Security Analytics 8 Administration

COURSE DESCRIPTION

The Symantec Security Analytics 8 Administration course is designed for participants who want to learn how to use the Symantec Security Analytics platform to perform various types of network-based monitoring and forensic analysis, including incident-response investigation, increased real-time situational awareness, and continuous monitoring for indicators of compromise (IOCs) and advanced persistent threats (APTs).

Delivery Method

Instructor-led and Virtual Academy

Duration

Three days

Course Objectives

By the completion of this course, you will be able to:

- Understand key concepts of network forensics, with a focus on threat hunting and incident response
- Use basic and advanced filtering techniques to assist in reducing response time by narrowing down searches for specific data
- Perform detection of potential security incidents hidden in network traffic through file and artifact extraction
- Improve on incident response through data enrichment and integrated threat intelligence services
- Identify suspicious activity and correlate Indicators of Compromise to an attack vector or specific incident
- Discover how Security Analytics' open API enables integration with existing Symantec and third-party security solutions

Who Should Attend

The Security Analytics 8 Administration course is intended for students who wish to master the core functions of Security Analytics to perform threat hunting and incident response. It is designed for students who have not taken any previous training courses about Security Analytics.

Prerequisites

This course assumes that students have a solid understanding of networking concepts, such as local-area networks (LANs), the Internet, security, and IP protocols.

Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Module 1: Introduction to Security Analytics

- This module will introduce Symantec Security Analytics and why the network visibility that Security Analytics provides is critical in protecting business operations.

Module 2: Introduction to Network Forensics

- This module will introduce computer forensics, with a focus on modern network forensics concepts. It will discuss terminology and common methods and tools used in the SOC today.

Module 3: Threat Hunting and Incident Response

- This module will talk about what present-day cyber-attacks look like and core challenges around discovering resolving these attacks. It will cover how the cyber kill-chain methodology can be used in combination with threat hunting techniques to interrupt on-going attacks. This module will also discuss the fundamentals of incident response, including terminology and core concepts used when performing remediation of discovered security incidents.

Module 4: Improving security posture through effective planning and solution design

- This module addresses the planning and solution-design process for deployments of Security Analytics solutions. It identifies the points within a network where Security Analytics can most effectively capture packet data. It will also cover installation options and basic configuration.

Module 5: Reduce incident response time

- This module will discuss the challenges around lengthy incident response times. It will also cover how filtering can assist in reducing response time by narrowing down searches for specific data. It will also demonstrate, with filtering, that removing excess "noise", especially in very large data sets improves on overall response time. Best practices for filtering and searching will also be covered.

Module 6: Detecting network traffic anomalies

- This module will examine the challenges with detection of potential security incidents hidden in network traffic. It will cover how Security Analytics provides file and artifact extraction from captured packet data. Topics include what artifacts are and how Security Analytics can provide additional context for and processing of any interesting artifacts that may be found. Use cases that demonstrate contextualization benefits for incident responders and security administrators will also be discussed.

Module 7: Improve on early incident detection

- This module will talk about best practices for network-based analysis using Security Analytics. This module will also examine how Security Analytics can identify suspicious activity and correlate Indicators of Compromise to an attack vector or specific incident.

Module 8: Enriching incident response efforts

- This module will address incident response challenges around inadequate information and cover basic and advanced reporting tools within Security Analytics. Improved incident prevention and response from the enhanced information available will be discussed.

Module 9: Enhancing incident response through integrations with other security products

- This module will discuss how Security Analytics' open API enables integration with existing Symantec and third-party security solutions, providing customers with the valuable context and evidence they lack. Threat intelligence integration will also be examined.

Module 10: Review of Security Analytics Administration

- This module will provide a review of topics covered in this course.