KIN TRAINING · FORMATION & CERTIFICATION

Analyste SOC : détection et réponse aux incidents

Détectez, qualifiez et traitez les incidents de sécurité au sein d'un SOC.

CY-SOC | Intermédiaire | Formation

Description

Cette formation prépare aux missions quotidiennes de l'analyste SOC (niveau 1/2) : compréhension des menaces, exploitation d'un SIEM, analyse de logs, qualification des alertes, investigation et réponse aux incidents. Les travaux pratiques s'appuient sur des scénarios d'attaque réalistes et le référentiel MITRE ATT&CK.

Informations

Durée
3 jours

Domaine
Cybersécurité

Formats
Présentiel, Distanciel, Blended

Langue
Français

Objectifs

- Comprendre l'organisation d'un SOC et le cycle de vie d'un incident
- Exploiter un SIEM : collecte, corrélation, règles de détection
- Analyser des logs et qualifier des alertes
- Conduire une investigation et coordonner la réponse à incident

Prérequis

- Connaissances en réseaux et systèmes
- Notions de sécurité des SI

Public visé

- Analystes SOC débutants
- Administrateurs sécurité et systèmes
- Techniciens souhaitant évoluer vers la détection

Programme détaillé

01. Le SOC et les menaces

- Organisation, niveaux et missions du SOC
- Cyber kill chain et MITRE ATT&CK
- Sources de données et journaux

02. SIEM et détection

- Architecture et fonctionnement d'un SIEM
- Cas d'usage et règles de corrélation
- Réduction des faux positifs

03. Analyse et investigation

- Analyse de logs système, réseau et applicatifs
- Qualifier et prioriser une alerte
- Investigation et recherche d'indicateurs de compromission

04. Réponse à incident

- Processus de réponse et confinement
- Communication et escalade
- Post-mortem et amélioration continue