MINISTERE DE LA COMMUNAUTE FRANCAISE

ADMINISTRATION GENERALE DE L'ENSEIGNEMENT

ENSEIGNEMENT DE PROMOTION SOCIALE

DOSSIER PEDAGOGIQUE

UNITE D'ENSEIGNEMENT

FORMATION CONTINUE : INCIDENT RESPONSE AND FORENSICS SECURITY

ENSEIGNEMENT SUPERIEUR DE TYPE COURT
DOMAINE : SCIENCES

CODE : 7532 12 U32 D1

CODE DU DOMAINE DE FORMATION : 710
DOCUMENT DE REFERENCE INTER-RESEAUX

Approbation du Gouvernement de la Communauté française du
sur avis conforme du Conseil général

FORMATION CONTINUE : INCIDENT RESPONSE AND FORENSICS SECURITY

ENSEIGNEMENT SUPERIEUR DE TYPE COURT

1. FINALITÉS DE L'UNITÉ D'ENSEIGNEMENT

1.1. Finalités générales

Dans le respect de l'article 7 du décret du 16 avril 1991 organisant l'enseignement de promotion sociale de la Communauté française, cette unité de formation doit :

- concourir à l'épanouissement individuel en promouvant une meilleure insertion professionnelle, sociale, culturelle et scolaire ;
- répondre aux besoins et demandes en formation émanant des entreprises, des administrations, de l'enseignement et d'une manière générale des milieux socio-économiques et culturels.

1.2. Finalités particulières

L'unité d'enseignement vise à permettre à l'étudiant de fournir une réponse appropriée aux incidents dans l'entreprise, ainsi qu'entreprendre les démarches de forensiques adéquates.

2. CAPACITES PREALABLES REQUISES

2.1. Capacités

Pour l'introduction à la sécurité des systèmes d'information :

En respectant les consignes liées à l'évaluation,
dans le respect du temps imparti,
sous la forme demandée et dans un local défini :

- ♦ d'expliquer différents concepts liés à la sécurisation des systèmes d'information et de communication ;
- ♦ d'identifier des outils et des technologies de sécurisation des systèmes d'information et de communication appropriés dans un scénario ou un contexte ;

2.2. Titre pouvant en tenir lieu

Attestation de réussite de l'unité d'enseignement « Formation continue : Introduction à la sécurité des systèmes d'information », code N° 7532 10 U32 D1, classée dans l'enseignement supérieur de type court.

3. ACQUIS D'APPRENTISSAGE

Pour atteindre le seuil de réussite, l'étudiant sera capable,

Au départ d'exercices ou de situations,
en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...),
en disposant de l'accès à la documentation requise et d'un réseau,
dans le respect des lois et règlements,

- de décrire et de documenter un incident de cybersécurité ;
- de mettre en place une réponse appropriée à l'incident de sécurité ;
- de maîtriser et réaliser les démarches forensiques en respectant les procédures ;

Pour la détermination du degré de maîtrise, il sera tenu compte :

- du degré de pertinence des solutions retenues,
- du respect du temps alloué,
- du degré de cohérence de sa réponse à l'incident,
- du degré de respect des démarches et procédures,
- du degré de clarté et de précision du vocabulaire technique.

4. PROGRAMME

L'étudiant sera capable de :

Au départ d'exercices ou de situations,
en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...),
en disposant de l'accès à la documentation requise et d'un réseau,
dans le respect des lois et règlements

Pour la récolte des infos et des preuves dans le respect des procédures :

- Effectuer la récolte de preuves numériques ;
- Effectuer l'acquisition de forensique numérique ;
- Effectuer les acquisitions et imageries des supports numériques au cours du processus d'enquête ;
- Examiner et analyser les textes, graphiques, multimédia et images numériques ;
- Conduire un examen approfondi des supports de mémoires informatiques (disques durs, etc.) ;
- Récupérer les informations et données numériques de supports de mémoires informatiques (disques durs, etc.) ;
- Collecter les données par l'usage de technologies et méthodes forensiques respectant les procédures de manipulation des preuves, en ce compris la collecte de copies physiques et électroniques de documents ;
- Suivre scrupuleusement des procédures strictes de manipulation de données et de preuves ;

- Maintenir un journal des transactions ("audit trail") (c'est-à-dire : chaîne de possession/surveillance/responsability ("chain of custody")) et d'intégrité des preuves ;
- Procéder à l'examen technique, l'analyse et le rapportage de preuves informatiques ;
- Préparer et maintenir un dossier forensique ;
- Utiliser les outils forensiques et des méthodes d'investigations pour trouver des données électroniques, des historiques d'usage d'Internet, de traitement de texte, d'images et autres types de fichiers ;
- Extraire et collecter des informations volatiles et non volatiles des systèmes d'exploitation (Exemple : Microsoft Windows, Apple Mac OS, Linux…) ;
- Récupérer des fichiers effacés et des partitions à partir des systèmes d'exploitation (Exemple : Microsoft Windows, Apple Mac OS, Linux…) ;
- Effectuer des recherches sur base de mots-clefs, à partir de mots et phrases dans des systèmes d'information.

Pour la conduite de l'enquête et la procédure forensique :

- Jouer le rôle de premier intervenant en sécurisant et en évaluant une scène où un délit informatique a eu lieu, en dirigeant les entrevues préliminaires, en documentant la scène de délit, en regroupant et préservant les preuves numériques, en faisant rapport sur la scène numérique du délit ;
- Mener l'enquête sur des évènements par la recherche de preuves d'une menace ou attaque interne ("insider threat") ;
- Mener l'enquête et analyser toutes les réactions et activités liées à un incident "cybersécurité" ;
- Planifier, coordonner et diriger les activités de récupération/remise en fonctionnement des systèmes informatiques ainsi que les taches d'analyse des incidents ;
- Examiner toutes les informations disponibles, les preuves et artefacts liés à un incident ou évènement informatique ;
- Effectuer de la rétro-ingénierie pour des fichiers de logiciels malveillants connus et suspects ;
- Effectuer une évaluation détaillée des données et de toutes preuves d'activités afin d'analyser de la façon la plus détaillée les circonstances et les implications d'un évènement ;
- Identifier les données, images et/ou activité qui pourraient être la cible d'une enquête interne ;
- Mettre en place des mécanismes de maintien de Cyber Threat Intelligence et des éléments d'apprentissages essentiels pour soutenir une démarche de profilage pro-active et des capacités de modélisation de scénario (veille technologique) ;
- Explorer et faire des recherches dans les espaces mémoires "libres" ;
- Enregistrer et documenter les temps d'accès, de modification et de création (MAC times) en tant que preuve d'accès et de séquence des évènements ;
- Examiner les types de fichiers et les informations d'en-tête de fichiers ;
- Analyser les communications électroniques ce y compris les e-mail, web mail et les programmes de messageries instantanées par Internet ;
- Examiner l'historique de navigation Internet/web ;
- Générer les rapports qui détaillent les approches et méthodologies de travail ainsi que le journal des transactions (« audit trail ») qui documentent les actions entreprises pour assurer l'intégrité du processus interne d'investigation ;
- Récupérer les fichiers actifs, systèmes et cachés avec une estampille temporelle ;
- Faire usage adéquat des techniques, méthodes et analyses pour contourner ou tenter de contourner les mécanismes de protection des fichiers sur base de secrets (mot de passe, etc.) ;
- Effectuer de la détection de techniques anti-forensique ;
- Suivre, maintenir et promouvoir la conscientisation sur les règles (policies) et procédures de manipulation, d'examinassions de preuve et de sécurité en laboratoire ;

- Effectuer les analyses post-intrusion de supports médias numériques pour déterminer qui, où, quoi, quand et comment l'intrusion s'est déroulée ;
- Appliquer les outils, techniques et méthodologies forensiques avancés ainsi que les techniques de reconstruction d'attaque ;
- Effectuer les activités forensiques fondamentales ;
- Identifier et vérifier les sources et origines potentielles d'incidents ;
- Effectuer les analyses de corrélation d'évènements ;
- Extraire et analyser les logs de différents dispositifs tels que proxies, pare-feu, IPS et IDS, ordinateurs fixes et portables, serveurs, SIM/SIEM, routeurs, switchs, serveurs d'authentification, DHCP, etc ;
- Garantir que le rapport des incidents et des vulnérabilités supposées et des dysfonctionnements soit traité avec respect pour la confidentialité.

Pour la communication interne/externe :

- Participer à la production de rapports d'incident
- Fournir de l'assistance à la préparation des perquisitions, des ordres de justices, etc.
- Fournir les témoignages d'experts en soutien aux procédures et examens forensiques conduits par un autre examinateur.

5. CHARGE(S) DE COURS

Un enseignant ou un expert.

L'expert devra justifier de compétences issues d'une expérience professionnelle actualisée dans le domaine en relation avec le programme du présent dossier pédagogique.

6. CONSTITUTION DES GROUPES OU REGROUPEMENT

Il est recommandé de ne pas dépasser deux étudiants par poste de travail.

7. HORAIRE MINIMUM DE L'UNITE D'ENSEIGNEMENT

7.1. Dénomination du cours	Classement	Code U	Nombre de périodes
Laboratoire de sécurité informatique	CT	S	80
7.2. Part d'autonomie		P	20
Total des périodes			100
Nombre d'ECTS			6