|  |  |
| --- | --- |
| **Bloc de compétences 3 Semestre 2** | |
| **Finalité métier :** Le métier de la cybersécurité consiste à répondre aux besoins de sécurité des services informatiques d’une organisation notamment au regard du développement des menaces et attaques en provenance d’internet et des risques liés aux usages numériques.  Les contextes de travail, ouverts et évolutifs, nécessitent de mener une veille informationnelle et technologique et de prendre en compte leurs aspects humains, technologiques, organisationnels, économiques et juridiques.  Le métier implique de respecter la réglementation, les méthodes, les normes et standards qui prévalent dans la législation nationale et internationale ainsi que dans les recommandations des organismes gouvernementaux et professionnels. | **Contexte professionnel** : Vous travaillez pour le compte d’une société de conseil en technologies spécialisée dans la cybersécurité. Rattaché (e) au responsable de la sécurité des systèmes d’information (RSSI) de l’équipe sécurité, vous intervenez auprès des différents clients.  Vous serez chargée ou chargé de :   * Protéger les données à caractère personnel de vos clients * Préserver leur identité numérique * Sécuriser les équipements et les usages des utilisateurs * Veiller à la disponibilité, l’intégrité et la confidentialité des services informatiques |

|  |  |
| --- | --- |
| **3.4. Garantir la disponibilité, l’intégrité et la confidentialité des services informatiques et des données de l’organisation face à des cyberattaques Semestre 2** | |
| **Votre mission :** Vous participez aux activités d’analyse, de veille technologique des risques et de protection des données sur les deux sites informatiques de l’entreprise. Vous mettez en place des processus de sécurisation de certaines applications et infrastructures afin d’anticiper les risques, mettre en échec les tentatives de piratage et garantir la fiabilité et la disponibilité des données des services. Les données à caractère personnel sont manipulées et sécurisées en tenant compte des exigences du règlement général sur la protection des données (RGPD). | **Contexte professionnel** : Vous êtes embauché en tant que technicien supérieur en informatique pour renforcer le service cybersécurité de la Direction des Systèmes d’Information (DSI) d’une PME située à Paris. Une partie du service informatique est basée sur Toulouse. Vous assurez des activités de support technique et fonctionnel dans la sécurisation applicative et d’infrastructure afin de protéger le système d’information et les données, y compris celles à caractère personnel. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.4 A 2** | **Encadrer le développement du site web de l’entreprise pour être conforme au respect de la vie privée des utilisateurs finaux imposé par le RGPD.** | | | | | |
| Durée totale en heures du scénario pour la séquence  4 h | L’audit du site internet de l’entreprise, développé à l’aide d’un CMS, a révélé certains manquements aux obligations légales du RGPD, notamment en ce qui concerne le recueil du consentement des personnes au traitement de leurs données à caractère personnel (DCP). Votre travail consiste à participer au projet de conformité du site en ciblant la mise à jour des formulaires qui recueillent ces données. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Organiser la collecte et la conservation des preuves numériques. * Appliquer les procédures garantissant le respect des obligations légales. | Savoirs technologiques   * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.   Savoirs économiques, juridiques et managériaux   * Droit de la preuve électronique. | | * Les preuves numériques sont conservées de manière sécurisée et dans le respect de la législation. * Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées. | | Prérequis :  B1.4. Travailler en mode projet  B3.1. Protéger les données à caractère personnel.  Notion de preuve électronique et droit de la preuve électronique (CEJMA)  Transversalités :  B1.3. Développer la présence en ligne de l’organisation. |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 30 min | Sous la responsabilité du chef de projet, les différentes tâches seront planifiées et renseignées dans un outil collaboratif.  Votre travail consiste à mettre à jour la vue du formulaire d’inscription au site pour recueillir le consentement de la personne en utilisant le principe de confirmation du consentement par courrier électronique (*double opt-in)* et permettre son retrait si la personne le souhaite. Le principe de minimisation des données sera appliqué :   1. Supprimer les champs correspondants à des données facultatives. 2. Ajouter les éléments nécessaires au recueil du consentement de la personne au traitement (case à cocher et raison de la collecte des données). 3. Ajouter les éléments permettant aux utilisateurs de retirer leur consentement ou d’accéder à leurs données. 4. Tester l’affichage du formulaire. | | * Le site web de l’entreprise (*avec un formulaire d’inscription qui recueille des informations non pertinentes pour le traitement correspondant et qui ne contient pas de demande de consentement)*. * L’environnement technique de tests : serveur web et de base de données (*machines virtuelles ou environnement local)*. * Base de données du site web version 1. * Environnement de développement. | | * La vue du formulaire d’inscription au site est mise à jour et garantit le principe de minimisation et de collecte du consentement. * Le tableau de bord de l’outil collaboratif est mis à jour. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1 h 30 | Votre travail consiste à développer la partie traitement du formulaire d’inscription au site conformément au RGPD :   1. Traiter la validation du formulaire. 2. Conserver la preuve du consentement. 3. Mettre en place et tester la procédure permettant à la personne d’accéder à tout moment à la « preuve du consentement ». 4. Mettre en place et tester la procédure de retrait du consentement demandé par la personne. | | * Fiche de savoirs juridiques liés au consentement. * Fiches d’aide à la réalisation de la tâche (*liens vers des tutoriels, propositions de plugins à utiliser pour répondre au besoin, exemples de scripts PHP …).* * Le site web de l’entreprise mis à jour (*Tâche 1)* * Base de données du site web version 2. | | * Le formulaire d’inscription est mis à jour et garantit l’obligation du consentement avant enregistrement des données. * Les données collectées sont enregistrées dans la base de données. * La procédure de collecte du consentement et de la conservation de sa preuve est opérationnelle. * La base de données est mise à jour. * Le tableau de bord de l’outil collaboratif est mis à jour. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1 h 30 | Votre travail consiste à mettre à jour votre site pour donner la possibilité à vos utilisateurs d’appliquer leur droit d’accès, de modification ou de suppression de leurs données.   1. Créer une page spécifique dédiée contenant un formulaire de demande précise. 2. Tester chaque fonctionnalité. 3. Inclure le lien vers cette page dans tous les endroits nécessaires (pied de page, formulaire…) | | * Fiches d’aide à la réalisation de la tâche (*liens vers des tutoriels, propositions d’extensions à mettre en place pour répondre au besoin, exemples de scripts PHP …).* * Le site web de l’entreprise mis à jour (à l’issue de la séance 2). | | * Le site web est mis à jour dans l’environnement de test. * Les procédures garantissant le respect des droits des personnes sont opérationnelles. * La base de données est mise à jour. * Un test d’extraction des données d’un utilisateur dans un format lisible est effectué. * Le tableau de bord de l’outil collaboratif est mis à jour. | |
| **Séance 4** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 30 min | Le site web utilise des cookies.  Votre travail consiste à créer un bandeau de consentement des cookies pour être en conformité avec le RGPD. | | * Fiches d’aide à la réalisation de la tâche (*liens vers des tutoriels, propositions d’extensions à mettre en place pour répondre au besoin, exemples de scripts PHP …).* * Le site web de l’entreprise mis à jour (*séance 3)* | | * Le site web est mis à jour dans l’environnement de test. * La base de données est mise à jour dans l’environnement de test. * La preuve du consentement est collectée. * L’archive du code (site et base de données) est transmise à l’équipe de validation. * Le tableau de bord de l’outil collaboratif est mis à jour. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.4 B2** | **Mettre en place les mesures de sécurité préventives contribuant à l’intégrité et à la confidentialité des données du site Web de l’entreprise Semestre 2** | | | | | |
| 10 h | Vous avez mis en place une veille technologique sur les vulnérabilités des applications web. Une absence ou une mauvaise gestion de sécurisation du site Web constitue une menace importante à votre système d’information.  Les axes de sécurité des données de cette séquence contribuent aux objectifs de confidentialité et d’intégrité des données du site et portent à la fois sur le code applicatif, les échanges sécurisés des données entre le client et le serveur ainsi que sur les authentifications des utilisateurs sur le site. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Caractériser les risques liés à l’utilisation malveillante d’un service informatique. * Identifier les obligations légales qui s’imposent en matière d’archivage et de protection des données de l’organisation. * Recenser les conséquences d’une perte de disponibilité, d’intégrité ou de confidentialité | Savoirs technologiques   * Typologie des risques et leurs impacts. * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. * Sécurité des applications *Web* : risques, menaces et protocoles. * Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.   Savoirs économiques, juridiques et managériaux   * Les risques des cyberattaques pour l’organisation : économique, juridique, atteinte à l’identité de l’entreprise. * Les organisations de lutte contre la cybercriminalité. | | * Les risques associés à l’utilisation malveillante d’un service informatique sont caractérisés. * Les conséquences des actes malveillants sur un service informatique sont identifiées. * Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées : * l'authentification et la confidentialité des échanges sont vérifiées ; * les vulnérabilités connues sont contrôlées. | | Prérequis :  Séquence 3.2 B1  Transversalités :  Séquence 3.2. A2  Bloc 3 - 3.3 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2 h 30 | Vous participez, avec votre équipe, à un audit de sécurité du site web de l’entreprise.   1. Prendre connaissance des failles de sécurité les plus critiques publiées par OWASP (Open Web Application Security Project). 2. Tester les injections de données externes qui peuvent compromettre le contenu du site ou de la base de données (*injection SQL, failles JavaScript, redirections d’URL, inclusions de fichiers*). 3. Etablir le rapport des vulnérabilités détectées sur le site et de leur impact sur votre entreprise. | | *Note aux auteurs : cette séance peut être exploitée soit pour découvrir les vulnérabilités les plus connues des sites web, soit pour mettre en application les bonnes pratiques et les mesures applicatives pour sécuriser le site.*   * Fiches de savoirs sur les menaces liées aux applications web. * Fiche des savoirs juridiques sur les risques des cyberattaques. * CyberEdu Sensibilisation et initiation à la cybersécurité - module 3 : les aspects réseau et applicatifs. * Fiche d’aide aux tests de sécurité du site web. * Code du site web (*présentant les failles de sécurité étudiées*). * Failles OWASP. * Rapport des vulnérabilités pré-rempli. | | * Le rapport des vulnérabilités détectées sur le site web est rédigé. * Les risques afférents aux vulnérabilités détectées sur le site web sont évalués. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 4 h 30 | Afin d’améliorer l’intégrité des données du site web, vous participez à la correction des vulnérabilités détectées en vous appuyant sur le document des “recommandations pour la sécurisation des sites web” rédigé par l’ANSSI.   1. Appliquer les bonnes pratiques de programmation. 2. Corriger quelques vulnérabilités liées aux injections des données en provenance du client (*requêtes paramétrées, filtrage et typage des données, plugin de sécurité, formats de saisie minimisant les données collectées, liste blanche, redirections statiques, vérifications d’URL avec des expressions régulières, recours aux index dans une liste blanche, contrôles stricts de la forme de la donnée externe…*). 3. Tester la correction des vulnérabilités détectées. 4. Mettre à jour le rapport des vulnérabilités. | | * CyberEdu Sensibilisation et initiation à la cybersécurité - module 3 : les aspects réseau et applicatifs. * Fiches de savoirs sur les bonnes pratiques et les mesures de protection des données pour garantir leur confidentialité, leur disponibilité et leur intégrité. * Fiches d’aide à la protection de l’intégrité des données du site web. * Rapport des vulnérabilités du site mis à jour avec la planification des corrections des vulnérabilités détectées. | | * Les vulnérabilités sont corrigées. * L’application web est mise à jour. * Le rapport des vulnérabilités est mis à jour. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2 h 30 | Le RSSI sensibilise l’équipe de cyber-sécurité sur les principales menaces identifiées par la CNIL au cours du cycle de vie d’un mot de passe utilisateur et vous demande de prendre les mesures nécessaires pour éviter ces risques.   1. Renforcer la politique de gestion des mots de passe des utilisateurs qui s’inscrivent au site web de l’entreprise en respectant les exigences de la CNIL (*limiter le nombre de tentatives d’échec de connexion, utiliser les techniques de type CAPTCHA - Completely Automated Public Turing test to tell Computers and Human Apart -, mettre des contraintes sur les mots de passe, stocker les mots de passe chiffrés à l’aide d’un algorithme de hachage irréversible réputé fort ou d’une librairie ou d’une extension éprouvée*…). 2. Prévoir la gestion du renouvellement du mot de passe périodique et sur demande. 3. Tester les nouvelles fonctionnalités. | | * Ressources CNIL : <https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>.   <https://www.cnil.fr/fr/securiser-vos-sites-web-vos-applications-et-vos-serveurs>   * Failles OWASP (attaque par force brute). * Mooc SecNumEdu de l’ANSSI : Chapitre 2 – Sécurité de l’authentification, unité 5 - Notions de cryptographie. | | * La politique de gestion des mots de passe des utilisateurs du site est mise en place et est opérationnelle. * Les mots de passe sont stockés de manière chiffrée dans la base de données. * La procédure de demande de renouvellement de mot de passe est opérationnelle. * La procédure de renouvellement périodique est opérationnelle. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 30 min | Les communications entre le serveur web et le client s’effectuent en utilisant un canal sécurisé afin de garantir la confidentialité, l’authenticité et l’intégrité des échanges à travers des réseaux non sûrs.   1. Vérifier l’authenticité du certificat et donc du serveur TLS (Transport Layer Security) depuis un poste client (identité enregistrée dans le certificat identique à celle de l’entreprise, certificat en cours de validité, non révoqué, signature correcte). 2. Exporter le certificat dans le format par défaut. 3. Réaliser une analyse de trames lors d’un échange de mot de passe entre le client et le serveur web pour vérifier la confidentialité des informations transmises et repérer les combinaisons cryptographiques échangées entre le client et le serveur. | | * Fiches de savoirs sur le protocole TLS. * Paramètres d’authentification d’un utilisateur de test. * Machine virtuelle du serveur Apache (*contenant l’ensemble des certificats et la clé privée*). | | * Le certificat est importé. * Une capture de l’analyse de trames avec repérage des échanges cryptographiques est générée. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.4 C2** | **Sécuriser l’infrastructure de l’entreprise Semestre 2** | | | | | |
| 5 h | Votre travail consiste à mener une veille technologique efficace des menaces et des vulnérabilités des systèmes d’information. Cette veille vous permet de mettre en œuvre des mesures préventives pour garantir la sécurité du système d’information et la disponibilité des serveurs et des données. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Caractériser les risques liés à l’utilisation malveillante d’un service informatique * Recenser les conséquences d’une perte de disponibilité, d’intégrité ou de confidentialité * Identifier les obligations légales qui s’imposent en matière d’archivage et de protection des données de l’organisation * Appliquer les procédures garantissant le respect des obligations légales | Savoirs technologiques   * Typologie des risques et leurs impacts. * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. * Authentification, privilèges et habilitations des utilisateurs : principes et techniques. * Gestion des droits d’accès aux données : principes et techniques. * Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique. * Chiffrement, authentification et preuve : principes et techniques. * Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.   Savoirs économiques, juridiques et managériaux   * Les risques des cyberattaques pour l’organisation : économique, juridique, atteinte à l’identité de l’entreprise. * Les organisations de lutte contre la cybercriminalité. | | * Les conséquences des actes malveillants sur un service informatique sont identifiées. * Les obligations légales en matière d’archivage et de protection des données sont identifiées et respectées. * Les preuves numériques sont conservées de manière sécurisée et dans le respect de la législation. * Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées : * un schéma présentant la segmentation du réseau est disponible ; * les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ; * l'authentification et la confidentialité des échanges sont vérifiées ; * la sécurité de l'administration est prise en compte ; * les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ; * les accès aux données sont contrôlés à chaque étape d’une transaction ; * les systèmes et les applications sont actualisés en fonction des alertes de sécurité ; * les vulnérabilités connues sont contrôlées. | | Prérequis :  Bloc 3 - 3.2 B1 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1 h 30 | L’infrastructure du réseau de votre entreprise a été mise à jour avec différents éléments de sécurisation. Le RSSI vous demande de vérifier si la nouvelle infrastructure répond à tous les objectifs de sécurité souhaités.   1. Etudier le schéma réseau de l’entreprise. 2. Vérifier les éléments de sécurisation. 3. Vérifier et compléter l’adressage IP. 4. Rédiger un document indiquant le rôle de chaque serveur et pour les éléments de sécurité, l’objectif de sécurisation correspondant ainsi que les protocoles concernés. Pour les objectifs non couverts, indiquer les pistes et/ou les éléments nécessaires pour les atteindre. | | * La malette CyberEdu - Sensibilisation et initiation à la cybersécurité - module 3 : les aspects réseau et applicatifs. * Schéma réseau de l’entreprise (*et dans l’idéal l’infrastructure correspondante, y compris un VPN reliant le service informatique de Paris et de Toulouse)*. * Cahier des charges listant les objectifs de sécurité de l’infrastructure réseau liés à la sécurité des données (confidentialité, intégrité, disponibilité et preuve). | | * Le schéma réseau est mis à jour. * Le document de synthèse des éléments d’infrastructure et de leurs rôles ainsi que les protocoles mis en œuvre est rédigé. * L’inventaire des objectifs de sécurité non atteints et les éléments nécessaires pour y parvenir est réalisé (notamment la *redondance d’éléments matériels sur les serveurs tels que : redondance d’alimentation électrique, de cartes réseaux, onduleur… pour assurer la disponibilité des données et des services)*. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1 h | Afin de sécuriser votre infrastructure, vous mettez en place les actions suivantes :   1. Mettre en place une veille (automatisée ou non) sur les alertes de vulnérabilités (*en vous inscrivant par exemple au bulletin CERT-FR*). 2. Proposer des outils de détection des vulnérabilités à votre RSSI. 3. Restreindre les accès logiques à vos serveurs en ouvrant uniquement les ports nécessaires. 4. Automatiser l’installation des mises à jour critiques. | | * Machines virtuelles de l’infrastructure (*web, base de données, client*) * Cahier des charges de sécurité des serveurs (*liste des ports à ouvrir sur chaque serveur, composants à supprimer…)* * Procédure de configuration des accès autorisés. | | * La veille technologique des vulnérabilités est efficace, organisée et automatisée. * La liste comparative des caractéristiques des outils de détection des vulnérabilités est établie. * Les accès logiques sont mis en place. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1 h 30 | Afin de garantir la disponibilité des données du site web en cas d’attaque sur le serveur web, vous devez assurer la sauvegarde des données sur le site et en dehors.   1. Réaliser la sauvegarde de la base de données selon le cahier des charges fourni par le RSSI. 2. Réaliser des tests de restauration des données. 3. Assurer une authentification distante sécurisée pour effectuer la sauvegarde du serveur de la base de données dans le cloud. | | * Machines virtuelles de l’infrastructure des deux sites (*web, base de données, client, serveur de sauvegarde, serveur VPN*) * Cahier des charges des sauvegardes de la base de données (*planification, automatisation, clone du serveur, sauvegardes locales et distantes*…). * Accès à une solution de cloud. * Procédure d’accès distant sécurisé (*ssh par exemple*). | | * La base de données est sauvegardée sur site selon la planification souhaitée. * La restauration de la base de données est opérationnelle. * La sauvegarde du serveur est réalisée dans le cloud. * La mise à jour quotidienne de la base de données dans le cloud est automatisée. * L’accès distant est sécurisé. | |
| **Séance 4** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1 h | Un plan de continuité d’activité (PCA) a été conçu mais n’a jamais testé.  Appliquer la procédure fournie pour tester le PCA. | | * Environnement PCA (machines virtuelles nécessaires, PCA entre le site de Paris et Toulouse). * Procédure de test du PCA. | | * L’environnement technique de test du PCA est mis en place. * Le rapport de test du PCA est rédigé. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence**  **B3.4 D2** | **Sécuriser les services informatiques et l’accès aux fichiers de configuration et aux données qu’ils hébergent afin de garantir leur intégrité**  **Semestre 2** | | | | | |
| 8 h | Votre travail consiste à mettre en œuvre la politique de gestion des accès utilisateurs recommandée par la CNIL et décrite par votre RSSI pour garantir la confidentialité et l’intégrité des données et sécuriser les accès aux serveurs de votre entreprise. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Caractériser les risques liés à l’utilisation malveillante d’un service informatique * Organiser la collecte et la conservation des preuves numériques * Appliquer les procédures garantissant le respect des obligations légales. * Identifier les obligations légales qui s’imposent en matière d’archivage et de production des données de l’organisation. | Savoirs technologiques   * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. * Authentification, privilèges et habilitations des utilisateurs : principes et techniques. * Gestion des droits d’accès aux données : principes et techniques. * Protection et archivage des données : principes et techniques. * Chiffrement, authentification et preuve : principes et techniques. * Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique. | | * Les risques associés à l’utilisation malveillante d’un service informatique sont caractérisés. * Les conséquences des actes malveillants sur un service informatique sont identifiées. * Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées : * les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ; * l'authentification et la confidentialité des échanges sont vérifiées ; * les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ; * les systèmes et les applications sont actualisés en fonction des alertes de sécurité ; * les vulnérabilités connues sont contrôlées. | | Prérequis :  Bloc 3 - Séquence 3.2 A2  Transversalités :  Bloc 3 - 3.3 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 3 h | L’audit de sécurité du patrimoine informatique a révélé une mise en place des accès aux ressources matérielles et logicielles (services et données) qui peuvent altérer et compromettre l’intégrité des données du système d’information.   1. Informer les utilisateurs de la mise en place du système de journalisation. 2. Mettre en place et configurer une traçabilité des accès sur les serveurs sensibles. 3. Journaliser les événements liés aux modifications de fichiers sur des serveurs. 4. Activer la journalisation sur les serveurs sensibles. 5. Analyser les logs générés (client syslog/suite Elasticsearch). | | * Environnement technique d’infrastructure (*machines virtuelles avec les serveurs concernés par les tâches de la séquence*). * Politique de gestion des accès et des habilitations mise en place. * Liste des mouvements du personnel (utilisateurs et collaborateurs avec définition de leurs habilitations). | | * La journalisation des événements est opérationnelle. * Les logs générés sont analysés. * Les compromissions éventuelles sont remontées au RSSI. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 4 h | L’analyse des logs a révélé des vulnérabilités. Le RSSI a mis à jour la politique de gestion des accès et des habilitations que vous devez appliquer au sein de l’entreprise.   1. Mettre en œuvre les contre-mesures des vulnérabilités détectées. 2. Réaliser une revue des habilitations à chaque mouvement du personnel (nouveaux arrivants, départs…). | | * Environnement technique d’infrastructure (*machines virtuelles avec les serveurs concernés par les tâches de la séquence*). * Politique de gestion des accès et des habilitations mise en place (*création de comptes nominatifs avec uniquement les accès nécessaires aux bases de données, politique spécifique des mots de passe administrateurs, authentification forte des administrateurs, comptes de moindres privilèges pour les activités courantes, suppression ou désactivation des comptes d’application créés par défaut, solution sécurisée et accès restreint aux interfaces web d’administration de services, verrouillage automatique de session, identifiant unique à chaque utilisateur, politique de mot de passe utilisateur conforme aux exigences de la CNIL, nombre d’échecs de connexion limité, changement de mot de passe à la première connexion, principe du moindre privilège*…). * Liste des mouvements du personnel (utilisateurs et collaborateurs avec définition de leurs habilitations). | | * Les vulnérabilités détectées sont corrigées. * La revue des habilitations est mise à jour. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1 h | Le service juridique impose aux comptables de générer des preuves numériques sur les fiches de paie des salariés.  Vous préparez une démonstration destinée aux comptables pour leur montrer l’intérêt de mettre en œuvre la preuve numérique, à savoir vérifier l’intégrité du document numérique concerné qu’on veut prouver.   1. Générer une empreinte numérique d’une fiche de paie de test. 2. Modifier la fiche en question. 3. Générer une nouvelle fois l’empreinte. 4. Comparer les deux empreintes afin de leur montrer l’altération du document. 5. Sauvegarder la preuve numérique sur le serveur dédié à l’archivage des preuves numériques en utilisant un canal sécurisé. 6. Récupérer la fiche de paie et la preuve numérique par deux canaux différents. 7. Générer l’empreinte de la fiche de paie reçue sur le poste local. 8. Vérifier l’intégrité du document numérique. | | * Fonction de hachage cryptographique. * Fiche de paie de test. * Environnement technologique (serveur d’archivage). | | * L’empreinte numérique est générée. * Un test d'intégrité de l’empreinte est réalisé. * La preuve numérique est générée et archivée sur un serveur distant en utilisant un canal sécurisé. | |