Forcepoint DLP System Engineer Instructor-Led Training

Datasheet

September 2020

Forcepoint

forcepoint.com

Forcepoint Data Loss Prevention (DLP) System Engineer Instructor-Led Training

DTIMP

During this five-day hands-on instructor led course, you will create and test a Forcepoint DLP deployment, perform in-depth analysis of DLP component architecture, integrate Forcepoint DLP with local and cloud based products, build policies, leverage configurable script classifiers, create and fine tune fingerprint and machine learning classifiers, configure discovery tasks to crawl files and databases, build, install, and manage DLP endpoints, use data endpoints for application control, encryption and discovery, manage incident data through security manager as well as through SQL, and perform maintenance tasks, such as dealing with failovers, upgrades and troubleshooting of all of the above, including advanced debugging of DLP logs.

Audience

- System engineers, high level system administrators, IT staff
- Consultants, system architects
- Sales engineers, implementation specialists, deployment specialists
- Network architects, professional services, and technical support

Course objectives

- Deploy and configure Forcepoint DLP components.
- Describe the DLP architecture.
- Perform advanced integration and deployment.
- Explain the methodology used for troubleshooting the DLP product.
- Analyze policies, rules, and classifiers.
- Examine the use of file fingerprinting, machine learning, OCR, and pre-defined policies.
- Configure and deploy DLP endpoint.
- Configure and enable cloud-based integrations with DLP.
- Configure and manage incidents, alerts, and reporting.

Format:

Instructor-led in-person

Duration:

40 hours, typically delivered in 5 sessions (8 hours per session), including exam time

Exam Price:

One attempt is included

Prerequisites for attendance

- Completion of the Forcepoint DLP Administrator Course and certification
- 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% is required to obtain certification.

Course Outline

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 (policy engine interface, PE, crawler, OCR, endpoint servers,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 batchsServer, and message broker, as well as security manager and each DLP system module (WCG, ESG, DSS server, protector).
- 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).

Module 3: Integration 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.
- 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.
- Enable the web security linkings service, import URL categories, and test geolocation lookup on web DLP policies.

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.

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 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.
- Explain, configure, and test the different components of the customizable IDs classifier.

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, Office 365, Box.com).
- Differentiate between the three types of remediation scripts and explain how to use discovery remediation scripts using .bat files.
- 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.
- Configure and run a network discovery task using a crawler, and configure load balancing for the crawler.
- Run an incident management remediation script.

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.

- 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.
- Debug 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.

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 performing a manual backup of the fingerprint repository.
- Configure and test DLP alerts for various system health related events.

Terms and Conditions

- This course is limited to the topics described in this data sheet and may not address all of your unique requirements.
- Forcepoint trainings are standard and non-negotiable.
- Forcepoint provides the training “AS IS” and makes no warranties of any kind, express or implied.
- ILT courses must be completed within six months from purchase or the course may be forfeited.
- The training services in this course are provided pursuant to the Subscription Agreement.
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions.

For more information about this course or other Forcepoint training offerings, please visit https://www.forcepoint.com/services/training-and-technical-certification or contact Forcepoint Technical Learning Services at learn@forcepoint.com.

Forcepoint