



8SEC201-01 Cybersécurité défensive : vulnérabilité et incidents.

UQAC

UNIVERSITÉ DU QUÉBEC
À CHICOUTIMI

Hajar Moudoud
Hajar.moudoud@uqac.ca

Chapitre 4:

Intelligence en sécurité : visibilité et stratégie





Table des matières

- I. Introduction à l'intelligence en sécurité
- II. Collecte et traitement des données
- III. Analyse de données et génération de rapports
- IV. Mise en œuvre de la stratégie en intelligence en sécurité
- V. Gestion des incidents de sécurité
- VI. Évaluation de la vulnérabilité

Brèches de sécurité

- 2021, la brèche informatique Log4Shell qui a forcé le gouvernement du Québec à fermer 4000 sites internet vulnérables



- 2022, brèche informatique mondiale et historique – log4j:
 - Sophos
 - SonicWall
 - Unifi/Ubiquiti
 - VMWare

Constat 1 : Pointe de l'iceberg

1. Difficile de quantifier les incidents!

- Les victimes ne déclarent pas les incidents.

Exemple: Les banques ne sont pas obligées de divulguer les vols effectués sur les comptes de leurs clients.

- Les incidents les plus visibles sont les plus médiatisés.

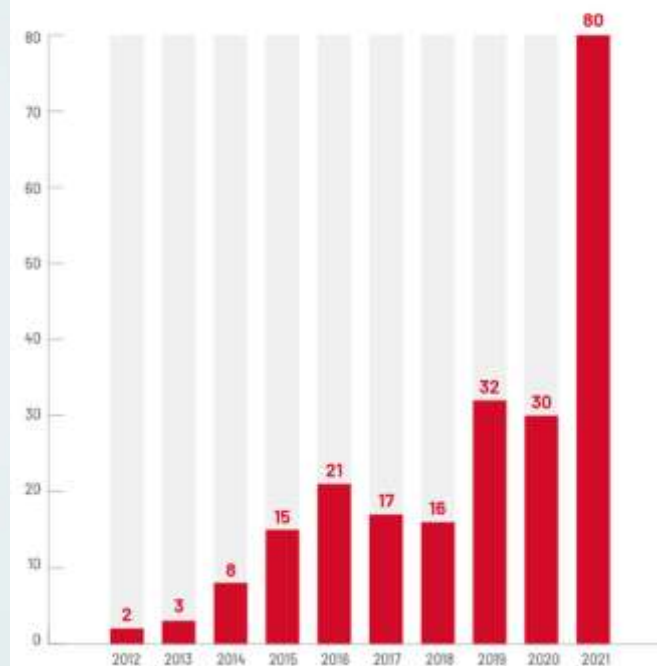
Exemple:- HeartBleed -- Revenue Canada (2014) (Fermeture du site web)
- Ransomware -- Université de Calgary (Ranson de \$20,000 juin 2016)



Constat 2 : Trop de vulnérabilités

- Le terme "jour zéro" désigne en fait deux choses : une vulnérabilité de jour zéro et un exploit de jour zéro. La vulnérabilité "zéro jour" désigne une faille de sécurité dans un logiciel - tel qu'un logiciel de navigation ou un logiciel de système d'exploitation - qui n'est pas encore connue du fabricant du logiciel ou des éditeurs d'antivirus.

Zero-Days Exploited
2012-2021





Constat 3: Cybersécurité défensive



Leçon apprise suite à un incident?

-Pauvre qualité du logiciel

- ☐ Vérifier les bornes des langages de programmation (e.g., C, C++, Java, etc.)
- ☐ Vérifier les intrants (e.g., SQL injection)

-Pauvre gestion de l'infrastructure

- ☐ Mettre à jour les logiciels!
- ☐ Limiter l'accès au strict minimum!
- ☐ Surveiller le trafic entrant et sortant!



Constat 4: Motif des attaques



□ Historiquement,

- Prouver ces compétences techniques
- Représailles envers un ancien employeur
- ...

□ Actuellement

- \$\$\$\$ – Extorsion (dénier de service vers un site populaire)
- \$\$\$\$ – Vol (carte de crédit, identité)
- \$\$\$\$ – Vol sur une grande échelle (transactions bancaires)
- \$\$\$\$ – Distribution de la publicité (SPAM)
- Sécurité nationale



Constat 5: Cibles



Première vague (push aléatoire)

- ☐ Disquettes
- ☐ Fichiers
- ☐ Courriels avec pièces jointes (SPAM)
- ☐ Génération aléatoire d'adresses

Seconde vague (pull de l'utilisateur)

- ☐ Applications populaires infectées
- ☐ Sites web infectés
- ☐ XSS

Troisième vague (cibler une organisation)

☐ « advanced persistent threat » (APT) est une attaque où la personne malveillante cherche à avoir un accès prolongé à un système informatique afin d'obtenir de l'information sensible.

Quatrième vague (cibler des particuliers ou des petites organisations)

- ☐ Scareware, Ransomware



Cybersécurité défensive ?



La cybersécurité défensive est un ensemble de mesures, de technologies et de pratiques visant à protéger les systèmes informatiques, les réseaux et les données contre les menaces en ligne



Cybersécurité défensive ?



Pare-feu

- ☐ Systèmes permettant de filtrer les flux de données entre deux domaines.

Systèmes de détection ou de prévention d'intrusion

- ☐ Systèmes permettant de détecter ou de prévenir les attaques informatiques.

Logiciels antivirus

- ☐ Systèmes permettant de détecter et d'éliminer les virus informatiques

Contrôle d'accès

- ☐ Authentification : Permettre d'identifier une entité.
- ☐ Autorisation : Vérifier si une entité peut accéder à un service ou à de l'information.
- ☐ Audit : Garder des traces de toutes les opérations effectuées



Cybersécurité défensive ?



Cryptographie

- ☐ Confidentialité : Limiter la diffusion des données aux seules entités autorisées.
- ☐ Intégrité : Vérifier que les données ne sont pas altérées lors de leur traitement.
- ☐ Non-répudiation : S'assurer que les entités engagées dans une communication ne peuvent nier d'y avoir participé.
- ☐ Anonymat et Domaine privé : S'assurer que les informations liées à l'identité ne sont pas divulguées.



Les actifs



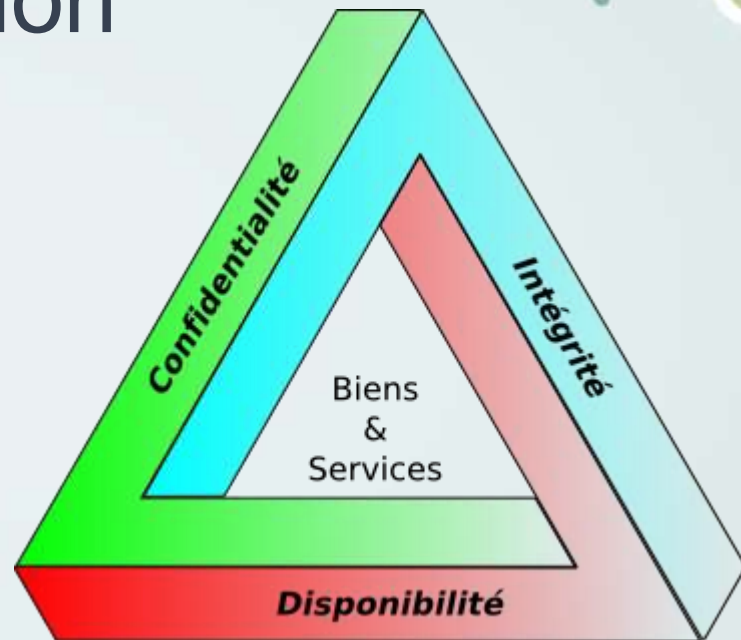
Les actifs informationnels représentent l'ensemble des données et des systèmes d'information nécessaires au bon déroulement d'une entreprise.

- Base de données Clients
- Base de données Employés
- Portail web transactionnel
- Code source d'une application
- Base de données Usagers

Clés de la sécurité de l'information

Trios du CID:

1. Confidentialité : il s'agit de protéger les informations sensibles contre les fuites ou les accès non autorisés. Cela implique de s'assurer que les informations sont uniquement accessibles aux personnes autorisées.
2. Intégrité : il s'agit de garantir que les informations ne sont pas altérées ou endommagées de manière intentionnelle ou accidentelle. Cela peut inclure la protection contre les attaques telles que la modification de données ou la falsification de données.
3. Disponibilité : il s'agit de garantir que les informations sont accessibles en temps voulu aux utilisateurs autorisés. Cela peut inclure la protection contre les attaques telles que les attaques par déni de service (DoS) qui rendent les informations inaccessibles.





Clés de la sécurité:

Confidentialité



Menaces

- ☐ Surveillance du réseau
- ☐ Vol de fichiers (Fichiers de mots de passe, Fichiers de données)
- ☐ Espionnage
- ☐ Ingénierie sociale

Contre-mesures

- ☐ Cryptographie (Chiffrement)
- ☐ Contrôle d'accès (Mot de passe à usage unique)
- ☐ Classification des actifs
- ☐ Formation du personnel



Clés de la sécurité: Intégrité



Menaces

- ☐ Attaques malicieuses (Virus, Bombes logiques, Portes dérobées)
- ☐ Erreurs humaines

Contre-mesures

- ☐ Cryptographie (Authentification, signature)
- ☐ Contrôle d'accès (Mot de passe à usage unique)
- ☐ Système de détection d'intrusion
- ☐ Formation du personnel



Clés de la sécurité:

Disponibilité



Menaces

- ☐ Attaques malicieuses (Dénis-de-service)
- ☐ Inondation
- ☐ Vulnérabilités logicielles
- ☐ Attaques accidentelles
- ☐ Pannes (Environnemental, logiciel, matériel)
- ☐ Attaques malicieuses (Virus, Bombes logiques, Portes dérobées)
- ☐ Erreurs humaines

Contre-mesures


- ☐ Pare-feu
- ☐ Système de détection d'intrusion
- ☐ Formation du personnel




Cybersécurité défensive – approche traditionnelle

Le rôle des responsables des l'expert en cyber sécurité

❑ Se basant sur le fait que les systèmes informatiques sont intrinsèquement vulnérables (bogues de logiciel, mauvais design, ...), les responsables des TI doivent mettre en place les moyens de résister aux diverses menaces afin de protéger les actifs de leurs entreprises.



Cybersécurité défensive – approche traditionnelle



Déployer une infrastructure adéquate résistant aux attaques et assurant l'intégralité des actifs (et leurs propriétés).

☐ Prévention


- ☐ Contrôle d'accès
- ☐ Mise à jour des logiciels
- ☐ Pare-feu, Systèmes de prévention d'intrusion (SPI)

☐ Détection

- ☐ Antivirus
- ☐ Systèmes de détection d'intrusion (SDI)
- ☐ Audit


☐ Réaction

- ☐ Pare-feu



Cybersécurité défensive – approche traditionnelle

Exemple



Protéger le périmètre du réseau.

- ☐ Pare-feu, SDI, SPI

Protéger les serveurs publics.


- ☐ Logiciels mis à jour régulièrement
- ☐ Zones démilitarisées

Partitionner le réseau interne.

- ☐ Contrôle d'accès, pare-feu, SDI, SPI


Protéger les serveurs internes et les usagers.

- ☐ Logiciels mis à jour régulièrement
- ☐ Antivirus




Cybersécurité défensive – approche actuelle •

L'intelligence en sécurité




L'intelligence en sécurité (ou "SI", pour "Security Intelligence") est une approche de la sécurité informatique qui utilise des données et des analyses pour comprendre les menaces et les comportements anormaux afin de mieux protéger les systèmes et les réseaux.

L'intelligence en sécurité se concentre sur la collecte, l'analyse et l'utilisation des données de sécurité pour aider les organisations à prendre des décisions éclairées en matière de sécurité et à améliorer leur capacité à prévenir, détecter et répondre aux menaces informatiques.




Cybersécurité défensive – approche actuelle • L'intelligence en sécurité




Importance de l'intelligence en sécurité dans la gestion des risques de cybersécurité:

1. Comprendre les menaces : L'intelligence en sécurité aide les organisations à comprendre les menaces actuelles et futures, les tendances et les techniques utilisées par les cybercriminels pour pénétrer dans les systèmes.
2. Améliorer la détection : L'utilisation de données de sécurité et d'analyse permet aux organisations de mieux détecter les menaces et les comportements anormaux.
3. Prévention des futurs incidents : L'intelligence en sécurité peut aider les organisations à développer des stratégies de sécurité plus efficaces pour prévenir les futurs incidents de sécurité.



Cybersécurité défensive – approche actuelle •

L'intelligence en sécurité



4. Réponse rapide et efficace aux incidents : En cas d'incident de sécurité, l'intelligence en sécurité peut aider les organisations à comprendre rapidement la nature de la menace et à prendre des mesures pour limiter les dommages.
5. Meilleure gestion des risques : L'intelligence en sécurité peut aider les organisations à évaluer les risques de sécurité et à développer des plans pour les gérer.
6. Optimisation de la sécurité : L'intelligence en sécurité permet aux organisations d'optimiser leurs investissements en sécurité en identifiant les domaines où les ressources peuvent être utilisées de manière plus efficace.



Cybersécurité défensive – approche actuelle •

L'intelligence en sécurité: Collecte de données



1-Collecte de données :

La première étape consiste à collecter des données de sécurité à partir de différentes sources, telles que les systèmes de détection d'intrusion (IDS), les systèmes de protection contre les logiciels malveillants (antivirus), les systèmes de gestion de la sécurité (SIEM) et les plateformes de sécurité en nuage.

2-Normalisation des données :

Une fois les données collectées, elles doivent être normalisées pour pouvoir être utilisées efficacement.

3-Analyse des données :

L'analyse des données peut inclure l'utilisation d'algorithmes d'apprentissage automatique pour identifier les comportements anormaux et les menaces potentielles.

4-Utilisation des données:

es données de sécurité peuvent être utilisées pour développer des stratégies de sécurité plus efficaces, pour améliorer la détection des menaces et pour informer les décisions en matière de sécurité.



Analyse de données et génération de rapports



Les techniques d'analyse de données :

1. **Analyse statistique** : L'analyse statistique implique l'utilisation de méthodes mathématiques pour décrire et résumer les données de sécurité. Les techniques statistiques peuvent inclure la régression, l'analyse de variance, la corrélation et la régression multiple.
2. **Apprentissage automatique** : L'apprentissage automatique est un domaine de l'intelligence artificielle qui implique l'utilisation d'algorithmes pour développer des modèles à partir de données. En intelligence en sécurité, ces modèles peuvent être utilisés pour identifier les comportements anormaux et les menaces potentielles.
3. **Analyse de graphes** : L'analyse de graphes implique l'utilisation de réseaux de données pour représenter les relations entre les éléments de sécurité. Les analystes peuvent utiliser ces graphes pour comprendre les relations entre les différents acteurs et les comportements de sécurité.




Analyse de données et génération de rapports




Les techniques d'analyse de données :


4. **Analyse de séquences** : L'analyse de séquences implique l'examen de séries de données chronologiques pour déterminer les relations entre les événements. Cette technique peut être utilisée pour comprendre la chronologie des incidents de sécurité et les relations entre les différents acteurs impliqués.
5. **Anomalie détection** : La détection d'anomalies implique l'utilisation de techniques pour identifier les comportements ou les événements qui sont différents des normes établies. En intelligence en sécurité, ces techniques peuvent être utilisées pour détecter les comportements anormaux qui peuvent indiquer une menace potentielle.




Outils d'analyse de données en intelligence en sécurité



1. **Logiciels de SIEM (Security Information and Event Management)** : Les logiciels de SIEM permettent la collecte et l'analyse en temps réel des journaux d'événements de sécurité provenant de différents systèmes et réseaux.
2. **Outils de gestion de la menace** : Les outils de gestion de la menace permettent la collecte et l'analyse de données sur les menaces potentielles, tels que les avis de menace et les bases de données de vulnérabilité.
3. **Outils d'analyse de graphes** : Les outils d'analyse de graphes permettent la visualisation des relations entre les différents acteurs et les comportements de sécurité.
4. **Outils de visualisation de données** : Les outils de visualisation de données permettent la création de représentations graphiques des données de sécurité pour aider à comprendre les informations dérivées de l'analyse de données.



Génération de rapports en intelligence en sécurité



La génération de rapports en intelligence en sécurité est un aspect important de l'analyse de données. Les rapports peuvent aider les décideurs à comprendre les menaces potentielles et à prendre des décisions éclairées en matière de sécurité,

-Les rapports peuvent être générés à différents intervalles:

- quotidiennement
- hebdomadairement
- mensuellement, en fonction des besoins de l'organisation.

-Les rapports peuvent être créés à l'aide:

- outils de génération de rapport intégrés aux logiciels
- logiciels de génération de rapport distincts



Mise en œuvre de la stratégie en intelligence en sécurité



La mise en œuvre de la stratégie en intelligence en sécurité est un aspect crucial pour garantir la sécurité des systèmes et des données.

Étapes clés à suivre pour mettre en œuvre une stratégie d'intelligence en sécurité :

1. **Élaboration d'une stratégie** : La première étape consiste à élaborer une stratégie en intelligence en sécurité qui définit les objectifs, les responsabilités et les ressources nécessaires pour renforcer la sécurité.
2. **Mise en place des outils et des processus** : La deuxième étape consiste à mettre en place les outils et les processus nécessaires pour collecter et analyser les données de sécurité. Cela peut inclure l'installation de logiciels de SIEM, d'outils de gestion de la menace et d'outils d'analyse de données.
3. **Formation et sensibilisation** : La troisième étape consiste à former les employés à l'importance de l'intelligence en sécurité et à leur fournir les compétences nécessaires pour collecter et analyser les données de sécurité.
4. **Surveillance et révision régulière** : La dernière étape consiste à surveiller les processus et à les réviser régulièrement pour garantir qu'ils fonctionnent de manière efficace et que les décisions en matière de sécurité sont basées sur des informations à jour.



La stratégie en intelligence en sécurité



L'élaboration de la stratégie en intelligence en sécurité est la première étape pour renforcer la sécurité des systèmes et des données.

La stratégie en intelligence en sécurité définit:

- les objectifs
- les responsabilités
- les ressources nécessaires pour renforcer la sécurité.



La stratégie en intelligence en sécurité



Étapes clés pour élaborer une stratégie en intelligence en sécurité :

1. **Évaluation des risques** : évaluer les risques de cybersécurité actuels et futurs, en prenant en compte les menaces potentielles, les vulnérabilités et les impacts potentiels sur les activités de l'entreprise.
2. **Définition des objectifs** : définir les objectifs de la stratégie en intelligence en sécurité. Cela peut inclure la protection des données sensibles, la détection et la réponse aux incidents de sécurité, la prévention des attaques futures et la mise en œuvre de mesures de sécurité pour les activités critiques.
3. **Allocation des ressources** : allouer les ressources nécessaires pour mettre en œuvre la stratégie d'intelligence en sécurité, y compris les outils, les employés et les processus nécessaires pour collecter et analyser les données de sécurité.
4. **Définition des responsabilités** : définir les responsabilités de chaque membre de l'équipe en matière de sécurité et à déterminer qui sera responsable de la mise en œuvre de la stratégie d'intelligence en sécurité.
5. **Élaboration d'un plan d'action** : élaborer un plan d'action détaillé qui décrit les étapes nécessaires pour mettre en œuvre la stratégie en intelligence en sécurité.

Évaluation de l'efficacité de la stratégie en intelligence en sécurité

Étapes clés pour évaluer l'efficacité de la stratégie en intelligence en sécurité :

1-Suivi des indicateurs de performance

- nombre d'incidents
- qualité des rapports d'analyse de données

2-Évaluation des risques

- faible, moyen, élevé

3-Feedback des utilisateurs

- Bon, moyen, faible



4-Examen de la conformité réglementaire

- conforme aux lois et réglementations en vigueur

5-Évaluation de la maturité de la sécurité

- mesurer la maturité de la sécurité







Gestion des incidents de sécurité

La gestion des incidents de sécurité fait partie intégrante de l'intelligence en sécurité.

Elle consiste à:

- identifier
- évaluer
- résoudre les incidents de sécurité





Gestion des incidents de sécurité: Définition

Un incident de sécurité est un événement ou une activité qui met en danger la confidentialité, l'intégrité ou la disponibilité des systèmes informatiques, des données ou des réseaux.

Les incidents de sécurité peuvent être causés par:



- erreurs humaines
- vulnérabilités logicielles
- attaques malveillantes
- défaillances matérielles.



Gestion des incidents de sécurité: Définition

Les types d'incidents de sécurité comprennent :

1. **Les attaques malveillantes** : incluent les virus, les logiciels espions, les chevaux de Troie, les ransomwares et les attaques DDoS (Distributed Denial of Service).
2. **Les erreurs humaines** : peuvent inclure la divulgation accidentelle d'informations sensibles, la perte de dispositifs de stockage de données et la mauvaise configuration de systèmes de sécurité.
3. **Les vulnérabilités logicielles** : peuvent être exploitées pour accéder aux systèmes informatiques et aux données sensibles.
4. **Les défaillances matérielles** : peuvent inclure des pannes de serveur, des erreurs de disque dur et des coupures de courant.



Gestion des incidents de sécurité

Étapes clés de la gestion des incidents de sécurité :

1. Identification des incidents :

- systèmes de surveillance de la sécurité
- alertes générées par les utilisateurs.

2. Évaluation des incidents :

- la gravité de la menace
- les actions nécessaires pour la neutraliser.

3. Containment :


- minimiser les dommages potentiels.

4. Investigation


- déterminer la cause de l'incident
- collecter les preuves pour aider à prévenir les incidents futurs.

5. Résolution :

- corriger les vulnérabilités identifiées
- remettre les systèmes affectés à un état normal de fonctionnement.



Gestion des incidents de sécurité





Étapes clés de la gestion des incidents de sécurité :

4. Documentation :

- documenter les incidents de sécurité
- analyse post-incident
- améliorer les processus futurs de gestion des incidents.

5. Communication :

- communiquer les résultats de la gestion des incidents (y compris les employés, les clients et les autorités réglementaires.)



Gestion des incidents de sécurité

Outils de gestion des incidents de sécurité

1. **Systèmes de détection d'intrusion (IDS)** : surveillent les activités réseau pour détecter les anomalies qui peuvent indiquer une attaque malveillante.
2. **Logiciels de gestion des incidents (SIM)** : aident à centraliser les informations sur les incidents de sécurité, à les prioriser et à les gérer de manière efficace.
3. **Outils de détection de menaces** : utilisent des algorithmes de machine learning pour détecter les menaces potentielles et fournir des informations sur les mesures à prendre pour les contenir.
4. **Outils de réponse aux incidents** : peuvent inclure des scripts préécrits pour automatiser certaines tâches de réponse aux incidents, tels que la suppression de fichiers malveillants.
5. **Outils de gestion des vulnérabilités** : peuvent aider les entreprises à identifier les vulnérabilités logicielles et à les gérer en les priorisant en fonction de leur gravité potentielle.



Audite de Sécurité: l'enjeu



Il ne faut pas mélanger les besoins et les moyens utilisés pour répondre à ces besoins.

- ☐ Quels sont les acteurs?
- ☐ Quels sont les actifs? ☐ Quels sont les objectifs?
- ☐ Quelles sont les règles de gestion à mettre en place?
- ☐ Quels sont les moyens opérationnels à mettre en place?
- ☐ ...




Audite de Sécurité: Politiques de sécurité




- Les politiques de sécurité sont des énoncés généraux dictées par les cadres supérieurs décrivant le rôle de la sécurité au sein de l'entreprise afin d'assurer les objectifs d'affaire.
- Pour mettre en œuvre ces politiques, une organisation doit être mise en place.
 - ❑ Définition des rôles, des responsabilités et des imputabilités

L'analyse de risque est à la base de cette activité




Évaluation des vulnérabilités




- L'évaluation de la vulnérabilité est un processus qui consiste à identifier les faiblesses et les points de vulnérabilité dans les systèmes et les réseaux informatiques d'une entreprise.

Les étapes clés de l'évaluation de la vulnérabilité incluent :

1. **Reconnaissance des actifs** : Identifier tous les actifs informatiques, tels que les serveurs, les ordinateurs de bureau, les réseaux, etc.
2. **Identification des vulnérabilités** : Identifier les vulnérabilités potentielles dans les actifs informatiques, telles que les faiblesses dans les logiciels, les configurations inappropriées, les accès non autorisés, etc.
3. **Évaluation des risques** : Évaluer les risques potentiels associés à chaque vulnérabilité identifiée en utilisant des méthodes telles que le calcul des probabilités de menace.
4. **Détermination des mesures de mitigation** : Déterminer les mesures à prendre pour gérer les vulnérabilités identifiées, telles que la mise à niveau du logiciel, la configuration de sécurité renforcée, etc.
5. **Surveillance continue** : Surveiller les systèmes et les réseaux informatiques pour s'assurer que les vulnérabilités sont gérées de manière adéquate et que de nouvelles vulnérabilités ne sont pas identifiées.



Outils d'évaluation de la vulnérabilité



1. **Scanneurs de vulnérabilité** : Les scanneurs de vulnérabilité sont des outils qui analysent les systèmes et les réseaux informatiques pour identifier les vulnérabilités potentielles.
2. **Vulnerability Management Platforms (VMP)** : Les plateformes de gestion des vulnérabilités sont des solutions complètes qui aident les entreprises à gérer les vulnérabilités identifiées dans leurs systèmes et réseaux informatiques.
3. **Outils de simulation d'attaque** : Les outils de simulation d'attaque sont des outils qui permettent aux entreprises de simuler des attaques potentielles pour évaluer la sécurité de leurs systèmes et réseaux informatiques.
4. **Outils de compliance** : Les outils de conformité aident les entreprises à s'assurer qu'ils respectent les réglementations et les normes de sécurité en vigueur..