proofpoint.
cybersecurity academy

Threat Protection Administrator Course

proofpoint.
certified guardian

The Proofpoint Threat Protection 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 the Email Protection Server, Targeted Attack Protection, Cloud Threat Response and Closed-Loop Email Analysis & Response.

Threat Protection Admin Course

FORMAT

Virtual Instructor-Led Training (VILT), Onsite Training At A Customer's Facility (OS)

DURATION

4
days

INTENDED AUDIENCE

Messaging and Security Administrators

Course Syllabus

Proofpoint products overview: In this lesson, you will learn to:

- Identify the different Proofpoint Threat Protection tools and products
- Understand the fundamental principles governing how each individual tool functions
- Describe the ways in which these tools are designed to integrate and interact with one another to achieve cohesive system operation

Mail Flow: In this lesson, you will learn:

- How the Protection Server manages Inbound and Outbound mail routes
- Mail Relays configuration
- How the protection server utilizes the SMTP Protocol through the SMTP session calls
- Configuring DNS and Domain Setup
- How Policy Routes work in the Protection Server
- Enabling and enforcing TLS to specific domains
- Generate Certificates

Message Processing: In this lesson, you will learn:
- How the Protection Server processes Inbound and Outbound messages
- Policies & Rules in the Protection Server
- How the Protection Server filters mail
- How to create SMTP Profiles

Email Firewall: In this lesson, you will learn how to:
- Add or modify rules based to specified mail conditions and enforcing dispositions
- Manage SMTP Rate Control with configuration settings and rules
- Configure Outbound Throttle and send mail thresholds
- Enable Bounce Management and reduce backscatter mail
- Create and modify Dictionaries to mitigate offensive content
- Configure Recipient Verification rules and profiles

Quarantine: In this lesson, you will learn how to:
- Create and delete quarantine folders
- Configure quarantine folder settings for specific messages and triggered rules
- Search for and release quarantined messages
- Manage Quarantine precedence order

Smart Search and Logging: In this lesson, you will learn:
- How to use Smart Search to find and investigate messages
- The purpose of different logs, entry formats and investigate mail flow
- How to use the search and filtering data within Audit Logs
- How to review and export Syslogs
- How to explore and understand PoD API

Alerts and Reporting: In this lesson, you will learn about:
- Creating alert profiles to receive system alerts
- Configuring alert rules to give greater control and flexibility over what alerts you want to receive
- Viewing and analyzing system alerts
- Viewing system reports to see how your system is performing

Email Authentication: In this lesson, you will learn how to:
- Explore the email security posture on how Email Authentication is implemented by the Protection Server
- Configure SPF policies and rules
- Configure DKIM polices, rules and signing
- Configure DMARC polices and rules
- Create Email Authentication keys

User Management: In this lesson, you will learn how to:
- Sync your Active Directory to the Proofpoint Protection Server
- Add or import User Profiles
- Create Groups and Sub-Groups
- Configure LDAP/Azure/SSO
- Configurate roles and access to Cloud & On-Prem UI's

Spam Detection: In this lesson, you will learn how to:
- Create Policies
- Create and tune rules to determine how you want Spam to be managed
- Create Safe and Block Lists
- Create Custom Spam rules specific to your organization's threats

Virus Protection: In this lesson, you will learn about:
- The purpose and operation of the Virus Protection Module
- Restrict to, or disable processing on, certain policy routes
- Creating Virus Protection Policies
- Creating and editing Virus Protection Rules

User Notifications: In this lesson, you will learn about:
- The purpose of Email Warning Tags
- Tag precedence
- Restricting message tagging to specific routes
- Customizing Email Warning Tags
- Configuring Email Digest

Targeted Attack Protection (TAP): In this lesson, you will learn about:
- URL Rewrite and its settings
- The purpose of Message Defence and configure settings
- TAP Dashboard and implement custom blocklists, add users and privileges
- The purpose of each TAP Dashboard API and create API keys and extract data

Threat Response: In this lesson, you will learn to:
- Differentiate between Cloud vs On-Prem Threat defense
- Explore Initial deployment tasks
- Configure and connect mail servers
- Enable automation workflows
- Create customizable lists for message attributes
- Import Sources
- Understand how Closed Loop Email Analysis & Response plays in to Threat Response

proofpoint.

https://www.proofpoint.com/us/cybersecurityacademy

DISCOVER THE PROOFPOINT PLATFORM →