

Symantec Data Loss Prevention 15.5: Administration

Course Summary

Description

The Symantec (Broadcom) Data Loss Prevention 15.5: Administration training course is a 5-day instructor-led virtual classroom that includes both lecture and hands-on experience. The hands-on labs include exercises for configuring Enforce server, detection servers, and DLP agents as well as performing policy creation and incident detection, incident response, incident reporting, and user and role administration. Additionally, you are introduced to deployment best practices and the following Symantec Data Loss Prevention products: Network Monitor, Network Prevent, Cloud Service for Email, Network Discover, Network Protect, Cloud Storage, Endpoint Prevent, and Endpoint Discover.

Objectives

At the end of this course, students will be able to configure and use Symantec Data Loss Prevention 15.5.

Topics

- Data Loss Prevention Landscape
- Overview of Symantec Data Loss Prevention
- Identifying and Describing Confidential Data
- Locating Confidential Data Stored on Premises and in the Cloud
- Understanding How Confidential Data is Being Used
- Educating Users to Adopt Data Protection Practices
- Preventing Unauthorized Exposure of Confidential Data
- Remediating Data Loss Incidents and Tracking Risk Reduction
- Enhancing Data Loss Prevention with Integrations
- Course Review

Audience

This training course is intended for attendees who are responsible for configuring and maintain Symantec Data Loss Prevention. Additionally, this course is intended for technical users responsible for creating and maintaining Symantec Data Loss Prevention policies and the incident response structure.

Prerequisites

This Symantec DLP training course assumes that students have a basic understanding of Windows server-class operating systems and commands, as well as networking and network security concepts.

Duration

Five days

Symantec Data Loss Prevention 15.5 Administration

Course Outline

- I. *Data Loss Prevention Landscape*
 - A. Data Loss Prevention landscape
 - B. Data loss risk management
 - C. Data Loss Prevention real-world use cases
- II. *Overview of Symantec Data Loss Prevention*
 - A. Symantec Data Loss Prevention Suite
 - B. Symantec Data Loss Prevention architecture
- III. *Identifying and Describing Confidential Data*
 - A. Identifying confidential data
 - B. Configuring Symantec Data Loss Prevention to recognize confidential data
 - C. Described Content Matching (DCM)
 - D. Exact Data Matching (EDM)
 - E. Indexed Data Matching (IDM)
 - F. Vector Machine Learning (VML)
 - G. Sensitive Image Recognition
 - H. Custom file type detection
- IV. *Locating Confidential Data Stored on Premises and in the Cloud*
 - A. Determining where to search for confidential data
 - B. Locating confidential data on corporate repositories
 - C. Locating confidential data in the Cloud
 - D. Locating confidential data on endpoint computers
- V. *Understanding How Confidential Data is Being Used*
 - A. Monitoring confidential data moving across the network
 - B. Monitoring confidential data being used on endpoint computers
- VI. *Educating Users to Adopt Data Protection Practices*
 - A. Implementing corporate training on data protection policies
 - B. Providing notifications of user policy violations
- VII. *Preventing Unauthorized Exposure of Confidential Data*
 - A. Using response rules to prevent the exposure of confidential data
 - B. Protecting confidential data in motion
 - C. Protecting confidential data in use
 - D. Protecting confidential data at rest
- VIII. *Remediating Data Loss Incidents and Tracking Risk Reduction*
 - A. Reviewing risk management frameworks
 - B. Using incident reporting options to identify and assess risk
 - C. Creating tools that support the organization's risk reduction process
 - D. Communicating risk to stakeholders
 - E. Understanding advanced reporting options and analytics
- IX. *Enhancing Data Loss Prevention with Integrations*
 - A. Symantec DLP integration mechanisms
 - B. Symantec Information Centric Security
 - C. Additional Integrations with Symantec Enterprise Solutions
- X. *Course Review*
 - A. Review of Symantec DLP products and architecture
 - B. Review of the states in a Data Loss Prevention implementation