# LDR551: **AI-Enabled SOC Leadership™**

**GSOM**
Security Operations Manager
giac.org/gsom

5 Day Program | 30 CPEs | Laptop Required

### You Will Be Able To

- Set a direction your team can act on
- Manage your budget with confidence
- Implement AI tools with guardrails
- Build a team sized for the workload
- Run a focused operation
- Stay in command during a crisis
- Communicate value and impact clearly

### Business Takeaways

- Security effort aligned to business risk
- Service commitments that hold
- Defensible technology and AI spending
- Retained expertise, lower turnover
- Faster response under clear authority
- Investment proven before it scales

**"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

**Build a Security Operation Center (SOC) You Can Trust When the Pressure is On.**

LDR551 takes you through the decisions that turn organizational priorities, people, and technology into effective security operations. Follow six connected stages of SOC design and operation — **Align, Design, Engineer, Lead, Operate, and Improve** — to build a new SOC or strengthen the one you lead today. Use AI to explore options, develop plans, and support SOC work, while learning how to verify its results, control its actions, and recognize when human judgment must lead. Prepare to make clearer decisions, develop your team, and put improvements into practice.

When a serious threat emerges, your SOC needs to find the evidence, decide what matters, and coordinate action before the attacker has a chance to get a foothold. Your ability to do that depends on choices made long before the first alert: what to monitor, who to hire, how to move work, and who may act.

As the SOC leader, you own those choices. You also face competing demands: expand coverage, reduce backlogs, develop your people, justify spending, and put AI to useful work. Every new service, tool, or automated action brings requirements for staff time, evidence, ownership, and support. You need a way to make those choices fit together and check whether they are working.

LDR551 gives you a practical path from defining the SOC's purpose to leading its operations and proving its improvements. Whether you are building a SOC from the ground up or improving an existing SOC, you will practice the decisions, conversations, and evidence reviews that move plans into daily work.

### Hands-On SOC Manager Training

In LDR551 you will practice the work a SOC leader performs, including reviewing evidence, comparing choices, explaining tradeoffs, assigning responsibility, and producing guidance and usable results. Exercises use the fictional organization, Ops Outpost, which has competing service demands, limited staff time, and changing security needs.

You will work with material such as service requests, technical proposals, case records, staffing information, simulated staff conversations, incident updates, and quality findings. Activities include creating a SOC charter, evaluating AI-enabled workflows, coaching employees, directing operational priorities, and defending improvement proposals.

AI-assisted activities give you opportunities to refine a draft, challenge an unsupported conclusion, or rehearse a difficult conversation. You remain responsible for the choices you make and the evidence supporting them. Debriefs explain how to adapt the methods and work products to your own SOC.

# Section Descriptions

### SECTION 1: Align and Design the SOC

Decide what the SOC must deliver, why the work matters, and what authority and resources it needs.

**TOPICS:**

- Organizational priorities, critical services, dependencies, threats, and obligations
- SOC mission, charter, scope, and initial success criteria
- Threat model creation and understanding organizational risk
- Cyber threat intelligence requirements and source quality
- Service design and operation

### SECTION 2: Engineer the SOC

Direct the technical choices that allow the SOC to deliver its services reliably and at a sustainable cost.

**TOPICS:**

- SOC tools and technology selection
- Agentic AI foundations and uses in the SOC
- Data collection, visibility gaps, retention, access, and cost
- Detection frameworks, languages, and coverage planning and evaluation
- Detection and analytic design/detection engineering as a process

### SECTION 3: Lead the SOC Team

Build and support a team that can perform the services and technical work the SOC has committed to deliver.

**TOPICS:**

- Team purpose, values, roles, and goals
- Building and designing your SOC workspace
- Skills, hiring assessments, and onboarding
- Training plan creation, career development, specialist and management paths, and succession
- The evolving role of the analyst in AI-enabled SOCs

### SECTION 4: Operate the SOC

Direct everyday work and major incidents as evidence, priorities, staffing, and available systems change.

**TOPICS:**

- Hunt selection, hypotheses, scope, staffing, time limits, and follow-up
- Intake, priority criteria, assignments, queue aging, backlog, and deferral
- Investigation oversight, alternative explanations, escalation, and closure
- Uses for AI during investigation
- Investigation quality review

### SECTION 5: Improve the SOC

Use clear metrics and measurements from SOC work to assess performance, and decide what needs correction, what deserves further investment, and which upstream choices need adjustment.

**TOPICS:**

- Defining clear security metrics
- Aligning SOC metrics with leadership
- Improving measurement and prioritization
- Balancing daily execution with SOC improvement initiatives
- SOC automation types and AI-powered automation

**"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 GIAC Security Operations Manager (GSOM) certification validates a practitioner's ability to field an effective Security Operations Center (SOC). GSOM certification holders are qualified to manage a technical team and strategically operate an SOC in alignment with an organization's business goals and security requirements.