LDR551: Building and Leading Security Operations Centers

GSOM
Security Operations Manager
giac.org/gsom

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- 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

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 cybersecurity 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 to their organization and demonstrate real value—a challenge when threats are hard to quantify and stakeholder requirements for the security team are often vague and difficult to translate. How does a SOC communicate their value and focus on operations that enable the organization? LDR551 breaks down security operations into clear and atomic functions that can be measured and improved. We then tie these core SOC activities to high-level organizational goals for easy communication with the SOCs constituency. Common questions SOC managers face are:

- How do we know our security teams are aligned to the unique threats facing our organization?
- How do we get consistent results and prove that we can identify and respond to threats in time to minimize business impact?
- How can we build a SOC team that is empowered and continuously improving, where analysts are empowered to solve problems while focusing on the mission at hand?

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.

What is a SOC Manager?

A SOC Manager leads an organization’s cybersecurity operations team by developing and guiding implementation of a cyber defense strategy that can minimize the impact of cybersecurity incidents. Leading a SOC is a complex role that requires merging technical and business sensibilities, and the skills to monitor performance, communicate requirements, and demonstrate results up and down the chain of command.

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 interactive 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

LDR551 starts with the critical elements necessary to build your Security Operations Center (SOC): understanding your enemies, planning your requirements, making a physical space, and building your team. Throughout this course section, students will learn how to build a strong foundation upon which an SOC can operate, focusing first on the most important users and data, and tailoring defense plans to threats most likely to impact your organization. Through workflow optimization, information organization, and data collection, you will learn how to ensure that your security operations will hit the ground running as efficiently as possible while protecting privileged SOC users and data.

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

Section 2 focuses on expanding our understanding of attacker tactics, techniques, and procedures and how we might identify them in our environment. This day discusses defensive theory and mental models that can guide our assessment and planning efforts, data collection and monitoring priorities, and cyber threat intelligence collection. The course focus of this section is ensuring your team has the visibility and data sources required to do the job, and that they will continue to operate without failure for the long term.

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

Section 3 is all about building and improving your threat detection capability. Starting with tool selection and setup to enable effective alert triage and analysis and moving towards analytic design, this section focuses on ensuring no attack goes unseen. We focus detection engineering as a core SOC discipline to be planned, tracked, and measured, show how to implement and manage detection use cases, and demonstrate how to plan and execute threat hunts. The results are a structured approach that leads to measurable improvements to your detection capability. Finally, we will look at active defense concepts and their role in a mature security operations capability. Taking the tools, processes, and concepts from Section 3 back to your SOC will ensure that no (virtual) stone in your environment remains unturned.

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

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. Section 4 begins with preparing your people, processes, IT infrastructure, and forensics toolset to quickly identify and remediate incidents. In this section, we will review best practices in cloud incident response, forensic analysis, playbook development, and cross-team collaboration. Lab exercises in Section 4 include incident response playbook design and implementation, investigation review and quality control, incident response goal setting, and cross-team collaboration.

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

The fifth and final section of LDR551 is all about measuring and improving security operations. We focus on three areas: motivating your people and minimizing burnout, measuring SOC performance, and continuous SOC assessment through adversary emulation and SOC capability and maturity models. We will also cover some of the more challenging elements of managing people in a dynamic and often high-pressure environment: building the right culture, addressing damaging behaviors, and handling common pitfalls of daily operations. By focusing on our team and continuously improving quality toward a clear set of strategic goals, we can ensure long term growth and success. In section five, you'll receive the tools, techniques, and insights to do just that. Hands-on exercises will include designing SOC metrics, continuous assessment and validation, and SOC quality improvement using lean management concepts and techniques.

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

> **"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

- Information Security Manager: OV-MGT-001
- Cyber Policy and Strategy Planner: OV-SPP-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

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