LDR551: Building and Leading Security Operations Centers

Course Overview

Whether you are looking to build a new SOC or take your current team to the next level, LDR551 will super-charge your people, tools, and processes. Each section of LDR551 is packed with hands-on labs that demonstrate key SOC capabilities, and each day concludes with "Cyber42" SOC leadership simulation exercises. Students will learn how to combine SOC staff, processes, and technology in a way that promotes measurable results and covers all manner of infrastructure and organizational requirements. Attackers are always improving, so a SOC that sits still is losing ground. LDR551 will give SOC managers and leaders the tools and mindset required to build the team, process, workflow, and metrics to defend against modern attackers by building the processes for continuously growing, evolving, and improving the SOC team over time.

If you are a SOC manager or leader looking to unlock the power of proactive, intelligence-informed cyber defense, then LDR551 is the perfect course for you! In a world where IT environments and threat actors evolve faster than many teams can track, position your SOC to defend against highly motivated threat actors. Highly dynamic modern environments require a cyber defense capability that is forward-looking, fast-paced, and intelligence-driven. This SOC manager training course will guide you through these critical activities from start to finish and teach you how to design defenses with your organization's unique risk profile in mind. Walk away with the ability to align your SOC activities with organizational goals.

Job Roles

- Security Operations Center Managers or Leads
- Security Directors
- New Security Operations Team Members
- Lead / Senior SOC Analysts
- Technical CISOs and Security Directors

NICE Framework Work Roles:

- Information Systems Security Manager, OV-MGT-001
- Cyber Policy and Strategy Planner, OV-SSP-002
- Executive Cyber Leadership, OV-EXL-001
- Program Manager, OV-PMA-001
- Cyber Defense Incident Responder, PR-CIR-001
- OT SOC Operator, ZZ-ICS-004

Prerequisites

This course does not have any specific prerequisites, but it is suggested that students have some experience in an operational security role. SANS courses such as SEC450: Blue Team Fundamentals: Security Operations and Analysis or MGT512: Security Leadership Essentials for Managers will give students a solid base-level understanding of the concepts that will be discussed.

Duration

6 Days

Certifications

GIAC Security Operations Manager (GSOM)

Contact Us

800.674.3550

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

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

LDR551: Building and Leading Security Operations Centers

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: SOC Design and Operational Planning

TOPICS: The State of the Cyber Defense Industry - Trends, Problems, and Priorities; SOC Planning - Charters, Mission, Team Planning, Org. charts and more; Mapping the SOC Functions - Collection, Detection, Triage, Investigation, and Incident Response; Team Creation, Hiring, and Training - Building Job Specifications, Interviews, Hiring, Training and More; Cyber Threat Intelligence for the SOC - Identifying, Collecting, and Processing the Most Important Sources; Building the SOC - Both Physical and Virtual

SECTION 2: SOC Telemetry and Analysis

TOPICS: Cyber Defense Theory and Mental Models; Critical SOC Tools and Technology; SOC Data Collection; Using MITRE ATT&CK to Plan and Prioritize Collection; SOC Analyst Capacity Planning; Protecting SOC Data and Capabilities from Interference

SECTION 3: Attack Detection, Hunting, and Triage

TOPICS: Analytic Frameworks and Tools; Threat Detection and Analytic Design; The Keys to Efficient Alert Triage; Detection Engineering Process and Lifecycle; SOC-Assisted Use Cases; Threat Hunting Process and Tracking; Active Defense Tactics and Techniques

SECTION 4: Incident Response

TOPICS: Planning and Preparation for Incident Response; Identification and Categorization of Incidents; Coordination During Incident Discovery; Incident Response Tools; Containment and Eradication Stage Activities; Incident Response in the Cloud; Investigation; Recovery, Post-Incident Activity, and Practice

SECTION 5: Metrics, Automation, and Continuous Improvement

TOPICS: Staff Retention and Burnout Mitigation; Building Your SOC Culture; Metrics, Goals, and Effective Execution; Measurement and Prioritization Issues; Automation in Security Operations; Analytic Testing and Adversary Emulation; SOC Capability Assessment; The Lean SOC

Course Objectives

- Construct a strong SOC foundation based on a clear mission, charter, and organizational goals
- Collect the most important logs and network data
- Build, train, and empower a diverse team
- Create playbooks and manage detection use cases
- Use threat intelligence to focus detection efforts on true priorities
- Apply threat hunting process and active defense strategies
- Implement efficient alert triage and investigation workflow
- Operate effective incident response planning and execution
- Choose metrics and long-term strategy to improve the SOC
- Employ team member training, retention, and prevention of burnout
- Perform SOC assessment through capacity planning, purple team testing, and adversary emulation

GIAC Security Operations Manager (GSOM)

The GIAC Security Operations Manager (GSOM) certification validates a practitioner's ability to effectively manage a technical team and strategically operate a Security Operations Center (SOC) to align with an organization's business goals and security requirements.

- Designing, planning, and managing an effective SOC program
- Prioritization and collection of logs, development of alert use cases, and response playbook generation
- Selecting metrics, analytics, and long-term strategies to assess and continuously improve SOC operations