LDR512: Security Leadership Essentials for Managers

GIAC SECURITY GSLC LEADERSHIP

Course Overview

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.

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.

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.

Job Roles

Information Systems Security Manager

Cyber Workforce Developer and Manager

Cyber Policy and Strategy Planner

Executive Cyber Leadership

Program Manager

IT Project Manager

Intended Audience

- 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

Duration

5 Days

Certifications

GIAC Security Leadership (GSLC)

Contact Us

☎ 800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

ATA APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

LDR512: Security Leadership Essentials for Managers

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: Building Your Security Program

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

SECTION 2: Technical Security Architecture

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

SECTION 3: Security Engineering

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

SECTION 4: Security Management and Leadership

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

SECTION 5: Detecting and Responding to Attacks

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

Prerequisites

This security management course covers the core areas of security leadership and assumes a basic understanding of technology, networks, and security. For those who are new to the field and have no background knowledge, the recommended starting point is the SEC301: Introduction to Information Security course. While SEC301 is not a prerequisite, it will provide the introductory knowledge to maximize the experience with LDR512.

Course Objectives

- 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 (GSLC)

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