Cybersécu

Notions générales:

- Principes de Peter: Selon ce principe, « dans une hiérarchie, tout employé a tendance à s'élever à son niveau d'incompétence », avec pour corollaire que « avec le temps, tout poste sera occupé par un employé incapable d'en assumer la responsabilité »
- KISS: Keep It Simple, Stupid → ligne directrice de conception qui préconise la simplicité dans la conception et que toute complexité non indispensable devrait être évitée dans toute la mesure du possible
- SMART: Specific, Measurable, Achievable, Relevant and Time-bound, en français spécifique, mesurable, atteignable, réaliste et temporellement défini
- Fast-Good-Cheap: cout qualité délais. Il n'est pas possible de faire vite, bien, et pas cher. Seulement deux objectifs peuvent être atteints.
- Matrice d'Einshower: Outil de priorisation des tâches selon important/pas important, urgent/pas urgent: A faire, A planifier, A déléguer, A abandonner
- Loi de Pareto: encore loi des 80-20, est une observation selon laquelle environ 80 % des effets sont le produit de seulement 20 % des causes
- Rationalité limitée: idée selon laquelle la capacité de décision d'un individu est altérée par un ensemble de contraintes comme le manque d'information, des biais cognitifs ou encore le manque de temps.

Lexique:

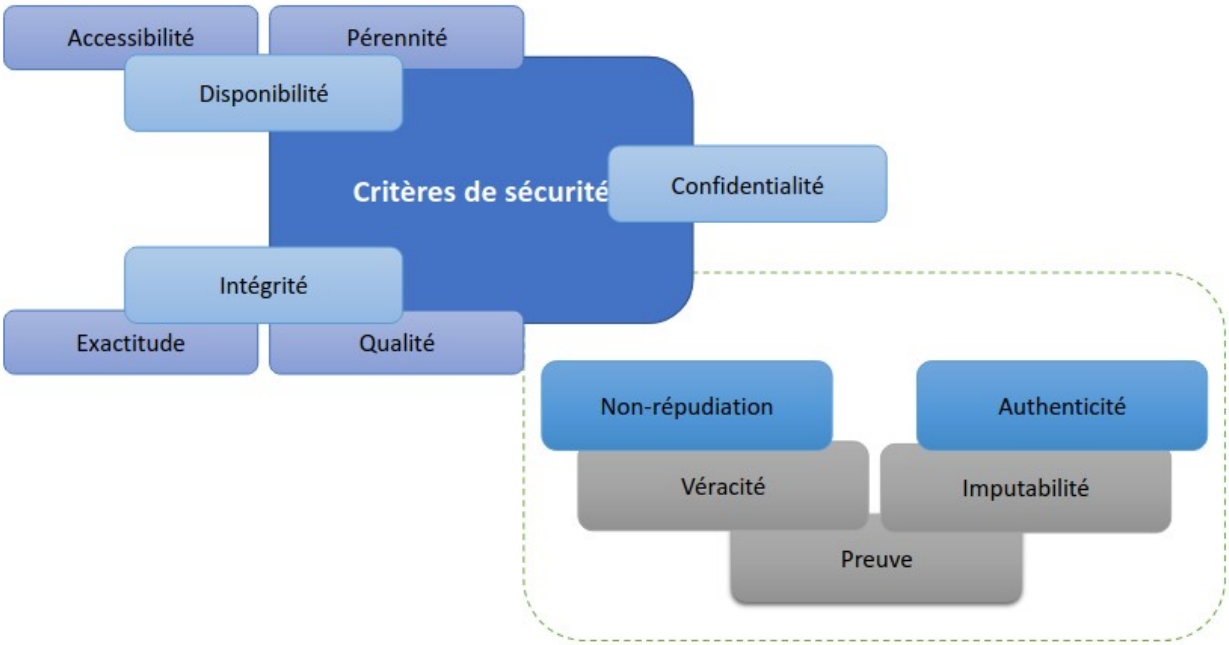
DIC → Disponibilité, Intégrité, Confidentialité
CNIL → Commission nationale de l'informatique et des libertés
RGPD → Règlement Général sur la Protection des Données
ANSSI → Agence Nationale de la Sécurité des Systèmes d'Information
DPO → Data Protection Officer, délégué à la protection des données
RSSI → Responsable sécurité des systèmes d'information
PSSI → Politique de sécurité des systèmes d'information
CTI → Cyber Threat Intelligence, activité liée à la collecte d'informations sur les menaces ou les acteurs de la menace
DPI → Droit de Propriété Intellectuelle
LIO → Lutte Informatique Offensive
LID → Lutte Informatique Défensive
L2I → Lutte Informatique d’Influence
LPM → Loi de Protection Militaire
SMSI → Système de Management de la Sécurité de l'Information
SSI → Sécurité des Systèmes d'Information
PTR → Plan de Traitement du Risque
TI → Technologies de l'information
SSIV → Système d'Information d'Importance Vitale
GSI → Gouvernance de la sécurité de l’information, processus par lequel la sécurité informationnelle est traitée au niveau exécutif et s’appuie sur la sécurité des technologies qui l’appréhendent
IRT → Incident response team
SOC → Security Operation Center, plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

CERT → Computer Emergency Response Team, équipe spécialisée en cybersécurité dédiée à la gestion des incidents de sécurité informatique pour prévenir, détecter et répondre aux cyberattaques visant les institutions d'un État, les grandes industries.
SIEM → Security Information Event Manager, gestionnaire de log en masse.
HFDS → Haut Fonctionnaire de Défense et de Sécurité
PSI → Plan de Secours Informatique
PCA → Plan de Continuité d'Activité
IOC → Indicators of Compromise, indices et des preuves d'une fuite de données
IOA → Indicators of Attack, indices pour déterminer si une attaque est en cours et doit être contenue
IOE → Indicator of Exposure, faiblesses de sécurité propres à un réseau exploitables par un attaquant.
TLP → Traffic Light Protocol, marquage pour la diffusion des informations
PAP -> Permissible Actions Protocol, marquage pour l'utilisation des informations
OSINT → Open-Source Intelligence, désigne l'ensemble des techniques et méthodes utilisées pour collecter et analyser des informations disponibles publiquement

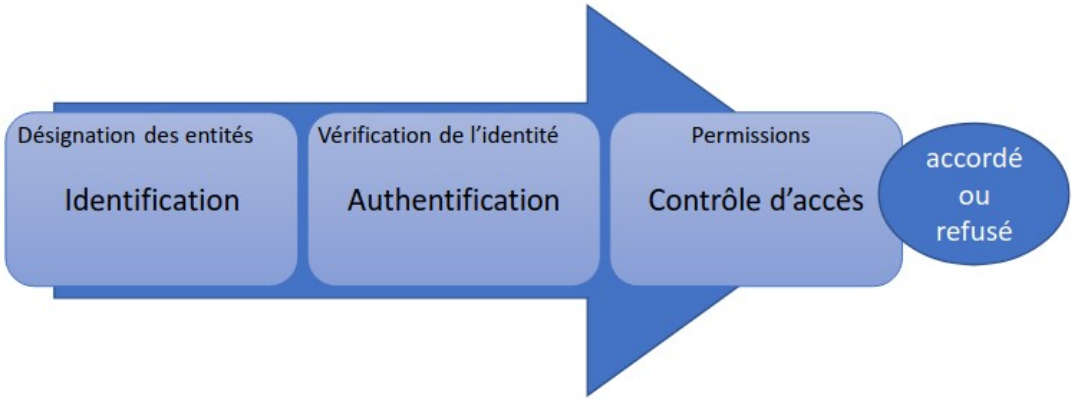
Séance 1:

Ecosystème:

Critères de base des objectifs de sécurité (DIC) → Disponibilité, Intégrité, Confidentialité



Non-répudiation → fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu

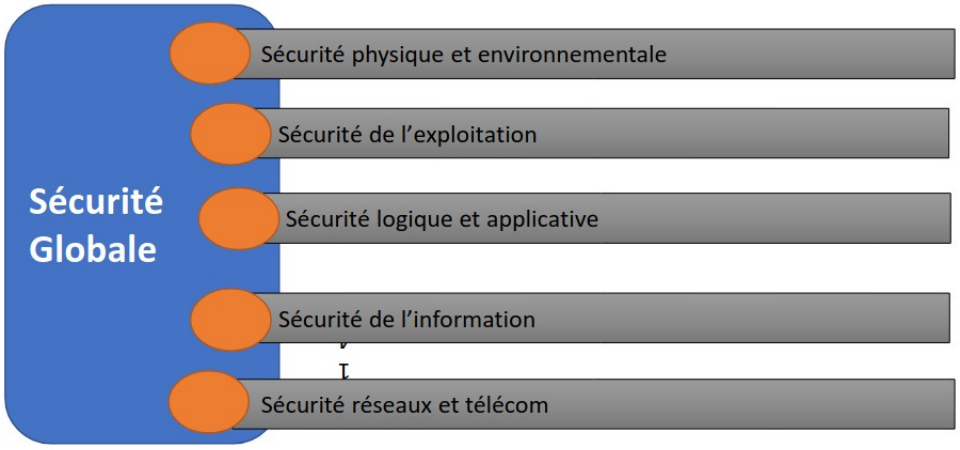


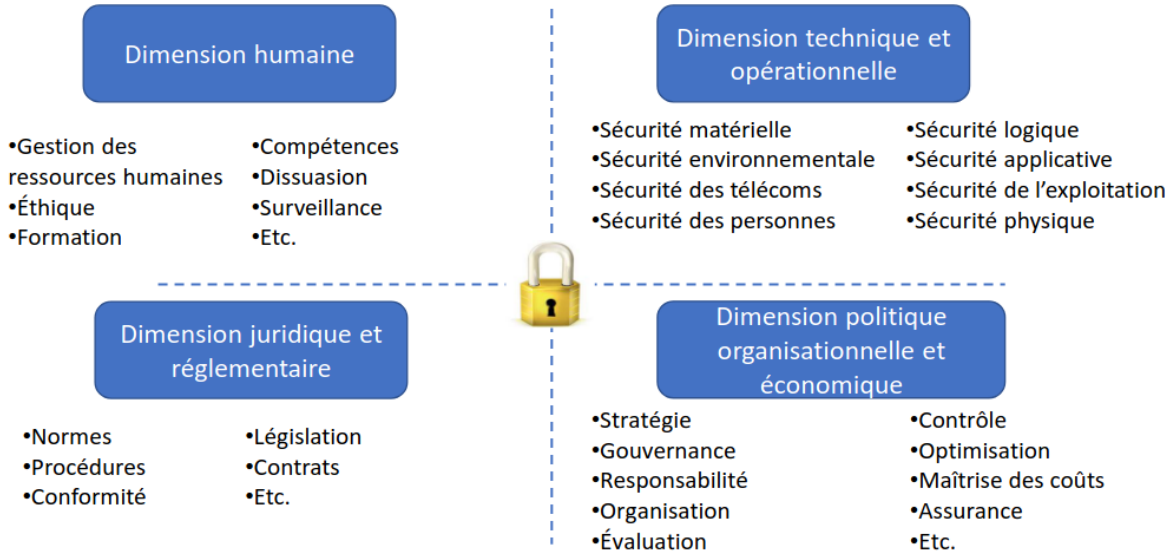
Cyberespace → Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. (autre nom d'internet)

Cybersécurité → État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une

cyberdéfense.
Cyberdéfense → Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

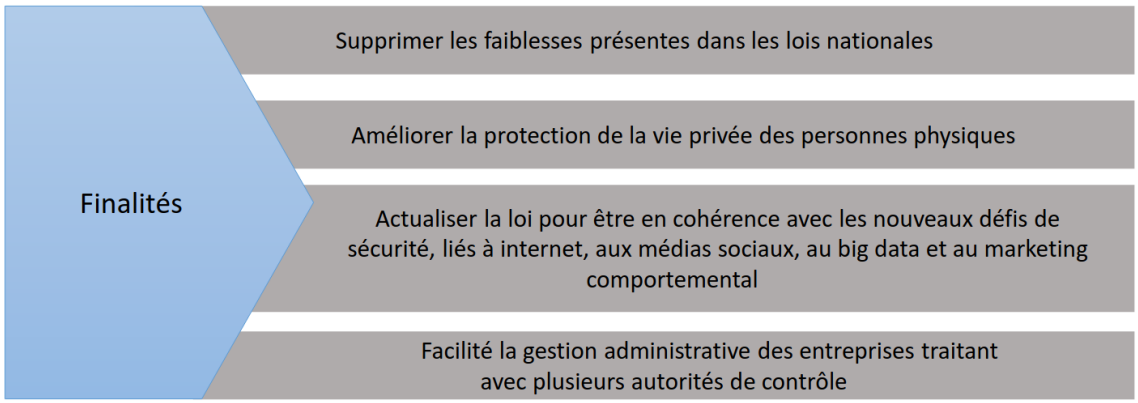
Sécurité informatique d'une entreprise assurée par une politique de sécurité, motivation et formation du personnel, mise en place de mesures proactives et réactive, mesure de sécurité par les axes managériaux, juridiques et techniques





Identité numérique:

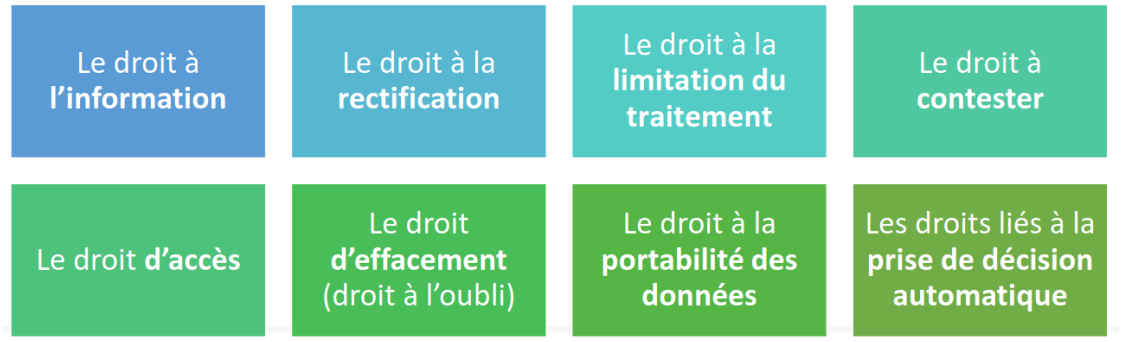
Les rares textes législatifs ou réglementaires qui font référence à l'identité numérique ne traitent en définitive que de la notion de « données personnelles »
En France c'est la CNIL qui protège les données à caractère personnel
Ce n'est pas un droit constitutionnel
RGPD énumère des exigences précises concernant la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et à la libre circulation de ces données



Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Le RGPD a identifié six principes à appliquer lors de la collecte ou du traitement des données, mentionnés au chapitre II du RGPD :

Droits accordés par le RGPD aux personnes concernées :



Séance 2:

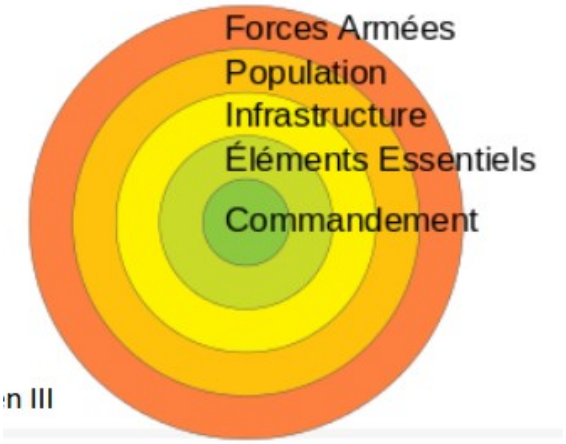
Intelligence économique, géopolitique

IE → Intelligence collective, maîtrise protection et exploitation de l'information
Cycle de l'information → détection, collecte, exploitation, diffusion. La veille englobe toutes ces étapes

Analyse PESTEL → politique, économique, sociologique, technologique, environnemental, légal. Groupes de forces macro-environnementales susceptibles d'influer sur les activités d'une organisation
Analyse SWOT → Strengths (forces), Weaknesses (faiblesses), Opportunities (opportunités), Threats (menaces). Positionne l'organisation dans son environnement global d'une manière plus dynamique
Cinq forces de Michael Porter → acteurs à surveiller parmi les concurrents directs, les nouveaux entrants, les fabricants de produits de substitution, les clients, les fournisseurs

Le niveau de protection de l'ensemble est égal à son élément le moins protégé.
Agir sur l'attitude et le comportement du public: La méthode employée pour façonner l'opinion se nomme «relations publiques».
Processus d'influence: identification des cibles → définition du message et identification des relais → choix du moment d'action → surveillance et ajustement

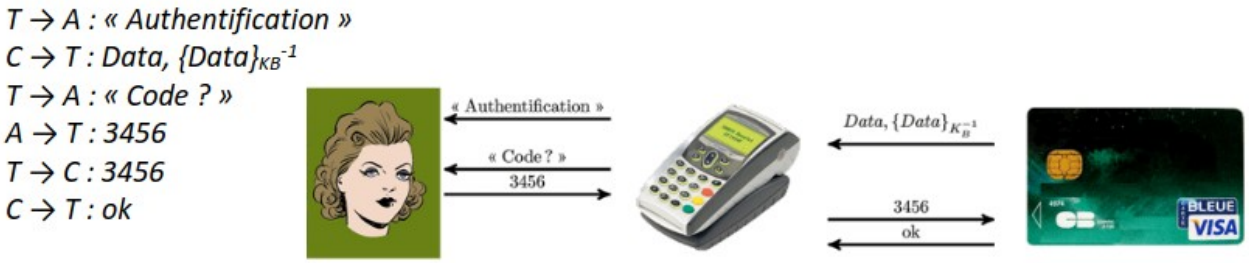
Théorie des cinq cercles de John A.Warden: le cyberespace lie les 5 cercles et donc les attaques cyber permettent d'atteindre la capacité à prendre des décisions sans action physique

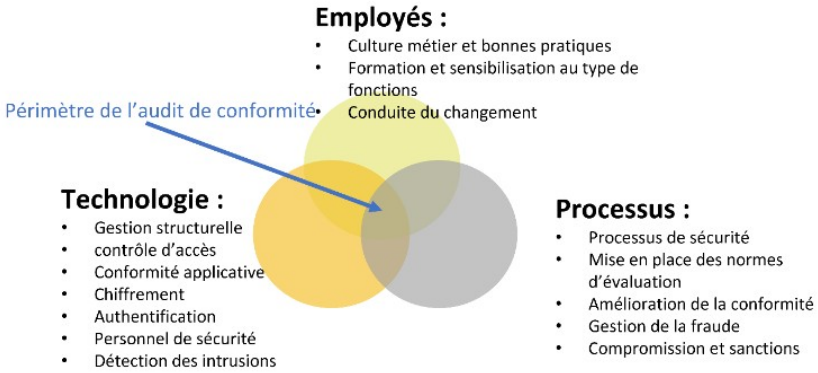


Obligations normatives, réglementaires et juridiques

NIS : Network and Information System Security. Répond aux enjeux: gouvernance, coopération, cybersécurité des OSE, cybersécurité de FSN
OSE → Opérateur de Service Essentiel
FSN → Fournisseur de Service Numérique
ENISA → Agence de l'union européenne pour la cybersécurité
OIV → Opérateurs d'Importance Vitale
Les OSE doivent garantir un socle minimal en termes de cybersécurité. Doit déclarer un responsable auprès de l'ANSSI, identifier ses systèmes d'informations essentiels, appliquer les

règles de sécurité dans les délais impartis, signaler les incidents, être soumis à des contrôles de sécurité
Les FSN doivent signaler les incidents et êtres soumis à des contrôles de sécurité
RGS → Référentiel Général de Sécurité fourni une méthodologie, des règles et bonnes pratiques
Entreprises, clauses de cybersécurité: engagements relatifs à la formation régulière du personnel en matière de sécurité des systèmes d'information, liste d'exigences techniques et engagement sur un niveau de sécurité précis (ex : respect de standards, normes, mise en œuvre de pratiques identifiées, etc.), règles de gestion et de notification des incidents (délais, coopération).
Clé de Luhn → En mathématiques et plus précisément en arithmétique modulaire, la formule de Luhn est utilisée pour ses applications en cryptologie. L'algorithme de Luhn, ou code de Luhn, ou encore formule de Luhn est aussi connu comme l'algorithme « modulo 10 » ou « mod 10 ». C'est une simple formule de somme de contrôle utilisée pour valider une variété de numéros de comptes, comme les numéros de cartes bancaires, les numéros d'assurance sociale canadiens, les numéros IMEI des téléphones mobiles ainsi que pour le calcul de validité d'un numéro SIRET.
PCI-DSS → La norme de sécurité des données de l'industrie des cartes de paiement



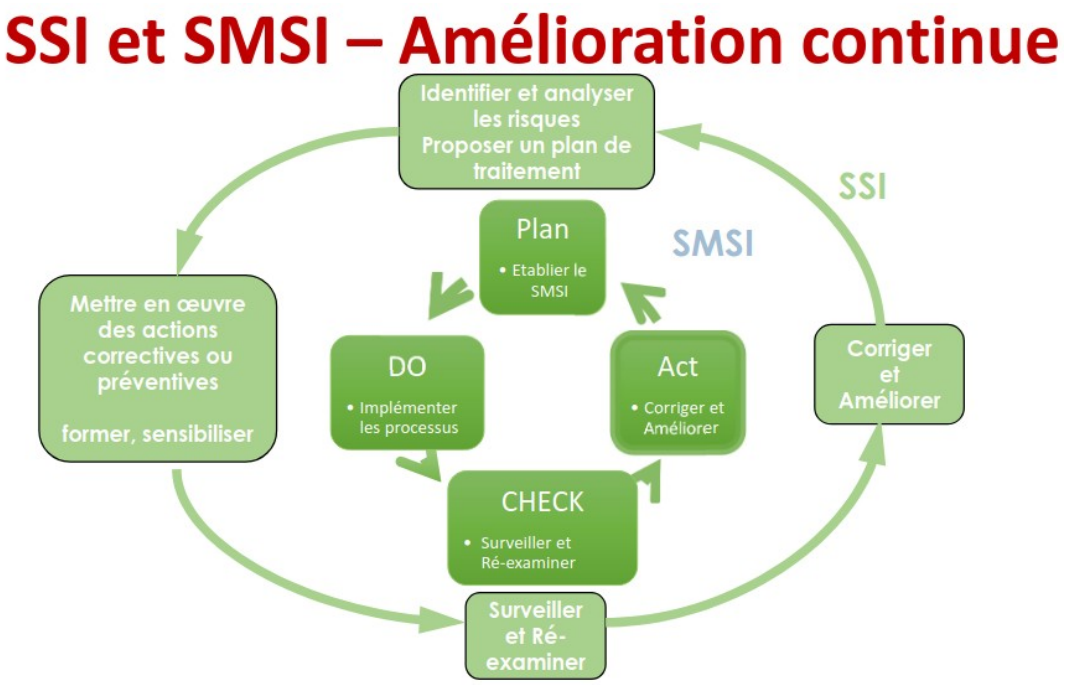


Référentiel de sécurité PCI-DSS

Séance 3:

Norme ISO 27000

Norme de sécurité de l'information
La sécurité est un processus
Les décisions doivent être prises au plus haut niveau
Norme ISO 27001 management de la sécurité et sécurité. Convient à toutes les organisations
PDCA → Modèle de gouvernance Plan → Do → Check → Act



27000 Vue d'ensemble et vocabulaire, 27001 exigences, 27002 code de bonne pratique pour la gestion de la sécurité de l'information, 27003 lignes directrices pour la mise en oeuvre du SMSI, 27004 management de la sécurité de l'information - mesurage, 27005 gestion des risques liés à la sécurité de l'information, 27006 audit de certification

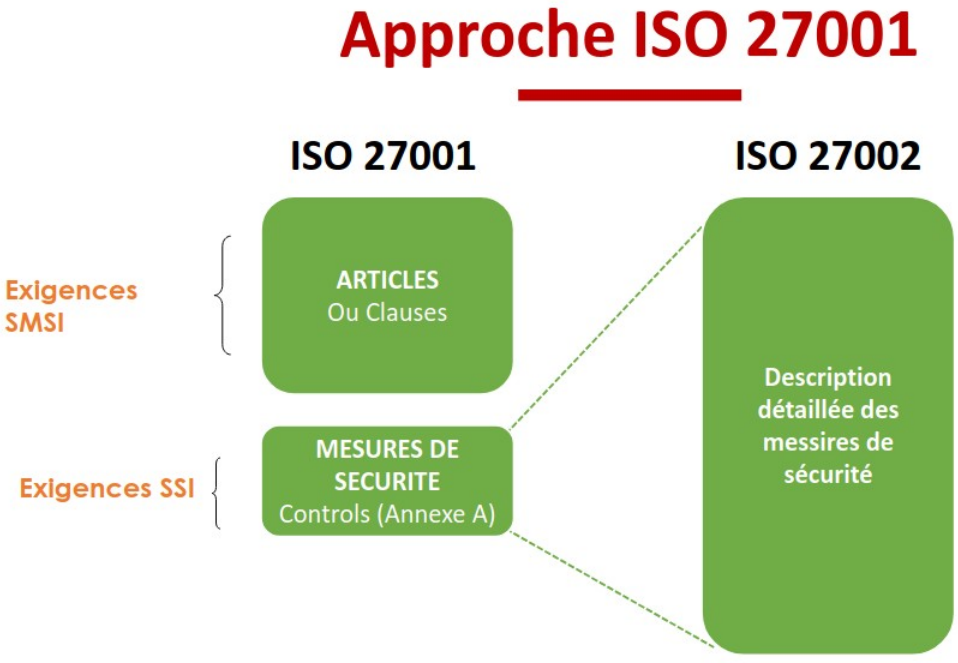
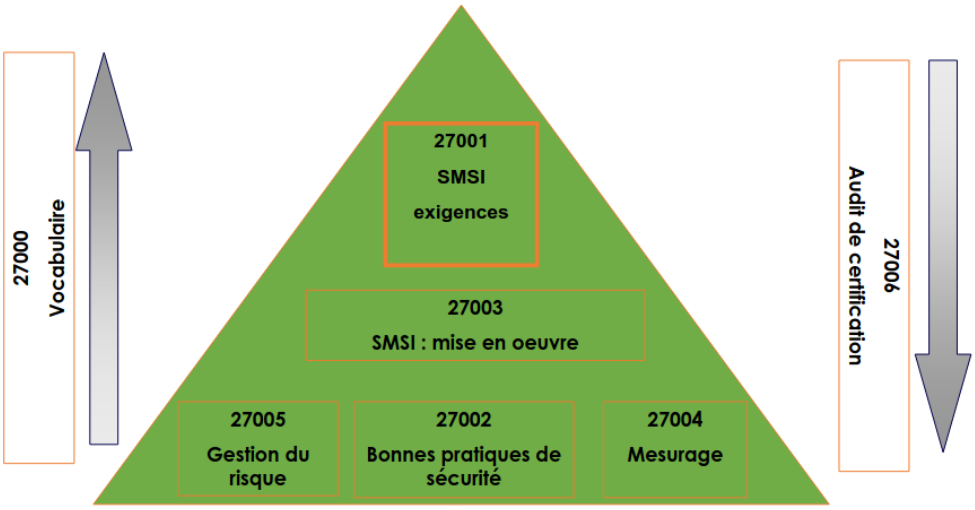
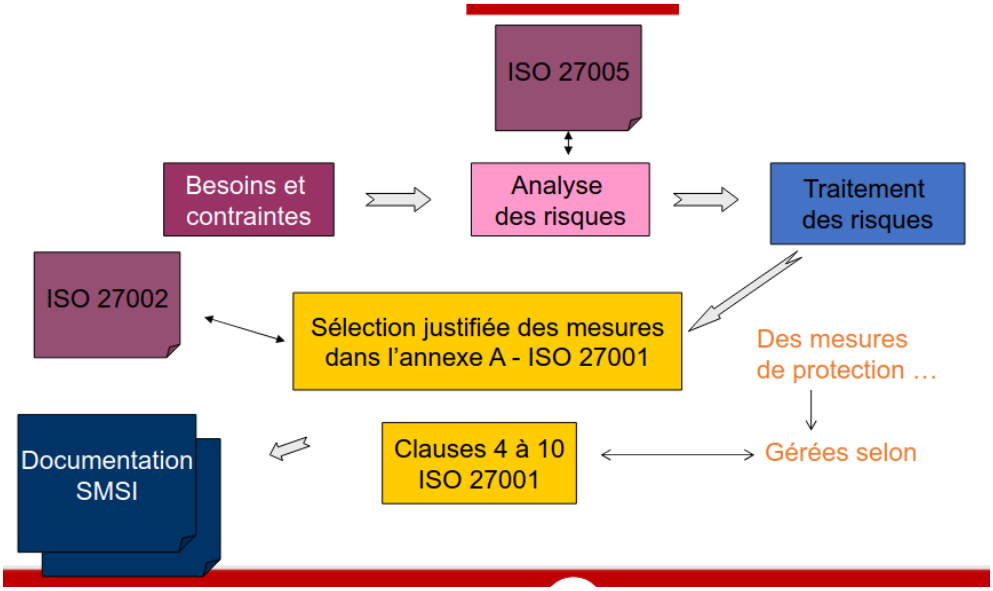


Schéma du positionnement des normes



Estimer le risque (probabilité, impact, gravité) et priorisation, les biens, les vulnérabilités, les actions déjà en place, les acteurs, ce qui est acceptable (acceptation). Evolution permanente donc veille permanente
Tableau de bord SSI permet d'avoir une vision synthétique technique et fonctionnelle aux niveaux décisionnels, de pilotage et opérationnels

Démarche globale 27001



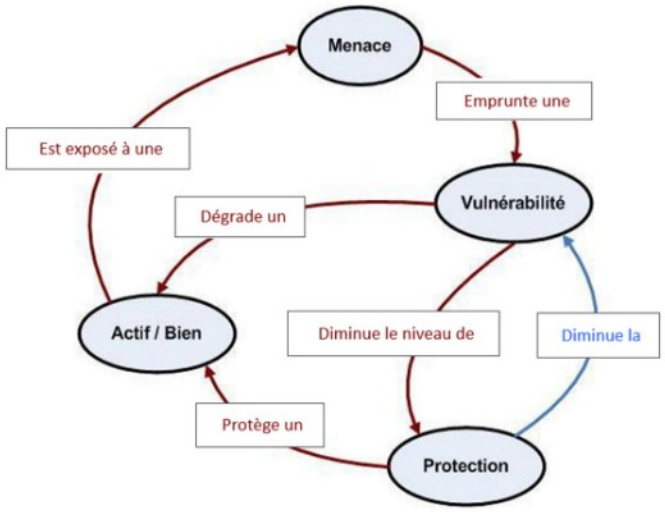
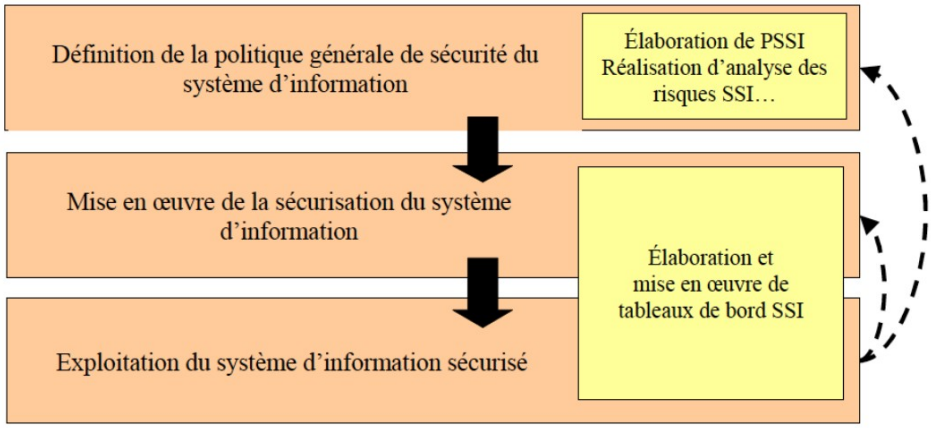


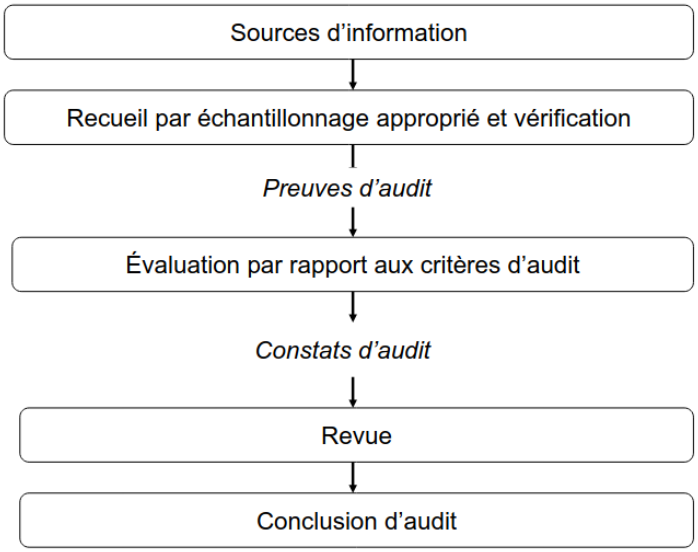
Diagramme de flux du Risque (Source AFAI)



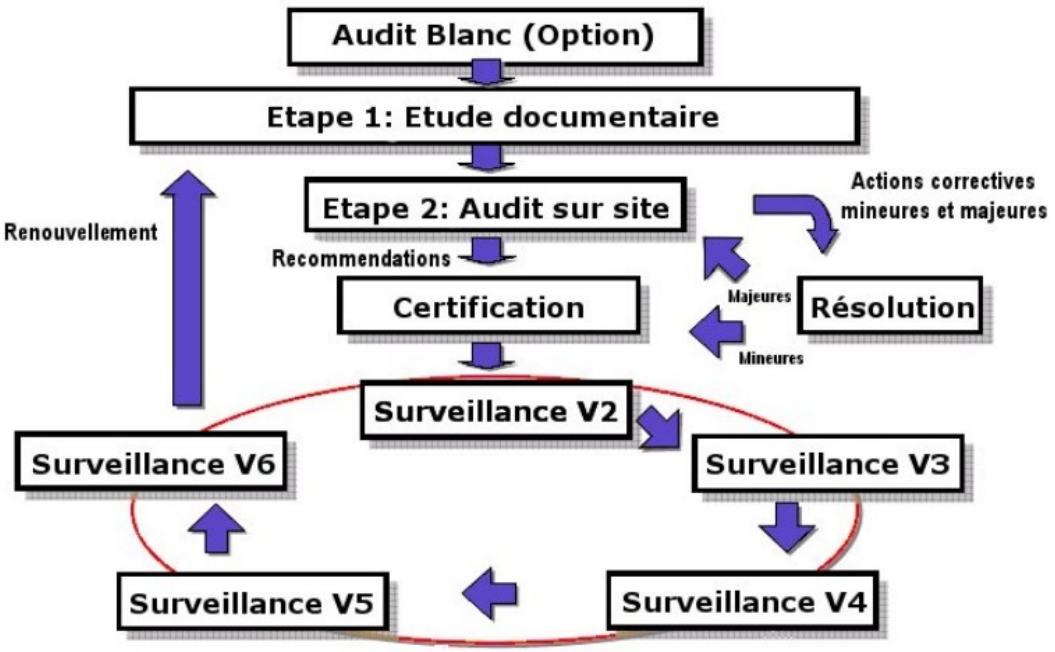
Audit :

Définition : Processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits

De la source d'information à la conclusion

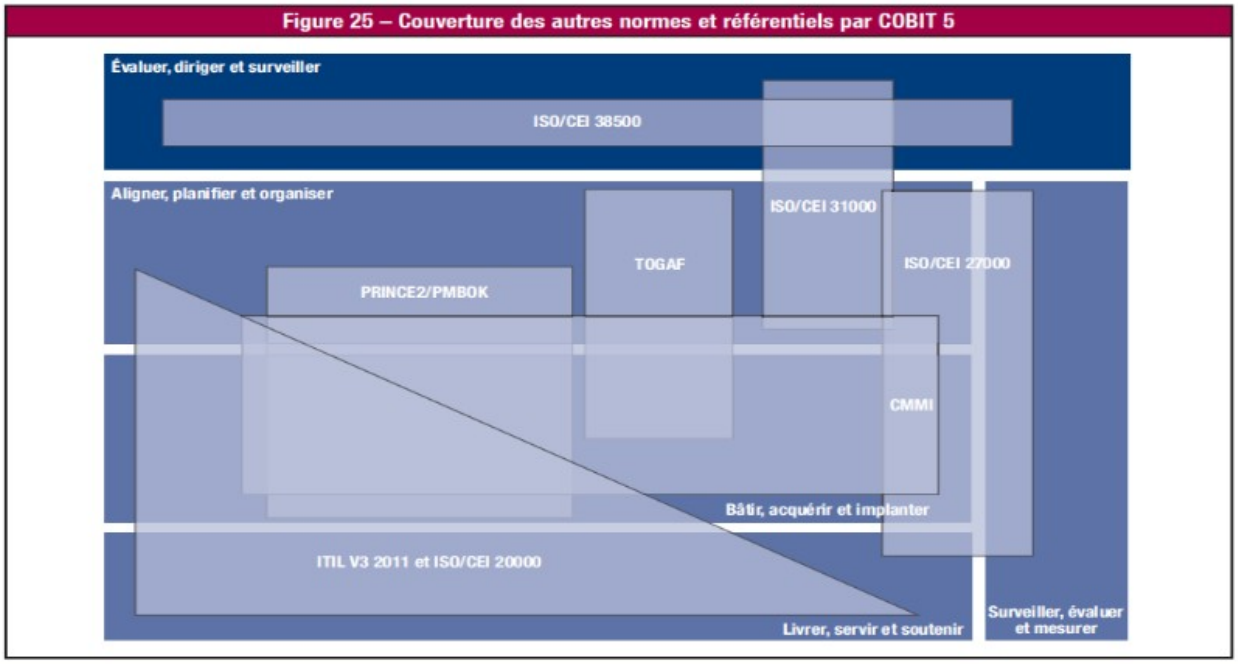


Certification ISO 27001



COBIT

Ensemble de recommandations et des process permettant d'évaluer les ressources informatiques qui s'inscrit dans une logique d'alignement et de maturité, par le contrôle et de l'audit. Outil largement utilisé dans la démarche d'IT Gouvernance.



!!Séance 4:

Gouvernance de système informatiques

Un projet est un ensemble de 4 composantes : un objectif, un budget, une durée (un planning), un cadre (un périmètre)

Les acteurs du projet sont : le Maître d'Ouvrage (MOA), le sponsor, l'équipe projet et le Maître d'Œuvre (MOE) ou Chef de Projet

Les contraintes d'un projet : elles sont au nombre de 3, le coût, le délai et le cadre, et sont représentées par un triangle. Lorsque le point reste dans les limites du triangle, tout au long de son déroulement, le projet est un succès.
Le pilotage d'un projet se déroule en 6 étapes :

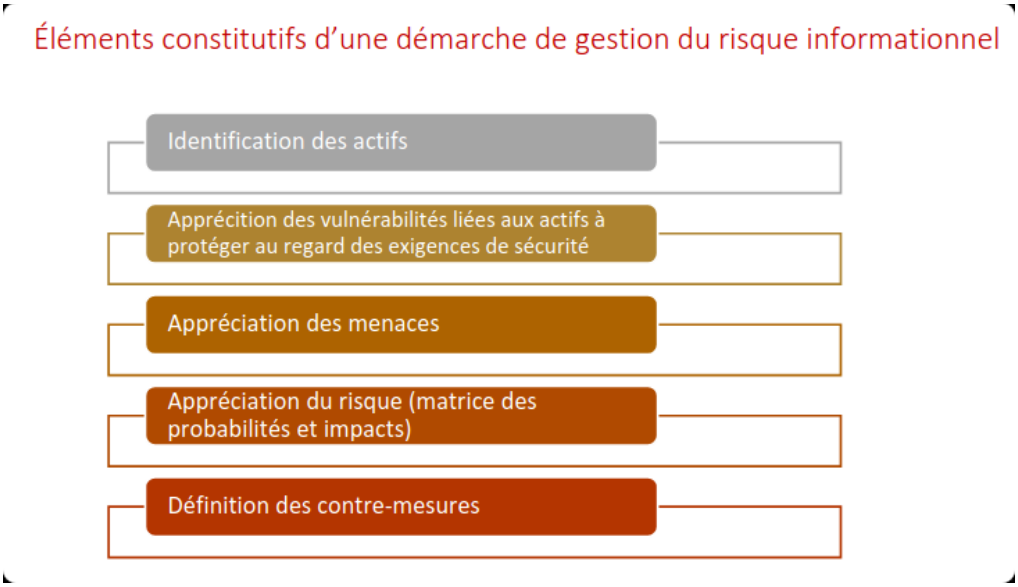
- La préparation du projet
- L'élaboration de la solution
- Le déploiement de la solution
- La validation pré-opérationnelle
- Le démarrage opérationnel et sa stabilisation
- La clôture du projet et le passage en MCO (Maintien en Condition Opérationnelle)

Les niveaux de maturité du SI : résoudre les problèmes informatiques ,optimiser les investissements informatiques et transformer les entreprises à l'aide du système d'information

Un risque est caractérisé par 3 composantes :

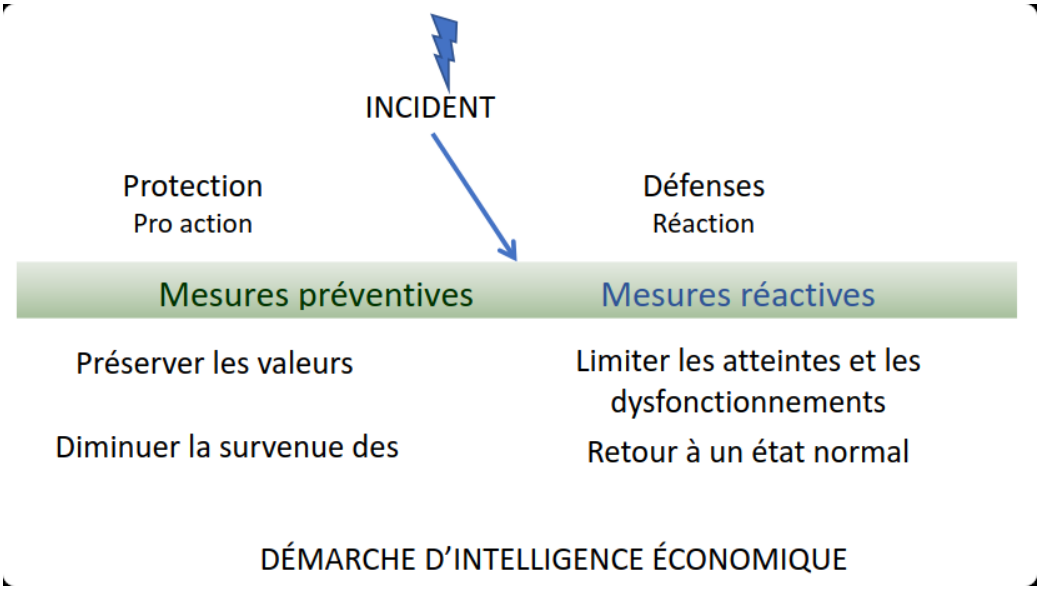
1. La menace ou le scénario matérialisant la source de risque
2. La/les vulnérabilités que la menace peut exploiter pour avoir des impacts
3. Les impacts, classés selon le niveau de gravité et le type

Analyse du risque : utilisation systématique d'informations pour identifier les sources afin de pouvoir estimer le risque
Évaluation du risque : processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance du risque
Appréciation du risque : ensemble des processus d'analyse et d'évaluation du risque
Traitement du risque : processus de sélection et de mise en œuvre des mesures visant à modifier le risque
Gestion du risque : activités coordonnées visant à diriger et à piloter une organisation vis-à-vis des risques et à maintenir les risques sous contrôle

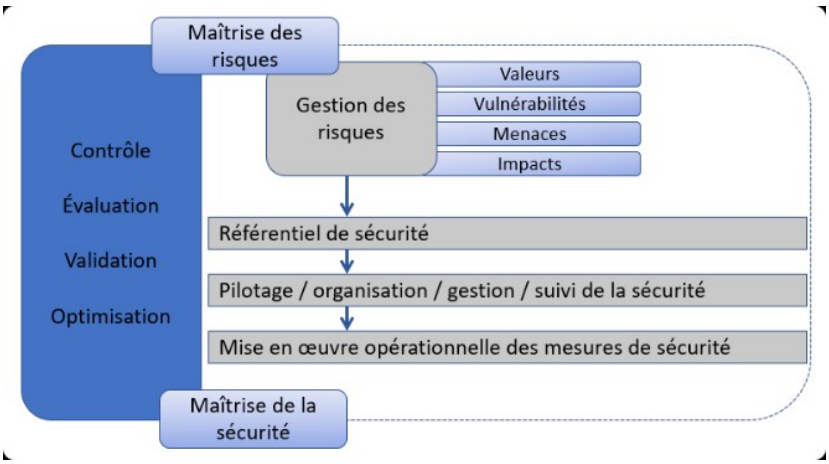


	Impacts				
Probabilité	Catastrophique 5	Majeur 4	Modéré 3	Mineur 2	Insignifiant 1
Très forte 5	10	9	8	7	6
Forte 4	9	8	7	6	5
Moyenne 3	8	7	6	5	4
Faible 2	7	6	5	4	3
Très faible 1	6	5	4	3	2

Risque extrême | Risque élevé | Risque moyen



DÉMARCHE D'INTELLIGENCE ÉCONOMIQUE



Processus : Ensemble de tâches logiquement reliées qui utilisent les ressources de l'entreprise pour réaliser un résultat. Suite d'activités qui, à partir d'une ou plusieurs entrées, produit un résultat représentant une valeur pour un client.

IMAGE ICI

!!!L'architecture fonctionnelle : La vision fonctionnelle de l'urbanisation a pour objectif de structurer l'ensemble des fonctions du système d'information.

Principes :

- Séparation du système d'information en blocs afin de:
- Limiter la portée de maintenance en cas de changement de structures de données
- Rendre neutre vis-à-vis du système d'information une modification dans les traitements d'un bloc
- Rendre possible une refonte progressive totale ou partielle du système d'information
- Idéalement, un système urbanisé comporte des blocs de plus ou moins grosse maille, dont les frontières sont « imperméables », et qui communiquent entre eux par échanges de message.
- Un bloc est « propriétaire » de ses données et de ses traitements

Les blocs fonctionnels

3 types de blocs fonctionnels (BF)

- BF1: Zone fonctionnelle
- BF2: Quartier fonctionnel
- BF3: Îlot fonctionnel

Rappel :

- 1 Zone fonctionnelle = 1 à N Quartier(s) fonctionnels
- 1 quartier fonctionnel = 1 à N îlot(s) fonctionnels

Chaque bloc (zone, quartier ou îlot) doit présenter une cohérence fonctionnelle interne forte et un couplage le plus faible possible avec les autres blocs.

A la frontière de chaque bloc, les échanges avec les autres blocs se font au moyen d'interfaces publiques que l'on appelle des « prises ».

Une prise est le moyen mis à la disposition du monde extérieur par un bloc pour proposer ses services. Ceux-ci peuvent être des services d'accès aux données dont il est propriétaire ou des traitements qu'il peut réaliser

Ces prises présentent les avantages suivants :

- Centraliser les appels de service et limiter le nombre d'interfaces
- Ajouter un niveau d'encapsulation supplémentaire
- Mutualiser les services : un service public et un seul pour répondre à des besoins identiques formulés par des demandeurs différents appartenant le cas échéant à des îlots, quartiers ou zones distincts
- Accroître la modularité
- Réduire au strict minimum les impacts à la suite d'une évolution d'un îlot dont les services publics sont sollicités par une diversité de demandeurs
- Faciliter la mise en œuvre de maintenances évolutives

Les blocs fonctionnels

1- Zone fonctionnelle

1er niveau de découpage du Système informatique, et le plus souvent au plus haut niveau de l'organisation informatique.

Une zone correspond à système

Les différentes zones fonctionnelles possibles :

▶ Zone échange (acquisition/restitution – interactions avec le monde extérieur) = Prise du SI

▶ Zone référentiel (de données et de règles)

- o Regroupement des informations communes aux différents éléments du SI

▶ Zone Opération

o 1 zone opération par métier principal
o Regroupement des SI nécessaires à la gestion opérationnelle du métier traité

▶ Zone décisionnelle unique
o Regroupement des blocs dédiés aux processus de gouvernance et d'analyse et utilisant des informations globalisées et historisées (statistiques, tableaux de bord,)

▶ Zon ressource
o Regroupement des systèmes dédiées à la gestion des ressources internes à l'entreprise (RH, comptabilité,)

2- Quartier fonctionnel

Un quartier
o Un sous-système (gestion des paiements, gestion des tarifs, gestion des voyages,)

3 – Ilot fonctionnel

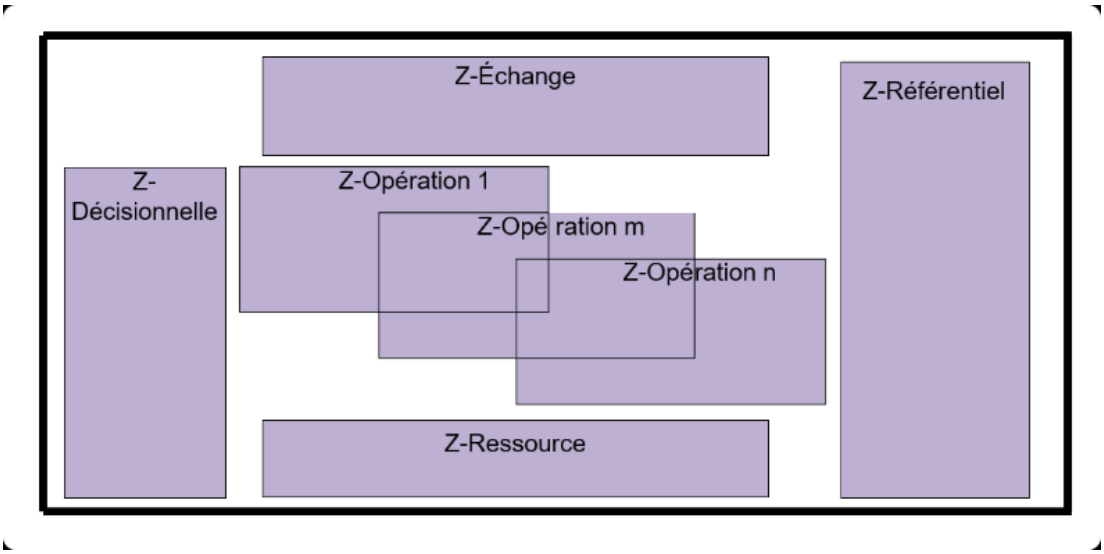
A une finalité fonctionnelle et comprend des traitements et des accès à des données pour cette finalité.

Les services au sein de l'îlot sont effectués indépendamment du chemin suivi par l'information en amont ou en aval de l'îlot.

Un îlot émet des résultats normalisés exploitables par d'autres îlots

Un îlot va typiquement correspondre à
o Une application ou une grande fonction applicative
o Un module d'un progiciel

Exemples : acceptation des paiements échelonnés, gestion des paiements immédiats, gestion des paiements échelonnés, facturation…)



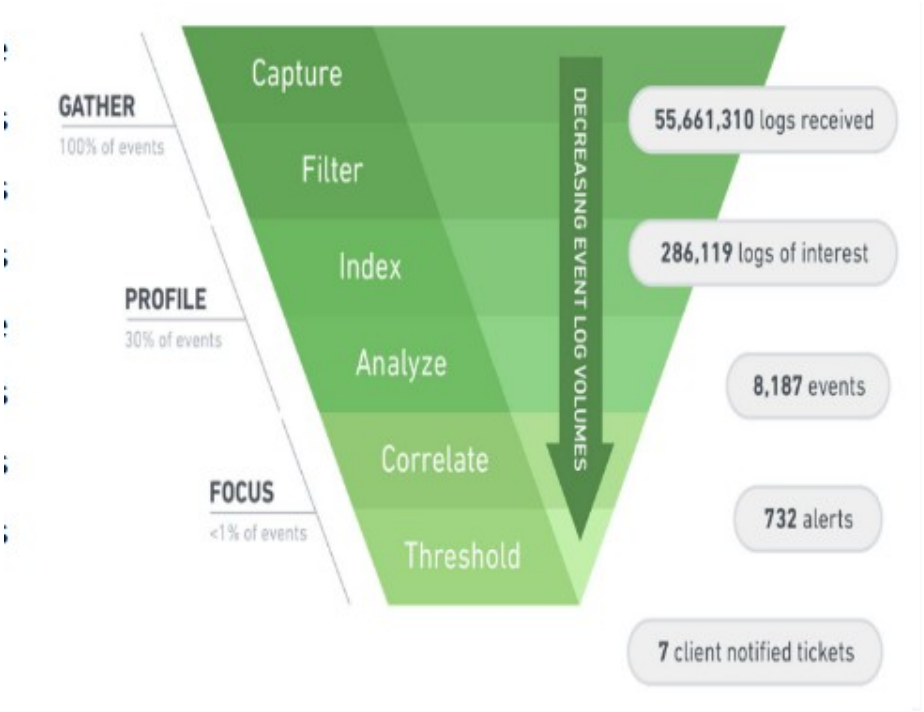
Séance 5:

Réponse à incident

• L'équipe de réponse aux incidents en/us IRT : équipe de membres de l'organisation dûment qualifiés et dignes de confiance qui gère les incidents tout au long de leur cycle de vie.
• Événement de sécurité de l'information : événement indiquant une violation possible de la sécurité de l'information ou une défaillance des contrôles.
• Incident de sécurité de l'information : un ou plusieurs événements de sécurité de l'information liés et identifiés qui peuvent nuire aux actifs d'une organisation ou compromettre ses opérations.
• Gestion des incidents de sécurité de l'information : manœuvre d'une approche cohérente et efficace du traitement des incidents de sécurité de l'information.
Les organisations s'assurent que les incidents de sécurité de l'information sont documentés, catégorisation, classés et partagés, afin que les métriques soient dérivées de données agrégées sur une période donnée. Ceci facilitera le processus de prise de décision stratégique.

5 étapes pour mettre en place :
- Planifier et préparer
- Détection et signalement
- Evaluation et décision
- Réponses
- Leçons apprises

En ce qui concerne les logs on cherche à collecter le minimum nécessaire pour ne pas avoir trop à gérer et être noyé, mais pour ne rien rater non plus.



Séance 9 :

Cyber Threat Intelligence

- La Cybermenace Intelligence (CTI): Est le processus de collecte, d'analyse et d'utilisation des informations sur les cybermenaces potentielles et réelles pour protéger les systèmes et les actifs d'une organisation.
- Discipline : Basée sur des techniques du renseignement, qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyberespace (cyber-attaques).

- Objectif : Dresser un portrait des attaquants ou de mettre en exergue des tendances (secteurs d'activités touchés, méthodes utilisées, etc.)
- Profiling : Permet de mieux se défendre et d'anticiper au mieux les différents incidents en permettant une détection aux prémices d'une attaque d'envergure.

TTP plus bas

Les IoC sont utilisés lors de la phase de réponse à un incident pour déterminer l'ampleur d'une attaque et des données compromises.
• Les indicateurs d'attaque (IoA pour Indicators of Attack) sont utilisés pour déterminer si une attaque est en cours et doit être contenue avant qu'elle ne puisse causer plus de dommages.
• Mais en termes d'enquêtes, il y a deux préoccupations principales :
• L'attaque est-elle en cours ? IoA
• Le problème a-t-il été maîtrisé ? IoC
• Les enquêteurs utilisent les indicateurs de compromission ou d'attaque laissés par un attaquant pour répondre à ces deux questions.

Fuzzing : donner des données random en entrée à un logiciel pour voir si ça plante ou si il y a une erreur

13 serveurs racine DNS

Mutex :
• Les mutex sont généralement utilisés par les créateurs de logiciels malveillants pour éviter l'infection d'un système par différentes instances du même logiciel malveillant.
• Lorsque le cheval de Troie infecte un système, la première étape consiste à obtenir un descripteur d'un mutex « nommé », si le processus échoue, le logiciel malveillant disparaît.

Code couleurs TLP :
Clear : La divulgation n'est pas limitée
Vert : Divulgation limitée, restreinte à la communauté
Ambre : Divulgation limitée, restreinte à l'organisation des participants et à ses clients
Ambre + strict : Divulgation limitée, restreinte à l'organisation des participants
Rouge : Ne pas divulguer, réservé au participants uniquement

Code couleurs PAP :

Clear : Utilisation libre dans le respect des licences et de la loi, pas de contrainte relative à l'exploitation ou à la manipulation de l'information
Vert : Utilisation encadrée autorisant les interactions non intrusives avec des sources malveillantes
Ambre : Utilisation limitée à une exploitation passive de la donnée, c'est-à-dire aux seules actions non directement visibles des sources malveillantes
Rouge : Utilisation limitée aux investigations numériques ou à la détection, sur des infrastructures dédiées : seules les personnes ayant le besoin d'en connaître ont accès à ces infrastructures

	PAP:RED	PAP:AMBER	PAP:GREEN	PAP:CLEAR
TLP:RED	P1	P2	N/A	N/A
TLP:AMBER	P3	P4	P5	N/A
TLP:GREEN	N/A	P6	P7	NA
TLP:CLEAR	N/A	N/A	N/A	P8

Cycle de vie d'un IOC/IOA :
1- Collecte
2- Validation
3- Analyse
4- Classement
5- Stockage
6- Utilisation
7- Mise à jour

MITRE ATT&CK (MITRE ATT&CK) framework, est une base de connaissances universellement accessible et continuellement mise à jour servant à modéliser, détecter, anticiper et lutter contre les menaces de cybersécurité basées sur les comportements adverses connus des cybercriminels.
MITRE TTP : Tactics, Techniques, et Procedures, méthodologie de classification des menaces en cybersécurité.