ECOLE INGENIEURS JULES VERNE

TITRE INGENIEUR CYBERSECURITE

REFERENTIEL D'ACTIVITES, DE COMPETENCES ET D'EVALUATION

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	REFERENTIEL D'ÉVALUATION MODALITÉS D'ÉVALUATION
Elaborer et mettre en œuvre une politique de sécurité des systèmes d'information **Activités 1.** ▪ Élaboration d'une politique et d'une stratégie de cybersécurité ▪ Mise en œuvre d'une organisation cyber sécuritaire dans le cadre légal et règlementaire	▪ Sensibiliser les directeurs et les collaborateurs aux enjeux et aux menaces cyber sécuritaires ▪ Participer à la définition des principes et des objectifs en termes de sécurité d'un système d'information ▪ Définir la stratégie cyber sécuritaire d'un Système d'informations (SI) ▪ Concevoir l'organisation ou la réorganisation de la sécurité d'un SI ▪ Intégrer les aspects juridiques et règlementaires liés au traitement, au stockage et à la protection des données	1. Etude de cas avec présentation orale 2. Examens sur table 3. Mises en situations professionnelles reconstituées

Prendre en compte les ODD et la RSE pour concevoir et maintenir en opération un dispositif de protection des SI efficient Activités 2. ▪ Conception d'une architecture de sécurité informatique globale efficiente et respectueuse de l'environnement ▪ Conduite des opérations de maintenance d'un système de sécurité durable	▪ Concevoir des architectures matérielles et logicielles sécurisées et optimisées du point de vue de leur consommation énergétique ▪ Maintenir un niveau d'équipements et de logiciels en phase avec les nouvelles technologies de cyberdéfense ▪ Gérer l'obsolescence des équipements et des composants en privilégiant la circularité ▪ Favoriser au sein des équipes internes et externes, l'adoption de règles de stockage et de traitement durables des données ▪ Adopter une conduite des opérations de type inclusive efficiente et éthique ▪ Garantir l'accès aux données informatiques pour les collaborateurs en situation de handicap selon le RGAA[1]	1. Etude de cas avec présentation orale 2. Élaboration d'une monographie écrite 3. Mises en situations professionnelles reconstituées.

[1] Référentiel Général d'Amélioration de l'Accessibilité

Intégrer le fonctionnement et la culture d'une entreprise pour gérer les hommes et les budgets **Activités 3.** ▪ Communication professionnelle et technique en anglais et en français ▪ Élaboration, présentation et défense du budget alloué à la cybersécurité ▪ Animation et motivation d'équipes multiculturelles et pluridisciplinaires	▪ Communiquer à l'oral et à l'écrit en anglais pour encadrer des équipes multiculturelles ▪ Exercer son leadership de manière à favoriser la transition numérique et la sécurisation des SI ▪ Coconstruire les objectifs avec les équipes à l'intérieur du budget alloué pour la cybersécurité ▪ Fédérer et motiver des équipes pluridisciplinaires : réseau, logiciels, utilisateurs… ▪ Elaborer et expliciter la partie du budget consacré à la cyber sécurité ▪ Récompenser l'engagement et l'efficience dans le travail réalisé par les équipes	1. Conduite de Projets 2. Mises en situations professionnelles reconstituées. 3. Projet de fin d'études

Analyser les systèmes et réseaux informatiques pour établir un diagnostic cyber sécuritaire **Activités 4.** ▪ Mise en œuvre de tests de sécurité par attaque simulée ▪ Réalisation d'un audit de sécurité complet avec préconisations d'amélioration	▪ Identifier, caractériser et cartographier les vulnérabilités et les risques inhérents à un SI ▪ Conduire des audits de sécurité en analysant les procédures et les processus de défense ▪ Effectuer des tests de pénétration (pentests) pour vérifier la robustesse des dispositifs défensifs ▪ Etablir un diagnostic global et préconiser des évolutions ▪ Proposer des solutions innovantes pour déjouer les cyber attaques	1. Etude de cas avec présentation orale 2. Conduite de Projets 3. Mises en situations professionnelles reconstituées

Piloter des projets complexes en France ou à l'international pour améliorer la protection des SI contre les cyberattaques **Activités 5.** ▪ Conception et conduite d'un projet informatique en cybersécurité ▪ Rédaction d'un cahier des charges fonctionnel et technique pour développer et mettre en place un dispositif de cybersécurité	▪ Identifier les parties prenantes d'un projet lié à la cybersécurité : commanditaire, usagers, fournisseurs… ▪ Définir les contours et les objectifs du projet pour la partie cybersécurité ▪ Établir un cahier des charges fonctionnel et technique en français et en anglais ▪ Définir les livrables en spécifiant les coûts, le niveau de qualité attendu, et les délais ▪ Mobiliser les outils, les méthodes et les indicateurs de performance pour conduire le projet ▪ Produire des livrables tels qu'attendus par le commanditaire du projet	1. Etude de cas avec présentation orale 2. Conduite de Projets 3. Mises en situations professionnelles reconstituées

Mobiliser les mathématiques et l'algorithmie pour développer des solutions logicielles sécurisées **Activités 6.** ▪ Développement ou supervision du développement d'applications logicielles sécurisées ▪ Évaluation de l'offre de solutions pour sécuriser les applications ou les systèmes d'exploitation ▪ Accompagnement des utilisateurs dans l'adoption d'un nouveau logiciel de cyberdéfense	▪ Superviser le développement ou développer des logiciels sécurisés ▪ Adapter les applications logicielles et systèmes d'exploitation existants face aux nouvelles menaces ▪ Exécuter le cahier des charges d'un développement logiciel pour la sécurisation du SI ▪ Tester la sécurité d'une nouvelle application face à des attaques concrètes simulées (Pentests) ▪ Documenter et accompagner l'utilisateur dans le maniement d'un nouvel outil logiciel de cyber sécurité	1. Etude de cas avec présentation orale 2. Examens sur table 3. Mises en situations professionnelles reconstituées

Optimiser l'anticipation et la gestion des incidents ou des crises de sécurité **Activités 7.** ▪ Gestion des cyberattaques en temps réel et en équipe ▪ Anticipation et détection en amont des intrusions dans le SI avec l'aide de l'IA ▪ Adaptation des processus et procédures de défense grâce au retour sur expérience	▪ Elaborer des procédures et processus de réponse à des incidents de sécurité ▪ Gérer en équipe pluridisciplinaire et en temps réel une cyberattaque ▪ Concevoir et mettre en place des solutions de détection d'incidents à base d'IA ▪ Exploiter l'IA pour analyser des données massives liés à des incidents de sécurité (Forensic) ▪ Capitaliser sur l'expérience de crise pour améliorer le système de sécurité du SI	1. Etude de cas avec présentation orale 2. Examens sur table 3. Mises en situations professionnelles reconstituées