TRAPS 3.4: DEPLOIEMENT ET OPTIMISATION (EDU-285)

Présentation

Traps™ Advanced Endpoint Protection de Palo Alto Networks® permet de prévenir la prevention de l'exploitation sophistiquées de vulnérabilités ainsi que des attaques utilisant des malwares inconnus.
A la fin de cette formation de 2 jours en français, menée par un instructeur certifié, l'étudiant participant à cette formation sera à même de déployer Traps dans des grandes infrastructures, et d'en optimiser la configuration.

PROGRAMME PREVU

Mod 1 : Déploiement de Traps

- Distribution de l'agent
- Options de déploiement SSL/TLS
- Déploiement dans un contexte VDI
- Journalisation externe et intégration SIEM

Mod 2 : Dimensionnement de Traps

- Contrôle d'accès par rôle (RBAC)
- Principes de déploiements, avec options de serveurs ESM multiples
- Principes de migration

Mod 3 : Optimisation de Traps

- Optimisation de la configuration du serveur
- Définition des conditions
- Défintion de politiques optimisées
- Maintenance de bon fonctionnement

Mod 4 : Analyses post-attaques (avancé)

- Requêtes à l'agent
- Ressources pour des tests avec des maliciels
- Metasploitt
- Analyse de fichiers de vidage avec windbg

Mod 5 : Diagnostics avancés

- Architectures Endpoint Security Manager et Traps
- Scénarios de diagnostic avec dbconfig et cytool
- Diagnostic de compatibilité des applications
- Diagnostic de connectivité BITS

Objectifs du Cours

Au travers de théorie exposée par un instructeur certifié et d'exercices pratiques, les étudiants apprendront comment designer, installer, et optimiser des déploiements Traps sur les grandes infrastructures : celles avec des serveurs multiples et/ou des milliers de postes clients.
Parmi les exercices pratiques proposés, les étudiants auront l'occasion d'automatiser le déploiement de Traps, préparer les images pour les déploiements VDI, déployer des serveurs multiples, faire le design et l'implémentation de politiques personnalisées ; tester Traps avec des exploits créées par Metasploit ; et analyser des dumps d'exploitation via Windbg.

Caractéristiques du cours

• **Niveau du cours :** Intermédiaire
• **Durée du cours :** 2 jours
• **Format du cours :** Théorie présentée par un instructeur et pratique via un Lab
• **Version couverte dans le cours :** Palo Alto Networks Traps Advanced Endpoint Protection v3.4

Audience

• Ingénieurs Sécurité, Admins Systèmes, Ingénieurs support

Pré-requis

• Les étudiants doivent avoir suivi la formation Traps 281 ou la formation « PSE : Endpoint Associate »
• Des compétences d'administration Windows, et la connaissance des concepts de la sécurité en entreprise sont également requis

Vous former dans un centre de formation agréé Palo Alto Networks vous permet de vous préparer au mieux à la protection des 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

AUTHORIZED TRAINING CENTER

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