Forcepoint DLP Administrator Virtual Instructor-Led Training

Datasheet

<May 2020>

Forcepoint

forcepoint.com

Forcepoint Data Loss Prevention (DLP) Administrator Virtual Instructor-Led Training

DTADM

The Forcepoint DLP Administrator course is designed for people who 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. They 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 and IT staff
- DLP incident and forensic analysts

Format:

Virtual Instructor-Led Training*

Duration:

16 hours, typically delivered in 4 sessions (4 hours per session), 2 hours outside of class for the exam

Course Price:

$1,150 USD non-discountable

Exam Price:

One attempt is included

Course objectives

- Identify and define core DLP terminology, resources, and architecture.
- Explain each DLP license type and its related features.
- Define and create each type of DLP classifier.
- Define and create each type of DLP resource, including URL categories, action plans, and notifications.
- Define and create each type of DLP policy, rule, and exception.
- Manage policies and rules using bulk updates and policy levels.
- Explain and test the capabilities and modes of OCR.
- Use the Online Applications feature to detect web file uploads.
- Manage the DLP CASB integration.
- Build, deploy, and manage the Forcepoint One Endpoint.
- Define the terms specific to DLP incident reporting.
- List and explain the report types in the report catalog.
- Manage and customize incident reports.
- Analyze and Perform each type of workflow on a DLP incident.
- Explain the features of the Incident Risk Ranking dashboard.
- Identify, define, and explain common regulatory compliance specifications.
- Create and manage policies to meet regulatory compliance specifications.
- Create and configure an administrator with role-based permissions.
- Define and perform discovery activities.
- Define and perform fingerprinting and machine learning activities.
- Explain the functionality of file tagging and how DLP integrates with it.
- Import file tags, create classifiers, and use in a policy and rule, including applying tags with discovery.
- Review the operational status of DLP components and services.
- Identify the items included in, and perform a DLP backup and restore.
- Identify and analyze the primary logs used in DLP security manager.
- Manage DLP incident storage.

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 DLP Administrator Certification exam. One exam attempt 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 pass.

Course Outline

Module 1: Summarize the basic concepts of Forcepoint DLP.

- Define the acronym "DLP" and explain how DLP can affect an organization.
- Identify and define core DLP terms.
- Identify the different states of data that Forcepoint DLP can protect.
- Access Forcepoint Security Manager and perform initial configuration of Forcepoint DLP.
- Define what a DLP system module is and explain the basic function each agent performs.
- Locate and configure registered system modules in a DLP environment.
- Identify the parts of a DLP incident envelope and where they are stored.
- Given a flow diagram, explain the sequence of steps in a DLP transaction.
- Identify the different channels and associated transaction types that Forcepoint DLP can protect.
- Identify available Forcepoint DLP product information resources and where they can be accessed.
- Explain where Forcepoint DLP fits into the Forcepoint Human Point System.

Module 2: Explain the Forcepoint DLP licensing model.

- Explain the DLP license types and their related features.
- Analyze the content of a DLP subscription XML file.
- Deploy a new DLP subscription file.

Module 3: Create and manage Forcepoint DLP classifiers.

- List and explain each Forcepoint classifier type.
- Create a functional example of each Forcepoint classifier type.
- Access the list of predefined script classifiers and identify several commonly used categories.
- Configure the parameters of a predefined script classifier.

Module 4: Create and manage Forcepoint DLP resources.

- List and explain each Forcepoint DLP resource.
- Configure a connection to and import a user directory.
- Create a functional example of each Forcepoint DLP resource.
- Import URL categories by enabling the linking service.
- List and explain the default action plans.
- Create a custom action plan.
- List and explain the default notifications.
- Use dynamic variables in notifications.
- Configure the default notification.

Module 5: Create and manage Forcepoint DLP policies and rules.

- Define what a DLP policy is, identify three broad types of them, and explain what they do.
- Explain how cumulative rules can be used in DLP.
- Configure, deploy, and test a quick policy.
- Configure and test a predefined policy.
- Configure, deploy, and test a custom policy and rule.
- Explain the purpose and function of a rule exception.
- Explain how to perform a bulk update of multiple policies and rules.
- Explain how policy levels provide scope and processing order for policies, then create a new policy level and assign policies to it.

Module 6: Analyze a transaction using OCR.

- Explain the capabilities and modes of OCR.
- Configure a policy engine to work with an OCR server.
- Submit a transaction to the OCR engine and examine the results.

Module 7: Manage Forcepoint DLP cloud applications and CASB.

- Use the Online Applications feature to detect web file uploads to Google Drive or Dropbox.
- Explain aspects of the Forcepoint DLP CASB integration, including license management functionality, how to locate logs from CASB Cloud Agents, and how to configure and perform a cloud discovery scan.

Module 8: Install and manage the Forcepoint One Endpoint.

- Identify the core features of the Forcepoint One Endpoint.
- Explain the current OS and software compatibility of the Forcepoint One Endpoint.
- Explain the endpoint global and profile settings.
- Obtain the necessary files and build an installer package for the Forcepoint One Endpoint.
- Deploy the Forcepoint One Endpoint.
- Identify supported endpoint encryption methods.
- Use the Forcepoint One Endpoint to encrypt files copied to removable media.
- Explain the DLP endpoint temporary bypass feature.
- Temporarily bypass the Forcepoint One Endpoint.
- Configure the endpoint browser extension to work in monitor-only mode.
- Test the endpoint browser extension in monitor-only mode.
- Explain the DLP endpoint employee coaching feature.
- Confirm the function of the employee coaching feature.

Module 9: Analyze and report on Forcepoint DLP incidents.

- Define the core terminology of Forcepoint DLP incident reporting.
- List and explain the report types in the report catalog.
- Analyze an incident in an Incident List report.
- Perform each UI-based incident workflow action.
- Explain the function of DLP incident batch operations.
- Perform a remediation operation on a batch of incidents.
- Explain the features of the incident risk ranking dashboard.

Module 10: Configure Forcepoint DLP to conform to regulatory compliance specifications.

- Define the term AUP (Acceptable Usage Policy).
- Explain how to create policies that comply with your Acceptable Usage Policy.
- Explain governmental regulatory compliance specifications.
- Deploy DLP policies that meet a specific set of regulatory compliance specifications.
- Give a high-level overview of delegated administrators and role-based permissions.
- Configure a delegated administrator to have role-based permissions.

Module 11: Implement Forcepoint DLP discovery.

- Define terminology specific to discovery.
- Perform discovery activities including configuration, task execution, and analysis of discovery incidents.

Module 12: Implement fingerprinting and machine learning.

- Define terminology specific to fingerprinting and machine learning.
- Perform file fingerprinting activities includinging configuration, task execution, and tuning of results.
- Perform machine learning activities, including configuration, task execution, and tuning of results.

Module 13: Apply policies using third party file tagging software.

- Explain the functionality of classification labels and how to integrate them into the DLP data labeling framework.
- Integrate Boldon James into the DLP data labeling framework.
- Create a file labeling classifier to manage files that contain sensitive or proprietary information.
- Create and deploy a data usage policy using a file labeling classifier.
- Create and deploy a discovery policy with an action plan capable of assigning file classification labels.
- Integrate Microsoft Information Protection into the DLP data labeling framework.

Module 14: Monitor and maintain Forcepoint DLP system health.

- Examine the DLP Infrastructure System Summary and identify where to examine CPU and memory resources.
- Review the operational status of components and services for DLP supplementary servers.
- Review the operational status of components and services for protectors, Web Security Gateways, and Email Security Gateways.
- Examine and evaluate performance indicator charts for a policy engine.
- Examine and evaluate performance indicator charts for the fingerprint repository.
- Examine and evaluate performance indicator charts for an endpoint server.
- Examine and evaluate performance indicator charts for the OCR server.
- Identify what is included in a DLP backup, and then configure and perform a DLP backup task.
- Identify and analyze the primary logs used in DLP Security Manager.
- Export and report on information found in the primary DLP logs.
- Manage incident storage by evaluating utilization, resizing it as needed, and archiving and restoring incident partitions.

**To attend this virtual online course, you must have a computer with:*

- A high-speed internet connection (minimum of 1MB connection required)
- An up to date web browser (Google Chrome recommended)
- PDF Viewer
- Zoom client
- Speakers and microphone or headset (headset recommended)

A separate tablet or ebook reader is also recommended for the course and lab book delivery

Terms and Conditions

- Virtual Instructor Led Trainings (VILTs) are delivered as live instructor-led training in an online classroom—No on-site delivery element.
- 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.
- VILT 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.