

**SAVE  
\$500!**

REGISTER & PAY BY  
**February 6**

USE CODE  
**EarlyBird23**

Register Now!  
[sans.org/sans-2023](https://sans.org/sans-2023)

# SANS 2023

April 2–7 | Orlando, FL or Virtual  
**NETWORKS**

Advance your career and protect your organization with world-class **cybersecurity training and GIAC certifications**. Choose from 40+ hands-on, immersion-style courses taught by real-world practitioners.

Look inside  
for your Live  
Training Guide!



**“SANS offers the best training and value for the money out there. This course has been nothing different. I’ve learned so much, it’s been brilliant. Keep up the great work!”**

— Ashwin Venkat, F5 Networks

## Featured New Courses!

FOR509: Enterprise Cloud Forensics and Incident Response

FOR608: Enterprise-Class Incident Response  
and Threat Hunting

SEC497: Practical Open-Source Intelligence (OSINT)

SEC595: Applied Data Science and Machine Learning for  
Cybersecurity Professionals

The stakes are higher than ever in our industry. As more conflicts move online, we must take a stronger stance to protect our infrastructure, financial livelihoods, and reputation. SANS' mission is to help cyber pros like you to keep the world safe. That is why I am urging you to make 2023 the year of learning. There has never been a more important time to invest in yourself and your skills.



We want to make it easy for you to choose the right training and certifications. I am honored to provide you with a comprehensive SANS 2023 Course Catalogue and pull-out Training Calendar. Our community of practitioners has raised the bar on content this year. From innovative tactics to counteract emerging threats to helping those new to cyber build a foundation for service, SANS strives to give you what you need to detect and defend. I encourage you to review the catalogue in print or at [sans.org](https://sans.org) to help map your year of learning.

Thank you for your continued support of SANS. Together, we will further our mission to make the world a safer place for all.

Sincerely,

Eric Bassel  
Chief Executive Officer  
SANS Institute

# SANS 2023

April 2-7 | Orlando, FL  
Hyatt Regency Orlando  
9801 International Dr. | Orlando, FL 32819

**SEE PAGE 65 FOR HOTEL INFORMATION**

## SAVE \$500!

REGISTER & PAY BY

**February 6**

USE CODE

**EarlyBird23**

[sans.org/sans-2023](https://sans.org/sans-2023)

Dear Colleagues and Friends,

The heart of SANS is our community. It is that spark that arises when great thinkers are in a room solving the toughest challenges, and the camaraderie in celebrating a job well done. That energy is why we strive at SANS to host events that do more than educate and entertain. We want our events to change lives.

On behalf of SANS, I hope that you will join us in Orlando, Florida from April 2-7 for SANS 2023. With over 40 courses and 1,500 hours of training, it will be our greatest training event yet. Our high-energy program has world-class instructors, hands-on labs, riveting evening talks, and endless opportunities to network. The SANS 2023 Solutions Expo, Lunch & Learn Sessions, and Bonus Sessions provide you with innovative solutions to solve tomorrow's challenges.

And, of course, come for the fun. We have an array of interactive experiences from our family-friendly Welcome Reception to competitive NetWars Tournaments, and an exclusive discount to visit Walt Disney World®.

This will be a must-attend event. I encourage you to register NOW to reserve your spot. If you cannot make it in person, please join us Live Online. We want you to be part of the action wherever you are.

I look forward to seeing you in Orlando, or for any of our live events this year. If you have questions or suggestions, please reach out to me directly at [jawad@sans.org](mailto:jawad@sans.org). I always welcome feedback from our community.

Sincerely,

Jason Awad  
Director, North America Live Training



## SANS 2023 Special Offer

This year, SANS is excited to offer attendees the opportunity to purchase specially priced Walt Disney World® Theme Park tickets. To secure your tickets at our special rate, please go to [www.mydisneygroup.com/sans2023](https://www.mydisneygroup.com/sans2023) or call **407-566-5600** and provide group code **G0824586**.

# Two Ways to Train at SANS 2023

Train In-Person or Live Online with industry experts at dynamic, live training events

[sans.org/sans-2023](https://sans.org/sans-2023)

## Benefits of In-Person Training

In-Person training offers great destinations to choose from or a venue close to home.

- Engage with our unparalleled faculty, comprised of the industry's top cybersecurity practitioners
- Enjoy networking opportunities to meet, share, and learn from your peers
- Practice hands-on information security challenges in classroom labs
- Use courseware delivered both electronically and in print, including MP3 course archives that are downloadable to review following the event
- Meet with emerging solution providers as they reveal the latest tools and technologies critical for you to master information security

***"The combination of highly relevant material, hands-on exercises, and instructors who supplemented the material with real-world stories and examples made the course material come alive in a way no other delivery method could."***

—Ted Nichols, Blue Cross Blue Shield of South Carolina

## Benefits of Live Online Training

Live Online training offers access without travel to the same world-class SANS faculty via live streaming, and delivers the same learning results as SANS In-Person training.

- Interactive Q&A with instructors and peers
- Real-time support from virtual Technical Assistants
- Hands-on labs in a virtual environment
- Courseware delivered both electronically and in print
- Extended access to class recordings, to review topics on your own time
- Dedicated chat channels using Slack for networking
- Practice your skills with SANS virtual cyber ranges

***"The Live Online delivery platform ensures students are able to access content, virtual machines, labs, resources, and chat 24 hours a day...Additionally, after the course ends, access is still available! Priceless!!"***

—Britni T., U.S. federal agency








Certify the Skills and Knowledge You Learn in SANS Training  
[www.giac.org](https://www.giac.org)



Courses at a Glance

For an up-to-date course list, please check the website at [sans.org/sans-2023](https://sans.org/sans-2023)

		Page No.	 Available In-Person	 Available via Live Online	 Bundle OnDemand with this course	GIAC CERTIFICATIONS	 Meets DoDD 8140 (8570) Requirements	 This GIAC Cert is ANAB Accredited	GIAC CyberLive Testing Available
CLOUD	SEC488	Cloud Security Essentials	8	✓	✓	✓	GCLD: Cloud Security Essentials	✓	
	SEC510	Public Cloud Security: AWS, Azure, and GCP	14	✓	✓	✓	GPCS: Public Cloud Security		
	SEC522	Application Security: Securing Web Apps, APIs, and Microservices	15	✓	✓	✓	GWEB: Web Application Defender		
	SEC540	Cloud Security and DevSecOps Automation	16	✓	✓	✓	GCSA: Cloud Security Automation	✓	
	SEC541	Cloud Security Attacker Techniques, Monitoring, and Threat Detection	17	✓	✓	✓	GCTD: Cloud Threat Detection		
CYBER DEFENSE	SEC450	Blue Team Fundamentals: Security Operations and Analysis	20	✓	✓	✓	GSOC: Security Operations		
	SEC497	Practical Open-Source Intelligence (OSINT) <span>NEW</span>	21	✓	✓	✓	GOSI: Open Source Intelligence		
	SEC501	Advanced Security Essentials – Enterprise Defender	22	✓	✓	✓	GCED: Enterprise Defender	✓	✓
	SEC503	Network Monitoring and Threat Detection In-Depth	23	✓	✓	✓	GCIA: Intrusion Analyst	✓	✓
	SEC511	Continuous Monitoring and Security Operations	24	✓	✓	✓	GMON: Continuous Monitoring		✓
	SEC530	Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise	25	✓	✓	✓	GDSA: Defensible Security Architecture		
	SEC555	SIEM with Tactical Analytics	26		✓	✓	GCDA: Detection Analyst		
	SEC573	Automating Information Security with Python	27	✓	✓	✓	GPYC: Python Coder		
	SEC595	Applied Data Science and Machine Learning for Cybersecurity Professionals <span>NEW</span>	28	✓	✓	✓			
DFIR	FOR498	Battlefield Forensics & Data Acquisition	10	✓	✓	✓	GBFA: Battlefield Forensics and Acquisition		
	FOR500	Windows Forensic Analysis	30	✓	✓	✓	GCFE: Forensic Examiner	✓	✓
	FOR508	Advanced Incident Response, Threat Hunting, and Digital Forensics	31	✓	✓	✓	GCFA: Forensic Analyst	✓	✓
	FOR509	Enterprise Cloud Forensics and Incident Response <span>NEW</span>	32	✓	✓	✓	GCFR: Cloud Forensics Responder		✓
	FOR572	Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	33	✓	✓	✓	GNFA: Network Forensic Analyst		✓
	FOR578	Cyber Threat Intelligence	34	✓	✓	✓	GCTI: Cyber Threat Intelligence		
	FOR585	Smartphone Forensic Analysis In-Depth	35	✓	✓	✓	GASF: Advanced Smartphone Forensics		
	FOR608	Enterprise-Class Incident Response & Threat Hunting <span>NEW</span>	36	✓	✓	✓			
	FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	37	✓	✓	✓	GREM: Reverse Engineering Malware		✓
ICS	ICS410	ICS/SCADA Security Essentials	12	✓	✓	✓	GICSP: Global Industrial Cyber Security Professional	✓	✓
	ICS612	ICS Cybersecurity In-Depth	55	✓					
LEADERSHIP	MGT414	SANS Training Program for the CISSP® Certification	11	✓	✓	✓	GISP: Information Security Professional	✓	
	MGT512	Security Leadership Essentials for Managers	48	✓	✓	✓	GSLS: Security Leadership	✓	✓
	MGT514	Security Strategic Planning, Policy, and Leadership	49	✓	✓	✓	GSTRT: Strategic Planning, Policy, and Leadership		
	MGT516	Managing Security Vulnerabilities: Enterprise and Cloud	50	✓	✓	✓			
	MGT521	Leading Cybersecurity Change: Building a Security-Based Culture	51		✓	✓			
	MGT551	Building and Leading Security Operations Centers	52	✓	✓	✓			
	SEC566	Implementing and Auditing Security Frameworks and Controls	53	✓	✓	✓	GCCC: Critical Controls		
NEW2 CYBER	SEC301	Introduction to Cyber Security	6	✓	✓	✓	GISF: Information Security Fundamentals	✓	
	SEC401	Security Essentials: Network, Endpoint, and Cloud	7	✓	✓	✓	GSEC: Security Essentials	✓	✓
	SEC504	Hacker Tools, Techniques, and Incident Handling	9	✓	✓	✓	GCIH: Incident Handler	✓	✓
	SEC542	Web App Penetration Testing and Ethical Hacking	40	✓	✓	✓	GWAPT: Web Application Penetration Tester		✓
	SEC550	Cyber Deception - Attack Detection, Disruption and Active Defense <span>NEW</span>	41	✓	✓				
	SEC560	Enterprise Penetration Testing <span>NEW</span>	42	✓	✓	✓	GPEN: Penetration Tester	✓	✓
	SEC588	Cloud Penetration Testing <span>NEW</span>	43	✓	✓	✓	GCPN: Cloud Penetration Tester		
	SEC599	Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses	44	✓	✓	✓	GDAT: Defending Advanced Threats		
	SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	45	✓	✓	✓	GXPN: Exploit Researcher and Advanced Pen Tester		✓
	SEC699	Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection	46		✓	✓			
NETWARS	CORE	NetWars Tournament	58	✓					
	DFIR	NetWars Tournament	58	✓					
	Cyber Defense	NetWars Tournament	58	✓					

Contents					Courses subject to change. Visit <a href="https://www.sans.org/sans-2023">www.sans.org/sans-2023</a> for updates							
2	2 Ways to Train . . . . .	1	Cloud Security Careers . . . . .	13	SANS Challenge Coins . . . . .	38	SANS Technology Institute . . . . .	56	OnDemand . . . . .	60	Hotel Information . . . . .	65
	Courses at a Glance . . . . .	2–3	Why Renew GIAC Certification . . . . .	18	Offensive Operations Careers . . . . .	39	SANS Faculty . . . . .	57	SANS Summits . . . . .	61	Justify Your Training. . . . .	65
	GIAC Certifications/CyberLive . . . . .	4	Cyber Defense Careers . . . . .	19	Cybersecurity Leadership Careers . . . .	47	Cyber Ranges . . . . .	58	NICE Framework . . . . .	62–63		
	New2Cyber – Where to Start . . . . .	5	DFIR and Threat Hunting Careers . . . .	29	ICS Careers . . . . .	54	SANS Security Awareness . . . . .	59	Free Cybersecurity Resources . . . . .	64		

## Introducing CyberLive

### Raising the bar even higher on GIAC Certifications

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

Learn more at [giac.org/cyberlive](https://giac.org/cyberlive)

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

—Ben Boyle,  
GXPN, GDAT, GWAPT

## GIAC Certifications

### Achieve the Highest Standard in Cybersecurity Certification

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](https://GIAC.ORG)

**GIAC**  
CERTIFICATIONS

## 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 IT 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

Scan for  
SANS Roadmap ▶



See center bind-in for your  
Cybersecurity Career Guide.

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

—Frank Perrilli, IESO





## GIAC Certifications

Achieve the Highest Standard  
in Cybersecurity Certification

### CYBERLIVE

#### Introducing CyberLive

##### Raising the bar even higher on GIAC Certifications

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

Learn more at [giac.org/cyberlive](https://giac.org/cyberlive)

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

—Ben Boyle,  
GXPN, GDAT, GWAPT

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](https://GIAC.ORG)**

**GIAC**  
CERTIFICATIONS

# 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 IT 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

Scan for  
SANS Roadmap ▶



See center bind-in for your  
Cybersecurity Career Guide.

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

—Frank Perrilli, IESO

# SEC301: Introduction to Cyber Security



5  
Day Program

30  
CPEs

9  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) for prioritization of critical security resources
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand how a computer works

## 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)

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 issues makes this 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)
- Communicate 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

**DAY 1:** Security's Foundation

**DAY 2:** Computer Functions and Networking

**DAY 3:** An Introduction to Cryptography

**DAY 4:** Cybersecurity Technologies – Part 1

**DAY 5:** Cybersecurity Technologies – Part 2

**"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

**"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



# SEC401: Security Essentials Bootcamp Style



6  
Day Program

46  
CPEs

18  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- Master the core areas of cybersecurity and know how to create a security program that is built on a foundation of Detection, Response, and Prevention
- Apply practical tips and tricks that focus on addressing high-priority security problems within your organization and doing the right things that lead to security solutions that work
- Know how adversaries adapt tactics and techniques, and how to adapt your defense accordingly
- Identify what ransomware is and how to better defend against it
- Leverage a defensible network architecture (VLANs, NAC, and 802.1x) based on advanced persistent threat indicators of compromise
- Understand and apply the Identity and Access Management (IAM) methodology, including aspects of strong authentication (Multi-Factor Authentication)

## Who Should Attend

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking

## NICE Framework Work Roles

- Security Control Assessor (OPM 612)
- Database Administrator (OPM 421)
- Data Analyst (OPM 422)
- Technical Support Specialist (OPM 411)
- Network Operations Specialist (OPM 441)
- System Administrator (OPM 451)
- Systems Security Analyst (OPM 461)
- Cyber Instructional Curriculum Developer (OPM 711)
- IT Investment/Portfolio Manager (OPM 804)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

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 the 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

**DAY 1:** Network Security & Cloud Essentials

**DAY 2:** Defense-in-Depth

**DAY 3:** Vulnerability Management and Response

**DAY 4:** Data Security Technologies

**DAY 5:** Windows and Azure Security

**DAY 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](https://sans.org/courses)

WAYS TO TRAIN FOR SEC401

**At Orlando**  
[sans.org/sans-2023](https://sans.org/sans-2023)

**Live Online**  
[sans.org/sans-2023](https://sans.org/sans-2023)

**OnDemand**  
[sans.org/ondemand](https://sans.org/ondemand)

# SEC488: Cloud Security Essentials



6  
Day Program

36  
CPEs

20+  
Labs

Sunday, April 2–Friday, April 7

## 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 utilize any of the leading CSPs
- Protect secrets used in cloud environments
- Leverage cloud logging capabilities to establish accountability for events that occur in the cloud environment
- Identify the risks and risk control ownership based on the deployment models and service delivery models of the various products offered by cloud service providers (CSPs)

## Who Should Attend

Anyone who works in a cloud environment, is interested in cloud security, or needs to understand the risks involved in using cloud service providers should take this course, including:

- Security engineers
- Security analysts
- System administrators
- Risk managers
- Security managers
- Security auditors
- Anyone new to the cloud

## NICE Framework Work Roles

- Security Architect (OPM 652)
- Systems Security Analyst (OPM 461)
- Information Systems Security Manager (OPM 722)

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

**DAY 1:** Identity and Access Management

**DAY 2:** Compute and Configuration Management

**DAY 3:** Data Protection and Automation

**DAY 4:** Networking and Logging

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

**DAY 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

# SEC504: Hacker Tools, Techniques, and Incident Handling



6 Day Program | 38 CPEs | 40 Labs  
Sunday, April 2–Friday, April 7

## Who Should Attend

- Incident handlers
- Leaders of incident response teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack
- General security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks

## NICE Framework Work Roles

- Technical Support Specialist (OPM 411)
- Systems Security Analyst (OPM 461)
- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Cyber Instructional Curriculum Developer (OPM 711)
- Cyber Instructor (OP 712)
- Security Awareness & Communications Manager (OP 712)
- Information Systems Security Manager (OPM 722)
- IT Investment/Portfolio Manager (OPM 804)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Incident Responder (OPM 531)
- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Mission Assessment Specialist (OPM 112)
- Target Network Analyst (OPM 132)
- Cyber Intel Planner (OPM 331)

**“Incident response is the most underused aspect in small companies. SEC504 gives us the ability to help management understand the value.”**

—David Freedman, Nationwide Payment Solutions

\*DoDD 8140  
IAT Level III  
[sans.org/dod/dodd-8140](https://sans.org/dod/dodd-8140)

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

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-premises platforms. We'll examine the latest threats to organizations, from watering hole attacks to cloud application service MFA 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 365

## Syllabus Summary

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

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

**DAY 3:** Password and Access Attacks

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

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

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

WAYS TO TRAIN FOR SEC504

At Orlando  
[sans.org/sans-2023](https://sans.org/sans-2023)

Live Online  
[sans.org/sans-2023](https://sans.org/sans-2023)

OnDemand  
[sans.org/ondemand](https://sans.org/ondemand)



# FOR498: Battlefield Forensics & Data Acquisition



**GBFA**  
Battlefield Forensics  
and Acquisition  
[giac.org/gbfa](http://giac.org/gbfa)

6  
Day Program

36  
CPEs

34  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where it is stored
- Handle and process a scene properly to maintain evidentiary integrity
- Perform data acquisition from at-rest storage, including both spinning media and solid-state storage
- Identify the numerous places that data for an investigation might exist
- Perform Battlefield Forensics by going from evidence seizure to actionable intelligence in 90 minutes or less
- Assist in preparing the documentation necessary to communicate with online entities such as Google, Facebook, Microsoft, etc.

## Who Should Attend

- Federal agents and law enforcement personnel who want to master proper acquisition methodologies and ensure that all data are collected properly and in a defensible manner
- First responders who attend to a scene where digital equipment seizure may take place—it is crucial at this point to perform proper scene management, identification, preservation, and acquisition
- Digital forensic analysts who want to consolidate and expand their understanding of data storage and acquisition in today's digital storage world
- Information security professionals who want to learn the acquisition and triage skills needed to begin Windows digital forensics investigations
- Incident response team members who need to preserve indicated computers for digital forensics to help solve their Windows data breach and intrusion cases
- Media exploitation analysts who need to collect and preserve systems in Document and Media Exploitation (DOMEX) operations on systems used by an individual
- Department of Defense and intelligence community professionals tasked with rapid collection and triage of systems
- Anyone interested in an understanding of the proper preservation of systems and who has a background in information systems, information security, and computers

FOR498 provides the necessary skills to identify the many and varied data storage mediums in use today, and teaches you how to collect and preserve this data in a forensically sound manner despite how and where it may be stored. You will learn digital acquisition from computers, portable devices, networks, and the cloud, as well as Battlefield Forensics—the art and science of identifying and starting to extract actionable intelligence from a hard drive in 90 minutes or less.

## Business Takeaways

- Understand how to collect data from a wide range of storage
- Understand how to collect and leverage RAM from a running machine
- Learn how to manage and document a scene and collected evidence
- Collect key forensic artifacts from a Windows system in minutes
- Understand what can and cannot be collected from portable devices
- Find and extract online data even when the data is no longer there!
- Learn how to carve and rebuild files and partial data from deleted space

## Syllabus Summary

**DAY 1:** Scene Prep, Management, and Storage Interfaces

**DAY 2:** Portable Devices and Acquisition Processes

**DAY 3:** Triage and Data Acquisition

**DAY 4:** Non-Traditional and Cloud Acquisition

**DAY 5:** Apple Acquisition and Internet of Things

**DAY 6:** Beyond the Forensic Tools: The Deeper Dive

**“This course provided information I can take back to my company and begin using immediately. It will be very easy to show leadership the ROI on this course.”**

—Jennifer Welsh, CNO Financial Group

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

—J-Michael Roberts, Corvus Forensics

# MGT414: SANS Training Program for the CISSP Certification



6  
Day Program | 52  
CPEs

Sunday, April 2–Friday, April 7

## 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

**“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

### \*DoDD 8140

IAT Level III – IAM Level II & III  
CNDSP Manager – IASAE I, II & III  
[sans.org/dod/dodd-8140](https://sans.org/dod/dodd-8140)

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

## 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 Misenar

## Syllabus Summary

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

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

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

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

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

**DAY 6:** Software Development Security

**“This course breaks the huge CISSP® study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent.”**

—Jeff Jones, Constellation Energy Group

WAYS TO TRAIN FOR MGT414

At Orlando  
[sans.org/sans-2023](https://sans.org/sans-2023)

Live Online  
[sans.org/sans-2023](https://sans.org/sans-2023)

OnDemand  
[sans.org/ondemand](https://sans.org/ondemand)

# ICS410: ICS/SCADA Security Essentials



6  
Day Program

36  
CPEs

15+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- Understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with control network infrastructure design (network architecture concepts, including topology, protocols, and components) and understand its relation to IEC 62443 and the Purdue Model
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Understand the systems' security lifecycle

## Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

## NICE Framework Work Roles

- Process Control Engineer/Instrument & Control Engineer (ZZ-ICS-001)
- ICS/SCADA Security Engineer (ZZ-ICS-002)
- ICS/OT Systems Engineer (ZZ-ICS-003)
- OT SOC Operator (ZZ-ICS-004)

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 organizations and Industrial Control Systems 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 are 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, 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

**DAY 1:** ICS Overview

**DAY 2:** Architectures and Field Devices

**DAY 3:** Communications and Protocols

**DAY 4:** Supervisory Systems

**DAY 5:** ICS Security Governance

**DAY 6:** Capstone Exercise

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

— Rafael Issa, Technip

**“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



# Cloud Security

Cloud computing represents the most transformational technology of our era, and cloud security will play a pivotal role in its adoption. Cloud security must be focused on where the cloud is going, not where it is today. The future demands in-depth technical cloud capabilities coupled with knowledge of the security and service features for each of the major cloud service providers (CSPs). Begin your journey to become a Cloud Security Ace.

SANS Cloud Security curriculum has been developed through an industry consensus process and is a holistic, hands-on approach to address public cloud security, which includes multicloud scenarios for established enterprises and developing organizations alike. Learn how CSPs compare and the corresponding nuances among them rather than merely learning the ins-and-outs of one platform.

Get hands-on with cloud security training and learn how to:

- Harden and configure public cloud services from AWS, Azure, and Google Cloud Platform (GCP)
- Automate security and compliance best practices
- Use cloud services to securely build and deploy systems and applications
- Inject security seamlessly into your DevOps toolchain
- Securely build, deploy, and manage containers
- Discover vulnerabilities and weaknesses in your cloud environments
- Find attacker activity in your cloud logs

#### Cloud Security Job Roles:

- Cloud Security Analyst
- Cloud Security Engineer
- Cloud Security Architect
- Cloud Security Manager
- DevSecOps Professionals

**“The world has shifted to the cloud and we as security professionals have to make the same shift.”**

—Daniel Harrison, Capital One

# SEC510: Public Cloud Security: AWS, Azure, and GCP



5  
Day Program

38  
CPEs

20+  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- I Navigate your organization through the security challenges and opportunities presented by cloud services
- I Identify the risks of the various services offered by cloud service providers (CSPs)
- I Select the appropriate security controls for a given cloud network security architecture
- I Evaluate CSPs based on their documentation, security controls, and audit reports
- I Confidently use the services of any of the leading CSPs
- I Protect secrets used in cloud environments

## Who Should Attend

Security analysts, security engineers, security researchers, cloud engineers, DevOps engineers, security auditors, system administrators, operations personnel, and anyone who is responsible for:

- I Evaluating and adopting new cloud offerings
- I Researching new vulnerabilities and developments in cloud security
- I Handling Identity and Access Management
- I Managing a cloud-based virtual network
- I Secure configuration management

## NICE Framework Work Roles

- I Security Architect – SP-ARC-002
- I Secure Software Assessor – SP-DEV-002
- I Security Control Assessor – SP-RSK-002
- I Information Systems Security Developer – SP-SYS-001

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.

## Business Takeaways

- I 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.
- I 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.
- I All security-minded organizations require professional reconfiguration, as most cloud services are highly insecure by default.
- I Storage security is much more than just closing public buckets. Even private assets can be compromised by competent attackers.
- I 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

**DAY 1:** Cloud Credential Management

**DAY 2:** Cloud Virtual Networks

**DAY 3:** Encryption, Storage, and Logging

**DAY 4:** Serverless Platforms

**DAY 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

# SEC522: Application Security: Securing Web Apps, APIs, and Microservices



**GWEB**  
Web Application  
Defender  
[giac.org/gweb](https://giac.org/gweb)

6  
Day Program

36  
CPEs

20+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Defend against the attacks specified in OWASP Top 10
- I Understand infrastructure security and configuration management
- I Securely integrate cloud components into a web application
- I Understand authentication and authorization protocols, including single sign-on, and their implementation
- I Cross-domain web request security
- I Protective HTTP headers
- I Defend SOAP, REST and GraphQL APIs
- I Securely implement Microservice architecture

## Who Should Attend

- I Application developers
- I Application security analysts or managers
- I Application architects
- I Penetration testers who are interested in learning about defensive strategies
- I Security professionals who are interested in learning about web application security
- I Auditors who need to understand defensive mechanisms in web applications
- I Employees of PCI-compliant organizations who need to be trained to comply with PCI requirements

## NICE Framework Work Roles

- I Software Developer – SP-DEV-001
- I Secure Software Assessor – SP-DEV-002
- I Information Systems Security Developer – SP-SYS-001
- I Systems Developer – SP-SYS-002
- I Research & Development Specialist – SP-TRD-001

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 class will not only raise awareness about common security flaws in modern web applications, but it will also teach students how to recognize and mitigate these flaws early and efficiently.

## Business Takeaways

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

## Syllabus Summary

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

**DAY 2:** Input-Related Defenses

**DAY 3:** Authentication and Authorization

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

**DAY 5:** APIs and Microservices Security

**DAY 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



# SEC540: Cloud Security and DevSecOps Automation



5  
Day Program

38  
CPEs

35+  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- I Understand how DevOps works and identify keys to success
- I Wire security scanning into automated CI/CD pipelines and workflows
- I Build continuous monitoring feedback loops from production to engineering
- I Automate configuration management using Infrastructure as Code (IaC)
- I Secure container technologies (such as Docker and Kubernetes)
- I Use native cloud security services and third-party tools to secure systems and applications

## Who Should Attend

- I Anyone working in or transitioning to a public cloud environment
- I Anyone working in or transitioning to a DevOps environment
- I Anyone who wants to understand where to add security checks, testing, and other controls to cloud and DevOps Continuous Delivery pipelines
- I Anyone interested in learning how to migrate DevOps workloads to the cloud, specifically Amazon Web Services (AWS) and Microsoft Azure
- I Anyone interested in leveraging cloud application security services provided by AWS or Azure
- I Developers
- I Software architects
- I Operations engineers
- I System administrators
- I Security analysts
- I Security engineers
- I Auditors
- I Risk managers
- I Security consultants

## NICE Framework Work Roles

- I Enterprise Architect – SP-ARC-001
- I Software Developer – SP-DEV-001
- I Information Systems Security Developer – SP-SYS-001
- I Systems Developer – SP-SYS-002
- I Research & Developmental Specialist – SP-TRD-001

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

- I Build a security team that understands modern cloud security and DevSecOps practices
- I Partner with DevOps and engineering teams to inject security into automated pipelines
- I Leverage cloud services and automation to improve security capabilities
- I Ensure your organization is ready for cloud migration and digital transformation initiatives

## Syllabus Summary

**DAY 1:** DevOps Security Automation

**DAY 2:** Cloud Infrastructure Security

**DAY 3:** Cloud Security Operations

**DAY 4:** Cloud Security as a Service

**DAY 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

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

# SEC541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection



**GCTD**  
Cloud Threat Detection  
[giac.org/gctd](https://giac.org/gctd)

5  
Day Program

30  
CPEs

20+  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- Research attacks and threats to cloud infrastructure and how they could affect you
- Break down a threat into detectable components
- Effectively use AWS and Azure core logging services to detect suspicious behaviors
- Make use of cloud native API logging as the newest defense mechanism in cloud services
- Move beyond the cloud-provided Graphic User Interfaces to perform complex analysis
- Perform network analysis with cloud-provided network logging

## Who Should Attend

- Security analysts
- Security engineer
- Security architects
- Vulnerability assessor
- Incident responders

## NICE Framework Work Roles

- Cyber Defense Analyst: PR-CDA-001
- Cyber Defense Infrastructure Support Specialist: PR-INF-001
- Cyber Defense Incident Responder: PR-CIR-0001
- Adversary Emulation Specialist/Red Teamer: PR-VAM-001
- Threat/Warning Analyst: AN-TWA-001

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, keeping ahead of fast-moving development teams, and trying to 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, ability to capture appropriate data, and most importantly to be able 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
- Decreases risk of costly attacks by understanding and leveraging cloud specific security services
- Lessen the impact of breaches that do happen
- Learn how to fly the plane, not just the ability to read the manual

## Syllabus Summary

**DAY 1:** Management Plane and Networking Logging

**DAY 2:** Computer and Cloud Services Logging

**DAY 3:** Cloud Services and Data Discovery

**DAY 4:** Microsoft Ecosystem

**DAY 5:** Automate Response Actions and CloudWars

**“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

**“The lab guide is very detailed. Allowing me to learn and understand what I was doing. They also provided us with sufficient time to complete the labs and we were never rushed into doing anything.”**

—Sambit Sarkar, ICE Data Services

# Why Renew?

## Design Your Renewal Path

### Advanced Expertise

When you renew, you're showing yourself and others in the industry that not only do you have a certification, but you've gone above and beyond to gain advanced knowledge and experience in order to keep that certification.

### Dependability

The longer your certification is active, the more years of verified knowledge and hands-on technical abilities you have. Employers value certifications, and maintaining your certification shows your employer that you're someone they can depend on.

### Security

Renewing ensures your personal security knowledge, your job security, and the security of your enterprise—all in one.

### Respect

Your industry peers know how much time and effort is involved in maintaining a certification, and the longer you maintain your certifications, the more you'll be recognized as an expert in your field.

Up to  
**36 CPEs**

### GIAC/SANS Affiliated Programs

- Can be applied to five certifications
- New GIAC certifications
- SANS training courses, including Live and OnDemand training

Up to  
**36 CPEs**

### Advance Your Career

- Can be applied to two certifications
- Advance your knowledge
- Graduate level courses
- Published technical work

Up to  
**18 CPEs**

### Other Industry Training

- Can be applied to one certification
- DoD or military training
- Skill-based training courses
- ANAB accredited industry training\*
- All-day or multi-day training events & summits (Live Online or in person)

Up to  
**12 CPEs**

### Community Participation

- Can be applied to one certification
- Participating in GIAC exam development activities
- Writing an article for an information assurance publication

Up to  
**12 CPEs**

### SANS NetWars

- Up to 12 CPEs
- Can be applied to two certifications
- NetWars Tournament
- NetWars Continuous

Up to  
**12 CPEs**

### Cyber Ranges

- DoD exercises
- CTFs
- Other hands-on activities

Up to  
**12 CPEs**

### Work Experience

- Can be applied to one certification
- Relevant experience that aligns with your certification's objectives and skillset



# Cyber Defense

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

The Cyber Defense focus is on defending the organization from cyberattacks. This is done by developing and implementing multiple security controls in a defense-in-depth strategy, verifying their effectiveness, and continuously monitoring and improving defenses.

Cyber Defense courses will teach you to:

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

#### Cyber Defense Job Roles:

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

**“The world has never had a greater need for cyber defense than it does now. Between attacks on hospitals, schools, and infrastructure, and the upswing in disruptive ransomware, costly business email compromise, and more, the threat environment and price of security failures are quickly increasing. At SANS, our authors and instructors work tirelessly to create and deliver world-class training to jumpstart your team with the tools, mindset, and technical skills you need to repel this new wave of highly damaging attacks.”**

—John Hubbard

# SEC450: Blue Team Fundamentals: Security Operations and Analysis



**GSOC**  
Security Operations  
[giac.org/gsoc](https://giac.org/gsoc)

6  
Day Program

36  
CPEs

16+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Security Data Collection—How to make the most of security telemetry, including endpoint, network, and cloud-based sensors
- I Automation—How to identify the best opportunities for SOAR platform and other script-based automation
- I Efficient Security Process—How to keep your security operations tempo on track with in-depth discussions on what a SOC or security operations team should be doing at every step, from data generation to detection, triage, analysis, and incident response
- I Quality Triage and Analysis—How to quickly identify and separate typical commodity attack alerts from high-risk, high-impact advanced attacks, and how to do careful, thorough, and bias-free security incident analysis
- I False Positive Reduction—Detailed explanations, processes, and techniques to reduce false positives to a minimum

## Who Should Attend

This course is intended for those who are early in their career or new to working in a SOC environment, including:

- I Security analysts
- I Incident investigators
- I Security engineers and architects
- I Technical security managers
- I SOC managers looking to gain additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC
- I Anyone looking to start their career on the blue team

## NICE Framework Work Roles

- I Cyber Defense Analyst (OPM 511)
- I Cyber Defense Infrastructure Support Specialist (OPM 521)

SEC450 provides students with technical knowledge and key concepts essential for security operation 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 team members.

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** Blue Team Tools and Operations

**DAY 2:** Understanding Your Network

**DAY 3:** Understanding Endpoints, Logs, and Files

**DAY 4:** Triage and Analysis

**DAY 5:** Continuous Improvement, Analytics, and Automation

**DAY 6:** Capstone: Defend the Flag

**“SEC450 was the best technical training course I’ve ever taken in my 20 years in security. It’s extremely and immediately transferable to SOC professionals and cyber defenders in general.”**

—Chris May, CMU

**“I have been waiting a few months to take this training, and it is far exceeding my expectations. For a SOC analyst, SEC450 is a must.”**

—Yuri Cannavacciuolo, University of Miami

**“I would recommend SEC450 to any SOC analyst as the course material is very applicable to their day-to-day work. As a security architect, I would also recommend this course to my colleagues because a lot of the material can help inform our projects.”**

—Jessica Lopez, Prudential Financial

# SEC497: Practical Open-Source Intelligence (OSINT) **NEW**



**GOSI**  
Open Source  
Intelligence  
[giac.org/gosi](https://giac.org/gosi)

6  
Day Program

36  
CPEs

29  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Perform a variety of OSINT investigations while practicing good OPSEC
- I Create sock puppet accounts
- I Locate information on the internet, including some hard-to-find and deleted information
- I Locate individuals online and examine their online presence
- I Understand and effectively search the dark web
- I Create an accurate report of the online infrastructure for cyber defense, merger and acquisition analysis, pen testing, and other critical areas for an organization.

## Who Should Attend

- I OSINT investigators
- I Cyber threat intelligence analysts
- I Intelligence personnel
- I Law enforcement
- I Penetration testers/Red Team members
- I Cyber defenders
- I Recruiters
- I Journalists
- I Investigators
- I Digital forensics practitioners
- I Human resources personnel

## NICE Framework Work Roles

- I Data Analyst (OPM 422)
- I Threat/Warning Analyst (OPM 141)
- I All-Source Analyst (OPM 111)
- I Target Network Analyst (OPM 132)
- I All Source-Collection Manager (OPM 311)
- I All Source-Collection Requirements Manager (OPM 312)
- I Cyber Intel Planner (OPM 331)
- I 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.

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** OSINT and OPSEC Fundamentals

**DAY 2:** Essential OSINT Skills

**DAY 3:** Investigating People

**DAY 4:** Investigating Websites and Infrastructure

**DAY 5:** Automation, the Dark Web, and Large Data Sets

**DAY 6:** Capstone: Capture the Flag

**“SEC497 is full of helpful discussion and explanations. I learned about some techniques that I have not considered before.”**

—Brian O'Hara

**“Very relevant information that can be deployed immediately even by novice users. Excellent!”**

—Shay Christensen

# SEC501: Advanced Security Essentials – Enterprise Defender



6  
Day Program

38  
CPEs

26+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- Identify network security threats against infrastructure and build defensible networks that minimize the impact of attacks
- Utilize tools to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises systems and how to respond to attacks using the six-step incident handling process
- Perform penetration testing against an enterprise to determine vulnerabilities and points of compromise
- Use various tools to identify and remediate malware across your enterprise

## Who Should Attend

Security analysts, security engineers, security researchers, cloud engineers, DevOps engineers, security auditors, system administrators, operations personnel, and anyone who is responsible for:

- Evaluating and adopting new cloud offerings
- Researching new vulnerabilities and developments in cloud security
- Handling Identity and Access Management
- Managing a cloud-based virtual network
- Secure configuration management

## NICE Framework Work Roles

- Network Operations Specialist (OPM 441)
- Cyber Instructor (OP 712)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

Become an Enterprise Defender! Become an 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, in which 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.

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** Defensible Network Architecture

**DAY 2:** Penetration Testing

**DAY 3:** Security Operations Foundations

**DAY 4:** Digital Forensics and Incident Response

**DAY 5:** Malware Analysis

**DAY 6:** Enterprise Defender Capstone

**“This is the best technical training course I have ever taken. SEC501 exposed me to many valuable concepts and tools but also gave me a solid introduction to those tools so that I can continue to study and improve on my own.”**

—Curt Smith, Hildago Medical Services

**\*DoDD 8140**  
IAT Level III  
[sans.org/dod/dodd-8140](https://sans.org/dod/dodd-8140)



# SEC503: Network Monitoring and Threat Detection In-Depth



6  
Day Program

46  
CPEs

37+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

- Network monitoring, system, Security Operations Center, and security analysts
- Network engineers/administrators
- Hands-on security managers

## NICE Framework Work Roles

- Cyber Defense Analyst (OPM 511)

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 you can intelligently examine network traffic to identify emerging threats, perform large-scale correlation for threat hunting, and reconstruct network attacks.

## Business Takeaways

- Avoid your organization becoming another front-page headline
- Increase detection in traditional, hybrid, and cloud network environments
- Increase efficiency in threat modeling for network activities
- Decrease attacker dwell time

## Syllabus Summary

**DAY 1:** Network Monitoring and Analysis: Part I

**DAY 2:** Network Monitoring and Analysis: Part II

**DAY 3:** Signature-Based Threat Detection and Response

**DAY 4:** Building Zero-Day Threat Detection Systems

**DAY 5:** Large-Scale Threat Detection, Forensics, and Analytics

**DAY 6:** Advanced Network Monitoring and Threat Detection Capstone

**“From a heavy background in host forensics and limited knowledge in network analysis and forensics, SEC503 has filled in a lot of the gaps in knowledge I have had throughout my career.”**

—Jared H., U.S. Military

**“This course is outstanding! It has changed my view on my network defense tools and the need to correlate data through multiple tools.”**

—Ben Clark, EY

**“I feel like I have been working with my eyes closed before this course.”**

—S. Ainscow, Barrett Steel

**\*DoDD 8140**  
IAT Level III  
[sans.org/dod/dodd-8140](https://sans.org/dod/dodd-8140)

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

WAYS TO TRAIN FOR SEC503

**At Orlando**  
[sans.org/sans-2023](https://sans.org/sans-2023)

**Live Online**  
[sans.org/sans-2023](https://sans.org/sans-2023)

**OnDemand**  
[sans.org/ondemand](https://sans.org/ondemand)

# SEC511: Continuous Monitoring and Security Operation



**GMON**  
Continuous Monitoring  
[giac.org/gmon](https://giac.org/gmon)

**6**  
Day Program

**48**  
CPEs

**21+**  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

- I Security architects
- I Senior security engineers
- I Technical security managers
- I Security Operations Center (SOC) analysts, engineers, and managers
- I CND analysts
- I Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)

## NICE Framework Work Roles

- I Security Architect (OPM 652)
- I Cyber Defense Analyst (OPM 511)
- I Cyber Defense Infrastructure Support Specialist (OPM 521)

This course assesses the current state of security architecture and continuous monitoring and provides a new approach to security architecture that can be easily understood and defended. You will learn to assess deficiencies in your organization's security architecture and leave with a list of meaningful action items to ensure your organization is an effective vehicle for frustrating adversaries. You'll also be equipped with the knowledge to continuously monitor that architecture for deviations from the expected security posture.

## Business Takeaways

- I Design a defensible security architecture
- I Implement meaningful changes to your organization's security architecture
- I Maximize the capabilities of your current information security architecture
- I Evaluate existing security and implement continuous monitoring
- I Make sense of data to rapidly enable the detection of potential intrusions or unauthorized actions

## Syllabus Summary

**DAY 1:** Current State Assessment, Security Operations Centers, and Security Architecture

**DAY 2:** Network Security Architecture

**DAY 3:** Network Security Monitoring

**DAY 4:** Endpoint Security Architecture

**DAY 5:** Automation and Continuous Security Monitoring

**DAY 6:** Capstone: Design, Detect, Defend

**“SEC511 is a VERY worthwhile addition to the Cyber Defense curriculum for Blue Teamers.”**

—Robert Peden, NextGear Capital

**“SEC511 has not only focused on specific things to learn but has also helped to facilitate a way of thinking analytically.”**

—Calvin Harris, Exelon

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



**GDSA**  
Defensible Security  
Architecture  
[giac.org/gdsa](https://giac.org/gdsa)

6  
Day Program

36  
CPEs

23+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

- I Security architects
- I Network engineers
- I Network architects
- I Security analysts
- I Senior security engineers
- I System administrators
- I Technical security managers
- I CND analysts
- I Security monitoring specialists
- I Cyber threat investigators

## NICE Framework Work Roles

- I Enterprise Architect (OPM 651)
- I Security Architect (OPM 652)

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

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

## Syllabus Summary

- DAY 1:** Defensible Security Architecture and Engineering: A Journey Towards Zero Trust
- DAY 2:** Network Security Architecture and Engineering
- DAY 3:** Network-Centric Application Security Architecture
- DAY 4:** Data-Centric Application Security Architecture
- DAY 5:** Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks
- DAY 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 to having the instructor here in person.”**

—Edmund L., Singapore Federal Agency

# SEC555: SIEM with Tactical Analytics



**GCDA**  
Continuous Monitoring  
[giac.org/gcda](https://giac.org/gcda)

6 | 46 | 21  
Day Program | CPEs | Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Demonstrate ways most SIEMs commonly lag current open-source solutions (e.g., ELK)
- I Gain a current understanding of SIEM use, architecture, and best practices
- I Know what type of data sources to collect logs from
- I Deploy a scalable logs solution with multiple ways to retrieve logs
- I Operationalize ordinary logs into tactical data
- I Develop methods to handle billions of logs from many disparate data sources
- I Understand best practice methods for collecting logs
- I Dig into log manipulation techniques challenging many SIEM solutions

## Who Should Attend

- I Security analysts
- I Security architects
- I Detection engineers
- I Senior security engineers
- I Technical security managers
- I Security Operations Center analysts, engineers, and managers
- I CND analysts
- I Security monitoring specialists
- I System administrators
- I Cyber threat investigators
- I Digital Forensic and Incident Response (DFIR) analysts
- I Individuals working to implement Continuous Security Monitoring
- I Individuals working in a hunt team capacity

## NICE Framework Work Roles

- I Network Operations Specialist (OPM 441)

Many organizations have logging capabilities but lack the people and processes to analyze them. In addition, logging systems collect vast amounts of data from a variety of data sources which require an understanding of the sources for proper analysis. This class is designed to provide training, methods, and processes for enhancing existing logging solutions. This class will also provide understanding of the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free SIEM solution, to give you hands-on experience and facilitate the right mindset for large-scale data analysis.

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** SIEM Architecture

**DAY 2:** Service Profiling with SIEM

**DAY 3:** Advanced Endpoint Analytics

**DAY 4:** Baselining and User Behavior Monitoring

**DAY 5:** Tactical SIEM Detection and Post-Mortem Analysis

**DAY 6:** Capstone: Design, Detect, Defend

**“SEC555 teaches excellent, pertinent information along with practical, easy-to-follow lab exercises. A tremendously valuable course!”**

—Travis Logue, Coinstar

**“A truly well-constructed course geared toward maximizing knowledge transfer”**

—Jason Nickola, Pulsar Security

**“I would highly recommend SEC555 for anyone looking for an in-depth way to finely tune their SIEM. The tools, tips, and tricks that I can take away from this aren’t just for your standard SOC analyst, but also great for compliance and management pros.”**

—Richard Pangman, Wawanesa Insurance



# SEC573: Automating Information Security with Python



**GPYC**  
Python Coder  
[giac.org/gpyc](https://giac.org/gpyc)

6 Day Program | 36 CPEs | 128 Labs

Sunday, April 2–Friday, April 7

## 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

## Who Should Attend

- Security professionals who benefit from automating routine tasks so they can focus on what's most important
- Forensic analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evil-doers in their networks
- Penetration testers who are ready to advance from utilizing scripts to intelligently crafting and running them
- Security professionals who want to evolve from security tool consumer to security solution provider

## 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)

The challenges faced by security professionals are constantly evolving, so there is a huge demand for those who can understand technical problems and quickly develop solutions. If you have to wait on a vendor to develop a tool to recover a forensics artifact, or to either patch or exploit that new vulnerability, then you will always be behind. It is no longer an option for employers serious about information security to operate without the ability to rapidly develop their own tools.

This course will give you the skills to develop solutions so that your organization can operate at the speed of the adversary.

SEC573 is an immersive, self-paced, hands-on, and lab-intensive course. After covering the essentials required for people who have never coded before, the course will present students with real-world forensics, defensive, and offensive challenges. You will develop a malware dropper for an offensive operation; learn to search your logs for the latest attacks; develop code to carve forensics artifacts from memory, hard drives, and packets; automate the interaction with an online website's API; and write a custom packet sniffer. Through fun and engaging labs, you'll develop useful tools and build essential skills that will make you the most valuable member of your information security team.

## Business Takeaways

- Automatically execute existing applications and process their output
- Create programs that increase efficiency and productivity
- Develop tools to provide the vital defenses our organizations need

## Syllabus Summary

**DAY 1:** Essentials Workshop with pyWars

**DAY 2:** Essentials Workshop with MORE pyWars

**DAY 3:** Defensive Python

**DAY 4:** Forensics Python

**DAY 5:** Offensive Python

**DAY 6:** Capture-the-Flag Challenge

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

—Caleb Jaren, Microsoft

# SEC595: Applied Data Science and Machine Learning for Cybersecurity Professionals **NEW**

6 Day Program | 36 CPEs | 30 Labs  
Sunday, April 2–Friday, April 7

## 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 genetic 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 your problem into something that can be solved with machine learning
- Blue team and SOC members looking to identify anomalies and perform custom threat hunting

## NICE Framework Work Roles

- Data Analyst (OPM 422)

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!

## 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

**DAY 1:** Data Acquisition, Cleaning, and Manipulation

**DAY 2:** Data Exploration and Statistics

**DAY 3:** Essentials of Machine Learning

**DAY 4:** Essentials of Machine Learning

**DAY 5:** Essentials of Machine Learning

**DAY 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 how to work my own data.”**

—Oscar Garzon, Thought Machine

# Digital Forensics & Incident Response (DFIR) and Threat Hunting

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

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

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

## DFIR & Threat Hunting Job Roles:

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

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

—James Tayler, Context Information Security

# FOR500: Windows Forensic Analysis



**6**  
Day Program

**35**  
CPEs

**22+**  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Perform proper Windows forensic analysis by applying peer-reviewed techniques focusing on Windows 7, Windows 8/8.1, Windows 10, Windows 11, and Windows Server products
- I Use state-of-the-art forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geolocation, browser history, profile USB device usage, cloud storage usage, and more
- I 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
- I 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
- I Audit cloud storage usage, including detailed user activity, identifying deleted files, signs of data exfiltration, and even documenting files available only in the cloud
- I 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

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

## NICE Framework Work Roles

- I Cyber Crime Investigator (OPM 221)
- I Cyber Defense Forensics Analyst (OPM 212)

FOR500 builds in-depth and comprehensive digital forensics knowledge of Microsoft Windows operating systems by analyzing and authenticating forensic data. You will learn to track detailed user activity and organize findings, as well as apply digital forensic methodologies to a variety of case types and situations. This will enable you to apply the right methodology to achieve the best outcome in the real world.

## Business Takeaways

- I Build the skills necessary to conduct in-depth forensic analysis of all Windows operating systems—including on Windows XP through Windows 11—and Windows Server products
- I Develop in-house capabilities to investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions
- I Identify forensic artifact and evidence locations to answer crucial questions, including application execution, file access, data theft, external device usage, cloud services, device geolocation, file downloads, anti-forensics, and detailed system and user activity
- I Receive a pre-built forensic lab setup via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation
- I Build tool-agnostic investigative capabilities by focusing on analysis techniques instead of how to use a particular tool. Deeper understanding of core forensic artifacts and stronger analysis skills make any available tool more effective for attendees.

## Syllabus Summary

**DAY 1:** Digital Forensics and Advanced Data Triage

**DAY 2:** Registry Analysis, Application Execution, and Cloud Storage Forensics

**DAY 3:** Shell Items and Removable Device Profiling

**DAY 4:** Email Analysis, Windows Search Index, SRUM, and Event Logs

**DAY 5:** Web Browser Forensics

**DAY 6:** Windows Forensics Challenge

**“This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience.”**

—Alexander Applegate, **Auburn University**

**“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



6  
Day Program

36  
CPEs

27  
Labs

Sunday, April 2–Friday, April 7

## 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)

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

## Syllabus Summary

**DAY 1:** Advanced Incident Response & Threat Hunting

**DAY 2:** Intrusion Analysis

**DAY 3:** Memory Forensics in Incident Response & Threat Hunting

**DAY 4:** Timeline Analysis

**DAY 5:** Incident Response & Hunting Across the Enterprise |  
Advanced Adversary & Anti-Forensics Detection

**DAY 6:** The APT Threat Group Incident Response Challenge

**“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 enterprises security posture.”**

—Ian Howard, Tesco

# FOR509: Enterprise Cloud Forensics and Incident Response **NEW**



**GCFR**  
Cloud Forensics  
Responder  
[giac.org/gcfr](http://giac.org/gcfr)

6  
Day Program

36  
CPEs

20  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

- I Incident response team members who may need to respond to security incidents/ intrusions impacting cloud hosted software, infrastructure or platforms and need to know how to detect, investigate, remediate, and recover from compromised systems across the enterprise cloud
- I Threat hunters who are seeking to understand threats more fully and how to learn from them in order to more effectively hunt threats and counter their tradecraft
- I SOC analysts looking to better understand alerts, build the skills necessary to triage events, and fully leverage cloud log sources
- I Experienced digital forensic analysts who want to consolidate and enhance their understanding of cloud-based forensics
- I Information security professionals who directly support and aid in responding to data breach incidents and intrusions
- I Federal agents and law enforcement professionals who want to master advanced intrusion investigations and incident response, and expand their investigative skills beyond traditional host-based digital forensics
- I SANS FOR500, FOR508, SEC541, and SEC504 graduates looking to add cloud-based forensics to their toolbox.

## NICE Framework Work Roles

- I Cyber Defense Incident Responder (OPM 531)
- I Cyber Crime Investigator (OPM 221)
- I Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- I Cyber Defense Forensics Analyst (OPM 212)
- I All Source-Collection Requirements Manager (OPM 312)

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

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

## Syllabus Summary

**DAY 1:** Microsoft 365 and Graph API

**DAY 2:** Microsoft Azure

**DAY 3:** Amazon Web Services (AWS)

**DAY 4:** Google Workspace

**DAY 5:** Google Cloud

**DAY 6:** Multi-Cloud Intrusion Challenge

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

—Marc Stroebe, 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

WAYS TO TRAIN FOR FOR509

**At Orlando**  
[sans.org/sans-2023](http://sans.org/sans-2023)

 **Live Online**  
[sans.org/sans-2023](http://sans.org/sans-2023)

 **OnDemand**  
[sans.org/ondemand](http://sans.org/ondemand)

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



**GNFA**  
Network Forensic  
Analyst  
[giac.org/gnfa](http://giac.org/gnfa)

6  
Day Program

36  
CPEs

18  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- I Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- I Reverse engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- I Decrypt captured SSL/TLS traffic to identify attackers' actions and what data they extracted from the victim
- I Use data from typical network protocols to increase the fidelity of the investigation's findings
- I Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- I Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- I Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past

## Who Should Attend

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

## NICE Framework Work Roles

- I Cyber Defense Incident Responder (OPM 531)
- I Cyber Crime Investigator (OPM 221)
- I Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- I Cyber Defense Forensics Analyst (OPM 212)
- I Threat/Warning Analyst (OPM 141)
- I Target Network Analyst (OPM 132)

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

Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. FOR572 covers the tools, technology, and processes required to integrate network evidence sources into your investigations to provide better findings and get the job done faster.

## Business Takeaways

- I Round out your team's investigations to include network perspective inherent in all environments
- I Build baselines that can be used to proactively identify malicious activity early in a compromise, before large-scale damage is done
- I Provide additional value for existing network data collections that support existing operational requirements
- I Ensure critical observations from the network are not overlooked in proactive hunting or post-compromise IR actions

## Syllabus Summary

**DAY 1:** Off the Disk and Onto the Wire

**DAY 2:** Core Protocols and Log Aggregation/Analysis

**DAY 3:** NetFlow and File Access Protocols

**DAY 4:** Commercial Tools, Wireless, and Full-Packet Hunting

**DAY 5:** Encryption, Protocol Reversing, OPSEC, and Intel

**DAY 6:** Network Forensics Capstone Challenge

**“Best course material on network forensics available. I've learned so many quick tips about how to do things more effectively.”**

—Mike Ahrendt, KPMG

**“I feel like the last week has been a massive eye-opener into what extra info I can now use in my forensic investigations.”**

—Will Barton, Emsou

WAYS TO TRAIN FOR FOR572

At Orlando  
[sans.org/sans-2023](http://sans.org/sans-2023)

 Live Online  
[sans.org/sans-2023](http://sans.org/sans-2023)

 OnDemand  
[sans.org/ondemand](http://sans.org/ondemand)

# FOR578: Cyber Threat Intelligence



**GCTI**  
Cyber Threat  
Intelligence  
[giac.org/gcti](https://giac.org/gcti)

6  
Day Program

36  
CPEs

24  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- I Identify and create intelligence requirements through practices such as threat modeling
- I Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- I Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- I Learn the different sources to collect adversary data and how to exploit and pivot off of those data
- I Validate information received externally to minimize the costs of bad intelligence

## Who Should Attend

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

## NICE Framework Work Roles

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

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, and 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

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

## Syllabus Summary

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

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

**DAY 3:** Collection Sources

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

**DAY 5:** Dissemination and Attribution

**DAY 6:** Capstone

**“Threat intelligence analysis has been an art for too long, now it can finally become a science at SANS. 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



# FOR585: Smartphone Forensic Analysis In-Depth



**GASF**  
Advanced Smartphone  
Forensics  
[giac.org/gasf](http://giac.org/gasf)

6  
Day Program

36  
CPEs

31+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Select the most effective forensic tools, techniques, and procedures to effectively analyze smartphone data
- I Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- I Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- I Interpret file systems on smartphones and locate information that is not generally accessible to users
- I Identify how the evidence got onto the mobile device—so if the user created the date, you avoid the critical mistake of reporting false evidence obtained from tools
- I Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices

## Who Should Attend

- I Experienced digital forensic examiners
- I Media exploitation analysts
- I Information security professionals
- I Incident response teams
- I Law enforcement officers, federal agents, and detectives
- I Accident reconstruction investigators
- I IT auditors
- I Graduates of SANS SEC575, FOR308, FOR498, FOR500, FOR508, FOR518, FOR572, or FOR610 who want to take their skills to the next level

## NICE Framework Work Roles

- I Cyber Crime Investigator (OPM 221)
- I Cyber Defense Forensics Analyst (OPM 212)

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, acquisition shortfalls, extraction techniques (jailbreaks and roots), and encryption. It offers the most unique and current instruction to arm you with mobile device forensic knowledge you can immediately apply to cases you're working on the day you get back to work.

## Business Takeaways

- I Understand Android and iOS artifacts that aid in investigations
- I Understand application artifacts on iOS and Android
- I Leverage smartphone usage to determine device locations when issues occur
- I Gain insight into how a device is used—car connections, hands-free, watches, etc.
- I Decrease potentials of malware infecting mobile devices by understanding how infections occur and how to investigate malware that lands on mobile devices
- I Gain a deep understanding of SQLite databases and how a bulk of smartphone data exists on a device
- I Better understand commercial tools your company is already using and utilize the free scripts the course provides to fill the gaps these tools might have
- I Stay ahead of mobile technology changes and investigative trends with the SANS FOR585 Alumni Community Group

## Syllabus Summary

**DAY 1:** Smartphone Overview, Fundamentals of Analysis, SQLite Introduction, Android Forensics Overview, and Android Backups

**DAY 2:** Android Forensics

**DAY 3:** iOS Device Forensics

**DAY 4:** iOS Backups, Malware and Spyware Forensics, and Detecting Evidence Destruction

**DAY 5:** Third-Party Application Analysis

**DAY 6:** Smartphone Forensic Capstone Exercise

**“This course makes me want to rework every cell-phone case I’ve ever done.”**

—Anastasia L., GWU

**“FOR585 course content provides extremely relevant material, guiding examiners to crucial artifacts for investigations and validation. It outlines key details for every forensic challenge.”**

—Quinn L., U.S. Federal Agency

# FOR608: Enterprise-Class Incident Response & Threat Hunting **NEW**

6  
Day Program

36  
CPES

22  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

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

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

## NICE Framework Work Roles

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

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

—Reggie M., Amazon

FOR608: Enterprise-Class Incident Response & Threat Hunting focuses on identifying and responding to incidents too large for individual machines. By using example tools built to operate at enterprise-class scale, students learn the techniques to collect focused data for incident response and threat hunting. You will also dig into analysis methodologies to learn multiple approaches to understand attacker movement and activity across hosts of varying functions and operating systems by using an array of analysis techniques.

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** Proactive Detection and Response

**DAY 2:** Scaling Response and Analysis

**DAY 3:** Modern Attacks Against Windows and Linux

**DAY 4:** Analyzing macOS and Docker Containers

**DAY 5:** Cloud Attacks and Response

**DAY 6:** Capstone: Enterprise-Class IR Challenge

**“The elastic work was very impressive. I have been using it for a number of years, but it introduced me to new ways to ingest data that could have saved me a lot of work in the past.”**

—Simon H., CyberCX

# FOR610: Reverse-Engineering Malware: Malware Analysis Tools & Techniques



6 Day Program | 36 CPEs | 48 Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- I Build an isolated, controlled laboratory environment for analyzing the code and behavior of malicious programs
- I Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- I Uncover and analyze malicious JavaScript and other components of web pages, which are often used by exploit kits for drive-by attacks
- I Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis
- I Use a disassembler and a debugger to examine the inner workings of malicious Windows executables
- I Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse, and otherwise slow down the analyst
- I Recognize and understand common assembly-level patterns in malicious code, such as code L injection, API hooking, and anti-analysis measures

## Who Should Attend

- I Individuals who deal with incidents involving malware and want to learn how to understand key aspects of malicious programs
- I Technologists who have informally experimented with aspects of malware analysis and are looking to formalize and expand their expertise in this area
- I Forensic investigators and IT practitioners looking to expand skillsets and learn how to play a pivotal role in the incident response process

## NICE Framework Work Roles

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

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

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

## Syllabus Summary

**DAY 1:** Malware Analysis Fundamentals

**DAY 2:** Reversing Malicious Code

**DAY 3:** Analyzing Malicious Documents

**DAY 4:** In-Depth Malware Analysis

**DAY 5:** Examining Self-Defending Malware

**DAY 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 to improve my knowledge of malware techniques, to understand how to better protect assets, and how to successfully complete the eradication steps.”**

—Eric B., Nestle

# SANS Challenge Coins

## The Ultimate Recognition to Elite Cybersecurity Professionals

Hundreds of SANS Institute students have stepped up to the challenge and conquered. They've mastered the concepts and skills, beat out their classmates, and proven their prowess. These are the elite, the recipients of a SANS Challenge Coin, an award given to a select portion of the thousands of students that have taken any of the SANS courses.

The coins—more precisely, Round Metal Objects (RMO)—were initially created to recognize students who demonstrate exceptional talent and significantly contribute to, and lead, the cybersecurity profession and community. The coins are meant to be an honor; they're also intended to be rare. SANS Institute uses the coins to identify and honor those who excel at detecting and eradicating threats, those who understand the critical importance of cybersecurity and continually strive to further not only their own knowledge, but the knowledge of the entire cybersecurity field. These students actively share their experiences and encourage learning through participation in the community; they're typically leaders in the community.

The challenges through which students can earn a coin are typically held on the last day of class for a SANS course. Students compete in a Capture-the-Flag (CTF) or Capstone Challenge and must successfully overcome a number of obstacles to prove their proficiency during timed, hands-on incidents. The CTFs and Capstone Challenges are created by SANS' top instructors—each one a cybersecurity practitioner, subject-matter expert, experienced teacher, and professional leader in their own right.





# Offensive Operations

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

As adversaries evolve and attacks become more sophisticated, pen testers and Red Teams need to emulate current real-world attack techniques, discover issues, and properly report those findings in order to deliver significant value to the security team. Our goal is to continually broaden the scope of our offensive-related courses to cover every possible attack vector of the entire threat landscape.

SANS Offensive Operations courses will teach you to:

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

## Offensive Operations Job Roles:

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

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

—Mike Dozier, Savannah River Nuclear Solutions

# SEC542: Web App Penetration Testing and Ethical Hacking



6  
Day Program

36  
CPEs

30+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- Apply OWASP's methodology to your web application penetration tests to ensure they are consistent, reproducible, rigorous, and under quality control
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL injection flaws to determine true risk to the victim organization
- Understand and exploit insecure deserialization vulnerabilities with ysoserial and similar tools
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks with ZAP, BurP's Intruder, and ffuf

## 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 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

**DAY 1:** Introduction and Information Gathering

**DAY 2:** Content Discovery, Authentication, and Session Testing

**DAY 3:** Injection

**DAY 4:** XSS, SSRF, and XXE

**DAY 5:** CSRF, Logic Flaws, and Advanced Tools

**DAY 6:** Capture the Flag

**“This course 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

**“SEC542 provides rapid exposure to a variety of tools and techniques invaluable to recon on target site.”**

—Gareth Grindle, QA Ltd.

# SEC550: Cyber Deception – Attack Detection, Disruption and Active Defense **NEW**

6  
Day Program

36  
CPEs

15+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

- Understand why cyber deception completely changes the information security game
- Use cyber deception to detect attackers on your network as much as 90% faster than through the use of traditional detection technologies
- Collect actionable threat intelligence and attack attribution information through the use of deception technologies
- Create an environment where attackers need to be perfect to avoid detection, while you need to be right only once to catch them
- Actively engage attackers in real time
- Thwart attacks before attackers send a single packet towards your network
- Take back the advantage from attackers

## Who Should Attend

- General security practitioners
- Deception planners
- Security decision makers
- Security program architects
- Incident responders
- Cyber defenders/Blue Team personnel
- Threat hunters
- Purple teamers
- Chief information security officer (CISO)
- Cybersecurity analyst/engineer

## NICE Framework Work Roles

- Cyber Defense Analyst (OPM 511)

Traditional defensive controls are failing us. The time it takes for an attacker to go from initial compromise to lateral movement is rapidly decreasing while the time it takes to detect and effectively respond to breaches is measured in weeks or even months. To reduce risk, defenders need better ways to quickly detect adversary activity while also collecting information to facilitate faster and more effective response.

SEC550 will provide you with an understanding of the core principles of cyber deception, enabling you to plan and implement cyber deception campaigns to fit virtually any environment. You'll be able to turn the tables on attackers so that while they need to be perfect to avoid detection, you need to be right only once to catch them.

## Business Takeaways

- Design, implement, evaluate, and manage a comprehensive cyber deception program
- Detect attacker activity on your network more quickly
- Reduce false positive alerts
- Respond to attacks more effectively
- Deter or thwart attacks before they occur

## Syllabus Summary

**DAY 1:** Understanding the Problem

**DAY 2:** Deception Foundations

**DAY 3:** Deception Techniques and Technologies, Part I

**DAY 4:** Deception Techniques and Technologies, Part II

**DAY 5:** Deception Concepts, Planning, and Evaluation

**DAY 6:** Capstone Exercise

**“SEC550 is the next step in the evolution of cyber defense—learning how to make the hackers’ jobs harder, tracking their movement, and getting attribution.”**

—Mike Leach, Nationwide

**“I think this is industry-changing information and tactics—the potential to shift from reactive to proactive defense.”**

—Jamey Kistner, Torrid

# SEC560: Enterprise Penetration Testing **NEW**



**6**  
Day Program

**36**  
CPEs

**30+**  
Labs

Sunday, April 2–Friday, April 7

## 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)

**\*DoDD 8140**

Vulnerability Assessment Analyst  
[sans.org/dod/dodd-8140](https://sans.org/dod/dodd-8140)

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

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

- It offers in-depth technical excellence along with industry-leading methodologies to conduct high-value penetration tests
- We drill deep into 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
- We discuss 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
- We 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
- The course sections address common pitfalls that arise in penetration tests and ethical hacking projects, providing real-world strategies and tactics to avoid these problems and maximize the quality of test results
- We cover several 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
- The course stresses 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
- We analyze how penetration testing and ethical hacking should fit into a comprehensive enterprise information security program
- We focus on pen testing modern organizations, many of which are using Azure AD for identity management

## Syllabus Summary

**DAY 1:** Comprehensive Pen Test Planning, Scoping, and Recon

**DAY 2:** In-Depth Scanning and Initial Access

**DAY 3:** Assumed Breach, Post-Exploitation, and Passwords

**DAY 4:** Lateral Movement and Command and Control (C2)

**DAY 5:** Domain Domination and Azure Annihilation

**DAY 6:** Penetration Test and Capture-the-Flag Exercise

WAYS TO TRAIN FOR SEC560

**At Orlando**  
[sans.org/sans-2023](https://sans.org/sans-2023)

**Live Online**  
[sans.org/sans-2023](https://sans.org/sans-2023)

**OnDemand**  
[sans.org/ondemand](https://sans.org/ondemand)

# SEC588: Cloud Penetration Testing **NEW**



**GCPN**  
Cloud Penetration  
Tester  
[giac.org/gcpn](https://giac.org/gcpn)

6  
Day Program

36  
CPEs

28  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

Both attack-focused and defense-focused security practitioners will benefit significantly from SEC588 by understanding vulnerabilities, insecure configurations, and the associated business risk to their organizations. The course is designed to help penetration testers, vulnerability analysts, risk assessment officers, DevOps engineers, site reliability engineers, and those working in many other areas.

## 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)
- Cyber Ops Planner (OPM 332)

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

—Jonus Gerrits, Phillips66

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
- Learn 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

**DAY 1:** Architecture, Discovery, and Recon at Scale

**DAY 2:** Attacking Identity Systems

**DAY 3:** Attacking and Abusing Cloud Services

**DAY 4:** Vulnerabilities in Cloud-Native Applications

**DAY 5:** Infrastructure Attacks and Red Teaming

**DAY 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



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



**GDAT**  
Defending Advanced  
Threats  
[giac.org/gdat](https://giac.org/gdat)

6  
Day Program

36  
CPEs

25  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

- I Security architects and security engineers
- I Red teamers and penetration testers
- I Technical security managers
- I Security Operations Center analysts and engineers
- I Individuals looking to better understand how persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents

## NICE Framework Work Roles

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

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

- I Understand how recent high-profile attacks were delivered and how they could have been stopped
- I 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

**DAY 1:** Introduction and Reconnaissance

**DAY 2:** Payload Delivery and Execution

**DAY 3:** Exploitation, Persistence, and Command and Control

**DAY 4:** Lateral Movement

**DAY 5:** Action on Objectives, Threat Hunting, and Incident Response

**DAY 6:** APT Defender Capstone

**“SEC599 gave me interesting insight into Exploit Guard that will certainly drive great conversation at work. Best labs of any class I’ve taken.”**

—Jeremiah Hainly, The Hershey Company

**“SEC599 is an excellent course. Every tool, technique, and process discussed during the course can be applied to real-world environments with little additional information required, and there isn’t a single thing learned that can’t be used to improve the cybersecurity position of clients.”**

—Mac Connolly

**“SEC599 is a very well structured look at the attacker life cycle and how to defend each stage so that even if defense fails, detection is faster.”**

—Taz Wake, Halkyn Consulting

# SEC660: Advanced Penetration Testing, Exploit Writing & Ethical Hacking



6  
Day Program

46  
CPEs

30+  
Labs

Sunday, April 2–Friday, April 7

## You Will Be Able To

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

## Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

## NICE Framework Work Roles

- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Exploitation Analyst (OPM 121)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Cyber Operator (OPM 321)

SEC660 is designed as a logical progression point for students who have completed SEC560: Network Penetration Testing and Ethical Hacking or for those with existing penetration testing experience. This course provides you with in-depth knowledge of the most prominent and powerful attack vectors and furnishes an environment to perform these attacks in numerous hands-on scenarios. The course goes far beyond simple scanning for low-hanging fruit and teaches you how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

## 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

## Syllabus Summary

**DAY 1:** Network Attacks for Penetration Testers

**DAY 2:** Crypto and Post-Exploitation

**DAY 3:** Python, Scapy, and Fuzzing

**DAY 4:** Exploiting Linux for Penetration Testers

**DAY 5:** Exploiting Windows for Penetration Testers

**DAY 6:** Capture-the-Flag Challenge

**“SEC660 has been nothing less than excellent. Both the instructor and assistant are subject-matter experts who have extensive knowledge covering all aspects of the topics covered and then some.”**

—Brian Anderson, Northrop Grumman Corporation

**“The quality of the labs and coursework in SEC660 showcases the value SANS training has over other providers. It was an excellent, challenging, and rewarding course.”**

—Michael R., U.S. Military

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

5  
Day Program

30  
CPes

30+  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- Use automation strategies such as Ansible, Docker, and Terraform to deploy a full multi-domain enterprise environment
- Execute adversary emulations at the press of a button with Covenant, Caldera, and Prelude Operator
- Build a proper process, tooling, and planning for purple teaming
- Build adversary emulation plans mimicking threat actors such as APT-28, APT-34, and Turla
- Execute techniques such as Kerberos Delegation attacks, Attack Surface Reduction/Applocker bypasses, AMSI, Process Injection, and COM Object Hi-jacking

## Who Should Attend

- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Red team members
- Blue team members
- Purple Team members
- Forensics specialists who want to better understand offensive tactics

## 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)

This course provides advanced purple team training, with a focus on adversary emulation for data breach prevention and detection. Throughout this course, students will learn how real-life threat actors can be emulated in a realistic enterprise environment, including multiple AD forests. In true purple fashion, the goal of the course is to educate students on how adversarial techniques can be emulated (manual and automated) and detected (use cases/rules and anomaly-based detection). A natural follow-up to SEC599, this is an advanced SANS course offering, with 60 percent of class time spent in 29 hands-on labs!

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** Introduction and Key Tools

**DAY 2:** Initial Intrusion Strategies Emulation and Detection

**DAY 3:** Lateral Movement Emulation and Detection

**DAY 4:** Persistence Emulation and Detection

**DAY 5:** Running Adversary Emulation Campaigns

**“I’ve been in this field a long time, and I’ve learned something new from each segment of SEC699. That’s not something I’m used to at this point in my career.”**

—Taya Steere, Lyft

**“Overall, SEC699 was the best course I’ve followed as an incident responder and SOC analyst. It stimulates the real-world attacks and defending possibilities using numerous kinds of techniques. It provided me with a structure and focus on how to mature our current SOC capabilities.”**

—Maurice Von Wintersport, Philips

# Cybersecurity Leadership

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

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

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

SANS Cybersecurity Leadership courses will teach you to:

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

## Cybersecurity Leadership Job Roles:

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

**“This training applies to all aspects of my job,  
from network management to project management.”**

—David Chaulk, Enbridge

# MGT512: Security Leadership Essentials for Managers



5 Day Program | 30 CPEs | 23 Labs  
Sunday, April 2–Thursday, April 6

## You Will Be Able To

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage and lead technical teams and projects
- Build a vulnerability management program
- Inject security into modern DevOps workflows

## Who Should Attend

Security analysts, security engineers, security researchers, cloud engineers, DevOps engineers, security auditors, system administrators, operations personnel, and anyone who is responsible for:

- Evaluating and adopting new cloud offerings
- Researching new vulnerabilities and developments in cloud security
- Handling identity and access management
- Managing a cloud-based virtual network
- Secure configuration management

## NICE Framework Work Roles

- Authorizing Official/Designating Representative (OPM 611)
- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Security Awareness & Communications Manager (OPM 712)
- Information Systems Security Manager (OPM 722)
- Communications Security (COMSEC) Manager (OPM 723)
- Cyber Workforce Developer and Manager (OPM 751)
- Cyber Policy and Strategy Planner (OPM 752)
- Executive Cyber Leadership (OPM 901)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)
- Product Support Manager (OPM 803)
- IT Investment/Portfolio Manager (OPM 804)

\*DoDD 8140  
IAM Level 1, 2, 3  
[sans.org/dod/dodd-8140](https://sans.org/dod/dodd-8140)

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

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 that 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

**DAY 1:** Building Your Security Program

**DAY 2:** Technical Security Architecture

**DAY 3:** Security Engineering

**DAY 4:** Security Management and Leadership

**DAY 5:** Detecting and Responding to Attacks

**“I’m really enjoying the flow between the content delivery and the Cyber42 game.”**

—Jamil A., U.S. Government

**“The [Cyber42] ‘game’ we are playing makes you think about real world problems and the different teams show how different groups will come up with their own solutions for the same problem. One of the few ‘games’ that actually forces some decisions based on previous decisions.”**

—Max H., U.S. Government

WAYS TO TRAIN FOR MGT512

At Orlando  
[sans.org/sans-2023](https://sans.org/sans-2023)

Live Online  
[sans.org/sans-2023](https://sans.org/sans-2023)

OnDemand  
[sans.org/ondemand](https://sans.org/ondemand)



# MGT514: Security Strategic Planning, Policy, and Leadership



**GSTRT**  
Strategic Planning,  
Policy, and Leadership  
[giac.org/gstrt](https://giac.org/gstrt)

5  
Day Program

30  
CPEs

15  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- I Develop strategic security plans
- I Create effective information security policy
- I Understand the different phases of the strategic planning process
- I Apply increased knowledge of key planning tools
- I Cultivate fundamental skills to create strategic plans that protect your company
- I Enable key innovations
- I Facilitate working effectively with your business partners
- I Advance security strategic plans that incorporate business and organizational drivers

## Who Should Attend

- I CISOs
- I Information security officers
- I Security directors
- I Security managers
- I Aspiring security leaders
- I Security personnel who have team lead or management responsibilities
- I Anyone who wants to go beyond technical skills
- I Technical professionals who want to learn to communicate with senior leaders in business terms

## NICE Framework Work Roles

- I Executive Cyber Leadership: OV-EXL-001
- I Information Systems Security Manager: OV-MGT-001
- I Program Manager: OV-PMA-001
- I IT Project Manager: OV-PMA-002
- I Cyber Workforce Developer and Manager: OV-SSP-0001
- I Cyber Policy and Strategy Planner: OV-SPP-002

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

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

## Syllabus Summary

**DAY 1:** Strategic Planning Foundations

**DAY 2:** Strategic Roadmap Development

**DAY 3:** Security Policy Development and Assessment

**DAY 4:** Leadership and Management Competencies

**DAY 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 to 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: Managing Security Vulnerabilities: Enterprise and Cloud

5  
Day Program

30  
CPEs

16+  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- Create, implement, and mature your vulnerability management program and get buy-in from your stakeholders
- Utilize techniques for building and maintaining 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

## Who Should Attend

- CISOs
- Vulnerability program managers and analysts managing vulnerabilities in the enterprise or cloud
- Information security managers, architects, analysts, officers, and directors
- Aspiring information security leaders
- Risk management, business continuity, and disaster recovery professionals
- IT operations managers and administrators
- Cloud service managers, administrators, integrators, developers, and brokers
- Cloud service security and risk managers
- Government IT professionals who manage vulnerabilities in the enterprise or cloud

## NICE Framework Work Roles

- Program Manager: OV-PMA-001
- Information Systems Security Manager: OV-MGT-001
- Security Architect: SP-ARC-001
- Enterprise Architect: SP-ARC-002
- Cyber Workforce Developer and Manager: OV-SPP-001
- Cyber Policy & Strategy Planner: OV-SPP-002
- IT Project Manager: OV-PMA-001
- IT Program Auditor: OV-PMA-005
- Executive Cyber Leadership: OV-EXL-001
- Information Systems Security Developer: SP-SYS-001
- Systems Developer: SP-SYS-002
- System Administrator: OM-ADM-001
- Database Administrator: OM-DTA-001
- Research & Development Specialist: SP-TRD-001
- Security Control Assessor: SP-RSK-002
- Security Awareness & Communications Manager: OV-TEA-003

Vulnerability, patch, and configuration management are not new security topics. In fact, they are some of the oldest security functions, and yet we still struggle to manage these capabilities effectively. The quantity of outstanding vulnerabilities for most large organizations is overwhelming, and all organizations struggle to keep up with the never-ending onslaught of new vulnerabilities in their infrastructure and applications. When you add in the cloud and the increasing speed with which all organizations must deliver systems, applications, and features to both their internal and external customers, security may seem unachievable. This course will show you the most effective ways to mature your vulnerability management program and move from identifying vulnerabilities to successfully treating them.

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** Overview: Cloud and Asset Management

**DAY 2:** Identify

**DAY 3:** Analyze and Communicate

**DAY 4:** Treat

**DAY 5:** Buy-in, Program, and Maturity

**“An understanding of vulnerability management and cloud security is becoming not only valuable but a necessity to keep one’s organization secure in this constantly changing and dynamic environment.”**

—Kae David, EY

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

5  
Day Program

30  
CPEs

16  
Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- I More effectively communicate the business value of cybersecurity to your Board of Directors and executives, improve collaboration with your peers, and more effectively engage your workforce
- I Explain what organizational culture is, its importance to cybersecurity, and how to map and measure both your organization's overall culture and security culture
- I Align your cybersecurity culture to your organization's strategy, including how to leverage different security frameworks and maturity models
- I Explain what organizational change is, identify different models for creating change, and learn how to apply those models
- I Enable and secure your workforce by integrating cybersecurity into all aspects of your organization's culture
- I Dramatically improve both the effectiveness and impact of your security initiatives, such as DevSecOps, Cloud migration, Vulnerability Management, Security Operations Center, and other related security deployments

## Who Should Attend

- I Chief information security officers
- I Chief risk officers/risk management leaders
- I Security awareness, engagement, or culture managers
- I Senior security managers who lead large-scale security initiatives
- I Information security managers, officers, and directors
- I Information security architects and consultants
- I Aspiring information security leaders
- I Business continuity/disaster recover leaders
- I Privacy/ethics officers

## NICE Framework Work Roles

- I Security Awareness and Communications Manager: OV-TEA-003
- I Authorizing Official/Designating Representative: SP-RSK-001
- I Security Control Assessor: SP-RSK-002
- I Information Systems Security Manager: OV-MGT-001
- I Communications Security Manager: OV-MGT-002

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.

## Business Takeaways

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

## Syllabus Summary

**DAY 1:** Fundamentals of Culture and Organizational Change

**DAY 2:** Motivating Change

**DAY 3:** Enabling and Measuring Change

**DAY 4:** Making the Business Case

**DAY 5:** Capstone Workshop

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

—Lindsay O'Bannon, Deloitte Global

**“Entertaining and thought provoking and helped me understand what actions I can take to change the culture of my company.”**

—Kevin Nicholl

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

 **Live Online**  
[sans.org/sans-2023](https://sans.org/sans-2023)

 **OnDemand**  
[sans.org/ondemand](https://sans.org/ondemand)

# MGT551: Building and Leading Security Operations Centers



**GSOM**  
Security Operations  
Manager  
[giac.org/gsom](https://giac.org/gsom)

5 Day Program | 30 CPEs | 15 Labs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- I Collecting the most important logs and network data
- I Build, train, and empower a diverse team
- I Create playbooks and manage detection use cases
- I Use threat intelligence to focus your budget and detection efforts
- I Understand threat hunting and active defense strategies
- I Implement efficient alert triage and investigation workflow
- I Implement effective incident response planning and execution
- I Choose metrics and long-term strategy to improve the SOC

## Who Should Attend

This course is intended for those who are looking to build a Security Operations Center (SOC) for the first time or improve the one their organization is already running. Ideal student job roles for this course include:

- I SOC managers or leads
- I Security directors
- I New security operations team members
- I Lead/senior SOC analysts
- I Technical CISOs and security directors

## NICE Framework Work Roles

- I Information Security Manager: OV-MGT-001
- I Cyber Policy and Strategy Planner: OV-SPP-002
- I Executive Cyber Leadership: OV-EXL-001
- I Program Manager: OV-PMA-001
- I Cyber Defense Incident Responder: PR-CIR-001
- I OT SOC Operator

Information technology is so tightly woven into the fabric of modern business that cyber risk has become business risk. Security Operations Centers (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 your defenses around your 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

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

## Syllabus Summary

**DAY 1:** SOC Design and Operational Planning

**DAY 2:** SOC Telemetry and Analysis

**DAY 3:** Attack Detection, Hunting, and Triage

**DAY 4:** Incident Response

**DAY 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

# SEC566: Implementing and Auditing Security Frameworks and Controls



**GCCC**  
Critical Controls  
[giac.org/gccc](https://giac.org/gccc)

5  
Day Program

30  
CPEs

13  
Labs

Sunday, April 2–Thursday, April 6

## 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 network 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

## Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Compliance analysts
- IT administrators
- Department of Defense (DoD) personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC440, MGT516, MGT551, MGT512, SEC401, or SEC501

## NICE Framework Work Roles

- Security Control Assessor – SP-RSK-002

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/IEC 27000, and other frameworks into a cohesive strategy to defend your organization while complying with industry standards.

## Business Takeaways

- Maximize compliance analyst's time 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
- Report the status of cybersecurity defense efforts to senior leadership in clear terms

## Syllabus Summary

**DAY 1:** Introduction and Overview of the CIS Critical Controls

**DAY 2:** Data Protection, Identity and Authentication, Access Control Management, Audit Log Management

**DAY 3:** Server, Workstation, Network Device Protections (Part 1)

**DAY 4:** Server, Workstation, Network Device Protections (Part 2)

**DAY 5:** Governance and Operational Security

**“A comprehensive walk-through of the Critical Security Controls, not just focusing on the ‘what,’ but, more importantly, the ‘why.’ It’s been an invaluable learning experience for me.”**

—Justin Cornell, LOM (UK) Limited

**“All labs were easy to follow and performed as expected.”**

—Shawn Bilak, Southern Company



# Industrial Control Systems (ICS) Security

The current landscape presents a diverse and chaotic picture of the threats facing industrial control system owners and operators.

Attacks that cause physical damage or impact physical processes are no longer limited to theory or speculation. We are now seeing incidents where malicious actors successfully intrude, cause system damage, and impact operations using ICS-tailored malware. You need to be prepared to defend your control systems against increasingly sophisticated adversaries.

SANS ICS Security courses will teach you to:

- Recognize ICS components, purposes, deployments, significant drivers, and constraints
- Identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats
- Understand approaches to system and network defense architectures and techniques
- Perform ICS incident response focusing on security operations and prioritizing the safety and reliability of operations
- Implement effective cyber and physical access controls

## ICS Job Roles:

- ICS/OT Security Assessment Consultant
- ICS Security Engineer
- ICS Security Analyst
- Control Systems Engineer
- ICS Cybersecurity Engineer
- ICS/OT Security Manager

**“The training starts with theory and quickly progresses into full hands-on interaction with all components. This experience is not easy to find.”**

—Bassem Hemida, Deloitte

# ICS612: ICS Cybersecurity In-Depth

5

Day Program

31

CPEs

Sunday, April 2–Thursday, April 6

## You Will Be Able To

- Learn active and passive methods to safely gather information about an ICS environment
- Identify vulnerabilities in ICS environments
- Determine how attackers can maliciously interrupt and control processes and how to build defenses
- Implement proactive measures to prevent, detect, slow down, or stop attacks
- Understand ICS operations and what “normal” looks like
- Build choke points into an architecture and determine how they can be used to detect and respond to security incidents
- Manage complex ICS environments and develop the capability to detect and respond to ICS security events

## Who Should Attend

- ICS410 Course 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

**“Excellent content combined with real-world labs and stories is an awesome combination.”**

—Michael Bruggeman, Wipro

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.

## Author Statement

“I am very excited to be part of the author team that has worked on and will be bringing this great course to the dedicated industrial control system community. This course has been designed to provide students with practitioner-focused, hands-on lab exercises that have been developed to reinforce the skills necessary for professionals working to defend critical operational environments. As these control system environments become increasingly cyber-enabled, interconnected, and targeted by adversaries; it is essential that the capabilities of the workforce continue to progress in order to ensure safe and reliable operations. The lab exercises, tools, control system components, exposure to leading ICS solutions, and development of expanded defender capabilities in this course will be immediately applicable for students.”

—Tim Conway, ICS Curriculum Director

## Syllabus Summary

**DAY 1:** The Local Process

**DAY 2:** System of Systems

**DAY 3:** ICS Network Infrastructure

**DAY 4:** ICS System Management

**DAY 5:** Covfefe Down!

**“I would overall recommend this course to anyone in my organization because it provides hands-on and a comprehensive view of the subject. Top of the line.”**

—Michael D., U.S. Military

**“Awesome course and lab with the best instructor ever!!!”**

—YD Badger

**“Best course ever. This should be a semester, not one week.”**

—Michael Jacobs, Saudi Aramco

**SANS TECHNOLOGY INSTITUTE**

An NSA Center of Academic Excellence in Cyber Defense

# 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**

**SANS**  
**TECHNOLOGY**  
**INSTITUTE**

# SANS Faculty



**SANS instructors are a select group of highly skilled practitioners who have earned respect and recognition as being among the top minds in cybersecurity. Not only have these individuals proven their expertise in the field, they have demonstrated extraordinary ability to train others to progress their own capabilities.**

## SANS Faculty at a Glance

### 150+ Instructors

Each of our 120+ certified instructors is a highly skilled professional currently working in cybersecurity.

### 16+ Years

SANS faculty spend an average of more than 16 years as cybersecurity practitioners before being selected to become SANS Certified Instructors.

### 40+ Books

SANS faculty members have authored more than 40 books on information security.

### 150+ Tools

More than 150 open-source cybersecurity tools have been created by SANS Instructors. List of tools available at [sans.org/free](https://sans.org/free).

### 3,500+ Resources

SANS faculty members have produced more than 3,500 research papers and webcasts on information security topics.

## Commitment

SANS instructors are committed to providing engaging and active learning environments focused on key skills, taught through lecture, immersive hands-on labs, and interactive discussions. “Passionate” is a word many use to describe a 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](https://sans.org/instructors)

# SANS CYBER RANGES

## Skills Assessment and Practical Application

SANS Cyber Ranges focus on practical application and skills assessment, offering insight into what you and your team are excelling at and what skills warrant additional training and practice. Range participants problem-solve and develop skills through interactive, story-driven exercises that bring real-world context to the challenges at hand. SANS Cyber Ranges cover a broad spectrum of disciplines and the full range of difficulty levels, from beginner to expert.



### Grow Your Expertise

There is a natural progression from one range to another as the disciplines increase in specialty, complexity, seniority, and risk. Ranges are built upon each other to form a holistic and complete practice portfolio for our students to experience.

Learn more about SANS Cyber Ranges, upcoming range events, pricing, and more at [sans.org/cyber-ranges](https://sans.org/cyber-ranges)





# SECURITY AWARENESS

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, organizations gain a comprehensive, data-driven approach to managing their unique levels of human risk.

### EndUser Training

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.

### Phishing Simulation

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.

## 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.

### IT Administrator Training

Twelve modules highlighting real-world attack and mitigation scenarios progress learners along an increasingly complex training path that includes topics such as: Attack Mitigation Technologies, Supply Chain Attacks, and Security Program Management among others.

### Developer Training

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.

### Industrial Control System (ICS) Training

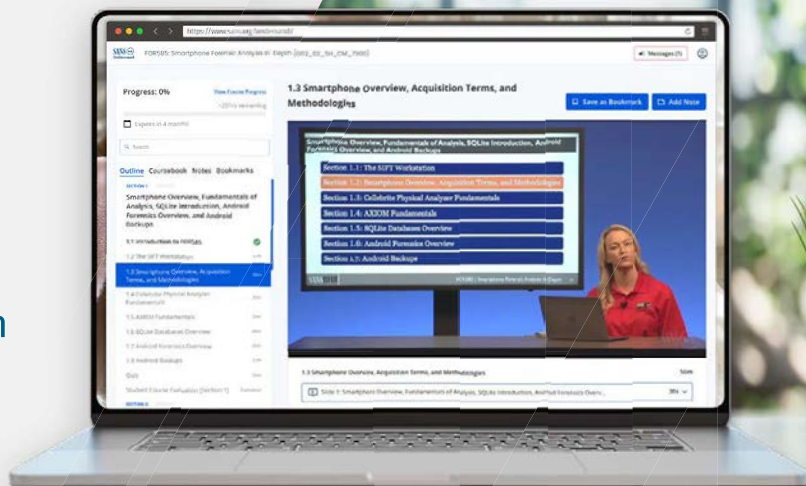
One-of-a-kind training built exclusively around protecting critical infrastructure over 12 modules that provide a progressive and engaging learning path.

Visit [sans.org/awareness](https://sans.org/awareness) to learn more.

# SANS OnDemand

Train at your own pace  
anytime, anywhere with  
SANS OnDemand

[sans.org/ondemand](https://sans.org/ondemand)



**SANS OnDemand** offers our world-class cybersecurity training in a self-paced online training format, with four months of extended access to your course and labs. Enjoy the ultimate learning flexibility with OnDemand—rewind and revisit your training content so you can reinforce the material and improve retention.

**With complete control over the pace of learning, SANS OnDemand fits every learning style.**

- ▶ Students can control the pace, learning environment, and schedule
- ▶ Instructor lectures, class exercises, and virtual labs are available for four months
- ▶ Repeatable hands-on labs and quizzes help you prepare for 40+ different GIAC exams
- ▶ No travel budget, no problem. Learn from anywhere. Home, office, or on the road
- ▶ On your own, but not alone. SANS subject-matter experts are available to answer your questions

“I don’t think I would get nearly as much out of this course if I did not get the class material delivered via the OnDemand platform. It’s an excellent way to replay content and critical topics.”

—Kenneth Huss, Cisco

## Limited-Time SANS Online Training Specials

Options include tablets, laptops, or discounts. For more information visit:  
[sans.org/ondemand](https://sans.org/ondemand)



## New SANS OnDemand Training App

Allows You to Take  
Cybersecurity Training  
Anywhere, Anytime.



# SANS Summits

**YOUR Community –  
Working TOGETHER to Solve  
Cybersecurity Challenges TODAY**

BREAKING CONTENT

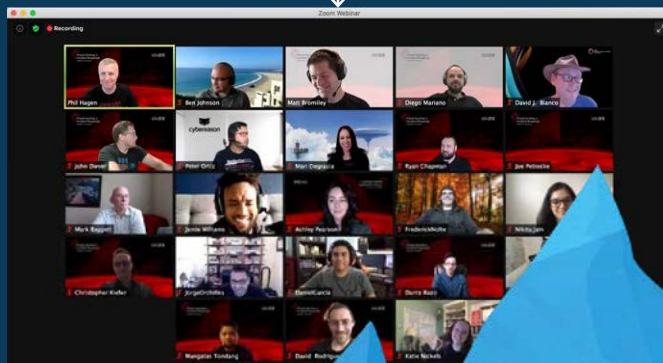
NEVER-BEFORE-SEEN RESEARCH

SOLUTIONS YOU CAN USE

**In-Person with  
Exclusive Benefits**

OR

**Online Free for the  
Global Community**



## 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.

“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

## Upcoming SANS Summit & Training Events

### Cyber Threat Intelligence

Crystal City, VA & Virtual

SUMMIT: Jan 30–31 | TRAINING: Feb 1–6

### New2Cyber

Baltimore, MD & Virtual

SUMMIT: Mar 14

### ICS Security

Orlando, FL & Virtual

SUMMIT: May 1–2 | TRAINING: May 3–8

### CloudSecNext

Denver, CO & Virtual

SUMMIT: Jun 12–13 | TRAINING: Jun 14–19

## Additional Summits planned for 2023

- Ransomware
- Security Awareness
- Blockchain Security
- Cybersecurity Leadership
- Blue Team
- Pentest Hackfest

Visit [sans.org/summits](https://sans.org/summits) for the full schedule.



# NICE Framework

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

Use this as a blueprint to organize cybersecurity work into Categories, Specialty Areas, Work Roles Tasks, and Knowledge, Skills, and Abilities (KSAs).

[www.nist.gov/itl/applied-cybersecurity/nice](http://www.nist.gov/itl/applied-cybersecurity/nice)

Analyze (AN)			
NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)	
Threat Analysis (TWA)	Threat/Warning Analyst	FOR578 (GCTI)	FOR572 (GNFA)
		SEC504 (GCIH)	FOR589
Exploitation Analysis (EXP)	Exploitation Analyst	SEC497 (GOSI)	FOR610 (GREM)
		FOR532	FOR710
All-Source Analysis (ASA)	All-Source Analyst	SEC660 (GPEN)	SEC661
		SEC660 (GXPN)	SEC542 (GWAPT)
All-Source Analysis (ASA)	Mission Assessment Specialist	FOR578 (GCTI)	FOR532
		SEC497 (GOSI)	FOR589
All-Source Analysis (ASA)	Mission Assessment Specialist	SEC504 (GCIH)	FOR578 (GCTI)
		SEC560 (GPEN)	FOR532
All-Source Analysis (ASA)	Mission Assessment Specialist	SEC588 (GCPN)	FOR589
		SEC560 (GPEN)	SEC699
Targets (TGT)	Target Developer	SEC442 (GWAPT)	FOR509 (GCFR)
		SEC565	FOR518 (GIME)
Targets (TGT)	Target Developer	SEC588 (GCPN)	FOR532
		SEC660 (GXPN)	FOR585 (GASF)
Targets (TGT)	Target Developer	SEC760	FOR589
		SEC661	FOR572 (GNFA)
Targets (TGT)	Target Developer	SEC599 (GDAT)	FOR572 (GNFA)
		SEC497 (GOSI)	FOR532
Targets (TGT)	Target Network Analyst	FOR578 (GCTI)	FOR589
		SEC504 (GCIH)	FOR572 (GNFA)
Targets (TGT)	Target Network Analyst	SEC560 (GPEN)	FOR572 (GNFA)

Collect and Operate (CO)			
NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)	
Collection Operations (CLO)	All Source-Collection Manager	SEC497 (GOSI)	FOR518 (GIME)
		FOR498 (GBFA)	FOR532
Collection Operations (CLO)	All Source-Collection Manager	FOR578 (GCTI)	FOR589
		FOR508 (GCFA)	FOR608
Collection Operations (CLO)	All Source-Collection Manager	FOR509 (GCFR)	FOR608
		SEC497 (GOSI)	FOR509 (GCFR)
Cyber Operational Planning (OPL)	Cyber Ops Planner	FOR498 (GBFA)	FOR532
		FOR578 (GCTI)	FOR589
Cyber Operational Planning (OPL)	Cyber Ops Planner	FOR508 (GCFA)	FOR589
		SEC497 (GOSI)	FOR532
Cyber Operational Planning (OPL)	Cyber Ops Planner	SEC565	SEC699
		SEC560 (GPEN)	SEC599 (GDAT)
Cyber Operational Planning (OPL)	Cyber Ops Planner	SEC542 (GWAPT)	SEC467
		SEC588 (GCPN)	SEC556
Cyber Operational Planning (OPL)	Cyber Ops Planner	SEC660 (GXPN)	SEC497 (GOSI)
		SEC660 (GXPN)	SEC497 (GOSI)
Cyber Operations (OPS)	Cyber Operator	SEC565, SEC699	FOR589
		SEC599 (GDAT)	FOR578 (GCTI)
Cyber Operations (OPS)	Cyber Operator	FOR532	FOR578 (GCTI)
		FOR508 (GCFA)	FOR608
Cyber Operations (OPS)	Cyber Operator	FOR528	SEC560 (GPEN)
		FOR532	SEC660 (GXPN)
Cyber Operations (OPS)	Cyber Operator	FOR572 (GNFA)	SEC556
		FOR578 (GCTI)	SEC467
Cyber Operations (OPS)	Cyber Operator	FOR589	SEC573 (GPVC)

Industrial Control Systems (NICE 2020)			
NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)	
Operations Technology Engineering	Process Control Engineer/Instrument & Control Engineer	ICS410 (GICSP)	ICS612
	ICS/SCADA Security Engineer	ICS410 (GICSP)	ICS515 (GRID)
	ICS/OT Systems Engineer	ICS410 (GICSP)	ICS515 (GRID)
OT Security Operations Center	OT SOC Operator	ICS410 (GICSP)	ICS418

Oversee and Govern (OV)			
NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)	
Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	LEG523 (GLEG)	SEC403
	Privacy Officer/Privacy Compliance Manager	SEC301 (GISF)	ICS456 (GCIP)
Legal Advice and Advocacy (LGA)	Privacy Officer/Privacy Compliance Manager	MGT512 (GSLC)	SEC504 (GCIH)
	Privacy Officer/Privacy Compliance Manager	MGT512 (GSLC)	SEC504 (GCIH)
Training, Education and Awareness (TEA)	Cyber Instructional Curriculum Developer	SEC401 (GSEC)	MGT521
	Cyber Instructional Curriculum Developer	MGT433 (SSAP)	SEC504 (GCIH)
Training, Education and Awareness (TEA)	Cyber Instructor	SEC401 (GSEC)	SEC501 (GCED)
	Cyber Instructor	SEC504 (GCIH)	SEC403, SEC402
Training, Education and Awareness (TEA)	Security Awareness & Communications Manager	MGT433 (SSAP)	SEC402
	Security Awareness & Communications Manager	MGT512 (GSLC)	SEC403
Cybersecurity Management (MGT)	Information Systems Security Manager	MGT512 (GSLC)	MGT551 (GSOM)
	Information Systems Security Manager	MGT514 (GSTRT)	SEC504 (GCIH)
Cybersecurity Management (MGT)	Communications Security (COMSEC) Manager	MGT520	SEC488 (GCLD)
	Communications Security (COMSEC) Manager	MGT521	SEC488 (GCLD)
Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	SEC301 (GISF)	SEC504 (GCIH)
	Cyber Workforce Developer and Manager	MGT512 (GSLC)	SEC504 (GCIH)
Strategic Planning and Policy (SPP)	Cyber Policy and Strategy Planner	MGT512 (GSLC)	SEC504 (GCIH)
	Cyber Policy and Strategy Planner	MGT514 (GSTRT)	SEC504 (GCIH)
Executive Cyber Leadership (EXL)	Executive Cyber Leadership	MGT512 (GSLC)	MGT551 (GSOM)
	Executive Cyber Leadership	MGT514 (GSTRT)	SEC504 (GCIH)
Program/Project Management (PMA) and Acquisition	Program Manager	MGT512 (GSLC)	MGT520
	Program Manager	MGT514 (GSTRT)	MGT521
Program/Project Management (PMA) and Acquisition	IT Project Manager	MGT512 (GSLC)	MGT520
	IT Project Manager	MGT525 (GCPM)	MGT521
Program/Project Management (PMA) and Acquisition	Product Support Manager	MGT512 (GSLC)	MGT520
	Product Support Manager	MGT525 (GCPM)	MGT521
Program/Project Management (PMA) and Acquisition	IT Investment/Portfolio Manager	SEC401 (GSEC)	MGT512 (GSLC)
	IT Investment/Portfolio Manager	SEC504 (GCIH)	MGT512 (GSLC)
Program/Project Management (PMA) and Acquisition	IT Program Auditor	AUD507 (GSNA)	SEC402
	IT Program Auditor	SEC460 (GEVA)	SEC403

Securely Provision (SP)			
NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)	
Risk Management (RSK)	Authorizing Official/ Designating Representative	SEC301 (GISF) MGT512 (GSLC) MGT415	SEC402 SEC403
	Security Control Assessor	SEC460 (GEVA) AUD507 (GSNA) SEC560 (GPEN) SEC542 (GWAPT) SEC588 (GCPN)	SEC401 (GSEC) SEC510 (GCPS) SEC566 (GCCC) MGT516 SEC588 (GCPN)
Software Development (DEV)	Software Developer	SEC522 (GWEB) SEC540 (GCSA)	SEC542 (GWAPT)
	Secure Software Assessor	SEC542 (GWAPT) SEC510 (GCPS) SEC522 (GWEB)	SEC540 (GCSA) SEC573 (GPYC)
Systems Architecture (ARC)	Enterprise Architect	SEC530 (GDSA) SEC510 (GPCS)	SEC540 (GCSA)
	Security Architect	SEC488 (GCLD) SEC511 (GMON)	SEC530 (GDSA) SEC510 (GPCS)
Technology R&D (TRD)	Research & Development Specialist	SEC568 SEC573 (GPYC) SEC540 (GCSA)	SEC522 (GWEB) SEC510 (GPCS)
Systems Requirements Planning (SRP)	Systems Requirements Planner	MGT525 (GCPM) SEC402 SEC403	
Test and Evaluation (TST)	System Testing & Evaluation Specialist	SEC460 (GEVA) SEC568 SEC560 (GPEN) SEC588 (GCPN) SEC542 (GWAPT)	SEC556 AUD507 (GSNA), SEC402 SEC403
Systems Development (SYS)	Information Systems Security Developer	SEC540 (GCSA) SEC522 (GWEB) SEC542 (GWAPT)	SEC510 (GPCS)
	Systems Developer	SEC540 (GCSA) SEC522 (GWEB)	SEC542 (GWAPT)

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

Protect and Defend (PR)			
NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)	
Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst	SEC401 (GSEC) SEC450 (GSOC) SEC504 (GCIH) SEC501 (GCED) SEC503 (GCIA) SEC511 (GMON) SEC573 (GPYC) SEC541	SEC586 SEC550 FOR532 FOR578 (GCTI) FOR589 FOR610 (GREM) FOR710
Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	SEC568 SEC401 (GSEC) SEC450 (GSOC) SEC501 (GCED)	SEC511 (GMON) SEC586 SEC460 (GEVA)
Incident Response (CIR)	Cyber Defense Incident Responder	SEC504 (GCIH) FOR508 (GCFA) FOR572 (GNFA) FOR509 (GCFR) FOR608 FOR610 (GREM) FOR518 (GIME) FOR528	FOR578 (GCTI) FOR532 FOR589 FOR710 ICS515 (GRID) SEC541 SEC586
Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	SEC460 (GEVA) SEC542 (GWAPT) SEC588 (GCPN) SEC560 (GPEN)	SEC556 SEC660 (GXPN) MGT516
	Pen Tester	SEC560 (GPEN) SEC542 (GWAPT) SEC556	SEC588 (GCPN) SEC660 (GXPN) SEC467
	Adversary Emulation Specialist/Red Teamer	SEC565 SEC599 (GDAT) SEC699 SEC670	SEC504 (GCIH) SEC556 SEC660 (GXPN) SEC760

Operate and Maintain (OM)			
NICE Specialty Area	Work Role	Recommended Course (GIAC Certification)	
Data Administration (DTA)	Database Administrator	SEC401 (GSEC) FOR308	FOR498 (GBFA)
	Data Analyst	SEC401 (GSEC) SEC573 (GPYC) SEC497 (GOSI) FOR578 (GCTI) SEC595	FOR308 FOR498 (GBFA) FOR585 (GASF) FOR518 (GIME)
Knowledge Management (KMG)	Knowledge Manager	SEC301 (GISF) SEC402 SEC403 FOR308	FOR498 (GBFA) FOR585 (GASF) FOR518 (GIME)
Customer Service and Technical Support (STS)	Technical Support Specialist	SEC401 (GSEC) SEC505 (GCWN) SEC504 (GCIH)	
Network Services (NET)	Network Operations Specialist	SEC401 (GSEC) SEC501 (GCED) SEC555 (GCDA)	
Systems Administration (ADM)	System Administrator	SEC401 (GSEC) SEC505 (GCWN) SEC586	FOR308 FOR498 (GBFA)
Systems Analysis (ANA)	Systems Security Analyst	SEC401 (GSEC) SEC488 (GCLD) SEC504 (GCIH) AUD507 (GSNA) SEC505 (GCWN)	SEC586 FOR308 FOR585 (GASF) FOR518 (GIME)



## 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](https://sans.org/course-preview)

### Summit Presentations

Top-of-mind presentations  
[sans.org/presentations](https://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](https://cyberaces.org)

### SANS Workshops

Hands-on virtual training that give you the opportunity to dive into course material  
[sans.org/workshops](https://sans.org/workshops)

### Cyber Ranges

Prepare for real-world IT and cybersecurity roles with interactive learning scenarios  
[sans.org/cyber-ranges](https://sans.org/cyber-ranges)

## Social Media



Find us at [@SANSInstitute](https://twitter.com/SANSInstitute), and connect with us to stay informed on the latest SANS resources

New2Cyber	Leadership
Blue Team	Cloud
Offensive Ops	ICS
DFIR	Security Awareness

[sans.org/blog/SANS-Social-Channels-Podcasts](https://sans.org/blog/SANS-Social-Channels-Podcasts)

## Webcasts

[sans.org/webcasts](https://sans.org/webcasts)



## Blogs

[sans.org/blog](https://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](https://sans.org/podcasts)

## SANS Cyber Academies



### VetSuccess Academy

### Women's Immersion Academy

### Cyber Workforce Academy

### Cyber Diversity Academy

### HBCU Academy

[sans.org/scholarship-academies](https://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](https://sans.org/newsletters)

## Free Cybersecurity Resources



### Internet Storm Center

A free analysis and warning service  
[isc.sans.edu](https://isc.sans.edu)

### Free Tools

150+ open-source tools from SANS Instructors  
[sans.org/tools](https://sans.org/tools)

### Whitepapers

Top-of-mind papers  
[sans.org/white-papers](https://sans.org/white-papers)

### Posters & Cheat Sheets

[sans.org/posters](https://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](https://sans.org/information-security-policy)

### CIS Controls v8

[sans.org/blog/cis-controls-v8](https://sans.org/blog/cis-controls-v8)

### Annual Security Awareness Report

Utilize data-driven actions to manage your human risk and push your program into the future of security awareness  
[go.sans.org/lp-wp-2022-sans-security-awareness-report](https://go.sans.org/lp-wp-2022-sans-security-awareness-report)

### NICE Framework

Use the NICE Framework as a guide to advance your career with recognized cybersecurity certifications from GIAC  
[giac.org/workforce-development/government/niceframework](https://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](https://sans.org/account/create) to create your free account today and gain access to the above available resources and more!

# Hotel Information

## Hyatt Regency Orlando

9801 International Drive  
Orlando, FL 32819  
1-866-227-5938

This family-friendly Orlando resort is just minutes from major theme parks including Universal Orlando®, Walt Disney World®, and SeaWorld® Orlando. Enjoy shopping, dining, and more than 100 unique entertainment options, all within a 2-mile radius of the hotel.

### Hotel Special Rates and Reservations

A special discounted rate of **\$245.00** S/D plus applicable taxes will be honored based on space availability.

***These rates are only available through February 24, 2023.***

A limited number of Government Per Diem rooms at the prevailing rate are available with proper ID.

All rates include the resort fee which provides access to complimentary Internet in your room, two bottles of water in room daily, two I-Ride Trolley tickets through International Drive, unlimited local and 800 phone calls, 10% discount on spa services, daily access to 24hr fitness center, complimentary group fitness classes, bike rentals, and pool activities (floats, rafts, etc.) offered in both pools.

To make a regular reservation, please visit [hyatt.com/en-US/group-booking/MCORO/G-GMW0](https://hyatt.com/en-US/group-booking/MCORO/G-GMW0)

To make a government per diem reservation, please visit [hyatt.com/en-US/group-booking/MCORO/G-GMW0/GOVT](https://hyatt.com/en-US/group-booking/MCORO/G-GMW0/GOVT)

## Justify Your Training

Once you decide on the next training course that's right for your career goals, you want to make the business case to your employer as to why you need to invest the time and budget.

Information to emphasize with your manager:

- **Tasks you will be able to perform after completing the course**
- **How the training will benefit your organization's security**
- **Relevant cost and travel information**

SANS has justification letter templates available via this QR code. Download a sample template, personalize it for your employer, and you'll be one step closer to gaining the critical skills required to protect your organization and advance your career.





5705 Salem Run Blvd.  
Suite 105  
Fredericksburg, VA 22407

## **At the heart of everything we do is our training and certification.**

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 sitting 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](http://www.sans.org)**

**Register for SANS 2023 at [sans.org/sans-2023](http://sans.org/sans-2023)**