# Fiche du cours

**50 h**

**Titre :**

SEC150 - Programmation Python pour la Cybersécurité

**Description :**

Introduction pratique à Python appliquée au domaine de la cybersécurité. Ce cours enseigne aux étudiants à automatiser des tâches courantes de sécurité, analyser des logs, effectuer des scans réseau simples et créer de petits outils internes utiles aux équipes Blue Team, Red Team et DevSecOps.
On y aborde les bases du langage dans un contexte sécurité, la manipulation de fichiers sensibles, l'automatisation via sockets et API, ainsi que l'intégration des scripts dans des environnements opérationnels. Le cours met l'accent sur la simplicité, la rigueur et les bonnes pratiques nécessaires pour produire des scripts exploitables et sécurisés.

**Objectifs :**

- Comprendre les bases de Python dans un contexte cybersécurité.*
- Automatiser des tâches courantes : scans, parsing de logs, collecte d'informations.*
- Écrire des scripts simples et sécurisés pour la surveillance ou la détection.*
- Manipuler les flux réseau et les données issues de systèmes SIEM/API.*
- Intégrer des outils dans un environnement SOC, pentest ou cloud.*
- Acquérir de bonnes pratiques de code (gestion des erreurs, logs, formatage).

**Chapitres :**

1. Introduction au langage Python dans un contexte sécurité*
2. Lecture et parsing de fichiers de logs, JSON et CSV*
3. Sockets et réseau : port scanning et surveillance basique*
4. Automatisation via API et requêtes HTTP*
5. Manipulation de données en temps réel (alerte et reporting)*
6. Librairies utiles en cybersécurité (Scapy, Requests, logging)*
7. Sécurisation des scripts : exceptions, droits, journalisation*
8. Mini-projets : port scanner, log parser, bot d'alerte*
9. Capstone : développement d'un outil automatisé de détection ou d'analyse

**À la fin :**

Vous saurez écrire et structurer des scripts Python dédiés à la cybersécurité, automatiser des tâches d’analyse et de surveillance, manipuler des flux réseau ou des données de logs, et intégrer vos outils dans un environnement opérationnel. Vous aurez acquis des réflexes de développement sécurisés (gestion d’erreurs, logs, bonnes pratiques) et serez capable de produire des scripts exploitables par une équipe SOC ou pentest. Ce cours constitue une base indispensable avant d’aborder les modules avancés de sécurité réseau, pentest ou DevSecOps.