

OPÉRATIONS EN CYBERSÉCURITÉ

Face à l'évolution des cybermenaces, il devient crucial pour les organisations de détecter et de réagir rapidement aux incidents de sécurité. Dans le contexte actuel des menaces, il est essentiel d'adopter une attitude proactive face à une violation. Cela signifie que, malgré des capacités de pointe pour identifier et protéger les actifs les plus critiques d'une organisation, une attention particulière doit être portée aux opérations de sécurité quotidiennes, qui permettront à l'organisation de garder une longueur d'avance et de gagner la confiance de ses clients.



Cette formation offre une compréhension complète des opérations de cybersécurité dans les environnements d'entreprise modernes. Il aborde les outils, techniques, cadres et « *workflows* » utilisés par les équipes opérationnelles de cybersécurité (SOC) afin de détecter, de gérer et de se remettre des cybermenaces. Les participants acquerront une expérience pratique des outils SIEM, des plateformes de veille sur les menaces, des processus de réponse aux incidents, et bien plus encore.

OBJECTIFS

- Comprendre la structure et les fonctions d'un centre d'opérations de sécurité (SOC).
- Utiliser des outils tels que les SIEM, les analyseurs de paquets et les systèmes de détection des terminaux.
- Identifier et analyser les incidents de cybersécurité à l'aide des journaux et des données réseau.
- Appliquer la veille sur les menaces aux décisions opérationnelles.
- Mettre en œuvre des procédures et une documentation de réponse aux incidents.
- Comprendre les enjeux réglementaires et éthiques des opérations de cybersécurité.

CONTENU

1. Introduction aux opérations de cybersécurité et aux SOC

- Présentation des opérations de sécurité en entreprise
- Rôles et responsabilités des SOC (analystes, ingénieurs, intervenants en cas d'incident)
- Introduction au cadre de cybersécurité du NIST et à MITRE ATT&CK

2. Principes fondamentaux de la surveillance et de la journalisation de la sécurité

- Importance de la collecte et de la centralisation des journaux
- Types de journaux
 - Système
 - Application
 - Pare-feu
 - IDS/IPS
- Stratégies d'analyse, de normalisation et de conservation des journaux

3. Gestion des informations et des événements de sécurité (SIEM)

- Composants et architecture SIEM
- Utilisation de plateformes telles que Splunk, ELK Stack ou QRadar
- Création de règles de corrélation et génération d'alertes

4. Analyse du trafic réseau et inspection des paquets

- Compréhension des protocoles (TCP/IP, DNS, HTTP/S)
- Utilisation d'outils tels que Wireshark, Zeek et NetFlow
- Identification des schémas malveillants dans le trafic réseau

5. Outils de détection et de réponse aux points d'extrémité (EDR)

- Concepts EDR et surveillance des points d'extrémité en temps réel
- Détection comportementale et collecte de données télémétriques
- Utilisation d'outils tels que CrowdStrike, Carbon Black ou Sysmon

6. Renseignements sur les menaces et analyse des indicateurs

- Qu'est-ce que le renseignement sur les menaces ?
- Types de renseignements
 - Stratégiques
 - Tactiques
 - Opérationnels
- Formats, flux et normes IOC (STIX/TAXII, MISP)

7. Procédures de traitement et de tri des alertes

- Techniques de gestion des alertes et de priorisation
- Procédures et guides d'escalade
- Bonnes pratiques de documentation et de communication

8. Cycle de vie de la réponse aux incidents

- Phases
 - Préparation, Détection, Confinement, Éradication, Reprise et Leçons apprises
- Rôle de la coordination et de la communication lors des incidents
- Plans de réponse aux incidents et exercices sur table

9. Fondamentaux de l'investigation numérique

- Imagerie forensique, analyse de la mémoire, examen du système de fichiers
- Chaîne de traçabilité et traitement des preuves
- Outils : FTK Imager, Volatility, Autopsy

10. Automatisation et orchestration de la sécurité (SOAR)

- Automatisation des tâches répétitives du SOC grâce à des playbooks
- Présentation des plateformes SOAR telles que Palo Alto Cortex XSOAR et Splunk Phantom
- Scripting de workflows de réponse aux incidents avec Python

11. Gestion des vulnérabilités et recherche des menaces

- Outils d'analyse des vulnérabilités
 - Nessus
 - OpenVAS
- Processus de gestion des correctifs
- Recherche proactive des menaces à l'aide d'approches basées sur des hypothèses

12. Considérations relatives à la conformité, aux lois et à la réglementation

- Présentation des lois
 - RGPD
 - HIPAA
 - Norme PCI-DSS
- Aspects juridiques liés à la réponse aux incidents et à l'investigation numérique
- Obligations en matière de conservation des données, de confidentialité et de notification des violations

13. Opérationnalisation de la veille sur les menaces

- Enrichissement des alertes SIEM avec la veille sur les menaces
- Cartographie TTP vers MITRE ATT&CK
- Utilisation des plateformes de veille sur les menaces (TIP) au sein du SOC