GIAC
CERTIFICATIONS

www.giac.org

GIAC Catalog

2024

GIAC's Certification Journey

GIAC's new Certification Journey offers candidates a level of flexibility to create their own path to success. With GIAC Certification Categories and GIAC Certification Portfolios, candidates now have multiple avenues to demonstrate their knowledge and expertise and attain industry-recognized milestones.

Why Certify with GIAC?

Research continually shows that credentialed employees are more empowered and contribute greater value to their organization.

Benefits for Organizations

Performance

81%
of candidates produce higher quality work

77%
are more innovative

72%
are more effecient

Source: Pearson VUE 2021 and 2023

The Testing Effect

Certifications are a critical part of cybersecurity training. Research shows and businesses confirm the action of testing and taking an exam is shown to increase learning and retention levels.

Studies on the Testing Effect show that candidates recall 50% more of learned information by testing rather than studying.

Benefits for Students

Personal Validation

92%
feel more confident in their abilities

84%
are more determined to succeed professionally

34%
receive salary increases

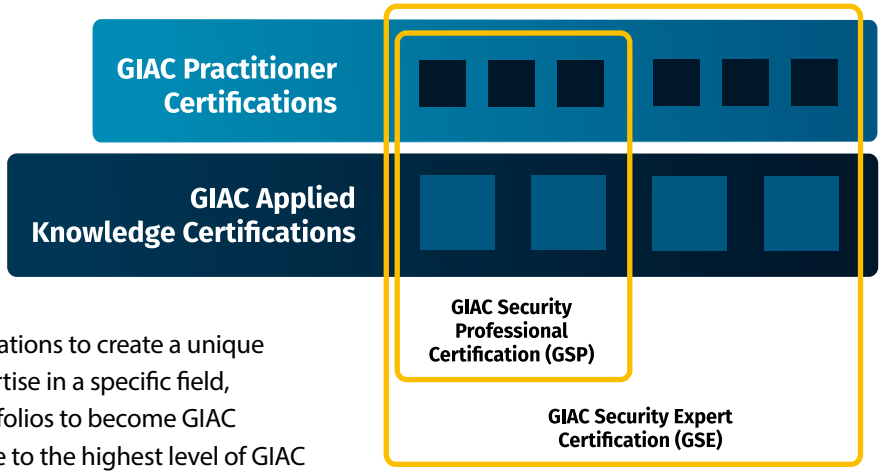
Source: Pearson VUE 2021 and 2023

> *"I don't get certs to impress anyone else. I do it for me. I'll get out of my defender comfort zone and conquer that fear of 'What if I'm not good enough?"*
>
> Danny Akacki | GPEN

> *"I value the instant respect and credibility GIAC professionals receive. People know you've worked hard to obtain the certification and they recognize the critical skills and knowledge that come with it."*
>
> Ben Boyle | GWAPT, GXPN, GPEN

Create Your Own Path

GIAC offers two Categories of stackable certifications to meet the needs of different professionals: Practitioner Certifications and Applied Knowledge Certifications.



Candidates can choose from a wide range of certifications to create a unique portfolio of credentials that demonstrate their expertise in a specific field, or across multiple focus areas. Those who build Portfolios to become GIAC Security Professionals (GSPs) may choose to advance to the highest level of GIAC certification, the GIAC Security Expert (GSE).

GIAC Certification Categories:

GIAC Practitioner Certifications

GIAC Practitioner exams are designed to validate a practitioner's abilities and likelihood of success in a real-world work environment. These certifications:

- Are ideal for candidates who are starting their Certification Journey or looking to continue on their path to become a GIAC Security Professional or GIAC Security Expert
- Span the breadth of infosec and are a mile deep for specialized, job-focused tasks across industry focus areas including offensive operations, cyber defense, cloud security, DFIR, management, and ICS
- May include CyberLive questions, requiring candidates to prove their skill and perform real-world job tasks in a virtual machine environment
- Are stackable with GIAC Applied Knowledge Certifications, enabling candidates to build their Certification Portfolios to become a GIAC Security Professional (GSP) and/or a GIAC Security Expert (GSE)

As always, the best ways to prepare for any GIAC Practitioner exam are with the affiliate training course and GIAC practice tests, both available for purchase.

GIAC currently offers 40+ Practitioner Certifications and will continue to add more certifications into this category.

GIAC Applied Knowledge Certifications

Taking testing to the next level, GIAC Applied Knowledge Certifications are designed to provide a more comprehensive and rigorous assessment of knowledge and skills. These certifications:

- Cover a range of topics to provide candidates with a more thorough understanding of the subject matter
- Are 100% CyberLive and are designed to push beyond individual technical skills. CyberLive questions require candidates to synthesize their skills and use them to solve real-world challenges in a virtual machine environment
- Are ideal for candidates who wish to challenge themselves and demonstrate their mastery of a subject
- Are stackable with GIAC Practitioner Certifications, enabling candidates to build their Portfolios to become a GIAC Security Professional (GSP) and/or a GIAC Security Expert (GSE)

Unlike GIAC Practitioner exams, preparation for GIAC Applied Knowledge exams is not directly linked to a specific affiliate training course. To prepare for a GIAC Applied Knowledge Certifications, GIAC recommends that candidates review the content within the primary fit affiliate course, however, candidates should not rely on this course alone. Along with content and labs included in primary fit course, candidates should review the Areas Covered list found on each Applied Knowledge certification page. Ample work experience will also equip candidates for success.

Finally, candidates may purchase a Demo Question Set. Demo Question Sets are made for one-time use/purchase and include 3 questions.

GIAC currently offers 6 Applied Knowledge Certifications:

GIAC Experienced Cybersecurity Specialist Certification (GX-CS)

Solidifies a candidate's proficiency in hands-on IT systems roles. Holders of this certification validate their capability to solve intricate, multifaceted problems using diversified security practices and innovative techniques.

GIAC Experienced Intrusion Analyst Certification (GX-IA)

Showcases a candidate's capability to tackle intricate and distinctive challenges faced by Intrusion Analysts. Those certified validate their capacity to resolve multi-step issues by integrating diverse concepts and methodologies to identify malicious activities.

GIAC Experienced Incident Handler Certification (GX-IH)

Highlights a candidate's advanced incident response expertise. Proficiency in hands-on attacker techniques coupled with incident response tools and practices verifies that certified individuals possess the skills and knowledge to elevate team performance to new heights.

GIAC Experienced Forensic Analyst (GX-FA)

Showcases a candidate's expertise in hands-on digital forensics and threat hunting roles. Certified individuals validate their capability in processing, analyzing, and interpreting enterprise host-based forensic artifacts, along with mastery in detecting threats and malicious activities.

GIAC Experienced Penetration Tester (GX-PT)

Substantiates a candidate's seasoned expertise in red team and purple team skills. Certified individuals validate their capability in mapping networks, identifying vulnerabilities, and exploiting hosts across diverse environments. They demonstrate this through a range of tasks performed under time-restricted and testing conditions.

GIAC Experienced Forensics Examiner (GX-FE)

Demonstrates that a candidate is qualified for a hands-on Windows forensics analyst role. Certification holders will have validated their ability to validated their ability to analyze a Windows host to uncover evidence that proves a user performed a particular activity on the device.

GIAC currently offers 6 Applied Knowledge Certifications and will continue to add more certifications into this category.

GIAC Certification Portfolios:

GIAC Security Professional (GSP)

Building your Certification Portfolio to become a GIAC Security Professional (GSP) proves your depth and breadth of knowledge. The GSP is both a new milestone for candidates and a midpoint for those on their journey to becoming a GIAC Security Expert (GSE).

To become a GIAC Security Professional:

- Candidates must accumulate a Portfolio of 3 GIAC Practioner Certifications and 2 GIAC Applied Knowledge Certifications. Candidates can focus where they want by choosing any combination of certifications.
- Candidates can build their Certification Portfolio over any amount of time as long as the number of required certifications within your portfolio remain active.

Candidates who become GIAC Security Professionals will be presented with a GIAC Security Professional Coin.

GIAC Security Expert (GSE)

Building your Certification Portfolio to become a GIAC Security Expert (GSE) is the most prestigious credential in the IT security industry. These candidates have proven that they are the elite of information security and top practitioners in the field.

To become a GIAC Security Expert:

- Candidates must accumulate a portfolio of 6 GIAC Practioner Certifications and 4 GIAC Applied Knowledge Certifications. Candidates can focus where they want by choosing any combinations of certifications.
- Candidates can build their Certification Portfolio over any amount of time as long as the number of required certifications within your portfolio remain active.

To recognize candidates who have demonstrated the highest, most-elite level of knowledge and skill, GIAC Security Experts will be presented with a GIAC Security Expert Coin.

> *"The GSE certification offered a specific challenge--a goalpost that I could pursue intentionally. It motivated me to learn skills outside my comfort areas and offered a framework within which I could grow as a security professional. As with other meaningful pursuits, GSE was more about the journey than the destination for me. As I attained and applied knowledge, I met people along the way who became my colleagues and collaborators. And I gained confidence in my learning abilities, which allowed me to continue to excel even after earning GSE."*
>
> Lenny Zeltser, GSE

Multiple Ways to Become an Expert

SANS instructors are renowned for being some of the most respected cybersecurity experts in the world. With diverse backgrounds, each instructor brings a unique set of experiences and perspectives that make them stand out in the industry. It's clear that no two instructors have had the same journey to becoming an expert, making it even more impressive that they've achieved such an elite level of expertise.

Lenny Zeltser

Job Role: CISO at Axonius and SANS Instructor

Journey to Becoming a GSE: 2.5 years

Certifications Earned: GCIA, GCIH, GCUX, GCWN, GPPA, GSEC, GSE

Ismael Valenzuela

Job Role: Vice President of Threat Research & Intelligence at Blackberry and SANS Instructor

Journey to Becoming a GSE: 16 months

Certifications Earned: GCFA, GCIA, GCIH, GCUX, GCWN, GDSA, GMON, GPEN, GREM, GSNA, GWAPT, GSE

The Benefits of Stackable Skills

GIAC's New Certification Journey was built on the idea of skill stacking and the benefits that skill stacking produces.

Skill stacking is the concept that individuals can make themselves more valuable by gaining a wide range of skills instead of pursuing one skill or talent. As candidates build their GSP and GSE Portfolios, they can master complementary skills that support each other, creating a unique and diversified skill set. Skill stacking:

- Makes work more rewarding
- Increases your value as an employee
- Makes work more interesting
- Diversifies your skill set
- Makes success more achievable
- Creates new opportunities

https://www.indeed.com/career-advice/career-development/what-is-skill-stacking

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

> *"Cyberlive is a gamechanger in the certification world. The virtualized environment emulates the real world, forcing the candidate to demonstrate hands-on practical knowledge that can't be faked."*
>
> Matthew Swenson, CEO Black Rainbow Group

Cyber Defense Certifications

Defending against attacks is only possible with the right skill set – and confidence in your abilities and those of your team. GIAC's Cyber Defense certifications focus on three areas: cyber defense essentials, blue team operations, and purple team, spanning the entire defense spectrum. Whether your needs are beginner-level, advanced, or for a specialized area of defense, GIAC has the credentials you need to keep your organization safe from the latest threats.

Cyber Defense Essentials Certifications

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 - Network, Endpoint, and Cloud

GCED Enterprise Defender

- Network and cloud-based defensive infrastructure
- Penetration testing; Digital forensics; Incident response
- Packet analysis; Intrusion analysis; Malware analysis

SANS Course: SEC501: Advanced Security Essentials – Enterprise Defender

Purple Team Certifications

GFACT Foundational Cybersecurity Technologies

- Core Computing Components: Hardware and Virtualization, Networking, Operating Systems, Web, Cloud, and Data Storage
- IT Fundamentals and Concepts: Logic and Programming, Windows, and Linux
- Security Foundations and Threat Landscape: Concepts, Exploitation and Mitigation, Forensics and Post Exploitation

SANS Course: SEC275: Foundations - Computers, Technology, & Security

GCIH Certified Incident Handler

- Incident response and cyber investigation best practices
- Identifying common exploitation, persistence, and evasion techniquesUsing and
- Detecting Hacker Tools (Nmap, Metasploit, and Netcat)

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

GDAT Defending Advanced Threats

- Advanced Persistent Threat 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 – Purple Team Tactics & Kill Chain Defenses

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

– Trey Blalock, GWAPT, GCFA, GPEN

Blue Team Operations Certifications

GOSI Open Source Intelligence

- Open Source Intelligence Methodologies and Frameworks
- OSINT Data Collection, Analysis, and Reporting
- Harvesting Data from the Dark Web

SANS Course: SEC497: Practical Open-Source Intelligence (OSINT)

GCIA Certified Intrusion Analyst

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

SANS Course: SEC503: Network Monitoring and Threat Detection In-Depth

GCWN Windows Security Administrator

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

SANS Course: SEC505: Securing Windows and PowerShell Automation

GSOC Security Operations Certified

- SOC monitoring and incident response using incident management systems, threat intelligence platforms, and SIEMs
- Analysis and defense against the most common enterprise-targeted attacks
- Designing, automating, and enriching security operations to increase efficiency

SANS Course: SEC450: Blue Team Fundamentals: Security Operations and Analysis

GMLE GIAC Machine Learning Engineer

- Machine Learning
- Data Science
- Anomaly Detection & Optimization

SANS Course: SEC595: Applied Data Science and AI/ Machine Learning for Cybersecurity Professionals

GMON Continuous Monitoring

- Security Architecture and Security Operations Centers
- Network Security Architecture and Monitoring
- Endpoint Security Architecture, Automation and Continuzous Monitoring

SANS Course: SEC511: Continuous Monitoring and Security Operations

GDSA GIAC Defensible Security Architecture

- Defensible Security Architecture: network-centric and data-centric approaches
- Network Security Architecture: hardening applications across the TCP/IP stack
- Zero Trust Architecture: secure environment creation with private, hybrid or public clouds

SANS Course: SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise

GCDA Certified 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

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

Offensive Operations Certifications

Offensive operations practitioners are in high demand due to their skill at discovering and exploiting vulnerabilities across the threat landscape. GIAC's offensive operations certifications cover critical domains and highly specialized usages, ensuring professionals are well-versed in essential offensive abilities. GIAC certifications prove that you have the offensive knowledge and skills necessary to skills neccessary to conduct penetration test engagemnets, execute red team operations and exploit systems to expose vulnerabilities.

Penetration Testing Certifications

GCIH Certified Incident Handler

- Incident Handling and Computer Crime Investigation
- Computer and Network Hacker Exploits
- Attacker Techniques (Nmap, Masscan, Metasploit and Netcat)

SANS Course: SEC504: Hacker Tools, Techniques, and Incident Handling

GPEN Penetration Tester

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

SANS Course: SEC560: Enterprise Penetration Testing

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

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: iOS and Android Application Security Analysis and Penetration Testing

GXPN Exploit Researcher and Advanced Penetration Tester

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

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

GAWN Assessing and Auditing Wireless Networks

- Attacking weak encryption, 802.11 fuzzing attacks, and bluetooth attacks
- Bridging the air gap, DoS on wireless networks, high-frequency RFID attacks, and RFID applications
- Sniffing wireless, wireless basics, wireless client attacks, WPA, and Zigbee

SANS Course: SEC617: Wireless Penetration Testing and Ethical Hacking

GCPN Cloud Penetration Tester

- Cloud Penetration Testing Fundamentals, Environment Mapping, and Service Discovery
- AWS and Azure Cloud Services and Attacks
- Cloud Native Applications with Containers and CI/CD Pipeline

SANS Course: SEC588: Cloud Penetration Testing

Purple Team Certifications

GDAT Defending Advanced Threats

- Advanced Persistent Threat 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 – Purple Team Tactics & Kill Chain Defenses

GFACT Foundational Cybersecurity Technologies

- Core Computing Components: Hardware and Virtualization, Networking, Operating Systems, Web, Cloud, and Data Storage
- IT Fundamentals and Concepts: Logic and Programming, Windows, and Linux
- Security Foundations and Threat Landscape: Concepts, Exploitation and Mitigation, Forensics and Post Exploitation

SANS Course: SEC275: Foundations: Computers, Technology, & Security

Red Team Certifications

GRTP Red Team Professional

- Building an adversary emulation plan using gathered threat intelligence
- Creating a comprehensive attack infrastructure
- Performing, retesting, and replaying of Red Team activities

SANS Course: SEC565: Red Team Operations and Adversary Emulation

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

"My GIAC penetration testing certification is important to me because just knowing or being able to read a vulnerability management tool report isn't good enough. Being able to and knowing how to exploit a vulnerability not only looks good for you, but the impact it has on the business is extremely valuable."

– Nick Villa, GPEN

Industrial Control Systems Certifications

Attacks on industrial control infrastructure are occurring with increasing frequency and strength. Control systems across the globe need strong infosec teams behind them to ensure these threats do not succeed. GIAC's industrial control systems certifications cover what ICS professionals need to know: how to protect and defend critical industrial systems and respond to incidents that will inevitably occur. By getting certified in ICS, you confirm your ability to protect essential infrastructure as well as your value to the workplace.

Industrial Control Systems Certifications

GICSP Global Industrial Cyber Security 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 Visibility, Detection, and Response

Start Your Cyber Career with GIAC

If you're just beginning your career in cyber security, you've come to the right place. With SANS training and GIAC certifications, you'll learn essential, foundational skills and prove you can apply that knowledge at any enterprise. Whether you have a background in IT or no computer experience, we've got the solution you need to kick-start your cyber security career.

New to Cyber?

Foundational Cybersecurity Technologies Certification

- For students with no technical experience
- Proves a practitioner's knowledge of essential foundational computer, technology, and cybersecurity concepts
- Prepare with **SANS SEC275**: Foundations-Computers, Technology, and Security

Information Security Fundamentals Certification

- For students with some understanding of computers
- Proves a practitioner's knowledge of security's foundation, computers and networking, and cybersecurity technologies.
- Prepare with **SANS SEC301**: Introduction to Cybersecurity

Security Essentials Certification

- For students with a background in information systems and networking
- Proves a practitioner's knowledge of information security beyond simple terminology and concepts
- Prepare with **SANS SEC401**: Security Essentials: Network, Endpoint, and Cloud

Learn more at **giac.org/certifications**

Digital Forensics & Incident Response Certifications

It takes intuition and specialized skills to find hidden evidence and hunt for elusive threats. GIAC's Digital Forensics and Incident Response certifications encompass abilities that DFIR professionals need to succeed at their craft, confirming that professionals can detect compromised systems, identify how and when a breach occurred, understand what attackers took or changed, and successfully contain and remediate incidents. Keep your knowledge of detecting and fighting threats up to date – and your work role secure – with DFIR certifications.

Digital Forensics & Incident Response Certifications

GCFE Forensic Examiner

- Windows Forensics and Data Triage
- Windows Registry Forensics, USB Devices, Shell Items, Email Forensics and Log Analysis
- Advanced Web Browser Forensics (Chrome, Edge, Firefox)

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 Incident Response, Threat Hunting, and Digital Forensics

GNFA Network Forensic Analyst

- Network architecture, network protocols, and network protocol reverse engineering
- Encryption and encoding, NetFlow analysis and attack visualization, security event & incident logging
- Network analysis tools and usage, and open source network security proxies

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

- Fundamentals of mobile forensics and conducting forensic exams
- Device file system analysis and mobile application behavior
- Event artifact analysis and the identification and analysis of mobile device malware

SANS Course: FOR585: Smartphone Forensic Analysis In-Depth

GREM Reverse Engineering Malware

- Analysis of Malicious Document Files, Analyzing Protected Executables, and Analyzing Web-Based Malware
- In-Depth Analysis of Malicious Browser Scripts and In-Depth Analysis of Malicious Executables
- Malware Analysis Using Memory Forensics and Malware Code and Behavioral Analysis Fundamentals

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

GBFA Battlefield Forensics and Acquisition

- Efficient data acquisition from a wide range of devices
- Rapidly producing actionable intelligence
- Manually identifying and acquiring data

SANS Course: FOR498: Digital Acquisition and Rapid Triage

GIME iOS and macOS Examiner

- Mac and iOS File Systems, System Triage, User and Application Data Analysis
- Mac and iOS Incident Response, Malware, and Intrusion Analysis
- Mac and iOS Memory Forensics and Timeline Analysis

SANS course: FOR518: Mac and iOS Forensic Analysis and Incident Response

CYBERLIVE

GCFR Cloud Forensics Responder

- Log generation, collection, storage and retention in cloud environments
- Identification of malicious and anomalous activity that affect cloud resources
- Extraction of data from cloud environments for forensic investigations

SANS Course: FOR509: Enterprise Cloud Forensics and Incident Response

CYBERLIVE

GEIR Enterprise Incident Responder

- enterprise-level incident response, threat detection, and advanced analysis methodologies.
- analyze artifacts across Windows, Linux, macOS, containers, and cloud environments
- large-scale event correlation, timeline analysis, and managing incident response teams.

SANS Course: FOR608: Enterprise-Class Incident Response & Threat Hunting

DoD 8140 APPROVED

GRID Response and Industrial Defense

- Active Defense Concepts and Application, Detection and Analysis in an ICS environment
- Discovery and Monitoring in an ICS environment, ICS-focused Digital Forensics, and ICS-focused Incident Response
- Malware Analysis Techniques, Threat Analysis in an ICS environment, and Threat Intelligence Fundamentals

SANS Course: ICS515: ICS Visibility, Detection, and Response

DoD 8140 APPROVED

ANAB ACCREDITED

GCIH Certified Incident Handler Certification

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

SANS Course: SEC504: Hacker Tools, Techniques, and Incident Handling

Cybersecurity Leadership Certifications

Enterprise security isn't just the responsibility of an organization's cybersecurity professionals. Keeping the business secure requires input from all levels of leadership. With enterprises in need of protecting against an endless and increasing onslaught of information security threats, technology management skills alone are no longer sufficient. GIAC's Leadership certifications confirm the practical skills to build and lead security teams, communicate with both technical teams and business leaders, and develop capabilities that strengthen your organization's security posture.

Leadership Certifications

GSLC Security Leadership

- Building a security program that meets business needs
- Managing security operations and teams
- Managing security projects and the lifecycle of the program

SANS Course: LDR512: Security Leadership Essentials for Managers

GSTRT Strategic Planning, Policy, and Leadership

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

SANS Course: LDR514 :Security Strategic Planning, Policy, and Leadership

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 Systems, Applications, and the Cloud

GSOM Security Operations Manager

- Designing, planning, and managing an effective SOC program
- Prioritizing and collecting logs, developing alert use cases, and response playbook generation
- Using metrics, analytics, and long-term strategy to assess and improve SOC operations

SANS Course: LDR551: Building and Leading Security Operations Centers

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: LDR525: Managing Cybersecurity Initiatives and Effective Communication

GCCC Critical Controls Certification

- Implement, track, measure, and assess CIS Controls best practices
- Prioritize controls based on evolving threats
- Understand the importance of each control

SANS Course: SEC566: Implementing and Auditing CIS Controls

GISP Information Security Professional

- Asset Security; Communications and Network Security; Software Development Security
- Identity and Access Management; Security and Risk Management
- Security Assessment and Testing; Security Engineering; Security Operation

SANS Course: LDR414: SANS Training Program for CISSP Certification

"I am GIAC Security Leadership certified. GSLC is important to me because I didn't just learn about security, I also learned how to manage security. The GSLC was beneficial for me, for my team, and for my organization. The GIAC GSLC offers great ROI."

- Mirza Ahmed, GSLC, GSNA, GCCC

Cloud Security Certifications

Securing the cloud is now essential across our global infrastructure. GIAC's cloud security certifications are designed to help you master the practical steps necessary for defending systems and applications in the cloud against the most dangerous threats. From web application security and DevOps automation to cloud-specific penetration testing – across public cloud, multi-cloud, and hybrid-cloud scenarios – we've got the credentials both professionals and organizations need to ensure cloud security at any enterprise.

GWEB Web Application Defender

- Access Control, AJAX Technologies and Security Strategies, Security Testing, and Authentication
- Cross Origin Policy Attacks and Mitigation, CSRF, and Encryption and Protecting Sensitive Data
- Web Application and HTTP Basics, Web Architecture, Configuration, and Security

SANS Course: SEC522: Application Security: Securing Web Apps, APIs, and Microservices

GCSA Cloud Security Automation

DoD 8140 APPROVED

ANAB ACCREDITED

- Using cloud services with Secure DevOps principles, practices, and tools to build & deliver secure infrastructure and software
- Automating Configuration Management, Continuous Integration, Continuous Delivery, and Continuous Monitoring
- Use of open-source tools, the Amazon Web Services toolchain, and Azure services

SANS Course: SEC540: Cloud Security and DevSecOps Automation

GCLD Cloud Security Essentials

DoD 8140 APPROVED

ANAB ACCREDITED

- Evaluation of cloud service provider similarities, differences, challenges, and opportunities
- Planning, deploying, hardening, and securing single and multi-cloud environments
- Basic cloud resource auditing, security assessment, and incident response

SANS Course: SEC488: Cloud Security Essentials

"The amount of knowledge from the class and hands-on modules are so on point, I keep revisiting the class materials on a weekly basis for work."

– Beeson Cho

GPCS Public Cloud Security

- Evaluation and comparison of public cloud service providers
- Auditing, hardening, and securing public cloud environments
- Introduction to multi-cloud compliance and integration

SANS Course: SE510: Cloud Security Controls and Mitigations

GCTD Cloud Threat Detection

- Detecting attacks in the cloud
- Cloud investigations and cyber threat intelligence
- Assessments and automation in AWS and Azure

SANS Course: SEC541: Cloud Security Threat Detection

GCPN Cloud Penetration Tester

- Cloud Penetration Testing Fundamentals, Environment Mapping, and Service Discovery
- AWS and Azure Cloud Services and Attacks
- Cloud Native Applications with Containers and CI/CD Pipeline

SANS Course: SEC588: Cloud Penetration Testing

GCFR Cloud Forensics Responder

CYBERLIVE

- Log generation, collection, storage and retention in cloud environments
- Identification of malicious and anomalous activity that affect cloud resources
- Extraction of data from cloud environments for forensic investigations

SANS Course: FOR509: Enterprise Cloud Forensics and Incident Response

Why Renew?

Keep your certification active to stay relevant in the cybersecurity workforce!

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.

* Visit www.giac.org/knowledge-base/renewal for more details.

What Counts?

GIAC accepts many different types of CPE credits to accommodate your busy lifestyle. Combine categories to earn your 36 CPEs over four years

GIAC/SANS Affiliated Programs

Up to **36 CPEs**

- Can be applied to **five certifications**
- New GIAC Certification (Practitioner or Applied Knowledge)
- SANS training courses, including Live and OnDemand training

Advance Your Career

Up to **36 CPEs**

- Can be applied to **two certifications**
- ANAB accredited Industry Training*
- Graduate level courses
- Published technical work

Other Industry Training

Up to **18 CPEs**

- 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)

Community Participation

Up to **12 CPEs**

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

SANS NetWars

Up to **12 CPEs**

- Can be applied to **two certifications**
- NetWars Tournament
- NetWars Continuous

Cyber Ranges

Up to **12 CPEs**

- Can be applied to **one certification**
- DoD exercises
- Capture the Flag
- Other hands-on activities

Work Experience

Up to **12 CPEs**

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

GIAC
CERTIFICATIONS

www.giac.org

Sept 2024