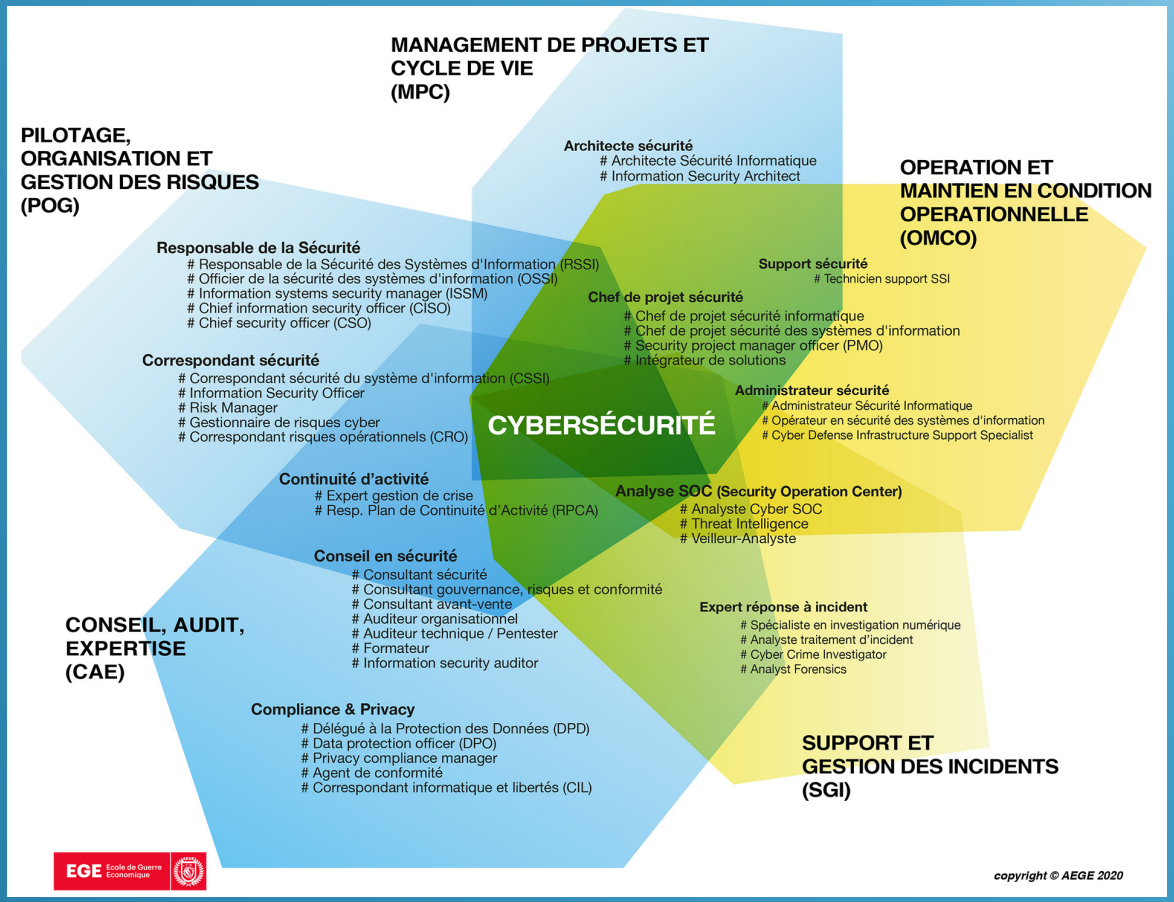
Management de la sécurité

Savoir organiser et manager la Sécurité des Systèmes d'Information d'une structure.

ANDN SERVICES

Schéma de l'organisation cybersécurité



Pilotage, organisation et gestion des risques (POG)

Le RSSI

Responsable de la cybersécurité:

Il garantit la sécurité, la disponibilité et l'intégrité du SI et des données.

Il fait partie de la famille POG (métier management totalement dédié sécurité).

Souvent appelé RSSI (Responsable de la sécurité des systèmes d'informations) ou CISO (Chief Information Security Officier).

Si le RSSI est souvent rattaché à la Direction des systèmes d'information, il est parfois rattaché à la direction générale de l'entreprise dans les grands groupes, compte tenu des enjeux et des risques (notamment juridiques) portés par le système d'information.

Les missions du RSSI

Les missions du RSSI sont multiples:

Il définit, met en œuvre, anime et contrôle la politique de sécurité de l'information en conformité avec la loi et les règlementations.

Opérations de sécurité: Analyse des menaces immédiates en temps réel et trie des problèmes

Les missions du RSSI

- Cyber-risque et cyber-intelligence: Être conscient des menaces de sécurité qui se développent et aider la direction à comprendre les problèmes de sécurité potentiels qui pourraient résulter d'acquisitions ou d'autres mouvements de grandes entreprises.

- Perte de données et prévention de la fraude: S'assurer que le personnel interne n'utilise pas abusivement, ne modifie pas ou ne vole pas les données

Les missions du RSSI

- Architecture de sécurité : Planification, achat et déploiement du matériel et des logiciels de sécurité et assurez-vous que l'infrastructure informatique et réseau est conçue en tenant compte des meilleures pratiques de sécurité.

- Gestion des Identités et des Accès : S'assurer que les données et les systèmes restreints ne sont accessibles qu'aux personnes autorisées.

Les missions du RSSI

- Architecture des applications : Implémenter des programmes qui réduisent les risques tels que des correctifs système réguliers. Concevoir des plans stratégiques qui gèrent la mise en œuvre des technologies de sécurité de l'information utilisées au sein de l'organisation.

- Investigations et Forensics : Pour déterminer comment une violation s'est produite en cas d'occurrence, il faut traiter avec les responsables, s'il s'agit du personnel interne, et il faut faire des plans pour éviter que la même crise ne se reproduise.

Les missions du RSSI

- Gouvernance SI : S'assurer que les initiatives susmentionnées se déroulent sans heurts et obtenir le financement chaque fois que nécessaire et s'assurer que le chef d'entreprise comprend leur importance.

- Évaluation, Atténuation et Évitement des risques : un RSSI doit effectuer une enquête et un inventaire approfondis des actifs informationnels, de la propriété intellectuelle et d'autres fonds numériques de valeur, connaître les menaces auxquelles ils sont susceptibles de faire face, décider des mesures à prendre pour protéger ces éléments de tout dommage ou perte.

Les missions du RSSI

- Conformité légale et réglementaire : Il est important de comprendre comment les actifs informationnels et les fonds numériques d'une entreprise entrent dans le champ d'application des lois et réglementations applicables et en respectant les exigences connexes telles que les évaluations, les audits, les rapports, la vie privée, la confidentialité, etc. Le responsable de la cybersécurité doit être prêt à faire face à une faille de sécurité, à évaluer et à gérer les conséquences juridiques, commerciales et financières.

Les missions du RSSI

- S'assurer que toutes les politiques de sécurité d'entreprise sont développées et conformes aux normes de sécurité définies.
- Sélection d'experts en sécurité informatique et les guider en permanence. Leur offrir diverses formations, les aider chaque fois que nécessaire et amplifier leurs compétences en leadership pour qu'ils atteignent un poste plus élevé.
- Concevoir et mettre en œuvre des programmes de formation pour sensibiliser les utilisateurs et la conformité à la sécurité.

Les missions du RSSI

- Rester à jour avec toute l'infrastructure moderne pour les différents systèmes de sécurité au sein de l'organisation.
- Rechercher les vulnérabilités, menaces ou événements existants au sein des réseaux ou des systèmes de votre organisation.

Opération et maintien en condition opérationnelle (OMCO)

Définition

- Le MCO est l'ensemble des stratégies nécessaires pour garantir que les applications, infrastructures et matériels soient disponibles à tout moment.
- Il existe un grand nombre de causes de dysfonctionnements: incendie, piratage, dégâts des eaux, grève, vols de données, panne matériels
- Il est donc nécessaire de mettre en place des solutions pour permettre d'offrir une protection optimale de toute l'infrastructure informatique et du SI.

Pourquoi le MCO ?

- La communication digitale est le principal levier de développement des entreprises. La production s'appuie grandement sur les équipements informatiques. Donc un grand risque sur ces équipements = un grand risque sur les entreprises.

- MCO != entretient et réparation il est aussi là pour mettre en œuvre une stratégie pour faire en sorte que tout soit toujours performants durant le cycle de vie (maintien et prévention des risques).

En quoi consiste le MCO ?

- Garantir la dispo des équipements et du matériel info
- Maintenance préventive et corrective
- Soutien technique (maintenance, gestion, update, etc)
- Soutien logistique (maintenance et installation matériel en cas de panne)

En quoi consiste le MCO ?

- C'est la raison pour laquelle le MCO doit avoir des évolutions continues à travers:
  - Une optimisation permanente des équipements via les mises à jour et autres maintenances
  - Une bonne gestion à travers la prise de décision, la maintenance, la gestion des risques…
  - Un accompagnement à distance et sur le terrain des utilisateurs au sein de l'entreprise (dirigeants et employés) pour assurer une meilleure performance et une protection des systèmes utilisés
  - Un maintien des équipements pour avoir une durée de vie maximale et réduire au minimum les risques de pannes
  - Un approvisionnement en cas de rechange ou de réparation nécessaires

Management de projets et cycle de vie (MPC)

Définition du PDCA

- PDCA (Plan, Do, Check, Act)
- Planifier, Réaliser, Vérifier, Agir

- PDCA étant un cycle il implique une amélioration continue à chaque fois que le cycle est déclenché, et il revient donc à son commencement.

Concept du cycle PDCA

- La base de cet outil est dans la répétition. Il est appliqué de façon successive dans les processus dans le but d'une amélioration continue.
- Il est donc nécessaire de planifier, standardiser et documenter au mieux.

Plan (=Planifier)

- Définition des problèmes
- Etablissement d'objectifs
- Choix des méthodes
- Chercher plusieurs causes plausibles aux problèmes

Plan (=Planifier)

- Il est nécessaire pour planifier une solution à un problème d'identifier la cause de celui-ci. (Méthode des 5 Pourquoi)
- Par exemple: les données ne sont plus accessibles
- 1) Pourquoi les données ne sont plus accessibles ? Le disque dur est mort (vérification)
- 2) Pourquoi le disque dur est-il mort ? La tête de lecture a été décalée
- 3) Pourquoi la tête de lecture a été décalée ? Il y a eu des vibrations dans la baie du serveur
- 4) Pourquoi il y a eu des vibrations ? Le générateur de secours à sa batterie en fin de vie et génère des vibrations lors de surtension
- 5) Pourquoi le générateur de secours à sa batterie en fin de vie ? Elle date de 5 ans il est nécessaire de la changer

Do (=Réaliser)

- Mettre en pratique la méthode
- Exécuter la méthode
- Réajuster si nécessaire
- Ne pas chercher la solution absolue, mais ce qui est plausible
- Mesurer et enregistrer les résultats

Do (=Réaliser)

- Il est important de répéter cette étape donc il est préférable de réaliser ce qui est possible dans l'immédiat que d'essayer de réaliser des choses trop complexes dans le cadre actuel ou qui freinerait la progression du projet.
- Il est important de définir des standards atteignables et mesurer si les modifications apportées sont acceptables.

Check (=Vérifier)

- Vérifiez si le standard est atteint
- Vérifiez ce qui fonctionne et ce qui ne fonctionne pas
- Vous demandez « pourquoi ? » à chaque étape. Si un problème est détecté réappliquer la méthode des 5 pourquoi.
- Déterminer depuis les réponses le procédé définitif à adopter.

Act (=Agir)

- La planification est-elle prête ? Continuer à planifier
- Le projet contient-il des éléments non-conforme ? Prendre des mesures pour corriger et prévenir les erreurs
- Améliorer le système de travail
- Répétez les solutions qui se sont avérées appropriées

Act (=Agir)

- Cette phase la étant la quatrième et dernière, le concept du PDCA recommande de recommencer le cycle pour poursuivre une amélioration continue et ininterrompue.

Pérenniser la méthode

- Appliquer la phase Do (Réaliser) seulement après avoir totalement réaliser la phase Plan (Planifier).
- Si la phase Act (Agir) comporte un excès de répétitions et/ou d'essais il est nécessaire de retourner à la planification (Plan).
- Evitez de créer une coupure dans le cycle, en effet il n'est pas conseillé de sauter des phases ou de ne pas y consacrer assez de temps.

Les erreurs du PDCA

- Un manque de raisonnement en répondant aux 5 pourquoi
- Une analyse de scénario incomplète
- Des suivis incomplets
- Une mise en pratique inefficace
- Des mesures inexactes
- Une standardisation peu détaillée

Indicateurs clés de la DSI

1) Le taux de vulnérabilité

- Le taux de vulnérabilité renvoie au nombre de corrections effectuées au cours d'une période donnée sur le nombre total de corrections identifiées et jugées à réaliser, basé sur leur degré de criticité ou celle du système sous-jacent.

2) La disponibilité des systèmes

- Le taux de disponibilité des systèmes et réseau fait partie généralement des indicateurs les plus souvent cités par les DSI et les différents responsables de production.
- L'objectif ciblé est de 99% de disponibilité.

- Dans cette optique, il est nécessaire d'anticiper l'évolution des besoins en ressources informatiques. Notamment, dans le but d'éviter les surcharges lors des périodes de forte activité pour les métiers.

- Dans cette dynamique la virtualisation et les outils d'automatisation des datacenters contribuent à améliorer la souplesse des DSI.

3) Suivi des mise à jour des versions logiciels

- L'état du nombre de composants matériels et/ou logiciels non maintenus doit être réalisé par la DSI (postes de travail, serveurs, outils de sécurité…), avec pour objectif un ratio de moins de 10%.
- Il est aussi nécessaire de répertorier les composants non-conformes c'est-à-dire ceux ou les règles de sécurité ne sont pas appliquées.
- Exemple: un système maintenu par un logiciel sur lequel la DSI n'a pas ou plus la main
- Dans cette logique, il est nécessaire d'installer correctifs en plus des mise à jour.

4) Le nombre d'attaques

- Il est conseillé de réaliser régulièrement une vue du nombre d'attaques en direction du système d'information.
- Il existe 3 types d'attaques dans ce contexte:
  - Les attaques en environnement de messagerie
  - Les attaques en environnement intranet
  - Les attaques internet

- Pour chaque attaque il est nécessaire d'évaluer le nombre de postes de travails infectés.

5) Le degré de protection des données

- Le niveau de protection des données se mesure à l'aide de plusieurs indicateurs:
  - La part des métiers ayant réaliser une classification des données par niveaux de criticité
  - La part des métiers ayant identifié les données à archiver
  - La part des projets pour lesquels la maitrise d'ouvrage a réalisé une analyse des risques formalisée
  - La part des projets pour lesquels la MOA a exprimé des besoins en matière de sécurité
  - Le pourcentage d'applications couvertes par une politique de gestion des accès

6) Le temps de rétablissement en cas d'incident

- L'une des principales jauges du DSI en matière de sécurité est le temps de rétablissement après un incident par systèmes.
- Les moyens mis en place pour chacune des plates-formes devront être mise en cohérence avec le risque économique d'arrêt de l'application sur une certaine durée.
- Pour mesurer cet indicateur, il est recommandé de réaliser des tests grandeur nature sur des sites/applications miroirs avec des configurations au plus proches de celle du système en production (Iso Prod).

7) L'impact des attaques informatiques sur l'image de l'entreprise

- Les piratage de sites web et campagnes de hameçonnage (phishing, présentent un impact direct sur l'image d'une entreprise. D'où l'importance d'un tableau de bord pour assurer le suivi de cette dimension de la sécurité.

- Du point de vue du DSI, cette grille intègre en général trois indicateurs majeurs:
  - Le nombre de sites web contrefaits
  - Le nombre de noms de domaine usurpés
  - Le nombre de plaintes extérieures (par exemple phishing)

8) Le taux de prestataires intervenant sur les systèmes sensibles

- Cet indicateur est considéré comme critique par les DSI et RSSI.
- La part des prestataires externes occupants des postes IT critiques (administration réseaux, administration système..) doit faire l'objet d'un compte-rendu annuel.
- On estime qu'il ne faut pas excéder le ratio de 20% en matière de prestataire externe sur ce sujet.

9) Le taux de collaborateurs sensibilités à la sécurité informatique

- Il est difficile de mesurer le degré de sensibilisation des collaborateurs, il peut s'agir par exemple de mesurer la part des collaborateurs accédant au SI qui ont suivi une formation sur la sécurité informatique sur les trois dernières années.
- L'objectif sur un an étant dans l'idéal d'atteindre un ratio proche de 100% pour les salariés intervenant sur des systèmes critiques.

10) Le taux d'applications dotées de politique de gestion des accès

- Plusieurs indicateurs permettent de piloter la gestion des accès au SI:
  - Le pourcentage d'applications dotées d'une politique de gestion d'accès
  - Le pourcentage d'accès non-autorisés à des systèmes sensibles
  - Les pertes de mots de passe (mots de passe réinitialisés)
  - L'évolution du nombre d'identifiants générique (réduire à moins de 5%)

11) Le niveau de conformité du système d'information

- Les procédures de sécurité IT sont-elles correctement appliquées par la DSI et les métiers, notamment en matière de protection et de traçabilité des données (RPGD) ?
- Trois indicateurs annuels permettent de se faire une idée sur la question:
  - Le taux de contrôle (nombre d'audits de sécurité effectué sur le nombre d'audits cible)
  - Le taux de conformité (nombre d'audits effectués avec succès sur le nombre d'audits effectués)
  - Le taux de correction (nombre d'audits corrigés sur le nombre d'audits défectueux)

12) L'état de l'organisation et de la gouvernance de la sécurité

- Plusieurs éléments permettent de rendre compte du niveau de structuration de l'organisation et de la gouvernance de la sécurité du SI (maturité).
- Les comités de sécurité stratégique, en général au moins une fois par an ont-ils bien lieu ? Qu'en est-il des comités de sécurité opérationnels dont la tenue doit être en principe trimestrielle ?

- Enfin, le nombre de correspondants SSI responsables de la bonne application des règles de sécurité informatiques est-il suffisant et combien sont-ils ?

Identifier les actifs

Classification de l'information ou des actifs informationnels

- A l'aide d'un programme de sensibilisation à la cybersécurité sur la culture et les besoins de votre entreprise, la classification ou catégorisation des actifs informationnels est une étape essentielle dans le processus de gestion des risques informationnels.

- Cette étape permet de déterminer la criticité des actifs pour l'entreprise, en fonction de 3 objectifs de sécurité de l'information à savoir, la disponibilité, l'intégrité et la confidentialité.

La valeur de l'information ?

- L'information doit être traitée et protégée selon sa valeur et son niveau de confidentialité. Les utilisateurs doivent connaître la différence et traiter correction l'information en fonction de ses besoins en matière de protection.

- Pour déterminer la confidentialité de l'information, chacun doit se demander si sa divulgation non autorisée pourrait nuire à l'organisation et à sa réputation.

- Dans l'idéal tous les documents doivent être classifiés, crées ou utilisés en fonction de leur valeur pour votre organisation, de leur sensibilité et de leur niveau de confidentialité.

Qui est responsable ?

- La classification d'un actif devrait être effectuée par le propriétaire ou détenteur de celui-ci. Cette personne connait généralement les impacts d'affaires du à une perte de disponibilité, d'intégrité et de confidentialité de l'actif.
- Le détenteur connait aussi les lois et règlementations relatives à l'information de l'actif (Ex; RPGD, PASSI, PCI-DSS).

Méthodes de classifications

- Il existe plusieurs méthodes de classification de l'information.
- Une première consiste à définir une matrice de 3 ou 4 niveaux d'impact pour chaque élément du DIC (« Disponibilité », « Intégrité », « Confidentialité »).
- Chaque niveau est décrit (cote 1 = impact minime, cote 4 = impact très grave), l'idéal étant de pourvoir des exemples ou barèmes spécifiques à l'organisation afin de réduire les ambiguïtés et d'éviter les interprétations lors de l'attribution de la cote.

Méthodes de classifications

- Une secondé méthode consiste à mettre en priorité les critères d'impact les plus importants pour l'organisation et d'établir un arbre de décision pour chaque élément du DIC.

- L'exercice de classification permet d'optimiser les efforts de l'analyse de risques. En effet, cette analyse pourrait s'effectuer prioritairement sur les actifs les plus critiques, identifiés lors de la classification.

Modélisation du risque cyber

Définition du cyber-risque

- Dans les méthodes de gestion des risques, le risque est défini par l'impact d'un événement à risque multiplié par la probabilité que l'événement se produise.
- En ce qui concerne la cybercriminalité, nous pouvons affiner cette définition comme suit : le cyber-risque est égal aux dégâts potentiels aux actifs informatiques et à l'infrastructure, multiplié par la probabilité d'une attaque réussie.

Cyber-risque=Dégât potentiel x Probabilité d'attaque.

Principe de sécurité

- Les technologies de modélisation et de simulation sont « l'ingrédient secret » d'une gestion efficace des risques de sécurité.

- Dans le cas de la cyber-sécurité, les technologies de modélisation et de simulation offrent des avantages considérables, comme :
  - Prédiction de l'exposition au risque avant l'exploitation
  - Vérification de la modification prévue du réseau, avant qu'elle ne soit appliquée à l'environnement de production
  - Optimisation des contrôles de sécurité et des ressources
  - Analyse et comparaison de réseaux complexes
  - Formation rentable du personnel de cyber-sécurité

Construire un modèle

- La modélisation est le processus de réplication ou de création d'une représentation réaliste d'un environnement ou d'une situation.
- Dans le cas de la cyber-sécurité, la modélisation est le processus de création d'une vue normalisée de la situation en matière de cyber-sécurité.
- Le modèle contient généralement des informations sur l'infrastructure du réseau, les contrôles de sécurité, les vulnérabilités, les services professionnels, et les menaces.
- Le modèle est un moyen efficace de représenter l'état actuel d'un réseau, ou de montrer un état passé ou futur.
- Par exemple, une organisation peut souhaiter modéliser son propre réseau pour tester les capacités de défense, modéliser le réseau d'un concurrent à des fins offensives, ou comparer les modèles pour envisager des modifications et des relations de cause à effet.

Simulation

- La simulation permet d'imiter les activités des pirates, en utilisant des vulnérabilités connues, des informations sur l'infrastructure et les contrôles de sécurité en place.
- Le résultat de ce processus automatisé est un ensemble de scénarios d'attaques possibles, chacun ayant un ensemble spécifique de mesures pouvant être prises par les pirates (humains et/ou machines) afin de s'infiltrer dans l'infrastructure de l'organisation.

Simulation

- En simulant des scénarios d'attaque potentiels par rapport au modèle réseau, il est possible d'obtenir une évaluation réaliste de l'exposition au risque.
- La combinaison de la modélisation et de la simulation permet de combiner des interactions complexes en dehors de l'environnement réseau en direct - de sorte que l'infrastructure réelle n'est pas affectée.

- Comme il y a potentiellement un très grand nombre de scénarios d'attaque pour un réseau complexe, la technologie de simulation d'attaque doit être très rapide et évolutive pour être efficace dans des environnements réels.

La modélisation

- Utiliser la modélisation et la simulation pour la gestion des risques

- Le tableau suivant fournit un bref résumé de la façon dont les technologies de modélisation et de simulation sont utilisées pour automatiser le processus de gestion des risques de sécurité.

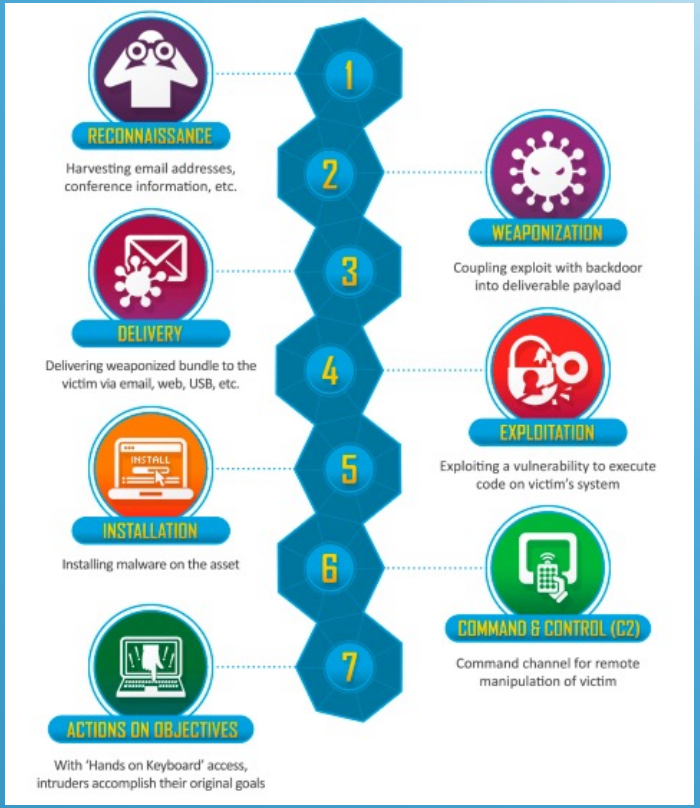
La modélisation

Étape de gestion du risque	Rôle de la modélisation et de la simulation
1. Actifs et cartographie du réseau	Découvre tous les actifs, réseaux, et configurations. Crée une vue normalisée de l'infrastructure et de ses vulnérabilités.
2. Évaluation du risque	Les scénarios d'attaque représentent toutes les conséquences possibles des menaces, des vulnérabilités, et les contre-mesures disponibles. Chaque scénario a une probabilité de créer des dégâts potentiels (conséquence). Risque = possibilité de scénario x dégâts potentiels.
3. Priorisation	Une fois que le risque a été calculé pour chaque scénario d'attaque, la priorisation se fait directement. En fonction des ressources et du temps disponibles, l'organisation mettra l'accent sur l'atténuation des vulnérabilités qui sont exploitables dans les scénarios d'attaque les plus risqués et/ou la configuration des contre-mesures.
4. Mise à jour	En utilisant la modélisation type « what-if », l'organisation peut vérifier l'efficacité des modifications potentielles en se basant sur la simulation des attaques sur un modèle futuriste - permettant l'optimisation des modifications proposées et la vérification que ces modifications atteignent leur objectif de sécurité sans interruption inutile des activités.
5. Suivi de progression	Les mises à jour continues du modèle permettent à l'organisation d'identifier automatiquement les modifications apportées aux actifs et aux réseaux, et de mesurer l'efficacité des modifications apportées, en comparant la simulation d'attaque de l'état actuel et l'état précédent du modèle.

La cyber Kill Chain

Les étapes d'une attaque informatique

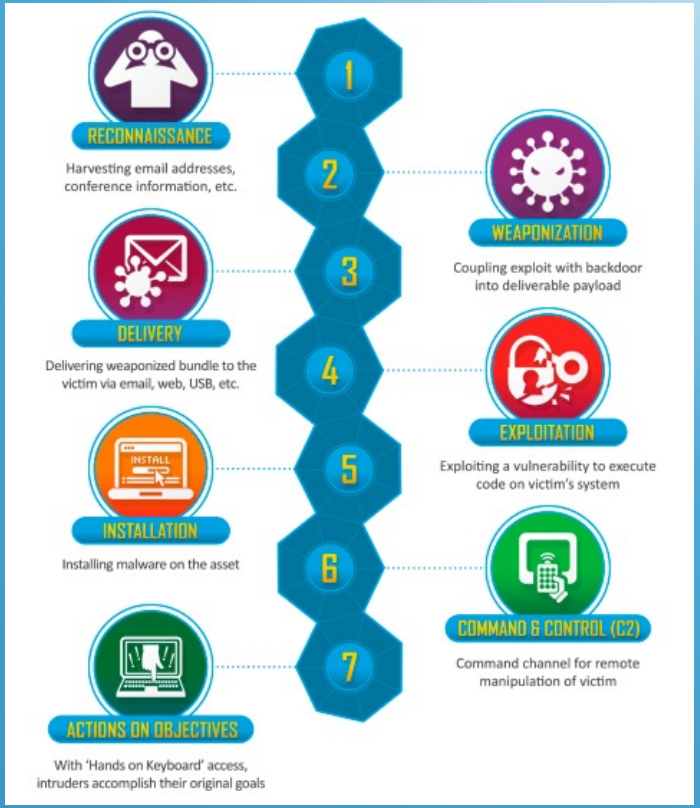
- 1. Reconnaissance – sélection la cible, recherche et identification des vulnérabilités du réseau cible
- 2. Armement – création d'un logiciel malveillant exploitant une ou plusieurs vulnérabilités
- 3. Livraison – transmission de l'arme à la cible – pièces jointes de courrier électronique, site web et clés USB



ANDN SERVICES

Les étapes d'une attaque informatique

- 4. Exploitation – exploitation des vulnérabilités par le logiciel malveillant
- 5. Installation – le logiciel malveillant installe un point d 'accès utilisable par l'attaquant
- 6. Commandement et contrôle – C2 – Accès permanent au réseau cible
- 7. Actions sur l'objectif – exfiltration de données, destruction de données ou chiffrement des données, etc



ANDN SERVICES

CVE / CVS

Qu'est-ce qu'une CVE

- CVE pour Common Vulnerabilites and Exposures en anglais, désigne une liste publique de failles de sécurité informatique. Lorsqu'on parle de CVE, on fait généralement référence à une faille de sécurité à laquelle un identifiant CVE a été attribué.

- Les avis de sécurités publiés par les fournisseurs et chercheurs mentionnent presque toujours au moins un identifiant CVE.
- Les CVE permettent aux professionnels de:
  - coordonner leurs efforts visant à hiérarchiser et résoudre les vulnérabilités
  - renforcer la sécurité des systèmes informatiques.

Le fonctionnement du système CVE

- La liste CVE est supervisée par l'organisme MITRE.
- Les entrées de la liste CVE sont brèves, elles ne comprennent pas de données techniques ni d'informations à propos des risques, effets et des correctifs.
- D'autres bases de données sont plus exhaustives mais se basent sur les identifiants CVE pour permettre de différencier de manière fiable une faille de sécurité d'une autre.

Les identifiants CVE

- Les identifiants CVE sont attribués par des autorités déléguées les CNA (CVE Numbering Authority).
- Les rapports de CVE peuvent avoir diverses origines:
  - Un fournisseur
  - Un chercheur
  - Un utilisateur avisé (Bug Bounty)

Les identifiants CVE

- En général, un identifiant CVE est attribué avant la publication de l'avis de sécurité, mais les fournisseurs ne révèlent pas l'existence d'une faille de sécurité tant qu'un correctif n'a pas été développé et testé.
- L'objectif est d'éviter qu'un cybercriminel n'exploite une faille non corrigée.
- Une fois publique, une entrée de la liste CVE comprend un identifiant CVE au format CVE-2021-7654321, une courte description de la vulnérabilité ou de la faille de sécurité ainsi que des références notamment des liens vers des rapports et des avis concernant la vulnérabilité.

Critères d'attribution d'un identifiant CVE

- Les identifiants CVE sont attribués aux failles qui répondent à un ensemble de critères:
- 1) Possibilité de correction indépendante
- Chaque faille doit pouvoir être corrigée indépendamment d'autre problèmes
- 2) Reconnaissance par le fournisseur concerné ou documentation
- L'éditeur de logiciel ou le fabricant doit reconnaître le problème et son effet négatif sur la sécurité. Ou alors la personne qui a signalé le problème doit partager un rapport de vulnérabilité qui permet de démontrer que le problème a un effet négatif et qu'il enfreint la politique de sécurité du système touché.
- 3) Les failles qui touchent plus d'un produit doivent recevoir différents identifiants CVE. Sauf dans le cas de bibliothèques, protocoles ou normes partagés s'il n'existe aucun moyen d'utiliser le code partagé sans être affecté par la vulnérabilité.

Qu'est-ce que le CVSS (Common Vulnerability Score System)

- Il existe plusieurs systèmes qui permettent d'évaluer la gravité d'une vulnérabilité, notamment le système CVSS (Common Vulnerability Scoring System).
- Ce système est un ensemble de normes ouvertes utilisées pour attribuer un nombre à une vulnérabilité afin d'en évaluer la gravité.
- Les scores CVSS servent aux bases de données NVD et CERT pour évaluer l'impact des vulnérabilités.
- Les scores sont compris entre 0 et 10, et les nombres les plus élevés correspondent au plus haut degré de gravité pour une vulnérabilité.

Le score

- 0 = risque nul
- 0.1 à 3.9 = risque faible
- 4.0 à 6.9 = risque modéré
- 7.0 à 8.9 = risque élevé
- 9.0 à 10 = risque critique

- Le score donne une idée, mais il est nécessaire de rentrer dans le détail de son calcul pour mieux comprendre en quoi une faille est dangereuse.

Le calcul détaillé

- Le calcul d'un score CVSS passe par trois blocs de critères qui répondent à trois questions clés:
  - Quel impact aura la vulnérabilité ?
  - Quel danger représente-t-elle à l'instant présent ?
  - Comment s'applique-t-elle à un cas de figure particulier ?

Quel impact aura la vulnérabilité ?

- Quel est le vecteur d'attaque ? (AV)
- Plus un attaquant peut exploiter la vulnérabilité de loin, plus elle sera dangereuse. À l'inverse, si l'assaillant doit obtenir un accès physique à un ordinateur de l'entreprise, la vulnérabilité sera bien plus difficile à exploiter. Et pour cause : l'attaquant devra aussi trouver une solution pour s'infiltrer dans les bâtiments de l'entreprise.

- Quelle est la complexité de l'attaque ? (AC)
- Ce critère mesure la complexité des moyens à déployer pour lancer l'attaque : faut-il un gadget, un logiciel particulier ? Le calculateur ne nous laisse choisir qu'entre deux options : basse et haute.

Quel impact aura la vulnérabilité ?

- Quel est le degré d'interaction avec les utilisateurs ? (UI)
- L'utilisateur a besoin de cliquer quelque part ou de lancer un programme pour que l'attaquant puisse exploiter la vulnérabilité ? En effet, plus l'attaquant pourra agir seul, plus la vulnérabilité sera dangereuse. On parle de faille « zero clic » quand un attaquant peut s'en prendre à une victime sans la pousser au préalable à l'erreur.

Quel impact aura la vulnérabilité ?

- Faut-il un certain niveau de privilège pour lancer l'attaque ? (PR)
- Chaque système informatique propose différents niveaux d'accès pour les utilisateurs. Par exemple, sur votre ordinateur personnel, vous pouvez créer un compte administrateur, qui pourra changer certains paramètres profonds de la machine, et un compte « invité » qui ne pourra pas par exemple installer ou désinstaller des logiciels. À l'échelle d'un réseau, le fonctionnement est similaire.
- Pour faire les manipulations nécessaires à l'exploitation de certaines failles, il faut obtenir un accès administrateur. Cela signifie que l'attaquant devra au préalable obtenir des identifiants d'un responsable du réseau avec un phishing, ou pirater un compte avec les bonnes autorisations.

Quel impact aura la vulnérabilité ?

- Quelle est la portée de l'attaque ? (S)
- Ce critère répond à une question : la faille de sécurité affecte-t-elle la sécurité d'autres produits ? Autrement dit, est-ce qu'un attaquant peut rebondir sur la vulnérabilité pour attaquer d'autres logiciels ? Va-t-elle produire des dégâts collatéraux ?

Quel impact aura la vulnérabilité ?

- La vulnérabilité affecte-t-elle la confidentialité de l'information ? (C)
- Ici, il s'agit de mesurer la perte de confidentialité de l'information. Autrement dit, de mesurer à quel volume d'informations les attaquants ont obtenu un accès.

- La vulnérabilité affecte-t-elle l'intégrité du logiciel ? (I)
- La vulnérabilité permet-elle de modifier le logiciel concerné ? Permet-elle de manipuler certaines fonctionnalités ?

Quel impact aura la vulnérabilité ?

- La vulnérabilité affecte-t-elle la disponibilité du logiciel ? (A)
- Ce critère permet de mesurer à quel point le hacker peut prendre la main sur le système. Si la vulnérabilité lui permet de prendre le contrôle et de bloquer l'accès aux autres utilisateurs, le score sera maximal.

Quel danger représente-t-elle à l'instant présent ?

- Une fois la base du calcul posée, le calculateur propose une deuxième série de critères, qui va permettre de pondérer le score que nous venons d'obtenir avec un « score temporel ». Il faut répondre à trois questions :
- Où en est le développement d'un code pour exploiter la vulnérabilité ?
- Où en est le développement d'un patch pour réparer la vulnérabilité ? Existe-t-il des contre-mesures ?
- À quel point les chercheurs sont-ils sûrs que la vulnérabilité existe telle que décrite ?

Comment s'applique-t-elle à un cas de figure particulier ?

- Une troisième série de critères permet de faire émerger un « score environnemental ».
- Il pondère la dangerosité de la faille en fonction des particularités de l'organisation concernée. L'évaluateur est invité à annoter chacun des critères du score de base pour qu'ils correspondent plus correctement au fonctionnement réel, et non théorique du logiciel concerné.

Les limites du score CVSS

- Les critères manquent de parfois de précision : chaque question est limitée entre 2 et 4 réponses. Ces cases prédéfinies facilitent le calcul, mais elles réduisent sa précision. À cause de ces arrondis, une différence inférieure à deux points entre deux scores n'est pas forcément significative.

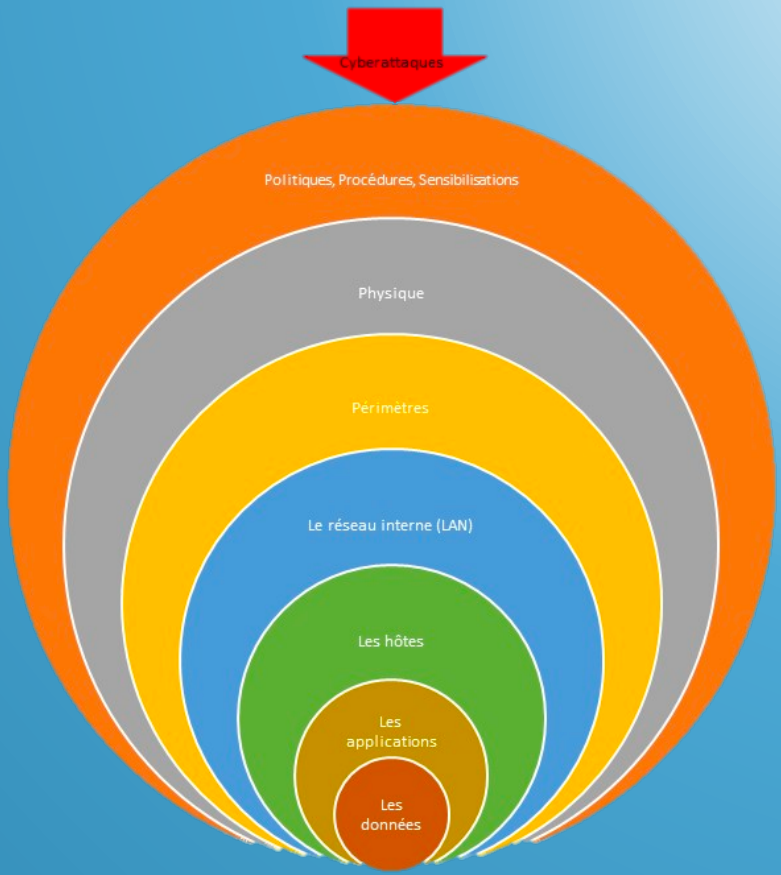
- Un score soumis à interprétation : deux évaluateurs d'une vulnérabilité ne trouveront pas forcément le même score CVSS, puisque les critères laissent une marge d'interprétation. Le désaccord sur un score est d'ailleurs situation commune dans le milieu du bug bounty. Des chercheurs présentent des vulnérabilités aux entreprises, qui vont discuter avec eux de la sévérité de la faille.

Défense en profondeur

La défense en profondeur

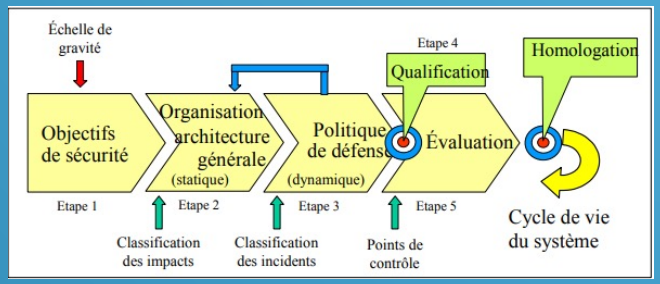
Le principe de la défense en profondeur est la mise en place de plusieurs barrières indépendantes.

L'objectif est d'augmenter nos chances de détection d'un intrus et de réduire ses chances de succès.



Défense en profondeur

- La méthode de défense en profondeur en 4 étapes :
  - Détermination des biens des objectifs de sécurité
  - Élaboration de l'organisation et de l'architecture générale du système (la profondeur du dispositif
  - Élaboration de la politique de défense qui comprend deux volets : le premier organise le renseignement et le second la défense réactive correspondante (interaction, planification)
  - La cohérence globale du système

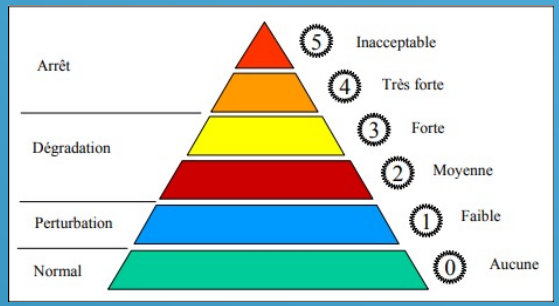


ANDN SERVICES

Défense en profondeur

- **Première étape : détermination des biens et des objectifs de sécurité**
  - Acteur identifié
  - Besoin identifié
  - Analyses des risques
- Chaque élément est lié à l'échelle de gravité ci-dessous (type Echelle INES : International Nuclear Event Scale)

Catégorie	Niveau	Gravité	Critère
Arrêt	5	Inacceptable	L'événement met en cause la survie de l'entreprise (le fait redouté est arrivé).
	4	Très forte	L'événement présente un risque très important et nécessite donc des mesures d'urgence immédiates.
Dégradation	3	Forte	L'événement n'entraîne pas de risque important mais une partie significative du système a été touchée.
	2	Moyenne	L'événement a une conséquence sur le fonctionnement normal et doit entraîner une réaction immédiate.
Perturbation	1	Faible	L'événement n'a pas de conséquences notables mais doit être traité pour rétablir un fonctionnement normal.
Fonctionnement normal	0	Aucune importance du point de vue de la sécurité	Fonctionnement normal.



Défense en profondeur

- **Deuxième étape : Élaboration de l'organisation et de l'architecture générale du système**

- On identifie les points suivants :

  - découpage des zones en fonction des risques, des acteurs, des grandes fonctions de l'entreprise
  - détermination des barrières (moyen technique, procédural et humain)
  - classification des zones en fonction de leur sensibilité et détermination des règles de passage de l'une à l'autre
  - découpage des zones en domaines de confiance : introduction des cloisonnements organisationnels en général (la profondeur de l'organisation)
  - répartition privé/commun dans chaque domaine et entre domaines.

Défense en profondeur

- **Troisième étape : Élaboration de la politique de défense**
  - Détermination de la défense globale et coordonnée
    - détection (détermination des points de contrôle et de détection des attaques)
    - remontée de l'information
    - corrélation des événements
    - alerte
- Planification
  - détermination des reconfigurations possibles (normal ou dégradé)
  - plans de réaction ou bien de continuité

Défense en profondeur

- Défense globale (trois axes) :
  - Organisationnel
  - Mise en œuvre
  - Technologique

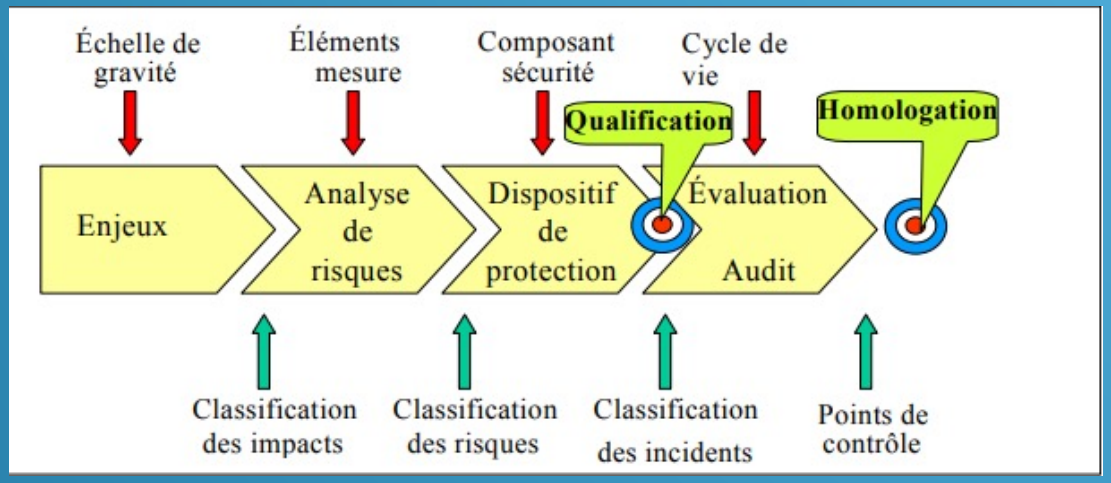
- La politique de défense doit déterminer pour les différents incidents de sécurité leur gravité afin de bénéficier de l'apport "pédagogique" de la méthode permettant une meilleure sensibilisation des personnels.

Défense en profondeur

- **Quatrième étape : La cohérence globale du système**
  - Il s'agit de conduire la qualification (Autrement dit : validé l'organisation mis en place lors des étapes précédentes) à travers deux mécanismes :
  - L'approche qualitative
  - L'approche démonstrative

Défense en profondeur

- **Quatrième étape : La cohérence globale du système**
  - Approche qualitative :
    - vise à vérifier le respect des principes de la défense en profondeur définit précédemment
    - vérifie aussi le respect de la méthode telle que mise en place dans la société



ANDN SERVICES

Défense en profondeur

- **Quatrième étape : La cohérence globale du système**
- L'approche démonstrative
  - Etape 1 : Permet de classer les impacts potentiels de la menace, et détermine les éléments pour les classifier
  - Etape 2 : architecture du système, a comme résultat un classement des incidents de sécurité en fonction des composants défaillants.
  - Mise en évidences des points de contrôle et du bon fonctionnement des moyens de détections

Défense en profondeur

- La méthode de qualification de défense en profondeur utilise donc deux méthodes démonstratives d'analyse qui sont :
  - l'analyse par scénario « enveloppe »
    - cette analyse consiste à établir un scénario couvrant le risque maximum
    - donc inclus forcément tout les autres scenarii possible
  - l'analyse par « composant défaillant »
    - il s'agit de postuler un incident de sécurité et une défaillance aléatoire d'un autre composant situé entre l'incident et l'événement redouté pour analyser la protection restante et vérifier qu'elle est suffisante.

Défense en profondeur

- **Il y a une 5ème étape dont nous n'avons pas parler :**
  - **L'amélioration continu :**
  - **Retour d'expérience**
  - **Étude statistique**
  - **Audit périodique**
  - **Tableau de bord**

Les méthondes de gestion de risques
ISO 27005, EBIOS RM

Qu'est-ce qu' « un risque » ?

- Un risque est la possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actif ou un groupe d'actifs et nuise à l'organisation

  ISO 27005 : Le risque est mesuré en termes de combinaison entre la vraisemblance d'un évènement et ses conséquences.

RISQUE = Menaces x Vulnérabilités x Impacts

Qu’est-ce qu’ « une menace » ?

- ISO 27001 :
  Une menace – threat – est une cause pouvant affecter la sécurité d’un actif –asset.

- La menace est le facteur le plus difficile à évaluer.
  Elle est évolutive dans le temps et dans l’espace et on peut la quantifiée qu’au moment où elle se produit.
- Sous-estimer une menace peut entraîner des risques inconsidérés.
- Surestimer une menace peut entraîner un risque de blocage de la production.
- Il est donc primordiale de l’estimer au mieux.

Qu'est-ce qu' « une vulnérabilité » ?

- Une vulnérabilité ou faille est la faiblesse qui permet à un attaquant de porter atteinte à l'intégrité du système informatique.

- Les vulnérabilités sont d'origines multiples:
  - Techniques
  - Opérationnelles
  - Physiques
  - Humaines

Qu’est-ce qu’ « un impact » ?

- L’impact représente la conséquence du risque sur l’organisme
- Sur les missions
- Sur la sécurité des personnes
- Financiers
- Juridiques
- Sur l’image de l’entreprise
- Sur les tiers

Les méthodes d'analyse de risques

- Il existe des méthodes normalisées pour les Analyses de Risques :
- EBIOS – Expression des Besoins et Identifications des Objectifs de Sécurité
- MEHARI – Méthode Harmonisée d'analyse des Risques
- ISO 27005

EBIOS

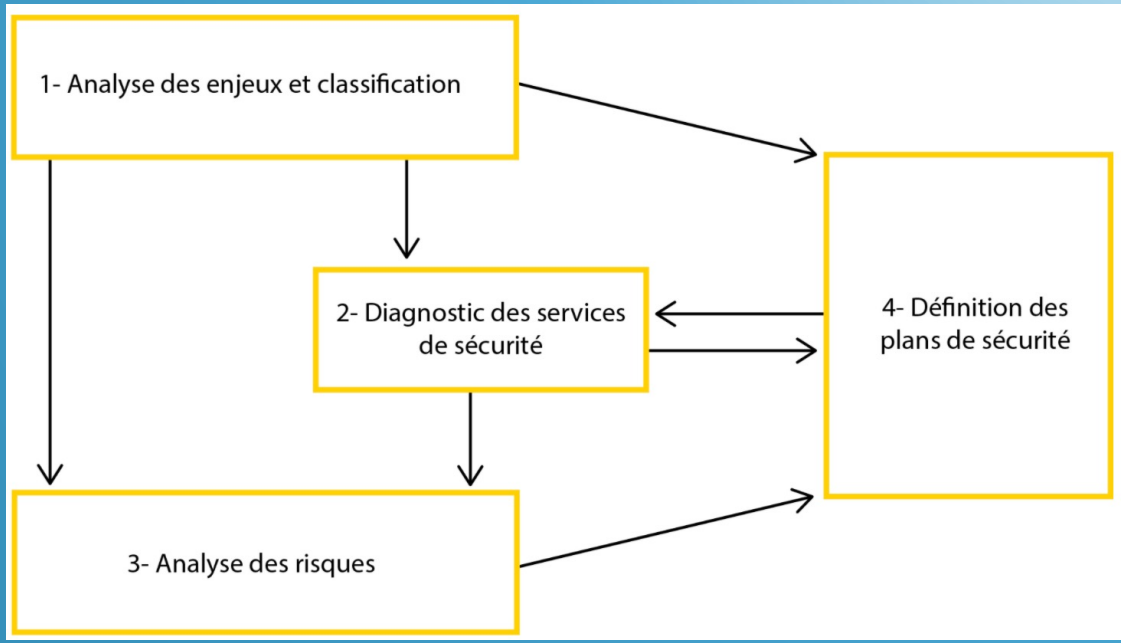
- EBIOS Risk Manager est la méthode de gestions des risques publiée par L'ANSSI avec le soutien du club EBIOS.
- C 'est une boite à outils adaptable selon l'objectif du projet.
- Elle permet de :
  - Mettre en place ou renforcer un processus de management du risque
  - Apprécier et traiter les risques relatifs à un projet numérique
  - Définir le niveau de sécurité à atteindre pour un produit ou un service
- Elle s'applique à toutes les entreprises, peu importe leur taille. Que le SI soit déjà présent ou non.

MEHARI

MEHARI est la méthode de gestions des risques publiée par le CLUSIF.

C 'est un ensemble de bases de connaissance permettant une analyse précise de situations de risque.

Elle se base sur les enjeux métiers pour définir des diagnostiques des services de sécurités et réalisés son analyse de risque.



ISO 27005

- C'est une norme dédiée à la gestion des risques. Ce n'est pas une méthode d'analyse de risques mais un guide.
- Elle pose les bases de la gestion des risques :

1. Etablissement du contexte
2. Identification des risques
3. Estimation des risques
4. Evaluation du risqué
5. Traitement du risque
6. Acceptation du risque
7. Activités transverse : communication et surveillance

Les normes ISO 27000X

Qu’est-ce que la famille ISO 27000

- L’ISO est une Organisation Internationale qui participe à l’élaboration de Standard.
- La famille ISO 27000 permet d’organiser et structurer la démarche de la gestion de la sécurité des SI.

Qu'est-ce que la famille ISO 27000

- ISO 27001 : processus permettant le management de la sécurité de l'information – SMSI
- ISO 27002 : catalogue de bonnes pratiques de sécurité
- ISO 27003 : différentes phases initiales à accomplir afin de respecter la norme ISO 27001
- ISO 27004 : définit les contrôles de fonctionnement du SMSI
- ISO 27005 : décrit les processus de la gestion des risques
- ISO 27006 : décrit les exigences relatives aux organismes qui auditent et certifient les SMSI des sociétés.

Mettre en place une solution de SIEM

- **SIEM**
  - Security Information and Event Management
- C'est Système de Collecte et de Centralisation des log en temps réel
- Les membres de l'équipe SOC traitent ces logs à l'aide d'outils et de machine learning de manière automatiser la détection de comportement anormal et de repérer chaque potentiel attaque.

Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?

- **Le scénario du SOC interne**
- **Les avantages :**
  - Une équipe interne dédiée avec une forte réactivité :
    - un SOC interne présente l'avantage de bénéficier d'employés dédiés qui connaissent très bien l'écosystème de l'entreprise et ses enjeux.
    - cette maîtrise permet souvent une forte réactivité dans la résolution des problèmes de sécurité.

- Les journaux d'événements et tous les éléments de suivi des alarmes et incidents sont stockés en internes.
- Voilà qui réduit un éventuel risque lié au transfert de données en externe.

- La communication en cas d'attaque est souvent plus rapide car elle utilise les moyens de communication propres à l'entreprise.
- Les solutions mises en place sont fortement personnalisées pour coller aux besoins de l'entreprise.

Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?

- **Le scénario du SOC interne**
- **Avoir un SOC interne requiert la gestion permanente de plusieurs éléments :**

- **Le recrutement des compétences et la formation :**
  - un SOC nécessite de disposer d'experts sur chacun des périmètres adressés.
  - aujourd'hui le recrutement d'analystes SOC et d'experts en cybersécurité est un véritable défi et peut prendre un certain temps.
  - Enfin, le maintien et la montée en compétences de ces experts sur les nouvelles technologies, normes ou processus requiert du temps et un budget non négligeable.

- **La montée en maturité :**
  - les ressources internes n'étant sollicitées que par l'écosystème interne, le processus pour disposer d'un SOC vraiment opérationnel est assez long.
  - à titre d'exemple la mise en place du SOC Michelin aura mis plus de 4 ans pour atteindre sa phase de maturité.

Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?

- **La portée de l'expertise métier :**
  - gérer l'inconnu est le paradoxe le plus compliqué en termes de pilotage de risques.
  - il peut être plus difficile en interne de découvrir des menaces qui seront plus évidentes pour une entreprise spécialisée dans l'identification des comportements malveillants.
  - un SOC interne aura besoin d'une première confrontation avec une menace nouvelle pour bien la traiter ultérieurement.
- **La documentation des processus internes est bien souvent oubliée :**
  - la connaissance repose souvent sur un nombre restreint d'experts devenant ainsi indispensables.
  - à la clé, sans surprise, un facteur de risque de perte de connaissance en cas de départ.
- **Visibilité budgétaire consolidée des dépenses :**
  - la mise en place d'un SOC interne implique un investissement initial important avec des dépenses associées qui restent difficile à recouper.

Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?

- **Le scénario du SOC externe**

- **Les avantages :**
  - opter pour le SOC externe via un tiers représente une excellente alternative pour faciliter une mise en place à un coût maitrisé. Avec des avantages multiples :

- **Obtenir et justifier d'un budget par le top management**
  - choisir un SOC externe apporte de la transparence et simplifie la promotion d'un projet de SOC au sein de l'entreprise.
  - en effet, un projet de SOC externalisé passe généralement par un processus d'appel d'offre et la validation d'un budget au niveau de la direction.

- **Améliorer l'image et la communication**
  - disposer d'un SOC externe permet de réassurer le top management.
  - la perception associée au recours à un expert externe est souvent meilleure que celle issue d'un SOC réalisé en interne.
  - en outre, la vulgarisation des éléments techniques est facilitée au profit d'une meilleure compréhension des enjeux et besoins par la direction.
  - et aussi du RSSI mieux positionné pour expliquer sa valeur et démontrer un retour sur investissement.

Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?

- **Disposer de compétences en cybersécurité**
  - Dans ce modèle, des personnes compétentes et opérationnelles sont mises à disposition immédiatement sans avoir à attendre de longs processus de recrutement.
  - C'est aussi un moyen de bénéficier de l'expérience d'analystes qui ont surveillé d'autres environnements et qui suivent généralement des processus éprouvés.

- **Facilité de mise en œuvre**
  - D'après une étude réalisée par PWC, les DSI et CISO privilégient ce type de SOC car ils ont conscience de la complexité de sa mise en œuvre d'un tel dispositif :
    - mise en place de nombreux outils, recherche d'experts dans le domaine, maitrise des outils, analyse des incidents, forensic.

- **Des niveaux de services élevés**
  - Organisé et mature, ce type de SOC offre également l'avantage de proposer des niveaux de services élevés (ex : 24/7).
  - De plus, avec le SLA (Service Level Agreement), l'ensemble de la prestation est cadré et précis, épargnant à l'entreprise les mauvaises surprises, notamment lors d'attaques.

Mettre en place une solution de SIEM

- **Accès à une « Threat intelligence »**
  - Une « threat intelligence » représente un service de renseignement sur les menaces.
  - Cette veille sur les menaces et incidents est très difficile à réaliser seul.
  - Un opérateur de SOC est bien placé pour consolider de nombreuses sources de renseignement, externes et internes, pour y parvenir.

- **Des coûts réduits**
  - Enfin un SOC externe coûte nettement moins cher car le matériel, les solutions et les experts sont pour la plupart mutualisés.
  - Pour une surveillance et analyse 24/7 via un SOC externalisé, il faut compter un budget entre 300k€ à 700k€ alors qu'une internalisation du SOC coûte entre 1 000k€ et 2 000k€ - ce qui inclut le développement et le maintien de la plateforme mais pas les coûts technologiques.
  - Ajoutons qu'il s'agit là d'une dépense d'exploitation (OPEX) et non d'infrastructure, une dépense donc plus facile à intégrer dans le budget.

Mettre en place une solution de SIEM

- **Les challenges :**
- Le SOC externe requiert une gestion permanente des éléments suivants :
  - Des experts en externes :
    - bien qu'expérimentés, les personnes dédiées ne peuvent connaitre aussi bien l'infrastructure de l'organisation et leurs compétences sont souvent mutualisées.
    - dans ce contexte, le partenaire doit prendre le temps de bien comprendre les problématiques métier de l'organisation et mettre en place des procédures impliquant des personnes internes et externes.
- Données stockées et analysées en dehors du périmètre de l'entreprise :
  - externaliser des données, disposer d'éléments en dehors de l'entreprise peut être synonyme de risques si les mesures de sécurité n'ont pas été mises en œuvre.
- La réversibilité peut s'avérer complexe notamment si le prestataire s'appuie sur des solutions propriétaires.
- Toutefois, même avec des solutions du marché et une documentation claire, l'interopérabilité reste limitée et la reprise de compétences sur les règles de détection et les procédures en place peut en pâtir.
- Un changement de mentalité requis :
  - accepter le traitement de la sécurité par des tiers n'est pas forcément naturel et demande une conduite du changement.

Mettre en place une solution de SIEM

SOC	Avantages	Inconvénients
Interne	• Bonne connaissance de l'entreprise • Toutes les données sont stockées et traitées en interne • Une communication et une corrélation plus facile des événements entre chaque département	• Coût élevé pour déployer et le MCO (maintien en condition opérationnel) • Budget difficile à obtenir et à justifier • Difficulté à trouver des experts • Montée en maturité très lente • Manque de documentation sur les processus internes • Risque de conflit d'intérêts entre les services
Externe	• Coûts plus abordable et maitrisé • Budget plus simple à définir et à justifier auprès du top management • Mise à disposition d'experts • Évolutivité et flexibilité • Mise à disposition des dernières tendances et expériences tirés d'autres clients • Accès aux « Threat Intelligence » • Pas de conflit d'intérêt avec les autres départements (conseil externe et reporting) • Accès immédiat à un SOC mature.	• Données stockées et traitées en dehors du périmètre de l'entreprise • Manque de personnes dédiées à l'environnement / à l'entreprise • Réversibilité délicate • Changement de mentalité au sein de l'organisation

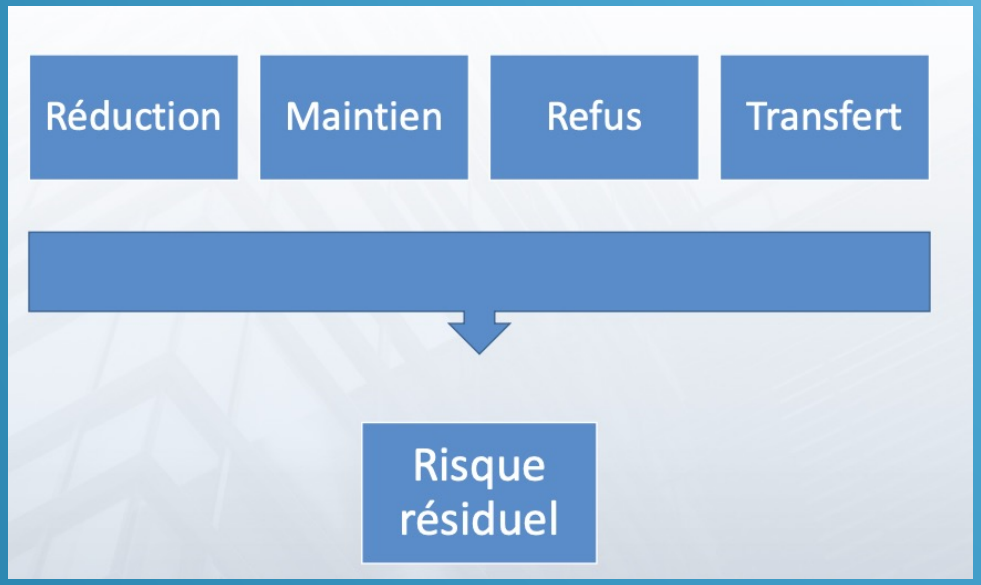
La gestion du risque

Définition du risque

- Un risque est la vraisemblance qu'une menace exploite une vulnérabilité afin d'impacter un actif.
- RISQUE = MENACE x VULNERABILITES x VRAISEMBLANCE x IMPACT
- Un risque se formule sous forme de scénario afin qu'il soit compréhensible du management.
- L'exécution du scénario de risque amène à une conséquence pour le propriétaire de l'actif.

Traitement du risque

- Il y a quatre options de traitement de risque



Risque résiduel

- Un risque résiduel est un risque qui persiste après un traitement du risque.
- S'il n'est pas acceptable, vous devez repartir dans un cycle d'évaluation et de traitement jusqu'à ce que le niveau de ce risque devienne acceptable.

Risque induit

- Un risque induit est un risque introduit suite à la mise en œuvre d'une mesure de sécurité

Espérance de perte unique

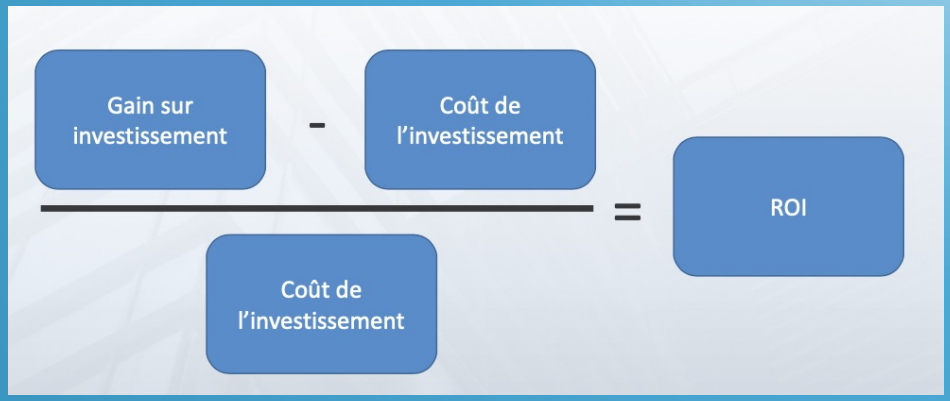
- Espérance de Perte Unique (EPU) : Correspond à une perte suite à un évènement unitaire
- La Valeur de l'Actif (VA) x Facteur d'Exposition (FE) = Espérance de Perte Unique (EPU)
- Exemple : 60% du chiffre d'affaire journalier est impacté en cas d'attaque sur les services web e-commerce de l'entreprise.
  - La valeur du chiffre d'affaire journalier est de 100 000 €
  - 60% correspond au Facteur d'Exposition
  - Chiffre d'affaire journalier x Facteur d'Exposition = 100 000 € x 0,6 = 60 000 €
  - Espérance de Perte Unique = 60 000 €
- Terme anglophone : Single Loss Expectancy (SLE)

Espérance de perte annuelle

- Espérance de Perte Annuelle (EPA) : Correspond à la perte sur un an
- Espérance de Perte Unique (EPU) x Taux d'Occurrence Annuel (TOA) = Espérance de Perte Annuelle (EPA)
- Exemple : 60% du chiffre d'affaire journalier est impacté en cas d'attaque sur les services web e-commerce de l'entreprise. L' évènement se produit 1 journée par trimestre.
  - Chiffre d'affaire journalier = 100 000 €
  - Espérance de Perte Unique = 60 000 €
  - Taux d'Occurrence Annuel : 4
  - Espérance de Perte Unique x Taux d'Occurrence Annuel = 60 000 € x 4 = **240 000 €**
  - Espérance de Perte Annuelle = **240 000 €**
- Terme anglophone : Annualized Loss Expectancy (ALE)

Return of investment (ROI)

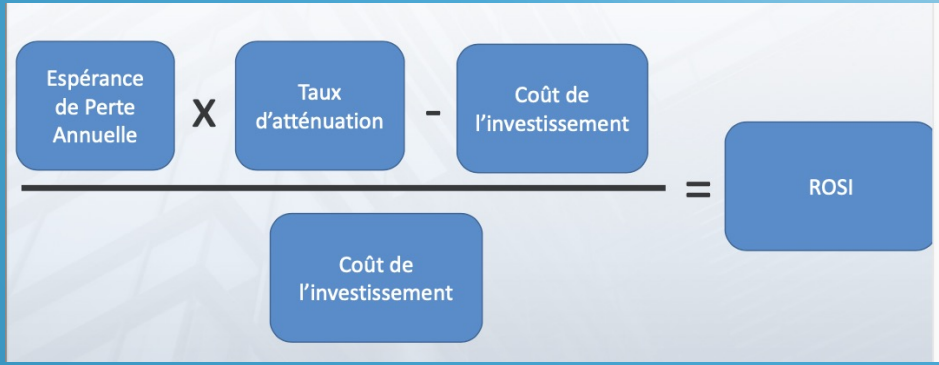
- Retour sur investissement
- Terme Anglophone: Return Of Investment (ROI)



ANDN SERVICES

Return of security investment (ROSI)

- Retour sur l'investissement sécurité
- Taux d'atténuation: Capacité de la solution à atténuer la perte annuelle
- Terme Anglophone: Return Of Security Investment (ROSI)



Return of security investment (ROSI)

- Hypothèse: Scénario solution Anti-DDOS
- 1 incident par mois
- Espérance de Perte Unique (EPU) = 20 000€
- Taux d'Atténuation (TA): La solution sélectionnée bloque 80% des attaques DDOS
- Le coût de la solution est de 50 000€ par an

Return of security investment (ROSI)

- ROSI = ((Espérance de Perte Annuel x Taux d'atténuation) – Coût de l'investissement)/ Coût de l'investissement
- ROSI = (((Espérance de Perte Unique x Taux d'Occurrence Annuel) x Taux d'atténuation) – Coût de l'investissement) / Coût de l'investissement
- ROSI = ((20 000 € x 12) x 0,8) – 50 000 €) / 50 000 € = 2,84
- L'investissement réalisé est de 50 000 € et permet d'économiser142 000 € par an.
- On ne parle pas de gain mais d'économie réalisée

Return of security investment (ROSI)

- Exemple: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment

Des questions ?