|  |  |
| --- | --- |
| **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 |

|  |  |
| --- | --- |
| **3.3. Sécuriser les équipements et les usages des utilisateurs Semestre 1** | |
| **Votre mission :**  Votre travail consiste à lister les menaces et les risques sur les équipements informatiques et à mettre en place les mesures de protection pour les prévenir.  Vous êtes également chargée ou chargé 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 d’une ESN, vous intervenez comme technicien(ne) niveau 1 auprès d’une entreprise de taille intermédiaire de 500 salariés. Vous exercez des activités de sécurisation des équipements et de leurs usages par les utilisateurs. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.3 A1** | **Informer les utilisateurs sur les cybermenaces, les risques et promouvoir les bonnes pratiques de sécurité numérique** | | | | | |
| Durée totale en heures du scénario pour la séquence  6h | Vous travaillez pour une entreprise cliente, une PME de 500 salariés récemment touchée par un rançongiciel et dont le responsable souhaiterait que vous animiez des ateliers de sensibilisation à la cybersécurité afin d’éviter qu’un tel incident ne se reproduise.  Votre travail consiste dans un premier temps à prendre conscience des enjeux des nouvelles modalités de travail pour l’entreprise cliente tels que le télétravail, le nomadisme, le PAP (« prenez vos appareils personnels » ou BYOD – *Bring Your Own Device* en anglais) en identifiant les avantages qu’elles procurent pour les salariés et l’employeur mais aussi les risques notamment en termes de sécurisation des données, et de violation de la vie privée.  Dans un second temps, vous serez chargé de prévoir la communication auprès des utilisateurs de l’entreprise sur les risques liés à ces usages et la promotion des bonnes pratiques de sécurité informatique. Vous organiserez des ateliers de sensibilisation en lien avec l’actualité des menaces et des attaques en cours. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Informer les utilisateurs sur les risques associés à l’utilisation d’une ressource numérique et promouvoir les bons usages à adopter. * Gérer les accès et les privilèges appropriés. | Savoirs technologiques   * Typologie des risques et leurs impacts. * Sécurité des terminaux utilisateurs et de leurs données : principes et outils.   Savoirs économiques, juridiques et managériaux   * La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique | | * Des supports de communication interne sont accessibles aux utilisateurs. | | Prérequis :  Bloc 3 - 3.1 et 3.2 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2h | Votre tâche va consister, à travers l’étude d’un MOOC, à préparer les réponses aux questions suivantes afin de proposer un guide de bonnes pratiques sous forme de FAQ à soumettre au responsable de l’entreprise cliente avant diffusion.   1. Comment repérer les formats et les extensions d'un fichier sur un PC (windows, Mac, linux), sur un smartphone/tablette (Android, IoS)… 2. Y a-t-il des formats plus risqués que d'autres ? 3. Y a-t-il des sources plus sûres que d'autres ? 4. Comment se protéger des rançongiciels ? 5. Toutes ces mesures ne sont-elles pas un peu « parano » notamment quand on connait l’expéditeur ou la source d’un fichier ? | | * MOOC SecNumEdu de l’ANSSI - Chapitre 3. SÉCURITÉ SUR INTERNET – Unité 2 : Les fichiers en provenance d'Internet. * Un dossier sur l’entreprise cliente : organigramme, infrastructure, inventaire matériel et logiciel… * Des ressources du web sur des blogs, forums, par exemple : Étude d’un témoignage « J'ai déjà eu recours à une pratique déconseillée sans aucun problème ». | | Synthèse des réponses aux questions sous forme de FAQ, contextualisée par rapport à l’entreprise cliente. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Séance 2** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 2h | À partir du dossier de l’entreprise cliente et des informations concernant la mise en place massive du télétravail (possible pour tous les employés 1 j/semaine), vous allez :   1. Élaborer une synthèse présentant les bonnes pratiques en termes de séparation des usages entre personnel et professionnel dans ce contexte. 2. Vous appuyer sur des exemples de bonnes ou de mauvaises pratiques identifiées dans le contexte pour mieux sensibiliser les utilisateurs sur la sécurité et la séparation des usages professionnels-personnels.   *Remarque aux auteurs : On s’appuie sur un contexte type « étude de cas » pour aborder les problématiques liées à la « Séparation des usages » entre personnel et professionnel.* | * MOOC SecNumEdu de l’ANSSI - Chapitre 4 SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME – Unité 5 : Séparation des usages. * Un dossier sur l’entreprise cliente : organigramme, infrastructure, inventaire matériel et logiciel, kit de télétravail comportant un volet sur la mise en place du télétravail, une charte spécifique à l’utilisation des appareils professionnels dans la sphère privée, la politique de gestion des mises-à-jour en cas de durée de télétravail prolongée… * Lien vers des sites concernant le BYOD et le télétravail : * [www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques](http://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques) * www.cnil.fr/fr/salaries-en-teletravail-quelles-sont-les-bonnes-pratiques-suivre * https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail<https://www.stormshield.com/fr/actus/teletravail-et-cybersecurite-comment-allier-mobilite-et-securite-informatique> | Document de synthèse présentant les bonnes pratiques en termes de séparation des usages entre personnel et professionnel. |
| **Séance 3** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 2h | À partir des éléments produits dans les séances précédentes, vous êtes chargé(e) de préparer la communication de l’entreprise sur les risques engendrés par les usages liés à ces nouvelles modalités de travail et la promotion des bonnes pratiques au sein de l’entreprise. Vous organiserez des ateliers de sensibilisation en lien avec l’actualité des menaces et des attaques majeures en cours pour amener les utilisateurs à :   1. Identifier les points clés de la charte informatique. 2. Séparer leurs usages entre personnel et professionnel. 3. Appliquer la politique vis-à-vis des fichiers en provenance d'Internet. | * MOOC SecNumEdu de l’ANSSI - Chapitre 4 SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME – Unité 5 : Séparation des usages. * Lien vers des sites qui recensent l’actualité des cybermenaces, par exemple : https://www.cybermalveillance.gouv.fr/blog, <https://www.globalsecuritymag.fr/>, <https://www.mag-securs.com/> | Les supports de communication destinés aux utilisateurs de l’entreprise cliente sont réalisés **en lien avec l’actualité des cybermenaces et des attaques rapportées récemment** (vidéo, audio, documents des ateliers de sensibilisation, … ). |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.3 B1** | **Sécuriser le poste de travail : sécuriser les mots de passe, mettre à jour le système d’exploitation et les applications, installer un antivirus et un pare-feu** | | | | | |
| 6h30 | Votre travail consiste, au sein de l’équipe « bureautique », à participer aux tâches de sécurisation des terminaux utilisateurs fixes ou nomades, de leurs données et de leur connexion au réseau interne ou distant. Désormais sensibilisé au concept de menace/vulnérabilité/faille en sécurité informatique, vous appliquerez les procédures de sécurisation des postes de travail approuvés par l’entreprise cliente. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Identifier les menaces et mettre en œuvre les défenses appropriées. * Gérer les accès et les privilèges appropriés. * Vérifier l’efficacité de la protection. | Savoirs technologiques   * Sécurité des terminaux utilisateurs et de leurs données : principes et outils.   Savoirs économiques, juridiques et managériaux   * La sécurité des équipements personnels des utilisateurs et de leurs usages. | | * Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées : * l’accès physique au terminal et à ses données est sécurisé ; * les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ; * les flux réseaux sont identifiés et sécurisés ; * des supports de communication interne sont accessibles aux utilisateurs ; * l’efficacité de la protection mise en œuvre est évaluée. | | Prérequis :  Bloc 1 - 1.1  Bloc 3 - 3.1  Bloc 3 - 3.2 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2h | Afin de sensibiliser les utilisateurs à l’utilité d’un mot de passe fort et de sa sécurisation, vous êtes chargé de :   1. Préparer une notice présentant les points clés à connaître sur les attaques (directes et indirectes) sur mots de passe et les parades (nombres de facteurs d’authentification, longueur et complexité des mots de passe, chiffrement des données…) à mettre en œuvre dans le contexte de l’entreprise cliente. 2. Effectuer une recherche sur les logiciels de gestion des mots de passe et proposer une mise en œuvre documentant leur bonne utilisation pour l’entreprise cliente | | MOOC SecNumEdu de l’ANSSI : Chapitre 2 SÉCURITÉ DE L'AUTHENTIFICATION :  UNITÉ 1 - Principes de l'authentification.  UNITÉ 3- Sécuriser ses mots de passe.  UNITÉ 4 - Gérer ses mots de passe. | | * Une notice présentant les points clés à connaître et à mettre en œuvre dans le contexte de l’entreprise cliente pour renforcer la sécurité des mots de passe et des dispositifs fixes et nomades (ordinateurs, smartphone...) de l’entreprise. * Une mise en œuvre documentée d’un logiciel de gestion des mots de passe présentant une « bonne » utilisation adaptable au contexte de l’entreprise cliente. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Afin de sensibiliser davantage les utilisateurs à l’utilité d’un mot de passe fort, vous êtes chargé de préparer une démonstration de « craquage » de mots de passe en force brute, en utilisant des dictionnaires générés au préalable et des outils d’attaque (crunch, xHydra, JohnTheRipper…). | | * MOOC SecNumEdu de l’ANSSI : Chapitre 2 SÉCURITÉ DE L'AUTHENTIFICATION - UNITÉ 2 - Attaques sur les mots de passe. * Une fiche technologique sur l’utilisation sur une machine linux des outils d’attaque (crunch, xHydra, JohnTheRipper…). * Une machine virtuelle linux avec crunch et xHydra installés (par exemple kali). | | * Un dictionnaire généré à partir des chiffres et des lettres sur une longueur courte donnée (*permettant un test rapide*). * Démonstration du craquage de mot de passe enregistrée sous forme de vidéo. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h30 | Vous recevez un nouveau poste de travail, vous êtes chargé de mettre à jour le système, de configurer les mises à jour et de le paramétrer en fonction des recommandations de l’entreprise cliente.   1. Installer les mises à jour du système d’exploitation et des applications. 2. Configurer la politique de mises à jour du système et des applications. 3. Configurer les paramètres de données personnelles. 4. Configurer la sauvegarde de l’état du système et la gestion des points de restauration et tester une restauration du système avant l’installation de la dernière application. 5. Configurer la sauvegarde des données du dossier “Mes documents” avec l’outil intégré de Windows et tester une restauration des données. | | * Une machine virtuelle cliente Windows 10. * Une fiche technique décrivant la configuration de Windows 10 (Base et avancée). * MOOC SecNumEdu de l’ANSSI : Chapitre 4 SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME – Unité 1 : Applications et mises à jour.   Liens :  <https://www.ssi.gouv.fr/particulier/guide/restreindre-la-collecte-de-donnees-sous-windows-10/>  <https://www.ssi.gouv.fr/administration/guide/recommandations-pour-le-deploiement-securise-du-navigateur-mozilla-firefox-sous-windows/>  *NB : la mise à niveau de Windows 10 vers la version 1703 (Creators Update) permet de configurer les paramètres de données personnelles.* | | * Document (diaporama, vidéo…) présentant sur des exemples la notion de vulnérabilité en sécurité informatique. * Compte-rendu détaillé des opérations effectuées constituant la partie 1 du rapport de sécurisation. | |
| **Séance 4** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Vous recevez un nouveau poste de travail, vous êtes chargé de :   1. Installer un antivirus ou configurer l’anti-virus associé au système d’exploitation. 2. Installer un fichier qui simule la présence d’un virus. 3. Vérifier que l’antivirus le détecte bien et choisir l’action à effectuer (quarantaine ou suppression). 4. Planifier l’analyse anti-virale régulière et configurer la recherche de virus potentiels. | | * Une machine virtuelle cliente Windows 10 * Un lien vers des antivirus « gratuits » et vers la configuration de l’antivirus intégré à Windows * Un ensemble de ressources pour tester l’antivirus dont un fichier infecté par un virus de gravité faible. * MOOC SecNumEdu de l’ANSSI : Chapitre 4 SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME – Unité 2 : Options de configuration de base / Logiciels de sécurité. | | * L’antivirus est correctement installé et efficace contre le virus testé. * L’analyse anti-virale est planifiée avec une périodicité adéquate. * La recherche de virus potentiels sur les supports amovibles et les fichiers provenant d’internet est activée et l’action à effectuer suite à une détection est la quarantaine. * Compte-rendu détaillé des opérations effectuées constituant la partie 2 du rapport de sécurisation. | |
| **Séance 5** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Vous recevez un nouveau poste de travail, vous êtes chargé de :   1. Configurer le pare-feu proposé avec le système d’exploitation du poste de travail de façon à limiter strictement les communications réseau aux seules applications autorisées (dont ping). 2. Vérifier que les applications accèdent au réseau et que l’on peut « pinguer ». 3. Vérifier qu’aucune autre communication n’est possible. | | * Une machine virtuelle cliente Windows 10. * Une fiche technique décrivant la configuration du pare-feu intégré de Windows 10. * Une fiche de savoirs expliquant la notion de pare-feu. * MOOC SecNumEdu de l’ANSSI : Chapitre 4 SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME – Unité 2 : Options de configuration de base / Logiciels de sécurité. | | Compte-rendu détaillé des opérations effectuées et des tests constituant la partie 3 du rapport de sécurisation. | |
| **Séance 6** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Vous recevez un poste de travail qui appartenait à un ancien collaborateur inutilisé depuis 6 mois, vous êtes chargé de :   1. Supprimer toutes les données à caractère personnel et tous les fichiers du précédent utilisateur. 2. Vérifier la conformité du poste « suspect » avec la politique de sécurité de l’entreprise (mise à jour, antivirus, pare-feu, confidentialité…) issue de votre rapport de sécurisation. | | Une machine virtuelle cliente Windows 10 « suspecte ». | | Compte-rendu détaillé des tests effectués et des opérations de sécurisation constituant le rapport d’audit de sécurité du poste de travail « suspect ». | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.3 C1** | **Mettre en place les accès et les privilèges appropriés pour les utilisateurs** | | | | | |
| 5h | Votre travail consiste, au sein de l’équipe « système » à participer aux tâches de gestion des utilisateurs. Il s’agira de contrôler leurs droits d’accès et leur authentification, de faire respecter les bons usages, puis de déterminer les impacts d’une perte de Données à Caractère Personnel (DCP) ) ou de données professionnelles. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Gérer les accès et les privilèges appropriés. | Savoirs technologiques   * Authentification, privilèges et habilitations des utilisateurs : principes et techniques. * Gestion des droits d’accès aux données : principes et techniques.   Savoirs économiques, juridiques et managériaux   * La sécurité des équipements personnels des utilisateurs et de leurs usages. | | * Les accès et privilèges respectent les règles organisationnelles : * les utilisateurs sont authentifiés ; * les habilitations sont configurées ; * l’accès aux données est contrôlé ; * les privilèges sont restreints. | | Prérequis :  Bloc 1 - 1.1, 1.2, 1.3 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 3 h | Vous êtes informé du fait que tous les utilisateurs internes ont potentiellement un accès complet aux coordonnées complètes des clients saisies sur le site marchand de l’entreprise (pourtant chaque utilisateur se connecte avec ses identifiants sur son poste de travail et au CMS.  Votre tâche consiste à :   1. Déterminer comment les utilisateurs peuvent accéder aux données des clients. 2. Identifier où se trouve la faille qui permet à tous les utilisateurs d’accéder à ces données sensibles. 3. Identifier les accès et les privilèges dont disposent les utilisateurs ou les groupes d’utilisateurs sur le CMS et sur sa base de données 4. Restreindre les droits des intervenants sur le site en leur attribuant le rôle plus adéquat correspondant à leur activité sur le site, seul le u groupe d’utilisateurs autorisés aura accès aux données des clients. 5. Désactiver l’accès à l’administration directement depuis le site. 6. Modifier l’adresse d’accès au panneau d’administration du site. | | * Une machine virtuelle (VM) avec un CMS installé associé à une base de données. * Une machine virtuelle cliente avec des utilisateurs créés. * Le ou les comptes d’un utilisateur pour se connecter à la VM cliente, au CMS, à la base de données. * Une liste d’utilisateurs formant un groupe qui sera autorisé à accéder aux données des clients. | | * Un cas d’utilisation qui montre comment un utilisateur, depuis la connexion sur son poste, peut accéder aux données. * Une description de l’accès mal paramétré qui accorde un privilège inapproprié. * Les nouvelles modalités d’accès des intervenants au site sont revues et corrigées pour limiter l’accès aux données des clients. * Le groupe d’utilisateurs autorisé à administrer le site est défini et les droits sont bien configurés.   Les nouvelles modalités d’accès au portail d’administration du site sont testées et mises en œuvre. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Votre travail consiste à mettre en place un partage de fichiers entre les utilisateurs du service communication afin de mettre à leur disposition des documents et des vidéos. Le partage est accessible sur le poste de travail de l’adjoint administratif du service.   1. Mettre en place le partage de fichiers simple sur le poste de travail de l’adjoint administratif du service. 2. Mettre en place un accès en lecture seule pour consultation ou en lecture et modification suivant les habilitations du cahier des charges. | | * Cahier des charges définissant les dossiers et les fichiers à partager ainsi que les droits à mettre en place sur le partage en fonction des utilisateurs. * Fiches des savoirs technologiques de la gestion des utilisateurs et des permissions de partage Windows. * Une machine virtuelle cliente Windows 10. | | * Le partage est mis en place et accessible depuis les autres postes sur le même réseau physique. * Les droits d’accès sur le partage sont mis en place en tenant compte des contraintes demandées. * Un compte rendu des tests doit montrer via des captures d’écran la réalité des droits d’accès sur le partage mis en place. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Suite au vol de l’ordinateur portable d’un des employés du service communication, les vidéos du prototype du produit phare de l’entreprise sont divulguées sur Internet.   1. Recenser les mesures que pourrait prendre l’entreprise cliente à l’avenir pour éviter qu’un tel incident ait un impact s’il devait se reproduire. 2. Recenser les autres risques qu’elle encoure avec la mise en place du partage de fichiers d’un répertoire d’un poste de travail ? | | * Charte informatique de l’entreprise cliente. * Liens internet vers des articles de presse sur le même thème et vers des bonnes pratiques en termes de confidentialité des informations. | | * Une liste des mesures classées par degré d’urgence et par « facilité de mise en œuvre » dans le contexte de l’entreprise cliente. | |

|  |  |
| --- | --- |
| **3.3. Sécuriser les équipements et les usages des utilisateurs Semestre 2** | |
| **Votre mission :**  Votre travail consiste à participer aux activités d’audit et de sécurisation du parc informatique afin de prévenir les menaces externes et internes en déployant des outils et dispositifs de sécurité adaptés au contexte de l’entreprise cliente.  Vous participerez aux actions permettant de vérifier la traçabilité des actions menées sur les données, la journalisation des événements système et la stratégie d’audit d’accès sur un dossier ou un fichier. | **Contexte professionnel** : Rattaché(e) au RSSI de l’équipe sécurité d’une ESN, vous intervenez comme technicien(ne) sécurité auprès d’une entreprise de taille intermédiaire de 2000 salariés. Vous exercez des activités d’audit et de sécurisation des équipements et de leurs usages par les utilisateurs. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.3 A2** | **Participer aux activités d’audit et de sécurisation des éléments de la chaîne de connexion** | | | | | |
| 5h | Votre travail consiste à participer aux activités d’audit et de sécurisation des éléments de la chaîne de liaison afin de prévenir les menaces externes et internes en déployant les outils et les dispositifs de sécurité adaptés au contexte de l’entreprise cliente. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Identifier les menaces et mettre en œuvre les défenses appropriées. | Savoirs technologiques   * Sécurité des terminaux utilisateurs et de leurs données : principes et outils.   Savoirs économiques, juridiques et managériaux  La sécurité des équipements personnels des utilisateurs et de leurs usages. | | * Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées : * l’accès physique au terminal et à ses données est sécurisé ; * les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ; * les flux réseaux sont identifiés et sécurisés; * des supports de communication interne sont accessibles aux utilisateurs; * l’efficacité de la protection mise en œuvre est évaluée. | | Prérequis :  Bloc 3 Semestre 1  Bloc 1 Semestre 1  Transversalités  Bloc 2 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Vous devez analyser la chaîne de connexion mise en place dans l’entreprise cliente. Pour cela, vous effectuerez les opérations suivantes :   1. Identifier les matériels, les supports de communication et les équipements réseau. 2. Identifier les services accessibles aux utilisateurs de l’entreprise cliente. 3. Analyser la chaîne de connexion et sa configuration. | | * Un dossier sur l’entreprise cliente : organigramme, schéma d’infrastructure réseau filaire et sans fil, inventaire matériel et logiciel… * Les fiches des savoirs technologiques sur la sécurisation de la chaine de liaison, les couches du modèle OSI. * Une interview du RSSI basée sur l’analyse de la chaîne de connexion, mettant en avant les éléments à sécuriser. * Un fichier reproduisant le réseau dans un logiciel simulateur de réseau. * Une machine virtuelle cliente Windows 10. | | * Un document d’identification des éléments de la chaîne de liaison (VLAN, adresse IP du poste, adresse du serveur DNS, adresse du routeur, commutateur d'accès, borne wifi, accès distant). | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Séance 2** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 2h | À partir de l’étude précédente, vous êtes chargé(e) de proposer des modifications afin de :   1. Mieux contrôler les flux réseaux sur les postes de travail des utilisateurs de l’entreprise cliente *(adressage IP correspondant au bon vlan, sécurisation du wifi…).* 2. Mieux contrôler les accès distants aux postes (*bureau à distance avec authentification, ssh pour accéder au serveurs,* *pare-feu des postes…) ;* 3. Mettre en œuvre et documenter ces modifications. | * Un dossier sur l’entreprise cliente : organigramme, schéma d’infrastructure réseau filaire et sans fil, inventaire matériel et logiciel… * Une interview du RSSI basée sur l’analyse de la chaîne de connexion, mettant en avant les éléments à sécuriser. * Un fichier reproduisant le réseau dans un logiciel simulateur de réseau. * Une machine virtuelle cliente Windows 10. | * Un document d’identification des éléments de la chaîne de liaison modifiés (VLAN, adresse IP du poste, adresse du serveur DNS, adresse du routeur, commutateur d'accès, borne wifi, accès distant) et de sécurisation des accès distants. * Un fichier modélisant le réseau modifié dans un logiciel simulateur de réseau. |
| **Séance 3** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 1h | Les commerciaux de l’entreprise cliente utilisent des connexions à distance de type VPN nomade au SI de l’entreprise.   1. À partir des différentes sources internet, identifier les éléments permettant la connexion VPN nomade. 2. Vérifier la présence et la configuration de ces éléments à partir d’un poste d’un commercial et d’un compte utilisateur de test du groupe Ventes. | * Un dossier sur l’entreprise cliente : organigramme, schéma d’infrastructure réseau, inventaire matériel et logiciel… * Liens internet : * https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/ipsec | * Un document expliquant les points clés de la solution VPN mise en place dans l’entreprise cliente. |
| **Séance 4** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 1h | Vous êtes chargé(e) d’étudier la mise en place du modèle de sécurité « zéro confiance » (*zero trust)* pour les connexions à distance des commerciaux de l’entreprise cliente.   1. À partir des différentes sources internet, établir un document expliquant les points clés du modèle de sécurité « zéro confiance ». 2. Proposer des recommandations pour évoluer vers le modèle de sécurité « zéro confiance ». | * Un dossier sur l’entreprise cliente : organigramme, schéma d’infrastructure réseau, inventaire matériel et logiciel… * Liens internet : * <https://www.journaldunet.com/solutions/dsi/1440884-modeles-de-securite-pourquoi-miser-sur-le-zero-trust/> * https://www.globalsecuritymag.fr/Pourquoi-le-modele-Zero-Trust-va,20190517,87152.html (zero trust vs vpn) * <https://www.microsoft.com/fr-ww/security/business/zero-trust> | * Un document expliquant les points clés du modèle de sécurité « zéro confiance ». * Un document de recommandations pour faire évoluer le SI vers le modèle de sécurité « zéro confiance ». |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.3 B2** | **Mettre en place les accès et les privilèges appropriés dans un environnement Linux** | | | | | |
| 6h | Votre travail consiste à sécuriser les postes d’administration sous linux et l’accès au serveur web et bases de données du service informatique. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Gérer les accès et les privilèges appropriés : | Savoirs technologiques   * Authentification, privilèges et habilitations des utilisateurs : principes et techniques. * Gestion des droits d’accès aux données : principes et techniques.   Savoirs économiques, juridiques et managériaux   * La sécurité des équipements personnels des utilisateurs et de leurs usages | | * Les accès et privilèges respectent les règles organisationnelles : * les utilisateurs sont authentifiés ; * les habilitations sont configurées ; * l’accès aux données est contrôlé ; * les privilèges sont restreints. | | Prérequis :  Bloc 3 Semestre 1  Bloc 1 Semestre 1  Transversalités  Bloc 2 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Vous êtes chargé (e) de mettre à disposition les fichiers de documentation technique du service informatique de l’entreprise cliente sur un poste d’administration sous Linux. | | * Le cahier des charges définissant les partages et les nouveaux droits à mettre en place en fonction des utilisateurs. * Les fiches des savoirs technologiques de la gestion des utilisateurs et des permissions d’accès sur un serveur Linux. * Une machine virtuelle linux graphique. | | * Les droits d’accès sur le dossier sont mis en place en tenant compte des contraintes demandées. * Un compte rendu des tests avec les différents utilisateurs doit montrer, via des captures d’écran, la réalité du partage mis en place. | |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h30 | Vous êtes chargé(e) de vérifier la conformité des postes d’administration sous Linux.   1. Recenser les applications et les processus installés ainsi que leurs droits et les utilisateurs/groupes autorisés à les exécuter. 2. Effectuer les modifications nécessaires à l’application du cahier des charges en cas de non-conformité. | | * Cahier des charges définissant les applications et processus autorisés sur les postes d’administration. * Fiches des savoirs technologiques de la gestion des processus et de leurs droits sous Linux. * Une machine virtuelle linux graphique. | | * Les processus et leurs droits sont mis en place en tenant compte des contraintes demandées. * Les applications et processus non autorisés sont supprimés. * Un compte rendu montrant via des captures d’écran la réalité des processus et des droits mis en place. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h30 | Vous êtes chargé (e) d’augmenter le niveau de sécurité du poste d’administration sous Linux qui vous a été attribué. Après vous être informé sur la politique de sécurité mise en place dans l’entreprise, réaliser un durcissement du système, en respectant les contraintes et les recommandations émanant du RSSI. | | * Contraintes et recommandations émanant du RSSI pour le durcissement des systèmes linux des postes de travails sensibles. * Fiches des savoirs technologiques de la sécurisation des postes sous Linux. * Une machine virtuelle linux graphique. | | * Le durcissement du système linux des postes de travail sensibles est mis en place en tenant compte des contraintes demandées. * Un mode opératoire permettant de réaliser le durcissement du système linux sur d’autres postes de travail sensibles. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2h | Vous êtes chargé(e) de mettre en place le contrôle d'accès à la base de données du serveur web du service informatique qui gère des documentations techniques.   1. Configurer les droits d’accès à la base de données à l’aide de commandes SQL Standards, le serveur de bases de données étant accessible via un accès distant sécurisé en mode console (vous créerez un compte avec le droit en lecture seule, un en écriture, un autre en modification, et un compte administrateur avec tous les droits). 2. Vérifier la sécurité de l’accès à la base de données en testant plusieurs accès avec plusieurs comptes d’utilisateur. 3. Vérifier la sécurité de l’application web de gestion des documentations techniques. Le cas échéant vous préconiserez des modifications afin d’en améliorer la sécurité. | | * Une machine virtuelle linux hébergeant le serveur web et l’application web avec la base de données de gestion des documentations techniques. * Les fiches des savoirs technologiques de la sécurisation des applications web. * Les fiches des savoirs technologiques de la sécurisation des bases de données en SQL. * Un cahier des charges définissant les droits (lecture seule, écriture, modification) à mettre en place en fonction des utilisateurs. | | * Les droits d’accès aux bases de données sont mis en place en tenant compte des contraintes demandées. * Un mode opératoire permettant de sécuriser et de vérifier l’accès aux bases de données et la sécurité de l’applications web de gestion des documentations techniques, ainsi que les modifications préconisées afin d’en améliorer la sécurité. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.3 C2** | **Auditer la sécurité des postes et mettre en place la sauvegarde et la rétention des fichiers journaux des accès à Internet des utilisateurs de l’entreprise.** | | | | | |
| 3h | Votre travail consiste à participer aux activités d’audit de la sécurité des postes de l’entreprise cliente et à mettre en place la sauvegarde et la rétention des fichiers journaux des accès à Internet des utilisateurs de l’entreprise. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Vérifier l’efficacité de la protection | Savoirs technologiques   * Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique. * Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.   Savoirs économiques, juridiques et managériaux   * La sécurité des équipements personnels des utilisateurs et de leurs usages | | * Des supports de communication interne sont accessibles aux utilisateurs. * Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées * Les accès et privilèges respectent les règles organisationnelles : * L’efficacité de la protection mise en œuvre est évaluée. | | Prérequis :  Bloc 3 Semestre 1 et 3.3 A2, B2, C2  Bloc 1 Semestre 1  Transversalités  Bloc 2 |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Vous êtes chargé(e) d’évaluer les plans de secours de l’entreprise cliente : le plan de reprise d'activité (PRA) et le plan de continuité d'activité (PCA). Ceci afin d’évaluer s’ils répondent aux exigences de sécurité et s’ils permettent de traiter les incidents liés à la sécurité. | | * Une fiche de savoirs sur les notions de plan de secours, de contrat de service, de PRA et de PCA. * Une fiche de savoirs sur la gestion des incidents de sécurité. * Le PRA et le PCA de l’entreprise cliente. * Un document décrivant les attentes de la société cliente en matière de sécurité de ses postes de travail. | | Une analyse argumentée du PRA et du PCA mis en place au sein de l’entreprise cliente au regard des exigences de sécurité. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Dans le cadre de la politique de sécurité, vous devez pouvoir présenter les journaux d’audit d’accès à un poste de travail et à un répertoire de ce poste.   1. Mettre en place ces audits. 2. Effectuer des tests afin de vérifier leur fonctionnement. | | * Une fiche de savoirs technologiques décrivant l’observateur d’événements et les fonctions d’audit de sécurité. * Une machine virtuelle cliente Windows 10. | | Un compte rendu montrant, via des captures d’écran et des tests, le bon fonctionnement de l’audit mis en place. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 1h | Dans le cadre de la règlementation, vous devez pouvoir présenter les fichiers journaux des accès à Internet des utilisateurs de l’entreprise.   1. Mettre en place la sauvegarde de ces fichiers journaux. 2. Tester la restauration de ces fichiers journaux.   *Remarque pour les auteurs : la visualisation du contenu des logs n’est possible par l’administrateur que si on peut la tracer et la justifier par des impératifs techniques, il faudra bien le mentionner.* | | * Une fiche des savoirs sur la gestion des journaux des accès à Internet, leur sauvegarde et leur rétention. * Une fiche des savoirs technologiques décrivant l’accès aux logs du serveur proxy (mode web et mode console). * Une machine virtuelle avec un serveur proxy configuré et des logs. | | Un mode opératoire décrivant les procédures de sauvegarde et de restauration des fichiers journaux des accès à Internet des utilisateurs de l’entreprise. | |