GIAC
CERTIFICATION CATALOG
2021

The Highest Standard in Cybersecurity Certification

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.

GIAC
CERTIFICATIONS

Why certify with GIAC?

GIAC certifications span the breadth of infosec

GIAC certifications are a mile deep for specialized job-focused tasks across industry focus areas including offensive operations, cyber defense, cloud security, DFIR, management, and ICS.

GIAC exams test real-world skills

Every certification confirms a practitioner's abilities and likelihood of success in a real-world work environment. GIAC exams with CyberLive take this validation a step further, requiring candidates to perform lab-based, hands-on tasks.

Industry recognition and respect

GIAC certifications are listed as preferred qualifications on thousands of job postings across the globe. That's because hiring managers and infosec professionals know that GIAC certifications are a guarantee of critical skill mastery.

Dedication to exam quality and relevancy

Our team of exam developers is made up of experts who have devoted their professional lives to infosec - both at GIAC and as practitioners in the field. Every detail of our exams is rigorously evaluated by a psychometrician to ensure fairness and accuracy.

Start the path to become a security expert

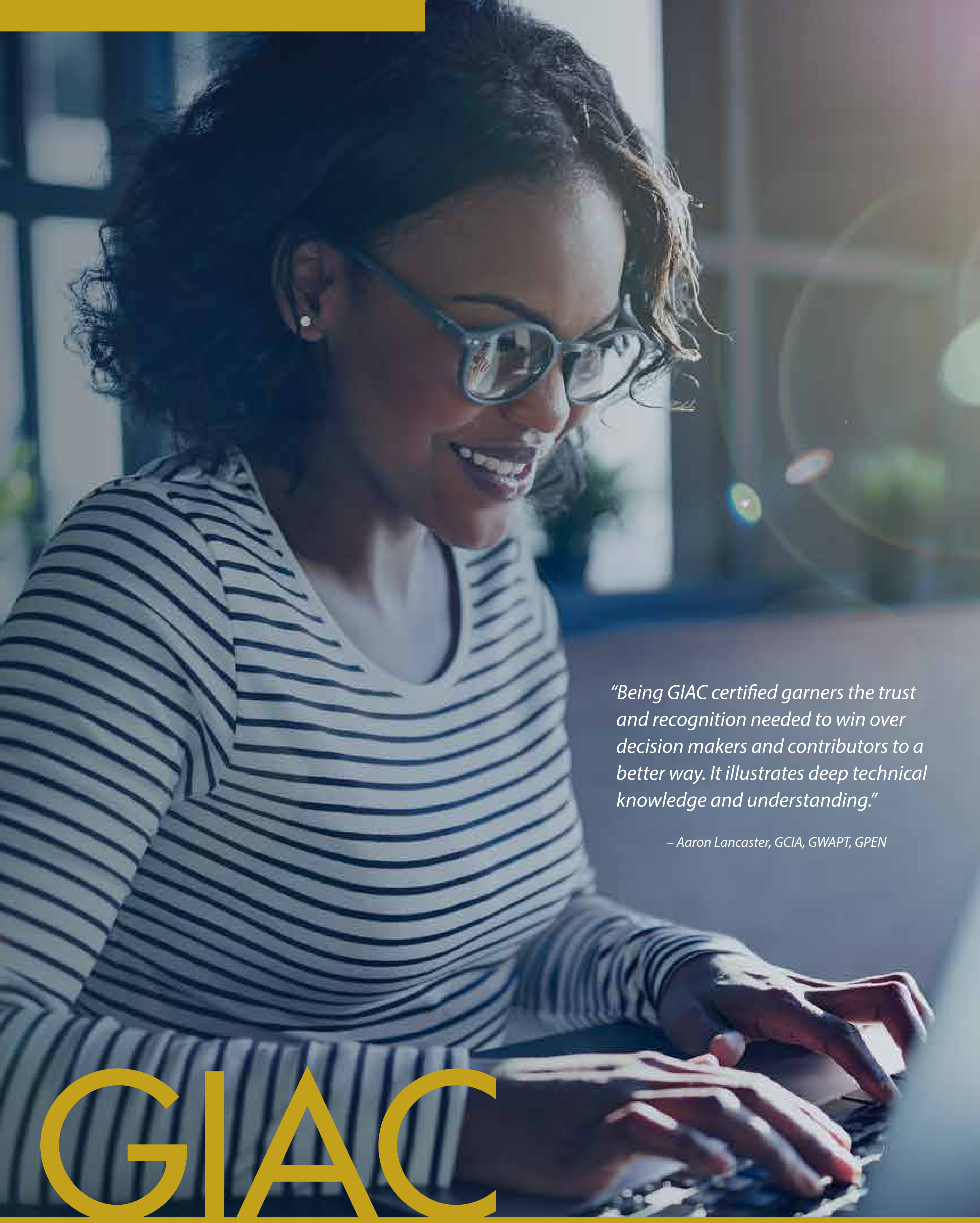
GIAC can guide you on your career journey through progressively more complex skills and job roles. The GIAC Security Expert (GSE), recently ranked the highest-value certification in the industry, is widely recognized as one of the most challenging and meaningful credentials in cybersecurity.

Become part of the SANS & GIAC family

Everyone who successfully completes their certification exam is welcomed into the community to share information, explore resources, and create new connections. High scorers are invited to join the GIAC Advisory Board.

"Attackers are always evolving, 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, GMON, GSEC



"Being GIAC certified garners the trust and recognition needed to win over decision makers and contributors to a better way. It illustrates deep technical knowledge and understanding."

– Aaron Lancaster, GCIA, GWAPT, GPEN

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 two areas: blue team operations and cyber defense essentials, 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.

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: **SEC487** Open-Source Intelligence (OSINT) Gathering & Analysis

GCIA Intrusion Analyst

CYBERLIVE

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

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

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

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

> *"GIAC has helped open doors for me in my cyber-security 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*

Cyber Defense Essentials Certifications

GCUX Unix Security Administrator

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

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

GISF Information Security Fundamentals

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

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

GSEC Security Essentials

CYBERLIVE

- 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

Purple Team Certifications

GFACT Defending Advanced Threats

- 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 Incident Handler

CYBERLIVE

- 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

GISP Information Security Professional

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

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

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

"If a hiring manager is trying to structure desired experience paired with relevant certs, then the practical component of the exam makes them more sure that someone could step in and do the things that their job entails from day one."

– Jason Nickola, GSE and COO, Pulsar Security

Raising the bar even higher on GIAC certifications.

CYBERLIVE

GIAC's CyberLive exams feature practical questions in a lab environment requiring test takers to perform hands-on tasks mimicking what they might find in their daily work. Practical testing provides added value to both practitioners and employers, and CyberLive testing sets GIAC apart as a leader in infosec skill validation.

- CyberLive goes beyond theory by testing the practical application of critically needed infosec abilities
- CyberLive provides a new tool for employers to identify skilled practitioners in key disciplines
- CyberLive skill validation confirms practitioners could start a new job and get right to work on day one

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

Current exams featuring CyberLive. More to come in the near future:

GCIH GPEN GXPN GWAPT GREM GSEC GCIA GCFA

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 work across specialized red, purple, and exploit development teams.

Penetration Testing Certifications

GPEN Penetration Tester

CYBERLIVE

- 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

CYBERLIVE

- 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** Mobile Device Security and Ethical Hacking

GXPN Exploit Researcher and Advanced Penetration Tester

CYBERLIVE

- 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

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

Red Team Operations Certifications

GCIH Incident Handler

CYBERLIVE

- 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

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

GEVA Enterprise Vulnerability Assessor

- Vulnerability assessment framework planning and methodology in an enterprise environment
- Discovery and validation of vulnerabilities using tactics like network scanning and PowerShell scripting
- Remediation and reporting techniques utilizing proper data management

SANS Course: **SEC460** Enterprise Threat and Vulnerability Assessment

Purple Team Certifications

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

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

> *"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*

Stay relevant with renewal

Keep your hard-earned GIAC certification active to remain current and competitive in the cybersecurity workforce. We recommend the CPE option: collect 36 credits over four years to keep your certification active. Here are the many ways to earn CPEs by simply staying active in the industry.

GIAC/SANS Affiliated Programs

Up to 36 CPEs

- Can be applied to 3 certifications
- SANS training courses, including Live and OnDemand training
- New GIAC certifications
- GIAC gold paper

Accredited Professional Activities

Up to 36 CPEs

- Can be applied to 2 certifications
- Accredited professional training or certification
- Graduate level courses
- Published technical work

Other Industry Training

Up to 18 CPEs

- Can be applied to 1 certification
- Multi-day skills-based training
- In-person conferences/seminars
- Vendor training
- Virtual presentations/conferences/seminars

NetWars & Cyber Ranges

Up to 12 CPEs

- Can be applied to 1 certification
- SANS NetWars
- DoD hands-on Cyber Range activities

Work Experience

Up to 12 CPEs

- Can be applied to 1 certification
- Relevant technical & management experience

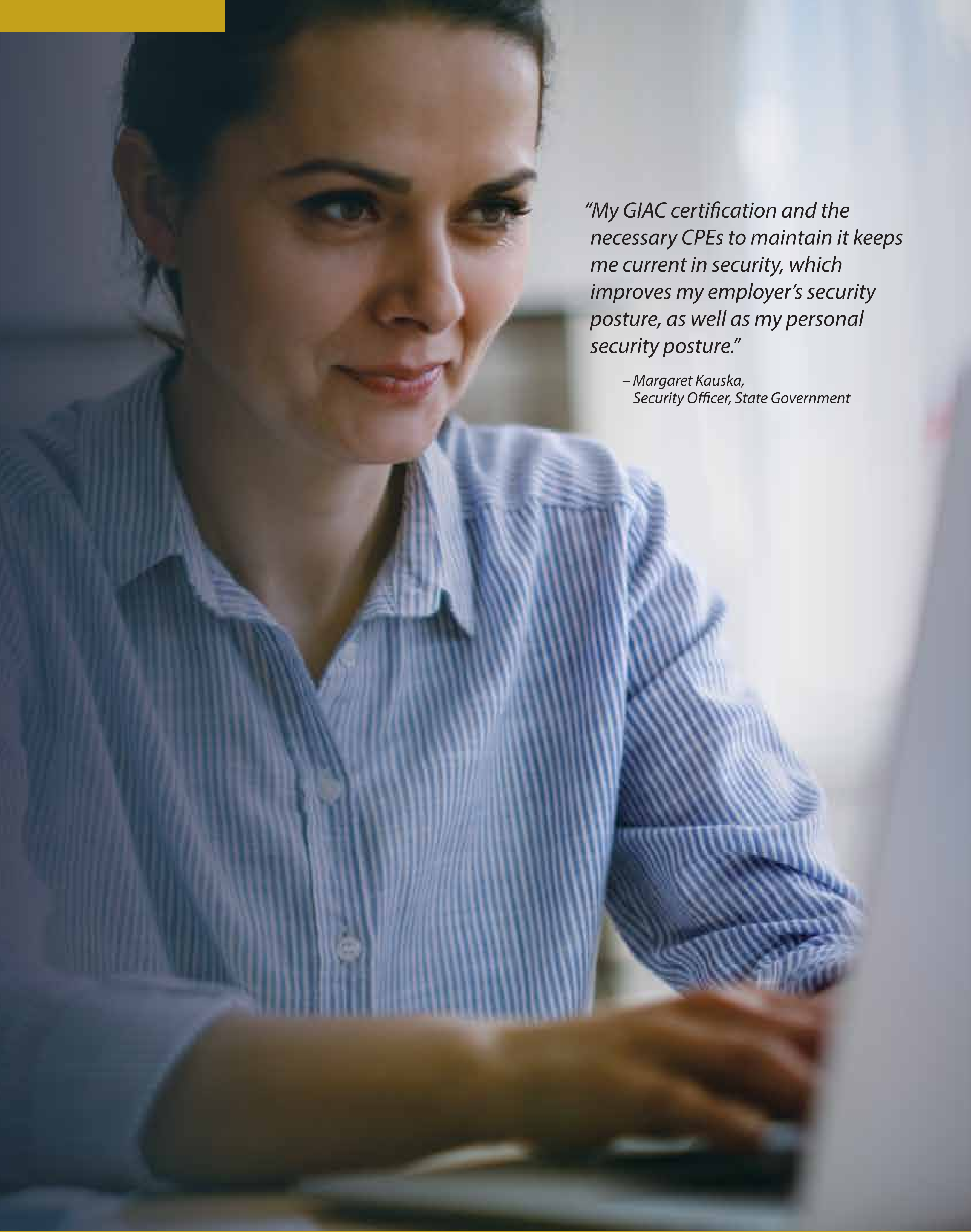
Community Participation

Up to 12 CPEs

- Can be applied to 1 certification
- Participating in GIAC exam development activities
- Participating in SANS webcasts
- Writing an article for an information assurance publication

Other renewal options:

- Successfully complete the current certification exam.
- Maintain your GSE to automatically renew all other GIAC certifications!



> *"My GIAC certification and the necessary CPEs to maintain it keeps me current in security, which improves my employer's security posture, as well as my personal security posture."*
>
> *– Margaret Kauska,*
> *Security Officer, State Government*

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

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 system 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.

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

> *'The best thing about a GIAC cert is that beyond earning the certification itself, you enter a sharing community of specialists that allows you to continue learning and sharing what you learn."*
>
> *– Frederik Raabye, GWAPT, GSEC*

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?

GFACT

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

GISF

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

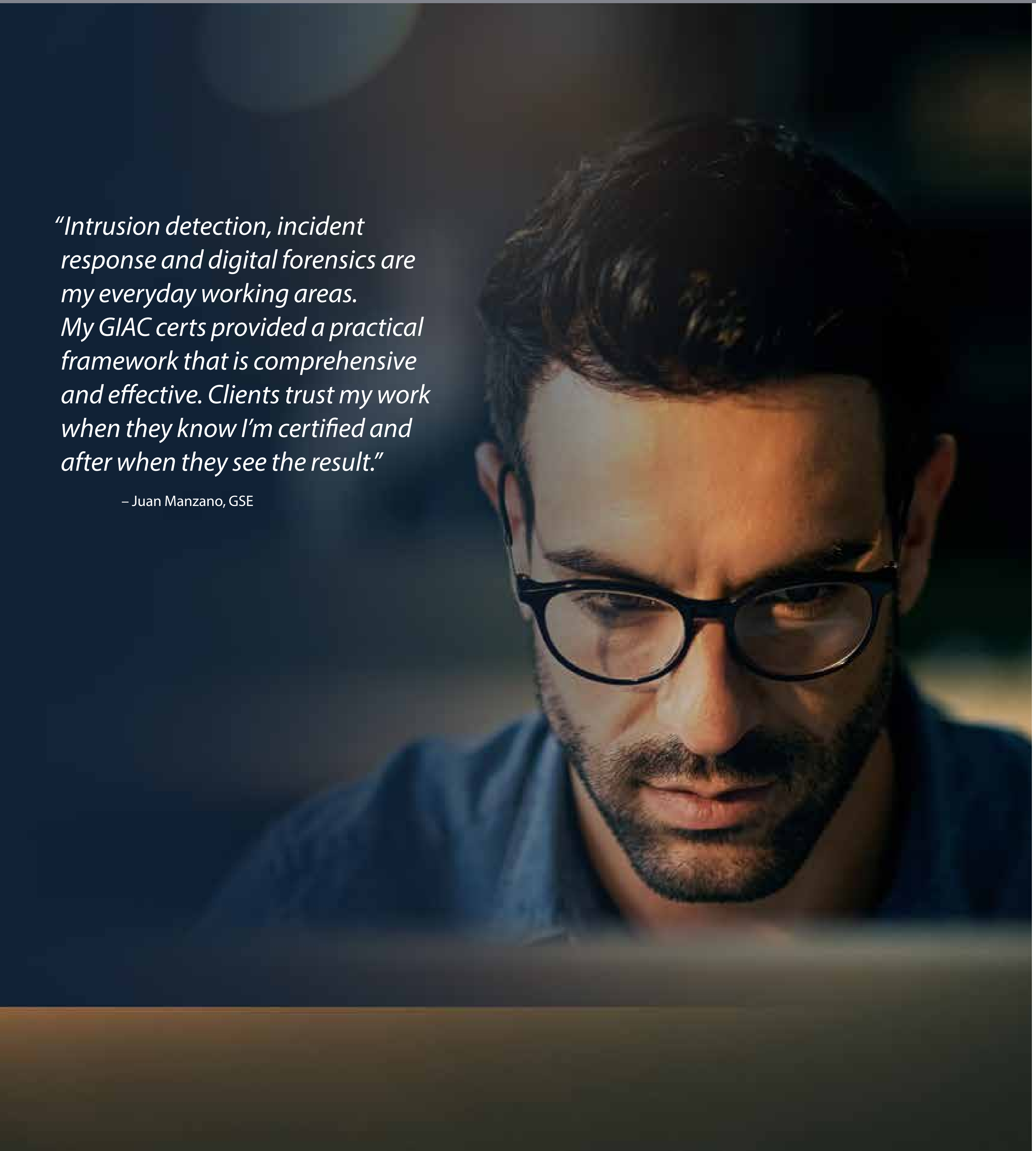
GSEC

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



"Intrusion detection, incident response and digital forensics are my everyday working areas. My GIAC certs provided a practical framework that is comprehensive and effective. Clients trust my work when they know I'm certified and after when they see the result."

– Juan Manzano, GSE

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.

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**

CYBERLIVE

- 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 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**

CYBERLIVE

- 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

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**: Battlefield Forensics and Data Acquisition

Management, Legal & Audit 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. Managers need technical knowledge as well as traditional management skills to be effective leaders for their infosec teams. GIAC's Management 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.

Management Certifications

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

GSOM GIAC 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: **MGT551** Building and Leading Security Operations Centers

Legal Certifications

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

Audit Certifications

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

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

> *"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

- 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

GCSA Cloud Security Automation

- 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 DevOps Automation

GCLD Cloud Security Essentials

- 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

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**: Public Cloud Security: AWS, Azure, and GCP

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

> *"An understanding of vulnerability management and cloud security is becoming not only valuable, but a necessity to keep one's organization secure in this constantly changing and dynamic environment."*
>
> – Kae David, GSEC

How to get started in Cloud Security

Today's cybersecurity practitioners need the latest cloud security skills not only to succeed in their careers, but to carry out their mission of keeping our world safe. SANS & GIAC have the resources you need to build your cloud security career.

Explore resources to increase your awareness

Immersing yourself in the latest cloud security research is the first step to building the knowledge you need for a cloud career. Check out these free resources from SANS & GIAC for a deeper dive into the world of cloud security:

- Read up on the latest cloud developments in the SANS blog
- Check out downloadable posters and cheat sheets
- Read research papers written by cloud practitioners
- Practice in your home lab with open-source cloud tools

85%
of respondents have team members with security certifications.

94%
believe that their certifications have better prepared them for their current role.

82%
of organizations prefer to hire candidates with certifications.

Learn from experts to broaden your knowledge

After exploring new resources and familiarizing yourself with cloud terms and tools, it's time to begin gaining actionable knowledge to apply at work. Take it one step further by learning from cloud security experts.

- Join free SANS summits to learn from the best
- Listen to cloud security webcasts featuring industry experts
- Checkout SANS.edu's new grad certificate in Cloud Security
- Watch videos detailing the latest tools & tech

Master the basics with SEC488 & GCLD

The best way to ensure you've got the foundational skills for a career in cloud security is by taking SANS SEC488: Cloud Security Essentials. After training, prove your skills with the GIAC Cloud Security Essentials certification. GCLD is designed to confirm your ability implement preventive, detective, and reactionary techniques to defend valuable cloud-based workloads. With this certification under your belt, you'll be qualified for most junior-level cloud security job roles.

Build higher-level, specialized skills

Once you've mastered the basics, it's time to gain the specialized skills you need for career advancement. Are you interested in cloud architecture and infrastructure? Checkout the GIAC Cloud Security Automation (GCSA) certification. Want to be the go-to public cloud and multi cloud expert at your organization? Master the Big 3 with GIAC Public Cloud Security (GPCS). Do you prefer a more offensive angle? Gain cloud pen test skills with the GIAC Cloud Penetration Tester (GCPN) certification. Interested in securing web applications? Consider GIAC Web Application Defender (GWEB).

Stay in the cloud community

No matter which direction you decide to go, the important thing is to keep learning. Continue to engage with the community, whether on social media or at summits, to be the first to know about the latest developments in the field – and to share your own expertise with others who are just beginning their journey into cloud security.

Learn more at giac.org/cloud

SANS Institute

Helping Individuals and Organizations Master Cybersecurity

Advanced Degrees

For IT professionals seeking to advance their careers by focusing on cybersecurity leadership and management.

SANS Security Awareness

Training for organizations that need to improve cybersecurity throughout their organization.

Interactive Learning

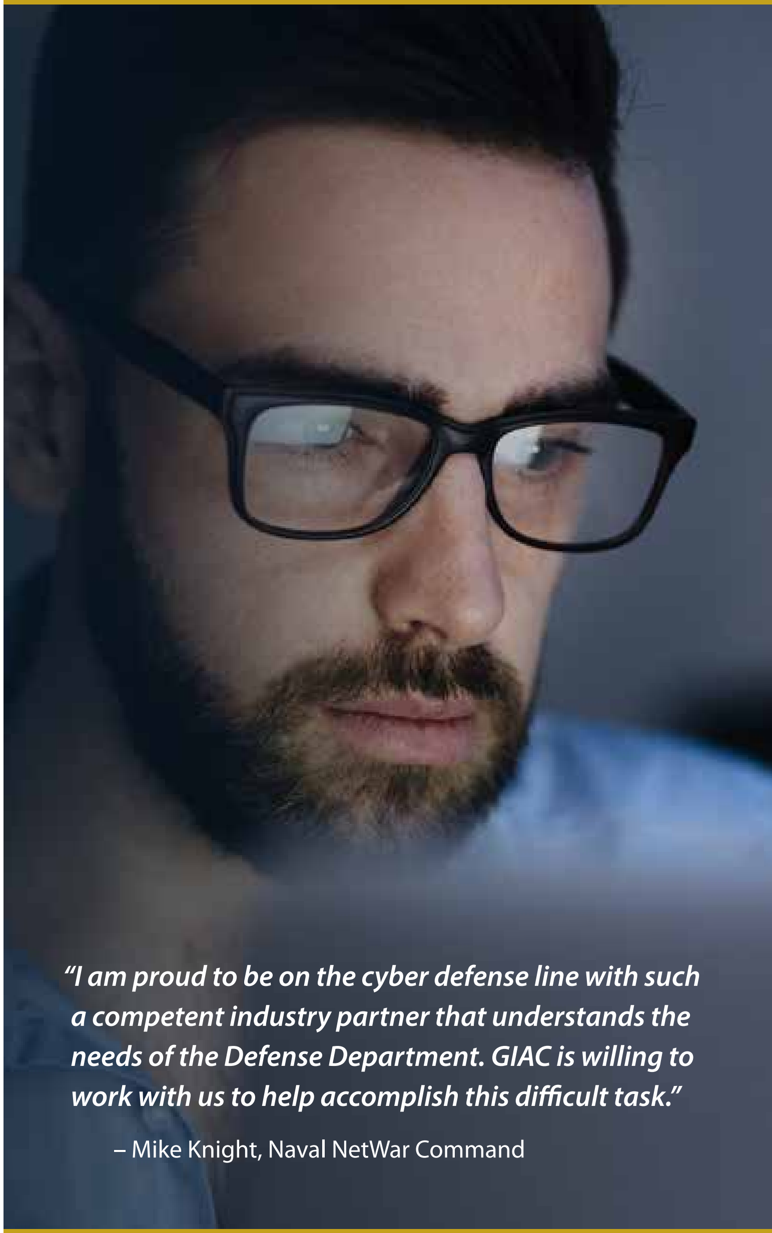
Hands-on cyber range learning with a focus on mastering the skills that information security professionals can use in their jobs every day.

CyberTalent Sourcing

For organizations in need of trained and certified cybersecurity experts.

GIAC CERTIFICATIONS

WWW.GIAC.ORG



> *"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

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.

giac.org/government