Certification Program

250-433: Administration of Blue Coat Security Analytics 7.2 Exam

Study Guide v. 1.0

Symantec Study Guide Table of Contents

Recommended Preparation Materials

Recommended Courses and Experience

Instructor Led: https://www.symantec.com/services/education-services/training-courses

- Blue Coat Security Analytics Administrator 7.2
- Blue Coat Security Analytics Professional 7.2
- Recommended 6-9 months of experience working with Symantec Security Analytics 7.2 in a production or lab environment.

Product Documentation Referenced in This Exam

1. Security Analytics Technical Support articles, documentation sets, and alerts including, but not limited to: https://support.symantec.com/en_US/dpl.1145515.html
   o Administration and Management Guide
   o Release Notes
   o Reference Guide
   o Best practices

Symantec™ | Certification Program

Exam Objectives

The following tables list the Symantec SCS Certification exam objectives for the Security Analytics 7.2 exam and how these objectives align to the corresponding Symantec courses and the referenced documentation.

For more information on the Symantec Certification Program, visit http://go.symantec.com/certification

EXAM SECTION 1: Solution Design

Exam Objectives	Topics from *Security Analytics 7.2 Documentation and Courses*
Describe Security Analytics as it pertains to the industry.	• **Course**: Security Analytics Administrator
Describe the features and functionality of Security Analytics.	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide
Describe the Security Analytics architecture including each product's architecture.	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide

EXAM SECTION 2: Installation and Configuration

Exam Objectives	Topics from *Security Analytics 7.2 Documentation and Courses*
Describe how to install and configure Security Analytics	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide

Exam Objectives	Topics from *Security Analytics 7.2 Documentation and Courses*
Determining Appropriate Storage Capacity	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide
Determining how to connect to different network topologies	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide
Describe the difference between physical and virtual appliance	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide

EXAM SECTION 3: Management and Reporting

Exam Objectives	Topics from *Security Analytics 7.2 Documentation and Courses*
Understand the Web Based Interface	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide
Understanding Reports	• **Course**: Security Analytics Administrator • **Documentation**: Security Analytics Administration and Management Guide
Understand and describe Filters and Advanced Filters	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide
Understand and Describe Indicators	• **Course**: Security Analytics Administrator • **Documentation**: o Security Analytics Administration and Management Guide
Understand how to Extract Content	• **Course**: Security Analytics Professional • **Documentation**: o Security Analytics Administration and Management Guide

Exam Objectives	Topics from *Security Analytics 7.2 Documentation and Courses*
Configuring Data Enrichment	• **Course**: Security Analytics Professional • **Documentation**: ○ Security Analytics Administration and Management Guide

EXAM SECTION 4: Advanced Analysis

Exam Objectives	Topics from *Security Analytics 7.2 Documentation and Courses*
Understand the Virtual File System	• **Course**: Security Analytics Professional • **Documentation**: ○ Security Analytics Administration and Management Guide
Identify Indicators of Compromise	• **Course**: Security Analytics Professional • **Documentation**: ○ Security Analytics Administration and Management Guide