BLUE COAT CERTIFIED SECURITY ANALYTICS PROFESSIONAL

DURATION: 2 DAYS

COURSE OVERVIEW

The Blue Coat Certified Security Analytics Professional (BCSAP) course designed for participants who want to learn how to use the Blue Coat 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).

TARGET AUDIENCE

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

COURSE OBJECTIVES

After completing this course, you will 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 the Security Analytics platform for incident-response
4. Use comparisons and advanced display filters to narrow search results
5. Apply kill-chain analysis to discover and describe indicators of compromise

COURSE CONTENT

The Blue Coat Certified Security Analytics Professional (BCSAP) course covers:

1. Theory of Operation
2. File Extraction
3. Data Enrichment
4. Threat BLADES
5. Kill Chain Analysis
6. To Look for Indicators of Compromise (IOCs)
7. Integration
8. The Virtual File System (VFS)

COURSE PREREQUISITES

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, tcp dump, and Wireshark. Basic to advanced knowledge of best practices for incident response and continuous monitoring will provide a significant advantage.