ICDE Institut de Cyber Défense Européen

CATALOGUE DES FORMATION 2023

L'Importance des Formations ICDE

Dans une ère définie par la transformation numérique et le paysage des menaces en constante évolution, rester en avance sur les cyberattaques n'est plus un choix, c'est devenu impératif. ICDE est votre partenaire dans ce voyage essentiel. ICDE s'engage à habiliter les individus et les organisations avec les connaissances et les compétences nécessaires pour naviguer dans le monde complexe de la cybersécurité. Notre mission est de nous assurer que vous disposez des outils non seulement pour survivre, mais aussi pour prospérer dans un monde interconnecté.

Chez ICDE, notre engagement va au-delà de la simple offre d'une large gamme de formations. Ce qui nous distingue vraiment, c'est le mélange unique d'expertise, d'innovation et de praticité. Nos formations ne sont pas simplement théoriques ; elles sont méticuleusement conçues pour offrir une expérience pratique et des connaissances approfondies. Nous croyons en l'équipement des apprenants avec des compétences qui vont au-delà de la salle de classe, vous assurant d'être prêt à relever les défis réels auxquels vous serez confrontés dans votre vie professionnelle.

Les offres d'ICDE s'adressent à des individus à divers stades de leur parcours en cybersécurité, que vous fassiez vos premiers pas dans ce domaine passionnant ou que vous soyez un professionnel chevronné cherchant à améliorer vos compétences. Ce qui rend ICDE exceptionnel, c'est notre engagement à fournir une formation ancrée dans des scénarios du monde réel et des applications pratiques. Nos formations sont structurées pour vous assurer d'acquérir les compétences nécessaires pour faire face aux situations que vous pourriez rencontrer dans votre vie professionnelle.

À mesure que notre monde devient de plus en plus interconnecté, la cybersécurité ne consiste pas seulement à protéger les données, mais aussi à sécuriser l'avenir. Chez ICDE, nous comprenons notre rôle essentiel pour habiliter les individus et les organisations à protéger leurs paysages numériques, assurant ainsi un avenir résilient et sécurisé pour tous.

Nos formations ne sont pas seulement enseignées ; elles sont élaborées par une équipe de professionnels de la cybersécurité qui ont vécu les défis et les réussites du domaine. Que vous visiez à vous spécialiser dans la cyberdéfense, la cyberattaque, la cybercriminalistique ou la gestion de la sécurité, nous offrons une gamme diversifiée de formations pouvant être adaptées à vos objectifs de carrière spécifiques. Lorsque vous choisissez ICDE, vous choisissez l'expertise, l'innovation et la praticité, le tout dans le but de vous habiliter pour réussir dans le monde en constante évolution de la cybersécurité.

Formations offensives

Les formations liées à la cybersécurité offensive vous dotent des connaissances et des compétences nécessaires pour endosser le rôle de Pentester. Les participants ont l'opportunité d'explorer le monde de l'intrusion éthique de l'évaluation des vulnérabilités, en apprenant à identifier, exploiter et atténuer les failles de sécurité. Dans un environnement sûr et contrôlé, vous vous confronterez à des scénarios du monde réel pour affiner votre expertise en cybersécurité offensive, garantissant que vous pouvez protéger efficacement votre organisation contre les acteurs malveillants.

Pourquoi les formations en cyberattaques offensives sont-elles importantes pour vous ?

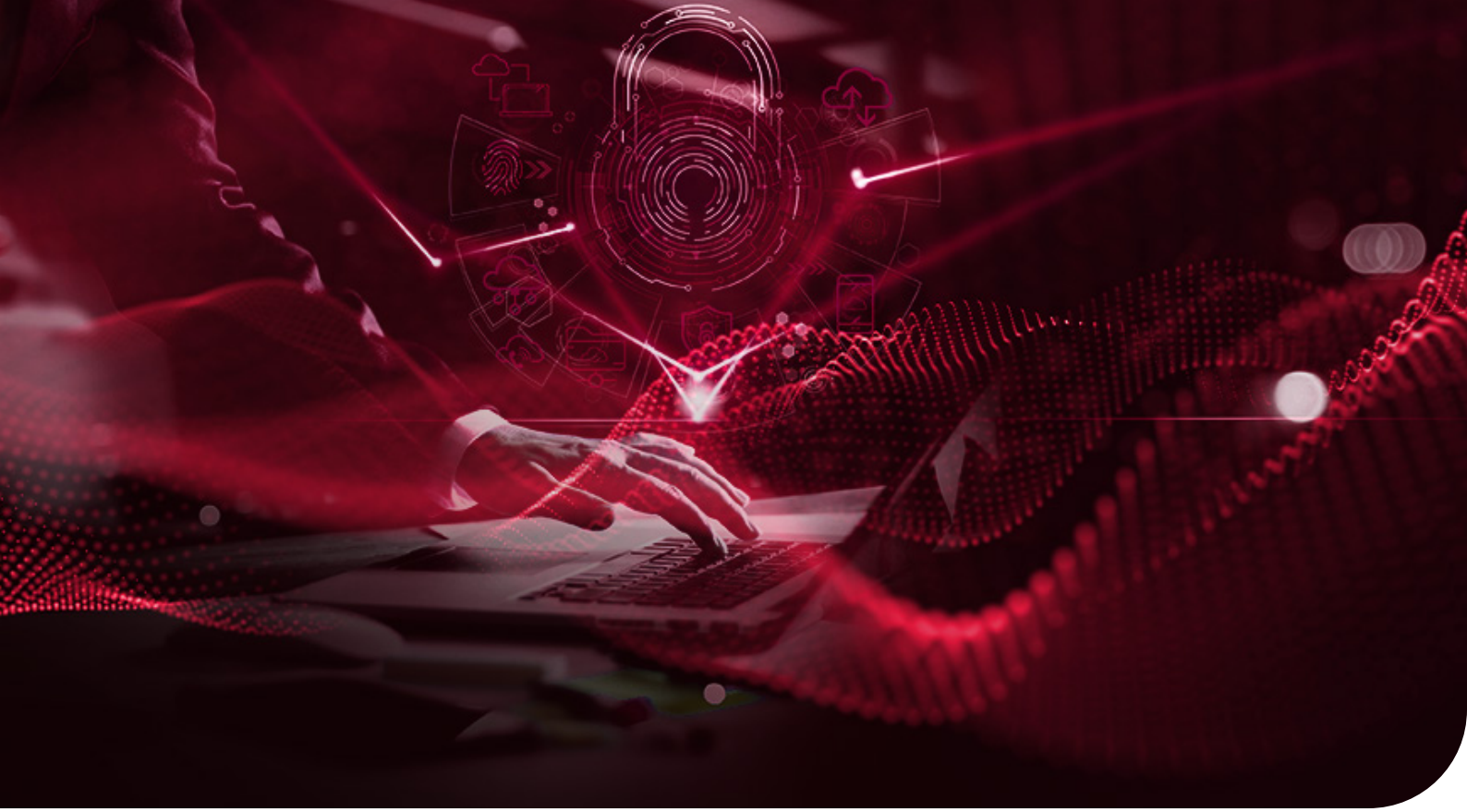
Participer à des formations en cybersécurité offensive ne consiste pas seulement à comprendre l'esprit d'un hacker, mais à devenir un auditeur technique confirmé (pentester). Ces formations sont essentielles pour ceux qui souhaitent protéger les paysages numériques car elles fournissent les compétences et les idées nécessaires pour identifier et atténuer les vulnérabilités de manière proactive. Dans un monde où les acteurs malveillants du cyber espace continuent d'évoluer, maîtriser l'art du test d'intrusion garantit que les participants peuvent rester un pas en avant des menaces potentielles, protégeant efficacement leurs actifs numériques.

Ce portefeuille comprend trois formations :

- Fondamentaux des tests d'intrusion
- Tests d'intrusion avancés
- Formation OSINT – techniques de collecte du renseignement

Fondamentaux des tests d'intrusion

La formation sur les Fondamentaux des tests d'intrusion est conçue pour les débutants dans le domaine offensif cherchant à renforcer leurs compétences en matière d'audit technique et à se familiariser avec les techniques et les outils utilisés dans ce domaine. Offert par l'ICDE, cette formation vise à permettre aux candidats de développer une base solide de connaissances et de compétences pour mener des tests d'intrusion et formuler des recommandations en matière de remédiation. Il couvre un large éventail de sujets, notamment l'identification des vulnérabilités, les techniques d'exploitation, les attaques basées sur le web, les attaques réseau, les attaques sans fil, les attaques physiques, et bien plus encore.



Objectifs pédagogiques

- Comprendre les principes et les méthodologies des tests d'intrusion.
- Acquérir des compétences dans l'identification et l'exploitation des vulnérabilités dans les systèmes, les réseaux, le WEB.
- Apprendre les outils essentiels et les techniques utilisées dans le domaine des tests d'intrusion.
- Développer les compétences pour mener des évaluations et rapports associés.

Public

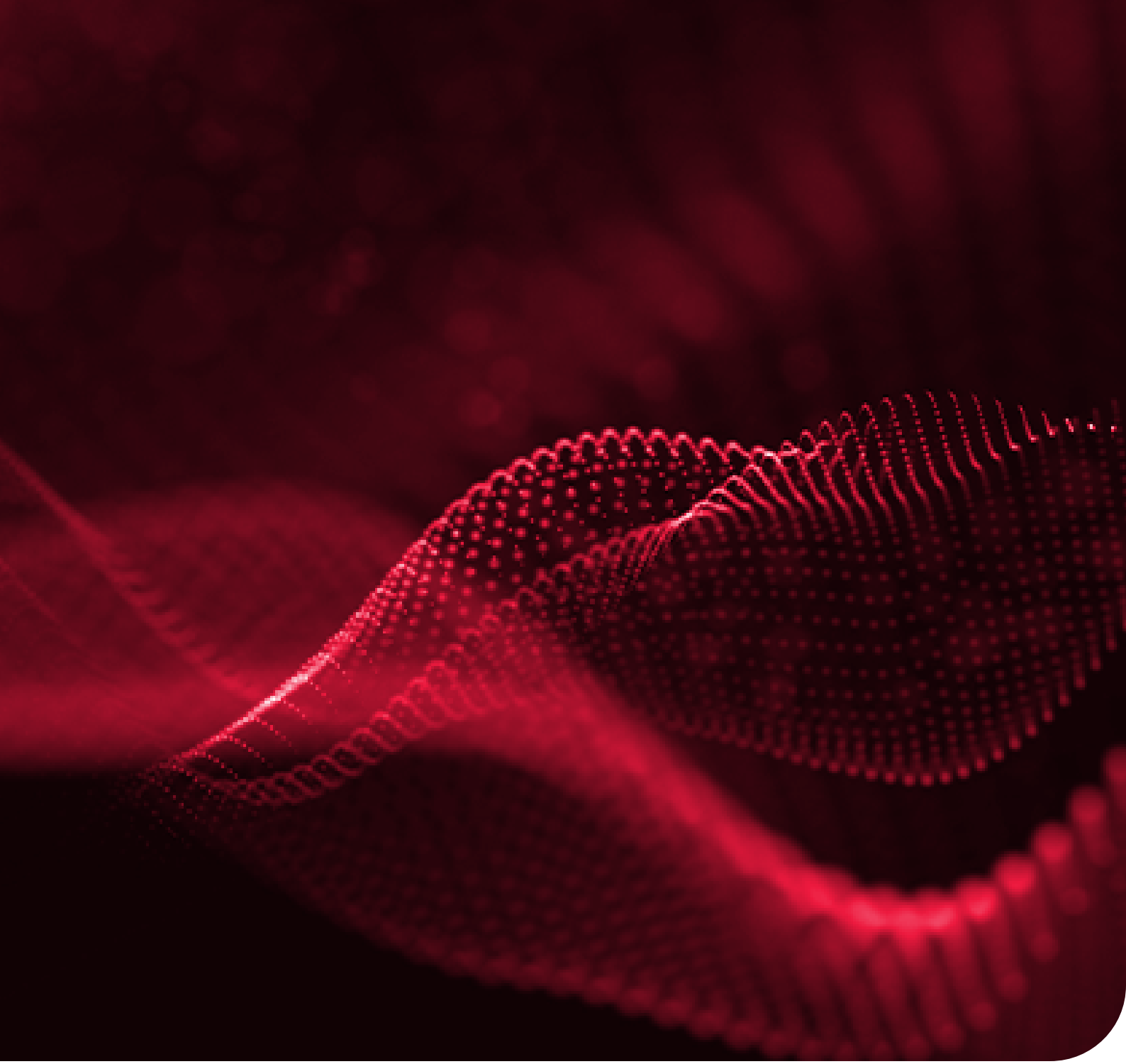
- Étudiants cherchant à entrer dans le domaine de la cybersécurité et à se spécialiser dans les tests d'intrusion et les évaluations de vulnérabilités.
- Professionnels de la cybersécurité débutants cherchant à se spécialiser dans les tests d'intrusion et les évaluations de vulnérabilités.
- Professionnels de la sécurité informatique souhaitant ajouter des compétences en tests d'intrusion et en évaluation de vulnérabilités à leur profil de compétences existant.

Prérequis

- Connaissances de base des principes, tels que les réseaux informatiques, la sécurité des systèmes d'exploitation, la gestion de l'identité et de l'accès, et la sécurité des applications web.
- Compréhension de base des techniques et des outils de tests d'intrusion, tels que la reconnaissance des ports et des services, l'analyse des vulnérabilités, les attaques par force brute, les attaques par déni de service, et l'exploitation des vulnérabilités.
- Connaissances de base des principaux systèmes d'exploitation, tels que Windows et Linux, ainsi que des compétences en ligne de commande pour ces systèmes d'exploitation.
- Connaissances de base des principaux langages de programmation, tels que Python, ainsi que des compétences en programmation de base.

Programme de la formation

Jour 1	**Section 1 – Contexte actuel** • La cybercriminalité aujourd'hui • Terminologie • Principes de la sécurité de l'information • Les différentes phases d'une attaque • Définition d'un test d'intrusion • Aspects légaux et réglementaires liés aux tests d'intrusion • Méthodes et framework pour un test d'intrusion **Section 2 – Cadrage et objectifs** • Identification des objectifs • Définition du périmètre • TD/ Framework pentest ESD Academy • TP 1/ Questionnaire de pré-engagement • Gestion et affectation des ressources • Suivi des objectifs du test • Règles de pré-engagement (RoE) • TP 2/ Rédaction d'un contrat de pré-engagement
Jour 2	**Section 3 - Préparer son test d'intrusion** • Préparation d'une machine pour test d'intrusion • Automatisation et scripting • Outils, matériels connus • TD/ Rubber Ducky • Templating de documents • TD/ Suivi test d'intrusion **Section 4 – Collecte d'informations** • Ingénierie des sources publiques (OSINT) • Relevé passif et actif d'informations sur l'organisation cible • TD/ Présentation des outils d'OSINT • TP 3/ Relevé d'informations & Reconnaissance **Section 5 – Énumération de l'infrastructure** • Énumération du périmètre • Évasion sur infrastructure sécurisée • Énumération des protocoles • TD/ Présentation des outils d'énumération • TP 4/ Énumération de l'infrastructure **Section 6 – Analyse des vulnérabilités** • Scan de vulnérabilités • Présentation des différents outils • TD/ Présentation OpenVAS • Les vulnérabilités connues • TP 5/ Identification des vulnérabilités



Programme de la formation

Jour 3	**Section 7 – Exploitation** • Recherche d'Exploits • Présentation des outils/frameworks d'attaque • TD/ Présentation metasploit • Déploiement et exécution de charges • TP 6/ Exploitation des vulnérabilités • Écoute passive et active des infrastructures • Bruteforcing **Section 8 – Post-Exploitation** • Élévation de privilèges (Méthodes, outils, vulnérabilités linux, ...) • Etude des persistances (ADS, base de registre, planificateur de tâches, services) • Mouvements latéraux • TP 7/ Post-Exploitation et mouvement lateraux

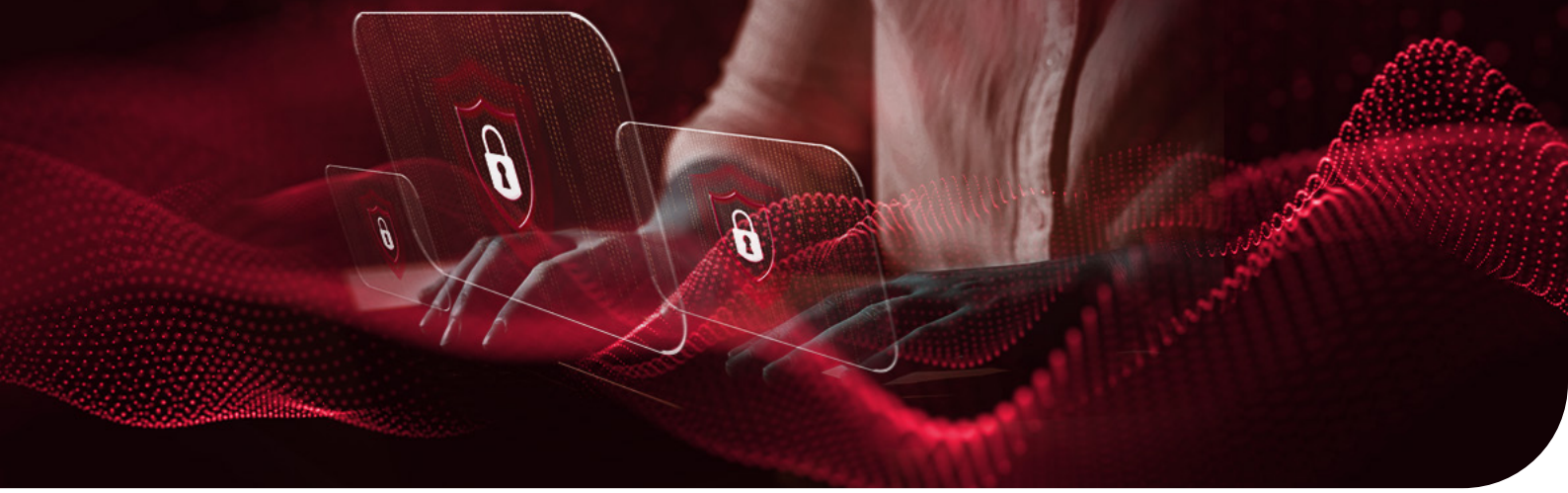
Programme de la formation

Jour 4	**Section 1 - Sécurité Wi-Fi** • Introduction • Les normes et protocoles 802.11 • TD 1 / Analyse de flux avec wireshark • Contexte de la sécurité Wi-Fi • TD 2/ Présentation de la suite Aircrack-ng • TD 3/ SSID Caché • Étude des protocoles (WEP, WPA,WPS; ...) • TD 4 / Attaque sur le protocole WPA2 • Méthodes et attaques des réseaux sans fil • Contre-mesures et sécurisation (WIDS/802.1x) • TD5 / Chellam **Section 2 – Introduction aux applications Web** • Composants du web (Client/serveur, AJAX, DOM) • Protocole HTTP(S) • Présentation de l'outil Burpsuite • TD 6 / Présentation de Burp suite **Section 3 – Top 10 OWASP 2021** • Injections (SQL, LDAP, code, etc.) • TD7 / Injection SQL manuelle et automatisée • TP1/ Injection SQL • Faiblesse d'authentification • TD8/ Bruteforce avec burp suite • Exposition de données sensibles • TD9/ Exposition de donnée sensible • TP2/ Recherche de fichiers sensibles • XML External Entities (XXE) • Faiblesse des contrôles d'accès • TP3/ IDOR / LFI / RFI / CSRF / VERB • Mauvaise configuration de sécurité • Cross-Site Scripting-XSS (Stored/Reflected/DOM Based) • TD10 / Vol de cookie avec XSS • TP4/ Exploitation XSS • Désérialisation non sécurisée • Composants vulnérables • TP5 / Exploitation de composants vulnérables • Logging et monitoring laxiste
Jour 5	**Section 4 – Fuzzing et Post-Exploitation** • Post-exploitation web (weevely, webshell, ...) • Fuzzing web (Payload, ZED, ...) • TD11 / Présentation des outils de fuzzing **Section 5 – Analyse et rapport** • Étude et analyse des résultats • Mise en perspective des résultats • Rédaction de rapports • Restitution de livrables exploitable par un CODIR • Recommandations, plans d'action et suivi • TP6 / Réalisation d'un test d'intrusion web

Tests d’intrusion avancés

La formation sur les tests d’intrusion avancés est une formation idéale pour devenir un véritable expert en tests d’intrusion et en évaluations de vulnérabilités. Vous apprendrez comment appliquer les techniques les plus avancées, maîtriser la méthodologie des tests d’intrusion et utiliser des outils et des techniques avancés pour tester les vulnérabilités. Vous acquerrez également de l’expertise dans la rédaction de rapports détaillés sur les vulnérabilités et les recommandations de remédiation.

Cette formation est conçue pour les professionnels de la cybersécurité souhaitant améliorer leurs compétences en matière de tests d’intrusion et d’évaluation de vulnérabilités, ainsi que pour les professionnels de la sécurité informatique cherchant à élargir leurs compétences existantes. Les sujets abordés vont de la reconnaissance des réseaux et de la collecte d’informations à l’exploitation de vulnérabilités complexes, en passant par les phases de post-exploitation, de furtivité et d’évasion des défenses de sécurité.



Objectifs pédagogiques

- Développer une connaissance approfondie des techniques de hacking les plus avancées afin de pouvoir proposer des solutions de sécurité efficaces aux clients.
- Acquérir une expertise approfondie dans l'utilisation des outils de test de vulnérabilité les plus avancés pour pouvoir détecter les vulnérabilités les plus complexes dans les systèmes informatiques.
- Savoir comment identifier les risques potentiels et les vulnérabilités de sécurité les plus critiques dans les réseaux et les applications.
- Savoir comment rédiger des rapports de vulnérabilité précis et détaillés, avec des recommandations de remédiation adaptées aux besoins du client.
- Acquérir les compétences pour effectuer des tests d'intrusion avancés et des évaluations de vulnérabilité sur les réseaux et les applications, en utilisant des techniques avancées de contournement de la sécurité.
- Se tenir au courant des dernières tendances en matière de piratage éthique et des meilleures pratiques en matière de sécurité des systèmes informatiques.
- Comprendre les différentes mesures de prévention de sécurité les plus avancées qui peuvent être mises en place pour protéger les systèmes informatiques.

Public

- Pentesters
- Professionnels de la cybersécurité
- Analystes de la cybersécurité
- Ingénieurs en sécurité réseau
- Consultants en cybersécurité
- Professionnels de l'informatique
- Personnel gouvernemental/militaire

Prérequis

- Une solide connaissance des systèmes d'exploitation, des réseaux et des applications.
- Au moins 1 à 2 ans d'expérience dans le domaine de la cybersécurité ou dans un rôle connexe.
- Une compréhension approfondie des méthodologies de test d'intrusion et des outils de tests d'intrusion.
- Des compétences en programmation et en script pour automatiser des tâches et exploiter des vulnérabilités.

Programme de la formation

Jour 1 matin	**Section 1 - Préparation et initialisation des phases à l'exploitation** • Introduction et Terminologie • Étude des séquences d'exploitation • Focus sur les types de charges • Création de différents types de charges pour • l'exploitation • Déclencher les charges
Jour 1 Après-midi	• Automatiser l'exploitation • **TP1**/Création et intégration d'une charge
Jour 2 Matin	**Section 2 - Positionnement -Attaquant externe** • Introduction sur les attaques externes • Social Engineering (Phishing, détournement de messagerie, ...) • Recherche d'identifiants sur les bases de « Leak »
Jour 2 après-midi	**Section 3 - Positionnement -Attaquant interne** • Introduction sur les attaques internes • Attaque sur le protocole NTLM • **TP2**/Attaque de type « relay» LLMNR & NBT-NS
Jour 3 matin	• Attaque sur le protocole Kerberos **Section 4 - Phases de Post-Exploitation** • Énumération Post-Exploitation • Identification des chemins d'attaques
Jour 3 après-midi	• Obtention d'identifiants supplémentaires • **TP3**/Extraction des credentials en mémoire) • Mouvement latéral • **TP4**/Mouvement latéral
Jour 4 matin	• Pivoting • **TP5**/Pivoting • Escalade de privilèges verticale
Jour 4 Après-midi	• **TP6**/Escalade de privilège verticale • Escalade de privilèges horizontale • Zoom sur la sécurité des systèmes industriels
Jour 5 Matin	**Section 5 - Persistance** • Golden Ticket/Silver Ticket • Skeleton Key/Admin SDHolder • DCSync
Jour 5 Après-midi	• **TP7**/Intrusion externe

Formation OSINT - techniques de collecte du renseignement

La formation OSINT – techniques de collecte du renseignement est conçeu pour valider les compétences des professionnels de la cybersécurité dans la collecte, l'analyse et la présentation de données en source ouverte dans le cadre de la cybersécurité. Il couvre un large éventail de sujets, notamment les sources de données OSINT, les techniques de collecte de données OSINT, les outils et techniques d'analyse de données OSINT, etc.

Il est adapté aux professionnels de la cybersécurité, aux analystes du renseignement, aux consultants en sécurité et aux agents de la force publique qui souhaitent se spécialiser dans l'Intelligence en Source ouverte (OSINT). Il peut également être utile aux personnes travaillant dans le marketing, les services de renseignement, la recherche et l'analyse de marché. En obtenant cette certification, les candidats peuvent améliorer leur employabilité et accéder à des opportunités professionnelles plus avancées dans le domaine de la cybersécurité.

Objectifs pédagogiques

- Comprendre les principes de base de l'OSINT et son importance dans la cybersécurité.
- Maîtriser les techniques de collecte d'informations ouvertes pour obtenir des renseignements sur les cibles.
- Savoir utiliser des outils d'OSINT pour la collecte d'informations ouvertes.
- Comprendre les risques liés à l'utilisation d'informations sensibles obtenues via l'OSINT.
- Connaître les techniques de protection de la vie privée et de la sécurité opérationnelle lors de la collecte d'informations ouvertes.
- Apprendre à utiliser les informations recueillies pour évaluer la sécurité d'une cible et planifier des opérations de sécurité.
- Comprendre les règles éthiques et légales entourant la collecte d'informations ouvertes.

Public

- Enquêteurs
- Détectives privés
- Analystes
- Veilleurs
- Avocats
- Cabinet de recouvrement
- Service de renseignement
- Journalistes

Prérequis

- Une compréhension de base des concepts de la sécurité informatique et des réseaux informatiques.
- Une connaissance pratique de l'utilisation des outils OSINT courants, tels que Maltego, SpiderFoot, Social-Searcher, etc.
- Une connaissance pratique des techniques d'analyse de données OSINT, telles que l'analyse des réseaux sociaux, l'analyse d'images, l'analyse de données géospatiales, etc.

Programme de la formation

Jour 1	**Section 1 – présentation générale OSINT – Les différentes branches de l'OSINT** • OSINT – Open Source Intelligence • SOCMINT – Social Media Intelligence • IMINT/ROIM – Renseignement d'intérêt image • GEOINT – Renseignement Géospatial • Exercice 1 : Simple Recherche élémentaire – Test des compétences • Démonstration d'un attendu d'OSINT – Livrable • Explication du livrable • Eléments saillants • État d'esprit • Bonnes pratiques de sécurité • Rappel Juridique sur l'OSINT en France **Section 2 – les Google dorks – Les Opérateurs Google** • Voir l'invisible avec les opérateurs de recherches (Yandex, Google, Bing, Shodan) • Bloqué ? Supprimé ? Utiliser le cache et les archives • Création d'un avatar (Tips & Tricks) • Reverse Image – Retour d'expérience, tips & tricks sur cas concret • Enquête sur les cryptomonnaies • Recherche sur une société • Linkedin Search API • Bases de données INPI • Sociétés chinoises • Agrégateur de données
Jour 2	**Section 3 – SOCMINT** • Les outils et plug-ins à connaître • Recherche avancée sur Twitter • Analyse avancée de comptes • Analyse & croisement de données • Extraction de données avec des scripts Python • Recherche avancée sur Facebook • Tips & Tricks • Faire des recherches sur le nouveau Graph Search • Suivre la propagation d'URL • Recherche sur les différentes applications Google • Google Calendar / Documents / Contacts • Hangouts • Google Maps • GaiaID • Recherche avancée sur LinkedIn • Reverse Email

Programme de la formation

Jour 3	• Telegram • Présentation et utilisation de TDLib • Tips & Tricks • Réseaux sociaux mobiles (Whatsapp, Tiktok, Clubhouse, TamTam, Signal, etc.) via émulateur Android • Trouver qui se cache derrière un numéro de téléphone • Retrouver qui est cette personne • Weibo & Wechat • Tips & Tricks • Les différents bypass et retours d'expériences • Scraping Weibo via API • Géolocalisation sur Weibo • Recherche avancée sur Vkontakte • Extractions de données via script Python • Utiliser la géolocalisation • Exercice SOCMINT combiné sur applications Android & réseaux sociaux **Section 4 – IMINT/GEOINT** • Les outils • Utilisation de l'API Overpass • Cell Tower & Wifi Catching • Maritime & Aviation Intelligence • L'utilisation des fréquences radio dans l'OSINT • Cas bombardiers russes – Conflit Ukraine • Étude de plusieurs cas concrets de recherche d'un élément avec croisement
Jour 4	**Section 5 – OSINT** • Les outils • Recherche sur une personne • Recherche par visage • Recherche par nom • Recherche par fait • Croisement • Analyse d'un site web • IP & DNS • Utilisation des pages d'erreurs • Structure du site • Chercher selon la technologie • Créer son premier scraper de données avec mise en forme & visualisation simple • ADINT : Advertising Intelligence • Scraping sur des sites d'annuaires • Scraping sur des sites internet • OSINT Actif : Social Engineering—État de l'art • Deep Web : Comment trouver ce que l'on cherche dans l'obscurité ? • Cas concret : Recherche d'une personne ayant fait de multiples fraudes et arnaques. Cette personne a disparu de la circulation.

Formations cybersécurité défensives

Nos formations en cybersécurité défensive sont conçues pour vous aider à devenir un gardien de la cybersécurité. Vous acquerrez une expertise en sécurité réseau, et des systèmes. De la configuration des dispositifs de sécurité à la compréhension des subtilités des protocoles, ces formations fournissent une boîte à outils complète pour protéger les actifs numériques. Avec des compétences pratiques en matière de défense proactive et de réduction des risques, vous serez bien préparé pour protéger votre organisation contre toute une gamme de menaces.

Pourquoi les formations en cybersécurité défensive sont-elles importantes pour vous ?

Les formations en cybersécurité défensive sont conçues pour les individus et les organisations cherchant à renforcer leurs forteresses numériques. Face à des menaces de plus en plus sophistiquées, il est essentiel de comprendre en profondeur la sécurité réseau, et des systèmes. Ces formations permettent aux participants de sécuriser les actifs numériques et les réseaux, en veillant à ce qu'ils disposent des connaissances et des compétences nécessaires pour créer des défenses de cybersécurité résilientes et solides, réduisant les risques et protégeant les données essentielles de leur organisation.

Ce portefeuille comprend les formations suivants :

- Sécurité Windows
- Sécurité Linux

Sécurité Windows

La formation sur la Sécurité Windows est conçue pour valider les compétences des professionnels de la cybersécurité en matière de sécurité des systèmes Windows, de gestion des vulnérabilités et de renforcement des systèmes Windows. Il couvre un large éventail de sujets, notamment la sécurité des systèmes Windows, les méthodes de gestion des vulnérabilités, les techniques de renforcement des systèmes Windows, la configuration de la sécurité Windows, etc.

Il est adapté aux professionnels de la cybersécurité, aux administrateurs système, aux ingénieurs en sécurité, aux architectes en sécurité et aux responsables de la sécurité cherchant à renforcer leurs compétences en matière de sécurité du système d'exploitation Windows. En obtenant cette certification, les candidats peuvent améliorer leur employabilité et accéder à des opportunités professionnelles plus avancées dans le domaine de la cybersécurité.

Objectifs pédagogiques

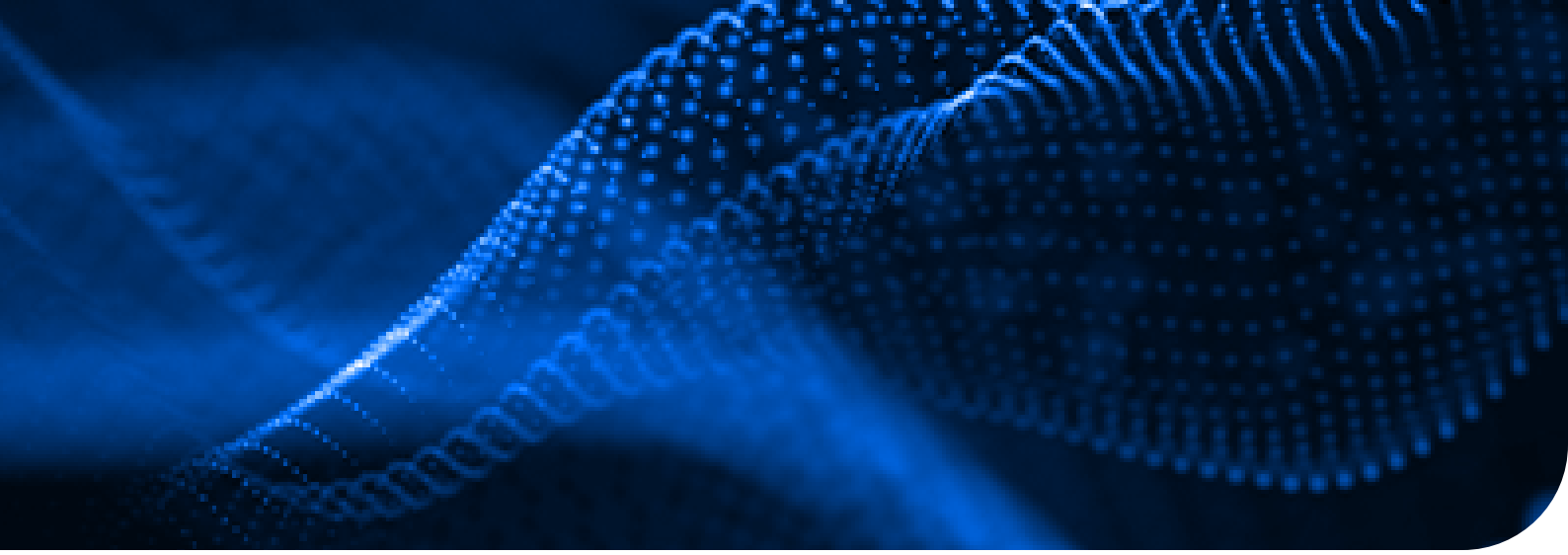
- Comprendre les concepts de base du durcissement de la sécurité Windows ;
- Identifier les vulnérabilités courantes dans les configurations de sécurité Windows et les meilleures pratiques pour les résoudre ;
- Comprendre les principes fondamentaux du durcissement de la sécurité Windows, y compris les mesures de sécurité, les stratégies de groupe, les paramètres de sécurité avancés et les solutions de sécurité tierces ;
- Apprendre à durcir les configurations de sécurité pour les réseaux Windows, y compris les services de domaine Active Directory, les serveurs de fichiers, les serveurs Web et les clients Windows ;
- Comprendre les meilleures pratiques en matière de gestion des correctifs, des mises à jour et des configurations de sécurité pour les systèmes Windows ;
- Acquérir les compétences nécessaires pour auditer et évaluer les configurations de sécurité Windows existantes, identifier les vulnérabilités potentielles et proposer des solutions de sécurité efficaces.

Public

- Professionnels de la cybersécurité cherchant à renforcer leurs compétences en matière de sécurité du système d'exploitation Windows.
- Administrateurs système souhaitant comprendre les risques de sécurité associés aux systèmes d'exploitation Windows et mettre en place des mesures de sécurité adéquates.
- Ingénieurs en sécurité et architectes en sécurité cherchant à concevoir des systèmes Windows sécurisés.
- Étudiants souhaitant se spécialiser dans la sécurité du système d'exploitation Windows et développer des compétences dans ce domaine pour leur future carrière.

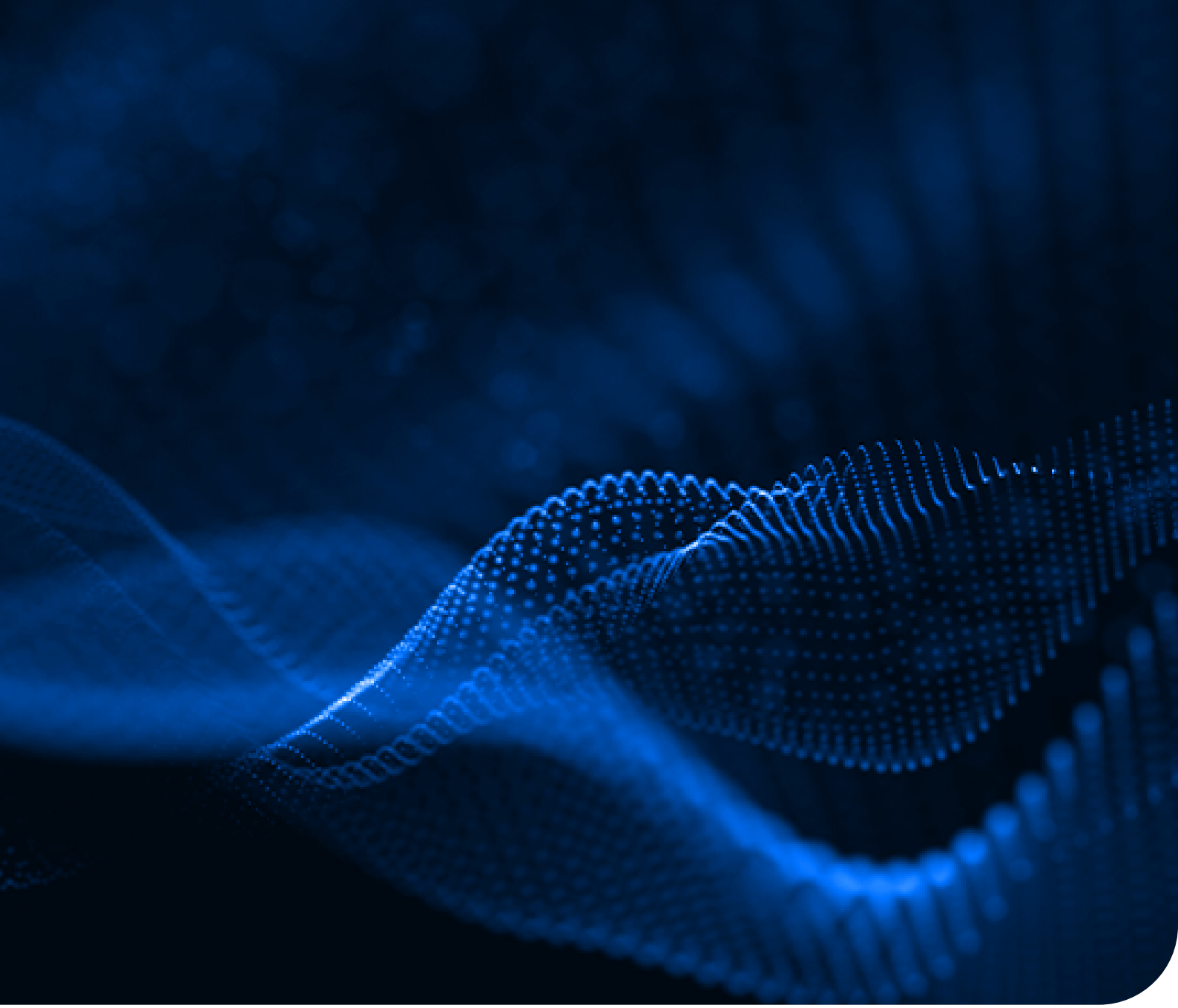
Prérequis

- Connaissance pratique de l'installation et de la configuration de Windows Server et/ou de Windows Desktop.
- Compréhension des concepts de base de l'administration des systèmes Windows, tels que les politiques de sécurité, les comptes d'utilisateurs, les services, etc.
- Connaissance pratique des outils de gestion des systèmes Windows, tels que PowerShell, l'Éditeur de stratégie de groupe, etc.
- Connaissance pratique des principes de base de la sécurité informatique, tels que les attaques courantes, les vulnérabilités, les méthodes de réduction des risques, etc.
- Expérience pratique de la configuration de la sécurité Windows, y compris la configuration du pare-feu, de l'antivirus, etc.



Programme de la formation

Jour 1	**Section 1 – Introduction sur l'écosystème actuel** • L'évolution des systèmes d'information et de leurs menaces • Segmentation et études des phases d'un attaquant (CyberKill Chain & MITRE ATT&CK) • Chronologie et évolutions majeures des systèmes d'exploitation Windows • Les attaques courantes dans un domaine Windows • TP 1 / Mener une étude Cyber Kill-Chain **Section 2 – Durcissement des domaines Windows** • Cohérence et défauts de conception Active Directory (AGDLP, GPO, Relations approbations, délégation) • Sécurité des droits d'administrations (ACL, Red Forest ESAE, Silo, Bastion, délégation) • Sécurité des comptes à privilèges (AdminSDHolder, LAPS, PAM) • Utilisation d'une infrastructure de clés publiques PKI (NPS, Radius, WIFI, carte à puce ...) • Sécurisation des protocoles d'administration (RPC, WMI, WinRM) • Sécurité des services et comptes de services managés • TP 2 / Implémenter LAPS
Jour 2	• Système de prévention de perte de données (Classification, Marquage, DLP) • Surveillance et journaux d'événements (Surveillance en profondeur, Sysmon) • Microsoft ATA et Threat Intelligence • TP 3 / Appliquer les règles de classification et de surveillance sur des données confidentielles • TP 4 / Renforcer la journalisation (Sysmon + Journalisation WMI pivoting) **Section 3 – Durcissement des serveurs et postes clients** • Sécurisation du démarrage (UEFI, Bitlocker, ...) • Sécurité des applications (Applocker, Device Guard) • Sécurité de l'authentification (SSP, credential guard) • Contrôler l'élévation de privilèges (UAC) • Fonctionnalité antivirale (Defender, AMSI, SmartScreen) • Sécurité de Powershell (Politique de restriction, JEA, Journalisation) • Réduction de la surface d'attaque (Serveur Core / Nano) • TP 5 / Déployer Bitlocker • TP 6 / Configurer PowerShell JEA **Section 4 – Durcissement des protocoles réseau** • L'authentification Microsoft (NTLM, NET-NTLM, Kerberos) • Les protocoles Microsoft (WPAD, SMB, RDP, LLMNR, ...) • Étude et recherche de vulnérabilités protocolaires • TP 7 / Sécuriser LLMNR & SMB



Programme de la formation

Jour 3	**Section 5 – Mécanisme de défense avancé** • Détection des attaques avancées • Auditer son architecture • TP 8 / Auditer son architecture et préparer un plan de contre-mesure
Jour 4	**Section 6 – Durcissement des domaines Azure** • Rappel sur Azure et IAM • Authentification et autorisation Azure • Zoom sur les attaques Azure • Renforcement des défenses Azure • Auditer son architecture cloud

Sécurité Linux

La formation sur la Sécurité Linux est conçue pour valider les compétences des professionnels de la cybersécurité en matière de sécurisation des systèmes Linux, y compris la configuration, la gestion et la résolution des problèmes de sécurité. Il couvre un large éventail de sujets, notamment la sécurité des systèmes Linux, les outils et techniques de test de vulnérabilité, les méthodes de renforcement des systèmes Linux, etc.

Il est adapté aux professionnels de la cybersécurité, aux administrateurs système, aux ingénieurs en sécurité, aux architectes en sécurité, aux auditeurs de sécurité et aux responsables de la sécurité qui travaillent avec des systèmes Linux et cherchent à renforcer leurs compétences en matière de sécurité Linux. En obtenant cette certification, les candidats peuvent améliorer leur employabilité et accéder à des opportunités professionnelles plus avancées dans le domaine de la cybersécurité.

Objectifs pédagogiques

- Administrateurs système Linux cherchant à améliorer leurs compétences en matière de sécurité.
- Ingénieurs en sécurité travaillant sur la sécurisation des systèmes Linux.
- Architectes en sécurité concevant des architectures de sécurité pour les environnements Linux.
- Auditeurs de sécurité évaluant l'efficacité des mesures de sécurité dans les environnements Linux.
- Responsables de la sécurité supervisant les opérations de sécurité pour les environnements Linux.

Public

- Étudiants cherchant à entrer dans le domaine de la cybersécurité et souhaitant se spécialiser dans les tests d'intrusion et les évaluations de vulnérabilités.
- Professionnels de la cybersécurité débutants cherchant à se spécialiser dans les tests d'intrusion et les évaluations de vulnérabilités.
- Professionnels de la sécurité informatique cherchant à ajouter des compétences en tests d'intrusion et en évaluation de vulnérabilités à leur profil de compétences existant.

Prérequis

- Connaissance pratique des systèmes Linux, y compris la configuration, la gestion et la résolution des problèmes.
- Compréhension de base des concepts de sécurité informatique, tels que la sécurité réseau, la gestion de la sécurité de l'information et les méthodes de test de vulnérabilités.
- Expérience pratique de la sécurisation des systèmes Linux, y compris la configuration de la sécurité, la gestion des correctifs de sécurité et la mise en place de mesures de sécurité pour les systèmes Linux.
- Expérience pratique de l'utilisation d'outils de test de vulnérabilités pour les systèmes Linux.

Programme de la formation

Jour 1	**Section 1 - Introduction sur les principes de sécurité et de durcissement** • Principe de minimisation • Principe de moindre privilège • Défense en profondeur • Intrusion et impact **Section 2 - Installation du système** • Partitionnement • Chiffrement du système (LUKS) • Sécurité du démarrage (Chiffrement /boot) • Sécurité du démarrage (Boot & Grub) • Sécurité du démarrage (Secure Boot) • Chiffrement des données (Ecryptfs) **Section 3 - Sécurité de l'authentification** • PAM • Authentification renforcée
Jour 2	**Section 4 - Sécurité des accès** • Rappel sur les droits d'accès • Sécurité des droits d'accès (umask, chattr, SUID, ACL, ...) • Protection des fichiers sensibles (AIDE, HIDS) **Section 5 - Sécurité des services réseaux** • SSH • NFS • Firewalling (Firewalld, IPtables) • Fail2ban • Portsentry • Pile applicative
Jour 3	**Section 6 - Sécurité du système** • Sudo • SELinux • Apparmor • Hardening Système • Isolation de processus (chroot, ...) • Détection antivirale • Sauvegarde
Jour 4	**Section 7 - Journalisation et sécurité** • Principe de journalisation sécurisé • Rappel sur les journaux Linux • Auditd • rsyslog **Section 8 - Auditer et renforcer** • Principe d'audit • Référentiels • Outils

Formations en réponse aux incidents et investigation numérique

Nos formations en réponse aux incidents et investigation numériques sont conçues pour vous aider à devenir un intervenant en incidents compétent et un enquêteur numérique qualifié. Apprenez à gérer et à répondre aux incidents de sécurité, à analyser les menaces et à mener des enquêtes tout en respectant les exigences légales. Ces formations fournissent des compétences pratiques pour la collecte, la préservation et l'analyse de preuves numériques, vous assurant d'être bien préparé à atténuer les menaces et à répondre efficacement aux incidents cyber.

Ce portefeuille comprend les formations suivantes :

- Investigation numérique Windows
- Investigation numérique Linux
- Réponse aux incidents

Investigation numérique Windows

La formation sur l'Investigation numérique sous Windows est une formation pratique destinée aux professionnels de la sécurité informatique cherchant à acquérir des compétences en investigation numérique dans l'environnement Windows, ainsi qu'aux professionnels souhaitant ajouter des compétences en investigation numérique à leur profil de compétences existant. La formation couvre un large éventail de sujets, notamment les normes et méthodologies de l'investigation numérique, les concepts fondamentaux de Windows, les techniques de prévention et de détection des intrusions, l'analyse des artefacts système et la génération et l'analyse des chronologies.

Les participants apprendront les méthodes de prévention et de détection des intrusions, la collecte et l'analyse de données, l'utilisation d'outils d'investigation numérique et la rédaction de rapports d'incident détaillés. La formation comprend également des travaux pratiques pour permettre aux participants de mettre en pratique les compétences acquises et de se familiariser avec les outils utilisés dans des situations réelles.

Objectifs pédagogiques

- Comprendre les normes et méthodologies d'investigation numérique pour l'environnement Windows.
- Maîtriser les concepts fondamentaux de Windows pour pouvoir collecter et analyser des données numériques.
- Être capable de prévenir et de détecter les intrusions dans l'environnement Windows.
- Savoir analyser les artefacts de système pour identifier les preuves numériques lors d'une investigation.
- Être capable de générer et d'analyser une chronologie des événements lors d'une investigation numérique.
- Connaître les outils d'investigation numérique disponibles pour l'environnement Windows.
- Être capable de collecter et d'analyser des données numériques lors d'une investigation.
- Savoir générer des rapports détaillés sur les incidents.
- Mettre en pratique les compétences acquises lors de travaux pratiques.
- Se familiariser avec les outils utilisés en situation réelle.

Public

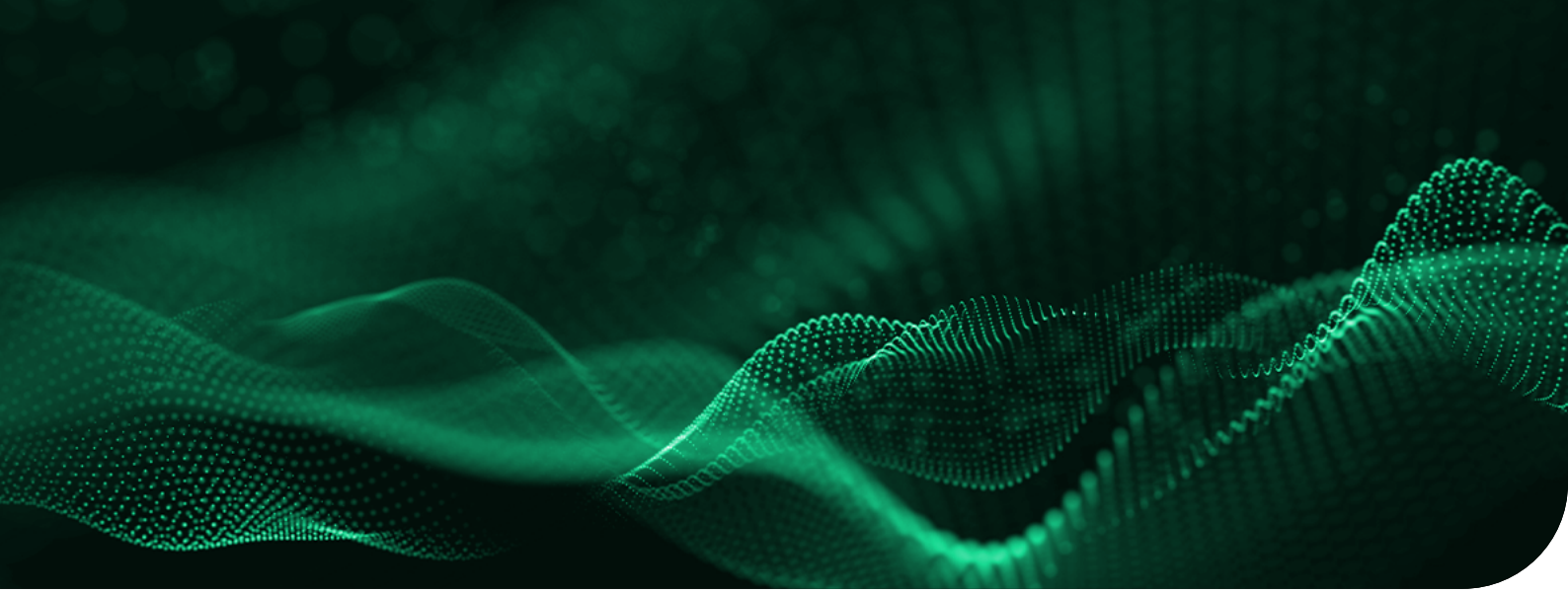
- Analystes de sécurité travaillant dans un Centre Opérationnel de Sécurité (SOC) ou une Équipe d'Intervention en Cas d'Incident de Sécurité (CSIRT).
- Ingénieurs en sécurité concevant, mettant en œuvre et gérant des solutions de sécurité pour les SOC et les CSIRT.
- Architectes en sécurité concevant des architectures de sécurité pour les SOC et les CSIRT.
- Auditeurs de sécurité évaluant l'efficacité des opérations de sécurité dans les SOC et les CSIRT.
- Enquêteurs numériques travaillant sur des enquêtes impliquant des systèmes Windows et cherchant à renforcer leurs compétences en analyse numérique.
- Avocats travaillant sur des affaires légales impliquant des preuves numériques provenant de systèmes Windows.
- Forces de l'ordre travaillant sur des enquêtes criminelles impliquant des systèmes Windows.

Prérequis

- Connaissance pratique des opérations de sécurité, y compris la détection, l'analyse et la réponse aux incidents de sécurité.
- Compréhension de base des concepts de sécurité informatique, tels que la sécurité réseau, la gestion de la sécurité de l'information et les méthodes de test de vulnérabilités.
- Expérience pratique de l'utilisation d'outils de collecte de données de sécurité, tels que les SIEM (Systèmes d'Information et de Gestion des Événements de Sécurité), les outils de collecte de journaux, etc.
- Expérience pratique de l'analyse numérique forensique sur les systèmes Windows, y compris la récupération de preuves numériques, l'analyse de données et la validation de l'intégrité des données.

Programme de la formation

Jour 1 matin	**Section 1 - État de l'art de l'investigation numérique** • Introduction à l'investigation numérique • Vocabulaire • Les différentes disciplines • Indicateur de compromission • Méthodologie d'investigation • ATT&CK et Arbres d'attaque
Jour 1 après-midi	**Section 2 - Les fondamentaux Windows et Collecte des données** • Fondamentaux Windows • Structure des répertoires • Séquence de boot • Bases de Registres • Logs et événements • Services • Volume Shadow Copy Service • Généralités sur les disques durs • Fondamentaux NTFS • Analyse live • Analyse offline : imaging • Analyse offline : collecte • Les outils d'analyse
Jour 2 matin	**Section 3 - Artefacts** • Différents artefacts internet • Pièces jointes • Open/Save MRU • Flux ADS Zone.Identifier • Téléchargements • Historique Skype • Navigateurs internet • Historique • Cache • Sessions restaurées • Cookies • Différents artefacts exécution • UserAssist • Timeline Windows 10 • RecentApps • Shim cache • Jump list • Amcache.hve • BAM/DAM • Last-Visited MRU • Prefetch



Jour 2 après-midi	• Différents artefacts fichiers/dossiers • Shellbags • Fichiers récents • Raccourcis (LNK) • Documents Office • IE/Edge Files • Différents artefacts réseau • Termes recherchés sur navigateur • Cookie • Historique • SRUM (ressource usage monitor) • Log wifi • Différents artefacts comptes utilisateur • Dernières connexions • Changement de mot de passe • Échec/Réussite d'authentification • Événement de service (démarrage) • Événement d'authentification • Type d'authentification • Utilisation du RDP • Différents artefacts USB • Nomination des volumes • Evénement PnP (Plug & Play) • Numéros de série • Différents artefacts fichiers supprimés tools • Récupération de la corbeille • Thumbcache • Thumb.db • WordWheelQuery • Spécificités Active Directory • TP 3 / Première investigation • TP 4 / Deuxième investigation
Jour 3 matin	**Section 4 - Analyse mémoire et Anti Forensic** • Acquisition • Volatility • TP 5 / Investigation mémoire • Principes d'Anti Forensic • Techniques d'Anti Forensic
Jour 3 après-midi	• Tools pour Anti Forensic • TP6 / Anti Forensic

Investigation numérique Linux

La formation sur l'Investigation numérique sous Linux est conçue pour les professionnels de la sécurité informatique cherchant à acquérir des compétences approfondies en investigation numérique sur les systèmes Linux. Il couvre un large éventail de sujets, notamment la méthodologie d'une enquête numérique, les techniques de récupération de données, l'analyse de la RAM et de la mémoire de masse, l'analyse des journaux système et la rédaction de rapports.

Au cours de cette formation, les participants apprendront à utiliser des outils spécialisés pour collecter et analyser des preuves numériques, y compris des outils d'analyse de la RAM tels que Volatility, ainsi que des outils d'analyse des journaux système. Les participants apprendront également à appliquer les meilleures pratiques pour la collecte et la préservation de preuves numériques, notamment la chaîne de custody, l'identification des artefacts numériques pertinents et la rédaction de rapports détaillés. Cette formation est idéale pour les professionnels de la sécurité informatique cherchant à améliorer leurs compétences en enquête numérique sur les systèmes Linux, ainsi que pour ceux qui souhaitent ajouter des compétences en enquête numérique à leur profil de compétences existant.

Objectifs pédagogiques

- Comprendre les bases de l'investigation numérique sur les systèmes Linux.
- Apprendre à identifier et collecter des preuves numériques sur des systèmes Linux.
- Comprendre les méthodes et outils pour l'analyse des fichiers et des données sur des systèmes Linux.
- Apprendre à manipuler les systèmes de fichiers, la mémoire vive et les journaux système sur des systèmes Linux pour collecter des preuves numériques.
- Apprendre à utiliser des outils de ligne de commande pour effectuer des recherches avancées et l'analyse de données sur des systèmes Linux.
- Comprendre les méthodes pour analyser les artefacts de réseau sur des systèmes Linux.
- Apprendre à identifier et à documenter les vulnérabilités de sécurité sur les systèmes Linux.
- Comprendre les techniques et les meilleures pratiques pour la présentation des résultats d'une investigation numérique sur des systèmes Linux.

Public

- Analystes de sécurité travaillant dans un Centre Opérationnel de Sécurité (SOC) ou une Équipe d'Intervention en Cas d'Incident de Sécurité (CSIRT).
- Ingénieurs en sécurité concevant, mettant en œuvre et gérant des solutions de sécurité pour les SOC et les CSIRT.
- Architectes en sécurité concevant des architectures de sécurité pour les SOC et les CSIRT.
- Auditeurs de sécurité évaluant l'efficacité des opérations de sécurité dans les SOC et les CSIRT.
- Responsables de la sécurité supervisant les opérations de sécurité dans les SOC et les CSIRT.

Prérequis

- Connaissance pratique des opérations de sécurité, y compris la détection, l'analyse et la réponse aux incidents de sécurité.
- Compréhension de base des concepts de sécurité informatique, tels que la sécurité réseau, la gestion de la sécurité de l'information et les méthodes de test de vulnérabilités.
- Expérience pratique de l'utilisation d'outils de collecte de données de sécurité, tels que les SIEM (Systèmes d'Information et de Gestion des Événements de Sécurité), les outils de collecte de journaux, etc.
- Expérience pratique de la gestion des vulnérabilités et du déploiement de correctifs de sécurité.

Programme de la formation

Jour 1	**Section 1 - La réponse à incident et l'investigation numérique** • Normes et méthodologies • NIST / SANS • PRIS / ISO • Cadre légal **Section 2 - Linux : Concepts fondamentaux** **Section 3 - Live Forensics** • Sources et commandes associées • Outils **Section 4 - Prélèvement** • Concepts et Pré-requis

Jour 2	**Section 5 - La mémoire vive**
	• Prélèvement
	  • Physique
	  • Virtualisée
	• Validation du prélèvement
	• Chain of custody/evidence
	• Analyse
	• Fonctionnement de Volatility 2/3
	• Concepts (profil, vtype, volshell)
	• Liste des modules + méthodologie
	• TP
	Section 6 - La mémoire vive (TP/TD)
	• TP/TD

Jour 3	**Section 7 - La mémoire de masse** • Prélèvement • physique • Virtualisée • Analyse • Concepts (ext4, VFS, ...) • Timeline • Génération et analyse • Artefacts • Services • Journalisation système • logs
Jour 4	**Section 8 - Cas d'étude 1 – Exploitation d'un frontal web** **Section 9 - Cas d'étude 2 – Exploitation de la CVE-2012-22205** **Section 10 - Cas d'étude 3 – Rootkit Userland**

Réponse aux incidents

La formation Réponse aux incidents vise à valider les compétences des professionnels de la cybersécurité dans la détection, l'analyse et la réponse aux incidents de sécurité dans un environnement opérationnel. Il couvre un large éventail de sujets, notamment la réponse aux incidents de sécurité, la collecte de données, la recherche de menaces (Threat hunting), etc. De plus, la formation équipe les participants des compétences nécessaires pour rédiger des rapports détaillés sur les incidents de sécurité et des recommandations de remédiation.

Il est destiné aux professionnels de la cybersécurité, aux analystes de sécurité, aux ingénieurs en sécurité, aux architectes en sécurité, aux auditeurs de sécurité et aux responsables de la sécurité qui travaillent dans des environnements de sécurité opérationnelle et cherchent à renforcer leurs compétences en matière de réponse aux incidents de sécurité. En obtenant cette certification, les candidats peuvent améliorer leur employabilité et accéder à des opportunités professionnelles plus avancées dans le domaine de la cybersécurité.

Objectifs pédagogiques

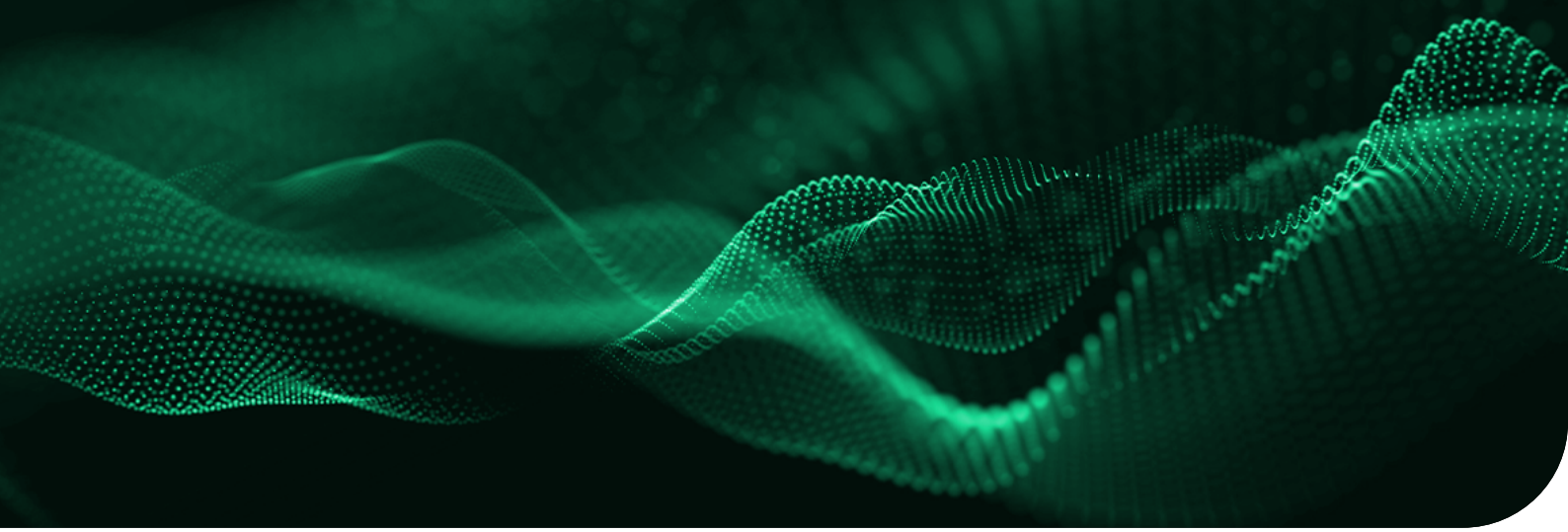
- Comprendre les concepts clés de la réponse aux incidents : les participants seront en mesure de comprendre les concepts clés de la réponse aux incidents, notamment les différentes phases de la réponse aux incidents, les rôles et responsabilités de l'équipe de réponse aux incidents, les outils et techniques utilisés dans la réponse aux incidents, et les meilleures pratiques pour mener une enquête de réponse aux incidents efficace.
- Apprendre à planifier et à préparer une réponse aux incidents : les participants seront en mesure de planifier et de préparer une réponse aux incidents en développant des plans d'urgence, en établissant des procédures de communication et de notification, en formant et en éduquant le personnel sur les procédures de réponse aux incidents, et en mettant en place des outils et des technologies pour soutenir la réponse aux incidents.
- Développer des compétences pour détecter et répondre à des incidents de sécurité : les participants apprendront à détecter et à répondre à des incidents de sécurité, y compris la collecte et l'analyse des preuves numériques, la gestion des incidents, l'atténuation des attaques en cours, et la restauration des systèmes affectés.
- Comprendre les meilleures pratiques en matière de réponse aux incidents : les participants seront en mesure de comprendre les meilleures pratiques en matière de réponse aux incidents, notamment les normes de conformité, les réglementations, les lois et les directives, ainsi que les recommandations et les conseils de sécurité actuels.
- Préparer des rapports d'incident efficaces : les participants apprendront à préparer des rapports d'incident clairs et concis, qui incluent des informations sur la nature et l'étendue de l'incident, les mesures prises pour y répondre, et les recommandations pour éviter les incidents similaires à l'avenir.
- Participer à des simulations de réponse aux incidents : les participants auront l'opportunité de participer à des simulations de réponse aux incidents pour mettre en pratique les compétences acquises et les meilleures pratiques de la réponse à incident.

Public

- Analystes de sécurité travaillant dans un Centre Opérationnel de Sécurité (SOC) ou une Équipe d'Intervention en Cas d'Incident de Sécurité (CSIRT).
- Ingénieurs en sécurité concevant, mettant en œuvre et gérant des solutions de sécurité pour les SOC et les CSIRT.
- Architectes en sécurité concevant des architectures de sécurité pour les SOC et les CSIRT.
- Auditeurs de sécurité évaluant l'efficacité des opérations de sécurité dans les SOC et les CSIRT.
- Responsables de la sécurité supervisant les opérations de sécurité dans les SOC et les CSIRT.

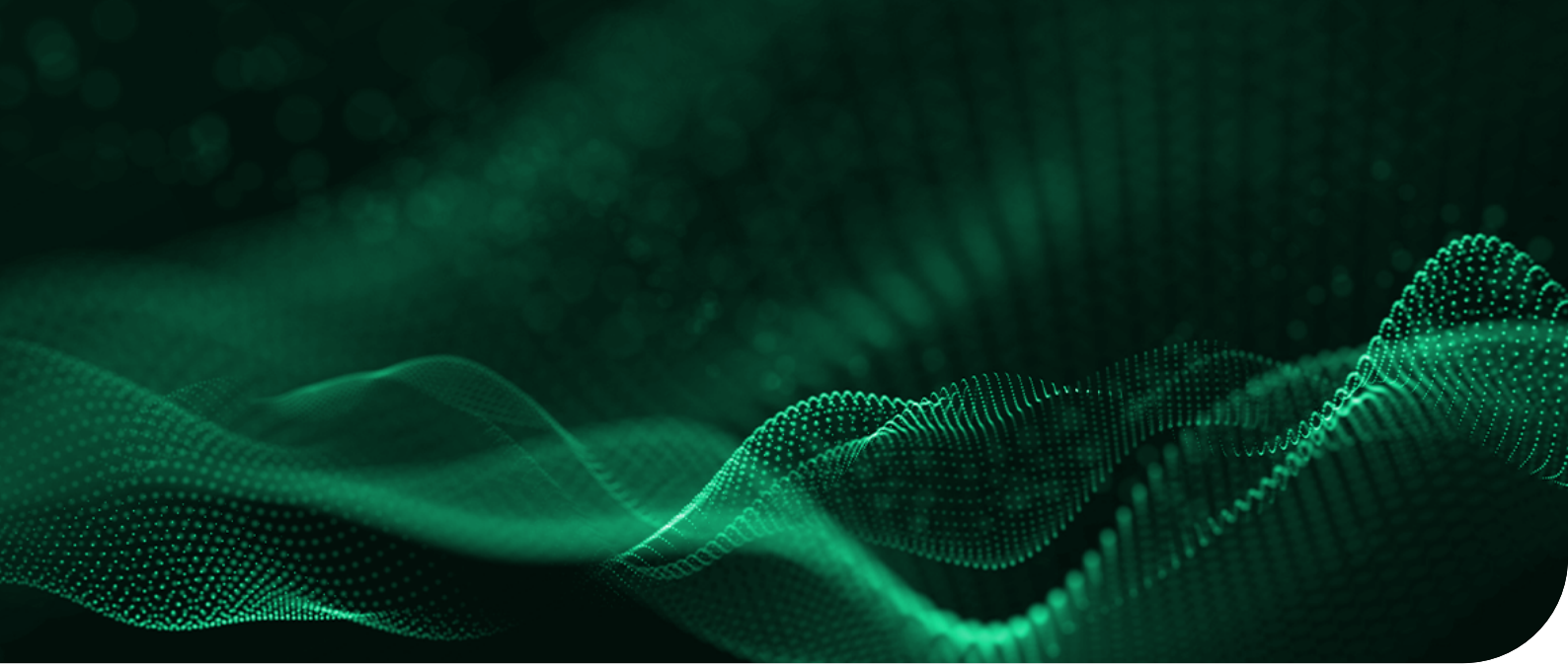
Prérequis

- Connaissance pratique des opérations de sécurité, y compris la détection, l'analyse et la réponse aux incidents de sécurité.
- Compréhension de base des concepts de sécurité informatique, tels que la sécurité réseau, la gestion de la sécurité de l'information et les méthodes de test de vulnérabilités.
- Expérience pratique de l'utilisation d'outils de collecte de données de sécurité, tels que les SIEM (Systèmes d'Information et de Gestion des Événements de Sécurité), les outils de collecte de journaux, etc.
- Expérience pratique de la gestion des vulnérabilités et du déploiement de correctifs de sécurité.



Programme de la formation

Jour 1	**Section 1 - Introduction** • La menace cyber en 2023 (statistique réponse aux incidents) • Les acteurs de la cybercriminalité (APT, cybercrime, hacktivisme, etc.) • Les différents vecteurs d'attaques • Mitre ATT&CK • Les métiers de la cybersécurité en 2023 • Définition de la réponse à incident et l'investigation numérique (CERT, CSIRT, ISAC, CERTFR, FIRST) • SOC vers le CSIRT (proactive vs réactive) **Section 2 - Méthodologie de la réponse à incident** • Préparation • Identification • Confinement • Eradication • Restauration • Enseignement **Section 3 - Cadre légal** • CERT vs CSIRT • CNIL • PRIS • Réseaux FIRST, TI
Jour 2	**Section 4 - Microsoft Windows : concepts fondamentaux** • Histoire de Windows • Architecture (user land, Kernel-land) • API Windows • Framework .net • Processus clés • Threads • Virtual Memory • Service Windows • VBS • Base de registre • Pilote • WMI • CERT • EVT (type, Id) • Répertoire • Tâches planifiés • Credential gard • Active directory (Architecture, catalog global, GPO, etc.) • Questionnaire



Programme de la formation

Jour 3

Section 5 - Tactiques courantes et logiciels malveillants

- Les différentes techniques utilisées (TTPs communes, evasion, anti-vm, signature)
- « Initial access »
  - SPF, DMARK
  - Attaque par dictionnaire
  - Social engeneering
- “Execution”
  - Procédure courante (.vbs, WSH, PS)
  - Répertoires utilisés
  - Évasion (Process Hollowing, anti-vm, polymorphisme, etc.)
- “Persistence”
  - Tâches planifiées
  - .dll injection
  - Base de registre
- “Privilege escalation”
  - DLL hijacking
- “Credential access”
  - NTML hash
  - Attaque par dictionnaire
- “Discovery”
  - net user, localgroup
  - /etc/passwd
  - dscacheutil
  - Get—aduser
- “Lateral movement”
  - RDP, SSH, SCCM, Altiris
  - PTH, Golden ticket
  - Cookie hijacking
- “Command and control & exfiltration”
  - Fast flux, Web service, email
  - Cobalt strike, Brute ratel, Sliver
  - Services utilisés par les C2 (regsvr32.exe, rundll32.exe, wscript.exe, mshta.exe, cscript.exe, msxsl.exe)
- Détection de logiciels malveillants (automatique, manuelle)
  - Sigcheck
  - Pestudio
- Lab1 (Analyser une charge)

Programme de la formation

Jour 4

Section 6 - Artefacts Windows

- Artefact informations systèmes
  - informations systèmes
  - informations réseaux
- Artefact journaux d'événement
  - .evtx, .etw ; template, Auditpol
  - Journaux, EventID, template, Sysmon
  - Création de compte
  - Connexions et tentatives de bruteforce
  - Connexions RDP
  - Identifier un Pass the hash
  - Identifier un process hollowing
  - Identifier tentative d'utilisation de WMI
  - Énumération
  - Suppression des journaux
  - Zircolite
  - Lab2 (recherche charges utile)
- Artefact d'exécution
  - Prefech
  - Amcache.hve
  - Shimcache
  - .lnk
  - Recents app
  - Jumplist
  - SRUM
  - Fichiers récents
  - Shellbags
  - Background Activity Moderator
- Artefact WEB & Email
  - Navigateur (Chrome, Firefox, Edge, etc.)
  - .pst
- Artefact exécution de scripts
  - Log Powershell
  - History
  - Wecutil
- Artefact USB
  - USBTOR
  - Setupapi
- Artefact suppression de fichiers
  - $Recycle.Bin
  - Snapshot
  - Rifiuti2
  - Thumbcache
- MFT
  - NTFS, Timestamp, MACB
  - Résident ou non résident
  - ADS
- Powerforensic
- Artefact mouvements latéraux
  - PSEXEC
  - PTH
  - Partage
  - Tâches planifiées
  - WINRM
  - Teamviewer, RDP, VNC
  - GPO
- Lab3 (Artefact Windows)

Programme de la formation

Jour 5

Section 7 - Mémoire vive

- Acquisition des données volatiles (physique, VM)
- Acquisition de masse
- Volatility 3
  - profils
  - modules
  - Injection processus, code (PE, Shellcode)
  - Yara scan
- Swap, Hybernation
- Analyse de la mémoire de masse
- Lab 3 (Analyse de données volatiles)
- Lab 4 (Analyse de données volatiles 2)

Section 8 - Timeline

- Acquisition des données du disque
- Acquisition de masse
- MFT, NTFS, Timestamp, MACB
- DFIR ORC
- Powerforensic
- MFT
- ADS
- Supertimeline
- Fichiers supprimés (thumbcache, thumbs.db)
- Carving
- Lab 4 ()

Section 9 — Anti Forensics

- Anti-Forensics/Timestomping
- utiliser VSS, Prefetch en cas d'anti forensics

Section 10 — Gnu/linux

- Live Forensic
- Sources et commandes associées
- Outils (Osquery, Vélociraptor…)
- Prélèvements
- Prérequis
- La mémoire vive
- Prélèvement
- Analyse
- La mémoire de masse
- Prélèvement
- Analyse
- Artefacts

Section 11 — Aller plus loin

- Playbook
- Aller plus loin
- Ressources
- Les auteurs

Formations en Fondamentaux de la Cybersécurité

Cette formation complète en cybersécurité est conçue pour habiliter les apprenants avec une compréhension approfondie des principes fondamentaux de la cybersécurité, une large sensibilisation à diverses menaces, et un ensemble robuste de techniques pour protéger les systèmes, les réseaux et les données critiques. De plus, les participants acquerront une connaissance complète du paysage complexe des réglementations et de la législation en matière de cybersécurité, les équipant de l'expertise nécessaire pour gérer habilement les risques et naviguer efficacement à travers les situations de crise dans le domaine de la cybersécurité.

Objectifs pédagogiques

- Comprendre la menace cyber et s'en protéger en abordant les métiers et leurs quotidiens

Public

- Tous les publics intéressés par le domaine de la cybersécurité.

Prérequis

- Aucun.

Programme de la formation

Jour 1	Introduction à la cybersécurité et menaces courantes **Section 1 - Introduction à la cybersécurité :** • Définitions et objectifs de la cybersécurité • Les acteurs de la cybersécurité : hackers, pirates informatiques, employés malveillants, etc. • Les enjeux de la cybersécurité pour les entreprises et les particuliers • Les domaines de la cybersécurité : sécurité des systèmes, sécurité des réseaux, sécurité des données, etc. **Section 2 - Les menaces courantes en cybersécurité :** • Les différents types de menaces en cybersécurité : les malwares, les attaques par déni de service (DDoS), l'ingénierie sociale, l'hameçonnage, etc. • Les conséquences des attaques : pertes financières, atteinte à la réputation, pertes de données sensibles, etc. • Les dernières tendances et évolutions dans le domaine de la cybersécurité
Jour 2	Sécurité des systèmes et des réseaux **Section 3 - Sécurité des systèmes :** • Les concepts de base de la sécurité des systèmes : authentification, autorisation, chiffrement, etc. • La sécurité des systèmes d'exploitation : Windows, Linux, macOS, etc. • Les vulnérabilités courantes des systèmes : exploitation de failles, piratage de comptes, etc. • Les outils pour protéger les systèmes : antivirus, pare-feu, anti-spyware, etc. • Les meilleures pratiques pour la sécurité des systèmes : mises à jour, gestion des comptes, etc. **Section 4 - Sécurité des réseaux :** • Les concepts de base de la sécurité des réseaux : topologies, protocoles, etc. • Les menaces pour les réseaux : attaques de réseau, sniffing de paquets, attaques de type « man-in-the-middle », etc. • Les outils pour protéger les réseaux : pare-feu, IDS/IPS, VPN, etc. • Les meilleures pratiques pour la sécurité des réseaux : gestion des accès, surveillance des flux, etc.
Jour 3	Sécurité des données et gestion des risques **Section 5 - Sécurité des données :** • Les concepts de base de la sécurité des données : confidentialité, intégrité, disponibilité, etc. • Les menaces pour les données : vol de données, destruction de données, etc. • Les techniques pour protéger les données : chiffrement, contrôle d'accès, etc. • Les outils pour la sécurité des données : gestionnaires de mots de passe, solutions de backup, etc. **Section 6 - Gestion des risques :** • Les concepts de base de la gestion des risques en cybersécurité : identification des risques, évaluation des risques, etc. • Les techniques pour gérer les risques : stratégies de prévention, plans de continuité d'activité, etc. • Les meilleures pratiques pour la gestion des risques en cybersécurité

Programme de la formation

Jour 4	Conformité et législation **Section 7 - Conformité et réglementation :** • Les réglementations en matière de cybersécurité : GDPR, PCI DSS, etc. • Les audits de sécurité : ISO 27001, SOC 2, etc. • Les implications de la conformité pour les organisations : sanctions financières, réputation, etc. • Les meilleures pratiques pour la conformité et la réglementation en matière de cybersécurité **Section 8 - Législation :** • Les lois en matière de cybersécurité : loi informatique et libertés, loi sur la sécurité nationale, etc. • Les implications juridiques des attaques : responsabilité, obligations de notification, etc. • Les meilleures pratiques pour la conformité légale en matière de cybersécurité
Jour 5	Attaques avancées et gestion de crise **Section 9 - Attaques avancées :** • Les attaques sophistiquées : APT (Advanced Persistent Threats), attaques de type « zéro-Jour», etc. • Les vecteurs d'attaques émergents : l'Internet des Objets (IoT), l'intelligence artificielle (AI), etc. • Les techniques avancées d'attaques : techniques de phishing, ingénierie sociale, etc. • Les outils pour la détection et la prévention des attaques avancées : analyse comportementale, sécurité basée sur l'identité, etc. **Section 10 - Gestion de crise :** • La gestion de crise en cybersécurité : planification, gestion des incidents, etc. • Les rôles et responsabilités dans la gestion de crise : équipes de réponse aux incidents, direction, etc. • Les meilleures pratiques pour la gestion de crise en cybersécurité : communication, coordination, etc. **Section 11 - Études de cas et pratiques :** • Études de cas sur les cyberattaques : WannaCry, Equifax, etc. • Pratiques pour la cybersécurité : simulations d'attaques, formation de sensibilisation à la sécurité, etc. • TP final pour mettre en pratique les compétences acquises pendant la formation

Formations en gestion de la sécurité

Nos formations en Gestion de la Sécurité sont conçues pour ceux qui aspirent à diriger et gérer des initiatives de cybersécurité. Apprenez à manager efficacement, à gérer les risques et à garantir la conformité au sein de votre organisation. Ces formations plongent dans la création et la mise en œuvre de politiques et de stratégies de cybersécurité, vous dotant des compétences nécessaires pour protéger les actifs numériques et gérer des équipes de sécurité. L'évaluation des risques, l'analyse et l'atténuation de la sécurité sont au cœur de nos préoccupations, garantissant que vous pouvez prendre des décisions éclairées pour protéger efficacement votre organisation.

Cette sélection comprend les formations suivantes :

- Gestion des risques avec EBIOS
- Mise en œuvre de la norme ISO/IEC 27001 T Auditeur ISO/IEC 27001
- ISO/IEC 27005:2022
- Manager en DevSecOps

Gestion des risques avec EBIOS

Conformément à la méthodologie EBIOS, cette formation aide les individus à acquérir les connaissances et les compétences nécessaires pour naviguer avec succès dans les principes et les composantes de la gestion des risques applicables à tous les actifs pertinents dans le domaine de la sécurité de l'information. Cette formation est conçue pour les professionnels impliqués dans la sécurité de l'information, y compris les responsables de la sécurité de l'information, les professionnels de l'informatique, les responsables de la continuité des activités et de la gestion des risques, les responsables de la conformité, les consultants, les auditeurs et toute personne intéressée par la sécurité de l'information.

Objectifs pédagogiques

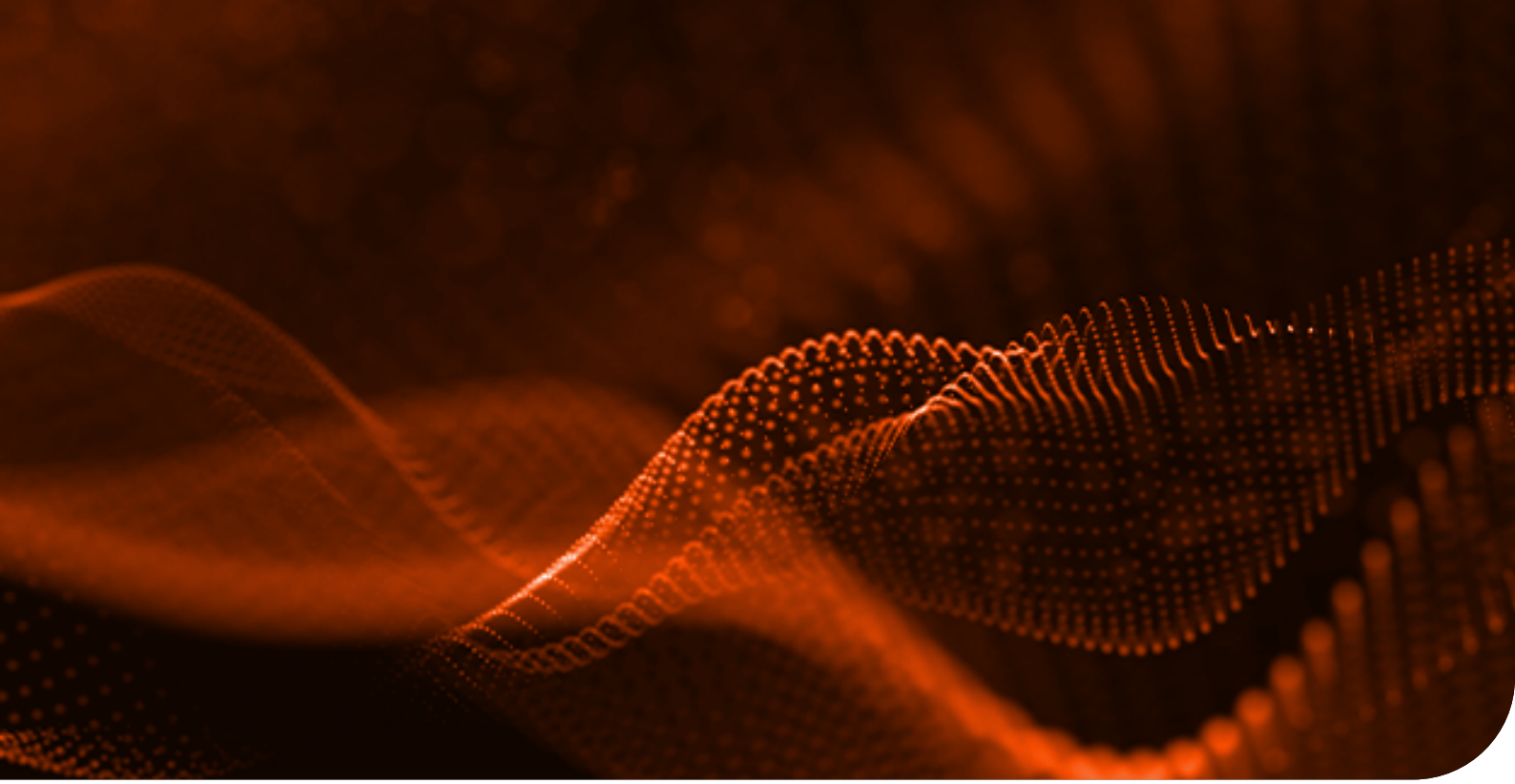
- Comprendre les bases de la gestion des risques en utilisant la méthode EBIOS.
- Apprendre à suivre les étapes de la méthode EBIOS (pilote, contrôle, recadrage) en tant que professionnel compétent.
- Expliquer les conclusions et les résultats clés d'une étude EBIOS.
- Acquérir les compétences pour mener efficacement une étude EBIOS.
- Développer les capacités pour gérer les risques de sécurité dans les systèmes d'information d'une organisation.
- Apprendre à analyser et à communiquer les résultats d'une étude EBIOS.

Public

- Les personnes intéressées à acquérir des connaissances et un aperçu des principes fondamentaux de la gestion des risques.
- Les individus impliqués dans les tâches d'évaluation des risques utilisant la méthode EBIOS.
- Les gestionnaires visant à maîtriser les méthodologies pour la réalisation d'évaluations des risques en utilisant la méthode EBIOS.
- Les gestionnaires s'efforçant d'exceller dans les techniques d'évaluation et de communication des résultats d'une évaluation des risques basée sur la méthode EBIOS.
- Les professionnels impliqués dans la planification de la continuité et l'évaluation des risques, tels que les responsables de la continuité des activités.
- Les consultants et les auditeurs cherchant à élargir leur expertise dans l'évaluation des risques avec la méthode EBIOS.
- Les individus souhaitant élargir leur expertise dans l'évaluation des risques avec la méthode EBIOS, tels que les consultants et les auditeurs.

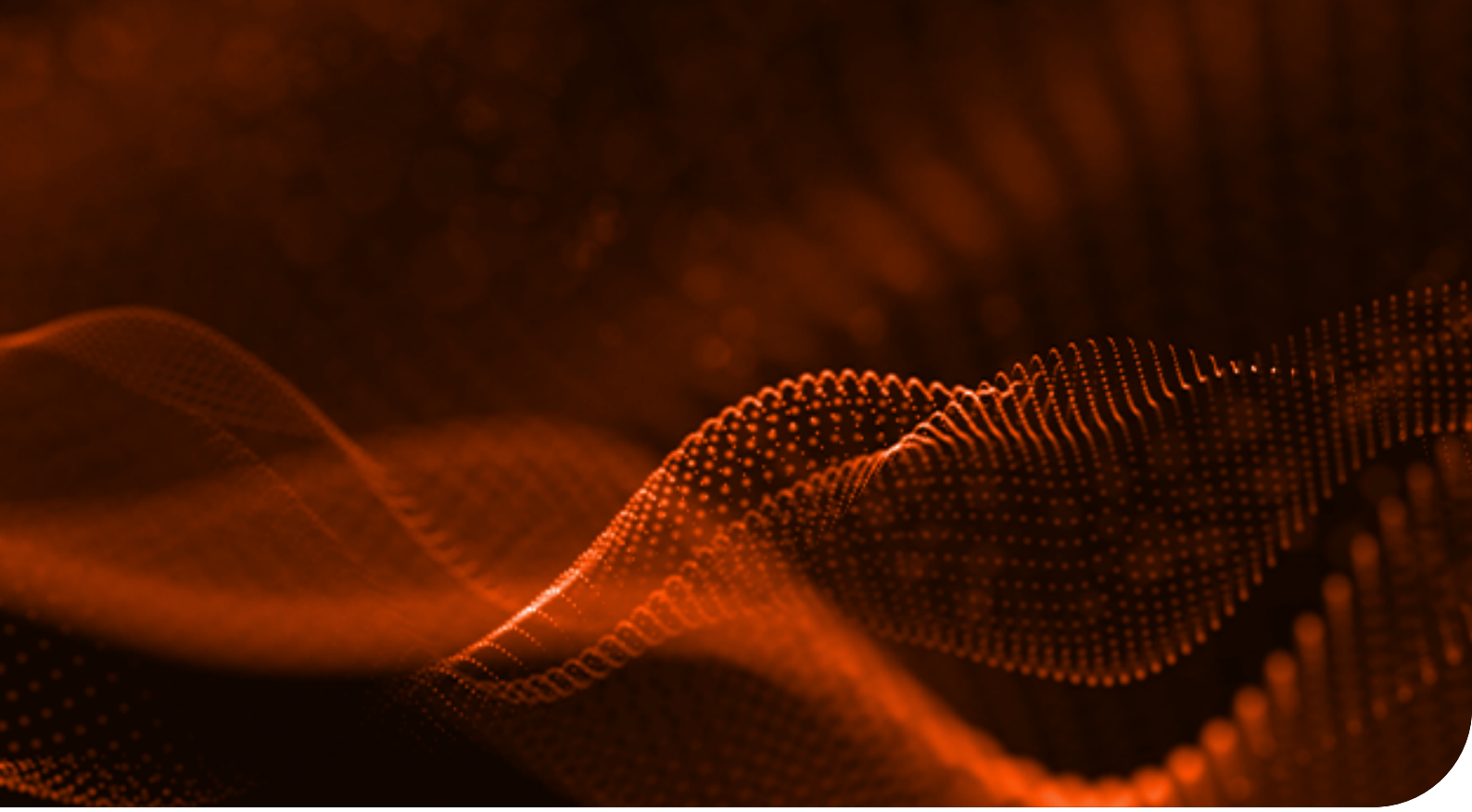
Prérequis

- Une connaissance fondamentale de la gestion des risques.



Programme de la formation

Jour 1 matin	**Section 1 – Objectifs et structure de la formation** • Présentation du groupe • Points généraux • Objectifs et structure de la formation • Approche pédagogique • Évaluation des apprentissages **Section 2 – Introduction à la méthode EBIOS Risk Manager** • Les fondamentaux de la gestion des risques • Présentation d'EBIOS • Zoom sur la Cybersécurité (menaces prioritaires) • Principales définitions EBIOS RM • **Exercice 1** / Compréhension de la terminologie • Concept phare et atelier de la méthode EBIOS RM • Récapitulatif **Section 3 – Atelier 1 « Cadrage et socle de sécurité »** • Présentation de l'atelier • Définition du cadre de l'étude et du projet • Identification du périmètre métier et technique • Identification des événements redoutés et évaluation de leurs niveaux de gravité • Déterminer le socle de sécurité • **Exercice 2 /** Identifier les événements redoutés • Récapitulatif de l'atelier
Jour 1 après-midi	**Section 4 - Atelier 2 « Sources de risques »** • Présentation de l'atelier • Identifier les sources de risques (SR) et leurs Objectifs visés (OV) • Évaluer la pertinence des couples • Évaluer les couples SR/OV et sélectionner ceux jugés prioritaires pour l'analyse • Évaluer la gravité des scénarios stratégiques • **Exercice 3** / évaluer les couples SR/OV • Récapitulatif de l'atelier



Jour 2 matin	**Section 5 - Atelier 3 « Scénarios stratégiques »** • Présentation de l'atelier • Évaluer le niveau de menace associé aux parties prenantes • Construction d'une cartographie de menace numérique de l'écosystème et les parties prenantes critiques • **Exercice 4** / évaluer le niveau de menace associé aux parties prenantes • Élaboration des scénarios stratégiques • **Exercice 5** / élaboration de scénarios stratégiques • Définition des mesures de sécurité sur l'écosystème • Récapitulatif de l'atelier
Jour 2 après-midi	**Section 6 - Atelier 4 « Scénarios opérationnels »** • Présentation de l'atelier • Élaboration des scénarios opérationnels • Évaluation des vraisemblances • Pour aller plus loin (Threat modeling, ATT&CK, CAPEC) • **Exercice 6** / scénario opérationnel • Récapitulatif de l'atelier **Section 7 - Atelier 5 « Traitement du risque »** • Présentation de l'atelier • Réalisation d'une synthèse des scénarios de risque • Définition de la stratégie de traitement • Définir les mesures de sécurité dans un plan d'amélioration continue de la sécurité (PACS) • Évaluation et documentation des risques résiduels • Mise en place du cadre de suivi des risques • **Exercice 7** / PACS (Plan d'amélioration continue de la sécurité) • Conclusion
Jour 3 matin	**Certification Exam**

ISO/IEC 27001 Implementeur

L'ISO/IEC 27001 Implementeur est une formation destinée aux professionnels souhaitant se spécialiser dans la gestion de la sécurité de l'information et la mise en œuvre de la norme ISO/IEC 27001. Il couvre un large éventail de sujets, tels que les principes de la sécurité de l'information, la gestion des risques liés à la sécurité de l'information, la mise en œuvre de la norme ISO/IEC 27001, etc. De plus, la formation dote les participants des compétences nécessaires pour maintenir un système de management de la sécurité de l'information efficace.

Cette formation s'adresse aux professionnels de la cybersécurité, aux responsables de la sécurité de l'information, aux responsables de la conformité réglementaire, aux auditeurs de sécurité, aux responsables des risques, aux architectes de sécurité, et à tout professionnel travaillant dans des environnements de sécurité opérationnelle et cherchant à renforcer leurs compétences en matière de gestion de la sécurité de l'information et de mise en œuvre de la norme ISO/IEC 27001. En obtenant cette certification, les professionnels de la cybersécurité peuvent améliorer leur employabilité et accéder à des opportunités professionnelles plus avancées dans le domaine de la cybersécurité et de la sécurité informatique.

Objectifs pédagogiques

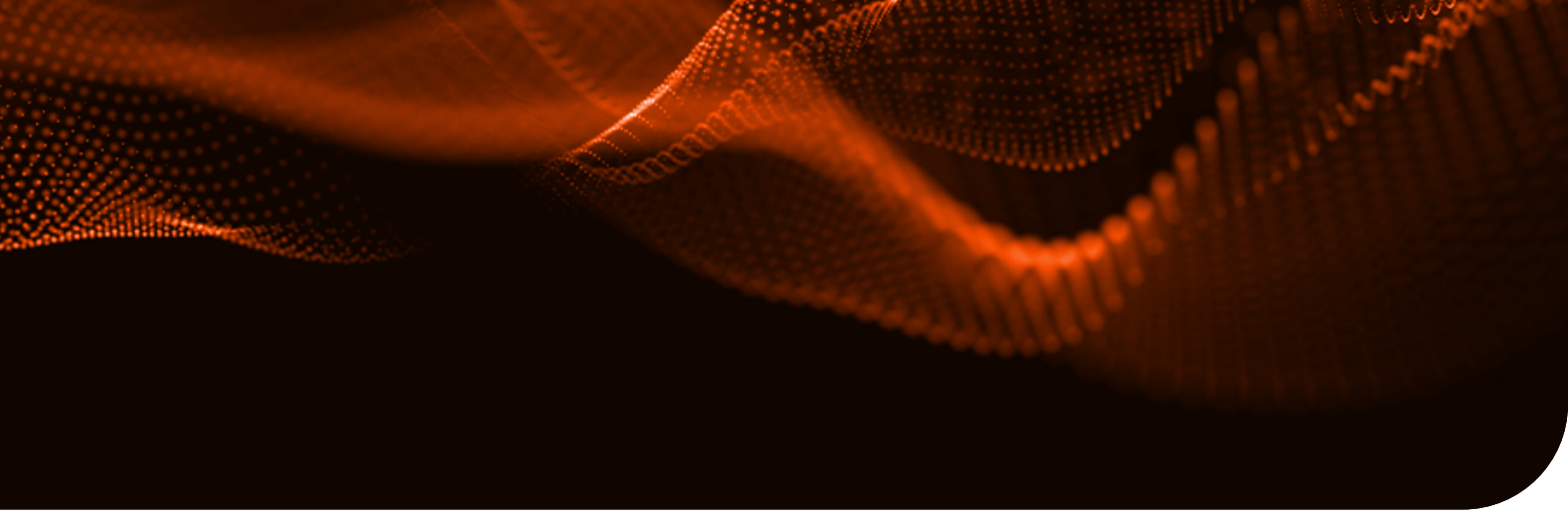
- Comprendre la norme ISO/IEC 27001 et son intégration avec le Système de Management de la Sécurité de l'Information (SMSI).
- Identifier les différentes étapes de la mise en œuvre d'un SMSI.
- Comprendre l'approche basée sur les risques dans la mise en œuvre d'un SMSI.
- Savoir comment réaliser des audits de conformité avec la norme ISO/IEC 27001.
- Évaluer les performances du SMSI et proposer des améliorations.
- Comprendre le rôle du SMSI dans la gestion de la sécurité de l'information et sa contribution à la conformité réglementaire.

Public

- Responsables de la sécurité de l'information et gestionnaires de la sécurité informatique cherchant à renforcer leurs compétences dans la mise en œuvre de la norme ISO/IEC 27001.
- Auditeurs de sécurité évaluant la conformité à la norme ISO/IEC 27001 et cherchant à renforcer leurs compétences dans la mise en œuvre de la norme.
- Architectes de sécurité concevant des architectures de sécurité pour des environnements de sécurité opérationnelle.
- Responsables de la conformité réglementaire devant s'assurer que leur organisation est conforme à la norme ISO/IEC 27001.
- Consultants en sécurité informatique fournissant des conseils en gestion de la sécurité de l'information et en mise en œuvre de la norme ISO/IEC 27001 à leurs clients.

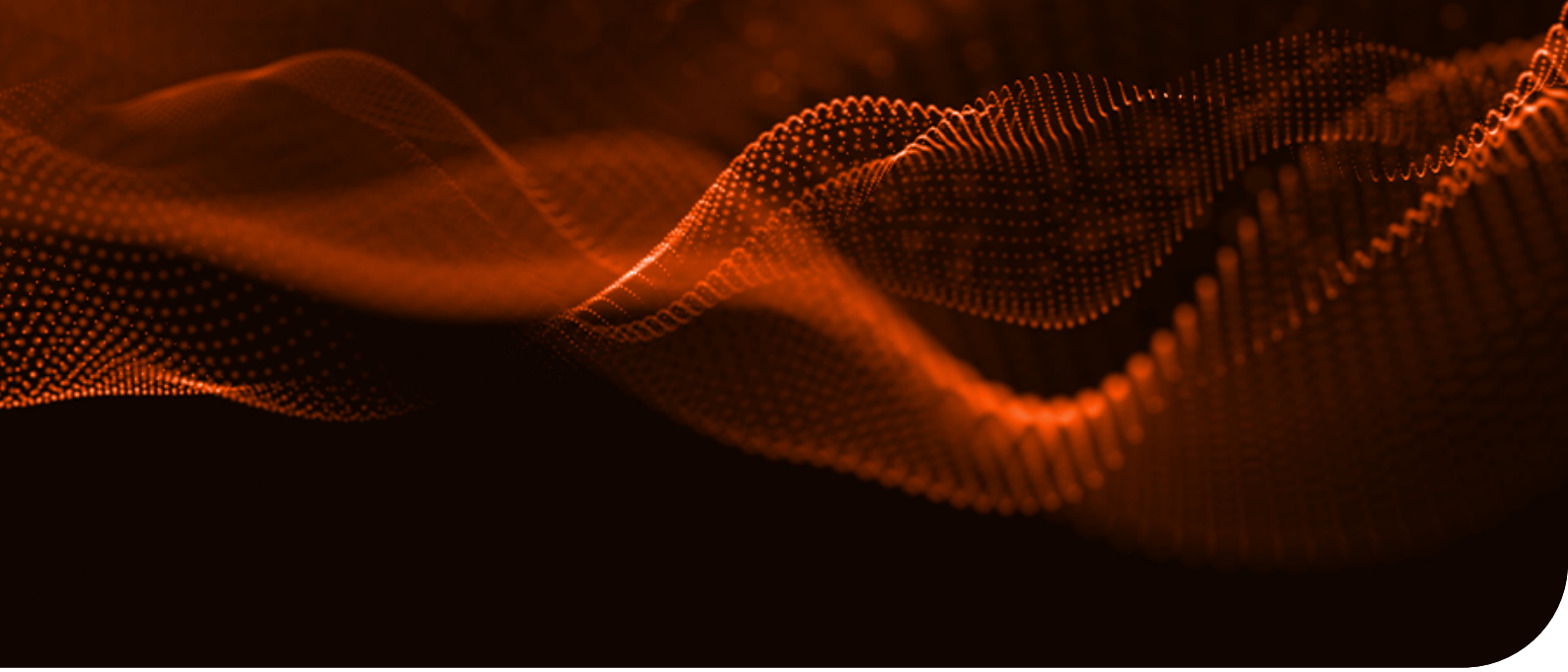
Prérequis

- Connaissance pratique de la gestion de la sécurité de l'information, y compris la gestion des risques, la protection des informations sensibles et la gestion des incidents de sécurité.
- Compréhension de base des concepts de sécurité informatique, tels que la sécurité réseau, la gestion de la sécurité de l'information et les méthodes de test de vulnérabilité.
- Expérience pratique dans un environnement de sécurité opérationnelle.
- Expérience théorique dans l'élaboration de politiques de sécurité, la mise en place de procédures et la formation du personnel aux mesures de sécurité.
- Expérience pratique de la communication avec les parties prenantes internes et externes.

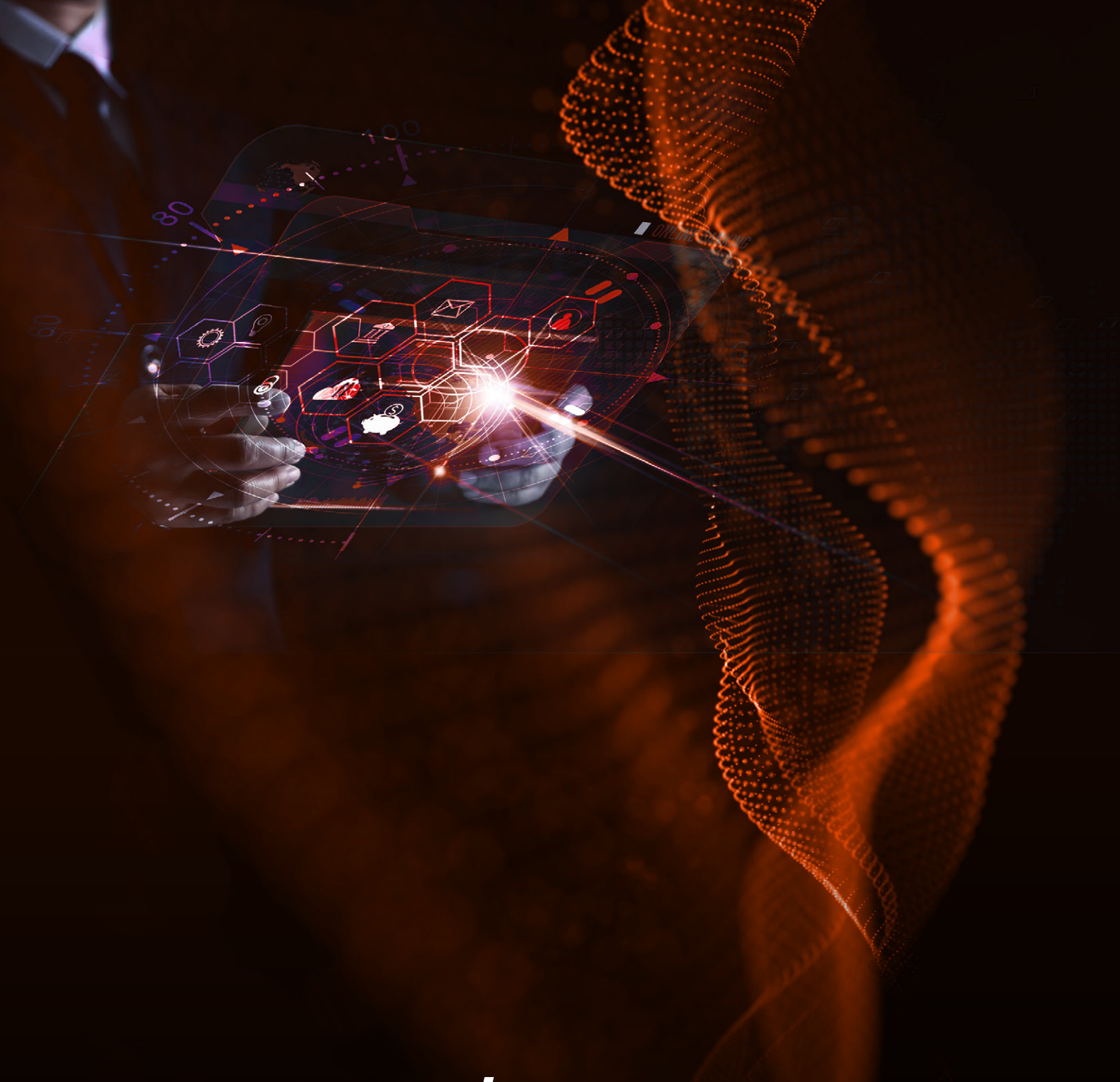


Programme de la formation

Jour 1 matin	**Section 1 - Introduction à la norme ISO/IEC 27001:2022** • Normes : Définition de l'ISO • Présentation de la norme ISO/IEC 27001:2022 • Explication d'un Système de Management de la Sécurité de l'Information (SMSI) • Aperçu des principes d'un système de management intégré • Perfectionnement continu et utilisation d'un modèle PDCA • Vue d'ensemble de la structure normative • Avantages de la norme ISO/IEC 27001:2022 • Relation entre SMSI et stratégie d'entreprise **Section 2 - Domaine d'application de la norme ISO/IEC 27001:2022** • Perspective normative contre approche méthodologique • Distinction entre norme et réglementation • ISO/IEC 27002 : Bonnes pratiques pour le management de la sécurité de l'information • ISO/IEC 27003 : Mise en œuvre d'un SMSI • ISO/IEC 27004 : Indicateurs de performance du SMSI • ISO/IEC 27005 : Évaluation des risques • ISO/IEC 27006 : Organismes d'audit et de certification du SMSI • ISO/IEC 27007 : Audit du SMSI • ISO/IEC 27008 : Audit des mesures de sécurité • ISO/IEC 27035 : Gestion des incidents de sécurité • ISO/IEC 27037 : Preuves numériques • ISO 22301 : Continuité d'activité • **Exercice 1** : Système de management intégré
Jour 1 après-midi	**Section 3 - Planification et séquencement du projet « ISO/IEC 27001 »** • Logique d'implémentation • Organisation d'un SMSI • Erreurs courantes à éviter
Jour 2 matin	**Section 4 - Lancement du projet** • Contextualisation • Exigences associées • Identification des parties prenantes et compréhension de leurs attentes • Exercice 2 : Contexte, Exigences associées, Parties prenantes et leurs attentes/besoins • Analyse des écarts (Gap analysis) • Examen des options disponibles (validation du champ d'application) • Détermination des objectifs de sécurité de l'information • **Exercice** 3 : Analyse des écarts « Gap analysis » et champ d'application



Jour 2 après-midi	**Section 5 - Élaboration de la structure du SMSI** • Structure de gouvernance du SMSI • Leadership de la direction • Élaboration de la structure documentaire • Communication encadrée • Établissement d'une méthode d'évaluation des risques • Identification des actifs vitaux • Exercice 4 : Actifs vitaux • Politique de sécurité • Exercice 5 : PSI - Partie haute • Processus de gestion des incidents de sécurité • Processus de formation et de sensibilisation • Indicateurs de rendement du SMSI • **Exercice 6** : Indicateurs de rendement du SMSI
Jour 3 après-midi	**Section 6 - Gestion des risques du SI** • Identification, analyse et évaluation des risques • Rédaction du plan de gestion des risques • Exercice 7 : Gestion des risques
Jour 4 matin	• Ajustement des mesures de sécurité et formalisation de la déclaration d'applicabilité • **Exercice 8** : Contrôles de la DDA
Jour 4 après-midi	**Section 7 - Audits internes et suivi des actions** • Exigences normatives • Objectifs des audits internes • Planification des audits internes • Suivi des actions • **Exercice 9** : Audits internes
Jour 5 matin et après-midi	**Section 8 - Le processus de certification de la norme ISO/IEC 27001:2022** • Organismes de certification • Non-conformités • Catégories d'audits (initiaux, complémentaires, surveillances, renouvellements) • Préparation à l'audit de certification • Après la certification • **Exercice 10** : Certification



Auditeur ISO/IEC 27001

Le formations d'auditeur ISO/IEC 27001 est conçu pour acquérir les compétences nécessaires pour effectuer des audits d'un Système de Management de la Sécurité de l'Information (SMSI) en utilisant des principes, des méthodologies et des pratiques d'audit généralement acceptés. Grâce à des exercices pratiques, vous aurez une compréhension approfondie des procédures d'audit, ainsi que la capacité de gérer les relations avec les clients, de diriger des équipes d'audit, de superviser les programmes d'audit et de résoudre efficacement les conflits.

Objectifs pédagogiques

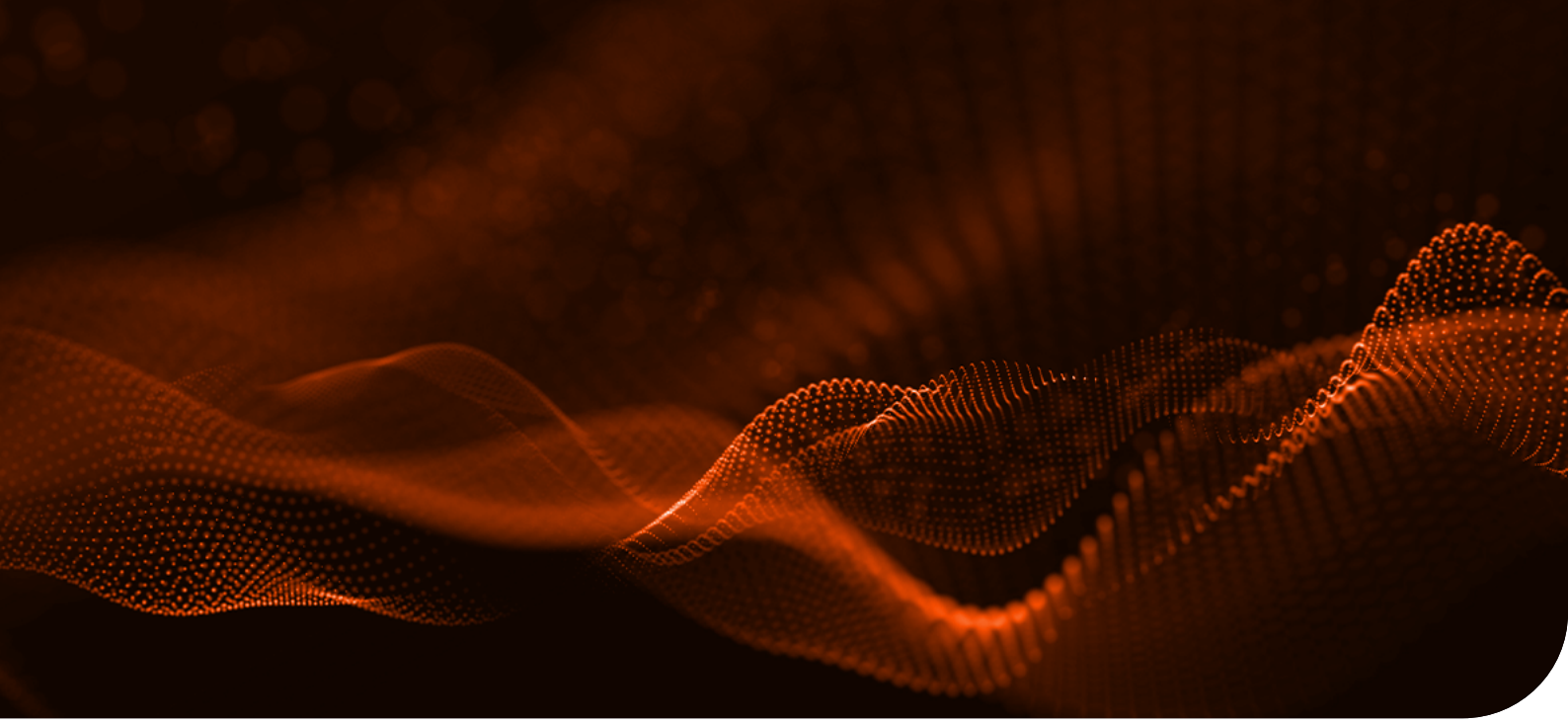
- Acquérir une compréhension approfondie des concepts fondamentaux et des principes sous-tendant un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO/IEC 27001.
- Apprendre à interpréter les exigences de la norme ISO/IEC 27001 en tant qu'auditeur, en fournissant une perspective unique sur la conformité au SMSI.
- Évaluer la conformité au SMSI avec les normes de la norme ISO/IEC 27001, en appliquant des principes et des concepts fondamentaux d'audit.
- Maîtriser les compétences nécessaires pour planifier, exécuter et conclure un audit de conformité à la norme ISO/IEC 27001, en respectant les directives de la norme ISO/IEC 17021-1, les recommandations de la norme ISO 19011 et les meilleures pratiques d'audit établies.
- Superviser efficacement un programme d'audit ISO/IEC 27001 pour assurer une conformité continue et une gestion de la sécurité.

Public

- Individus ayant pour objectif de diriger et d'effectuer des audits des systèmes de gestion de la sécurité de l'information (SMSI).
- Managers ou consultants visant l'excellence dans le processus d'audit des systèmes de gestion de la sécurité de l'information.
- Personnes responsables du suivi de la conformité d'une organisation aux règles du SMSI.
- Experts techniques se préparant à des audits de systèmes de gestion de la sécurité de l'information.
- Consultants expérimentés dans l'administration de la sécurité de l'information.

Prérequis

- Une compréhension fondamentale de la norme ISO/IEC 27001 et une connaissance approfondie des principes d'audit.



Programme de la formation

Jour 1	Introduction au système de management de la sécurité de l'information (SMSI) et à la norme ISO/IEC 27001 : **Section 1 : Concepts et principes fondamentaux de l'audit** **Section 2 : L'impact des tendances et de la technologie dans l'audit** **Section 3 : Audit fondé sur les preuves** **Section 4 : Audit basé sur les risques** **Section 5 : Lancement du processus d'audit** **Section 6 : Audit de la première étape**
Jour 2	Principes de l'audit, préparation et lancement d'un audit : • Atelier 1 : Scénarios stratégiques • Atelier 2 : Scénarios opérationnels • Atelier 3 : Traitement des risques **Section 7 : Clôture des formations**
Jour 3	Activités d'audit sur site • Préparation à l'étape 2 de l'audit • Étape 2 de l'audit • Communication durant l'audit • Procédures d'audit • Création de plans de test d'audit
Jour 4	Clôture de l'audit • Rédaction des constatations d'audit et des rapports de non-conformité • Documentation d'audit et revue de qualité • Clôture de l'audit • Évaluation des plans d'action par l'auditeur • Après l'audit initial • Management d'un programme d'audit interne • Clôture de la formation
Jour 5	Examen du certificat

ISO/IEC 27005:2022

La formation ISO/IEC 27005:2022 est conçue pour les professionnels ayant de l'expérience dans la sécurité de l'information et ayant précédemment travaillé avec la norme ISO/ IEC 27001. Les participants apprendront comment utiliser la norme ISO/IEC 27005 comme un outil de gestion des risques liés à la sécurité de l'information et comment appliquer les méthodes EBIOS dans leur travail quotidien. Au cours de la formation, les participants apprendront à identifier les actifs et les menaces, à évaluer les risques, à déterminer les mesures de sécurité et à élaborer un plan de traitement des risques. La réussite de cet examen permettra aux participants de démontrer leur compétence en matière de gestion des risques liés à la sécurité de l'information et de renforcer leur CV.

Objectifs pédagogiques

- Comprendre les concepts de base de la sécurité de l'information, les normes ISO/IEC 27001 et ISO/IEC 27005.
- Savoir identifier les actifs et les menaces liés à la sécurité de l'information et évaluer les risques associés.
- Connaître les différentes méthodes de gestion des risques et savoir les appliquer dans la pratique.
- Savoir établir un plan de traitement des risques de sécurité de l'information, y compris la détermination des mesures de sécurité appropriées.
- Acquérir les compétences pour mener une évaluation des risques de sécurité de l'information de manière efficace et efficiente.
- Savoir communiquer les résultats de l'évaluation des risques aux parties prenantes concernées.
- Être capable de passer l'examen de certification ISO/IEC 27005 avec succès.
- Appliquer les connaissances et les compétences acquises dans leur travail quotidien pour renforcer la sécurité de l'information au sein de leur organisation.

Public

- Professionnels de la sécurité de l'information travaillant dans des organisations de toutes tailles, y compris les gouvernements, les entreprises, les organisations à but non lucratif et les organisations de santé.
- Consultants en sécurité de l'information cherchant à renforcer leurs compétences en gestion des risques liés à la sécurité de l'information et à améliorer leur employabilité.
- Auditeurs de sécurité cherchant à renforcer leurs compétences en évaluation des risques liés à la sécurité de l'information et à améliorer leur employabilité.
- Responsables de la sécurité de l'information cherchant à renforcer leurs compétences en gestion des risques liés à la sécurité de l'information et à améliorer leur employabilité.
- Débutants dans le domaine de la sécurité de l'information cherchant à se familiariser avec les méthodes et les outils de gestion des risques liés à la sécurité de l'information.

Prérequis

- Connaissances générales en sécurité des systèmes d'information.

Programme de la formation

Jour 1 Matin	MATIN (ISO/IEC 27005:2022) **Section 1 – Fondamentaux de la gestion des risques** • Définition du risque (dictionnaire, ISO/IEC 27005:2022, EBIOS Risk Manager) • Composantes d'un risque (actif, vulnérabilité, menace, scénario, calcul du risque) • Interaction entre les composantes d'un risque • Exercice 1 : composer un risque • Étude des risques – méthodes et normes • Norme vs méthodologie • Rappel d'une norme ISO/IEC • Lien entre les normes ISO 27001 et 27005 • Gouvernance, risque, ISO/IEC 27005:2022, lien avec la norme ISO/IEC 27001 • Développer un programme de gestion des risques **Section 2 – Présentation de la norme ISO/IEC 27005:2022** • Présentation de la norme ISO/IEC 27005:2022 (clauses) • Structure de la norme ISO/IEC 27005:2022 • Cycle de la norme • PDCA (roue de Deming) • Approche processus • Évolution ISO/IEC 27005:2011 vs 2022 **Section 3 – La phase de contexte par ISO/IEC 27005:2022** • Définition d'une organisation, appétit du risque • Identification des exigences de base des parties prenantes • Exercice 2 : établir le contexte d'une organisation • Identifier les objectifs, cycle d'itération • Considérer la gestion des risques dans une organisation • Critères d'acceptation des risques • Critère d'évaluation des risques • Critères pour la conséquence • Critères pour la probabilité • Critères de détermination du niveau de risque • Exercice 3 : établir les critères d'une organisation
Jour 1 Après-Midi	APRÈS-MIDI (ISO/IEC 27005:2022) **Section 4 – Cycle d'analyse** • Définition du cycle d'analyse • Approche par événements / par actif **Section 5 – Phase d'identification des risques** • Identification des actifs • Identification des vulnérabilités • Identification des menaces • Identification des conséquences • Exercice 4 : identifier les actifs, les événements et les porteurs de risque • Identifier les sources de risques et les objectifs visés • Exercice 5 : identifier les sources de risques et les objectifs visés • Identification des parties prenantes • Exercice 6 : identifier les parties prenantes et les chemins d'attaque • Valeur et liens entre les actifs • Exercice 7 : identifier les actifs supports • Identifier les scénarios opérationnels • Exercice 8 : identifier les scénarios opérationnels

Programme de la formation

Jour 2 Matin	MATIN (ISO/IEC 27005:2022) **Section 6 – Phase d'estimation et d'évaluation des risques** • Approche qualitative vs quantitative • Les différentes méthodes de calcul des risques • Estimer le niveau de sévérité de la conséquence • Exercice 9 : estimer la sévérité de la conséquence • Estimer la probabilité d'occurrence • Exercice 10 : estimer la probabilité d'occurrence • Déterminer le niveau de risque • Exercice 11 : déterminer le niveau de risque • Comparer le résultat de l'estimation des risques avec les critères de risque • Prioriser les risques • Exercice 12 : prioriser les risques • Établir un plan de traitement des risques
Jour 2 Après-Midi	APRÈS-MIDI (ISO/IEC 27005:2022) **Section 7 – Phase de traitement et d'acceptation des risques** • Les différentes options de traitement du risque • Déterminer les contrôles nécessaires à la mise en œuvre des options de traitement • Comparer les contrôles avec ceux de l'annexe A ISO/IEC 27001 • Exercice 13 : comparer les contrôles avec l'annexe A de la norme ISO/IEC"27001 • Produire une déclaration d'applicabilité (DDA) • Mettre en place un plan de traitement des risques • Exercice 14 : mettre en place un plan de traitement des risques • Notions de risques bruts, nets, résiduels • Évaluer le risque résiduel • Approuver par les porteurs de risques
Jour 3 Après-Midi	MATIN (ISO/IEC 27005:2022) **Section 8 – Communication et surveillance** • Établir un plan de communication • Mettre en place les indicateurs pour une surveillance optimale dans un modèle PDCA
Jour 3 Après-Midi	**APRÈS-MIDI (ISO/IEC 27005:2022)** **Section 9 – Alignement au SMSI** • Contexte de l'organisation • Leadership et engagement • Phase de communication • Créer une matrice de communication • Exercice 15 : créer une matrice de communication • Communiquer les risques résiduels au PCA et la réponse à incident • Phase de documentation • Informations documentées sur les processus • Informations documentées sur les résultats • Surveillance et révision des facteurs influençant les risques • Exemple du SFDT (source-function-destination-trigger) • Exercice 16 : créer un scénario de surveillance • Action corrective • Amélioration continue

Manager du DevSecOps

La formation de Manager du DevSecOps proposé par l'ICDE est une formation pratique destinée aux professionnels de la sécurité des systèmes d'information souhaitant acquérir des compétences en matière de gestion de projets de développement sécurisé, en adoptant les meilleures pratiques DevSecOps. La formation couvre un large éventail de sujets, notamment les normes et les méthodologies de développement, l'analyse des risques appropriée à DevOps, la gestion des incidents de sécurité. Cette formation convient aux responsables de la sécurité qui souhaitent renforcer leurs compétences en matière de DevSecOps.

Objectifs pédagogiques

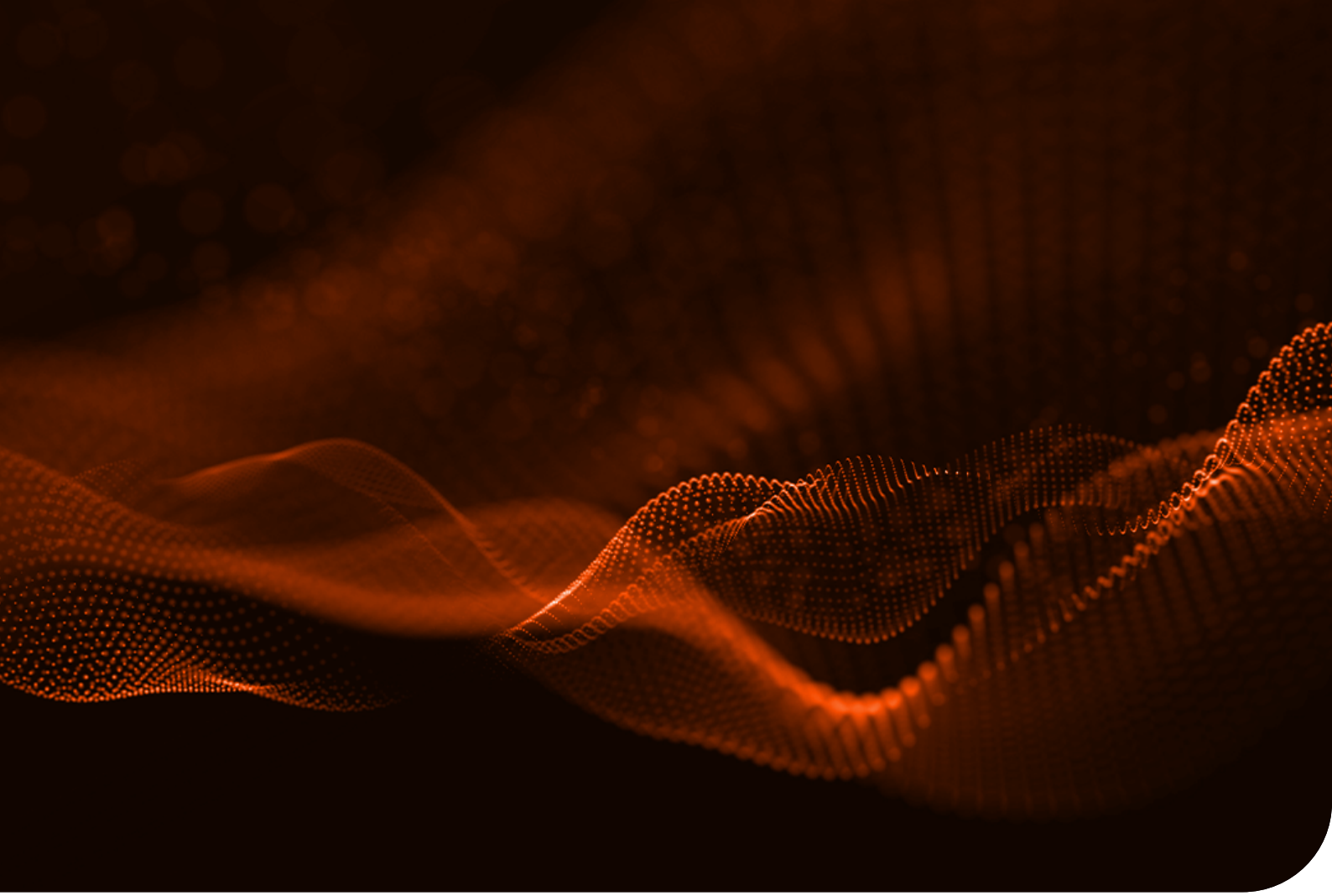
- Comprendre les concepts de DevOps et de DevSecOps ainsi que leurs avantages et limites.
- Comprendre l'impact de la sécurité sur les pipelines DevOps et comment intégrer la sécurité dès le début du cycle de développement logiciel.
- Comprendre les différents outils, processus et techniques utilisés en DevSecOps.
- Savoir comment mettre en place et gérer des processus DevSecOps efficaces pour les équipes de développement.
- Comprendre la conformité DevSecOps, la gouvernance et les pratiques de conformité réglementaire.
- Communiquer et collaborer efficacement avec les équipes de développement, de sécurité et de gestion pour garantir une approche cohérente de la sécurité dans toute l'organisation.

Public

- Professionnels cherchant à renforcer l'intégration de la sécurité dans DevOps. T Analystes, spécialistes et architectes en transition vers des rôles DevSecOps. T Praticiens visant des postes de direction en sécurité DevOps.
- Architectes et leaders technologiques axés sur des systèmes sécurisés et évolutifs avec DevSecOps.
- Gestionnaires axés sur l'évaluation des risques et l'atténuation en matière de développement et de déploiement.
- Développeurs seniors axés sur la programmation sécurisée et le leadership dans le développement axé sur la sécurité.

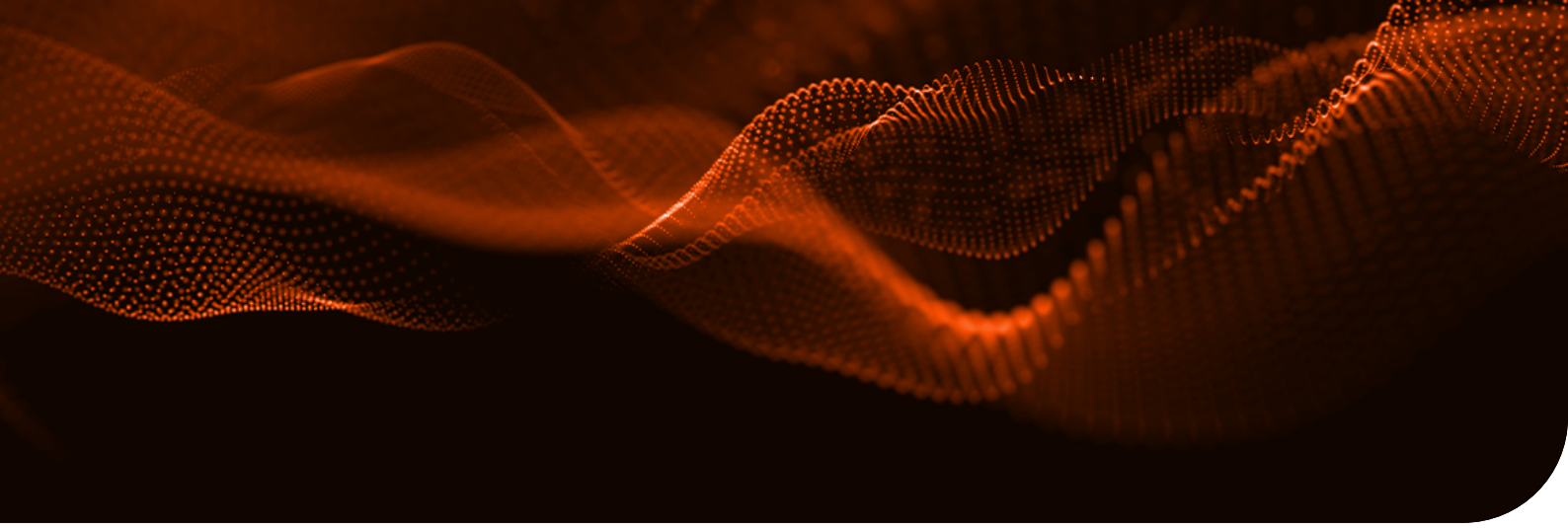
Prérequis

- Connaissances généralistes en sécurité de l'information, gestion des risques, conformité SSI.



Programme de la formation

Jour 1 matin	**Section 1 – Les enjeux du DevSecOps pour les organisations** • Comprendre le DevOps et ses enjeux • Différences entre DevOps et modèle classique • Les bénéfices du DevSecOps • La philosophie de l'agile **Section 2 – Les problèmes de compréhension du DevSecOps par les managers de la SSI** • Le modèle de sécurité DevSecOps • L'intégration du DevSecOps dans un SMSI • Les approches de défense en profondeur **Section 3 – Les problèmes de compréhension du DevSecOps par les techniciens de la SSI** • La perception de la sécurité de l'information comme une contrainte • Donner un sens à la sécurité de l'information
Jour 1 après-midi	**Section 4 – Intégrer le DevSecOps dans la gouvernance d'une organisation** • Les missions principales d'un manager en sécurité de l'information • Approche par les risques • Conformité avec le socle normatif • La mise en condition de sécurité (MCS) **Section 5 – Quel modèle, référentiel choisir pour le DevSecOps** • Présentation des différents modèles et référentiels • Microsoft SDL • OWASP SAMM • BSIMM • OWASP ASVS



Programme de la formation

Jour 2	**Section 6 – Phase 1 : Préparer un SDLC adapté** • Activité 1.1 : budgétiser un SDLC • Activité 1.2 : Identifier une équipe pour le SDLC **Section 7 – Phase 2 : Former l'équipe au DevSecOps** • Activité 2.1 : Créer une formation « tous les profils » • Activité 2.2 : Créer une formation « technique » **Section 8 – Phase 3, Analyser les risques** • Fonctionnement d'une analyse de risque • Activité 3.1 : Obtenir les besoins de sécurité et les scénarios graves • STRIDE et DIC(T) • Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege • Adapter les méthodes d'analyses de risques classiques au DevSecOps avec le Bugs bar • Activité 3.2 : Modéliser les menaces • Qu'est-ce que la modélisation des menaces (Threat modeling) • Créer un diagramme • Identifier les menaces • Utilisation de Microsoft Threat modeling tools • Obtenir la vraisemblance des risques avec la modélisation des menaces • Construire la matrice des risques via les objectifs de sécurité et la vraisemblance des menaces • Activité 3.3 : Calcul des risques • Activité 3.4 : Choisir une option de traitement • Activité 3.5 : Créer un plan de traitement des risques • Ne pas oublier les données à caractère personnel **Section 9 – Phase 4, Mise en conformité et intégration d'outils** • Aller plus loin avec l'implémentation d'un référentiel de conformité adapté au DevSecOps • Activité 4.1 : Identifier les référentiels, normes, lois • Activité 4.2 : Appliquer l'analyse des écarts • L'OWASP AVSV • Activité 4.3 : Intégration d'un SAST • Activité 4.4 : Intégration d'un DAST **Section 10 – Phase 5, Auditer et améliorer la sécurité** • Activité 5.1 : Planifier un test d'intrusion • Activité 5.2 : Adapter le système de suivi des bugs du SDLC à STRIDE • Activité 5.3 : Préparer un tableau de bord • Activité 5.4 : Préparer un plan de réponse à incident • Activité 5.5 : Aller plus loin avec un modèle de maturité • Activité 5.6 : Veille SSI

ICDE

Contactez-nous

L'équipe est prête à vous assister pour toutes les questions que vous pourriez avoir concernant les formations, les certifications ou les laboratoires. Vous pouvez rapidement prendre contact via le formulaire de contact ci-dessous, par e-mail ou directement par téléphone.

Lieu

229 rue Saint-Honoré 75001
Paris

E-mail & Web

contact@icde.eu
www.icde.eu