ROLE-BASED

CyberVista®

Critical Knowledge: **SOC Analyst**

A Skilled SOC

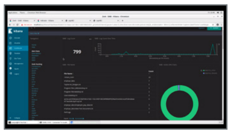
The Security Operations Center (SOC) is an organization's digital watch tower, where skilled cybersecurity practitioners actively monitor, detect, and remediate potential threats on the network.

With limited training resources readily available, managers are forced to require senior SOC analysts (Tiers II and III) to train new hires over the course of an average of 6-8 months, depleting precious personnel-hours and potentially creating security risk within the organization.

CyberVista now offers a 100% online training program designed to develop Tier I analysts on the technical facets of SOC in half the time, at a fraction of the cost, while minimizing security risk.

Domain 4, SIEM Analysis

Domain 3, Log Analysis



Domain 4, SIEM Analysis

What is the Critical Knowledge: SOC Analyst Course?

CyberVista's SOC Analyst course is a comprehensive role-based program that builds off of our baseline Critical Knowledge program. This course is broken down into six (6) units, covering fundamental cybersecurity concepts then focuses on more technical and task-oriented subject matter as it relates specifically to Tier I SOC functions.

Participants conduct guided lab exercises and complete tasks on virtual machines provided, with hours of on-demand lessons by an experienced instructor to help reinforce correct practice and application of skills. 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 Tier I SOC analysts**
- **Entry-level and junior information security analysts** who want to expand their career within security operations
- **Network or systems admins** interested in making the transition into a technical cybersecurity role

Benefits of Training

- Role-based training to fast-track incoming analysts' time to operational status
- Task-oriented lessons to ensure long term comprehension and retention
- Live online or on-demand instruction to reduce burnout of Tier II & III analysts
- Participants have the option to also prepare for the CySA+ certification

Course Domains

1

SOC ORG. & PROCESSES

Understand the roles and responsibilities of both the SOC and SOC analysts within an organization.

2

THREATS & VULN. ANALYSIS

Conduct vulnerability assessments and analysis, threat research, and establish known-good and known-bad network baselines.

3

DEVICE LOG ANALYSIS

Understand the importance and mechanisms of device logs, be able to conduct log analysis, and create scripts to automate analysis.

4

COMP. ORG. EVENT CORRELATION

Understand the purpose and application of SIEMS, conduct analysis of SIEM results, correlate multiple network events, and detect evidence of post-attack strategies.

5

PCAP ANALYSIS

Capture live traffic and conduct analysis on captured packets for indicators of network attacks.

6

INCIDENT RESPONSE

Understand the Incident Response phases and determine indicators of compromise for given incidents.

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**
- **Kali Linux & Security Onion Virtual Machines**
- **Practical Labs**
- **SOC Analyst SOP Cheatsheet & Video Transcript PDF**
- **Final Assessment**
- **(Optional) Practice Exam Preparation for CompTIA CySA+ certification**
- **Engagement & Performance Analytics** (for SOC Manager or CIO)

Strengthen your security operations.

If you're ready to transform your SOC 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®