SANS GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

Global Information Assurance Certification (GIAC) develops and administers the premier certifications for information security professionals. More than 30 certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains. GIAC certifications provide the highest and most rigorous assurance of cybersecurity knowledge and skill available to industry, government, and military clients across the world.

SANS + GIAC

The most trusted source for information security training, certification and research.

SANS Training

SANS Training: Develops real-world knowledge and hands-on skills

Certification

GIAC Certifications: Assure the highest levels of job- specific knowledge

Research

SANS Research: Advancement of InfoSec theory and practice

The highest standard in cybersecurity certification.

Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad, general InfoSec certifications are no longer enough. Professionals need specific skills and specialized knowledge to meet multiple, varied threats. GIAC offers more than 30 certifications. Each certification focuses on specific job skills and requires unmatched and distinct knowledge.

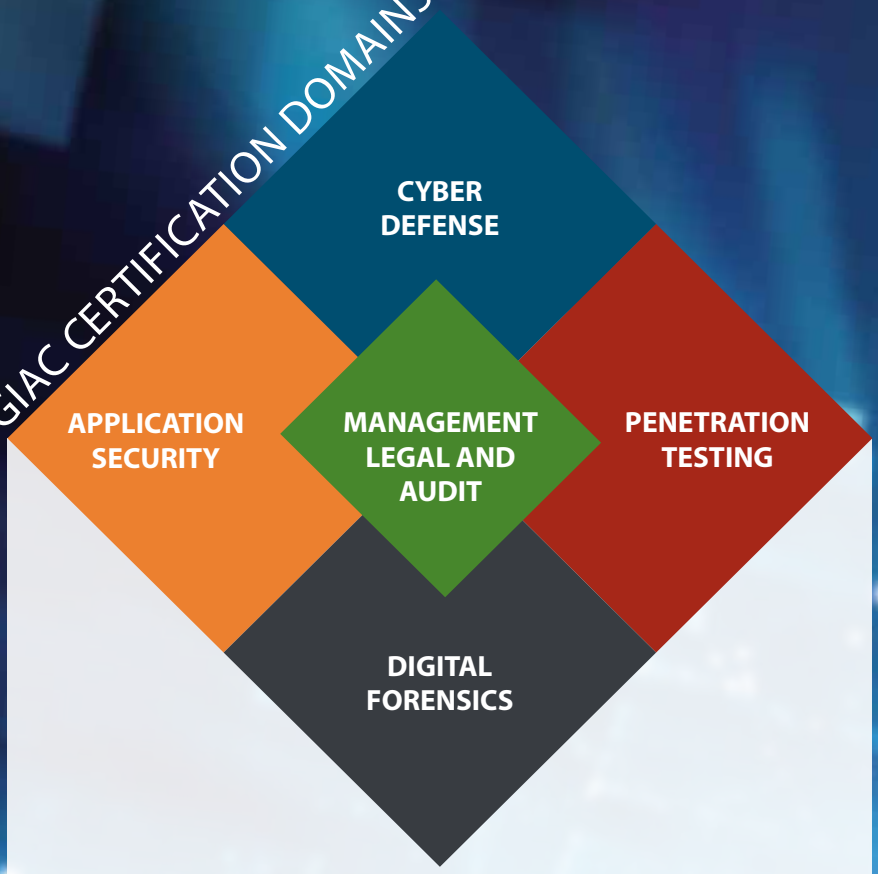
Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, technical, real-world knowledge and skills are the only reliable means to reduce security risk. SANS is the leader in providing training that builds practical knowledge, hands-on skills, and technical depth. A GIAC certification ensures mastery of real-world knowledge and skills.

Most Trusted Certification Design

The design of a certification exam can impact the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC's on-staff psychometrician and reviewed by experts in each technical area. More than 80,000 certifications have been issued since 1999. GIAC certifications meet ANSI/ISO 17024 standards.

GIAC CERTIFICATION DOMAINS



CYBER DEFENSE

The essential skills and techniques needed to protect and secure an organization's critical information assets, business systems, and industrial controls.

SANS Training Courses: 18 | GIAC Certifications: 10

PENETRATION TESTING

The identification and assessment of potential attacks and vulnerabilities, and implementation of defenses and immediate responses to contain, mitigate, and remediate risks.

SANS Training Courses: 13 | GIAC Certifications: 7

DIGITAL FORENSICS

The acquisition and examination of evidence from digital systems to find and recover known artifacts essential to information and systems security.

SANS Training Courses: 8 | GIAC Certifications: 5

APPLICATION SECURITY

The design, development, and defense of secure application software and systems.

SANS Training Courses: 6 | GIAC Certifications: 3

MANAGEMENT, LEGAL AND AUDIT

The leadership and management of security teams and risk analysis techniques to conduct a technical audit of essential information systems.

SANS Training Courses: 14 | GIAC Certifications: 6

Why Certification?

Better Job Performance

More than 50% of IT managers say their staff was significantly more effective or more effective on the job after certification.
(IT SKills and Salary Report, Global Knowledge, 2012)

More Hiring Potential

U.S. Department of Defense Directive 8140 (8570) requires certification of all cybersecurity professionals.

Cybersecurity jobs are 50% more likely to require certification than IT jobs.
(2015 Burning Glass)

GIAC Gold Status

Today's cybersecurity leaders need both technical expertise and communication skills. Candidates work with an advisor to submit a peer-reviewed "Gold Paper" in their area of Information Security expertise. Approved papers are published in the SANS Reading Room for industry reference.

.001%

GSE: The Certification Like No Other

Only the true security elite hold a GIAC Security Expert certification (GSE). For good reason. It's the most prestigious, most demanding certification in the information security industry. The GSE's performance-based, hands-on nature sets it apart from any other certification in the IT security industry. Those who earn the GSE master the wide variety of skills, across multiple domains, required by top security professionals. They demonstrate expertise in applying knowledge in a hands-on environment.

GSEs are verified network packet ninjas with world-class incident response capabilities. In addition to superior technical skills, GSEs must have demonstrated a keen awareness of important business drivers and considerations, a skillset that is too rare among less seasoned technical personnel.

GSE. For the very few, the very best, cybersecurity professionals.

SANS | GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

GIAC Certification Portfolio

CYBER DEFENSE*

GIAC Certification	SANS Course	Areas Covered
 Information Security Fundamentals	**SEC301** Intro to Information Security	• Information Security Foundations • Cryptography • Network Protection Strategies and Host Protection
 Security Essentials	**SEC401** Security Essentials	• Prevention of attacks and detection of adversaries • Networking Concepts, Defense in Depth, Secure Communications • Foundational Windows and Linux Security
 Enterprise Defender	**SEC501** Advanced Security Essentials	• Defensive Network Infrastructure and Packet Analysis • Pen Testing and Vulnerability Analysis and Mitigation • Incident Response, Malware and Data Loss Prevention
 Perimeter Protection Analyst	**SEC502** Perimeter Protection	• Network Security, IP and Packet Decoding • Endpoint-Host Security • Logging Wireless, Encryption, VPNs and Cloud
 Intrusion Analyst	**SEC503** Intrusion Detection	• Fundamentals of Traffic Analysis and Application Protocols • Open Source IDS: Snort and Bro • Network Traffic Forensics and Monitoring
 Windows Security Administrator	**SEC505** Securing Windows and Powershell Automation	• Windows OS and Application Hardening • PowerShell Scripting and Managing Cryptography • Server Hardening, IPSec, Dynamic Access Control and DNS
 Unix Security Administrator	**SEC506** Securing Linux/Unix	• Hardening Linux/Unix • Application Security in Depth • Digital Forensics in the Linux/Unix Environment
 Continuous Monitoring	**SEC511** Continuous Monitoring	• Security Architecture and Security Operations Centers (SOCs) • Network Security Architecture and Monitoring • Endpoint Security Architecture, Automation and Continuous Monitoring
 Critical Controls	**SEC566** Critical Security Controls	• Overview of the Critical Controls and Asset Inventories • Vulnerability Assessments and Remediation, Privileges, Logging • Email and Browser Protections, Malware, Control of Network Access and Protocols, Data Protection and Recovery and Secure Configurations • Wireless Device Control, Application Security, Incident Response, and Penetration Testing
 Global Industrial Cybersecurity Professional	**ICS410** ICS/SCADA Security Essentials	• Industrial Control Systems (ICS/SCADA) and Information Technology • Defending ICS Devices, Workstations, Servers and Networks • ICS/SCADA Security Governance

*SANS training is not required for Certification Challenge

PENETRATION TESTING

DIGITAL FORENSICS

GIAC Certification	SANS Course	Areas Covered
 Incident Handler	**SEC504** Hacker Tools and Incident Handling	• Incident Handling and Computer Crime Investigation • Computer and Network Hacker Exploits • Hacker Tools (Nmap, Nessus, Metasploit and Netcat)
 Penetration Tester	**SEC560** Network Pen Testing	• Comphrehensive Pen Test Planning, Scoping and Recon • In-Depth Scanning and Exploitation, Post-Exploitation and Pivoting • In-Depth Password Attacks and Web App Pen Testing
 Web Application Penetration Tester	**SEC542** Web App Pen Testing	• Web App Pen Testing and Ethical Hacking: Configuration, Identity and Authentication • Injection, JavaScript, XSS, and SQL Injection • CSRF, Logic Flaws and Tools (sqlmap, MetaSploit, and BeEF)
 Python Coder	**SEC573** Python for Pen Testers	• Python Essentials: Variable and Math Operations, Strings and Functions and Compound Statements • Data Structures and Programming Concepts, Debugging, System Arguments and ArgParcer • Python Application Development for Pen Testing: Backdoors and SQL Injection
 Mobile Device Security Analyst	**SEC575** Mobile Device Security	• Mobile Device Architecture and Common Threats (Android and iOS) • Platform Access, Application Analysis and Reverse Engineering • Penetration Testing Mobile Devices: Probe Mapping, Enterprise and Network Attacks, Sidejacking, SSL/TLS Attacks, SQL and Side Injection
 Assessing and Auditing Wireless Networks	**SEC617** Wireless Ethical Hacking and Pen Testing	• Wireless Data Collection, WiFi MAC Analysis, and Wireless Tools (Kismet and Wireshark), Attacking WEP • Client, Crypto and Enterprise Attacks • Advanced WiFi Attacks: DoS Attacks, Fuzzing, Bridging the Airgap, Bluetooth, DECT and ZigBee
 Exploit Researcher and Advanced Penetration Tester	**SEC660** Advanced Pen Testing	• Network Attacks, Crypto, Network Booting and Restricted Environments • Python, Scapy and Fuzzing • Exploiting Windows and Linux for Penetration Testers
 Forensic Examiner	**FOR408** Windows Forensic Analysis	• Windows Forensics and Data Triage • Windows Registry Forensics, USB Devices, Shell Items, Key Word Searching, Email and Event Logs • Web Browser Forensics (FireFox, IE and Chrome) and Tools (Nirsoft, Woanware, SQLite, ESEDatabaseView and Hindsight)
 Forensic Analyst	**FOR508** Advanced Digital Forensics	• Advanced Incident Response and Digital Forensics • Memory Forensics, Timeline Analysis and Anti-Forensics Detection • Threat Hunting and APT Intrusion Incident Response
 Network Forensic Analyst	**FOR572** Advanced Network Forensics	• Network Forensics in Depth: Web Proxy Servers, Payload Reconstruction, Packet Capture and Tools (tcpdump and Wireshark) • NetFlow Analysis, Visualization, Network Protocols and Wireless Investigations • Logging, OPSEC, Encryption, Protocol Reversing and Automation

GIAC Certification	SANS Course	Areas Covered
 Advanced Smartphone Forensics	**FOR585** Advanced Smartphone Forensics	• Smartphone Overview and Malware Forensics • Android, iOS and Blackberry Forensics • Third-Party Applications and Other Devices (Windows, Nokia and Knock-Off Devices)
 Reverse Engineering Malware	**FOR610** Reverse Engineering Malware	• Malware Analysis and Malicious Code Fundamentals and Analysis • In-Depth Malware Analysis and Tools (OllyDbg, Process Dumping Tools and Imports-Rebuilding Tools) • Self-Defending Malware, Malicious Documents and Memory Forensics
APPLICATION SECURITY		
 Web Application Defender	**DEV522** Defending Web Applications	• Web Application Architecture, Authentication and Authorization Vulnerabilities and Defense and Mitigation • Proactive Defense and Operation Security, AJAX and Web Services Security • Clickjacking, DNS Rebinding, Flash, Java, SSO and IPv6
 Secure Software Programmer-Java	**DEV541** Securing Code in JAVA/JEE	• Data Validation, Authentication and Session Management • Java Platform and API Security • Secure Development Lifecycle
 Secure Software Programmer- .NET	**DEV544** Securing Code in .Net	• Data Validation, Authentication and Session Management • .NET Framework Security • Secure Development Lifecycle
MANAGEMENT, LEGAL AND AUDIT		
 Information Security Professional	**MGT414** SANS Training for CISSP®	• Security and Risk Management, Asset Security and Security Engineering, Communication and Network Security • Identity and Access Management, Security Assessment and Security Operations • Software Development Security
 Security Leadership	**MGT512** Leadership Essentials	• Managing the Enterprise, Planning, Network and Physical Plant • IP Concepts, Attacks Against the Enterprise and Defense-in-Depth • Secure Communications (Cryptography, Wireless, Steganography, Web and OPSEC), Intellectual Property, Incident Handling, Disaster Recovery/Planning and Risk Management
 Project Manager	**MGT525** IT Project Management	• Project Management Structure and Framework • Time and Cost Management, Communications and Human Resources • Quality and Risk Management, Procurement, Stakeholder Management and Project Integration
 Law of Data Security & Investigations	**LEG523** Law of Data Security	• IT Security Law and Policy, E-Records, E-Discovery and Business Law • Contracting for Data Security (Sarbanes-Oxley, Gramm-Leach-Bliley, HIPPA, EU Data Directive and Data Breach Notice Laws) • IT Compliance and How to Conduct Investigations and Crisis Management
 Systems and Network Auditor	**AUD507** Auditing and Monitoring Networks	• Auditing, Risk Assessments and Reporting • Network and Perimeter Auditing/Monitoring, and Web Application Auditing • Auditing and Monitoring in Windows and Unix Environments

SANS

HELPING INDIVIDUALS
AND ORGANIZATIONS
MASTER CYBERSECURITY

Cybersecurity Awareness

Securing The Human for organizations that need to improve cybersecurity throughout their organization.

CyberTalent

CyberTalent Sourcing

SANS CyberTalent for organizations in need of trained and certified cybersecurity experts.

NETWARS

Interactive Learning

Hands-on cyber range learning with a focus on mastering the skills that information security professionals can use in their jobs every day.

SANS Technology Institute

Advanced Degrees

SANS Technology Institute for IT professionals seeking to advance their career by focusing on cybersecurity leadership and management.

"I think the exam was both fair and practical. These are the kind of real-world problems I expect to see in the field."
– Carl Hallberg, GREM, Wells Fargo

"GIAC made the testing process much better than other organizations. The material is spot on with what I do at work, daily."
– Jason Pfister, GMON, EWEB

"It feels like SANS and GIAC are working with the candidates to help them to meet the required standards, which are achievable with hard work."
– Thomas Gurney, GCIA

"It's an awesome effort: great questions, excellent material and presentation throughout the (training event) week. I've really enjoyed it and will recommend it to many. Thank you GIAC/SANS!"
– Nicholas B., GCIH, Intrasys

SANS | GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

INFO@GIAC.ORG WWW.GIAC.ORG

Summer 2016