GIAC™
CERTIFICATIONS

www.giac.org

GIAC Catalog

2026

Prove Your Skills. Advance Your Career.

Choose Your GIAC Path

GIAC's certification journey gives you flexible ways to prove what you know by certification category and by portfolio certifications. Build skills, validate skills, earn miletsons, and show real capability with creentials employers trust.

The Power of Certification

Research shows that certification pays off for you and your organization.

Benefits for Organizations

Source: Pearson VUE 2024 Value of Certification Report

81% produce higher quality work

77% more innovative and enhance work outcomes

72% more efficient and productive

82% greater ability to mentor and support co-workers

74% increased work autonomy and independence

74% perform a task/fill a role they could not before

Benefits for Employees

Source: Pearson VUE 2024 Value of Certification Report

92% feel more confident in their abilities

84% are more determined to succeed professionally

78% are more satisfied with their jobs

74% have greater work autonomy and independence

80% successfully met their goal whether it was a pay raise, job promotion, productive gains, and/or personal satisfaction

GIAC® The Gold Standard in Cybersecurity Certifications

- 50+ certifications across every major cybersecurity domain
- Real world, hands-on testing that validates job ready skills
- Maps to over 100+ specific job roles and requirements
- Updated annually to match today's threat landscape
- Trusted globally by Fortune 100 and governments worldwide
- DoD Approved and compliant with 8140 Directive
- Legally defensible with alignment to ISO 17024

Maximizing ROI With Certifications

Investing in IT certification impacts the bottom line for businesses.

The **ROI** per credentialed employee is extimated to be as high as

$30,000

64% of IT decision makers estimate that each credentialed IT employee adds

$10,000

or more in the **additional value** of their cfontribituions compaired to their non-certified counterparts.

"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."

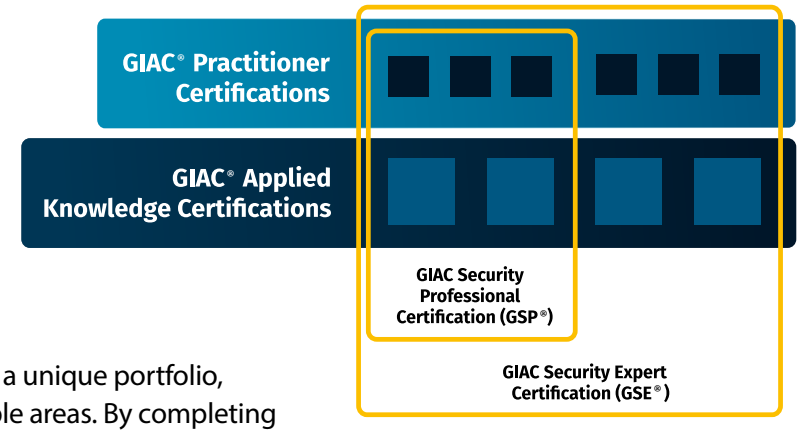
Ben Boyle, GWAPT®, GXPN™, GPEN®

"Attackers are always evlovling, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it's a continuous fight."

Jason Sevilla, GCIH®, CMON®, GSEC®

Create Your Own Path

There is no single path in cybersecurity. GIAC lets you build a journey that fits your goals. Specialize deeply in one area or expand multiple domains.



Two ways to certify

- Practitioner Certifications
- Applied Knowledge Certifications

Practitioners can mix and match certifications to build a unique portfolio, showcasing expertise in specific fields or across multiple areas. By completing a portfolio, you can earn the GIAC Security Professional (GSP) certification. From there, you can aim for the GIAC Security Expert (GSE) certification, the pinnacle of GIAC credentials.

Stack Skills. Build Momentum.

GIAC's 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:

- Increase your value and options
- Make growth more achievable
- Unlock new opportunities
- Keep work interesting and rewarding

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

GIAC Certification Categories:

GIAC Practitioner Certifications

These certifications validate your skills and ability to succeed in real-world roles.

- ideal for those new to a focus area or working toward a GSP or GSE.
- Cover a broad range of infosec topics like offensive operations, cyber defense, cloud security, management, and ICS.
- May include hands-on CyberLive® - Real lab, Real tools, Real Skills exam format questions.
- Stackable with Applied Knowledge Certifications to build a portfolio.

The best preparation includes Affiliated Partner SANS Course training and GIAC practice exams. GIAC offers 45+ Practitioner Certifications.

GIAC® Applied Knowledge Certifications

Next level hands on certification.

GIAC Applied Knowledge Certifications are designed to measure deeper, more complex capability.

- Cover a range of topics to validate a candidate more thorough understanding of the subject matter
- 100% CyberLive® exams are designed to push beyond individual technical skills. CyberLive® questions require you to synthesize your skills and use them to solve real-world challenges in a virtual machine environment
- Designed for candidates who wish to challenge themselves and demonstrate mastery of a subject
- Stackable with Practitioner Certifications to build portfolios toward the GSP® or GSE® certifications.

Unlike Practitioner exams, preparation for Applied Knowledge Certifications is not tied to a specific training course. GIAC recommends reviewing the Areas Covered list on the certification page, combining it with relevant training, hands-on experience, and practical labs to ensure success.

Demo Question Sets are available for purchase. These sets include three one-time-use questions designed to provide insight into the exam format.

GIAC Currently offers 6 Applied Knowledge Certifications with the ability to show expertise in Offensive Operations, Cyber Defense, and Digital Forensics and Incident Response Areas.

Offensive Operations

GIAC Experienced Incident Handler Certification (GX-IH)®

GIAC Experienced Penetration Tester (GX-PT)®

Cyber Defense

GIAC Experienced Cybersecurity Specialist Certification (GX-CS)®

GIAC Experienced Intrusion Analyst Certification (GX-IA)®

Digital Forensics

GIAC Experienced Forensic Analyst (GX-FA)®

GIAC Experienced Forensics Examiner (GX-FE)™

GIAC Certification Portfolios:

GIAC Security Professional (GSP®)

The GSP portfolio demonstrates depth and breadth , an important milestone on the path to becoming a GSE Expert.

Requirements to earn GSP:

- 3 GIAC Practitioner Certifications + 2 GIAC Applied Knowledge Certifications (any combination)
- Certifications can be earned on your timeline but must remain active

You will receive a GIAC Security Professional Coin.

GIAC Security Expert (GSE®)

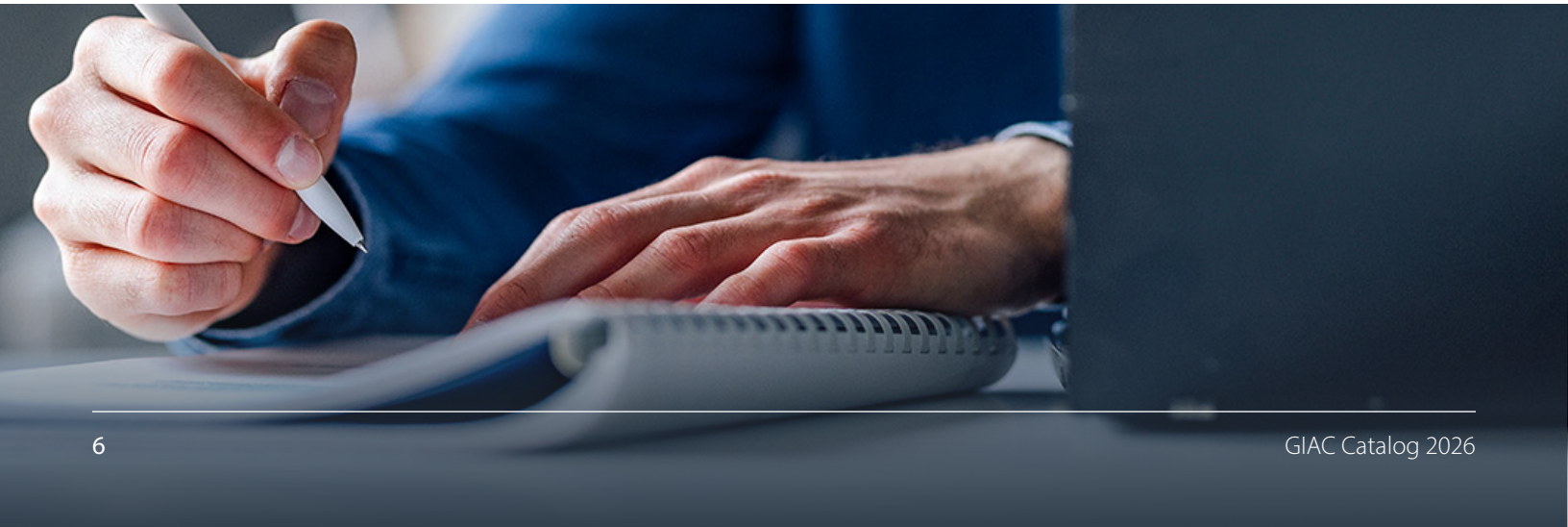
The most prestigeious credential in the IT security industry. Built for professionals who want to prove elite, across domain capability.

Requirements to earn GSE:

- 6 GIAC Practitioner Certifications + 4 GIAC Applied Knowledge certifications (any combination)
- Certifications can be earned on your own timeline, but must remain active

You will receive 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

There is no single route to expertise. SANS instructors and industry leaders come from diverse backgrounds. What they share is relentless practice, continued learning, real experience, and validated skills.

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®

CyberLive:
Real labs. Real tools. Real skills.

CyberLive is a hands-on exam format that replaces traditional multiple-choice testing with performance-based challenges in realistic lab environments to validate real-world capability.

Virtual Machines:

Full-scale lab systems that behave like physical computers: install, attack, defend, and run services.

Real Security Tools:

Exact tools used by professionals every day including all the quirks and challenges.

Authentic Code:

Real code, real exploits, real impacts.

> *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

GSEC® Security Essentials

ANAB | DoD 8140 | NIS2 | DORA

- 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

ANAB | NIS2 | DORA

- 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™

GSOA® Strategic OSINT Analyst

- Automate data collection and analysis with Python scripting.
- Investigate the Dark Web, track cryptocurrency transactions, and analyze disinformation.
- Apply international OSINT techniques and perform image, video, and audio forensics.

SANS® Course: SEC587™: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™

Purple Team Certifications

GFACT® Foundational Cybersecurity Technologies

ANAB | DoD 8140

- 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

ANAB | DoD 8140 | NIS2 | DORA

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

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

GDAT™ Defending Advanced Threats

DoD 8140

- 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™

Blue Team Operations Certifications

GOSI™ Open Source Intelligence

DoD 8140 | NIS2 | DORA

- 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

ANAB | DoD 8140

- 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™

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™ Machine Learning Engineer

- Machine Learning
- Data Science
- Anomaly Detection & Optimization

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

GISF® Information Security Fundamentals

ANAB | DoD 8140

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

SANS Course: SEC301™: Intro to Cyber Security™

GMON® Continuous Monitoring

DoD 8140 | NIS2 | DORA

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

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

GDSA™ Defensible Security Architecture

DoD 8140 | NIS2 | DORA

- 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

DoD 8140

- 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.

Purple Team Certifications

GDAT™ Defending Advanced Threats

DoD 8140

- 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

ANAB | DoD 8140

- 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

DoD 8140

- 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

DoD 8140

- 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*

Penetration Testing Certifications

GCIH® Certified Incident Handler

ANAB | DoD 8140 | NIS2 | DORA

- 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™

GPEN® Penetration Tester

ANAB | DoD 8140 | NIS2 | DORA

- 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

DoD 8140

- 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™

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™

GXPN™ Exploit Researcher and Advanced Penetration Tester

DoD 8140 | NIS2 | DORA

- Network Attacks, Cryptography and Restricted Environments
- Scapy, fuzzing, and source code analysis
- 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™

GMOB® Mobile Device Security Analyst

DoD 8140

- 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™

GOAA™ Offensive AI Analyst

- AI-powered reconnaissance & OSINT automation
- AI-aided vulnerability discovery, patch diffing, and exploit generation
- Malware development with AI
- Legal, ethical, and OPSEC considerations

SANS Course: SEC535™: Offensive AI - Attack Tools and Techniques™

GASAE™ AI Security Automation Engineer

- Automating asset discovery, configuration management and incident response workflows
- Applying AI concepts such as LLMs, RAG and agentic AI to detection and response
- Analyzing host artifacts and integrating automation into SOC operations
- Using automated attack chaining and breach and attack platforms to assess defensive readiness

SANS Course: SEC598™: AI and Security Automation for Red, Blue, and Purple Teams™

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

ANAB | DoD 8140 | NIS2 | DORA

- 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

DoD 8140 | NIS2 | DORA

- 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™

Start Your Cyber Career with GIAC®

If you're just beginning your career in cyber security, you've come to the right place. With affiliated partner 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

ANAB | DoD 8140 | NIS2 | DORA

- 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

ANAB | DoD 8140 | NIS2 | DORA | SEC

- 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

DoD 8140

- 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™

GLIR® Linux Incident Responder

- Linux Incident Response, Threat Hunting, and Intrusion Analysis
- Linux File Systems, System Triage, and Evidence Collection
- Linux User Data, Application, and Timeline Analysis

SANS Course: FOR577™: ALinux Incident Response and Threat Hunting™

GCTI® Cyber Threat Intelligence

DoD 8140 | NIS2 | DORA | SEC

- 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

AI-FOCUSED

NIS2 | DORA

- 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

DoD 8140

- 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

AI-FOCUSED

- 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™

GCFR™ Cloud Forensics Responder

CYBERLIVE

DoD 8140

- 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™

GEIR™ Enterprise Incident Responder

CYBERLIVE

NIS2 | DORA | SEC

- 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™

GRID™ Response and Industrial Defense

DoD 8140 | NIS2 | DORA

- 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™

GCIH® Certified Incident Handler Certification

CYBERLIVE

ANAB | DoD 8140 | NIS2 | DORA

- 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

AI-FOCUSED

GSLC® Security Leadership

ANAB | DoD 8140 | NIS2 | DORA

- 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™

AI-FOCUSED

GSTRT™ Strategic Planning, Policy, and Leadership

DoD 8140 | NIS2 | DORA | SEC

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

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

AI-FOCUSED

GCCC® Critical Controls Certification

NIS2 | DORA

- 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™

GSOM™ Security Operations Manager

NIS2 | DORA

- 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™

GCIL™ Cyber Incident Leader

NIS2 | DORA | SEC

- Preparing for, assessing, remediating and closing an incident
- Developing, managing and improving the IM team and process
- Identifying threats, vulnerabilities and common malicious attacks, and handling each incident type

SANS Course: LDR553™: Cyber Incident Management™

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

Up to 36 CPEs

GIAC/SANS Affiliated Programs

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

Up to 36 CPEs

Advance Your Career

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

Up to 18 CPEs

Other Industry Training

- Can be applied to **three certifications**
- DoD or Military Training
- Skill-based training courses
- All-day or multi-day training events & summits (virtual or in person)

Up to 12 CPEs

Community Participation

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

Up to 12 CPEs

SANS NetWars

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

Up to 12 CPEs

Cyber Ranges

- Can be applied to **three certifications**
- DoD exercises
- Capture the Flag
- Other hands-on activities

Up to 12 CPEs

Work Experience

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

Cloud Security Certifications

Securing the cloud is now essential across our global infrastructure. GIAC's cloud security certifications validate that you have the necessary skills 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.

Cloud Security Certifications

GWEB™ Web Application Defender

DoD 8140

- 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

ANAB | DoD 8140

- 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™

> *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*

GCLD™ Cloud Security Essentials

ANAB | DoD 8140

- 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: SEC502™: Cloud Security Tactical Defense™

GPCS™ Public Cloud Security

AI-FOCUSED

DoD 8140

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

SANS Course: SEC510™: Cloud Security Controls and Mitigations™

GCTD™ Cloud Threat Detection

AI-FOCUSED

- 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™

AI-FOCUSED

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™

CYBERLIVE

GCFR™ Cloud Forensics Responder

DoD 8140

- 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™

GCAD™ Cloud Security Architecture and Design

NIS2 | DORA

- Identity and access management
- Design and implement Zero-Trust concepts
- Network architecture and design

SANS Course: SEC549™: Cloud Security Architecture™

Cloud Security Micro-Credential

AWS Secure Builder Micro-Credential

- Securing AWS environments, including IAM, CI/CD security, and workload hardening.
- Monitoring solutions, mitigating attack vectors, and applying incident response best practices for enhanced AWS infrastructure security
- AWS zero trust principles and supply chain security for a resilient infrastructure.

SANS Course: SEC480™: AWS Secure Builder™

GIAC
CERTIFICATIONS

for additonal information,
visit GIAC.org

February 2026