TRAPS 6.1: GESTION DU SERVICE CLOUD (EDU-290)

Aperçu

La solution Traps Advanced Endpoint Protection de Palo Alto Networks protège contre les attaques utilisant des exploits zero-day et des malwares inconnus précédemment. Suivre ce cours de deux jours mené par un instructeur certifié permettra de mettre en place, de configurer le service Traps Management Service et d'installer l'agent Traps.

Module 1: Aperçu de Traps
- Prévention des menaces multi-méthodes de Traps
- Composants Traps et ressources utiles

Module 2: Utilisation des Apps Cortex
- Cortex et le Hub d'applications
- Déroulé d'un lancement de projet Traps

Module 3: Traps Management Service
- Interface web de Traps Management Service
- Agent Traps et installation
- Postes et groupes de postes
- Règles et profils des politiques

Module 4: Protection anti Malwares via Traps
- Aperçu de la protection anti Malware Traps
- Profils de restriction et de malwares
- Protection via l'analyse comportementale

Module 5: Protection ant Exploit via Traps
- Prévention contre les exploits et contre les techniques d'exploits
- Module de protection d'Exploit et profils
- Bases de la gestion des processus (optionnel)

Module 6: Gestion des évènements de sécurité
- Evènements de Sécurité
- Exceptions
- Capacités de réponse à incident
- Analyse automatique des dumps mémoire

Module 7: Diagnostiquer Traps
- Méthodologies et ressources à utiliser pour diagnostiquer Traps
- Application Cytool de Traps
- Journaux Serveurs, agent et les data stores de l'agent
- Travailler avec le support

Module 8: Communications Agent-Serveur
- Architecture multi-régions
- Communication Agent-Serveur

Module 9: Infrastructure des services Cortex
- Services communs
- App "Log Forwarding"
- Service "Directory Sync"

Module 10: Opérations avancées
- Initiative XDR
- Protection des containers Linux
- Protection des machines Android (optionnel)

Objectifs du Cours

Ce cours permet de comprendre comment Traps protège contre les attaques reposant sur des exploits et des malwares. Des labs permettent aux étudiants de mettre en place, puis de se familiariser et configurer le service cloud Traps Management Service, installer l'agent Traps sur des postes Windows/Linux, construire des règles et des profils, gérer les évènements de sécurité, les journaux, la création d'exceptions, ainsi que les actions de réponse centralisées.

Caractéristiques du cours

- **Niveau du cours :** Intermédiaire
- **Durée du cours :** 2 jours
- **Format du cours :** Théorie présentée par un instructeur, et pratique sur des machines Windows et Linux via des labs
- **Logiciel :** Palo Alto Networks Traps Advanced Endpoint Protection

Audience

Ingénieurs sécurité orientés postes de travail, administrateurs systèmes, et ingénieurs support

Prérequis

Les étudiants doivent être familiers avec les concepts de sécurité en entreprise

Formation chez un partenaire agréé Palo Alto Networks

Vous former chez un partenaire agréé Palo Alto Networks vous permet de vous préparer au mieux à la mise en place de mécanismes de protection contre les nouvelles menaces de l'âge digital.

Les certifications Palo Alto Networks vous permettent de garantir le niveau de connaissance nécessaire à prévenir les cyberattaques en permettant l'utilisation de vos applications de manière protégée.

Exclusive Networks France
ARCS DE SEINE – BAT A
20, quai du Point du Jour
92100 Boulogne Billancourt

Tel: +33 (0)1 41 31 53 04
Fax: +33 (0)1 41 31 47 86
formation@exclusive-networks.com
Centre agréé n°11 92 18378 92