

Palo Alto Networks TRAPS : Cloud Service Operations PAN-EDU-290

MIEL

Centre Agréé :
N°11 91 03 54 591

Pour contacter le
service formation :
01 60 19 16 27

Pour consulter le
planning des formations :
www.miel.fr/formation

Formations sur Paris,
Bievres (91) et en
régions

PRESENTATION DE LA FORMATION

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.

DUREE DE LA FORMATION

2 jours

PUBLIC CONCERNE

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

PRE-REQUIS

Les stagiaires devront être familiers avec les concepts de sécurité en entreprise.

CONTENU DE COURS

Les stagiaires vont apprendre comment Traps protège contre l'exploitation de vulnérabilités et les attaques utilisant des Malwares.

Pendant les labs, les stagiaires vont :

- Explorer et configurer la plateforme Cloud Traps Management Service et installer les agents Traps sur les périphériques ;
- Construire des policy rules et des profiles, activer et désactiver la protection des processus ;
- Intégrer Traps avec Palo Alto Networks Wildfire®, qui permet la protection et la détection de malwares zero-day.

Niveau du cours : Introduction

Format du cours : Ce cours allie théorie et pratique sur un environnement de lab.

Version logicielle : Palo Alto Networks Traps Advanced Endpoint Protection

Voici le détail des points abordés pendant la formation :

Jour 1 - Module 1 : Introduction à Traps

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

APPELEZ LE 01 60 19 16 27

- Jour 1 - Module 2 : Utiliser les applications Cortex
 - Cortex et Cortex Hub
 - Création d'une instance Traps
- Jour 1 - Module 3 : Traps Management Service
 - Interface Web Traps
 - Installation des agents Traps et de l'agent multi-plateforme
 - Politiques et profils
- Jour 1 - Module 4 : Flux de protection contre les logiciels malveillants
 - Vue d'ensemble des modules de protection contre les programmes malveillants
 - Restrictions Profiles, Malware Profiles et Scanning
 - Protection comportementale contre les menaces
- Jour 2 - Module 5 : Flux de protection contre l'exploitation de vulnérabilité
 - « Application Exploit Prevention »
 - Techniques d'exploitation et mécanismes de défense
 - Notions de base de la gestion des processus (facultatif)
- Jour 2 - Module 6 : Manager les événements de sécurité
 - Évènements de sécurité
 - Exceptions
 - Possibilités de réponses
 - Analyse automatique des informations
- Jour 2 - Module 7 : Troubleshooting
 - Troubleshooting : Méthodologies et Ressources
 - Traps Cytool et Agent Identification
 - Traps Agent Log Files et Agent Persist Databases
 - Travailler avec le support technique
- Jour 2 - Module 8 : Communications Agent-Serveur
 - Architecture Multi-Région
 - Communication Agent-Serveur
- Jour 2 - Module 9 : Infrastructure de services Cortex
 - Services partagés
 - Application Log Forwarding
 - Directory Sync Service
- Jour 2 - Module 10 : Opérations avancées
 - Initiatives XDR
 - Protection des conteneurs Linux
 - Protection des périphériques Android

CERTIFICATION PREPAREE

Cette formation prépare à la certification Palo Alto Networks PSE Endpoint Associate + PSE Endpoint Professional (**pour les partenaires uniquement**)

APPELEZ LE 01 60 19 16 27