Symantec Data Loss Prevention 16.x Differences

Course Code: 000240

Course Description

The *Symantec Data Loss Prevention 16.0 Differences* course is designed for experienced Data Loss Prevention (DLP) administrators and users who are already familiar with Symantec DLP and want to learn latest the features introduced in Symantec DLP 16.0. The course covers endpoint, detection, storage, reporting, and API features in the 16.0 release. These features include enhanced support for LiveUpdate (for upgrading DLP Agents), the new Linux DLP Agent, thirdparty certificates for Endpoint Servers and DLP Agents, User Risk-Based Detection (powered by an integration with Symantec Information Centric Analytics), Structured

Data Matching, High-Speed File-System Scanning (for Network Discover), and Incident Reporting enhancements.

Delivery Method

Instructor-Led

Duration

Two days

This includes a half-day of instructor lecture and two days of access to a Symantec DLP 16.0 practice environment.

Course Objectives

By the completion of this course, you will be able to:

- Understand Symantec DLP 16.0 endpoint, detection, storage, reporting, and API features
- Understand how to important Symantec DLP 16.0 features such as User Risk-Based Detection, Structured Data Matching, and High-Speed File-System Scanning

Practice Environment

Students in this course are provided access to a Symantec DLP 16.0 practice environment (sandbox) in which to explore and experiment with the latest version of the product.

Prerequisites

- Strong knowledge of Symantec DLP
- Experience using Symantec DLP

Additional Courses Available

- Symantec Data Loss Prevention 16.0 Differences (eLearning)
- Symantec Data Loss Prevention 15.x Administration
- Symantec Data Loss Prevention 15.5 Planning and Implementation
- Symantec Data Loss Prevention 15.5 Policy Authoring and Incident Remediating

Course Outline

Module 1: Symantec DLP 16.0 Endpoint Features

- LiveUpdate Enhancements for DLP Agent Updates
- Linux DLP Agent
- General Endpoint Updates
- Windows DLP Agent Support for Microsoft Information Protection Classification of Microsoft Outlook Emails
- Mac DLP Agent Print Coverage
- Translatable Strings for Endpoint Messages
- Endpoint IPv6 Support
- Custom Certificates for Endpoint Servers and DLP Agents

Module 2: Symantec DLP 16.0 Detection Features

- Improved Data Identifier Engine
- Structured Data Matching
- Boolean Compact Policy (BCP) Tree
- User Risk-Based Detection

Module 3: Symantec DLP 16.0 Storage, Reporting, & API Features

- High-Speed File-System Scans
- Incident List Enhancements
- Incident Masking
- Enforce REST APIs