EPITA

Bachelor en Sciences et Ingénierie - Sécurité du numérique

Référentiel d'activités, de compétences et d'évaluation - RNCP

Activités	Compétences	Modalités	Critères
1 - Identifier et analyser les événements de sécurité de l'entreprise ; collecter des informations techniques ou non, des Systèmes d'Information de l'entreprise ou de sources ouvertes permettant la rédaction de rapports d'incidents. 2 - Produire ou contribuer à l'élaboration de plans d'actions suite à la détection d'activités suspectes ou malveillantes.	1 - Appliquer les mathématiques, autres sciences de base ainsi que les disciplines d'ingénierie et compréhension des équipements, outils applicables, des technologies et processus techniques indispensables à la sécurité informatique, à un niveau suffisant pour atteindre les autres acquis de formation. 2 - Analyser des produits, processus et systèmes techniques dans le cadre d'un audit technique de sécurité en appliquant : • les méthodes analytiques et expérimentales existantes appropriée pour mener à bien la conception, le développement, les tests et le déploiement de solutions informatiques orientées sécurité ; • en identifiant les contraintes non techniques (sociétales, de sécurité, environnementales, économiques et industrielles), notamment dans le cadre de la gestion des risques et de la gestion des crises. 3 - Concevoir et développer des produits, processus et systèmes relevant de la sécurité informatique : • en respectant des contraintes imposées • en sélectionnant et en appliquant les méthodologies de conception appropriées • en tenant compte des aspects non techniques (sociétaux, d'hygiène et de sécurité, environnementaux, économiques et industriels).	• Mise en situation professionnelle via des études de cas pratiques nécessitant l'élaboration et la rédaction d'un état de l'art et d'un état des lieux d'un domaine d'application de la cybersécurité (réseaux, télécom, ...) sur une thématique inspirée de celles d'entreprises. • Réalisation de projets informatiques concrets basés sur des situations authentiques et sur le développement d'outils et d'applications répondant à un cahier des charges, certains projets seront construits ex nihilo tandis que d'autres partiront d'une base existante. • Projet de recherche suivant plusieurs phases : consultation et analyse de papiers scientifiques de recherche sur l'existant, élaboration d'un cahier des charges répondant au problème avec un chercheur du domaine, conception de la solution selon les méthodes scientifiques de la recherche et possible conception d'une affiche de recherche ou d'un papier de recherche sur le sujet soutenu devant le chercheur concerné.	Les méthodes utilisées sont appropriées techniquement et prennent en compte toutes les contraintes (techniques, fonctionnelles et non fonctionnelles). Les conclusions rédigées des études menées sont pertinentes. Les solutions envisagées sont réalisables et efficaces. La complexité du contexte est efficacement analysée et dans toutes ses composantes. Les productions scientifiques sont approfondies et pertinentes.

Activités	Compétences	Modalités	Critères
	4 - Mener des recherches bibliographiques, à consulter et utiliser avec un œil critique des bases de données scientifiques et d'autres sources d'informations appropriées, à réaliser des simulations et analyses afin d'approfondir les études et la recherche sur des sujets techniques dans le domaine de la cybersécurité. 5 - Concevoir et mener des études expérimentales, interpréter les données et tirer des conclusions dans le domaine de la cybersécurité dans le cadre d'audit de sécurité et de tests d'intrusion. 6 - Identifier, formuler et résoudre des problèmes complexes, à gérer des activités ou projets techniques ou professionnels dans le domaine de la sécurité informatique.		
3 – Intégrer les enjeux et le contexte de la cybermenace afin d'analyser et de pouvoir la qualifier pour produire un rapport sur le niveau d'exposition d'une organisation.	7 - Identifier les aspects non techniques (humains, sociétaux, de sécurité, environnementaux, économiques et industriels) de la pratique de l'ingénierie informatique et la gestion d'une infrastructure informatique logicielle ou physique. 8 - Identifier les problèmes économiques, organisationnels et de gestion (gestion de projet, gestion des risques et du changement...) dans le milieu industriel, des entreprises et des acteurs gouvernementaux de la cybersécurité. 9 - Consulter, appliquer et respecter les normes, codes de bonnes pratiques et les réglementations de sécurité de la cybersécurité dans le cadre de la conception de solutions informatiques orientées sécurité. 10 - Interpréter des données pertinentes et à appréhender la complexité dans la sécurité du numérique, afin d'éclairer les décisions nécessitant une réflexion sur des problèmes sociaux et éthiques importants. 11 - Formuler des recommandations aux utilisateurs, développeurs et aux décideurs suite à l'analyse du contexte de cybersécurité de l'entreprise.	• Exercices individuels et en groupes de mises en situation en prenant en compte les enjeux du développement durable, les règlementations en vigueur et les bonnes pratiques du développement pour s'assurer de la sécurité des utilisateurs et de leurs données. Ces exercices prendront la forme d'études de cas réels (ou authentiques) sur des projets techniques ayant un fort impact humain, sociétal ou environnemental et comportant une problématique à résoudre. • Évaluations sur les connaissances théoriques des normes et règlementations sous forme de soutenance, d'exposés ou de devoirs papiers. • Réalisation d'un audit de la gestion d'une entreprise et des projets techniques liés à la sécurité.	Tous les aspects non techniques et non fonctionnels impactant le projet sont identifiés. Les contraintes économiques et organisationnelles sont identifiées et leurs impacts sur le développement de solutions informatiques sont précisés. Le contexte règlementaire et ses effets sur le développement des projets sont étudiés. L'audit produit est pertinent et approfondi.

Activités	Compétences	Modalités	Critères
4 - Réaliser une veille permanente vis-à-vis des scénarii d'attaques, des nouvelles menaces, des vulnérabilités associées et sur les techniques de développement sécurisé.	12 - Communiquer des informations, idées, problèmes et solutions de manière efficace avec la communauté des ingénieurs et la société en général. 13 - Travailler de manière efficace dans un contexte national et international, en tant qu'individu et membre d'une équipe, et à collaborer de manière efficace avec des ingénieurs et non-ingénieurs, aptitude à gérer des activités ou projets techniques ou professionnels complexes dans la sécurité des systèmes d'information, en assumant la responsabilité de ses décisions. 14 - Entreprendre et innover, dans le cadre de projets personnels ou par l'initiative et l'implication au sein de l'entreprise dans des projets entrepreneuriaux. 15 - Suivre les évolutions scientifiques et technologiques dans le domaine de l'ingénierie informatique et dans le domaine de la sécurité informatique et à s'engager dans un apprentissage tout au long de la vie.	• Exercices individuels et en groupes sous forme de jeux de rôle et d'improvisation dans un contexte technique ou non, dans un contexte national ou international. • Réalisation de projets techniques et théoriques dans un environnement international piloté et proposé par des entités internationales.	Les productions développées impliquent tous les publics concernés Les moyens de communication adaptés aux publics ont été déployés. Les projets permettent développer des solutions innovantes. La dimension internationale est prise en compte dans toutes les productions pertinentes.
5 - Administrer et paramétrer des solutions de sécurité en assurant leur fonctionnement optimal, le traitement des journaux d'activités et leur conformité aux normes en vigueur, notamment les outils de détection des menaces.	16 - Concevoir, développer, tester et déployer des solutions informatiques orientées sécurité. 17 - Planifier et gérer des projets en prenant en compte la gestion des risques et la gestion de crises afin de garantir la réalisation et la pérennité du projet. 18 - Formuler des recommandations aux développeurs de solutions informatique et former les utilisateurs et clients aux bonnes pratiques de l'utilisation de la solution.	• Réalisation d'un projet informatique en plusieurs phases : création d'un site web sécurisé prenant en compte les bonnes pratiques techniques préconisées, déploiement manuel puis automatique du site "on premise" ou sur une infrastructure cloud, mise en place de la remontée des logs du site pour automatiser les actions de sécurité et scénarii blue/red team selon des temporalités prévues et inattendues pour garantir la résilience du produit. Ce projet sera défendu lors d'une soutenance.	Les projets développés intègrent la problématique de sécurité. Tous les facteurs de risques ont été pris en compte. Les projets produits sont résilients et les propositions d'amélioration de sécurité sont pertinentes.

Activités	Compétences	Modalités	Critères
6 - Concevoir et développer des solutions de sécurité : outils d'investigation, d'analyse des journaux d'activité et de détection d'intrusion. 7 - Contribuer à la définition de l'architecture technique des Systèmes d'Information en lien avec les équipes concernées. 8 - Mettre en œuvre la recette, l'industrialisation et la mise en production d'une solution de sécurité en lien avec le responsable du projet.		• Conception d'outils d'intrusion individuellement et par équipe sur différents systèmes d'exploitation et sur différentes applications en mode blue/red team.	Les scénarii d'attaque/défense sont bien analysés et la réponse apportée est appropriée.
9 - Réaliser des audits techniques sur les Systèmes d'Information de l'entreprise pour	19 - Évaluer le niveau de sécurité d'un système d'information. 20 - Définir des politiques de sécurité afin de les mettre en œuvre dans l'entreprise.	• Réalisation d'un audit technique de sécurité (offensif) en utilisant des méthodes d'osint, de cartographie et de pentest notamment. Cet audit fera l'objet d'un rapport qui identifiera les points	Les sources de risques sont toutes identifiées. Les tests de sécurité ont été réalisés.

Activités	Compétences	Modalités	Critères
évaluer leur robustesse. 10 - Réaliser ou piloter la mise en œuvre de scans de vulnérabilités et de contrôles techniques, en continu et de manière automatisée.		faibles du produit audité, qui pourra être un système d'information, une machine distante ou tout autre produit potentiellement vulnérable. • Mise en situation professionnelle au travers de sénarii red/blue team visant à construire une infrastructure de bout en bout et à la défendre/l'attaquer. • Réalisation d'un audit de systèmes d'information existants ou fictifs explicitant les politiques de sécurité mises en place et celles devant être mises en place sous la forme d'un rapport et/ou d'une soutenance.	Les propositions pour garantir la sécurité sont adaptées au contexte, à la nature et au niveau de risque. Les politiques de sécurité sont explicitées.