SOC ANALYST

Durée : 3 à 5 jours

Objectifs de la Formation

- Comprendre le rôle et les responsabilités d'un analyste SOC.
- Comprendre les techniques d'analyse de logs et de traçabilité pour l'investigation.
- Comprendre les étapes de réponse aux incidents, de la détection à la remédiation.
- Identifier les indicateurs de compromission et les événements sur les réseaux et systèmes.
- Utiliser les outils SIEM, IDS/IPS, firewalls pour la détection et prévention des attaques.
- Rester informé des dernières menaces via la veille sécurité (CTI).

Public Concerné

- Consultant en cybersécurité
- Administrateur système
- Analyste SOC junior
- Ingénieur en informatique

Prérequis

- Bases en sécurité de l'information
- Fonctionnement d'un système Windows et/ou Linux
- Maîtrise du langage shell

Programme de la Formation

Etat de l'art de la défense du SI

- Introduction · Terminologie · Les différents types de SOC
- La défense en profondeur · Prioriser sa défense
- La cyber Kill Chain · Framework MITRE ATT&CK
- Focus sur le métier d'analyste SOC

Prévention des menaces

- Exploitation du CTI pour une défense proactive
- Threat Intelligence et Cyber Threat Intelligence · Concepts de l'intelligence
- Outils : OpenCTI, MISP, Threat Quotient, ElecticIQ, OpenTAXII
  Threat Hunting · Gestion des Vulnérabilités

L'art de l'analyse du flux réseau

- Introduction à l'analyse réseau
- Analyse de trafic avec WireShark · Présentation de l'analyse des PCAPs
  Utilisation stratégique de Snort

Approfondissement des analyses systèmes

- Introduction à l'analyse systèmes · Sources de données
- Analyse comportementale (UBA) · La suite SysInternals
- OsQuery : Advanced System State Exploration

Technologies SIEM

- SIEM / CIM · La corrélation des données au coeur des SIEMs
- Exploiter Splunk : stratégies et insights pour la sécurité réseau
  Exploration de la Suite ELK (Logstash, ElasticSearch, Kibana) · Meilleures pratiques

Optimisation de l'alerting et de l'automatisation

- Contextualisation et priorisation des alertes · La détection
- Optimisation de la détection avec les règles SIGMA
- Utilisation d'ElastAlert pour renforcer l'alerting dans ELK · Splunk Alerting

Evaluation de l'efficacité des systèmes de détection

- Importance des tests réguliers · Différentes approches de testing
- Analyse et documentation des résultats · Plan d'action · Quelques outils de tests

Gestion des incidents et analyse forensique

- Réponse aux incidents · Principes fondamentaux de l'analyse forensique
- Analyse des e-mails

Moyens Techniques et Humains

- Intervenant : Formateur professionnel spécialisé dans la continuité d'activité.
- Utilisation d'outils pédagogiques adaptés.

Méthodes Pédagogiques Mobilisées

- Alternance entre méthodes affirmatives, interrogatives et actives.
- Utilisation de ressources formatives, évaluatives et de mémorisation.

Évaluation

- **Tests intermédiaires :** Evaluations régulières tout au long de la formation
- **Projet pratique :** Simulation d'un environnement réel de cybersécurité
- **Examen final :** Questions théoriques et exercices pratiques