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

2021-2022 DRAFT

Dernière modification

2021-03-19

Coordinateur/coordinatrice du module

Sylvain Pasini (HES-SO, sylvain.pasini@heig-vd.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.

	Berne	Lausanne		Lugano	Zurich		
Leçons			**X** F 100%					
Documentation			**X** F 70%	**X** E 30%				
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

- Cryptography basics
- Knowledge of at least one programming language, such as C, Python, Java

Brève description du contenu et des objectifs

The course will first give the necessary background knowledge in the field of cybersecurity such as CIA and availability as well as data security.

Thereby, the module will define a threat and risk assessment accompanied with main security standards and General Data Protection Regulation (GDPR).

Based on that, it will go in deep to permit the student to have a complete overview how identify and list threats and risks. Then, the student will be able to propose and implement a list of mitigation mechanisms. This will be applied in three security fields: software development, software security and web security based on tools.

The course covers the following core topics:

- Reminder of basic knowledge about security
- Security development
- Software security
- Web security

Objectifs, contenus, méthodes

Objectifs d'apprentissage, compétences à acquérir

- Understand and choose the appropriate cryptographic primitive(s)
- Identify and list the threats and risks of a system and propose different kind of mitigation mechanisms
- Understand, apply and use processes and tools towards secure development
- Understand, identify vulnerabilities in software and web applications then propose mitigations

Contenu des modules avec pondération du contenu des cours

Basics (25%):

- Confidentiality, integrity, availability, authenticity, authorization, accounting
- Threat model, malwares, etc.
- Data Protection and GDPR
- Risk and threat analysis and standards

Secure development (25%):

- SDLC: fundamentals of DevOps and how DevOps teams can build and deliver secure software
- Secure DevOps: How to build security into Continuous Delivery and Continuous Deployment
- The tools, patterns, and techniques of security automation in DevOps

Software security (25%):

- Software vulnerability identification (SANS Top 25)
- Software exploitation techniques and tools
- Software protections and mitigations

Web application security (25%):

- Web vulnerabilities (OWASP top 10)
- Web exploitation techniques and tools
- Web protections and mitigations

Méthodes d'enseignement et d'apprentissage

This course involves theoretical presentations and hands-on exercises.

Bibliographie

Lecture slides, references to internet resources and books are mentioned during the module introduction.

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

Sans aides

Cas spécial: examen de répétition oral

Type de l'examen

oral

Durée de l'examen

30 minutes

Aides autorisées

Sans aides