SANS | GIAC CERTIFICATIONS

SANS 2022 CURRICULUM AND TRAINING BROCHURE

Train to Reduce Cyber, Business, and Human Risk

EDUCATE, EMPOWER, AND EVOLVE YOUR WORKFORCE

70+ hands-on courses

120+ extraordinary SANS-certified instructors

40+ certifications

SANS Focus Areas

- New2Cyber
- Cyber Defense & Blue Team Ops
- Offensive Operations
- Digital Forensics & Incident Response (DFIR) and Threat Hunting
- Cybersecurity Leadership
- Cloud Security
- Industrial Control Systems (ICS)
- Purple Team

The SANS Promise

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

SANS INSTITUTE

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

Contents

About the SANS Institute

Launched in 1989 as a cooperative for information security thought leadership, SANS' ongoing mission is to empower cybersecurity professionals with the practical skills and knowledge they need to make our world a safer place.

SANS is dedicated to delivering and validating hands-on cybersecurity skills because we understand that everyone in an organization—from non-technical employees to IT security staff and all the way up to the security leadership team—has a role to play in establishing a critical line of defense in the battle against ever-evolving adversaries.

"SANS Security Awareness is one of the best security awareness programs I have seen in my 20+ years as a technologist."
—James Gentile CIO, Arizona Medical Board

"The two SANS CyberTalent academy graduates I hired are both quickly becoming my top performers and I am very happy with their level of commitment, security knowledge, and technical skills."
—Eldon Myers, TSYS

TRAIN & CERTIFY
INVEST IN YOUR FUTURE

Cyber security 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.

Whether you're an individual learner or managing a team, this is your golden moment, your shining opportunity, to grow your career in mission-critical, truly meaningful work that contributes to your organization's success in reducing risk:

- **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 cyber security problems using advanced tools**
- **Improve your ability to identify and remediate vulnerabilities**
- **Mitigate risk and impact to your organization**

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

70+
Cybersecurity Courses

40+
GIAC Certifications

120+
Certified Instructors

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.

Multiple Training Formats

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

OnDemand
Anytime, anywhere access to SANS training. Receive training from the same top-notch SANS instructors who teach at our live training events – bringing the true SANS experience right to you.

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 SANS conferences 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 that 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

SANS PREPARES YOU FOR **THREATS FROM EVERY ANGLE**

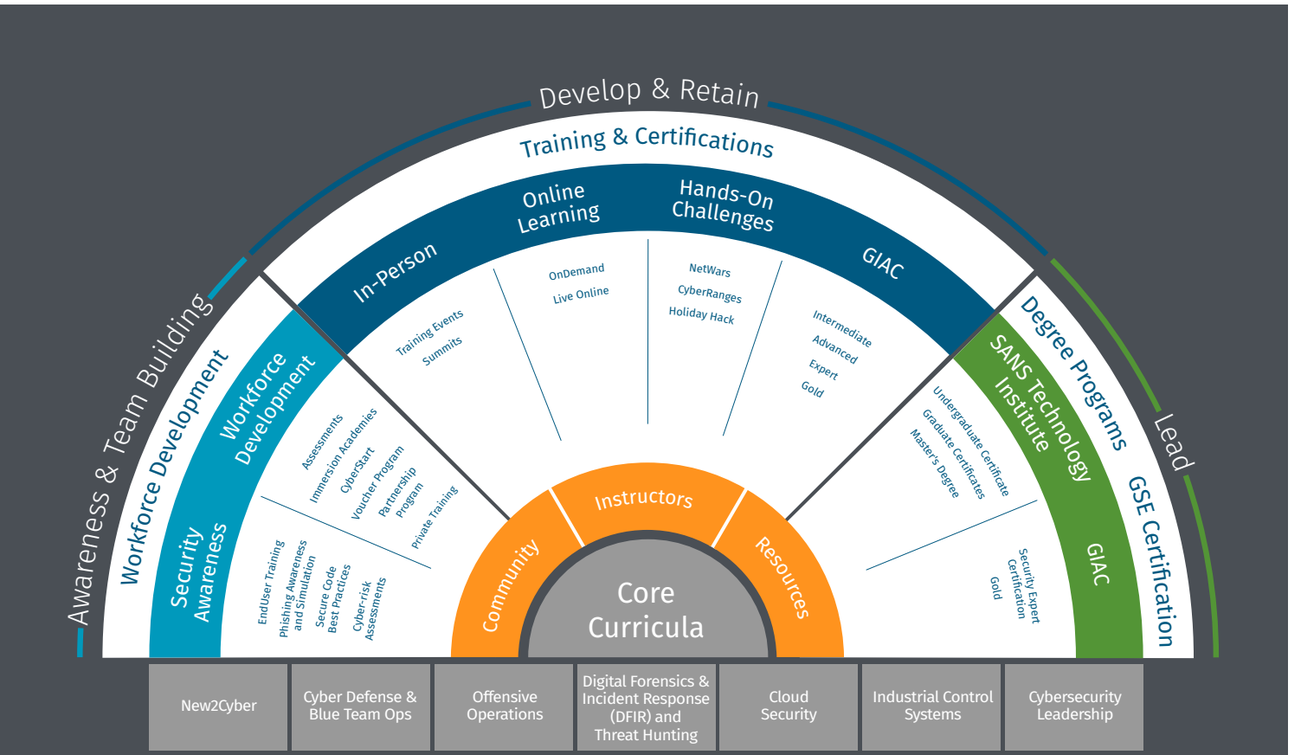
Get Started in Cybersecurity

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 that 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/cyber-security-programs/bachelors-degree



Build an Outcome-Driven Cybersecurity Workforce

Recruit

Create a cyber-resilient workforce with SANS Security Awareness: Comprehensive security awareness training tools to better manage human risk
sans.org/awareness

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

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

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 subjects include:

- **EndUser Training:** Culturally relevant, effective, and easy to implement, EndUser Training provides the training required to move beyond compliance and build a truly mature awareness program.
- **Phishing Education and Simulation:** Designed to integrate and supplement a security awareness program. Deployed using a unique tiered-template methodology to advance learners at any level.
- **Secure Code Training for Web and Application Developers:** Role-based and progressive training paths geared towards all those involved in the development process.
- **Risk Assessments:** A holistic approach that considers organizational culture, human behavior, and technical controls to manage human risk by highlighting the cybersecurity areas that require the most attention.

TABLE OF CONTENTS

Featured Cybersecurity Leadership Training and Certifications

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

Engage your workforce with:

Snack Attack! Ransomware Awareness Program. Shake things up and engage your workforce with this memorable and measurable training program. Snack Attack features creative storytelling, fun gamification elements, and stunning visuals that are tightly aligned for measurable learning outcomes.

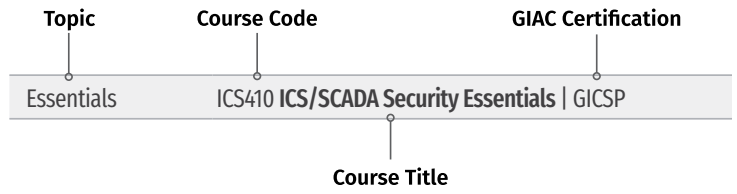
Backed by proven learning principles, SANS Security Awareness programs combine content from hundreds of the world's best security practitioners, security awareness officers, and learning behavior specialists to reflect real-world cyberattacks that engage and educate users, empowering them to contribute to cultural change and prevent attacks.

SANS Security Awareness subjects include:

- Four SCORM-compliant modules pre-packaged so you can assign and track via your own internal Learning Managment System
- Ransomware-awareness themes that include:
  - Social engineering
  - Malware identification
  - Phishing recognition
  - Compromised emails
  - Social media
  - Third-party devices
  - Vishing
  - Spearphishing
  - Browsers, plugins and digital tools
  - Personal information protection
  - And more!
- Accessibility features for broad learner access
- Program support tools to help drive adoption

For global workforces, the SANS SCORM-compliant modules are deployable in 15 languages.

SANS Training Roadmap



Baseline Skills

NEW TO CYBERSECURITY | COMPUTERS, TECHNOLOGY, & 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 & 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.

FORENSICS ESSENTIALS

Every Forensics and IR Professional Should Know

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

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**

CLOUD SECURITY ESSENTIALS

Every Cloud Security Professional Should Know

ESSENTIALS	SEC488 **Cloud Security Essentials** | GCLD
DEVSECOPS	SEC534 **Secure DevOps: A Practical Introduction**

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

CLOUD FUNDAMENTALS

Take Flight Into Cloud Security

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

FOUNDATIONAL LEADERSHIP

Every Cybersecurity Manager Should Know

CISSP® TRAINING	MGT414 **SANS Training Program for CISSP® Certification** | GISP
RISK MANAGEMENT	MGT415 **A Practical Introduction to Cyber Security Risk Management**
SECURITY AWARENESS	MGT433 **Managing Human Risk: Mature Security Awareness Programs**
CIS Controls	SEC440 **CIS Critical Controls: A Practical Introduction**

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	SEC487 **Open-Source Intelligence (OSINT) Gathering and Analysis** | 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 IR Professional Should Know

ENDPOINT FORENSICS	FOR500 **Windows Forensic Analysis** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA 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.

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 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**
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.

CORE LEADERSHIP

Transformational Cybersecurity Leader

TECHNOLOGY LEADERSHIP	MGT512 **Security Leadership Essentials for Managers** | GSLC
SECURITY STRATEGY	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
SECURITY CULTURE	MGT521 **Leading Cybersecurity Change: Building a Security-Based Culture**

Operational Cybersecurity Executive

VULNERABILITY MANAGEMENT	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
SOC	MGT551 **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
BUSINESS LEADERSHIP & MANAGEMENT	Cyber42

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 **Intrusion Detection In-Depth** | GCIA
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA
POWERSHELL	SEC586 **Blue Team Operations: Defensive PowerShell**
PYTHON CODING	SEC573 **Automating Information Security with Python** | GPYC
DATA SCIENCE	SEC595 **Applied Data Science and Machine Learning for Cybersecurity Professionals**

Open-Source Intelligence

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

SPECIALIZED OFFENSIVE OPERATIONS | FOCUSED TECHNIQUES & AREAS

Network, Web & 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**
ACTIVE DEFENSE	SEC550 **Cyber Deception - Attack Detection, Disruption and Active Defense**
BLOCKCHAIN	SEC554 **Blockchain and Smart Contract Security**
RED TEAM	SEC565 **Red Team Exercises and Adversary Emulation**
MOBILE	SEC575 **Mobile Device Security and Ethical Hacking** | GMOB
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	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 and Incident Response**
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

Digital Forensics & Media Exploitation

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

SPECIALIZATION IN CLOUD SECURITY

Specialization for Advanced Skills & Roles

APPLICATION SECURITY	SEC522 **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB
AUTOMATION & COMPLIANCE	SEC557 **Continuous Automation for Enterprise and Cloud Compliance**
CLOUD PEN TEST	SEC588 **Cloud Penetration Testing** | GCPN
CLOUD FORENSICS	FOR509 **Enterprise Cloud Forensics and Incident Response**

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

CLOUD CYBERSECURITY LEADERSHIP AND GOVERNANCE

Every Cloud Security Leader Should Know

VULNERABILITY MANAGEMENT	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
DESIGN & IMPLEMENTATION	MGT520 **Leading Cloud Security Design and Implementation**

LEADERSHIP SPECIALIZATIONS

Cloud Cybersecurity Leadership

VULNERABILITY MANAGEMENT	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
DESIGN & IMPLEMENTATION	MGT520 **Leading Cloud Security Design and Implementation**
AUTOMATION & COMPLIANCE	SEC557 **Continuous Automation for Enterprise and Cloud Compliance**

Management Specialization

AUDIT & MONITOR	AUD507 **Auditing and Monitoring Networks, Perimeters & Systems** | GSNA
LAW & INVESTIGATIONS	LEG523 **Law of Data Security and Investigations** | GLEG
PROJECT MANAGEMENT	MGT525 **Managing Cybersecurity Initiatives & Effective Communication** | GCPM
INCIDENT RESPONSE	MGT553 **Cyber Incident Management**

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

"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

Fundamentals, Essentials, Advanced

Featured New2Cyber Training and Certifications

FOR308 Digital Forensics Essentials

This course provides the necessary knowledge to understand the Digital Forensics and Incident Response disciplines, how to be an effective and efficient Digital Forensics practitioner or Incident Responder, and how to effectively use digital evidence.

sans.org/FOR308

SEC301 Introduction to Cyber Security

GISF GIAC Information Security Fundamentals

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management.

sans.org/SEC301

SEC401 Security Essentials – Network, Endpoint, and Cloud

GSEC GIAC Security Essentials

This course will provide the essential information security skills and techniques you need to protect and secure your critical information and technology assets, whether on-premises 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!

sans.org/SEC401

Additional Courses and Certifications

SEC275 Foundations - Computers, Technology, & Security

SEC402 Cybersecurity Writing: Hack the Reader

Review full course descriptions and demos at **sans.org/courses**

Learn about newest courses in development at **sans.org/new-sans-courses**

Enhance your training with:

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

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

"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

Featured Cyber Defense & Blue Team Ops Training and Certifications

SEC450 Blue Team Fundamentals: Security Operations and Analysis

This course provides an accelerated on-ramp for new cyber defense team members and SOC managers. The curriculum introduces students to a defender's common tools and packs in essential explanations of those tools, processes, and data flow that every blue team member needs to know.

sans.org/SEC450

SEC586 Blue Team Operations: Defensive PowerShell

Are you a Blue Teamer who has been asked to do more with less? Do you wish you could detect and respond at the same pace as your adversaries who are breaking into and moving within the network? This course teaches deep automation and defensive capabilities using PowerShell. Come join us and learn how to automate everything from regular hardening and auditing tasks to advanced defenses. The course will provide you with skills for near real-time detection and response and elevate your defenses to the next level.

sans.org/SEC586

SEC511 Continuous Monitoring and Security Operations

GMON GIAC Continuous Monitoring

The Defensible Security Architecture and Network Security Monitoring 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.

sans.org/SEC511

SEC530 Defensible Security Architecture and Engineering

GDSA GIAC Defensible Security Architecture

This course will help you establish and maintain a holistic and layered approach to security, balancing detection, prevention, and response capabilities with implementation of appropriate network controls. You'll learn the fundamentals of engineering a defensible security architecture.

sans.org/SEC530

Additional Courses and Certifications

SEC487	**Open-Source Intelligence (OSINT) Gathering and Analysis** GOSI Certification
SEC501	**Advanced Security Essentials – Enterprise Defender** GCED Certification
SEC503	**Intrusion Detection In-Depth** | GCIA Certification
SEC505	**Securing Windows and PowerShell Automation** GCWN Certification
SEC555	**SIEM with Tactical Analytics** | GCDA Certification
SEC573	**Automating Information Security with Python** GPYC Certification
SEC587	**Advanced Open-Source Intelligence (OSINT) Gathering and Analysis**
SEC595	**Applied Data Science and Machine Learning for Cybersecurity Professionals**

Review full course descriptions and demos at **sans.org/courses**

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**

Learn about newest courses in development at **sans.org/new-sans-courses**

SANS CURRICULUM FOCUS AREA

OFFENSIVE OPERATIONS

Organizations rely on offensive tactics to discover and understand their system vulnerabilities so they can work to 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

"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

Featured Offensive Operations Training and Certifications

SEC460 Enterprise and Cloud | Threat and Vulnerability Assessment

GEVA — GIAC Enterprise Vulnerability Assessor

In this course, you will learn to use real industry-standard security tools for vulnerability assessment, management, and mitigation. SEC460 is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise.

sans.org/SEC460

SEC560 Network Penetration Testing and Ethical Hacking

GPEN — GIAC Penetration Tester

This course prepares you to conduct high-value penetration testing engagements step by step and end to end. SEC560 starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, Windows Domain attacks, and Azure AD (Active Directory), with over 30 detailed hands-on labs throughout.

sans.org/SEC560

SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

GXPN — GIAC Exploit Researcher and Advanced Penetration Tester

SEC660 is a logical progression for students who have completed SEC560 or for those with existing penetration testing experience. The course goes far beyond simply scanning for low-hanging fruit and teaches you 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.

sans.org/SEC660

Additional Courses and Certifications

SEC467	**Social Engineering for Security Professionals**
SEC504	**Hacker Tools, Techniques, and Incident Handling** GCIH Certification
SEC542	**Web App Penetration Testing and Ethical Hacking** GWAPT Certification
SEC550	**Cyber Deception – Attack Detection, Disruption and Active Defense**
SEC554	**Blockchain and Smart Contract Security**
SEC556	**IoT Penetration Testing**
SEC564	**Red Team Exercises and Adversary Emulation**
SEC575	**Mobile Device Security and Ethical Hacking** GMOB Certification
SEC580	**Metasploit Kung Fu for Enterprise Pen Testing**
SEC588	**Cloud Penetration Testing** | GCPN Certification
SEC617	**Wireless Penetration Testing and Ethical Hacking** GAWN Certification
SEC642	**Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**
SEC661	**ARM Exploit Development**
SEC760	**Advanced Exploit Development for Penetration Testers**

Review full course descriptions and demos at **sans.org/courses**

Learn about newest courses in development at **sans.org/new-sans-courses**

Enhance your training with:

- Core Netwars, CyberCity **sans.org/netwars**
- SANS Summit: Pen Test 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**

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

"This training is invaluable to a practitioner! The tools and knowledge that you gain from it is just outstanding!"

—James Tayler, **Context Information Security**

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

Featured Digital Forensics & Incident Response (DFIR) and Threat Hunting Training and Certifications

FOR500 Windows Forensic Analysis

GCFE GIAC Forensic Examiner

In this course, you'll build in-depth and comprehensive digital forensics knowledge of Microsoft Windows operating systems by analyzing and authenticating forensic data, tracking detailed user activity, and organizing findings.

sans.org/FOR500

FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics

GCFA GIAC Forensic Analyst

This course teaches advanced skills to hunt, identify, counter, and recover from a wide range of threats within enterprise networks, including advanced persistent threat (APT) nation-state adversaries, organized crime syndicates, and hactivists. You'll use threat hunting to catch intrusions while they are in progress, rather than after attackers have attained their objectives.

sans.org/FOR508

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

GNFA GIAC Network Forensic Analyst

This course covers the tools, technology, and processes required to integrate network data sources into your investigations, with a focus on efficiency and effectiveness. There are many use cases for network data, including proactive threat hunting, reactive forensic analysis, and continuous incident response. Learn the techniques that can help close gaps in these use cases and dive into the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more.

sans.org/FOR572

Additional Courses and Certifications

FOR308	**Digital Forensics Essentials**
FOR498	**Battlefield Forensics & Data Acquisition** GBFA Certification
FOR509	**Enterprise Cloud Forensics and Incident Response**
FOR518	**Mac and iOS Forensic Analysis and Incident Response**
FOR578	**Cyber Threat Intelligence** | GCTI Certification
FOR585	**Smartphone Forensic Analysis In-Depth** GASF Certification
FOR610	**Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM Certification

Review full course descriptions and demos at **sans.org/courses**

Learn about newest courses in development at **sans.org/new-sans-courses**

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**

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.

As a result, 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

"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

Deliver, Communicate, Lead

Featured Cybersecurity Leadership Training and Certifications

MGT512 Security Leadership Essentials for Managers

GSLC GIAC Security Leadership

In this course, managers are empowered with the technical knowledge and management skills necessary to lead security teams. The entire security stack is covered, including data, network, host, application, and user controls in conjunction with key management topics that address the overall security lifecycle.

sans.org/MGT512

MGT514 Security Strategic Planning, Policy, and Leadership

GSTRT GIAC Strategic Planning, Policy, and Leadership Certification

This course teaches cybersecurity leaders how to build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management skills to better lead, inspire, and motivate teams.

sans.org/MGT514

MGT551 Building and Leading Security Operations Centers

GSOM GIAC Security Operations Manager

MGT551 will help you build a high-performing SOC tailored to your organization and the threats it faces. We will give you the tools you need to manage an effective defense, measure progress towards your goals, and build out more advanced processes like threat hunting, active defense, and continuous SOC assessment. Best of all, each section is packed with hands-on labs, introductions to some of the industry's best free and open-source tools, and an interactive game in which you will apply your new SOC management skills in real-world scenarios.

sans.org/MGT551

Additional Courses and Certifications

AUD507	**Auditing & Monitoring Networks, Perimeters, and Systems** GSNA Certification
LEG523	**Law of Data Security & Investigation** | GLEG Certification
MGT414	**SANS Training Program for CISSP® Certification** GISP Certification
MGT415	**A Practical Introduction to Cyber Security Risk Management**
MGT433	**Managing Human Risk: Mature Security Awareness Programs** | SSAP Practitioner
MGT520	**Leading Cloud Security Design and Implementation**
MGT521	**Leading Cybersecurity Change: Building a Security-Based Culture**
MGT525	**Managing Cybersecurity Initiatives and Effective Communication** | GCPM Certification
SEC440	**CIS Critical Controls: A Practical Introduction**
SEC557	**Continuous Automation for Enterprise & Cloud Compliance**
SEC566	**Implementing and Auditing CIS Critical Controls** GCCC Certification

Review full course descriptions and demos at **sans.org/courses**

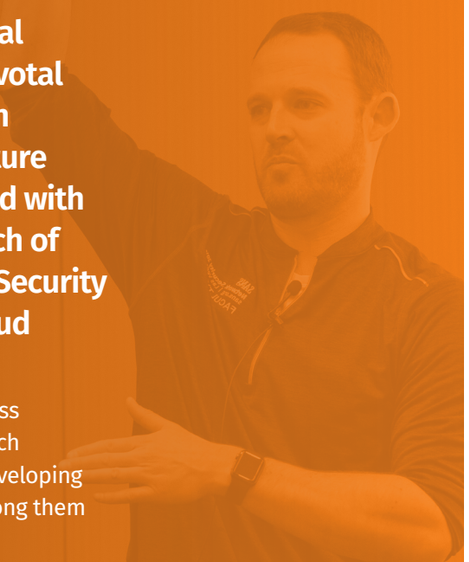
Learn about newest courses in development at **sans.org/new-sans-courses**

Enhance your training with:

- SEC405: Business Finance Essentials **sans.org/SEC405**
- CISO Scorecard and Cloud Security Maturity Model Poster **sans.org/posters/ciso-scorecard-cloud-maturity-model**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a certificate in Cybersecurity Management **sans.edu/academics/certificates/cybersecurity-management**

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 (CPSs). SANS Cloud Security curriculum will take you on a 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.

SANS Cloud Security is here to 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

"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

Featured Cloud Security Training and Certifications

SEC488 Cloud Security Essentials

GCLD GIAC Cloud Security Essentials

This course covers Amazon Web Services, Azure, Google Cloud, and other cloud service providers. Like foreign languages, cloud environments have similarities and differences, and this course will introduce you to the language of cloud security. Upon completion of this course, you will be able to advise and speak about a wide range of cybersecurity topics and help your organization successfully navigate the challenges and opportunities presented by cloud service providers.

sans.org/SEC488

SEC510 Public Cloud Security: AWS, Azure, and GCP

GPCS GIAC Public Cloud Security

This course is an in-depth analysis of the security of managed services for the Big 3 cloud providers: Amazon Web Services, Azure, and Google Cloud Platform. Students will leave the course confident that they have the knowledge they need when adopting services and Platform-as-a-Service (PaaS) offerings in each cloud. Students will launch unhardened services, analyze the security configuration, validate that they are insufficiently secure, deploy patches, and validate the remediation.

sans.org/SEC510

SEC540 Cloud Security and DevSecOps Automation

GCSA GIAC Cloud Security Automation

This course provides security professionals with a methodology to secure modern Cloud and DevOps environments. Students learn how to implement more than 20 DevSecOps security controls to build, test, deploy, and monitor cloud infrastructure and services. Immersive hand-on labs ensure that students not only understand theory, but how to configure and implement each security control. By embracing the DevOps culture, students will walk away from SEC540 battle-tested and ready to build to their organization's Cloud and DevSecOps Security Program.

sans.org/SEC54S

Additional Courses and Certifications

SEC522	**Application Security: Securing Web Apps, APIs, and Microservices** | GWEB Certification
SEC541	**Cloud Security Attacker Techniques, Monitoring, and Threat Detection**
SEC557	**Continuous Automation for Enterprise and Cloud Compliance**
MGT516	**Managing Security Vulnerabilities: Enterprise and Cloud**
MGT520	**Leading Cloud Security Design and Implementation**

Review full course descriptions and demos at **sans.org/courses**

Learn about newest courses in development at **sans.org/new-sans-courses**

Enhance your training with:

- Free Resources: Posters, cheat sheets, whitepapers, webcasts, blogs, ebooks, and more **sans.org/cloud-security**
- SANS Summits: CloudSecNext 2022 **sans.org/summit**
- The SANS Technology Institute's undergraduate and graduate cybersecurity programs, including a certificate in Cloud Security **sans.edu/academics/certificates/cloud-security**

SANS CURRICULUM FOCUS AREA

INDUSTRIAL CONTROL SYSTEMS (ICS)

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. We need to be prepared to defend our control systems against increasingly sophisticated adversaries.

SANS Industrial Control Systems 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

"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

Featured Industrial Control Systems Training and Certifications

ICS410 ICS/SCADA Security Essentials

GICSP Global Industrial Cyber Security Professional

ICS410 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 is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

sans.org/ICS410

ICS418 ICS Security Essentials for Managers

ICS418 empowers leaders responsible for securing critical infrastructure and operational technology environments. The course addresses the need for dedicated ICS security programs, the teams that run them, and the skills required to map industrial cyber risk to business objectives to prioritize safety. ICS418 will help you 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.

sans.org/ICS418

ICS456 Essentials for NERC Critical Infrastructure Protection

GCIP GIAC Critical Infrastructure Protection

This course empowers students with knowledge of the what and the how of the version 5/6/7 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations.

sans.org/ICS456

Review full course descriptions and demos at **sans.org/courses**

Learn about newest courses in development at **sans.org/new-sans-courses**

ICS515 ICS Visibility, Detection, and Response

GRID GIAC Response and Industrial Defense

This course will help you gain visibility and asset identification in your Industrial Control System/ Operational Technology 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.

sans.org/ICS515

ICS612 ICS Cybersecurity In-Depth

This course is an in-classroom lab setup that move students through a variety of exercises that demonstrate how an adversary can attack a poorly architected ICS and how defenders can secure and manage the environment. 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.

sans.org/ICS612

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**

SANS CURRICULUM FOCUS AREA

PURPLE TEAM

These courses help Red and Blue Teams join forces so that they can effectively create a strong feedback loop and identify detection and prevention controls that can be implemented for immediate improvement.

Featured Purple Team Training and Certifications

SEC599 Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses

GDAT GIAC Defending Advanced Threats

This course will equip 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 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

CYBER RANGES

SANS Cyber Ranges

SANS Cyber Ranges provide an essential step in your cybersecurity training, allowing you to apply your skills and gain practical experience in an interactive and isolated environment, with no real-world risk, built by industry-leading SANS instructors.

Learn more at **sans.org/cyber-ranges**

Netwars

Netwars is our premier Cyber Range, appropriate for all cybersecurity skill levels. Netwars poses a series of multifaceted, interactive, and situational cybersecurity challenges. The challenges test a wide variety of disciplines and subject matter across 5 levels that increase in difficulty. These challenges may be completed individually or as a team. Netwars also features an automated hint system to help participants solve questions they may find particularly difficult. The available hints help participants develop new skills and ensure that every participant steadily progresses through the challenge.

- For individuals and teams up to five, of all skill levels
- Custom virtual machine based challenges
- Scorecard of you or your team's performance upon completion
- Automated hint system; hints do not affect scores
- Real-time score board of players/teams

BootUp CTF

Bootup CTF is a capture-the-flag style cyber range consisting of over 125 multi-disciplinary cybersecurity questions. Bootup is browser-based and is for both individuals and teams.

Private Ranges

SANS offers a variety of private range products. From leadership table-top exercises with Cyber42 to full cyber warfare simulations with CyberCity and Cyber STX, SANS has the most advanced tactical cyber ranges for your teams and leaders.

SANS INSTITUTE
MISSION & INITIATIVES

SANS Institute Mission

To empower current and future cybersecurity practitioners around the world with immediately useful knowledge and capabilities, we deliver industry-leading community programs, resources, training, and events.

We invite individuals to take advantage of these programs to further their skills and careers, and we invite organizations to stand with us in these efforts.

sans.org/mission

Mission. Integrity. Collaboration.

These are the values that guide SANS in choosing how to best contribute to our global security community.

We collaborate with a broad community of cyber professionals and organizations, partnering with those who share our mission and commitment to creating a diverse, capable, and innovative industry.

We leverage our expertise and our training capabilities to deliver research, career tools, cyber ranges, and many other widely available learning opportunities.

SANS Institute Initiatives

To make cybersecurity a more accessible career choice for more people, and to ensure that the community is always keeping their skills sharp. We offer a number of initiatives to make cybersecurity a more accessible career choice for more people and to ensure that the community is always keeping its skills sharp.

Mission-Related Initiatives

Explore these opportunities for education and career development and join us in our mission to create a more secure world.

sans.org/about/initiatives

Internet Storm Center

Global incident alert network with more than 15,000 global target IPs and 250-300 active submitters watching for new data
isc.sans.edu

CyberStart America

A free national program for high school students to master cybersecurity as a gateway to the industry, up their digital skills, and compete for college scholarships
cyberstartamerica.org

HBCU Programs

Creating a bridge to diversify cybersecurity with innovative Black talent from Historically Black Colleges and Universities
sans.org/hbcu

Cyber Academies

SANS' women's, veteran's, and diversity academies for helping underrepresented groups launch new cyber careers every year
sans.org/security-resources

Free Cybersecurity Resources
sans.org/free

SANS | GIAC CERTIFICATIONS

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/cyber-security-summit

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

Tech Tuesdays
Hands-on virtual environments that give you the opportunity to dive into course material
sans.org/tech-tuesday-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

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
sans.org/security-awareness-training/resources/reports/sareport-2021

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 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

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**

Join the SANS.org Community for Free

Membership of 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!