MENTION CYBERSECURITE

DOCUMENT DE PRÉSENTATION GÉNÉRALE

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)

Spécifique Rennes: répartition sur SD9 SD10 SD11:
Cours de dominante **et** spécifique mention Cyber

Cours de dominante

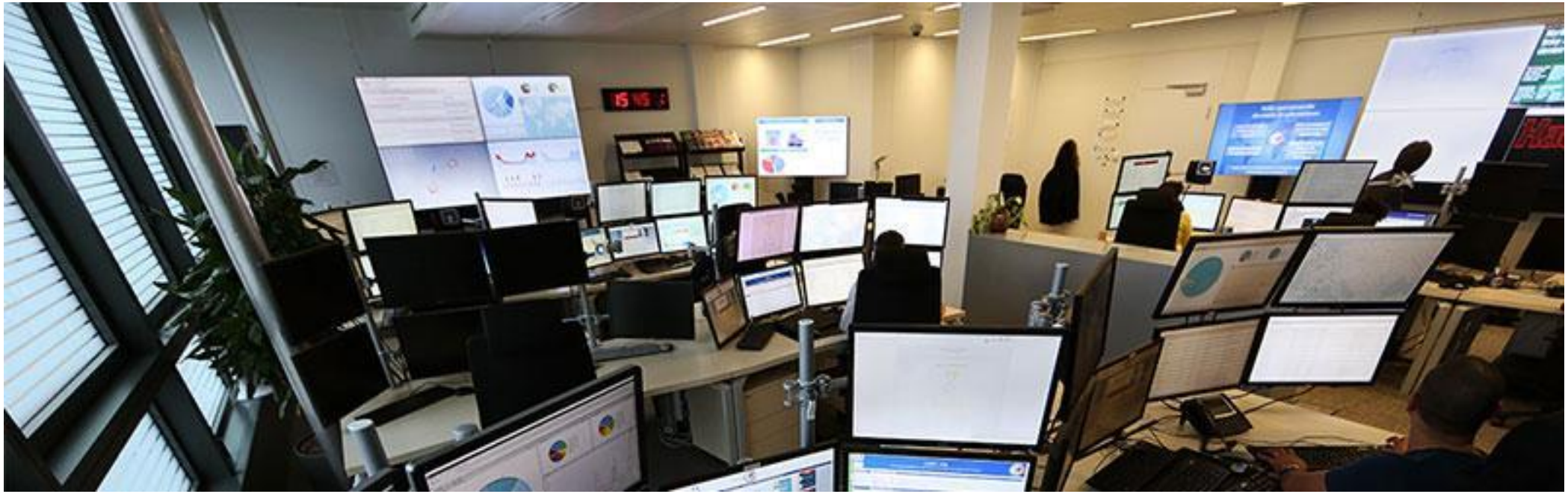
SYSTÈMES CONCURRENTS ET RÉPARTIS
(40HEE/24HPE)

SYSTÈMES D'EXPLOITATION
(40HEE/24HPE)

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

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

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



Le centre de Cyberdéfense de l'ANSSI

DÉTECTION D'INTRUSION (60HEE/36HPE - AVEC MASTER SIF)

Le but du cours est de découvrir et pratiquer les différentes approches pour surveiller la sécurité des systèmes d'information (signature et détection d'anomalie). Le cours approfondit la corrélation d'alertes et les travaux de recherche récents du domaine.

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

Le cours de protection des contenus s'intéresse aux méthodes permettant de tracer des objets digitaux et au protocoles permettant de préserver la vie privée des utilisateurs.

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.

CRYPTOGRAPHIE 1 ET II (30+30HEE/36HPE)

Primitives cryptographiques: AES, RSA, SHA,

Protocole cryptographiques: TLS

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.

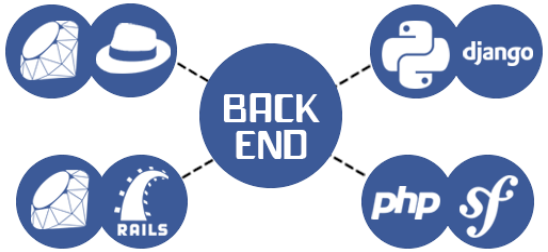
INTRO AUX ATTAQUES EN MÉMOIRE (30HEE/18HPE)

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.

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.



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.

Ingénierie logicielle

Architecte sécurité

Recherche & Développement

Conseil et audit

Profils cibles de sortie

Gouvernance en sécurité