|  |  |
| --- | --- |
| **Bloc de compétences 3 Semestre 1 et 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 |

|  |  |
| --- | --- |
| **3.2. Préserver l'identité numérique de l'organisation - Déployer les moyens appropriés de preuve électronique Semestre 1** | |
| **Votre mission**  Votre travail consiste à protéger l’identité numérique de votre client et à mettre en place des moyens de preuve électronique.  Vous êtes également chargé(e) de former les utilisateurs à certains « réflexes » préventifs pour réduire les risques liés aux malveillances. | **Contexte professionnel** : Rattaché(e) au RSSI junior de l’équipe sécurité, vous intervenez auprès d’une entreprise de taille intermédiaire de 2300 salariés pour vérifier la qualité de son identité numérique, recenser les sources de sa présence digitale, lister les menaces associées et les mesures de protection à mettre en place pour s’en prémunir. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.2 A1** | **Caractériser l’identité numérique d’une entreprise et évaluer ce qui peut la menacer** | | | | | |
| Durée totale en heures du scénario pour la séquence  5h | En vous appuyant sur des éléments techniques et juridiques, votre travail consiste à expliquer de quoi est constituée l’identité numérique de votre client en vue de la protéger des menaces associées à sa présence digitale. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * **Protéger l’identité numérique d’une organisation** | Savoirs technologiques   * Typologie des risques et leurs impacts. * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. * Sécurité et sûreté : périmètre respectif.   Savoirs économiques, juridiques et managériaux   * L’identité numérique de l’organisation : risques et protection juridique. * La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique. * Les risques des cyberattaques pour l’organisation : économique, juridique, atteinte à l’identité de l’entreprise. * Obligations légales de notification en cas de faille de sécurité. * Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions. * Les organisations de lutte contre la cybercriminalité. | | * L’identité numérique de l’organisation est protégée en s’appuyant sur des moyens techniques et juridiques. | |  |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Recenser les sources qui fondent la présence digitale du client : courriels, messageries instantanées, sites web institutionnels et applications web, applications mobiles, réseaux sociaux et traces associées. | | * Le site web d’une entreprise réelle ([par exemple](https://www.cognizant.com/fr-fr/)) qui comporte des liens vers des adresses électroniques, des liens vers des pages Facebook, Twitter. Des profils de collaborateurs de cette entreprise peuvent être trouvés dans un réseau social professionnel. | | Une liste de sources qui constituent l’ensemble de l’identité numérique de l’entreprise cliente : nature de la source, lien pour la consulter. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Pour chaque constituant de l’identité numérique du client, accéder à ce qu’il contient et dire en quoi il permet de construire l’identité numérique du client et en quoi une altération de son contenu par un pirate pourrait nuire à cette identité en termes de risques. | | * Le site web de l’organisation cliente. | | Un tableau comportant pour chaque source d’identité une description de son contenu et le risque que représenterait une modification malveillante de ce contenu. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Après avoir lu un article relatant une cyberattaque contre votre client, identifier le type d’attaque utilisé par les pirates, dire quels principes de sécurité ont été violés (principes DIC) et pourquoi, identifier le moyen utilisé par les pirates et ce qui a été volé. Dire en quoi cette attaque a pu nuire à l’identité numérique de votre client. | | * Le site web de l’organisation cliente. * Un article relatant une cyberattaque de cette entreprise ([par exemple](https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/cybercriminalite/actualite-892240-cognizant-objet-piratage-ransomware-type-maze.html)). | | Une note comportant le type d’attaque, le moyen utilisé par les pirates, ce qui a été volé ainsi qu’une explication sur l’incidence de l’attaque sur l’identité numérique du client. | |
| **Séance 4** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2h | Parmi les mesures de protection techniques et juridiques que vous connaissez, décrire celles qui auraient pu être mises en œuvre pour prévenir et éviter la cyberattaque subie par votre client mais aussi pour y remédier après qu’elle ait eu lieu. | | * Le site web de l’organisation cliente. * Un article relatant une cyberattaque de cette entreprise ([par exemple](https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/cybercriminalite/actualite-892240-cognizant-objet-piratage-ransomware-type-maze.html)). | | Une note indiquant les mesures de protection à mettre en place en expliquant pour chacune d’elles comment elle contribue à prévenir et/ou à surmonter l’attaque étudiée. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.2 B1** | | **Comprendre les techniques, les méthodes et les moyens de la preuve électronique** | | | | | | | | | | |
| 4h | | Votre travail consiste dans un premier temps à étudier les méthodes et les moyens de preuve électronique (ou numérique) que votre entreprise met en place auprès de ses clients et, dans un second temps, à intervenir chez un nouveau client pour réaliser un audit des moyens liés à la preuve numérique.  Votre travail consiste, auprès de l’entreprise cliente, à :   * étudier les méthodes de cryptographie et de chiffrement ainsi que la notion de confidentialité d’une donnée ; * mettre en place une solution de chiffrement des fichiers ; * étudier des protocoles d’accès à distance sécurisés et non sécurisés. | | | | | | | | | | |
| **Compétences travaillées** | | **Savoirs associés** | | | | **Indicateurs de performance** | | | | **Prérequis / Transversalités** |
| * Déployer les moyens appropriés de preuve électronique. | | Savoirs technologiques   * Chiffrement, authentification et preuve : principes et techniques.   Savoirs économiques, juridiques et managériaux   * Droit de la preuve électronique. | | | | * La preuve numérique est déployée de manière sécurisée et dans le respect de la législation. | | | | Prérequis  Notion de preuve électronique et droit de la preuve électronique (CEJMA)  Séquence 3.3 B1  Transversalité  Thème 4 question 2 du programme de CEJM.  Bloc 1 : 1.2 et 1.5 |
| **Séance 1** | | **Tâches à réaliser** | | | **Ressources fournies** | | | | **Résultats attendus** | | | |
| 1h30 | | Afin de connaître les méthodes et les moyens de preuve numérique que votre entreprise met en place auprès de ses clients, vous allez étudier les méthodes de cryptographie et de chiffrement ainsi que la notion de confidentialité d’une donnée.  À l’aide des informations contenues dans l’UNITÉ 5 - Notions de cryptographie du Chap 2 du Mooc SecNumEdu de l’ANSSI, répondre au questionnaire sur la signature numérique. | | | * Mooc SecNumEdu de l’ANSSI : Chap 2 SÉCURITÉ DE L'AUTHENTIFICATION - UNITÉ 5 - Notions de cryptographie. * Fiche de savoirs sur la cryptographie et la confidentialité d’une donnée. * Questionnaire de synthèse des connaissances sur la notion de chiffrement symétrique et asymétrique, de clé et de signature électronique, de certificat. | | | | Questionnaire de synthèse complété et corrigé en ligne. | | | |
| **Séance 2** | | **Tâches à réaliser** | | | **Ressources fournies** | | | | **Résultats attendus** | | | |
| 1h30 | | Vous êtes sollicité pour mettre en place une solution de chiffrement des fichiers et des disques durs des ordinateurs portables de l’entreprise cliente pour les protéger en cas de vol.   1. Mettre en place la solution proposée par Microsoft sur des machines Windows 10. 2. Comparer avec d’autres solutions proposées par des éditeurs de logiciels de sécurité. | | | Fiche technologique sur les options de compression et de chiffrement des systèmes Windows | | | | * Procédure d’installation et d’utilisation de la solution de chiffrement des fichiers et des disques durs intégrée à Windows comportant une procédure de stockage des informations de récupération en cas de perte de mot de passe. * Comparatif avec 2 autres solutions de chiffrement de fichiers et/ou disque dur complet. | | | |
| **Séance 3** | | **Tâches à réaliser** | | | **Ressources fournies** | | | | **Résultats attendus** | | | |
| 1h | | Une des machines linux que l’entreprise utilise pour l’administration des serveurs doit pouvoir être accessible depuis l’ordinateur de l’administrateur.  Vous êtes chargé de tester l’accès à distance à cette machine :   1. Tester l’accès via le protocole telnet et un client de terminal (Putty par exemple), ensuite utiliser ssh pour réaliser les mêmes opérations. 2. Utiliser un analyseur de trames (wireshark ou tcpdump) pour visualiser les informations transmises entre les deux postes. 3. Comparer les informations transmises dans les deux cas et rédiger des recommandations pour les installations de ces protocoles sur les serveurs. | | | * Une fiche technologique sur l’utilisation de ssh, telnet et tcpdump sur une machine linux. * Une machine virtuelle (VM) linux avec telnetd, tcpdump et sshd installés (par exemple kali). * Éventuellement une seconde VM client Windows avec putty et wireshark installés.   *NB : les manipulations client/serveur peuvent se faire sur une seule machine en faisant une capture sur la carte de bouclage* | | | | * Captures de trames montrant la lecture du mot de passe en clair de la session telnet, et le chiffrement avec ssh. * Une liste de recommandations expliquant le problème rencontré et comment y remédier.   *(Voir si on demande de désinstaller le démon telnet pour garantir la sécurité)* | | | |
| **Séquence 3.2 A2** | **Mettre en œuvre la signature numérique des courriels, le chiffrement et le hachage des fichiers et les certificats SSL - Semestre 2** | | | | | | | | | | | | |
| 4h | Vous intervenez chez un nouveau client, suite à l’audit précédent, pour mettre en place des moyens liés à la preuve numérique.  Votre travail consiste, auprès de l’entreprise cliente, à :   * mettre en place un système de signature des courriels ; * mettre en œuvre les techniques de chiffrement et de hachage d'un fichier sur les documents confidentiels ; * former les utilisateurs à la vérification des certificats des serveurs web externes auxquels ils se connectent dans leur tâches quotidiennes | | | | | | | | | | | | |
| **Compétences travaillées** | | **Savoirs associés** | | | | **Indicateurs de performance** | | | | **Prérequis / Transversalités** | | |
| * Déployer les moyens appropriés de preuve électronique. | | Savoirs technologiques   * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. * Protection et archivage des données : principes et techniques. * Chiffrement, authentification et preuve : principes et techniques.   Savoirs économiques, juridiques et managériaux   * L’identité numérique de l’organisation : risques et protection juridique. * Droit de la preuve électronique | | | | * L’identité numérique de l’organisation est protégée en s’appuyant sur des moyens techniques et juridiques. * La preuve numérique est déployée de manière sécurisée et dans le respect de la législation. | | | | Prérequis  Notion de preuve électronique et droit de la preuve électronique (CEJMA)  Transversalité  Thème 4 question 2 du programme de CEJM. | | |
| **Séance 1** | **Tâches à réaliser** | | | | | **Ressources fournies** | | | | **Résultats attendus** | | | |
| 1h | 1. Mettre en place un système de signature des courriels de l’entreprise cliente. 2. Installer et configurer le système de signature des courriels, puis expliquer à un des employés comment s’y prendre et comment vérifier que les courriels qu’il reçoit sont bien signés de son expéditeur. | | | | | Une fiche technologique sur l’installation et la configuration d’un système de signature de courriels | | | | Une documentation technique et utilisateur de la solution de signature de mails utilisée. | | | |
| **Séance 2** | **Tâches à réaliser** | | | | | **Ressources fournies** | | | | **Résultats attendus** | | | |
| 1h30 | Votre travail consiste à mettre en œuvre les techniques de chiffrement et de hachage d'un fichier sur les documents confidentiels de l’entreprise cliente.  Mettre en œuvre les techniques de chiffrement symétrique avec OpenSSL sur votre machine linux. | | | | | * Une fiche technologique sur les techniques de chiffrement et de hachage. * Quelques fichiers exemples avec leur hachage, leur version chiffrée ou déchiffrée. * Une fiche technologique sur l’installation d’OpenSSL et l’utilisation de ses primitives pour chiffrer/déchiffrer un fichier. * Une VM linux avec openSSL installé. | | | | * Une documentation technique et utilisateur montrant les différentes étapes de chiffrement et de déchiffrement d’un fichier avec différents algorithmes. * Les fichiers chiffrés ou déchiffrés. | | | |
| **Séance 3** | **Tâches à réaliser** | | | | | **Ressources fournies** | | | | **Résultats attendus** | | | |
| 1h30 | Le site extranet de l’entreprise est migré de http à https, vous êtes chargé(e) de rédiger une documentation à destination des utilisateurs internes pour préparer la connexion au site https de l’entreprise et les former à la vérification des certificats des serveurs web externes auxquels ils se connectent dans leur tâches quotidiennes (site des fournisseurs, des compagnies aériennes…) | | | | | * Une fiche technologique sur les certificats SSL et la gestion des certificats sous Windows. * MOOC SecNumEdu de l’ANSSI - Chapitre 3 SÉCURITÉ SUR INTERNET - L'envers du décor d'une connexion Web (notions sur le fonctionnement basique d'une connexion web, proxy, HTTPS et les certificats). * Une VM avec le serveur web de l’entreprise cliente configuré en https. | | | | La documentation de la mise en place d’une connexion HTTPS depuis un ordinateur client vers un serveur identifié par son certificat SSL est rédigée. | | | |