Module : Sécurité dans les clouds				Code	
				ING-4-SSIR-S9-P2	
Période	**Semestre 1**	*Volume horaire*	**42 H**	*ETCS*	**4**

Responsable	M. Mourad MILLITI	*email*	Melliti@gmail.com
Equipe pédagogique	M. Mourad MILLITI		

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

Ce module porte sur la sécurité dans les clouds

Acquis d'apprentissage :

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

- Maitriser le durcissement des infrastructures de virtualisation et des gestionnaires des Conteneurs **(C1.1)**

- Maitriser la protection contre les menaces externes et internes des infrastructures Cloud **(C2.1)**

- Identifier, évaluer et corriger les vulnérabilités dans les systèmes et les applications implémentés dans le Cloud **(C6.1)**

- Développer et mettre en œuvre des politiques, des procédures et des pratiques de sécurité adaptées aux besoin et aux exigences du cloud. **(C8.3)**

- Identifier et évaluer les risques associés à l'utilisation des services cloud. **(C5.2)**

- Préparer et tester des plans de réponse aux incidents et de reprise après sinistre pour garantir la continuité des opérations en cas de problème. **(C5.3)**

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

- Notions de base sur le cloud computing et la virtualisation

3. Répartition d'Horaire de Module

Intitulé de l'élément d'enseignement	***Total***	***Cours***	***TD***	***Atelier***	***PR***
Module Sécurité dans les clouds	42h	27h	6h	9h	

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

- Supports de Cours
- Projecteur et Tableau
- Atelier

5. Contenu *(Descriptifs et plans des cours / Déroulement / Détail de l'évaluation de l'activité pratique)*	Durée allouée
Module : Sécurité dans les clouds	

Séance 1 : Introduction aux environnements cloud 1- Définition du Cloud Computing et ses modèles de service 2- Avantages et défis de l'adoption du cloud pour les organisations/entreprises 3- Importance de la sécurité dans les environnements cloud	Cours	3H
Séance 2 : Fondements de la sécurité dans le cloud 1- Principes de base de la sécurité de l'information appliqués au cloud 2- Modèle de responsabilité partagée entre le fournisseur de services cloud et le client 3- Exigences de conformité et réglementations applicables (GDPR, etc.)	Cours	3H
Séance 3 : Mécanismes de sécurité dans les environnements cloud 1- Authentification, autorisation et gestion des identités dans le cloud 2- Cryptographie et gestion des clés 3- Surveillance et auditabilité des services cloud	Cours	3H
Séance 4 : Stratégies de protection des données dans le cloud 1- Chiffrement des données au repos, lors du traitement et en transit 2- Gestion des sauvegardes et récupération des données 3- Politiques de gestion du cycle de vie des données et gestion de la rétention	Cours	3H
Séance 5 : Gestion des incidents de sécurité dans le cloud 1- Planification et réponse aux incidents spécifiques au cloud 2- Communication et notification des incidents 3- Exercices de simulation et tests de réaction aux incidents	TD	3H
Séance 6 : Sécurité des applications et développement dans le cloud 1- Bonnes pratiques pour le développement sécurisé d'applications cloud-native 2- Sécurité des conteneurs et des microservices 3- Intégration continue et livraison continue (CI/CD) sécurisées	Cours	3H
Séance 7 : Gestion des incidents de sécurité dans le cloud 1- Gouvernance et conformité dans le cloud 2- Gestion des risques liés à la conformité réglementaire 3- Contrôles de sécurité et évaluation des fournisseurs de services cloud 4- Audit et rapports de conformité	Cours	3H
Séance 8 : Sécurité des gestionnaires de conteneurs (Docker, etc.) 1- Fonctionnement d'un gestionnaire de conteneurs 2- Modèle de menace, surface d'attaque, vulnérabilité potentielles et connues 3- Durcissement des gestionnaires de conteneurs	Cours	3H
Séance 9 : Sécurité des infrastructures 1- Fonctionnement général et sécurité d'OpenStack 2- Fonctionnement et sécurité de Kubernetes 3- Sécurité des cloud providers 4- Modèles de déploiement prenant en compte la sécurité	Cours	3H
Séance 10 : Cas d'études : Sécurité et durcissement de KVM 1- Fonctionnement de la virtualisation avec KVM 2- Fonctionnement des gestionnaires de machines virtuelles	Cours	3H

3- Modèle de menace, surface d'attaque, vulnérabilité potentielle et connues de KVM 4- Durcissement des gestionnaires de machines virtuelles et de la virtualisation avec KVM		
Séance 11, 12, 13 **TP1: Sécurisattion des Conteneurs** 1- Création d'un Template de conteneur docker en utilisant dockerfilemp 2- Manipulation de cgroups afin de limiter, compter et isoler l'utilisation des ressources (RAP/CPU/DISQUE..) **TP2: Capabilities & Secomp avec** Docker 1- Manipulation des linux capabilities en utilisant --cap-add 2- Manipulation des linux capabilities avec --cap-drop 3- Utilisation de la fonctionnalité SECCOMP pour filtrer les appels systémes **TP3: Atelier Gestionnaire de Conteneurs et sécurité** 1- Sécurité Kubernetes et OpenShift 2- Créer une image de conteneur durcie en terme de sécurité via Sécurité Kubernetes et OpenShift et/ou Rancher	TP	9H
Séance 14 1- Forum pour discuter des défis rencontrés lors des audits 2- Réponses aux questions des participants 3- Récapitulation des points clés	Cours /TD	3H

6. Mode d'évaluation de Module*(nombre, types et pondération des contrôles)*

Eléments d'enseignement	Coeff	DS	EX	TP	PR
	2	40%	60%		

Pour valider le module, les étudiants passeront un examen dont le coefficient est de 60%, un DS dont le coefficient est de 40% .

La durée de tous les examens (Examen, DS…) est de 1h30.

Le DS est planifié 7 semaines après le début du module.

Quant à l'examen, il est planifié après l'écoulement des 14 semaines et portera sur toutes les thématiques enseignées tout au long des 42 heures.

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