Unified Email DLP Course

OEM: Proofpoint • Code: UNIFIED_EMAIL_DLP_COURSE

COURSE DESCRIPTION

This instructor led course teaches learners how to deploy and manage Unified Email DLP by applying data classification, creating and refining policies, configuring notifications and encryption, and investigating incidents through centralized workbench workflows. Live lab exercises provide experience with real-world use cases.

AUDIENCE PROFILE

- Email DLP Analysts and Administrators

PREREQUISITES

- This section doesn't contain any content.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- This section doesn't contain any content.

COURSE OUTLINE

Module 1: Introduction

- Course goals and structure
- Student Guide and Lab Access

Module 2: Foundations of Unified Email DLP

- What Unified Email DLP solves
- DLP Core Concepts
- DLP Workflow Basics
- Roles and Integration Other Security

Module 3: Proofpoint Platform Overview

- Threat Protection Platform: Role and interaction with DLP
- Data Security Platform: Architecture and components
- User Management
- Workbench overview
- Identity Provider Configuration
- Users & Groups
- Access Policies
- Access Requests
- Hands-on: Log in to the Training Threat Protection and Data Security platforms.

Module 4: Message Processing

- End-to-end mail flow through the platform
- Policy Routes (traffic flows, routing logic)
- Handling of headers/attachments/body, file types, and nested archives
- Processing stages: intake → classification → policy evaluation → action
- Performance considerations & troubleshooting techniques
- Smart Search
- Hands-on: Find a Message in Smart Search and see delivery indicators.

Module 5: Data Classification

- Data Identifiers (Dictionaries, Smart IDs, Classifiers, Exact Data Matching, Index Data Matching)
- Detectors (Operator, Score, Proximity Statement)
- Data Classes
- Testing Detectors and Data Classes
- Snippet Masking Policies (privacy-preserving evidence)
- Hands-on: Build a custom identifier and map it to a data class.

Module 6: Email DLP

- DLP Folders (organization, lifecycle, deployment strategy)
- DLP Rules (conditions, policy routes, actions: block, quarantine, encrypt, notify)
- DLP Use Cases (outbound PCI, insider IP, BEC + DLP)
- Hands-on: Create a DLP rule that will detect and stop the behavior of the use case.

Module 7: Data Security Workbench

- Alerts (triage, severity, workflows, comments, remediation)
- Tag (labelling evidence and cases)
- Dashboard (Customization, trend analysis, reporting)
- Hands-on: Investigate a DLP alert and remediate according.

Module 8: Proofpoint Encryption

- Proofpoint Encryption components
- Encryption triggers via DLP policies
- Recipient experience & Secure Reader Utilization
- Sender experience & key handling