Carmel
Trainings & Deployments

CTR-903 SIEM Administration and Operations

About this course

This 24-hours course will teach you how to utilize SIEM (Security Information and Event Management) for security operations such as proactive monitoring, threat hunting, and log management. In this course, you'll learn day-to-day administration tasks such as transferring security logs from the network and workstations to the SIEM Tool, analyzing security events once they arrive at the SIEM to determine whether there was an incident, and using other companion tools for case management, threat intelligence, and playbook creation for the Security Operation Center (SOC) for a streamlined process. You'll also learn about SIEM's history and generations, the benefits it provides to the SOC and the company, and how to assure its interoperability with other security stack products. As platforms such as Splunk, Wazuh, The Hive, MISP, and Cortex will be built alongside their integration, the lab will include activities that will place students hands-on that will reinforce the information captured during the course.

Audience profile

This course is for anyone with basic IT knowledge and fundamentals in cybersecurity. This course also is for individuals who are interested in taking the role of security analyst, cyber threat hunters and some other interesting role in the SOC.

At course completion

After completing this course, students will be able to:

- Understand SIEM and its importance within the SOC.
- SIEM administration during security operations to perform activities like monitoring, threat hunting and incident management.
- Installation of Wazuh, Splunk and its integration with tools like The Hive, MISP and Cortex
- Generations and historical coming of SIEM
- Log collection activities from workstations, networks and other security devices
- Deploy and manage the SIEM agents.

Course details

Module 1: Introduction to SIEM

This module gives students an overview of the Security Information and Event Management (SIEM) Platform, including what it does and how it may help organizations gain insight by correlating logs and security events from various sources and identifying anomalies within them.

Module 2: SIEM generations and history

This module covers the several generations of SIEM, as well as the history of the security community's journey to the current version of SIEM we use today, and a glimpse into where the industry is headed with the Next Gen SIEM platform. In general, the development of SIEM as a security tool.

Module 3: Why SIEM is important and benefit to security operations
This session demonstrates how the SIEM may help with security operations and risk assessment in general. You'll discover why SIEM is often referred to as the "heart" of the SOC, and how correlations and validations help enterprises see threats more clearly.

Module 4: Tools and Features Involve in a SIEM
This module covers a variety of functions found in a SIEM platform, including threat hunting and correlation, vulnerability management, and asset management. You'll discover that forensic capabilities and automatic reaction are also expected to be included in the next-generation SIEM.

Module 5: SIEM Implementation and Best Practices
This module covers SIEM installation, network log collections, workstation log collections, and other security device log collections, as well as how to secure all log sources' connections to SIEM. You'll learn how to use a variety of lab tasks to help you understand installation, log collection, and integration better. Throughout the lab, you'll learn how to set up Wazuh, Splunk, and other related technologies like MISP, The Hive, and Cortex.

Module 6: SIEM Integration with other SOC Technologies
This module will demonstrate how the SIEM may be configured to work with existing security infrastructure such as firewalls, threat intelligence platforms, and case management for event sharing and response. You'll discover how SIEM may be used in conjunction with Next-Generation Antivirus and EDR to assist reaction to harmful activity.

Module 7: Uses cases from Open Sources and Commercial SIEM Tools
This module explores the usage of Wazuh and Splunk for monitoring of activities across networks and leveraging the cyber kill chain to understand the mindset of the attackers and how it can help infuse the understanding of the role of security analyst within an organization.

Module 8: Next Generation SIEM and SOAR
This module explores the opportunities presented by the next generation SIEM and SOAR (Security Orchestration and Automation Response) to security operations. The student will learn the use of a playbooks leveraging logic app in Azure Sentinel to power up automatic incident response, speeding up the combinations with which a team can respond to incident bringing to play all the necessary security products up in the orchestration.

Prerequisites

- Level test - American test
- Networking fundamentals, including common networking protocols, topologies, hardware, media, routing, switching, and addressing.
- Linux and Windows fundamentals.
- Installation, configuration, and troubleshooting for Windows-based & Linux systems.
- Basic concepts of cybersecurity CIA Triad.
- Basic understanding of scripting and Linux Terminal syntax