

# **Enterprise Computing Solutions - Education Services**

# **TRAINING OFFERING**

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com

Phone: 0870 251 1000



# **Symantec Data Loss Prevention 16.x Administration**

CODE: LENGTH: PRICE:

SYM 000236 40 Hours (5 days) £3,375.00

# **Description**

The Symantec Data Loss Prevention 16.x 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 components: Network Monitor, Network Prevent, Network Discover, Network Protect, Endpoint Prevent, and Endpoint Discover. In addition, the course includes some introductory discussion of the integration with Symantec CloudSOC CASB.

NOTE: This course is delivered on a Microsoft Windows platform.

#### 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.

# **Objectives**

By the end of this course, you will be able to configure and use Symantec Data Loss Prevention 16.x.

# **Prerequisites**

- 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

#### **Programme**

# Module 1: Data Loss Prevention Landscape

- Data loss risk management
- Data Loss Prevention landscape
- Data Loss Prevention 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)
- User Risk-Based Detection
- Exact matching (EDM and EMDI)
- Indexed Document Matching (IDM)
- Vector Machine Learning (VML)
- Sensitive Image Recognition
- Custom file type detection
- Using policy templates
- 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, run a high-speed Discover scan, scan a Windows target, scan endpoint computers for confidential data

# Module 5: Understanding How Confidential Data is Being Used

- Monitoring confidential data moving across the network
- Monitoring confidential data being used in the Cloud
- Monitoring confidential data being used on endpoint computers
- Hands-On Labs: Update the DLP Agent using
- LiveUpdate, 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, create custom attributes, 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: Define incident statuses and status groups, configure Smart Responses, configure roles and users, reassign users' default roles, create work queues, test workflow, use reports to track risk exposure and reduction

# Module 9: Enhancing Data Loss Prevention with Integrations

- Symantec DLP integration mechanisms
- Symantec DLP integrations with other Symantec products
- Symantec DLP + Microsoft Purview Information Protection (MPIP)
- Hands-On Labs: Use the incident "flag for deletion" function, create a Web report, schedule and send reports

#### Module 10: Course Review

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

#### **Session Dates**

On request. Please Contact Us

# **Additional Information**

This training is also available as onsite training. Please contact us to find out more.