Sécurité : SIEM et Veille technologique sécurité

Référence : **SECMSIEMVTS** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Bonnes connaissances réseau / système. • Maîtrise de l'administration Linux. • Notions de Scripting.

PROFIL DES STAGIAIRES

• Consultants en sécurité. • Ingénieurs / Techniciens. • Responsables techniques.

OBJECTIFS

• Apprendre à détecter les menaces parmi un grand volume d'information. • Comprendre les limites des outils de sécurité classiques. • Découvrir les principes technologiques derrière l'acronyme SIEM. • Devenir efficace dans la veille technologique. • Obtenir les clés pour monter une équipe de veille au sein d'une organisation.

CERTIFICATION PREPAREE

Aucune

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 Sécurité défensive

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 : Veille Technologique

- Enjeux de la veille technologique
- Objectifs propres à la cybersécurité
- Définition d'une vulnérabilité
- Définition de l'exploitation
- Types de mesures correctives
- Base de données CVE et score CVSS
- Sources d'information (listes de diffusion Twitter, Reddit, etc.)
- Flux RSS (Tiny Tiny RSS)
- Automatisation (Google Alerts, Zapier, Netvibes)
- Organisation d'une équipe de veille (CERT, CSIRT, ENISA)

JOUR 2

- Rôle de la détection d'intrusion
- Terminologie : Faux-positifs, détection, prévention, etc.
- Architecture et types d'IDS
- Présentation de l'IDS Suricata
- Déploiement et configuration de base
- Langage d'écriture de règles
- Journalisation via Syslog
- Ateliers : Mise en place d'une architecture IDS virtualisée : firewall, cible, attaquant - Jeu d'attaques et création de règles de détection (scans, bruteforce, exploitation de vulnérabilité)

JOUR 3

- Présentation du HIDS OSSEC et architecture
- Déploiement et configuration de base
- Syntaxe d'écriture de règles
- Atelier : Ecriture de règles
- Limites des IDS
- Intégration avec les autres composants du SI
- Points importants dans le cadre d'un appel d'offre

JOUR 4 : Défis modernes posés à la supervision classique

- Objectifs d'un SIEM
- Architecture et fonctionnalités
- Syslog et centralisation des journaux
- Synchronisation du temps (NTP)
- Présentation d'ELK
- Configuration avancée de Logstash
- Ateliers : Configuration d'agents Logstash - Ecritures de Groks avancés - Environnement hétérogène : Linux, Windows
- Visualisation des résultats dans Kibana
- Conclusion (Discussions sur les solutions alternatives - Préparation des points-clés pour un appel d'offre)

JOUR 5