Forcepoint Data Loss Prevention (DLP)

CERTIFIED SYSTEM ENGINEER INSTRUCTOR LED COURSE

FORCEPOINT

Forcepoint DLP System Engineer Course

COURSE OVERVIEW

During this 5-day hands-on instructor led course, you will gain an understanding of the key core competencies and skills needed to practice as a System Engineer handling Forcepoint Data Loss Prevention. The core competencies are design, deployment, integration, maintenance, and troubleshooting.

This course prepares engineers or other professionals who are about to manage or lead system engineering development of Forcepoint Data Loss Prevention from concept creation to production.

AUDIENCE

- System Engineers, Administrators, and IT professionals assisting with DLP deployment, configuration, and administration
- Consultants, system architects, integrators and planners who help customers with Forcepoint DLP implementations
- Sales Engineers, Implementation Specialists, Deployment Specialists, Network Architects, Professional Services, Technical Support

COURSE OBJECTIVES

- Given a set of environmental, acceptable usage, and user requirements, deploy and configure Forcepoint DLP in various enterprise environments
- Explain the interaction processes between DLP components
- Explain the methods used for evaluating necessary sizing of DLP
- Perform advanced configuration of custom classifiers, predefined classifiers, rules and policies
- Formulate policies leveraging predefined classifiers for regulatory compliance, the prevention of IP loss, and data theft
- Build, configure, and deploy DLP Endpoint
- Configure and enable cloud-based integrations with DLP, including online services and Forcepoint CASB
- Explain integration of DLP with RMS and file tagging software
- Indicate primary log files used to review component function, and itemize useful topics to debug
- Compile and analyse incident reporting data
- Compare and configure multiple incident workflows
- Perform maintenance activities on Forcepoint DLP, including automated and manual upgrade, failover, backup, and restore

PREREQUISITES FOR ATTENDANCE

- Certification on the Forcepoint DLP Administrator Course.
- Intermediate 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 System Engineer Exam. The exam is included in the price of the course. Both a hands-on practical exam and a 48-question multiple-choice exam will be administered on the final day of the course. A minimum score of 80% on the multiple-choice online exam is required to obtain certification.

Format:

Instructor Led In-person

Duration:

40 hours total - 5 days, 8 hours per day – plus 30-60 minutes of homework each session

Price:

$7,000 USD non-discountable

Language:

English

COURSE DAILY AGENDA

SESSION 1

Module 1: Components and Initial Setup

- Provide an organized list of available resources for support when working with Forcepoint DLP
- Classify the basic methodologies for Forcepoint DLP deployment depending on the scale (Single Datacenter or Multiple Datacenter).
- Identify software components (PEI, PE, Crawler, OCR, EP Servers, EP Agents) and hardware components used by Forcepoint DLP
- Itemize and explain the software components and database locations used in Forcepoint Security Manager infrastructure
- Install and configure Forcepoint Security Manager, Forcepoint DLP, Analytics Engine, Web Content Gateway, and Email Security Gateway

Module 2: DLP Architecture

- Diagram and explain the internal architecture used by Policy Engine, Data Batch Server, and Message Broker, as well as Security Manager and each DLP System Module (WCG, ESG, DSS Server, Protector)
- Follow the flow of transaction processing during Policy Engine analysis
- Document possible options for deployment patterns, including web and email traffic monitoring
- Formulate sizing requirements for DLP Deployments, based on environment and user demands
- Configure and demonstrate Policy Engine load balancing features
- Generate artificial traffic using regression testing tools (PolicyEngineClient.exe, ContentExtractorClient.exe)

SESSION 2

Module 3: Integrations and Advanced Deployment

- Explain basic configuration and troubleshooting for a DLP Protector
- Explain basic configuration and troubleshooting for a DLP Mobile Agent
- Identify upgrade requirements and procedures for upgrading a Protector or Mobile Agent
- Explain basic configuration and troubleshooting for LDAP import and ResourceResolver
- Identify basic requirements and functions when integrating DLP with Web Security, including DLP only Content Gateway
- Analyze methods of integrating DLP with Email Security, including leveraging Email Security action plans in DLP and configuring Email Gateway for Office 365
- Explain basic configuration and troubleshooting for the Analytics Engine
- Identify the elements of the Incident Risk Ranking interface elements in Forcepoint Security manager, and explain their functions
- Configure and test email encryption using Forcepoint Secure Messaging (Park and Pull)
- Modify a Protector deployment to pair with a Web Content Gateway in ICAP mode
- Install, configure, and test Squid on a Protector
- Enable the Web Security Linking Service, Import URL Categories, and test Geolocation Lookup on Web DLP Policies
- Configure an Email Encryption action plan and leverage it in a DLP Policy. Test functionality using a 3rd party MTA
- Configure a DLP Policy that monitors and enforces against inbound mail. Perform remediation on incidents created by this policy

Module 4: Troubleshooting and Debugging

- Compare methodologies for diagnosing and resolving potential issues occurring in Forcepoint DLP
- Discuss and analyze DLP Troubleshooting use cases
- Document log and debug topic structure used in Policy Engine debugging
- Document log and debug topic structure used for DLP system modules (Security Manager, Protector, Content Gateways, Analytics Engine)
- Enable debugging of Tomcat logs on Forcepoint Security Manager
- Enable debugging of Policy Engine logs on an appliance (Email Security Gateway), and use debug information to track live transactions as they are submitted

SESSION 3

Module 5: Policies, Rules, and Classifiers

- Define an Acceptable Use Policy as a preface to configuring Policies and Rules
- Identify and define the three categories of DLP Policies
- Analyze Boolean Logic as used in DLP Policies, and formulate examples, including an “off switch” argument
- Explain how DLP interacts with Microsoft RMS using protected file classifiers
- Analyze the uses of and compare the inherent accuracy of the different types of classifiers DLP uses (Key Phrases, Dictionaries, Regular Expressions, Scripts, File Properties, Machine Learning, Fingerprinting)
- Document the syntax used, and analyze basic use cases for Regular Expression classifiers
- Explain what the different components of Script (a.k.a. predefined) classifiers, and how Natural Language Processing functions
- Analyze use cases involving configurable Script Classifiers, including the Email to Competitors classifier
- Define exceptions to DLP policies using LDAP search expressions
- Given an example of an Acceptable Use Policy, create a .bat file to automate regression testing using PolicyEngineClient
- Explain, configure, and test the different components of the Customizable IDs Classifier
- Perform stress testing on DLP Email policies using an SMTP “Black Hole”

Module 6: Discovery and Cloud

- Define the potential resources we can scan using Forcepoint DLP Discovery
- Explain the methods used to assist Crawlers when dealing with very large discovery tasks
- Manually administrate Discovery jobs using WorkSchedulerWebServiceClient
- Explain configuration of Discovery tasks against cloud services (Sharepoint Online, Exchange Online, Office365, Box.com)
- Differentiate between the three types of Remediation Scripts and explain how to use Discovery Remediation Scripts using .bat files
- Explain the basic functionality of Classifier Administration software (Boldon James) and how DLP integrates with those classifiers, including reading and writing document tags, as well as updates to the reporting interface.
- Explain basic configuration for deploying a DLP Email Gateway in the cloud using Microsoft Azure
- Explain basic configuration for integrating Forcepoint DLP with Forcepoint CASB, including adding 'Cloud Services' as destinations for DLP Policies
- Configure and run a Network Discovery task using a Crawler, and configure load balancing for the Crawler
- Manually delete a Discovery task using WorkSchedulerWebServiceClient
- Configure and run a Database Discovery task against Oracle Enterprise
- Create and run an Incident Management Remediation Script
- Create a Policy Remediation Script, add it to an action plan, and test functionality
- Create an Endpoint Remediation Script, add it to an action plan, and test functionality
- Install a trial version of Boldon James Office Classifier, and experiment with DLP interaction using hierarchical content tags

SESSION 4

Module 7: Fingerprinting, Machine Learning, and OCR

- Document and analyze the implications of the N-gram (5-word sliding window) fingerprinting algorithm
- List and explain best practices when performing both file and database fingerprinting, including the use of validation scripts
- Explain the functionality of Machine Learning versus Fingerprinting, and differentiate PreciseID from the Support Vector Machine (SVM) algorithm
- Diagram and explain Workscheduler (Crawler) architecture, functionality, and debugging
- Explain how Fingerprint tasks may be recorded and replayed for troubleshooting purposes
- Document the architecture and explain the functionality of OCR
- Analyze methods for troubleshooting OCR, including log file locations, best topics to debug, and manual testing using OCRClient
- Create a File Fingerprint Classifier, configure it in a policy, and run multiple tests differentiated using an Ignored Section classifier
- Perform Database Fingerprinting on an imported .csv file, configure the classifier in a policy, and test functionality
- Prepare training sets for a Machine Learning classifier, create the classifier and fine tune accuracy, then evaluate success using an automated test script (.bat file with PolicyEngineClient)
- Install a DSS Server with an OCR component, then test OCR using both external email traffic and manually generated traffic using OCRClient

Module 8: Forcepoint DLP Endpoint

- Diagram and analyze endpoint server architecture
- Diagram and analyze endpoint agent architecture, including log file locations and debugging
- Explain and demonstrate Endpoint command line functionality (WDEUtil)
- Document web browser integration using Browser Extensions, and explain troubleshooting methods with use cases
- Differentiate between Unhooked and Trusted Endpoint applications
- Explain how to use Tasklist from the command line to thoroughly Unhook and application and all related .dll files
- Explain how serial numbers may be used to identify removable media for use in DLP Policies
- Deploy Endpoints manually, using SCCM or GPO
- Review installation procedure and explain how to configure and use DLP Endpoint on XenApp and XenDesktop
- Build and install a DLP Endpoint package, then test Temporary Bypass function
- Configure and deploy a custom message file for custom Endpoint alerts as part of an Endpoint package
- Install an Endpoint in Stealth Mode
- Debug an Endpoint agent and perform log analysis
- Use Tasklist to completely unhook an application and all .dll files, then test to confirm success
- Create an Endpoint encryption action plan and test using emulated USB Removable Media, then attempt decryption using Forcepoint Decryption Utility

SESSION 5

Module 9: Incident Management, Reporting, and Maintenance

- Explain syslog configuration and integration with a syslog server (Splunk)
- List the types of configurable DLP Alerts
- Explain and demonstrate advanced functions of system health dashboard and system, traffic, and audit logs
- Explain the functions of the User Risk Report
- Demonstrate pulling various data points manually from SQL (wbsn-data-security)
- Explain and demonstrate what permissions can be limited for delegated admins and the effects in Forcepoint Security Manager
- Perform each possible workflow in Incident Management
- Configure and test the DLP Force Release feature
- Configure and test Incident Notifications with Action Links (Email Based Incident Workflow)
- Perform a manual incident dump from SQL using .bat files
- Schedule and run a Backup task, while manually modifying the backup .vbs script, and performing a manual backup of the Fingerprint Repository
- Configure and test DLP Alerts for various system health related events

TERMS AND CONDITIONS

- System Engineer trainings 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 System Engineer course “AS IS” and makes no warranties of any kind, express or implied
- You must register for the System Engineer course offering within 90 days of the Order or the course is forfeited
- System Engineer 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

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