SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

MGT512: **Security Leadership Essentials for Managers**

GSLC
Security Leadership
giac.org/gslc

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

Course Author Statement

"I have found that technical professionals who are taking on management responsibility need to learn how to convey security concepts in ways that non-technical people can understand. At the same time, managers who are new to security need to learn more about the different domains of cybersecurity. In both cases, there is a need to learn about the work of managing security. That is why this course focuses on the big picture of securing the enterprise, from governance all the way to the technical security topics that serve as the foundation for any security manager. Ultimately, the goal of the course is to ensure that you, the advancing manager, can make informed choices to improve security at your organization."

— Frank Kim

> **"This course was very relevant to my new role as Director of IT."**
>
> — Brian Harris, **Jackson EMC**

> **"MGT512 is valuable because it is relevant/current to the security landscape from my management vantage point."**
>
> — Michael Bradley, **Prudential Financial**

Leading Security Initiatives to Manage Information Risk

Security managers need both technical knowledge and management skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics.

This course empowers you to become an effective security manager and get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle, including governance and technical controls focused on protecting, detecting, and responding to security issues.

This course will prepare you to:

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage technical personnel
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Lead a Security Operations Center (SOC)
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud
- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

How the Course Works

MGT512 uses case scenarios, group discussions, team-based exercises, in-class games, and a security leadership simulation to help students absorb both technical and management topics.

The course uses the Cyber42 leadership simulation game. This web-application-based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

sans.org/mgt512

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Building Your Security Program

The course starts with a tour of the information and topics that effective security managers and leaders must know to function in the modern security environment. This includes an understanding of the different types of cybersecurity frameworks available to structure your security team and program. Risk is central to effective information security management, and key risk concepts are discussed to lay the foundation for effective risk assessment and management. Security policy is a key tool that security managers use to manage risk. We'll cover approaches to policy to help you plan and manage your policy process. Finally, security functions, reporting relationships, and roles and responsibilities are discussed to give the advancing manager a view into effective security team and program structure.

TOPICS: Security Frameworks; Understanding Risk; Security Policy; Program Structure

SECTION 3: Protecting Data and Systems

Section 3 focuses on protecting data and systems. This includes building an understanding of cryptography concepts, encryption algorithms, and applications of cryptography. Since encrypting data alone is not sufficient, we'll discuss the distinction between privacy and security to give managers a primer on key privacy concepts. To implement new initiatives, security leaders must also develop negotiating skills and the ability to manage highly technical team members. Finally, we cover security awareness, which is a huge component of any security program that must drive activities that lead to changes in human behavior and create a more risk-aware and security-aware culture.

TOPICS: Data Protection; Negotiations Primer; Privacy Primer; Security Awareness

SECTION 5: Detecting and Responding to Attacks

Section 5 focuses on detection and response capabilities. This includes gaining appropriate visibility via logging, monitoring, and strategic thinking about a security information and event management (SIEM) system. When making a large investment, such as a SIEM, managers must also conduct a thorough analysis of vendors. Once implemented, the logs in a SIEM are a core component of any Security Operations Center (SOC). We'll discuss the key functions of a SOC along with how to manage and organize your organization's security operations. The incident response process is discussed in relation to identifying, containing, eradicating, and recovering from security incidents. This leads into a discussion of longer-term business continuity planning and disaster recovery. Managers must also understand physical security controls that, when not implemented appropriately, can cause technical security controls to fail or be bypassed. The course ends with a war game that simulates an actual incident. This tabletop simulation contains a number of injects or points at which students are presented with additional information to which they can respond. After dealing with the incident itself, the simulation concludes with a game focused on choosing appropriate security controls to mitigate future incidents.

TOPICS: Logging and Monitoring; Vendor Analysis; Security Operations Center; Incident Response; Contingency Planning; Physical Security

SECTION 2: Protecting Networks and Systems

Section 2 provides foundational knowledge to protect networks and systems. This includes a thorough discussion of network security that is modeled around the various layers of the network stack. This leads into a discussion on building a vulnerability management program and the associated process to successfully find and fix vulnerabilities. Finally, we cover malware and attack examples and corresponding host security controls for the endpoint and server. These topics give managers a deeper understanding of what their teams are talking about and where various issues and protections lay within the seven layers of the network model.

TOPICS: Network Security; Vulnerability Management; Host Security

SECTION 4: Leading Modern Security Initiatives

Section 4 covers what managers need to know about leading modern security initiatives. Managers must be knowledgeable about software development processes, issues, and application vulnerabilities. We'll look at the secure SDLC, OWASP Top Ten, and leading-edge development processes built on DevSecOps. For any project or initiative, security leaders must also be able to drive effective project execution. Having a well-grounded understanding of the project management process makes it easier to move these projects forward. We'll also discuss modern infrastructure-as-code approaches and tools to automate consistent deployment of standard configurations. The cloud is a major initiative that many organizations are either tackling now or planning to undertake. To get ready for these initiatives, we'll provide an overview of Amazon Web Services (AWS) to serve as a reference point and discuss key cloud security issues based on the Cloud Security Alliance guidance. The cloud, the rise of mobile devices, and other factors are highlighting weaknesses in traditional, perimeter-oriented security architectures. This leads to a discussion of the Zero Trust Model.

TOPICS: Application Security; DevSecOps; Project Management; Infrastructure as Code; Cloud Security; Modern Security Architecture

Who Should Attend

- Security Managers
  - Newly appointed information security officers
  - Recently promoted security leaders who want to build a security foundation for leading and building teams
- Security Professionals
  - Technically skilled security administrators who have recently been given leadership responsibilities
- Managers
  - Managers who want to understand what technical people are telling them
  - Managers who need an understanding of security from a management perspective

GSLC
Security Leadership
giac.org/gslc

GIAC Security Leadership

The GIAC Security Leadership (GSLC) certification validates a practitioner's understanding of governance and technical controls focused on protecting, detecting, and responding to security issues. GSLC certification holders have demonstrated knowledge of data, network, host, application, and user controls along with key management topics that address the overall security lifecycle.

- Cryptography concepts & applications for managers, networking concepts & monitoring for managers
- Managing a security operations center, application security, negotiations and vendors, and program structure
- Managing security architecture, security awareness, security policy, and system security
- Risk management and security frameworks, vulnerability management, incident response and business continuity