Forcepoint DLP System Engineer Instructor-Led

Datasheet

May 2022

Forcepoint

forcepoint.com

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

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 other products, build policies, and leverage configurable script classifiers. Using the knowledge you have gained from the Forcepoint DLP Administrator course, you will create and fine tune fingerprint and machine learning classifiers; configure discovery tasks to crawl files and databases; build, install, and manage DLP endpoints; and use data endpoints for application control, encryption, and discovery. You will perform advanced incident data management and maintenance tasks through Security Manager, such as dealing with failovers, upgrades and troubleshooting, including advanced debugging of DLP logs.

Audience

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

Format:

Instructor-led

Duration:

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

Course Price:

$3500 USD

Exam Price:

One attempt is included

Course objectives

- Summarize the history of Forcepoint DLP.
- Identify the primary Forcepoint DLP components.
- Describe the Forcepoint DLP installation process.
- Configure the DLP base environment.
- Install the Analytics Engine to enable data analysis.
- Install Protector for web scanning.
- Describe DLP Policy Engine architecture and event lifecycle.
- Summarize the DLP Policy structure and test a DLP policy.
- Describe the Analytics Engine architecture
- Explain and test incident data flow.
- Describe the benefits of deploying a Supplemental Server.
- Install and configure a Supplemental Server.
- Create and test Fingerprinting and Machine Learning.
- Install F1E to protect your sensitive data.
- Test F1E anti-tampering and temporary bypass functions.
- Identify Endpoint log files.
- Trace Endpoint agent issues.
- Exclude applications from DLP Endpoint.
- Debug F1E using log files.
- Create and run a Network Discovery task and an Endpoint Discovery task.
- Run DLP reports.
- Configure DLP roles.
- Generate Discovery reports and troubleshoot the crawler.
- Identify and run remediation scripts.
- Describe the DLP component update process.
- Describe automatic DLP component synchronization.
- Configure backup and restore procedures.
- Use the upgrade validation tool and upgrade DLP.
- Describe the infrastructure database.

- Investigate Policy Engine timeouts.

Prerequisites for attendance

- Completion of the Forcepoint DLP Administrator Course and certification
- Intermediate knowledge of networking and computer security concepts

Certification exams

This course prepares you for 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 40-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: The Evolution of Forcepoint DLP

- Data security story
- Forcepoint story

Module 2: Installing Forcepoint DLP

- Identifying the primary Forcepoint DLP components
- Preparing for installation
- Installing Forcepoint Security Manager
- Configuring DLP base environment
- Configuring Protector for email scanning
- Performing initial testing of DLP

Module 3: Installing Additional DLP Components

- DLP module review
- Installing Analytics Engine
- Installing Protector for web

Module 4: DLP Policy Engine

- Describing Policy Engine architecture and event life cycle
- Summarizing DLP policy structure
- Testing Policy Engine

Module 5: Analyzing data

- Describing the Analytics Engine architecture and algorithm
- Running Analytics Engine manually
- Testing Analytics Engine

Module 6: Supplemental Server

- Describing the benefits of deploying Supplemental Server.
- Installing Supplemental Server.

Module 7: Configuring Fingerprinting and Machine Learning

- Describing the classifiers created by crawlers
- Configuring advanced file fingerprint
- Configuring advanced database fingerprinting
- Configuring machine learning

Module 8: Forcepoint One Endpoint (F1E)

- Describing Endpoint Server architecture and endpoint communication
- Installing Forcepoint One Endpoint (F1E) to include anti-tampering
- Using Forcepoint One Endpoint (F1E)

Module 9: Troubleshoot DLP Endpoint Scanning

- Troubleshooting endpoint agents
- Tracing endpoint agent issues
- Excluding applications from DLP endpoint
- Debugging F1E

Module 10: DLP Discovery tasks

- Discovering hidden data
- Load balancing the crawler
- Creating a Network Discovery task
- Using Endpoint Discovery

Module 11: DLP Maintenance

- Identifying and running reports
- Configuring DLP roles
- Generating Discovery task reports
- Deleting a discovery job
- Identifying types of remediation script
- Running a remediation script
- Inspecting a remediation script
- Updating DLP components
- Moving and replacing forensics
- Describing automatic DLP component synchronization
- Recording fingerprint task
- Configuring DLP backup and DSS restore procedures
- Performing a DLP backup
- Using the upgrade validation tool
- Fixing common SQL issues
- Describing the Forcepoint infrastructure
- Investigating Policy Engine timeouts

Module 12: Complex Classifiers

- Identifying types of classifier
- Building a data security policy
- Combining multiple classifiers
- Describing nested transactions logic

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