Réponse aux incidents et analyse forensique

TEB3012-NIRN_

Domaine : **Sciences** Grade académique : **Bachelier en informatique, orientation sécurité des sytèmes - Namur**
Niveau de certification : **6** Cycle : **Premier Cycle** Année académique : **2026-2027** (Q1)

CRÉDITS ECTS	VOLUME HORAIRE
5	**48 h**
PRÉREQUIS *Aucun*	CO-REQUIS *Aucun*

IMPLANTATION	DIRECTEUR DE DÉPARTEMENT DU DOMAINE	RESPONSABLE DE L'UE	ENSEIGNANTS INTERVENANTS
Département technique de Namur	Willem Kuypers	Adrien VOISIN	Adrien VOISIN

PROGRAMME D'ÉTUDES

Programme	Bloc	Caractère
IE-Bachelier en informatique, orientation sécurité des systèmes	3	Obligatoire

Partie 1 Contribution de l'UE au profil d'enseignement du programme et acquis d'apprentissage spécifiques (AAS) sanctionnés par l'évaluation

CONTEXTUALISATION

Dans le cadre de la formation en sécurité des systèmes, l'UE: "Réponse aux incidents et analyse forensique" offre une mise en situation d'un cyber incident pour que les étudiants puissent appréhender les méthodes et les outils propres à cette discipline.

ACQUIS D'APPRENTISSAGE SPÉCIFIQUES (AAS)

Au terme de l'activité, l'étudiant sera capable de :

- De nommer et d'expliquer les méthodes, les concepts et les outils utilisés dans le contexte d'un processus de réponse d'incident
- D'analyser un incident dans le contexte de la sécurité informatique et de proposer une méthodologie d'investigation numérique adaptée
- D'utiliser des outils "Digital Forensic" pour identifier et analyser des données critiques dans le contexte d'une investigation numérique
- D'expliquer par écrit comment identifier et interpréter une preuve numérique analysée durant les séances pratiques

OBJECTIFS DE DÉVELOPPEMENT DURABLE

Document annexe à la fiche UE accessible via un lien explicitant en quoi le programme d'études s'inscrit dans une politique de développement durable. Une ou plusieurs UE spécifique(s) pourraient être ciblée(s) dans cette annexe.

Partie 2 Description de l'unité d'enseignement

OBJECTIFS

L'objectif de cette UE est d'apprendre aux étudiants les bases théoriques et pratiques d'un processus de réponse d'incident.

CONTENU

Concepts et définitions générales

Indicateurs de compromission Windows

Indicateurs de compromission Linux

Récolte de preuves numériques sous Windows

Récolte de preuves numériques sous Linux

Analyse de logiciels malveillants

Introduction à l'OSINT

Threat Intelligence

SOURCES ET RÉFÉRENCES

Voisin, A., & Duvillié, G. (2026). *La réponse d'incident: Analyser et réagir face à une cyberattaque*. De Boeck Supérieur.

SUPPORTS DE COURS

Activité d'apprentissage	Support

AIRN3012 — Réponse aux incidents et analyse forensique	• Slides et vidéos présentées par l'enseignant disponible via Moodle • Livre: La réponse d'incident, analyser et réagir face à une cyberattaque, Voisin - Duvillié, Deboeck Supérieur 2026 (Disponible à la bibliothèque) • Énoncé des séances de laboratoire (Moodle)

Partie 3 Méthodologie mise en œuvre et éventuel découpage de l'UE

DESCRIPTION DES ACTIVITÉS D'APPRENTISSAGE (AA) AU REGARD DE LEUR STATUT

Activité d'apprentissage	Heures	Langue d'enseignement	Langue d'évaluation
AIRN3012 — Réponse aux incidents et analyse forensique	48 h	Français	Français

MÉTHODES D'ENSEIGNEMENT ET D'APPRENTISSAGE

Activité d'apprentissage	Méthodes d'enseignement et d'apprentissage
AIRN3012 — Réponse aux incidents et analyse forensique	*À définir*

DÉTERMINATION DE LA COHÉRENCE PÉDAGOGIQUE EN CAS DE REGROUPEMENT D'AA FAISANT L'OBJET D'UNE ÉVALUATION DISTINCTE

À définir

Partie 4 Évaluation de l'unité d'enseignement

STRUCTURE DU DISPOSITIF GÉNÉRAL D'ÉVALUATION (EN LIEN AVEC LE PROGRAMME D'ÉTUDES)

À définir

MÉTHODOLOGIE DE CONSTRUCTION DE LA NOTE FINALE DE L'UE

À définir

LA PONDÉRATION DE L'ÉVALUATION DE L'UE À DES FINS DE DÉLIBÉRATION LORS DU CALCUL DE LA MOYENNE

Au sein du programme d'études, lors du calcul de la moyenne, la pondération de l'évaluation de l'unité d'enseignement est effectuée sur base des crédits affectés à cette unité d'enseignement et évalués

MODALITÉS D'ÉVALUATION

Épreuve intégrée	Modalités d'évaluation
AIRN3012	Examen écrit en auditoire 100% (identique pour la seconde session)

MODALITÉS CONCRÈTES D'ÉVALUATION

Une mention sur la fiche informera les étudiants du fait que les précisions sur les épreuves seront disponibles sur Moodle au plus tard 6 semaines avant l'évaluation.