Fiche du cours

Titre :

SOC500 - Threat Hunting, SIEM & Sécurité Opérationnelle

Description :

Ce cours forme les étudiants aux techniques de détection et de réponse aux incidents dans un environnement opérationnel. Il aborde la mise en place et l'exploitation d'un SIEM, la chasse aux menaces, l'analyse de logs et la corrélation d'événements. Les participants apprennent à identifier des comportements suspects, à enquêter sur des incidents en temps réel et à automatiser des alertes de sécurité. L'approche est orientée Blue Team, avec des scénarios réalistes et des exercices pratiques.

Objectifs :

- Comprendre le fonctionnement et les enjeux d'un SOC.*
- Déployer et configurer un SIEM pour collecter et corréler des événements.*
- Réaliser des activités de threat hunting et d'investigation.*
- Analyser des logs systèmes, réseau et applicatifs.*
- Mettre en place une détection et une réponse efficace aux incidents.

Chapitres :

1. Introduction aux opérations de sécurité (SOC) et Blue Team*
2. Déploiement et configuration d'un SIEM (ex. Wazuh / Splunk)*
3. Ingestion et normalisation des logs systèmes, réseaux et applicatifs*
4. Corrélation d'événements et création de règles d'alerte*
5. Threat hunting : recherche proactive de menaces*
6. Investigation en temps réel et gestion d'incidents*
7. Automatisation des réponses et playbooks de sécurité*
8. Étude de cas pratique : attaque simulée et réponse en conditions réelles

À la fin :

Vous serez capable de détecter et d'analyser des incidents de sécurité dans un environnement SOC, d'exploiter un SIEM pour corréler des événements et identifier des comportements anormaux, et de mettre en place une réponse rapide et structurée. Ce cours vous donnera une expérience pratique de la cybersécurité opérationnelle, essentielle pour des rôles d'analyste SOC, de threat hunter ou de Blue Team engineer.