Programme de l'école d'été 2026 en Cyberdéfense à l'UQAC

Horaire de l'atelier	Date	Sujet	Formateur
9am – 12 pm	**2 juin 2026**	Approches modernes de DevSecOps	Jonathan Roy
2 pm – 5 pm	**2 juin 2026**	La conformité de sécurité avec un processus DevSecOps	Vincent Bureau
9am – 12 pm	**3 juin 2026**	Initiation au Pentest interne	Romain Carnus et Mathieu Novis
2 pm – 5 pm	**3 juin 2026**	Ethical hacking et tests d'intrusion avancés	Romain Carnus et Mathieu Novis
9am – 12 pm	**4 juin 2026**	Modélisation des menaces en cybersécurité et protection des données personnelles	Adel Tayeb-Cherif
2 pm – 5 pm	**4 juin 2026**	L'utilisation de l'IA en cyber sécurité	Elyes Manai

Jour 1 – Atelier 1

Bio de Jonathan Roy:

Jonathan Roy est professeur en cybersécurité à l'Université du Québec à Chicoutimi (UQAC) et cumule plus de 20 ans d'expérience, tant en industrie qu'en milieu académique, dans la conception, la sécurisation et l'évaluation de systèmes logiciels. Avant de rejoindre le monde universitaire, il a dirigé des initiatives en architecture de sécurité pour de grandes organisations issues de divers secteurs, développant une expertise en sécurité d'entreprise, en infrastructures infonuagiques et en gestion des risques. Il s'intéresse à l'utilisation de l'intelligence artificielle explicable (XAI) pour automatiser des tâches clés en cybersécurité des systèmes logiciels et des systèmes d'IA, notamment l'évaluation des risques, la priorisation des vulnérabilités et l'identification des incidents.

Titre de la formation : Approches modernes de DevSecOps

Résumé :

Nous aborderons des tâches concrètes liées à l'intégration automatisée et continue de la sécurité dans le cycle de développement logiciel. La séance comprendra une partie théorique suivie d'une activité pratique. Elle est conçue pour un public débutant, mais pourra inclure des éléments plus avancés selon les profils des participant·e·s.

Jour 1 – Atelier 2

Bio de Vincent Bureau : Expert en gouvernance des données, protection de la vie privée et sécurité de l'information, Vincent est fondateur de DPOsolutions et chargé de cours à l'UQAC.

Titre de la formation : La conformité de sécurité avec un processus DevSecOps

Résumé :

Face à la montée discontinue des menaces portées par les matériels et logiciels numériques, la loi européenne sur la cyber-résilience (CRA) apporte une réponse en adressant deux problèmes majeurs :

1. Le faible niveau de cybersécurité des produits associés à des vulnérabilités généralisées,
2. Le manque de contrôle des utilisateurs.

Sur la base d'un cas d'application concernant d'une entreprise canadienne offrant des technologies médicales au marché européen, les étudiants devront réviser le portefeuille des produits de l'entreprise selon la classification CRA et définir un programme de conformité comprenant un processus DevSecOps.

Jour 2 – Atelier 3 et Atelier 4

Bio de Romain Carnus : Diplômé en 2011 d'un master en informatique en France à l'école d'ingénieurs INSA Centre-Val-de-Loire, Romain a depuis occupé des postes de chercheur, architecte en sécurité, chef de projet, évaluateur en sécurité, pentester et chercheur en cybersécurité dans plusieurs organisations de tailles diverses, notamment Airbus Defence and Space, le ministère français de l'Intérieur, Hitachi Energy, Oppida et GoSecure.

Pendant plus de dix ans, Romain a développé des compétences en sécurité offensive dans des sociétés de services en tant que pentester et évaluateur en sécurité. En tant qu'hacker éthique chez GoSecure, Romain a travaillé sur une variété de missions, ce qui lui a permis d'approfondir de nombreux aspects de la cybersécurité, avec un intérêt particulier pour les systèmes de contrôle industriel (ICS) et les systèmes embarqués (IoT). En tant que chercheur en cybersécurité chez Hitachi Energy, Romain a contribué à la sécurité des produits de réseaux électriques par le biais de recherches de vulnérabilités, découvrant plus de 20 vulnérabilités zero-day.

Romain se considère comme un généraliste, mais est généralement plus attiré par les aspects techniques de la cybersécurité, notamment les concepts de bas niveau comme les aspects internes des systèmes d'exploitation et les protocoles de sécurité.

Bio de Mathieu Novis : Mathieu a obtenu son diplôme en 2018 avec une licence en informatique. Pendant plus de trois ans, il a contribué à sécuriser une entreprise de télécommunications américaine, identifiant des vulnérabilités pour une valeur supérieure à 1,1 million de dollars. À l'issue de cette période, l'entreprise s'est estimée suffisamment mature pour lancer un programme de bug bounty, que Mathieu a pris en charge. Ses efforts ont permis de détecter de multiples vulnérabilités critiques telles que cross-site scripting (XSS), falsification de requêtes côté serveur (SSRF) ou exécution de code à distance (RCE).

Engagé dans une démarche d'amélioration continue, Mathieu a collaboré étroitement avec les équipes de remédiation afin de garantir une gestion rapide et approfondie des vulnérabilités. Il possède une expérience pratique des simulations d'attaques complexes, incluant des scénarios de ransomware et de cryptolocker, ainsi que des techniques d'exploitation avancées comme l'élévation de privilèges et l'exfiltration de données.

Souhaitant constamment approfondir son expertise, il poursuit régulièrement de nouvelles opportunités de formation. Ses compétences en relecture de code ont été renforcées par plusieurs projets de recherche. Mathieu reste déterminé à proposer des solutions innovantes pour protéger les organisations face aux menaces émergentes, leur permettant ainsi de maintenir la sécurité de leurs opérations et de se concentrer sur leur cœur de métier.

Résumé des ateliers 3 et 4 : Initiation au pentest interne : Cette formation vise à familiariser les participants avec les techniques d'attaque classiques ciblant un environnement Windows d'entreprise. Une première partie théorique abordera quelques concepts clés liés Active Directory, aux protocoles réseau et aux vecteurs d'attaque. La seconde partie sera entièrement pratique, avec des exercices dans un environnement virtuel

pour permettre aux élèves de mettre en œuvre certaines des techniques vues précédemment.

Jour 3 – Atelier 5

Biographie d'Adel Tayeb-Cherif : Adel travaille dans le domaine de la cybersécurité depuis plus de 15 ans et possède une solide formation en ingénierie informatique. Avant de se spécialiser en cybersécurité, il a travaillé pendant 7 ans comme développeur logiciel, ce qui lui a permis d'acquérir une compréhension technique approfondie des systèmes qu'il sécurise aujourd'hui. Il occupe actuellement le poste d'Architecte et Leader en cybersécurité chez Ericsson, où il encadre les équipes et collabore étroitement avec les parties prenantes sur les enjeux liés à la sécurité.

Au fil de sa carrière, il a contribué à l'élaboration de stratégies de sécurité, accompagné des équipes dans la mise en œuvre de bonnes pratiques, et partagé son expertise pour former d'autres professionnels du domaine.

Parmi les reconnaissances obtenues, il a reçu le *Bravo Award* chez Bell, la plus haute distinction de l'entreprise, soulignant son rôle déterminant dans un projet clé de sécurité IoT.

Adel est animé par une curiosité constante, une forte détermination et un engagement envers l'amélioration continue. Il valorise le travail d'équipe et place l'ambition au cœur de sa démarche professionnelle, avec pour objectif de faire progresser la cybersécurité de manière durable et collaborative.

Description de l'atelier Threat Modeling :

Titre de la formation : Modélisation des menaces en cybersécurité et protection des données personnelles

Cette formation propose une introduction pratique à la modélisation des menaces (threat modeling), une étape essentielle dans le processus de sécurisation des systèmes informatiques dès leur conception. Les participants apprendront à identifier, analyser et anticiper les menaces de sécurité ainsi que les risques liés à la protection des données personnelles, à l'aide de méthodologies reconnues dans l'industrie.

Nous utiliserons les *Data Flow Diagrams (DFD)* comme outil principal de visualisation pour représenter les composants d'un système, leurs interactions, et les flux de données. À partir de ces *DFDs*, deux approches complémentaires seront appliquées :

- STRIDE, un cadre de référence pour identifier les principales menaces en matière de sécurité informatique.
- LINDDUN, une méthode spécialisée pour analyser les risques portant sur la protection des données personnelles.

Objectifs pédagogiques :

- Comprendre l'importance de la modélisation des menaces dans le cycle de développement.
- Maîtriser les bases des *DFDs* pour représenter les architectures systèmes.
- Appliquer méthodiquement STRIDE pour analyser les menaces liées à la sécurité.
- Appliquer LINDDUN pour évaluer les risques affectant la protection des données personnelles.
- Savoir proposer des mesures de mitigation pour les risques identifiés.

Public cible :

Cette formation s'adresse aux développeurs, architectes, responsables de la sécurité, et à toute personne impliquée dans la conception ou l'évaluation de systèmes informatiques soucieux d'intégrer la sécurité et la protection des données personnelles dès les premières étapes du développement.

Jour 3 – Atelier 6

Bio d'Elyes Manai :

Elyes Manai a obtenu un master de recherche en intelligence web à l'École supérieure d'économie numérique (Tunisie) en 2018, puis un doctorat en informatique à l'Université Laval en 2025. Ses recherches portent sur l'application de l'intelligence artificielle à la cybersécurité, notamment l'IA explicable (XAI), l'audit de modèles, les pipelines d'IA sécurisés et la fiabilité des modèles.

Le professeur Manai possède le titre de *Google Developer Expert* en apprentissage automatique (ML GDE), une désignation attribuée à 200 spécialistes IA dans le monde par Google. Il a également été instructeur en apprentissage profond chez NVIDIA, mentor technique à l'accélérateur *Google for Startups*, cofondateur de la communauté PyData Tunisia, et chef de la communauté Facebook *Developer Circles Tunisia*. Il a animé plus de 200 conférences, ateliers et formations autour de l'IA, tant au Canada qu'à l'international, en milieu académique, industriel et communautaire. Il s'implique aussi activement dans la vulgarisation, l'encadrement et le transfert de connaissances en IA.

Titre de la formation : *L'utilisation de l'IA en cyber sécurité*

Résumé : Cette formation propose une initiation aux approches analytiques, statistiques et algorithmiques utilisées pour détecter et caractériser des comportements malveillants. Exploitation de jeux de données spécialisés en cybersécurité pour construire des modèles de classification, de détection d'anomalies et d'analyse automatisée de journaux d'événements (logs). Nous aborderons des tâches concrètes de détection d'intrusion avec une approche à la fois technique (prétraitement, entraînement de modèles) et stratégique (interprétation des résultats, optimisation). La séance comprendra une partie théorique suivie d'une activité pratique.