Symantec Data Loss Prevention 15.5 Policy Authoring and Incident Remediation

COURSE DESCRIPTION

The *Symantec Data Loss Prevention 15.5 Policy Authoring and Incident Remediation* course is intended for DLP policy authors and incident remediators who need to understand how to create, maintain, and refine DLP policies and how to create effective incident remediation workflows to drive toward their organization's data-loss risk reduction goals. The hands-on labs include exercises for authoring policies (detection rules and response rules) and performing incident detection, incident response, and incident reporting. The course assumes that Symantec Data Loss Prevention (DLP) is already implemented in the organization's environment and is configured to cover the relevant vectors for the organization: Data in Motion, Data at Rest, and Data in Use, whether on-premises or in the cloud. For this reason, the course does not cover how to implement, maintain, or troubleshoot the servers and cloud components of the DLP product suite, or the technical configuration of individual DLP products beyond policy authoring and incident remediation.

Delivery Method
Instructor-led

Duration
Two days

Course Objectives
By the end of this course, you will be able to create policies and track and remediate incidents in Symantec Data Loss Prevention 15.5.

Who Should Attend
This course is intended for anyone responsible for creating and maintaining Symantec Data Loss Prevention policies (consisting of detection and response rules) and/or for tracking and remediating incidents.

Prerequisites
You should have a general understanding of the channels that are covered in your Symantec Data Loss Prevention implementation as well as a good idea of the types of confidential data your organization wants to protect.

Hands-On
This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Lesson 1: Setting Risk Reduction Goals for Your Data Loss Prevention Program

- Understanding data-loss risk reduction frameworks
- Understanding Symantec Data Loss Prevention coverage
- Identifying confidential data
- Setting initial risk-reduction goals
- Understanding the feedback loop between policies and incidents

Lesson 2: Identifying and Describing Confidential Data in Your Data-Loss-Prevention Policies

- Configuring Symantec Data Loss Prevention to recognize confidential data
- Described Content Matching (DCM)
- Exact Data Matching (EDM)
- Indexed Document Matching (IDM)
- Vector Machine Learning (VML)
- Sensitive Image Recognition
- Custom file type detection
- Advanced policy tips
- **Hands-On Labs**: Create policy groups, configure a policy for Personally Identifiable Information (PII) detection, configure a policy for PCI compliance, configure a policy to protect confidential documents, configure a policy to protect source code, configure a policy for Form Recognition, use a template to add a DLP policy, export policies for use at a Disaster Recovery (DR) site, configure Optical Character Recognition (OCR)

Lesson 3: Protecting Confidential Data using your Data-Loss-Prevention Policies

- Using response rules in DLP policies to protect confidential data
- Educating Users to adopt data protection practices
- Protecting confidential data in motion
- Protecting confidential data in use
- Protecting confidential data at rest
- **Hands-On Labs**: Configure the Active Directory lookup plugin, configure email notifications, configure onscreen notifications, configure SMTP blocking, test Optical Character Recognition (OCR) and the "HIPAA and HITECH (including PHI)" policy, configure endpoint blocking, configure endpoint User Cancel, scan and quarantine files on a server file share target, scan and quarantine files on an endpoint target

Lesson 4: Remediating Data Loss Incidents and Tracking Risk Reduction

- Using incident reporting options to identify and assess risk
- Creating tools that support the organization's risk reduction process
- Communicating risk to stakeholders
- Understanding advanced reporting options and analytics
- **Hands-On Labs**: Configure roles and users, use reports to track risk exposure and reduction, define incident statuses and status groups, configure and use Smart Responses, schedule and send reports

Lesson 5: Course Review

- Review of Symantec DLP policy authoring
- Review of Symantec DLP incident remediation