MAÎTRISE EN INFORMATIQUE
CYBERSÉCURITÉ



Le programme de maîtrise en informatique, concentration Cybersécurité est conçu en collaboration avec l'industrie et enseigné par des professionnels oeuvrant dans l'industrie du cybersécurité.

Vos futures et futurs stagiaires :

- ont déjà un diplôme de premier cycle en informatique ou dans une discipline connexe.
- sont des spécialistes en cybersécurité pour toutes les types d'entreprises et les organisations publiques (gouvernement et autres instances publiques).
- ont un esprit d'analyse et de synthèse, une rigueur intellectuelle ainsi que des aptitudes à l'écoute et à la communication.
- sont aptes à intégrer des équipes de cybersécurité autant en prévention qu'en réaction à des attaques;
- sont disponibles pour des stages de quatre à six mois.

DES EXEMPLES DE CE QUE NOS STAGIAIRES PEUVENT FAIRE POUR VOUS

- Mettre en place un processus de gestion des incidents.
- Gérer des vulnérabilités et appliquer une approche proactive contre les cyberattaques.
- Établir des métriques d'évaluation de la sécurité.
- Maîtriser les principaux systèmes d'exploitation disponibles sur le marché. Savoir renforcer la sécurité de ces systèmes.
- Apporter du soutien sur les enjeux de sécurité entourant la virtualisation et les systèmes mobiles.
- Effectuer la recherche d'informations sur une cible d'attaque.
- Différencier les types d'attaques.
- Utiliser des trousses et outils de piratage de façon éthique.
- Utiliser les bonnes techniques pour détecter des cyberattaques.
- Comprendre les différentes étapes d'une enquête de piratage
- Utiliser des outils de diagnostic pour repérer du code malveillant.
- Identifier différents types de cyberattaques.
- Apporter du soutien lors de la gestion d'incidents suite à une attaque.
- Appliquer les standards d'architecture dans un contexte d'entreprise.
- Formuler une architecture pour les besoins de sécurité d'une entreprise.
- Effectuer l'analyse et l'évaluation d'un document d'architecture de sécurité.

Spécificité de la formation

- Permet de maîtriser les tenants et aboutissants de la sécurité informatique et de la gestion de celle-ci ;
- Permet d'approfondir ses connaissances sur les surfaces d'attaque exposées et sur les stratégies efficaces de protection et de défense par une infrastructure de TI ;
- Développe la capacité à critiquer une stratégie mise en place dans une organisation ;
- Permet de maîtriser la nature, le rythme et les outils des cyberattaques ;
- Développe la capacité à dresser et exécuter un plan d'intervention en cas d'incident de sécurité.

CONNAISSANCES ET COMPÉTENCES

Session	Description

S-1	• **Planification et prévention en sécurité des TI**
	  ◦ Processus de gestion des incidents ; gestion des vulnérabilités; application d'une approche proactive contre les cyberattaques ; mesures d'évaluation de la sécurité.
	• **Sécurité des systèmes**
	  ◦ Connaissance, maîtrise et renforcement de la sécurité des principaux systèmes d'exploitation ; enjeux de sécurité liés à la virtualisation et aux systèmes mobiles.
	• **Introduction aux attaques informatiques**
	  ◦ Compréhension des étapes d'une cyberattaque ; différencier les types d'attaques; utilisation éthique des trousses et des outils de piratage ; techniques de détection d'une cyberattaque.
	• **Criminalistique en sécurité des TI**
	  ◦ Notion de criminalistique ; bases du droit et des crimes liés aux technologies ; évaluation des règles de sécurité minimale en matière de criminalistique ; enquête lors d'un incident de sécurité en TI ; règles et mécanismes de conservation de la preuve en droit criminel.
	• **Cryptographie**
	  ◦ Systèmes de chiffrement, authentification des messages, échanges de clés, signatures numériques, certificats numériques, hachage cryptographique ; infrastructure à clé publique ; sélection du système cryptographique en fonction de la situation ; évaluation de la sécurité potentielle d'un système.

S-2	• **Sécurité des logiciels**
	  ◦ Rôles, tâches et mise en place de la sécurité des données ; outils et techniques liés à la sécurité des données ; cycle de vie d'un logiciel ; description des environnements logiciels ; spécificités des applications Web ; concepts de base de sécurité applicative.
	• **Système et réseau**
	  ◦ Caractéristiques de l'architecture des composantes des réseaux informatiques dans un contexte de sécurité ; compréhension des principes d'architecture réseau et de sécurité.
	• **Réaction aux attaques et analyses des attaques**
	  ◦ Caractéristiques des types de cyberattaques; gestion d'incidents à la suite d'une attaque.
	• **Architecture de sécurité**
	  ◦ Modèles d'architecture ; application des standards d'architecture ; conception d'une architecture de sécurité en fonction des besoins de sécurité d'une entreprise ; analyse et évaluation d'un document d'architecture de sécurité

AGENCEMENT DES SESSIONS D'ÉTUDES (S) ET DES STAGES DE TRAVAIL (T)

Groupe	AUT	HIV	ÉTÉ	AUT
Arrimage international (M1)	S-1	S-2	T-1 (4 ou 6 mois)	
Autre arrimage	S-1	S-2	T-1 (4 mois)	S-3 (cours à option)