complexity of exploit development and the difficulty of acquiring and analyzing the software that runs on IoT systems can create intimidating barriers to those wanting to enter this field.

SEC661: ARM Exploit Development is designed to break down those barriers. It has been built from the ground up to give students a solid foundation in exploit development on the ARM platform. The course starts by going over the fundamentals of the architecture and some basic ARM assembly. Initial emphasis is placed on key data structures and how they work together so that students gain a better understanding of why certain vulnerabilities occur.

Students are provided with the tools they need to set up and work in an ARM environment. From there, we go through several hands-on labs that explore memory corruption vulnerabilities and show how to craft custom input in order to gain control of execution. We will also cover common exploit mitigations and techniques for bypassing them. Finally, students will demonstrate their understanding of the core concepts taught in this highly technical course by crafting their own exploits against two emulated ARM routers.

Author Statement

"If you have been looking to get into exploit development or are looking to grow and solidify your skills, this course was designed for you. ARM is taking the world by storm. With billions of new devices being introduced each year, understanding the fundamentals of security vulnerabilities in ARM and how they can be exploited is a valuable skill that will continue to be in high demand for years to come. My goal in writing this course is to ignite the passion within you and equip you with the skills you need to take you to the next level."

— John deGruyter

SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

5 Day Program	30 CPEs	Laptop Required

Business Takeaways

- Build realistic adversary emulation plans to better protect your organization
- Deliver advanced attacks, including application whitelisting bypasses, cross-forest attacks (abusing delegation), and stealth persistence strategies
- Building SIGMA rules to detect advanced adversary techniques

Prerequisites

- This is a fast-paced, advanced course that requires a strong desire to learn advanced red and blue team techniques. The following SANS courses are recommended either prior to or as a companion to taking this course: SEC599 and SEC560.
- Experience with programming in any language is highly recommended. At a minimum, students are advised to read up on basic programming concepts.
- You should also be well versed with the fundamentals of penetration testing prior to taking this course. Familiarity with Linux and Windows is mandatory. A solid understanding of TCP/IP and networking concepts is required. Please contact the author at **evanbuggenhout@nviso.be** if you have any questions or concerns about the prerequisites.

SEC699 is SANS' advanced purple team offering, with a key focus on adversary emulation for data breach prevention and detection. Throughout this course, students will learn how real-life threat actors can be emulated in a realistic enterprise environment. In true purple fashion, the goal of the course is to educate students on how adversarial techniques can be emulated and detected.

A natural follow-up to SEC599, this is an advanced SANS course offering, with 60 percent of class time spent on labs. Highlights of class activities include:

- A course section on typical automation strategies such as Ansible, Docker and Terraform. These can be used to deploy a full multi-domain enterprise environment for adversary emulation at the press of a button
- Building a proper process, tooling, and planning for purple teaming
- Building adversary emulation plans that mimic real-life threat actors such as APT-28, APT-34, and Turla in order to execute these plans using tools such as Covenant and Caldera
- In-depth techniques such as Kerberos Delegation attacks, Attack Surface Reduction/Applocker bypasses, AMSI, Process Injection, COM Object Hi-jacking and many more...
- SIGMA rule-building to detect the above techniques

Course authors Erik Van Buggenhout (the lead author SEC599) and James Shewmaker (the co-author SEC660) are both certified GIAC Security Experts (GSEs) and are hands-on practitioners who have built a deep understanding of how cyber attacks work through both red team (penetration testing) and blue team (incident response, security monitoring, threat hunting) activities. In this course, they combine these skill sets to educate students on adversary emulation methods for data breach prevention and detection.

The SEC699 journey is structured as follows:

- In Section 1, we will lay the foundations that are required to perform successful adversary emulation and purple teaming. As this is an advanced course, we will go in-depth on several tools that we'll be using and learn how to further extend existing tools.
- Sections 2–4 will be heavily hands-on lecturing a number of advanced techniques and their defenses (focused on detection strategies). Section 2 focuses on Initial Access techniques, Section 3 covers Lateral Movement and Privilege Escalation, while Section 4 deals with Persistence.
- Finally, in Section 5, we will build an emulation plan for a variety of threat actors. These emulation plans will be executed in Covenant, Caldera, and Prelude Operator.

Author Statement

After the success of SEC599, I'm very excited to unleash this course offering upon the SANS audience! SEC699 is an amazing course that came about because we listened to student requests for a hands-on adversary emulation class leveraging an enterprise lab environment. This is it!

SEC699 attendees will learn advanced red and blue team techniques for proper purple teaming in an enterprise environment. Throughout the week we do not just focus on explaining tips and tricks, but also empower students to build and adapt their own tooling for proper adversary emulation. This includes, for example, custom Caldera, SIGMA and Velociraptor development.

The SEC699 lab environment is fully built using Teraform playbooks and covers multiple domains and forests that can be attacked! Students spin up the lab environment in their own AWS account and can thus keep on practicing months (and years) after they took the class!

—Erik Van Buggenhout

SEC760: Advanced Exploit Development for Penetration Testers

6 Day Program	46 CPEs	Laptop Required

You Will Be Able To

- Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems.
- Use the advanced features of IDA Pro and write your own IDAPython scripts.
- Perform remote debugging of Linux and Windows applications.
- Understand and exploit Linux heap overflows.
- Fuzz closed-source applications
- Unpack and examine Windows update packages
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities.
- Perform Windows Kernel debugging B
- Reverse engineer and exploit Windows kernel drivers

What You Will Receive

- A four-month license to IDA Pro, which is provided by Hex-Rays, is included in this course. In order to obtain the license, you must agree to the terms, including providing your name and an e-mail address, so that Hex-Rays may assign the license. After the course ends, students may choose to extend the license at a discounted rate by contacting Hex-Rays. (If you choose to opt-out, then you must bring a copy of IDA Pro 7.4 advanced or later.)
- Various preconfigured virtual machines, such as Windows 10
- Various tools on a course USB that are required for use in class
- Access to the in-class Virtual Training Lab with many in-depth labs
- Access to recorded course audio to help hammer home important network penetration testing lessons

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skill set to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skill set regardless of the increased complexity. SEC760: Advanced Exploit Development for Penetration Testers, the SANS Institute's only 700-level course, teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, kernel and driver exploitation, one-day exploitation through patch analysis, and other advanced attacks
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success

Authors' Statement

"As a perpetual student of information security, I am excited to offer SEC760: Advanced Exploit Writing for Penetration Testers. Exploit development is a hot topic as of late and will continue to increase in importance moving forward. With all of the modern exploit mitigation controls offered by operating systems such as Windows 7 and 8, the number of experts with the skills to produce working exploits is highly limited. More and more companies are looking to hire professionals with the ability to conduct a Secure-SDLC process, perform threat modeling, determine if vulnerabilities are exploitable, and carry out security research. This course was written to help you get into these highly sought-after positions and to teach you cutting-edge tricks to thoroughly evaluate a target, providing you with the skills to improve your exploit development."
—Stephen Sims

"Teaching and helping author SEC760: Advanced Exploit Writing for Penetration Testers has given me the opportunity to distill my past experiences in exploit writing and technical systems knowledge into a format worth sharing. This course is meant to give you a look into a number of different exploitation techniques and serves as an amazing jumping-off point for exploitation of any modern application or system. Even if you don't plan on having a career in exploit writing or vulnerability research, this course will be valuable in understanding the thought process that goes into constructing an exploit and what technologies exist to stop an exploit writer from being successful."
—Jaime Geiger

SANS CURRICULUM FOCUS AREA

Digital Forensics & Incident Response (DFIR) and Threat Hunting

Organizations of all sizes need personnel who can master incident response techniques to properly identify compromised systems, provide effective containment of the breach, and rapidly remediate the incident.

Similarly, government and law enforcement agencies require skilled personnel to perform media exploitation and recover key evidence from adversary systems and devices. SANS Incident Response, Threat Hunting and Digital Forensics will teach you to:

- Hunt for the adversary before and during an incident across your enterprise
- Acquire in-depth digital forensics knowledge of Microsoft Windows and Apple OSX operating systems
- Examine portable smartphone and mobile devices to look for malware and digital forensic artifacts
- Incorporate network forensics into your investigations, providing better findings and getting the job done faster
- Leave no stone unturned by incorporating memory forensics into your investigations
- Triage, preserve, configure and examine new sources of evidence that only exist in the cloud and incorporate these new sources into your investigations
- Understand the capabilities of malware to derive threat intelligence, respond to information security incidents, and fortify defenses
- Identify, extract, prioritize, and leverage cyber threat intelligence from advanced persistent threat (APT) intrusions
- Recognize that a properly trained incident responder could be the only defense an organization has during a compromise
- Properly identify, collect, preserve, and respond to data from a wide range of storage devices and repositories, ensuring that the integrity of the evidence is beyond reproach
- Deal with the specifics of ransomware to prepare for, detect, hunt, respond to, and deal with the aftermath of ransomware
- Hunt for threat intelligence within the cybercriminal underground using Human Intelligence (HUMINT) elicitation techniques and blockchain analytics tools to trace criminal cryptocurrency transactions

Enhance your training with:

- DFIR Netwars: **sans.org/netwars**
- SANS Summits: DFIR; Threat Hunting and Incident Response; and Cyber Threat Intelligence **sans.org/summit**
- Free Resources: Webcasts, blogs, research, and other features like SIFT Workstation and EZ Tools **digital-forensics.sans.org**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a Graduate Certificate in Incident Response **sans.edu**

Digital Forensics & Incident Response (DFIR) and Threat Hunting Job Roles:

- Threat Hunter
- Digital Forensics Analyst
- Malware Analyst
- Cloud Security Analyst
- Incident Responder
- Media Exploitation Analyst
- Threat Intelligence Analyst
- Law Enforcement Professional

FOR498: Battlefield Forensics & Data Acquisition

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where they are stored
- Handle and process a scene properly to maintain evidentiary integrity
- Perform data acquisition from at-rest storage, including both spinning media and solid-state storage
- Identify the numerous places that data for an investigation might exist
- Perform Battlefield Forensics by going from evidence seizure to actionable intelligence in 90 minutes or less
- Assist in preparing the documentation necessary to communicate with online entities such as Google, Facebook, Microsoft, etc.
- Understand the concepts and usage of large-volume storage technologies, including JBOD, RAID storage, NAS devices, and other large-scale, network-addressable storage
- Identify and collect user data within large corporate environments where they are accessed using SMB
- Gather volatile data such as a computer system's RAM
- Recover and properly preserve digital evidence on cellular and other portable devices
- Address the proper collection and preservation of data on devices such as Microsoft Surface/ Surface Pro, where hard-drive removal is not an option
- Address the proper collection and preservation of data on Apple devices such as MacBook, MacBook Air, and MacBook Pro, where hard-drive removal is not an option
- Properly collect and effectively target email from Exchange servers, avoiding the old-school method of full acquisition and subsequent onerous data culling
- Properly collect data from SharePoint repositories
- Access and acquire online mail stores such as Gmail, Hotmail, and Yahoo Mail accounts

"In DFIR, things rarely go as planned. This course teaches you about the options to control when things aren't working as expected."

— J-Michael Roberts, **Corvus Forensics**

THE CLOCK IS TICKING. YOU NEED TO PRIORITIZE THE MOST VALUABLE EVIDENCE FOR PROCESSING. LET US SHOW YOU HOW.

The FOR498: Digital Acquisition and Rapid Triage course will help you to:

- Acquire data effectively from:
  - PCs, Microsoft Surface, and Tablet PCs
  - Apple Devices, Mac, and Macbooks
  - RAM and memory
  - Smartphones and portable mobile devices
  - Cloud storage and services
  - Network storage repositories
- Produce actionable intelligence in 90 minutes or less

The first step in any investigation is the gathering of evidence. Digital forensic investigations are no different. The evidence used in this type of investigation is data, and this data can live in many varied formats and locations. You must be able to first identify the data that you might need, determine where that data resides, and, finally, formulate a plan and procedures for collecting that data.

With digital forensic acquisitions, you will typically have only one chance to collect data properly. If you manage the acquisition incorrectly, you run the risk of not only damaging the investigation, but more importantly, destroying the very data that could have been used as evidence.

With the wide range of storage media in the marketplace today, any kind of standardized methodology for all media is simply untenable. Many mistakes are being made in digital evidence collection, and this can cause the guilty to go free and, more importantly, the innocent to be incarcerated. The disposition of millions and millions of dollars can rest within the bits and bytes that you are tasked with properly collecting and interpreting.

An examiner can no longer rely on "dead box" imaging of a single hard drive. In today's cyber sphere, many people utilize a desktop, laptop, tablet, and cellular phone within the course of a normal day. Compounding this issue is the expanding use of cloud storage and providers, and the proper collection of data from all these domains can become quite overwhelming.

This in-depth digital acquisition and data handling course will provide first responders and investigators alike with the advanced skills necessary to properly respond to, identify, collect, and preserve data from a wide range of storage devices and repositories, ensuring that the integrity of the evidence is beyond reproach. Constantly updated, FOR498 addresses today's need for widespread knowledge and understanding of the challenges and techniques that investigators require when addressing real-world cases.

Numerous hands-on labs throughout the course will give first responders, investigators, and digital forensics teams practical experience needed when performing digital acquisition from hard drives, memory sticks, cellular phones, network storage areas, and everything in between.

During a digital forensics response and investigation, an organization needs the most skilled responders possible, lest the investigation end before it has begun. FOR498: Battlefield Forensics & Acquisition will train you and your team to respond, identify, collect, and preserve data no matter where that data hides or resides.

Certification: GIAC Battlefield Forensics and Acquisition (GBFA)
giac.org/gbfa

FOR500: Windows Forensic Analysis

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform in-depth Windows forensic analysis by applying peer-reviewed techniques focusing on Windows 7, Windows 8/8.1, Windows 10, Windows 11, and Windows Server products
- Use state-of-the-art forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geolocation, browser history, profile USB device usage, cloud storage usage, and more
- Perform "fast forensics" to rapidly assess and triage systems to provide quick answers and facilitate informed business decisions
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), email analysis, and Windows Registry parsing
- Audit cloud storage usage, including detailed user activity, identifying deleted files, signs of data exfiltration, and even uncovering detailed information on files available only in the cloud
- Identify items searched by a specific user on a Windows system to pinpoint the data and information that the suspect was interested in finding, and accomplish detailed damage assessments
- Use Windows Shell Bag analysis tools to articulate every folder and directory a user or attacker interacted with while accessing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders accessed on it, and what user plugged it in by parsing Windows artifacts such as Registry hives and Event Log files
- Learn Event Log analysis techniques and use them to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver
- Mine the Windows Search Database to uncover a massive collection of file metadata and even file content from local drives, removable media, and applications like Microsoft Outlook, OneNote, SharePoint, and OneDrive
- Determine where a crime was committed using Registry data and pinpoint the geolocation of a system by examining connected networks and wireless access points
- Use browser forensic tools to perform detailed web browser analysis, parse raw SQLite and ESE databases, and leverage session recovery artifacts to identify web activity, even if privacy cleaners and in-private browsing software are used
- Parse Electron Application databases allowing the investigation of hundreds of third-party applications including most chat clients
- Specifically determine how individuals used a system, who they communicated with, and files that were downloaded, modified, and deleted

MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT THE UNKNOWN

All organizations must prepare for cybercrime occurring on computer systems and within corporate networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Corporations, governments, and law enforcement agencies increasingly require trained forensics specialists to perform investigations, recover vital intelligence from Windows systems, and ultimately get to the root cause of the crime. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation experts capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and available artifacts is a core component of information security. You will learn how to recover, analyze, and authenticate forensic data on Windows systems, track individual user activity on your network, and organize findings for use in incident response, internal investigations, intellectual property theft inquiries, and civil or criminal litigation. You'll be able to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data and use it to your advantage.

Proper analysis requires real data for students to examine. This continually updated course trains digital forensic analysts through a series of hands-on laboratory exercises incorporating evidence found on the latest technologies, including Microsoft Windows versions 10 and 11, Office and Microsoft 365, Google Workspace (G Suite), cloud storage providers, Microsoft Teams, SharePoint, Exchange, and Outlook. Students will leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows 7 systems to just-discovered Windows 11 artifacts.

FOR500: Windows Forensic Analysis will teach you to:

- Conduct in-depth forensic analysis of Windows operating systems and media exploitation on Windows XP, Windows 7, Windows 8/8.1, Windows 10, Windows 11 and Windows Server products
- Identify artifact and evidence locations to answer crucial questions, including application execution, file access, data theft, external device usage, cloud services, device geolocation, file transfers, anti-forensics, and detailed system and user activity
- Become tool-agnostic by focusing your capabilities on analysis instead of how to use a particular tool
- Extract critical findings and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

FOR500 starts with an intellectual property theft and corporate espionage case taking over six months to create. You work in the real world, so your training should include real-world practice data. Our instructor course development team used incidents from their own investigations and experiences to create an incredibly rich and detailed scenario designed to immerse students in an actual investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems in the enterprise. The detailed workbook teaches the tools and techniques that every investigator should employ step by step to solve a forensic case. The tools provided for a complete forensic lab that can be used after the end of class.

Certification: GIAC Certified Forensic Examiner (GCFE)
giac.org/gcfe

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker's presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection

"FOR508 exceeded my expectations in every way. It provided me the skills, knowledge, and tools to effectively respond to and handle APTs and other enterprise-wide threats."

— Josh M., **U.S. Federal Agency**

ADVANCED THREATS ARE IN YOUR NETWORK – IT'S TIME TO GO HUNTING!

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident or contain propagating ransomware. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions. This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and ransomware syndicates.

FOR508: Advanced Incident Response and Threat Hunting Course will help you to:

- Understand attacker tradecraft to perform compromise assessments
- Detect how and when a breach occurred
- Quickly identify compromised and infected systems
- Perform damage assessments and determine what was read, stolen, or changed
- Contain and remediate incidents of all types
- Track adversaries and develop threat intelligence to scope a network
- Hunt down additional breaches using knowledge of the adversary
- Build advanced forensics skills to counter anti-forensics and data hiding from technical subjects

The course exercises and final challenges illustrate real attacker traces found via end point artifacts, event logs, system memory, and more:

- **Phase 1**—Patient zero compromise and malware C2 beacon installation
- **Phase 2**—Privilege escalation, lateral movement to other systems, malware utilities download, installation of additional beacons, and obtaining domain admin credentials
- **Phase 3**—Searching for intellectual property, network profiling, business email compromise, dumping enterprise hashes
- **Phase 4**—Find exfiltration point, collect and stage data for theft
- **Phase 5**—Exfiltrate files from staging server, perform cleanup and set long-term persistence mechanisms (alternatively this phase would be used to deploy ransomware)

Business Takeaways

- Understand attacker tradecraft to perform proactive compromise assessments
- Upgrade detection capabilities via better understanding of novel attack techniques, focus on critical attack paths, and knowledge of available forensic artifacts
- Develop threat intelligence to track targeted adversaries and prepare for future intrusion events
- Build advanced forensics skills to counter anti-forensics and data hiding from technical subjects for use in both internal and external investigations

Certification: GIAC Certified Forensic Analyst (GCFA)
giac.org/gcfa

FOR509: Enterprise Cloud Forensics and Incident Response

6 Day Program	36 CPEs	Laptop Required

Course Topics

- Cloud Infrastructure and IR data sources
- Microsoft 365 and Graph API Investigations
- Azure Incident Response
- AWS Incident Response
- Google Workspace Investigations
- GCP Incident Response

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where it is located
- Identify and utilize new data only available from cloud environments
- Utilize cloud-native tools to capture and extract traditional host evidence
- Quickly parse and filter large data sets using scalable technologies such as the Elastic Stack
- Understand what data is available in various cloud environments

What You Will Receive

- SOF-ELK(R) Virtual Machine – a publicly SOF-ELK(R) Virtual Machine - a publicly available appliance running the Elastic Stack and the course author's custom set of configurations and lab data. The VM is preconfigured to ingest cloud logs from Microsoft 365, Azure, AWS, Google Workspace and GCP. It will be used during the class to help students wade through the large number of records they are likely to encounter during a typical investigation.
- Case data to examine during class.
- Electronic workbook with detailed step-by-step instructions and examples to help you master cloud forensics

"FOR509 was absolutely awesome! The depth of knowledge is unparalleled. I see this becoming a very popular class in the future."

—Terrie Myerchin, **AT&T**

Find the Storm in the Cloud

FOR509: Enterprise Cloud Forensics and Incident Response will help you:

- Understand forensic data only available in the cloud
- Implement best practices in cloud logging for DFIR
- Learn how to leverage Microsoft Azure, AWS and Google Cloud Platform resources to gather evidence
- Understand what logs Microsoft 365 and Google Workspace have available for analysts to review
- Learn how to move your forensic processes to the cloud for faster data processing

With FOR509: Enterprise Cloud Forensics and Incident Response, examiners will learn how each of the major cloud service providers (Microsoft Azure, Amazon AWS and Google Cloud Platform) are extending analysts capabilities with new evidence sources not available in traditional on-premise investigations. From cloud equivalents of network traffic monitoring to direct hypervisor interaction for evidence preservation, forensics is not dead. It is reborn with new technologies and capabilities.

Incident response and forensics are primarily about following breadcrumbs left behind by attackers. These breadcrumbs are primarily found in logs. Your knowledge of the investigation process is far more important than the mechanics of acquiring the logs.

This class is primarily a log analysis class to help examiners come up to speed quickly with cloud based investigation techniques. It's critical to know which logs are available in the cloud, whether they are turned on by default, and how to interpret the meaning of the events they contain.

Numerous hands-on labs throughout the course will allow examiners to access evidence generated based on the most common incidents and investigations. Examiners will learn where to pull data from and how to analyze it to find evil. The data will be available in your VM rather than accessed directly via the cloud to ensure a consistent lab experience.

Business Takeaways

- Understand digital forensics and incident response as it applies to the cloud
- Identify malicious activities within the cloud
- Cost-effectively use cloud-native tools and services for DFIR
- Ensure the business is adequately prepared to respond to cloud incidents
- Decrease adversary dwell time in compromised cloud deployments

"Thanks a lot for FOR509 course. I believe this course provides a great way to get a really compressed introduction into the different cloud service providers and what is forensically possible there."

—Marc Stroebel, **HvS-Consulting AG**

Certification: GIAC Cloud Forensics Responder (GCFR)
giac.org/gcfr

FOR518: Mac and iOS Forensic Analysis and Incident Response

6 Day Program	36 CPEs	Laptop Required

IMPORTANT NOTE: MAC HARDWARE REQUIRED

You Will Be Able To

- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals' usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyze and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- Acquire and analyze memory from Mac systems
- Acquire iOS and analyze devices in-depth

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

This consistently updated FOR518 course provides the techniques and skills necessary to take on any Mac or iOS case without hesitation. The intense hands-on forensic analysis and incident response skills taught in the course will enable analysts to broaden their capabilities and gain the confidence and knowledge to comfortably analyze any Mac or iOS device. In addition to traditional investigations, the course presents intrusion and incident response scenarios to help analysts learn ways to identify and hunt down attackers that have compromised Apple devices.

FORENSICATE DIFFERENTLY!

FOR518: Mac and iOS Forensic Analysis and Incident Response will teach you:

- Mac and iOS Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) and Apple File System (APFS) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- User and Device Activity: How to understand, profile, and conduct advanced pattern-of-life on users and they devices through their data files and preference configurations.
- Advanced Intrusion Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Apple Technologies: How to understand and analyze many Mac and iOS-specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

FOR518: Mac and iOS Forensic Analysis and Incident Response aims to train a well-rounded investigator by diving deep into forensic and intrusion analysis of Mac and iOS. The course focuses on topics such as the HFS+ and APFS file systems, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who completes this course will have the skills needed to take on a Mac or iOS forensics case.

"It was very interesting to learn that certain 'forensic' tools could report data as being encrypted even though one could still get other data."

— Gary Titus; **Stroz Friedberg LLC**

"Within the first two days or training, I had enough knowledge to go back to work and solve two outstanding issues."

— Beau G., **Information Systems Solutions**

Certification: GIAC iOS and macOS Examiner (GIME)
giac.org/gime

FOR528: Ransomware for Incident Responders

4 Day Program	24 CPEs	Laptop Required

Who Should Attend

- Information security professionals who want to learn how to collect, parse, and analyze forensic artifacts in support of ransomware incident response
- Incident response team members who need to use deep-dive digital forensics to help solve their Windows data breach and intrusion cases, perform damage assessments, and develop indicators of compromise
- Incident triage analysts such as those working in a Security Operations Center, Computer Incident Response Team, or similar
- Managed Services Provider (MSP) and Managed Security Services Providers (MSSPs) analysts who may need to aid in ransomware incident response
- Law enforcement officers, federal agents, and detectives who want to become deep subject-matter experts on ransomware investigations
- Medical and hospitality IT staff who may need to response to ransomware events
- Anyone interested in a deep understanding of Ransomware-specific Incident Response who has a background in information systems, information security, computers

You Will Be Able To

- Ransomware Evolution and History
- Windows Forensics Artifacts Critical to Ransomware Incident Response
- Evidence Acquisition Tools and Techniques
- Initial Access
- Execution and Defense Evasion
- Persistence
- Privilege Escalation and Credential Access
- Lateral Movement
- Active Directory Attacks
- Data Access
- Data exfiltration
- Archive creation and data staging
- Data exfiltration routes
- Backup and Recovery tampering
- Payload deployment
- Encryption specifics including source code review
- Decryptors
- Cobalt Strike architecture, components, and payloads
- Dealing with an active threat
- Conti ransomware operations case study
- Hunting methods and techniques

Learning to thwart the threat of human-operated ransomware once and for all!

The term "Ransomware" no longer refers to a simple encryptor that locks down resources. The advent of Human-Operated Ransomware (HumOR) along with the evolution of Ransomware-as-a-Service (RaaS) have created an entire ecosystem that thrives on hands-on the keyboard, well-planned attack campaigns. It is a rapidly growing threat that has evolved from being a single machine infection following an ill-advised mouse click to becoming a booming enterprise capable of crippling large and small networks alike.

Organizations are at risk of losing their data and information to these attacks, which can lead to revenue losses, reputational damage, theft of employee time and productivity, and inability to function normally. It is now common to see these large-scale sophisticated attacks where the ransomware actors first establish persistence and execute tools on their target, then move laterally throughout the organization, ultimately exfiltrating data before deploying their ransomware payloads.

Even though payments to ransomware actors slowed down in 2022 as compared to previous years, that same year there were over 2,600 posts made to extortion sites related to ransomware. This number does not include an unknown quantity of incidents that were resolved through communication and/or negotiation behind the scenes prior to public notification. Of the reported incidents from 2022, the following are the top 10 sectors in terms of compromise:*

- Construction
- Hospital and Health Care
- Government Administration
- IT Services and IT Consulting
- Law Practice
- Automotive
- Financial Services
- Higher Education
- Insurance
- Real Estate

The FOR528: Ransomware for Incident Responders course teaches students how to deal with the specifics of ransomware to prepare for, detect, hunt, respond to, and deal with the aftermath of ransomware. The class features a hands-on approach to learning using real-world data and includes a full-day Capture-the Flag-challenge to help students solidify their learning. The four-day class teaches students what artifacts to collect, how to collect them, how to scale out your collection efforts, how to parse the data, and how to review the parsed results in aggregate.

The course also provides in-depth details along with detection methods for each phase of the ransomware attack lifecycle. These phases include initial access, execution, defense evasion, persistence, attacks on active directory, privilege escalation, credential access, lateral movement, data access, data exfiltration, and payload deployment.

Unfortunately, many businesses will find themselves falling victims to ransomware attacks because they feel they are not in danger. No matter if you are a small, medium, or large organization, every internet-connected network is at risk, and the threat is not going away any time soon.

The time to be proactive about ransomware is now!

*Statistics from ecrime.ch

FOR532: Enterprise Memory Forensics In-Depth

4 Day Program	24 CPEs	Laptop Required

You Will Be Able To

- Integrate Memory forensics into their investigation workflow
- Acquire Memory on single machines with Linux, Windows and MacOS
- Acquire interesting Memory parts from many machines
- Understand how Memory works
- Identify the key Memory structures
- Effortlessly walk through the memory using volshell to identify even more traces of an attack and better understand how malware can hide
- Find malware using a standardized process
- Uncover malware capabilities and configurations
- Understand which attacker actions lead to which traces in Memory
- Understand DKOM (direct kernel object manipulation)
- Understand advanced detection countermeasures that attackers apply to beat EDRs and other detection mechanisms
- Extract memory artifacts needed for the investigation
- Extract and understand user artifacts that tell you what happened on a system
- Counter ransomware actors by identifying exfiltration credentials
- Analyze Memory dumps of single processes with windbg
- Use volatility 2 and 3 to find analyze Memory images
- Understand what options malware authors have to hide the presence of malware or make investigations harder
- Analyze Memory in structured and unstructured ways
- Analyze Memory in a team approach (using centralized analysis servers)
- Write your own tools to fill the gaps of current tools
- Write your own volatility plugin
- Scale Memory forensics to thousands of machines
- Automate parts of Memory forensics
- Leverage frequency of occurence analysis (stacking) to single out machines that need a closer look

ATTACKER TRACES ARE MOST VULNERABLE IN MEMORY. TIME TO GO HUNTING!

Memory forensics is an integral part of successful incident response investigations. Over the last year, incident response procedures have grown from investigating single computer images at time to investigating hundreds of thousand machines all at once. In the beginning of every investigation, the attacker is way ahead. Incident responders need to find ways to get ahead of the attackers quickly and kick them out of our networks. While there has been a lot of light shed on scaling hard drive artifact-based investigations to large numbers of endpoints, the memory forensics part has been the neglected part of classical forensics for a while. This rapidly changes as many attacks are way more lilkely to be uncovered when looking into memory than with more classical means. Memory forensics ties into many disciplines in cyber investigations. From the classical law enforcement investigations that focus on user artifacts via malware analysis to large-scale hunting, memory forensics has several applications that for many teams are still terra incognita. The FOR532 Enterprise Memory Forensics In-Depth class strives to change that and speed up your incident response, your threat hunting, and your malware analysis significantly.

A major step to get started with memory forensics is to understand, that memory can be complex at times, but in a nutshell analyzing memory just means knowing what bytes at specific locations mean. In other terms, the better you can read the street map of memory, the more you can get out of it. For that reason, we will spend some time understanding how memory works. You will become familiar with key memory structures and what they mean.A clear understanding will help you understand how the different presented tools work and what their advantages and limitations are.

In memory forensics, the saying “A fool with a tool is still a fool” is even more important than in classical forensics. Memory being a very dynamic kind of dataset can be easily misinterpreted which in real investigations can lead to false-negatives or send you down a rabbit hole quickly. For that reason, it is important to understand how the various tools work. Not every aspect you might need for an investigation will already be covered by a tool. Another aspect of the class is to understand what you need and how to use easy measures to get your hands on the data.

Finally, when you understand memory on one machine, it is time to scale your investigation to a larger number of machines. Both structured analysis as well as with unstructured analysis matter. We will use cutting edge toools to scale memory forensics in a unique way.

The digital evidence we leverage in the labs is designed to resemble real cases the author came across in his career. You will be working on the evidence a significant amount of time in many different labs. As it is important to understand how attackers leave certain traces, every now and then you will be asked to switch sides and attack a system that you later analyze. This approach enables incident responders to have a 360 degree view on modern incident response analysis.

In the second half of Section 4 you can put your newly acquired knowledge into action in a scoreboard-style capture the flag. You will be presented with new evidence that was built based on real-world cases and score points for correctly answered questions. Regardless of how new you are to memory forensics, there will be interesting traces for you to find in the evidence.

The main goal of the class is to demonstrate, that memory forensics is not as complicated as it seems at first. You will get a set of techniques and tools to add a lot of value to your investigations by saving time and resources as well as rendering results you would not have gotten by using classical IR tactics. Add memory forensics to your toolchest now to battle evil faster and more efficiently even at scale.

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL/TLS traffic to identify attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage meddler-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- Apply the knowledge you acquire during the week in a full-day capstone lab, modeled after real-world nation-state intrusions and threat actors

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career but overlooking their network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or may even prove useful in definitively proving a crime actually occurred.

FOR572 was designed to cover the most critical skills needed for the increased focus on network communications and artifacts in today's investigative work, including numerous use cases. Many investigative teams are incorporating proactive threat hunting to their skills, in which existing evidence is used with newly-acquired threat intelligence to uncover evidence of previously-unidentified incidents. Others focus on post-incident investigations and reporting. Still others engage with an adversary in real time, seeking to contain and eradicate the attacker from the victim's environment. In these situations and more, the artifacts left behind from attackers' communications can provide an invaluable view into their intent, capabilities, successes, and failures.

In FOR572, we focus on the knowledge necessary to examine and characterize communications that have occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high--evel NetFlow analysis, low-level pcap-based dissection, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is underway.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting cybercrime victims and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of threat hunters, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS DFIR alumni can take their existing operating system or device knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

FOR572 is an advanced course – we hit the ground running on day one. Bring your entire bag of skills: forensic techniques and methodologies, full-stack networking knowledge (from the wire all the way up to user-facing services), Linux shell utilities, and everything in between. They will all benefit you throughout the course material as you FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE (OR PACKET) AT A TIME

Certification: GIAC Network Forensic Analyst (GNFA)
giac.org/gnfa

FOR578: Cyber Threat Intelligence

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn the different sources to collect adversary data and how to exploit and pivot off of it
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- Establish structured analytical techniques to be successful in any security role

THERE IS NO TEACHER BUT THE ENEMY!

All security practitioners should attend FOR578: Cyber Threat Intelligence to sharpen their analytical skills. This course is unlike any other technical training you have ever experienced. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills.

It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques to complement their existing knowledge and help them establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary's intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that addresses an organization's key knowledge gaps, pain points, or requirements. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organizations looking to establish or update their response and detection programs to deal with increasingly sophisticated threats. Malware is an adversary's tool, but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries' methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritize intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritization and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats.

In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578: Cyber Threat Intelligence will equip you, your security team, and your organization with the level of tactical, operational, and strategic cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and accurately and effectively counter those threats.

"I could take this course five times more and get something new each time! So much valuable info to take back to my organization."

—Charity Willhoite, **Armor Defense, Inc.**

"This course is terrific! Class discussion and relevant case studies are extremely helpful for better understanding the content."

—Larci Robertson, **Epsilon**

Certification: GIAC Cyber Threat Intelligence (GCTI)
giac.org/gcti

FOR585: Smartphone Forensic Analysis In-Depth

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Select the most effective forensic tools, techniques, and procedures to effectively analyze smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device - we'll teach you how to know if the user created the data, which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone on a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes
- Understand how data are stored on smartphone components (SD cards) and how encrypted data can be examined by leveraging the smartphone
- Extract and use information from smartphones and their components, including Android, iOS, BlackBerry 10, Windows Phone, Chinese knock-offs, and SD cards (bonus labs available focusing on BlackBerry, BlackBerry backups, Nokia [Symbian], and SIM card decoding)
- Perform advanced forensic examinations of data structures on smartphones by diving deeper into underlying data structures that many tools do not interpret
- Analyze SQLite databases and raw data dumps from smartphones to recover deleted information
- Perform advanced data-carving techniques on smartphones to validate results and extract missing or deleted data
- Apply the knowledge you acquire during the course to conduct a full-day smartphone capstone event involving multiple devices and modeled after real-world smartphone investigations

SMARTPHONES HAVE MINDS OF THEIR OWN. DON'T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE, SUGGESTIONS, OR APPLICATION ASSOCIATIONS AS USER ACTIVITY. IT'S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Smartphone Forensic Analysis In-Depth will teach you those skills.

Every time the smartphone "thinks" or makes a suggestion, the data is saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data was put on the device. Examination and interpretation of the data is your job and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 31 hands-on labs, a forensic challenge, and a bonus take-home case that allows students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest smartphone operating systems, third-party applications, acquisition short-falls, extraction techniques (jailbreaks and roots), malware and encryption. This intensive six-day course offers the most unique and current instruction on the planet, and it will arm you with mobile device forensic knowledge you can immediately apply to cases you're working on the day you leave the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's time for the good guys to get smarter and for the bad guys to know that their smartphone activity can and will be used against them!

SMARTPHONE DATA CAN'T HIDE FOREVER – IT'S TIME TO OUTSMART THE MOBILE DEVICE!

Certification: GIAC Advanced Smartphone Forensics (GASF)
giac.org/gasf

FOR608: Enterprise-Class Incident Response & Threat Hunting

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Understand when incident response requires in-depth host interrogation or light-weight mass collection
- Deploy collaboration and analysis platforms that allow teams to work across rooms, states, or countries simultaneously
- Collect host- and cloud-based forensic data from large environments
- Discuss best practices for responding to Azure, M365, and AWS cloud platforms
- Learn analysis techniques for responding to Linux and Mac operating systems
- Analyze containerized microservices such as Docker containers
- Correlate and analyze data across multiple data types and machines using a myriad of analysis techniques
- Conduct analysis of structured and unstructured data to identify attacker behavior
- Enrich collected data to identify additional indicators of compromise
- Develop IOC signatures and analytics to expand searching capabilities and enable rapid detection of similar incidents in the future
- Track incidents and indicators from beginning to end using built-for-purpose incident response engagement tooling

Who Should Attend

This course is aimed at digital forensics, incident response, intrusion detection, and threat hunting professionals in medium to large organizations, who constantly face battles with enterprise scale and complexity.

Please note that FOR608 is an advanced course that skips over introductory material of Windows host- and network-based forensics and incident response. Although this class is not necessarily more technical than our 500-level classes, it does assume that prior knowledge so that topics and concepts are not repeated.

NICE Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Prerequisites

FOR608 is an advanced level course that skips over introductory material of Windows host- and network-based forensics and incident response. This class is not necessarily more technical than our 500-level classes, but it does assume that knowledge so that topics and concepts are not repeated.

Students must have multiple years of DFIR experience and/or have taken classes such as:

- FOR500: Windows Forensics Analysis, and/or
- FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

Enterprises today have thousands, maybe even hundreds of thousands – of systems ranging from desktops to servers, from on-site to the cloud. Although geographic location and network size have not deterred attackers in breaching their victims, these factors present unique challenges in how organizations can successfully detect and respond to security incidents. Our experience has shown that when sizeable organizations suffer a breach, the attackers seldom compromise one or two systems. Without the proper tools and methodologies, security teams will always find themselves playing catch-up, and the attacker will continue to achieve success.

FOR608: Enterprise-Class Incident Response and Threat Hunting focuses on identifying and responding to incidents too large to focus on individual machines. The concepts are similar: gathering, analyzing, and making decisions based on information from hundreds of machines. This requires the ability to automate and the ability to quickly focus on the right information for analysis. By using example tools built to operate at enterprise-class scale, students will learn the techniques to collect focused data for incident response and threat hunting. Students will then dig into analysis methodologies, learning multiple approaches to understand attacker movement and activity across hosts of varying functions and operating systems by using timeline, graphing, structured, and unstructured analysis techniques.

Business Takeaways

- Reduce financial and reputational impact of a breach by more efficiently and precisely managing the response
- Learn IR management techniques that optimize resource usage during an investigation
- Deploy collaboration and analysis platforms that allow teams to work across rooms, states, or countries simultaneously
- Understand and hunt for techniques attackers use to hide from EDR and application control tools on Windows systems
- Learn analysis techniques for responding to compromised Linux and macOS systems
- Be able to respond and analyze containerized microservices such as Docker containers
- Discuss best practices for responding to the most popular cloud environments—specifically Microsoft365/AzureAD, and AWS

"The course content covers a lot of important topics focused on detection and response. I enjoyed the sections on Threat Driven Intelligence and TimeSketch for creating incident timelines."

—Reggie M., **Amazon**

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Build an isolated, controlled laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks
- Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis
- Use a disassembler and a debugger to examine the inner workings of malicious Windows executables
- Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files
- Derive Indicators of Compromise (IOCs) from malicious executables to strengthen incident response and threat intelligence efforts

NICE Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst(OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

"This is a truly a step-by-step mentorship course. The content is immediately applicable to DFIR job roles."

—Chad Reams, **Parsons Inc.**

Learn to turn malware inside out! This popular reversing course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to your ability to derive threat intelligence, respond to cybersecurity incidents, and fortify enterprise defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen's capabilities by interacting with the malicious program.

The course continues by discussing essential assembly language concepts relevant to reverse engineering. You will learn to examine malicious code with the help of a disassembler and a debugger in order to understand its key components and execution flow. In addition, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by malicious programs.

Next, you will dive into the world of malware that thrives in the web ecosystem, exploring methods for assessing suspicious websites and de-obfuscating malicious JavaScript to understand the nature of the attack. You will also learn how to analyze malicious Microsoft Office, RTF, and PDF files. Such documents act as a common infection vector as a part of mainstream and targeted attacks. You will also learn how to examine "file-less" malware and malicious PowerShell scripts.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files' structure to bypass the packer's protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

The course culminates with a series of Capture-the-Flag challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical, hands-on malware analysis skills in a fun setting.

Hands-on lab exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systemic manner. When performing the exercises, you will study the supplied specimens behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

Certification: GIAC Reverse Engineering Malware (GREM)
giac.org/grem

FOR710: Reverse-Engineering Malware: Advanced Code Analysis

5 Day Program	36 CPEs	Laptop Required

Course Topics

- Code deobfuscation
- Program execution
- Shellcode analysis
- Steganography
- Multi-stage malware
- WinDbg Preview
- Encryption algorithms
- Data obfuscation
- Python scripting for malware analysis
- Dynamic Binary Instrumentation (DBI) Frameworks
- Binary emulation frameworks
- Payload and config extraction
- Scripting with Ghidra
- YARA rules
- Yara-python
- SMDA disassebler

What You Will Receive

- Windows 10 VM with pre-installed malware analysis and reversing tools
- Real-world malware samples to examine during and after class
- Coursebooks and workbook with detailed step-by-step exercise instruction

As defenders hone their analysis skills and automated malware detection capabilities improve, malware authors have worked harder to achieve execution within the enterprise. The result is modular malware with multiple layers of obfuscation that executes in-memory to hinder detection and analysis. Malware analysts must be prepared to tackle these advanced capabilities and use automation whenever possible to handle the volume, variety and complexity of the steady stream of malware targeting the enterprise.

FOR710: Advanced Code Analysis continues where FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques course leaves off, helping students who have already attained intermediate-level malware analysis capabilities take their reversing skills to the next level. Authored by SANS Certified Instructor Anuj Soni, this course prepares malware specialists to dissect sophisticated Windows executables, such as those that dominate the headlines and preoccupy incident response teams across the globe.

Developing deep reverse-engineering skills requires consistent practice. This course not only includes the necessary background and instructor-led walk throughs, but also provides students with numerous opportunities to tackle real-world reverse engineering scenarios during class.

FOR710 Advanced Code Analysis will prepare you to:

- Tackle code obfuscation techniques that hinder static code analysis, including the use of steganography
- Identify the key components of program execution to analyze multi-stage malware in memory
- Locate and extract deobfuscated shellcode during program execution
- Develop comfort with non-executable file formats during malware analysis
- Probe the structures and fields associated with a PE header
- Use WinDBG Preview for debugging and assessing key process data structures in memory
- Identify encryption algorithms in ransomware used for file encryption and key protection
- Recognize Windows APIs that facilitate encryption and articulate their purpose
- Investigate data obfuscation in malware, pinpoint algorithm implementations, and decode underlying content
- Create Python scripts to automate data extraction and decryption
- Build rules to identify functionality in malware
- Use Dynamic Binary Instrumentation (DBI) frameworks to automate common reverse engineering workflows
- Write Python scripts within Ghidra to expedite code analysis
- Use Binary Emulation frameworks to simulate code execution

"As malware gets more complicated, malware analysis has as well. In recent years, malware authors have accelerated their production of dangerous, undetected code using creative evasion techniques, robust algorithms, and iterative development to improve upon weaknesses. Proficient reverse engineers must perform in-depth code analysis and employ automation to peel back the layers of code, characterize high-risk functionality and extract obfuscated indicators."

—Anuj Soni, **Course Author**

SANS CURRICULUM FOCUS AREA

Cybersecurity Leadership

As the threat landscape continues to evolve, cybersecurity has become more valuable to organizations than ever before. Business leaders now understand the importance of securing high-value information assets and the significant risk associated with a breach or attack.

Organizations need cybersecurity leaders and managers who can pair their technical knowledge with essential leadership skills so they can effectively lead projects, teams, and initiatives in support of business objectives.

The Cybersecurity Leadership focus area delivers applicable and practical approaches to managing cyber risk. This series of hands-on, interactive courses helps current and aspiring cybersecurity leaders take their management skills to the level of their technical knowledge.

SANS Cybersecurity Leadership courses will teach you to:

- Develop your management and leadership skills
- Understand and analyze risk
- Create effective cybersecurity policy
- Build a vulnerability management program
- Develop strategic security plans that incorporate business and organizational goals
- Effectively engage and communicate with key business stakeholders
- Measure the impact of your security program
- Establish and mature your security culture
- Protect and lead enterprise and cloud environments

Enhance your training with:

- Go Beyond Good Enough. Become A Transformational Cybersecurity Leader or an Operational Cybersecurity Executive. **sans.org/cybersecurity-leadership/triads**
- We are growing a diverse community of next generation cybersecurity leaders. Join the conversation in our new Discord channel. **sansurl.com/leadership-discord**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a certificate in Cybersecurity Management **sans.edu**

"This training applies to all aspects of my job, from network management to project management."

—David Chaulk, **Enbridge**

Cybersecurity Leadership Job Roles:

- CISO
- CIO
- Director
- Security Manager
- SOC Manager
- Auditor
- Lawyer
- Privacy Officer

SEC405: Business Finance Essentials

1 Day Course	6 CPEs	Laptop Required

You Will Be Able To

- Fully understand what your Chief Financial Officer (CFO) and finance team are saying
- Stand out as an engaged partner in shared business success
- Follow a repeatable eight-step Finance Framework that helps you understand and communicate finance more effectively
- Discover and successfully interpret an organization's financial goals
- Better align the cybersecurity program to the strategic priorities of the organization
- Better understand the business side of an enterprise, including business decisions and tradeoffs
- Improve partnerships with key leaders
- Achieve alignment of your cybersecurity program

Who Should Attend

- CISOs
- Information Security Officers
- Information Security Directors
- Information Security Managers
- Information Security Leaders
- All those who aspire to become an effective information security leader

Topics

- What you must know about finance
- A clear business case
- Financial stewardship
- A multi-year budget
- How we do this work

What You Will Receive

- Electronic courseware for learning how to understand business finance
- Course book
- Lab workbook with completed examples
- MP3 audio files of the complete course lecture
- An enabling and repeatable eight-step Finance Framework created to help you understand and communicate finances more effectively

Turn Your Financial Uncertainty into Financial Clarity!

SEC405: Business Finance Essentials will:

- Increase your business financial literacy
- Improve your understanding and awareness of business financial health
- Prepare you to partner with your organization's finance team
- Provide you with the skills and knowledge to serve as a trusted financial advisor to your organization

What would it feel like to have confidence in navigating your business financials before dedicating another hour to cybersecurity work or spending another dollar of your cybersecurity budget? This course will give you the confidence and clarity to understand and effectively communicate financial stewardship. The knowledge and skills you learn in SEC405 will contribute to your own success as well as the success of the cybersecurity team you are privileged to lead, and, ultimately, the success of your organization.

In Business Finance Essentials you will learn the importance of a clear business case by creating one yourself during a course exercise. Need to design a multi-year budget? No problem! We will talk about the rationale for that design and then undertake an exercise to create such a budget. You'll be able to use these examples as templates later when you need to do these tasks yourself!

What will the Chief Financial Officer notice after you take this course and apply the concepts you've learned?

- You ask better questions of your CFO, Controller, and Finance team
- You can interpret common financial statements
- You demonstrate strong financial stewardship
- You are able to create a multi-year budget
- You make a greater effort to work with finance colleagues

What strategies can build a meaningful relationship with your Chief Financial Officer?

- Understand what is important to your CFO
- Demonstrate the interest, skills, and knowledge that make you stand out
- More specifically, be able to interpret a balance sheet, cash flow statement, and income statement

How can you demonstrate financial stewardship?

- Think through and assess such concepts as "before the next dollar is spent" and "before the next hour is spent"
- Ensure that your efforts are definitively focused on the highest risks

What does a Chief Information Security Officer need to know about finance to be successful?

- How to successfully navigate the mysterious realm of business finance
- How to secure multi-year funding for cybersecurity projects
- How to create a business case

LDR414: SANS Training Program for the CISSP Certification

6 Day Program	52 CPEs	Laptop Not Needed

You Will Be Able To

- Understand the eight domains of knowledge that are covered on the CISSP® exam
- Analyze questions on the exam and be able to select the correct answer
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- Understand and explain all of the concepts covered in the eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

What You Will Receive

- Electronic courseware for each of the eight domains
- 320 questions to test knowledge and preparation for each domain
- MP3 audio files of the complete course lectures

"This course really pulls a lot together for me and it has been hugely valuable. I know parts of this are going to impact my approach to my work from the first day back."

— Merewyn Boak, **Apple**

Need training for the CISSP® exam?

SANS LDR414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the Certified Information Systems Security Professional (CISSP®) exam.

LDR414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

After completing the course, students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

Course Authors' Statement

"The CISSP® certification has been around for nearly 25 years. The exam is designed to test your understanding of the Common Body of Knowledge, which may be thought of as the universal language of information security professionals. It is often said to be a mile wide and two inches deep. The CISSP® exam covers a lot of theoretical information that is critical for a security professional to understand. However, this material can be dry, and since most students do not see the direct applicability to their jobs, they find it boring. The goal of this course is to bring the eight domains of knowledge of the CISSP® to life. The practical workings of this information can be discovered by explaining important topics with stories, examples, and case studies. We challenge you to attend the SANS CISSP® training course and find the exciting aspect of the eight domains of knowledge!"
—Eric Conrad and Seth Misenar

Certification: GIAC Information Security Professional (GISP)
giac.org/gisp

LDR415: A Practical Introduction to Cyber Security Risk Management

2 Day Course	12 CPEs	Laptop Required

You Will Be Able To

- Perform a complete risk assessment
- Inventory an organization's most critical information assets
- Assign a data owner and custodian to an information asset
- Assign classification values to critical information assets
- Prioritize risk remediation efforts as a result of performing a risk assessment
- Evaluate risk management models for use in their own organization

Who Should Attend

- Any security engineers, compliance directors, managers, auditors – basically any SANS alumni potentially
- Auditors
- Directors of security compliance
- Information assurance management
- System administrators

What You Will Receive

- Electronic courseware for learning how to perform risk management
- A unique course spreadsheet tool for performing risk management
- Open source tools for performing risk management
- MP3 audio files of the complete course lecture

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decision on how best to defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

Author Statement

Most every time we talk with an organization, whether that be a private company or a government agency, we meet people who want to use risk assessment as a tool, but are not actually using it as they could. No organization has enough resources to do everything they would like to defend themselves. At some point a priority decision has to be made. We either make those decisions individually based on whatever need seems to be the most pressing in from of us today, or we take a methodical approach, getting as much input from the business as possible. Risk management is the tool we have available for taking the methodical path.

This course has been written with practicality and usability in mind. Risk models and learning ALE to pass a certification test is fine. But to defend our systems, we need practical skills in risk assessment. This course will teach students the hands-on skills necessary to immediately start using risk assessment as a tool to defend their organization.

– James & Kelli Tarala

"Excellent introduction to the area of risk assessment."

— Ernie H., **U.S. Military**

Section Descriptions

SECTION 1: A Practical Introduction to Assessing Cyber Security Risk

TOPICS: Understanding Risk; How to Perform a Simple Risk Assessment; Risk Assessment Case Study; Formal Risk Management Models & Tools

SECTION 2: A Practical Introduction to Managing Cyber Security Risk

TOPICS: Control Focused Risk Management; Event Focused Risk Management; Presenting Risk to Business Owners; Risk Remediation & Response; Tracking Long Term Risk

LDR433: Managing Human Risk

3 Day Course	18 CPEs	Laptop Not Needed

This Course Will Prepare You to:

- Master how to map and benchmark your program's maturity against your peers'
- Understand the Security Awareness Maturity Model and how to leverage it as the roadmap for your program
- Ensure compliance with key standards and regulations
- Implement models for learning theory, behavioral change, and cultural analysis
- Define human risk and explain the three different variables that constitute it
- Explain risk assessment processes
- Leverage the latest in Cyber Threat Intelligence and describe the most common tactics, techniques, and procedures used in today's human-based attacks
- Identify, measure, and prioritize your human risks and define the behaviors that manage those risks
- Define what security culture is and the common indicators of a strong security culture
- Explain your organization's overall culture and how to most effectively align cybersecurity with and embed into your organization'sculture
- Measure the impact of your program, track reduction in human risk, and how to communicate to senior leadership the value of the program

"I think the course is really engaging and works at two levels: (1) It would provide someone starting out with a solid foundational knowledge, (2) It allows an existing program to benchmark and get new ideas, to supplement the existing work."

—Brian Wright,
Student Loans Company Unlimited

People have become the primary attack vector. Manage your human risk.

Learn the key lessons and the roadmap to build a mature awareness program that will truly engage your workforce, change their behavior and ultimately manage your human risk. Apply models such as the BJ Fogg Behavior Model, AIDA Marketing funnel, and Golden Circle, and learn about the Elephant vs. the Rider. Concepts include how to assess and prioritize your top human risks and the behaviors that manage those risks, how to engage, train and secure your workforce by changing their behaviors and culture, and how to measure the impact and value of that change.

The course content is based on lessons learned from hundreds of programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom plan to implement as soon as you return to your organization.

Business Takeaways:

- Align your security awareness program with your organization's strategic security priorities
- Effectively identify, prioritize and manage your organization's top human risks.
- More closely integrate your security awareness efforts with your security team'soverall risk management efforts.
- Make the most of your investment by sustaining your program long term, going beyond changing behavior to embedding a strong security culture
- Communicate and demonstrate the value of the change to your senior leadership in business terms

Hands-On Training:

A big part of the course is not only learning but applying what you learn working as groups with your peers. Not only does this provide you a far better understanding and application of course content, but enables you to interact and learn from others. This three section course has eight interactive labs. Each lab is approximately 30 minutes to complete as a team, with another 20-30 minutes of group discussion.

- **Section 1:** Determine Your Program'sMaturity Level, Creating an Advisory Board, Identify and Prioritize the Top Human Risks to Your Organization
- **Section 2:** Identify and Prioritize the Key Behaviors that Manage Your Top Human Risks, Leverage the AIDA Model to Sell MFA, Putting it All Together, Creating an Engagement Plan
- **Section 3:** Define Your Organization'sCulture, Measuring a Key Human Risk and Behaviors that Manage that Risk

Additional Free Resources

- Security Awareness Roadmap: Managing Your Human Risk, poster
- Annual Security Awareness Report™: Managing Human Risk
- Career Developoment for Security Awareness, Engagement, and Culture Professionals
  (For those of you who are looking to get involved in this field, or are already involved but looking to grow, consider reading this blog on how to develop your career path.

Certification: SANS Security Awareness Professional (SSAP)

SEC440: CIS Critical Controls: A Practical Introduction

2 Day Course	12 CPEs	Laptop Not Needed

You Will Be Able To

- Understand a security framework and its controls based on recent and evolving threats facing organizations
- Prepare you to interpret a security framework based on data from publicly known attacks, breach reports, and large scare data analytics from the Verizon Data Breach Investigation Report (DBIR), along with data from the Multi-State Information Sharing and Analysis Center® (MS-ISAC®)
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals accomplished with each control
- Identify tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each controls the effectiveness of each control
- Identify specific metrics to establish a baseline and measure the effectiveness of security controls

Introduction to Critical Security Controls

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? Does your organization need an on-ramp to implementing a prioritized list of technical protections?

In February of 2016, then California Attorney General, Vice President Kamala Harris recommended that "The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

SANS has designed SEC440 as an introduction to the CIS Critical Controls, in order to provide students with an understanding of the underpinnings of a prioritized, risk-based approach to security. The technical and procedural controls explained in the CIS Controls were proposed, debated and consolidated by various private and public sector experts from around the world. Previous versions of the CIS Controls were prioritized with the first six CIS Critical Controls labeled as "cyber hygiene" and now the CIS Controls are now organized into Implementation Groups for prioritization purposes.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The course introduces security and compliance professionals to approaches for implementing the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

"The 20 Critical Security Controls provide updated/ current trends in InfoSec. The course provided an excellent explanation of the controls and how to apply them."

— Dan Sherman, **RIC Audit FRB**

Section Descriptions

SECTION 1: Introduction and Critical Controls 1–9

Section 1 will introduce you to Critical Controls 1–9, including the name, purpose, and why each matters in the bigger picture of cybersecurity.

- **CIS Critical Control 1:** Inventory and Control of Enterprise Assets
- **CIS Critical Control 2:** Inventory and Control of Software Assets
- **CIS Critical Control 3:** Data Protection
- **CIS Critical Control 4:** Secure Configuration of Enterprise Assets and Software
- **CIS Critical Control 5:** Account Management
- **CIS Critical Control 6:** Access Control Management
- **CIS Critical Control 7:** Continuous Vulnerability Management
- **CIS Critical Control 8:** Audit Log Management
- **CIS Critical Control 9:** Email and Web Browser Protections

SECTION 2: Critical Controls 10–18 and Conclusion

Section 2 will introduce you to Critical Controls 10–18, including the name, purpose, and why each matters in the bigger picture of cybersecurity.

- **Critical Control 10:** Malware Defenses
- **Critical Control 11:** Data Recovery
- **Critical Control 12:** Network Infrastructure Management
- **Critical Control 13:** Network Monitoring and Defense
- **Critical Control 14:** Security Awareness and Skills Training
- **Critical Control 15:** Service Provider Management
- **Critical Control 16:** Application Software Security
- **Critical Control 17:** Incident Response Management
- **Critical Control 18:** Penetration Testing

SEC474: Building A Healthcare Security & Compliance Program

2 Day Course	12 CPEs	Laptop Required

You Will Be Able To

- Tackle the challenges at hand – many HIPAA compliance regulations run counter to business objectives, so we will explore why this is and how to overcome the issue
- Interpret the Security Rule text in-depth, including an analysis of every line item of the regulation and what it means to your organization
- Draft sound policy that supports business as well as compliance objectives
- Perform a risk assessment, enumerate threat data, analyze vulnerabilities, and select proper safeguards to lower risk
- Define the value of the compliance program for the organization
- Create a culture of compliance
- Establish lines of communication and reporting channels
- Understand the value of internal monitoring and auditing by learning the key components of a continuous monitor reporting and improvement program
- Promote a culture of compliance

Who Should Attend

- Healthcare CSO/CIO/CISOs
- Information security managers/ administrators
- IT security analysts/managers/directors
- HIPAA compliance officers
- Compliance analysts
- Medical records supervisors
- Compliance auditors
- Healthcare security consultants
- IT managers in healthcare organizations

What You Will Receive

- Physical and digital workbooks
- Virtual machine tailored to the course
- HIPAA-based risk assessment tool

One of the challenges organizations face in complying with the Health Insurance Portability and Accountability Act (HIPAA) is that the act's regulatory and privacy standards are not prescriptive enough to help organizations successfully build an effective security and compliance program. Audit and assessment engagements with government agencies such as the Office of Civil Rights (OCR) and with state attorney generals during and after reportable data breaches or privacy-related security incidents can be overwhelming for organizations to navigate without previous knowledge or experience.

To address tight budget restrictions, many healthcare organizations promote security and compliance team members from within the organization in order to cultivate and retain talent internally. These professionals have a wide range of experience and skill sets. The SANS SEC474 course can help organizations level-set and prepare healthcare compliance and security by sharing first-hand knowledge and experiences.

The goal of this course is to show that HIPAA compliance in itself is neither an antidote nor a cure for the shortcoming of an organization's healthcare security. The ultimate goal is to develop, maintain, and demonstrate a secure environment for the organization by implementing repeatable processes based on industry best practices. When that is achieved, evidence of HIPAA compliance is a result of those efforts.

Healthcare organizations in the United States face two major challenges: first, to properly secure the organization from tactical risk, and second, to achieve compliance with the array of government regulations known as HIPAA. This course will help students develop the skills to make measurable improvements to the overall security posture of their organization's IT infrastructure while also building and maintaining a compliance program. Using the safeguards of the HIPAA Security Rule along with the NIST Framework 800-66 to identify and assess risk, students will learn how to report progress on their compliance activities and their security value in support of the organization's mission.

Students will gain skills and knowledge in SEC474 that they will be able to use on their first day back at work. Students will leave the classroom knowing what it takes to establish and nurture a culture of compliance where both compliance and business objectives are promoted as a singular goal. They will be able not only to assess compliance, but also to measure the maturity and effectiveness of compliance activities.

This course will prepare you to:

- Take steps to meet compliance standards, particularly those of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH)
- Protect your healthcare organization from cyber-threats, unintended data disclosures, and mishandling of data in the enterprise
- Understand the most prevalent security concerns specifically around the healthcare industry such as data disclosures, ransomware, unauthorized access and modification, incident response, and business continuity planning
- Apply the HIPAA Security Rule in practice
- Build an organizational security plan
- Understand the job roles in a compliance program

AUD507: Auditing Systems, Applications, and the Cloud

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Apply risk-based decision making to the task of auditing enterprise security
- Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- Conduct a proper risk assessment of an enterprise to identify vulnerabilities and develop audit priorities
- Establish a well-secured baseline for computers and networks as a standard to conduct audit against
- Perform a network and perimeter audit using a repeatable process
- Audit virtualization hosts and container environments to ensure properly deployment and configuration
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit a web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize automated tools to audit Windows and Linux systems
- Audit Active Directory Domains

Controls That Matter – Controls That Work

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program, covering systems, applications, and the cloud. After covering a variety of high-level audit issues and general audit best practices, students will have the opportunity to delve into the technical "how-to" for determining the key controls that can be used to provide a high level of assurance to an organization. Real-world examples provide students with tips on how to verify these controls in a repeatable way, as well as many techniques for continuous monitoring and automatic compliance validation. These same real-world examples help the students learn how to be most effective in communicating risk to management and operations staff.

Students will leave the course with the know-how to perform effective tests of enterprise security in a variety of areas including systems, applications, and the cloud. The combination of high-quality course content, provided audit checklists, in-depth discussion of common audit challenges and solutions, and ample opportunities to hone their skills in the lab provides a unique setting for students to learn how to be an effective enterprise auditor.

Business Takeaways

- Gain confidence in whether you have the correct security controls and they are working well
- Lower your audit costs with effective, efficient security audits
- Improve relevance of IT audit reporting, allowing the organization to focus on what really matters
- Improve security compliance while reducing compliance and security risks, protecting your reputation and bottom line

Hands-On Training

This course goes beyond simply discussing the tools students could use; we give them the experience to use the tools and techniques effectively to measure and report on the risk in their organizations. AUD507 uses hands-on labs to reinforce the material discussed in class and develop the "muscle memory" needed to perform the required technical tasks during audits. In sections 1-5, students will spend about 25% of their time in lab exercises. The final section of the course is a full-day lab that lets students challenge themselves by solving realistic audit problems using and refining what they have learned in class.

Students learn how to use technical tests to develop the evidence needed to support their findings and recommendations. Each section affords students opportunities to use the tools and techniques discussed in class, with labs designed to simulate real-world enterprise auditing challenges and to allow the students to use appropriate tools and techniques to solve these problems.

"Today's NetWars was definitely a challenge and for me I needed the team so we could all use our strengths. Excellent coverage of everything we've learned without repeating exact exercises we had done in the week. Good way to know I did understand what we've been learning all week. The workbook was a good reference to return to."

—Carmen P., **U.S. Government**

"The hands-on labs reinforce the learning from the book. I learn best when I can touch and feel the material being taught."

—Rodney Newton, **SAP**

Certification: GIAC Systems and Network Auditor (GSNA)
giac.org/gsna

LDR512: Security Leadership Essentials for Managers

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage and lead technical teams and projects
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Lead a Security Operations Center (SOC)
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud
- Build security engineering capabilities using automation and Infrastructure as Code (IaC)
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

"This course was very relevant to my new role as Director of IT."

— Brian Harris, **Jackson EMC**

"LDR512 is valuable because it is relevant/current to the security landscape from my management vantage point."

— Michael Bradley, **Prudential Financial**

Leading Security Initiatives to Manage Information Risk

Take this course to learn the key elements of any modern security program. LDR512 covers a wide range of security topics across the entire security stack. Learn to quickly grasp critical information security issues and terminology, with a focus on security frameworks, security architecture, security engineering, computer/network security, vulnerability management, cryptography, data protection, security awareness, application security, DevSecOps, cloud security, and security operations.

The course uses the **Cyber42 leadership simulation game** to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. Throughout the class you will participate in twenty-three Cyber42 activities.

This course will help your organization:

- Develop leaders that know how to build a modern security program
- Anticipate what security capabilities need to built to enable the business and mitigate threats
- Create higher performing security teams

Hands-On Training

LDR512 uses case scenarios, group discussions, team-based exercises, in-class games, and a security leadership simulation to help students absorb both technical and management topics. About 60–80 minutes per day is dedicated to these learning experiences using the Cyber42 leadership simulation game. This web application based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

Course Author Statement

"Technical professionals who are thrust into management roles need to learn how to convey security concepts in ways that non-technical people can understand. At the same time, managers who are new to security need to learn more about the different domains of cybersecurity. In both cases, there is a need to learn about the work of managing security. That is why this course focuses on the big picture of securing the enterprise, from governance all the way to the technical security topics that serve as the foundation for any security manager. Ultimately, the goal of the course is to ensure that you, the advancing manager, can make informed choices to improve security at your organization."

—Frank Kim

Certification: GIAC Security Leadership (GSLC)
giac.org/gslc

LDR514: Security Strategic Planning, Policy, and Leadership

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

"This course is great content for leaders within the field. It pushes people to stop always focusing on the technical aspects of cybersecurity and really understand what the business needs from its security function as a whole to enable the business"

—Alexander Walker, **TechVets**

"The knowledge gained in class will directly translate to an increased maturity in my organization's security policy as topics and principles discussed are implemented."

— Mike Parkin, **Chapters Health System**

Aligning Security Initiatives with Strategy

As security professionals, we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny. This course gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. These policies must be aligned with an organization's culture. In LDR514, we break down the steps to policy development so that you have the ability to design and assess policies that can successfully guide your organization.

Leadership is a skill that must be learned, exercised, and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and having the vision to see and effectively use available resources toward the end goal. Effective leadership entails persuading team members to accomplish their objectives, removing the obstacles preventing them from doing it, and maintaining the well-being of the team in support of the organization's mission. LDR514 will teach you to use management tools and frameworks to better lead, inspire, and motivate your teams.

Hands-On Training

LDR514 uses business case studies, fictional companies, and the Cyber42 leadership simulation game to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. This web application-based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

The course also uses case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world situations. You will be able to use these same activities with your own team members at work.

"I loved the labs and exercises. They were exactly what I was looking for as the new marketplace security PM on my team."

—Rebecca Gaudet, **Microsoft**

Certification: GIAC Strategic Planning, Policy, and Leadership (GSTRT)
giac.org/gstrt

LDR516: Managing Security Vulnerabilities: Enterprise and Cloud

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Create, implement, and mature your vulnerability management program and get buy-in from your stakeholders
- Implement techniques for building and maintaining an accurate and useful inventory of IT assets in the enterprise and the cloud
- Identify processes and technologies that are effective across both infrastructure and applications and know how to configure them appropriately
- To be aware of common false positives or false negatives in your identification arsenal
- Prioritize unblocked vulnerabilities for treatment based on a variety of techniques
- Effectively report and communicate vulnerability data within your organization
- Identify and report on the risk associated with vulnerabilities that are blocked and cannot currently be prioritized for remediation
- Have a better understanding of modern treatment capabilities and how to better engage with treatment teams
- Make vulnerability management more fun and engaging for all those involved
- Differentiate how to deal with application layer vulnerabilities versus infrastructure vulnerabilities
- Understand how your strategies and techniques might change as you move to the cloud, implement private cloud, or roll out DevOps within your organization

Business Takeaways

This course will help your organization:

- Understand what is working and what is not working in modern day vulnerability programs
- Anticipate and plan for the impacts related to cloud operating environments
- Realize why context matters and how to gather, store, maintain, and utilize contextual data effectively
- Effectively and efficiently communicate vulnerability data and its associate risk to key stakeholders
- Determine how to group vulnerabilities meaningfully to identify current obstacles or deficiencies
- Know which metrics will drive greater adoption and change within the organization
- Understand what remediation capabilities are available to assist technology teams in resolving vulnerabilities and proactively

Stop Treating Symptoms. Cure the Disease.

Whether your vulnerability management program is well established or you are just getting started, this course will help you think differently about vulnerability management. You will learn how to move past the hype to successfully prioritize the vulnerabilities that are not blocked, then clearly and effectively communicate the risk associated with the rest of the vulnerabilities in your backlog that, for a variety of reasons, cannot currently be remediated. You'll also learn what mature organizations are doing to ease the burden associated with vulnerability management across both infrastructure and applications as well as across both their cloud and non-cloud environments. LDR516 is based on the Prepare, Identify, Analyze, Communicate, and Treat (PIACT) Model.

LDR516 helps you think strategically about vulnerability management in order to mature your organization's program, but it also provides tactical guidance to help you overcome common challenges. By understanding and discussing solutions to typical issues that many organizations face across both traditional and cloud operating environments, you will be better prepared to meet the challenges of today and tomorrow. Knowing that many organizations are adopting cloud services in addition to continuing to manage their more traditional operating environments, we'll also look at different cloud service types throughout the course and how they impact the program both positively and negatively. We will highlight some of the tools and processes that can be leveraged in each of these environments and present new and emerging trends.

Hand-On Training

LDR516 uses the Cyber42 leadership simulation game, critical thinking labs based on outlined scenarios, and demonstrations to provide you with the information you need to skillfully fight the VM battle. Cyber42 helps students absorb and apply the content throughout the course. In this web-based continuous tabletop exercise, students play to improve security culture, manage budget and schedule, and improve specific vulnerability management capabilities at the fictional organization, the "Everything Corporation" or "E Corp." This puts you in real-world scenarios that require you to think through various options for improving the organization's maturity by responding to specific events.

"This course is essential for both well-established and developing vulnerability management teams."

—Robert Adams, **CBC**

"A great course to utilize if new to cloud vulnerability management."

—Amaan Mughal

LDR520: Leading Cloud Security Design and Implementation

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Define a strategy for securing a workload in the cloud for medium-size and large enterprises that can support their business objectives
- Establish a security roadmap based on the security strategy that can support a fast-paced cloud adoption and migration path while maintaining a high degree of security assurance
- Understand the security basics of the cloud environment across different types of service offerings, then explain and justify to other stakeholders the decisions within the security roadmap
- Build an effective plan to mature a cloud security posture over time, leveraging security capabilities offered by cloud providers to leapfrog in security capabilities
- Explain the security vision of the organization in the cloud domain to your Board Directors and executives, collaborate with your peers, and engage your workforce, driving the security culture change required for the cloud transformation

"This type of training, i.e., cloud security from a management perspective, is rare and the quality of this one is definitely amazing."

—Benoit Ramillon, **UEFA**

Building and Leading a Cloud Security Program

Cloud adoption is popular across all types of industry, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions. However, an organization 's cloud transition requires numerous key decisions.

This course focuses on what managers, directors, and security leaders need to know to develop their cloud security roadmap, to manage the implementation of cloud security capabilities. Making the right security decisions when adopting the cloud requires understanding the technology, process, and people related to the cloud environment. This complements traditional IT management techniques that managers are accustomed to and helps with making the appropriate informed decisions. We will cover the key objectives of security controls in the cloud environment, including planning, deploying, and running the environment from the starting point to a progressively more mature state. There will be a focus on locking down the environment, securing the data, maintaining compliance, enhancing security visibility to the operations, and managing the security response on a continuous basis. Students will learn the essentials to lead the security effort for the cloud transition journey.

Business Takeaways:

- Establish cloud security program supporting the fast pace business transformation
- Make informed decisions on cloud security program
- Anticipate the security capabilities and guardrails to build for the securing the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Author Statement

"Cloud transition is common in many organizations these days, but many security leaders feel overwhelmed and underprepared for the security aspects of the cloud. When organizations accept security as an integral part of the transformation path, they can not only achieve the same level of security as their in-house IT environment, but also take advantage of a huge opportunity to leapfrog in security using cloud capabilities. In MGT520, we discuss industry-proven techniques to plan for the security aspects of cloud transformation. This course will arm students with the necessary information to confidently lead their organization towards securing the cloud workload and leveraging cloud capabilities to further enhance their security maturity in the IT environment."

—Jason Lam

LDR521: Leading Cybersecurity Change: Building a Security-Based Culture

5 Day Course	30 CPEs	Laptop Not Needed

You Will Be Able To

- More effectively communicate the business value of cybersecurity to your Board of Directors and executives, improve collaborate with your peers, and more effectively engage your workforce
- Explain what organizational culture is, its importance to cybersecurity, and how to map and measure both your organization's overall culture and security culture
- Align your cybersecurity culture to your organization's strategy, including how to leverage different security frameworks and maturity models
- Explain what organizational change is, identify different models for creating change, and learn how to apply those models
- Enable and secure your workforce by integrating cybersecurity into all aspects of your organization's culture
- Dramatically improve both the effectiveness and impact of your security initiatives, such as DevSecOps, Cloud migration, Vulnerability Management, Security Operations Center and other related security deployments
- Create and effectively communicate business cases to leadership and gain their support for your security initiatives
- How to measure your security culture and how to present the impact of a strong security culture to leadership
- Leverage numerous templates and resources from the Digital Download Package and Community Forum that are part of the course and which you can then build on right away

Build and Measure a Strong Security Culture

Drawing on real-world lessons from around the world, the SANS LDR521 course will teach you how to leverage the principles of organizational change in order to develop, maintain, and measure a security-driven culture. Through hands-on instruction and a series of interactive labs and exercises, you will apply these concepts to a variety of different real-world security initiatives and quickly learn how to embed cybersecurity into your organization's culture immediately.

Apply findings from Daniel Kahneman's Nobel prize-winning research, Thayler and Sunstein's Nudge Theory, and Simon Sinek's Golden Circle. Learn how Spock, Homer Simpson, the Elephant and Rider and the Curse of Knowledge all are keys to building a strong cybersecurity culture at your company.

Business Takeaways

- Create a far more secure workforce, both in their attitudes about cybersecurity and also in employee behaviors
- Enable the security team to create far stronger partnerships with departments and regions throughout the organization
- Dramatically improve the ROI of cybersecurity initiatives and projects through increased success and impact
- Improve communication between the cybersecurity team and business leaders
- Create stronger and more positive attitudes, perceptions and beliefs about the cybersecurity team

Hands-On Training

This five-section course includes 16 interactive labs that walk you through exercises and apply the lessons learned to a variety of typical real-world security situations and challenges. Many of the labs are carried out as teams, ensuring that you learn not only from the course materials but from other students and their experiences. Finally, the last section is a capstone event as you work through a series of case studies to see which team can create the strongest security culture. Culture is a very human and global challenge, and as such we want to expose you to as many different situations and perspectives as possible.

Notice to Students

The course is recommended for more senior and/or more experienced cybersecurity managers, officers, and awareness professionals. If you are new to cybersecurity, we recommend some of SANS' more basic courses, such as SEC301, SEC401, or LDR433.

"I am just so happy with this material focusing on embedding secure values into our global culture – exactly what my company needs help with NOW."

—Lindsay O'Bannon, **Deloitte Global**

LDR523: Law of Data Security and Investigations

5 Day Program	30 CPEs	Laptop Not Needed

You Will Be Able To

- Work better with other professionals at your organization who make decisions about the law of data security and investigations
- Exercise better judgment on how to comply with privacy and technology regulations, both in the United States and in other countries
- Evaluate the role and meaning of contracts for technology, including services, software, and outsourcing
- Help your organization better explain its conduct to the public and to legal authorities
- Anticipate cyber law risks before they get out of control
- Implement practical steps to cope with technology law risk
- Better explain to executives what your organization should do to comply with information security and privacy law
- Better evaluate technologies, such as digital archives and signatures, to comply with the law and serve as evidence
- Make better use of electronic contracting techniques to get the best terms and conditions
- Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard).

"LEG523 provides a great foundation and introduction to the legal issues involving cybersecurity."

— Tracey Kinslow, **TN Air National Guard**

LEG523 is constantly updated to address changing trends and current events, including:

- Supply chain terms and conditions
- The rising influence of the European Union's General Data Protection Regulation (GDPR) in interpretation of cybersecurty law in the United States and around the world
- Understanding cyber insurance for a ransomware event
- Facing a cyber crisis? Filing a lawsuit in the courts of another country
- The arrest and criminal indictment of two Coalfire penetration testers in Iowa
- How to balance the right to data privacy versus the right to data security under GDPR and the new California Consumer Privacy Act
- Adopt peer review of cybersecurity program to better evidence legal compliance
- Video demonstration of how technical expert witnesses can handle adversarial cross-examination in a live online court hearing
- Creative insertion of terms, comments, and conditions in blockchain to influence commercial relationships such as contracts for technology services
- How to make better legal records of digital assets and trading platforms

New law on privacy, e-discovery, and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the cybersecurity team. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies, and insurance security questionnaires.

This course covers the law of crime, policy, contracts, liability, compliance, cybersecurity, and active defense – all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues, or other investigations.

The Global Information Assurance Certification (GLEG) associated with LEG523 demonstrates to employers that you have absorbed the sophisticated content of this course and are ready to put it to use. This coveted GIAC certification distinguishes any professional – whether a cybersecurity specialist, auditor, lawyer, or forensics expert – from the rest of the pack. It also strengthens the credibility of forensics investigators as witnesses in court and can help a forensics consultant win more business. And the value of the certification will only grow in the years to come as law and security issues become even more interconnected.

The course also provides training and continuing education for many compliance programs under information security and privacy mandates such as GLBA, HIPAA, FISMA, GDPR, and PCI-DSS.

Each successive section of this course builds upon lessons from the earlier sections in order to comprehensively strengthen your ability to help your public or private sector enterprise cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with cybersecurity. We cover topical stories, such as Home Depot's legal and public statements about its payment card breach and lawsuits against QSA security vendor Trustwave filed by cyber insurance companies and credit card issuers (third parties with which Trustwave had no relationship!).

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Professionals from outside the United States attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence, and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

One thing that sets this course apart is its emphasis on ethics. The course teaches practical lessons on ethical performace by cyber defenders and digital investigators.

LDR525: Managing Cybersecurity Initiatives and Effective Communication

5 Day Program	30 CPEs	Laptop Not Needed

You Will Be Able To

- Understand predictive/waterfall, adaptive/agile development approaches and how they interact with product and project life cycles.
- Learn how to use and implement lean/agile tools, complexity models, root cause analysis
- Recognize the top failure mechanisms related to security projects, so that your projects can avoid common pitfalls
- Create a project charter which increases stakeholder engagement
- Document project requirements and create requirements traceability matrix to track changes throughout the project lifecycle
- Clearly define the scope of a project in terms of cost, schedule, and technical deliverables
- Develop a project schedule, including critical path tasks and milestones
- Cultivate user stories to drive adaptive sprint cycles
- Create accurate project cost and time estimates
- Develop planned and earned value metrics for your project deliverables and automate reporting functions
- Effectively manage conflict situations and build communication skills with your project team
- Analyze project risks in terms of probability and impact, assign triggers and risk response responsibilities
- Create project earned value baselines and project forecasts based on actual performance
- Communicate effectively with stakeholders, technical staff, and management teams

"LDR525 offers tools and techniques that will directly improve the planning, execution, and closing of your projects."

— Michael Long, **ARCYBER**

Meet and exceed your security program's goals.

SANS LDR525: Managing Security Initiatives and Effective Communication provides the training necessary to maintain the Project Management Professional (PMP)® and other professional credentials. SANS Institute is a PMI® authorized training partner.

This course is focused on delivering bottom line value from security initiatives while following modern adaptive, agile, iterative, and predictive development approaches and leveraging the benefits of increased effective organizational communication. During this class students learn how to improve project planning methodology and project task scheduling to get the most out of critical IT resources. We utilize cyber security project case studies to increase practical understanding of real-world issues. LDR525 follows the basic methodologies and principles from the updated PMBOK® Guide, also providing specific implementation techniques for success. Throughout the five sections, all aspects of leading security initiatives—from project business justification analysis, selecting the appropriate development approach that fits your stakeholder and organizational structure using predictive, adaptive, and hybrid implementations tailored to drive value—are covered. We focus on planning for and managing cost, time, quality, and risk while your project is active, to completing, closing, and documenting as your project finishes. A copy of the PMBOK® Guide Seventh edition is provided to all participants. Students can reference the PMBOK® Guide and use course material along with the knowledge gained in class to prepare for the GIAC Certified Project Manager Exam (GCPM) and earn PDUs/CPEs to maintain the Project Management Professional (PMP)® and other professional credentials.

Project management methodologies and frameworks are highlighted that can be applied across any product life cycle, in any industry. Although our primary focus is the application of security initiatives, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, risk, and compliance aspects affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

NOTE: PMP® and PMBOK® are registered marks of the Project Management Institute, Inc. PMP® exams are not hosted by SANS. You will need to make separate arrangements to take the PMP® exam and this course is not an official PMP® prep class.

Course Author Statement

"Managing projects to completion, with an alert eye on quality, cost, and time, is something most of us need to do on an ongoing basis. In this course, we break down project management into its fundamental components and galvanize your understanding of the key concepts with an emphasis on practical application and execution of service-based IT and InfoSec projects. Since project managers spend the vast majority of their time communicating with others, throughout the week we focus on traits and techniques that enable effective technical communication. As people are the most critical asset in the project management process, effective and thorough communication is essential."
—Jeff Frisk

Certification: GIAC Certified Project Manager (GCPM)
giac.org/gcpm

LDR551: Building and Leading Security Operations Centers

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Collect the most important logs and network data
- Build, train, and empower a diverse team
- Create playbooks and manage detection use cases
- Use threat intelligence to focus your budget and detection efforts
- Utilize threat hunting and active defense strategies
- Implement efficient alert triage and investigation workflow
- Implement effective incident response planning and execution
- Choose metrics and a long-term strategy to improve the SOC
- Implement team member training, retention, and prevention of burnout
- Understand SOC assessment through capacity planning, purple team testing, and adversary emulation

"There are so many [organizations] that seem to be trying to reinvent the wheel. All they need to do is invest in this course for real-world, actionable information that can put them on a solid path toward building, staffing, and leading their own SOC."

—Brandi Loveday-Chesley

"I would recommend this course to anyone running a security operations team. I'd further recommend it to more experienced analysts so they can begin to see the bigger picture."

—Robert Wilson, **University of South Carolina**

Managers must show alignment to the business and demonstrate real value – a challenge when the threats are constantly changing and sometimes unseen. Managing a security operations center (SOC) requires a unique combination of technical knowledge, management skills, and leadership ability. LDR551 bridges gaps by giving students the technical means to build an effective defense and the management tools to build an effective team. Common questions SOC leaders face are:

- How do we know our security teams are aligned to the unique threats facing our organization?
- How do we get consistent results and prove that we can identify and respond to threats in time to minimize business impact?
- How can we build an empowering, learning environment where analysts can be creative and solve problems while focusing on the mission at hand?

Whether you are looking to build a new SOC or take your current team to the next level, LDR551 will super-charge your people, tools, and processes. Each section of LDR551 is packed with hands-on labs and introductions to some of the industry's best free and open source tools, and each day concludes with Cyber42 SOC leadership simulation exercises. Students will learn how to combine SOC staff, processes, and technology in a way that promotes measurable results and covers all manner of infrastructure and business processes. Most importantly, students will learn how to keep the SOC growing, evolving, and improving over time.

Business Takeaways

- Strategies for aligning cyber defense to organizational goals
- Tools and techniques for validating security tools and processes
- Methodologies for recruiting, hiring, training, and retaining talented defenders and effective management and leadership techniques for technical teams
- Practical approaches to optimizing security operations that can be applied immediately

Hands-On Training

While this course is focused on management and leadership, it is by no means limited to non-technical processes and theory. The course uses the Cyber42 interactive leadership simulation game to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. Throughout the five days of instruction, students will work on fifteen hands-on exercises covering everything from playbook implementation to use case database creation, attack and detection capability prioritization and visualization, and purple team planning, threat hunting, and reporting. Attendees will leave with a framework for understanding where their SOC should be focusing its efforts, how to track and organize defensive capabilities, and how to drive, verify, and communicate SOC improvements.

Certification: GIAC Security Operations Manager (GSOM)
giac.org/gsom

LDR553: Cyber Incident Management

5 Day Course | 30 CPEs | Laptop Required

You Will Be Able To

- Implement various incident response frameworks
- Scope incidents correctly
- Define the incident management team's objectives
- Effectively manage a team under extreme pressure
- Be aware of human responses to facing catastrophically impactful urgent changes
- Structure, manage, and deliver briefings to upper management and the Board
- Plan and control communications when managing a serious incident
- Communicate with attackers about the pros and cons thereof
- Know where and how to track the incident
- Plan, coordinate, and execute counter compromise activities
- Master incident reports both during and post closure
- Understand the steps to close the incident and return to business as usual
- Understand the constraints of third-party or supply-chain incidents
- Plan for and deal with a compromised supply-chain organization
- Foster better cyber incident management support in other departments through combined training and exercises
- Plan, setup, and run cyber incident management training exercises
- Integrate Cyber Threat Intelligence to the IM team and capabilities
- Understand how bug bounties can be supported and how they can cause major incidents
- Develop the team to be able to investigate cloud attacks
- Support the Legal team in Business Email Compromise attacks and the nuances of types
- Track and improve the IM team's capability with playbooks and runbooks
- Comprehend the value and risks that AI could bring to the overall IR and IM process
- Improve readiness for ransomware attacks via simulated exercises

What is Cyber Incident Management?

Cyber Incident Management (IM) sits above Incident Response (IR) and is tasked to manage incidents that get too big for the Security Operations Center (SOC) and IR. These tend to be the more impactful or larger incidents that IR is not scaled to handle as it requires significant liaison with internal and external partners to coordinate the investigation, forensics, planning, recovery, remediation, and to brief the corporate comms, C-level staff and board as needed. Less technical and more business focused, the IM team will take the output from IR and relay it to the necessary teams as they coordinate wider investigations and hardening, hygiene and impact assessment as they plan towards recovery. A strong IR lead may fulfill the IM role, but during critical incidents IRs are often shoulder deep in malware, systems, logs and images to process to the point where all technically capable IR staff are kept focused on technical tasks. IMs are more business focused and IR is more technically focused.

Open in Case of Emergency

LDR553 looks at all the common and major cyber incident types, explains what the key issues are, and how plan a recovery. Whilst you may have a full team of technical staff standing by to find, understand, and remove the attackers, they need information, tasking, managing, supporting, and listening to maximize their utilization and effectiveness. We focus on building a team to remediate the incident, on managing that team, on distilling the critical data for briefing, and how to run that briefing. We look at communication at all levels from the hands-on team to the executives and Board, investigative journalists, and even the attackers.

This course empowers you to become an effective incident management team member or leader; ensuring you fully understand the different issues facing incident commanders in the immediate, short and medium term. As well as becoming comfortable with terminology, you will understand what preparatory work you can undertake at different stages to help you get ahead of the situation. LDR553 was developed to ensure efficient management of a diverse range of incidents with a focus on cyber; however, the methodology, concepts and guidance will apply to many regular major and critical incidents.

Business Takeaways

- Develop staff that know how to lead or contribute to a cyber incident management team
- Manage your incidents more effectively
- Resolve incidents quicker
- Understand the gaps in your security incident plans and response strategies
- Create higher performing security incident teams
- Plan ahead to handle some of the most devastating potential attacks

"Brilliant insight. Excellent content. An absolute must course for anyone dealing with incident management."

—Gary Smith

SEC566: Implementing and Auditing Security Frameworks and Controls

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each control and how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Security Controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

Notice to Students

The CIS released version 8 of the Controls in May 2021. This course content is updated to reflect the changes in the CIS Controls, as well as the most recent versions of the NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC).

Building and Auditing Critical Security Controls

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

In addition to defending their information systems, many organizations have to comply with a number of cybersecurity standards and requirements as a prerequisite for doing business. Dozens of cybersecurity standards exist throughout the world and most organizations must comply with more than one such standard. Is your organization prepared to comply and remain in compliance?

In February of 2016, then California Attorney General, Vice President Kamala Harris stated that "the 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

The Center for Internet Security (CIS) Critical Controls are specific security controls that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

As threats and attack surfaces change and evolve, an organization's security should as well. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the CIS Critical Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the CIS Critical Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by international governments, the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

SEC566 will enable you to master the specific and proven techniques and tools needed to implement and audit Version 8 of the CIS Controls as documented by the Center for Internet Security (CIS), as well as those defined by NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC). Students will learn how to merge these various standards into a cohesive strategy to defend their organization and comply with industry standards.

SANS' in-depth, hands-on training will teach security practitioners to understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats. SEC566 shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, this course is the best way to understand how you will measure whether the Controls and other standards are effectively implemented.

"Loved this course. It provides a method of measuring your security posture and applying the concept to any organization."

—John M., **U.S. Military**

Certification: GIAC Critical Controls Certification (GCCC)
giac.org/gccc

SANS

CISO NETWORK

An exclusive networking and knowledge-sharing opportunity for security leaders

SANS supports the cyber security community through the provision of world-leading training, certification, skills development programmes and through a vast array of free resources.

In addition, we have created a networking group for senior security professionals.

Our aim is to help ease the pressure of working as a security decision-maker by providing an environment in which ideas and lessons-learned can be shared amongst a peer group of influencers and thought leaders.

The network is open exclusively to security leaders at the highest level and connects a unique group of professionals who have the appetite and the authority to make a meaningful difference. By sharing ideas and lessons learnt from a wide variety of industries, the SANS CISO Network provides its members with a platform to influence our digital future and make the world a safer place.

SANS CISO Networking Events

- Listen to presentations from SANS Instructors and other global experts
- Take part in closed-door Q&A sessions
- Hear case studies and threat landscape updates from real-world practitioners
- Network with like-minded CISOs
- Address key topics and share knowledge on current challenges that face CISOs today
- Learn about the SANS Institute's initiatives and gain access to SANS Instructors
- Be among the first to receive access to newly created SANS resources
- Exclusive access to our online CISO Community platform

SANS CISO Network Advisory Board

James Lyne

James Lyne is the Chief of Innovation at SANS Institute. James has worked with many organisations on security strategy, handled a number of severe incidents and is a frequent industry advisor. He is a certified instructor at the SANS Institute and is often a headline presenter at industry conferences.

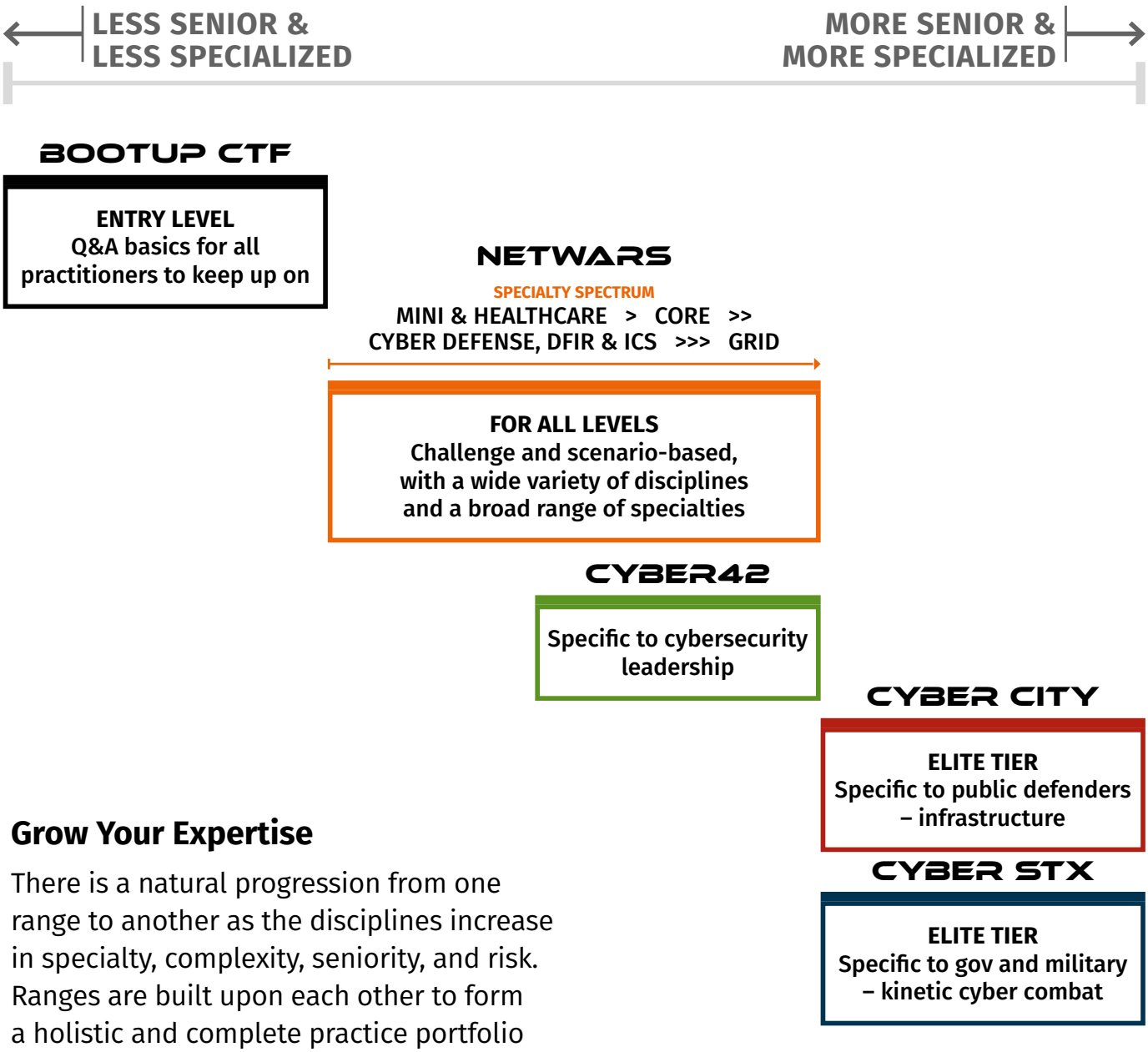
Frank Kim

Founder of ThinkSec, a security consulting and CISO advisory firm. Previously, as CISO at the SANS Institute, Frank led the information risk function for the most trusted source of computer security training and certification in the world. With the SANS Institute, Frank continues to lead the CISO and cloud security curricula, helping to develop the next generation of security leaders.

Join the SANS CISO Network

Apply to join this exclusive network today and see the list of upcoming events by visiting **sans.org/ciso-network**

RANGE SELECTION



Grow Your Expertise

There is a natural progression from one range to another as the disciplines increase in specialty, complexity, seniority, and risk. Ranges are built upon each other to form a holistic and complete practice portfolio for our customers to experience.

Learn more about SANS Cyber Ranges, upcoming range events, pricing, and more at **sans.org/cyber-ranges**

SANS CURRICULUM FOCUS AREA

Cloud Security

Cloud computing represents the most transformational technology of our era, and cloud security will play a pivotal role in its adoption. Cloud security must be focused on where the cloud is going, not where it is today. The future demands in-depth technical cloud capabilities coupled with knowledge of the security and service features for each of the major cloud service providers (CSPs). Begin your journey to become a Cloud Security Ace.

Our curriculum has been developed through an industry consensus process and is a holistic, hands-on approach to address public cloud security, which includes multicloud and hybrid-cloud scenarios for the enterprise and developing organizations alike. Learn how various CSPs interact and the nuances among them rather than merely learning the ins-and-outs of one platform.

Get your hands dirty in cloud security training by teaching you how to:

- Harden and configure public cloud services from AWS, Azure, and Google Cloud Platform (GCP)
- Automate security and compliance best practices
- Use cloud services to securely build and deploy systems and applications
- Inject security seamlessly into your DevOps toolchain
- Securely build, deploy, and manage containers and Kubernetes
- Discover vulnerabilities and weaknesses in your cloud environments
- Find attacker activity in your cloud logs

Enhance your training with:

- We are building a diverse community of cloud security professionals. Join us in our new Discord channel. **sansurl.com/cloud-discord**
- **SANS Cloud Ace podcast** has now launched. Stay tuned in at **sans.org/podcasts/cloud-ace**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a certificate in Cloud Security **sans.edu**

"The world has shifted to the cloud and we, as security professionals, have to make the same shift."

—Daniel Harrison, **Capital One**

Cloud Security Job Roles:

- Cloud Security Analyst
- Cloud Security Engineer
- Cloud Security Architect
- Cloud Security Manager
- DevOps Professionals

SEC488: Cloud Security Essentials

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Navigate your organization through the security challenges and opportunities presented by cloud services
- Identify the risks of the various services offered by cloud service providers (CSPs)
- Select the appropriate security controls for a given cloud network security architecture
- Evaluate CSPs based on their documentation, security controls, and audit reports
- Confidently use the services of any of the leading CSPs
- Protect secrets used in cloud environments
- Leverage cloud logging capabilities to establish accountability for events that occur in the cloud environment
- Identify the risks and risk control ownership based on the deployment models and service delivery models of the various products offered by cloud service providers (CSPs).
- Evaluate the trustworthiness of CSPs based on their security documentation, service features, third-party attestations, and position in the global cloud ecosystem.
- Secure access to the consoles used to access the CSP environments.
- Implement network security controls that are native to both AWS and Azure.
- Follow the penetration testing guidelines put forth by AWS and Azure to invoke your "inner red teamer"to compromise a full stack cloud application

Business Takeaways

- Understand the current cloud deployment
- Protect cloud-hosted workloads, services, and virtual machines
- Cost-effectively select appropriate services and configure properly to adequately defend cloud resources
- Get in front of common security misconfigurations BEFORE they are implemented in the cloud
- Ensure business is aligning to industry regulations and laws when operating in the cloud
- Decrease adversary dwell time in compromised cloud deployments

License to Learn Cloud Security

Research shows that most enterprises have strategically decided to deploy a multicloud platform, including Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), other cloud service providers. Mature CSPs have created a variety of security services that can help customers use their products in a more secure manner, but only if the customer knows about these services and how to use them properly. This course covers real-world lessons using security services created by the Big 3 CSPs, as well as open-source tools. Each section of the course features hands-on lab exercises to help students hammer home the lessons learned. We progressively layer multiple security controls in order to end the course with a functional security architecture implemented in the cloud.

This course will equip you to implement appropriate security controls in the cloud, often using automation to "inspect what you expect." We will begin by diving headfirst into one of the most crucial aspects of cloud - Identity and Access Management (IAM). From there, we'll move on to securing the cloud through discussion and practical, hands-on exercises related to several key topics to defend various cloud workloads operating in the different CSP models of: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Functions as a Service (FaaS).

Hands-On Training

SEC488: Cloud Security Essentials reinforces the training material via multiple hands-on labs in each section of the course. Labs are performed via a browser-based application rather than virtual machine. Each lab is designed to impart practical skills that students can bring back to their organizations and apply on the first day back in the office. The labs go beyond the step-by-step instructions by providing the context of why the skill is important and instilling insights as to why the technology works the way it does.

Certification: GIAC Cloud Security Essentials (GCLD)
giac.org/gcld

SEC510: Public Cloud Security: AWS, Azure, and GCP

5 Day Course	38 CPEs	Laptop Required

You Will Be Able To

- Understand the inner workings of cloud services and Platform as a Service (PaaS) / Infrastructure as a Service (IaaS) offerings in order to make more informed decisions in the cloud
- Understand the design philosophies that undergird each provider and how these have influenced their services in order to properly prescribe security solutions for them
- Discover the unfortunate truth that many cloud services are adopted before their security controls are fully fleshed out
- Understand Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) in depth.
- Understand the intricacies of Identity and Access Management, one of the most fundamental concepts in the cloud and yet one of the last understood
- Understand cloud networking and how locking it down is a critical aspect of defense-in-depth in the cloud
- Analyze how each provider handles encryption at rest and in transit in order to prevent sensitive data loss
- Apply defense-in-depth techniques to protect data in cloud storage
- Compare and contrast the serverless platforms of each provider
- Explore the service offering landscape to discover what is driving the adoption of multiple cloud platforms and to assess the security of services at the bleeding edge, such as serverless platforms
- Utilize multicloud IAM and cloud Single Sign-On to provide secure access to resources across cloud accounts and providers
- Automate security and compliance checks using cloud-native platforms and open-source solutions
- Understand Terraform Infrastructure-as-Code well enough to share it with your engineering team as a starting point for implementing the controls discussed in the course

"The course content has been very well put together, well researched, and is very applicable."

—Dan Van Wingerden, **Radiology Partners**

Multiple clouds require multiple solutions.

SEC510 provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Students will launch unhardened services, analyze the security configuration, validate that they are insufficiently secure, deploy patches, and validate the remediation. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services and will leave the course confident that they have the knowledge they need when adopting services and Platform as a Service (PaaS) / Infrastructure as a Service (IaaS) offerings in each cloud.

The Big 3 cloud providers alone provide more services than any one company can consume. As security professionals, it can be tempting to limit what the developers use to the tried-and-true solutions of yesteryear. Unfortunately, this approach will inevitably fail as the product development organization sidelines a security entity that is unwilling to change. Functionality drives adoption, not security, and if a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. SEC510 gives you the ability to provide relevant and modern guidance and guardrails to these teams to enable them to move both quickly and safely.

Hands-On Training

SEC510: Public Cloud Security: AWS, Azure, and GCP consolidates all of the concepts discussed in the lectures through hands-on labs. In the labs, students will assess a modern web application written with Next.js, React, and Sequelize that leverages the cloud native offerings of each provider. Each lab includes step-by-step guide as well as a no-hints option for students who want to test their skills without further assistance. This allows students to choose the level of difficulty that is best for them and fall back to the step-by-step guide as needed.

SEC510 also offers students an opportunity to participate in CloudWars Bonus Challenges each day in a gamified environment, while also providing more hands-on experience with the cloud security and relevant tools.

Course Authors' Statement

"The move to leveraging multiple public cloud providers introduces new challenges and opportunities for security and compliance professionals. As the service offering landscape is constantly evolving, it is far too easy to prescribe security solutions that are not accurate in all cases. While it is tempting to dismiss the multicloud movement or block it at the enterprise level, this will only make the problem harder to control.

"Why do teams adopt additional cloud solutions in the first place? To make their jobs easier or more enjoyable. Developers are creating products that make money for the business, not for the central security team. If a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. Security should embrace the inevitability of the multicloud movement and take on the hard work of implementing guardrails that enable the organization to move quickly and safely.

"The multicloud storm is coming, whether you like it or not."

— Brandon Evans and Eric Johnson

Certification: GIAC Public Cloud Security (GPCS)
giac.org/gpcs

SEC522: Application Security: Securing Web Apps, APIs, and Microservices

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Defend against the attacks specified in OWASP Top 10
- Infrastructure security and configuration management
- Securely integrating cloud components into a web application
- Authentication and authorization mechanisms, including single sign-on patterns
- Cross-domain web request security
- Protective HTTP headers
- Defending SOAP, REST and GraphQL APIs
- Securely implement Microservice architecture
- Defending against input related flaws such as SQL injection, XSS and CSRF

"Labs were fun and challenging."

—Linh Sithihao, **Dignity Health**

"[Labs are] thought out and easy to follow with good practical knowledge learned."

—Barbara Boone, **CDC**

"Lots of good hands-on exercises using real-world examples."

—Nicolas Kravec, **Morgan Stanley**

"The exercises are a good indicator of understanding the material. They worked flawlessly for me."

—Robert Fratila, **Microsoft**

It's not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how.

During the course, we demonstrate the risks of web applications and the extent of sensitive data that can be exposed or compromised. From there, we offer real world solutions on how to mitigate these risks and effectively evaluate and communicate residual risks.

After attending the class, students will be able to apply what they learned quickly and bring back techniques to not only better secure their applications, but also do so efficiently by adding security early in the software development life cycle, shifting left security decisions and testing, thus saving time, money, and resources for the organization.

Business Takeaways

- Comply with PCI DSS 6.5 requirements
- Reduce the overall application security risks, protect company reputation
- Adopt the Shifting left mindset where security issues addressed early and quickly. This avoids the costly rework.
- Ability to adopt modern apps with API and microservices in a secure manner
- This course prepares students for the GWEB certification

Hands-on Training

The provided VM lab environment contains realistic application environment to explore the attacks and the effects of the defensive mechanisms. The exercise is structured in a challenge format with hints available along the way. The practical hands-on exercises help students gain experience to hit the ground running back at the office. There are 20 labs in section 1 to section 5 of the class and in the last section, there is a capstone exercise called Defending the Flag where there is 3–4 hours of dedicated competitive exercise time.

- **SECTION 1:** HTTP Basics, HTTP/2 traffic inspection and spoofing, Environment isolation, SSRF and credential-stealing
- **SECTION 2:** SQL Injection, Cross Site Request Forgery, Cross Site Scripting, Unicode and File Upload
- **SECTION 3:** Authentication vulnerabilities and defense, Multifactor authentication, Session vulnerabilities and testing, Authorization vulnerabilities and defense, SSL vulnerabilities and testing, Proper encryption use in web application
- **SECTION 4:** WSDL enumerations, Cross Domain AJAX, Front End Features and CSP (Content Security Policy), Clickjacking
- **SECTION 5:** Deserialization and DNS rebinding, GraphQL, API gateways and JSON, SRI and Log review
- **SECTION 6:** Defending the Flag capstone exercise

Certification: GIAC Certified Web Application Defender (GWEB)
giac.org/gweb

SEC540: Cloud Security and DevSecOps Automation

5 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Understand how DevOps works and identify keys to success
- Wire security scanning into automated CI/CD pipelines and workflows
- Build continuous monitoring feedback loops from production to engineering
- Automate configuration management using Infrastructure as Code (IaC)
- Secure container technologies (such as Docker and Kubernetes)
- Use native cloud security services and third-party tools to secure systems and applications
- Securely manage secrets for Continuous Integration servers and applications
- Integrate cloud logging and metrics
- Perform continuous compliance and security policy scanning

Authors' Statement

"DevOps and the cloud are radically changing the way that organizations design, build, deploy, and operate online systems. Leaders like Amazon, Etsy, and Netflix are able to deploy hundreds or even thousands of changes every day, continuously learning, improving, and growing - and leaving - their competitors far behind. Now DevOps and the cloud are making their way from Internet 'Unicorns' and cloud providers into enterprises.

"Traditional approaches to security can't come close to keeping up with this rate of accelerated change. Engineering and operations teams that have broken down the "walls of confusion " in their organizations are increasingly leveraging new kinds of automation, including Infrastructure as Code, Continuous Delivery and Continuous Deployment, microservices, containers, and cloud service platforms. The question is: Can security take advantage of the tools and automation to better secure its systems?

"Security must be reinvented in a DevOps and cloud world."

— Ben Allen, Jim Bird, Eric Johnson, and Frank Kim

The Cloud Moves Fast. Automate to Keep Up.

Common security challenges for organizations struggling with the DevOps culture include issues such as:

- Upfront peer code reviews and security approvals may not occur for change approval and audit requirements
- Missing infrastructure and application scanning can allow attackers to find an entry point and compromise the system
- Cloud security misconfigurations may publicly expose sensitive data or introduce new data exfiltration paths

Security teams can help organizations prevent these issues such as using DevOps tooling and cloud-first best practices. This course provides development, operations, and security professionals with a deep understanding of and hands-on experience with the DevOps methodology used to build and deliver cloud infrastructure and software. Students learn how to attack and then harden the entire DevOps workflow, from version control to continuous integration and running cloud workloads. Each step of the way, students explore the security controls, configuration, and tools required to improve the reliability, integrity, and security of on-premise and cloud-hosted systems. Students learn how to implement more than 20 DevSecOps security controls to build, test, deploy, and monitor cloud infrastructure and services.

Business Takeaways

- Build a security team that understands modern cloud security and DevSecOps practices
- Partner with DevOps and engineering teams to inject security into automated pipelines
- Leverage cloud services and automation to improve security capabilities
- Ensure your organization is ready for cloud migration and digital transformation initiatives

Hands-On Training

SEC540 goes well beyond traditional lectures and immerses students in hands-on application of techniques during each section of the course. Each lab includes a step-by-step guide to learning and applying hands-on techniques, as well as a "no hints" approach for students who want to stretch their skills and see how far they can get without following the guide. This allows students, regardless of background, to choose the level of difficulty they feel is best suited for them -always with a frustration-free fallback path. Immersive hand-on labs ensure that students not only understand theory, but how to configure and implement each security control.

The SEC540 lab environment simulates a real-world DevOps environment, with more than 10 automated pipelines responsible for building DevOps container images, cloud infrastructure, automating gold image creation, orchestrating containerized workloads, executing security scanning, and enforcing compliance standards. Students are challenged to sharpen their technical skills and automate more than 20 security-focused challenges using a variety of command line tools, programming languages, and markup templates.

The SEC540 course labs come in both AWS and Azure versions. Students will choose one cloud provider at the beginning of class to use for the duration of the course. Students are welcome to do labs for both cloud providers on their own time once they finish the first set of labs.

For advanced students, 2 hours of CloudWars Bonus Challenges are available during extended hours each day. These CloudWars challenges provide additional opportunities for hands-on experience with the cloud and DevOps toolchain.

Certification: GIAC Cloud Security Automation (GCSA)
giac.org/gcsa

SEC541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Research attacks and threats to cloud infrastructure and how they could affect you
- Break down a threat into detectable components
- Effectively use AWS and Azure core logging services to detect suspicious behaviors
- Make use of cloud native API logging as the newest defense mechanism in cloud services
- Move beyond the cloud-provided Graphic User Interfaces to perform complex analysis
- Perform network analysis with cloud-provided network logging
- Understand how application logs can be collected and analyzed inside the cloud environment
- Effectively put into practice the AWS and Azure security specific services
- Integrate container, operating system, and deployed application logging into cloud logging services for more cohesive analysis
- Centralize log data from across your enterprise for better analysis
- Perform inventory of cloud resources and sensitive data using scripts and cloud native tooling
- Analyzing Microsoft 365 activity to uncover threats
- Ability to leverage cloud native architecture to automate response actions to attacks

Authors' Statement

"Cloud service providers are giving us new tools faster than we can learn how to use them. As with any new and complex tool, we need to get past the surface-level 1how-to in order to radically reshape our infrastructure. This course is an overview of the elements of AWS and Azure that we may have used before but are ready to truly explore. By the end of the class, you ll be confident knowing that you have the skills to start looking for the threats and building a true threat detection program in AWS and Azure."

—Shaun McCullough and Ryan Nicholson

Attackers can run but not hide. Our radar sees all threats.

SEC541 is a cloud security course that investigates how attackers are operating against Amazon Web Services (AWS) and Microsoft Azure environments, the attacker's characteristics, and how to detect and investigate suspicious activity in your cloud infrastructure. You will learn how to spot the malice and investigate suspicious activity in your cloud infrastructure. In order to protect against cloud environment attacks, an organization must know which types of attacks are most likely to happen in your environment, be able to capture the correct data in a timely manner, and be able to analyze that data within the context of their cloud environment and overall business objectives.

SEC541 starts each day by walking through a real-world attack campaign against a cloud infrastructure. We will break down how it happened, what made it successful, and what could have been done to catch the attackers in the act. After dissecting the attacks, we learn how to leverage cloud native and cloud integrated capabilities to detect, threat hunt, or investigate similar attacks in a real environment, and building our arsenal of analytics, detections and best practices. The course dives into the AWS and Azure services, analyzing logs and behaviors and building analytics that the students can bring back to their own cloud infrastructure.

Business Takeaways

- Decrease the average time an attacker is in your environment
- Demonstrate how to automate analytics, thus reducing time
- Help your organization properly set up logging and configuration
- Decreases risk of costly attacks by understanding and leveraging cloud specific security services
- Lessen the impact of breaches that do happen
- Learn how to fly the plane, not just the ability to read the manual

Hands-on Training

The labs in this course are hands-on explorations into AWS and Azure logging and monitoring services. **About 75% of labs are AWS and 25% Azure.** Each lab will start by researching a particular threat and the data needed to detect it. In most labs, the students will conduct the attack against their accounts, generating the logs and data needed to perform analysis. Students will use native AWS and Azure services and open-source products to extract, transform, and analyze the threat. The course lecture coupled with the labs will give students a full picture of how those services within AWS & Azure work, the data they produce, common ways to analyze the data, and walk away with the ability to discern and analyze similar attacks in their own cloud environment.

- **SECTION 1:** SEC541 environment deployment, analyzing cloud API logs with CloudTrail, parsing JSON-formatted logs with JQ, network analysis
- **SECTION 2:** Environment setup, application/OS log lab with OpenCanary, CloudWatch agent and customization, strange ECS behavior, finding data exfiltration
- **SECTION 3:** Metadata services and GuardDuty, cloud inventory, discovering sensitive data in unapproved location with Macie, vulnerability assessment with Inspector, data centralization with Graylog
- **SECTION 4:** Microsoft 365 Exchange investigation, introduction to Kusto Query Language, log analytics analysis using Azure CLI, Microsoft Defender for Cloud and Sentinel, Azure network traffic analysis
- **SECTION 5:** Setup the automate forensics workflow, analyze the results, participate in the CloudWars Challenge

Certification: GIAC Cloud Threat Detection (GCTD)
giac.org/gctd

SEC549: Enterprise Cloud Security Architecture

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Enable business through secure cloud architectural patterns
- Connect the dots between architectural patterns and real-life infrastructure
- Build a secure, scalable identity foundation in the cloud
- Centralize your organization's workforce identity to prevent sprawl
- Build micro-segmented networks using hub and spoke patterns
- Configure centralized network firewalls for inspecting north-south and east-west traffic
- Learn how to incorporate both network-based and identity-based controls
- Ability to create data perimeters for cloud-hosted data repositories
- Centralize and share Key Management Service (KMS) resources across an organization
- Enable Security Operations to respond in the Cloud
- Understand the telemetry and logging available across service models (IaaS, PaaS and SaaS)
- Design recovery processes leveraging break-glass accounts
- Strategically approach a phased cloud migration

"I would recommend this course. It hits many core aspects of secure design. Additionally, lack of Cloud Security Architecture and Strategy, and Insecure Design have been highlighted as a top risk by organizations like Cloud Security Alliance and OWASP. Cloud security architecture topics need to have more attention and focus in general."

—Greg Lewis, **SAP**

Design it Right from the Start

Without a mental model for threats in the cloud, architects attempt to strong-arm design patterns intended for the on-premise world onto cloud systems, hindering the speed of cloud adoption and modernization. Worse yet, failure to identify trust boundaries in the cloud results in missing security controls at the identity or network-planes and poor security outcomes. SEC549 introduces students to security architecture as it applies to the cloud. Students take away from this course a clear mental model of the cloud and the controls available to them, allowing students to shift their threat models to this new, vastly different world with distributed perimeters and unfamiliar trust boundaries.

It's inevitable that even the most mature organizations will have their security posture challenged, therefore in this course we dive deep into architectures which enable Security Operation Centers to monitor, detect, respond and recover from incidents in the cloud. Students learn how to effectively support business goals with robust logging of cloud telemetry and centralization of events and insights gathered at the edge. This course empowers the Architect to ensure adequate logging is configured in cloud environments and develop recovery strategies emphasizing the need to design for availability.

SEC549 is constructed around the cloud migration journey of a fictional company and the challenges they encounter along the way. Students are tasked with phasing in a centralized identity plan, building large scale micro-networks, and designing big data services for cloud-hosted applications. Both network-layer and identity-layer controls are covered in-depth as complementary mechanisms for securing access to distributed resources. The importance of centralizing identity is a core take-away of this course as showcased through the discussion of fragmented identity and its perils, especially with the rise of the Cloud and the adoption of multiple cloud service providers. Students are taught the foundational concepts used when designing for phased identity consolidation so they can confidently tackle similar challenges on the job.

Business Takeaways:

- Mitigate the risk posed by nascent cloud technologies and their rapid adoption
- Decrease the risk of cloud migrations by planning for phased approach
- Help your organization prevent identity sprawl and tech debt through centralization
- Enable business growth by creating high-level guardrails
- Prevent costly anti-patterns from becoming entrenched
- Move your organization towards a Zero-Trust posture through the uplifting of existing access patterns

Hands-On Training:

The hands-on portion of the course is unique and especially suited to the student who wants to architect for the cloud. Each lab is performed by observing and correcting an anti-pattern presented as an architectural diagram. The "correct" version of each diagram is implemented as live infrastructure in AWS and made available to the student to explore the configurations. In this course, the students have access to an enterprise-scale AWS Organization and can observe all details discussed in the labs and throughout the course.

Each of the sections of the course discusses security design considerations for all three major clouds, however there is an emphasis on working with AWS and labs are structured around concepts in AWS.

SEC588: Cloud Penetration Testing

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Conduct cloud-based penetration tests
- Assess cloud environments and bring value back to the business by locating vulnerabilities
- Understand first-hand how cloud environments are constructed and how to scale factors into the gathering of evidence
- Assess security risks in Amazon and Microsoft Azure environments, the two largest cloud platforms in the market today
- Immediately apply what you have learned to your work

Aim Your Arrows To The Sky And Penetrate The Cloud

You have been asked to perform a penetration test, security assessment, maybe an Attacker Simulation or a red team exercise. The environment in question is mainly cloud-focused. It could be entirely cloud-native for the service provider or Kubernetes-based. Perhaps the environment in question is even multi-cloud, having assets in both Amazon and Azure. What if you have to assess Azure Active Directory, Amazon Web Services (AWS) workloads, serverless functions, or Kubernetes? SEC588: Cloud Penetration Testing will teach you the latest penetration testing techniques focused on the cloud and how to assess cloud environments.

Computing workloads have been moving to the cloud for years. Analysts predict that most, if not all, companies will have soon have workloads in public and other cloud environments. While organizations that start in a cloud-first environment may eventually move to a hybrid cloud and local data center solution, cloud usage will not decrease significantly. So when assessing risks to an organization going forward, we need to be prepared to evaluate the security of cloud-delivered services.

The most commonly asked questions regarding cloud security when it comes to penetration testing are: Do I need to train specifically for engagements that are cloud-specific? and Can I accomplish my objectives with other pen test training and apply it to the cloud? In cloud-service-provider environments, penetration testers will not encounter a traditional data center design, there will be new attack surface areas in the service (control) planes of these environments. Learning how such an environment is designed and how you as a tester can assess what is in it is a niche skill set that must be honed. What we rely on to be true in a classical data center environment such as who owns the Operating System and the infrastructure and how the applications are running will likely be very different. Applications, services, and data will be hosted on a shared hosting environment unique to each cloud provider.

SEC588: Cloud Penetration Testing draws from many skill sets required to assess a cloud environment properly. If you are a penetration tester, the course will provide a pathway to understanding how to take your skills into cloud environments. If you are a cloud-security-focused defender or architect, the course will show you how the attackers are abusing cloud infrastructure to gain a foothold in your environments.

The course dives into topics of classic cloud Virtual Machines, buckets, and other new issues that appear in cloud-like microservices, in-memory data stores, files in the cloud, serverless functions, Kubernetes meshes, and containers. It also covers Azure and AWS penetration testing, which is particularly important given that AWS and Microsoft account for more than half of the market. The goal is not to demonstrate these technologies but to teach you how to assess and report on the actual risk your organization could face if these services are left insecure.

"SANS course SEC588 taught me more than I expected. With the rapid development of new technologies offered by cloud providers, SEC588 has given me an important framework for cloud pen testing."

—Jonus Gerrits, **Phillips 66**

"This emerging course perfectly complements the change in the direction of red team engagement scopes."

—Kyle Spaziani, **Sanofi**

Certification: GIAC Cloud Penetration Tester (GCPN)
giac.org/gcpn

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Create, implement, and mature your vulnerability management program and get buy-in from your stakeholders
- Implement techniques for building and maintaining an accurate and useful inventory of IT assets in the enterprise and the cloud
- Identify processes and technologies that are effective across both infrastructure and applications and know how to configure them appropriately
- To be aware of common false positives or false negatives in your identification arsenal
- Prioritize unblocked vulnerabilities for treatment based on a variety of techniques
- Effectively report and communicate vulnerability data within your organization
- Identify and report on the risk associated with vulnerabilities that are blocked and cannot currently be prioritized for remediation
- Have a better understanding of modern treatment capabilities and how to better engage with treatment teams
- Make vulnerability management more fun and engaging for all those involved
- Differentiate how to deal with application layer vulnerabilities versus infrastructure vulnerabilities
- Understand how your strategies and techniques might change as you move to the cloud, implement private cloud, or roll out DevOps within your organization

Business Takeaways

This course will help your organization:

- Understand what is working and what is not working in modern day vulnerability programs
- Anticipate and plan for the impacts related to cloud operating environments
- Realize why context matters and how to gather, store, maintain, and utilize contextual data effectively
- Effectively and efficiently communicate vulnerability data and its associate risk to key stakeholders
- Determine how to group vulnerabilities meaningfully to identify current obstacles or deficiencies
- Know which metrics will drive greater adoption and change within the organization
- Understand what remediation capabilities are available to assist technology teams in resolving vulnerabilities and proactively

Stop Treating Symptoms. Cure the Disease.

Whether your vulnerability management program is well established or you are just getting started, this course will help you think differently about vulnerability management. You will learn how to move past the hype to successfully prioritize the vulnerabilities that are not blocked, then clearly and effectively communicate the risk associated with the rest of the vulnerabilities in your backlog that, for a variety of reasons, cannot currently be remediated. You'll also learn what mature organizations are doing to ease the burden associated with vulnerability management across both infrastructure and applications as well as across both their cloud and non-cloud environments. MGT516 is based on the Prepare, Identify, Analyze, Communicate, and Treat (PIACT) Model.

MGT516 helps you think strategically about vulnerability management in order to mature your organization's program, but it also provides tactical guidance to help you overcome common challenges. By understanding and discussing solutions to typical issues that many organizations face across both traditional and cloud operating environments, you will be better prepared to meet the challenges of today and tomorrow. Knowing that many organizations are adopting cloud services in addition to continuing to manage their more traditional operating environments, we'll also look at different cloud service types throughout the course and how they impact the program both positively and negatively. We will highlight some of the tools and processes that can be leveraged in each of these environments and present new and emerging trends.

Hand-On Training

MGT516 uses the Cyber42 leadership simulation game, critical thinking labs based on outlined scenarios, and demonstrations to provide you with the information you need to skillfully fight the VM battle. Cyber42 helps students absorb and apply the content throughout the course. In this web-based continuous tabletop exercise, students play to improve security culture, manage budget and schedule, and improve specific vulnerability management capabilities at the fictional organization, the "Everything Corporation" or "E Corp." This puts you in real-world scenarios that require you to think through various options for improving the organization's maturity by responding to specific events.

"This course is essential for both well-established and developing vulnerability management teams."

—Robert Adams, **CBC**

"A great course to utilize if new to cloud vulnerability management."

—Amaan Mughal

MGT520: Leading Cloud Security Design and Implementation

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Define a strategy for securing a workload in the cloud for medium-size and large enterprises that can support their business objectives
- Establish a security roadmap based on the security strategy that can support a fast-paced cloud adoption and migration path while maintaining a high degree of security assurance
- Understand the security basics of the cloud environment across different types of service offerings, then explain and justify to other stakeholders the decisions within the security roadmap
- Build an effective plan to mature a cloud security posture over time, leveraging security capabilities offered by cloud providers to leapfrog in security capabilities
- Explain the security vision of the organization in the cloud domain to your Board Directors and executives, collaborate with your peers, and engage your workforce, driving the security culture change required for the cloud transformation

"This type of training, i.e., cloud security from a management perspective, is rare and the quality of this one is definitely amazing."

—Benoit Ramillon, **UEFA**

Building and Leading a Cloud Security Program

Cloud adoption is popular across all types of industry, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions. However, an organization 's cloud transition requires numerous key decisions.

This course focuses on what managers, directors, and security leaders need to know to develop their cloud security roadmap, to manage the implementation of cloud security capabilities. Making the right security decisions when adopting the cloud requires understanding the technology, process, and people related to the cloud environment. This complements traditional IT management techniques that managers are accustomed to and helps with making the appropriate informed decisions. We will cover the key objectives of security controls in the cloud environment, including planning, deploying, and running the environment from the starting point to a progressively more mature state. There will be a focus on locking down the environment, securing the data, maintaining compliance, enhancing security visibility to the operations, and managing the security response on a continuous basis. Students will learn the essentials to lead the security effort for the cloud transition journey.

Business Takeaways:

- Establish cloud security program supporting the fast pace business transformation
- Make informed decisions on cloud security program
- Anticipate the security capabilities and guardrails to build for the securing the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Author Statement

"Cloud transition is common in many organizations these days, but many security leaders feel overwhelmed and underprepared for the security aspects of the cloud. When organizations accept security as an integral part of the transformation path, they can not only achieve the same level of security as their in-house IT environment, but also take advantage of a huge opportunity to leapfrog in security using cloud capabilities. In MGT520, we discuss industry-proven techniques to plan for the security aspects of cloud transformation. This course will arm students with the necessary information to confidently lead their organization towards securing the cloud workload and leveraging cloud capabilities to further enhance their security maturity in the IT environment."

—Jason Lam

SANS | GIAC CERTIFICATIONS

Voucher Program

The SANS Voucher Program allows organizations to:

- Efficiently purchase training in bulk using a single procurement process as compared to employees individually procuring courses
- Centrally administer use of training funds and monitor investments for optimal budgeting using the SANS Admin Tool
- Track and measure student course progress, final test scores and earned certifications

Training Investments & Reduced Pricing

To open a Voucher Account, an organization pays an agreed-upon training investment. Based on the amount of the training investment, that organization could be eligible for reduced pricing.

Investment and reduced pricing:

- Can be applied to any live, OnDemand or online SANS training course, SANS Summit, GIAC certification, or certification renewal*
- Balance can be increased at any time by making additional investments
- Need to be utilized within 12 months; however, the term can be extended by investing additional funds before the end of the 12-month term

**Current exceptions are the Partnership Program, Security Awareness Training, and SANS workshops hosted at events run by other companies.*

Flexibility & Control

The online SANS Admin Tool allows organizations to manage their training at anytime from anywhere.

With the SANS Admin Tool, the Administrator can:

- Approve and manage student enrollment
- View fund usage and balance in real time
- View students' certification status and test results
- Obtain OnDemand course progress by student per course

Get Started

Visit **sans.org/group-purchasing** and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little as one week of purchase, your employees can begin their training.

sans.org/group-purchasing

SANS CURRICULUM FOCUS AREA

Industrial Control Systems (ICS) Security

The current landscape presents a diverse and chaotic picture of the threats facing industrial control system owners and operators.

Attacks that cause physical damage or impact physical processes are no longer limited to theory or speculation. We are now seeing incidents where malicious actors successfully intrude, cause system damage, and impact operations using ICS-tailored malware. You need to be prepared to defend your control systems against increasingly sophisticated adversaries.

SANS ICS Security courses will teach you to:

- Recognize ICS components, purposes, deployments, significant drivers, and constraints
- Identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats
- Understand approaches to system and network defense architectures and techniques
- Perform ICS incident response focusing on security operations and prioritizing the safety and reliability of operations
- Implement effective cyber and physical access controls

Enhance your training with:

- Grid Netwars, ICS Netwars **sans.org/netwars**
- SANS Summit: ICS Security Summit & Training **sans.org/summit**
- Free Resources: Webcasts, blogs, forums, research, and more **ics.sans.org**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a Graduate Certificate in Industrial Control Systems **sans.edu**

"The training starts with theory and quickly progresses into full hands-on interaction with all components. This experience is not easy to find."

—Bassem Hemida, **Deloitte**

Industrial Control Systems Job Roles:

- ICS/OT Security Assessment Consultant
- ICS Security Engineer
- ICS Security Analyst
- Control Systems Engineer
- ICS Cybersecurity Engineer
- ICS/OT Security Manager

ICS410: ICS/SCADA Security Essentials

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and their relation to IEC 62443 and the Purdue Model.
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense to detect host and network-based intrusions via intrusion detection technologies
- Implement incident response and handling methodologies
- Map different ICS technologies, attacks, and defenses to various cybersecurity standards including the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, the Center for Internet Security Critical Security Controls, and COBIT 5

"A mix of hands-on and theoretical class, being driven by a highly skilled instructor, makes this the best training in ICS security."

—Rafael Issa, **Technip**

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems (ICS) is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of ICS components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT /OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Author Statement

"This course provides students with the essentials for conducting cybersecurity work in industrial control system environments. After spending years working with industry, we believe there is a gap in the skill sets of industrial control system personnel, whether it be cybersecurity skills for engineers or engineering principles for cybersecurity experts. In addition, both information technology and operational technology roles have converged in today's industrial control system environments, so there is a greater need than ever for a common understanding between the various groups who support or rely on these systems. Students in ICS410 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications."

– Justin Searle

Certification: Global Industrial Cyber Security Professional (GICSP)
giac.org/gicsp

ICS418: ICS Security Essentials for Managers

2 Day Course	12 CPEs	Laptop Required

You Will Be Able To

- Articulate the value of ICS security and tie cyber risk to business risk decisions
- Trend current and future technology changes to address business needs
- Measure successes in industrial cyber risk management, complete with metrics for executives and boards
- Use best practices to enable ICS security incident detection and response for their teams
- Leverage external information, including threat intelligence, to guide their ICS security program
- Provide governance, oversight, execution, and support across industrial facilities for ICS security initiatives and projects
- Apply the differences between IT and ICS security for an effective control system cybersecurity program
- Develop their security workforce to address gaps in hiring, training, and retention
- Apply advanced techniques to help shape and shift their organization's culture of security

Who Should Attend

ICS418 is aimed at managers of staff who are responsible for securing the day to day running of operational technology and industrial control system environments across an organization—this includes distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Managers of these teams often come from a diverse background with either a focus on management skills and minimal understanding of ICS environments, or technical individuals who rise in the ranks to a leader with minimal management skill development.

The course was designed to bridge the gap between those two skill sets, "raising the water level for all ships" when it comes to ICS security managers, including:

- **Manager asked to "Step-Over"**
  Traditional information technology (IT) security manager that must create, lead, or refine an ICS Security program
- **Practitioner to Manager: "Step-Up"**
  Industrial engineer, operator, or ICS security practitioner promoted to a manager position to create, lead, or refine an ICS security program
- **Manager Development: "In-Place"**
  An existing ICS security manager that is looking to further develop their leadership skills, specific to industrial security

ICS security is an ever-changing field requiring practitioners to continually adapt defense strategies to meet new challenges and threats. To compound the issue, any security changes need to be thoroughly tested to maintain the safety and reliability of industrial operations.

Globally, "critical infrastructure" and "operators of essential services" represent hundreds of thousands – if not millions—of industrial organizations. Some of them are the lifelines to our modern society, like water, energy, food processing, and critical manufacturing—but every industrial facility deserves to know their process is secure and safe. With increased threats, new technology trends, and evolving workforce demands, it is vital for security managers in operational technology (OT) to be trained in techniques to defend their facilities and their teams.

The two-day ICS418 fills the identified gap amongst leaders working across critical infrastructure and OT environments. It equips new or existing managers responsible for OT/ICS, or converged IT/OT cybersecurity. The course provides the experience and tools to address industry pressures to manage cyber risk to prioritize the business—as well as the safety and reliability of operations. ICS leaders will leave the course with a firm understanding of the drivers and constraints that exist in these cyber-physical environments and will obtain a nuanced understanding of how to manage the people, processes, and technologies throughout their organizations.

Authors' Statement

"Now, more than ever, it is important to train and equip ICS security leaders with the skills and knowledge they need to protect critical infrastructure. This course is the culmination of decades of experience in building and managing OT/ICS security teams—and it is the course we wish was available to us when we started on our ICS security journey. We've drawn across our roles in different industrial sectors and teams—as former company executives, team leads, incident responders, and managers—to create a course empowering leaders facing the greatest challenge of our time: industrial control system cybersecurity."

—Jason D. Christopher & Dean C. Parsons

Section Descriptions

SECTION 1: ICS Security Manager Core Development and Responsibilities

Industrial control systems (ICS) security managers must be able to create and sustain cybersecurity programs with challenging constraints. These leaders must be able to manage industrial cyber risks, plan for evolving technologies, and incorporate ICS-specific security standards. On the first day, students will learn the differences between traditional information technology (IT) and operational technology (OT) systems, as well as the associated threats, vulnerabilities, and potential impacts from ICS-specific cyber attacks. Once these elements of industrial cyber risk are established, students will explore using industry best practices, guidelines, and standards to assess and measure ICS security programs.

TOPICS: Overview of ICS and Critical Infrastructure; Attack History & Modern Adversaries; Cybersecurity Risk, Impacts, Goals and Safety; ICS Technology Trends; IT and OT Security Differences; ICS Incident Response Management; Industrial Cyber Risk Management; ICS Policy, Frameworks, Regulations and Compliance; Strategy Planning and Tactical Priorities

SECTION 2: ICS Security Team Development Focus

The second section of this course builds on the concepts around building an ICS security program and explores the workforce needs to manage the day-to-day tasks, planning, and reporting required to minimize cyber risk. Students will be equipped with a common understanding of the ICS security and safety culture, the skills required to perform various job functions, and both company-wide and team-specific security controls.

TOPICS: Governance, Oversight, Execution, and Support; Dedicated ICS Security Efforts and Measuring Value; Organization Roles and Responsibilities; Key Performance Indicators; Building and Maturing Effective ICS Security Teams; Building and Maturing ICS Cyber Defense Programs; ICS Security Awareness and Safety Culture; Executive Metrics and Communications

ICS456: Essentials for NERC Critical Infrastructure Protection

5	31	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Understand the cybersecurity objectives of the NERC Critical Infrastructure Protection (CIP) standards
- Understand the NERC regulatory framework, its source of authority, and the process for developing CIP standards, as well as their relationship to the other Bulk Electric System (BES) reliability standards
- Speak fluent NERC CIP and understand how seemingly similar terms can have significantly different meanings and impacts on your compliance program
- Break down the complexity to more easily identify and categorize BES cyber assets and systems
- Develop better security management controls by understanding what makes for effective cybersecurity policies and procedures
- Understand physical and logical controls and monitoring requirements
- Make sense of the CIP-007 system management requirements and their relationship to CIP-010 configuration management requirements, and understand the multiple timelines for assessment and remediation of vulnerabilities
- Determine what makes for a sustainable personnel training and risk assessment program
- Develop strategies to protect and recover BES cyber system information
- Know the keys to developing and maintaining evidence that demonstrates compliance and be prepared to be an active member of the audit support team.
- Sharpen your CIP Ninja!

This course empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Reliability Corporation (NERC), and the Regional Entities, provides multiple approaches for identifying and categorizing Bulk Electric System (BES) cyber systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

This course goes far beyond other NERC Critical Infrastructure Protection (CIP) courses that only teach what the standards are by providing information that will help you develop and maintain a defensible compliance program and achieve a better understanding of the technical aspects of the standards. Our 25 hands-on labs utilize three provided virtual machines that enable students to learn skills ranging from securing workstations to performing digital forensics and lock picking. Our students consistently tell us that these labs reinforce the learning and prepare them to do their jobs better.

You Will Learn:

- BES cyber system identification and strategies for lowering their impact rating
- Nuances of NERC-defined terms and the applicability of CIP standards and how subtle changes in definitions can have a big impact on your program
- The significance of properly determining cyber system impact ratings and strategies for minimizing compliance exposure
- Strategic implementation approaches for supporting technologies
- How to manage recurring tasks and strategies for CIP program maintenance
- Effective implementations for cyber and physical access controls
- How to break down the complexity of NERC CIP in order to communicate with your leadership
- What to expect in your next CIP audit, how to prepare supporting evidence, and how to avoid common pitfalls
- How to understand the most recent Standards Development Team's efforts and how that may impact your current CIP program

"This is best-in-class NERC CIP training. The courseware provides valuable compliance approaches and software tools for peer collaboration to build consent on implementation."

— Jeff Mantong, **WAPA**

Certification: GIAC Critical Infrastructure Protection (GCIP)
giac.org/gcip

ICS515: ICS Visibility, Detection, and Response

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Analyze ICS-specific threats and take proper courses of action to defend the industrial control systems
- Establish collection, detection, and response strategies for your ICS networks
- Use proper procedures during ICS incident response
- Examine ICS networks and identify the assets and their data flows in order to understand the network information needed to identify advanced threats
- Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using the SANS ICS515 Student Kit, which you retain after the class ends
- Gain in-depth knowledge on ICS targeted threats and malware including STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, and EKANS
- Leverage technical tools such as Shodan, Wireshark, Zeek, Suricata, Volatility, FTK Imager, PDF analyzers, PLC programming software, and more
- Create indicators of compromise (IOCs) in YARA
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, the Collection Management Framework, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

ICS515: ICS Visibility, Detection, and Response will help you gain visibility and asset identification in your Industrial Control System (ICS)/Operational Technology (OT) networks, monitor for and detect cyber threats, deconstruct ICS cyber attacks to extract lessons learned, perform incident response, and take an intelligence-driven approach to executing a world-leading ICS cybersecurity program to ensure safe and reliable operations.

The course will empower students to understand their networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This approach is important to being able to counter sophisticated threats such as those seen with malware including STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, and ransomware. In addition, the efforts are also critical to understanding and running a modern day complex automation environment and achieving root cause analysis for non cyber-related events that manifest over the network. Students can expect to come out of this course with core skills necessary for any ICS cybersecurity program.

The course uses a hands-on approach with numerous technical data sets from ICS ranges and equipment with emulated attacks and real world malware deployed in the ranges for a highly simulated experience detecting and responding to threats. Students will also interact with and keep a programmable logic controller (PLC), physical kit emulating electric system operations at the generation, transmission, and distribution level, and virtual machine set up as a human machine interface (HMI) and engineering workstation (EWS).

Students will spend roughly half the course performing hands on skills across more than 25 technical exercises and an all day technical capstone. Students will gain a practical and technical understanding of defining an ICS cybersecurity strategy, leveraging threat intelligence, performing network security monitoring, and performing incident response. Frameworks such as the ICS Cyber Kill Chain, Collection Management Framework, and Active Cyber Defense Cycle will be taught to give students repeatable frameworks and models to leverage post class.

The strategic and technical skills presented in this course serve as a basis for ICS organizations looking to show that ICS defense is do-able.

Author Statement

"This class was developed from my experiences in the U.S. intelligence community, at Dragos and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you'll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defense is do-able."

– Robert M. Lee

"This course was like a catalyst. It not only boosted my knowledge about the threats facing ICS environments and provided me with a framework to actively defend these threats, it also inspired me to learn more."

—Srinath Kannan, **Accenture**

Certification: GIAC Response and Industrial Defense (GRID)
giac.org/grid

ICS612: ICS Cybersecurity In-Depth

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Gain hands-on experience with typical assets found within an industrial environment, including Programmable Logic Controller (PLC), operator interfaces for local control, Human Machine Interface (HMI) servers, Historian server, switches, routers, and firewall(s).
- Gain an understanding of PLC execution through hands-on exercises.
- Identify security methods that can be applied to real-time control and Input/Output systems.
- Understand the pros and cons of various PLC and HMI architectures with recommendations for improving security postures of these real-time control systems.
- Identify where critical assets exist within an industrial environment.
- Understand the role and design of an Industrial Demilitarized Zone (IDMZ).
- Gain hands-on experience with firewalls placed within the industrial zone to achieve cell-to-cell isolation and perimeter restrictions.
- Dissect multiple industrial protocols to understand normal and abnormal traffic used in the operational control of assets.
- Gain an understanding of the role of IT network services within ICS and identify security methods that can be applied.
- Use the RELICS virtual machine for asset and traffic identification.
- Troubleshoot configuration errors within an operational environment.
- Understand adversary approaches in targeting and manipulating industrial control systems.

ICS-AWARE MALWARE AND ATTACKS ON CRITICAL INFRASTRUCTURE ARE INCREASING IN FREQUENCY AND SOPHISTICATION. YOU NEED TO IDENTIFY THREATS AND VULNERABILITIES AND METHODS TO SECURE YOUR ICS ENVIRONMENT. LET US SHOW YOU HOW!

The ICS612: ICS Cybersecurity In-Depth course will help you:

- Learn active and passive methods to safely gather information about an ICS environment
- Identify vulnerabilities in ICS environments
- Determine how attackers can maliciously interrupt and control processes and how to build defenses
- Implement proactive measures to prevent, detect, slow down, or stop attacks
- Understand ICS operations and what "normal" looks like
- Build choke points into an architecture and determine how they can be used to detect and respond to security incidents
- Manage complex ICS environments and develop the capability to detect and respond to ICS security events

The course concepts and learning objectives are primarily driven by the hands-on focused labs. The in-classroom lab setup was developed to simulate a real-world environment where a controller is monitoring/controlling devices deployed in the field along with a field-mounted touchscreen Human Machine Interface (HMI) available for local personnel to make needed process changes. Utilizing operator workstations in a remotely located control center, system operators use a SCADA system to monitor and control the field equipment. Representative of a real ICS environment, the classroom setup includes a connection to the enterprise, allowing for data transfer (i.e., Historian), remote access, and other typical corporate functions.

The labs move students through a variety of exercises that demonstrate how an attacker can attack a poorly architected ICS (which, sadly, is not uncommon) and how defenders can secure and manage the environment.

"I loved that this course was lab heavy. I feel 100% more comfortable around OT equipment now. That's saying a lot since my background and experience has been strictly IT."

—Jim J., **Pilot Flying J**

"The pods and student kits offered provide a powerful, hands-on learning experience that exceeded expectations far beyond what any software simulation or slide-based lecture could do. Step-by-step instructions are good, but I really enjoyed when we had exercises that didn't have all the answers and forced the student to think critically about how to solve the problem. That's where real learning occurred for me."

—Joseph P., **Deloitte & Touche LLP**

SANS CURRICULUM FOCUS AREA

Purple Team

Bring your teams together to test, measure, and improve your organization's people, processes, and technologies. Security professionals are most effective when they understand that offense informs defense and defense informs offense.

Featured Purple Team Training and Certifications

SEC598 Security Automation for Offense, Defense, and Cloud

SEC598 uses real-world examples of how to automate tasks within complex environments to prepare you for applying automation to resolve cybersecurity challenges in prevention, detection, and response when facing security incidents.

sans.org/SEC598

SEC599 Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses

GDAT GIAC Defending Advanced Threats

Get equipped with the knowledge and expertise you need to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries through a Purple Team strategy.

sans.org/SEC599

SEC699 Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection

This course is SANS' advanced Purple Team offering, with a key focus on adversary emulation for data breach prevention and detection. Throughout this course, students will learn how real-life threat actors can be emulated in a realistic enterprise environment, including multiple AD forests. In true purple fashion, the goal of the course is to educate students on how adversarial techniques can be emulated (manual and automated) and detected (use cases/rules and anomaly-based detection). A natural follow-up to SEC599, this is an advanced SANS course offering, with 60 percent of class time spent on labs!

sans.org/SEC699

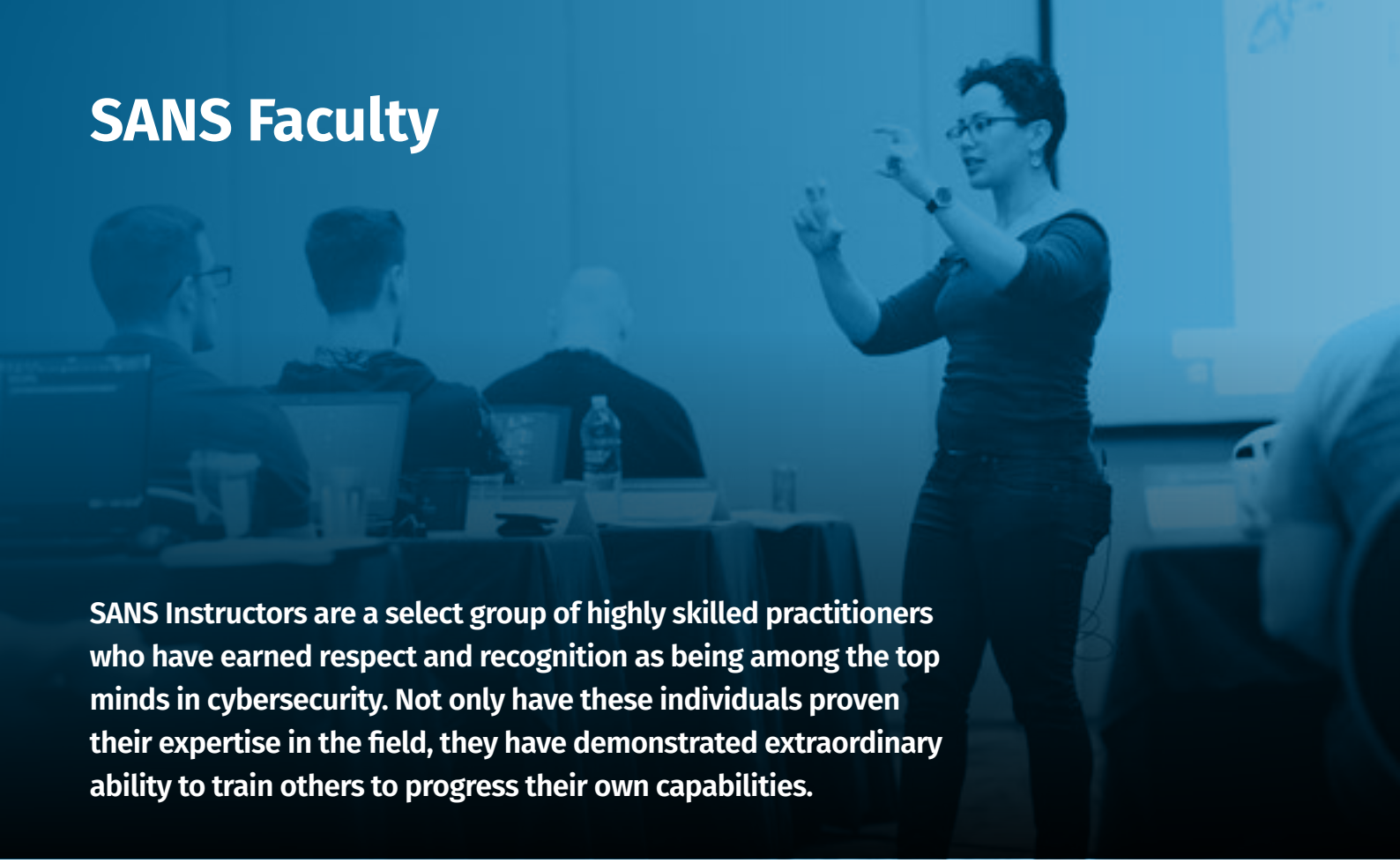
Enhance your training with:

- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a Purple Team Operations grad certificate program **sans.edu**
- The threat landscape is ever-evolving with new vulnerabilities emerging daily. SANS' commitment to helping you stay ahead of risks is not limited to courses. Engage with the cybersecurity community and discover emerging trends and cutting-edge concepts via our webcasts, blogs, tools, and research at **sans.org/purple-team**

Review full course descriptions and demos at **sans.org/courses**

Learn about newest courses in development at **sans.org/new-sans-courses**

SANS Faculty



SANS Instructors are a select group of highly skilled practitioners who have earned respect and recognition as being among the top minds in cybersecurity. Not only have these individuals proven their expertise in the field, they have demonstrated extraordinary ability to train others to progress their own capabilities.

SANS Faculty at a Glance

150+ Instructors

Each of our 120+ certified instructors is a highly skilled professional currently working in cybersecurity.

16+ Years

SANS faculty spend an average of more than 16 years as cybersecurity practitioners before being selected to become SANS Certified Instructors.

40+ Books

SANS faculty members have authored more than 40 books on information security.

150+ Tools

More than 150 open-source cybersecurity tools have been created by SANS Instructors. List of tools available at **sans.org/free**.

3,500+ Resources

SANS faculty members have produced more than 3,500 research papers and webcasts on information security topics.

Commitment

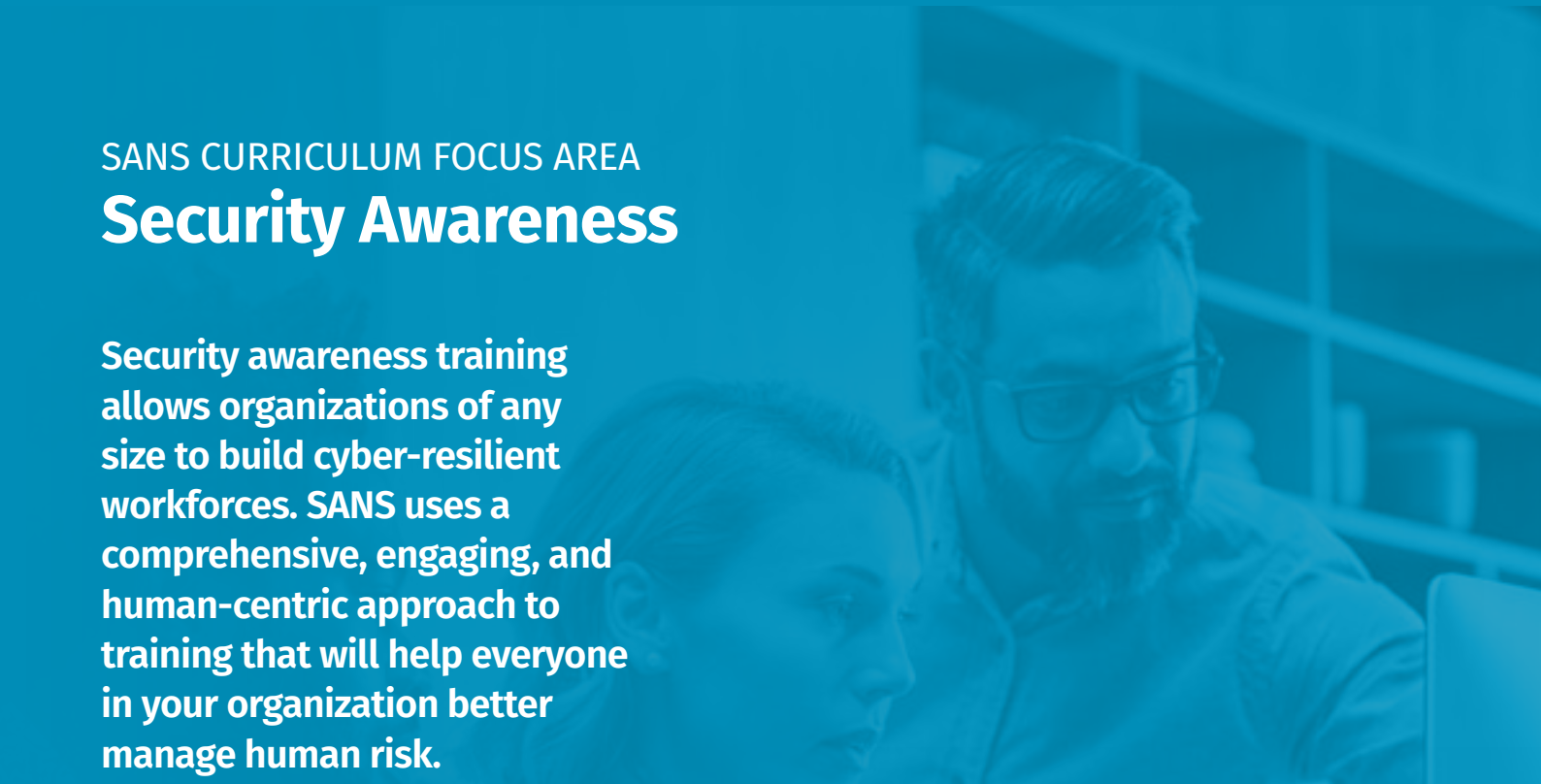
SANS instructors are committed to providing engaging and active learning environments focused on key skills, taught through lecture, immersive hands-on labs and interactive discussions. “Passionate” is a word many use to describe a Certified SANS instructor.

Their goal is your success, and we promise that you will be able to apply what you learn as soon as you return to work.

Meet the SANS faculty:
sans.org/instructors

SANS CURRICULUM FOCUS AREA

Security Awareness



Security awareness training allows organizations of any size to build cyber-resilient workforces. SANS uses a comprehensive, engaging, and human-centric approach to training that will help everyone in your organization better manage human risk.

Backed by proven learning principles, SANS Security Awareness programs combine content from hundreds of the world's best cybersecurity practitioners, security awareness officers, and learning-behavior specialists to reflect real-world cyber attacks. These dynamic programs engage and educate participants, empowering them to contribute to cultural change and prevent attacks.

SANS Security Awareness supports your entire organization in the following ways:

- **Support Every Employee with EndUser Training and Phishing Simulation**
  Culturally relevant, effective, and easy to implement, EndUser Training provides the training required to move beyond compliance and build a truly mature awareness program. Supplement this with a phishing platform designed by experts and deployed using a unique tiered-template methodology to advance learners at any level.
- **Support Your Leadership with Services that Shine**
  With SANS, your security leaders have access to the resources required to ensure success. From the world's largest security awareness online community to the industry-leading SANS Security Awareness Maturity Model™ and a Client Success team backed by industry experts, SANS focuses on driving your program maturity.
- **Support Focused Responsibilities with Specialized Training**
  Not all learners are created equal and many job functions require additional instruction. SANS delivers role-based and progressive training paths targeted for IT practitioners and organizations with industrial control or power utility functions.

"The 'Who' and 'What' of training and awareness is just what I needed to take back home."

—David N., **U.S. Federal Department**

MGT433 Managing Human Risk: Mature Security Awareness Programs

SANS Security Awareness Professional (SSAP)

Learn the key lessons and the roadmap to build a mature awareness program that your workforce will love and that has an impact you can measure. Apply models such as the BJ Fogg Behavior Model, AIDA Marketing funnel, and Golden Circle, and learn about the Elephant vs. the Rider.

sans.org/MGT433

MGT521: Leading Cybersecurity Change: Building a Security-Based Culture

Learn how to build, manage, and measure a strong security culture by leveraging the latest in organizational change and real-world lessons learned. Apply findings from Daniel Kahneman's Nobel prize-winning research, Nudge Theory, and the Golden Circle. Learn how Spock, Homer Simpson, and Newton's First Law all are keys to building a strong cybersecurity culture.

sans.org/MGT521

Featured EndUser Training Modules

Security Essentials—Social Engineering; Malware; Email & Phishing; Passwords; Targeted Attacks; Social Networks; Mobile Devices

Role-specific Training—Insider Threat; Help Desk; Privileged Access; International Travel; Sr. Leadership; 3rd-party Risk Management

Distributed Workforce—Working Remotely; Cyber Secure Homes; Protecting Kids Online; Virtual Conferencing

Digital Transformation—Cloud Services; Cloud Computing; IaaS and PaaS; Office 365 and Google Workspace

Compliance—GDPR; PCI DSS; PII; FERPA; FCPA; GLBA; HIPAA; ITAR; CCPA; CUI

SANS Security Awareness EndUser Modules cover over 60 topics and support 34 languages

Featured Specialized Training Modules

IT Administrator Training—12 modules covering Security Program Management; Attack Mitigation Technologies; Securing Web Servers; Supply Chain Attacks; and more!

Developer Training—OWASP Top-10; Mobile App Security; SDLC; Secure Coding Principles; Top Design Flaws; Threat Awareness; Classic Issues

Industrial Control System (ICS) Training—ICS Attack Surfaces; Server Security; Network Security; Information Assurance; Incidence Handling

NERC CIP training—NERC CIP Policy Requirements; Asset Identification; BES Cyber System Recovery; CIP-014 Overview; Incident Response

Live Training

Train In-Person or Live Online with industry experts at dynamic, live training events

sans.org/find-training

Benefits of In-Person Training

In-Person training offers great destinations to choose from or a venue close to home.

- Engage with our unparalleled faculty, comprised of the industry's top cybersecurity practitioners
- Enjoy networking opportunities to meet, share, and learn from your peers
- Practice hands-on information security challenges in classroom labs
- Use courseware delivered both electronically and in print, including MP3 course archives that are downloadable to review following the event
- Meet with emerging solution providers as they reveal the latest tools and technologies critical for you to master information security

"The combination of highly relevant material, hands-on exercises and instructors who supplemented the material with real-world stories and examples made the course material come alive in a way no other delivery method could."

—Ted Nichols, **Blue Cross Blue Shield of South Carolina**

Benefits of Live Online Training

Live Online training offers access without travel to the same world-class SANS faculty via live streaming, and delivers the same learning results as SANS In-Person training.

- Interactive Q&A with instructors and peers
- Real-time support from virtual Technical Assistants
- Hands-on labs in a virtual environment
- Courseware delivered both electronically and in print
- Extended access to class recordings, to review topics on your own time
- Dedicated chat channels using Slack for networking
- Practice your skills with SANS virtual cyber ranges

"The Live Online delivery platform ensures students are able to access content, virtual machines, labs, resources, and chat 24 hours a day...Additionally, after the course ends, access is still available! Priceless!!"

—Britni T., **U.S. federal agency**

GIAC CERTIFICATIONS

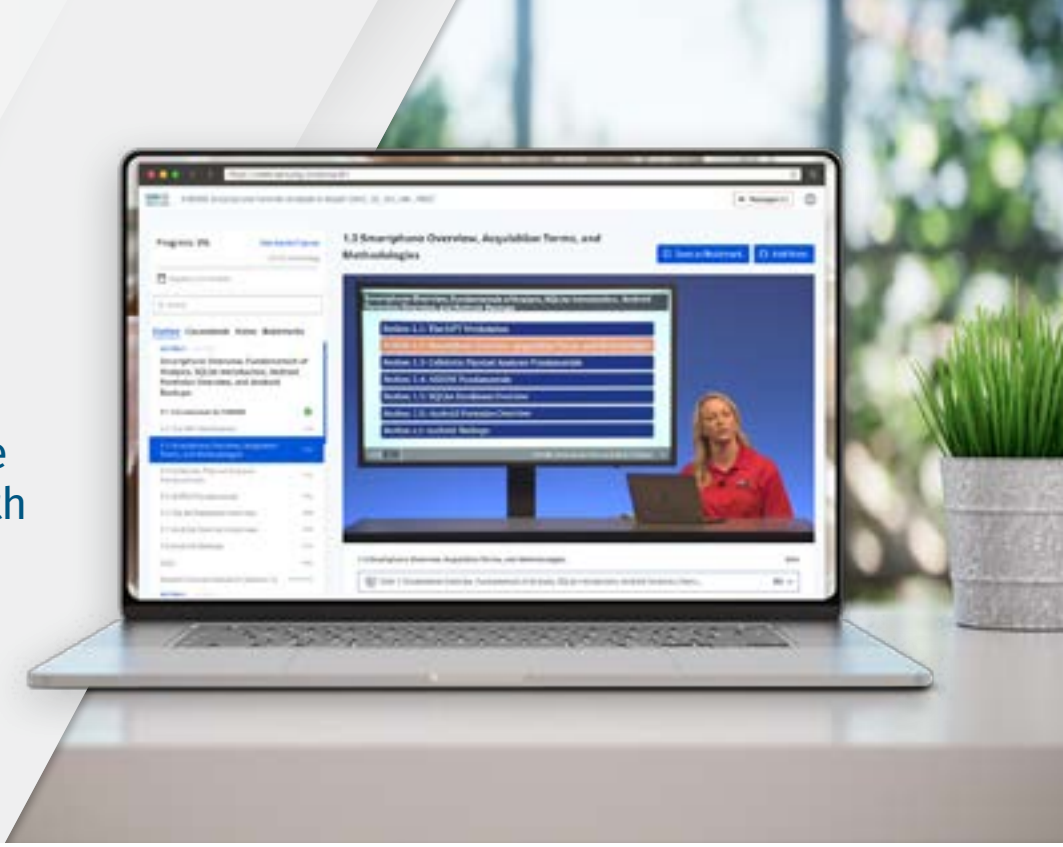
Certify the Skills and Knowledge You Learn in SANS Training

www.giac.org

SANS OnDemand

Train at your own pace anytime, anywhere with SANS OnDemand

sans.org/ondemand



SANS OnDemand offers our world-class cybersecurity training in a self-paced online training format, with four months of extended access to your course and labs. Enjoy the ultimate learning flexibility with OnDemand – rewind and revisit your training content so you can reinforce the material and improve retention.

With complete control over the pace of learning, SANS OnDemand fits every learning style.

- **Students can control the pace, learning environment, and schedule**
- **Instructor lectures, class exercises, and virtual labs are available for four months**
- **Repeatable hands-on labs and quizzes help you prepare for 40+ different GIAC exams**
- **No travel budget, no problem. Learn from anywhere. Home, office or on the road**
- **On your own, but not alone. SANS subject-matter experts are available to answer your questions**

> "I don't think I would get nearly as much out of this course if I did not get the class material delivered via the OnDemand platform. It's an excellent way to replay content and critical topics."
>
> —Kenneth Huss, **Cisco**

Limited-Time SANS Online Training Specials
Options include tablets, laptops, or discounts. For more information visit:
sans.org/ondemand

New SANS OnDemand Training App

Allows You to Take Cybersecurity Training **Anywhere, Anytime.**

SANS Summits

**YOUR Community –
Working TOGETHER to Solve
Cybersecurity Challenges TODAY**

BREAKING CONTENT

NEVER BEFORE SEEN RESEARCH

SOLUTIONS YOU CAN USE

Online Free for the Global Community

OR

In-Person with Exclusive Benefits

SANS Summits bring the community together to harness industry minds, leaders, novices, and associate groups to discuss the most challenging cybersecurity problems today.

When new challenges come up (and they always do), where do practitioners go to help discuss what to do, how to approach, and what works? How will they solve problems that do not have solutions yet?

SANS Summits are designed to help those in need and tackle new ideas, test, debate, and challenge existing practices and improve upon them. SANS Summits also support those just starting to find their footing by giving them a place to help explore, learn, and connect with the larger community of professionals.

These Summits are more than a group to help solve problems. This is the community focused on each niche area of cybersecurity from DFIR, Offensive Operations, Blue Team Operations, Cyber Threat Intelligence, New to Cyber, and more. Every group of cybersecurity practitioners, leaders, and those just starting will find their home at a SANS summit. We are there to tackle the unknown – tackle new challenges – learn together – and we might have fun doing it.

"The free, Live Online Summits this year were a welcome way to get high-quality knowledge, inspiration, and networking while working remotely. It enabled me to share training opportunities and experiences with teammates that I would not have been able to share otherwise."

—Jen Fox, Information Security Program Specialist

Top 5 Reasons to Attend

#1 In-depth technical talks on "First Release" or ZERO DAY skills and techniques

#2 Interactive panel discussions from industry experts

#3 Networking with leading experts, and your peers tackling the same hard-to-solve problems

#4 Access to Summit recordings and presentations

#5 As an attendee, you'll walk away from your Summit experience with a fresh perspective, a better connection with the community and new tools that you can immediately leverage in your work.

Visit **sans.org/summits** for the latest 2023 schedule

Develop Skills with Hands-on Labs and Ranges

Our labs provide hands-on experience that reinforces course concepts and learning objectives. Students learn the HOW along with the WHAT/WHY through a combination of lab instructions with a step-by-step electronic workbook directly tied to the material to develop skills in a hands-on environment.

Our hands-on labs are interactive and auto-updating, sometimes in multiple environments (AWS, Azure, etc.). Not point-and-click, but actual interactive labs that update in real time.

Relevant Tools

Students must use proper cybersecurity and analysis tools to complete a lab. In many cases, multiple devices and multiple steps are needed. Each student is armed with a virtual machine (VM) or tools that do not require complex installation. Many VM environments are set up so that you can use the same tools when back in your environments on similar complex scenarios you might encounter daily.

The **SIFT Workstation** is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite.

Eric Zimmerman's Tools
These open source digital forensics tools can be used in a wide variety of investigations including cross validation of tools, providing insight into technical details not exposed by other tools, and more.

Slingshot is an Ubuntu-based Linux distribution with the MATE Desktop Environment built for use in the SANS Offensive Operations curriculum and beyond. Designed to be stable, reliable and lean, Slingshot is built with Vagrant and Ansible.

REMnux® is a Linux toolkit for reverse-engineering and analyzing malicious software. REMnux provides a curated collection of free tools created by the community. Analysts can use it to investigate malware without having to find, install, and configure the tools.

"The course material is backed up with very well-crafted labs that give you an opportunity to actually use and interact with the tools and techniques covered in the course."

—Michael R., **Palo Alto Networks**

SANS instructors offer more than 100 free popular workstations and tools enhancing and enabling practitioners across the cybersecurity community

Real-World Scenarios

Authors design labs based on current and real-world challenges they encounter daily in their jobs, investing months creating complex, believable, and realistic scenarios using existing threat actors. SANS interactive ranges and threat-based attack data are built from the ground up, mimicking organizations and entities that come under attack weekly. These environments are so believable that SANS instructors are often asked how we received permission to use “real” attack data to teach students in class.

Self-Correcting Instructions

The labs include self-correcting instructions with a step-by-step online workbook to walk students through complex labs. If you get stuck, an intricate hint and learning system with embedded videos is built to explain each step thoroughly. If needed, the student can unhide the exact command to input or utilize the tool to complete the step.

Skills Assessment and Practical Application

SANS Cyber Ranges focus on practical application and skills assessment, offering insight into what you and your team are excelling at and what skills warrant additional training and practice. Range participants problem-solve and develop skills through interactive, story-driven exercises that bring real-world context to the challenges at hand. SANS Cyber Ranges cover a broad spectrum of disciplines and the full range of difficulty levels, from beginner to expert.

SANS
CYBER RANGES

SANS PREPARES YOU FOR

Threats From Every Angle

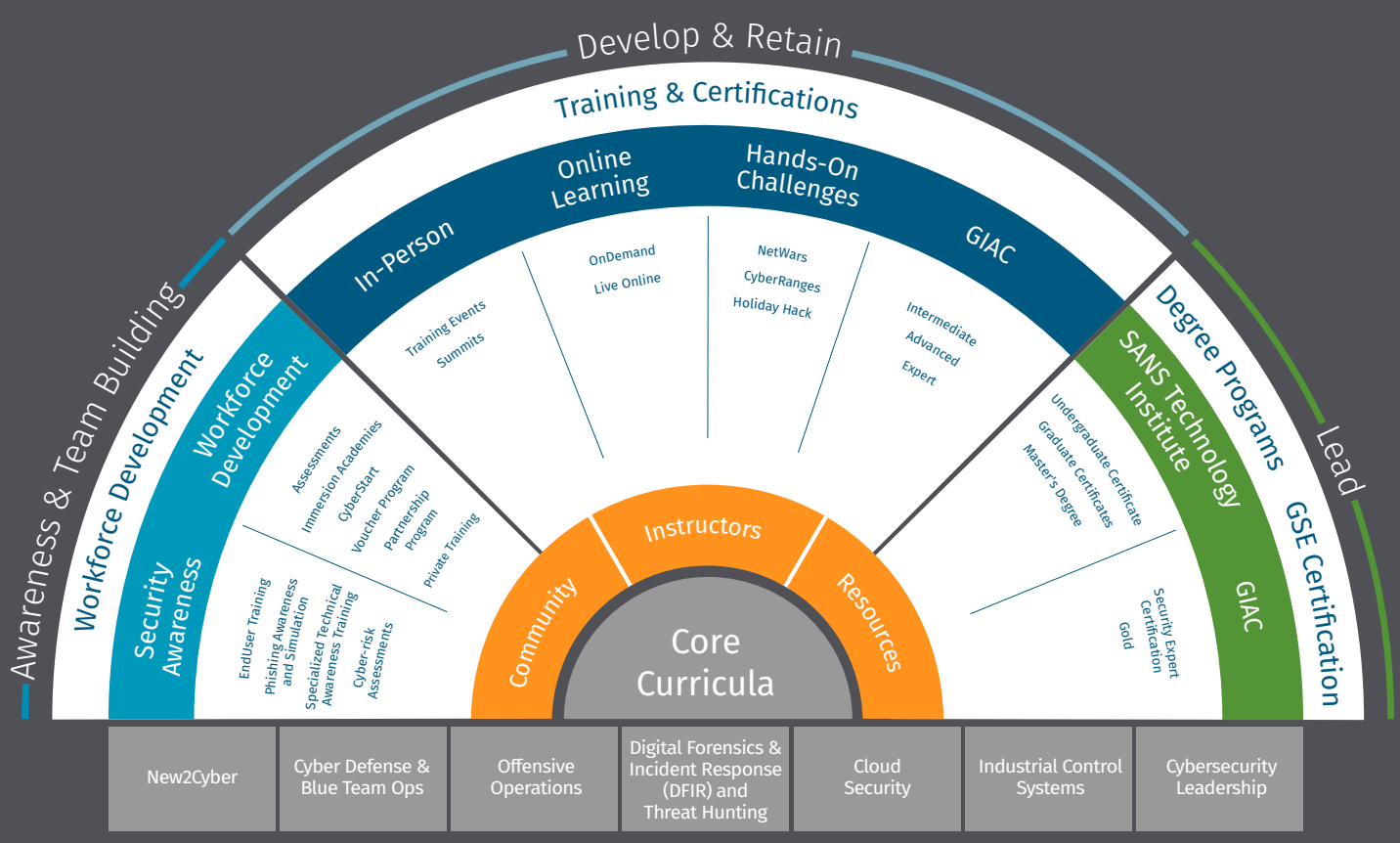
Get Started in Cybersecurity

Cybersecurity is an exciting career choice within everyone's reach. Utilize SANS resources to get started on your journey:

- Our New2Cyber curriculum helps non-technical professionals enter cybersecurity by building foundational knowledge and skills for entry-level roles. **sans.org/cybersecurity-careers**
- Earn an accredited degree or certificate to launch your cybersecurity career. **sans.edu**

Scholarship Academies: Scholarship programs empower underrepresented groups and bring more talent into critical roles. **sans.org/scholarship-academies**

Bachelor's Degrees in Applied Cybersecurity (BACS): Bring in 70 credits from any accredited community college or four-year college and earn a bachelor's degree after completing 50 credits at **SANS.edu**.
sans.edu/bacs-degree



Build an Outcome-Driven Cybersecurity Workforce

Recruit

Recruit the right cyber talent with SANS CyberTalent: Talent assessments and Immersion Academies for women, veterans, and minorities
sans.org/hire-cyber-talent

Develop

Training Roadmap: Create a plan to develop the skills for you or your team's cybersecurity skill development
sans.org/cyber-security-skills-roadmap

Create a cyber-resilient workforce with SANS Security Awareness: Comprehensive security awareness training tools to better manage human risk
sans.org/awareness

Summits: SANS hosts highly focused, expert-led conferences throughout the year that feature presentations and discussions on leading issues
sans.org/summit

GIAC Certifications: 40+ cybersecurity certifications are available in cyber defense, offensive operations, digital forensics, ICS/SCADA, and more
giac.org

Cyber Ranges: A suite of live and online hands-on interactive scenario challenges to help you master a wide range of skills
sans.org/cyber-ranges

Retain

SANS Technology Institute: Advanced degrees designed to build a strong cybersecurity workforce
sans.edu

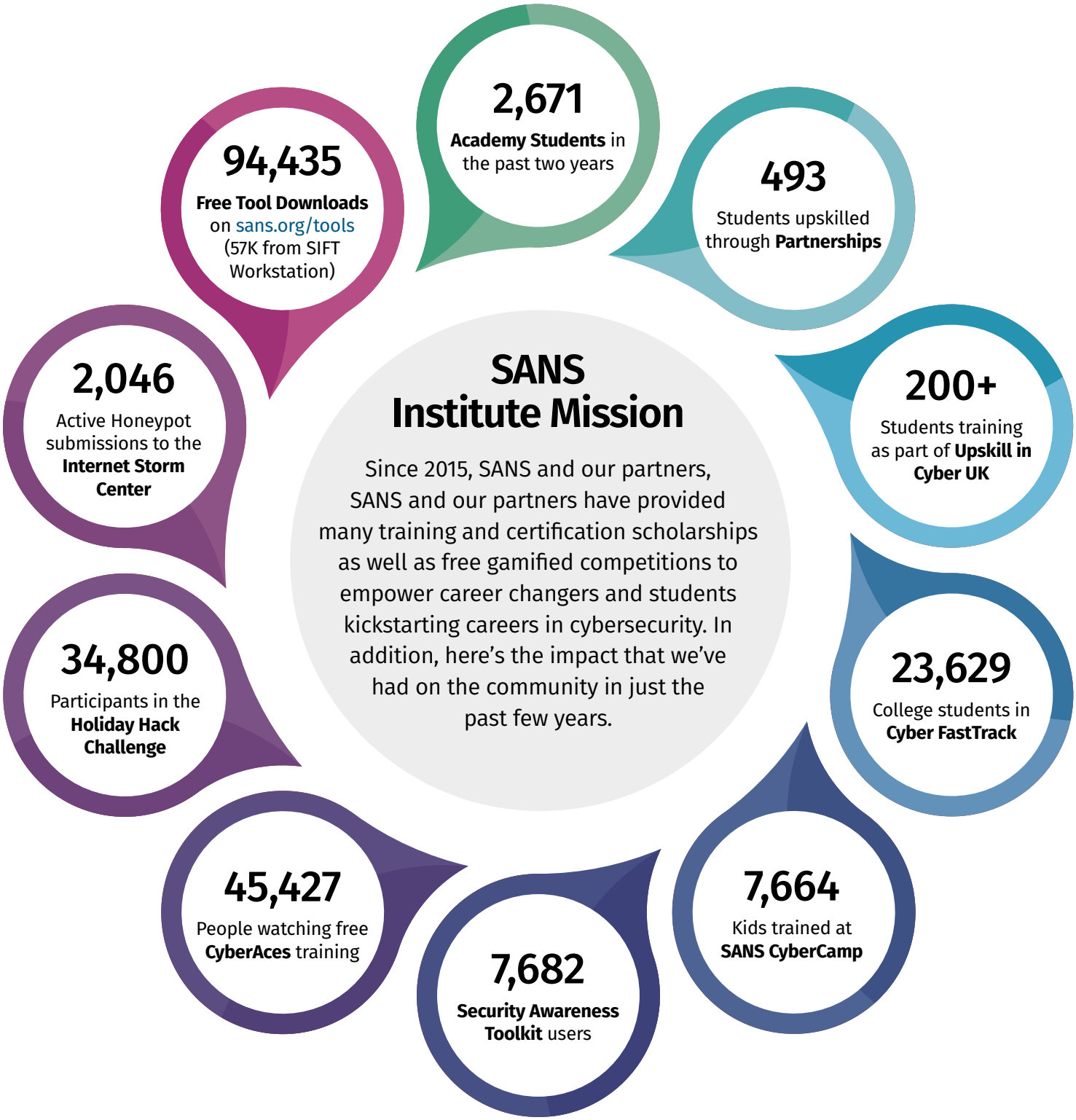
GSE: GIAC Security Expert: The cybersecurity industry's most prestigious certification validates that an individual has truly mastered the skills required to excel in this field
giac.org/get-certified/giac-security-expert

Leadership Development: Develop the next generation of world-class cybersecurity leaders
sans.org/cybersecurity-leadership

"The SANS Institute is renowned and respected for its world-class cyber training. CACI is pleased to team with SANS on this critical workforce development initiative, which will help fill a pressing need for cybersecurity experts in industry and government."

—Mike Mourelatos, CACI Vice President and Chief Technology Officer - **National Services**

SANS INSTITUTE
Mission & Initiatives



*Number reflect Jan 2020 forward

sans.org/mission

MISSION | INTEGRITY | COLLABORATION

Internet Storm Center

Global incident alert network with more than 15,000 global target IPs and 250–300 active submitters watching for new data.

HBCU Programs

Summits, cyber range challenges, and other events and training are now being offered in support of HBCU cyber programs.

Cyber Academies

SANS' women's, veterans, and diversity academies help more underrepresented groups to launch new cyber careers every year.

Veteran Cyber Academy Australia

SANS, in partnership with Allectum, has created an intensive and immersive 16 week training program, the Academy aims to encourage and develop potential new cybersecurity professionals.

Cyber Reskilling Program Bahrain

SANS, in partnership with Tamkeen, are set to launch the Cyber Reskilling Program Bahrain, which aims to identify and rapidly re-skill individuals for roles in cybersecurity in just eight weeks.

Upskill in Cyber UK

SANS, in partnership with HM Government, launched Upskill in Cyber. The programme aims to identify and rapidly reskill individuals for roles in cyber security, in just ten weeks.

Cyber FastTrack

Identifying up-and-coming cyber talent through collegiate competition.

"SANS Academy allowed me to gain knowledge in a new career area I couldn't have afforded myself. Also, its (SANS Cyber Academy) receptions with employers landed me my first job in cybersecurity."

—Amy R., **Mid Cybersecurity Engineer**

Partnerships and Solutions

Working with businesses and governments, to create bespoke training and development solutions that directly support specific operational requirements.

SANS frequently works with organisations to create bespoke skills development solutions. We consult, advise, and then build tailored packages for corporate and government partners looking to enhance their cyber security capability. We also provide tools that allow organisations to measure and model the effectiveness of these unique solutions.

SANS has the experience and knowledge to deliver solutions across employee assessment, recruitment selection, team development, and intense technical training.

"We work with governments and enterprises across different countries, cultures, and continents," explains Jan Pieter Spaans, Managing Director Mainland Europe. "Our services include direct solutions, like providing SANS training courses privately."

All of SANS' cyber security training courses can be delivered privately, in an organisation's training facility or HQ. SANS Private Training is delivered by a qualified SANS Instructor with the utmost of discretion. SANS can, of course, provide security cleared Instructors as required.

"Our services go beyond training, though. We also assist security managers in ensuring their team's skills are kept up to date," says Jan Pieter Spaans. "We can build and deploy programmes that increase staff retention through skills development or assess an organisation's needs and then deliver bespoke solutions that deliver across recruitment, on boarding and training."

Begin a discussion with SANS

For an initial discussion with a SANS Institute Director, contact SANS via emea@sans.org or +44 203 384 3470. Alternatively contact:

Stephen M Jones
Managing Director UK & Nordics
sjones@sans.org

Ned Baltagi
Managing Director ME & GCC Regions
nbaltagi@sans.org

Jan-Pieter Spaans
Managing Director Mainland Europe
jspaans@sans.org

Suresh Mustapha
Regional Managing Director SANS Asia Pacific & Latin-America
smustapha@sans.org

HMG Cyber Schools Programme

SANS was selected to devise and run the first extracurricular cyber security learning programme for schools in the UK. Cyber Discovery is a multi phase programme that uses an assessment tool and gamified learning platform developed by SANS as well as online and face to face initiatives to enhance the cyber security skills and knowledge of young people.

Stephen Jones, SANS Managing Director for UK and Nordics says, "We are proud to be delivering this vital training programme in support of the UK's National Cyber Security Strategy and look forward to seeing a great increase in the number of young people taking an interest in cyber security as a future career choice. By assessing, selecting and training students with a natural flair for cyber we intend to help close the skills gap that remains a challenge to all nations."

HMG's Cyber Schools Programme launched in in Autumn 2017 and falls within the UK government's CyberFirst initiative.

SANS has experience of delivering similar training programmes for school students in other nations.

Upskill in cyber Programme

Cyber security is rapidly becoming a top global priority for governments and businesses. Even though the UK has a world-class cyber security sector, there is still currently a significant shortage of skilled cyber security professionals.

SANS, in partnership with HM Government, launched Upskill in Cyber. The HM Government funded programme aims to identify and rapidly re-skill individuals for roles in cyber security, in just ten weeks. 200 students undertake two SANS training courses. In addition, they receive soft skills development, to ensure they are immediately deployable within the cyber security workforce. Successful graduates will complete the programme with two GIAC certifications - GFACT and GSEC.

Bespoke Training Solutions

Private training is ideal for organisations that need an entire team to take a particular SANS course. However, often an organisation needs to implement a bespoke training programme that incorporates several SANS training courses.

SANS works closely with organisations, taking time to understand their specific training needs. After a consultation process, a unique training and development solution is created that meets these needs – based on courses from across the SANS Cyber Security Training Curriculum and additional SANS products.

Uniquely, we are able to provide training recommendations, and then deliver that programme ourselves.

Assessment and Candidate Selection

SANS works regularly with organisations, helping them to streamline their recruitment processes and procedures.

"The traditional mode of candidate selection generally relies on sifting CVs," explains Ned Baltagi, Director, SANS ME & GCC Regions. "Organisations tell us regularly that this is time consuming and doesn't provide the reliable - and predictable - results they need when selecting front-line cyber security staff."

SANS CyberTalent is one such selection product. It is a suite of assessment tools that improves the effectiveness of a cyber security recruitment and selection process.

SANS CyberTalent products use psychometric and skills testing to assess candidates' aptitude and suitability for particular roles. The online assessments leverage SANS' experience in the field of cyber security training and GIAC certification to gauge technical skills and knowledge.

CyberTalent provides managers and HR teams with a deeper understanding of candidates' technical and conceptual makeup.

Assessing Team Strengths and Weaknesses

SANS CyberTalent and other bespoke solutions extend beyond candidate selection. SANS works closely with many organisations, helping them to ensure their security team keeps developing and evolving.

"Security teams must change and adapt – new attack vectors emerge, technologies evolve and businesses themselves change," states Jan Pieter Spaans. "Training is an integral part of this development process... but training needs vary across a team. Training just isn't a one size-fits-all business."

To support managers in developing and improving their team, SANS provides assessment products such as SANS NetWars, SANS Private Ranges and SANS CyberTalent. These allow Security and HR managers to achieve a clear understanding of their team's strengths, weaknesses and training needs.

SANS then builds a unique training programme that focusses on addressing a team or individual's specific requirements.

Career development also aids staff retention and ensures a security team remains effective. SANS helps employers create bespoke training programmes using the extensive SANS training curriculum.

Following a consultation process, SANS delivers programmes that meet business needs and also offer security professionals a career roadmap.

Training Programmes

SANS is experienced in building residential training programmes for many different types of organisation – governments, enterprises, and military bodies - spanning different geographic regions and business cultures.

These programmes vary in scale and focus, and are designed to precisely meet a client's requirements. SANS Cyber Academy is a cyber security training programme that demonstrates this capability.

"SANS first identifies candidates with the potential to succeed in cyber security using CyberTalent Aptitude Assessments."

"Successful applicants are undertaking two SANS training courses. The training prepares them for security roles by introducing them to fundamental cyber security principles. Our students are taught using material from SANS' training courses, through real-life, practical simulations and team exercises."

TAILORED GROUP TRAINING OPTIONS

SANS Institute's Private Information Security Training options allow you to create a custom training program for any group of 25 students or more, anywhere in the world.

With options for commercial groups and government organizations, private information security training will be specifically designed to meet your needs using SANS' top technology and instruction. We'll provide you with SANS' world-class courses and Certified Instructors live onsite, online or a combination of both via our Live Online training format.

SANS Private Training Benefits include:

- A Certified SANS Instructor
- Confidential, live in-class discussion regarding the courseware and viable real world examples for your industry
- Limit the health risk and avoid the complications associated with current travel restrictions
- Sensitive Topics. Organisations turn to the Private Training program so they can have classes where students can discuss topics freely and the instructor can focus on material that may pertain to a sensitive matter or recent breach
- Courses are offered globally and delivered onsite at your preferred location.

"The SANS OnSite program has been advantageous for our security training program. The 'cost savings' have been astronomical... The instructors have been great and the students enjoy being in class with colleagues that share concerns and duties for ongoing security projects."

- Tonya Henderson, Health & Human Services

Group Purchasing

Manage your team's training budget, track student's progress and save money and track from a single Voucher Account.

The SANS Voucher Program allows an organization to manage their training budget from a single SANS Voucher Account. Once the Account is opened, the organization can utilize funds from their Account for SANS training and certifications for their employees via their online SANS Admin Tool. Through the Admin Tool, the organization's Program Administrator can also approve training and view usage reports.

By creating a SANS Voucher Account your organization can:

- Simplify the procurement process with a single invoice and payment
- Lock-in your hard fought training budget and utilize within a 12 month term
- Control how, where, and for whom funds are spent
- Allow employees to register for training while managing approvals centrally
- Easily change course attendees if previous plans change

If you are interested in learning more about developing and training your team, please reach out to us at **emea@sans.org** or **asiapacific@sans.org**

Experience the SANS training In Person experience.

"I have always loved this stuff. Stepping into the deep end with world class instructors is a dream come true. There is no time to reinvent the wheel, so this experience is priceless"

- Keith Dunnigan,
Best Western Hotels & Resorts

Find the best course and training event for you:
sans.org/upcomingevents

Customer Reviews

SANS is the most-trusted source for cybersecurity training, certifications, degrees, and research. But don't just take our word for it – here's what our students have to say.

"SANS is the best information security training you'll find anywhere. World-class instructors, hands-on instruction, actionable information you can really use, and NetWars."

—Jeff S., **NetJets, Inc.**

"The course material is backed up with very well-crafted labs that give you an opportunity to actually use and interact with the tools and techniques covered in the course."

—Michael R., **Palo Alto Networks**

"SANS courses are fully aligned to what is happening in the industry. Course materials are continuously updated based on new developments in cybersecurity. It is rigorous, challenging, and relevant."

—Karim Lalji, Managing Security Consultant, **TELUS**

"Something that I think is perhaps underrated about SANS courses is, as everyone knows, you come along and drink from an information fire hose on attacks and tools, but along the way you gain a level of comfort and intuition around broad sets of technologies, which is really handy when navigating the world of InfoSec."

—James S.

"Excellent. All of this was well presented, handled, and delivered. The platform that was utilized was perfect. For a distance learning option, it was very interactive and well worth the time."

—Terrie M., **AT&T**

"The labs from all SANS courses are always top notch. I have taken SANS training since 2007 and it has always maintained the highest level/standards, without question the best training content on the planet."

—Nicolas Stevens

"As usual, SANS has produced a great course and learning experience. I loved SEC540 content, and the labs brought together everything we learned. Once again, I'll be back again next year."

—Daniel Bachrach, **Deloitte**

"Our instructor was great. When we were stuck, he really helped us understand and kept us all engaged. He answered every question immediately and completely and finished all the dangling threads."

—Stephen K., **NAVSUP**

"Nobody else in the industry is as comprehensive as SANS or as up-to-date and knowledgeable. If you want to learn how to do your job right, I don't think there's any better training out there."

—Ronald C., **S-RM**

Free Cybersecurity Resources

Free Training and Events

Test Drive SANS Courses
Identify the right course for you by using our free one-hour course previews to explore subjects and verify materials that match your skill level
sans.org/course-preview

Summits
Immersive training experiences that arm attendees with deep knowledge and actionable information and have a lasting impact on their careers and their organizations' security programs
sans.org/summits

Summit Presentations
Top-of-mind presentations
sans.org/presentations

Solutions Forums & Event Tracks
Engage, connect, and learn from invited speakers who showcase their products and current capabilities using specific examples relevant to the industry
sans.org/sponsorship/events

SANS Cyber Aces Online
This free online course teaches the core concepts needed to assess and protect information security systems
cyberaces.org

SANS Workshops
Hands-on virtual training that give you the opportunity to dive into course material
sans.org/workshops

Cyber Ranges
Prepare for real-world IT and cybersecurity roles with interactive learning scenarios
sans.org/cyber-ranges

Podcasts

Blueprint
Advancing cyber defense skills
sans.org/podcasts/blueprint

Cloud Ace
Future of cloud security
isc.sans.edu/podcasts/cloud-ace

GIAC: Trust Me, I'm Certified
Industry leaders in cybersecurity
giac.org/podcasts/trust-me-im-certified

Internet Storm Center
Daily InfoSec threat updates
isc.sans.edu/podcast.html

Free Cybersecurity Resources

Internet Storm Center
A free analysis and warning service
isc.sans.edu

Free Tools
150+ open-source tools from SANS Instructors
sans.org/tools

Whitepapers
Top-of-mind papers
sans.org/white-papers

Posters & Cheat Sheets
sans.org/posters

Webcasts
Live web broadcasts combining knowledgeable speakers with presentation slides
sans.org/webcasts

Blogs
Top-of-mind topics for the SANS community
sans.org/blog

Security Policy Templates
Security policy templates from information security subject-matter experts and leaders for your use
sans.org/information-security-policy

CIS Controls v8
sans.org/blog/cis-controls-v8

Annual Security Awareness Report
Utilize data-driven actions to manage your human risk and push your program into the future of security awareness
go.sans.org/lp-wp-2022-sans-security-awareness-report

NICE Framework
Use the NICE Framework as a guide to advance your career with recognized cybersecurity certifications from GIAC
giac.org/workforce-development/government/niceframework

SANS Holiday Hack Challenge
The SANS Holiday Hack Challenge is a FREE annual game of new, fun, high-quality, and hands-on cybersecurity challenges where you learn new skills, help Santa defeat cybersecurity villains, and save the whole holiday season from treachery.
sans.org/mlp/holiday-hack-challenge

sans.org/free

SANS Cyber Academies

VetSuccess Academy
sans.org/scholarship-academies/vetsuccess

Women's Immersion Academy
sans.org/scholarship-academies/womens-academy

Cyber Workforce Academy
sans.org/scholarship-academies/cyber-workforce

Cyber Diversity Academy
sans.org/scholarship-academies/diversity-academy

HBCU Academy
sans.org/scholarship-academies/hbcu-cyber-academies/

Newsletters

NewsBites
A semiweekly executive summary of the most important cybersecurity news articles published recently
sans.org/newsletters/newsbites

@Risk
A weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, and other valuable data
sans.org/newsletters/at-risk

OUCH!
A free monthly security awareness newsletter designed for the common computer user, in over 20 languages
sans.org/newsletters/ouch

Social Media

Find us at **@SANSInstitute**, and connect with us to stay informed on the latest SANS resources

New2Cyber	**@new_2_cyber**
Blue Team	**@SANSDefense**
Offensive Ops	**@SANSOffensive**
DFIR	**@sansforensics**
Leadership	**@secleadership**
Cloud	**@SANSCloudSec**
ICS	**@SANSICS**
Security Awareness	**@SANSAwareness**

Join the SANS.org Community for Free

Membership in the SANS.org Community grants you access to cutting-edge resources that our expert instructors contribute to daily and that can't be found elsewhere including cybersecurity news, training, and free tools.

Go to sans.org/account/create to create your free account today and gain access to the above available resources and more!

SANS | GIAC CERTIFICATIONS

www.sans.org

For the most up-to-date Training Calendar visit **www.sans.org/events**

v0623