SYMANTEC SECURITY ANALYTICS 7.2.x PROFESSIONAL

COURSE DESCRIPTION

The Symantec Security Analytics Professional course is designed for participants who want to learn how to use the Symantec Security Analytics platform to perform virtually any type of network-based monitoring and forensic analysis, including incident-response investigation, real-time situational awareness, and continuous monitoring for indicators of compromise (IOCs) and advanced persistent threats (APTs). This course covers:

- How Security Analysis Works
- File and Artifact Extraction
- Anomaly Detection and Modeling
- Data Enrichment
- Threat Intelligence Services
- Kill Chain Analysis
- Indicators of Compromise (IOCs)
- Malware Integration
- The Virtual Filesystem (VFS)

Delivery Method
Instructor-led and Virtual Academy

Duration
Two-days and is designed to be delivered subsequent to the two-day Symantec Security Analytics Administrator course.

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

- Map high-level operational functions to internal system modules and identify how data flows through the system
- Use reports and extractions to find and analyze relevant data to solve problems
- Use comparisons and advanced display filters to narrow search results
- Import/export PCAPs for forensic analysis and archival functions
- Use actions, alerts, and real-time extractor
- Use the Security Analytics platform for incident-response
- Apply kill-chain analysis to discover and describe indicators of compromise
- Navigate and query the virtual file system

Who Should Attend
IT or network security professionals who want to master the use of Blue Coat Security Analytics and who have completed the Symantec Security Analytics Administrator course.

Prerequisites
Participants should have a sound understanding of the OSI reference model and common networking protocols, and how those protocols make connections, keep state, and transfer data, along with basic experience with network packet and flow analysis, including the use of PCAP files, tcpdump, and Wireshark. Basic to advanced knowledge of best practices for incident response and continuous monitoring will provide a significant advantage.

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