CYB201 - Détection et remédiation d'attaques

Mis à jour le 25-09-2026

Code : CYB201

Unité d'enseignement de type mixte

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale : EPN05 - Informatique / Vania CONAN

Contact national :

EPN05- Informatique

2 rue Conté
33.1.14A
75003 Paris

Sanaz MANSOURI
sanaz.mansouri@lecnam.net

Présentation

Prérequis

bases des réseaux IP (RSX101), urbanisation services en réseau (RSX103), sécurité des réseaux (RSX112), virtualisation (SMB111)

Objectifs pédagogiques

Cette formation vise dans un premier temps à donner des éléments de compréhension des principes de détection des attaques, puis à fournir des éléments concrets concernant la mise en place des logiciels de détection et de définir les stratégies de réponses aux incidents. La formation fournit les méthodes et les outils pour définir et implémenter des stratégies efficaces de protection et de réponses aux incidents de sécurité.

Compétences

Compétences acquises :

- Comprendre les enjeux de la détection d'une attaque
- Connaître les avantages et limites des différents algorithmes de détection
- Connaître les stratégies de réponses aux incidents
- Identifier les éléments à mettre en place dans un SOC
- Savoir mettre en œuvre des SIEM, EDS, IDS

Savoirs :

- Mettre en œuvre ELASTIC Endpoint Security, Snort, ZEEK, SURICATA, Bro

Programme

Contenu

Cet enseignement prépare l'auditeur à détecter et à répondre aux différents types d'attaques de sécurité informatique.

Ce cours débute par la présentation des différentes menaces auxquelles est exposé un système d'information, pose les bases méthodologiques de l'analyse en partant d'un modèle de chaîne d'attaque (Cyber Kill Chain). Le cours présente ensuite les différentes approches de détection des attaques, par signature ou par détection d'anomalies ainsi que différentes familles d'algorithmes associés. Le cours conclut avec les stratégies complètes de détection et de réponse aux incidents dans les réseaux et les environnements virtualisés.

Les principaux sujets traités sont :

Principes

Présentation de la menace, des canaux de contrôle, du profil d'une Attaque

Principe d'une chaîne d'attaques (Cyber Kill Chain)

Principes de détection d'attaques

Systèmes Experts de détection par règles, par signature (Snort et Bro) et détection d'abus et d'anomalies

Approches supervisées pour la détection d'attaque

Application des réseaux de neurones

Apprentissage machine (GNN – Graph Neural Networks)

Machines à vecteurs de support (SVM – Support Vector Machine)

Règles d'association

Méthodes ensemblistes

Approches non-supervisées pour la détection d’attaque

Détection de changement

Approches statistiques

Techniques de clustering

Détecteurs hybrides

Techniques de remédiation d'attaque

Le SOC (Security Operation Center)

Les SOAR (Security Orchestration, Automation and Response)

Les SIEM (Security Information and Event Management) : gestion de l’information des événements de sécurité

Les EDR (Endpoint Detection and Response) : détection et blocage des attaques

Les IDS (Intrusion Detection System)

Techniques d’analyse comportementale (UBA)

Modalités de validation

- Contrôle continu
- Examen final

Description des modalités de validation

Contrôle continu et examen final.