Palo Alto Networks Cloud Services Operations TRAPS

Référence : **PAN-EDU-290** Durée : **2 jours** Certification : **PSE**

CONNAISSANCES PREALABLES

• être familiers avec les concepts de sécurité en entreprise.

PROFIL DES STAGIAIRES

• Ingénieurs Sécurité des Endpoints, Administrateurs systèmes, et Ingénieurs support technique.

OBJECTIFS

• Palo Alto Networks® Traps™ Advanced Endpoint Protection vous protège contre l'exploitation des vulnérabilités sophistiquées et les attaques utilisant des malwares inconnus. . • Suite à ces 2 jours de formations, délivrés par un formateur certifié, les stagiaires seront aptes à configurer Traps Management Service et installer l'agent Traps sur les périphériques..

CERTIFICATION PREPAREE

Palo Alto Networks PSE Endpoint Associate

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Palo Alto

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Introduction à Traps

- Comment les attaques sophistiquées fonctionnent-elles aujourd'hui?
- Prévention des menaces multi-méthodes Traps
- Composants et ressources Traps

Services Cloud

- Application Framework et Portail Services Cloud
- Services partagés et Flux d'intégration Traps

« Cloud-Based Management »

- Tableau de bord et Licensing Traps
- Installation de l'agent et de l'agent multi-plateforme
- « Endpoints » et "Endpoint Groups"

« Policy Rules » et Profiles

- « Profiles » et « Policy Rules
- « Agent Settings Profile »

Flux de protection contre les logiciels malveillants

- Vue d'ensemble des modules de protection contre les programmes malveillants
- « Restrictions Profiles », « Malware Profiles » et « Scanning »

« Exploits » et Exploitations Techniques

- « Application Exploit Prevention »
- Techniques d'exploitation et mécanismes de défense
- Notions de base de la gestion des processus (facultatif)

« Exploit Protection Modules »

- Architecture et aperçu
- « Exploit Protection Modules » (EPMs)

- « Exploit Profiles »

Gestion des événements

- Journaux d'événements de sécurité et exceptions
- « Endpoint » et « Server Logs »
- Gérer les fichiers mis en quarantaine

Dépannage Basique Traps

- Dépannage : Méthodologies et Ressources
- “Traps Cytool” et “Agent Identification”
- “Traps Agent Log Files” et “Agent Persist Databases”
- Travailler avec le Support technique

Architecture Traps

- Services AWS utilisés par TrapsService
- Architecture Multi-Regionale
- « Agent File Uploads » et « Downloads »
- « Agent-Server Communication »

“Directory Sync Service”

- « Directory Sync Service » – Activation et mise en place
- Dépannage