Edition de la partie 2 - INFOSEC

Eric DUPUIS[1,2*]

Résumé
Ce document inclut l'ensemble de la partie 2 - InfoSec de CYBERDEF101.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.
Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101 (SEC101 du Cnam). Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

Mots clefs
Part2,InfoSec

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *Directeur Orange Campus Cyber*
***email** : eric.dupuis@lecnam.net – eric.dupuis@orange.com

Notes de cours SECOPS 2022-2023

Vérifiez la disponibilité d'une version plus récente de

CourseNotes-FR-SEC101-PART2-INFOSEC.pdf sur GITHUB CYBERDEF [1]

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/CourseNotes-FR-SEC101-PART2-INFOSEC.pdf

Infosec

1. Intro

Dans cet **ouvrage**, vous découvrirez (MMD)(http://fletcherpenney.net/mmd [2]) les concepts [3] et principes fondamentaux de la cybersécurité en entreprise Vous comprendrez les différents mécanismes de sécurité, les différentes menaces et vulnérabilités [4] qui existent dans notre monde numérique et comment vous en protéger, vous et votre organisation.

Vous découvrirez également les différents types [5]

de menaces liées à la cybersécurité, notamment les virus, les logiciels malveillants, les attaques de phishing et les ransomwares, ainsi que la manière de les identifier et de les atténuer. Vous apprendrez également l'importance de la sécurité des réseaux et comment sécuriser et entretenir vos systèmes et réseaux informatiques.

En outre, vous découvrirez le rôle des professionnels de la cybersécurité et les différentes possibilités de carrière dans ce domaine. Vous aurez également l'occasion de mettre en pratique vos compétences au moyen d'exercices pratiques et de simulations.

À la fin de ce cours, vous disposerez de bases solides en matière de cybersécurité et serez bien équipé pour vous protéger, vous et votre organisation, des menaces en ligne.

Les menaces pour la cybersécurité sont tout type d'activité malveillante ou d'attaque qui présente un risque pour les systèmes, réseaux ou dispositifs informatiques. Ces menaces peuvent prendre de nombreuses formes et viser des individus, des organisations ou des pays entiers. Voici quelques types courants de menaces pour la cybersécurité :

- **Les virus** : Un virus est un type de logiciel malveillant qui peut infecter un ordinateur et se propager à d'autres ordinateurs. Les virus peuvent se propager par le biais de pièces jointes à des courriels, de téléchargements ou par la visite de sites Web infectés.
- Les logiciels malveillants : Un logiciel malveillant est un terme général désignant tout logiciel conçu pour nuire ou perturber les systèmes informatiques. Cela inclut les virus, les chevaux de Troie, les vers et d'autres types de logiciels malveillants.
- Attaques par hameçonnage : Une attaque par hameçonnage est un type de cyberattaque qui utilise des courriels ou des sites Web frauduleux pour inciter les gens à divulguer des informations sensibles. Les menaces pour la cybersécurité sont tout type d'activité ou d'attaque malveillante qui présente un risque pour les systèmes, réseaux ou dispositifs informatiques. Ces menaces peuvent prendre de nombreuses formes et viser des individus, des organisations ou des pays entiers. Voici quelques types courants de menaces de cybersécurité :
- Attaques de phishing : Une attaque par hameçonnage est un type de cyberattaque qui utilise des courriels ou des sites Web frauduleux pour inciter les gens à divulguer des informations sensibles, telles que des identifiants de connexion ou des informations financières.
- Ransomware : Un ransomware est un type de logiciel malveillant qui crypte les fichiers d'une victime, les rendant inaccessibles jusqu'à ce qu'une rançon soit versée aux attaquants.

2. `http://fletcherpenney.net/mmd`
3. `https://rawgit.com/fletcher/MultiMarkdown-6-Syntax-Guide/master/index.html`
4. `https://tex.stackexchange.com/questions/554444/defining-a-new-command-using-a-conditional`
5. Ceci est une foot note

- Attaques par déni de service (DoS) : Une attaque par déni de service est une tentative de rendre un ordinateur ou une ressource réseau indisponible pour ses utilisateurs prévus en le submergeant de trafic ou de demandes.
- Attaques de type "Man-in-the-middle" (MitM) : Une attaque MitM est un type de cyberattaque où l'attaquant intercepte et altère la communication entre deux parties à leur insu.
- Attaques par injection SQL : Une attaque par injection SQL est un type de cyberattaque qui consiste à injecter un code malveillant dans une base de données par le biais d'un champ de saisie, tel qu'une barre de recherche ou un formulaire de connexion.

Il est important que les particuliers et les organisations soient conscients de ces types de menaces et prennent des mesures pour s'en protéger et protéger leurs systèmes.

1.1 Virus

Un virus informatique est un type de logiciel malveillant conçu pour infecter un ordinateur et se répliquer. Pour ce faire, il s'attache à d'autres fichiers ou programmes et se propage d'un ordinateur à l'autre.

Un virus peut avoir divers effets négatifs sur un ordinateur, comme la suppression de fichiers, le vol d'informations sensibles ou le ralentissement du système. Certains virus sont également conçus pour afficher des messages gênants ou malveillants ou pour rediriger les utilisateurs vers des sites web frauduleux.

> 👁 **Nota sur virus :** se propagent généralement par le biais de pièces jointes à des courriels, de téléchargements ou par la visite de sites web infectés. Ils peuvent également se propager par le biais de supports amovibles tels que les clés USB ou en étant installés par le biais de vulnérabilités logicielles.

Les composants sécurité en CYBER Il existe plusieurs composantes clés de la cybersécurité qu'il est important de comprendre afin de protéger efficacement les systèmes et réseaux informatiques. Ces composants sont les suivants :

- La sécurité du réseau : La sécurité du réseau consiste à protéger un réseau informatique contre les accès ou les attaques non autorisés. Cela peut se faire par l'utilisation de pare-feu, de systèmes de détection d'intrusion et d'autres mesures de sécurité.
- Sécurité des points d'accès : La sécurité des terminaux fait référence à la protection des appareils individuels tels que les ordinateurs, les ordinateurs portables et les smartphones qui se connectent à un réseau. Cela peut impliquer l'utilisation de logiciels antivirus, de pare-feu et d'autres mesures de sécurité pour protéger ces appareils contre les cybermenaces.
- Sécurité des applications : La sécurité des applications consiste à protéger les applications et les logiciels qui sont utilisés sur un ordinateur ou un réseau contre les vulnérabilités et les attaques. Cela peut être réalisé par l'utilisation de pratiques de codage sécurisées, de tests et d'autres mesures.
- Sécurité des données : La sécurité des données consiste à protéger les données sensibles contre un accès ou une divulgation non autorisés. Cela peut impliquer l'utilisation du cryptage, des contrôles d'accès et d'autres mesures pour garantir que les données ne sont accessibles qu'aux personnes autorisées.
- Gestion des identités et des accès : La gestion des identités et des accès implique les processus et les technologies utilisés pour gérer et sécuriser l'accès aux systèmes et aux ressources. Cela peut inclure l'authentification des utilisateurs, les autorisations et les systèmes de contrôle d'accès.

- Reprise après sinistre et continuité des activités : La reprise après sinistre et la continuité des activités font référence aux processus et aux plans mis en place pour garantir qu'une organisation puisse continuer à fonctionner en cas de sinistre ou d'autres perturbations. Il peut s'agir de systèmes de sauvegarde et de procédures de restauration des systèmes et des données.

Une cybersécurité efficace nécessite une combinaison de ces éléments, ainsi qu'une maintenance et une surveillance permanentes pour garantir que les systèmes et les réseaux restent sécurisés.

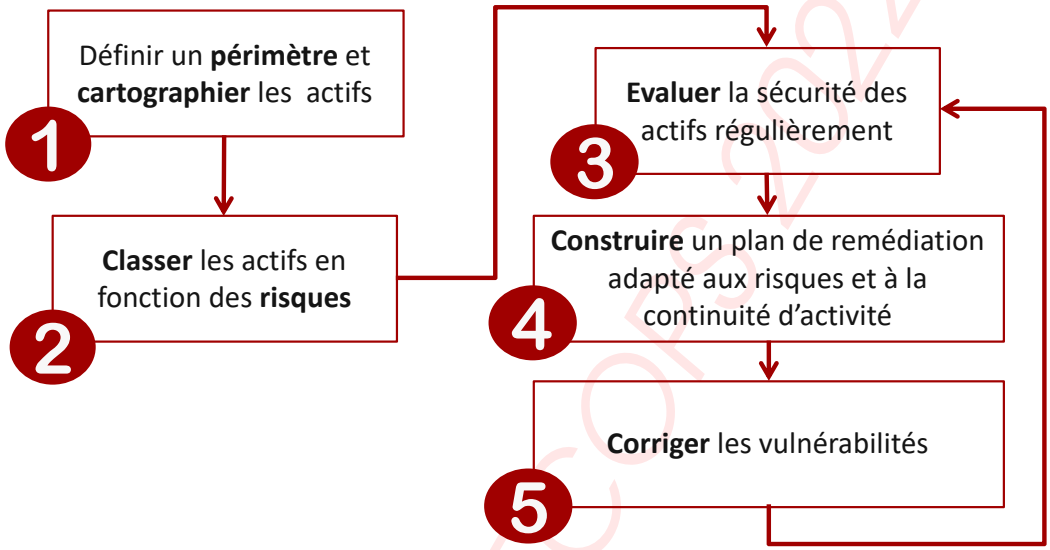

FIGURE 1. Image de texte - (slbl-img-vul-process.pdf)

La cybersécurité et la cyberdéfense sont des concepts connexes mais distincts.

La cybersécurité désigne la pratique consistant à protéger les systèmes, réseaux et dispositifs informatiques contre les cybermenaces et les vulnérabilités. Cela peut impliquer l'utilisation d'une variété de technologies, de processus et de pratiques pour garantir la sécurité des systèmes et des données.

La cyberdéfense, quant à elle, fait référence aux actions et mesures prises pour se défendre contre les cyberattaques et autres menaces. Cela peut inclure l'utilisation de pare-feu, de systèmes de détection d'intrusion et d'autres mesures de sécurité pour prévenir les attaques, les détecter et y répondre si elles se produisent.

En résumé, la cybersécurité est un terme plus large qui englobe toutes les mesures prises pour se protéger des cybermenaces, tandis que la cyberdéfense fait spécifiquement référence aux mesures et tactiques défensives utilisées pour prévenir ou répondre aux attaques.

Table des matières

Table des figures