LDR512: **Security Leadership Essentials for Managers™**

GSLC
Security Leadership
giac.org/gslc

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Apply cybersecurity frameworks and assess risks
- Lead technical teams and manage security projects
- Develop vulnerability management and SOC programs
- Integrate security in DevOps and automate with IaC
- Foster a security-aware culture and shared knowledge
- Secure modern architectures, including cloud and GenAI
- Communicate effectively with technical teams

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

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 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 (GenAI) 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 25 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.

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

Section 1 starts with the core knowledge needed to operate effectively in today's security environment. It covers key cybersecurity frameworks, risk management fundamentals, and practical approaches to security policy. The section also explores security functions, reporting structures, and roles and responsibilities to help leaders build and manage effective security programs.

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

SECTION 2: Technical Security Architecture

Section 2 equips leaders with a practical understanding of traditional and modern security architectures, covering network, host, cloud, and identity security fundamentals. It examines malware and endpoint protections, core cloud concepts using Amazon Web Services (AWS) as a reference point, and key Identity and Access Management (IAM) risks, while showing how Zero Trust principles address the limits of perimeter-based security.

TOPICS: Security Architecture Overview; Network Security; Host Security; Cloud Security; IAM; Zero Trust

SECTION 3: Security Engineering

Section 3 prepares leaders to oversee security engineering practices, covering cryptography fundamentals, application security, and secure development approaches. It also addresses DevSecOps, Infrastructure as Code (IaC), and the governance and risk considerations introduced by machine learning models (LLMs), GenAI, and modern AI systems.

TOPICS: Security Engineering; Data Protection; Application Security; DevSecOps, GenAI and LLM Security, GenAI Security Controls

SECTION 4: Security Management and Leadership

Section 4 covers what managers need to know about leading security initiatives, including vulnerability management, security awareness, and building a risk-aware culture. It also introduces privacy fundamentals, vendor analysis and negotiation, and the management practices required to execute security projects effectively.

TOPICS: Vulnerability Management; Security Awareness; Privacy and Negotiation Primers; Vendor Analysis; Managing and Leading Teams

SECTION 5: Detecting and Responding to Attacks

Section 5 focuses on what managers need to know about detection, response, and operational resilience. It addresses visibility through logging and monitoring, the role of security information and event management (SIEM) and Security Operations Centers (SOC), and effective incident response. The section also introduces business continuity, disaster recovery, and the importance of physical security in supporting technical controls.

TOPICS: Logging and Monitoring; SOC; Cyber Incident Management; 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**