



Eighth Edition - 2018 - Exam Essentials
French translation

Ver. 1.1
Translated by 0x21.fr
<https://github.com/0x21fr/CISSP2018>
Mailto: cissp@0x21.fr

Contents

Introduction	3
Domain 1: Security and Risk Management	4
Chapter 1: Security Governance Through Principles and Policies	4
Chapter 2: Personnel Security and Risk Management Concepts	7
Chapter 3 : Business Continuity Planning	12
Chapter 4: Laws, Regulations, and Compliance	13
Domain 2: Asset Security	16
Chapter 5: Protecting Security of Assets	16
Domain 3: Security Architecture and Engineering	18
Chapter 6: Cryptography and Symmetric Key Algorithms.....	18
Chapter 7: PKI and Cryptographic Applications	20
Chapter 8: Principles of Security Models, Design, and Capabilities	22
Chapter 9: Security Vulnerabilities, Threats, and Countermeasures.....	24
Chapter 10: Physical Security Requirements.....	28
Domain 4: Communication and Network Security	32
Chapter11: Secure Network Architecture and Securing Network Components	32
Chapter 12: Secure Communications and Network Attacks	36
Domain 5: Identity and Access Management (IAM)	40
Chapter 13: Managing Identity and Authentication	40
Chapter 14: Controlling and Monitoring Access	42
Domain 6: Security Assessment and Testing.....	44
Chapter 15: Security Assessment and Testing.....	44
Domain 7: Security Operations.....	46
Chapter 16: Managing Security Operations	46
Chapter 17: Preventing and Responding to Incidents	48
Chapter 18: Disaster Recovery Planning	52
Chapter 19: Incidents and Ethics	53
Domain 8: Software Development Security	56
Chapter 20: Software Development Security.....	56
Chapter 21: Malicious Code and Application Attacks.....	57

Introduction

Ce document, d'environ 60 pages, est juste une synthèse des différents points abordés lors de la préparation de la certification CISSP. C'est une énumération des questions à se poser et des sujets à maîtriser. Le but ici est de réaliser un survol, plutôt exhaustif, des périmètres, sans rentrer dans le détail.

Il sera donc nécessaire d'approfondir les concepts à l'aide des ouvrages officiels.

➔ <https://www.isc2.org/Training/Self-Study-Resources>

Cette liste de points importants est issue du « CISSP Official Study Guide », 8ème édition, paru en avril 2018

➔ <https://www.amazon.com/CISSP-Certified-Information-Security-Professional/dp/1119475937>

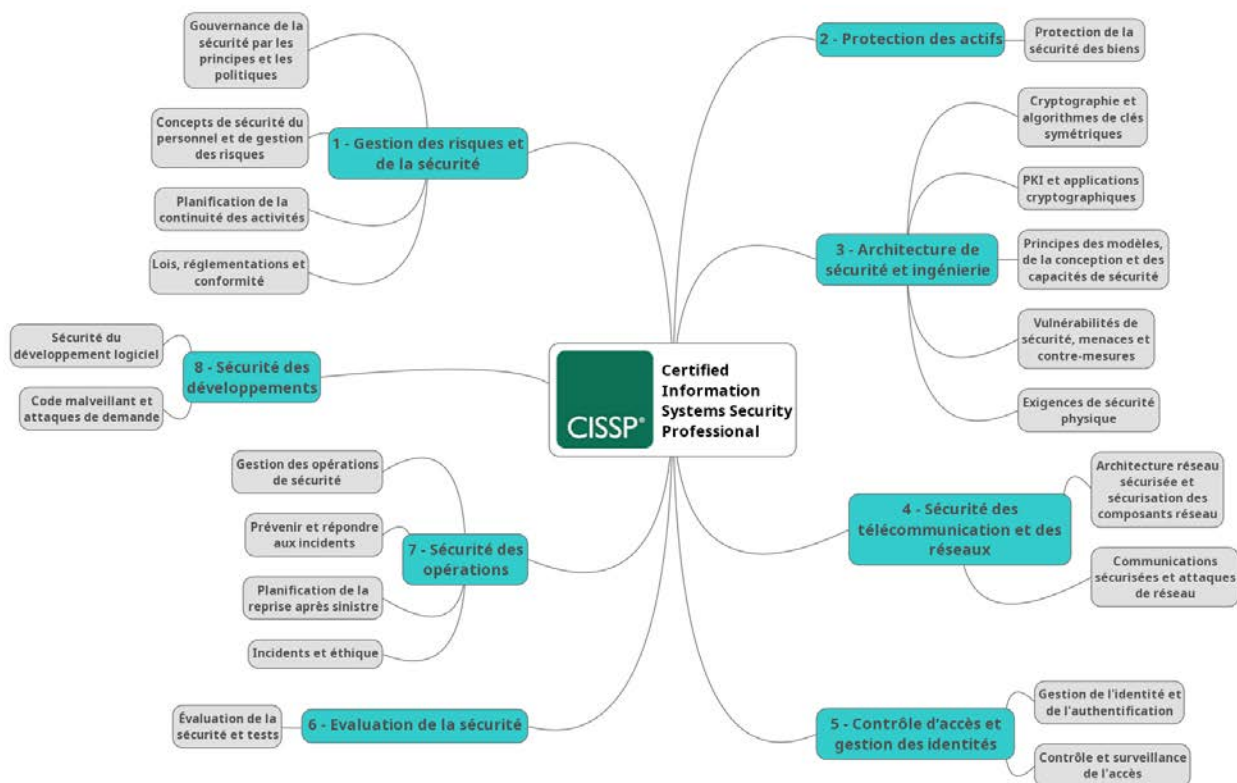
Le but, ici, est de proposer une sorte de checklist composée de l'ensemble des acronymes et des termes importants sous leur forme anglaise.

Effectivement, volontairement, les titres ne sont pas traduits, ce qui peut conduire, pour les moins anglophones, à quelques difficultés d'interprétation ou de compréhension. Mais le but est de conserver un lien fort avec la terminologie officielle tout en proposant une traduction juste des définitions et explications.

Même si la traduction de certain terme peut sembler incertaine, ou approximative, les textes d'explication permettront de comprendre rapidement le sens des sujets abordés.

Le but est vraiment de trouver le juste milieu entre l'anglais et le français ! Quelle idée de tenter de traduire « fuzzing » par exemple ! Alors que le plus important est d'en comprendre le sens dans le contexte qui nous intéresse.

L'organisation du document respecte le plan officiel du « Common Body of Knowledge » (CBK) de l'ISC2 :



Domain 1: Security and Risk Management

Dans la terminologie CISSP, le « **sujet** » est la personne ou le processus souhaitant accéder à une ressource; « **l'objet** » représente la ressource ou le service.

Chapter 1: Security Governance Through Principles and Policies

- Understand the CIA Triad elements of Confidentiality, Integrity, and Availability

« **Confidentialité** » est le principe que les « objets » ne sont pas divulgués (no disclosed) à des « sujets » non autorisés.

« **Intégrité** » est le principe que les « objets » gardent leur véracité et ne sont modifiés intentionnellement que par les « sujets » autorisés.

« **Availability** » est le principe que les sujets autorisés ont accès à des objets de façon ininterrompu.

- Be able to explain how identification works

« L'identification » est le processus par lequel le « sujet » déclare son identité et la traçabilité (accountability) est initiée. Le « sujet » doit prouver son identité au système pour démarrer le processus d'authentification, d'autorisation, et de traçabilité

- Understand the process of authentication

« L'authentification » est le processus qui vérifie ou teste que l'identité déclarée est valide.

« L'authentification » requiert que les informations concernant le « sujet » correspondent exactement à l'identité indiquée.

- Know how authorization fits into a security plan (Savoir comment l'autorisation s'inscrit dans un plan de sécurité)

Une fois que le « sujet » est authentifié, les accès doivent être autorisés.

Le processus d'autorisation s'assure que les activités demandées ou les accès aux objets sont possible compte tenu des droits et des privilèges assigné à l'identité authentifiée.

- Understand security governance

La gouvernance de la sécurité est une collection de pratiques pour supporter, définir, et diriger les efforts de sécurité de l'organisation.

- Be able to explain the auditing process

Auditing, or monitoring, est les moyens par lesquels les action des sujets sont tracés lorsqu'ils sont authentifiés sur un système.

L'audit (auditing) doit détecter les actions mal intentionnées d'un sujet, les tentatives d'intrusion, et les défaillances systèmes.

En reconstituant les événements, l'audit permet de constituer des preuves pour d'éventuelle poursuite, et permet de produire des rapports d'analyses et de problèmes.

- Understand the importance of accountability

La politique de sécurité des organisations peut être correctement appliquée que si la traçabilité (accountability) est maintenue.

En d'autres mots, la sécurité peut être correctement maintenue que si les actions des sujets sont correctement tracées.

La traçabilité est reliée à la capacité de prouver l'identité d'un sujet et ses activités.

- Be able to explain nonrepudiation

La non-répudiation assure qu'un sujet lié à une activité ou à un événement ne peut pas nier ces actions.

La non-répudiation empêche qu'un sujet revendique de ne pas avoir fait une action ou de ne pas être en cause dans un évènement.

- Understand security management planning

Le management de la sécurité est basé sur 3 types de plans: stratégique, tactique, et opérationnel.

Un plan **stratégique** est un plan sur le long terme qui est plutôt stable.

Un plan **tactique** est un plan sur le moyen terme développé pour produire plus de détails sur la réalisation des objectifs énoncés dans le plan stratégique.

Un plan **opérationnel** est un plans très détaillé sur le court terme, basé sur la les plans stratégique et tactique.

- Know the elements of a formalized security policy structure

Pour créer plan de sécurité compréhensif vous devez suivre les éléments en place : la politique de sécurité, les standards, les lignes de bases (baselines), les lignes directrices (guidelines), et les procédures. Cette formalisation énonce clairement les exigences de sécurité et crée une diligence raisonnable (due diligence) de la part des parties responsables.

- Understand key security roles

Les principaux rôles de sécurité sont : **Senior management**, **Organizational owner** (propriétaire de l'organisation), **Upper management** (Haute direction), **Security professional**, **User**, **Data owner** (propriétaire des données), **Data custodian** (gardien des données, opérateur), and **Auditor**.

En créant une hiérarchie des rôles de sécurité, vous limitez le risque global.

- Know how to implement security awareness training (formation de sensibilisation)

Avant que la **formation** proprement dite puisse avoir lieu, la **sensibilisation à la sécurité** en tant que telle doit être réalisée pour les utilisateurs.

Une fois cela accompli, la formation, ou l'enseignement des employés pour effectuer leurs tâches de travail et pour se conformer à la politique de sécurité, peut commencer.

Tous nouveaux employés requièrent un certain niveau de formation afin qu'ils soient en mesure de se conformer à la politique de sécurité.

L'éducation est une démarche plus détaillée dans laquelle les étudiants apprennent beaucoup plus qu'ils n'ont réellement besoin de savoir pour accomplir leurs tâches. L'éducation est souvent associé à la validation d'une certification par l'utilisateur ou à la recherche d'un emploi.

- Know how layering simplifies security

Le « Layering » (superposition/couche) est l'adoption de contrôles multiples en séries. L'utilisation de **solution multicouche** permet de nombreux contrôles pour se prémunir contre les menaces.

- Be able to explain the concept of abstraction

L'abstraction est utilisée pour collecter des éléments similaires dans des groupes, des classes ou des rôles auxquels sont affectés des contrôles de sécurité, des restrictions ou des autorisations en tant que collectif. Cela ajoute de l'efficacité à l'exécution d'un plan de sécurité.

- Understand data hiding

La dissimulation de données (data hiding) porte très bien son nom : Empêcher les données d'être découvertes ou accessibles par un sujet. C'est souvent un élément clé des contrôles de sécurité ainsi que de la programmation.

- Understand the need for encryption

Le cryptage est l'art et la science de cacher le sens ou l'intention d'une communication à des destinataires indésirables.

Le cryptage peut prendre de nombreuses formes et être appliqué à tous les types de communications électroniques: fichiers texte, audio et vidéo, ainsi que les programmes eux-mêmes.

Le cryptage est un élément important dans les contrôles de sécurité, en particulier en ce qui concerne la transmission de données entre les systèmes.

- Be able to explain the concepts of change

Le « **changement** » dans un environnement sécurisé peut introduire des failles, des chevauchements, des objets manquants et des oublis pouvant mener à de nouvelles vulnérabilités. Le seul moyen de maintenir la sécurité face au changement est de gérer systématiquement le changement. C'est la « gestion du changement ».

- Know why and how data is classified

Les données sont classifiées pour simplifier le processus d'attribution de contrôles de sécurité à des groupes d'objets plutôt qu'à des objets individuels. Les deux schémas de classification communs sont le secteur public / militaire et commercial / secteur privé.

Connaître les cinq niveaux de classification **gouvernementale / militaire** :

- Top secret, Secret, Confidential, Sensitive but unclassified, Unclassified

Connaître les quatre niveaux de classification des **entreprises commerciales et du secteur privé** :

- Confidential, Private, Sensitive, Public

- Understand the importance of declassification

Une déclassification est requise lorsqu'un actif ne justifie plus la protection de son niveau de classification ou de sensibilité actuellement attribué.

- Know the basics of COBIT

Control Objectives for Information and Related Technology (COBIT) (ou objectifs de contrôle de l'information et des technologies associées) est un référentiel de bonnes pratiques d'audit informatique et de gouvernance des systèmes d'information d'origine américaine.

COBIT est utilisé pour organiser les solutions de sécurité complexes des entreprises.

- Know the basics of threat modeling

La **modélisation des menaces** (threat modeling) est le processus de sécurité où les menaces potentielles sont identifiées, catégorisées et analysées. La modélisation des menaces peut être réalisée comme une **mesure proactive** lors de la conception et du développement ou comme **mesure réactive** une fois qu'un produit a été déployé.

Les concepts clés incluent les actifs, les attaquants, les logiciels, STRIDE (modèle de classification développé par Microsoft), les diagrammes, réduction/décomposition et DREAD (modèle d'évaluation des risques utilisé par Microsoft, OpenStack ...)

STRIDE :

- Spoofing of user identity
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of service (D.o.S)
- Elevation of privilege

DREAD :

- Damage - how bad would an attack be?
- Reproducibility - how easy is it to reproduce the attack?
- Exploitability - how much work is it to launch the attack?
- Affected users - how many people will be impacted?
- Discoverability - how easy is it to discover the threat?

- Understand the need for security-minded acquisitions

L'intégration de la gestion des risques de cyber sécurité aux stratégies et pratiques d'acquisition est un moyen d'assurer une stratégie de sécurité plus robuste et plus efficace dans les organisations de toutes tailles. Lorsque les achats sont effectués sans considérations de sécurité, les risques inhérents à ces produits demeurent tout au long de leur durée de vie.

- Discuss and describe the CIA Triad ***

CIA désigne la **Confidentialité**, l'**Intégrité**, et la disponibilité (**Availability**). Ce terme est utilisé pour se référer aux trois mots clés composant une solution de sécurité.

- What are the requirements to hold a person accountable for the actions of their user account ? ***

Les exigences de traçabilité sont : l'identification, l'authentification, l'autorisation, et l'audit.

Chacun de ces composants doit être légalement supportable pour vraiment tenir quelqu'un responsable de ses actions.

- Describe the benefits of change control management ***

Les avantages du management de la gestion des changements comprennent la prévention des risques de sécurité en raison de changements incontrôlés, la documentation et le suivi de toutes les modifications dans l'environnement, la standardisation, la mise en conformité avec la politique de sécurité, et la facilité de retour arrière.

- What are the seven major steps or phases in the implementation of a classification scheme ? ***

1. Identifiez le gardien (the custodian) et définissez ses responsabilités.
2. Spécifiez les critères d'évaluation de la façon dont les informations seront classées et étiquetées.
3. Classifiez et étiquetez chaque ressource (Le propriétaire procède à cette étape, mais un superviseur devrait l'examiner).
4. Documentez les exceptions à la politique de classification qui ont été découvertes et intégrez-les dans les critères d'évaluation.
5. Sélectionnez les contrôles de sécurité qui seront appliqués à chaque niveau de classification pour fournir le niveau de protection nécessaire.
6. Spécifiez les procédures de dé classification des ressources et les procédures de transfert de la garde d'une ressource à une entité externe.
7. Créer un programme de sensibilisation à l'échelle de l'entreprise pour instruire tout le personnel sur le système de classification.

- Name the six primary security roles as defined by (ISC)2 for CISSP ***

Les six rôles sont:

Senior management, IT/Security staff, Owner, Custodian, Operator/user, and Auditor

- What are the four components of a complete organizational security policy and their basic purpose ? ***

Les quatre composantes d'une politique de sécurité organisationnelle sont :

- **Policies** : la politique large de sécurité
- **Standards** : les définitions des standards hardware et software conformes à la sécurité
- **Guidelines** : utilisés quand il n'y a pas de procédures adaptées
- **Procedures** : instructions détaillées, étape par étape, pour réaliser une tâche de manière sécurisée

Chapter 2: Personnel Security and Risk Management Concepts

- Know how privacy fits into the realm of IT security (Savoir comment la vie privée s'inscrit dans le domaine de la sécurité informatique)

Connaître les multiples significations et définitions de la vie privée. Pourquoi il est important de protéger ? Les problèmes qui l'entourent, en particulier dans un environnement de travail

- Be able to discuss third-party governance of security.

La gouvernance par une tierce partie (third-party governance) est le système de surveillance qui peut être imposé par la loi, la réglementation, les normes de l'industrie ou les exigences de licence.

- Be able to define overall risk management

Le management du risque global (overall risk management) est le processus d'identification des facteurs qui pourraient endommager ou divulguer les données, l'évaluation des facteurs à la lumière de la valeur des données et des coûts de contre-mesure, et la mise en œuvre des solutions rentables pour atténuer ou réduire les risques est connu comme la gestion des risques.

En effectuant la gestion des risques, vous jetez les bases d'une réduction globale des risques.

- Understand risk analysis and the key elements involved

L'analyse des risques est le processus par lequel la haute direction reçoit des détails afin de décider quels risques doivent être atténués (**mitigated**), lesquels doivent être transférés (**transferred**) et lesquels doivent être acceptés (**accepted**) .

Pour évaluer pleinement les risques et prendre ensuite les précautions appropriées, vous devez analyser les éléments suivants : les actifs (**assets**), l'évaluation des actifs (**asset valuation**), les menaces (**threats**), la vulnérabilité (**vulnerability**), l'exposition (**exposure**), le risque (**risk**), le risque réalisé (**realized risk**), les sauvegardes et protections (**safeguards**), les contre-mesures (**countermeasures**), les attaques (**attacks**) et les violations (**breaches**).

- Know how to evaluate threats

Les menaces (**threats**) peuvent provenir de nombreuses sources : du système d'information lui-même (de l'IT), des humains et/ou de sources naturelles. L'évaluation de la menace devrait être réalisée par d'un comité, une équipe, pour fournir le plus large éventail de perspectives. En évaluant l'ensemble des risques sous tous les angles, vous réduisez la vulnérabilité du système.

- Understand quantitative risk analysis

L'analyse quantitative des risques met l'accent sur les valeurs et les pourcentages. Une analyse quantitative complète n'est pas possible en raison des aspects intangibles du risque. Le processus implique l'évaluation des actifs et l'identification des menaces, puis la détermination de la fréquence potentielle d'une menace et des dommages qui en résultent. Le résultat est une analyse coût / bénéfice des protections mise en place.

- Be able to explain the concept of an exposure factor (EF)

Un facteur d'exposition (**exposure factor**) est un élément de l'analyse de risque quantitative qui représente le pourcentage de perte qu'une organisation subirait si un actif spécifique était affecté par un risque réalisé. En calculant les facteurs d'exposition, vous êtes en mesure de mettre en œuvre une politique saine de gestion des risques

- Know what single loss expectancy (SLE) is and how to calculate it

Le SLE (**Single Loss Expectancy**) est un élément d'analyse de risque quantitatif qui représente le coût associé à un seul risque réalisé par rapport à un actif spécifique. La formule est :

$$\text{SLE} = \text{Valeur de l'Actif (AV)} \times \text{Facteur d'Exposition (EF)}$$

- Understand annualized rate of occurrence (ARO)

L'ARO (**Annualized Rate of Occurrence**) est un élément de l'analyse quantitative des risques qui représente la fréquence attendue avec laquelle une menace ou un risque spécifique se produira, ou se concrétisera, au cours d'une même année. Comprendre les ARO vous permet en outre de calculer le risque et de prendre les précautions appropriées.

- Know what annualized loss expectancy (ALE) is and how to calculate it

ALE (**Annualized Loss Expectancy**) est un élément de l'analyse quantitative des risques qui représente le coût annuel possible de toutes les instances d'une menace spécifique contre un actif spécifique. La formule est :

$$\text{ALE} = \text{espérance de perte unique (SLE)} \times \text{taux d'occurrence annualisé (ARO)}$$

$$\text{ALE} = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Loss Expectancy (ARO)}$$

- Know the formula for safeguard evaluation

En plus de déterminer le coût annuel d'une solution de réduction du risque (safeguard), vous devez calculer l'ALE (Annualized Loss Expectancy) pour l'actif si la protection est mise en œuvre. Utilisez la formule:

ALE avant mise en œuvre d'une solution - ALE après mise en œuvre d'une solution - coût annuel de la solution =
valeur de la solution de réduction du risque pour l'organisation

Ou:

$(ALE1 - ALE2) - ACS = \text{valeur de la solution}$

- Understand qualitative risk analysis

L'analyse qualitative des risques repose plus sur des scénarios que sur des calculs. Les chiffres exacts en Dollars ou en Euros ne sont pas affectés aux pertes possibles. Les menaces sont plutôt classées sur une échelle pour évaluer leurs risques, leurs coûts et leurs effets. Une telle analyse aide les responsables à créer des politiques de gestion des risques appropriées.

- Understand the Delphi technique

La technique **Delphi** est simplement un processus de rétroaction et de réponse anonyme (**anonymous feedback-and-response process**) utilisé pour arriver à un consensus. Un tel consensus donne aux parties responsables la possibilité d'évaluer correctement les risques et de mettre en œuvre des solutions.

- Know the options for handling risk (manipulation du risque)

La **réduction** des risques, ou l'**atténuation** des risques (mitigation), est la mise en œuvre de solutions et de contre-mesures.

Assigner un risque ou **transférer** un risque place le coût de la perte qu'un risque sur une autre entité ou organisation. La souscription à une **police d'assurance** est une forme d'affectation ou de transfert de risque.

L'**acceptation** du risque signifie que la direction a évalué le rapport coût / bénéfice d'une solution et a déterminé que le **coût de la contre-mesure** l'emportera largement sur le **coût éventuel de la perte** lié à un risque. Cela signifie également que la direction a **décidé d'accepter les conséquences** et la perte si le risque est réalisé.

- Be able to explain total risk, residual risk, and controls gap

Le **risque total** est le niveau de risque auquel une organisation serait confrontée si aucune solution n'était mise en œuvre. Pour calculer le risque total, utilisez cette formule:

$\text{Menaces (Threats)} \times \text{Vulnérabilités} \times \text{Valeur de l'Actif (Asset Value)} = \text{Total Risk}$

Le **risque résiduel** est le risque que la direction a choisi d'accepter plutôt que de l'atténuer.

La différence entre le risque total et le risque résiduel est l'écart de contrôle (**controls gap**). C'est la quantité de risque qui est réduite en mettant en œuvre des mesures de protection. Pour calculer le risque résiduel, utilisez la formule suivante:

$\text{Risque total (total risk)} - \text{écart de contrôle (controls gaps)} = \text{Risque résiduel}$

- Understand control types

Le terme **contrôle d'accès** fait référence à une large gamme de contrôles qui exécutent des tâches telles que s'assurer que seuls les utilisateurs autorisés peuvent se connecter et empêcher les utilisateurs non autorisés d'accéder aux ressources. Les **types de contrôle** comprennent la prévention (**preventive**), la détection (**detective**), la correction (**corrective**), la dissuasion (**deterrent**), la récupération (**recovery**), la directive (**directive**) et la compensation (**compensation**).

Les contrôles peuvent également être **catégorisés** en fonction de leur implémentation: **administrative**, **logique** ou **physique**.

- Understand the security implications of hiring new employees

Pour planifier correctement la sécurité, vous devez avoir **des standards**, **des normes**, pour les descriptions des différents postes, la classification des tâches, les responsabilités de chaque postes.

Vous devez adopter une démarche permettant de prévenir les collusions (entente illicite), de vérifier les antécédents, d'attribuer les autorisations de sécurité. Vous devez également avoir des standards concernant les contrats d'emploi et les accords de non-divulgaration.

En déployant de tels mécanismes, vous vous assurez que les nouveaux employés connaissent les normes de sécurité requises, protégeant ainsi les actifs de votre organisation.

- Be able to explain separation of duties

La séparation des tâches (**separation of duties**) est le concept de sécurité qui consiste à répartir les tâches critiques, importantes et sensibles entre plusieurs personnes. En séparant les tâches de cette manière, vous vous assurez qu'aucune personne ne peut compromettre la sécurité du système.

- Understand the principle of least privilege

Le principe du « moindre privilège » (**least privilege**) stipule que, dans un environnement sécurisé, les utilisateurs doivent se voir accorder le **minimum d'accès nécessaire** à l'accomplissement de leurs tâches professionnelles ou de leurs responsabilités professionnelles. En limitant l'accès des utilisateurs aux éléments dont ils ont besoin pour accomplir leurs tâches, vous **limitez la vulnérabilité** des informations sensibles.

- Know why job rotation and mandatory vacations are necessary

La rotation des tâches (**job rotation**) a deux fonctions. Il offre un type de redondance des connaissances (knowledge redundancy) et le déplacement du personnel (moving personnel) réduit les risques de fraude, de modification des données, de vol, de sabotage et d'utilisation abusive des informations (misuse of information). Des vacances obligatoires (**mandatory vacations**) d'une à deux semaines sont utilisées pour auditer et vérifier les tâches et les privilèges des employés. Cela se traduit souvent par la détection facile d'abus, de fraude ou de négligence.

- Understand vendor, consultant, and contractor controls

Le contrôle des vendeurs, des marchands, de fournisseurs (**vendor**), des consultants et des relations contractuelles est utilisé pour définir les niveaux de performance, les attentes, la rémunération et les conséquences pour les entités, les personnes ou les organisations externes à l'organisation principale. Souvent, ces contrôles sont définis dans un document ou une politique connu sous le nom d'accord de niveau de service (**service-level agreement - SLA**).

- Be able to explain proper termination policies

Une politique de résiliation de contrat de travail définit la procédure de licenciement des employés. Elle devrait inclure des éléments comme avoir toujours un témoin, désactiver l'accès au réseau de l'employé et effectuer un entretien de sortie. Une politique de résiliation devrait également inclure l'accompagnement de l'employé licencié hors des locaux en exigeant le retour des token de sécurité, des badges et des biens de la société.

- Know how to implement security awareness training and education

Avant que la **formation** proprement dite puisse avoir lieu, la **sensibilisation à la sécurité** (awareness training) en tant que telle doit être réalisée pour les utilisateurs.

Une fois cela accompli, la formation, ou l'enseignement des employés pour effectuer leurs tâches de travail et pour se conformer à la politique de sécurité, peut commencer.

Tous nouveaux employés requièrent un certain niveau de formation afin qu'ils soient en mesure de se conformer à la politique de sécurité.

L'éducation est une démarche plus détaillée dans laquelle les étudiants apprennent beaucoup plus qu'ils n'ont réellement besoin de savoir pour accomplir leurs tâches. L'éducation est souvent associé à la validation d'une certification par l'utilisateur ou à la recherche d'un emploi.

- Understand how to manage the security function

Pour gérer la fonction de sécurité, une organisation doit mettre en œuvre une **gouvernance de sécurité** adéquate et suffisante. Le fait d'effectuer une évaluation des risques pour piloter la politique de sécurité est l'exemple le plus clair et le plus direct de la gestion de la fonction de sécurité. Cela concerne également le budget, les mesures, les ressources, les stratégies de sécurité de l'information et l'évaluation de l'exhaustivité et de l'efficacité du programme de sécurité.

▪ Know the six steps of the risk management framework

Les six étapes du cadre de gestion des risques sont les suivantes :

1. Catégoriser (**Categorize**)
2. Sélectionner (**Select**)
3. Mettre en œuvre (**Implement**)
4. Evaluer (**Assess**)
5. Autoriser (**Authorize**)
6. Surveiller (**Monitor**)

▪ Name six different administrative controls used to secure personnel ***

Les réponses possibles incluent :

- la description du poste (job description)
- le principe de moins de privilège (least privilege)
- la séparation des fonctions (separation of duties)
- les responsabilités professionnelles (job responsibilities)
- la rotation des tâches (job rotation)
- la formation (cross-training)
- l'évaluation de performance (performance reviews)
- la vérification des antécédents (background checks)
- les avertissements d'action de travail (job action warnings)
- les formations de sensibilisation (awareness training)
- la formation professionnelle (job training)
- les entrevues de départ, de licenciement (exit interviews/terminations)
- les accords/clauses de non-divulgence (nondisclosure agreements)
- les accords de non-concurrence (non compete agreements)
- les contrats de travail (employment agreements)
- les déclarations de confidentialité (privacy declaration)
- les politiques d'utilisation acceptable (acceptable use policies)

▪ What are the basic formulas used in quantitative risk assessment ? ***

$$\text{SLE (Single Loss Expectancy)} = \text{AV (Asset Value)} \times \text{EF (Exposure Factor)}$$

$$\text{ARO (Annualized Rate Occurrence)} = \text{Annual frequency}$$

$$\text{ALE} = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Loss Expectancy (ARO)}$$

$$\text{Cost/benefit} = (\text{ALE1} - \text{ALE2}) - \text{ACS (Annual Cost of Safeguard)}$$

▪ Describe the process or technique used to reach an anonymous consensus during a qualitative risk assessment ***

La technique DELPHI (ou méthode de Delphes) est un processus anonyme de feedback-and-response utilisé pour permettre à un groupe d'atteindre un **consensus anonyme**. Son objectif principal est d'obtenir des réponses honnêtes et sans influence de tous les participants.

Les participants sont généralement rassemblés dans une seule salle de réunion ; pour chaque demande, chaque participant écrit sa réponse sur un papier anonymement ; les résultats sont compilés et soumis au groupe pour évaluation ; le processus est répété jusqu'à ce qu'un consensus soit atteint.

▪ Discuss the need to perform a balanced risk assessment. What are the techniques that can be used and why is this necessary ? ***

L'évaluation des risques (**risk assessment**) implique souvent une approche hybride utilisant des méthodes quantitatives et qualitatives.

Une analyse purement quantitative n'est pas possible; tous les éléments et les aspects de l'analyse ne peuvent pas être quantifiés parce que certains sont qualitatifs, certains sont subjectifs et certains sont intangibles. Étant donné

qu'une évaluation des risques purement quantitative n'est pas possible, il est essentiel d'équilibrer les résultats d'une analyse quantitative.

La méthode consistant à combiner une analyse quantitative et qualitative dans une évaluation finale du risque organisationnel est connue sous le nom d'évaluation hybride (**hybrid assessment**) ou d'analyse hybride (**hybrid analysis**).

Chapter 3 : Business Continuity Planning

▪ Understand the four steps of the BCP, business continuity planning process

Le plan de continuité des activités (**Business Continuity Planning - BCP**)(PCA en Français) comprend quatre phases distinctes :

- La portée et la planification du projet (project scope and planning)
- L'évaluation de l'impact sur les activités (business impact assessment)
- Le plan de continuité (continuity planning)
- L'approbation et la mise en œuvre (approval and implementation)

▪ Describe how to perform the business organization analysis

Dans l'analyse de l'organisation de l'entreprise, les personnes responsables de la conduite du BCP (Business Continuity Planning) déterminent quels départements et individus ont un intérêt dans le plan de continuité de l'activité. Cette analyse est utilisée comme base pour la sélection de l'équipe BCP et, après validation par l'équipe BCP, est utilisée pour guider les prochaines étapes du développement du BCP.

▪ List the necessary members of the business continuity planning team

L'équipe BCP devrait être composée, au minimum :

- des représentants de chacun des départements opérationnels et de support
- d'experts techniques du département informatique
- du personnel de sécurité avec des compétences en BCP
- des représentants légaux connaissant les responsabilités juridiques, réglementaires et contractuelles des entreprises
- des représentants de la haute direction.

Les membres supplémentaires de l'équipe dépendent de la structure et de la nature de l'organisation.

▪ Know the legal and regulatory requirements that face business continuity planners

Les chefs d'entreprise doivent faire preuve de diligence raisonnable pour s'assurer que les intérêts des actionnaires sont protégés en cas de catastrophe. Certaines industries sont également soumises à des réglementations fédérales, étatiques et locales qui imposent des procédures de BCP/PCA spécifiques. De nombreuses entreprises ont également des obligations contractuelles envers leurs clients qui doivent être respectées, avant et après une catastrophe.

▪ Explain the steps of the business impact assessment process

Les cinq étapes du processus d'évaluation des impacts (**Business Impact Assessment - BIA**) dans les entreprises sont :

- L'identification des priorités (identification of priorities)
- L'identification des risques (risk identification)
- L'évaluation des probabilités (likelihood assessment)
- L'évaluation de l'impact (impact assessment)
- La hiérarchisation des ressources (resource prioritization)

▪ Describe the process used to develop a continuity strategy

Pendant la phase de développement de la stratégie, l'équipe BCP détermine les risques qui seront atténués. Dans la phase de mise en place et lors du processus BCP lui-même, les mécanismes et procédures permettant d'atténuer les risques sont conçus. Le plan doit ensuite être approuvé par la haute direction et mis en œuvre. Le personnel doit également recevoir une formation sur ses rôles dans le processus BCP.

- Explain the importance of fully documenting an organization's business continuity plan

Formaliser le processus BCP dans un document fournit à l'organisation un enregistrement écrit des procédures à suivre en cas de catastrophe. Il empêche le syndrome « c'est dans ma tête » et assure la progression ordonnée des événements en cas d'urgence.

- Why is it important to include legal representatives on your business continuity planning team ? ***

De nombreuses réglementations ou lois fédérales, étatiques ou locales exigent des entreprises qu'elles appliquent les dispositions de type BCP/PCA. La présence d'un représentant légal dans vos équipes BCP vous permet de rester en conformité avec les lois, règlements et obligations contractuelles.

- What is wrong with the « seat-of-the-pants » approach to business continuity planning ? ***

Le terme « seat-of-the-pant » se réfère à une approche basée sur l'intuition et l'expérience plutôt que sur la planification et la méthode.

L'approche du « **seat-of-the-pant** » (siège-du-pantalon) est une excuse utilisée par les individus qui ne veulent pas investir du temps et de l'argent dans la création d'un BCP. Cela peut mener à la catastrophe quand un plan fermement n'a pas été établi pour gérer correctement une situation d'urgence stressante.

- What is the difference between quantitative and qualitative risk assessment ? ***

L'évaluation quantitative des risques implique l'utilisation du nombre et des formules pour prendre une décision. L'évaluation qualitative des risques comprend des facteurs non numériques, tels que les émotions, la confiance, la stabilité des équipes.

- What critical components should be included in your business continuity training plan ? ***

Le plan de formation du BCP devrait inclure un **briefing global** pour l'ensemble des employés et une **formation spécifique** pour les personnes ayant une implication directe ou indirecte avec le BCP.

De plus, le personnel de réserve doit être formé pour chaque rôle clé du BCP.

- What are the four main steps of the business continuity planning process ? ***

Le plan de continuité des activités (**Business continuity planning**) (BCP)(PCA en Français) comprend quatre phases distinctes :

- La portée et la planification du projet (project scope and planning)
- L'évaluation de l'impact sur les activités (business impact assessment)
- Le plan de continuité (continuity planning)
- L'approbation et la mise en œuvre (approval and implementation)

Chapter 4: Laws, Regulations, and Compliance

- Understand the differences between criminal law, civil law, and administrative law

Le droit pénal protège la société contre les actes qui violent les principes fondamentaux auxquels nous croyons. Les violations du droit pénal sont poursuivies par les gouvernements fédéraux et des États.

Le droit civil fournit le cadre pour la transaction d'affaires entre les personnes et organisations. Les violations du droit civil sont portées devant le tribunal et débattues par les deux parties concernées.

Le droit administratif est utilisé par les organismes gouvernementaux pour mener à bien leurs activités quotidiennes.

- Be able to explain the basic provisions of the major laws designed to protect society against computer crime

La loi sur la fraude et l'abus informatiques (The Computer Fraud and Abuse Act - **CFAA** - initialement de 1984) protège les ordinateurs utilisés par le gouvernement ou dans le commerce entre états, d'une variété d'abus.

La loi sur la sécurité informatique (The Computer Security Act - **CSA** - 1987) décrit les mesures que le gouvernement doit prendre pour protéger ses propres systèmes contre les attaques.

La Loi sur la réforme de la sécurité de l'information du gouvernement (Government Information Security Reform Act - **GISRA** - 2000) développe davantage le programme de sécurité de l'information du gouvernement fédéral.

- Know the differences among copyrights, trademarks, patents, and trade secrets

Les droits d'auteur (Copyrights) protègent les œuvres originales de l'auteur, telles que les livres, les articles, les poèmes et les chansons.

Les marques de commerce (Trademarks) sont des noms, des slogans et des logos qui identifient une entreprise, un produit ou un service.

Les brevets (Patents) offrent une protection aux créateurs de nouvelles inventions.

La loi sur les secrets d'affaires (Trade secret law) protège les secrets d'exploitation d'une entreprise

- Be able to explain the basic provisions of the Digital Millennium Copyright Act of 1998

Le **Digital Millennium Copyright Act** interdit le contournement des mécanismes de protection contre la copie placés dans les médias numériques et limite la responsabilité des fournisseurs de services Internet pour les activités de leurs utilisateurs.

- Know the basic provisions of the Economic Espionage Act of 1996

La Loi sur l'espionnage économique (The Economic Espionage Act) prévoit des sanctions à l'encontre des personnes reconnues coupables de vol de secrets commerciaux. Des pénalités plus sévères s'appliquent lorsque l'individu sait que l'information bénéficiera à un gouvernement étranger.

- Understand the various types of software license agreements

Les contrats de licence contractuels (Contractual license agreements) sont des accords écrits entre un fournisseur de logiciel et un utilisateur. Les accords **Shrink-Wrap** (emballage rétractable) sont écrits sur l'emballage du logiciel et prennent effet lorsqu'un utilisateur ouvre le paquet. Les accords **Click-Wrap** (contrat au clic) sont inclus dans un package mais nécessitent que l'utilisateur accepte les termes au cours du processus d'installation du logiciel.

- Explain the impact of the Uniform Computer Information Transactions Act on software licensing.

La loi sur les transactions d'informations informatiques uniformes (The Uniform Computer Information Transactions Act - **UCITA**) fournit un cadre (a Framework) pour l'application des accords de rétraction (**Shrink-Wrap**) et de contrat au clic (**Click-Wrap**) par les gouvernements fédéral et des États.

- Understand the notification requirements placed on organizations that experience a data breach

Comprendre les exigences de notification imposées aux organisations confrontées à une violation de données (data breach).

Le SB 1386 de la Californie (California's SB 1386) a mis en œuvre la première exigence d'État (statewide requirement) afin d'aviser les personnes d'une violation de leurs informations personnelles. Tous les États Américains, sauf trois, ont finalement suivi avec des lois similaires. Actuellement, la loi fédérale exige seulement une notification des personnes lorsqu'une organisation couverte par la **HIPAA** (Health Insurance Portability and Accountability Act - 1996) viole leurs informations de santé protégées.

- Understand the major laws that govern privacy of personal information in both the United States and the European Union

Les États-Unis ont un certain nombre de lois sur la protection de la vie privée qui influent sur l'utilisation de l'information par le gouvernement ainsi que sur l'utilisation d'informations par des industries spécifiques telles que les sociétés de services financiers et les organisations de santé.

L'Union Européenne a une directive plus complète sur la confidentialité des données qui régit l'utilisation et l'échange de renseignements personnels.

- Explain the importance of a **well-rounded compliance program** (un programme de conformité bien équilibré)

La plupart des organisations sont soumises à une grande variété d'exigences légales et réglementaires liées à la sécurité de l'information. L'élaboration d'un programme de conformité garantit que vous devenez et restez conforme à ces exigences qui se chevauchent souvent.

- Know how to incorporate security into the procurement and vendor governance process

L'utilisation accrue des services de type « cloud » par de nombreuses organisations nécessite une attention accrue à la conduite des contrôles (reviews) de la sécurité de l'information pendant le processus de sélection des fournisseurs et dans le cadre de la gouvernance continue des fournisseurs.

- What are the key **rights guaranteed to individuals** under the European Union's directive on data privacy ? ***

Les particuliers ont le droit d'**accéder à leurs données personnelles** et de **connaître la source** des informations incluses dans leurs dossiers. Ils ont également le droit de **corriger** les enregistrements inexacts. Chaque individu a **le droit de refuser le consentement du traitement** de leurs données et ont un recours légal si ces droits sont violés.

- What are some common question that organizations should ask when considering **outsourcing information storage, processing, or transmission** ? ***

Voici quelques **questions courantes** que les organisations peuvent poser sur les **fournisseurs de services externalisés** :

- Quel (s) type (s) d'informations sensibles sont stockées, traitées ou transmises par le fournisseur ?
- Quels contrôles sont en place pour protéger les informations de l'organisation ?
- Comment les informations de notre organisation sont-elles séparées de celles des autres clients (cloisonnement, ségrégation) ?
- Si le cryptage est utilisé comme contrôle de sécurité, quels sont les algorithmes de cryptage et les longueurs de clé utilisés? Comment la gestion des clés est-elle gérée ?
- Quels types de vérification ou d'audit de sécurité le fournisseur effectue-t-il ? et quel accès le client a-t-il à ces vérifications ?
- Le fournisseur compte-t-il sur d'autres tiers pour stocker, traiter ou transmettre des données ?
- Comment les dispositions du contrat relatives à la sécurité s'étendent-elles à ces tiers ?
- Où auront lieu le stockage, le traitement et la transmission des données ? si à l'extérieur du pays d'origine du client et/ou du fournisseur, quelles implications cela a-t-il ?
- Quel est le processus de réponse aux incidents du fournisseur et quand les clients seront-ils informés d'une violation de sécurité potentielle ?
- Quelles dispositions sont en place pour assurer l'intégrité et la disponibilité continues des données sur les clients ?

- What are some common steps that employers take to **notify employees of system monitoring** ? ***

Les employeurs prennent couramment certaines mesures pour informer les employés de la surveillance comprennent, telles que :

- les clauses des contrats de travail stipulant que l'employé ne devrait pas s'attendre à la protection de la vie privée lorsqu'il utilise du matériel de bureau,
- similairement, des déclarations écrites dans les politiques d'utilisation et de protection de la vie privée des entreprises,
- des bannières d'ouverture de session avertissant que toutes les communications sont soumises à une surveillance,
- et des étiquettes sur les ordinateurs et les téléphones avertissant de la surveillance.

Domain 2: Asset Security

Chapter 5: Protecting Security of Assets

- Understand the importance of data classifications

Les propriétaires de données (data owners) sont chargés de **définir les classifications** des données et de s'assurer que les systèmes et les données sont correctement marqués. En outre, les propriétaires de données (data owners) **définissent des exigences** pour protéger les données selon différentes classifications, telles que le cryptage des données sensibles au repos et en transit. Les classifications de données sont généralement définies dans les **stratégies de sécurité** ou les **stratégies de données**.

- Know about PII and PHI

L'information personnellement identifiable (Personally identifiable information - **PII**) est toute information qui peut identifier un individu. **L'information de santé protégée** (Protected health information - **PHI**) est toute information liée à la santé qui peut être liée à une personne en particulier. De nombreuses lois et réglementations exigent la protection des PII et des PHI.

- Know how to manage sensitive information

Les informations sensibles (sensitive information) sont des informations classifiées, et une bonne gestion permet d'éviter toute divulgation non autorisée entraînant une perte de confidentialité. Une **gestion appropriée** inclut le **marquage** (marking), la **manipulation** (handling), le **stockage** (storing) et la **destruction** (destroying) des informations sensibles. Les deux domaines où les organisations manquent souvent sont : la protection, lors de leur manipulation, de manière adéquate, des supports de sauvegarde contenant des informations sensibles et destruction des supports ou équipements qui sont arrivés à la fin de leur cycle de vie.

- Understand record retention

Les politiques de rétention (record retention) des enregistrements garantissent que les données sont conservées dans un état utilisable lorsque qu'elles sont utiles et détruites lorsqu'elles ne le sont plus. De nombreuses lois et réglementations imposent de conserver les données pour une durée déterminée, mais en l'absence de réglementations formelles, les organisations doivent spécifier la période de rétention dans une politique. Les données du journal d'audit doivent être conservées suffisamment longtemps pour pouvoir reconstituer les incidents passés, mais l'organisation doit déterminer sur quelle durée elle souhaite enquêter. Une tendance actuelle avec de nombreuses organisations est de réduire les responsabilités juridiques en mettant en œuvre des politiques de rétention de courte durée avec le courrier électronique.

- Know the difference between different roles

Le propriétaire des données (Data owner) est la personne **responsable de la classification**, de l'étiquetage et de la **protection** des données. **Les propriétaires du système** (System owners) sont responsables des systèmes qui traitent les données. **Les propriétaires d'entreprise** et de mission (Business and mission owners) possèdent les processus et s'assurent que les systèmes apportent de la valeur à l'organisation. **Les processeurs (chargés du traitement) de données** (Data processor) sont généralement des entités tierces qui traitent des données pour une organisation. **Les administrateurs** (Administrator) autorisent l'accès (grant access) aux données en fonction des instructions fournies par les propriétaires des données. **Un utilisateur** (A user) accède à des données au cours de l'exécution de son travail. **Un gardien** (A custodian) a des responsabilités quotidiennes pour la protection et le stockage des données.

- Understand the seven Safe Harbor principles

La loi Européenne sur la protection des données (The EU Data Protection law) impose la protection des données privées. Les parties tierces acceptent de se conformer aux **sept principes de la « sphère de sécurité »** (The « Safe Harbor ») en tant que moyen de s'assurer qu'ils respectent la législation de l'Union Européenne sur la protection des données. Les sept principes sont **la notification** (notice), **le choix** (choice), **le transfert ultérieur** (onward

transfer), **la sécurité** (security), **l'intégrité des données** (data integrity), **l'accès** (access) et **la mise en vigueur** (enforcement).

▪ Know about security control baselines

Les lignes de base du contrôle de sécurité fournissent une liste de contrôles qu'une organisation peut appliquer comme référence. Toutes les lignes de base ne s'appliquent pas à toutes les organisations. Cependant, une organisation peut appliquer des techniques de cadrage et d'adaptation pour mettre en place une base de référence à ses besoins.

▪ Describe PII and PHI ***

L'information personnellement identifiable (Personally identifiable information - PII) est toute information qui peut identifier un individu. Il comprend des informations pouvant être utilisées pour distinguer ou retracer l'identité d'une personne, telles que le nom, le numéro de sécurité sociale ou le numéro d'identification national, la date et le lieu de naissance, le nom de jeune fille de la mère et les enregistrements biométriques. **L'information de santé protégée** (Protected health information - PHI) est toute information liée à la santé qui peut être liée à une personne en particulier. PHI ne s'applique pas seulement aux fournisseurs de soins de santé. Tout employeur qui fournit, ou complète, des politiques de soins de santé recueille et manipule les PHI

▪ Describe the best method to sanitize SSDs ***

Les disques SSD (Solid State Drive) doivent être détruits physiquement pour les rendre hors d'usage. Les méthodes traditionnelles utilisées pour des disques durs, telles que la démagnétisation (degaussing) et ne sont pas fiables.

▪ Name four classification levels that an organization can implement for data ***

Les organisations peuvent utiliser **les niveaux de classification qu'elles souhaitent**. Deux exemples sont les classes (classe 3, classe 2, classe 1 et classe 0) et les niveaux de confidentialité (privés, sensibles et publiques).

▪ List the seven principles outlined by the Safe Harbor program ***

Le programme de « **sphère de sécurité** » (The Safe Harbor program) comprend les sept principes suivants :

- la notification (notice)
- le choix (choice)
- le transfert ultérieur (onward transfer)
- la sécurité (security)
- l'intégrité des données (data integrity)
- l'accès (access)
- la mise en vigueur (enforcement)

Domain 3: Security Architecture and Engineering

Chapter 6: Cryptography and Symmetric Key Algorithms

- Understand the role that confidentiality, integrity, and nonrepudiation play in cryptosystems

La confidentialité (**Confidentiality**) est l'un des principaux objectifs de la cryptographie. Il protège le secret des données tant qu'il est au repos et en transit. L'intégrité (**Integrity**) fournit au destinataire d'un message l'assurance que les données n'ont pas été altérées (volontairement ou involontairement) entre le moment où ils ont été créées et le moment où ils ont été accédées. La non-répudiation (**Nonrepudiation**) fournit une preuve indéniable que l'expéditeur d'un message l'a effectivement rédigé. Cela empêche l'expéditeur de nier par la suite qu'il est à l'origine du message.

- Know how cryptosystems can be used to achieve authentication goals

L'authentification fournit des garanties quant à l'identité d'un utilisateur. Un schéma possible qui utilise l'authentification est le protocole de challenge-response, dans lequel l'utilisateur distant est invité à crypter un message en utilisant une clé connue seulement des parties communicantes. L'authentification peut être réalisée avec des systèmes cryptographiques symétriques et asymétriques.

- Be familiar with the basic terminology of cryptography.

Lorsqu'un expéditeur souhaite transmettre un message privé à un destinataire, l'expéditeur prend le message en clair (**plaintext**), ou « non crypté » (**unencrypted**) et le chiffre (**encrypts**) à l'aide d'un algorithme et d'une clé. Cela produit un message chiffré (**a ciphertext message**) qui est transmis au destinataire. Le destinataire utilise ensuite un algorithme et une clé similaires pour déchiffrer le texte chiffré et recréer le message en clair (**plaintext**) original pour le visionner.

- Understand the difference between a code and a cipher and explain the basic types of ciphers

Les codes sont des systèmes cryptographiques de symboles qui fonctionnent sur des mots ou des phrases et qui sont parfois secrets mais ne garantissent pas toujours la confidentialité. Les chiffrements (**ciphers**), cependant, sont toujours destinés à cacher la vraie signification d'un message. Sachez comment fonctionnent les types de chiffrement suivants:

- les chiffrements de transposition (transposition ciphers),
- les chiffrements de substitution (substitution ciphers), y compris les masques jetables (one-time pads),
- les chiffrements de flux (stream ciphers),
- et les chiffrements par bloc (block ciphers).

- Know the requirements for successful use of a one-time pad

Pour qu'un masque jetable (one-time pad) réussisse, la clé doit être générée de manière aléatoire (randomly) sans aucun motif connu. La clé doit être au moins aussi longue que le message à chiffrer. Les caractères composant la clé doivent être protégés contre la divulgation physique, et chaque clé doit être utilisée une seule fois et ensuite mis au rebut.

- Understand the concept of zero-knowledge proof

La preuve de connaissance zéro (zero-knowledge proof) est un concept de communication. Un type spécifique d'informations est échangé mais aucune donnée réelle n'est transférée, comme avec les signatures numériques et les certificats numériques.

- Understand split knowledge

La division des connaissances (Split knowledge) signifie que l'information ou le privilège requis pour effectuer une opération est réparti entre plusieurs utilisateurs. Cela garantit qu'aucune personne n'a des privilèges suffisants pour compromettre la sécurité de l'environnement. M of N Control est un exemple de connaissance partagée.

- Understand work function (work factor)

La fonction de travail (Work function), ou facteur de travail (work factor), est un moyen de mesurer la force d'un système de cryptographie en mesurant l'effort en termes de coût et/ou de temps pour déchiffrer les messages. Habituellement, le temps et l'effort requis pour effectuer une attaque par brute-force complète contre un système de cryptage est ce qui représente une évaluation de la fonction de travail (work function). La sécurité et la protection offertes par un système cryptographique sont directement proportionnelles à la valeur de sa fonction ou son facteur de travail.

- Understand the importance of key security

Les clés cryptographiques fournissent l'élément nécessaire au secret à un système cryptographique. Les cryptosystèmes modernes utilisent des clés d'au moins 128 bits pour assurer une sécurité adéquate. Il est généralement admis que la clé de 56 bits de la norme DES (Data Encryption Standard) n'est plus suffisamment longue pour assurer la sécurité.

- Know the differences between symmetric and asymmetric cryptosystems

Les clés des systèmes symétriques (Symmetric keycryptosystems), ou clé secrète, reposent sur l'utilisation d'une clé secrète partagée. Ils sont beaucoup plus rapides que les algorithmes asymétriques, mais ils manquent de support pour l'évolutivité (scalability), pour la distribution facile des clés et la non-répudiation (nonrepudiation). Les systèmes asymétriques (Asymmetric cryptosystems) utilisent des paires de clés publiques-privées pour la communication entre les parties, mais fonctionnent beaucoup plus lentement que les algorithmes symétriques.

- Be able to explain the basic operational modes of the Data Encryption Standard (DES) and Triple DES (3DES).

La norme DES (Data Encryption Standard) fonctionne selon quatre modes:

- le mode Electronic Codebook (ECB),
- le mode CBC (Cipher Block Chaining),
- le mode Cipher Feedback (CFB)
- et le mode Output Feedback (OFB).

Le mode ECB est considéré comme le moins sécurisé et n'est utilisé que pour les messages courts.

3DES utilise trois itérations de DES avec deux ou trois clés différentes pour augmenter la force effective de la clé à 112 ou 168 bits, respectivement.

- Know the Advanced Encryption Standard (AES)

EAS (Advanced Encryption Standard) utilise l'algorithme Rijndael et est la norme du gouvernement américain pour l'échange sécurisé de données sensibles mais non classifiées. AES utilise des longueurs de clé de 128, 192 et 256 bits et une taille de bloc fixe de 128 bits pour atteindre un niveau de sécurité beaucoup plus élevé que celui fourni par l'ancien algorithme DES.

- What is the major hurdle (obstacle majeur) preventing the widespread adoption (adoption répandue) of one-time pad cryptosystems to ensure data confidentiality ? ***

Le principal obstacle à l'adoption généralisée d'un crypto systèmes de type « masque jetable » (one-time pad) est la difficulté de créer et de distribuer les très longues clés dont dépend l'algorithme.

- Encrypt the message 'I will pass the CISSP exam and become certified next month' using columnar transposition with the keyword SECURE ***

La première étape du cryptage de ce message nécessite l'affectation de valeurs de colonne numériques aux lettres du mot clé secret:

S E C U R E
5 2 1 6 4 3

Ensuite, les lettres du message sont écrites dans l'ordre sous les lettres du mot-clé :

S E C U R E
5 2 1 6 4 3
I W I L L P

A S S T H E
C I S S P E
X A M A N D
B E C O M E
C E R T I F
I E D N E X
T M O N T H

Enfin, l'expéditeur encode le message en lisant chaque colonne; l'ordre de lecture des colonnes correspond aux numéros attribués dans la première étape. Cela produit le texte chiffré suivant:

I S S M C R D O W S I A E E M P E E D E F X H L H P N M I E T I A C X B C I T L
T S A O T N N

- Decrypt the message 'F R Q J U D W X O D W L R Q V B R X J R W L W' using the Caesar ROT3 substitution cipher ***

Ce message est déchiffré en utilisant la fonction suivante:

$$P = (C - 3) \text{ MOD } 26$$

C : F R Q J U D W X O D W L R Q V B R X J R W L W
P : C O N G R A T U L A T I O N S Y O U G O T I T

Et le message caché est : « Congratulations You Got It. »

Chapter 7: PKI and Cryptographic Applications

- Understand the key types used in asymmetric cryptography

Les clés publiques sont partagées librement entre les parties communicantes, tandis que les clés privées sont gardées secrètes. **Pour crypter** un message, utilisez la clé publique du destinataire. **Pour déchiffrer** un message, utilisez votre propre clé privée. **Pour signer** un message, utilisez votre propre clé privée. **Pour valider une signature**, utilisez la clé publique de l'expéditeur.

- Be familiar with the three major public key cryptosystems

RSA est le système de cryptographie à clé publique le plus célèbre; il a été développé par **Rivest, Shamir et Adleman** en 1977. Il dépend de la difficulté de factoriser le produit des nombres premiers.

El Gamal est une extension de l'algorithme d'échange de clés **Diffie-Hellman** qui dépend de l'arithmétique modulaire.

L'algorithme de courbe elliptique dépend du problème de logarithme discret de la courbe elliptique et fournit plus de sécurité que les autres algorithmes lorsque les deux sont utilisés avec des clés de même longueur.

- Know the fundamental requirements of a hash function

Les bonnes fonctions de hachage ont cinq exigences, elles doivent :

- permettre une entrée de n'importe quelle longueur,
- fournir une sortie de longueur fixe,
- rendre relativement facile le calcul de la fonction de hachage pour toute entrée,
- fournir une fonctionnalité unidirectionnelle
- et éviter les collisions

- Be familiar with the major hashing algorithms

Les successeurs de l'algorithme SHA (Secure Hash Algorithm), SHA-1 et SHA-2, constituent les fonctions de hash de message standard du gouvernement. **SHA-1** produit un résumé de message de 160 bits tandis que **SHA-2** prend en charge des longueurs variables, allant jusqu'à 512 bits. **SHA-3** reste en développement et le NIST pourrait le publier sous sa forme finale bientôt.

- Know how cryptographic salts improve the security of password hashing

Lorsque le hachage simple (straightforward hashing) est utilisé pour stocker les mots de passe dans un fichier de mot de passe, les attaquants peuvent utiliser des **tables arc-en-ciel** (rainbow tables) de valeurs pré calculées pour identifier les mots de passe couramment utilisés.

Ajouter des sels (**salts**) aux mots de passe avant de les hacher réduit l'efficacité des attaques des rainbow tables.

- Understand how digital signatures are generated and verified

Pour signer numériquement un message, utilisez d'abord une fonction de hachage pour générer un résumé de message. Ensuite, cryptez le résumé avec votre clé privée. Pour vérifier la signature numérique d'un message, déchiffrer la signature avec la clé publique de l'expéditeur, puis comparez le résumé du message à celui que vous générez vous-même. Si elles correspondent, le message est authentique.

- Know the components of the Digital Signature Standard (DSS)

DSS (Digital Signature Standard) utilise les hashing (message digest) SHA-1 et SHA-2 avec l'un des trois algorithmes de cryptage suivants: l'algorithme de signature numérique (Digital Signature Algorithm - DSA); l'algorithme Rivest, Shamir, Adleman (RSA); ou l'algorithme Elliptic Curve DSA (ECDSA).

- Understand the public key infrastructure (PKI)

Dans l'infrastructure à clé publique, les autorités de certification (CA) génèrent des certificats numériques contenant les clés publiques des utilisateurs du système. Les utilisateurs distribuent ensuite ces certificats aux personnes avec lesquelles ils souhaitent communiquer. Les destinataires du certificat vérifient les certificats à l'aide de la clé publique de l'autorité de certification

- Know the common applications of cryptography to secure email

La nouvelle norme pour les messages cryptés est le protocole S/MIME. Un autre outil de sécurité de messagerie populaire est Phil Zimmerman's Pretty Good Privacy (PGP). La plupart des utilisateurs du cryptage des e-mails utilisent les technologies intégrées à leur client de messagerie ou à leur service de messagerie Web.

- Know the common applications of cryptography to secure web activity

De facto, la norme pour le trafic Web sécurisé est l'utilisation de HTTP sur TLS (Transport Layer Security) ou de l'ancien protocole SSL (Secure Sockets Layer). La plupart des navigateurs Web prennent en charge les deux normes, mais de nombreux sites Web abandonnent la prise en charge du protocole SSL en raison de problèmes de sécurité.

- Know the common applications of cryptography to secure networking

Le protocol IPsec fournit un cadre commun, une norme, pour le cryptage du trafic réseau et est intégrée dans un certain nombre de systèmes d'exploitation communs. En **mode de transport** IPsec, le contenu des paquets est chiffré pour la communication entre peer. En **mode tunnel**, le paquet entier, y compris les informations d'en-tête, est chiffré pour les communications de passerelle à passerelle.

- Be able to describe IPsec

IPsec est un Framework d'architecture de sécurité qui prend en charge la communication sécurisée sur IP. IPsec établit un canal sécurisé en **mode transport** ou en **mode tunnel**. Il peut être utilisé pour établir une communication directe entre ordinateurs ou pour établir un VPN entre réseaux.

IPsec utilise deux protocoles:

- Authentication Header (**AH**)
- Encapsulating Security Payload (**ESP**)

- Be able to explain common cryptographic attacks

Les attaques par **Brute-force** sont des tentatives de recherche aléatoire de la clé cryptographique correcte.

Les attaques de type « texte clair connu » (**Known plaintext**), de type « texte chiffré choisi » (**chosen ciphertext**), et de type « texte clair choisi » (**chosen plaintext**) nécessitent que l'attaquant dispose d'une partie des informations en plus du texte chiffré.

L'attaque de l'homme du milieu (**man-in-the-middle**) exploite des protocoles qui utilisent deux cycles de chiffrement. L'attaque man-in-the-middle dupe les deux parties dans la communication avec l'attaquant au lieu.

L'attaque d'anniversaire (**the birthday attack**) est une tentative pour trouver des collisions dans les fonctions de hachage.

L'attaque de rejeu (**replay attack**) est une tentative de réutilisation des demandes d'authentification.

- Understand uses of digital rights management (DRM)

Les solutions de gestion des droits numériques (Digital rights management - DRM) permettent aux propriétaires de contenu d'imposer des restrictions sur l'utilisation de leur contenu par d'autres. Les solutions DRM protègent généralement les contenus de divertissement, tels que la musique, les films et les livres électroniques, mais sont parfois présentes dans l'entreprise, protégeant les informations sensibles stockées dans les documents.

- Explain the process Bob should use if he wants to send a confidential message to Alice using asymmetric cryptography ***

Bob devrait crypter le message en utilisant la clé publique d'Alice, puis transmettre le message crypté à Alice.

- Explain the process Alice would use to decrypt the confidential message encrypted using Alice public key ***

Alice devrait déchiffrer le message en utilisant sa clé privée.

- Explain the process Bob should use to digitally sign a message to Alice ***

Bob devrait générer un hash (message digest) à partir du message en texte clair à l'aide d'une fonction de hachage. Il devrait ensuite crypter le hash du message en utilisant sa propre clé privée pour créer la signature numérique. Enfin, il doit ajouter la signature numérique au message et la transmettre à Alice.

- Explain the process Alice should use to verify the digital signature on the message from Bob ***

Alice devrait déchiffrer la signature numérique dans le message de Bob en utilisant la clé publique de Bob. Elle doit ensuite créer un hash (message digest) du message à partir du message en texte clair en utilisant le même algorithme de hachage que celui utilisé par Bob pour créer la signature numérique. Enfin, elle devrait comparer les deux hash. S'ils sont identiques, la signature est authentique.

Chapter 8: Principles of Security Models, Design, and Capabilities

- Know details about each of the access control models

Connaître les modèles de contrôle d'accès et leurs fonctions.

Le modèle de machine d'état (**state machine model**) garantit que toutes les instances d'objets accédant aux objets sont sécurisées.

Le modèle de flux d'informations (**information flow model**) est conçu pour empêcher le flux d'informations non autorisé, non sécurisé ou restreint.

Le modèle de non-interférence (**noninterference model**) empêche les actions d'un sujet d'affecter l'état du système ou les actions d'un autre sujet.

Le modèle Take-Grant (**Take-Grant model**) dicte comment les droits peuvent être transmis d'un sujet à un autre ou d'un sujet à un objet.

Une matrice de contrôle d'accès (**control matrix**) est une table de sujets et d'objets qui indique les actions ou les fonctions que chaque sujet peut effectuer sur chaque objet.

Les sujets du modèle **Bell-LaPadula** ont un niveau d'autorisation qui leur permet d'accéder uniquement aux objets ayant les niveaux de classification correspondants. Cela impose la confidentialité.

Le modèle **Biba** empêche les sujets ayant des niveaux de sécurité inférieurs d'écrire sur des objets à des niveaux de sécurité plus élevés.

le modèle **Clark-Wilson** est un modèle d'intégrité qui repose sur l'audit pour s'assurer que les sujets non autorisés ne peuvent pas accéder aux objets et que les utilisateurs autorisés accèdent correctement aux objets.

Biba et **Clark-Wilson** renforcent l'intégrité. **Goguen-Meseguer** et **Sutherland** se concentrent sur l'intégrité. **Graham-Denning** se concentre sur la création et la suppression sécurisées de sujets et d'objets.

- Know the definitions of certification and accreditation

La **certification** est une technique d'évaluation de chaque partie d'un système informatique pour évaluer sa concordance avec les normes de sécurité. L'**accréditation** est le processus d'acceptation formelle d'une configuration certifiée d'une autorité désignée.

- Be able to describe open and closed systems

Les systèmes ouverts (**Open systems**) sont conçus selon les normes de l'industrie et sont généralement faciles à intégrer à d'autres systèmes ouverts. Les systèmes fermés (**Closed systems**) sont généralement des matériels et/ou logiciels propriétaires; leurs spécifications ne sont normalement pas publiées, et elles sont généralement plus difficiles à intégrer avec d'autres systèmes.

- Know what confinement, bounds, and isolation are

Le confinement (**Confinement**) limite un processus à la lecture et à l'écriture dans certains emplacements de mémoire. Les limites (**Bounds**) sont les limites de la mémoire qu'un processus ne peut dépasser lors de la lecture ou de l'écriture. L'isolement (**Isolation**) est le mode dans lequel un processus s'exécute lorsqu'il est confiné par l'utilisation de limites de mémoire.

- Be able to define object and subject in terms of access

Le **sujet** est l'utilisateur ou le processus qui effectue une demande d'accès à une ressource. L'**objet** est la ressource à laquelle un utilisateur ou un processus souhaite accéder.

- Know how security controls work and what they do

Les contrôles de sécurité utilisent des règles d'accès pour limiter l'accès d'un sujet à un objet.

- Be able to list the classes of TCSEC, ITSEC, and the Common Criteria

Ce tableau couvre et compare les classements équivalents et applicables pour TCSEC, ITSEC et CC (rappelez-vous que les classes de fonctionnalité F7 à F10 dans ITSEC n'ont pas de correspondante dans TCSEC).

UNIVERSITY of HAWAII WEST OAHU			
Standards Overview			
TCSEC	ITSEC	CC	Designation
A1	F6+E6	EAL 7	Verified Security
B3	F5+E5	EAL 6	Security Domains
B2	F4+E4	EAL 5	Structured Security
B1	F3+E3	EAL 4	Security Labels
C2	F2+E2	EAL 3	Controlled Access
C1	F1+E1	EAL 2	Discretionary Security
D	E0	EAL 1	Minimal Security

- Define a trusted computing base (TCB)

Une base d'ordinateur de confiance (Trusted Computing Base - TCB) est la combinaison du matériel, des logiciels et des contrôles qui forment une base de confiance qui répond à la politique de sécurité.

- Be able to explain what a security perimeter is

Un périmètre de sécurité (**security perimeter**) est la frontière imaginaire qui sépare le TCB (l'ordinateur de confiance) du reste du système. Les composants TCB communiquent avec des composants non-TCB en utilisant des chemins approuvés.

- Know what the reference monitor and the security kernel are

Le moniteur de référence (**The reference monitor**) est la partie logique du TCB qui confirme si un sujet a le droit d'utiliser une ressource avant d'accorder l'accès. Le noyau de sécurité (**The security kernel**) est la collection des composants TCB qui implémentent la fonctionnalité du moniteur de référence.

- Understand the security capabilities of information systems

Les fonctionnalités de sécurité courantes (**Common security capabilities**) incluent la protection de la mémoire, la virtualisation et le module de la plateforme de confiance (**Trusted Platform Module - TPM**).

- Name at least seven security models ***

Les modèles de sécurité comprennent :

- information flow,
- noninterference,
- Take-Grant,
- access control matrix,
- Bell-LaPadula,
- Biba,
- Clark-Wilson,
- Brewer and Nash (aka Chinese Wall),
- Goguen-Meseguer,
- Sutherland,
- Graham-Denning.

- Describe the primary components of TCB ***

Les composants principaux de la base d'une informatique sécurisée (Trusted computing base - TCB) sont les éléments matériels (hardware) et logiciels (software) utilisés pour appliquer la politique de sécurité (ces éléments sont appelés TCB), le périmètre de sécurité distinguant et séparant les composants TCB des composants non TCB, et le moniteur de référence qui sert de dispositif de contrôle d'accès à travers le périmètre de sécurité.

- What are the two primary rules or principles of the Bell-LaPadula security model ? Also, what are the two rules of Biba? ***

Les deux règles principales de **Bell-LaPadula** sont la simple règle de non-lecture vers le haut (**no read-up**) et la règle de l'étoile de non-écriture vers le bas (**star rule of no write-down**).

Les deux règles de **Biba** sont la règle simple d'aucune lecture vers le bas (**no read-down**) et la règle d'étoile de non-écriture vers le haut (**star rule of no write-up**).

- What is the difference between open and closed systems and open and closed source ? ***

Un système ouvert est un système avec des API publiées qui permettent à des tiers de développer des produits pour interagir avec lui. Un système fermé est un système propriétaire sans support de produit tiers. L'**open source** est une position de codage qui permet à un tiers d'afficher le code source d'un programme. Les **sources fermées** sont une position de codage opposée qui maintient le code source confidentiel.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

- Be able to explain the differences between multitasking, multithreading, multiprocessing, and multiprogramming

Le multitâche (**multitasking**) est l'exécution simultanée de plus d'une application sur un ordinateur et est géré par le système d'exploitation.

Le **multithreading** permet d'effectuer plusieurs tâches simultanées au sein d'un même processus.

Le multitraitement (**multiprocessing**) consiste à utiliser plusieurs processeurs pour augmenter la puissance de calcul.

La multiprogrammation (**multiprogramming**) est similaire au multitâche (multitasking) mais a lieu sur des systèmes mainframe et nécessite une programmation spécifique.

- Understand the differences between **single state** processors and **multistate** processors

Les processeurs à état unique (**single state processors**) sont capables de fonctionner à un seul niveau de sécurité à la fois, alors que les processeurs multi-états (**multistate processors**) peuvent fonctionner simultanément à plusieurs niveaux de sécurité.

- Describe the **four security modes** approved by the federal government for processing classified information

Les systèmes dédiés requièrent que tous les utilisateurs disposent des autorisations appropriées (**appropriate clearance**), des autorisations d'accès (**access permissions**) et le besoin de savoir (**need-to-know**) que toutes les informations stockées sur le système.

Le mode élevé (**system high mode**) du système supprime l'exigence de besoin de savoir (need-to-know) .

Le mode compartimenté (**compartmented**) supprime l'exigence de besoin de savoir (need-to-know) et la condition d'autorisation d'accès (access permission).

Le mode multi niveau (**multi level**) supprime les trois exigences.

- Explain the **two layered operating modes** used by most modern processors

Les applications utilisateur fonctionnent dans un environnement d'ensemble d'instructions limité appelé mode utilisateur (**user mode**).

Le système d'exploitation effectue des opérations contrôlées en mode privilégié (privileged mode), également connu sous le nom de mode système (**system mode**), mode noyau (**kernel mode**) et mode de supervision (**supervisory mode**).

- Describe the different **types of memory** used by a computer

La **ROM** est non volatile et ne peut pas être écrite par l'utilisateur. L'utilisateur peut écrire des données sur les puces **PROM** une seule fois. Les puces **EPROM** peuvent être effacées grâce à l'utilisation de la lumière ultraviolette et peuvent ensuite recevoir de nouvelles données. Les puces d'**EEPROM** peuvent être effacées avec le courant électrique et ensuite avoir de nouvelles données écrites. Les puces **RAM** sont volatiles et perdent leur contenu lorsque l'ordinateur est éteint.

- Know the security issues surrounding memory components

Three main security issues surround memory components: the fact that data may remain on the chip after power is removed, the fact that memory chips are highly pilferable, and the control of access to memory in a multiuser system.

Trois problèmes de sécurité principaux entourent les composants de la mémoire:

- le fait que les données peuvent rester sur la puce après la coupure de courant,
- le fait que les puces de mémoire soient hautement « chapardables » (pilferable),
- le contrôle de l'accès à la mémoire dans un système multi-utilisateur.

- Describe the different characteristics of **storage devices** used by computers

Le stockage principal est à la mémoire. Le stockage secondaire consiste en un support magnétique ou optique qui doit d'abord être lu et transféré dans la mémoire primaire avant que la CPU puisse utiliser les données.

Les dispositifs de stockage à accès aléatoire (**random**) peuvent être lus à tout moment, tandis que les dispositifs à accès séquentiel nécessitent un balayage à travers toutes les données stockées physiquement avant l'emplacement souhaité.

- Know the security issues surrounding **secondary storage devices**

Les périphériques de stockage secondaires présentent trois problèmes de sécurité principaux :

- les supports amovibles peuvent être utilisés pour voler des données,
- les contrôles d'accès et le chiffrement doivent être appliqués pour protéger les données,
- les données peuvent rester sur le support même après la suppression du fichier ou un formatage

- Understand security risks that input and output devices can pose

Les périphériques d'entrée/sortie peuvent faire l'objet d'écoute clandestine et illicites (eavesdropping and tapping), utilisés pour faire extraire des données d'une organisation, ou utilisés pour créer des points d'entrée non autorisés et non sécurisés dans les systèmes et les réseaux d'une organisation. Soyez prêt à reconnaître et à atténuer ces vulnérabilités.

- Understand I/O addresses, configuration, and setup

L'utilisation d'anciens périphériques PC nécessite une certaine compréhension des IRQ, des DMA et des I/O mappées en mémoire. Soyez prêt à reconnaître et contourner les conflits d'adresses potentiels et les mauvaises configurations et à intégrer les anciens périphériques avec leurs homologues Plug-and-Play (PnP).

- Know the purpose of firmware

Le micrologiciel (firmware) est un logiciel stocké sur une puce ROM. Au niveau de l'ordinateur, il contient les instructions de base nécessaires pour démarrer un ordinateur. Le micrologiciel (firmware) est également utilisé pour fournir des instructions d'utilisation dans les périphériques tels que les imprimantes.

- Be able to describe process isolation, layering, abstraction, data hiding, and hardware segmentation

L'isolation des processus garantit que les processus individuels peuvent accéder uniquement à leurs propres données. La superposition (**layering**), crée différents domaines de sécurité au sein d'un processus et limite la communication entre eux. **L'abstraction** crée des interfaces de type « boîtes noires » que les programmeurs peuvent utiliser sans avoir besoin de connaître le fonctionnement interne d'un algorithme ou d'un périphérique. Le masquage des données (**data hiding**) empêche la lecture des informations à partir d'un niveau de sécurité différent. La segmentation matérielle (**hardware segmentation**) impose l'isolation des processus avec des contrôles physiques

- Understand how a security policy drives system design, implementation, testing, and deployment.

Le rôle d'une politique de sécurité est d'informer et de guider la conception, le développement, la mise en œuvre, le test et la maintenance d'un système particulier.

- Understand cloud computing

Le « cloud computing » est le terme courant qui désigne un concept d'informatique où le traitement et le stockage sont effectués au travers d'une connexion réseau plutôt que localement. Le « cloud computing » est souvent considéré comme de l'informatique basée sur Internet.

- Understand mobile device security

La sécurité des périphériques implique une gamme d'options de sécurité potentielles ou de fonctionnalités pouvant être disponibles pour un périphérique mobile. Tous les appareils électroniques portables (**portable electronic devices - PEDs**) n'ont pas de bonnes caractéristiques de sécurité. Les fonctionnalités de sécurité PED incluent le cryptage complet, l'effacement à distance (**remote wiping**), le verrouillage (**lockout**), le verrouillage des écrans (**screen locks**), le contrôle des applications, la segmentation du stockage (**storage segmentation**), le suivi des actifs (**asset tracking**), le contrôle des stocks (**inventory control**), la gestion des périphériques mobiles (**device access control**), le stockage amovible (**removable storage**) et la désactivation des fonctionnalités inutilisées (**the disabling of unused features**).

- Understand mobile device application security

Les applications et les fonctions utilisées sur un appareil mobile doivent être sécurisées. Les concepts associés incluent la gestion des clés (**key management**), la gestion des informations d'identification (**credential management**), l'authentification (**authentication**), la géolocalisation (**geotagging**), le chiffrement (**encryption**),

la liste blanche (**whitelisting**) des applications et l'authentification transitive et de confiance (**transitive trust/authentication**).

- Understand BYOD

« Apportez votre propre appareil » (**Bring your own device - BYOD**) est une politique qui permet aux employés d'apporter leurs propres appareils mobiles personnels pour ensuite les utiliser pour se connecter au réseau de l'entreprise afin de bénéficier des ressources professionnelles et/ou Internet. Bien que le BYOD participe à améliorer le moral et la satisfaction des employés sur leur lieu de travail, il augmente les risques de sécurité pour l'organisation. Les problèmes liés à BYOD incluent la propriété des données, le support informatique, la gestion des correctifs et patch de sécurité, la gestion des antivirus, l'investigation criminalistique (forensics), la confidentialité, l'intégration (on-boarding/off-boarding process), l'adhésion aux politiques de l'entreprise, l'acceptation/ la collaboration des utilisateurs (user acceptance), les problématiques d'architecture et d'infrastructure, les caméras et micros embarquées, le cadre juridique.

- Understand embedded systems and static environments

Un **système intégré** (ou embarqué) (embedded system) est généralement conçu autour d'un ensemble limité de fonctions spécifiques par rapport au produit plus grand dont il est un composant. Les **environnements statiques** sont des applications, des systèmes d'exploitation, des ensembles de matériel ou des réseaux configurés pour un besoin, une fonctionnalité ou une fonction spécifique, puis configurés pour rester inchangés.

- Understand embedded systems and static environment security concerns

Les environnements statiques, les systèmes embarqués (**embedded systems**) et les autres environnements informatiques à usage limités ou unique nécessitent une gestion de la sécurité. Ces techniques peuvent inclure la segmentation d réseau, les couches de sécurité, les pare-feu applicatifs, les mises à jour manuelles, le contrôle des versions firmware, la redondance et la diversité des contrôles.

- Understand how the principle of least privilege, separation of privilege, and accountability apply to computer architecture

Le principe du moindre privilège (**least privilege**) garantit que seul un nombre minimum de processus est autorisé à fonctionner en mode supervision. La séparation des privilèges (**separation of privilege**) augmente la granularité des opérations sécurisées. La traçabilité (**Accountability**) garantit l'existence de solutions de vérification pour retracer les opérations effectuées.

- Be able to explain what covert channels are

Un « canal caché » (**covert channel**) est une méthode utilisée pour transmettre des informations mais qui n'est normalement pas utilisée dans un usage courant.

- Understand what buffer overflows and input checking are.

Un débordement de tampon (A buffer overflow) se produit lorsque le programmeur ne vérifie pas la taille des données d'entrée avant d'écrire les données dans un emplacement de mémoire spécifique. En fait, toute défaillance de validation des données d'entrée pourrait entraîner une violation de la sécurité

- Describe common flaws to security architectures.

Outre les dépassements de mémoire tampon (buffer overflows), les programmeurs peuvent laisser des portes dérobées (back doors) et des programmes privilégiés (privileged programs) sur un système après son déploiement. Même les systèmes bien écrits peuvent être sensibles aux attaques de type « time-of-check-to-time-of-use » (TOCTTOU). Tout changement d'état pourrait être une fenêtre d'opportunité potentielle pour un attaquant de compromettre un système.

- What are the terms used to describe the various computer mechanisms that allow multiple simultaneous activities ? ***

Les termes utilisés pour décrire les divers mécanismes informatiques qui permettent plusieurs activités simultanées sont :

- le traitement multitâche (multitasking),

- le multitraitement (multiprocessing),
- la multiprogrammation (multiprogramming),
- le multithreading,
- le traitement multi états (multistate processing).

▪ What are the four **security modes** for systems processing classified information ? **

Les quatre modes de sécurité sont :

- dédiés (dedicated),
- système élevé (system high),
- compartimenté (compartmented),
- multiniveau (multilevel).

▪ Name the three pairs of aspects or features used to describe **storage** ***

Les trois paires d'aspects ou de caractéristiques utilisés pour décrire le stockage sont :

- primaires vs. secondaires,
- volatiles vs. non volatiles,
- aléatoires vs séquentielles.

▪ Name some vulnerabilities found in distributed architectures ***

Les vulnérabilités trouvées dans une architecture distribuée incluent :

- des données sensibles trouvées sur les ordinateurs de bureau ou portables,
- un manque de compréhension de la sécurité de la part des utilisateurs,
- un risque accru de vol de composants physiques,
- un risque de compromission de l'ensemble du réseau par un logiciel installé par l'utilisateur (malware)
- des données sur les clients moins susceptibles d'être inclus dans les sauvegardes.

Chapter 10: Physical Security Requirements

▪ Understand why there is no security without **physical security**

Sans contrôle de l'environnement physique, les contrôles d'accès administratifs ou techniques (technical/logical) ne peuvent pas atteindre un niveau de sécurité adéquate. Si une personne malveillante peut accéder physiquement à vos locaux et/ou équipements, elle peut effectuer à peu près tout ce qu'elle veut, de la destruction à la divulgation et à l'altération.

▪ Be able to list **administrative physical security controls**

Des exemples de contrôles administratifs de la sécurité physique (**administrative physical security**) sont la construction et la sélection des locaux, la gestion du site, les contrôles du personnel, la sensibilisation (awareness training), la réponse à incident (emergency response), et les procédures d'urgence (emergency procedures).

▪ Be able to list the **technical physical security controls**

Les contrôles techniques de sécurité physique (Technical physical security controls) peuvent être des contrôles d'accès, la détection d'intrusion, les systèmes d'alarme, la vidéosurveillance (closed-circuit television - CCTV), la surveillance (monitoring), le système de chauffage/ventilation/climatisation (Heating, Ventilation and Air-Conditioning - HVAC), et détection incendies.

▪ Be able to name the **physical controls** for physical security

Les contrôles physiques pour la sécurité physique sont les clôtures (fencing), l'éclairage (lighting), les serrures (locks), les matériaux de construction, les sas d'accès (mantraps), les chiens et les gardes.

▪ Know the functional order of controls

L'ordre fonctionnel des contrôles (the functional order of controls) est :

- la dissuasion (deterrence),

- puis le déni (denial),
- puis la détection (detection),
- puis le retard (delay).

▪ Know the key elements in making a site selection and designing a facility for construction.

Les éléments clés dans la sélection d'un site sont la visibilité, la composition de la zone environnante (surrounding area), l'accessibilité de la zone et les impacts d'une catastrophe naturelle. Un élément clé dans la conception d'une installation pour la construction est de comprendre le niveau de sécurité requis par votre organisation et de la planifier avant le début de la construction.

▪ Know how to design and configure secure work areas.

Il ne devrait pas y avoir un accès égal à tous les locaux d'une organisation. Les zones qui contiennent des actifs de valeur ou d'importance plus élevée devraient avoir un accès restreint. Les biens précieux (valuable assets) et confidentiels devraient être situés dans le cœur ou le centre de protection d'un site. De plus, les salles serveurs ou d'ordinateurs centralisés ne doivent pas nécessairement être compatibles avec locaux dédiés au personnel.

▪ Understand the security concerns of a wiring closet

Une armoire de câblage (**wiring closet**) est l'endroit où les câbles réseau d'un bâtiment entier ou d'un étage sont connectés à d'autres équipements essentiels, tels que des panneaux de brassage (patch panels), des commutateurs (switch), des routeurs (routers), des extensions LAN (LAN extenders) et des liens vers les coeurs de réseau (backbone channels). La plupart de la sécurité d'une armoire de câblage (ou baie de brassage) se concentre sur la prévention de l'accès non autorisé physique. Si un intrus non autorisé accède à ce type de zone, il peut être en mesure de voler des équipements, de tirer ou de couper des câbles, ou même de positionner un dispositif d'écoute.

▪ Understand how to handle visitors in a secure facility.

Si une installation utilise des zones réglementées pour contrôler la sécurité physique, un mécanisme de gestion des visiteurs (**to handle visitors**) est requis. Souvent, une escorte est attribuée aux visiteurs, et leur accès et activités sont surveillées de près. Ne pas suivre les actions des étrangers lorsqu'ils ont accès à une zone protégée peut entraîner une activité malveillante (malicious activity) contre les actifs les plus protégés

▪ Know the three categories of security controls implemented to manage physical security and be able to name examples of each

Les contrôles de sécurité mis en place pour gérer la sécurité physique peuvent être divisés en trois groupes:

- administratif,
- technique
- et physique.

Comprendre quand et comment utiliser chaque groupe de contrôle, et être capable de lister des exemples de chaque type.

▪ Understand security needs for media storage

Les locaux de stockage des médias de sauvegarde ou d'archivage doivent être conçus pour stocker en toute sécurité les supports vierges, les supports réutilisables et les supports d'installation. Les préoccupations incluent le vol (theft), la corruption (corruption) et la récupération des données restantes (data remnant recovery). Les protections des installations de stockage multimédia (Media storage facility) comprennent des armoires verrouillées (locked cabinets) ou des coffres-forts (safes), l'utilisation d'un bibliothécaire/gardien (librarian/custodian), la mise en œuvre d'un processus d'enregistrement (check-in/check-out) et de nettoyage des médias (media sanitization).

▪ Understand the concerns of evidence storage

Le stockage des preuves (evidence storage) permet de conserver les journaux (logs), les images disques, les instantanés (snapshot) de machines virtuelles et d'autres sources de données pour la récupération, les enquêtes internes et les enquêtes judiciaires (forensic investigations). Les protections incluent des installations de stockage dédiées / isolées, le stockage hors ligne, le suivi des activités (tracking), la gestion des hash, les restrictions d'accès et le cryptage.

- Know the common threats to physical access controls

Quelle que soit la forme de contrôle d'accès physique utilisée, un agent de sécurité ou un autre système de surveillance doit être déployé pour empêcher les abus, le **camouflage** (masquerading) et le **ferrouillage** (piggybacking). Les abus du contrôle d'accès physique comprennent l'appui des portes sécurisées ouvertes et le contournement des serrures ou des contrôles d'accès. Le camouflage (**Masquerading**) consiste à utiliser l'identifiant de sécurité de quelqu'un d'autre pour accéder à une installation. Le « **Piggybacking** » consiste à suivre quelqu'un à travers une porte sécurisée sans être identifié ou autorisé personnellement

- Understand the need for audit trails and access logs

Les pistes d'audit et les journaux d'accès sont des outils utiles même pour le contrôle d'accès physique. Ils peuvent avoir besoin d'être créés manuellement par les gardes de sécurité; ou peuvent être générés automatiquement si des mécanismes de contrôle d'accès en place le permettent (cartes à puce, badges, lecteurs de proximité). Vous devriez également envisager la surveillance des points d'entrée avec un système vidéo CCTV. Grâce à CCTV, vous pouvez comparer les pistes de vérification et les journaux d'accès avec un historique visuellement enregistré des événements. De telles informations sont essentielles pour reconstruire les événements d'une intrusion, d'une violation ou d'une attaque.

- Understand the need for clean power

L'énergie fournie par les compagnies d'électricité n'est pas toujours cohérente et propre. La plupart des équipements électroniques exigent une alimentation propre pour fonctionner correctement. Les dommages à l'équipement causés par les fluctuations de puissance sont fréquents. De nombreuses organisations choisissent de gérer leur propre énergie électrique par plusieurs moyens. Un onduleur (**Uninterruptible Power Supply - UPS**) est un type de batterie auto-chargé qui peut être utilisé pour fournir une alimentation propre constante à un équipement sensible. Les onduleurs/UPS fournissent également une alimentation continue même après la panne de la source d'alimentation principale. Un onduleur peut continuer à fournir de l'énergie pendant quelques minutes à quelques heures selon sa capacité et la consommation de l'équipement.

- Know the terms commonly associated with power issues

Connaître les définitions de ce qui suit : fault, blackout, sag, brownout, spike, surge, inrush, noise, transient, clean, and ground.

- Understand how to control the environment

En plus des considérations d'énergie, le maintien de l'environnement implique un contrôle sur les mécanismes HVAC (Heating, Ventilation and Air-Conditioning). Les pièces contenant principalement des ordinateurs doivent être conservées à une température comprise entre 15 et 23 degrés Celsius (60 à 75 degrés Fahrenheit). L'humidité dans une salle informatique devrait être maintenue entre 40 et 60%. Trop d'humidité peut causer de la **corrosion**. Trop peu d'humidité provoque de l'**électricité statique**.

- Know about static electricity

Même sur des moquettes non statiques (ou antistatiques) (nonstatic carpeting) , si l'environnement a une faible humidité, il est toujours possible de générer des décharges statiques de 20 000 volts. De faibles décharge d'électricité statique peuvent tout de même détruire les équipements électroniques.

- Understand the need to manage water leakage and flooding

Les fuites d'eau (**water leakage**) et les inondations (**flooding**) doivent être traitées dans votre politique et procédures de sécurité environnementale. Les fuites de plomberie (**plumbing leaks**) ne sont pas quotidiennes, mais lorsqu'elles surviennent, elles causent souvent des dommages importants. L'eau et l'électricité ne se mélangent pas. Si votre système informatique entre en contact avec de l'eau, en particulier lorsqu'il fonctionne, des dommages sont inévitables. Dans la mesure du possible, placez les salles serveurs et les équipements informatiques critiques à l'écart de toute source ou conduite d'eau.

- Understand the importance of fire detection and suppression

La détection et la suppression des incendies ne doivent pas être négligées (not be overlooked). Protéger le personnel contre les dommages devrait toujours être **l'objectif le plus important** de tout système de sécurité ou de

protection. En plus de protéger les personnes, la détection et la suppression des incendies sont conçues pour minimiser les dommages causés par le feu, la fumée, la chaleur et pour minimiser les dommages causés par les composants utilisés lors de l'extinction (suppression materials), en particulier, en ce qui concerne l'infrastructure informatique.

- Understand the possible contamination and damage caused by a fire and suppression.

Les éléments destructeurs d'un feu comprennent la fumée et la chaleur, mais aussi les moyens de suppression, tel que l'eau ou l'acide sodique. La fumée endommage la plupart des périphériques de stockage. La chaleur peut endommager tout composant électronique ou informatique. Les moyens de suppression peuvent provoquer des courts-circuits, initier la corrosion ou rendre le matériel inutilisable. Toutes ces questions doivent être abordées lors de la conception d'un système d'extinction du feu.

- Understand personnel privacy and safety

En toutes circonstances et dans toutes les conditions, l'aspect le plus important de la sécurité est la protection des personnes. Ainsi, prévenir les dommages aux personnes est l'objectif le plus important pour toutes les solutions de sécurité.

- What kind of device helps to define an organization's perimeter and also serves to deter casual trespassing ? ***

Une clôture (fence) est une excellente protection de périmètre qui peut aider à prévenir les intrusions occasionnelles (casual trespassing). Les installations moyennement sécuritaires fonctionnent lorsque la clôture mesure de 6 à 8 pieds (feet) de hauteur et sont généralement des clôtures à cyclone, aussi appelée maillon de chaîne (chain link), dont le haut est torsadée ou barbelée (twisted or barbed) pour dissuader les grimpeurs occasionnels. Les installations plus sécurisées optent généralement pour des hauteurs de clôture de plus de 8 pieds et comprennent souvent plusieurs brins de barbelés ou de fils de rasoir enfilés au-dessus du tissu à maillons de chaîne pour dissuader davantage les grimpeurs.

- What is the problem with halon-based fire suppression technology ? ***

Halon se dégrade en gaz toxiques à 900 degrés Fahrenheit (420 degrés Celsius). De plus, il n'est pas écologique, il s'agit d'une substance appauvrissant la couche d'ozone. Le halon recyclé est disponible, mais la production de halons a cessé dans les pays développés en 2003. Le halon est souvent remplacé par un moyen plus écologique et moins toxique.

- What kinds of potential issues can an emergency visit from the fire department leave in its wake ? ***

Chaque fois que de l'eau est utilisée pour faire face à un incendie, à des flammes ou à de la fumée, les dégâts causés par l'eau deviennent une préoccupation sérieuse, en particulier lorsque de l'eau est projetée dans les zones où l'équipement électrique est utilisé. Non seulement les ordinateurs et autres appareils électriques peuvent être endommagés ou détruits par l'eau, mais de nombreuses formes de supports de stockage peuvent également être endommagées ou inutilisables. De plus, lorsqu'ils recherchent des points chauds à éteindre, les pompiers utilisent souvent des haches pour briser les portes ou couper des murs pour les atteindre le plus rapidement possible. Cela peut également entraîner des dommages physiques ou la destruction de dispositifs et / ou de câblage qui peuvent également se trouver à proximité.

Domain 4: Communication and Network Security

Chapter 11: Secure Network Architecture and Securing Network Components

- Know the OSI model layers and which protocols are found in each.

Les sept couches et les protocoles pris en charge par chacune des couches du modèle OSI sont les suivants:

- **Application** : HTTP, FTP, LPD, SMTP, Telnet, TFTP, EDI, POP3, IMAP, SNMP, NNTP, S-RPC, and SET
- **Presentation**: Encryption protocols and format types, such as ASCII, EBCDIC, TIFF, JPEG, MPEG, and MIDI
- **Session**: NFS, SQL, and RPC
- **Transport**: SPX, SSL, TLS, TCP, and UDP
- **Network**: ICMP, RIP, OSPF, BGP, IGMP, IP, IPsec, IPX, NAT, and SKIP
- **Data Link**: SLIP, PPP, ARP, RARP, L2F, L2TP, PPTP, FDDI, ISDN
- **Physical**: EIA/TIA-232, EIA/TIA-449, X.21, HSSI, SONET, V.24, and V.35

- Have a thorough knowledge of TCP/IP

Connaître la différence entre TCP et UDP; Familiarisez-vous avec les quatre couches TCP / IP (Application, Transport, Internet, and Link) et leur correspondance avec le modèle OSI. De plus, comprenez l'utilisation des ports connus et familiarisez-vous avec les sous-protocoles.

- Know the different cabling types and their lengths and maximum throughput rates

Connaître les différents types de câbles, leurs longueurs maximales (maximum length) et leurs débits maximums (maximum throughput). Ce inclus :

- STP, 10Base-T (UTP), 10Base2 (thinnet), 10Base5 (thicknet), 100Base-T, 1000Base-T,
- fiber-optic.

Vous devez être également familiarisé les catégories UTP de 1 à 7.

- Be familiar with the common LAN technologies

Les technologies LAN sont : Ethernet, Token Ring et FDDI. Connaître également :

- les communications analogiques et numériques;
- les communications synchrones et asynchrones;
- bande de base par rapport aux communications à large bande;
- les diffusions de type broadcast, multicast, and unicast
- CSMA, CSMA/CA et CSMA/CD; token passing; and polling.

- Understand secure network architecture and design.

La sécurité des réseaux doit prendre en compte les protocoles IP et non IP, le contrôle d'accès réseau, l'utilisation de services et de périphériques de sécurité, la gestion de protocoles multicouches et l'implémentation de la sécurité des points de terminaison (endpoint security).

- Understand the various types and purposes of network segmentation

La segmentation des réseaux peut être utilisée pour gérer le trafic, améliorer les performances et renforcer la sécurité. Les exemples de segments de réseau ou de sous-réseaux incluent **intranet**, **extranet** et **DMZ**.

- Understand the different wireless technologies

Les téléphones cellulaires (Cell phones), le Bluetooth (802.15) et les réseaux Wi-Fi (802.11) sont tous appelés « technologies sans fil », même s'ils sont tous différents. Soyez conscient de leurs différences, leurs forces et leurs faiblesses. Comprendre les bases de la sécurisation du réseau 802.11.

- Understand Fibre Channel

Fibre Channel est une forme de solution de stockage de données en réseau qui permet des transferts de fichiers à haute vitesse. Deux exemples d'implémentation: SAN (Storage Area Network) ou NAS (Network Attached Storage).

- Understand FCoE

FCoE (Fibre Channel over Ethernet) est utilisé pour encapsuler les communications Fibre Channel sur les réseaux Ethernet.

- Understand iSCSI

iSCSI (Internet Small Computer System Interface) est un standard de réseau de stockage basé sur IP.

- Understand 802.11 and 802.11a, b, g, n, and ac

802.11 est la norme IEEE pour les communications réseau sans fil. Les versions incluent :

- 802.11a (2 Mo),
- 802.11b (11 Mo),
- 802.11g (54 Mo).

La norme 802.11 définit également WEP (Wired Equivalent Privacy).

- Understand site survey

Une étude de site consiste à examiner la présence, la puissance et la portée des points d'accès sans fil déployés dans un environnement. Cette tâche implique généralement de se promener avec un appareil sans fil portable, en prenant note de la force du signal sans fil, et de cartographier les données sur une parcelle ou un schéma du bâtiment.

- Understand WEP

Le protocole WEP (Wired Equivalent Privacy) est défini par la norme IEEE 802.11. Il a été conçu pour offrir le même niveau de sécurité et de cryptage sur les réseaux sans fil que sur les réseaux filaires ou câblés. WEP offre une protection contre le reniflage de paquets (packet sniffing) et l'écoute clandestine (eavesdropping) contre les transmissions sans fil. Un avantage secondaire de WEP est qu'il peut être configuré pour empêcher l'accès non autorisé au réseau sans fil. WEP utilise une clé secrète partagée prédéfinie.

- Understand WPA

WPA (Wi-Fi Protected Access) était une alternative précoce à WEP. Cette technique était une amélioration mais elle-même n'était pas entièrement sécurisée. Il est basé sur les systèmes cryptographiques LEAP et TKIP et utilise une passphrase secrète.

- Understand WPA2

WPA2 est un nouveau schéma de chiffrement connu sous le nom de CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)(mode de comptage avec protocole de code d'authentification de message de chaînage de chiffrement) , basé sur le schéma de chiffrement AES.

- Understand EAP

EAP (Extensible Authentication Protocol) n'est pas un mécanisme spécifique d'authentification; c'est plutôt un cadre d'authentification. En effet, EAP permet aux nouvelles technologies d'authentification d'être compatibles avec les technologies de connexion sans fil ou point-à-point existantes.

- Understand PEAP

PEAP (Protected Extensible Authentication Protocol) encapsule les méthodes EAP dans un tunnel TLS qui fournit l'authentification et éventuellement le chiffrement.

- Understand LEAP

LEAP (Lightweight Extensible Authentication Protocol) est une alternative propriétaire de Cisco à TKIP pour WPA. Ce système a été mis au point pour remédier aux insuffisances du TKIP avant que le système 802.11i / WPA2 soit ratifié comme norme

- Understand MAC Filtering

Un filtre MAC (MAC filter) est une liste d'adresses MAC d'interface de clients Wi-Fi autorisées. Cette liste est utilisée par un point d'accès sans fil pour bloquer l'accès à tous les périphériques non autorisés.

- Understand SSID Broadcast

Les réseaux sans fil annoncent généralement leur SSID (Service Set Identifier) de façon régulière dans un paquet spécial connu sous le nom de « beacon frame ». Lorsque le SSID est diffusé, tout appareil doté d'une fonction de détection et de connexion automatique peut non seulement voir le réseau, mais il peut également établir une connexion avec le réseau.

- Understand TKIP

TKIP (Temporal Key Integrity Protocol) a été conçu pour remplacer le WEP sans nécessiter le remplacement du matériel sans fil existant. TKIP a été implémenté dans le réseau sans fil 802.11 sous le nom de WPA (Wi-Fi Protected Access).

- Understand CCMP

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)(mode de comptage avec protocole de code d'authentification de message de chaînage de chiffrement) a été créé pour remplacer WEP et TKIP / WPA. CCMP utilise AES (Advanced Encryption Standard) avec une clé de 128 bits.

- Understand captive portals

Un portail captif (captive portal) est une technique d'authentification qui redirige un client Web sans fil nouvellement connecté vers une page de contrôle d'accès au portail.

- Understand antenna types

Une grande variété de types d'antennes peut être utilisée pour les clients sans fil et les stations de base. Ceux-ci incluent des antennes polaires omnidirectionnelles aussi bien que beaucoup d'antennes directionnelles, telles que Yagi, cantenna, panneau, et parabolique.

- Know the standard network topologies

Les topologies réseau sont :

- en anneau (**ring**),
- en **bus**,
- en étoile (**star**),
- de type maillé (mesh).

- Know the common network devices

Les périphériques réseau communs sont :

- les pare-feu (**firewalls**)
- les routeurs (**routers**)
- les concentrateurs (**hubs**),
- les ponts (**bridges**),
- les modems (**modems**),
- les répéteurs (**repeaters**),
- les commutateurs (**switches**),
- les passerelles (**gateways**),
- les proxies (**proxies**).

▪ Understand the different types of firewalls

Il existe quatre types de pare-feu:

- le filtrage statique des paquets (**static packet filtering**),
- la passerelle au niveau de l'application (**application-level gateway**),
- la passerelle au niveau du circuit (**circuit-level gateway**),
- l'inspection dynamique (**stateful inspection**).

▪ Know the protocol services used to connect to LAN and WAN communication technologies

Il y a: Frame Relay, SMDS, X.25, ATM, HSSI, SDLC, HDLC, and ISDN.

▪ Name the layers of the OSI model and their numbers from top to bottom ***

- Application (7),
- Presentation (6),
- Session (5),
- Transport (4),
- Network (3),
- Data Link (2),
- Physical (1).

▪ Name three problems with cabling and the methods to counteract those issues ***

Les problèmes de câblage et leurs contre-mesures incluent

- **l'atténuation** (utilisation de répéteurs ou le non-respect des recommandations de distance),
- l'utilisation d'une **mauvaise catégorie** de câble (vérifiez les spécifications du câble par rapport aux exigences de débit),
- **la diaphonie** (crosstalk) (utiliser des câbles blindés, placer les câbles dans des conduits séparés ou utiliser des câbles de torsion différente par pouce)
- **les ruptures** de câble (cable breaks) (éviter de faire passer des câbles dans des endroits où le mouvement se produit),
- les interférences (utiliser un blindage de câble, utiliser des câbles avec des torsions supérieures par pouce),
- **l'espionner** (eavesdropping)(maintenir la sécurité physique sur tous les câbles, passer aux câbles à fibres optiques).

▪ What are the various technologies employed by wireless devices to maximize their use of the available radio frequencies ? ***

Certaines des technologies d'utilisation du spectre de fréquence sont :

- l'étalement du spectre (**spread spectrum**),
- l'étalement de spectre par saut de fréquence (**Frequency Hopping Spread Spectrum - FHSS**),
- L'étalement de spectre à séquence directe (**Direct Sequence Spread Spectrum - DSSS**),
- le multiplexage par répartition en fréquence orthogonale (**Orthogonal Frequency-Division Multiplexing - OFDM**).

▪ Discuss methods used to secure 802.11 wireless networking ***

Les méthodes pour sécuriser la mise en réseau sans fil 802.11 incluent

- la désactivation de la diffusion SSID (**SSID broadcast**),
- changer le SSID en quelque chose d'unique,
- activer le filtrage MAC (**MAC filtering**),
- considérer l'utilisation d'adresses IP statiques ou utiliser DHCP avec des réserves,
- activer la plus haute forme de cryptage offerte (**highest encryption**) (comme WEP, WPA ou WPA2 / 802.11i),
- traiter les accès sans fil comme des accès à distance et utiliser 802.1X, RADIUS ou TACACS,
- séparer les points d'accès sans fil du réseau local avec des pare-feu,

- surveiller toutes les activités des clients sans fil avec un IDS,
- envisager de demander aux clients sans fil de se connecter à un VPN pour accéder au réseau local.

▪ Name the LAN shared media access technologies and examples of their use, if known ***

Les technologies d'accès au média partagé LAN sont :

- CSMA, Carrier Sense Multiple Access, Écoute d'un Support à Accès Multiple
- CSMA/CA (Collision Avoidance) utilisé par 802.11 et AppleTalk,
- CSMA/CD (Collision Detection) utilisé par Ethernet,
- le passage de jeton (token passing) utilisé par Token Ring et FDDI / CDDI,
- le polling (utilisé par SDLC, HDLC et certains systèmes mainframe).

Chapter 12: Secure Communications and Network Attacks

▪ Understand the issues around remote access security management

La gestion de la sécurité de l'accès à distance requiert que les concepteurs de systèmes de sécurité traitent les composants matériels et logiciels d'une implémentation, ainsi que les problèmes liés à la stratégie, aux tâches de travail et au chiffrement.

▪ Be familiar with the various protocols and mechanisms that may be used on LANs and WANs for data communications

Il y a : SKIP, SWIPE, SSL, SET, PPP, SLIP, CHAP, PAP, EAP, and S-RPC.

et aussi : VPN, TLS/SSL, and VLAN.

▪ Know what tunneling is

Le tunneling est l'**encapsulation** d'un message transporté par un protocole dans un second protocole. Le second protocole effectue souvent un cryptage pour protéger le contenu du message.

▪ Understand VPNs

Les VPN sont basés sur le tunneling crypté. Ils peuvent offrir une authentification et une protection des données en tant que solution point à point. Les protocoles VPN courants sont **PPTP**, **L2F**, **L2TP** et **IPSec**.

▪ Be able to explain NAT

La translation d'adresses (Network address translation - NAT) protège le plan d'adressage d'un réseau privé, permet l'utilisation des adresses IP privées et permet à plusieurs clients internes d'obtenir un accès Internet via une ou quelques adresses IP publiques. Le NAT est pris en charge par de nombreux périphériques de sécurité, tels que les pare-feux, les routeurs, les passerelles et les proxies.

▪ Understand the difference between packet switching and circuit switching

En commutation de circuit, une voie physique dédiée est créée entre les deux parties communicantes. La commutation de paquets se produit lorsque le message ou la communication est divisé en petits segments et envoyé à travers les réseaux intermédiaires vers la destination. Dans les systèmes de commutation par paquets, il existe deux types de voies de communication, ou circuits virtuels: les circuits virtuels permanents (PVC) et les circuits virtuels commutés (SVC).

▪ Understand the difference between dedicated and nondedicated lines

Une ligne dédiée, ou ligne spécialisée (LS), est toujours activée et réservée à un client spécifique. Des exemples de lignes spécialisées comprennent les T1, T3, E1, E3 et le câble. Une ligne non dédiée nécessite une connexion avant que la transmission de données puisse avoir lieu. Il peut être utilisé pour se connecter à n'importe quel système distant utilisant le même type de ligne non dédiée. Les modems standards, DSL et RNIS sont des exemples de lignes non dédiées.

- Know various issues related to remote access security

Familiarisez-vous avec l'accès à distance, les connexions d'accès à distance (dial-up), les capture/déport d'écran (screen scrapers), les applications ou postes de travail virtuels et les problèmes généraux de sécurité du télétravail.

- Know the various types of WAN technologies

Sachez que la plupart des technologies WAN nécessitent unité de service du réseau et une unité de service des données (Channel Service Unit et Data Service Unit - CSU / DSU), parfois appelée commutateur WAN. Il existe de nombreux types de réseaux de transport et de technologies de connexion WAN, tels que X.25, Frame Relay, ATM et SMDS. Certaines technologies de connexion WAN nécessitent des protocoles spécialisés supplémentaires pour prendre en charge divers types de systèmes ou dispositifs spécialisés. Trois de ces protocoles sont SDLC, HDLC et HSSI.

- Understand the differences between PPP and SLIP

Le protocole PPP (Point-to-Point Protocol) est un protocole d'encapsulation conçu pour prendre en charge la transmission du trafic IP via des liaisons commutées ou point-à-point. PPP inclut une large gamme de services de communication, notamment l'assignation et la gestion des adresses IP, la gestion des communications synchrones, l'encapsulation standardisée, le multiplexage, la configuration des liaisons, la détection des erreurs et la négociation de fonctionnalités. PPP a été initialement conçu pour prendre en charge le CHAP et le PAP pour l'authentification. Cependant, les versions récentes de PPP prennent également en charge MS-CHAP, EAP et SPAP.

PPP a remplacé le protocole SLIP (Serial Line Internet Protocol). SLIP n'offrait aucune authentification, ne prenait en charge que les communications semi-duplex, ne disposait pas de fonctions de détection des erreurs et exigeait l'établissement et le démontage manuel des liaisons.

- Understand common characteristics of security controls

Les contrôles de sécurité doivent être transparents pour les utilisateurs. Les calculs de hachages (Hash totals) et les contrôles CRC (Contrôle de redondance cyclique) peuvent être utilisés pour vérifier l'intégrité des messages. Les séquences d'enregistrement sont utilisées pour assurer l'intégrité d'une séquence de transmission. L'enregistrement des transmissions (logging) aide à détecter les abus.

- Understand how email security works

Le courrier électronique Internet est basé sur SMTP, POP3 et IMAP qui sont intrinsèquement non sécurisés. L'utilisation de méthodes de sécurisation/chiffrement doit être traitée dans une politique de sécurité. Les solutions de sécurité de messagerie incluent l'utilisation de S / MIME, MOSS, PEM ou PGP.

- Know how fax security works

La sécurité des télécopies (Fax) repose principalement sur l'utilisation de transmissions cryptées ou de lignes de communication cryptées pour protéger les documents transférés. L'objectif principal est d'empêcher l'interception. Les journaux d'activité et les rapports d'exception peuvent être utilisés pour détecter des anomalies dans l'activité de télécopie qui pourraient être des symptômes d'attaque.

- Know the threats associated with PBX systems and the countermeasures to PBX fraud

Les contre-mesures à la fraude et à l'abus des PBX, PABX (Private Automatic Branch eXchange) comprennent plusieurs des mêmes précautions que vous pouvez employer pour protéger un réseau informatique classique: contrôles logiques ou techniques, contrôles administratifs et contrôles physiques.

- Understand the security issues related to VoIP

La VoIP (Voice over IP) est sujet au risque d'usurpation d'identité de l'appelant, d'hameçonnage (voice et phishing = vishing), de SPIT (SPam over Internet Telephony), d'attaques sur les logiciels et firmwares du gestionnaire d'appel, d'attaques matérielles vers les téléphones, de DoS (deny of service), de MitM (Man-in-the-middle), d'usurpation de contenu (spoofing) et d'attaques par sauts réseaux (switch hopping).

- Recognize what a phreaker is

Le piratage téléphonique (phreaking) est un type spécifique d'attaque dans lequel différents types de technologies sont utilisés pour contourner le système téléphonique pour réaliser des appels interurbains gratuits, modifier la fonction du service téléphonique, dérober des services spécialisés ou même provoquer des interruptions de service. Les outils communs des phreakers incluent les boîtes noires, rouges, bleues et blanches.

- Understand voice communications security

Les communications vocales sont vulnérables à de nombreuses attaques, d'autant plus que les communications vocales deviennent une partie importante des services réseau. Vous pouvez obtenir la confidentialité en utilisant des communications cryptées. Des contre-mesures doivent être déployées pour se protéger contre l'interception, l'écoute clandestine, l'écoute et d'autres types d'exploitation. Familiarisez-vous avec les sujets de communication vocale tels que POTS, PSTN, PBX et VoIP.

- Be able to explain what social engineering is

L'ingénierie sociale (social engineering) est un moyen par lequel une personne inconnue gagne la confiance de quelqu'un au sein de votre organisation en convainquant les employés qu'ils sont, par exemple, associés à la haute direction, au support technique ou au service d'assistance. La victime est souvent encouragée à modifier son compte utilisateur sur le système, par exemple en réinitialisant son mot de passe, afin que l'attaquant puisse l'utiliser pour accéder au réseau. La contre-mesure principale pour ce type d'attaque est la formation des utilisateurs (**user training**).

- Explain the concept of security boundaries

Une limite de sécurité (security boundary) peut être la division entre une zone sécurisée et une autre zone sécurisée. Il peut également s'agir de la division entre une zone sécurisée et une zone non sécurisée. Les deux doivent être traitées dans une politique de sécurité.

- Understand the various network attacks and countermeasures associated with communications security

Les systèmes de communication sont vulnérables à de nombreuses attaques, notamment le déni de service distribué (DDoS), l'écoute clandestine (eavesdropping), l'emprunt d'identité (impersonation), la relecture (replay), la modification, l'usurpation d'identité (spoofing) et les attaques ARP et DNS. Être capable de fournir des contre-mesures efficaces pour chacun.

- Describe the differences between transport mode and tunnel mode of IPSec ***

Le mode « transport » d'IPSec est utilisé pour les liaisons hôte-hôte (host-to-host) et ne chiffre uniquement que la charge utile (payload) et non son en-tête (header).

Le mode tunnel d'IPSec est utilisé pour les liaisons hôte-LAN et LAN-to-LAN et crypte la totalité de la charge utile et de l'en-tête d'origine, puis ajoute un en-tête.

- Discuss the benefits of NAT ***

La traduction d'adresses réseau (Network Address Translation - NAT) permet de cacher l'identité des systèmes internes aux entités externes. Le NAT est souvent utilisé pour traduire entre les adresses IP privées de la RFC 1918 et les adresses publiques allouées. Le NAT sert de pare-feu à sens unique, car il autorise uniquement le trafic entrant qui est en réponse à une requête interne précédente. NAT permet également d'utiliser un certain nombre d'adresses publiques allouées pour accorder la connectivité Internet à un plus grand nombre de systèmes internes.

- What are the main differences between circuit switching and packet switching ? ***

La **commutation de circuit** (circuit switching) est généralement associée à des connexions physiques. Le lien lui-même est physiquement établi, puis démonté pour la communication. La commutation de circuits offre des retards fixes connus (known fixed delays), prend en charge un trafic constant, est orientée connexion, n'est sensible qu'à la perte de la connexion plutôt qu'à la communication et est le plus souvent utilisée pour les transmissions vocales.

La **commutation de paquets** (packet switching) est généralement associée à des connexions logiques car le lien est simplement un chemin défini logiquement parmi les chemins possibles. Dans un système de commutation par paquets, chaque système ou liaison peut être utilisé simultanément par d'autres circuits. La commutation par

paquets divise la communication en segments, et chaque segment traverse le circuit jusqu'à la destination. La commutation de paquets a des retards variables car chaque segment peut emprunter son propre chemin, elle est habituellement employée pour le trafic en rafale, n'est pas orientée connexion physique, utilise souvent des circuits virtuels, est sensible à la perte de données et est utilisée pour toute forme de communication.

■ What are some security issues with email and options for safeguarding against them ? ***

Le courrier électronique (Email) est intrinsèquement non sécurisé car il est principalement un support de communication en texte brut et utilise des protocoles de transmission non cryptés. Cela permet à l'email d'être facilement usurpé (spoofed), spammé, inondé (flooded), écouté (eavesdropped), interféré, et piraté (hijacked). Les défenses contre ces problèmes incluent principalement des exigences d'authentification plus strictes et l'utilisation du chiffrement pour protéger le contenu pendant le transit.

Domain 5: Identity and Access Management (IAM)

Chapter 13: Managing Identity and Authentication

▪ Know the difference between subjects and objects

Vous pouvez remarquer que le contexte CISSP et la documentation de sécurité utilisent couramment les termes sujet et objet, il est donc important de connaître la différence entre eux. **Les sujets** sont des entités actives (telles que les utilisateurs) qui accèdent aux **objets** passifs (tels que les fichiers). Un utilisateur est un sujet qui accède à des objets au cours de l'exécution d'une action ou de l'accomplissement d'une tâche de travail.

▪ Know the various types of access control

Vous devriez être capable d'identifier le type de tout contrôle d'accès donné. Les contrôles d'accès peuvent être **préventifs** (pour arrêter les activités indésirables ou non autorisées), **détectives** (pour détecter une activité indésirable ou non autorisée) ou **correctifs** (pour restaurer les systèmes à la normale après une activité indésirable ou non autorisée). Les contrôles d'accès **dissuasif (deterrent)** tentent de décourager la violation des politiques de sécurité, en encourageant les personnes à décider de ne pas prendre une action indésirable. Les contrôles de **récupération (Recovery)** tentent de réparer ou de restaurer les ressources, les fonctions et les capacités après une violation des règles de sécurité. Les contrôles de la **directive** tentent de diriger, confiner ou contrôler l'action des sujets pour forcer ou encourager le respect de la politique de sécurité. Les contrôles de **compensation** offrent des options ou des alternatives aux contrôles existants pour faciliter l'application et la prise en charge d'une politique de sécurité.

▪ Know the implementation methods of access controls

Les contrôles sont implémentés en tant que contrôles **administratifs**, **logiques / techniques** ou **physiques**. Les contrôles **administratifs** (ou de gestion) incluent des stratégies ou des procédures pour implémenter et appliquer le contrôle d'accès global. Les contrôles **logiques / techniques** comprennent les mécanismes matériels ou logiciels utilisés pour gérer l'accès aux ressources et aux systèmes et assurer la protection de ces ressources et systèmes. Les contrôles **physiques** comprennent les barrières physiques déployées pour empêcher le contact direct et l'accès avec les systèmes ou les zones d'une installation.

▪ Understand the difference between identification and authentication.

Les contrôles d'accès dépendent d'une identification et d'une authentification efficaces, il est donc important de comprendre les différences entre eux. Les sujets revendiquent une identité, et l'identification peut être aussi simple qu'un nom d'utilisateur pour un utilisateur. Les sujets prouvent leur identité en fournissant des informations d'authentification telles que le mot de passe correspondant pour un nom d'utilisateur.

▪ Understand the difference between authorization and accountability.

Après authentification des sujets, les systèmes autorisent l'accès aux objets en fonction de leur identité avérée. Les journaux d'audit (**audit logs / audit trails**) enregistrent les événements, y compris l'identité du sujet qui a effectué une action. La combinaison d'une identification, d'une authentification et d'un audit efficaces assure la traçabilité (**accountability**).

▪ Understand the details of the three authentication factors

Les trois facteurs d'authentification sont :

- quelque chose que vous connaissez (**something you know**), comme un mot de passe ou un code PIN
- quelque chose que vous avez (**something you have**), comme une carte à puce ou un jeton
- quelque chose que vous êtes (**something you are**), basé sur la biométrie

L'authentification multifactorielle comprend deux ou plusieurs **facteurs d'authentification**, et son utilisation est plus sûre que l'utilisation d'un seul facteur d'authentification. Les mots de passe sont la forme d'authentification la plus faible, mais les stratégies de mot de passe contribuent à renforcer leur sécurité en imposant des exigences de

complexité et d'historique. Les cartes à puce comprennent des microprocesseurs et des certificats cryptographiques, et les jetons (**tokens**) créent des mots de passe à usage unique (**one-time passwords**). Les méthodes biométriques identifient les utilisateurs en fonction de caractéristiques telles que les empreintes digitales (fingerprints). Le taux d'erreur (the crossover error rate - CER) identifie la précision d'une méthode biométrique. Il montre deux types d'erreurs :

- les erreurs de Type 1 : les faux taux de rejet (**false rejection rate - FRR**)
- les erreurs de Type 2 : les taux de fausse acceptation (**false acceptance rate - FAR**)

▪ Understand single sign-on

L'authentification unique (Single sign-on - **SSO**) est un mécanisme qui permet aux sujets de s'authentifier une fois sur un système et d'accéder à plusieurs objets sans s'authentifier à nouveau. **Kerberos** est la méthode d'authentification unique la plus couramment utilisée dans les organisations. Elle utilise une cryptographie et des tickets symétriques pour prouver l'identification et fournir une authentification. Lorsque plusieurs organisations souhaitent utiliser un système d'authentification unique commun, elles utilisent souvent un système de gestion d'identité fédérée, dans lequel la fédération ou le groupe d'organisations s'accorde sur une méthode d'authentification commune. **SAML (Security Assertion Markup Language)** est couramment utilisé pour partager des informations d'identité fédérées.

Les autres méthodes SSO sont l'accès par script (**scripted access**), **SESAME** et **KryptoKnight**.

OAuth et **OpenID** sont deux nouvelles technologies SSO utilisées sur Internet. OAuth 2.0 est recommandé plutôt que OAuth 1.0 par de nombreuses grandes organisations telles que Google.

▪ Understand the purpose of AAA protocols

Plusieurs protocoles fournissent, de manière centralisés, des services d'authentification (**authentication**), d'autorisation (**authorization**) et de traçabilité (**accounting**). Les systèmes d'accès au réseau (ou d'accès à distance) utilisent des protocoles AAA. Par exemple, un serveur d'accès réseau est un client sur un serveur **RADIUS**, le serveur RADIUS fournit des services AAA. RADIUS utilise UDP et crypte le mot de passe uniquement. **TACACS+** utilise TCP et crypte la totalité de la session. **Diameter** est basé sur RADIUS et améliore plusieurs des faiblesses de RADIUS, mais Diameter n'est pas compatible avec RADIUS. Diamètre devient de plus en plus populaire avec les systèmes IP mobiles tels que les smartphones.

▪ Understand the identity and access provisioning life cycle

Le cycle de vie de l'approvisionnement (provisioning) et de l'identité (identity) d'accès fait référence à la **création**, la **gestion** et la **suppression** de comptes. Le provisionnement des comptes garantit que chaque compte dispose des privilèges appropriés en fonction des exigences des tâches à effectuées. Des révisions périodiques garantissent que les comptes n'ont pas de privilèges excessifs et suivent le principe du moindre privilège (**least privilege**). La révocation consiste à désactiver les comptes dès que possible (soon as possible) lorsqu'un employé quitte l'entreprise et à supprimer les comptes lorsqu'ils ne sont plus nécessaires.

▪ Name at least three access control types ***

Les types de contrôle d'accès incluent les contrôles d'accès **préventif**, **détectif**, **correctif**, dissuasif (**deterrent**), de récupération (**recovery**), **directive** et de **compensation**. Ils sont implémentés en tant que contrôles **administratifs**, contrôles **logiques/techniques**, et/ou contrôles **physiques**.

▪ Describe the three primary authentication factor types ***

Les trois types d'authentification sont :

- Type 1 : quelque chose que vous connaissez (something you know), comme un mot de passe ou un code PIN
- Type 2 : quelque chose que vous avez (**something you have**), comme une carte à puce ou un jeton
- Type 3 : quelque chose que vous êtes (**something you are**), basé sur la biométrie

- Name the method that allows users to **log on once** and access resources in multiple organizations without authenticating again ***

Les systèmes de gestion d'identité fédérée permettent d'étendre l'authentification unique (**single sign-on - SSO**) au-delà d'une seule organisation. SSO permet aux utilisateurs de s'authentifier une fois et d'accéder à plusieurs ressources sans s'authentifier à nouveau. Security assertion markup language (**SAML**) est un langage commun utilisé pour échanger des informations d'identité fédérées entre des organisations.

- Identify the three primary elements within the identity and access provisioning life cycle ***

Le cycle de vie de l'approvisionnement des identités et des accès comprend le **provisionnement** des comptes, l'**examen** et la gestion périodiques des comptes, et la **révocation** des comptes lorsqu'ils ne sont plus utilisés.

Chapter 14: Controlling and Monitoring Access

- Identify common authorization mechanisms

L'autorisation garantit que l'accès à l'activité ou à l'objet demandé est possible, compte tenu des privilèges attribués à l'identité authentifiée. Par exemple, il garantit que les utilisateurs disposant des privilèges appropriés peuvent accéder aux fichiers et autres ressources. Les mécanismes d'autorisation communs incluent le refus implicite (**implicit deny**), les listes de contrôle d'accès (**access control lists**), les matrices de contrôle d'accès (**access control matrixes**), les tables de capacités (**capability tables**), les interfaces contraintes (**constrained interfaces**), les contrôles dépendants du contenu (**content-dependent**) et les contrôles dépendants du contexte (**context-dependent**). Ces mécanismes appliquent des principes de sécurité tels que le besoin de savoir (**need-to-know**), le principe du moindre privilège (**least privilege**) et la séparation des tâches (**separation of duties**).

- Know details about each of the access control models

Avec les modèles de contrôle d'accès discrétionnaires (**discretionary**), tous les objets ont des propriétaires et les propriétaires peuvent modifier les autorisations. Les administrateurs gèrent de manière centralisée les contrôles non discrétionnaires (**nondiscretionary**). Les modèles de contrôle d'accès basés sur les rôles (**Role-based**) utilisent des rôles basés sur les tâches (**task-based**); les utilisateurs obtiennent des privilèges lorsque les administrateurs placent leurs comptes dans un rôle. Les modèles de contrôle d'accès basés sur des règles (**Rule-based**) utilisent un ensemble de règles, de restrictions ou de filtres pour déterminer l'accès. Les contrôles d'accès obligatoires (**Mandatory**) utilisent des étiquettes (**labels**) pour identifier les domaines de sécurité. Les sujets ont besoin d'étiquettes correspondantes pour accéder aux objets.

- Understand basic risk elements

Le risque est la possibilité ou la probabilité (**likelihood**) qu'une menace (**threat**) puisse exploiter une vulnérabilité et causer des dommages aux biens. La valorisation des actifs (**asset valuation**) identifie la valeur des actifs, la modélisation des menaces identifie les menaces contre ces actifs et l'analyse de vulnérabilité identifie les faiblesses des actifs précieux d'une organisation. L'agrégation d'accès est un type d'attaque qui combine, ou agrège, des informations non sensibles pour apprendre des informations sensibles et qui est utilisé dans des attaques de reconnaissance.

- Know how brute-force and dictionary attacks work.

Les attaques par force brute et par dictionnaire sont exécutées sur un fichier de base de données de mot de passe volé ou sur l'invite de connexion d'un système. Ils sont conçus pour découvrir les mots de passe. Dans les attaques par force brute, toutes les combinaisons possibles de caractères de clavier sont utilisées, tandis qu'une liste prédéfinie de mots de passe possibles est utilisée dans une attaque par dictionnaire. Les contrôles de verrouillage de compte empêchent leur efficacité contre les attaques en ligne.

- Understand the need for strong passwords

Les mots de passe forts rendent les utilitaires de cassage de mot de passe (**password-cracking**) moins efficaces. Les mots de passe forts incluent plusieurs types de caractères et ne sont pas des mots contenus dans un

dictionnaire. Les stratégies de mot de passe garantissent que les utilisateurs créent des mots de passe forts. Les mots de passe doivent être cryptés lorsqu'ils sont stockés et cryptés lorsqu'ils sont envoyés sur un réseau. L'authentification peut être renforcée en utilisant un facteur supplémentaire au-delà du mot de passe.

- Understand sniffer attacks

Dans une attaque de type **sniffer** (ou **snooping** attack), un attaquant utilise un outil de capture de paquet (tel qu'un sniffer ou un analyseur de protocole) pour capturer, analyser et lire des données envoyées sur un réseau. Les attaquants peuvent facilement lire les données envoyées sur un réseau en clair, mais le cryptage des données en transit contrecarre ce type d'attaque.

- Understand spoofing attacks

L'usurpation d'identité (spoofing) consiste à prétendre être quelque chose ou quelqu'un d'autre, et il est utilisé dans de nombreux types d'attaques, y compris les attaques de contrôle d'accès. Les attaquants essaient souvent d'obtenir les informations d'identification des utilisateurs afin qu'ils puissent usurper l'identité de l'utilisateur. Les attaques par usurpation d'identité incluent l'usurpation d'adresse e-mail, l'usurpation de numéro de téléphone et l'usurpation d'adresse IP. De nombreuses attaques de type phishing utilisent des méthodes d'usurpation d'identité.

- Understand social engineering

Une attaque d'ingénierie sociale est une tentative par un attaquant de convaincre quelqu'un de fournir des informations (comme un mot de passe) ou d'effectuer une action qu'il ne ferait pas normalement (par exemple cliquer sur un lien malveillant), compromettant la sécurité. Les ingénieurs sociaux tentent souvent d'accéder à l'infrastructure informatique ou à l'infrastructure physique. La formation des utilisateurs est un outil efficace pour empêcher le succès des attaques d'ingénierie sociale.

- Understand phishing

Les attaques par hameçonnage (**phishing**) sont couramment utilisées pour tenter d'inciter les utilisateurs à divulguer des informations personnelles (tel qu'un comptes d'utilisateur ou un mot de passe), à cliquer sur un lien malveillant ou à ouvrir une pièce jointe malveillante. Le **spear phishing** (la pêche au lancé) cible des groupes spécifiques d'utilisateurs, et le **whaling** (la pêche à la baleine) cible des cadres de haut niveau. le **vishing** (le phishing de la VoIP) utilise les technologies VoIP.

- Describe the primary difference between discretionary and nondiscretionary access control models ***

Un modèle de contrôle d'accès discrétionnaire (**discretionary** - DAC) permet au propriétaire, au créateur ou au dépositaire des données d'un objet de contrôler et de définir l'accès.

Les administrateurs administrent de manière centralisée les contrôles d'accès non discrétionnaires (**nondiscretionary**) et peuvent apporter des modifications qui affectent l'environnement entier.

- List three elements to identify when attempting to identify and prevent access control attacks ***

Les actifs (**assets**), les menaces (**threats**) et les vulnérabilités (**vulnerabilities**) doivent être identifiés par l'évaluation des actifs, la modélisation des menaces et l'analyse de la vulnérabilité.

- Name at least three types of attacks used to discover passwords ***

Les attaques par « **Brute-force** », par dictionnaire (**dictionary**), par écoute (**sniffer**), par table « arc en ciel » (**rainbow table**), par **social-engineering**, sont des attaques ayant pour objectif de découvrir des mots de passe.

Domain 6: Security Assessment and Testing

Chapter 15: Security Assessment and Testing

- Understand the importance of security assessment and testing programs

Les programmes d'évaluation et de test de la sécurité (**security assessment and test**) constituent un mécanisme important pour valider l'efficacité en continu des contrôles de sécurité. Ils comprennent une variété d'outils, notamment des évaluations de vulnérabilité, des tests de pénétration, des tests logiciels, des audits et des processus de gestion de la sécurité conçus pour valider les contrôles. Chaque organisation devrait avoir un programme d'évaluation et de test de sécurité défini et opérationnel.

- Conduct vulnerability assessments and penetration tests

Les évaluations de vulnérabilité (**vulnerability assessments**) utilisent des outils automatisés pour rechercher les vulnérabilités connues dans les systèmes, les applications et les réseaux. Ces failles (**flaws**) peuvent inclure des correctifs manquants (**missing patches**), des configurations incorrectes (**misconfigurations**) ou un code défectueux (**faulty code**) exposant l'organisation à des risques de sécurité. Les tests de pénétration utilisent également ces mêmes outils mais les complètent par des techniques d'attaque où un évaluateur tente d'exploiter les vulnérabilités et d'accéder au système.

- Perform software testing to validate code moving into production

Les techniques de test de logiciels vérifient que les fonctions de code sont correctement conçues et ne contiennent pas de failles de sécurité. La révision de code (**code review**) utilise un processus d'examen par les pairs pour valider formellement ou informellement le code avant de le déployer en production. Les tests d'interface évaluent les interactions entre les composants et les utilisateurs avec les tests d'API, les tests d'interface utilisateur et les tests d'interface physique.

- Understand the difference between static and dynamic software testing

Les techniques de test de logiciels **statiques**, telles que les révisions de code (code reviews), évaluent la sécurité des logiciels sans les exécuter ; elles analysent le code source de l'application ou l'application compilée. Les tests **dynamiques** évaluent la sécurité des logiciels dans un environnement d'exécution et constituent souvent la seule option pour les entreprises qui déploient des applications écrites par quelqu'un d'autre.

- Explain the concept of fuzzing

Le Fuzzing utilise des entrées modifiées pour tester les performances du logiciel dans des circonstances inattendues. Le « mutation fuzzing » modifie les entrées connues pour générer des entrées synthétiques qui peuvent déclencher un comportement inattendu. Le « generational fuzzing » développe des entrées basées sur des modèles d'entrées attendues pour effectuer la même tâche.

- Perform security management tasks to provide oversight to the information security program

Les responsables de la sécurité doivent effectuer une variété d'activités pour conserver une surveillance adéquate (**oversight**) du programme de sécurité de l'information. Les revues de journaux (**log reviews**), en particulier pour les activités d'administrateur, garantissent que les systèmes ne sont pas mal utilisés. Les examens de la gestion des comptes (**account management reviews**) garantissent que seuls les utilisateurs autorisés conservent l'accès aux systèmes d'information. La vérification de sauvegarde (**backup verification**) garantit que le processus de protection des données de l'organisation fonctionne correctement. Les principaux indicateurs de performance et de risque fournissent une vue d'ensemble de l'efficacité des programmes de sécurité.

- Conduct or facilitate internal and third-party audits

Les audits de sécurité ont lieu lorsqu'un tiers effectue une évaluation des contrôles de sécurité protégeant les actifs informationnels d'une organisation. Les audits internes sont effectués par le personnel interne d'une organisation et

sont destinés à être utilisés par la direction. Les audits externes sont effectués par un cabinet d'audit tiers et sont généralement destinés à l'organe de gouvernance de l'organisation.

▪ Describe the difference between TCP SYN scanning and TCP connect scanning ***

Le scan de type **TCP SYN** envoie un seul paquet à chaque port analysé avec l'indicateur SYN défini (flag à 1). Cela indique une demande d'ouverture d'une nouvelle connexion. Si le scanner reçoit une réponse dont les indicateurs SYN et ACK (flags à 1) sont définis, cela indique que le système passe à la deuxième phase de la poignée de main TCP en trois étapes (**three-way TCP handshake**) et que le port est ouvert. Le scan TCP SYN est également connu sous le nom de balayage « semi-ouvert » (« **half-open** » scanning).

Le scan de type **TCP connect** ouvre une connexion complète au système distant sur le port spécifié. Ce type de scan est utilisé lorsque l'utilisateur qui exécute l'analyse n'a pas les autorisations nécessaires pour exécuter une analyse semi-ouverte.

▪ What are the three port status values returned by the nmap network discovery scanning tool ***

Les trois valeurs d'état de port possibles renvoyées par nmap sont les suivantes :

- **Open** - Le port est ouvert sur le système distant et une application accepte activement les connexions sur ce port.
- **Closed** - Le port est accessible sur le système distant, ce qui signifie que le pare-feu autorise l'accès, mais aucune application n'accepte les connexions sur ce port.
- **Filtered** - Nmap ne peut pas déterminer si un port est ouvert ou fermé car un pare-feu interfère avec la tentative de connexion.

▪ What is the difference between static and dynamic code testing techniques ? ***

Les techniques de test de logiciels **statiques**, telles que les révisions de code, évaluent la sécurité des logiciels sans les exécuter en analysant le code source ou l'application compilée.

Les tests **dynamiques** évaluent la sécurité des logiciels dans un environnement d'exécution et constituent souvent la seule option pour les entreprises qui déploient des applications écrites par quelqu'un d'autre.

▪ What is the difference between mutation fuzzing and generational fuzzing ? ***

Le « **mutation fuzzing** » (dumb) prend les valeurs d'entrée précédentes du fonctionnement réel du logiciel et les manipule (ou les mute) pour créer une entrée fuzzed. Il peut modifier les caractères du contenu, ajouter des chaînes à la fin du contenu ou effectuer d'autres techniques de manipulation de données.

Le « generational fuzzing » (intelligent) développe des modèles de données et crée une nouvelle entrée fuzzed basée sur une compréhension des types de données utilisés par le programme.

Domain 7: Security Operations

Chapter 16: Managing Security Operations

- Understand **need to know** and the principle of **least privilege**

Besoin de savoir (**need to know**) et le principe du moindre privilège (**least privilege**) sont deux principes standards de sécurité informatique mis en œuvre dans des réseaux sécurisés. Ils limitent l'accès aux données et aux systèmes de sorte que les utilisateurs et les autres sujets ont uniquement accès à ce dont ils ont besoin. Cet accès limité aide à prévenir les incidents de sécurité et permet de réduire la portée des incidents lorsqu'ils se produisent. Lorsque ces principes ne sont pas respectés, les incidents de sécurité causent des dommages beaucoup plus importants à une organisation.

- Understand separation of duties and job rotation

La séparation des tâches (**separation of duties**) est un principe de sécurité de base qui garantit qu'aucune personne ne peut contrôler tous les éléments d'une fonction ou d'un système critique. Avec la rotation de poste (**job rotation**), les employés sont affectés à différents postes, ou, les tâches sont attribuées à différents employés. La **collusion** est un accord entre plusieurs personnes pour effectuer des actions non autorisées ou illégales. La mise en œuvre de ces politiques aide à prévenir la fraude en limitant les actions que les individus peuvent faire sans se mêler avec d'autres.

- Understand the importance of **monitoring** privileged operations

Les entités privilégiées sont fiables, mais elles peuvent abuser de leurs privilèges. Pour cette raison, il est important de surveiller (**monitoring**) toutes les attributions de privilèges et l'utilisation d'opérations privilégiées. L'objectif est de s'assurer que les employés de confiance (**trusted employees**) n'abusent pas des privilèges spéciaux qui leur sont accordés.

- Understand the information life cycle

Les données doivent être protégées tout au long de leur cycle de vie. Cela commence par classer et marquer (**classifying and marking**) correctement les données. Cela inclut également la manipulation (**handling**), le stockage (**storing**) et la destruction (**destroying**) corrects des données.

- Understand service level agreements

Les organisations utilisent des accords de niveau de service (**service level agreements - SLA**) avec des entités externes telles que les fournisseurs. Ces accords stipulent les attentes de performance telles que des temps d'arrêt maximum (**maximum downtimes**) et incluent souvent des pénalités si le vendeur ne répond pas aux attentes.

- Understand virtual assets

Les actifs virtuels (**virtual assets**) incluent les machines virtuelles, les réseaux définis par logiciel et les réseaux de stockage virtuels. Les hyperviseurs sont le composant logiciel principal qui gère les actifs virtuels, mais les hyperviseurs fournissent également aux attaquants une cible supplémentaire. Il est important que les serveurs physiques hébergeant des ressources virtuelles soient à jour avec les correctifs appropriés pour le système d'exploitation et l'hyperviseur. De plus, toutes les machines virtuelles doivent être tenues à jour.

- Recognize security issues with **cloud-based assets**

Les actifs basés sur le cloud (**cloud-based assets**) incluent toutes les ressources accessibles via le cloud. Le stockage des données dans le cloud augmente le risque. Par conséquent, des étapes supplémentaires peuvent s'avérer nécessaires pour protéger les données, en fonction de leur valeur. Lors de la location de services basés sur le cloud, vous devez comprendre qui est responsable de la maintenance et de la sécurité. Le fournisseur de services de cloud fournit moins de maintenance et de sécurité dans le modèle IaaS (Infrastructure as a Service).

- Explain configuration and change control management

De nombreuses interruptions et incidents peuvent être évités grâce à un programme efficace de gestion des configurations et des changements (**configuration and change management**). La gestion de la configuration garantit que les systèmes sont configurés de manière similaire et que les configurations des systèmes sont connues et documentées.

Les **baselining** garantissent que les systèmes sont déployés avec une base de référence ou de point de départ commun, et que la gestion des images (**imaging**) est une méthode de base commune.

La gestion des changements permet de réduire les pannes ou d'affaiblir les risques induits par des modifications non autorisées. Un processus de gestion des modifications nécessite des demandes de modification (**changes to be requested**), des approbations, et des documentations. Le contrôle de version (**Versioning**) utilise un système d'étiquetage (**labeling**) ou de numérotation (**numbering**) pour suivre les changements de versions et les mises à jour des logiciels.

- Understand patch management

La gestion des correctifs (**patch management**) garantit que les systèmes sont mis à jour avec les derniers correctifs. Vous devez savoir qu'un programme de gestion de correctifs efficace doit évaluer, tester, approuver et déployer les correctifs. De plus, sachez que les audits système vérifient le déploiement des correctifs approuvés sur les systèmes. La gestion des correctifs est souvent liée à la gestion des modifications et des configurations pour garantir que la documentation reflète les modifications. Lorsqu'une organisation ne dispose pas d'un programme de gestion des correctifs efficace, elle connaît souvent des pannes et des incidents liés à des problèmes connus qui auraient pu être évités.

- Explain vulnerability management

La gestion des vulnérabilités (**Vulnerability management**) inclut des routines d'analyses (scans) de vulnérabilité et des évaluations (assessments) de vulnérabilité périodiques. Les scanners de vulnérabilité peuvent détecter des vulnérabilités et des failles de sécurité connues telles que l'absence de correctifs ou de mots de passe faibles. Ils génèrent des rapports qui indiquent les vulnérabilités techniques d'un système et constituent une vérification efficace d'un programme de gestion des correctifs. Les évaluations de vulnérabilité vont au-delà des analyses techniques et peuvent inclure des révisions et des audits pour détecter les vulnérabilités.

- Define the difference between need to know and the principle of least privilege ***

Besoin de savoir (**need to know**) se concentre sur les autorisations et la capacité d'accéder à l'information, alors que le principe du moindre privilège (**least privilege**) se concentre sur les privilèges. Les privilèges incluent à la fois les droits et les autorisations. Les deux limitent l'accès des utilisateurs et des sujets à ce dont ils ont besoin. Le respect de ces principes empêche et limite la portée des incidents de sécurité.

- Name the common methods used to manage sensitive information ***

La gestion des informations sensibles inclut le marquage correct (**properly marking**), la manipulation (**handling**), le stockage (**storing**) et la destruction (**destroying**) en fonction de leurs classifications.

- List the three primary cloud-based service models and identify the level of maintenance provided by the cloud service provider in each of the models ***

Les trois modèles de service cloud sont :

- Software as a Service (SaaS),
- Platform as a Service (PaaS),
- Infrastructure as a Service (IaaS).

Le fournisseur de services cloud (**cloud service provider - CSP**) fournit plus de services de maintenance et de sécurité avec le modèle **SaaS** (Software), un peu moins avec le modèle **PaaS** (Platform), et le très peu avec le modèle **IaaS** (Infrastructure).

Alors que le National Institute of Standards and Technology - NIST SP 800-144 fournit ces définitions, les fournisseurs de services cloud (**cloud service provider - CSP**) utilisent parfois leurs propres termes et définitions dans les documents marketing.

- What control prevents outages due to unauthorized **modifications** in system configuration ? ***

La gestion des modifications, ou gestion des changements, (Change management) permet d'éviter les interruptions dues à des modifications non autorisées de la configuration du système.

Chapter 17: Preventing and Responding to Incidents

- Know incident response steps

Le CISSP CIB répertorie les étapes de la réponse aux incidents telles que la **détection**, la **réponse**, l'**atténuation** (mitigation), la **notification** (reporting), le **rétablissement** (recovery), la **remédiation** et les **leçons apprises** (lessons learned). Après avoir détecté et vérifié un incident, la première réponse consiste à limiter ou à contenir la portée de l'incident tout en protégeant les preuves. Selon les lois en vigueur, une organisation peut avoir besoin de signaler un incident aux autorités officielles, et, si les PII (**Personally Identifiable Information**) sont affectés, les individus doivent être informés. Les étapes de la remédiation et des leçons apprises (les retours d'expériences) comprennent l'analyse des causes profondes afin d'en déterminer la cause et de recommander des solutions pour éviter qu'elles ne se reproduisent.

- Know basic preventive measures

Des mesures préventives de base peuvent prévenir de nombreux incidents. Cela inclut la mise à jour des systèmes (**keeping systems up-to-date**), la suppression ou la désactivation des protocoles et services inutiles (**disabling unneeded protocols and services**), l'utilisation de systèmes de détection et de prévention des intrusions, l'utilisation de logiciels anti-malware avec des signatures à jour et l'activation de pare-feu réseau de type **host-based** et **network-based**.

- Know what denial-of-service (DoS) attacks are

Les attaques **DoS (denial-of-service)** empêchent un système de répondre à des demandes légitimes. Une attaque DoS commune est l'attaque **SYN flood**, qui perturbe la négociation TCP à trois étapes (three-way handshake). Même si les attaques plus anciennes ne sont plus aussi courantes aujourd'hui parce que les précautions de base les bloquent, vous pouvez toujours les tester car de nombreuses attaques plus récentes sont souvent des variantes de méthodes plus anciennes. Les attaques de smurf (**smurf attacks**) emploient un réseau d'amplification pour envoyer de nombreux paquets de réponse à une victime. Les attaques **Ping-of-death** envoient de nombreux paquets ping surdimensionnés à la victime, ce qui provoque le blocage, l'arrêt brutal ou le redémarrage de la victime.

- Understand botnets, botnet controllers, and bot herders

Les **Botnets** représentent des menaces importantes en raison du nombre important d'ordinateurs pouvant lancer des attaques, il est donc important de savoir de quoi il s'agit. Un botnet est une collection de PC compromis (souvent appelés zombies) organisés dans un réseau contrôlé par un criminel connu sous le nom de **Bot herder**. Les « Bot herders » utilisent un serveur de commande et de contrôle pour contrôler à distance les zombies et utilisent souvent le botnet pour lancer des attaques sur d'autres systèmes, ou pour envoyer des spams ou des phishing. Les Bot herders louent aussi l'accès au botnet à d'autres criminels.

- Understand zero-day exploits

Un exploit zero-day est une attaque qui utilise une vulnérabilité inconnue de tous, sauf de l'attaquant ou d'un groupe restreint de personnes. En surface, il semble que vous ne puissiez pas vous protéger contre une vulnérabilité inconnue, mais les pratiques de sécurité de base contribuent grandement à prévenir les exploits du zero-day. La suppression ou la désactivation des protocoles et services inutiles réduit la surface d'attaque, l'activation de pare-feu permet de bloquer de nombreux points d'accès, et l'utilisation de systèmes de détection et de prévention des intrusions permet de détecter et de bloquer les attaques potentielles. En outre, l'utilisation d'outils tels que les pots de miel (honeypots) et les cellules matelassées (padded cells) aide à protéger les réseaux actifs.

- Understand **man-in-the-middle** attacks.

Une attaque de type « homme du milieu » (**man-in-the-middle** - **MITM**) se produit lorsqu'un utilisateur malveillant peut obtenir une position logique entre les deux extrémités d'un lien de communication. Même s'il faut beaucoup de sophistication de la part de l'attaquant pour réussir une attaque de type « man-in-the-middle », la quantité de données obtenues à partir de l'attaque peut être significative.

- Understand sabotage and espionnage

Les employés malveillants (**malicious insiders**) peuvent effectuer un sabotage contre une organisation s'ils deviennent mécontents pour une raison quelconque. L'espionnage est lorsqu'une personne essaie de voler des informations en utilisant, ou pas, un employé interne. Les principes de sécurité de base, tels que la mise en œuvre du principe du moindre privilège (**least privilege**) et la désactivation immédiate des comptes pour les employés licenciés, limitent les dommages causés par ces attaques.

- Understand intrusion detection and intrusion prevention

Les IDS et les IPS sont des mesures détectives et préventives importantes contre les attaques. Connaître la différence entre la détection basée sur la connaissance (**knowledge-based detection**) (en utilisant une base de données similaire aux signatures anti-malware) et la détection basée sur le comportement (**behavior-based detection**). La détection basée sur le comportement commence par une ligne de base (**baseline**) pour reconnaître le comportement normal et compare l'activité avec la ligne de base pour détecter une activité anormale. La ligne de base peut être obsolète si le réseau est modifié. Elle doit donc être mise à jour lorsque l'environnement change.

- Recognize IDS/IPS responses

Un IDS (**détection**) peut répondre passivement en enregistrant et en envoyant des notifications ou en modifiant activement l'environnement. Certaines personnes se réfèrent à un IDS actif comme un IPS. Cependant, il est important de reconnaître qu'un IPS (**protection**) est placé en ligne avec le trafic et inclut la **capacité de bloquer le trafic** malveillant avant qu'il n'atteigne la cible.

- Understand the differences between **HIDSs** and **NIDSs**

Les IDS basés sur l'hôte (**Host-based IDS** - **HIDS**) peuvent surveiller l'activité sur un seul système. Un inconvénient est que les attaquants peuvent les découvrir et les désactiver. Un IDS basé sur le réseau (**network-based IDS** - **NIDS**) peut surveiller l'activité sur un réseau, de plus, un NIDS n'est pas aussi visible pour les attaquants.

- Understand honeypots, padded cells, and pseudo flaws

Un pot de miel (**honeypot**) est un système qui a souvent de faux défauts et de fausses données pour attirer les intrus. Les administrateurs peuvent observer l'activité des pirates pendant qu'ils se trouvent dans le honeypot, et tant que les pirates sont dans le honeypot, ils ne sont pas dans le réseau en direct. Certains IDS ont la possibilité de transférer des attaquants dans une cellule matelassée (**padded cell**) après détection. Bien qu'un pot de miel et une cellule matelassée soient similaires, notez qu'un pot de miel attire l'attaquant mais que l'attaquant est transféré dans la cellule matelassée.

- Understand methods to block malicious code

Le code malveillant est contrecarré avec une combinaison d'outils. L'outil évident est un logiciel anti-malware avec ses définitions à jour installées sur chaque système, à la limite du réseau, et sur les serveurs de messagerie. Toutefois, les stratégies qui appliquent des principes de sécurité de base, tels que le principe du moindre privilège (**least privilege**), empêchent les utilisateurs réguliers d'installer des logiciels potentiellement malveillants. De plus, éduquer les utilisateurs sur les risques et les méthodes couramment utilisés par les pirates pour propager des virus aide les utilisateurs à comprendre et à éviter les comportements dangereux.

- Understand penetration testing

Les tests de pénétration commencent par découvrir les vulnérabilités, puis imitent une attaque pour identifier les vulnérabilités qui peuvent être exploitées. Il est important de se rappeler que les tests de pénétration ne doivent pas être effectués sans le consentement exprès et la connaissance de la direction. De plus, étant donné que les tests de pénétration peuvent entraîner des dommages, ils doivent être effectués sur des systèmes isolés dans la mesure du

possible. Vous devez également reconnaître les différences entre les tests en boîte noire (**black-box testing - zero knowledge**), les tests en boîte blanche (**white-box testing - full knowledge**) et les tests en boîte grise (**gray-box testing - partial knowledge**).

- Know the types of log files

Les journaux de données (**log data**) sont enregistrées dans des bases de données et différents types de fichiers. Les fichiers journaux (**log files**) courants incluent les journaux de sécurité, les journaux système, les journaux d'application, les journaux de pare-feu, les journaux de proxy et les journaux de gestion des modifications. Les fichiers journaux doivent être protégés en les stockant de manière centralisée et en utilisant des autorisations pour restreindre l'accès. Les journaux archivés doivent être définis en lecture seule pour empêcher les modifications.

- Understand monitoring and uses of monitoring tools

La surveillance (**monitoring**) est une forme d'audit qui se concentre sur l'examen actif des données du fichier journal. La surveillance est utilisée pour tenir les sujets responsables de leurs actions et pour détecter les activités anormales ou malveillantes. Il est également utilisé pour surveiller les performances du système. Les outils de surveillance tels que les IDS (**Intrusion Detection System**) ou les SIEM (**security information and event management**) automatisent la surveillance et fournissent une analyse en temps réel des événements.

- Understand audit trails

Les pistes de contrôle (**audit trails**) sont les enregistrements créés par les événements et les occurrences dans une ou plusieurs bases de données ou fichiers journaux. Ils sont utilisés pour reconstruire un événement, extraire des informations sur un incident et prouver ou réfuter la culpabilité. L'utilisation des pistes de vérification (**audit trails**) est une forme passive de contrôle de la sécurité détective, et sont des preuves essentielles dans la poursuite des criminels.

- Understand sampling

L'échantillonnage (**sampling**), ou extraction de données, est le processus d'extraction d'éléments à partir d'un grand nombre de données pour construire une représentation significative ou un résumé de l'ensemble. L'échantillonnage statistique utilise des fonctions mathématiques précises pour extraire des informations significatives d'un grand volume de données. L'écérage (**clipping**) est une forme d'échantillonnage non statistique qui enregistre uniquement les événements qui dépassent un seuil.

- Understand how to maintain accountability

La responsabilité (accountability) est maintenue pour les sujets individuels grâce à l'utilisation de l'audit. Les journaux enregistrent les activités des utilisateurs et les utilisateurs peuvent être tenus responsables de leurs actions consignées. Cela favorise directement le bon comportement des utilisateurs et la conformité à la politique de sécurité de l'organisation.

- Understand the importance of security audits and reviews

Les vérifications (audits) et les examens (reviews) de sécurité aident à s'assurer que les programmes de gestion sont efficaces et suivis. Ils sont généralement associés aux pratiques de gestion des comptes pour prévenir les violations avec les principes du moindre privilège (least privilege) ou du besoin de savoir (need-to-know). Toutefois, ils peuvent également être exécutés pour superviser la gestion des correctifs (**patch management**), la gestion des vulnérabilités (**vulnerability management**), la gestion des modifications (**change management**) et les programmes de gestion de la configuration.

- Understand auditing and the need for frequent security audits

L'audit est un examen méthodique, ou une revue, d'un environnement pour assurer la conformité vi à vi de la réglementation et pour détecter des anomalies, des événements non autorisés ou des crimes purs et simples. Les environnements informatiques sécurisés reposent fortement sur l'audit. Globalement, l'audit sert principalement de contrôle de détection utilisé dans un environnement sécurisé. La fréquence d'un audit, ou revue, de sécurité de l'infrastructure informatique est basée sur le risque. Une organisation détermine s'il existe un risque suffisant pour justifier la dépense et l'interruption d'un audit de sécurité. Le degré de risque affecte également la fréquence à

laquelle un audit est effectué. Il est important de définir clairement et de respecter la fréquence des examens de vérification.

▪ Understand that auditing is an aspect of due care

Les audits de sécurité et l'efficacité des revues sont des éléments clés pour faire preuve de prudence (**due care**). La haute direction doit faire respecter la conformité à l'aide de revues de sécurité périodiques, sinon elle sera probablement tenue responsable de toute perte d'actif qui pourrait survenir.

▪ Understand the need to control access to audit reports

Les rapports d'audit abordent généralement des concepts communs tels que le but de l'audit, la périmètre de l'audit et les résultats découverts ou révélés par l'audit. Ils incluent souvent d'autres détails spécifiques à l'environnement et peuvent inclure des informations sensibles telles que des problèmes, des normes, des causes et des recommandations. Les rapports d'audit qui incluent des **informations sensibles** devraient recevoir une étiquette de classification et être traités de manière appropriée. Seules les personnes disposant de privilèges suffisants devraient y avoir accès. Un rapport d'audit peut être préparé dans différentes versions pour différents publics cibles afin d'inclure uniquement les détails requis par un public spécifique. Par exemple, les administrateurs de la sécurité peuvent avoir un rapport avec tous les détails pertinents, tandis qu'un rapport pour les cadres ne fournirait que des informations de haut niveau.

▪ Understand access review and user entitlement audits

Une revue/audit des accès garantit que les pratiques d'accès aux objets et de gestion des comptes prennent en charge la politique de sécurité. Les audits des droits des utilisateurs garantissent que le principe du moindre privilège est suivi et se concentrent souvent sur les comptes privilégiés.

▪ Audit access controls

Des examens et des audits réguliers des processus de contrôle d'accès aident à évaluer l'efficacité des contrôles d'accès. Par exemple, l'audit peut suivre le succès de la connexion et l'échec de n'importe quel compte. Un système de détection d'intrusion peut surveiller ces journaux et identifier facilement les attaques et informer les administrateurs.

▪ List the different phases of incident response identified in the CISSP CIB ***

Les étapes de réponse aux incidents répertoriées dans le CISSP CIB sont:

- la détection,
- la réponse,
- l'atténuation (mitigation),
- la notification (reporting),
- le rétablissement (recovery),
- la remédiation (remediation),
- les leçons apprises (lessons learned).

▪ Describe the primary types of intrusion detection systems ***

Les systèmes de détection d'intrusion peuvent être décrits comme :

- basés sur un hôte (**host-based**) ou sur un réseau (**network-based**),
- en fonction de leurs méthodes de détection basées sur la connaissance (**knowledge-based**) ou sur le comportement (**behavior-based**),
- et basés sur leurs réponses passives ou actives.

Les IDS basés sur l'hôte (**host-based**) examinent en détail les événements sur des ordinateurs individuels, y compris les activités de fichiers, les accès et les processus.

Les IDS basés sur le réseau (**network-based**) examinent les événements de réseau généraux et les anomalies grâce à l'évaluation du trafic.

Un IDS basé sur la connaissance (**knowledge-based**) utilise une base de données d'attaques connues pour détecter les intrusions.

Un IDS basé sur le comportement (**knowledge-based**) commence par une ligne de base d'activité (**baseline**) normale et mesure l'activité du réseau par rapport à cette ligne de base pour identifier une activité anormale.

Une réponse **passive** enregistrera l'activité et fournira souvent une notification.

Une réponse **active** répond directement à l'intrusion pour arrêter ou bloquer l'attaque.

- Describe the relationship between auditing and audit trails ***

L'audit est un examen méthodique ou une revue d'un environnement. Il englobe une grande variété d'activités pour assurer la conformité à la réglementation et pour détecter les anomalies, les événements non autorisés ou les crimes purs et simples. Les pistes d'audit (**audit trails**) fournissent les données qui prennent en charge un tel examen ou une telle revue, et sont essentiellement ce qui rend possible l'audit et la détection ultérieure des attaques et des comportements répréhensibles.

- What should an organization do to verify that accounts are managed properly ? ***

Les organisations devraient régulièrement effectuer des audits et des revues des différents accès. Ces audits ou revues peuvent détecter quand une organisation ne suit pas ses propres politiques et procédures liées à la gestion de compte.

Chapter 18: Disaster Recovery Planning

- Know the common types of natural disasters that may threaten an organization

Les catastrophes naturelles qui menacent généralement les organisations comprennent : les tremblements de terre (**earthquakes**), les inondations (**floods**), les tempêtes (**storms**), les incendies (**fires**), les **tsunamis** et les éruptions volcaniques (**volcanic eruptions**).

- Know the common types of man-made disasters that may threaten an organization

Les désastres causés par l'homme (man-made disasters) sont : les **explosions**, les incendies d'électricité (**electrical fires**), les actes **terroristes**, les coupures de courant (**power outages**), les défaillances d'infrastructures (**infrastructure failures**), les pannes matérielles et logicielles (**hardware/software failures**), les difficultés de main-d'œuvre (**labor difficulties**), le vol (**theft**) et le vandalisme (**vandalism**).

- Be familiar with the common types of recovery facilities

Les types d'installations courantes de récupération (**recovery facilities**), ou sites de « secours », sont les sites froids (**cold**), les sites tièdes (**warm**), les sites chauds (**hot**), les sites **mobiles**, les **bureaux de services** et les sites **multiples**. Assurez-vous de comprendre les avantages et les inconvénients de chaque installation.

- Explain the potential benefits behind mutual assistance agreements as well as the reasons they are not commonly implemented in businesses today

Les accords d'assistance mutuelle (**Mutual assistance agreements - MAAs**) offrent une alternative peu coûteuse aux sites de reprise après sinistre, mais ils ne sont pas couramment utilisés parce qu'ils sont difficiles à appliquer. Les organisations participant à un MAA peuvent également subir un arrêt d'activité par le même désastre. De plus, les MAA soulèvent des problèmes de confidentialité.

- Understand the technologies that may assist with database backup

Les bases de données bénéficient de trois technologies de sauvegarde. La mise en coffre électronique (**Electronic vaulting**) est utilisée pour transférer des sauvegardes de bases de données vers un site distant dans le cadre d'un transfert groupé (bulk transfer). Dans la journalisation à distance (**remote journaling**), les transferts de données sont plus fréquents. Avec la technologie de mise en miroir à distance (**remote mirroring**), les transactions de base de données sont mises en miroir sur le site de sauvegarde en temps réel.

- Know the five types of disaster recovery plan tests and the impact each has on normal business operations

Les cinq types de tests de plan de reprise après sinistre (**disaster recovery plan tests**) sont les tests de lecture (**read-through**), les procédures structurées (**structured walk-throughs**), les tests de **simulation**, les tests **parallèles** et les tests d'interruption totale (**full-interruption**). Les tests de type « checklist » sont purement des exercices de paperasse, alors que les tests structurées impliquent une réunion d'équipe de projet. Aucun n'a

d'impact sur les opérations commerciales. Les tests de simulation peuvent fermer des unités commerciales non critiques. Les tests parallèles impliquent le déplacement du personnel mais n'affectent pas les opérations quotidiennes. Les tests à interruption complets impliquent la fermeture des systèmes primaires et le transfert des responsabilités sur le site de récupération (recovery facility).

▪ What are some of the main concerns businesses have when considering adopting a mutual assistance agreement ? ***

Les entreprises ont trois principales préoccupations lorsqu'elles envisagent d'adopter un accord d'assistance mutuelle (**mutual assistance agreement - MAA**). Premièrement, la nature d'un MAA nécessite souvent que les entreprises soient situées à proximité géographique. Cependant, cette exigence augmente également le risque que les deux entreprises soient victimes de la même menace. Deuxièmement, les MAA sont difficiles à appliquer en pleine crise. Si l'une des organisations est affectée par un désastre et l'autre non, l'organisation non touchée peut reculer à la dernière minute, laissant l'autre organisation hors de la chance. Enfin, les problèmes de confidentialité (juridiques et commerciaux) empêchent souvent les entreprises de faire confiance aux autres avec leurs données opérationnelles sensibles.

▪ List and explain the five types of disaster recovery tests ***

Il existe cinq principaux types de tests de reprise après sinistre (**disaster recovery tests**):

- Les tests de lecture (**Read-through tests**) impliquent la distribution de listes de contrôle de récupération au personnel de récupération après sinistre pour examen.
- Les visites guidées structurées (**Structured walk-throughs tests**) sont des exercices « sur table » qui impliquent de rassembler l'équipe de récupération après sinistre pour discuter d'un scénario de catastrophe.
- Les tests de simulation (**Simulation tests**) sont plus complets et peuvent avoir une incidence sur une ou plusieurs unités d'affaires non critiques de l'organisation.
- Les tests parallèles (**Parallel tests**) impliquent le déplacement du personnel vers le site alternatif et le démarrage des opérations à cet endroit.
- Les tests à interruption complète (**Full-interruption tests**) impliquent le transfert du personnel vers le site alternatif et la fermeture des opérations sur le site principal.

▪ Explain the differences between the three types of backup strategies ***

Les sauvegardes complètes (**Full backups**) créent une copie de toutes les données stockées sur un serveur. Les sauvegardes incrémentielles (**Incremental backups**) créent des copies de tous les fichiers modifiés depuis la dernière sauvegarde complète ou incrémentielle. Les sauvegardes différentielles (**Differential backups**) créent des copies de tous les fichiers modifiés depuis la dernière sauvegarde complète, sans tenir compte des sauvegardes différentielles ou incrémentielles précédentes qui ont pu avoir lieu.

Chapter 19: Incidents and Ethics

▪ Know the definition of computer crime

Le crime informatique est un délit (ou une violation d'une loi ou d'un règlement) qui est dirigé contre un ordinateur ou qui le concerne directement.

▪ Be able to list and explain the six categories of computer crimes

Les crimes informatiques sont regroupés en six catégories:

- attaque militaire et de renseignement (**military and intelligence attack**),
- attaque commerciale (**business attack**),
- attaque financière (**financial attack**),
- attaque terroriste (**terrorist attack**),
- attaque rancune (**grudge attack**),
- attaque de sensations fortes (**thrill attack**).

Être capable d'expliquer le motif de chaque type d'attaque.

- Know the importance of collecting evidence

Dès que vous découvrez un incident, vous devez commencer à recueillir des preuves (**collect evidence**) et autant d'informations que possible sur l'incident. La preuve peut être utilisée dans une action en justice ultérieure ou dans la recherche de l'identité de l'attaquant. Les preuves peuvent également vous aider à déterminer l'ampleur des dommages.

- Understand that an incident is any violation, or threat of a violation, of your security policy

Les incidents doivent être définis dans votre stratégie de sécurité. Même si des incidents spécifiques peuvent ne pas être décrits, l'existence de la politique définit la norme (**standard**) pour l'utilisation de votre système. Un incident est un événement qui a un impact négatif sur la confidentialité, l'intégrité ou la disponibilité des données d'une organisation.

- Be able to list the four common types of incidents, and know the telltale signs of each

Un incident se produit lorsqu'une attaque ou une autre violation de votre politique de sécurité est effectuée contre votre système. Les incidents peuvent être regroupés en quatre catégories: **scanning**, **compromission**, **code malveillant** et **déni de service**. Être capable d'expliquer ce que chaque type d'incident implique et quels signes rechercher. Connaître les signes avant-coureurs (**telltale signs**) de chacun.

- Know the importance of identifying abnormal and suspicious activity

Les attaques génèrent une activité qui n'est pas normale. Reconnaître les activités anormales et suspectes est la première étape vers la détection des incidents.

- Know how to investigate intrusions and how to gather sufficient information from the equipment, software, and data

Vous devez posséder l'équipement, le logiciel ou les données pour l'analyser et l'utiliser comme preuve. Vous devez acquérir la preuve sans la modifier ou permettre à quelqu'un d'autre de la modifier.

- Know the three basic alternatives for confiscating evidence and when each one is appropriate

Premièrement, la personne qui possède la preuve pourrait la remettre volontairement. **Deuxièmement**, une citation à comparaître pourrait être utilisée pour obliger le sujet à livrer la preuve. **Troisièmement**, un mandat de perquisition (**a search warrant**) est très utile lorsque vous devez confisquer des preuves sans donner au sujet l'occasion de les modifier.

- Know the importance of retaining incident data

Étant donné que vous découvrirez certains incidents après qu'ils se sont produits, vous perdrez des preuves précieuses à moins que vous ne vous assuriez que les fichiers journaux critiques sont conservés pendant une période de temps raisonnable. Vous pouvez conserver les fichiers journaux et les informations d'état du système sur place ou dans les archives.

- Be familiar with how to report an incident.

La première étape consiste à établir une relation de travail entre le personnel de l'entreprise et l'autorité (police, ou autre ...) avec lequel vous travaillerez pour résoudre un incident. Lorsque vous avez un besoin de signaler un incident, rassemblez autant d'informations descriptives que possible et faites votre rapport en temps opportun.

- Know the basic requirements for evidence to be admissible in a court of law.

Pour être recevable, les preuves doivent être pertinentes à un fait en cause dans l'affaire, les faits doivent être importants pour l'affaire, et les preuves doivent être compétentes ou légalement recevables.

- Explain the various types of evidence that may be used in a criminal or civil trial

Une preuve réelle consiste en des objets réels qui peuvent être amenés dans la salle d'audience. La preuve documentaire consiste en des documents écrits qui fournissent un aperçu des faits. La preuve testimoniale (témoignage, attestation, ...) est constituée de déclarations verbales ou écrites faites par des témoins.

▪ Understand the importance of **ethics** to security personnel

Les praticiens de la sécurité ont un très haut niveau d'autorité et de responsabilité pour exécuter leurs fonctions. Le potentiel d'abus existe, et sans un code strict de comportement personnel, les praticiens de la sécurité pourraient être considérés comme ayant un pouvoir incontrôlé. L'adhésion à un code d'éthique permet de s'assurer que ce pouvoir n'est pas abusé.

▪ Know the (ISC) 2 Code of Ethics and **RFC 1087**, « Ethics and the Internet »

Tous les candidats CISSP doivent connaître le code de déontologie complet (ISC) 2 car ils doivent signer un accord selon lequel ils adhèrent à ce code. En outre, soyez familier avec les déclarations de base de la **RFC 1087 (Ethics and the Internet)**.

▪ What are the major categories of computer crime ? ***

Les principales catégories de crimes informatiques sont:

- attaque militaire et de renseignement (**military and intelligence attack**),
- attaque commerciale (**business attack**),
- attaque financière (**financial attack**),
- attaque terroriste (**terrorist attack**),
- attaque rancune (**grudge attack**),
- attaque de sensations fortes (**thrill attack**).

▪ What is the main motivation behind a **thrill attack** ? ***

Les attaques de « frisson » ou de « sensation » (**thrill attack**) sont motivées par des individus cherchant à atteindre un haut niveau de reconnaissance dans la pénétration réussie des systèmes informatiques.

▪ What is the difference between an interview and an interrogation ? ***

Les entrevues (**interviews**) sont menées avec l'intention de recueillir des informations auprès des individus pour vous aider dans votre enquête. Les interrogatoires (**interrogations**) sont menés avec l'intention de recueillir des éléments de preuve provenant de suspects qui seront utilisés dans une poursuite criminelle.

▪ What is the difference between an **event** and an **incident** ? ***

Un événement (**event**) est toute occurrence qui a lieu pendant une certaine période de temps. Les **incidents** sont des événements qui ont des conséquences négatives sur la confidentialité, l'intégrité ou la disponibilité de vos données.

▪ Who are the common members of an **incident response team** ? ***

Les équipes d'intervention aux incidents (**Incident response teams**) comprennent normalement des représentants de la haute direction (**senior management**), des professionnels de la sécurité de l'information (**information security professionals**), des représentants légaux (**legal representatives**), des représentants des affaires publiques et des communications (**public affairs/communications representative**) et des ingénieurs techniques (**technical engineers**).

▪ What are the **three phases** of the incident response process ? ***

Les trois phases du processus de réponse aux incidents sont :

- la détection et l'identification,
- la réponse et la notification (**response and reporting**),
- la récupération et la correction (**recovery and remediation**).

▪ What are the **three basic requirements** that **evidence** must meet in order to be admissible in court ? ***

Pour être recevable, la preuve doit être fiable (**reliable**), efficiente (**competent**) et concrète à l'affaire (material to the case).

Domain 8: Software Development Security

Chapter 20: Software Development Security

- Explain the basic architecture of a relational database management system (RDBMS)

Connaître la structure des bases de données relationnelles. Être capable d'expliquer la fonction des tables (**relations**), des lignes (**records/tuples**) et des colonnes (**fields/attributes**). Savoir comment les relations sont définies entre les tables et les rôles des différents types de clés. Décrire les menaces à la sécurité de la base de données posées par l'agrégation et l'inférence.

- Know the various types of storage

Expliquer les différences entre la mémoire primaire (**primary memory**) et la mémoire virtuelle (**virtual memory**), le stockage secondaire (**secondary storage**) et le stockage virtuel (**virtual storage**), le stockage à accès aléatoire (**random access**) et le stockage à accès séquentiel (**sequential access**), ainsi que le stockage **volatile** et le stockage **non volatile**.

- Explain how expert systems and neural networks function

Les systèmes experts (**expert systems**) se composent de deux composants principaux: une base de connaissances (**knowledge base**) qui contient une série de règles « si / alors » et un moteur d'inférence (**inference engine**) qui utilise ces informations pour tirer des conclusions sur d'autres données. Les réseaux de neurones (**neural networks**) simulent le fonctionnement de l'esprit humain (**human mind**) dans une certaine mesure en organisant une série de calculs en couches pour résoudre les problèmes. Les réseaux de neurones nécessitent une formation approfondie sur un problème particulier avant de pouvoir proposer des solutions.

- Understand the models of systems development

Sachez que le modèle « chute d'eau » (**waterfall model**) décrit un processus de développement séquentiel qui se traduit par le développement d'un produit fini. Les développeurs peuvent annuler une seule phase du processus si des erreurs sont découvertes. Le modèle en spirale (**spiral model**) utilise plusieurs itérations du modèle Waterfall pour produire un certain nombre de prototypes entièrement spécifiés et testés. Les modèles de développement **Agile** mettent l'accent sur les besoins du client et développent rapidement de nouvelles fonctionnalités qui répondent à ces besoins de manière itérative.

- Describe software development maturity models

Sachez que les modèles de maturité (**maturity models**) aident les éditeurs de logiciels à améliorer la maturité et la qualité de leurs processus logiciels en mettant en œuvre un processus évolutif allant des processus ad hoc et chaotiques, à des processus logiciels mûrs et disciplinés. Pouvoir décrire les modèles **SW-CMM (Software capability maturity model)** et **IDEAL (Initiating, Diagnosing, Establishing, Acting & Learning)**.

- Understand the importance of change and configuration management

Connaissez les trois composants de base du contrôle des modifications: le contrôle des demandes (**control request**), le contrôle des modifications (**change control**) et le contrôle des versions (**release control**), ainsi que leur contribution à la sécurité. Expliquer comment la gestion de la configuration contrôle les versions des logiciels utilisés dans une organisation.

- Understand the importance of testing

Les tests logiciels doivent être conçus dans le cadre du processus de développement. Les tests doivent être utilisés comme un outil de gestion pour améliorer les processus de conception, de développement et de production.

- What is the main purpose of a primary key in a database table ? ***

La clé primaire (**primary key**) identifie de manière unique chaque ligne de la table. Par exemple, un numéro d'identification d'employé peut être la clé primaire d'une table contenant des informations sur les employés.

- What is polyinstantiation ? ***

La **polyinstantiation** est une technique de sécurité de base de données qui semble permettre l'insertion de plusieurs lignes partageant la même information d'identification unique.

- Explain the difference between static and dynamic analysis of application code ***

L'analyse statique effectue l'évaluation du code lui-même, en analysant la séquence d'instructions pour les failles de sécurité. L'analyse dynamique teste le code dans un environnement de production en direct, en recherchant les failles d'exécution.

- How far backward does the waterfall model allow developers to travel when a development flaw is discovered ? ***

En cas de découverte d'un défaut de développement (**development flaw**), le modèle en « chute d'eau » ou « cascade » (**waterfall**) permet aux développeurs de revenir uniquement sur la dernière phase.

Chapter 21: Malicious Code and Application Attacks

- Understand the propagation techniques used by viruses

Les virus utilisent quatre techniques de propagation principales: l'infection de **fichiers**, l'injection de **service**, l'infection du secteur d'amorçage (**boot sector**) et l'infection par **macro** pour pénétrer les systèmes et propager leurs charges utiles malveillantes (**malicious payloads**). Vous devez comprendre ces techniques pour protéger efficacement les systèmes de votre réseau contre les codes malveillants.

- Know how antivirus software packages detect known viruses

La plupart des programmes antivirus utilisent des algorithmes de détection basés sur des signatures (**signature-based**) pour rechercher des modèles révélateurs de virus connus. Il est donc essentiel de mettre à jour périodiquement les fichiers de définitions de virus afin de maintenir la protection contre les nouveaux virus à mesure qu'ils apparaissent.

- Explain the techniques that attackers use to compromise password security

Les mots de passe sont le mécanisme de contrôle d'accès le plus couramment utilisé aujourd'hui, et il est essentiel que vous compreniez comment vous protéger contre les attaquants qui cherchent à compromettre leur sécurité. Connaître comment les craqueurs de mots de passe (**password crackers**), les attaques par dictionnaire (**dictionary attacks**) et l'ingénierie sociale (**social engineering**) peuvent être utilisés pour compromettre la sécurité des mots de passe.

- Be familiar with the various types of application attacks attackers use to exploit poorly written software

Les attaques d'applications sont l'une des plus grandes menaces pour l'informatique moderne. Les attaquants exploitent les débordements de mémoire tampon (**buffer overflows**), les trappes (**trap doors**), les vulnérabilités de temps de vérification à l'heure de l'utilisation (**time-of-check-to-time-of-use**) et les **rootkits** pour obtenir un accès illégitime à un système. Les professionnels de la sécurité doivent avoir une compréhension claire de chacune de ces attaques et des contre-mesures associées.

- Understand common web application vulnerabilities and countermeasures

Comme de nombreuses applications migrent vers le Web, les développeurs et les professionnels de la sécurité doivent comprendre les nouveaux types d'attaques qui existent dans cet environnement et les moyens de s'en protéger. Les deux exemples les plus courants sont les attaques par script intersite (**cross-site scripting - XSS**) et les attaques par injection SQL (**SQL injection**).

- Know the **network reconnaissance techniques** used by attackers preparing to attack a network

Avant de lancer une attaque, les pirates utilisent les scans IP pour rechercher les hôtes actifs sur un réseau. Ces hôtes sont ensuite soumis à des analyses de port et à d'autres sondes de vulnérabilité pour localiser les points faibles qui pourraient être attaqués dans le but de compromettre le réseau. Vous devriez comprendre ces attaques pour protéger votre réseau contre elles, en limitant la quantité d'informations que les pirates peuvent obtenir.

- What is the major difference between a **virus** and a **worm** ? ***

Les virus et les vers voyagent tous les deux d'un système à l'autre pour tenter d'envoyer leurs charges utiles malveillantes (**malicious payloads**) à autant de machines que possible. Cependant, les **virus** requièrent une **intervention humaine**, telle que le partage d'un fichier, d'une ressource réseau ou d'un message électronique, pour les propager. D'un autre côté, les **vers (worm)** cherchent des vulnérabilités et se propagent d'un système à l'autre **par leur propre pouvoir**, amplifiant ainsi considérablement leurs capacités de reproduction, en particulier dans un réseau bien connecté.

- Explain the four propagation methods used by Robert Tappan Morris's Internet worm ***

Le ver Internet a utilisé quatre techniques de propagation. Premièrement, il a exploité un bogue (**bug**) dans l'utilitaire Sendmail qui lui a permis de se propager en envoyant un message électronique spécialement conçu contenant son code au programme Sendmail sur un système distant. Deuxièmement, il a utilisé une attaque par mot de passe basée sur un dictionnaire (**dictionary-based password attack**) pour tenter d'accéder aux systèmes distants en utilisant le nom d'utilisateur et le mot de passe d'un utilisateur du système valide. Troisièmement, il a exploité une vulnérabilité de dépassement de tampon (**buffer overflow vulnerability**) dans le programme Finger pour infecter des systèmes. Quatrièmement, il a analysé les relations de confiance existantes avec d'autres systèmes sur le réseau et a tenté de se propager (**to spread itself**) à ces systèmes via le chemin de confiance.

- What are the actions an **antivirus** software package might take when it discovers an infected file ? ***

Si possible, le logiciel antivirus peut essayer de désinfecter (**disinfect**) un fichier infecté, en supprimant le code malveillant du virus. Si cela échoue, il peut soit mettre en quarantaine (**quarantine**) le fichier pour un examen manuel, soit le supprimer (**delete**) automatiquement pour éviter toute infection supplémentaire.

- Explain how a **data integrity assurance** package like Tripwire provides some secondary virus detection capabilities ***

Des paquets d'assurance d'intégrité des données (**Data integrity assurance packages**) comme Tripwire calculent des valeurs de hachage pour chaque fichier stocké sur un système protégé. Si un virus infecte un fichier, cela entraînerait une modification de sa valeur de hachage et déclencherait par conséquent une alerte d'intégrité de fichier.