Symantec Data Loss Prevention 11.5: Administration

COURSE DESCRIPTION

The *Symantec Data Loss Prevention 11.5: 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 reporting, workflow, incident response management, policy management and detection, response management, user and role administration, directory integration, and filtering. Additionally, you are introduced to deployment best practices and the following Symantec Data Loss Prevention products: Network Monitor, Network Prevent, Symantec Data Loss Prevention for Tablets, Network Discover, Network Protect, Endpoint Prevent, and Endpoint Discover. Note that this course is delivered on a Microsoft Windows platform.

Delivery Method
Virtual Academy

Duration
Five days

Course Objectives
By the end of this course, you will be able to configure and use Symantec Data Loss Prevention 11.5.

Who Should Attend
This course is intended for anyone responsible for configuring, maintaining, and troubleshooting 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
You must 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 Symantec Data Loss Prevention
- Symantec Data Loss Prevention overview
- Symantec Data Loss Prevention architecture

Navigation and Reporting
- Navigating the user interface
- Reporting and analysis
- Report navigation, preferences, and features
- Report filters
- Report commands
- Incident snapshot
- **Hands-on labs:** Become familiar with navigation and tools in the user interface. Create, filter, summarize, and distribute reports. Create users, roles, and attributes

Incident Remediation and Workflow
- Incident remediation and workflow
- Managing users and attributes
- Custom attribute lookup
- **Hands-on labs:** Remediate incidents, configure a user's reporting preferences, and custom attribute look-ups using a `.csv` file

Policy Management
- Policy overview
- Creating policy groups
- Using policy templates
- Building policies
- Policy development best practices
- **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

Described Content Matching
- DCM detection methods
- Use cases
- Using DCM in policies
- **Hands-on labs:** Create policies that include DCM and then use those policies to capture incidents

Exact Data Matching and Directory Group Matching
- Exact data matching (EDM)
- Directory group matching (DGM)
- Advanced EDM
- **Hands-on labs:** Create policies that include EDM and DGM, and then use those policies to capture incidents

Indexed Document Matching
- Indexed document matching (IDM)
- Using IDM in policies
- **Hands-on labs:** Create policies that include IDM rules and then use those policies to capture incidents

Vector Machine Learning
- Vector Machine Learning (VML)
- Creating a VML profile

Hands-on labs: Create a VML profile, import document sets, and create a VML policy

Network Monitor Review
- Review of Network Monitor
- Protocols
- Traffic filtering
- Network Monitor best practices
- **Hands-On Labs:** Apply IP and L7 filters

Introduction to Network Prevent
- Network Prevent overview
- Introduction to Network Prevent (Email)
- Introduction to Network Prevent (Web)
- **Hands-On Labs:** Configure Network Prevent (E-mail) response rules, incorporate them into policies, and use the policies to capture incidents

Introduction to Symantec Data Loss Prevention for Tablets
- Overview
- Installation and configuration
- MDM configuration and integration
- VPN configuration
- Policy and response rule configuration
- Reporting and remediation
- Logging and troubleshooting
- **Demonstration:** Configure Tablet Prevent response rules, incorporate them into policies, and use the policies to capture incidents

Introduction to Network Discover and Network Protect
- Network Discover and Network Protect overview
- Configuring Discover targets
- Protecting data
- FlexResponse platform
- Running and managing scans
- Reports and remediation
- Network Discover and Network 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
- Configuring Endpoint Prevent
- Detection capabilities at the Endpoint
- 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

Managing DLP Agents
- Managing agents
- **Hands-on labs:** Use the Enforce console to manage DLP Agents

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
- DLP Maturity model

System Administration
- Server administration
- Language support
- Credential management
- Troubleshooting
- Diagnostic tools
- Troubleshooting scenario
- Getting support
- **Hands-on labs:** Interpret event reports and traffic reports, configure alerts, and use the Log Collection and Configuration tool

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Specifications and product offerings are subject to change without notice.