FORCEPOINT

Forcepoint DLP Administrator e-Learning

Datasheet

October 2019

Forcepoint Data Loss Prevention (DLP) Administrator

DLPADMEL

In this eLearning, 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

- Consultants, System Architects, Integrators and Planners who help customers with Forcepoint DLP implementations
- System Administrators, Network Security Administrators, IT staff and Forcepoint DLP Analysts

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:
Computer-Based e-Learning

Duration:
8 hours of total content

Course Price:
$575 USD non-discountable

Exam Price:
$100 USD

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 can be purchased separately at a rate of $100. If you would like to take the certification exam following completion of the e-Learning course, please contact learn@forcepoint.com for purchase details. A minimum score of 80% on the multiple-choice online exam is required to pass.

"It helped me to firmly understand the basics of DLP implementation…."

Course Outline

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.

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

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)

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 e-Learning 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)*
- *Adobe Flash web browser plug in (v13 or higher)*
- *PDF Viewer*
- *Speakers and microphone or headset (headset recommended)*

Terms and Conditions

Forcepoint products may be used to address customer concerns regarding content that could be considered objectionable or offensive. As a result, portions of Forcepoint course materials and lab exercises that train on these products may use examples of such content to teach appropriate protection mechanisms. Enrollees should be aware of this possibility, and if they are concerned should not enroll in this course or should consider purchasing a custom course that could be created to utilize other examples.

Additional terms and conditions found here:

https://www.forcepoint.com/resources/training/forcepoint-training 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