+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 27/05/2024

S'inscrire

Formation Palo Alto Traps : déploiement et optimisation

(EDU-285)

2 jours (14 heures)

Présentation

Traps™ Advanced Endpoint Protection de Palo Alto Networks® permet de prévenir la prévention del'exploitation sophistiquée de vulnérabilités ainsi que des attaques utilisant des malwares inconnus. À 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. Au travers de théorie exposée par un instructeur certifié et d'exercices pratiques, les étudiants apprendront comment désigner, 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 créés par Metasploit ; et analyser des dumps d'exploitation via Windbg. Notre formation se basera sur la dernière version de l'outil à savoir PAN-OS 10.1.

Objectifs

Installer, et optimiser des déploiements Traps sur les grandes infrastructures

Public visé

Ingénieurs Sécurité, Admins Systèmes, Ingénieur support

Prérequis

- 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

Programme de la formation Palo Alto Traps : déploiement et

optimisation

Déploiement de Traps

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

Dimensionnement de Traps

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

Optimisation de Traps

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

Analyses post-attaques (avancé)

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

Diagnostics avancés

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

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes,

souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.