MENTION CYBERSECURITE

DOCUMENT DE PRÉSENTATION GÉNÉRALE

Diplomation autour de 8 dominantes

Energie	Vivant-Santé Environnement	Mathématiques et Data Sciences	Systèmes communicants et Objets connectés
Informatique et Numérique	Grands Systèmes en interaction	Construction, Ville, Transport	Physique et Nanotechnologies

La dominante informatique et numérique se décline en 4 mentions

Gif

Systèmes

Cybersécurité

Rennes

Gif

Intelligence Artificielle

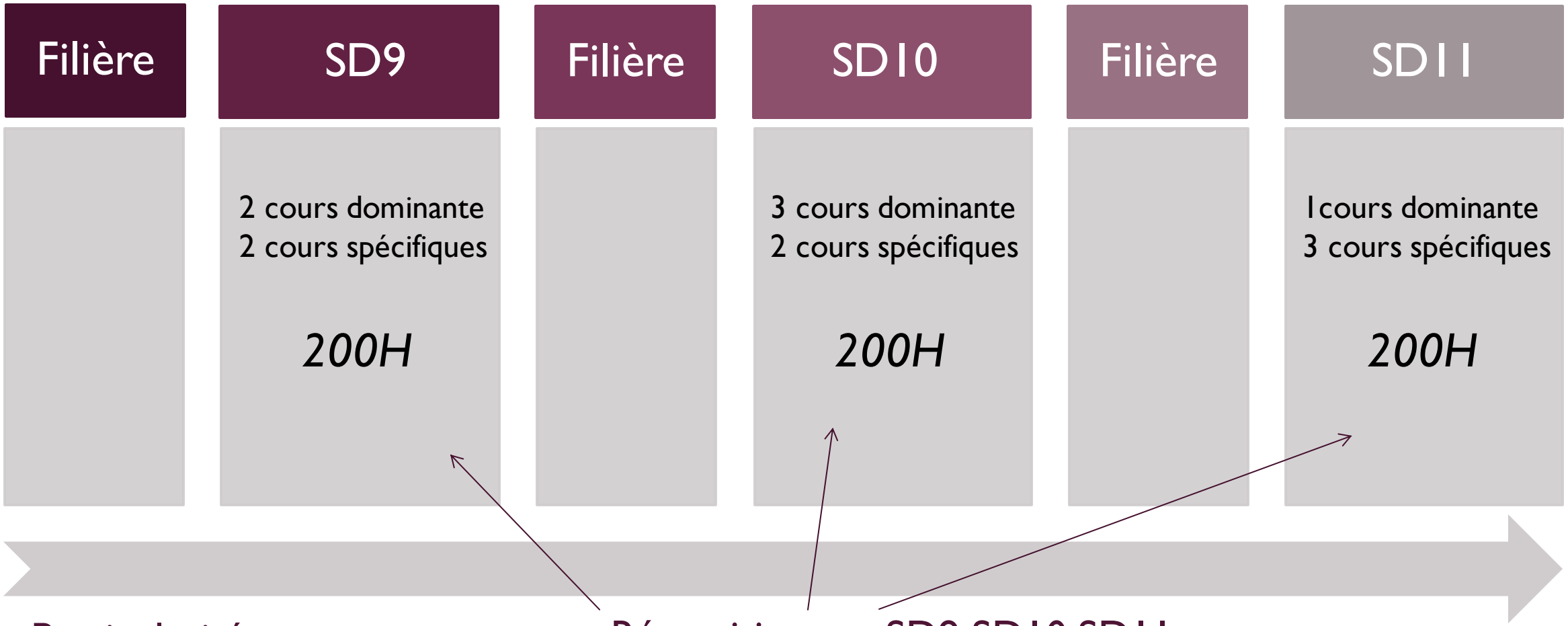
Science du Logiciel

Gif

Mention Cybersecurité

200 h: domaines **transverses** aux 4 mentions de la dominante informatique
400 h: domaines **spécifiques** à la mention Cyber
+ compatibilité Master de Sciences Informatique (SIF - Univ. Rennes, ENS, ...)
+ compatibilité Master Administration des Entreprises (IGR - à confirmer)

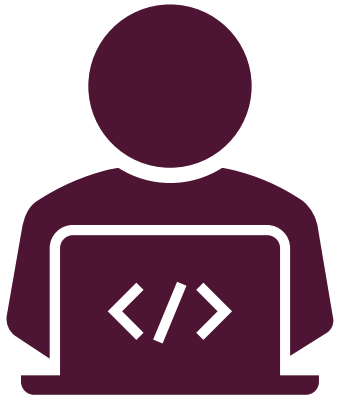
3 périodes de 9 semaines séparées par des périodes filières



Particularité Rennaise:

Répartition sur SD9 SD10 SD11

Cours de dominante **et** spécifique mention Cyber



GitLab

Jenkins

SD9

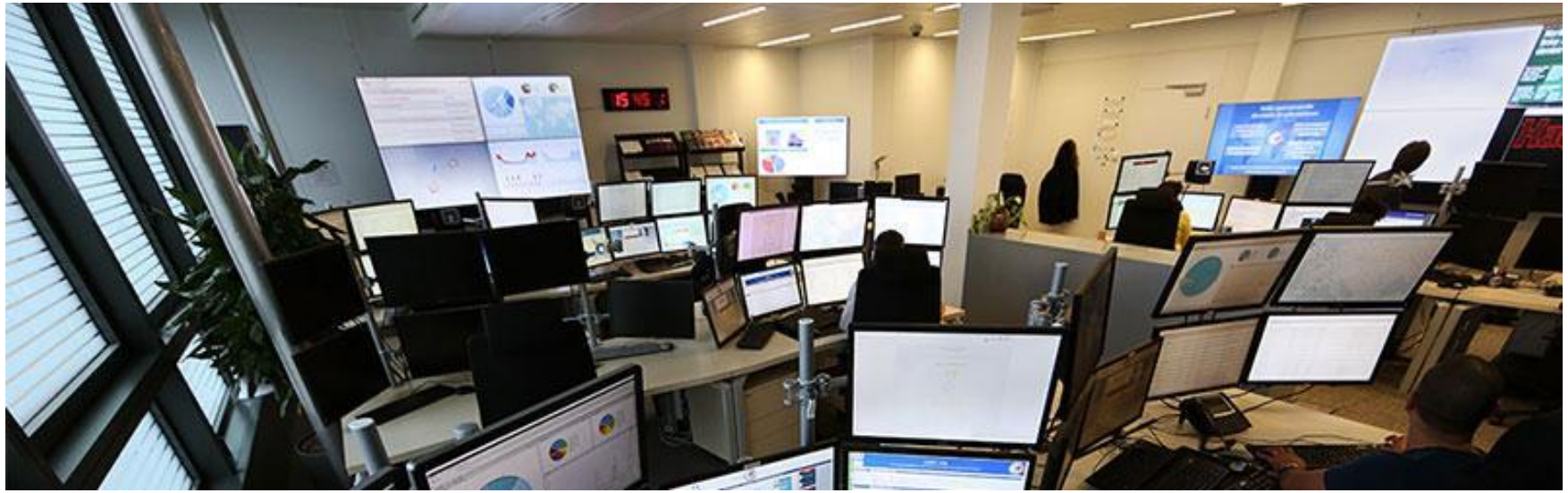
Cours de dominante

PROGRAMMATION ET OUTILS DE DÉVELOPPEMENT (60HEE/36HPE)

Consolider et approfondir les compétences en langages de programmation (30H – langage retenu C++ ou Java mais concepts universels) et méthodes de développement (6H - Intégration continue, Tests, Méthodes agiles).

Les interactions avec un système d'exploitation seront abordées entre autres par la programmation multitâche et la gestion de la mémoire.

SD9



Le centre de Cyberdéfense de l'ANSSI

Cours spécifique
Commun master SIF

DÉTECTION D'INTRUSION (60HEE/36HPE)

Le but du cours est de découvrir et pratiquer les différentes approches pour surveiller la sécurité des systèmes d'information.

Approches de détection présentées: signature et détection d'anomalie.

Le cours approfondit la corrélation d'alertes et les travaux de recherche récents du domaine.

SD9

Cours spécifique

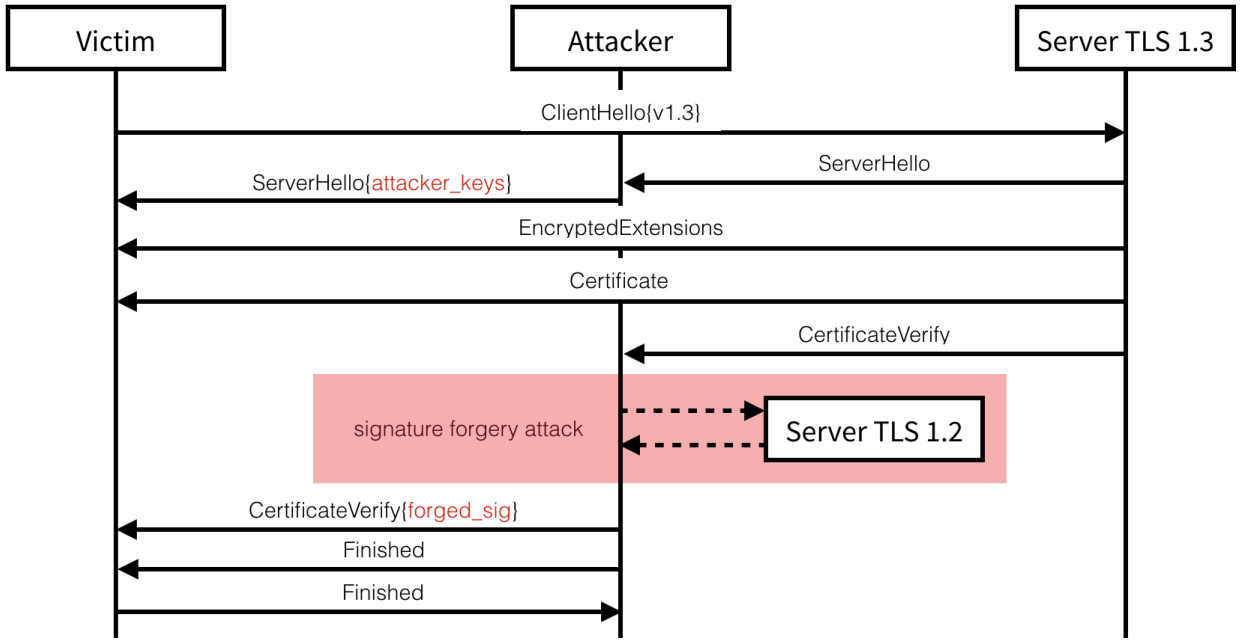
PROTECTION DES CONTENUS ET VIE PRIVÉE (30HEE/18HPE)

SD9

Cours de dominante

DROIT, ÉTHIQUE ET VIE PRIVÉE (20HEE/12HPE)

L'objectif de ce cours est de fournir aux futurs ingénieurs les éléments juridiques et philosophiques nécessaires à des experts responsables du numérique. Seront notamment abordées la protection des données personnelles et les responsabilités des opérateurs de services essentiels.



SD9+

SD10

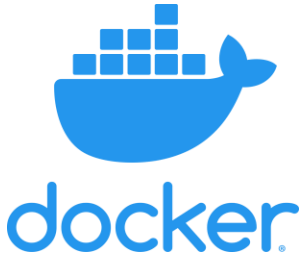
Cours spécifique

CRYPTOGRAPHIE I ET II (30+30HEE/36HPE)

Primitives cryptographiques: AES, RSA, SHA,

Protocole cryptographiques: TLS

SD10



Cours de dominante

SYSTÈMES D'EXPLOITATION (40HEE/24HPE)

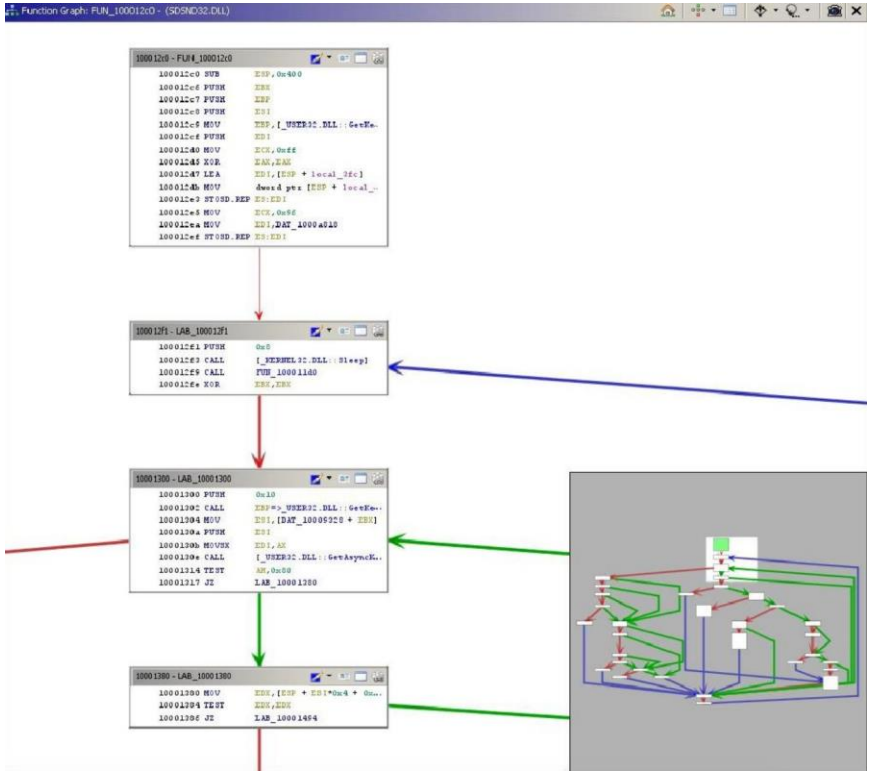
L'objectif de ce cours est de présenter ce qu'est un système d'exploitation, comment il gère l'ordonnancement des tâches, les processeurs multicœurs, la synchronisation entre processus et threads, la mémoire virtuelle et l'isolation entre processus. Ces fondamentaux sont nécessaires pour comprendre la classe des attaques en mémoire abordée dans un cours suivant, ainsi que les techniques de protection mises en place par les systèmes d'exploitation afin de s'en prémunir.

SD10

Cours de dominante

SYSTÈMES CONCURRENTS ET RÉPARTIS (40HEE/24HPE)

L'objectif de ce cours est de traiter les calculs distribués, les problèmes de concurrence et de consensus distribués, traités dans le domaine des systèmes répartis.
Dans le cadre de ces systèmes, il sera entre autres abordé comment réaliser des calculs sur des données massives.



SD10

Cours spécifique

RÉTROINGÉNIERIE, VIROLOGIE (40HEE/24HPE)

Ce cours permet de découvrir les logiciels malveillants et les techniques d'analyse et de rétroingénierie de tels codes binaires.

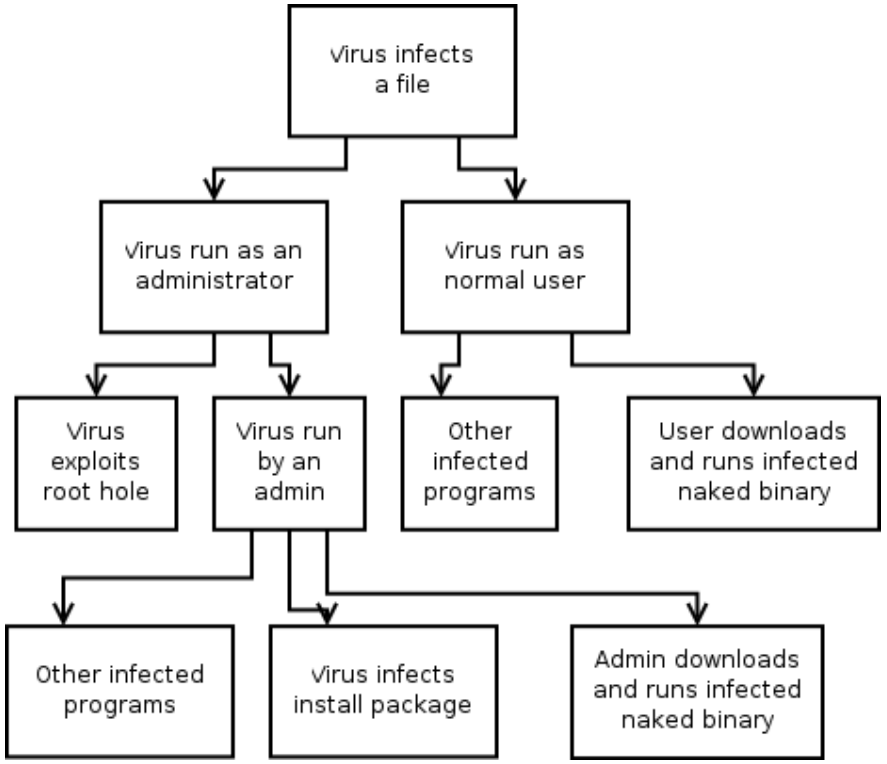
Compétence visée: savoir analyser dans IDA Pro ou Ghidra un logiciel malveillant.

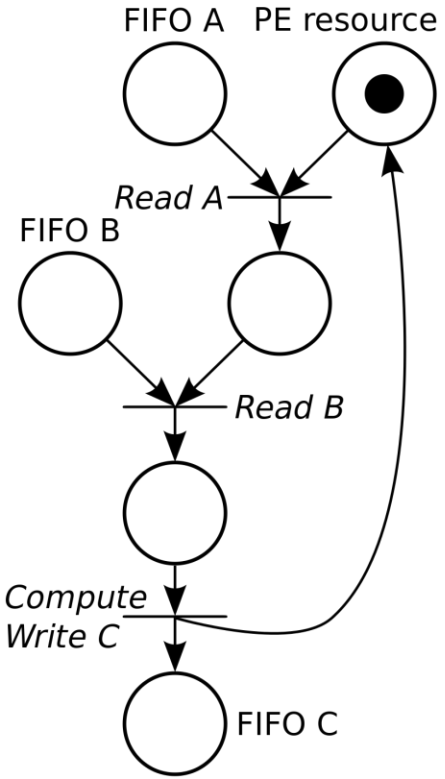
SD10

Cours spécifique

ATTAQUES EN MÉMOIRE (1 ET 2) (30HEE/18HPE)

Ce cours s'intéresse aux mécanismes de protection de la mémoire (W+X, randomisation de l'espace d'adressage, canaries, *shadow stack*) et à l'étude des attaques en mémoire. Cette classe d'attaque recourt à un ensemble de techniques d'exploitation des vulnérabilités introduites par les erreurs de gestion de la mémoire que l'on trouve communément dans les applications développées dans les langages bas niveau (C, C++). Les techniques modernes comme le Return Oriented Programming (ROP) sont présentées.





SDII

Cours de dominante

MODÉLISATION DES RISQUES ET DES ATTAQUES (20HEE/12HPE)

Comprendre et expliquer une attaque informatique est un travail difficile qui nécessite de se munir d'outils permettant de formaliser la description des actions de l'attaquant. Divers modèles de description seront abordés (arbres d'attaques, réseaux de Pétri, chaînes de Markov…)

SDII

Cours spécifique

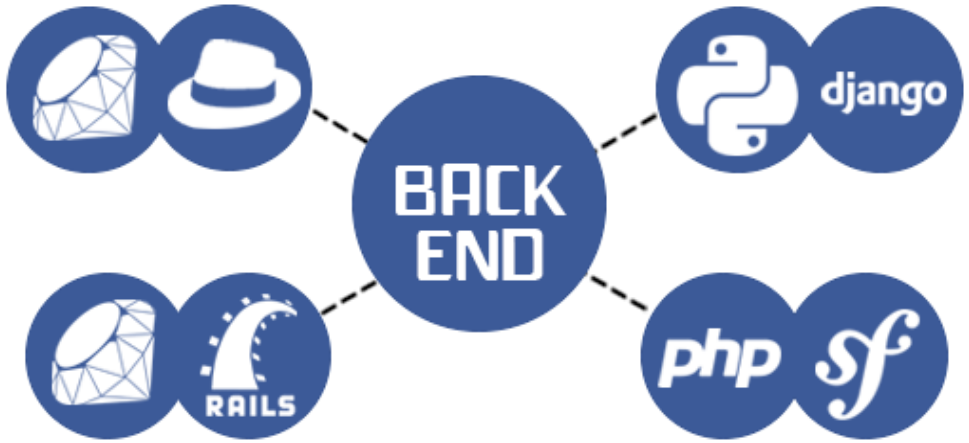
SÉCURITÉ DES SYSTÈMES D'EXPLOITATION (60HEE/36HPE)

Ce cours présente les mécanismes d'isolation, d'intégrité, de contrôle d'accès d'un système d'exploitation moderne.

Un focus particulier sera fait sur les OS GNU/Linux et Windows et les technologies associées comme par exemple Docker, SELinux.

Technologies étudiées: Kerberos, LDAP, Active Directory, LUKS, Bitlocker, SSH.

SDII



Cours spécifique

DÉVELOPPEMENT ET SÉCURITÉ WEB (60HEE/36HPE)

Ce cours traite d'une manière transverse des fondements du développement web: langages côté navigateur (HTML, CSS, Javascript), côté serveur (Java, PHP, Javascript). Quelques frameworks de développement sont présentés à titre d'illustration.

L'enseignement de la sécurité est réalisée de manière pratique sous la forme d'exercices dans une plate-forme vulnérable.

SDII

Cours spécifique

AUDIT PENTEST (60HEE/36HPE)

Ce cours présente les principes et la pratique de l'audit de test d'intrusion.

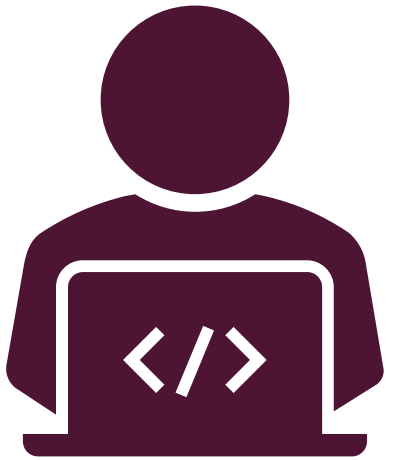
Il s'agit de mettre en pratique les techniques de découverte et d'exploitation de vulnérabilités dans des systèmes d'information et systèmes d'exploitation. Les aspects méthodologiques sont aussi abordés.

Ingénierie logicielle

Architecte sécurité

Recherche & Développement

Conseil et audit



Profils cibles de sortie

Gouvernance en sécurité

Partenaires