FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Forcepoint Data Loss Prevention (DLP)

CERTIFIED ADMINISTRATOR VIRTUAL INSTRUCTOR LED COURSE

COURSE DATASHEET

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Forcepoint Data Loss Prevention

COURSE OVERVIEW

In this virtual instructor led training course, you will learn how to test an existing deployment, how to administer policies and reports, handle incidents and endpoints, upgrade and manage the Forcepoint DLP system. You will develop skills in creating data policies, building custom classifiers and using predefined policies, incident management, reporting, and system maintenance.

AUDIENCE

- System administrators, Data security administrators, IT staff
- Sales Engineers, consultants, implementation specialists
- Forcepoint Channel Partners

COURSE OBJECTIVES

- Articulate the overall architecture, components, and processing order of data security transactions
- Use the DLP solution to support your organization's security policies and intercept necessary channels
- Understand the required and add-on components
- Implement the initial setup of a Forcepoint DLP deployment
- Configure DLP policies with appropriate action plans to match enterprise Data Security requirements
- Configure and understand reporting and logging
- Configure sustainable settings to store DLP related partitions, forensics and backups
- Ensure high availability of a DLP system and perform upgrades

Format:

Virtual Instructor Led*

Duration:

16 hours total - 4 sessions, 4 hours per session – plus 30-60 minutes of homework each session

Price:

$1,200 USD non-discountable

PREREQUISITES FOR ATTENDANCE

- General understanding of system administration and Internet services.
- Basic knowledge of networking and computer security concepts.
- A computer that meets the requirements noted at the end of this document.

CERTIFICATION EXAMS

This course prepares you to take and pass the Certified Forcepoint DLP Administrator Exam. The exam is included in the price of the course but the execution of the exam is not accomplished during the course. A minimum score of 80% on the multiple choice online exam is required to obtain certification.

COURSE OBJECTIVES

SESSION 1 - ARCHITECTURE

Module 1: DLP Introduction

- Articulate the key features and functions of Forcepoint DLP
- Know how to approach DLP solutions based on your organizations security policies
- Convey what new features are included in version 8.5
- Articulate the differences between the 3 kinds of channels; Data-in-Use, Data-in-Motion, Data-at-Rest
- Understand and set up the virtual training environment
- Perform testing with artificial traffic

Module 2: DLP Deployments

- Understand deployment patterns, topologies, plain and encrypted HTTP, plain and encrypted SMTP
- Articulate the overall architecture, components, and processing order of a data security transaction
- Know how to handle encrypted traffic
- Integrate network boxes and DLP software with existing networks
- Trace the data transactions as they are processed by the DLP components: Policy Engine Interface, Load Balancer, Policy Engine, Text Extractor, Resource Resolver, Submitting incidents to the DLP Manager.

SESSION 2 - POLICIES

Module 3: Policies

- Gain the ability to plan, implement and test DLP policies
- Describe types of DLP policies, rules and classifiers
- Create predefined and custom policies
- Edit and tune predefined policies
- Configure classifiers using key phrases and dictionaries
- Understand and use Regex classifiers
- Describe how custom logic works for nested transactions

Module 4: File Classifiers and Scripts

- Recognize file classifiers by Type, Size, and Name
- Tune predefined script classifiers, use them in DLP rules, distinguish various ways to detect credit card numbers and similar IDs depending on checksums, prefixes and support terms
- Generate a cumulative policy rule to distinguish matches, transactions and incidents
- Produce incident reporting for cumulative rules
- Create user-specific DLP rules, limit source and destination scope, create exceptions

SESSION 3 - ENDPOINTS

Module 5: Fingerprinting and Machine Learning

- Recognize the role of crawlers and how they operate
- Run OCR Server on crawler machines to extract text from images
- Describe the custom and structured fingerprinting components and subcategories
- Configure file fingerprinting tasks; understand how copy-pasting is being detected
- Configure database fingerprinting tasks to protect data records from leaks
- Understand the difference between Machine learning and Fingerprinting

Module 6: Data Endpoint

- Understand the initial setup of a Data Endpoint package (and how it is related to Web Endpoint)
- Create and deploy an Endpoint package on the selected platform
- Configure Endpoint policies to control Endpoint HTTP/HTTPS channel using browser extensions
- Configure Endpoint policies to control applications (including browsers) using hooking DLL
- Understand the incident flow for Endpoint Agents and Endpoint Servers
- Articulate best practices to do Data Endpoint deployment and upgrade
- Configure app exclusion lists and global properties for Endpoint
- Create action plans including Endpoint-specific actions (confirm and encrypt)

SESSION 4 - Incidents and Reports

Module 7: Discovery and Clouds

- Articulate the business need for the Discovery feature
- Create and configure network Discovery policies and tasks
- Create and configure endpoint Discovery policies and tasks
- Distinguish between the various Discovery policy templates
- Configure the crawler jobs and run troubleshooting, if they crash
- Understand the cloud-related discovery

Module 8: Incidents and Reports

- Understand how action plans and remediation scripts tie into Discovery
- Articulate and manage incident workflows using force-release and action-link feature
- Perform an escalation and other actions on an incident
- Execute bulk updates to DLP policies
- Configure limitations for DLP administrators
- Integrate and configure SIEM integration (syslog messages to ArcSight, QRadar, Splunk, etc.)
- Schedule and run incident reports, configure emailing them to the recipients

Module 9: Forcepoint DLP Maintenance

- Configure reliable storage and backups of accumulated data to be able to restore functions
- Use the sizing guide to decide about the DLP Manager hardware, the crawlers and EP Servers
- Understand how to bring the number of incidents to a manageable level
- Perform partition configuration in the database, store partitions, forensics and backups properly
- Configure alerts to provide system health and use dashboards
- List the main steps in the upgrade process of DLP deployment to the v8.5, understand the related incident data migration.

**To attend this web based course, you must have a computer with:*
- *A high-speed internet connection*
- *An up to date web browser*
- *Adobe Flash web browser plug in*
- *PDF Viewer*
- *Speakers and microphone or headset*

A separate tablet or eBook reader is also recommended for the course and lab book delivery. Test your connection to an Adobe Connect virtual class environment here.

TERMS AND CONDITIONS

- Virtual Instructor Led Trainings (VILT's) are delivered as live instructor led training - No onsite delivery element
- VILT's are limited and may not address all of your unique requirements
- The training services in this course are provided pursuant to the Subscription Agreement
- Forcepoint provides the training "AS IS" and makes no warranties of any kind, express or implied
- VILT's courses must be completed within 6 months from purchase or the course is forfeited
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions
- Forcepoint trainings are standard and non-negotiable

For more information about other Forcepoint training offerings, please visit our Customer or Partner training page.

Questions about Forcepoint training? Contact Forcepoint Technical Readiness and Training at salestraining@forcepoint.com