EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ECSF

CADRE EUROPÉEN DES COMPÉTENCES EN CYBERSÉCURITÉ

SEPTEMBRE 2022

À PROPOS DE L'ENISA

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union chargée d'atteindre un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'UE sur la cybersécurité, l'Agence de l'Union européenne pour la cybersécurité contribue à la politique de l'UE en matière de cybersécurité, renforce la fiabilité des produits, services et processus TIC grâce à des schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'UE, et aide l'Europe à se préparer aux cyber défis de demain. Grâce au partage des connaissances, au renforcement des capacités et à la sensibilisation, l'Agence collabore avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, renforcer la résilience des infrastructures de l'Union et, par conséquent, préserver la sécurité numérique de la société et des citoyens européens. De plus amples informations sur l'ENISA et ses travaux sont disponibles à l'adresse suivante : www.enisa.europa.eu.

CONTACT

Pour contacter l'éditeur, veuillez utiliser l'adresse euskills@enisa.europa.eu.

REMERCIEMENTS

Ce cadre est le résultat de l'avis et de l'accord des experts du groupe de travail ad hoc sur le cadre des compétences composé d'Agata BEKIER, Vladlena BENSON, Jutta BREYER*, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta POLEMI*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN et Jan HAJNY.

Fabio DI FRANCO et Athanasios GRAMMATOPOULOS ont dirigé cette activité pour l'ENISA.

AVIS JURIDIQUE

AVIS DE DROIT D'AUTEUR

ISBN : 978-92-9204-584-5 – DOI : 10.2824/859537

TABLE DES MATIÈRES

1. VUE D'ENSEMBLE

Responsable de la sécurité de l'information (CISO)

Intervenant en cas de cyber incident

Responsable juridique, politique et conformité en cybersécurité

Spécialiste du renseignement sur les cybermenaces

Architecte en cybersécurité

Auditeur en cybersécurité

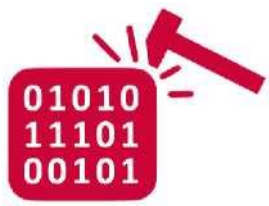
Éducateur en cybersécurité

Spécialiste de la mise en œuvre de la cybersécurité

Chercheur en cybersécurité

Gestionnaire de risques en cybersécurité

Enquêteur en criminalistique numérique



Testeurs d'intrusions

2. PROFILES

2.1 RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (CISO)

Titre du profil	Responsable de la sécurité de l'information (CISO)
Titre(s) alternatif(s)	Directeur du programme de cybersécurité Chargé de sécurité de l'information (ISO) Responsable de la sécurité de l'information Chef de la sécurité de l'information Responsable IT/TIC
Récapitulatif	Gère la stratégie de cybersécurité d'une organisation et sa mise en œuvre afin de garantir que les systèmes, services et actifs numériques soient correctement sécurisés et protégés.
Mission	Définit, maintient et communique la vision, la stratégie, les politiques et les procédures en matière de cybersécurité. Gère la mise en œuvre de la politique de cybersécurité dans l'ensemble de l'organisation. Assure l'échange d'informations avec les autorités externes et les organismes professionnels.
Élément(s) livrable(s)	• Stratégie de cybersécurité • Politique de cybersécurité
Tâche(s) principale(s)	• Définir, mettre en œuvre, communiquer et maintenir les objectifs, les exigences, les stratégies et les politiques de cybersécurité, alignés sur la stratégie commerciale pour soutenir les objectifs organisationnels • Préparer et présenter la vision, les stratégies et les politiques de cybersécurité pour approbation par la haute direction de l'organisation et assurer leur exécution • Superviser l'application et l'amélioration du Système de gestion de la sécurité de l'information (SGSI) • Sensibiliser la haute direction aux risques et menaces en matière de cybersécurité et à leur impact sur l'organisation • S'assurer que la direction générale approuve ces risques de cybersécurité • Élaborer des plans de cybersécurité • Développer des relations avec les autorités et les communautés liées à la cybersécurité • Signaler les incidents, les risques et les constatations à la haute direction • Suivre les progrès en matière de cybersécurité • Sécuriser les ressources pour mettre en œuvre la stratégie de cybersécurité • Négocier le budget de cybersécurité avec la direction générale • Assurer la résilience de l'organisation face aux cyberincidents • Gérer le renforcement continu des capacités au sein de l'organisation • Examiner, planifier et allouer les ressources appropriées en matière de cybersécurité
Compétence(s) clé(s)	• Évaluer et améliorer la posture de cybersécurité d'une organisation • Analyser et mettre en œuvre des politiques, certifications, normes, méthodologies et cadres en matière de cybersécurité • Analyser et se conformer aux lois, réglementations et législations liées à la cybersécurité • Mettre en œuvre les recommandations et les meilleures pratiques en matière de cybersécurité • Gérer les ressources de cybersécurité • Développer, défendre et diriger l'exécution d'une stratégie de cybersécurité • Influencer la culture de cybersécurité d'une organisation • Concevoir, appliquer, surveiller et réviser le Système de gestion de la sécurité de l'information (SGSI), soit directement, soit en dirigeant son externalisation • Examiner et améliorer les documents de sécurité, les rapports, les SLA et assurer l'atteinte des objectifs de sécurité • Identifier et résoudre les problèmes liés à la cybersécurité • Établir un plan de cybersécurité • Communiquer, coordonner et coopérer avec les parties prenantes internes et externes

	• Anticiper les changements nécessaires à la stratégie de sécurité de l'information de l'organisation et formuler de nouveaux plans • Définir et appliquer des modèles de maturité pour la gestion de la cybersécurité • Anticiper les menaces, les besoins et les défis à venir en matière de cybersécurité • Motiver et encourager les équipes	
Connaissances clés	• Politiques de cybersécurité • Normes, méthodologies et cadres de cybersécurité • Recommandations et bonnes pratiques en matière de cybersécurité • Lois, réglementations et législations relatives à la cybersécurité • Certifications liées à la cybersécurité • Exigences éthiques en matière d'organisation de la cybersécurité • Modèles de maturité en matière de cybersécurité • Procédures de cybersécurité • Gestion des ressources • Pratiques de gestion • Normes, méthodologies et cadres de gestion des risques	
e-Compétences (de e-CF)	A.7. Surveillance des tendances technologiques D.1. Élaboration d'une stratégie de sécurité de l'information E.3. Gestion des risques E.8. Gestion de la sécurité de l'information E.9. Gouvernance des SI	Niveau 4 Niveau 5 Niveau 4 Niveau 4 Niveau 5

2.2 CYBER INCIDENT RESPONDER (INTERVENANT EN CAS DE CYBER INCIDENT)

Titre du profil	Cyber incident responder
Titre(s) alternatif(s)	Gestionnaire d'incidents cybernétiques Expert en crise cybernétique Ingénieur d'intervention en cas d'incident Analyste du Centre des opérations de sécurité Cyber Fighter / Défenseur Analyste des opérations de sécurité (SOC Analyst) Gestionnaire SIEM cybersécurité
Récapitulatif	Surveiller l'état de cybersécurité de l'organisation, gérer les incidents lors des cyberattaques et assurer la continuité des opérations des systèmes TIC.
Mission	Surveille et évalue l'état de cybersécurité des systèmes. Analyse, évalue et atténue l'impact des incidents de cybersécurité. Identifie les causes profondes des cyber incidents et les acteurs malveillants. Conformément au plan de réaction aux incidents de l'organisation, rétablit les fonctionnalités des systèmes et des processus dans un état opérationnel, en recueillant des éléments probants et en documentant les mesures prises.
Élément(s) livrable(s)	• Plan d'intervention en cas d'incident • Rapport d'incident cybernétique
Tâche(s) principale(s)	• Contribuer à l'élaboration, à la mise à jour et à l'évaluation du plan d'intervention en cas d'incident • Élaborer, mettre en œuvre et évaluer les procédures liées à la gestion des incidents • Identifier, analyser, atténuer et communiquer les incidents de cybersécurité • Évaluer et gérer les vulnérabilités techniques • Mesurer l'efficacité de la détection et de la réponse aux incidents de cybersécurité • Évaluer la résilience des contrôles de cybersécurité et des mesures d'atténuation prises à la suite d'un incident de cybersécurité ou d'une violation de données • Adopter et développer des techniques de test de gestion des incidents • Établir des procédures pour l'analyse des résultats des incidents et les rapports sur le traitement des incidents • Documenter l'analyse des résultats des incidents et les actions de gestion des incidents • Coopérer avec les centres d'opérations sécurisées (SOC) et les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) • Coopérer avec le personnel concerné pour signaler les incidents de sécurité conformément au cadre juridique applicable
Compétence(s) clé(s)	• Mettre en pratique tous les aspects techniques, fonctionnels et opérationnels de la gestion et de la réponse aux incidents de cybersécurité • Recueillir, analyser et corréler des informations sur les cybermenaces provenant de sources multiples • Travailler sur les systèmes d'exploitation, les serveurs, les clouds et les infrastructures pertinentes • Travail sous pression • Communiquer, présenter et faire un rapport aux parties prenantes concernées • Gérer et analyser les fichiers journaux
Connaissances clés	• Normes, méthodologies et cadres de traitement des incidents • Recommandations et meilleures pratiques en matière de gestion des incidents • Outils de gestion des incidents • Procédures de communication pour la gestion des incidents • Sécurité des systèmes d'exploitation • Sécurité des réseaux informatiques • Cybermenaces • Procédures d'attaque de cybersécurité • Vulnérabilités des systèmes informatiques • Certifications liées à la cybersécurité • Lois, réglementations et législations relatives à la cybersécurité • Opération des centres d'opérations sécurisées (COS) • Opération des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT)

e-Compétences (de e-CF)	A.7. Surveillance des tendances technologiques B.2. Intégration de composant B.3. Essais B.5. Production de la documentation C.4. Gestion des problèmes	Niveau 3 Niveau 2 Niveau 3 Niveau 3 Niveau 4

2.3 RESPONSABLE JURIDIQUE, POLITIQUE ET CONFORMITE EN CYBERSECURITE

Titre du profil	Responsable juridique, politique et conformité en cybersécurité
Titre(s) alternatif(s)	Délégué à la protection des données (DPD) Responsable de la protection de la vie privée Consultant en droit cybernétique Conseiller juridique cybernétique Responsable de la gouvernance de l'information Responsable de la conformité des données Conseiller juridique en cybersécurité Responsable de la conformité informatique/TIC Consultant en Conformité aux Risques de Gouvernance (GRC)
Récapitulatif	Gère le respect des normes, des cadres juridiques et réglementaires liés à la cybersécurité en fonction de la stratégie de l'organisation et des exigences légales.
Mission	Supervise et assure le respect des cadres et politiques juridiques, réglementaires et liés à la cybersécurité et aux données, conformément à la stratégie et aux exigences légales de l'organisation. Contribue aux actions de l'organisation en matière de protection des données. Fournit des conseils juridiques dans le cadre de l'élaboration des processus de gouvernance de la cybersécurité de l'organisation et recommande des stratégies/solutions de remédiation pour garantir la conformité.
Élément(s) livrable(s)	• Manuel de conformité • Rapport de conformité
Tâche(s) principale(s)	• Garantir le respect des normes, lois et réglementations en matière de protection des données et fournir des conseils et des orientations juridiques en la matière • Identifier et documenter les lacunes en matière de conformité • Evaluer les facteurs relatifs à la vie privée et élaborer, tenir à jour, communiquer et former sur les politiques et procédures en matière de protection de la vie privée • Appliquer et faire valoir le programme de confidentialité et de protection des données de l'organisation. • Veiller à ce que les propriétaires, les détenteurs, les responsables du traitement, les sous-traitants, les personnes concernées, les partenaires internes ou externes et les entités soient informés de leurs droits, obligations et responsabilités en matière de protection des données. • Agir en tant que point de contact clé pour traiter les demandes et les plaintes concernant le traitement des données • Aider à la conception, à la mise en œuvre, à l'audit et aux tests de conformité afin de garantir la cybersécurité et la conformité à la vie privée • Suivre les audits et les activités de formation liées à la protection des données • Coopérer et partager des informations avec les autorités et les groupes professionnels • Contribuer à l'élaboration de la stratégie, de la politique et des procédures de cybersécurité de l'organisation • Développer et proposer une formation de sensibilisation du personnel pour atteindre la conformité et favoriser une culture de protection des données au sein de l'organisation • Gérer les aspects juridiques des responsabilités en matière de sécurité de l'information et des relations avec les tiers
Compétence(s) clé(s)	• Compréhension globale de la stratégie commerciale, des modèles et des produits et capacité à tenir compte des exigences juridiques, réglementaires et normatives • Mettre en œuvre des pratiques de protection des données et de la vie privée dans le cadre de la mise en œuvre des processus organisationnels, de la stratégie financière et de la stratégie commerciale. • Diriger l'élaboration de politiques et de procédures appropriées en matière de cybersécurité et de protection de la vie privée qui complètent les besoins de l'entreprise et les exigences légales ; assurer en outre son acceptation, sa compréhension et sa mise en œuvre, et les communiquer à tous les parties concernées • Effectuer, surveiller et examiner les évaluations des facteurs relatifs à la vie privée à l'aide de normes, de cadres, de méthodes et d'outils reconnus • Expliquer et communiquer les sujets relatifs à la protection des données et à la vie privée aux parties prenantes et aux utilisateurs • Comprendre, utiliser et respecter les exigences et les normes éthiques • Comprendre les implications des modifications du cadre juridique sur la stratégie et les politiques de l'organisation en matière de cybersécurité et de protection des données

Connaissances clés	• Collaborer avec d'autres membres de l'équipe et collègues • Lois, réglementations et législations liées à la cybersécurité • Normes, méthodologies et cadres de cybersécurité • Politiques de cybersécurité • Exigences, recommandations et pratiques exemplaires en matière de conformité juridique, réglementaire et législative • Normes, méthodologies et cadres d'évaluation des facteurs relatifs à la vie privée	
Compétences en ligne (à partir de e-CF)	A.1. Systèmes d'information et stratégie d'entreprise Alignement D.1. Élaboration d'une stratégie de sécurité de l'information E.8. Gestion de la sécurité de l'information E.9. Gouvernance des SI	Niveau 4 Niveau 4 Niveau 3 Niveau 4

2.4 SPÉCIALISTE DU RENSEIGNEMENT SUR LES CYBERMENANCES

Titre du profil	Spécialiste du renseignement sur les cybermenaces
Titre(s) alternatif(s)	Analyste en cyber-intelligence Modélisateur de cybermenaces Spécialiste en Cyber Threat Intelligence (CTI)
Récapitulatif	Recueillir, traiter, analyser des données et des informations pour produire des rapports de renseignement exploitables et les diffuser auprès des parties prenantes ciblées.
Mission	Gère le cycle de vie des renseignements sur les cybermenaces, y compris la collecte, l'analyse et la production de renseignements exploitables et leur diffusion aux intervenants en sécurité et à la communauté CTI, aux niveaux tactique, opérationnel et stratégique. Identifie et surveille les tactiques, techniques et procédures (TTP) utilisées par les acteurs de la cybermenace et leurs tendances, suit les activités des acteurs de la menace et observe comment les événements non cybernétiques peuvent influencer les actions liées à la cybercriminalité.
Élément(s) livrable(s)	• Manuel de renseignement sur les cybermenaces • Rapport sur les cybermenaces
Tâche(s) principale(s)	• Élaborer, mettre en œuvre et gérer la stratégie de renseignement sur les cybermenaces de l'organisation • Élaborer des plans et des procédures pour gérer les renseignements sur les menaces • Traduire les exigences de l'entreprise en exigences de renseignement • Mettre en œuvre la collecte de renseignements sur les menaces, l'analyse et la production de renseignements exploitables et la diffusion aux parties prenantes de la sécurité • Identifier et évaluer les acteurs des cybermenaces ciblant l'organisation • Identifier, surveiller et évaluer les tactiques, techniques et procédures (TTP) utilisées par les acteurs de la cybermenace en analysant les données, informations et renseignements open source et propriétaires • Produire des rapports exploitables basés sur des données de renseignements sur les menaces • Élaborer et conseiller sur les plans d'atténuation aux niveaux tactique, opérationnel et stratégique • Coopérer avec les parties prenantes pour partager et utiliser des renseignements pertinents sur les cybermenaces • Tirer parti des données de renseignement pour soutenir et aider à la modélisation des menaces, aux recommandations pour l'atténuation des risques et à la chasse aux cybermenaces • Formuler et communiquer des renseignements ouvertement et publiquement à tous les niveaux • Informer sur la gravité relative de la sécurité en expliquant l'exposition au risque et ses conséquences aux parties prenantes non initiées
Compétence(s) clé(s)	• Collaborer avec d'autres membres de l'équipe et collègues • Recueillir, analyser et corréler des informations sur les cybermenaces provenant de sources multiples • Identifier les TTP et les campagnes des acteurs de la menace • Automatiser les procédures de gestion des renseignements sur les menaces • Effectuer des analyses techniques et rédiger des rapports • Identifier les événements non cybernétiques ayant des implications sur les activités liées au cyberespace • Modéliser les menaces, les acteurs et les TTP • Communiquer, coordonner et coopérer avec les parties prenantes internes et externes • Communiquer, présenter et faire rapport aux parties prenantes concernées • Utiliser et appliquer les plateformes et outils CTI

Connaissances clés	• Sécurité des systèmes d'exploitation • Sécurité des réseaux informatiques • Contrôles et solutions de cybersécurité • Programmation informatique • Normes, méthodologies et cadres de partage des informations sur les cybermenaces (CTI) • Procédures de divulgation d'informations sensibles • Connaissances inter domaines et transfrontalières liées à la cybersécurité • Cybermenaces • Acteurs dans le domaine des cybermenaces • Procédures d'attaque de cybersécurité • Cybermenaces avancées et persistantes (APT) • Tactiques, Techniques et Procédures (TTP) des acteurs de la menace • Certifications liées à la cybersécurité	
e-Compétences (de e-CF)	B.5. Production de la documentation D.7. Science et analyse des données D.10. Gestion de l'information et des connaissances E.4. Gestion des relations E.8. Gestion de la sécurité de l'information	Niveau 3 Niveau 4 Niveau 4 Niveau 3 Niveau 4

2.5 ARCHITECTE DE CYBERSÉCURITÉ

Titre du profil	Architecte en cybersécurité
Titre(s) alternatif(s)	Architecte de solutions de cybersécurité Concepteur de cybersécurité Architecte de la sécurité des données
État récapitulatif	Planifier et concevoir des solutions de sécurité dès la conception (infrastructures, systèmes, actifs, logiciels, matériel et services) et des contrôles de cybersécurité.
Mission	Concevoir des solutions basées sur les principes de sécurité et de respect de la vie privée dès la conception. Créer et améliorer continuellement des modèles architecturaux et développe une documentation et des spécifications architecturales appropriées. Coordonner le développement, l'intégration et la maintenance sécurisés des composants de cybersécurité conformément aux normes et autres exigences connexes.
Élément(s) livrable(s)	• Schéma de l'architecture de cybersécurité • Rapport sur les exigences en matière de cybersécurité
Tâche(s) principale(s)	• Concevoir et proposer une architecture sécurisée pour mettre en œuvre la stratégie de l'organisation • Développer l'architecture de cybersécurité de l'organisation pour répondre aux exigences en matière de sécurité et de confidentialité • Produire de la documentation architecturale et des spécifications • Présenter la conception de l'architecture de sécurité de haut niveau aux parties prenantes • Établir un environnement sécurisé tout au long du cycle de développement des systèmes, services et produits • Coordonner le développement, l'intégration et la maintenance des composants de cybersécurité garantissant les spécifications de cybersécurité • Analyser et évaluer la cybersécurité de l'architecture de l'organisation • Assurer la sécurité des architectures de solutions par le biais d'examens de sécurité et de certification • Collaborer avec d'autres équipes et collègues • Évaluer l'impact des solutions de cybersécurité sur la conception et la performance de l'architecture de l'organisation • Adapter l'architecture de l'organisation aux menaces émergentes • Évaluer l'architecture mise en œuvre pour maintenir un niveau de sécurité approprié
Compétence(s) clé(s)	• Effectuer une analyse des exigences de sécurité des utilisateurs et de l'entreprise • Etablir des spécifications architecturales et fonctionnelles en matière de cybersécurité • Décomposer et analyser les systèmes pour développer des besoins liés à la sécurité et la confidentialité et identifier des solutions efficaces • Concevoir des systèmes et des architectures basés sur les principes de sécurité « security and privacy by design » et « by defaults ». • Guider et communiquer avec les responsables de la mise en œuvre et le personnel IT/OT • Communiquer, présenter et faire des rapports aux parties prenantes concernées • Proposer des architectures de cybersécurité en fonction des besoins et du budget des parties prenantes • Sélectionner les spécifications, procédures et contrôles appropriés • Renforcer la résilience face aux points de défaillance dans toute l'architecture • Coordonner l'intégration des solutions de sécurité

Connaissances clés	• Certifications liées à la cybersécurité • Recommandations et bonnes pratiques en matière de cybersécurité • Normes, méthodologies et cadres de cybersécurité • Analyse des exigences liées à la cybersécurité • Sécuriser le cycle de vie du développement • Modèles de référence de l'architecture de sécurité • Technologies liées à la cybersécurité • Contrôles et solutions de cybersécurité • Risques de cybersécurité • Cybermenaces • Tendances en matière de cybersécurité • Exigences, recommandations et pratiques exemplaires en matière de conformité juridique, réglementaire et législative • Procédures de cybersécurité héritées • Technologies d'amélioration de la vie privée (PET) • Normes, méthodologies et cadres de protection de la vie privée dès la conception	
e-Compétences (de e-CF)	A.5. Design d'architecture A.6. Conception de l'application 8.1. Développement d'applications 8.3. Essais 8.6. Ingénierie des systèmes TIC	Niveau 5 Niveau 3 Niveau 3 Niveau 3 Niveau 4

2.6 AUDITEUR EN CYBERSÉCURITÉ

Titre du profil	Auditeur en cybersécurité
Titre(s) alternatif(s)	Auditeur de la sécurité de l'information (auditeur informatique ou juridique) Auditeur de la conformité aux risques de gouvernance (GRC) Responsable de l'audit en cybersécurité Auditeur des procédures et processus de cybersécurité Auditeur des risques et de la conformité en matière de sécurité de l'information Analyste de l'évaluation de la protection des données
Récapitulatif	Réaliser des audits de cybersécurité sur l'écosystème de l'organisation. Assurer la conformité avec les informations juridiques, réglementaires et politiques, les exigences de sécurité, les normes de l'industrie et les bonnes pratiques.
Mission	Effectue des examens indépendants pour évaluer l'efficacité des processus et des contrôles et la conformité globale avec les politiques des cadres juridiques et réglementaires de l'organisation. Évalue, teste et vérifie les produits liés à la cybersécurité (systèmes, matériel, logiciels et services), les fonctions et les politiques garantissant le respect des lignes directrices, des normes et des réglementations.
Élément(s) livrable(s)	• Plan d'audit de cybersécurité • Rapport d'audit de cybersécurité
Tâche(s) principale(s)	• Élaborer la politique, les procédures, les normes et les lignes directrices de l'organisation en matière d'audit • Établir les méthodologies et les pratiques utilisées pour l'audit des systèmes • Établir l'environnement cible et gérer les activités d'audit • Définir la portée, les objectifs et les critères de l'audit • Élaborer un plan d'audit décrivant les cadres, les normes, la méthodologie, les procédures et les tests d'audit • Examiner l'objectif de l'évaluation, les objectifs et les exigences en matière de sécurité sur la base du profil de risque • Vérification du respect des lois et réglementations applicables en matière de cybersécurité • Vérification de la conformité aux normes applicables en matière de cybersécurité • Exécuter le plan d'audit et recueillir des éléments probants et des mesures • Maintenir et protéger l'intégrité des dossiers d'audit • Élaborer et communiquer des rapports d'évaluation de la conformité, d'assurance, d'audit, de certification et d'entretien • Surveiller les activités d'assainissement des risques
Compétence(s) clé(s)	• Organiser et travailler de manière systématique et déterministe sur la base de données probantes • Suivre et mettre en pratique les cadres, les normes et les méthodologies d'audit • Appliquer des outils et des techniques d'audit • Analyser les processus métier, évaluer et réviser la sécurité des logiciels ou du matériel, ainsi que les contrôles techniques et organisationnels • Décomposer et analyser les systèmes pour identifier les faiblesses et les contrôles inefficaces • Communiquer, expliquer et adapter les exigences légales et réglementaires et les besoins de l'entreprise • Collecter, évaluer, maintenir et protéger les informations d'audit • Audit avec intégrité, impartialité et indépendance
Connaissances clés	• Contrôles et solutions de cybersécurité • Exigences, recommandations et pratiques exemplaires en matière de conformité juridique, réglementaire et législative • Surveillance, test et évaluation de l'efficacité des audits de cybersécurité • Normes, méthodologies et cadres d'évaluation de la conformité • Normes, méthodologies et cadres d'audit • Normes, méthodologies et cadres de cybersécurité • Certification liée à l'audit • Certifications liées à la cybersécurité

e-Compétences (de e-CF)	B.3. Essais B.5. Production de la documentation E.3. Gestion des risques E.6 Gestion de la qualité des TIC E.8. Gestion de la sécurité de l'information	Niveau 4 Niveau 3 Niveau 4 Niveau 4 Niveau 4

2.7 ÉDUCATEUR EN CYBERSÉCURITÉ

Titre du profil	Éducateur en cybersécurité	
Titre(s) alternatif(s)	Spécialiste de la sensibilisation à la cybersécurité Formateur en cybersécurité Faculté de cybersécurité (professeur, maître de conférences)	
État récapitulatif	Améliore les connaissances, les aptitudes et les compétences des personnes en matière de cybersécurité.	
Mission	Concevoir, développer et mener des programmes de sensibilisation, de formation et d'éducation sur des sujets liés à la cybersécurité et à la protection des données. Utiliser des méthodes, des techniques et des instruments d'enseignement et de formation appropriés pour communiquer et améliorer la culture, les capacités, les connaissances et les compétences des ressources humaines en matière de cybersécurité. Promouvoir l'importance de la cybersécurité et la consolider dans l'organisation.	
Élément(s) livrable(s)	• Programme de sensibilisation à la cybersécurité • Matériel de formation en cybersécurité	
Tâche(s) principale(s)	• Élaborer, mettre à jour et fournir des programmes de cybersécurité et de protection des données et du matériel éducatif pour la formation et la sensibilisation sur la base du contenu, de la méthode, des outils et des besoins des stagiaires • Organiser, concevoir et fournir des activités de sensibilisation à la cybersécurité et à la protection des données, des séminaires, des cours et des formations pratiques • Surveiller, évaluer et rendre compte de l'efficacité de la formation • Évaluer et rendre compte des performances du stagiaire • Trouver de nouvelles approches en matière d'éducation, de formation et de sensibilisation • Concevoir, développer et fournir des simulations de cybersécurité, des laboratoires virtuels ou des environnements de cyber-gamme • Fournir des conseils sur les programmes de certification de cybersécurité pour les particuliers • Maintenir et améliorer continuellement l'expertise ; encourager et autonomiser l'amélioration continue et le renforcement des capacités en matière de cybersécurité	
Compétence(s) clé(s)	• Identifier les besoins en matière de sensibilisation, de formation et d'éducation à la cybersécurité • Concevoir, élaborer et mettre en œuvre des programmes d'apprentissage pour répondre aux besoins en matière de cybersécurité • Élaborer des exercices de cybersécurité, y compris des simulations à l'aide d'environnements de portée cybernétique • Proposer une formation en vue de certifications professionnelles en matière de cybersécurité et de protection des données • Utiliser les ressources de formation existantes en matière de cybersécurité • Élaborer des programmes d'évaluation pour les activités de sensibilisation, de formation et d'éducation • Communiquer, présenter et faire rapport aux parties prenantes concernées • Identifier et sélectionner les approches pédagogiques appropriées pour le public visé • Motiver et encourager les personnes	
Connaissances clés	• Normes, méthodologies et cadres pédagogiques • Élaboration de programmes de sensibilisation, d'éducation et de formation en matière de cybersécurité • Certifications liées à la cybersécurité • Normes, méthodologies et cadres d'éducation et de formation en matière de cybersécurité • Lois, réglementations et législations relatives à la cybersécurité • Recommandations et bonnes pratiques en matière de cybersécurité • Normes, méthodologies et cadres de cybersécurité • Contrôles et solutions de cybersécurité	
e-Compétences (de e-CF)	D.3. Services d'éducation et de formation D.9. Développement du personnel E.8. Gestion de la sécurité de l'information	Niveau 3 Niveau 3 Niveau 3

2.8 SPECIALISTE DE LA MISE EN ŒUVRE DE LA CYBERSÉCURITÉ

Titre du profil	Spécialiste de la mise en œuvre de la cybersécurité	
Titre(s) alternatif(s)	Cybersecurity implementer Spécialiste de la mise en œuvre de la sécurité de l'information Expert en solutions de cybersécurité Développeur en cybersécurité Ingénieur en cybersécurité Ingénieur Développement, Sécurité & Opérations (DevSecOps)	
Récapitulatif	Développer, déployer et exploiter des solutions de cybersécurité (systèmes, actifs, logiciels, contrôles et services) sur les infrastructures et les produits.	
Mission	Assurer le développement technique, l'intégration, les tests, la mise en œuvre, l'exploitation, la maintenance, la surveillance et le soutien liés à la cybersécurité des solutions de cybersécurité. Garantir le respect des spécifications et des exigences de conformité, assurer de bonnes performances et résoudre les problèmes techniques requis dans les solutions de cybersécurité de l'organisation (systèmes, actifs, logiciels, contrôles et services), les infrastructures et les produits.	
Élément(s) livrable(s)	• Solutions de cybersécurité	
Tâche(s) principale(s)	• Développer, mettre en œuvre, maintenir, mettre à niveau, tester des produits de cybersécurité • Fournir une assistance liée à la cybersécurité aux utilisateurs et aux clients • Intégrer des solutions de cybersécurité et assurer leur bon fonctionnement • Configurer en toute sécurité les systèmes, les services et les produits • Maintenir et améliorer la sécurité des systèmes, des services et des produits • Mettre en œuvre des procédures et des contrôles de cybersécurité • Surveiller et assurer la performance des contrôles de cybersécurité mis en œuvre • Documenter et rendre compte de la sécurité des systèmes, des services et des produits • Travailler en étroite collaboration avec le personnel IT/OT sur les actions liées à la cybersécurité • Mettre en œuvre, appliquer et gérer des correctifs aux produits pour remédier aux vulnérabilités techniques	
Compétence(s) clé(s)	• Communiquer, présenter et faire des rapports aux parties prenantes concernées • Intégrer des solutions de cybersécurité à l'infrastructure de l'organisation • Configurer les solutions en fonction de la politique de sécurité de l'organisation • Évaluer la sécurité et la performance des solutions • Développer du code, des scripts et des programmes • Identifier et résoudre les problèmes liés à la cybersécurité • Collaborer avec d'autres membres de l'équipe et collègues	
Connaissances clés	• Cycle de développement sécurisé • Programmation informatique • Sécurité des systèmes d'exploitation • Sécurité des réseaux informatiques • Contrôles et solutions de cybersécurité • Pratiques de sécurité offensives et défensives • Recommandations et bonnes pratiques en matière de codage sécurisé • Recommandations et bonnes pratiques en matière de cybersécurité • Normes, méthodologies et cadres d'essai • Procédures d'essai • Technologies liées à la cybersécurité	
e-Compétences (de e-CF)	A.5. Design d'architecture A.6. Conception de l'application 8.1. Développement d'applications 8.3. Essais 8.6. Ingénierie des systèmes TIC	Niveau 3 Niveau 3 Niveau 3 Niveau 3 Niveau 4

2.9 CHERCHEUR EN CYBERSÉCURITÉ

Titre du profil	Chercheur en cybersécurité	
Titre(s) alternatif(s)	Ingénieur de recherche en cybersécurité Directeur de la recherche en cybersécurité (CRO) Chargé de recherche principal en cybersécurité Chargé de recherche et développement (R&D) en cybersécurité Personnel scientifique en cybersécurité Chargé de recherche et d'innovation/Expert en cybersécurité Chercheur en cybersécurité	
Récapitulatif	Effectuer des recherches dans le domaine de la cybersécurité et intégrer les résultats dans les solutions de cybersécurité.	
Mission	Mener des recherches fondamentales/de base et appliquées, et faciliter l'innovation dans le domaine de la cybersécurité grâce à la coopération avec d'autres parties prenantes. Analyser les tendances et les découvertes scientifiques en matière de cybersécurité.	
Élément(s) livrable(s)	• Publication dans le domaine de la cybersécurité	
Tâche(s) principale(s)	• Analyser et évaluer les technologies, les solutions, les développements et les processus de cybersécurité • Mener des travaux de recherche, d'innovation et de développement sur des sujets liés à la cybersécurité • Formuler et émettre des idées de recherche et d'innovation • Faire progresser l'état actuel des connaissances sur les sujets liés à la cybersécurité • Aider au développement de solutions innovantes liées à la cybersécurité • Mener des expériences et développer une démonstration de faisabilité, des pilotes et des prototypes pour les solutions de cybersécurité • Sélectionner et appliquer des cadres, des méthodes, des normes, des outils et des protocoles, y compris la construction et la mise à l'essai d'une démonstration de faisabilité pour soutenir les projets • Contribuer à l'élaboration d'idées, de services et de solutions commerciales de pointe en matière de cybersécurité • Aider au renforcement des capacités liées à la cybersécurité, y compris la sensibilisation, la formation théorique, la formation pratique, les tests, le mentorat, la supervision et le partage • Identifier les réalisations intersectorielles en matière de cybersécurité et les appliquer dans un contexte différent ou proposer des approches et des solutions innovantes • Diriger ou participer aux processus et projets d'innovation, y compris la gestion de projet et la budgétisation • Publier et présenter des travaux scientifiques et des résultats de recherche et développement	
Compétence(s) clé(s)	• Générer de nouvelles idées et transférer la théorie dans la pratique • Décomposer et analyser les systèmes pour identifier les faiblesses et les contrôles inefficaces • Décomposer et analyser les systèmes pour développer des besoins en matière de sécurité et de confidentialité et identifier des solutions efficaces • Surveiller les nouvelles avancées dans les technologies liées à la cybersécurité • Communiquer, présenter et faire des rapports aux parties prenantes concernées • Identifier et résoudre les problèmes liés à la cybersécurité • Collaborer avec d'autres membres de l'équipe et collègues	
Connaissances clés	• Recherche, développement et innovation (RDI) dans le domaine de la cybersécurité • Normes, méthodologies et cadres de cybersécurité • Exigences légales, réglementaires et législatives relatives à la diffusion ou à l'utilisation de technologies liées à la cybersécurité • Aspects pluridisciplinaires de la cybersécurité • Procédures responsables de divulgation d'informations	
e-Compétences (de e-CF)	A.7. Surveillance des tendances technologiques A.9. Innover D.7. Science et analyse des données C.4. Gestion des problèmes D.10. Gestion de l'information et des connaissances	Niveau 5 Niveau 5 Niveau 4 Niveau 3 Niveau 3

2.10 GESTIONNAIRE DE RISQUES EN CYBERSÉCURITÉ

Titre du profil	Gestionnaire de risques en cybersécurité	
Titre(s) alternatif(s)	Analyste des risques liés à la sécurité de l'information Consultant en assurance des risques liés à la cybersécurité Évaluateur des risques liés à la cybersécurité Analyste des impacts liés à la cybersécurité Gestionnaire des risques cybernétiques	
Récapitulatif	Gérer les risques liés à la cybersécurité de l'organisation conformément à la stratégie de l'organisation. Élaborer, tenir à jour et communiquer les processus et les rapports de gestion des risques.	
Mission	Gère en permanence (identifie, analyse, évalue, estime, atténue) les risques liés à la cybersécurité des infrastructures, systèmes et services CTI en planifiant, appliquant, rapportant et communiquant l'analyse, l'évaluation et le traitement des risques. Établit une stratégie de gestion des risques pour l'organisation et veille à ce que les risques restent à un niveau acceptable pour l'organisation en sélectionnant des mesures d'atténuation et des contrôles.	
Élément(s) livrable(s)	• Rapport d'évaluation des risques en matière de cybersécurité • Plan d'action pour l'atténuation des risques en matière de cybersécurité	
Tâche(s) principale(s)	• Élaborer la stratégie de gestion des risques de cybersécurité d'une organisation • Gérer un inventaire des actifs de l'organisation • Identifier et évaluer les menaces et vulnérabilités liées à la cybersécurité des systèmes CTI • Identification du paysage des menaces, y compris les profils des attaquants, et estimation du potentiel d'attaques • Évaluer les risques en matière de cybersécurité et proposer les options de traitement des risques les plus appropriées, y compris les contrôles de sécurité, et l'atténuation et l'évitement des risques qui répondent le mieux à la stratégie de l'organisation • Surveiller l'efficacité des contrôles de cybersécurité et les niveaux de risque • Veiller à ce que tous les risques de cybersécurité restent à un niveau acceptable pour les actifs de l'organisation • Élaborer, tenir à jour, rendre compte et communiquer un cycle complet de gestion des risques	
Compétence(s) clé(s)	• Mettre en œuvre des cadres, des méthodologies et des lignes directrices de gestion des risques de cybersécurité et assurer le respect des réglementations et des normes • Analyser et consolider les pratiques de gestion de la qualité et des risques de l'organisation • Permettre aux propriétaires d'actifs d'entreprise, aux dirigeants et aux autres parties prenantes de prendre des décisions éclairées sur les risques afin de gérer et d'atténuer les risques • Construire un environnement conscient des risques de cybersécurité • Communiquer, présenter et faire des rapports aux parties prenantes concernées • Proposer et gérer des options de partage des risques	
Connaissances clés	• Normes, méthodologies et cadres de gestion des risques • Outils de gestion des risques • Recommandations et bonnes pratiques en matière de gestion des risques • Cybermenaces • Vulnérabilités des systèmes informatiques • Contrôles et solutions de cybersécurité • Risques en matières de cybersécurité • Surveillance, test et évaluation de l'efficacité des contrôles de cybersécurité • Certifications liées à la cybersécurité • Technologies liées à la cybersécurité	
e-Compétences (de e-CF)	E.3. Gestion des risques E.5. Amélioration des processus E.7. Gestion du changement d'entreprise E.9. Gouvernance des SI	Niveau 4 Niveau 3 Niveau 4 Niveau 4

2.11 ENQUETEUR EN CRIMINALISTIQUE NUMÉRIQUE

Titre du profil	Enquêteur en criminalistique numérique	
Titre(s) alternatif(s)	Digital Forensics Investigator Analyste en criminalistique numérique Cybersécurité & Spécialiste en criminalistique Consultant en criminalistique informatique	
Récapitulatif	S'assurer que l'enquête cybercriminelle révèle toutes les preuves numériques pour prouver l'activité malveillante.	
Mission	Relier les artefacts aux personnes physiques, capturer, récupérer, identifier et préserver les données, y compris les manifestations, les entrées, les sorties et les processus des systèmes numériques faisant l'objet d'une enquête. Fournir une analyse, une reconstruction et une interprétation des preuves numériques sur la base d'un avis qualitatif. Présenter une vue qualitative impartiale sans interpréter les résultats qui en résultent.	
Élément(s) livrable(s)	• Résultats de l'analyse de la criminalistique numérique • Éléments de preuve électroniques	
Tâche(s) principale(s)	• Élaborer une politique, des plans et des procédures d'enquête en criminalistique numérique • Identifier, récupérer, extraire, documenter et analyser les preuves numériques • Préserver et protéger les preuves numériques et les mettre à la disposition des parties prenantes autorisées • Inspecter les environnements à la recherche de preuves d'actions non autorisées et illégales • Documenter, rapporter et présenter systématiquement et de manière déterministe les conclusions et les résultats des analyses criminalistiques numériques • Sélectionner et personnaliser les techniques de test, d'analyse et de reporting en matière de criminalistique	
Compétence(s) clé(s)	• Travailler de manière éthique et indépendante, sans être influencé ou biaisé par des acteurs internes ou externes • Recueillir des informations tout en préservant leur intégrité • Identifier, analyser et corréler les événements de cybersécurité • Expliquer et présenter les preuves numériques d'une manière simple, directe et facile à comprendre • Élaborer et communiquer des rapports d'enquête détaillés et motivés	
Connaissances clés	• Recommandations et bonnes pratiques en matière de criminalistique numérique • Normes, méthodologies et cadres de la criminalistique numérique • Procédures d'analyse de la criminalistique numérique • Procédures d'essai • Procédures, normes, méthodologies et cadres d'enquête pénale • Lois, réglementations et législations relatives à la cybersécurité • Outils d'analyse des logiciels malveillants • Cybermenaces • Vulnérabilités des systèmes informatiques • Procédures d'attaque de cybersécurité • Sécurité des systèmes d'exploitation • Sécurité des réseaux informatiques • Certifications liées à la cybersécurité	
e-Compétences (de e-CF)	A.7. Surveillance des tendances technologiques B.3. Essais B.5. Production de la documentation E.3. Gestion des risques	Niveau 3 Niveau 4 Niveau 3 Niveau 3

2.12 TESTEUR D'INTRUSIONS

Titre du profil	Testeur d'intrusions
Titre(s) alternatif(s)	Pentester Hacker éthique Analyste de vulnérabilité Testeur en cybersécurité Expert en cybersécurité offensive Expert en cybersécurité défensive Expert Red Team Equipier Red Team
Récapitulatif	Évaluer l'efficacité des contrôles de sécurité, révéler et utiliser les vulnérabilités de cybersécurité, en évaluant leur criticité si elles sont exploitées par des acteurs de la menace.
Mission	Planifier, concevoir, mettre en œuvre et exécuter des activités de test d'intrusion et des scénarios d'attaque pour évaluer l'efficacité des mesures de sécurité déployées ou planifiées. Identifier les vulnérabilités ou les défaillances des contrôles techniques et organisationnels qui affectent la confidentialité, l'intégrité et la disponibilité des produits CTI (par exemple, les systèmes, le matériel, les logiciels et les services).
Élément(s) livrable(s)	• Rapport sur les résultats de l'évaluation de la vulnérabilité • Rapport d'essai de pénétration
Tâche(s) principale(s)	• Identifier, analyser et évaluer les vulnérabilités techniques et organisationnelles en matière de cybersécurité • Identifier les vecteurs d'attaque, découvrir et démontrer l'exploitation des vulnérabilités techniques en matière de cybersécurité • Conformité des systèmes d'essai et des opérations aux normes réglementaires • Sélectionner et développer des techniques de test d'intrusion appropriées • Organiser des plans de test et des procédures pour les tests d'intrusion • Établir des procédures pour l'analyse et la communication des résultats des tests d'intrusion • Documenter et communiquer les résultats des tests d'intrusion aux parties prenantes • Déployer des outils et des programmes de test d'intrusion
Compétence(s) clé(s)	• Développer des codes, des scripts et des programmes • Effectuer de l'ingénierie sociale • Identifier et exploiter les vulnérabilités • Effectuer des piratages éthiques • Penser de manière créative et hors des sentiers battus • Identifier et résoudre les problèmes liés à la cybersécurité • Communiquer, présenter et faire des rapports aux parties prenantes concernées • Utiliser efficacement les outils de test d'intrusion • Effectuer des analyses techniques et des rapports • Décomposer et analyser les systèmes pour identifier les faiblesses et les contrôles inefficaces • Examiner et évaluer la sécurité des codes
Connaissances clés	• Procédures d'attaque de cybersécurité • Appareils de technologie de l'information (TI) et de technologie opérationnelle (TO) • Procédures de sécurité offensives et défensives • Sécurité des systèmes d'exploitation • Sécurité des réseaux informatiques • Procédures de test de pénétration • Normes, méthodologies et cadres pour les tests de pénétration • Outils de test de pénétration • Programmation informatique • Vulnérabilités des systèmes informatiques • Recommandations et bonnes pratiques en matière de cybersécurité • Certifications liées à la cybersécurité

e-Compétences (de e-CF)	B.2. Intégration de composants B.3. Essais B.4. Déploiement de la solution B.5. Production de la documentation E.3. Gestion des risques	Niveau 4 Niveau 4 Niveau 2 Niveau 3 Niveau 4

3. BIBLIOTHÈQUE DES ELEMENTS LIVRABLES

La liste des éléments livrables fournit des exemples indicatifs et pratiques des éléments livrables / des produits de chaque profil. Les livrables énumérés sont proposés à titre d'exemples car la liste n'est pas exhaustive et ne couvre donc pas tous les aspects de chaque profil.

Titre du profil	Élément livrable	Description
Responsable de la sécurité de l'information (CISO)	Stratégie de cybersécurité	La stratégie de cybersécurité est un plan d'action conçu pour améliorer la sécurité et la résilience des infrastructures et des services d'une organisation.
Responsable de la sécurité de l'information (CISO)	Politique de cybersécurité	Une politique établissant des règles visant à garantir la cybersécurité de l'organisation.
Intervenant en cas de cyber incident	Plan d'intervention en cas d'incident	Un ensemble de procédures documentées détaillant les étapes à suivre à chaque étape d'une intervention en cas d'incident (préparation, détection et analyse, confinement, éradication et rétablissement, activité post-incident).
Intervenant en cas de cyber incident	Rapport d'incident cybernétique	Un rapport fournissant des détails sur un ou plusieurs cyber incidents.
Responsable juridique, politique et conformité en cybersécurité	Manuel de conformité	Un manuel fournissant une compréhension approfondie des obligations de conformité réglementaire d'une organisation. Il peut s'agir de politiques ou de procédures internes visant à assurer le respect des lois, des règlements et/ou des normes.
Responsable juridique, politique et conformité en cybersécurité	Rapport de conformité	Un rapport présentant l'état actuel de la posture de conformité d'une organisation.
Spécialiste du renseignement sur les cybermenaces	Manuel de renseignement sur les cybermenaces (ou manuel)	Un manuel présentant des outils et/ou des méthodologies pour la collecte et/ou le partage de renseignements sur les cybermenaces.
Spécialiste du renseignement sur les cybermenaces	Rapport sur les cybermenaces	Un rapport identifiant les principales menaces, et tendances observées en ce qui concerne les menaces, les acteurs de la menace et/ou les techniques d'attaque. Le rapport peut également inclure des mesures d'atténuation pertinentes.
Architecte en cybersécurité	Schéma de l'architecture de cybersécurité	Représentation visuelle de l'architecture du système de cybersécurité d'une organisation utilisée pour protéger les actifs contre les cyberattaques.
Architecte en cybersécurité	Rapport sur les exigences en matière de cybersécurité	Un rapport énumérant un ensemble d'exigences nécessaires pour assurer la cybersécurité d'un système.
Auditeur en cybersécurité	Plan d'audit de cybersécurité	Un plan qui présente la stratégie globale et les procédures qu'un auditeur suivra pour effectuer un audit de cybersécurité.
Auditeur en cybersécurité	Rapport d'audit de cybersécurité	Un rapport fournissant une compréhension approfondie du niveau de sécurité d'un système, évaluant ses forces et ses faiblesses en matière de cybersécurité. Il peut également prévoir des mesures correctives pour améliorer la cybersécurité globale du système.

Éducateur en cybersécurité	Programme de sensibilisation à la cybersécurité	Un programme d'activités de sensibilisation aux questions liées à la cybersécurité (par exemple, des conférences sur les attaques et les menaces) en aidant les organisations à prévenir et à limiter les risques liés à la cybersécurité.)
Éducateur en cybersécurité	Matériel de formation en cybersécurité	Matériel expliquant les concepts, les méthodologies et les outils liés à la cybersécurité pour la formation ou le perfectionnement des personnes. Il peut inclure des manuels pour les enseignants, des ensembles d'outils pour les étudiants et/ou des images virtuelles pour soutenir les sessions de formation pratiques.
Spécialiste de la mise en œuvre de la cybersécurité	Solutions de cybersécurité	Les solutions de cybersécurité peuvent inclure des outils et des services visant à protéger les organisations contre les cyberattaques.
Chercheur en cybersécurité	Publication dans le domaine de la cybersécurité	Publication académique traitant des conclusions et des résultats de la recherche dans le domaine de la cybersécurité. L'objectif de la publication pourrait être de faire progresser la technologie et/ou de développer de nouvelles solutions innovantes.
Gestionnaire des risques en cybersécurité	Rapport d'évaluation des risques en matière de cybersécurité	Un rapport énumérant les résultats de l'identification, de l'analyse et de l'évaluation des risques de cybersécurité d'un système. Il pourrait également inclure des contrôles visant à atténuer ou à réduire les risques identifiés à un niveau acceptable.
Gestionnaire des risques en cybersécurité	Plan d'action pour l'assainissement des risques de cybersécurité	Un plan d'action énumérant les activités liées à la mise en œuvre de mesures d'atténuation visant à réduire les risques en matière de cybersécurité.
Enquêteur en criminalistique numérique	Résultats d'analyse de la criminalistique numérique	Résultats d'analyse des données numériques permettant de mettre au jour des preuves potentielles d'incidents malveillants et d'identifier d'éventuels acteurs de la menace.
Enquêteur en criminalistique numérique	Éléments de preuve électroniques	Preuve potentielle dérivée de données contenues dans ou produites par un dispositif, dont le fonctionnement dépend d'un logiciel ou de données stockées ou transmises sur un système informatique ou un réseau (par exemple, collecte précise des journaux)
Testeur d'intrusion	Rapport sur les résultats de l'évaluation de la vulnérabilité	Rapport répertoriant et évaluant la criticité des vulnérabilités découvertes dans un système lors d'une analyse (généralement automatique) des vulnérabilités. Le rapport pourrait également suggérer des mesures correctives de base.
Testeur d'intrusion	Rapport d'essai d'intrusion	Un rapport fournissant une analyse détaillée et complète des vulnérabilités d'un système identifiées lors d'un test de sécurité. Le rapport pourrait également inclure des mesures correctives suggérées.

TP-09-22-510-FR-N

À PROPOS DE L'ENISA

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union chargée d'atteindre un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'UE sur la cybersécurité, l'Agence de l'Union européenne pour la cybersécurité contribue à la politique de l'UE en matière de cybersécurité, renforce la fiabilité des produits, services et processus TIC grâce à des schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'UE, et aide l'Europe à se préparer aux cyber défis de demain. Grâce au partage des connaissances, au renforcement des capacités et à la sensibilisation, l'Agence collabore avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, renforcer la résilience des infrastructures de l'Union et, par conséquent, préserver la sécurité numérique de la société et des citoyens européens. De plus amples informations sur l'ENISA et ses travaux sont disponibles à l'adresse suivante : www.enisa.europa.eu.

ENISA
Agence de l'Union européenne pour la cybersécurité

Bureau d'Athènes
Agamemnonos 14, Chalandri 15231, Attiki, Grèce

Bureau d'Héraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Héraklion, Grèce

enisa.europa.eu

ISBN : 978-92-9204-584-5
DOI : 10.2824/859537