Description du module, disponible en: FR

Cyber Security

Informations générales

Nombre de crédits ECTS

3

Code du module

TSM_CyberSec

Valable pour l'année académique

2026-27

Dernière modification

2025-10-14

Coordinateur/coordinatrice du module

Michael Mäder (HES-SO, michael.maeder@hefr.ch)

Explications concernant les langues d'enseignement par site :

- L'enseignement est dispensé dans la langue indiquée ci-dessous pour chaque site et chaque exécution du module.
- Les supports de cours sont disponibles dans les langues indiquées ci-dessous pour chaque site et chaque exécution du module. Lorsque plusieurs langues sont utilisées, la proportion de contenu disponible dans chaque langue est précisée (100 % = ensemble des supports de cours).
- Les examens (questions et réponses) sont entièrement rédigés dans la langue indiquée ci-dessous pour le site et l'exécution du module concernés. Ils se déroulent en présentiel.

	Lausanne			Lugano	Zurich		
Leçons		**X** F 100%					
Documentation		**X** F 20%	**X** E 80%				
Examen		**X** F 100%					

Catégorie de module

TSM approfondissement technico-scientifique

Leçons

2 leçons et 1 leçon de pratique par semaine

Compétences préalables

Connaissances préalables, compétences initiales

- Notions de base de la cryptographie
- Connaissance d'au moins un langage de programmation, tel que Python

Brève description du contenu et des objectifs

Le cours transmettra d'abord les connaissances de base nécessaires dans le domaine de la sécurité informatique telles que le principe de CID (confidentialité, intégrité, disponibilité), ainsi que la sécurité et sureté des données.

Le module approfondira cette base pour permettre à l'étudiant-e d'avoir une vue d'ensemble complète sur la façon d'identifier et de répertorier les menaces et les risques. Ensuite, l'étudiant-e sera en mesure de proposer et de mettre en œuvre une liste de mécanismes d'atténuation. Ce cours sera appliqué dans trois domaines de la sécurité : le développement sécurisé de logiciels, la sécurité des logiciels et la sécurité du Web basée sur des outils.

Le cours couvre les thèmes principaux suivants :

- Rappel des connaissances de base sur la sécurité.
- Développement de manière sécurisée (DevSecOps)
- Sécurité des logiciels
- Sécurité du Web
- Cyber Threat Intelligence
- Deception techniques
- Social engineering

Objectifs, contenus, méthodes

Objectifs d'apprentissage, compétences à acquérir

- Comprendre et être capable de choisir la ou les primitives cryptographiques appropriées.
- Identifier et répertorier les menaces et les risques d'un système et proposer différents types de mécanismes d'atténuation.
- Comprendre, appliquer et utiliser des processus et des outils pour un développement sécurisé.
- Comprendre et identifier les vulnérabilités des logiciels et des applications Web, puis proposer des mesures d'atténuation.

Contenu des modules avec pondération du contenu des cours

Notions de base (20%) :

- Confidentialité, intégrité, disponibilité, authenticité, autorisation, comptabilité.
- Modèle de menace, malwares, etc.
- Protection des données RGDP/nLPD
- Protection des données et techniques d'obfuscation des données (pseudonymisation, anonymisation) en lien avec RGDP/nLPD
- Intrusion Detection et SIEM (Security Information & Event Management)
- Analyse des risques et des menaces et normes

Développement sécurisé (40 %) :

- SDLC : principes fondamentaux de DevOps et comment les équipes DevOps peuvent créer et livrer des logiciels sécurisés.
- DevSecOps : comment intégrer la sécurité dans la livraison et le déploiement continus.
- Les outils, les modèles et les techniques d'automatisation de la sécurité dans DevOps.

Sécurité des logiciels (20 %) :

- Identification des vulnérabilités logicielles (SANS Top 25)
- Techniques et outils d'exploitation des logiciels
- Protections et atténuations des logiciels

Sécurité des applications Web (20%) :

- Vulnérabilités du Web (OWASP top 10)
- Techniques et outils d'exploitation du Web
- Protections et mesures d'atténuation pour le Web

Méthodes d'enseignement et d'apprentissage

Ce cours comprend des présentations théoriques et des exercices pratiques (labos).

Bibliographie

Les diapositives des cours, les références aux ressources Internet et aux livres sont mentionnées lors de l'introduction au module et tout au long du semestre.

Evaluation

Évaluation supplémentaire pendant le semestre

Le module comprend une ou des évaluation(s) supplémentaire(s) pendant le semestre. La note obtenue pour la ou les évaluation(s) supplémentaire(s) est valable à la fois pour l'examen final et pour l'examen de répétition.

Description de l'évaluation supplémentaire pendant le semestre

Travaux pratiques (TP) seront réalisés tout au long du semestre. Ces TP seront évalués et représenteront 30% de la note finale.

Principe pour les examens

En règle générale, tous les examens réguliers de fin de module se déroulent sous forme écrite. Concernant les examens de répétition, leur format (écrit ou oral) sera communiqué par l'enseignant-e en même temps que le calendrier des examens.

Examen de fin de module régulier et examen écrit de répétition

Type de l'examen

Examen écrit

Durée de l'examen

120 minutes

Aides autorisées

Les aides suivantes sont autorisées:

Aides électroniques autorisées

- Résumé personnel (nombre de pages limité)
- Pas de PC / Internet

Autres aides autorisées

Aucune autre aide autorisée

Exception : En cas d'examen électronique sur Moodle, des modifications des aides autorisées peuvent survenir. Dans ce cas, les aides autorisées seront annoncées par les enseignant-e-s avant l'examen.

Cas spécial: examen de répétition oral

Type de l'examen

Examen oral

Durée de l'examen

30 minutes

Aides autorisées

Sans aides