LDR553: **Cyber Incident Management™**

GCIL
Cyber Incident Leader
giac.org/gcil

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Run briefings under pressure with minimal prep and deliver real impact
- Lead meetings when the team is stressed, the facts are incomplete, and execs are impatient
- Build and test your own GenAI tools to draft briefs, simulate reactions, and organize chaos
- Survive a supply chain breach with minimal third-party support
- Distinguish between technical facts, assumptions, and noise during incident response
- Use the CIMTK framework to prioritize tasks and drive progress
- Track attacker behavior, infrastructure risk, and team readiness in real time

"Great insights, examples and relevant tools. I applied the third-party incident tool within minutes to an ongoing third-party incident. So I can't dream of a more relevant and useful course than this."

—Jonas Roos Christense, **Copenhagen Airports**

Open in Case of Emergency

While you can't predict when a major cyber incident will hit your organization, you can control how ready you are to face it. In the aftermath, when incident response teams are engrossed in unraveling the attacker's moves within your networks, they often find themselves overwhelmed. This is where your incident management team steps in, taking charge of managing findings, communications, regulatory notifications, and remediation. With a multitude of tasks and challenges on their plate, many are unseasoned and unprepared for the magnitude of responsibilities.

This course equips you to not just be a member of the incident management team but a leader or incident commander. It ensures a comprehensive understanding of the immediate, short, and medium-term issues an organization might encounter. Beyond familiarizing yourself with the terminology, you'll grasp preparatory actions at different stages to stay ahead of the situation. LDR553 is designed for efficient management of diverse incidents, with a primary focus on cyber, yet its methodology, concepts, and guidance are applicable to various regular major and critical incidents.

What Is Cyber Incident Management

Cyber Incident Management (IM) sits above Incident Response (IR) and is tasked to manage incidents that get too big for the Security Operations Center (SOC) and IR. These tend to be the more impactful or larger-scale incidents that IR is not staffed to handle as it requires significant liaison with internal and external partners to coordinate the investigation, forensics, planning, recovery, remediation, and to brief the corporate comms, C-level staff and board as needed. Less technical and more business focused, the IM team will take the output from IR and relay it to the necessary teams as they coordinate wider investigations and hardening, hygiene and impact assessment as they plan towards recovery. A strong IR lead may fulfill the IM role, but during critical incidents IRs are often shoulder deep in malware, systems, logs and images to process to the point where all technically capable IR staff are kept focused on technical tasks. IMs are more business focused and IR is more technically focused.

Business Takeaways

- Develop expert cyber incident management capabilities
- Accelerate incident resolution with streamlined processes
- Foster better vendor and legal coordination during third-party breach escalation
- Improve team performance during critical incidents
- Reduce workload without increasing risk with the integration of GenAI
- Build a stronger bridge between technical and non-technical functions during cyber events
- Integrate threat intelligence to anticipate threats

Section Descriptions

SECTION 1: Understanding the Incident, Building the Team with GenAI, Scoping and Tracking the Impact

In Section 1 we will focus on understanding incidents, standardizing language, and defining objectives. You will gather information, set goals for the Incident Management team, and assign responsibilities. The section introduces the Cyber Incident Management Tool Kit (CIMTK), team composition, task tracking, and GenAI support.

TOPICS: Initial Information Gathering; Using Common Language; Defining Your Objectives; Who's on Our Team; Building Our Communications Plan

SECTION 2: Communications, Planning and Executing Remediations

We will explore communications in great depth as we look at interactions with executives, attackers, our staff and the public/customers. You will learn approaches that can buy time to address issues and prevent data leaks. You will categorize network and data damage, prioritize remediation tasks, and eliminate vulnerabilities, developing skills to create comprehensive incident reports and conduct root-cause analysis.

TOPICS: Talking To or Working With the Attackers; Tracking the Incident, and Progress; Remediation of Network Damage; Root-Cause Analysis Methods and Outcomes; Reporting and Documenting the Case; Ejecting Attackers with Available Options

SECTION 3: Training, Leveraging Cyber Threat Intelligence, and Bug Bounties

In this section we explore training incident response teams and the broader organization. You will learn to develop effective training programs based on organizational maturity and specific needs. We examine integrating Cyber Threat Intelligence (CTI) into incident response efforts and we deep dive into developing strategies for managing supply-chain and third-party compromises including those that leave us in an information vacuum.

TOPICS: Developing the Wider Team; Analysing Training Needs; Developing the SOC/IR/IM Team; Leveraging Cyber Threat Intelligence; Third-Party Supply-Chain Compromise

SECTION 4: Cloud Incidents, Business Email Compromise, Credential Theft Attacks, and Incident Metrics

In Section 4 you will gain a comprehensive view, visualize incident timelines and address complex attack scenarios. You will learn to create timelines tailored to different audiences, understand credential theft attacks and the MITRE framework, and explore Business Email Compromise (BEC), as well as cloud-based attacks and management console breaches. Finally, you will explore IR/IM team improvement, KPIs, and efficacy metrics.

TOPICS: Timelines for Visualization; Defining Cloud Attacks; Credential Theft Attacks; Business Email Compromise; Cloud Assets and Management Console Attacks; Improving IR/IM in the Organization and Bringing Change

SECTION 5: AI for Incidents, Attacker Extortion, Ransomware, and Capstone Exercise

Section 5 examines AI applications, including Large Language Models and Generative AI. You will gain in-depth knowledge of ransomware incidents from examining historic cases and considering how to prepare and train to deal with encryption events. Finally, you will participate in a comprehensive capstone exercise (note this is open for all delivery formats including OnDemand).

TOPICS: Leveraging IA for IM; Ransomware; Summary and Review of the Sessions; Capstone Exercise

Who Should Attend

- Security managers
  - Newly appointed information security officers who will be leading incidents
  - Recently promoted security leaders who want to understand incident management better
- Security professionals
  - Technically skilled security staff who have recently been given incident commander responsibilities
  - Team leads with the responsibility to support cyber incidents and whom may need to remediate systems
- Managers
  - Managers who want to understand how to manage technical people during an incident
  - Leaders who need an understanding of cyber incidents from a management perspective
- Legal/HR/PR staff
  - Staff who are new to cyber incident management but may be called upon to provide critical support in tense situations and who want to understand better what may be expected from them

NICE Framework Work Roles

- Knowledge Manager (OM-KMG-001)
- Cyber Legal Advisor (OV-LGA-001)
- Privacy Officer/Privacy Compliance Manager (OV-LGA-002)
- Information Systems Security Manager (OV-MGT-001)
- Communications Security (COMSEC) Manager (OV-MGT-002)
- Cyber Policy and Strategy Planner (OV-SPP-002)
- Executive Cyber Leadership (OV-EXL-001)

"The labs were perfect. Today's capstone exercise brilliantly brought together the elements we had learned, adopting tools to help deliver the products required. And while its goal was to deliver the final exercise of the course, it really has sparked the imagination of everything we can do with what we have learned. Excellent work."

—Lee T., **Law Enforcement**

GCIL
Cyber Incident Leader
giac.org/gcil

GIAC Cyber Incident Leader

The GIAC Cyber Incident Leader (GCIL) certification validates a practitioner's ability to manage cyber incidents and lead a diverse incident management (IM) team to restore normal operations. GCIL holders demonstrate expertise in preparing for, assessing, handling, tracking, and documenting incidents; developing IM teams; managing vulnerabilities, threats, and attacks; facilitating communication; and improving IM processes.