SYMANTEC SECURITY ANALYTICS 7.2.X ADMINISTRATOR

DURATION: 2 DAYS

COURSE OVERVIEW

The Symantec Security Analytics Administrator course is intended for IT professionals who want to master the fundamentals of the Symantec Security Analytics solution.

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.

TARGET AUDIENCE

IT network or security professionals who wish to master the fundamentals of Symantec + Blue Coat products with a focus on network security and who may have not taken any previous Symantec and Blue Coat training courses.

COURSE OBJECTIVES

After you complete this course you should be able to:

1. Install, preconfigure, and license new instances of Security Analytics
2. Identify and evaluate reference scenarios and deployment options based on organizational needs, network configurations, and storage capacity
3. Select network locations for data capture and describe the potential implications
4. Explain the options for, limitations of, and differences among the use of taps, mirror/SPAN ports, and virtual infrastructure for capturing packet data
5. Identify the options and requirements for load distribution and the capabilities, benefits, and limitations of load-distributed configurations
6. Identify hardware specifications and requirements for physical appliances and storage modules, including the correct identification of the cabling requirements for connecting storage modules to 2G and 10G appliances
7. Navigate the GUI, identify the main functional areas of the GUI, and understand how tokens in the path bar, time-frame values, and other factors determine the information displayed
8. Create custom dashboards and widgets
9. Use the path bar to filter out noise and narrow your focus on relevant data

COURSE CONTENT

1. **Security Analytics Product Introduction**
2. **Solution Design**
3. **Installation and Setup**
4. **Security Analytics Web-based User Interface**
5. **Reports – What Do They Tell Me?**
6. **Using the Filter Bar**
7. **Using Advanced Filters**
8. **Indicators**
9. **Management, Monitoring, and Maintenance**

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

1. Participants should be familiar with network administration in distributed, enterprise-class LAN/WAN topologies,
2. Basic Unix/Linux administration and have some experience with using proxies, firewalls, routers and switches to implement network security policies.
3. Basic to advanced knowledge of best practices for incident response and continuous monitoring is a plus.

TEST CERTIFICATION

Recommended preparation for exam:

250-433 - Administration of Blue Coat Security Analytics 7.2