ROLE-BASED

CyberVista®

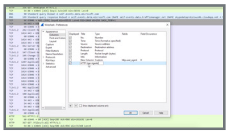
Critical Knowledge: **Incident Response**

Enhance incident response skills.

The Incident Response (IR) team is called in to respond and contain a breach when an organization's system has been compromised. Yet, upskilling individuals to act in a full IR capacity is not an easy task. The industry doesn't offer a well established learning path from a SOC Analyst or cybersecurity specialist role directly feeding into IR.

CyberVista now offers a 100% online role-based training program designed to effectively upskill employees and create a direct career development path into Incident Response more quickly and cost-effectively.

Domain 5, Forensics



Domain 3, Malware Pattern Analysis

Domain 5, Forensics

What is the Critical Knowledge: Incident Response Course?

Critical Knowledge: Incident Response is a comprehensive role-based course that builds on CyberVista's baseline Critical Knowledge program and SOC Analyst curriculum. Compiled into six (6) units, this training course covers highly technical and task-oriented subject matter parallel to explicit Incident Response functions.

Participants conduct guided lab exercises and complete tasks on virtual machines included in the course, with hours of on-demand lessons by an experienced instructor to help reinforce correct practice and application of skills. Practice exam assessments for CompTIA CySA+ are included as an added resource for employees interested in certification.

All CyberVista role-based Critical Knowledge courses are directly aligned with the National Cybersecurity Workforce Framework (NCWF), incorporating the knowledge, skills, abilities, and tasks (KSATs) to relevant cybersecurity job roles.

Who should take this course?

- **Newly hired Incident Response analysts**
- **Current cybersecurity employees** working in SOC or IR with 1-3 years of experience
- **Junior Pentesters and Red Teams** who want a better understanding of Blue Team or defensive operations
- **CERT, CSIRT, CIRT, or greater SOC teams**

Benefits of Training

- Role-based training to fast-track new hires' time to operational status
- Real-life, hands-on scenarios to ensure long term comprehension and retention
- Provide a clear, long term career development plan for employees

Course Domains

0

FOUNDATIONAL KNOWLEDGE

Establish or revisit foundational concepts on networking basics, hosting, and indicators of compromise.

1

INCIDENT RESPONSE OVERVIEW

Understand various roles within an organization and their responsibilities prior to, during, and after an incident occurs.

2

ATTACK LIFECYCLE

Overview of the Cyber KillChain and the Mitre Attack Framework.

3

HOST & NETWORK-BASED DETECTION & RESOLUTION

Become familiarized with means of detection and resolution of network intrusions and malware attacks.

4

ATTACK PATTERNS & MECHANISMS

Understand attacks listed in the OWASP Top Ten, the methods these attacks propagate and affect an organization, and remediation techniques.

5

FORENSICS

Become familiarized with digital forensics and techniques used, review case studies, and partake in additional hands-on exercises.

What's included?

A full-featured learning management system (LMS) enables both leaders and participants to access training materials throughout the program while also tracking progress and performance. This course also includes:

- **Diagnostic Assessment**
- **Video Lesson Library**
- **Configured REMnux and Windows 10 Virtual Machines**
- **Practice Labs**
- **Incident Response SOP Manual (PDF)**
- **Final Assessment**
- **(Optional) Practice Exam Preparation for CompTIA CySA+ certification**
- **Engagement and performance analytics** (for IR Manager or CIO)

Next level incident response starts here.

If you're ready to transform your Incident Response workforce, we're here to help create the right training strategy for your organization.

For more information contact us at **sales@cybervista.net** or call **844-558-4782.**

CyberVista®