Collaboration Security Administrator for the AI Era

OEM: Proofpoint • Code: COLLABORATION_SECURITY_ADMINISTRATOR_FOR

COURSE DESCRIPTION

The Proofpoint Collaboration Security Administrator certification course builds advanced administrative expertise in utilizing Proofpoint's comprehensive suite, focusing on the day-to-day operations and tasks carried out by those administrating Proofpoint platforms. This course dives into many of the Proofpoint products used to safeguard your organization from sophisticated email threats. Facilitated by our experienced instructors and with practical engaging labs this advanced hands-on course will equip you to administer and manage products like Email Protection, Targeted Attack Protection, Cloud Threat Response, Proofpoint's AI Satori Abuse Mailbox Agent, and Closed-Loop Email Analysis & Response.

AUDIENCE PROFILE

- Messaging, Administrators, and Security Analyst

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: Proofpoint Products Overview

- Identify the different Proofpoint Collaboration Security tools and products
- Understand the fundamental principles governing how each tool functions
- Describe how these tools integrate and interact with one another

Module 2: Mail Flow

- Understand mail routing and how inbound and outbound mail routes are configured

- Explain the purpose of mail relay

Module 3: Message Processing

- Understand how the Protection Server processes mail and how Proofpoint Dynamic Reputation informs filtering decisions
- Explain SMTP communication and session processing within the Protection Server
- Identify the components of a rule and how Policy Routes, delivery options, and Lists affect message handling
- Describe how policies, rules, and dispositions work together, including disposition precedence and rule firing order
- Configure SMTP Profiles to support specific mail routing needs

Module 4: Quarantine

- Create and delete quarantine folders
- Configure quarantine folder settings
- Search for and release quarantined messages
- Understand quarantine precedence order

Module 5: Investigation and Logging

- Describe the Config Master and agent architecture, and how PPS cluster support message processing and logging
- Use Cloud-Based and On-Prem Smart Search to investigate and troubleshoot mail flow
- Interpret log entry formats and use the Log Viewer to investigate mail flow issues
- Search and filter data within audit logs

Module 6: Protection Server Monitoring and Reporting

- Create alert profiles
- Configure alert rules
- View alerts
- View reports

Module 7: Encryption

- Understand the difference between message-level encryption and TLS
- Identify the connection phases of the TLS handshake
- Enable TLS and enforce TLS to specific domains

Module 8: User Management and Recipient Verification

- Understand the PPS User Hierarchy and User Repository, and create Import/Authorization profiles
- Configure Recipient Verification, including Data Connectors, Verification Source Profiles, and Verification Rules
- Add and manage Administrator users across Collaboration Security systems

Module 9: Email Digests and the End User Web Application

- Understand Email Digests and the differences between digest types
- Enable and configure Email Digests
- Enable and configure the Web-based Command Processor and End User Web Application

Module 10: Email Firewall - More Rules and Functions

- Recognize key built-in Email Firewall rules and apply best practices for their use
- Create and manage Dictionaries to mitigate offensive or unwanted content
- Configure Bounce Management to reduce backscatter mail
- Understand and configure SMTP Rate Control and Outbound Throttle settings

Module 11: Email Authentication

- Understand the fundamentals of SPF, DKIM, and DMARC
- Configure SPF, DKIM, and DMARC policies and rules
- Use Smart Search to review email authentication results

Module 12: Spam Detection

- Describe spam scoring, classification, and recommended rule configurations
- Use Threat Protection APIs to manage Safe List and Block List entries
- Identify, report, and troubleshoot false positives and negatives

Module 13: Virus Protection

- Understand the purpose and operation of the Virus Protection Module
- Create Virus Protection Policies
- Create and edit Virus Protection Rules

Module 14: Email Warning Tags

- Understand the purpose of Email Warning Tags
- Understand tag precedence
- Customize Email Warning Tags

Module 15: Targeted Attack Protection (TAP)

- Understand the purpose of URL Rewrite and enable and configure it
- Understand the purpose of Message Defense and enable and configure it
- Use TAP Dashboard tools, including URL Decoder, Blocklists, and user privilege management
- Create and use TAP Dashboard API keys to extract data

Module 16: Threat Response

- Differentiate between Cloud (CTR) and On-Prem (TRAP) Threat Response, and review the Messages and Incidents dashboards
- Configure mail servers, Quarantine Modes, and automation workflows in Threat Response

- Understand the CLEAR process and use APIs to manage incidents and messages