CyberVista®

ROLE-BASED

Cloud SOC

Scale Up Cloud Security in SOC.

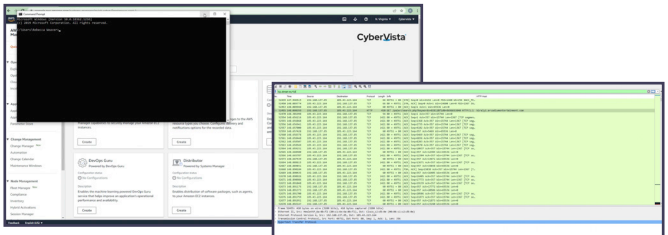
For many organizations, the Security Operations Center (SOC) acts as the keeper of enterprise data, networks, and applications, regularly providing reports on network activity and potential threats. However, with more systems migrating to the cloud, SOC teams must be able to manage multiple streams of data–both internal and external–and effectively log and assess different threats and vulnerabilities within their cloud infrastructure.

CyberVista's Cloud SOC course

What is the Cloud SOC Course?

CyberVista's Cloud SOC course is a five-hour, 100% online program that provides training for security professionals in the detection and identification of attacks on their cloud infrastructures. Learners will become familiar with network captures and logging in both the AWS and Azure instances. Additionally, learners will be prepared to conduct further vulnerability analysis and cloud inventory discovery.

Participants will gain first-hand knowledge of the implications of cloud security in SOC with instruction led by a subject matter expert and industry leader in security operations. This introductory role-based course serves as a precursor to the Critical Knowledge: SOC Analyst and the Cloud Incident Response programs.



Unit 3, Cloud Inventory and Data Discovery

Unit 2, Application Logging

Who should take this course?

- Security Professionals to familiarize themselves with cloud monitoring and detection concepts
- Tier I/II SOC Analysts
- Risk and Compliance Analysts
- Cloud Practitioners
- IT and Network Administrators

Benefits of Training

- Course taught by an industry leader in SOC
- Optional configurable Live Online training session
- Teaches to real-life scenarios and not certs

Course Units

1

ATTACK OVERVIEW AND NETWORK CAPTURE

This unit covers attack lifecycles (Cyber Kill Chain, Mitre Att&ck Framework) and network captures and logs.

- **Attack Lifecycle Review**
- **Network Captures and Logs**

2

LOGS OVERVIEW AND LOG TYPES

This unit introduces logging as a whole as well as various types of logs that security analysts will need while working in the cloud.

- **Log Overview**
- **Cloud Logging**
- **API Logging**
- **Application Logging**
- **Container Logs**

3

CLOUD MANAGEMENT AND VULNERABILITY ANALYSIS

This unit covers cloud inventory management, data discovery, and vulnerability analysis.

- **Cloud Inventory and Data Discovery**
- **Vulnerability Analysis**

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:** Easily administer a diagnostic assessment used to determine each team member's strengths and weaknesses.
- **Video Lesson Library:** Modular and engaging on-demand video lessons.
- **Expert Interviews:** Interviews with cybersecurity and IT leaders to provide context and real-world examples.
- **Knowledge Check Assessments:** Short, micro-quizzes throughout the lesson content to ensure engagement and knowledge retention.
- **Practice & Hands-on Activities:** Take-home activities and optional hands-on labs to reinforce practical applications of security concepts.
- **Final Assessment:** Participants conclude training with a final assessment to demonstrate knowledge and skills gained.

Your workforce needs work.

Interested in learning more about how CyberVista's Cloud SOC course can help your organization? Connect with our team for a free consultation.

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

CyberVista