Enterprise Computing Solutions - Education Services

OFERTA FORMATIVA

Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: formacion.ecs.es@arrow.com
Phone: +34 91 761 21 51

Symantec Data Loss Prevention 15.5 Administration

CÓDIGO:	DURACIÓN:	Precio:
SYM_00033628	40 Hours (5 días)	A consultar

Description

The *Symantec Data Loss Prevention 15.5 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 the Enforce server, detection servers, and DLP agents; creating policies; detecting and responding to incidents; performing incident reporting; and administering users and roles. You are introduced to the following Symantec Data Loss Prevention products: Network Monitor, Network Prevent, Network Discover, Network Protect, Cloud Storage Discover, Cloud Service for Email, Endpoint Prevent, and Endpoint Discover.
Note:
This course is delivered on a Microsoft Windows platform.

Objetivos

By the end of this course, you will be able to configure and use Symantec Data Loss Prevention 15.5.

Requisitos Previos

- Working knowledge of Windows server-class operating systems and commands
- Networking and Network Security concepts
- Technical users responsible for creating and maintaining policies and incident responses

Programa

Module 1: Data Loss Prevention Landscape

- Data Loss Prevention landscape
- Data loss risk management
- Data Loss Prevention real-world use cases

Module 2: Overview of Symantec Data Loss Prevention

- Symantec Data Loss Prevention Suite
- Symantec Data Loss Prevention architecture

Module 3: Identifying and Describing Confidential Data

- Identifying confidential data
- Configuring Symantec Data Loss Prevention to recognize confidential data
- Described Content Matching (DCM)
- Exact matching (EDM and EMDI)
- Indexed Document Matching (IDM)
- Vector Machine Learning (VML)
- Sensitive Image Recognition
- Custom file type detection
- Hands-On Labs: Tour the Enforce console, create policy groups, configure policies 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)

Module 4: Locating Confidential Data Stored on Premises and in the Cloud

- Determining where to search for confidential data
- Locating confidential data on corporate repositories
- Locating confidential data in the Cloud
- Locating confidential data on endpoint computers
- Hands-On Labs: Run a Content Enumeration Scan, scan a Windows target, scan endpoint computers for confidential data, scan a server for confidential data using Exact Match Data Identifiers (EMDI), configure a global policy for PII compliance

Module 5: Understanding How Confidential Data is Being Used

- Monitoring confidential data moving across the network
- Monitoring confidential data being used on endpoint computers
- Hands-On Labs: Configure Network Prevent for Email to monitor SMTP messages, use Network Prevent for Email to monitor SMTP messages, monitor Endpoint activity

Module 6: Educating Users to Adopt Data Protection Practices

- Implementing corporate training on data protection policies
- Providing notifications of user policy violations
- Hands-On Labs: Configure the Active Directory lookup plugin, configure email notifications, configure onscreen notifications

Module 7: Preventing Unauthorized

- Exposure of Confidential Data
- Using response rules to prevent the exposure of confidential data
- Protecting confidential data in motion
- Protecting confidential data in use
- Protecting confidential data at rest
- Hands-On Labs: 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

Module 8: Remediating Data Loss Incidents and Tracking Risk Reduction

- Reviewing risk management frameworks
- 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

Module 9: Enhancing Data Loss Prevention with Integrations

- Symantec DLP integration mechanisms
- Symantec Information Centric Security
- Additional integrations with Symantec Enterprise solutions
- Hands-On Labs: Create the views schema and user, run the incident data view setup script, verify incident data views creation, use incident data views, create an ICT tag policy for file discovery, scan for file tags using Network Discover

Module 10: Course Review

- Review of Symantec Data Loss products and architecture
- Review of the stages in a Data Loss Prevention implementation

Follow on courses

- Symantec Data Loss Prevention 15.5 Planning and Implementation
- Symantec Data Loss Prevention 15.5 Policy Authoring and Incident Remediation

Examen y certificación

250-533: Administration of Symantec Data Loss Prevention 15.5

Más información

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.

Fechas Programadas

A petición. Gracias por contactarnos.

Información Adicional

Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.