Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB6033 Gr. 01
Titre : Renseignement sur les cybermenaces et analyse de risques de cyberattaques
Session : Automne 2024 Horaire et local
Professeur : Elouasbi, Samir

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e aura maitrisé et mis à l'épreuve les techniques de détection, de réponse et de lutte contre les menaces persistantes avancées (APT) et les campagnes de logiciels malveillants.

Contenu

Introduction au concept du renseignement, métier d'analyste de risque et niveaux de renseignement sur les menaces. Planification, direction et génération des besoins en matière de renseignement. Évaluation du risque d'intrusions adverses : chaîne de destruction, modèle diamant, comportement adverse, indicateur de compromission. Sources de données pour l'analyse d'intrusion : open source intelligence (OSINT), etc. Structuration et stockage d'information sur les renseignements: techniques-tactiques-procédures (TTP), Malware Information Sharing Platform (MISP), MITRE ATT&CK, etc. Outils analytiques. Dissémination du renseignement aux niveaux tactique, opérationnel et stratégiques. Études de cas.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

Ce cours vise principalement à :

- Développer des Compétences en Détection et Réponse aux Menaces : Les étudiants apprendront à identifier et à neutraliser efficacement les APT et les logiciels malveillants.
- Approfondir la Compréhension des Menaces de Cybersécurité : Le cours se concentre sur une compréhension détaillée des tactiques et stratégies des cyberattaquants.
- Mettre en Pratique les Connaissances Théoriques : Les étudiants auront l'opportunité de mettre en œuvre leurs connaissances à travers des études de cas et des projets pratiques.
- Renforcer les Compétences Analytiques et Critiques : Le cours encourage le développement de capacités d'analyse et de réflexion critiques, essentielles pour évaluer et contrer les menaces de sécurité.
- Maîtrise pratique des outils et logiciels de cybersécurité : les étudiants auront l'occasion d'utiliser efficacement diverses technologies pour l'analyse de menaces, la surveillance réseau, et la réponse aux incidents.

3. Stratégies pédagogiques :

Il s'agit d'un cours magistral en présentiel avec des exercices pratiques, des études de cas et des ateliers de démonstration.

4. Heures de disponibilité ou modalités pour rendez-vous :

Sur rendez-vous.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Introduction au renseignement en cybersécurité** • Présentation du syllabus et des objectifs du cours • Introduction aux concepts clés de la cybersécurité et du renseignement • Discussion sur l'importance du renseignement dans la lutte contre les APT **Exercice** : Rédaction d'un résumé sur l'importance du renseignement en cybersécurité	9 septembre 2024
2	**Rôle de l'Analyste de Risque et Niveaux de Renseignement** • Présenter les fonctions, défis et compétences nécessaires pour un analyste de risque • Introduire les différents niveaux de renseignement sur les menaces (tactique, opérationnel, stratégique) • Importance des niveaux de renseignement sur les menaces dans l'analyse de risque **Étude de cas :** Choisir un incident de cybersécurité et analyser les risques associés et l'application des différents niveaux de renseignement.	16 septembre 2024
3	**Processus de planification et Direction du Renseignement** • Principes de Base de la Planification du Renseignement : cycle de renseignement et définition des objectifs basés sur les besoins et les menaces • Génération et Priorisation des Besoins en Renseignement : évaluation des risques et contexte des menaces • Analyse et Interprétation des Données de Renseignement pour la prise des décisions • Exploration d'outils et de logiciels : Maltego et Shodan **Devoir :** exploration et utilisation d'un outil pour la planification et l'analyse du renseignement	23 septembre 2024
4	**Évaluation des Risques d'Intrusion (théorie)** • Introduction aux Modèles d'Analyse des Risques • La Chaîne de Destruction • Le Modèle Diamant • Les Indicateurs de Compromission (IoC) • Pyramide de la douleur	30 septembre 2024
5	**Évaluation des Risques d'Intrusion (pratique) – Partie 1**	7 octobre 2024
6	**Semaine d'études**	14 octobre 2024

7	**Évaluation des Risques d'Intrusion (pratique) – Partie 2** **Énoncé du projet**	21 octobre 2024 **(Non présentiel)**
8	**Examen de mi-session**	28 octobre 2024
9	**Sources de Données pour l'Analyse d'Intrusion** • Importance des données dans la détection et l'analyse des intrusions • Types de Données en Cybersécurité : logs, données de Pare-feu et antivirus, IDS/IPS • OSINT et son utilisation pour la collecte d'informations **Atelier pratique :** OSINT avec Maltego	4 novembre 2024
10	**Structuration et stockage d'information sur les renseignements** • Principes fondamentaux : organisation, classification et analyse des données • Formats standards pour le partage de renseignements : STIX et TAXII • Plateformes et outils : MISP et MITRE ATT&CK	11 novembre 2024
11	**Atelier pratique :** Comprendre et identifier les TTP utilisés par les adversaires en utilisant le cadre MITRE ATT&CK.	18 novembre 2024 **(Non présentiel)**
12	**Outils Analytiques en Cybersécurité** • Motivation : Détection, analyse et réponse aux menaces • IDS/IPS : Fonctionnement, avantages et limites • Plateformes SIEM : Caractéristiques, avantages et limites • Outils d'analyse de Malware : Utilisation, avantages et limites **Ateliers pratiques :** Wireshark ou Ghidra	25 novembre 2024
13	**Dissémination du renseignement** • Définition et objectifs • Les niveaux de dissémination : Tactique, opérationnelle et stratégique • Méthodes et formats de communication efficaces **Travail sur le projet**	2 décembre 2024 **(Non présentiel)**
14	**Présentation des projets**	9 décembre 2024
15	**Examen final**	16 décembre 2024

6. Évaluation du cours :

- Devoir : 10%
- Projet : 20%
- Examen de mi-session : 30%
- Examen final : 40%

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

- **Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks.** Alexey Kleymenov et Amr Thabet. Packt Publishing 2019. ISBN: 1789610788
- **Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats**. Alex Matrosov, Eugene Rodionov, et Sergey Bratus. No Starch Press 2019. ISBN: 1593277164
- **Malware Data Science: Attack Detection and Attribution.** Joshua Saxe et Hillary Sanders. No Starch Press 2018. ISBN: 1593278594

9. Page Web du cours :

https://moodle.uqo.ca