

Symantec Data Loss Prevention 9.0 Administration

COURSE DESCRIPTION

The Symantec Data Loss Prevention 9.0 Administration course is designed to provide you with the fundamental knowledge and hands-on lab experience to configure and administer the Symantec Data Loss Prevention Enforce platform. The hands-on labs will include exercises for reporting, workflow, and incident response management, policy management and detection, response management, user and role administration, directory integration and filtering. Additionally, the student will be introduced to the following Symantec Data Loss Prevention products: Network Monitor, Network Prevent, Network Discover, Network Protect, Endpoint Prevent and Endpoint Discover as well as deployment best practices. Please note, this course is delivered on a Microsoft Windows platform and does not include installation and initial configuration for each server.

Delivery Method

Instructor-led

Duration

Four days

Course Objectives

This course provides instruction on Symantec Data Loss Prevention 9.0. At the completion of the course, the student will be able to:

- Describe the features, concepts, components, and terminology of Symantec Data Loss Prevention 9.0
- Configure Reports and Remediate Incidents
- Create and Modify Policies and Response Rules
- Leverage Policy and Response Management Best Practices.
- Create and Modify Discover Targets
- Create and Manage Roles and Users
- Carry out System Administration Tasks including Performance Management
- Describe Enterprise Enablement Best Practices
- Perform Diagnostics
- Leverage Deployment Best Practices

Who Should Attend

This course is intended for those responsible for the application configuration, maintenance and troubleshooting of Symantec Data Loss Prevention. Additionally, this course is applicable for the technical users responsible for creating and maintaining Symantec Data Loss Prevention policies and the incident response structure.

Prerequisites

Student should have a working knowledge of windows server-class operating systems and commands, as well as networking and network security concepts.

Hands-On

This course includes practical exercises that enable you to test your new skills and begin to transfer them into your working environment.

COURSE OUTLINE

Introduction to Data Loss Prevention

- Data Loss Prevention overview
- Importance of Data Loss Prevention
- Data Loss Prevention Stakeholders
- Use Cases and Key Customer Case Studies

Introduction to Symantec Data Loss Prevention

- Symantec Data Loss Prevention Overview
- Navigating the User Interface
- **Hands-On Labs:** Become familiar with navigation and tools in the user interface.

Reporting, Incident Remediation and Workflow

- Reporting and Analysis
- Report Navigation, Preferences and Features
- Report Filters
- Report Commands
- Incident Snapshot
- Incident Remediation and Workflow
- **Hands-On Labs:** Create, filter, summarize and distribute reports, remediate incidents, configure a user's reporting preferences.

Policy Management

- Policy Overview
- Using Policy Templates
- Solution Packs
- Building Policies
- **Hands-On Labs:** Use policy templates and policy builder to configure and apply new policies.

Response Rule Management

- Response Rule Overview
- Creating Automated Response Rules
- Creating Smart Response Rules
- Response Rule Best Practices
- **Hands-On Labs:** Create and use automated and smart response rules.



TrueMatch Detection Methods

- Overview of Detection Methods
 - Described Content Matching (DCM)
 - Exact Data Matching (EDM)
 - Directory Group Matching (DGM)
 - Indexed Document Matching (IDM)
- **Hands-On Labs:** Create policies that include DCM, EDM, DGM, and IDM rules (including policies that combine these methods), and then use those policies to capture incidents.

Advanced EDM

- Preparing a data source
- Best Practices for index creation and refresh
- Remote EDM indexing

Policy Best Practices

- Policy Deployment Best Practices
- Policy Lifecycle Best Practices

Network Monitor Review

- Review of Network Monitor
- Protocols
- Traffic Filtering
- Network Monitor Best Practices
- **Hands-On Labs:** Applying IP and L7 Filters.

Introduction to Network Prevent

- Network Prevent Overview
- Introduction to Network Prevent (Email)
- Introduction to Network Prevent (Web)
- Network Prevent Best Practices
- **Hands-On Labs:** Configure Network Prevent (Email) response rules, incorporate them into policies, and use the policies to capture incidents.

Introduction to Network Discover and Protect

- Network Discover and Protect Overview
- Configuring Discover Targets
- Protecting Data
- Running and Managing Scans
- Reports and Remediation
- Network Discover and Protect Best Practices
- **Hands-On Labs:** Create and run a file system target using various response rules, including quarantining.

Introduction to Endpoint Prevent

- Endpoint Prevent Overview
- Detection capabilities at the Endpoint
- Managing agents
- Creating Endpoint Response Rules
- Capturing Endpoint Prevent Incidents and viewing them in reports
- Endpoint Prevent Best Practices
- **Hands-On Labs:** Create Endpoint Response Rules, monitor and block Endpoint actions, and view Endpoint Incidents.

Introduction to Endpoint Discover

- Endpoint Discover Overview
- Creating and running Endpoint Discover targets
- Using Endpoint Discover Reports and Reporting features
- **Hands-On Labs:** Create Endpoint Discover targets, run Endpoint Discover targets and view Endpoint Discover incidents.

Enterprise Enablement

- Preparing for Risk Reduction
- Risk Reduction

System Administration

- Symantec Data Loss Prevention Architecture
- Server Administration
- Operational Management
- Directory Integration
- Troubleshooting
- **Hands-On Labs:** Create attributes (status and custom). Create policy groups. Create users and roles. Interpret event reports and traffic Reports. Configure alerts and directory integration (custom attribute lookups using .csv file).