Module : L'art de la protection du secret				Code	
				ING-4-SSIR-S9-P3	
Période	**Semestre 1**	*Volume horaire*	**21 H**	*ECTS*	**2**

Responsable	**Tarek Hdiji**	*email*	Tarek.Hdiji@yahoo.com
Equipe pédagogique	**Tarek Hdiji**		

1. Objectifs de Module *(Savoirs, aptitudes et compétences)*

Ce module développe une compréhension fondamentale de la cyber sécurité et de son lien avec la sécurité des informations et des réseaux

Acquis d'apprentissage :

A la fin de cet enseignement, l'élève sera capable de :

- Maîtriser la nécessite le domaine de Cyber Security (**C1.2**)
- Caractériser les meilleures pratiques de la Cyber Security. (**C1.2**)
- Développer et concevoir un projet dans le domaine Cyber Security (**C1.3**)
- Communiquer les solutions et les outils dans le domaine Cyber Security (**C3.3**)

Compétences
C1.2 : Ce cours prépare les étudiants à poursuivre leurs études en sécurité plus avancée cours. Ce cours exploratoire contient des modules qui expliquent pourquoi la cyber sécurité est nécessaire, les types de outils utilisés pour lutter contre une menace de cyber sécurité et les opportunités croissantes de carrière dans ce domaine passionnant.
C1.3 : Développer et concevoir un projet dans le domaine Cyber Security
C3.3 : Communiquer les solutions et les outils dans le domaine Cyber Security

2. Pré-requis*(autres UE et compétences indispensables pour suivre l'UE concernée)*

- Introduction à la cyber sécurité recommandée
- Formation sur la Sécurité de l'information et Réseaux

3. Répartition d'Horaire de Module					
Intitulé de l'élément d'enseignement	***Total***	***Cours***	***TD***	***Atelier***	***PR***
Module : **L'art de la protection du secret**	21	15			6

4. Méthodes pédagogiques et moyens spécifiques au Module
(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Supports de Cours : document de la certification essentiel Cyber Security
- Logiciels de simulation : Projet sur la sécurité de l'information et réseau

Bibliographie

1- Cisco.netacad.net
2- https://www.netacad.com/portal/resources/course-resources/cybersecurity-essentials

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[i])*	Durée allouée	
Séance 1 : Introduction à la cyber sécurité : 1. La nécessité de la cyber sécurité 2. Attaques, concepts et techniques 3. Protection des données et confidentialité 4. Protection de l'entreprise 5. La cyber sécurité dans votre futur	Cours TD Projet	2,5 H 0H 0,5 H
Séance 2 Cyber sécurité - Un monde de magiciens, de héros et de criminels : 1. Récapituler les conséquences de l'intégration de systèmes et de données à des équipements tiers sur la sécurité. 2. Récapituler les divers types d'attaques. 3. Utiliser les outils et techniques appropriés pour détecter les menaces pour la sécurité et les vulnérabilités dans un scénario donné.	Cours TD Projet	2 H 0 H 1 H
Séance 3	Cours	3H

Le cube magique de cyber sécurité 1. Décrire les trois dimensions du cube. 2. LA TRIADE CID Décrire les principes de confidentialité, d'intégrité et de disponibilité. 3. Les états des données Expliquer la différence entre les trois états possibles pour des données. 4. Les mesures de cyber sécurité 5. Comparer les différents types de contre-mesures en matière de cyber sécurité. 6. Le cadre de gestion de la sécurité IT Décrire le modèle de cyber sécurité ISO. Menaces, vulnérabilités et attaques de cyber sécurité 1. Expliquer les types de programmes malveillants. 2. Récapituler les divers types d'attaques 3. Récapituler les attaques par ingénierie sociale et l'efficacité de chacune d'entre elles. 4. Expliquer les types d'attaques par des connexions sans fil. 5. Expliquer les types d'attaques via des applications	TD Projet	0 H 0 H
Séance 4 L'art de protéger les secrets : 1. Contrôle d'authentification, d'autorisation ou d'accès approprié dans un scénario donné 2. Les concepts de chiffrement généraux dans un scénario donné 3. Les méthodes de chiffrement appropriées dans un scénario donné 4. Le contrôle approprié pour répondre aux objectifs de sécurité dans un scénario donné 5. Les concepts de chiffrement généraux dans un scénario donné. 6. Les méthodes de chiffrement appropriées dans un scénario donné. 7. La PKI, la gestion de certificat et les composants associés appropriés dans un scénario donné.	Cours TD Projet	3 H 0 H 0 H
Séance 5 Le royaume des cinq neufs 1. L'importance des concepts liés au risque. 2. Les procédures courantes de gestion des incidents. 3. Les bonnes pratiques en matière de gestion des risques. 4. Le contrôle approprié pour répondre aux objectifs de sécurité dans un scénario donné.	Cours TD Projet	1.5 H 0 H 1,5 H
Séance 6	Cours	3 H

Fortification du royaume : 1. Implémenter les paramètres de configuration de la sécurité sur des appareils réseau et d'autres technologies 2. Implémenter les protocoles et services courants dans un scénario donné. 3. Implémenter des procédures d'enquête de base dans un scénario donné. 4. Comparer et opposez la sécurité physique et les contrôles environnementaux. 5. Résumer les bonnes pratiques en matière de gestion des risques. 6. Le contrôle approprié pour répondre aux objectifs de sécurité dans un scénario donné 7. Expliquer les types de programmes malveillants 8. Analyser un scénario et sélectionnez les techniques de protection et de dissuasion appropriées. 9. Résumer les technologies et les concepts relatifs à la sécurité mobile. 10. La solution appropriée pour établir la sécurité de l'hôte dans un scénario donné 11. Implémenter les contrôles appropriés pour garantir la sécurité des données. 12. Comparer les différents moyens de réduire les risques de sécurité dans des environnements statiques 13. Le contrôle d'authentification, d'autorisation ou d'accès approprié dans un scénario donné 14. Installer et configurez des contrôles de sécurité pour la gestion des comptes en respectant les bonnes pratiques. 15. : Utiliser les méthodes de chiffrement appropriées dans un scénario donné	TD Projet	0 H 0 H
Séance 7 Présentation et évaluation de projet **:**	Cours TD Projet	0 H 0 H 3 H

6. Mode d'évaluation de Module*(nombre, types et pondération des contrôles)*					
Eléments d'enseignement	Coeff	DS	EX	TP	PR
Module - **L'art de la protection du secret**			60%		40%

La durée de l'examen est de 1h30.

Quand à l'examen, il est planifié après l'écoulement des 7 semaines et portera sur toutes les thématiques enseignées tout au long des 21 heures.

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.

[i] Le détail des évaluations partielles ayant donné lieu à chaque note finale comptabilisée en section 6 doit être précisé (Pour les TP : éventuellement évaluation séance par séance et évaluation en dernière séance, Projets : évaluation du travail accompli, de l'assiduité, du rapport et de la soutenance éventuels,…)