SANS

"Real life examples of case scenarios with clients were a great addition to the course."

– **Arnaud Ruiz**, Daimler AG

"I learned new tools and models that I want to go use immediately."

– **Jamie Bosley**, Caterpillar

"SEC560 was a good dive into how real world attacks & hackers work. I really enjoyed it."

– **Jeremy Dour**, UPS

Securing the Connected Vehicle
Cybersecurity Training Roadmap

Visit **sans.org/training** to view training by location, course, or by delivery.

SANS

SANS offers training at our live events, including the Automotive Cybersecurity Summit, and training online. Visit sans.org/training to view classes by modality. Access course demos with the OnDemand Platform.

GIAC CERTIFICATIONS

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

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.

Securing the Connected Vehicle
Cybersecurity Training Roadmap

Quick Summary	Course Code	GIAC Certification
SIEM	SEC555 SIEM with Tactical Analytics	GCDA
	Course Title	

"SEC504 helped to understand attack techniques as well as how to defend against them."

– **Shadi Abufarha**, General Motors

Security Professional

Security Essentials	SEC401 Security Essentials Bootcamp Style	GSEC
Control Systems	ICS410 ICS/SCADA Security Essentials	GICSP
Hacker Techniques	SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	GCIH

Security Operations

Intrusion Detection	SEC503 Intrusion Detection In-Depth	GCIA
Monitoring & Operations	SEC511 Continuous Monitoring and Security Operations	GMON

Advanced Security Operations

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

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

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	

Incident Response & Threat Hunting

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

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

Security Management

Strategic Planning	MGT514 Security Strategic Planning, Policy, and Leadership	GSTRT
Critical Controls	SEC440 Critical Security Controls: Planning, Implementing, and Auditing	

Advanced Security Management

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

Security Developer / Designer

Secure Web Apps	DEV522 Defending Web Applications Security Essentials	GWEB

Secure Development

Cloud & DevOps	SEC540 Cloud Security and DevOps Automation	

Secure Coding & Frameworks

JAVA/JEE	DEV541 Secure Coding in Java/JEE: Developing Defensible Applications	
.NET	DEV544 Secure Coding in .NET: Developing Defensible Applications	GSSP-.NET