GIAC Certifications 2018

GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

"Excellent examination of skills. GIAC does a good job of leveraging knowledge and skill ability with IT intuition – an important pairing in a real cybersecurity position."

– Garrett Brown, GCIH

GIAC develops and administers premier, professional information security certifications. More than 30 cybersecurity 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 around the world.

The Highest Standard in Cybersecurity Certification

Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and 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 focusing on specific job skills requiring 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 100,000 certifications have been issued since 1999. Many GIAC certifications meet ANSI/ISO 17024 standards and DoDD 8140 requirements.

WWW.GIAC.ORG

"GIAC has helped open doors for me in my cybersecurity career. The security of your cyber-assets depend directly on the skills and knowledge of your security team that GIAC exams validate."

– Trey Blalock, GWAPT, GCFA, GPEN

Cyber Defense Certifications

Whether an attacker is successful in penetrating an organization's network depends on the strength and intelligence of that organization's cyber defense professionals. Defending against attacks is an ongoing challenge, with new threats emerging daily and advanced persistent threats on everyone's mind. Well-prepared organizations understand that what has worked and will always work is taking a risk-based approach to cyber defense.

Ensuring the highest level of cybersecurity means having the expertise and knowledge to focus on the right areas of cyber defense.

GISF Information Security Fundamentals

- Information Security Foundations
- Cryptography
- Network Protection Strategies and Host Protection

SANS Course: **SEC301** Intro to Cyber Security

GSEC Security Essentials

- Prevention of Attacks and Detection of Adversaries
- Networking Concepts, Defense in Depth, Secure Communications
- Foundational Windows and Linux Security

SANS Course: **SEC401** Security Essentials Bootcamp Style

GCED Enterprise Defender

- Defensive Network Infrastructure and Packet Analysis
- Pen Testing and Vulnerability Analysis and Mitigation
- Incident Response, Malware and Data Loss Prevention

SANS Course: **SEC501** Advanced Security Essentials - Enterprise Defender

GCIA Intrusion Analyst

- Fundamentals of Traffic Analysis and Application Protocols
- Open-Source IDS: Snort and Bro
- Network Traffic Forensics and Monitoring

SANS Course: **SEC503** Intrusion Detection In-Depth

GCWN Windows Security Administrator

- Windows OS and Application Hardening
- PowerShell Scripting and Managing Cryptography
- Server Hardening, IPSec, Dynamic Access Control and DNS

SANS Course: **SEC505** Securing Windows and PowerShell Automation

GCUX Unix Security Administrator

- Hardening Linux/Unix
- Application Security in Depth
- Digital Forensics in the Linux/Unix Environment

SANS Course: **SEC506** Securing Linux/Unix

GMON Continuous Monitoring

- Security Architecture and Security Operations Centers (SOCs)
- Network Security Architecture and Monitoring
- Endpoint Security Architecture, Automation and Continuous Monitoring

SANS Course: **SEC511** Continuous Monitoring and Security Operations

GCDA Detection Analyst

- SIEM Architecture and SOF-ELK
- Service Profiling, Advanced Endpoint Analytics, Baselining and User Behavior Monitoring
- Tactical SIEM Detection and Post-Mortem Analysis

SANS Course: **SEC555** SIEM with Tactical Analytics

GCCC Critical 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

SANS Course: **SEC566** Implementing & Auditing Critical Security Controls In-Depth

COMING SOON

GDAT Defending Advanced Threats

- Advanced Persistent Threats Models and Methods
- Detecting and Preventing Payload Deliveries, Exploitation, and Post-Exploitation Activities
- Using Cyber Deception to Gain Intelligence for Threat Hunting and Incident Response

SANS Course: **SEC599** Defeating Advanced Adversaries - Implementing Kill Chain Defenses

More job-specific certifications mean more secure systems.

GIAC offers more than 30 certifications that target actual job-based skills, because in today's complex threat landscape a "one-size-fits-all" approach puts your systems at increased risk.

"As a SOC Manager I have additional confidence in my team's abilities because they hold GIAC certifications."

– Brent Deterding,
SOC Manager, Secureworks

Penetration Testing Certifications

High-value penetration testing doesn't involve just throwing a bunch of hacks at a target environment and declaring victory when a shell prompt magically pops up. Instead, the best penetration testers focus on understanding their craft in depth.

Pen test professionals provide significant value to organizations by improving their security stance through technical excellence and implementation of well-understood and repeatable methodologies. Ultimately, pen testers deliver real savings through information security to the business.

GIAC certifications are developed with these principles in mind and to ensure that penetration testers and ethical hackers achieve the status of certified expert penetration testers and ethical hackers.

"I think the exam was both fair and practical. I expect to see these real-world problems in the field."

– Carl Hallberg, GREM, Wells Fargo

GCIH Incident Handler

- Incident Handling and Computer Crime Investigation
- Computer and Network Hacker Exploits
- Hacker Tools (Nmap, Nessus, Metasploit and Netcat)

SANS Course: **SEC504** Hacker Tools, Techniques, Exploits, & Incident Handling

GPEN Penetration Tester

- Comprehensive Pen Test Planning, Scoping, and Recon
- In-Depth Scanning and Exploitation, Post-Exploitation, and Pivoting
- In-Depth Password Attacks and Web App Pen Testing

SANS Course: **SEC560** Network Penetration Testing and Ethical Hacking

GWAPT Web Application Penetration Tester

- 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)

SANS Course: **SEC542** Web App Penetration Testing and Ethical Hacking

GPYC Python Coder

- Python Essentials: Variable and Math Operations, Strings and Functions, and Compound Statements
- Data Structures and Programming Concepts, Debugging, System Arguments, and Argparse
- Python Application Development for Pen Testing: Backdoors and SQL Injection

SANS Course: **SEC573** Automating Information Security with Python

GMOB Mobile Device Security Analyst

- 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 Client-Side Injection

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

GAWN Assessing and Auditing Wireless Networks

- Wireless Data Collection, WiFi MAC Analysis, Wireless Tools (Kismet and Wireshark), and Attacking WEP
- Client, Crypto, and Enterprise Attacks
- Advanced WiFi Attacks: DoS Attacks, Fuzzing, Bridging the Air Gap, Bluetooth, DECT, and ZigBee

SANS Course: **SEC617** Wireless Penetration Testing and Ethical Hacking

GXPN Exploit Researcher and Advanced Penetration Tester

- Network Attacks, Crypto, Network Booting, and Restricted Environments
- Python, Scapy, and Fuzzing
- Exploiting Windows and Linux for Penetration Testers

SANS Course: **SEC660** Advanced Penetration Testing, Exploit Writing, & Ethical Hacking

Incident Response, Forensics, and Threat Hunting Certifications

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been operating inside the victim's network undetected for months or even years. A properly trained and GIAC-certified incident responder could be the only defense an organization has during a compromise. As a forensics investigator, you need to know what you're up against, and you need to have the most up-to-date knowledge of how to detect and fight it.

Becoming a GIAC Incident Response and Forensic Certified professional ensures that you have the knowledge and performance efficiency to hunt for cybersecurity threats and respond to incidents properly.

"GIAC's testing process is much better than their competitors. The material is spot on with what I do at work every day."

– Jason Pfister, GMON, EWEB

GCFE Forensic Examiner

- 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)

SANS Course: **FOR500** Windows Forensic Analysis

GCFA Forensic Analyst

- Advanced Incident Response and Digital Forensics
- Memory Forensics, Timeline Analysis, and Anti-Forensics Detection
- Threat Hunting and APT Intrusion Incident Response

SANS Course: **FOR508** Advanced Digital Forensics, Incident Response, and Threat Hunting

GNFA Network Forensic Analyst

- 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

SANS Course: **FOR572** Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

GCTI Cyber Threat Intelligence

- Strategic, Operational, and Tactical Cyber Threat Intelligence
- Open-Source Intelligence and Campaigns
- Intelligence Applications and Kill Chain

SANS Course: **FOR578** Cyber Threat Intelligence

GASF Advanced Smartphone Forensics

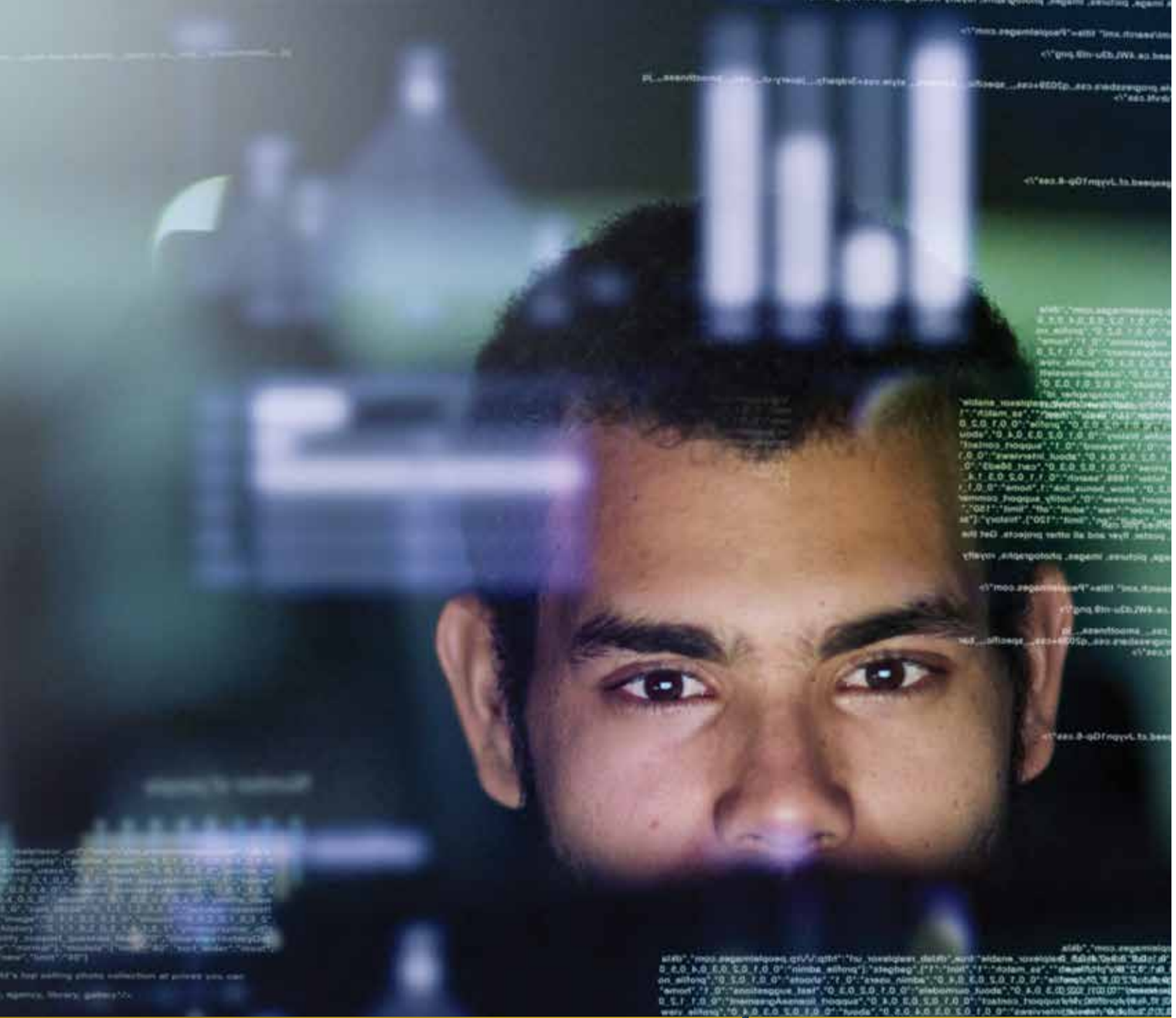
- Smartphone Overview and Malware Forensics
- Android, iOS, and Blackberry Forensics
- Third-Party Applications and Other Devices (Windows, Nokia, and Knock-Off Devices)

SANS Course: **FOR585** Advanced Smartphone Forensics

GREM 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

SANS Course: **FOR610** Reverse-Engineering Malware: Malware Analysis Tools and Techniques



DoDD 8140 (8570)
No other certification partner does more than GIAC.

GIAC offers more certifications that align with DoDD 8140 than anyone else. We're the most trusted source for training and certification in the industry.

You're safe here.

www.giac.org/certifications/dodd-8140

"I am proud to be on the cyber defense line with such a competent industry partner that understands the needs of the Defense Department. GIAC is willing to work with us to help accomplish this difficult task."

– Mike Knight, Naval NetWar Command

Developer Certifications

GIAC certifications prove performance mastery of intensive, practical steps necessary for defending applications and systems against the most dangerous threats.

GIAC developer certifications are developed through a consensus process involving subject-matter experts, including developers, architects, administrators, security managers, and information security professionals. The developer certifications address secure coding principles, security fundamentals and awareness, and the in-depth technical aspects of the most crucial areas of application security and secure development processes.

GWEB Web Application Defender

- 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

SANS Course: **DEV522** Defending Web Applications Security Essentials

GSSP-JAVA Secure Software Programmer-Java

- Data Validation, Authentication, and Session Management
- Java Platform and API Security
- Secure Development Lifecycle

SANS Course: **DEV541** Secure Coding in Java/JEE: Developing Defensible Applications

GSSP-.NET Secure Software Programmer- .NET

- Data Validation, Authentication and Session Management
- .NET Framework Security
- Secure Development Lifecycle

SANS Course: **DEV544** Secure Coding in .NET: Developing Defensible Applications

"GIAC certifications show a confirmation of the skills acquired in conjunction with a SANS training course, rather than just a certificate of completion." – Kirk K. Wah Yick, GCFA, GPEN, GASF

Industrial Control Systems Certifications

Industrial Control System (ICS) environments remain a target for cyber attackers. GIAC ICS certifications equip security professionals and control system engineers with the security awareness, work-specific knowledge, and hands-on technical skills they need to secure automation and control system technology. GIAC certifications validate that both security professionals and control system engineers are equipped with the knowledge and skills they need to safeguard our critical infrastructures.

GICSP Global Industrial Cybersecurity Professional

- Industrial Control Systems (ICS/SCADA) and Information Technology
- Defending ICS Devices, Workstations, Servers, and Networks
- ICS/SCADA Security Governance

SANS Course: **ICS410** ICS/SCADA Security Essentials

GCIP Critical Infrastructure Protection

- CIP Compliance and Enforcement
- Access Controls and Vulnerability Assessments
- Incident Response and Recovery

SANS Course: **ICS456** Essentials for NERC Critical Infrastructure Protection

GRID Response and Industrial Defense

- Overview and Application of Active Defense and Threat Intelligence
- Industrial Control Systems (ICS/SCADA) Digital Forensics, Incident Response, and Threat Analysis
- Monitoring and Detection, ICS/SCADA Networks and Systems

SANS Course: **ICS515** ICS Active Defense and Incident Response

Management, Legal & Audit Certifications

Information security is now more critical to organizations than ever before. As a result, InfoSec teams now have more visibility, budget, and opportunity. However, with increased responsibility comes increased scrutiny. InfoSec leaders must learn how to navigate this new world of managing and leading security.

Technical knowledge is no longer sufficient for leading a security function across complex organizations. Today's security leaders must combine technical knowledge with leadership and management skills that are rooted in a deep understanding of the business.

GIAC Management and Leadership Certifications build the next generation of cyber leaders and managers, preparing them to be a vital part of developing and delivering the organization's strategy.

GISP Information Security Professional

- Security and Risk Management, Asset Security and Security Engineering, and Communication and Network Security
- Identity and Access Management, Security Assessment, and Security Operations
- Software Development Security

SANS Course: **MGT414** SANS Training Program for CISSP Certification

GSLC Security Leadership

- 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

SANS Course: **MGT512** Security Leadership Essentials For Managers with Knowledge Compression™

GSTRT Strategic Planning, Policy, and Leadership

- Business and Threat Analysis
- Security Programs and Security Policy
- Effective Leadership and Communication

SANS Course: **MGT514** Security Strategic Planning, Policy, and Leadership

GCPM Project Manager

- Project Management Structure and Framework
- Time and Cost Management, Communications, and Human Resources
- Quality and Risk Management, Procurement, Stakeholder Management, and Project Integration

SANS Course: **MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep

GLEG Law of Data Security & Investigations

- IT Security Law and Policy, E-Records, E-Discovery, and Business Law
- Contracting for Data Security (Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, EU Data Directive, and Data Breach Notice Laws)
- IT Compliance and How to Conduct Investigations and Crisis Management

SANS Course: **LEG523** Law of Data Security and Investigations

GSNA Systems and Network Auditor

- Auditing, Risk Assessments and Reporting
- Network and Perimeter Auditing/Monitoring, and Web Application Auditing
- Auditing and Monitoring in Windows and Unix Environments

SANS Course: **AUD507** Auditing & Monitoring Networks, Perimeters and Systems

"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

.001%

GSE: The Certification Like No Other

Only the true security elite hold a GIAC Security Expert certification (GSE). In fact, they constitute about .001% of all GIAC certification holders. The GSE is the most prestigious and demanding certification in the information security industry. The GSE's performance-based, hands-on nature sets it apart from any other certification in cybersecurity. Those who earn the GSE have mastered the wide variety of skills, across multiple domains, required by top security professionals.

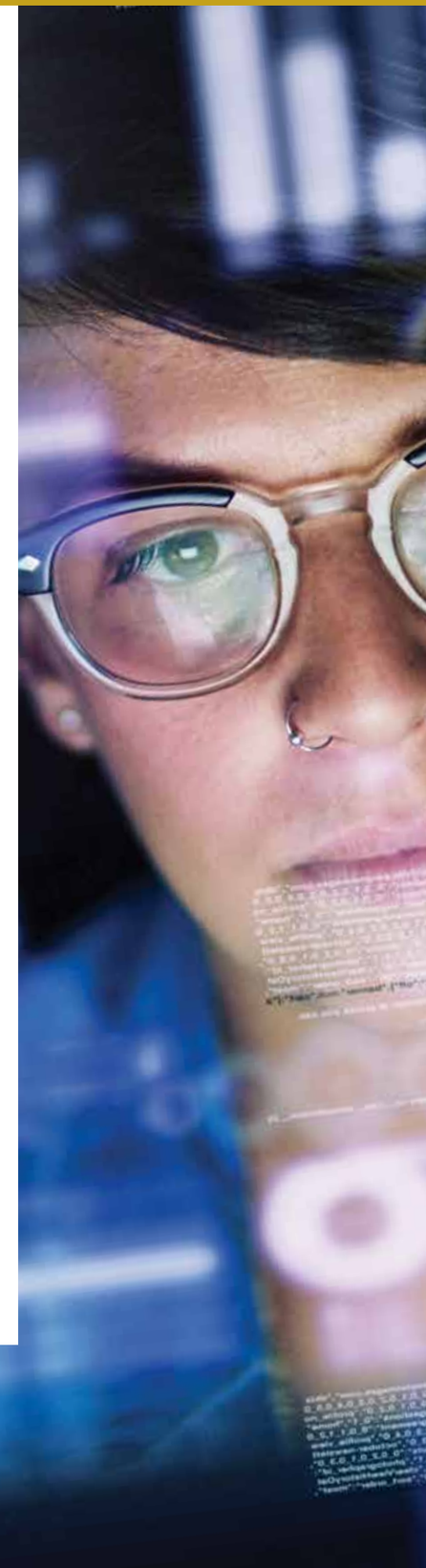
GSE holders have demonstrated expertise in applying knowledge in a hands-on environment.

They are verified network packet ninjas with world-class incident response capabilities. In addition to superior technical skills, GSE holders must have demonstrated a keen awareness of important business drivers and considerations, an exceptionally rare skill set among technology professionals.

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

GSE
GIAC SECURITY EXPERT CERTIFICATION

GIAC Certifications develops and administers the premier certifications for information security professionals. More than 30 certifications align with SANS training and ensure mastery in critical and 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

HELPING INDIVIDUALS
AND ORGANIZATIONS
MASTER CYBERSECURITY

SANS SECURITY AWARENESS

SANS Security Awareness training 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 careers by focusing on cybersecurity leadership and management.

GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

WWW.GIAC.ORG