



**“SEC555 uses real-world events and hands-on training to allow me to immediately improve my organizations security stance.”**

- Frank Giachino, Bechtel

**“ICS410 provides good cross-training for the IT professional and control specialist. It provides knowledge for a hybrid skillset that few people really have”**

- Joe Lehmann, Shell

**“SEC560 was the best course and CTF that I’ve ever attended. I will highly recommend this course to my coworkers.”**

- Ray White, Celanese



SANS offers training at our live events, including the Oil & Gas Cybersecurity Summit, and training online. Visit [sans.org/training](http://sans.org/training) to view classes by modality. Access course demos with the OnDemand Platform.



GIAC Certifications provide the highest assurance of cybersecurity knowledge and skill available to clients across the world. GIAC Certifications meet ANSI / ISO 17024 standards and align with the NICE framework.



SANS Security Awareness Training covers every end-user, no matter their learning level. Create a culture of security awareness with programs such as End-User Training, Phishing Training, and Developer Training.

# Cybersecurity

## Training Roadmap

# Cybersecurity Training Roadmap

Quick Summary

Course Code

GIAC Certification

View the full course catalog: [sans.org/training](https://sans.org/training)

Security Professional		
Security Essentials	SEC401 Security Essentials Bootcamp Style	GSEC
Control System Essentials	ICS410 ICS/SCADA Security Essentials	GICSP
Hacker Techniques	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	GCIH
NERC CIP	ICS456 Essentials for NERC Critical Infrastructure Protection	GCIP

**“SEC511 was hands-down the best technical training I’ve taken. Excellent materials, excellent instruction. Real-world scenarios you can apply on your first day back in the office.”**

- Justin Griffin, Southern California Edison

Security Operations		
Intrusion Detection	SEC503 Intrusion Detection In-Depth	GCIA
Monitoring & Operations	SEC511 Continuous Monitoring and Security Operations	GMON
Defending Control Systems	ICS515 ICS Active Defense and Incident Response	GRID

Penetration Testing		
Networks	SEC560 Network Penetration Testing and Ethical Hacking	GPEN
Web Apps	SEC542 Web App Penetration Testing and Ethical Hacking	GWAPT
Wireless	SEC617 Wireless Penetration Testing and Ethical Hacking	GAWN

Incident Response & Threat Hunting		
Windows Forensics	FOR500 Windows Forensics Analysis	GCFE
Incident Response	FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics	GCFA
Network Forensics	FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	GNFA

Security Management		
Strategic Planning	MGT514 Security Strategic Planning, Policy, and Leadership	GSTRT
Critical Controls	SEC566 Implementing and Auditing the Critical Security Controls - In-Depth	GCCC

Advanced Security Operations		
SIEM	SEC555 SIEM with Tactical Analytics	GCDA
Cloud Security	SEC545 Cloud Security Architecture and Operation	GCWN
Purple Team	SEC599 Defeating Advanced Adversaries: Purple Team Tactics and Kill Chain Defenses	GDAT

Advanced Penetration Testing		
Networks	SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	GXPN
Web Apps	SEC642 Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques	
Purple Team	SEC599 Defeating Advanced Adversaries: Purple Team Tactics and Kill Chain Defenses	GDAT

Advanced Incident Response		
Malware Analysis	FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	GREM
Threat Intelligence	FOR578 Cyber Threat Intelligence	GCTI

Security Manager		
Leadership Essentials	MGT512 Security Leadership Essentials For Managers	GSLC
New to Cybersecurity	SEC301 Introduction to Cyber Security	GISF

Advanced Security Management		
CISSP	MGT414 SANS Training Program for CISSP® Certification	GISP
Law & Investigations	LEG523 Law of Data Security and Investigations	GLEG