

LDR512: Security Leadership Essentials for Managers



GSLC
Security Leadership
giac.org/gslc

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Decipher the pros and cons of different reporting relationships
- Manage and lead technical teams and projects
- 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
- Build security engineering capabilities using automation and Infrastructure as Code (IaC)
- Understand and secure generative AI (GenAI) services
- 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



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 and applications for managers, networking concepts and 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

Leading Security Initiatives to Manage Information Risk

Take this security management course to learn the key elements of any modern security program. LDR512 covers a wide range of security topics across the entire security stack. Learn to quickly grasp critical information security issues and terminology, with a focus on security frameworks, security architecture, security engineering, computer/network security, vulnerability management, cryptography, data protection, security awareness, cloud security, application security, DevSecOps, generative AI security, and security operations.

The training course uses the Cyber42 leadership simulation game to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. Throughout the class you will participate in 23 Cyber42 activities.

What Is Security Management?

Security management is all about managing information risk. This means that you need the appropriate level of technical knowledge and leadership 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. Being an effective security leader requires you to get up to speed quickly on information security issues and terminology to build a modern security program. Creating a high-performing security team means that you can anticipate what security capabilities need to be built to enable the business and mitigate threats.

Business Takeaways

This course will help your organization:

- Develop leaders that know how to build a modern security program
- Anticipate what security capabilities need to be built to enable the business and mitigate threats
- Create higher performing security teams

Hands-On Security Manager Training

This leadership-focused security training course 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. About 60–80 minutes per day is dedicated to these learning experiences using the Cyber42 leadership simulation game.

This leadership simulation 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.

“This is an excellent primer for management types. I come from a technical background and can see the value there plain as day.”

—Matt Zaycer, Pilot Flying J

Section Descriptions

SECTION 1: Building Your Security Program

The course starts with a tour of the information 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, so we'll discuss key risk concepts in order 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, we'll discuss security functions, reporting relationships, and roles and responsibilities to give the advancing manager a view into effective security team and program structure.

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

SECTION 2: Technical Security Architecture

Section 2 provides coverage of traditional and modern security architectures focused on technical topics. This includes a thorough discussion of network security that is modeled around the various layers of the network stack. As modern attacks are also focused on the computing devices we cover malware and attack examples along with corresponding host security controls for the endpoint and server. The cloud is a major initiative that many organizations is changing the way organizations operate and design their controls. To get ready for these initiatives, we provide an overview of Amazon Web Services (AWS) to serve as a reference point and discuss key cloud security issues. The cloud, the rise of mobile devices, and other factors are highlighting weaknesses in traditional, perimeter-oriented security architecture which leads into a discussion of the Zero Trust Model.

TOPICS: Security Architecture Overview; Network Security; Host Security; Cloud Security; Identity and Access Management; Zero Trust

SECTION 3: Security Engineering

Section 3 focuses on security engineering best practices. This includes building an understanding of cryptography concepts, encryption algorithms, and applications of cryptography which are foundational elements of building any secure system. Since encrypting data alone is not sufficient, we discuss the distinction between privacy and security to give managers a primer on key privacy concepts. Managers must also be knowledgeable about software development processes, issues, and application vulnerabilities. We cover application security and leading development processes built on DevSecOps. Current engineering approaches also include modern infrastructure as code approaches and tools to automate consistent deployment of standard configurations. Finally, generative AI has led to the growth of AI usage and newer Large Language Model application architectures which need to be secured.

TOPICS: Security Engineering; Data Protection; Privacy Primer; Application Security; Privacy Engineering

SECTION 4: Security Management and Leadership

Section 4 covers what managers need to know about leading security initiatives. Every security leader should know how to build a vulnerability management program and the associated process to successfully find and fix vulnerabilities. Additionally, security awareness is a huge component of any security program that helps drive activities to change human behavior and create a more risk-aware and security-aware culture. To implement new initiatives, security leaders must also develop negotiation skills and conduct thorough analysis of vendors. Finally, for any project or initiative, security leaders must also be able to drive effective project execution. Having a well-grounded understanding of the management and leadership practices makes it easier to move your projects forward.

TOPICS: Vulnerability Management; Security Awareness; Negotiations Primer; Vendor Analysis; Managing and Leading Teams

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. 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.

TOPICS: Logging and Monitoring; Security Operations Center (SOC); Incident Handling; Contingency Planning; Physical Security

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Security personnel who have team lead or management responsibilities
- Anyone who wants to go beyond technical skills
- Technical professionals who want to learn to communicate with senior leaders in business terms

NICE Framework Work Roles

- Information Systems Security Manager (OPM 722)
- Cyber Workforce Developer and Manager (OPM 751)
- Cyber Policy and Strategy Planner (OPM 752)
- Executive Cyber Leadership (OPM 901)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

“This course is great content for leaders within the field. It pushes people to stop always focusing on the technical aspects of cybersecurity and really understand what the business needs from its security function as a whole to enable the business.”

—Alexander Walker, TechVets