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

2023-24

Dernière modification

2022-10-11

Coordinateur/coordinatrice du module

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

Explication des définitions de langue par lieu :

- Les cours se dérouleront dans la langue définie ci-dessous par lieu/exécution.
- Les documents sont disponibles dans les langues définies ci-dessous. Pour le multilinguisme, voir la répartition en pourcentage (100% = documents complets)
- L'examen est disponible à 100% dans chaque langue sélectionnée pour chaque lieu/exécution.

	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, Java.

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

Objectifs, contenus, méthodes

Objectifs d'apprentissage, compétences à acquérir

- Comprendre et 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 et RGDP
- Analyse des risques et des menaces et normes

Développement sécurisé (35 %) :

- 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 (25%) :

- 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

Conditions d'admission

Le module n'utilise pas de conditions d'admission.

Principe pour les examens

En règle générale, tous les examens de fin de module réguliers et les examens de rattrapage sont organisés sous la forme écrite

Examen de fin de module régulier et examen écrit de répétition

Type de l'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

Cas spécial: examen de répétition oral

Type de l'examen

oral

Durée de l'examen

30 minutes

Aides autorisées

Sans aides