SYMANTEC SECURITY ANALYTICS 7.2.X PROFESSIONAL

DURATION: 2 DAYS

COURSE OVERVIEW

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 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.

TARGET AUDIENCE

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.

COURSE OBJECTIVES

After you complete this course you should be able to:

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

COURSE CONTENT

1. **How Security Analysis Works**
2. **File and Artifact Extraction**

3. **Anomaly Detection and Modeling**
4. **Data Enrichment**
5. **Threat Intelligence Services**
6. **Kill Chain Analysis**
7. **Indicators of Compromise (IOCs)**
8. **Malware Integration**
9. **The Virtual Filesystem (VFS)**

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

1. A sound understanding of the OSI reference model and common networking protocols and how those protocols make connections, keep state and transfer data
2. Basic experience with network packet and flow analysis, including the use of PCAP files, tcp dump, and Wire shark.
3. Basic to advanced knowledge of best practices for incident response and continuous monitoring

TEST CERTIFICATION

Recommended preparation for exam:

250-433 - Administration of Blue Coat Security Analytics 7.2