USCB14 - Détection des attaques

Mis à jour le 22-04-2022

Code : USCB14

Unité spécifique de type mixte

4 crédits

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

Cnam Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
bzh_master_cybersecurite@lecnam.

Présentation

Prérequis

UTC505, RSX101, RSX112

Objectifs pédagogiques

Description :

Cet enseignement prépare l'auditeur à détecter les intrusions et les attaques. Ce cours présente les canaux de contrôles de malwares les plus répandus, pose les bases de l'analyse d'un trafic réseau puis présente différentes approches de détection, par signature ou par détection d'anomalies ainsi que les architectures et outils de détections.

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.

Compétences

Compétences acquises :

- Comprendre les enjeux de la détection d'une attaque
- Connaître les avantages et limites des différents algorithmes de détection
- 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, Snort, Bro

Programme

Contenu

- Présentation de la menace
  - Canaux de contrôle
  - Profil d'une Attaque
  - TTP et IoC
- Cyber Kill Chain
- Principes de détection d'attaques
  - Systèmes Experts
    - Systèmes experts de détection par règles ou par signatures (Snort et Bro)
    - Détection d'abus
    - Détection d'anomalies
  - Approches supervisées et semi-supervisées
    - Réseaux de neurones
    - SVM
    - Règles d'association
    - Méthodes ensemblistes
  - Approches non-supervisées
    - Détection de changement
    - Approches statistiques
    - Techniques de clustering
  - Détecteurs hybrides
- Détection d'attaque dans un SI
  - Le SOC (Security Operation Center)
  - Fonctions d'un SOC
  - Les SOAR (Security Orchestration, Automation and Response)

- Outils de détections
  - 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)
  - Outils d’analyse comportementale (UBA)

Modalités de validation

- Contrôle continu
- Projet(s)
- Mémoire

Description des modalités de validation

Examen – Contrôle continu - projet