

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

Jour 1 - Module 2 : Services Cloud

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

APPELEZ LE 01 60 19 16 27

- Jour 1 - Module 3 : « Cloud-Based Management »
 - Tableau de bord et Licensing Traps
 - Installation de l'agent et de l'agent multi-plateforme
 - « Endpoints » et « Endpoint Groups »

- Jour 1 - Module 4 : « Policy Rules » et Profiles
 - « Profiles » et « Policy Rules »
 - « Agent Settings Profile »

- Jour 1 - Module 5 : Flux de protection contre les logiciels malveillants
 - Vue d'ensemble des modules de protection contre les programmes malveillants
 - « Restrictions Profiles », « Malware Profiles » et « Scanning »

- Jour 2 - Module 6 : « Exploits » et Exploitations Techniques
 - « Application Exploit Prevention »
 - Techniques d'exploitation et mécanismes de défense
 - Notions de base de la gestion des processus (facultatif)

- Jour 2 - Module 7 : « Exploit Protection Modules »
 - Architecture et aperçu
 - « Exploit Protection Modules » (EPMs)
 - « Exploit Profiles »

- Jour 2 - Module 8 : Gestion des événements
 - Journaux d'événements de sécurité et exceptions
 - « Endpoint » et « Server Logs »
 - Gérer les fichiers mis en quarantaine

- Jour 2 - Module 9 : 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

- Jour 2 - Module 10 : Architecture Traps
 - Services AWS utilisés par TrapsService
 - Architecture Multi-Regionale
 - « Agent File Uploads » et « Downloads »
 - « Agent-Server Communication »

- Jour 2 - Module 11 : «Directory Sync Service»
 - « Directory Sync Service » – Activation et mise en place
 - Dépannage

CERTIFICATION PREPAREE

Cette formation prépare à la certification Palo Alto Networks PSE Endpoint Associate

APPELEZ LE 01 60 19 16 27