SYMANTEC DATA LOSS PREVENTION 15.0 ADMINISTRATION

DURATION: 5 DAYS

COURSE OVERVIEW

The Symantec Data Loss Prevention 15.0 Administration course is designed to provide you with the fundamental knowledge to configure and administer the Symantec Data Loss Prevention Enforce platform. 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, Cloud Detection Service, Network Discover, Network Protect, Cloud Storage, Endpoint Prevent, and Endpoint Discover. Note that this course is delivered on a Microsoft Windows platform.

TARGET AUDIENCE

The Symantec Data Loss Prevention Administration course is intended for attendees who are responsible for configuring and maintaining 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

COURSE OBJECTIVES

By the end of this course, you will be able to configure and use Symantec Data Loss Prevention 15.0.

COURSE CONTENT

Module 1:Data Loss Prevention Landscape •

1. Data Loss Prevention landscape •
2. Data loss risk management •
3. Data Loss Prevention real-world use cases

Module 2: Overview of Symantec Data Loss Prevention •

1. Symantec Data Loss Prevention Suite •
2. Symantec Data Loss Prevention architecture

Module 3: Identifying and Describing Confidential Data •

1. Identifying confidential data •

2. Configuring Symantec Data Loss Prevention to recognize confidential data •
3. Described Content Matching (DCM) •
4. Exact Data Matching (EDM)
5. Indexed Document Matching (IDM) •
6. Vector Machine Learning (VML) •
7. Sensitive Image Recognition •
8. Custom file-type detection

Module 4: Locating Confidential Data at Rest •

1. Determining where to search for confidential data •
2. Locating confidential data on corporate repositories •
3. Locating confidential data in the cloud •
4. Locating confidential data on endpoint computers

Module 5: Understanding How Confidential Data is Being Used •

1. Monitoring confidential data moving across the network •
2. Monitoring confidential data being used on endpoint computers

Module 6: Educating End Users to Adopt Data-Protection Practices •

1. Implementing corporate training on data protection policies •
2. Providing notifications of user policy violations

Module 7: Preventing Unauthorized Exposure of Confidential Data •

1. Using response rules to prevent the exposure of confidential data •
2. Protecting confidential data in motion •
3. Protecting confidential data in use •
4. Protecting confidential data at rest

Module 8: Remediating Data Loss Incidents and Tracking Risk Reduction •

1. Reviewing risk management frameworks •
2. Using incident reporting options to identify and assess risk •
3. Creating tools that support the organization's risk reduction process •
4. Communicating risk to stakeholders •
5. Understanding advanced reporting options and analytics

Module 9: Enhancing Data Loss Prevention Through Integrations •

1. Understanding Symantec DLP integration mechanisms
2. Understanding Symantec DLP in the context of Symantec Information Centric Security
3. Understanding additional Symantec DLP integrations with other Symantec solutions

Module 10: Review of Symantec Data Loss Prevention

1. Review of Symantec DLP products and architecture
2. Review of the stages in a Data Loss Prevention implementation