LDR551: Building and Leading Security Operations Centers™

GSOM
Security Operations Manager
giac.org/gsom

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Construct a strong SOC foundation based on a cEstablish mission-driven SOC foundation aligned with organizational goals
- Develop advanced threat intelligence and detection capabilities
- Build and empower high-performance security teams
- Create robust incident response and threat hunting strategies
- Implement critical metrics for continuous SOC improvement
- Master team development, retention, and performance optimization
- Execute comprehensive security assessment through advanced testing methodologies

Business Takeaways

- Implement strategies for aligning cyber defense to organizational goals
- Decrease risk profile due to improved security validation tools and techniques
- Apply methodologies for recruiting, hiring, training, and retaining talented cyber defenders
- Streamline effective cross-team coordination and collaboration
- Employ immediate security optimization improvements using current assets
- Reduce financial spend due to smoother cyber security operations

"There are so many [organizations] that seem to be trying to reinvent the wheel. All they need to do is invest in this course for real-world, actionable information that can put them on a solid path toward building, staffing, and leading their own SOC."

—Brandi Loveday-Chesley

Prevent – Detect – Respond | People – Process – Technology

Information technology is so tightly woven into the fabric of modern business that cyber risk has become business risk. SOC managers must align their operations to organizational priorities and demonstrate measurable value, a challenge when threats are hard to quantify and stakeholder expectations are often vague. How does a SOC leader communicate value, justify investments, and focus efforts on what truly protects the business?

LDR551 breaks down security operations into clear, measurable functions that can be tracked and continuously improved. We then connect these core SOC activities directly to organizational goals, giving you the frameworks to communicate impact with executives and stakeholders in language they understand. Common questions SOC leaders face:

- How do we ensure our security teams are aligned to the unique threats facing our organization?
- How do we achieve consistent detection and response results that minimize business impact?
- How can we build empowered, high-performing teams that solve problems proactively while avoiding burnout?
- What metrics actually matter, and how do we demonstrate continuous improvement to leadership?

Whether you're building a new SOC from the ground up or elevating your current team's capabilities, LDR551 delivers the strategies, frameworks, and hands-on experience to transform your operations. Each section includes practical labs covering mission planning, threat modeling, detection engineering, playbook development, and quality improvement, culminating in Cyber42 SOC leadership simulation exercises that test decision-making under pressure.

You'll learn to combine people, processes, and technology in ways that produce measurable results across any infrastructure or organizational structure. Attackers continuously evolve, a SOC that stands still falls behind. LDR551 equips you with the leadership mindset, proven frameworks, and continuous improvement processes needed to build resilient teams that stay ahead of sophisticated threats over the long term.

Hands-On SOC Manager Training

While LDR551 is focused on management and leadership, it is by no means limited to non-technical processes and theory. The 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 five days of instruction, students will work on seventeen hands-on exercises covering everything from playbook implementation to use case database creation, attack and detection capability prioritization and visualization, purple team planning, threat hunting, and reporting. Attendees will leave with a framework for understanding where a SOC manager should be focusing efforts, how to track and organize defensive capabilities, and how to drive, verify, and communicate SOC improvements.

Section Descriptions

SECTION 1: SOC Design and Operational Planning

Section 1 introduces the core mission and foundational models of a modern SOC, establishing the strategic and operational context for effective leadership.

TOPICS: SOC Planning; Cyber Threat Intelligence for the SOC; Building the SOC; Hiring and Staffing for the SOC; Creating a Positive SOC Culture

SECTION 2: SOC Telemetry and Analysis

Section 2 of LDR551 focuses on expanding our understanding of attacker tactics, techniques, and procedures and how we might identify them in our environment.

TOPICS: Critical SOC Tools and Technology; SOC Data Collection; Using MITRE ATT&CK to Plan Collection; Protecting SOC Data and Capabilities; SOC Capacity Planning

SECTION 5: Metrics, Automation, and Continuous Improvement

The fifth and final section of LDR551 is all about measuring and improving security operations.

TOPICS: AI And Automation in Security Operations; Staff Retention and Burnout Mitigation; Metrics, Goals, and Effective Execution

SECTION 3: Attack Detection, Hunting, and Triage

Section 3 of LDR551 is all about building and improving your threat detection capability.

TOPICS: Analytic Frameworks for Improving Detection; Detection Engineering; Threat Hunting and Active Defense; The Keys to Efficient Alert Triage

SECTION 4: Incident Response

From toolsets to proven frameworks to tips and tricks learned in countless real-world scenarios, section four covers the full response cycle, from preparation to identification to containment, eradication, and recovery, for operations managers.

TOPICS: Planning and Preparation for Incident Response; Incident Identification, Containment, and Response; Coordination During Incident Discovery

"I would recommend this course to anyone running a security operations team. I'd further recommend it to more experienced analysts so they can begin to see the bigger picture."

—Robert Wilson, **University of South Carolina**

Who Should Attend

This course is intended for those who are looking to build a Security Operations Center for the first time or improve the one their organization is already running. Ideal student job roles for this course include:

- 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

- Security Control Assessor (OPM 612)

GSOM
Security Operations Manager
giac.org/gsom

GIAC Security Operations Manager

The GSOM certification validates a professional's ability to run an effective Security Operations Center (SOC). GSOM-certified professionals are well-versed in the management skills and process frameworks needed to strategically operate and improve a SOC and its team.

- 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 strategy to assess and continuously improve SOC operations