

Data Security Administrator for the AI Era

OEM: Proofpoint

COURSE DESCRIPTION

expertise to effectively configure, manage, and administer core products within Proofpoint's Data Security platform. These products include Cloud DLP, Endpoint DLP, and Email DLP. This course focuses on key skills such as configuration, customization, and day-to-day management, enabling administrators to defend data and detect risky behavior. This course provides hands-on experience within a classroom-lab environment to hone the data security administrator's skill set and effectively create policies to address common use cases.

AUDIENCE PROFILE

- Data Security 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: Platform Overview

- Identify the components of Proofpoint's Data Security platform
- Navigate your tenant and system entitlements
- Navigate the Data Security Workbench
- Create, edit, and manage explorations, alerts, and reports
- Create explorations with Advanced Query with AI

Module 2: User Management

- Configure your Identity Provider

- Add, edit, and assign permissions to user accounts
- Audit console user activities The Data Security Administrator certification course equips system administrators with the

Module 3: Data Classification

- Identify the purpose and tools of the Data Classification application
- Create effective and efficient data classes and data detectors, including AI classifiers
- Navigate and interact with the Data Security Posture Management Platform (DSPM)
- Create and apply data snippet masking policies

Module 4: Endpoint Agent Realm Configuration

- Explain the features of Endpoint DLP and ITM
- Identify the components of Endpoint/ITM SaaS
- Configure agent realms

Module 5: Endpoint Agent Deployment

- Install agents on endpoints
- Install and configure the agent updater on endpoints

Module 6: Endpoint Agent Policy Configuration

- Identify which features are controlled through agent policies
- Configure effective agent policies
- Assign agent policies to your agent realms

Module 7: Endpoint and ITM Rules and Conditions

- Identify when to use detection, prevention, and endpoint rules
- Create, edit, and apply rules
- Evaluate and fine-tune rules to better fit specific use cases

Module 8: Endpoint Content Scanning

- Identify types of content that can be scanned for sensitive data

Module 9: Enable content scanning on an agent realm Email Processes and Policy Routes

- Explain the architecture of email services
- Configure email outbound and inbound messages and policy routes

Module 10: Email Policy Enforcement and Message Investigation

- Configure firewall rules and Email DLP rules
- Evaluate and identify when to use Smart Send

- Navigate Smart Search Cloud Administration, Rule Configuration, and

Module 11: Cloud DLP Rules Configuration and Management

- Configure cloud providers
- Explain access rules, data rules, app governance rules, and configuration and security posture rules
- Configure policies to match specific use cases

Module 12: Notification Policies

- Identify types of end-user notifications available through Data Security
- Create and apply notification policies
- Create exploration subscriptions

Module 13: Data Security for AI

- Explain how Data Security for AI can improve visibility into enterprise AI activity
- Monitor and govern shadow AI use
- Identify and protect sensitive data in prompts and uploads