le cnam
Nouvelle-Aquitaine

Fiche récapitulative

CYB201 | Détection et remédiation d'attaques

Mise à jour le 29/04/2026

50
Total d'heures d'enseignement

6
Crédits ECTS

Date non définie
Début des cours prévu

Programme

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)

Objectifs : aptitudes et compétences

Objectifs :

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 oeuvre des SIEM, EDS, IDS

Savoirs :

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

Prérequis

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

Délais d'accès

Le délai d'accès à la formation correspond à la durée entre votre inscription et la date du premier cours de votre formation.

- UE du 1er semestre et UE annuelle : inscription entre mai et octobre
- UE du 2e semestre : inscription de mai jusqu'à mi-mars

Exemple : Je m'inscris le 21 juin à FPG003 (Projet personnel et professionnel : auto-orientation pédagogique). Le premier cours a lieu le 21 octobre. Le délai d'accès est donc de 4 mois.

Modalités

Modalités pédagogiques :

Pédagogie qui combine apports académiques, études de cas basées sur des pratiques professionnelles et expérience des élèves. Équipe pédagogique constituée pour partie de professionnels. Un espace numérique de formation (ENF) est utilisé tout au long du cursus.

Modalités de validation :

Contrôle continu et examen final.
Les centres de présentation des examens sont Angoulême, Bordeaux, Dax, Limoges, Niort, Pau et Poitiers.

Tarif

Plusieurs dispositifs de financement sont possibles en fonction de votre statut et peuvent financer jusqu'à 100% de votre formation.

Salarié : Faites financer votre formation par votre employeur

Demandeur d'emploi : Faites financer votre formation par Pôle emploi

Votre formation est éligible au CPF ? Financez-la avec votre CPF

Si aucun dispositif de financement ne peut être mobilisé, nous proposons à l'élève une prise en charge partielle de la Région Nouvelle-Aquitaine avec un reste à charge. Ce reste à charge correspond au tarif réduit et est à destination des salariés ou demandeurs d'emploi.

Pour plus de renseignements, consultez la page Financer mon projet formationopen_in_new ou contactez nos conseillers pour vous accompagner pas à pas dans vos démarches.

Passerelles : lien entre certifications

- CYC9106A - Diplôme d'ingénieur Cybersécurité

Taux de réussite

Les dernières informations concernant le taux de réussite des unités dcenseignement composant les diplômes

↓ Taux de réussite