RÉSUMÉ THÉORIQUE – FILIÈRE INFRASTRUCTURE DIGITALE – Option Cybersécurité

M209 – S'initier aux fondamentaux de la Cybersécurité

30 heures

SOMMAIRE

1. Identifier la terminologie liée à la Cybersécurité

- Définir la Cybersécurité
- Connaitre les objectifs de la Cybersécurité

2. Découvrir les différentes normes et standards de la Cybersécurité

- Connaitre les normes de la sécurité organisationnelle
- Identifier les normes de la sécurité technique
- Connaitre les référentiels réglementaires de la Cybersécurité

3. Définir les critères de la Cybersécurité

- Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005
- Définir les niveaux de chaque critère

4. Découvrir les métiers de la Cybersécurité

- Identifier les domaines de la Cybersécurité
- Découvrir le référentiel métier de l'ANSSI
- Connaitre les tendances des métiers de la Cybersécurité

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

Identifier la terminologie liée à la Cybersécurité

Dans ce module, vous allez :

- Découvrir les piliers de la Cybersécurité
- Identifier la terminologie liée à la Cybersécurité
- Appréhender les différentes postures de la Cybersécurité

6 heures

CHAPITRE 1

Définir la Cybersécurité

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le terme Cybersécurité
- Identifier les terminologies de la Cybersécurité
- Connaitre les tactiques, techniques et procédures utilisées par les attaquants

3 heures

CHAPITRE 1

Définir la Cybersécurité

1. **Définition de la Cybersécurité selon la norme ISO**
2. Terminologie de la Cybersécurité
3. Exemples des tactiques, techniques et procédures utilisées par les attaquants

Cybersécurité : définition

La Cybersécurité est la pratique qui consiste à protéger les systèmes critiques et les informations sensibles contre les attaques numériques. Également appelée Technologies de l'information (IT), les mesures de cybersécurité visent à lutter contre les menaces qui pèsent sur les systèmes et les applications en réseau, qu'elles proviennent de l'intérieur ou de l'extérieur d'une organisation.

Selon la norme ISO 27032 : « La Cybersécurité est liée à la sécurité de l'information et à la sécurité physique »

Pourquoi la cybersécurité est-elle importante ?

La cybersécurité est importante, car elle contribue à protéger les données d'une entreprise d'un piratage informatique de données qui, mises dans de mauvaises mains, pourraient nuire à l'entreprise ou aux personnes. Les archives des organismes médicaux, du gouvernement, des entreprises et des institutions financières regorgent d'informations personnelles. Un incident de sécurité les concernant peut ternir la réputation d'une entreprise et/ou lui faire perdre de l'argent. L'entreprise peut être victime de vol de données, d'effacement de données ou de fraude.

Cybersécurité : définition

Les personnes, les processus et la technologie au sein d'une entreprise doivent tous se compléter pour créer une défense efficace contre les cyberattaques :

Personnes :

Les utilisateurs doivent comprendre et respecter les principes de base relatifs à la sécurité des données, notamment en choisissant des mots de passe forts, en se méfiant des pièces jointes des courriels et en sauvegardant leurs données.

Processus :

Les organisations doivent disposer d'un cadre de travail pour gérer les tentatives de cyberattaques et celles qui réussissent. Il vous renseigne sur la manière d'identifier les attaques, de protéger les systèmes, de détecter les menaces et d'y répondre, et de vous remettre d'une attaque.

Technologie :

La technologie est indispensable pour fournir aux organisations et aux particuliers les outils de sécurité informatique nécessaires pour se protéger contre les cyberattaques. Trois entités principales doivent être protégées : les dispositifs de point d'extrémité tels que les ordinateurs, les appareils intelligents et les routeurs; les réseaux; et le nuage.

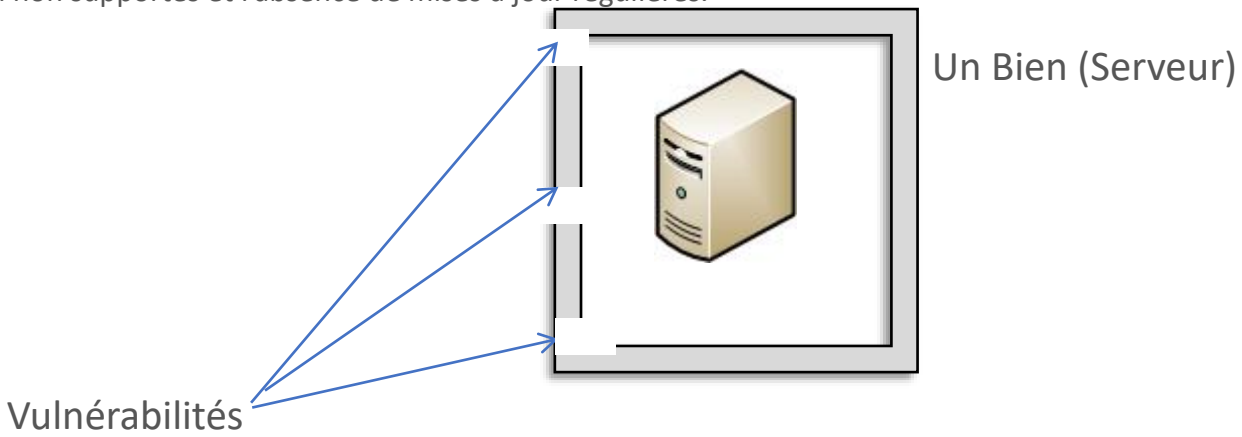
CHAPITRE 1

Définir la Cybersécurité

1. Définition de la Cybersécurité selon la norme ISO
2. **Terminologie de la Cybersécurité**
3. Exemples des tactiques, techniques et procédures utilisées par les attaquants

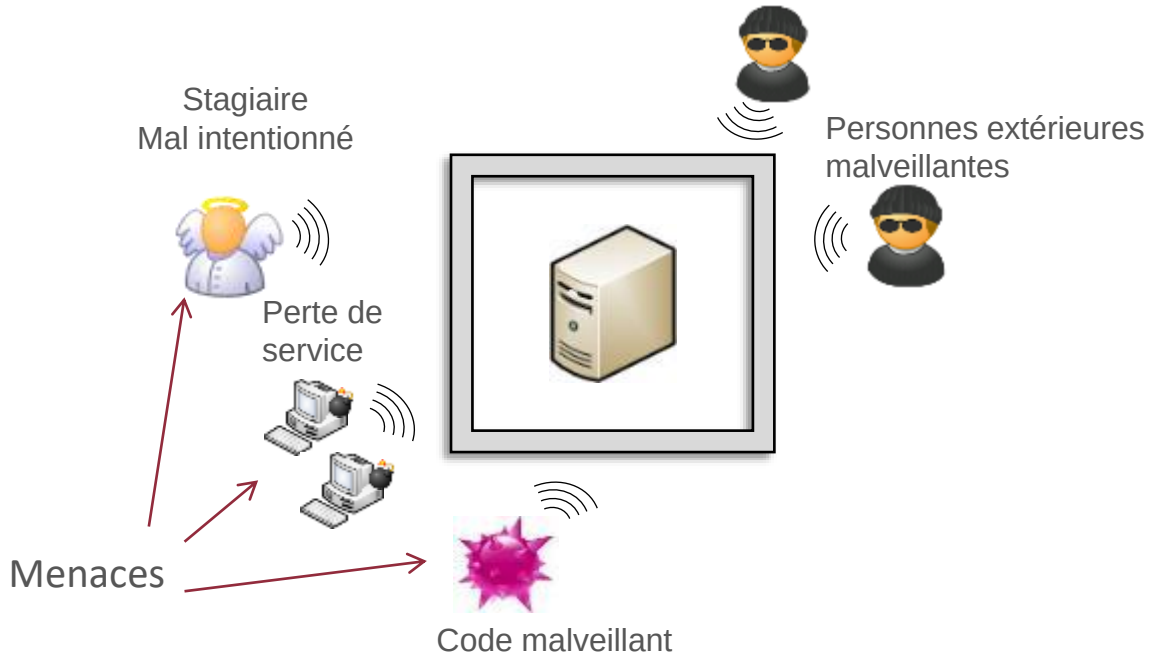
Notion de Vulnérabilité

- **Vulnérabilité : Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien)
- **Exemples :**
  - Emplacement situé dans une zone sujette aux inondations ;
  - Travail non surveillé des équipes extérieurs ;
  - L'utilisation de logiciels ou systèmes d'exploitation non supportés et l'absence de mises à jour régulières.



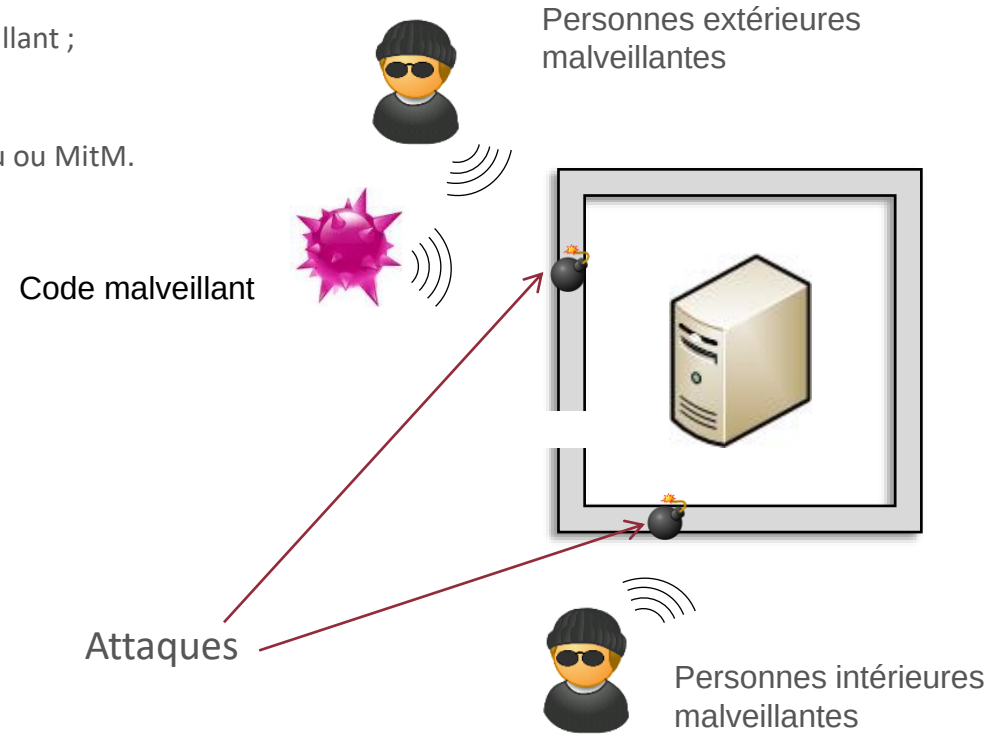
Notion de Menace

- **Menace : Cause potentielle d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.
- **Exemples** :
  - Vol de supports ou de documents ;
  - Inondation ;
  - Usurpation d'identité.



Notion d'Attaque

- **Attaque : Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité** →
- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.
- **Exemples** :
  - Les attaques par logiciel malveillant ;
  - Le déni de service (DDoS) ;
  - L'attaque de l'homme au milieu ou MitM.



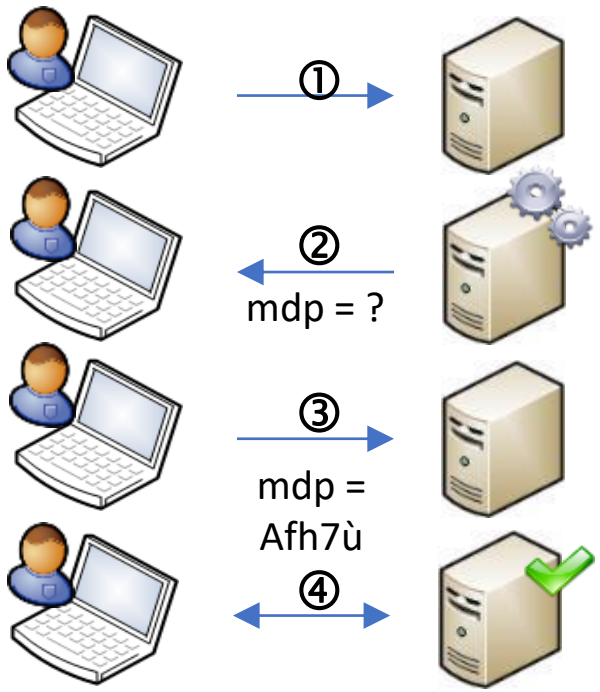
PARTIE 1

Illustration des notions Vulnérabilité, Menace et Attaque :

Cas pratique : Authentification dans l'application VNC (Virtual Network Computing)

L'utilisateur effectue une demande de connexion au serveur depuis son PC client

L'utilisateur s'authentifie selon la méthode choisie par le serveur



Description du fonctionnement normal de l'application

Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat*, etc.) et envoie cette demande d'authentification à l'utilisateur demandeur

Le serveur valide l'authentification (si elle est correcte) et autorise donc la connexion

Usage normal de l'application

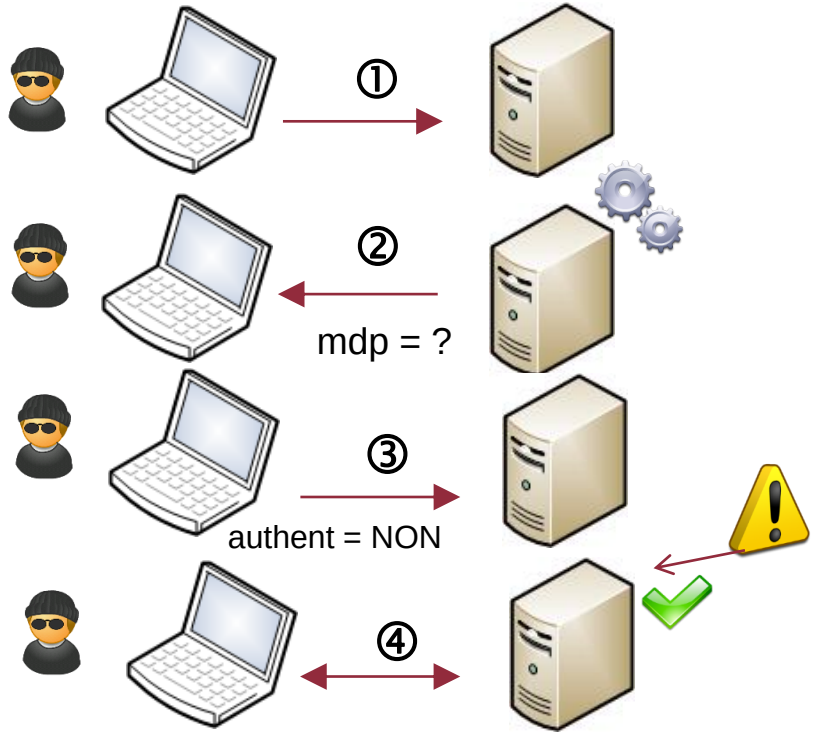
PARTIE 1

Illustration des notions Vulnérabilité, Menace et Attaque :
Cas pratique : Contournement de l'authentification dans l'application VNC

L'attaquant effectue une demande de connexion au serveur depuis son PC client.

Exploitation de la vulnérabilité présente dans l'application

L'attaquant choisit de s'authentifier avec le mécanisme de son choix, et non pas avec le mécanisme choisi par le serveur. Ici il choisit la méthode « pas d'authentification ».



Description du fonctionnement **modifié** par un attaquant.

Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat*, etc.) et envoie cette demande d'authentification à l'utilisateur demandeur.

Le serveur valide l'authentification (car elle est valide i.e. aucune authentification est une méthode valide) et autorise donc la connexion.

Référence : CVE-2006-2369

Remarque

- Contournement : solution temporaire apportée à un bug en attente de correctif. Elle permet d'atténuer les effets du bug et d'accomplir la tâche en cours

PARTIE 1

CHAPITRE 1

Définir la Cybersécurité

1. Définition de la Cybersécurité selon la norme ISO
2. Terminologie de la Cybersécurité
3. **Exemples des tactiques, techniques et procédures utilisées par les attaquants**

Menaces courantes:

Pour mieux se protéger, il est primordial de savoir à quoi s'attendre, et donc de connaître à minima les attaques informatiques les plus courantes.

En voici une liste non-exhaustive :

- Virus ;
- Hameçonnage & ingénierie sociale ;
- Fraude interne ;
- Déni de service distribué (DDoS) ;
- Menace persistantes évoluée ;
- Homme du milieu (MitM).

Menace persistante évoluée: Attaque prolongée et ciblée par laquelle une personne non autorisée accède au réseau et passe inaperçue pendant une longue période

Fraude interne: Tromperie ou dissimulation intentionnelle dans le but d'obtenir un gain financier personnel

Hameçonnage & ingénierie sociale : Tout contenu qui amène les utilisateurs à effectuer une action dangereuse, comme révéler des informations confidentielles ou télécharger un logiciel

Homme du milieu (MitM): Attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis

Déni de service distribué: Attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser

Virus : Programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire

Attaques sophistiquées sur les objets connectés:

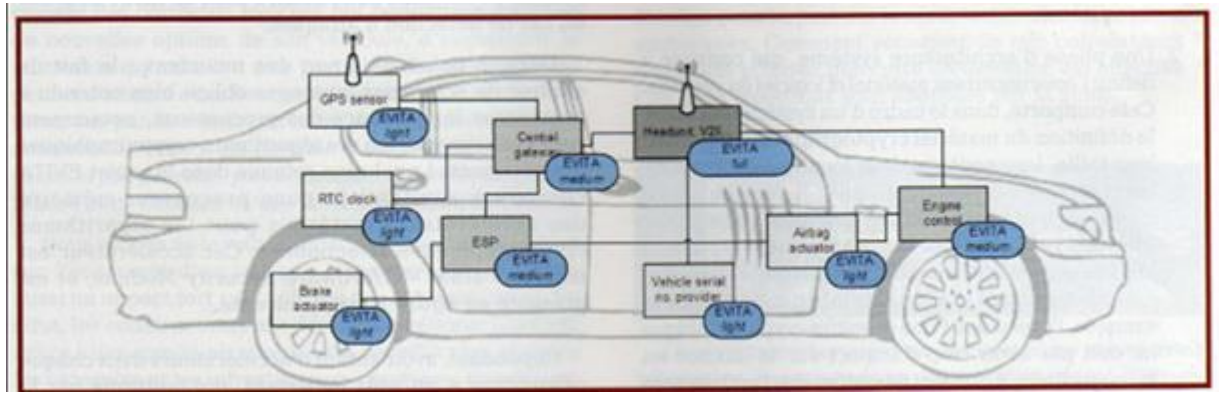
Les objets connectés sont des appareils reliés à Internet par un protocole de communication pour informer l'utilisateur de leur état. Ils sont présents dans l'ensemble des secteurs.

Exemples : **Attaques sur une voiture connectée**

De plus en plus de données sensibles sont générées par les voitures, qui font face à des menaces courantes dans l'informatique, comme les ransomwares ou les attaques contre des serveurs Web.

Exemple : Prise de contrôle du système de frein.

Deux chercheurs en sécurité ont réussi à prendre le contrôle complet, à distance, d'une Jeep Cherokee.

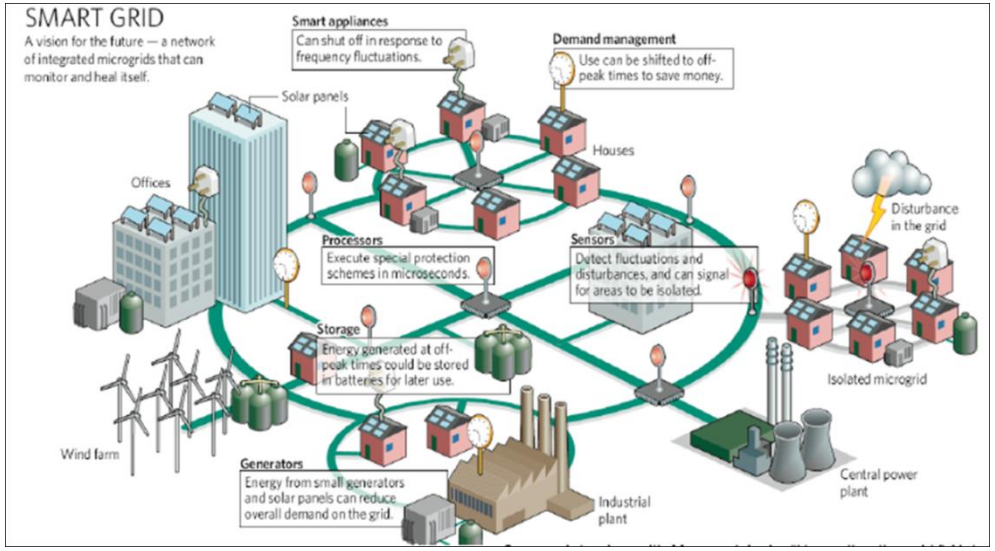


Attaques sophistiquées sur les objets connectés:

Smart Grid (Réseau intelligent) : Réseau de distribution d'électricité qui favorise la circulation d'information entre les fournisseurs et les consommateurs afin d'ajuster le flux d'électricité en temps réel et d'en permettre une gestion plus efficace.

Exemple : Blackout sur une grille.

Des compteurs intelligents au smart grid en passant par les systèmes de contrôle industriel, le secteur électrique repose de plus en plus sur l'informatique et l'échange de données entre un nombre croissant d'acteurs. Gage d'efficience, cette informatisation engendre de nouveaux risques, à l'image du blackout qu'ont subi des centaines de milliers d'ukrainiens en 2015. En Suisse, comme ailleurs, le défi consiste à élever le niveau général de sécurité d'une branche particulièrement hétéroclite.



PARTIE 1

CHAPITRE 2

Connaitre les objectifs de la Cybersécurité

Ce que vous allez apprendre dans ce chapitre :

- Comprendre la posture défensive
- Comprendre la posture offensive
- Identifier les enjeux d’une politique de sécurité des SI

3 heures

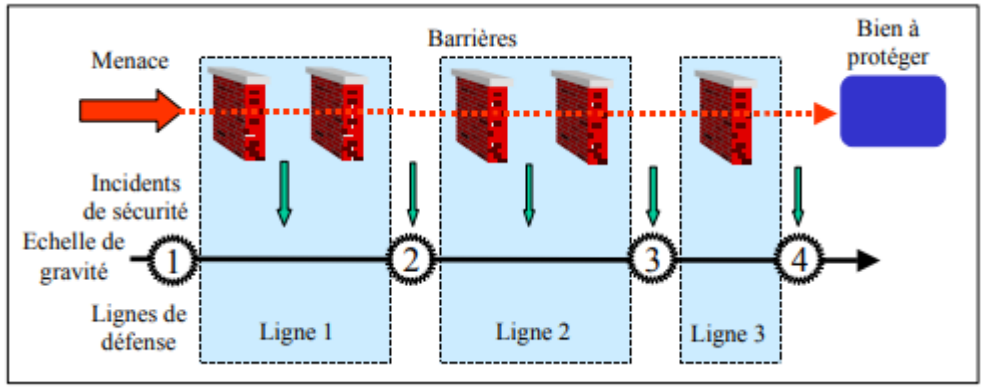
CHAPITRE 2

Connaitre les objectifs de la Cybersécurité

1. **Posture défensive**
2. Posture offensive
3. Enjeux d’une politique de sécurité des SI

Définition - La défense en profondeur

- La posture défensive se focalise sur des mesures réactives, telles que l'application de correctifs logiciels et la recherche et la remédiation des vulnérabilités du système.
- La défense en profondeur (DEP) est une doctrine de Cybersécurité dans laquelle une série de mécanismes défensifs sont superposés afin de protéger des données et des informations précieuses. Si un mécanisme échoue, un autre intervient immédiatement pour déjouer une attaque.
- Le concept de défense en profondeur a été conçu à l'origine par la National Security Agency (NSA) des États-Unis et tire son nom d'une stratégie militaire courante. Une stratégie de cybersécurité de défense en profondeur est similaire aux défenses en couches d'un château médiéval avec des douves, des ponts-levis, des tours, etc.
- Les éléments de la défense en profondeur :
  - Contrôles de sécurité réseau ;
  - Logiciels antivirus ;
  - Analyse de l'intégrité des données ;
  - Analyse comportementale.



PARTIE 1

Modèle "Zero Trust"

- La modèle "Zero Trust" est une stratégie de cybersécurité centrée sur les données pour l'informatique d'entreprise qui part du principe qu'aucun utilisateur final, aucun dispositif informatique, aucun service web ou aucune connexion réseau n'est fiable, même lorsqu'une demande d'accès provient du périmètre du réseau de l'entreprise.
- Parce que les acteurs malveillants peuvent exister à la fois à l'intérieur et à l'extérieur d'un réseau, le modèle "Zero Trust" soutient les principes suivants :
  - Ne jamais faire confiance ;
  - Toujours vérifier ;
  - Appliquer le principe du moindre privilège.

Exemples d'exercices de défense

Représentant la ligne de défense de l'entreprise, la **Blue Team** utilise les outils, protocoles, systèmes et autres ressources de sécurité pour protéger l'entreprise et identifier les failles dans ses capacités de détection. L'environnement de la Blue Team doit refléter le dispositif de sécurité actuel de l'entreprise, qui est susceptible de comporter des outils mal configurés, des logiciels non corrigés ou d'autres risques connus ou inconnus.

Exemples d'exercices de défense :

- Exécution d'une recherche DNS ;
- Analyse numérique visant à établir une ligne de base des activités réseau afin de repérer plus facilement les activités inhabituelles ou suspectes ;
- Audit, configuration et surveillance des logiciels de sécurité dans l'ensemble de l'environnement ;
- Vérification de la configuration et de la mise à jour des dispositifs de sécurité du périmètre, tels que les pare-feux, les antivirus et les logiciels antimalware ;
- Mise en œuvre du principe du moindre privilège, ce qui signifie que l'entreprise accorde le niveau d'accès le plus bas possible à chaque utilisateur ou terminal afin de limiter les déplacements latéraux sur le réseau en cas de compromission ;
- Mise en œuvre de la microsegmentation, une technique de sécurité qui consiste à diviser les périmètres en petites zones pour maintenir un accès séparé à chaque partie du réseau.

Remarque

Blue Team : un groupe est composé de consultants spécialisés dans la réponse à incident, qui conseillent l'équipe de sécurité informatique sur les améliorations à apporter pour bloquer les cyberattaques et menaces sophistiquées. L'équipe de sécurité informatique est ensuite chargée d'assurer la protection du réseau interne contre divers types de risques.

CHAPITRE 2

Connaitre les objectifs de la Cybersécurité

1. Posture défensive
2. **Posture offensive**
3. Enjeux d’une politique de sécurité des SI

02 – Connaitre les objectifs de la Cybersécurité

Posture offensive

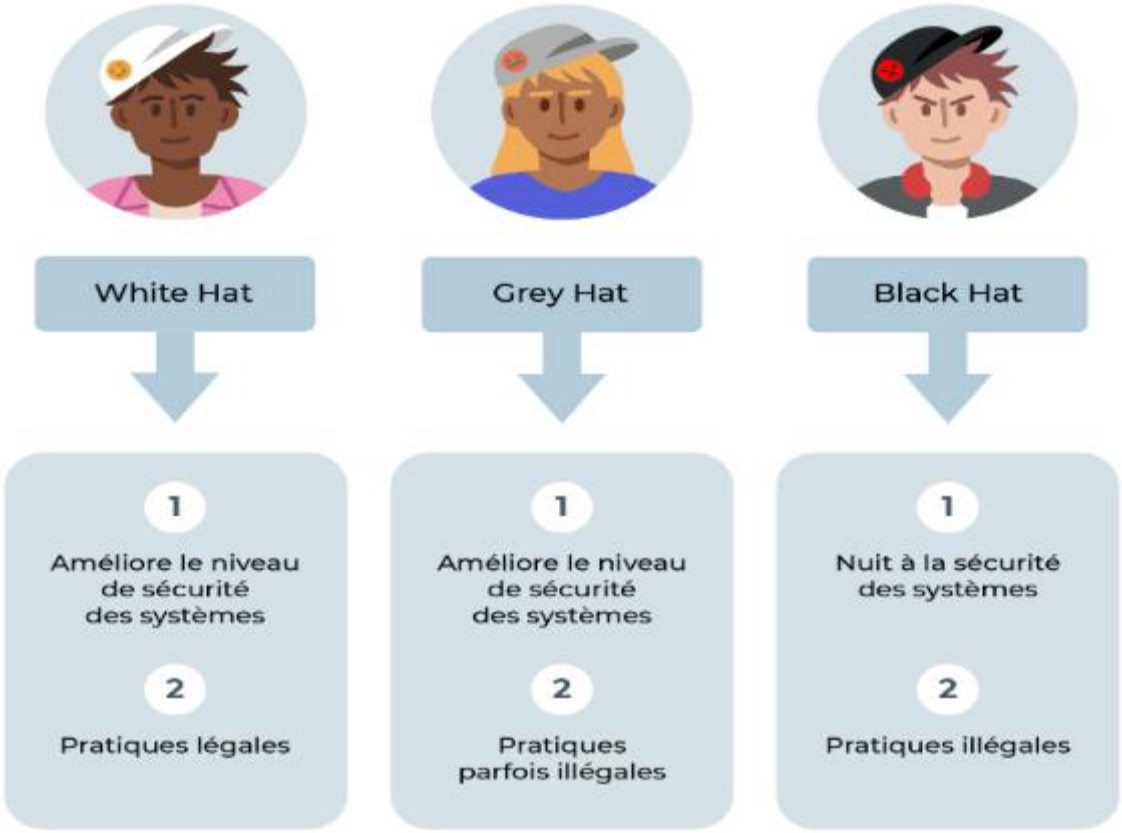
Définition

- La posture offensive est une approche proactive pour protéger les systèmes informatiques, les réseaux et les individus contre les attaques.
- La posture offensive consiste à attaquer son propre système pour en découvrir les points faibles et y apporter des solutions
- Types d'attaquants :
    - **Les White Hat (hackers bien intentionnés)** utilisent leur talent de hacker dans le but de défendre les entreprises, ce sont les professionnels de la sécurité informatique, les hackers éthiques qui attaquent, dans un cadre légal bien défini, un système d'information;
    - **Les Gray Hat** sont à la frontière de l'illégalité comme le disent certains, ils font des tests et préviennent leur cible par rapport aux failles découvertes pour correction avec un préavis avant divulgation;
    - **Les hackers sponsorisés,** à l'heure de la cyber-guerre, certains pays font souvent appel à ce groupe de hackers pour attaquer un autre pays, pendant que d'autres forment leurs propres éléments au besoin.
    - **Les script-kiddies** qui ne sont pas toujours formés et ont des connaissances peu approfondies en terme de sécurité et surtout de droit mais se contente de télécharger des outils sur internet pour faire leur test;
    - **Les Black Hat (hackers mal intentionnés)** très talentueux mais attaquent et cherchent à nuire. Dans le jargon, ils sont appelés "crackers".

PARTIE 1

PARTIE 1

Les 3 principaux types de hackers



Exemples d'activités de simulation d'attaque :

- **Test d'intrusion**, dans le cadre duquel un membre de la Red Team tente d'accéder au système à l'aide de diverses techniques réellement utilisées par les cyberadversaires ;
- **Tactiques d'ingénierie sociale**, qui visent à manipuler les collaborateurs ou d'autres membres du réseau pour qu'ils partagent, divulguent ou créent des identifiants réseau ;
- **Interception des communications** afin de cartographier le réseau ou d'obtenir plus d'informations sur l'environnement dans le but de contourner les techniques de sécurité courantes ;
- **Clonage** des cartes d'accès d'un administrateur pour accéder aux zones à accès restreint.

Red Team : équipe qui joue le rôle du cyberadversaire et tente d'identifier et d'exploiter les failles potentielles des cyberdéfenses de l'entreprise à l'aide de techniques d'attaque sophistiquées. Cette équipe offensive est généralement composée de professionnels de la sécurité chevronnés ou de cyberpirates éthiques indépendants qui exécutent des tests d'intrusion en imitant les techniques et méthodes d'attaque utilisées sur le terrain par les cyberadversaires.

Comparatif des deux approches

Grâce aux exercices Red Team / Blue Team, l'entreprise peut :

- Identifier les erreurs de configuration et les lacunes dans la protection offerte par les solutions de sécurité existantes ;
- Renforcer la sécurité du réseau afin de détecter les attaques ciblées et de réduire le temps de propagation ;
- Nourrir une saine concurrence entre les membres de l'équipe de sécurité et favoriser la coopération entre les équipes informatiques et de sécurité ;
- Sensibiliser ses collaborateurs aux risques liés aux vulnérabilités humaines susceptibles de compromettre la sécurité de l'entreprise ;
- Développer les compétences et la maturité des fonctions de sécurité de l'entreprise dans un environnement de formation sûr et à faible risque.

CHAPITRE 2

Connaitre les objectifs de la Cybersécurité

1. Posture défensive
2. Posture offensive
3. **Enjeux d’une politique de sécurité des SI**

PSSI, la politique de sécurité des systèmes d'information

- **Définition de l'ANSSI :**

« Une Politique de Sécurité des Systèmes d'Information (PSSI) reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration...) en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI. Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme. »

L'ANSSI complète cette vision en précisant que « *La PSSI vise à informer la maîtrise d'ouvrage et la maîtrise d'œuvre des enjeux tout en les éclairant sur ses choix en termes de gestion des risques et à susciter la confiance des utilisateurs et partenaires envers le système d'information. »*

Caractéristiques de la PSSI :

- Dimension stratégique ;
- Outil de communication ;
- Socle commun de mesures.

Remarques

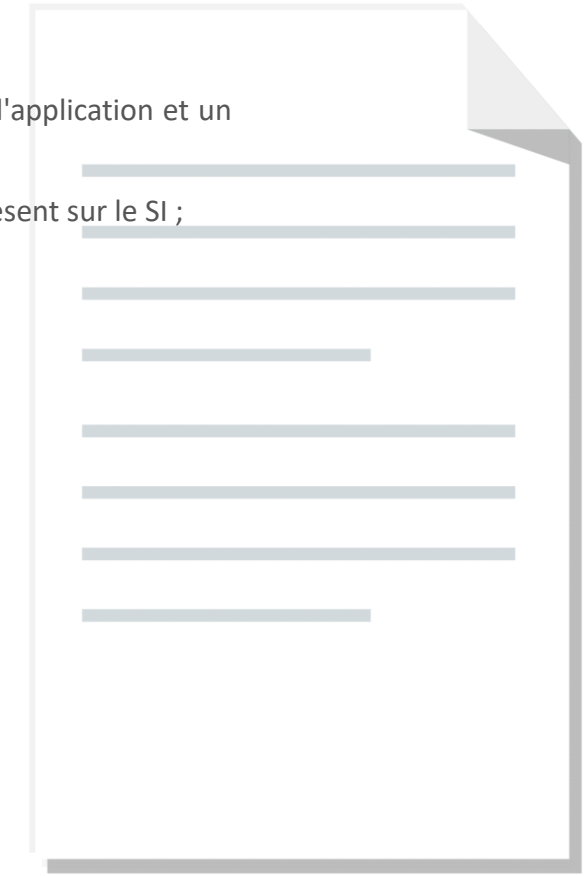
L'ANSSI est l'autorité nationale chargée d'assurer la sécurité des systèmes d'information de l'État Français et de contribuer à celle des opérateurs nationaux d'importance vitale (OIV).

PARTIE 1

Plan type de PSSI

On y trouve :

- La définition des enjeux d'une PSSI au regard de l'entreprise, son champ d'application et un inventaire des biens (physiques mais aussi organisationnels) à protéger ;
- Une analyse du contexte réglementaire de l'entreprise et des risques qui pèsent sur le SI ;
- La déclinaison des enjeux précédents en exigences et mesures de sécurité.



- Introduction
  - Note de cadrage
  - Mot de la direction
- Première partie
  - Enjeux de sécurité
  - Contraintes légales
  - Risques majeurs
- Deuxième partie
  - Exigences
  - Mesures de sécurité
- Annexes

PARTIE 2

Découvrir les différentes normes et standards de la Cybersécurité

Dans ce module, vous allez :

- Identifier les normes courante de la Cybersécurité
- Se familiariser avec les standards de gestion de vulnérabilités
- Appréhender les lois et les réglementations de Cybersécurité

7,5 heures

CHAPITRE 1

Connaitre les normes de la sécurité organisationnelle

Ce que vous allez apprendre dans ce chapitre :

- Découvrir la norme ISO 27001
- Découvrir la norme ISO 27005

2,5 heures

CHAPITRE 1

Connaitre les normes de la sécurité organisationnelle

1. **ISO 27001**
2. ISO 27005

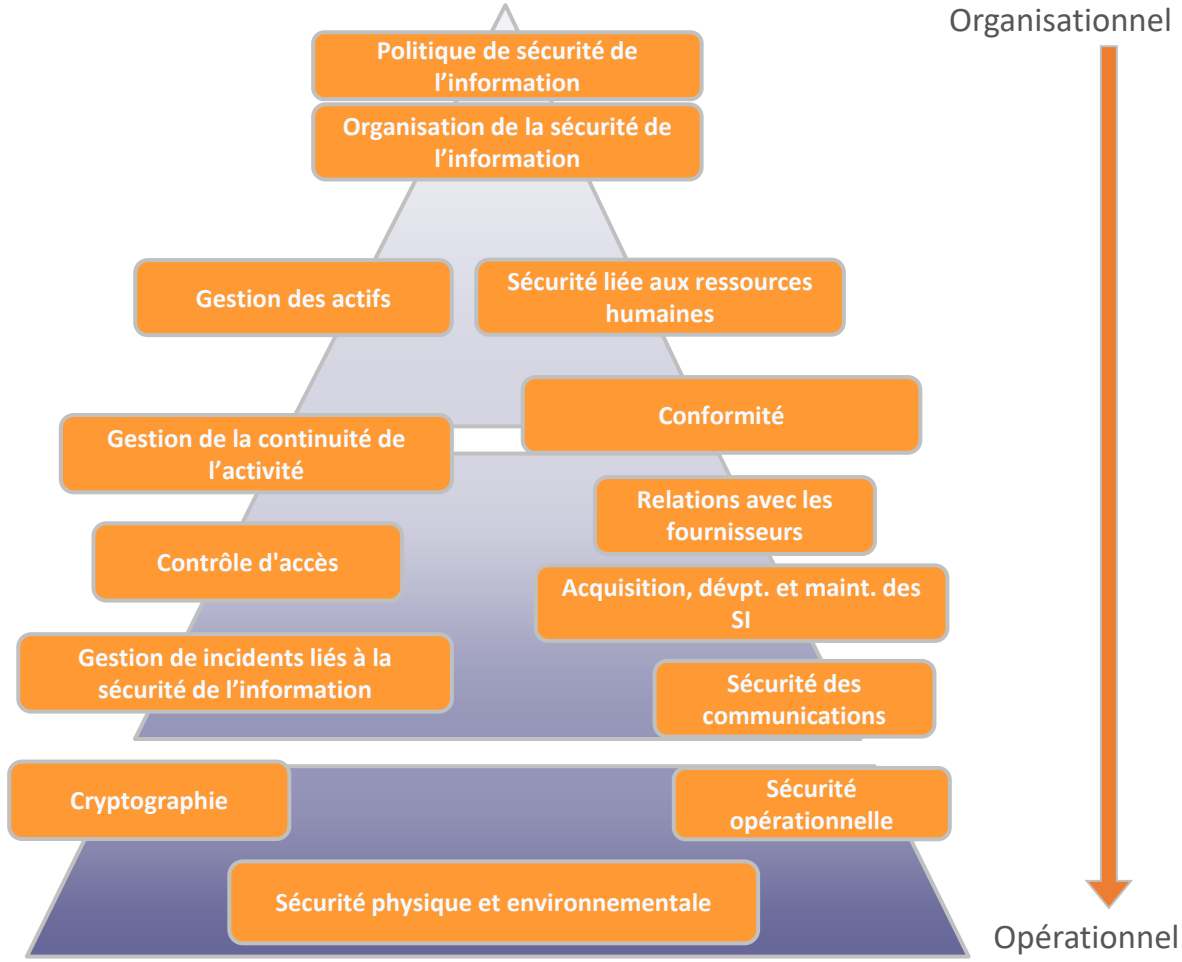
Descriptif de la norme

La famille de normes ISO 27000 est un recueil de **bonnes pratiques** dans le domaine de l'élaboration d'un **système de management de la sécurité des SI (SMSI) :**

Normes	Date et révision	Descriptif	Lien avec la PSSI
ISO 27001	2005 - 2013	Ce standard définit les exigences à mettre en place pour l'élaboration d'un système de management de la sécurité de l'information. Basé sur l'amélioration continue de type « roue de Deming » Plan / Do / Check / Act, il précise les points de contrôle à respecter et propose dans son annexe A 114 mesures issues de l'ISO 27002.	C'est la base pour la mise en place d'un SMSI (système de management de la sécurité de l'information).
ISO 27002	2005 - 2013	Ce standard présente un guide de bonnes pratiques à mettre en oeuvre pour des contrôles au regard des risques pesant sur l'information (confidentialité, intégrité et disponibilités). Il présente 114 mesures classées en 14 thèmes.	La méthodologie présentée dans le cours s'inspire directement des thèmes de l'ISO 27002 pour fixer les exigences et règles de sécurité.

ISO 27002 : Code de bonnes pratiques pour le management de la sécurité de l'information

- La norme ISO/IEC 27002:2013 constitue un code de bonnes pratiques. Elle est composée de 114 mesures de sécurité réparties en 14 chapitres couvrant les domaines organisationnels et techniques ci-contre.
- C'est en adressant l'ensemble de ces domaines que l'on peut avoir une approche globale de la sécurité des S.I.



PARTIE 2

CHAPITRE 1

Connaitre les normes de la sécurité organisationnelle

1. ISO 27001
2. **ISO 27005**

Gestion des risques (27005)

La norme 27005 présente **la démarche suivante :**

- Établissement du contexte de l'analyse des risques ;
- Définition de l'appréciation des risques SSI ;
- Choix pour le traitement du risque SSI ;
- Acceptation du risque ;
- Communication et concertation relative aux risques SSI ;
- Surveillance et revue du risque en SSI.

Remarques

- les méthodes EBIOS (Expression des besoins et identification des objectifs de sécurité) et MEHARI (méthode harmonisée d'analyse des risques) se basent de manière extensive sur la norme 27005

Avantages :

- Définit une démarche rationnelle qui a donné lieu à des méthodes qui fonctionnent ;
- Grande souplesse : utilisée en toutes circonstances, surtout lors des changements ;
- Pragmatique et utilisable seule, elle peut aussi bien convenir aux petites organisations.

Limites :

- L'organisation doit définir sa propre approche ;
- Méthodes nécessitant souvent de la formation et non adaptables à toutes les situations ;
- Dépendance vis-à-vis de la cartographie du SI : profondeur, étendue etc ;
- Tendance à l'exhaustivité ;
- Accumulation de mesures techniques sans cohérence d'ensemble.

Etapes de la démarche

Établissement du contexte
Il faut tout d'abord définir des critères :

- d'évaluation : seuil de traitement des risques, localement par actif menacé et globalement, pour toute l'organisation ;
- d'impact : seuil de prise en compte des risques ;
- d'acceptation : seuil d'acceptation des risques.

Appréciation des risques

- La première étape consiste à définir le contexte de la certification et les éléments qui le composent tels que l'organisme, le système d'information, les éléments essentiels à protéger les entités qui en dépendent et les différentes contraintes qui peuvent se présenter.

- Ensuite, il est nécessaire d'exprimer les besoins de sécurité des éléments essentiels et, identifier, caractériser en termes d'opportunités les menaces pesant sur le système d'information.

PARTIE 2

Etapes de la démarche

Traitement du risque

Pour définir les options de traitement, il faut mettre en adéquation le risque et le coût de traitement. Il existe quatre options du traitement du risque :

- Le refus ou l'évitement : le risque considéré est trop élevé, l'activité amenant le risque doit être supprimée ;
- Le transfert : le risque sera partagé avec une autre entité (un assureur, un sous-traitant) capable de le gérer ;
- La réduction : le risque doit être diminué. Il s'agit d'en réduire l'impact et/ou la potentialité de manière que le risque soit acceptable.
- Conservation du risque : le risque est maintenu tel quel.

Acceptation du risque

Il s'agit d'une homologation de sécurité effectuée par une autorité d'homologation désignée pour une durée déterminée. Cette homologation passe par l'examen d'un dossier de sécurité dont le contenu doit être défini : objectifs de sécurité, d'une cible de sécurité, politique de sécurité… La direction générale doit accepter les risques résiduels, donc accepter le plan de traitement du risque dans son ensemble.

Communication du risque

Il s'agit d'un échange et un partage régulier d'informations sur les risques entre le gestionnaire des risques, les décisionnaires et les parties prenantes concernant la gestion du risque.

Surveillance et réexamen du risque

Il faut s'assurer que le processus reste pertinent et adapté aux objectifs de sécurité des métiers de l'organisme. Il faut également identifier les changements nécessitant une réévaluation du risque ainsi que les nouvelles menaces et vulnérabilités.

CHAPITRE 2

Identifier les normes de la sécurité technique

Ce que vous allez apprendre dans ce chapitre :

- Découvrir les standards de gestion de vulnérabilités
- Se familiariser avec le référentiel OWASP

2 heures 30

CHAPITRE 2

Identifier les normes de la sécurité technique

1. **Standards de gestion de vulnérabilités (CVE, CVSS, CWE, NIST VDE, EXPLOIT-DB**
2. OWASP

PARTIE 2

Présentation des standards de gestion de vulnérabilités:

	CVE	CWE	CVSS
Nom complet	Common Vulnerabilities and Exposures	Common Weaknesses Enumeration	Common Vulnerabilities Scoring System
Description	Un dictionnaire de vulnérabilités et des expositions de sécurité connues publiquement	Un dictionnaire développé par la communauté des types de faiblesses logicielles	Une norme ouverte de l'industrie indépendante des fournisseurs conçue pour transmettre la gravité de la vulnérabilité
Liens	http://cve.mitre.org/index.html	https://cwe.mitre.org	http://www.first.org/cvss

Présentation des standards de gestion de vulnérabilités:

NIST NVD :

Référentiel du gouvernement américain des données de gestion de la vulnérabilité basées sur les normes, représentées à l'aide du Protocole d'automatisation du contenu de sécurité (SCAP). Ces données permettent l'automatisation de la gestion de la vulnérabilité, de la mesure de sécurité et de la conformité. Le NVD inclut des bases de données de références de liste de contrôle de sécurité, de défauts logiciels liés à la sécurité, de configurations erronées, de noms de produits et de mesures d'impact.

Lien : https://nvd.nist.gov/

EXPLOIT-DB :

Archive des exploits publics et des logiciels vulnérables correspondants, développés pour être utilisés par les testeurs de pénétration et les chercheurs sur la vulnérabilité. Son objectif est de constituer la collection la plus complète d'exploits, de shellcode et d'articles rassemblés par le biais de soumissions directes, de listes de diffusion et d'autres sources publiques, et de les présenter dans une base de données disponible et facile à naviguer. La base de données d'exploits est un référentiel pour les exploits et les preuves de concepts plutôt que des avis, ce qui en fait une ressource précieuse pour ceux qui ont besoin de données exploitables tout de suite.

Lien : https://www.exploit-db.com/

Exemples :

Vulnérabilité Heartbleed : Vulnérabilité critique dans la bibliothèque logicielle cryptographique populaire OpenSSL :

Classification

CWE CWE-200
CVE CVE-2014-0160
CVSS Base Score: **6.4** - AV:N/AC:L/Au:N/C:P/I:P/A:N
Access Vector: Network
Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: None

Vulnérabilité Apache Log4j : Une vulnérabilité a été découverte dans la bibliothèque de journalisation Apache log4j. Cette bibliothèque est très souvent utilisée dans les projets de développement d'application Java/J2EE ainsi que par les éditeurs de solutions logicielles sur étagère basées sur Java/J2EE.

CVE-2021-44832	Remote Code Execution
Severity	Moderate
Base CVSS Score	6.6 (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)
Versions Affected	All versions from 2.0-beta7 to 2.17.0, excluding 2.3.2 and 2.12.4

CHAPITRE 2

Identifier les normes de la sécurité technique

1. Standards de gestion de vulnérabilités (CVE, CVSS, CWE, NIST VDE, EXPLOIT-DB
2. **OWASP**

02 – Identifier les normes de la sécurité technique

OWASP

Présentation

- **L'Open Web Application Security Project (OWASP)** est une organisation à but non lucratif fondée en 2004 pour prévenir de manière proactive les attaques sur les applications web. Il s'agit du premier effort de normalisation des pratiques de développement sécurisé.

- Il y a dix types d'attaques qui sont spécifiés dans OWASP (Top 10, version 2017) :
  - L'injection ;
  - Le piratage de session ;
  - L'exposition de données sensibles ;
  - Les entités externes XML (XXE) ;
  - Le contournement des contrôles d'accès ;
  - Security misconfiguration ou mauvaise configuration de sécurité ;
  - Cross-Site Scripting (XSS) ou failles XSS ;
  - La désérialisation non sécurisée ;
  - L'utilisation de composants présentant des vulnérabilités connues ;
  - Le manque de surveillance et de monitoring.

PARTIE 2

Détails des Top 10 OWASP

1. **Injection :**

Une attaque par injection est une attaque permettant l'injection de **code arbitraire** dans l'application. Cela se produit lorsque des données non maîtrisées sont exécutées par le moteur présent sur le backend de l'application. Les données de l'attaquant sont exécutées **sans autorisations adéquates**.

L'injection de code non autorisée peut permettre à un attaquant d'accéder à des données auxquelles il n'a normalement pas accès.

2. **Piratage de session :**

Beaucoup d'applications exigent qu'un utilisateur se connecte pour arriver sur des pages auxquelles lui seul a accès. L'application est vulnérable à une attaque si un utilisateur malveillant peut obtenir un **accès non autorisé** aux mots de passe, clés et jetons pour pirater la session d'un autre utilisateur.

3. **Exposition de données sensibles :**

Les données stockées ou échangées via une application doivent être protégées pour éviter l'interception par une personne malveillante. Les bases de données qui enregistrent les données personnelles, les données de cartes de crédit, les noms d'utilisateur et les mots de passe représentent une cible de choix pour un pirate. Si ces données ne sont pas **chiffrées,** elles ne sont pas sécurisées et peuvent être récupérées lorsqu'elles sont en transit par exemple. L'utilisation de **techniques de chiffrement** et de pratiques de sécurité peut atténuer ce type d'attaques.

4. **Entités externes XML (XXE) :**

Le **format XML** permet de faciliter l'échange de données sous forme d'arborescence. Il est largement utilisé sur Internet. Il peut être exploité via l'injection XXE ou XML External Entity. XML External Entity est une attaque contre les applications qui parsent des entrées XML (exemple flux RSS). Cette attaque a lieu lorsque l'analyseur XML est mal configuré et contient une référence à une entité externe.

Détails des Top 10 OWASP

5. Contournement du contrôle d'accès :

Cette attaque vise les fonctionnalités des applications web qui nécessitent un **contrôle d'accès.** Dans ce cas, les pirates peuvent utiliser l'URL pour contourner l'authentification, par exemple. Ce type d'exploitation peut par exemple révéler comment une base de données est organisée.

6. Security Misconfiguration :

Une mauvaise configuration de sécurité est le plus souvent observée dans les en-têtes HTTP qui permettent de donner des indications sur la configuration du serveur, ou via la gestion des exceptions par défaut. Les codes d'erreur et les exceptions courantes peuvent donner à un attaquant un aperçu de l'application.

7. Cross-Site Scripting (XSS) :

Les **failles XSS** se produisent chaque fois qu'une application inclut des **données non fiables** dans une nouvelle page web sans validation ou échappement. Les failles XSS permettent aux attaquants d'exécuter des scripts dans le navigateur de la victime, ce qui peut détourner des sessions utilisateur, altérer des sites web ou rediriger l'utilisateur vers un site malveillant.

8. Désérialisation non sécurisée (Insecure Deserialisation) :

Une vulnérabilité de type "insecure deserialisation" permet à un utilisateur malveillant d'accéder et de modifier les fonctionnalités de l'application ciblée.

Détails des Top 10 OWASP

9. Utilisation de composants présentant des vulnérabilités connues :

Même si votre application est sécurisée, vous devez vous assurer que le framework, les bibliothèques, les appels API et la plateforme que vous utilisez ne sont pas vulnérables.

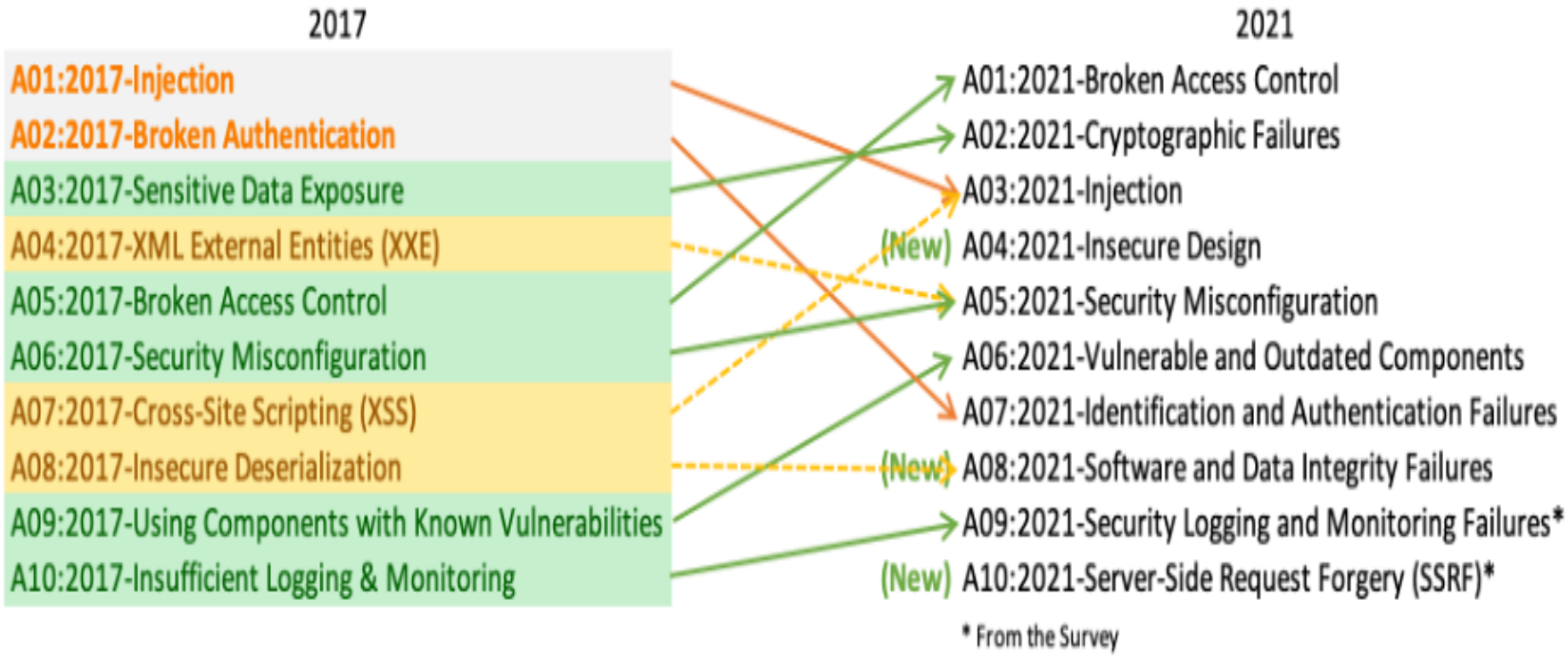
Lorsqu'une nouvelle vulnérabilité est découverte, un **correctif** est généralement proposé. Il faudra alors l'appliquer pour garantir la sécurité de l'application.

10. Manque de surveillance et de monitoring :

Pour garantir la sécurité d'une application, il est nécessaire de surveiller et de **monitorer** les connexions. De nombreux serveurs vulnérables servent de rebond aux attaquants. La mise en place de monitoring permettra de détecter une anomalie sur le serveur.

02 – Identifier les normes de la sécurité technique
OWASP

Nouvelle version 2021 du Top 10 OWASP :



PARTIE 2

CHAPITRE 3

Connaitre les référentiels réglementaires de la cybersécurité

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le règlement GDPR
- Découvrir la loi 09-08

2 heures 30 minutes

CHAPITRE 3

Connaitre les référentiels réglementaires de la cybersécurité

1. **RGDP**
2. Loi 09-08

Définition et périmètre

- Donnée personnelles : toute information se rapportant à une personne physique identifiée ou identifiable.
- Une personne peut être identifiée :
    - directement (exemple : nom, prénom) ;
    - ou indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).
- Traitement de données personnelles :
    - une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).
- RGPD :
    - Le sigle RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne ;
    - Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs ;
    - Le Règlement européen n° 2016/679, dit « Règlement général sur la protection des données » ou encore « RGPD » adopté le 27 avril 2016 et entré en application le 25 mai 2018.

Notions clés

- Responsable de traitement : personne physique ou morale, autorité publique, ou autre organisme qui détermine les moyens et les finalités d'un traitement, c'est à dire l'objectif et la façon de le réaliser.
- Sous-traitant : personne physique ou morale, autorité publique, ou autre organisme qui traite des données personnelles pour le compte du responsable de traitement.
- Quand et à qui s'applique le RGPD ?
    - Le RGPD s'applique à tous les organismes publics ou privés, quelque soient leur taille ou secteur d'activité (Administration, collectivité, entreprises, associations) :
        1. Établis sur le territoire de l'UE, que le traitement ait lieu ou non dans l'UE (critère de l'établissement).
        2. Établis hors UE, mais dont l'activité cible des personnes qui se trouvent dans l'UE et vise à leur offrir des biens ou des services ou à suivre leur comportement au sein de l'UE (critère du ciblage).
    - Le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier →Sont exclus les traitements effectués dans le cadre de politiques qui ne relèvent pas de la compétence de l'UE, ceux réalisés par des personnes physiques dans le cadre de leur vie privée et ceux réalisés par les autorités compétentes dans la sphère pénale.

CHAPITRE 3

Connaitre les référentiels réglementaires de la cybersécurité

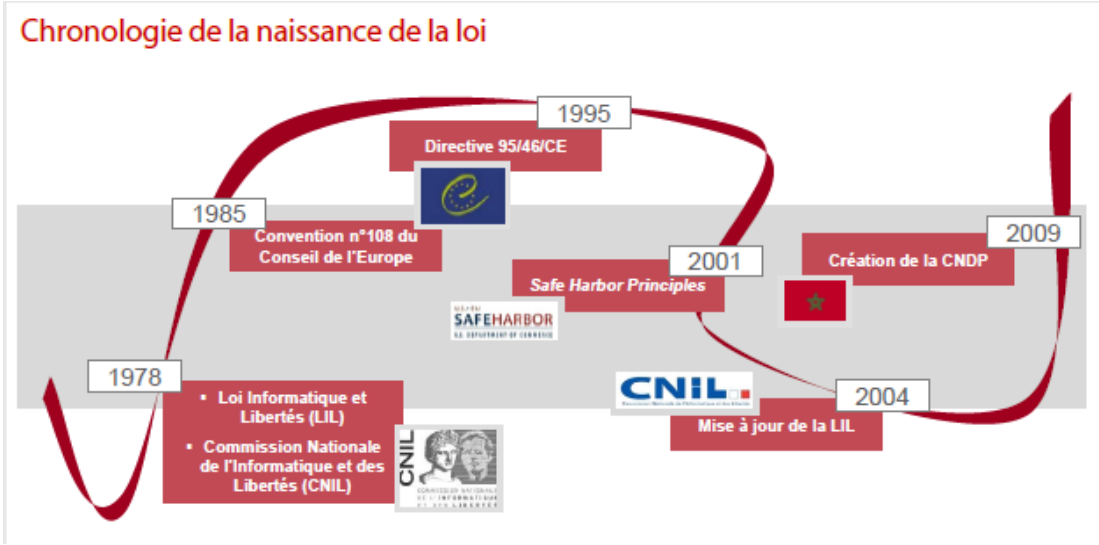
1. GDPR
2. **Loi 09-08**

03 – Connaitre les référentiels réglementaires de la Cybersécurité

Loi 09-08

Présentation:

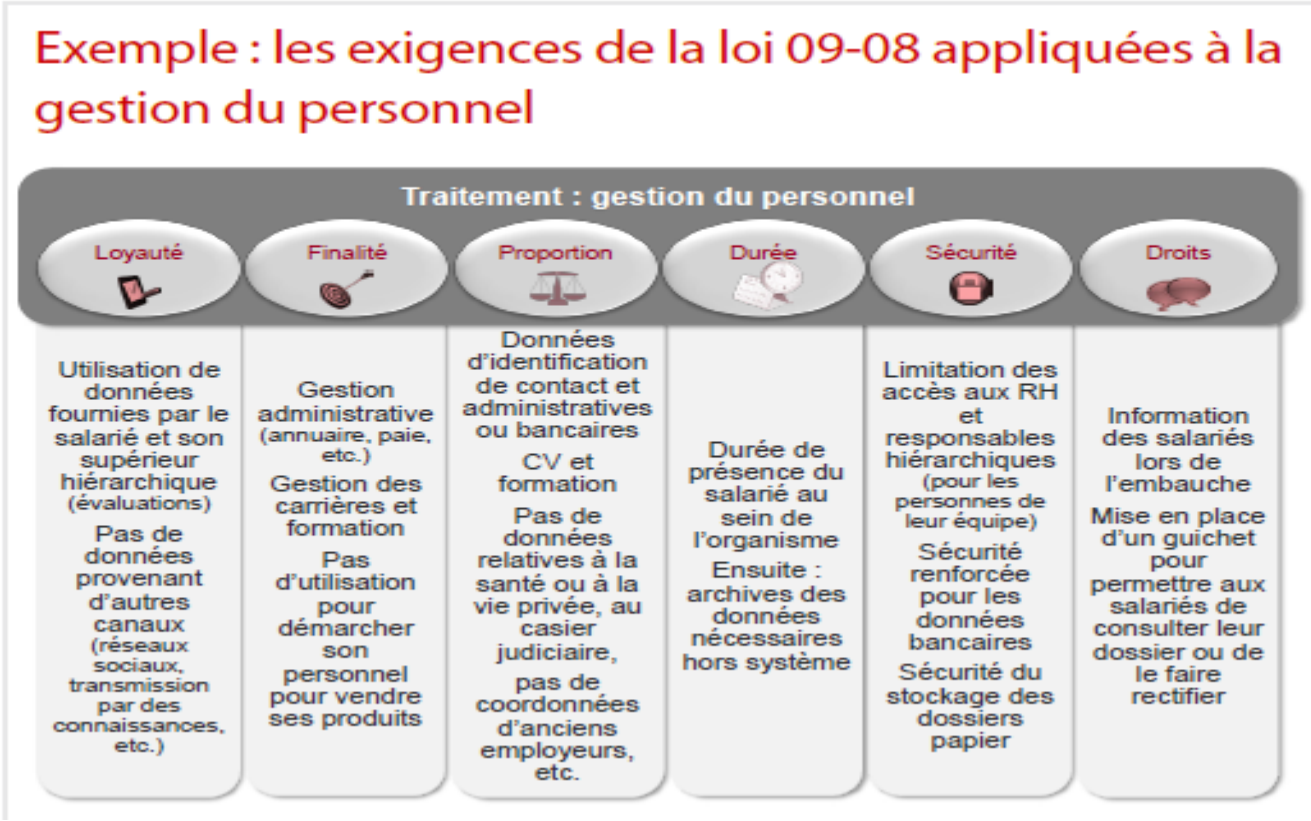
- Loi visant à assurer une protection efficace des particuliers contre les abus d'utilisation des données ;
- La Commission nationale de contrôle de la protection des données à caractère personnel ou CNDP est une commission marocaine, créée par la loi n°09-08 du 18 février 2009, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel2. Elle est chargée de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'homme ;
- La loi n° 09-08 relative à la «Protection des personnes physiques à l'égard du traitement des données à caractère personnel», adoptée en Février 2009 ainsi que l'article 24 de la constitution du 1er juillet 2011 entérinent désormais l'obligation pour les Dirigeants de tout mettre en œuvre pour garantir la conformité de leur organisme.



Source : Livre blanc AUSIM

PARTIE 2

Cas pratique



Source : Livre blanc AUSIM

PARTIE 2

PARTIE 3

Définir des critères de la Cybersécurité

Dans ce module, vous allez :

- Appréhender les critères de la Cybersécurité
- Identifier les niveaux de chaque critère

7 heures 30 minutes

CHAPITRE 1

Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le critère de la Disponibilité de l'information
- Comprendre le critère de la Confidentialité de l'information
- Comprendre le critère de l'Intégrité de l'information

4 heures

CHAPITRE 1

Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005

1. Disponibilité de l’information
2. Confidentialité de l’information
3. Intégrité de l’information

Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005

Disponibilité de l'information

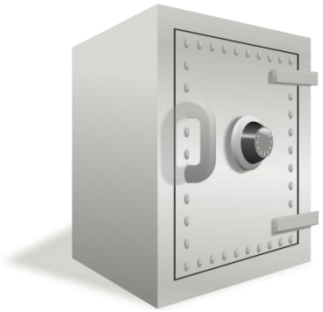
Définition

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Disponibilité:

Propriété d'accessibilité au moment voulu
des biens par les personnes autorisées (i.e. le bien
doit être disponible durant les plages d'utilisation prévues).

Bien à protéger



Mécanismes de sécurité pour atteindre les besoins de Disponibilité :

- Mise en place d'un système de clustering ;
- Mise en place d'un système d'équilibrage de charge ;
- Assurer la redondance de l'alimentation électrique ;
- Assurer la sauvegarde logicielle et des données ;
- Création d'un site de backup ;
- Avoir un plan de retour en arrière (fonction rollback) ;
- Activer la fonction failover sur les équipements.

PARTIE 3

CHAPITRE 1

Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005

1. Disponibilité de l’information
2. Confidentialité de l’information
3. Intégrité de l’information

Définition

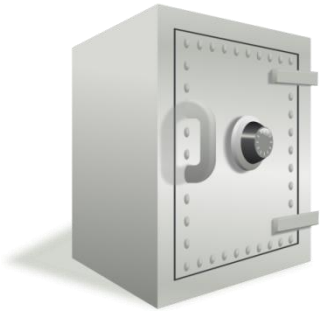
Confidentialité:

Propriété des biens de n'être accessibles qu'aux personnes autorisées.

Mécanismes de sécurité pour atteindre les besoins de Confidentialité :

- Chiffrement des données au repos (la base de données) ;
- Chiffrement des données en transit (TLS, PPTP, SSH, IPsec) ;
- Chiffrement du support physique ;
- Contrôle d'accès (physique et technique).

Bien à protéger



CHAPITRE 1

Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005

1. Disponibilité de l’information
2. Confidentialité de l’information
3. Intégrité de l’information

Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005
Intégrité

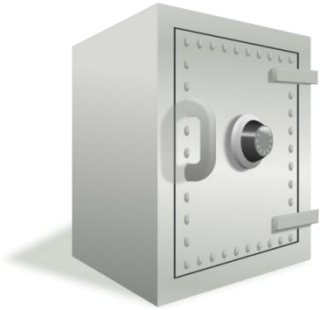
Définition

Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée).

Mécanismes de sécurité pour atteindre les besoins d'Intégrité:

- Hashing (intégrité des données) ;
- Gestion des configurations (intégrité système) ;
- Contrôle des changements (intégrité du processus) ;
- Contrôle d'accès (physique et technique) ;
- Signature numérique des logicielles ;
- Contrôle de redondance cyclique de transmission (CRC) sur les équipements.

Bien à protéger



PARTIE 3

CHAPITRE 2

Définir les niveaux de chaque critère

Ce que vous allez apprendre dans ce chapitre :

- Identifier les niveaux de la disponibilité de l'information
- Identifier les niveaux de l'intégrité de l'information
- Identifier les niveaux de la confidentialité de l'information

3 heures 30 minutes

CHAPITRE 2

Définir les niveaux de chaque critère

1. Niveaux de la Disponibilité de l’information
2. Niveaux de la Confidentialité de l’information
3. Niveaux de l’Intégrité de l’information

02 – Définir les niveaux de chaque critère

Disponibilité

Définitions et exemple

Disponibilité	Niveau	Définition
	4	Le bien ne peut pas être indisponible plus d'une heure
	3	Le bien ne peut pas être indisponible plus de 4 heures
	2	Le bien ne peut pas être indisponible plus d'une journée
	1	Le bien ne peut pas être indisponible plus d'une semaine

Disponibilité = **niveau 4 pour un site web**

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaitre ses services au public

PARTIE 3

CHAPITRE 2

Définir les niveaux de chaque critère

1. Niveaux de la Disponibilité de l’information
2. Niveaux de la Confidentialité de l’information
3. Niveaux de l’Intégrité de l’information

02 – Définir les niveaux de chaque critère

Confidentialité

Définitions et exemple

Confidentialité	Niveau	Définition
	4	Donnée secrète
	3	Donnée confidentielle
	2	Donnée à accès restreint
	1	Donnée interne
	0	Donnée publique

Confidentialité = **Niveau 0 d'un site web**

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

PARTIE 3

CHAPITRE 2

Définir les niveaux de chaque critère

1. Niveaux de la Disponibilité de l’information
2. Niveaux de la Confidentialité de l’information
3. Niveaux de l’Intégrité de l’information

02 – Définir les niveaux de chaque critère

Intégrité

Définitions et exemple

	Niveau	Définition
Intégrité	4	Aucune modification intempestive tolérée
	3	Toute modification intempestive doit être détectée et corrigée
	2	Toute modification intempestive doit être détectée
	1	Aucune exigence, la donnée peut être modifiée

Intégrité = **Niveau 4 d'un site web**

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable).

PARTIE 3

PARTIE 4

Découvrir les métiers de la Cybersécurité

Dans ce module, vous allez :

- Découvrir les domaines de la Cybersécurité
- Identifier les métiers de la Cybersécurité
- Se projeter sur les futurs métiers de la Cybersécurité

9 heures

CHAPITRE 1

Identifier les domaines de la Cybersécurité

Ce que vous allez apprendre dans ce chapitre :

- Identifier les domaines de la Cybersécurité
- Approfondir les caractéristiques de chaque domaine

3 heures 30 minutes

CHAPITRE 1

Identifier les domaines de la Cybersécurité

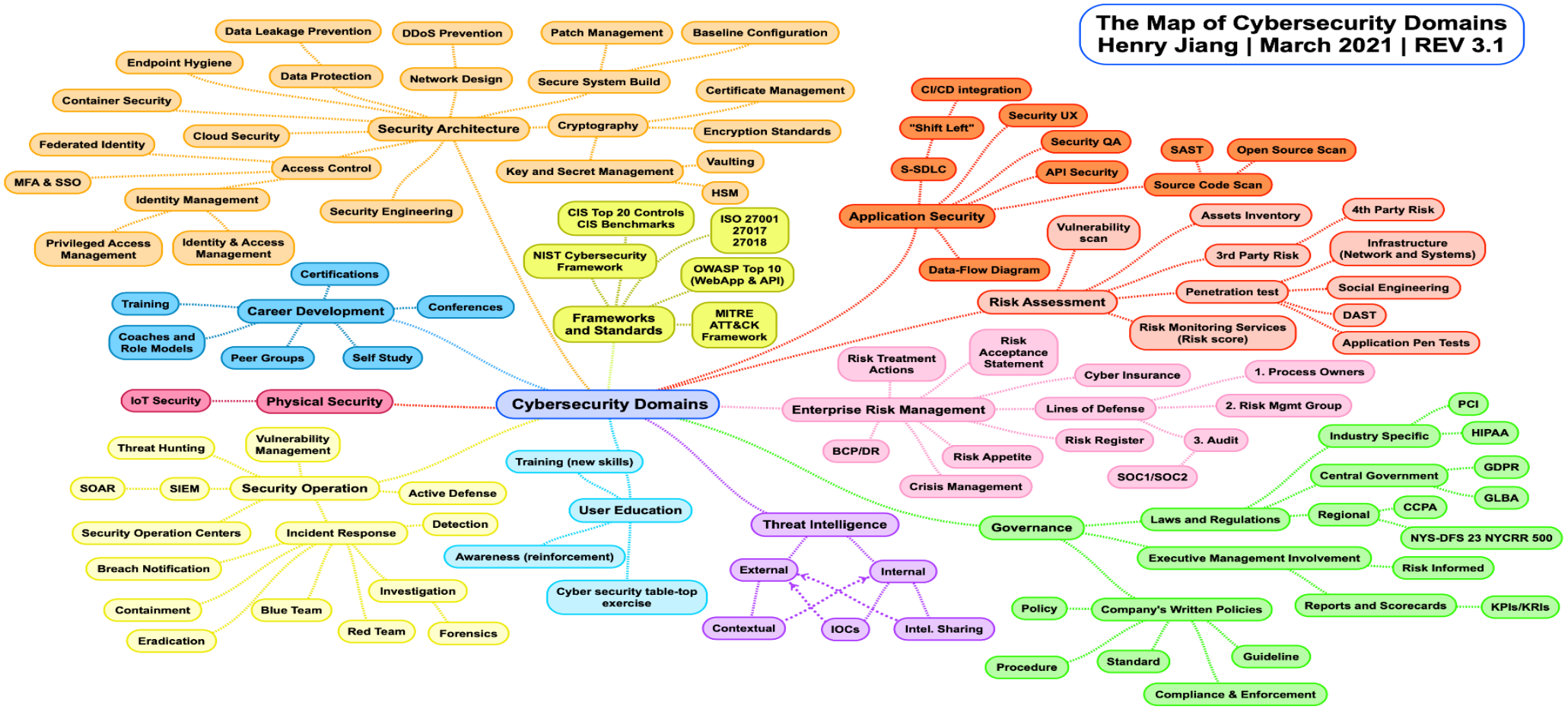
1. **Sécurité du développement**
2. Gouvernance
3. Gestion des risques
4. Sécurité physique

01 – Identifier les domaines de la Cybersécurité

Sécurité du développement

PARTIE 4

Domaines de la cybersécurité



Définitions et terminologie

La sécurité du développement (appelée aussi sécurité applicative) concerne les processus, outils et pratiques visant à protéger les applications contre les menaces tout au long de leur cycle de vie.

Qu'est-ce que le SAST :

Les tests statiques de sécurité des applications (SAST) analysent les fichiers source des applications, identifient avec précision l'origine des problèmes et facilitent la correction des failles sous-jacentes.

- Avantages des tests statiques de sécurité des applications pour les développeurs :
    - Identifier et éliminer les vulnérabilités dans le code source, binaire ou octet ;
    - Examen des résultats des analyses statiques en temps réel avec accès aux recommandations, navigation dans les lignes de code pour identifier plus rapidement les vulnérabilités et les audits collaboratifs ;
    - Pleinement intégré à l'environnement de développeur natif (IDE).

Définitions et terminologie

Qu'est-ce que le DAST ?

Les tests dynamiques de sécurité des applications (DAST) simulent des attaques contrôlées sur une application ou un service Web en cours d'exécution afin d'identifier les vulnérabilités exploitables dans un environnement en production.

- Avantages des tests dynamiques de sécurité des applications (DAST) :

    - Fournit un point de vue complet sur la sécurité applicative en se concentrant sur ce qui est exploitable et en couvrant tous les composants (serveur, code personnalisé, open source, services) ;
    - Peut être intégré au développement, à l'assurance qualité et à la production pour offrir une vue holistique en continu ;
    - L'analyse dynamique permet d'adopter une approche plus large de la gestion des risques pour le portefeuille (des milliers d'applications) et peut analyser les applications héritées dans le cadre de la gestion des risques ;
    - Teste les applications fonctionnelles, de sorte que contrairement au SAST, il n'est pas soumis à des contraintes de langage et permet d'identifier les problèmes liés à l'exécution et à l'environnement.

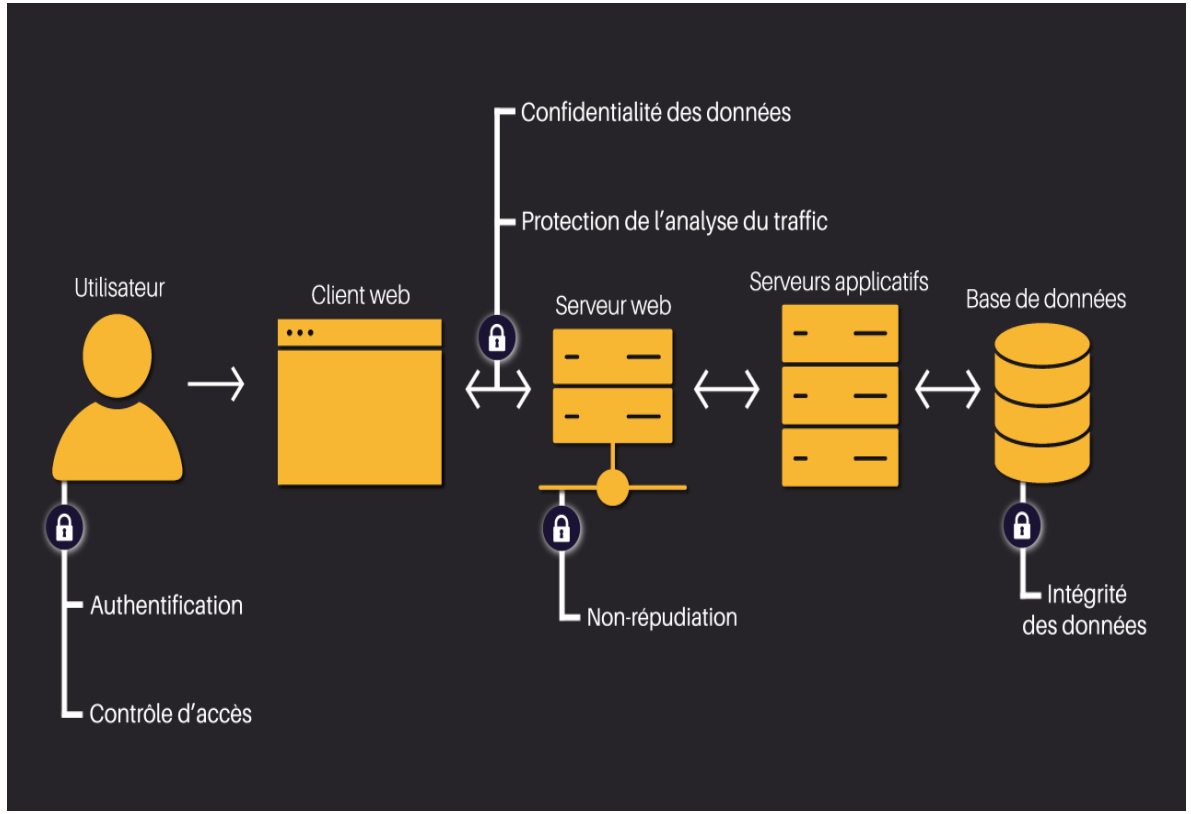
La sécurité dans une application web :

la sécurisation d'une application ou d'un système s'attache aux 6 aspects suivants :

•**L'authentification** :
• L'authentification consiste à savoir lier, grâce à une caractéristique discriminante (un mot de passe par exemple) une identité à une entité donnée d'un système (la partie administration d'un site, un processus en particulier ou 1 ordinateur par exemple). Elle s'applique à l'utilisateur, à l'émetteur d'un message ou à l'auteur d'un document.

•**Le contrôle d'accès** :
•Une fois authentifié, l'utilisateur souhaite accéder à des fonctionnalités offertes par l'application. Au préalable, il faut contrôler s'il a le droit d'y accéder. Assurer cette fonction c'est avoir la capacité de lier une ressource (une base de données par exemple) avec des droits d'accès à cette ressource et une entité.

•**La confidentialité** des données :
La confidentialité des données doit être assurée lors d'échange de données sensibles (mot de passe, données bancaires ou médicales.) Il s'agit de garantir que des données acquises illégalement soient inutilisables.



PARTIE 4

La sécurité dans une application web :

•La protection contre **l'analyse du trafic**:

La sécurité des communications repose sur des mécanismes déjà abordés et que nous approfondirons ensuite : mécanisme **d'authentification,** de **chiffrement** et de **hachage.** L'exemple le plus emblématique est l'utilisation des protocoles **SSL** (Secure Socket Layer) et **TLS** (Transport Layer Security) dans les échanges sur le Web grâce au protocole HTTPS dont vous avez évidemment entendu parler.

•**La non-répudiation** :

Cette fonction consiste à s'assurer que **l'envoi et la réception d'un message sont incontestables**. En d'autres termes, l'émetteur ou le récepteur d'une donnée ne doit pas être en mesure de nier son implication en cas de litige. Le moyen technologique repose sur les certificats, que nous verrons plus en détail plus loin dans le cours.

•**L'intégrité** des données ;

Il s'agit ici de prévenir l'altération volontaire ou accidentelle d'une donnée ou des services d'un système. Elle s'applique à la phase de **communication** entre composants, au **flux,** au **stockage** des données (altérations de contenu) et au **système** (détection d'intrusion).

CHAPITRE 1

Identifier les domaines de la Cybersécurité

1. Sécurité du développement
2. **Gouvernance**
3. Gestion des risques
4. Sécurité physique

01 – Identifier les domaines de la Cybersécurité

Gouvernance

Définition

- La gouvernance de la Cybersécurité, ou « cybersecurity governance » en anglais, relève de la responsabilisation des dirigeants de l'entreprise dans le choix des politiques de cybersécurité.
- La gouvernance de la sécurité de l'information a sa propre norme : **ISO/IEC 27014-2020.**
- L'organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC) définissent ainsi la gouvernance informatique comme « les concepts, objectifs et processus […] par lesquels les organisations peuvent évaluer, contrôler, surveiller et communiquer les processus relatifs à la sécurité de l'information ».

- **Activités de la gouvernance Cybersécurité :**
  - Élaboration de politiques, de normes et de processus de sécurité ;
  - Évaluation et gestion des risques de sécurité ;
  - Formation de sensibilisation à la sécurité ;
  - Assurance de sécurité des tiers et des fournisseurs ;
  - Rapport des tableaux de bord de sécurité.

PARTIE 4

CHAPITRE 1

Identifier les domaines de la Cybersécurité

1. Sécurité du développement
2. Gouvernance
3. **Gestion des risques**
4. Sécurité physique

Approche par l'analyse et le traitement du risque

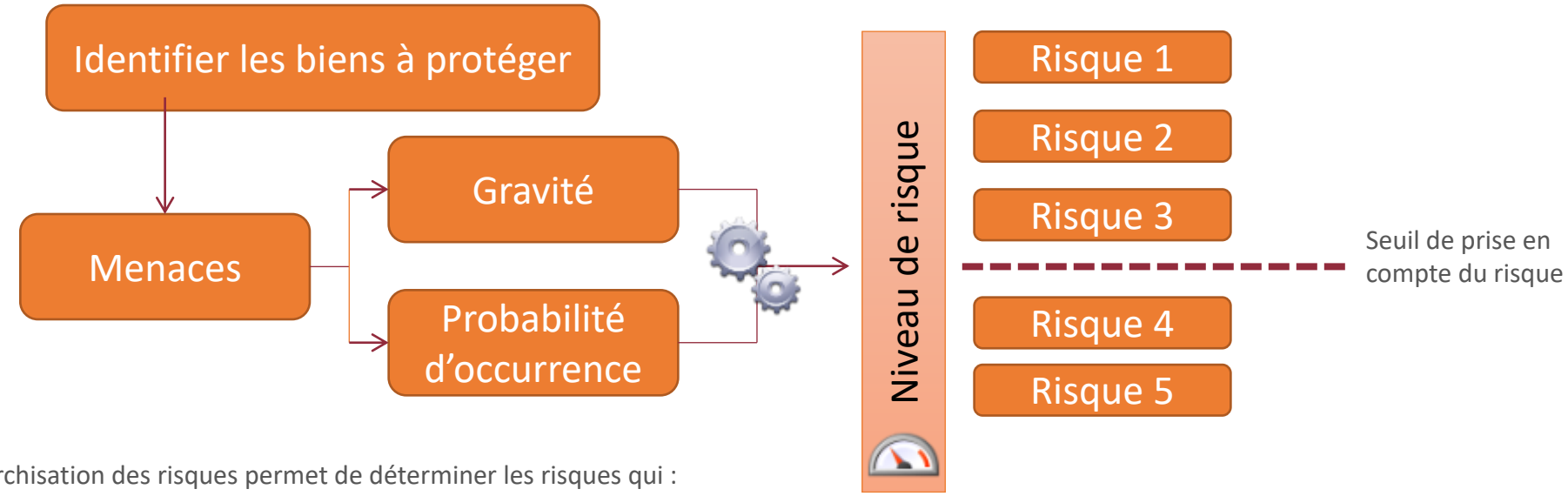
- L'analyse de risques doit être effectuée en amont du projet mais doit aussi évoluer au fur et à mesure de l'exploitation du système (analyse de risque dynamique dans la supervision du système (SOC)) et fonction de l'évolution des risques (évolution des vulnérabilités, des menaces, du système d'information).

- L'analyse de risque consiste à :
    - identifier les biens à protéger ;
    - analyser de la fréquence et la gravité du danger pour évaluer la criticité du risque ;
    - établir une hiérarchisation des risques : fréquence vs gravité ;
    - établir un seuil d'acceptabilité pour chacun de ces risques ;
        - seuil au-delà duquel le risque doit être pris en compte par les mesures de sécurité
    - identifier des mesures de sécurité.

Les mesures ainsi identifiées peuvent constituer un cahier de charges sécurité pour le projet qui soit réalisé en interne ou externalisé.

Approche par l'analyse et le traitement du risque

- Une démarche d'analyse de risque peut être schématisée ci-dessous :

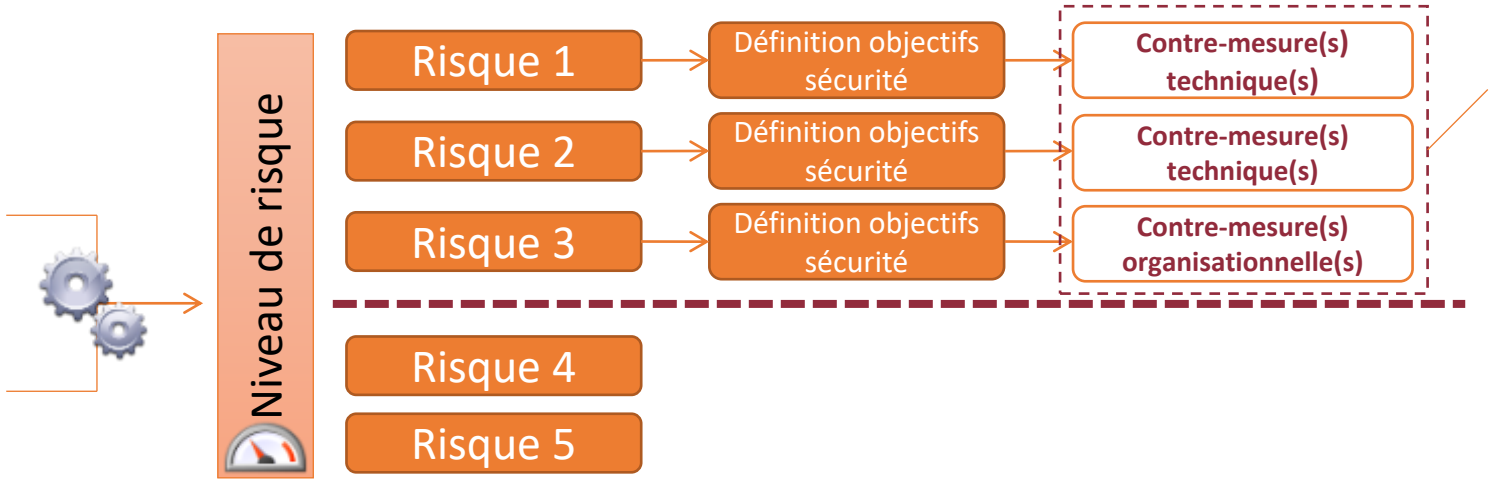


- La hiérarchisation des risques permet de déterminer les risques qui :
  - doivent absolument être traités et donc réduits par des mesures ;
  - ceux qui sont acceptables et avec lesquels le système peut exister.

PARTIE 4

Approche par l'analyse et le traitement du risque

- Pour les risques dont le niveau est supérieur au seuil de prise en compte :
  - Définir les objectifs de sécurité ;
  - Définir les mesures techniques et organisationnelles qui vont permettre d'atteindre ces objectifs.
- Pour les risques dont le niveau est inférieur au seuil de prise en compte :
  - un risque résiduel est le risque subsistant après le traitement de risque (car – par exemple – le coût pour compenser ce risque est trop élevé par rapport au risque encouru).



PARTIE 4

Approche par l'analyse et le traitement du risque

Une analyse de risque peut être assez complexe et nécessite rigueur et méthode, il faut notamment trouver le bon niveau d'abstraction.

Voici 3 exemples de méthodes d'analyses de risque compatibles avec les lignes directrices de l'ISO 27005 :

- **EBIOS :** Expression des Besoins et Identification des Objectifs de Sécurité
    - développée par le Club EBIOS auquel participe l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information
- **MEHARI :** Méthode Harmonisée d'Analyse de Risques
    - développée par le CLUSIF, Club de la Sécurité de l'Information Français
- **OCTAVE :** Operationally Critical Threat, Asset, and Vulnerability Evaluation
    - développée par l'Université de Carnegie Mellon

CHAPITRE 1

Identifier les domaines de la Cybersécurité

1. Sécurité du développement
2. Gouvernance
3. Gestion des risques
4. **Sécurité physique**

Définition

- La sécurité physique est la protection du personnel, du matériel, des logiciels, des réseaux et des données contre les actions physiques et les événements qui pourraient causer des pertes ou des dommages graves à une entreprise, une agence ou une institution. Cela comprend la protection contre les incendies, les inondations, les catastrophes naturelles, le cambriolage, le vol, le vandalisme et le terrorisme.
- La sécurité physique est composée de trois catégories :
    - Le contrôle d'accès : dispositif permettant un accès contrôlé à un lieu, un bâtiment, un local, une machine ou des équipements spécifiques (comme un coffre ou un véhicule).
    - La surveillance : dispositif permettant au personnel de sécurité de détecter et de localiser les intrus potentiels à l'aide d'équipements de surveillance tels que des caméras, des détecteurs de mouvement, des lumières de sécurité et du personnel comme des agents de sécurité et des chiens de garde.
    - Les tests : méthode d’évaluation du niveau de sécurité – sûreté des bien physiques.

Sécurité des locaux

- **Protéger physiquement les locaux contenant les biens sensibles :**
  - Contrôler l'accès aux locaux : usage de badges par exemple ;
  - Utiliser des alarmes pour identifier les intrusions ;
  - Protéger les clés ou badges dans des coffres par exemple.

- **Les prises d'accès réseau doivent être protégées de manière à être inaccessibles aux visiteurs/personnes mal intentionnées :**
  - Si les prises d'accès réseau doivent être exposées, ne pas les connecter au réseau. Mais plutôt le faire au besoin et désactiver ensuite.

- **Protéger contre les incidents environnementaux :**
  - Incendie : extincteur, détecteur de fumée, etc ;
  - Inondation : s'installer en zone non inondable, surélever les éléments, etc ;
  - Panne électrique : utiliser des onduleurs, etc.

Sécurité des équipements

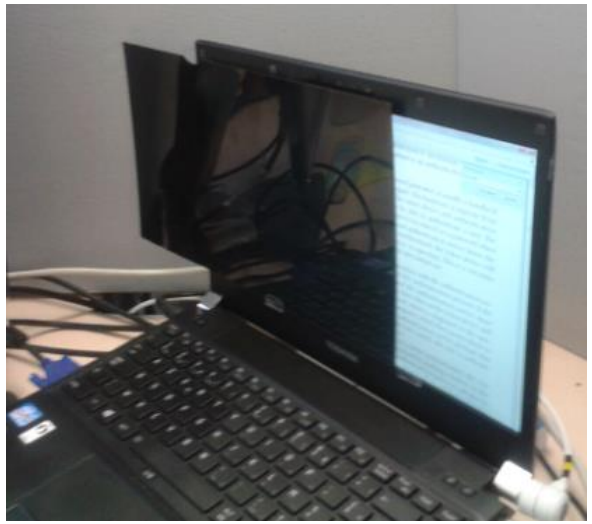
- **Attacher avec un câble de sécurité les équipements le permettant**

- **Protéger l'accès aux équipements :**
  - Avoir un code/mot de passe pour restreindre l'accès à son équipement :
    - lecteur d'empreinte ou signe sur téléphone ;
    - code PIN ou mot de passe ;
  - Demander un code/mot de passe pour sortir de la veille.

- **Verrouiller son écran en cas d'inactivité de quelques minutes**

- **Faire attention aux médias USB :**
  - Des clés USB piégées sont parfois offertes ou abandonnées ;
  - Toujours scanner (anti-virus) une clé USB avant de l'utiliser.

- **Utiliser les filtres de confidentialité d'écran :**
  - Écran d'ordinateur (fixe, portable) ;
  - Écran de téléphone.



CHAPITRE 2

Découvrir le référentiel métier de l'ANSSI

Ce que vous allez apprendre dans ce chapitre :

- Comprendre les métiers de a Cybersécurité
- Se focaliser sur les métiers Analyste SOC et Pentester

3 heures 30 minutes

CHAPITRE 2

Découvrir le référentiel métier de l’ANSSI

1. **Analyste SOC**
2. Pentester

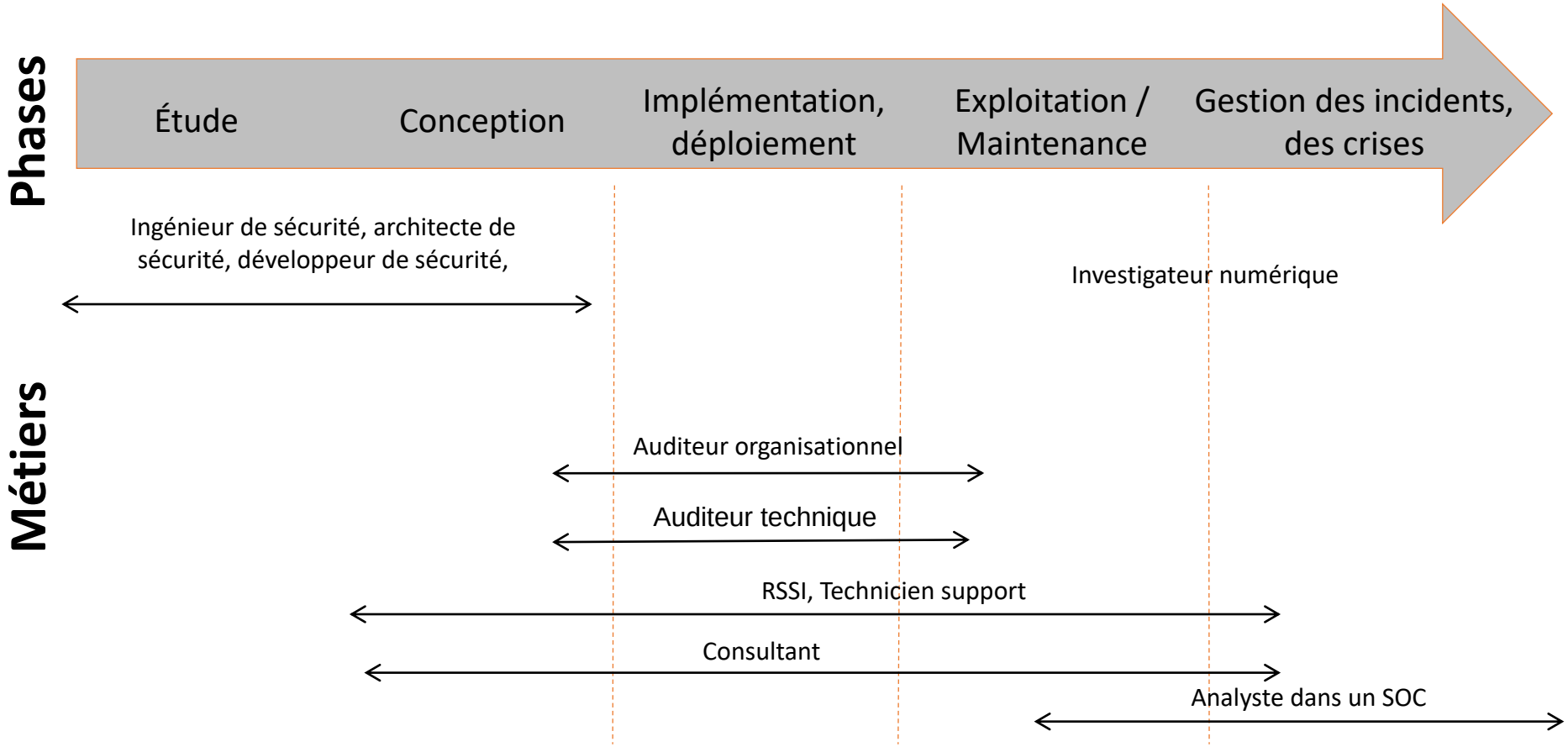
Principales fonctions

- Paramètre les systèmes de supervision de la sécurité (SIEM, sondes, *honeypots*, équipements filtrants). Catégorise, analyse et traite les alertes de sécurité de façon régulière pour en améliorer l'efficacité. Assure la détection, l'investigation et la réponse aux incidents de sécurité.

- L'analyste SOC analyse et interprète les alertes, les événements corrélés et recherche les vulnérabilités.

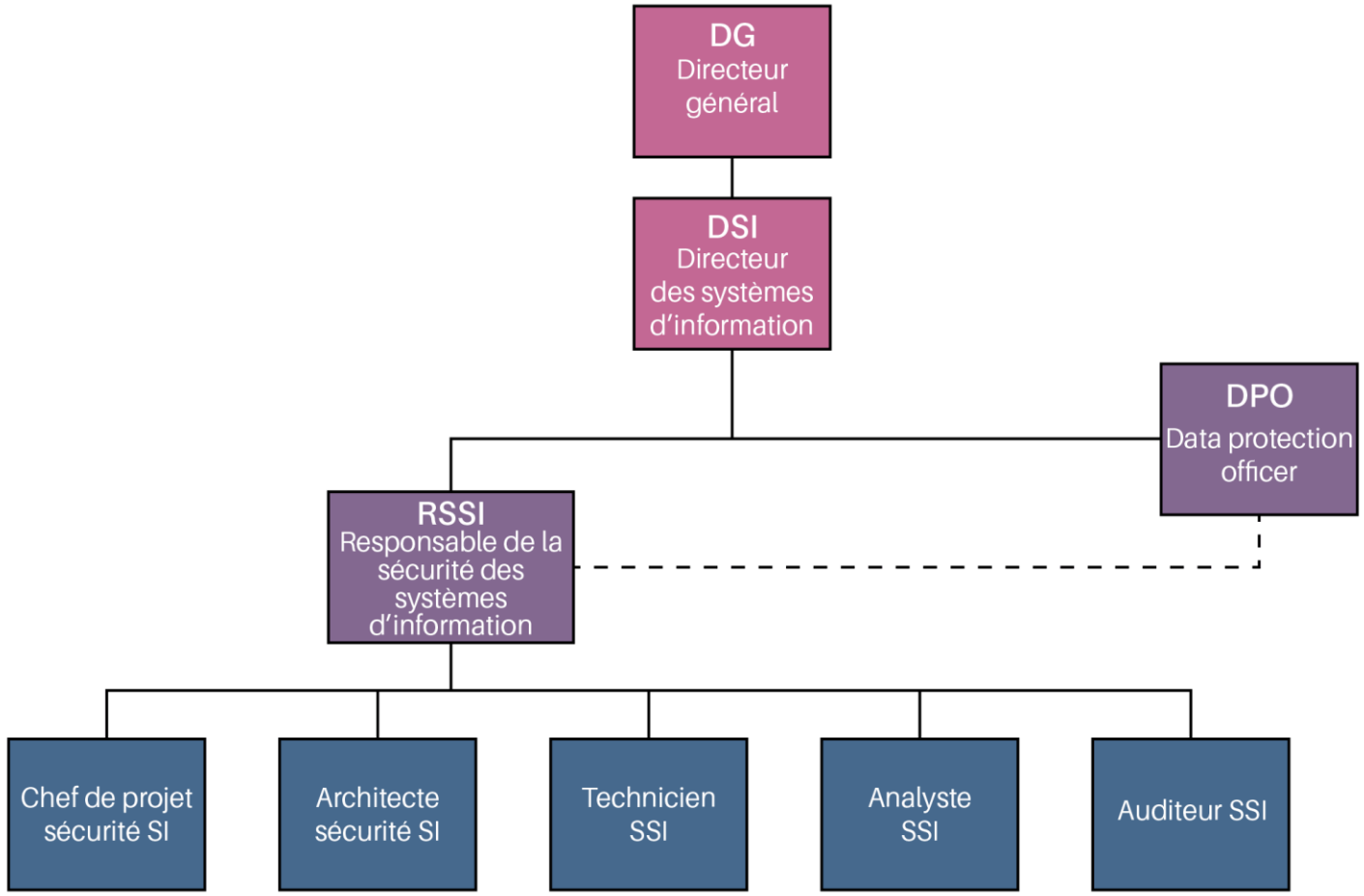
- **Compétences/Qualités nécessaires pour devenir analyste SOC :**
  - Maîtrise des techniques d'intrusion et de corruption des SI ;
  - Connaissance des règles de sécurité des systèmes d'information ;
  - Autonomie et organisation ;
  - Capacité d'analyse et de synthèse ;
  - Rigueur, sens de la méthode ;
  - Qualité rédactionnelle ;
  - Communication et expression orale.

Cartographie des métiers et compétence en SSI



PARTIE 4

Vue d'ensemble



Autres métiers de la cybersécurité

Le RSSI :

Cette personne est responsable de la sécurité des systèmes d'information. Elle manage tout le département sécurité. C'est donc un poste important, car il s'agit de communiquer directement ses résultats à la DSI voire au DG de l'entreprise dans certains cas. Cela veut aussi dire qu'en cas d'incident de sécurité majeur, vous pourriez bien être la première personne licenciée.

Le chef de projet sécurité SI :

Il développe ou supervise l'évolution d'un élément de la sécurité informatique de l'entreprise. C'est le métier le plus polyvalent, comme en général tous les métiers de "chef de projet". Il peut aussi consister à passer des commandes auprès des **ESN** (Entreprises de Services Numériques, ou SSII).

L'architecte sécurité SI :

Il prend en charge la cartographie de la sécurité de l'entreprise et conçoit les choix techniques en matière de sécurité.

Le technicien SSI :

C'est probablement le métier le plus opérationnel de tous, qui consiste à mettre en œuvre les configurations des applications et des réseaux, leur chiffrement, etc. Il nécessite un niveau Bac+2 en général.

Les métiers

L'analyste SSI :

Il travaille généralement à anticiper les menaces, en effectuant de la veille technologique. Lorsqu'un incident a eu lieu, c'est lui qui analyse l'étendue des dégâts et cherche le moyen de réparer la faille.

L'auditeur SSI :

Il teste la sécurité du système d'information d'une entreprise. Il peut intervenir en tant qu'élément externe ou interne à l'entreprise. C'est notamment lui qui va réaliser du *pentesting* (tests d'intrusion), en simulant des attaques pour vérifier si l'entreprise est suffisamment protégée.

Le DPO :

Enfin, le DPO (Data Protection Officer) est à la frontière entre la sécurité et le juridique. C'est un nouveau type de métier transverse, né avec la réglementation GDPR qui donne plus de responsabilités aux entreprises pour la protection des données qu'elles traitent. En cas de brèche de données, le DPO est le point de contact entre l'entreprise et l'autorité de contrôle (comme la CNDP).

CHAPITRE 2

Découvrir le référentiel métier de l'ANSSI

1. Analyste SOC
2. **Pentester**

02 – Découvrir le référentiel métier de l'ANSSI

Pentester

Fiche métier

- Le terme vient de la contraction de « penetration test » qui signifie « test d'intrusion ». Le pentester a donc la responsabilité de réaliser un pentest, une technique qui consiste à repérer les failles de sécurité en imitant les méthodes des hackers. C'est un métier très important dans la cybersécurité, puisqu'il permet d'anticiper les problèmes et de prioriser les décisions
- **Compétences nécessaires :**
    - Compétences en codage en plusieurs langages ;
    - Connaissance approfondie de la sécurité de l'information ;
    - Informatique légale et analyse numérique ;
    - Comprendre comment les violations affectent les organisations ;
    - Être un communicateur clair ;
    - Comprendre le facteur humain ;
    - Être capable de planifier et de créer des tests d'intrusion ;
    - La capacité de tester, tester, tester car ce sera une grande partie de votre travail quotidien.

Fiche métier

- **Missions**

Le pentester doit remplir différentes missions dans le cadre de son activité, mais il est possible de résumer son rôle en 3 axes majeurs :

- Contrôler la fiabilité des systèmes d'information : les vulnérabilités et les failles doivent être identifiées grâce aux tests pour éviter les intrusions non contrôlées dans les SI de l'entreprise ;
- Résoudre les failles : une fois les risques identifiés, des solutions doivent être trouvées et mises en place pour les résoudre. La sécurité de l'infrastructure informatique doit être renforcée et optimisée ;
- Conseiller : le métier de pentester inclut un rôle de conseiller, car il faut également expliquer les bonnes pratiques aux entreprises pour anticiper les menaces. Il pourra également conseiller des outils de protection plus pertinents et réaliser une veille pour rester à jour sur l'évolution des cybermenaces.

CHAPITRE 3

Connaitre les tendances des métiers de la Cybersécurité

Ce que vous allez apprendre dans ce chapitre :

- Appréhender l'approche DevSecOps
- Découvrir les futurs métiers de Cybersécurité
- Se focaliser sur le domaine de la Blockchain

2 heures

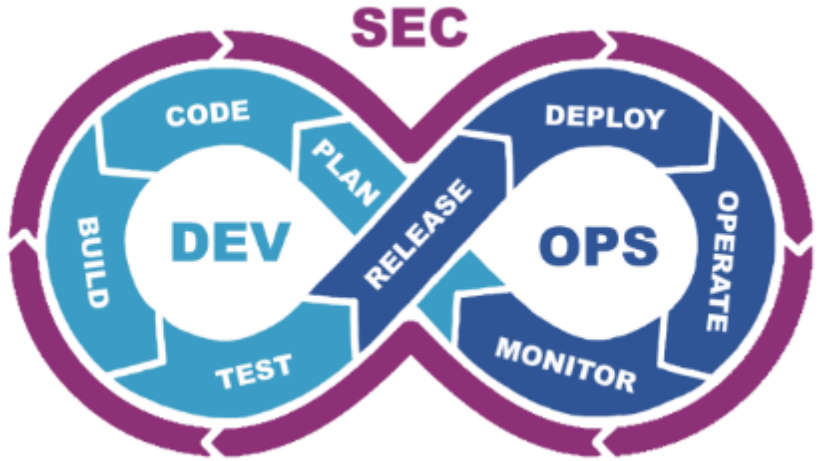
CHAPITRE 3

Connaitre les tendances des métiers de la Cybersécurité

1. **Métier de consultant DevSecOps**
2. Administrateur sécurité Blockchain

Workflow DEVSECOPS

- Le terme **DevOps** correspond au mélange des tâches qu'effectuent les équipes d'une entreprise chargées du développement des applications (Dev) et de l'exploitation des systèmes (Ops, pour opérations).
- Le **DevSecOps** a pour but d'introduire la sécurité à chaque étape du cycle DevOps. On retrouve donc ici le cycle infini DevOps renforcé par la sécurité



Compétences requises pour un consultant DevSecOps :

- Connaissance de la culture et des principes DevOps ;
- Compréhension des langages de programmation tels que Ruby, Perl, Java, Python et PHP ;
- Solides compétences en travail d'équipe et en communication ;
- Connaissance des techniques de modélisation des menaces et d'évaluation des risques ;
- Connaissance à jour des menaces de cybersécurité, des meilleures pratiques actuelles et des derniers logiciels ;
- Une compréhension des programmes tels que Puppet, Chef, ThreatModeler, Checkmarx, Immunio et Aqua. Ils peuvent également avoir besoin de connaître Kubernetes, Docker ou AWS.

CHAPITRE 3

Connaitre les tendances des métiers de la Cybersécurité

1. Métier de consultant DevSecOps
2. **Administrateur sécurité Blockchain**

Définition de la blockchain :

- **La blockchain** est un grand livre partagé et inaltérable qui facilite le processus d'enregistrement des transactions et de suivi des actifs dans un réseau commercial. Un *actif* peut être matériel (une maison, une voiture, de l'argent, un terrain) ou immatériel (propriété intellectuelle, brevets, droits d'auteur, marque). Pratiquement tout ce qui a de la valeur peut être suivi et échangé dans un réseau de blockchain, ce qui réduit les risques et les coûts pour toutes les parties concernées.

- **Compétences requises pour les administrateurs Blockchain :**

  - Expertise Blockchain ;
  - Compétences analytiques ;
  - Compétences en programmation et développement de logiciels ;
  - Connaissances juridiques et financières ;
  - État d'esprit adaptatif et innovant.

PARTIE 4

Ex : Modèle tableau Partie 1

Fichier	Table Début	Fin
A	0	3
B	4	6
C	7	12
D	13	29
E	18	35
F	30	38

	Serveur
Fonctionnalité	Les systèmes serveurs traitent les demandes des clients pour divers services.
Configuration	Les systèmes de serveurs ont une configuration plus complexe et sophistiquée.
Mode de Connexion	Ils prennent en charge la connexion simultanée de plusieurs utilisateurs.
Tâches exécutées	Les tâches complexes telles que l'analyse des données, le stockage et le traitement de grands ensembles de données ainsi que la satisfaction des demandes des clients sont courantes pour les systèmes de serveurs.
Power Off	L'arrêt des serveurs peut avoir de graves répercussions. Ils ne sont généralement jamais éteints.

Ex : Idée de SmartArt (Pour changer la forme, allez dans insertion, puis SmartArt)

Un langage de script (également appelé script) est une série de commandes qui peuvent être exécutées sans compilation.

Tous les langages de script sont des langages de programmation, mais tous les langages de programmation ne sont pas des langages de script.

Les langages de script utilisent un programme appelé interpréteur pour traduire les commandes.

Ex : Modèle Remarque Partie 1

Remarques

- Les chaînes sont écrites entre guillemets simples ou doubles.
- Les nombres sont écrits sans guillemets.

Ex : Modèle tableau Partie 2

Méthode	Description
length	C'est un entier qui indique la taille de la chaîne de caractères.
charAt()	Méthode qui permet d'accéder à un caractère isolé d'une chaîne.
substring(x,y)	Méthode qui renvoie un string partiel situé entre la position x et la position y-1.
toLowerCase()	Transforme toutes les lettres en minuscules.
toUpperCase()	Transforme toutes les lettres en Majuscules.

Ex : Idée SmartArt

Un serveur web

- Un serveur web sert à rendre accessibles des pages web sur internet via le protocole HTTP.
- Un serveur web répond par défaut sur le port 80.
- Pour qu'un site Web soit accessible à tout moment, le serveur Web sur lequel il est hébergé doit être connecté à Internet en permanence

Ex : Modèle Remarque Partie 2

Remarques

- Une méthode est une propriété dont la valeur est une fonction. Son rôle est de définir un comportement (action) pour l'objet
- On peut utiliser var au lieu de const

Ex : Modèle tableau Partie 3

Fonctionnalité	Syntaxe
Déplacer fichier1 dans le répertoire /tmp	mv fichier1 /tmp
Déplace le répertoire TEST dans le répertoire /tmp	mv TEST /tmp
Supprimer des fichiers	rm fichier1 fichier2
Supprimer un répertoire vide	rmdir rep

Ex : Idée SmartArt

Ex : Modèle Remarque Partie 3

Remarque

- Re-exécuter ce code en supprimant l'espace entre l'élément « div » et la balise « h1 »

Ex : Modèle tableau Partie 4

Sélecteur	Description
:disabled	Sélectionner les éléments désactivés
:invalid	Sélectionner les éléments don’t la valeur est invalide
:optional	Sélectionner les éléments d'entrée sans attribut "requis" spécifié
:required	Sélectionner les éléments d'entrée avec l'attribut "requis" spécifié
:valid	Sélectionner les éléments d'entrée avec des valeurs valides

Ex : Idée SmartArt

1. **Écouteur d'événement (Event Listner) :**
   L'écouteur d'événement est un objet qui attend qu’un certain événement se produise (un clic, un mouvement de souris, etc.)

2. **Gestionnaire d'événements :**
   le gestionnaire d'événements correspond généralement une fonction appelée suite à la production de l’événement.

Ex : Modèle Remarque Partie 4

Remarques

- Les événements **keydown** et **keypress** sont déclenchés avant toute modification apportée à la zone de texte.
- L'événement **keyup** se déclenche après que les modifications soient été apportées à la zone de texte.

Couleurs de la Charte Graphique à utiliser par l'expert

#0059A1
Partie 3

#008245
Partie 1

#FF7800
Partie 2

#40C3D5

#B2BD00
Partie 6

#08ACA2
Partie 5

#F2F2F2
Gris Fond
SmartArt

#565656
Gris texte
Partie 4

#BFBFBF
Gris légendes
et sources