Symantec Security Analytics 7.2.x Administrator

Course Summary

Description

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

This course is two days and is designed to be delivered in conjunction with the subsequent two-day Symantec Security Analytics Professional course (PT20255).

Objectives

After taking this course, students will be able to:

- Install, preconfigure, and license new instances of Security Analytics
- Identify and evaluate reference scenarios and deployment options based on organizational needs, network configurations, and storage capacity
- Select network locations for data capture and describe the potential implications
- Explain the options for, limitations of, and differences among the use of taps, mirror/SPAN ports, and virtual infrastructure for capturing packet data
- Identify the options and requirements for load distribution and the capabilities, benefits, and limitations of load-distributed configurations
- 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
- 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
- Create custom dashboards and widgets
- Use the path bar to filter out noise and narrow your focus on relevant data

Topics

- Security Analytics Product Introduction
- Solution Design
- Installation and Setup
- Security Analytics Web-based User Interface
- Reports – What Do They Tell Me?
- Using the Filter Bar
- Using Advanced Filters
- Indicators
- Management, Monitoring, and Maintenance

Audience

This course is designed for 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.

Prerequisites

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

Duration

Two days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically