# Déploiement et optimisation de TRAPS

Référence : **PAN-EDU-285** Durée : **2 jours** Certification : **PCNSE**

## CONNAISSANCES PREALABLES

• Il est fortement recommandé aux stagiaires d'avoir suivi le cours PAN-EDU-281 - Palo Alto Networks : Installation, configuration et gestion de TRAPS. • Les stagiaires doivent être familiers avec l'administration des systèmes Microsoft Windows ainsi que les concepts de sécurité informatique en entreprise.

## PROFIL DES STAGIAIRES

• Administrateurs systèmes. • Ingénieurs sécurité. • Support technique.

## OBJECTIFS

• Comprendre comment concevoir, implémenter et optimiser le déploiement de la solution Palo Alto Networks Traps dans des environnements complexes ou de taille importante. • Pendant les ateliers pratiques, les stagiaires vont distribuer de manière automatisée des agents, préparer des images master pour les environnements VDI, construire un environnement multiserveur, concevoir et implémenter des politiques personnalisées, tester Traps avec Metasploit et examiner les dumps mémoires générés lors du déclenchement de la protection.

## CERTIFICATION PREPAREE

Palo Alto Networks Systems Engineer : Platform – Professional

## 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

### JOUR 1

### Introduction

### Déploiement

- Distribution de l'agent poste de travail
- Options TLS/SSL
- Déploiement pour les environnements Virtual Desktop Infrastructure (VDI)

### Dimensionner le déploiement

- Contrôle d'accès basé sur des rôles
- Modèles de déploiement incluant plusieurs serveurs ESM
- Tâches de migration

### Optimiser Traps

- Optimiser les paramètres serveur
- Définition des conditions
- Concevoir des politiques optimisées
- Tâches de maintenance

### JOUR 2

### Recherche de preuve (forensics) avancé

- Requêtes vers les agents
- Outils de test pour les malwares
- Les techniques d'exploitations en détail
- Techniques d'exploitation avec Metasploit

- Analyse d’un dump mémoire

## Dépannage avancé

- ESM serveur et architecture Traps
- Outils de dépannage : dbconfig et cytool
- Problèmes de compatibilité des applications
- Connectivité BITS