“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 right now.”
—Ronald Craft, S-RM

2023 Career Guide
Building Experts, Securing Organizations – Together

Featured New Courses!
SEC549: Enterprise Cloud Security Architecture
SEC673: Advanced Information Security Automation with Python
FOR528: Ransomware for Incident Responders
FOR532: Enterprise Memory Forensics In-Depth
SEC565: Red Team Operations and Adversary Emulation
SEC670: Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control
How to Get the Most Out of This Career Guide

It is hard to believe how much has changed since the term “computer virus” was coined in 1983. Once a niche area, cybersecurity is now one of the most in-demand professions, with growth set to outpace supply of trained professionals.

The SANS Institute believes that our industry can work together to meet the needs of tomorrow. We can infuse agility and resilience into the cybersecurity community by accelerating learning, opening doors, and reimagining career paths.

The SANS 2023 Cybersecurity Career Guide, a curated portfolio of job roles, career paths, and must-have skills, is designed to provide a framework for advancement at every level. The guide maps out recommended training for focus-area job roles, the NICE Framework, and the coolest careers in cyber.

We hope that you will use this guide as you plan for your future. When you are ready, SANS is here to teach, validate, and certify the essential skills and knowledge required to take your career to the next level.
The world needs threat hunters, pen testers, incident responders, and cyber defenders more than ever. Take a glance at the cyber career landscape in 2023:

- The cybersecurity market will reach **$262 billion** in global spending by 2026.1
- The global cybersecurity workforce has reached **4.7 million** workers.2
- Wages are consistent across the United States and Europe. A senior-level cybersecurity analyst (8+ years of experience) in Germany earns an **average salary of €119,338 or US$126,000**.3
- By 2025, **3.5 million** cybersecurity jobs across the globe will be unfilled.4
- According to the U.S. Bureau of Labor Statistics, the number of information security analyst jobs is projected to grow by 35%, making this the **eighth-fastest-growing occupation** in the United States.5
- There will be a **350% increase** in open cybersecurity jobs from 2017 to 2025.6
- The hardest job to fill in 2023 is **Cloud Security Architect**.7
- **65% of organizations** plan to increase cybersecurity spending in 2023.8
- **41% of organizations** say cybersecurity investments are their #1 priority.
- There are **34,505 job openings** for penetration and vulnerability testers in the United States, with an average starting salary of $101,090.9
- The average age of a cybersecurity professional is **42**.10
- A cybersecurity salary is about **16% higher** than that of a similar non-security IT job.11
- There are **7,523 Chief Information Security Officers** in the United States in 2023.12
- 56% of U.S. and 40% of European CISOs say their ideal next role would be as a **board member**.13

---

2 Lake, S. (2022, October 20) The cybersecurity industry is short 3.4 million workers—that’s good news for cyber wages. Fortune. fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages
5 Lake, S. (2022, December 8) This cybersecurity job is one of the fastest-growing in the U.S.—and it pays six figures. Fortune. fortune.com/education/articles/this-cybersecurity-job-is-one-of-the-fastest-growing-in-the-us-and-it-pays-six-figures/#text=Among%20the%20fastest%20growing%20and%20highly%20demand%20jobs%20in%20the%20US
6 Malas, M. (2021, September 6) Microsoft builds fast-track to six-figure cybersecurity jobs at more than 180 colleges. Fortune. fortune.com/education/articles/microsoft-builds-fast-track-to-six-figure-cybersecurity-jobs-at-more-than-180-colleges
13 Cunningham, J. (October 13, 2022) CISO: A day in the life. enterprisersproject.com/article/2022/10/ciso-day-life#:~:text=The%20average%20tenure%20of%20a,environment%20more%20secure%20over%20time
Coolest Careers in Cyber

Organizations are hiring individuals with a unique set of skills and capabilities, and seek those who have the abilities and knowledge to fulfill many new job roles in the cybersecurity industry. The coolest careers in cybersecurity are the most in demand by employers. Which jobs are the coolest and most in demand? We know, so let us show you the hottest cybersecurity jobs for 2023.
Find Your Course by Job Role

Focus-Area Job Roles

Effective cybersecurity operations rely on layers of offensive testing, defensive architecture and monitoring, forensics and incident response, cloud security, and leadership. Advancing your capabilities in these focus areas is our mission because it furthers your ability to protect us all.

Cyber Defense
Our SANS Cyber Defense curriculum provides intensive, immersion training designed to help you and your staff master the practical steps necessary to defend systems and applications against the most dangerous threats.

Courses:
- FOR508
- SEC450
- SEC540
- FOR509
- SEC497
- SEC541
- FOR572
- SEC501
- SEC555
- FOR578
- SEC503
- SEC572
- IC5410
- SEC504
- SEC586
- IC5456
- SEC505
- SEC587
- IC5751
- SEC591
- SEC530

Offensive Operations
SANS Offensive Operations curriculum offers courses that cover topics ranging from introductory penetration testing and hardware hacking, all the way to advanced exploit writing and red teaming. Other courses provide specialized training such as purple teaming, wireless or mobile device security, and more.

Courses:
- FOR308
- FOR572
- LEG522
- FOR498
- FOR578
- SEC402
- FOR500
- FOR585
- SEC403
- FOR508
- FOR608
- SEC450
- FOR509
- FOR610
- SEC504
- FOR518
- FOR710
- SEC573
- FOR528
- IC535
- SEC672
- FOR532
- IC5612

Digital Forensics and Incident Response
Our DFIR curriculum will teach you how to detect compromised systems, identify how and when a breach occurred, understand what attackers took or changed, and successfully contain and remEDIATE INCIDENTS. The SANS ICS curriculum provides hands-on training in industrial control systems and defending ICS environments.

Courses:
- FOR308
- FOR578
- SEC497
- SEC587

Cybersecurity Leadership
The SANS Cybersecurity Leadership curriculum develops cyber leaders who have the practical skills to build and lead security teams, communicate with technical and business leaders alike, and develop capabilities that build your organization’s success.

Courses:
- MGT302
- SEC566
- MGT423
- MGT520
- MGT525
- MGT533
- LEG523
- MGT521
- AUD507
- IC5418
- MGT511
- MGT7413

Cloud Security
Explore our Flight Plan for easy-reference training and certification paths, curated by industry experts and based on common cloud security roles.

Courses:
- SEC488
- SEC549
- FOR509
- SEC510
- SEC522
- SEC566
- SEC587
- SEC541
- SEC588

Security Provisionals
Conceptualizes, designs, procures, and/or builds secure information technology systems, with responsibility for aspects of system and/or network development.

Courses:
- AUD507
- SEC403
- SEC542
- MGT515
- SEC460
- SEC566
- MGT516
- MGT516
- SEC510
- SEC566
- MGT525
- SEC511
- SEC588
- SEC301
- SEC522
- SEC372
- SEC401
- SEC530
- SEC672
- SEC402
- SEC540

Operate and Maintain
Provides leadership, management, direction, and development and advocacy so that the organization can effectively conduct cybersecurity work.

Courses:
- IC5456
- MGT512
- SEC403
- SEC407
- LEG523
- LEG525
- MGT520
- MGT515
- MGT533
- MGT541
- SEC591
- SEC592
- SEC595
- SEC673
- SEC596
- SEC597
- SEC598
- SEC599
- SEC600
- SEC597
- SEC598
- SEC601
- SEC672
- SEC673
- SEC674

Oversee and Govern
Provides leadership, management, direction, and development and advocacy so that the organization can effectively conduct cybersecurity work.

Courses:
- IC5456
- MGT512
- SEC403
- SEC407
- LEG523
- LEG525
- MGT520
- MGT515
- MGT533
- MGT541
- SEC591
- SEC592
- SEC595
- SEC673
- SEC596
- SEC597
- SEC598
- SEC599
- SEC600
- SEC597
- SEC598
- SEC601
- SEC672
- SEC673
- SEC674

Investigate
Investigates cybersecurity events or crimes related to information technology systems, network, and digital evidence.

Courses:
- FOR308
- FOR581
- FOR598
- FOR608
- SEC511
- SEC572
- SEC591
- SEC592
- SEC593
- SEC594
- SEC595
- SEC596

Protect and Defend
Identifies, analyzes, and mitigates threats to internal information technology systems and/or networks.

Courses:
- FOR508
- SEC401
- SEC565
- FOR509
- SEC450
- SEC573
- FOR518
- SEC460
- SEC586
- FOR528
- SEC467
- SEC588
- FOR532
- SEC501
- SEC599
- FOR572
- SEC503
- SEC660
- FOR578
- SEC504
- SEC670
- FOR608
- SEC511
- SEC699
- FOR610
- SEC541
- SEC699
- FOR710
- SEC542
- SEC760
- IC5375
- SEC556
- MGT516
- SEC560

Industrial Control Systems
The SANS ICS curriculum provides hands-on training courses focused on attacking and defending ICS environments.

Courses:
- IC5410
- IC5456
- IC5612
- IC5418
- IC5515

Open-Source Intelligence
Open-Source Intelligence courses support the efforts of the resourceful professionals working in this field to gather requirements from their customers and then, using open sources and mostly Internet resources, collect data relevant to their investigation.

Courses:
- FOR308
- SEC497
- SEC587

Security Provisionals
Conceptualizes, designs, procures, and/or builds secure information technology systems, with responsibility for aspects of system and/or network development.

Courses:
- AUD507
- SEC403
- SEC542
- MGT515
- SEC460
- SEC566
- MGT516
- MGT516
- SEC510
- SEC566
- MGT525
- SEC511
- SEC588
- SEC301
- SEC522
- SEC372
- SEC401
- SEC530
- SEC672
- SEC402
- SEC540

Operate and Maintain
Provides leadership, management, direction, and development and advocacy so that the organization can effectively conduct cybersecurity work.

Courses:
- IC5456
- MGT512
- SEC403
- SEC407
- LEG523
- LEG525
- MGT520
- MGT515
- MGT533
- MGT541
- SEC591
- SEC592
- SEC595
- SEC673
- SEC596
- SEC597
- SEC598
- SEC599
- SEC600
- SEC597
- SEC598
- SEC601
- SEC672
- SEC673
- SEC674

Oversee and Govern
Provides leadership, management, direction, and development and advocacy so that the organization can effectively conduct cybersecurity work.

Courses:
- IC5456
- MGT512
- SEC403
- SEC407
- LEG523
- LEG525
- MGT520
- MGT515
- MGT533
- MGT541
- SEC591
- SEC592
- SEC595
- SEC673
- SEC596
- SEC597
- SEC598
- SEC599
- SEC600
- SEC597
- SEC598
- SEC601
- SEC672
- SEC673
- SEC674

Investigate
Investigates cybersecurity events or crimes related to information technology systems, network, and digital evidence.

Courses:
- FOR308
- FOR581
- FOR598
- FOR608
- SEC511
- SEC572
- SEC591
- SEC592
- SEC593
- SEC594
- SEC595
- SEC596

Protect and Defend
Identifies, analyzes, and mitigates threats to internal information technology systems and/or networks.

Courses:
- FOR508
- SEC401
- SEC565
- FOR509
- SEC450
- SEC573
- FOR518
- SEC460
- SEC586
- FOR528
- SEC467
- SEC588
- FOR532
- SEC501
- SEC599
- FOR572
- SEC503
- SEC660
- FOR578
- SEC504
- SEC670
- FOR608
- SEC511
- SEC699
- FOR610
- SEC541
- SEC699
- FOR710
- SEC542
- SEC760
- IC5375
- SEC556
- MGT516
- SEC560

Industrial Control Systems
A security framework that protects operational technology and industrial control systems against accidental or intentional risks.

Courses:
- IC5410
- IC54515
- IC5418
- IC5612
Multiple Training Formats

SANS courses come in three primary formats to fit your schedule, budget, and preferred learning style.

**In-Person**
Experience SANS courses taught by world-renowned faculty in select locations during SANS In-Person training events. In-Person courses feature hands-on labs to practice your skills in a focused, immersive environment without distractions, plus opportunities to network with fellow cybersecurity professionals. In-Person classes give students the opportunity to:

- Engage with our unparalleled faculty that features 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 Nicholas, Blue Cross Blue Shield of South Carolina

**Live Online**
Avoid travel and attend scheduled live interactive streaming sessions direct from your SANS instructor. Live Online courses feature many of the activities that SANS students love at in-person training events—all to make the student’s online learning experience as fun and engaging as possible. SANS Live Online training offers:

- 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
- The opportunity to 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

**OnDemand**
Anytime, anywhere access to SANS training. In OnDemand courses, you’ll receive training from the same top-notch SANS instructors who teach at our live training events—bringing the true SANS experience right to you. OnDemand is designed to offer convenient and flexible online cybersecurity training on your terms. Students who use our OnDemand training option are able to avoid travel, learn from the best in the business, and study at their own pace. OnDemand training will enable you to:

- Enhance your experience with recorded instruction from world-class instructors who are top practitioners from every niche of cybersecurity
- Train anywhere and anytime with four months of online access to the OnDemand platform and mobile app
- Sharpen your skills with immediate application in an integrated, battle-tested and repeatable hands-on online lab environment
- Work with GIAC-Certified subject-matter experts throughout your course via email or Live Chat
- Hit the ground running with the new modern, easy-to-use OnDemand interface including updated video player, notetaking, quizzes, new bookmarking feature, and more

“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
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC275</td>
<td>Foundations: Computers, Technologies and Security</td>
</tr>
<tr>
<td>SEC301</td>
<td>Introduction to Cyber Security</td>
</tr>
<tr>
<td>SEC401</td>
<td>Security Essentials – Network, Endpoint, and Cloud</td>
</tr>
<tr>
<td>SEC488</td>
<td>Cloud Security Essentials</td>
</tr>
<tr>
<td>SEC10</td>
<td>Public Cloud Security: AWS, Azure, and GCP</td>
</tr>
<tr>
<td>SEC522</td>
<td>Application Security: Securing Web Apps, APIs, and Microservices</td>
</tr>
<tr>
<td>SEC540</td>
<td>Cloud Security and DevSecOps Automation</td>
</tr>
<tr>
<td>SEC541</td>
<td>Cloud Security Attacker Techniques, Monitoring, and Threat Detection</td>
</tr>
<tr>
<td>SEC406</td>
<td>Essential Linux Skills for the Security Professional</td>
</tr>
<tr>
<td>SEC450</td>
<td>Blue Team Fundamentals: Security Operations and Analysis</td>
</tr>
<tr>
<td>SEC497</td>
<td>Practical Open-Source Intelligence (OSINT)</td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
</tr>
<tr>
<td>SEC503</td>
<td>Network Monitoring and Threat Detection In-Depth</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
</tr>
<tr>
<td>SEC73</td>
<td>Automating Information Security with Python</td>
</tr>
<tr>
<td>SEC86</td>
<td>Security Automation with PowerShell</td>
</tr>
<tr>
<td>SEC87</td>
<td>Advanced Open-Source Intelligence (OSINT) Gathering and Analysis</td>
</tr>
<tr>
<td>SEC95</td>
<td>AI, Applied Data Science, and Machine Learning for Cybersecurity Professionals</td>
</tr>
<tr>
<td>SEC73</td>
<td>Advanced Information Security Automation with Python</td>
</tr>
<tr>
<td>AUD507</td>
<td>Auditing Systems, Applications, and the Cloud</td>
</tr>
<tr>
<td>SEC666</td>
<td>Implementing and Auditing Security Frameworks and Controls</td>
</tr>
<tr>
<td>MGTS14</td>
<td>SANS Training Program for the CISSP® Certification</td>
</tr>
<tr>
<td>MGTS12</td>
<td>Security Leadership Essentials for Managers</td>
</tr>
<tr>
<td>MGTS16</td>
<td>Building and Leading Vulnerability Management Programs</td>
</tr>
<tr>
<td>MGTS21</td>
<td>Leading Cybersecurity Change: Building a Security-Based Culture</td>
</tr>
<tr>
<td>MGTS51</td>
<td>Building and Leading Security Operations Centers</td>
</tr>
</tbody>
</table>
The age of cloud computing has arrived as organizations have seen the advantages of migrating their applications from traditional on-premises networks. However, the rapid adoption of cloud has left architects scrambling to design on this new medium. A shift to the cloud requires that cybersecurity professionals reorient their security goals around a new threat model to enable business requirements while improving their organization’s security posture. SEC549 is here to help enable this shift. The course takes an architectural lens to enterprise-scale, cloud infrastructure challenges. We address the security considerations architects need to tackle when tasked with business expansion into the cloud, from the centralization of workforce identity and network security controls to the secure usage of shared cloud-hosted data, and the design of effective logging strategies.

Business Takeaways
- Mitigate the risk posed by nascent cloud technologies and their rapid adoption
- Decrease the risk of cloud migrations by planning a 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

Syllabus Summary

SECTION 1: Cloud Account Management and Identity Foundations
SECTION 2: Implementing an Identity Perimeter in the Cloud
SECTION 3: Network Access Perimeters for the Cloud
SECTION 4: Data Access Perimeters in the Cloud
SECTION 5: Enabling the Cloud-Focused SOC
SEC673: Advanced Information Security Automation with Python

SEC673 is designed as the logical progression point for students who have completed SEC573: Automating Information Security with Python, or for those who are already familiar with basic Python programming concepts. We jump immediately into advanced concepts. SEC673 looks at coding techniques used by popular open-source information security packages and how to apply them to your own Python cybersecurity projects. We’ll learn from the best of them as we spend the week making information security for our project, named SPF100, as easy to develop and maintain as that of the most popular cybersecurity projects. Discover how to organize your code and use advanced programming concepts to make your code faster, more efficient, and easier to develop and maintain.

Course Topics
- Making your packages installable for Package Installer for Python (PIP) for easy distribution and updates
- Building a custom data structure that fits your application for faster development
- Using advanced features like decorators, generators, and context managers to simplify code
- Making programs run faster with multi-threading and multi-processing
- Eliminating cascading errors by implementing unit tests so small changes don’t become big errors
- Undertaking proper log generation and handling in Python applications in order to identify those “works for me” errors
- Implementing application automation and interaction so that you can move on to more important tasks
SEC565: Red Team Operations and Adversary Emulation

Develop and improve Red Team operations for security controls in SEC565 through adversary emulation, cyber threat intelligence, Red Team tradecraft, and engagement planning. Learn how to execute consistent and repeatable Red Team engagements that are focused on the effectiveness of the people, processes, and technology used to defend environments.

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.

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

Who Should Attend

- Security professionals interested in expanding their knowledge of Red Team engagements in order to understand how they are different from other types of security testing
- Penetration testers and Red Team members looking to better understand their craft
- Blue Team members, defenders, and forensic specialists looking to better understand how Red Team engagements can improve their ability to defend by better understanding offensive methodologies, tools, tactics, techniques, and procedures
- Auditors who need to build deeper technical skills and/or meet regulatory requirements
- Information security managers who need to incorporate or participate in high-value Red Team engagements

NICE Framework Work Roles

- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Partner Integration Planner (OPM 333)

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

Syllabus Summary

SECTION 1: Planning Adversary Emulation and Threat Intelligence

SECTION 2: Attack Infrastructure and Operational Security

SECTION 3: Getting In and Staying In

SECTION 4: Active Directory Attacks and Lateral Movement

SECTION 5: Obtaining the Objective and Reporting

SECTION 6: Immersive Red Team Capture the Flag

WAYS TO TRAIN FOR SEC565

In-Person: sans.org/mlp/in-person-training
Live Online: sans.org/mlp/live-online-training
OnDemand: sans.org/ondemand
SEC670: Red Teaming Tools – Developing Windows Implants, Shellcode, and Command and Control

SEC670 prepares you to create custom-compiled programs specifically for Windows and introduces students to techniques that real nation-state malware authors are currently using. You will learn the essential building blocks develop custom offensive tools through required programming, APIs used, and mitigations for techniques covering privilege escalation, persistence, and collection.

Learning how to develop custom-compiled tools for Windows is a skillset that is not being taught by universities or other academic organizations. As a result, the cybersecurity industry has a severe skills deficit that is limiting the overall capability of red team operations. Defense contractors and industries looking to hire Windows tools developers are facing a severe shortage of talent and are unable to further hone their defenses. SEC670 is the first course of its kind, giving students hands-on lab experience creating custom-compiled programs specifically for Windows using the C/C++ programming languages. Students will learn the internal workings of existing offensive tools that offer capabilities such as privilege escalation, persistence, and collection by creating their own tools using Windows APIs. Windows defenses have become more robust, and cloud-connected AV solutions are making it more challenging to operate under the radar. In response, this course introduces students to techniques that real nation-state malware authors are currently implementing in their implants.

**What You Will Learn**
- New calling conventions and data types specific to Windows
- How Windows processes, threads, and services work internally
- How to abuse Windows APIs to inject shellcode into other processes without detection
- How to create a hidden, persistent service
- How to hide from user-mode tools like Task Manager
- How to create and execute shellcode without detection
- How to bypass user-land hooks and implement your own
- How to control your implant from your C2

**Syllabus Summary**

**SECTION 1:** Windows Tool Development

**SECTION 2:** Getting to Know your Target

**SECTION 3:** Operational Actions

**SECTION 4:** Persistence: Die Another Day

**SECTION 5:** Enhancing Your Implant: Shellcode, Evasion, and C2

**SECTION 6:** Capture the Flag
FOR528: Ransomware for Incident Responders

Ransomware attackers have become more sophisticated, and their techniques constantly evolve. It is a threat that requires an immediate response, especially in the enterprise. FOR528: Ransomware for Incident Responders covers the entire life cycle of an incident, from initial detection to incident response and postmortem analysis. While there is no way to prepare for every scenario possible, this course uses deftly devised, real-world attacks and their subsequent forensic artifacts to provide you, the analyst, with all that you need to respond when the threat become a reality.

Course Topics

- Ransomware evolution and history
- Windows forensics artifacts critical to ransomware incident response
- Evidence acquisition tools and techniques
- Parsing forensic artifacts
- Ingesting parsed data into a SIEM
- Analyzing SIEM/aggregator data via TimeSketch and Kibana
- Initial access
- Execution and defense evasion
- Persistence
- Active directory attacks
- Privilege escalation and credential access
- Lateral movement
- Data access
- Data exfiltration
- Backup and recovery tampering
- Payload deployment
- Encryption specifics including source code review
- Decryptors
- Cobalt Strike architecture, components, and payloads
- Dealing with an active threat
- Hunting methods and techniques

Syllabus Summary

SECTION 1: Ransomware Incident Response Fundamentals

SECTION 2: Ransomware Modus Operandi

SECTION 3: Advanced Ransomware Concepts

SECTION 4: Course Capture-the-Flag Challenge
FOR532: Enterprise Memory Forensics In-Depth

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 a number of applications that for many teams are still terra incognita. The FOR532: Enterprise Memory Forensics In-Depth course strives to change that and significantly speed up your incident response, threat hunting and malware analysis.

Syllabus Summary

SECTION 1: Fundamentals of Memory Forensics
SECTION 2: Diving Deeper and User Artifacts
SECTION 3: Intrusion Forensics
SECTION 4: Beyond Classical Memory Forensics

Who Should Attend

▐ Incident response team members
▐ Threat hunters
▐ Experienced digital forensic analysts
▐ Federal agents and law enforcement professionals
▐ Information security professionals
▐ Red Team members, penetration testers, and exploit developers
▐ SANS FOR508, FOR608, and FOR610 graduates looking to take their skills to the next level

WAYS TO TRAIN FOR FOR532

In-Person
sans.org/mlp/in-person-training
Live Online
sans.org/mlp/live-online-training
OnDemand
sans.org/ondemand

FOR589: Cybercrime Intelligence

The cyber-threat landscape continues to rapidly evolve due to technological advancements, increased investments in offensive cyber operations from nation-states, and a cybercriminal ecosystem that breeds new advanced persistent threat actors every day. FOR589 will teach you how to hunt for threat intelligence within the cybercriminal underground using human intelligence elicitation techniques and blockchain analytics tools to trace criminal cryptocurrency transactions. Following the completion of the course, each student will be prepared to social engineer cybercriminals, produce dark web intelligence, provide unique intelligence support to incident response cases, extract cryptocurrency artifacts from mobile and computer devices, negotiate with ransomware operators on behalf of a client, support law enforcement partners with attribution efforts, and investigate anti-money laundering cases involving cryptocurrency transactions on and off the blockchain.

Who Should Attend

▐ Cyber Threat Intelligence Analysts
▐ Cyber Intelligence Professionals
▐ Criminal Actor Investigators
▐ Financial Crime Investigators
▐ Threat Hunters
▐ Incident Responders.
▐ Forensic Analysts
▐ Information Security Professionals
▐ Federal Agents and Law Enforcement Professionals
SEC406: Essential Linux Skills for the Security Professional

You Will Be Able To
- Find and execute Linux programs
- Refine the results returned using appropriate options and parameters found in the manual pages
- Modify our environment using variables and aliases
- Secure and appropriately leverage administrative credentials and closely guard them with Least Required Privilege
- Schedule tasks on Linux
- Verify system settings are applied by auditing your system
- Manage networking settings and the host-based firewall
- Retain your work over multiple sessions using terminal managers such as Tmux and Screen

Linux is the operating system of millions of systems all around the world. No matter what area of cybersecurity you work in or the vertical you support, to do your job effectively you need to understand how Linux works and how to secure it. Skilled attackers certainly know how to use and operate in a Linux environment and love nothing more than to find your security tools running on improperly secured Linux boxes. SEC406 teaches the Linux essentials every security professional needs to know to run the many open-source tools that are crucial to doing your job.

Who Should Attend
- Security professionals looking to learn the basics of Linux operating systems
- Administrators needing information on how to secure common Internet applications on the Linux platform
- Auditors, incident responders, and information security analysts who need greater visibility into Linux security tools, procedures, and best practices

FOR577: Linux Incident Response & Analysis

You Will Learn
- The common Linux distributions in use today
- The incident response cycle and its relationship to threat intelligence and threat hunting on Linux platforms
- Common attacker tools, techniques and procedures used by advanced threat actors to compromise Linux systems in modern environments
- Attacker anti-forensic techniques and how to combat them
- Linux filesystems and timestamps
- How user interaction changes data within Linux
- Evidence collection from Linux platforms
- Key logs application logs, essential to DFIR investigations
- Triage collection techniques to speed up the incident response process
- Techniques for using live response tools to facilitate investigations
- Key actions to significantly improve security protections and facilitate effective incident response

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. FOR577: Linux Incident Response & Analysis 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.

Who Should Attend
- Incident responders
- General IT practitioners
- Security engineers
- Security Operations Center analysts
- Military and intelligence operators
- Federal agents and law enforcement officers
**SEC446: Hardware-Assisted Hacking**

This course addresses a range of security problems related to hardware, such as physical security measures, encryption, and communication vulnerabilities. By learning about hardware hacking and gaining hands-on experience with breaking and manipulating hardware with software, students will be able to identify and analyze potential vulnerabilities in various hardware systems. This knowledge can be applied to a range of contexts, including cybersecurity, IT, and hardware design, to create more secure and robust systems. Ultimately, this course helps to develop a deeper understanding of hardware security and how to protect against potential attacks.

**Who Should Attend**
- Cybersecurity professionals who want to learn the basics of hardware hacking
- Hardware engineers
- Embedded system developers
- Penetration testers
- Product security engineers
- Information security consultants
- Cybersecurity researchers

**You Will Learn**
- The foundations of both hardware theory and hardware practice related to hardware and software security
- Practical experience in identifying and analyzing potential security vulnerabilities in various hardware systems and mitigations against potential attacks
- The basics of binary numeric representation and operations used in microcontroller (and microprocessor) implementation
- Flash, EEPROM, and Pulse Width Modulation
- Arduino programming and hardware development
- How to exploit the physical capabilities of several devices
- Novel attack techniques like side-channel attacks and supply chain chipping attacks
- Real-world hacking used on credit card readers, medical IV pumps, and Cisco firewalls
- How to build circuits and prototypes on their own
- How to control servos and recover sensitive information from hardware components

**COMING SOON!**
**SEC446**: 6 Day Program | 36 CPEs

**SEC554: Blockchain and Smart Contract Security**

SEC554 will teach you all topics relevant to securing, hacking, and using blockchain and smart contract technology. The course takes a detailed look at the technology that underpins multiple implementations of blockchain, the cryptography and transactions behind them, the various smart contract languages like Solidity and Rust, and the protocols built with them like NFTs, DeFi, and Web3. The labs in the course provide the hands-on training and tools needed to deploy, audit, scan, and exploit blockchain and smart contract assets, as well as to defend them and identify threats and threat actors using them for malicious purposes.

**Who Should Attend**
- Smart contract developers
- Blockchain developers
- Security engineers, architects, or analysts
- Penetration testers
- Compliance officers
- Executives or managers
- Employees of government agencies
- Cryptocurrency users

**You Will Be Able To**
- Interact with and get data from public blockchains
- Exploit several types of smart contract vulnerabilities
- Test and exploit weak cryptography/entropy
- Discover and re-create private keys
- Understand what cryptojackers do and how to trace and track movements on blockchain
- Combat non-technical or social engineering types of attacks that adversaries use to access and steal from victims

**COMING SOON!**
**SEC554**: 5 Day Program | 30 CPEs
SEC568: **Combating Supply Chain Attacks with Product Security Testing**

Think Red, Act Blue – Attackers are using new methods of compromising software supply chains that bypass traditional security controls on products spanning multiple attack surfaces. SEC568 is a complete training program designed to equip you with the skills and knowledge necessary to execute product security assessments through deeply technical risk analysis.

**Who Should Attend**

This course is useful both for individuals looking to enter the product security testing domain and those who seek to formalize and expand their skills in this area while focusing on combating supply chain attacks. Both attack-focused and defense-focused security practitioners will be interested in this course by gaining a deep understanding of how to perform an effective product security assessment. This course enhances the skills of not only penetration testers and defenders, but is applicable to those designing and implementing corporate security controls in networks and endpoints across many verticals. Job roles that can benefit from SEC568 include:

- Network and systems penetration testers
- Application developers
- Security auditors
- Security Operations Center analysts, incident responders and security engineers

**You Will Be Able To**

- Conduct a product security test
- Reduce the impact of supply chain attacks on your organization
- Evaluate a Windows, Linux, or Android product for threats
- Perform basic static firmware analysis to understand what is running on a device
- Determine how a system changes because of installing new software
- Use Exploratory Data Analysis (EDA) techniques to analyze and present a large amount of data
- Dissect propriety protocols
- Build a threat model to articulate the biggest risks and mitigations
- Construct attack trees and use a risk scoring methodology to determine the risk of each threat discovered in previous phases

<table>
<thead>
<tr>
<th>5 Day Program</th>
<th>30 CPEs</th>
<th>20 Labs</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMING SOON!</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SEC598: **Security Automation for Offense, Defense, and Cloud**

SEC598: Security Automation for Offense, Defense, and Cloud will equip you with the expertise to apply automated solutions to prevent, detect, and respond to security incidents. The cybersecurity skill gap continues to push organizations to adopt automation to deal with security operations, so most automation training focuses exclusively on DevSecOps and automation tools/scripting. SEC598 takes another approach: students first train to understand the concept of automation, then learn how existing technologies can be best leveraged to build automation stories that translate repeatable problems to automated scripts.

**Who Should Attend**

- Security architects
- Security engineers
- Incident responders
- Enterprise risk analysts
- Ethical hackers
- Penetration testers
- Red Team members
- Blue Team members
- Purple Team members
- Security Operations Center analysts
- Cloud engineers

<table>
<thead>
<tr>
<th>6 Day Program</th>
<th>36 CPEs</th>
<th>21 Labs</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMING SOON!</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**You Will Be Able To**

- Understand the security issues that most organizations are facing today
- Translate security issues into smaller problems, define automated solutions for those specific problems, and then fully chain features that can be used to tackle multiple issues in an automated manner
- Use tools like Terraform, Ansible, CHEF Puppet, and many more 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
- Evaluate real-world scenarios within a combination of on-premise and cloud environments using a reference framework that can be immediately used and implemented in your organization

<table>
<thead>
<tr>
<th>6 Day Program</th>
<th>36 CPEs</th>
<th>21 Labs</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMING SOON!</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WHERE TO START
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
• Develop effective security metrics that provide a focused playbook that the IT team can implement, auditors can validate, and executives can understand
• Identify the latest attack vectors and implement controls to prevent and detect them
• Build an internal security roadmap that can scale today and into the future

For detailed course description, visit sans.org/courses

WAYS TO TRAIN FOR SEC275
OnDemand
sans.org/ondemand

You Will Learn
| Computer components and concepts |
| Operating systems, containers, and virtualization |
| Linux |
| Networking fundamentals |
| The Web: Search engine and servers |
| Practical programming in Python and C |
| Windows foundations |
| Advanced computer hardware (e.g., CPU and memory) |
| Encryption |
| Introduction to basic security concepts |
| Introduction to forensics, reconnaissance, exploitation, privilege escalation, and network and computer infiltration (e.g., lateral movement) |

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.

Who Should Attend
| 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 program |

For detailed course description, visit sans.org/courses
SEC301: Introduction to Cyber Security

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 infused with real-life examples. A balanced mix of technical and managerial instruction makes the course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management. Organizations often tap someone who has no information security training and say, “Congratulations, you are now a security officer.” If you need to get up to speed fast, SEC301 rocks!

**Business Takeaways**

- Understand the fundamentals of risk management, security policy, and authentication/authorization/accountability (AAA)
- Have the ability to communicate about a wide variety of attacks including social engineering, drive-by downloads, watering hole attacks, lateral movement, and more
- Secure your organization’s assets through the application of the Principles of Least Privilege
- Avoid being the next mega-breach headline story on the six o’clock news

**Syllabus Summary**

SECTION 1: Security’s Foundation
SECTION 2: Computer Functions and Networking
SECTION 3: An Introduction to Cryptography
SECTION 4: Cybersecurity Technologies – Part 1
SECTION 5: Cybersecurity Technologies – Part 2

**Who Should Attend**

- People who are new to information security and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don’t understand but want to understand
- Professionals who need to be conversant in basic security concepts, principles, and terms, but who don’t need “deep in the weeds” detail
- Those who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification
- Managers who worry their company may be the next mega-breach headline story on the 6 o’clock news

**NICE Framework Work Roles**

- Authorizing Official/Designating Representative (OPM 611)
- Knowledge Manager (OPM 431)
- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Cyber Instructor (OPM 712)
- Communications Security (COMSEC) Manager (OPM 723)

---

**WAYS TO TRAIN FOR SEC301**

- **In-Person**
  - sans.org/mlp/in-person-training
- **Live Online**
  - sans.org/mlp/live-online-training
- **OnDemand**
  - sans.org/ondemand

---

**For detailed course description, visit sans.org/courses**

---

**GISF Information Security Fundamentals**

giac.org/gisf

---

**It’s a very good course if you need the basic foundation. It’s a very helpful class to take because it expands on some basic concepts.”**

—Shruti Iyer, DCS Corporation

---

**“The SEC301 content was excellent. A wide gambit of information was provided that will prove applicable at work and also in life in general. The labs provided excellent instructions & were great at reinforcing the material.”**

—Jimmy T., U.S. Military

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. SEC401 will also show you how to directly apply the concepts learned into a winning defensive strategy, all in terms of the modern adversary. This is how we fight; this is how we win!

Business Takeaways
- Address high-priority security problems
- Leverage the strengths and differences among the top three cloud providers (AWS, Microsoft Azure, and Google Cloud Platform)
- Build a network visibility map to validate the attack surface
- Reduce your organization’s attack surface through hardening and configuration management

Syllabus Summary
- SECTION 1: Network Security & Cloud Essentials
- SECTION 2: Defense-in-Depth
- SECTION 3: Vulnerability Management and Response
- SECTION 4: Data Security Technologies
- SECTION 5: Windows and Azure Security
- SECTION 6: Linux, Mac and Smartphone Security

“SEC401 is a great intro and overview of network security. It covered just enough information to get a baseline level of knowledge without going too in-depth on any one topic.”
—Josh Winter, Washington County, MN

“SEC401 has been an excellent experience all around. It is content-heavy and rich, and regardless of your technical ability and experience, you will leave with a far better understanding of many aspects of cybersecurity.”
—Paul F., Australian Federal Government

For detailed course description, visit sans.org/courses
More businesses than ever are moving sensitive data and mission-critical workloads to the cloud, and not just to one cloud service provider (CSP). Organizations are responsible for securing their data and mission-critical applications in the cloud. When leveraging a multicloud platform to develop and accelerate business applications, cost and speed benefits can quickly be reversed if security professionals can’t properly secure the cloud environment and respond to the inevitable breaches. New technologies introduce new risks. Help your organization successfully navigate both the security challenges and opportunities presented by cloud services.

**Business Takeaways**
- Understand the current cloud deployment
- Protect cloud-hosted workloads, services, and virtual machines
- Cost-effectively select appropriate services and configure properly to better 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

**Syllabus Summary**

**SECTION 1:** Identity and Access Management

**SECTION 2:** Compute and Configuration Management

**SECTION 3:** Data Protection and Automation

**SECTION 4:** Networking and Logging

**SECTION 5:** Compliance, Incident Response, and Penetration Testing

**SECTION 6:** CloudWars

“I learned a lot, went deeper technically than I expected to, and feel like this was absolutely a great use of my time. The instructors and TAs are top notch and made my experience taking this course a very positive one.”

—Marni Reemer, AWS
SEC510: **Public Cloud Security: AWS, Azure, and GCP**

Organizations in every sector are increasingly adopting cloud offerings to build their online presence. But although cloud providers are responsible for the security of the cloud, their customers are responsible for what they do in the cloud. Unfortunately, providers have made the customer’s job difficult by offering many services that are insecure by default. Worse yet, with each provider offering hundreds of different services and with many organizations opting to use multiple providers, security teams need a deep understanding of the underlying details of the different services in order to lock them down. As the landscape rapidly evolves and development teams eagerly adopt the next big thing, security is constantly playing catch-up in order to avert disaster. **SEC510: Public Cloud Security: AWS, Azure, and GCP** teaches you how the Big 3 cloud providers work and how to securely configure and use their services and PaaS/IaaS offerings.

**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

**Business Takeaways**
- Be proactive in embracing the multicloud trend safely. It is impossible for an organization to standardize on a single cloud provider. A survey from Forrester shows that 86% of organizations identify as multicloud. Even if you do not want to use multiple clouds, mergers and acquisitions makes this inevitable.
- Effective cloud security practitioners need to know how the Big 3 providers differ. Security concepts do not always translate from cloud to cloud. A great strategy for one can be catastrophic for another.
- All security-minded organizations require professional reconfiguration, as most cloud services are highly insecure by default.
- Storage security is much more than just closing public buckets. Even private assets can be compromised by competent attackers.
- Security is 5+ years behind development and needs to play catch-up. Technologies that security considers to be cutting-edge, like serverless, have been used in production for a very long time.

**Syllabus Summary**
**SECTION 1:** Cloud Credential Management
**SECTION 2:** Cloud Virtual Networks
**SECTION 3:** Encryption, Storage, and Logging
**SECTION 4:** Serverless Platforms
**SECTION 5:** Cross-Account and Cross-Cloud Assessment

“It is amazing how the lab was able to talk to three live cloud providers at the same time. It was impressive.”
—Christopher Hearn, Harris County

For detailed course description, visit [sans.org/courses](http://sans.org/courses)
SEC522: Application Security: Securing Web Apps, APIs, and Microservices

Web applications are increasingly distributed. What used to be a complex monolithic application hosted on premise has become a distributed set of services incorporating on-premise legacy applications along with interfaces to cloud-hosted and cloud-native components. Coupled with a lack of security knowledge, this means that web applications are exposing sensitive corporate data. Security professionals are asked to provide validated and scalable solutions to secure this content in line with best industry practices using modern web application frameworks. Attending this course will not only raise awareness about common security flaws in modern web applications, it will also teach students how to recognize and mitigate these flaws early and efficiently.

**Business Takeaways**
- Comply with PCI DSS 6.5 requirements
- Reduce the overall application security risks
- Protect company reputation
- Adopt the “shifting left” mindset wherein security issues are addressed early and quickly to avoid costly rework
- Adopt modern apps with API and microservices in a secure manner
- This course prepares students for the GWEB certification

**Syllabus Summary**

**SECTION 1:** Web Fundamentals and Secure Configurations

**SECTION 2:** Input-Related Defenses

**SECTION 3:** Authentication and Authorization

**SECTION 4:** Web Services and Front-End Security

**SECTION 5:** APIs and Microservices Security

**SECTION 6:** DevSecOps and Defending the Flag

“This training is essential for anyone who needs to understand web protocol and application security and their limitations. This course provides a practical approach to many theoretical scenarios with relevant POCs within the coursework.”

—Joel Samaroo, Visa, Inc.

“The exercises are a good indicator of understanding the material. They worked flawlessly for me.”

—Robert Fratila, Microsoft

For detailed course description, visit sans.org/courses
SEC540: Cloud Security and DevSecOps Automation

Organizations are moving to the cloud to enable digital transformation and reap the benefits of cloud computing. However, security teams struggle to understand the DevOps toolchain and how to introduce security controls in their automated pipelines responsible for delivering changes to cloud-based systems. Without effective pipeline security controls, security teams lose visibility into the changes released into production environments. SEC540 provides security professionals with a methodology to secure modern cloud and DevOps environments. By embracing the DevOps culture, students will walk away from SEC540 battle-tested and ready to build up their organization’s Cloud and DevSecOps Security Program.

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

Syllabus Summary

SECTION 1: DevOps Security Automation
SECTION 2: Cloud Infrastructure Security
SECTION 3: Cloud Security Operations
SECTION 4: Cloud Security as a Service
SECTION 5: Compliance as Code

“Labs were the best bit of the whole thing—well maintained. Keep it up.”
—Richard Ackroyd, PwC

“Great course! Excellent instructor! Lots of hands-on! Met my expectations definitely, and I will absolutely recommend it to other people.”
—Sandro Blatter, SBB

“SEC540 truly deserves the 5 of 5 excellent rating. I really can’t express how impressed I am with my first SANS course.”
—Dwayne Sander, ALERRT
SEC541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection

Cloud infrastructure provides organizations with new and exciting services to better meet the demands of their customers. However, these services bring with them new challenges, particularly for organizations struggling to make sense of the cloud native logs, keep ahead of fast-moving development teams, and learn how threats are adapting to cloud services. Securely operating cloud infrastructure requires new tools and approaches for better visibility into the cloud environment threat landscape, the ability to capture appropriate data, and, most importantly, the ability to analyze and correlate the data effectively and accurately to understand if the specific threat is legitimate based on your organization’s bigger picture.

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
- Decrease the 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

Syllabus Summary

SECTION 1: Management Plane and Networking Logging
SECTION 2: Computer and Cloud Services Logging
SECTION 3: Cloud Services and Data Discovery
SECTION 4: Microsoft Ecosystem
SECTION 5: Automate Response Actions and CloudWars

"Each day’s content is like a well-told story. The labs bring the lecture content to life."
—Frank Balluffi, BNY Mellon

"Using the labs was easy with well documented instructions. I like the fact that I could easily copy and paste the commands. This helps me to get through the lab fast but I also know that I can come back later after the course and take the time to review each command."
—Ludek Suk, Accenture
SEC530: **Defensible Security Architecture & Engineering: Implementing Zero Trust for the Hybrid Enterprise**

This course is designed to help you build and maintain a truly defensible security architecture by implementing Zero Trust principles, pillars, and capabilities, with a heavy focus on leveraging current infrastructure and investment. You will learn how to assess, reconfigure and validate existing technologies to significantly improve your organization’s 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 toward Zero Trust.

**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 both protection time and the likelihood of detection
- Improve prevention, detection, and response capabilities
- Reduce the attack surface

**Syllabus Summary**

**SECTION 1:** Defensible Security Architecture and Engineering: A Journey Towards Zero Trust

**SECTION 2:** Network Security Architecture and Engineering

**SECTION 3:** Network-Centric Application Security Architecture

**SECTION 4:** Data-Centric Application Security Architecture

**SECTION 5:** Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks

**SECTION 6:** Hands-On Secure-the-Flag Challenge

"SEC530 course content is relevant to today’s security landscape, and it was written in a clear and concise manner. The Live Online platform did not feel any different from having the instructor here in person."

—Edmund L., Singapore Federal Agency
SEC595: AI, Applied Data Science, and Machine Learning for Cybersecurity Professionals  NEW

SEC595 provides a crash-course introduction to practical data science, statistics, probability, and machine learning. The course is structured as a series of short discussions with extensive hands-on labs that help you develop a useful, intuitive understanding of how these concepts relate and can be used to solve real-world problems. If you've never done anything with data science or machine learning but want to use these techniques, this is definitely the course for you!

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
- Understand and build generic search algorithms

Who Should Attend
- InfoSec professionals who want to understand machine learning
- Professionals desiring to apply data science principles to real-world problems
- Anyone who has tried to learn the basics but can't figure out how to translate their problem into something that can be solved with machine learning
- Blue Team and Security Operations Center members looking to identify anomalies and perform custom threat hunting

NICE Framework Work Roles
- Data Analyst (OPM 422)

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

Syllabus Summary
SECTION 1: Data Acquisition, Cleaning, and Manipulation
SECTION 2: Data Exploration and Statistics
SECTION 3: Essentials of Machine Learning
SECTION 4: Essentials of Machine Learning
SECTION 5: Essentials of Machine Learning
SECTION 6: Essentials of Machine Learning

“SEC595 is an effective bootcamp focusing on core concepts and allowing students to practice techniques on cybersecurity data sets. It also teaches the soft skill of developing an intuition about using the tools to solve problems.”
—Roger Wajda, Secure Cloud Solutions, LLC

“The course exceeded my expectations. The delicate connection between theory, foundations, mathematical models, and real-life applicability was invaluable. Back home I will be able to take more advantage of tools, material at hand, and proper knowledge of how to work my own data.”
—Oscar Garzon, Thought Machine

For detailed course description, visit sans.org/courses

WAYS TO TRAIN FOR SEC595

In-Person  sans.org/mlp/in-person-training
Live Online  sans.org/mlp/live-online-training
OnDemand  sans.org/ondemand
SEC497: Practical Open-Source Intelligence (OSINT)  NEW

CURRICULUM: Cyber Defense

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

NICE Framework Work Roles
- Data Analyst (OPM 422)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- All Source-Collection Manager (OPM 311)
- Target Network Analyst (OPM 132)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Intel Planner (OPM 331)
- Cyber Ops Planner (OPM 332)

SEC497 is based on two decades of experience with open-source intelligence (OSINT) research and investigations supporting law enforcement, intelligence operations, and a variety of private sector businesses ranging from small start-ups to Fortune 100 companies. The goal is to provide practical, real-world tools and techniques to help individuals perform OSINT research safely and effectively. One of the most dynamic aspects of working with professionals from different industries worldwide is getting to see their problems and working with them to help solve those problems. SEC497 draws on lessons learned over the years in OSINT to help others. The course not only covers critical OSINT tools and techniques, it also provides real-world examples of how they have been used to solve a problem or further an investigation. Hands-on labs based on actual scenarios provide students with the opportunity to practice the skills they learn and understand how those skills can help in their research.

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

With Open-Source Intelligence (OSINT) being the engine of most major investigations in this digital age, the need for a more advanced course was inevitable. The data in almost every OSINT investigation becomes more complex to collect, exploit and analyze. OSINT practitioners around the world thus need to perform OSINT at scale and to access the means and methods to verify the reliability of their analysis in order to produce sound and unbiased reports. In SEC587 you will learn how to perform advanced OSINT gathering and analysis as well as understand and use common programming languages such as JSON and Python. SEC587 also will go into Dark Web and financial (cryptocurrency) topics as well as disinformation, advanced image and video OSINT analysis. This is an advanced fast-paced course that will give seasoned OSINT investigators new techniques and methodologies and entry-level OSINT analysts the extra depth they need to find, collect and analyze data sources.

“This content is the next level for OSINT researchers. It fills in the areas that I have not been using but wanted to learn.”

—Janie Brewer, Oracle

SEC501 will help you become an effective enterprise defender by enhancing your knowledge and skills in the specific areas of network architecture defense, penetration testing, security operations, digital forensics and incident response, and malware analysis. This course is essential for members of security teams of all sizes—from smaller teams, where you wear several (or all) hats and need a robust understanding of many facets of cybersecurity, to larger teams where your role is more focused and where gaining skills in additional areas adds to your flexibility and opportunities.

This course concentrates on examining your network traffic, looking for indications of an attack, and performing penetration testing and vulnerability analysis to proactively identify problems and issues in your enterprise. When a compromise does occur—and it will—you’ll be able to eradicate it because you will have already scoped your adversaries’ activities by collecting digital artifacts of their actions and analyzing malware they have installed on your systems. You can then undertake the recovery and remediation steps that would have been pointless if your adversary had persisted on your network.

For detailed course description, visit sans.org/courses

WAYS TO TRAIN FOR SEC501

SEC503: Network Monitoring and Threat Detection In-Depth

This course delivers the technical knowledge, insight, and hands-on training you need to confidently defend your network, whether traditional or cloud-based. You will learn about the underlying theory of TCP/IP and the most used application protocols so that you can intelligently examine network traffic to identify emerging threats, perform large-scale correlation for threat hunting, and reconstruct network attacks.

For detailed course description, visit sans.org/courses

WAYS TO TRAIN FOR SEC503
SEC450: **Blue Team Fundamentals: Security Operations and Analysis**

SEC450 provides technical knowledge and key concepts essential for Security Operations Center (SOC) analysts and new cyber defense team members. By providing a detailed explanation of the mission and mindset of a modern cyber defense operation, this course will jumpstart and empower those joining the next generation of Blue Teams.

**Business Takeaways**
- Make the most of security telemetry, including endpoint, network, and cloud-based sensors
- Minimize false positives
- Quickly and accurately triage security incidents
- Improve the effectiveness, efficiency, and success of your SOC

**You Will Be Able To**
- Perform a variety of OSINT investigations while practicing good operational security
- 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.

**NICE Framework Work Roles**
- Data Analyst (OPM 422)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Target Network Analyst (OPM 132)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Intel Planner (OPM 331)
- Cyber Ops Planner (OPM 332)

---

SEC505: **Securing Windows and PowerShell Automation**

Want to block Windows attacks, thwart the lateral movement of hackers inside your LAN, and prevent administrative credential theft? And you want to have fun learning PowerShell scripting at the same time? Then SEC505 is the course for you! In SEC505 you will learn how to use PowerShell to automate Windows security and harden PowerShell itself. No prior PowerShell scripting experience is required to take the course because you will learn PowerShell along the way. We will even write a PowerShell ransomware script together in a lab in order to implement better ransomware defenses. The course author, Jason Fossen, is a Faculty Fellow who has taught defensible PowerShell at SANS for more than a decade.

**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, 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

*DoDD 8140 – IAT Level III*
*sans.org/dod/dodd-8140*

For detailed course description, visit sans.org/courses

---

WAYS TO TRAIN FOR SEC450

- **In-Person**
  - sans.org/mlp/in-person-training
- **Live Online**
  - sans.org/mlp/live-online-training
- **OnDemand**
  - sans.org/ondemand

---

WAYS TO TRAIN FOR SEC505

- **Live Online**
  - sans.org/mlp/live-online-training
- **OnDemand**
  - sans.org/ondemand

---

*DoDD 8140 – Computer Environment*
*sans.org/dod/dodd-8140*

For detailed course description, visit sans.org/courses

---

*DoDD 8140 – Computer Environment*
*sans.org/dod/dodd-8140*

For detailed course description, visit sans.org/courses
SEC511: Continuous Monitoring and Security Operation

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

NICE Framework Work Roles
- Security Architect (OPM 652)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

WAYS TO TRAIN FOR SEC511

SEC555: SIEM with Tactical Analytics

You Will Learn
- Demonstrate ways most SIEMs commonly lag current open-source solutions (e.g., ELK)
- Gain a current understanding of 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

NICE Framework Work Roles
- Network Operations Specialist (OPM 441)

WAYS TO TRAIN FOR SEC555
SEC573: **Automating Information Security with Python**

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
- Develop automated systems that process data quickly and efficiently

NICE Framework Work Roles
- Secure Software Assessor (OPM 622)
- Research & Development Specialist (OPM 661)
- Data Analyst (OPM 422)
- Cyber Defense Analyst (OPM 511)
- Cyber Operator (OPM 321)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

WAYS TO TRAIN FOR SEC573
- In-Person: sans.org/mlp/in-person-training
- Live Online: sans.org/mlp/live-online-training
- OnDemand: sans.org/ondemand

SEC586: **Security Automation with PowerShell**

You Will Learn
- PowerShell scripting fundamentals from the ground up with respect to the capabilities of PowerShell 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 to deception
- Response techniques leveraging PowerShell-based automation

Who Should Attend
- Security Operations Center analysts
- System engineers
- System administrators
- Technical security managers
- Cyber threat investigators
- Certified Network Defender analysts

For detailed course description, visit sans.org/courses

WAYS TO TRAIN FOR SEC586
- In-Person: sans.org/mlp/in-person-training
- Live Online: sans.org/mlp/live-online-training
- OnDemand: sans.org/ondemand
AUD507: Auditing Systems, Applications, and the Cloud  NEW

Performing IT security audits at the enterprise level can be an overwhelming task. It is difficult to know where to start and which controls to audit first. Audits often focus on things that are not as important, wasting precious time and resources. Management is left in the dark about the real risk to the organization’s mission. Operations staff can’t use the audit report to reproduce or remediate findings. AUD507 gives the student the tools, techniques and thought processes required to perform meaningful risk assessments and audits. Learn to use risk assessments to recommend which controls should be used and where they should be placed. Know which tools will help you focus your efforts and learn how to automate those tools for maximum effectiveness.

Business Takeaways
- Gain confidence that 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

WAYS TO TRAIN FOR AUD507

SEC566: Implementing and Auditing Security Frameworks and Controls

High-profile cybersecurity attacks indicate that offensive attacks are outperforming defensive measures. Cybersecurity engineers, auditors, privacy and compliance team members are asking how they can practically protect and defend their systems and data and how they should implement a prioritized list of cybersecurity hygiene controls. In SEC566, you will learn how an organization can defend its information by using vetted cybersecurity frameworks and standards. You will specifically learn how to navigate security control requirements defined by the Center for Internet Security’s (CIS) Controls (v7.1/8.0), the NIST Cybersecurity Framework (CSF), the Cybersecurity Maturity Model Certification (CMMC), NIST SP 800-171, ISO/I EC 27000, and other frameworks into a cohesive strategy to defend your organization while complying with industry standards.

Business Takeaways
- Maximize the time of compliance analysts in mapping frameworks by learning a comprehensive controls matrix
- Reduce duplicate efforts of administrators implementing cybersecurity controls from different standards and frameworks
- Enjoy peace of mind that your organization has a comprehensive strategy for defense and compliance

WAYS TO TRAIN FOR SEC566
MGT512: Security Leadership Essentials for Managers

Security leaders need both technical knowledge and leadership skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics. This course empowers you to become an effective security leader and get up to speed quickly on information security issues and terminology. You won’t just learn about security, you will also learn how to lead security teams and manage programs by playing through 23 Cyber42 activities throughout the class, approximately 60–80 minutes daily.

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

Syllabus Summary
SECTION 1: Building Your Security Program
SECTION 2: Technical Security Architecture
SECTION 3: Security Engineering
SECTION 4: Security Management and Leadership
SECTION 5: Detecting and Responding to Attacks

“II’m really enjoying the flow between the content delivery and the Cyber42 game.”
—Jamil A., U.S. Government

“Course was amazing. Such valuable information in a great crash course of security leadership.”
—Ian D., U.S. Government

WAYS TO TRAIN FOR MGT512

In-Person
sans.org/mlp/in-person-training

Live Online
sans.org/mlp/live-online-training

OnDemand
sans.org/ondemand

For detailed course description, visit sans.org/courses
**MGT414: SANS Training Program for the CISSP® Certification**

**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

**Who Should Attend**
- Security professionals who want to understand the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® domains
- Security professionals and managers looking for practical ways to apply the eight domains of knowledge to their current activities

**Need training for the CISSP® exam?**
SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

The course 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.

**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. I challenge you to attend the SANS CISSP® training course and find the exciting aspect of the eight domains of knowledge!"

—Eric Conrad and Seth Misener

**Syllabus Summary**

**SECTION 1:** Introduction, Security, and Risk Management

**SECTION 2:** Asset Security and Security Engineering (Part 1)

**SECTION 3:** Security Engineering (Part 2): Communication and Network Security

**SECTION 4:** Identity and Access Management (IAM)

**SECTION 5:** Security Assessment and Testing; Security Operations

**SECTION 6:** Software Development Security

**“This class focuses like a laser on the key concepts you will need to understand for the CISSP® exam. Do not struggle with thousand-page textbooks. Let this course be your guide!”**

—Carl Williams, Harris Corporation

**“I have taken several CISSP® prep courses in the last several years and this by far is the best. Finally I feel that I have the confidence to take the test. Thanks.”**

—Jerry Carse, Sarum, LLC

**WAYS TO TRAIN FOR MGT414**

- In-Person: [sans.org/mlp/in-person-training](sans.org/mlp/in-person-training)
- Live Online: [sans.org/mlp/live-online-training](sans.org/mlp/live-online-training)
- OnDemand: [sans.org/ondemand](sans.org/ondemand)
The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. However, creating a security strategy and executing a plan that includes sound policy coupled with top-notch leadership is hard for IT and security professionals because we spend so much time responding and reacting. We almost never do strategic planning until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack. This information security course will provide you with the tools to build a cybersecurity strategic plan and an entire IT security policy and lead your teams in the execution of your plan and policy. By the end of class you will have prepared an executive presentation, read three business case studies, responded to issues faced by four fictional companies, analyzed 15 case scenarios, and responded to 15 Cyber42 events.

Business Takeaways

- Create a security plan that resonates with customers
- Develop leaders who know how to align cybersecurity with business objectives
- Build higher-performing security teams

Syllabus Summary

SECTION 1: Strategic Planning Foundations
SECTION 2: Strategic Roadmap Development
SECTION 3: Security Policy Development and Assessment
SECTION 4: Leadership and Management Competencies
SECTION 5: Strategic Planning Workshop

“"I enjoy the use of Cyber 42. I particularly enjoyed the extra addition of going through the answers and discussing which answers had what effects on everyone’s scores.””

—Alexander Walker, TechVets

“I wish I had taken this course 10 years ago when I first started in my role as a CISO. The work group discussions, tools, and theory are practical and applicable to my day-to-day work.”

—Mark Potter, NewWave
MGT516: **Building and Leading Vulnerability Management Programs**

**You Will Be Able To**
- Create, implement, and mature your vulnerability management program and get buy-in from your stakeholders
- Utilize techniques to build and maintain an accurate and useful inventory of IT assets in the enterprise and the cloud
- Determine what processes and technologies are effective across both infrastructure and applications and how to configure them appropriately
- Recognize which common false positives or false negatives to be aware of 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

**NICE Framework Work Roles**
- Security Control Assessor (OPM 612)
- Vulnerability Assessment Analyst (OPM 541)

For detailed course description, visit [sans.org/courses](https://sans.org/courses)

---

MGT521: **Leading Cybersecurity Change: Building a Security-Based Culture**

Cybersecurity leadership is no longer just about technology. It is ultimately about organizational change—change not only in how people think about cybersecurity but in what they prioritize and how they act, throughout every corner of the organization. Students will learn how to build, manage, and measure a strong cybersecurity culture by leveraging the latest in organizational change models and real-world lessons learned. In addition, students will apply everything they learn through a series of 16 interactive labs and case studies.

**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 use tools that implement controls through automation
- Create a scoring tool to measure the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Competently map critical controls to standards such as the NIST Cybersecurity Framework, NIST SP 800-171, the CMMC, and more

**NICE Framework Work Role**
- Security Control Assessor (SP-RSK-002)

For detailed course description, visit [sans.org/courses](https://sans.org/courses)
Information technology is so tightly woven into the fabric of modern business that cyber risk has become business risk. Security Operations Center (SOC) teams are facing more pressure than ever before to help manage this risk by identifying and responding to threats across a diverse set of infrastructures, business processes, and users. Furthermore, SOC managers are in the unique position of having to bridge the gap between business processes and the highly technical work that goes on in the SOC. MGT551 students will learn how to design their defenses around their unique organizational requirements and risk profile. We will give you the tools to build an intelligence-driven defense, measure progress towards your goals, and develop more advanced processes like threat hunting, active defense, and continuous SOC assessment.

**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
- Effective management and leadership techniques for technical teams
- Practical approaches to optimizing security operations that can be applied immediately

**P协调 slightly from the original document.**

**Syllabus Summary**
- **SECTION 1:** SOC Design and Operational Planning
- **SECTION 2:** SOC Telemetry and Analysis
- **SECTION 3:** Attack Detection, Hunting, and Triage
- **SECTION 4:** Incident Response
- **SECTION 5:** Metrics, Automation, and Continuous Improvement

“The exercises, while mostly non-technical, triggered the thinking process to ensure that all aspects for the building of a SOC are in place.”

—Wee Hian Peck, INTfinity Consulting PL

“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
FOR500 builds comprehensive digital forensics knowledge of Microsoft Windows operating systems that provides the means to recover, analyze, and authenticate forensic data, track user activity on the network, and organize findings for use in incident response, internal investigations, intellectual property theft inquiries, and civil or criminal litigation. This knowledge can be used to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Detailed and real-world exercises teach the tools and techniques that every investigator should employ step-by-step to solve a forensic case. The course is newly updated to cover all Windows versions through Windows 11!

Business Takeaways
- Build an in-house digital forensic capability that can rapidly answer important business questions and investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions.
- Enable more capable analysts, threat hunters, and incident response team members who can use deep-dive digital forensics to help solve Windows data breach cases, perform damage assessments, and develop indicators of compromise.
- Understand the wealth of telemetry available in the Windows Enterprise, at the endpoint and in cloud resources like Microsoft 365, Exchange, Unified Audit Logs, cloud storage, and chat clients.
- 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 documenting 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.

Who Should Attend
- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics who has a background in information systems, information security, and computers

NICE Framework Work Roles
- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)

Syllabus Summary
SECTION 1: Digital Forensics and Advanced Data Triage
SECTION 2: Registry Analysis, Application Execution, and Cloud Storage Forensics
SECTION 3: Shell Items and Removable Device Profiling
SECTION 4: Email Analysis, Windows Search Index, SRUM, and Event Logs
SECTION 5: Web Browser Forensics
SECTION 6: Windows Forensics Challenge

“Best forensics class I have had yet (and pretty much the only one that gives you some sort of framework on HOW to attack an exam).”
—Juan M.
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

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. The key is to constantly look for attacks that get past security systems and to catch intrusions in progress, rather than after attackers have completed their objectives and done worse damage to the organization. For the incident responder, this process is known as “threat hunting.” FOR508 teaches advanced skills to hunt, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivists.

Business Takeaways
- Understand attacker tradecraft to perform proactive compromise assessments
- Upgrade detection capabilities via a better understanding of novel attack techniques, a 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

Syllabus Summary
SECTION 1: Advanced Incident Response & Threat Hunting
SECTION 2: Intrusion Analysis
SECTION 3: Memory Forensics in Incident Response & Threat Hunting
SECTION 4: Timeline Analysis
SECTION 5: Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics Detection
SECTION 6: The APT Threat Group Incident Response Challenge

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

Who Should Attend
- Incident response team members
- Threat hunters
- Security Operations Center analysts
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement personnel
- Red Team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates looking to take their skills to the next level

NICE Framework Work Roles
- Cyber Defense Incident Responder (OPM 531)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

“I have been doing digital forensics for 13+ years. This course has still managed to build on my existing knowledge and made me challenge some pre-conceptions. It has given me tons of ideas to take home and develop to improve our enterprise’s security posture.”
—Ian Howard, Tesco

For detailed course description, visit sans.org/courses
The world is changing, and so is the data we need to conduct our investigations. Cloud platforms change how data is stored and accessed, removing the examiner’s ability to directly access systems and use classical data extraction methods. Unfortunately, many examiners are still trying to force old methods for on-premise examination onto cloud-hosted platforms. Rather than resisting change, examiners must learn to embrace the new opportunities presented to them in the form of new evidence sources. FOR509: Enterprise Cloud Forensics and Incident Response addresses today’s need to bring examiners up to speed with the rapidly changing world of enterprise cloud environments by uncovering the new evidence sources that only exist in the cloud.

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

Syllabus Summary

SECTION 1: Microsoft 365 and Graph API
SECTION 2: Microsoft Azure
SECTION 3: Amazon Web Services (AWS)
SECTION 4: Google Workspace
SECTION 5: Google Cloud
SECTION 6: Multi-Cloud Intrusion Challenge

“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

“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
Cyber threat intelligence represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary’s tool, but the real threat is the human one. Cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders. During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. FOR578: Cyber Threat Intelligence will train you and your team in the tactical, operational, and strategic cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

**Business Takeaways**

- Understand the everchanging cyber threat landscape and what it means for your organization
- Practice analytic techniques to inform key business leaders how to most effectively defend themselves and the organization against targeted threats
- Identify cost-effective ways to leverage open-source and community threat intelligence tools, and establish familiarity with some of the most impactful commercial tools available
- Effectively communicate threat intelligence at tactical, operational, and strategic levels
- Become a force multiplier for other core business functions, including security operations, incident response, and business operations

**Who Should Attend**

- Security practitioners
- Incident response team members
- Threat hunters
- Security Operations Center personnel and information security practitioners
- Digital forensic analysts and malware analysts
- Federal agents and law enforcement officials
- Technical managers
- SANS alumni looking to take their analytical skills to the next level

**NICE Framework Work Roles**

- Data Analyst (OPM 422)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Incident Responder (OPM 531)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Mission Assessment Specialist (OPM 112)
- Target Network Analyst (OPM 132)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Intel Planner (OPM 331)
- Partner Integration Planner (OPM 333)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)

**Syllabus Summary**

**SECTION 1: Cyber Threat Intelligence and Requirements**

**SECTION 2: The Fundamental Skillset: Intrusion Analysis**

**SECTION 3: Collection Sources**

**SECTION 4: Analysis and Production of Intelligence**

**SECTION 5: Dissemination and Attribution**

**SECTION 6: Capstone**

“Threat intelligence analysis has been an art for too long, now it can finally become a science at SANS. [Course authors] Mike Cloppert and Robert M. Lee are the industry ‘greybeards’ who have seen it all. They are the thought leaders who should be shaping practitioners for years to come.”

—Rich Barger, ThreatConnect

For detailed course description, visit sans.org/courses
Learn to turn malware inside out! This popular 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.

**Business Takeaways**
- Empower your internal teams to perform analysis in-house to lower the need for external expertise
- Expand your team’s analysis capabilities to offer more value to your internal or external stakeholders
- Increase the efficiency of your analysis tasks, so you can provide valuable insights faster
- Minimize the scope and cost of the potential intrusion by responding to security incidents more quickly

**Syllabus Summary**

**SECTION 1:** Malware Analysis Fundamentals
**SECTION 2:** Reversing Malicious Code
**SECTION 3:** Analyzing Malicious Documents
**SECTION 4:** In-Depth Malware Analysis
**SECTION 5:** Examining Self-Defending Malware
**SECTION 6:** Malware Analysis Tournament

“**I learned a great amount of valuable information in FOR610, including what areas I need to master for my job. The CTF lab was a wake up call regarding how much I don’t know, so thank you!”**

—Urban M., CNF Technologies

“**This course has helped me improve my knowledge of malware techniques and understand how to better protect assets and successfully complete the eradication steps.”**

—Eric B., Nestle
FOR518: Mac and iOS Forensic Analysis and Incident Response

FOR518 provides the necessary skills to identify the many and varied data storage mediums in use today, and to collect and preserve this data in a forensically sound manner despite how and where it may be stored. The course covers digital acquisition from computers to portable devices, networks, and the cloud. It then teaches the student rapid triage, or the art and science of identifying and starting to extract actionable intelligence from a hard drive in 90 minutes or less.

Who Should Attend
- Federal agents and law enforcement personnel
- First responders
- Digital forensic analysts
- Information security professionals
- Incident response team members
- Media exploitation analysts
- Department of Defense and intelligence community professionals
- Anyone interested in an understanding of the proper preservation of systems and who has a background in information systems, information security, and computers

WAYS TO TRAIN FOR FOR518

In-Person | sans.org/mlp/in-person-training
Live Online | sans.org/mlp/live-online-training
OnDemand | sans.org/ondemand

FOR518 is the first non-vendor-based Mac and iOS incident response and forensics course that focuses on the raw data, in-depth detailed analysis, and how to get the most out of their Mac and iOS cases. 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.

WAYS TO TRAIN FOR FOR518

In-Person | sans.org/mlp/in-person-training
Live Online | sans.org/mlp/live-online-training
OnDemand | sans.org/ondemand

For detailed course description, visit sans.org/courses
### FOR572: Advanced Network Forensics: Threat Hunting, Analysis & Incident Response

**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 recent 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

**Who Should Attend**
- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Security Operations Center personnel and information security practitioners
- Network defenders
- Information security managers
- Network engineers
- Information technology professionals
- Anyone interested in computer network intrusions and investigations

---

### FOR585: Smartphone Forensic Analysis In-Depth

**You Will Be Able To**
- Select the best 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 where the evidence went on the mobile device—so if the user created the date, 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

**NICE Framework Work Roles**
- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)

---

**WAYS TO TRAIN FOR FOR572**
- **In-Person**
  - sans.org/mlp/in-person-training
- **Live Online**
  - sans.org/mlp/live-online-training
- **OnDemand**
  - sans.org/ondemand

**WAYS TO TRAIN FOR FOR585**
- **In-Person**
  - sans.org/mlp/in-person-training
- **Live Online**
  - sans.org/mlp/live-online-training
- **OnDemand**
  - sans.org/ondemand
FOR710: Reverse-Engineering Malware: Advanced Code Analysis  

FOR710 prepares malware specialists to dissect sophisticated Windows executables, such as those that dominate the headlines and preoccupy incident response teams across the globe. 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.

You Will Be Able 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 to debug and assess 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

Business Takeaways
- Reduce the financial and reputational impact of a breach by more efficiently and precisely managing the response
- Learn incident response 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 to respond to compromised Linux and macOS systems
- Be able to respond to and analyze containerized microservices such as Docker containers

Who Should Attend
- Cyber security professionals
- Reverse engineers

NICE Framework Work Roles
- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/Counter Intelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

For detailed course description, visit sans.org/courses
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 is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

Author Statement

“Critical infrastructure organization and industrial control system security practitioners cannot lose sight of what makes them special. There is a need for unique hybrid skill sets in this space that intersects operations, engineering, technology, security, and safety. It is crucial for an organization that these unique skill sets be developed and harnessed in a way that recognizes the operational drivers and constraints of the process environment and technology used to control it. IT and OT are different and the ICS community needs to focus on the unique demands that are represented by the first letter in those acronyms and leverage the second letter in a manner that is informed by the risks to the organization and the overall mission.”
—Tim Conway, ICS Curriculum Director

Syllabus Summary

SECTION 1: ICS Overview
SECTION 2: Architectures and Field Devices
SECTION 3: Communications and Protocols
SECTION 4: Supervisory Systems
SECTION 5: ICS Security Governance
SECTION 6: Capstone Exercise

“‘A mix of a hands-on and theoretical class, being driven by a highly skilled instructor, makes this the best training in ICS security.”
—Rafael Issa, Technip

“The real-world, practical examples paired with an instructor who clearly knew the subject matter inside and out made this course invaluable.”
—Theresa Hanks, Booz Allen Hamilton
ICS515: ICS Visibility, Detection, and Response

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. Note: This class was previously named ICS515: ICS Active Defense and Incident Response. The course has gone through a significant update changing much of the content, most of the labs, and adding a day in course length.

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

Hands-On Training
- Build a Programmable Logic Controller using the SANS ICS515 Student Kit
- Identify information available about assets online through Shodan
- Complete an analysis of competing hypotheses
- Ingest threat intelligence reports
- Identify and leverage new active defense skills to guide incident responders to the Human Machine Interface (HMI) affected by an advanced persistent threat (APT) on the lab network
- Identify which system is affected by APT malware identified in the network and assemble a sample of the threat that can be analyzed
- From the infected HMI and samples of the APT malware identified, analyze the malware, extract information, and develop YARA rules to complete the active defense
- Address three different hands-on, real-world scenarios, one involving live data collected from an intrusion into the SANS ICS515 Student Kit, and the other involving data collected from a Distributed Control System infected with malware

Syllabus Summary
SECTION 1: ICS Cyber Threat Intelligence
SECTION 2: Visibility and Asset Identification
SECTION 3: ICS Threat Detection
SECTION 4: Incident Response
SECTION 5: Threat and Environment Manipulation
SECTION 6: Capstone Day, Under Attack!

“For 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

WAYS TO TRAIN FOR ICS515

For detailed course description, visit sans.org/courses

In-Person
sans.org/mlp/in-person-training

Live Online
sans.org/mlp/live-online-training

OnDemand
sans.org/ondemand
ICS456: Essentials for NERC Critical Infrastructure Protection

The ICS456 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 to identify and categorize BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations.

Who Should Attend
- IT and OT (ICS) cybersecurity
- Field support personnel
- Security operations
- Incident response
- Compliance staff
- Team leaders
- Governance
- Vendors/Integrators
- Auditors

You Will Be Able To
- Understand the cybersecurity objectives of the NERC 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 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

WAYS TO TRAIN FOR ICS456
- In-Person: sans.org/mlp/in-person-training
- Live Online: sans.org/mlp/live-online-training
- OnDemand: sans.org/ondemand

For detailed course description, visit sans.org/courses

ICS612: ICS Cybersecurity In-Depth

ICS612 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.

Who Should Attend
- ICS410 alumni – Students who have successfully completed ICS410: ICS/SCADA Security Essentials will have the base knowledge considered as a prerequisite for this course.
- Process control engineers
- Systems or safety system engineers
- Active defenders in ICS
- Anyone with significant control system experience interested in understanding processes and methods to secure the ICS environment

You Will Be Able To
- Use 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

WAYS TO TRAIN FOR ICS612
- In-Person: sans.org/mlp/in-person-training

For detailed course description, visit sans.org/courses
SEC504: **Hacker Tools, Techniques, and Incident Handling**

SEC504 helps you develop the skills to conduct incident response investigations. You will learn how to apply a dynamic incident response process to evolving cyber threats and how to develop threat intelligence to mount effective defense strategies for cloud and on-premise platforms. We'll examine the latest threats to organizations, from watering hole attacks to cloud application service multi-factor authentication bypass, enabling you to get into the mindset of attackers and anticipate their moves. SEC504 gives you the information you need to understand how attackers scan, exploit, pivot, and establish persistence in cloud and conventional systems. To help you develop retention and long-term recall of the course material, 50 percent of class time is spent on hands-on exercises, using visual association tools to break down complex topics. This course will boost your career by giving you the in-demand skills needed to conduct cyber investigations and utilize threat intelligence.

**Business Takeaways**
- Apply a dynamic approach to incident response
- Identify threats using host, network, and log analysis
- Best practices for effective cloud incident response
- Leverage PowerShell for data collection and cyber threat analysis
- Cyber investigation processes using live analysis, network insight, and memory forensics
- Defense spotlight strategies to protect critical assets
- How attackers leverage cloud systems against organizations
- 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
- How attackers exploit publicly accessible systems including Microsoft 36

**Syllabus Summary**

**SECTION 1:** Incident Response and Cyber Investigations

**SECTION 2:** Recon, Scanning, and Enumeration Attacks

**SECTION 3:** Password and Access Attacks

**SECTION 4:** Public-Facing and Drive-By Attacks

**SECTION 5:** Evasion and Post-Exploitation Attacks

**SECTION 6:** Capture-the-Flag Event

---

For detailed course description, visit [sans.org/courses](http://sans.org/courses)
SEC542: Web App Penetration Testing and Ethical Hacking

SEC542 enables students to assess a web application’s security posture and convincingly demonstrate the business impact should attackers exploit the discovered vulnerabilities. You will practice the art of exploiting web applications to find flaws in your enterprise’s web apps. You’ll learn about the attacker’s tools and methods and, through detailed hands-on exercises, you will learn a best practice process for web application penetration testing, inject SQL into back-end databases to learn how attackers exfiltrate sensitive data, and utilize cross-site scripting attacks to dominate a target infrastructure.

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

Syllabus Summary
SECTION 1: Introduction and Information Gathering
SECTION 2: Content Discovery, Authentication, and Session Testing
SECTION 3: Injection
SECTION 4: XSS, SSRF, and XXE
SECTION 5: CSRF, Logic Flaws, and Advanced Tools
SECTION 6: Capture the Flag

Who Should Attend
- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers, architects, and developers

NICE Framework Work Roles
- Security Control Assessor (OPM 612)
- Software Developer (OPM 621)
- Secure Software Assessor (OPM 622)
- System Testing and Evaluation Specialist (OPM 671)
- Information Systems Security Developer (OPM 631)
- Systems Developer (OPM 632)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Exploitation Analyst (OPM 121)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)

“SEC542 provides rapid exposure to a variety of tools and techniques invaluable to recon on a target site.”
—Gareth Grindle, QA Ltd.

“Sec542 taught me to truly focus on the methodology while performing a pen test. During the capture-the-flag event, I realized how much time can be wasted if you fail to respect your methodology.”
—Sean Rosado, RavenEye

For detailed course description, visit sans.org/courses

WAYS TO TRAIN FOR SEC542

In-Person
sans.org/mlp/in-person-training

Live Online
sans.org/mlp/live-online-training

OnDemand
sans.org/ondemand
SEC560: Enterprise Penetration Testing

SEC560 prepares you to conduct successful penetration testing for a modern enterprise, including on-premise systems, Azure, and Azure AD. You will learn the methodology and techniques used by real-world penetration testers in large organizations to identify and exploit vulnerabilities at scale and show real business risk to your organization. The course material is complemented with more than 30 practical lab exercises concluding with an intensive, hands-on Capture-the-Flag exercise in which you will conduct a penetration test against a sample target organization and demonstrate the knowledge you have mastered.

Business Takeaways

- Gain in-depth technical excellence and learn industry-leading methodologies to conduct high-value penetration tests
- Learn in-depth about the arsenal of tools with numerous hands-on exercises that show subtle, less-well-known, and undocumented features that are useful for professional penetration testers and ethical hackers
- Learn how the tools interrelate with each other in an overall testing process. Rather than just throwing up a bunch of tools and playing with them, we analyze how to leverage information from one tool to get the biggest bang out of the next tool
- Focus on the workflow of professional penetration testers and ethical hackers, proceeding step by step and discussing the most effective means for carrying out projects
- Learn about common pitfalls that arise in penetration tests and ethical hacking projects, with real-world strategies and tactics to avoid these problems and maximize the quality of test results
- Learn time-saving tactics based on years of in-the-trenches experience of real penetration testers and ethical hackers. There are tasks that might take hours or days unless you know the little secrets we cover that enable you to surmount a problem in minutes
- Understand the mindset of successful penetration testers and ethical hackers, which involves balancing the often-contravening forces of thinking outside the box, methodically trouble-shooting, carefully weighing risks, following a time-tested process, painstakingly documenting results, and creating a high-quality final report that gets management and technical buy-in
- Understand how penetration testing and ethical hacking should fit into a comprehensive enterprise information security program
- Focus on pen testing modern organizations, many of which are using Azure AD for identity management

Syllabus Summary

SECTION 1: Comprehensive Pen Test Planning, Scoping, and Recon

SECTION 2: In-Depth Scanning and Initial Access

SECTION 3: Assumed Breach, Post-Exploitation, and Passwords

SECTION 4: Lateral Movement and Command and Control (C2)

SECTION 5: Domain Domination and Azure Annihilation

SECTION 6: Penetration Test and Capture-the-Flag Exercise

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

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red Team members
- Blue Team members
- Forensics specialists who want to better understand offensive tactics
- Incident responders who want to understand the mindset of an attacker

NICE Framework Work Roles

- Security Control Assessor (OPM 612)
- System Testing and Evaluation Specialist (OPM 671)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Exploitation Analyst (OPM 121)
- Mission Assessment Specialist (OPM 112)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Cyber Operator (OPM 321)
SEC588: Cloud Penetration Testing

SEC588 will equip you with the latest cloud-focused penetration testing techniques and teach you how to assess cloud environments. The course dives into topics like cloud-based microservices, in-memory data stores, serverless functions, Kubernetes meshes, and containers. It also looks at how to identify and test cloud-first and cloud-native applications. You will also learn specific tactics for penetration testing in Azure and Amazon Web Services, particularly important given that Microsoft and AWS account for more than half the market. It is one thing to assess and secure a data center, but it takes a specialized skill set to evaluate and report on the risks to an organization if its cloud services are left insecure.

### Business Takeaways
- Learn how to assess and test cloud environments through real-world cloud-based labs
- Understand the differences between cloud-native, multi-cloud, and cloud hybrid infrastructures
- Penetration testing on real-world microservices
- Understand how containers and CI/CD Pipelines are abused
- Attack Kubernetes, Serverless Functions, and Windows Containers
- Understand how identity systems work in the cloud and how to attack them

### Syllabus Summary
- **SECTION 1:** Architecture, Discovery, and Recon at Scale
- **SECTION 2:** Attacking Identity Systems
- **SECTION 3:** Attacking and Abusing Cloud Services
- **SECTION 4:** Vulnerabilities in Cloud-Native Applications
- **SECTION 5:** Infrastructure Attacks and Red Teaming
- **SECTION 6:** Capstone Event

“SEC588 taught me crucial information needed before putting data in a cloud.”
—Maria Lopez, NVCC

“This emerging course perfectly complements the change in the direction of red team engagement scopes.”
—Kyle Spaziani, Sanofi

For detailed course description, visit sans.org/courses
**SEC460: Enterprise and Cloud | Threat and Vulnerability Assessment**

SEC460 will help you build your technical vulnerability assessment skills and techniques using time-tested, practical approaches to ensure true value across the enterprise. Throughout the course you will use real industry-standard security tools for vulnerability assessment, management, and mitigation; learn a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise; and practice 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 and gives you a tour of attackers’ perspectives that is crucial to discovering where they will strike.

**Who Should Attend**
- Vulnerability assessors
- IT system administrators
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers

**WAYS TO TRAIN FOR SEC460**
- **In-Person**
  - [sans.org/mlp/in-person-training](https://sans.org/mlp/in-person-training)
- **Live Online**
  - [sans.org/mlp/live-online-training](https://sans.org/mlp/live-online-training)
- **OnDemand**
  - [sans.org/ondemand](https://sans.org/ondemand)

For detailed course description, visit [sans.org/courses](https://sans.org/courses)

---

**SEC575: Mobile Device Security and Ethical Hacking  **

SEC575 will prepare you to effectively evaluate the security of mobile devices, assess and identify flaws in mobile applications, and conduct a mobile device penetration test, which are all critical skills required to protect and defend mobile device deployments. You will learn how to pen test the biggest attack surface in your organization; dive deep into evaluating mobile apps and operating systems and their associated infrastructure; and better defend your organization against the onslaught of mobile device attacks.

**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

**WAYS TO TRAIN FOR SEC575**
- **In-Person**
  - [sans.org/mlp/in-person-training](https://sans.org/mlp/in-person-training)
- **Live Online**
  - [sans.org/mlp/live-online-training](https://sans.org/mlp/live-online-training)
- **OnDemand**
  - [sans.org/ondemand](https://sans.org/ondemand)

For detailed course description, visit [sans.org/courses](https://sans.org/courses)
SEC617: Wireless Penetration Testing and Ethical Hacking

SEC617 will give you the skills you need to understand the security strengths and weaknesses in wireless systems. In this course, you will learn how to evaluate the ever-present cacophony of Wi-Fi networks and identify the Wi-Fi access points and client devices that threaten your organization; assess, attack, and exploit deficiencies in modern Wi-Fi deployments using WPA2 technology, including sophisticated WPA2-Enterprise networks; use your understanding of the many weaknesses in Wi-Fi protocols and apply it to modern wireless systems; and identify and attack Wi-Fi access points and exploit the behavioral differences in how client devices scan for, identify, and select access points.

Who Should Attend
- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision-makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

For detailed course description, visit sans.org/courses

WAYS TO TRAIN FOR SEC617
- Live Online: sans.org/mlp/live-online-training
- In-Person: sans.org/mlp/in-person-training
- OnDemand: sans.org/ondemand

6 Day Program  |  36 CPEs  |  24+ Labs

CURRICULUM: Offensive Operations

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

SEC599 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 through a Purple Team strategy.

Business Takeaways
- 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

Syllabus Summary
- SECTION 1: Introduction and Reconnaissance
- SECTION 2: Payload Delivery and Execution
- SECTION 3: Exploitation, Persistence, and Command and Control
- SECTION 4: Lateral Movement
- SECTION 5: Action on Objectives, Threat Hunting, and Incident Response
- SECTION 6: APT Defender Capstone

You Will Be Able To
- Use MITRE ATT&CK Navigator to assess different techniques
- Leverage MITRE ATT&CK as a “common language” in the organization
- Build your own Cuckoo sandbox solution to analyze payloads
- Develop effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlight key bypass strategies for script controls (Unmanaged Powershell, AMSI bypasses, etc.)
- Stop 0-day exploits using ExploitGuard and application whitelisting
- Highlight key bypass strategies in application whitelisting (focus on AppLocker)

NICE Framework Work Roles
- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Partner Integration Planner (OPM 333)

Ways To Train For SEC599
- In-Person: sans.org/mlp/in-person-training
- Live Online: sans.org/mlp/live-online-training
- OnDemand: sans.org/ondemand

For detailed course description, visit sans.org/courses

6 Day Program  |  36 CPEs  |  24+ Labs

WAYS TO TRAIN FOR SEC599
- In-Person: sans.org/mlp/in-person-training
- Live Online: sans.org/mlp/live-online-training
- OnDemand: sans.org/ondemand

CURRICULUM: Offensive Operations

SEC599:

GAWN: Assessing and Auditing Wireless Networks

GAWN

GDAT: Defending Advanced Threats

GDAT

For detailed course description, visit sans.org/courses
SEC660: Advanced Penetration Testing, Exploit Writing & Ethical Hacking

**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

**Business Takeaways**
- Perform penetration testing safely against network devices such as routers, switches, and NAC implementations
- Test cryptographic implementations
- Leverage an unprivileged foothold for post-exploitation and escalation
- Understand and utilize fuzz network and stand-alone applications
- Write exploits against applications running on Linux and Windows systems
- Bypass exploit mitigations such as ASLR, DEP, and stack canaries

**WAYS TO TRAIN FOR SEC660**

![In-Person](sans.org/mlp/in-person-training)
![Live Online](sans.org/mlp/live-online-training)
![OnDemand](sans.org/ondemand)

For detailed course description, visit sans.org/courses

---

SEC760: Advanced Exploit Development for Penetration Testers

**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
- Reverse engineer and exploit Windows kernel drivers

**Who Should Attend**
- Senior network and system penetration testers with exploit development experience
- Secure application developers (C and C++)
- Reverse-engineering professionals
- Senior incident handlers with exploit development experience
- Senior threat analysts with exploit development experience
- Vulnerability researchers
- Security researchers

**WAYS TO TRAIN FOR SEC760**

![In-Person](sans.org/mlp/in-person-training)
![Live Online](sans.org/mlp/live-online-training)
![OnDemand](sans.org/ondemand)

For detailed course description, visit sans.org/courses
Backed by proven learning principles, SANS Security Awareness programs combine content from hundreds of the world’s best cybersecurity practitioners, awareness professionals, and learning behavior specialists to create dynamic programs that engage and educate participants, empowering them to recognize and prevent cyberattacks.

**Support Every Employee in the Pursuit of Managing Human Risk**

Culturally relevant, effective, and easy to implement, EndUser training delivers the reinforcement required to mature any awareness program. When supplemented with our robust phishing platform, EndUser training teaches organizations a comprehensive, data-driven approach to managing their unique levels of human risk.

<table>
<thead>
<tr>
<th>EndUser Training</th>
<th>Delivering customizable, expert-authored security awareness training with a focus on measurable outcomes for organizations to develop a culture of security and manage human risk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Simulation</td>
<td>Expertly curated phishing simulations enable you to discover where risk exists, promote safe email practices, and deliver just-in-time training when and where appropriate.</td>
</tr>
</tbody>
</table>

**Upskill Technical Teams with Role-focused Security Training**

Modular training delivered on a continual basis offers timely, relevant content on current cyber hazards. SANS Security Awareness technical training modules are segmented into small, learnable components to increase engagement and knowledge retention.

<table>
<thead>
<tr>
<th>IT Administrator Training</th>
<th>Twelve modules highlighting real-world attack and mitigation scenarios enable learners to progress along an increasingly complex training path that includes topics such as attack mitigation technologies, supply chain attacks, and security program management, among others.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developer Training</td>
<td>Role-targeted secure code training delivered as an engaging mix of video-based and interactive exercises covering OWASP Top-10 vulnerabilities, mobile app security, threat awareness, and more.</td>
</tr>
<tr>
<td>Industrial Control System (ICS) Training</td>
<td>One-of-a-kind training built exclusively around protecting critical infrastructure and delivered through 12 modules that provide a progressive and engaging learning path.</td>
</tr>
</tbody>
</table>

Visit sans.org/awareness to learn more.
DISCOVER
THE BEST
COLLEGE IN
CYBERSECURITY

BACHELOR’S & MASTER’S DEGREES | UNDERGRADUATE & GRADUATE CERTIFICATES

SPRING 2022 NATIONAL CYBER LEAGUE CHAMPIONS
#1 Individual Player – #1 Team – #1 Power Ranking

Find out if the SANS course you’re interested in could count toward a certificate or degree.

Email info@sans.edu or call 301.241.7665

SANS.edu
82% of organizations prefer hiring candidates with certifications, and GIAC certifications are listed as preferred qualifications on thousands of cybersecurity job postings around the world.

Earning a GIAC certification proves you have the specific skills employers need to ensure enterprise security. Our hands-on practical testing, CyberLive, takes skill verification even further, signaling to employers that you have critical skill mastery.

Learn more at GIAC.ORG
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 advance their own capabilities.

SANS Faculty at a Glance

120+ 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
SANS instructors have created more than 150 open-source cybersecurity tools. List of tools available at sans.org/free.

3,500+ Free 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 SANS Certified Instructor.

Your success is their goal, and we promise that you will be able to apply what you learn from them as soon as you return to work.

Meet the SANS faculty: sans.org/instructors
SANS Summits
YOUR Community –
Working TOGETHER to Solve
Cybersecurity Challenges TODAY

CUTTING-EDGE CONTENT
NEVER-BEFORE-SEEN RESEARCH
SOLUTIONS YOU CAN USE

Online Free for the Global Community
OR
In-Person with Exclusive Benefits

Upcoming Cybersecurity Summits

• Cyber Threat Intelligence
• Neurodiversity in Cybersecurity
• Cybersecurity Leadership
• ICS Security
• Small Business Cyber
• AI Cybersecurity
• Blue Team
• Digital Forensics & Incident Response (DFIR)

• SANS Security Awareness: Managing Human Risk
• Ransomware
• Open-Source Intelligence (OSINT)
• Energy Cybersecurity
• CloudSecNext
• HackFest
• Blockchain
• New2Cyber

“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

“I've managed to learn something I didn’t know from nearly every session, and I've been made aware of additional tools or methodologies that will help.”
— Dallas M., PepsiCo

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.
Stay Sharp with 1–3 Day Courses
Live Online

SANS Stay Sharp Courses Offer You:

- Instructor-led training taught by the world’s leading cybersecurity professionals
- Targeted short courses to help you build specific technical knowledge and skills
- Quality training with less time away from work and home responsibilities
- Practical training you can start using the same week you take your course
- Virtual, livestream training delivered Live Online

“This training supercharges the skills that I need for my position. Rather than spending three months learning on the job, I can take a SANS course and be ready to jump into the work.”
— Bryan G., Federal Reserve System

SANS Stay Sharp Courses

MGT433: Managing Human Risk NEW
MGT433 enables organizations to effectively manage and measure their human risk by changing people's behavior and building a strong security culture.

MGT415: A Practical Introduction to Cyber Security Risk Management
MGT415 provides students with an introduction to thinking practically about risk management and teaches the skills necessary to perform risk assessments.

MGT520: Leading Cloud Security Design and Implementation
MGT520 provides the information security leader’s need to drive a secure cloud model and leapfrog on security to leverage the security capabilities in the cloud.

MGT553: Cyber Incident Management NEW
MGT553 focuses on the non-technical challenges facing leaders in times of extreme pressure.

SEC388: Introduction to Cloud Computing and Security NEW
SEC388 focuses on Azure and AWS, and shows you how to interact with each cloud provider by familiarizing you with common terminology, cloud services, security concerns, and solutions to cloud-based security shortcomings.

SEC467: Social Engineering for Security Professionals NEW
SEC467 will prepare you to add social engineering skills to your security strategy.

SEC556: IoT Penetration Testing NEW
SEC556 facilitates examining the entire IoT ecosystem, helping you build the vital skills needed to identify, assess, and exploit basic and complex security mechanisms in IoT devices.

SEC580: Metasploit for Enterprise Penetration Testing
SEC580 will teach you how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen.

ICS418: ICS Security Essentials for Managers
ICS418 empowers leaders responsible for securing critical infrastructure and operational technology environments.
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

**Summit Presentations**
Top-of-mind presentations
sans.org/presentations

**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 gives 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

**Social Media**
Find us at @SANSInstitute, and connect with us to stay informed on the latest SANS resources

- New2Cyber
- Cyber Defense
- Offensive Ops
- DFIR
- Leadership
- Cloud
- ICS
- Security Awareness
sans.org/blog/SANS-Social-Channels-Podcasts

**Webcasts**
sans.org/webcasts

**Blogs**
sans.org/blog

**Podcasts**

- **Blueprint**
  Advancing cyber defense skills

- **Cloud Ace**
  Future of cloud security

- **GIAC: Trust Me, I’m Certified**
  Industry leaders in cybersecurity

- **Internet Storm Center**
  Daily InfoSec threat updates
sans.org/podcasts

**SANS Cyber Academies**

- **VetSuccess Academy**

- **Women’s Immersion Academy**

- **Cyber Workforce Academy**

- **Cyber Diversity Academy**

- **HBCU Academy**
sans.org/scholarship-academies

**Newsletters**

- **NewsBites**
  A semiweekly executive summary of the most important cybersecurity news articles published recently

- **@Risk**
  A weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, and other valuable data

- **OUCH!**
  A free monthly security awareness newsletter designed for the common computer user, in over 20 languages
sans.org/newsletters

**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

- **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**
  The CIS Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today’s most pervasive and dangerous attacks.
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

- **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

---

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!
At the heart of everything we do is our mission.

Our mission at SANS is to empower cybersecurity professionals with the practical skills and knowledge to make the world a safer place. We believe that to lead it, you must live it. That’s why we partner with the industry’s foremost practitioners to develop and deliver cutting-edge training, certification, and academic programs. Our students learn from those who are active in the field today: the people on the front lines testing, trying, and designing new ways to secure our cyber domain.

When choosing SANS, you don’t just take a course, you become part of our community. Whether you are new to cyber or working in the executive ranks, we are committed to supporting you throughout your journey. We do this by providing multiple career tracks, free resources, summits, and varied modalities to access training. An investment in SANS is an investment in your career, organization, and the future.

*The SANS Promise: Everyone who completes SANS training can apply the skills and knowledge they’ve learned the day they return to work.*

www.sans.org