Formation Proofpoint - Administrateur Threat Protection

Threat Protection administrator

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La formation certifiante d'administrateur Proofpoint Threat Protection développe une expertise avancée en administration de la suite Proofpoint, en mettant l'accent sur les opérations et tâches quotidiennes des administrateurs de plateformes Proofpoint. Ce cours explore en profondeur les nombreux produits Proofpoint utilisés pour protéger votre organisation contre les menaces sophistiquées véhiculées par e-mail.
Ponctuée d'ateliers pratiques interactifs, cette formation avancée vous permettra d'administrer et de gérer des produits tels que Email Protection Server, Targeted Attack Protection, Cloud Threat Response et Closed-Loop Email Analysis & Response.

Référence	PPATP14
Durée	4 jours (28h)
Tarif	4 080 €HT
Repas	repas inclus

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| Identifier les différents outils et produits Proofpoint Threat Protection
| Décrire les principes fondamentaux qui régissent le fonctionnement de chaque outil
| Assurer un fonctionnement cohérent du système

Public

| Administrateurs de messagerie et de sécurité

Prérequis

| Aucun

Programme de la formation

Mail Flow
| 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
| 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
| 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
| 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
| 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
| 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
| 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
| 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
| 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
| 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
| 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)
| 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
| 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

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.

HUB Formation - 14 avenue de l'Opera - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785 00055