

<b>Intitulé de l'UE</b>	<b>Cybersécurité 1</b>
<b>Section(s)</b>	- (4 ECTS) Bachelier en Informatique et Systèmes orientation Réseaux et Télécommunications / Cycle 1 Bloc 2 option Sécurité

Responsable(s)	Heures	Période
Denis MANDOUX	45	Quad 2

Activités d'apprentissage	Heures	Enseignant(s)
Cybersécurité - théorie	20h	Denis MANDOUX
Cybersécurité - travaux pratiques	25h	Denis MANDOUX

Prérequis	Corequis

Répartition des heures
Cybersécurité - théorie : 20h de théorie
Cybersécurité - travaux pratiques : 25h d'exercices/laboratoires

Langue d'enseignement
Cybersécurité - théorie : Français, Anglais
Cybersécurité - travaux pratiques : Français, Anglais

Connaissances et compétences préalables
<ul style="list-style-type: none"> <li>Aucun prérequis n'est nécessaire, il est cependant fortement recommandé d'avoir réussi l'unité d'enseignement "Télécommunications et réseaux".</li> </ul>

Objectifs par rapport au référentiel de compétences ARES
<p><b>Cette UE contribue au développement des compétences suivantes</b></p> <ul style="list-style-type: none"> <li>Communiquer et informer <ul style="list-style-type: none"> <li>Choisir et utiliser les moyens d'informations et de communication adaptés</li> <li>Présenter des prototypes de solution et d'application techniques</li> </ul> </li> <li>Collaborer à la conception, à l'amélioration et au développement de projets techniques <ul style="list-style-type: none"> <li>Elaborer une méthodologie de travail</li> <li>Planifier des activités</li> <li>Analyser une situation donnée sous ses aspects techniques et scientifiques</li> <li>Rechercher et utiliser les ressources adéquates</li> <li>Proposer des solutions qui tiennent compte des contraintes</li> </ul> </li> <li>S'engager dans une démarche de développement professionnel <ul style="list-style-type: none"> <li>Travailler tant en autonomie qu'en équipe dans le respect de la structure de l'environnement professionnel</li> </ul> </li> <li>S'inscrire dans une démarche de respect des réglementations</li> </ul>

- Respecter les normes, les procédures et les codes de bonne pratique
- Collaborer à l'analyse et à la mise en œuvre d'un système informatique
  - Sur base de spécifications issues d'une analyse : (1) développer une solution logicielle ; (2) mettre en œuvre une architecture matérielle
  - Assurer la sécurité du système
- Intégrer des solutions télécoms sécurisées autour des réseaux locaux en y incluant la qualité de service
  - Mettre en place des solutions sécurisées d'accès aux réseaux (sans fil, ADSL, ...)
  - Interconnecter des réseaux de manière sécurisée, en gérant correctement des plans d'adressage et les aspects de sécurité (routage, ...)

### Acquis d'apprentissage spécifiques

A l'issue des activités d'apprentissage les apprenants doivent notamment être capable de :

- Connaître et expliquer les concepts essentiels relatifs à la cybersécurité.
- Situer différents éléments de sécurisation d'un réseau informatique et expliquer leur(s) fonction(s).
- Renforcer la sécurité des différents plans fonctionnels de routeurs et commutateurs en configurant diverses fonctionnalités telles que :
  - Sécurité physique, sécurisation des accès (SSH, niveaux de privilèges), authentification des mises à jour de routage, sécurité des ports, private VLAN, Listes de contrôle d'accès, DHCP snooping, Dynamic ARP Inspection, IP Source Guard, ...
- Configurer diverses fonctionnalités d'un UTM (Unified Threat Management) ou NGFW (Next Generation Firewall). Par exemple :
  - Configuration de base (gestion des comptes, logs, accès administratifs, ...)
  - Configuration des règles de pare-feu.
  - Configuration du routage
  - Configuration de VDOM (virtualisation de pare-feux)
  - Configuration du contrôle d'application
  - Configuration de l'antivirus
  - Configuration de VPN
  - etc
- Respecter les normes, méthodologies et règles de bonne pratique liés à la fonction d'administrateur réseau/sécurité.
- Etc.

### Contenu de l'AA Cybersécurité - théorie

Le contenu de l'activité est principalement basée sur :

- Les notions de base sur la cybersécurité.
- Les principaux équipements de sécurité rencontré dans un réseau local.
- Les menaces sur les réseaux IT modernes.
- La sécurisation de routeurs et commutateurs.
- La sécurisation périphérique d'un réseau via des routeurs filtrants et des pare-feu (NGFW/UTM).
- La conception et la sécurisation d'un réseau composé d'un site central et de plusieurs agences.

### Contenu de l'AA Cybersécurité - travaux pratiques

Projet de mise en oeuvre et de sécurisation d'un interréseau sur matériel physique

- Mise en oeuvre d'un réseau composé d'un site central et de plusieurs agences.
- Configuration des différents équipements afin de disposer d'un réseau fonctionnel.
- Sécurisation des périphériques réseau du site central et des agences.
- Configuration de la sécurité périmétrique du réseau via des routeurs filtrants et des pare-feu (NGFW/UTM).
- Documentation du réseau.

### Méthodes d'enseignement

**Cybersécurité - théorie** : cours magistral, approche par projets, elearning

**Cybersécurité - travaux pratiques** : travaux de groupes, approche par projets

### Supports

**Cybersécurité - théorie** : copies des présentations, activités sur eCampus, Exercices en ligne (Quizzineur)

**Cybersécurité - travaux pratiques** : Documentation liée au projet

#### Ressources bibliographiques de l'AA Cybersécurité - théorie

- Copies de présentations, Mandoux D. *Cybersécurité*, HEH - Campus Technique.
- Fortinet, Inc., *FortiOS™ Handbook - System Administration VERSION 6.0.6*, [En ligne] <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/admin-toc-final.pdf>.
- O. Santos, J. Stuppi, *CCNA Security 210-260 Official Cert Guide*, Cisco Press, septembre 2015.
- Cisco System Inc, *Cisco Guide to Harden Cisco IOS Devices*, [en ligne] <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>.

#### Ressources bibliographiques de l'AA Cybersécurité - travaux pratiques

- Copies de présentations, Mandoux D. *Cybersécurité*, HEH - Campus Technique.
- Fortinet, Inc., *FortiOS™ Handbook - System Administration VERSION 6.0.6*, [En ligne] <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/admin-toc-final.pdf>.
- O. Santos, J. Stuppi, *CCNA Security 210-260 Official Cert Guide*, Cisco Press, septembre 2015.
- Cisco System Inc, *Cisco Guide to Harden Cisco IOS Devices*, [en ligne] <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>.

#### Évaluations et pondérations

<b>Évaluation</b>	Épreuve intégrée
<b>Langue(s) d'évaluation</b>	Français, Anglais
<b>Méthode d'évaluation</b>	Examen théorique (70%) : questionnaire informatisé à compléter sur ordinateur. Evaluation continue (30%) : Evaluation continue pendant les séances de cours et TP de l'UE. Non remédiable en 2e session.

Année académique : **2020 - 2021**