

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'Einhower: 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

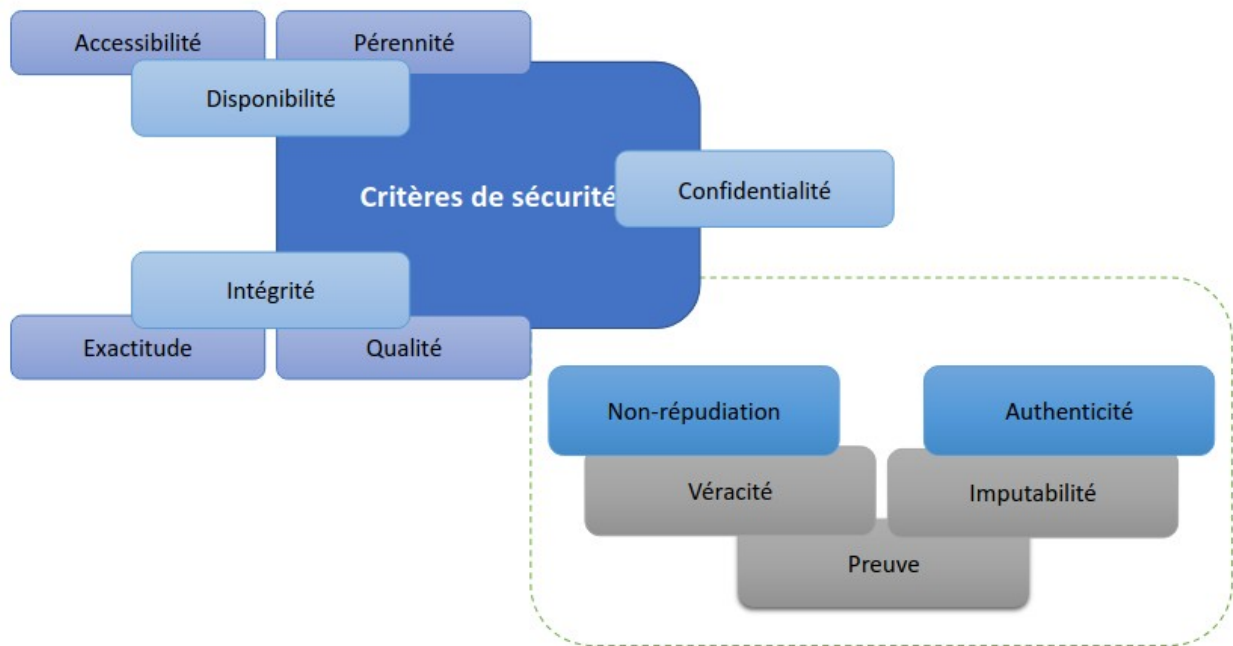
OSINT → Open-Source Intelligence, désigne l'ensemble des techniques et méthodes utilisées pour collecter et analyser des informations disponibles publiquement

AQSSI → L'autorité qualifiée pour la sécurité des systèmes d'information est la personne responsable, pour sa structure, de la sécurité des systèmes d'information. C'est l'autorité juridiquement responsable, sa responsabilité ne peut être déléguée.

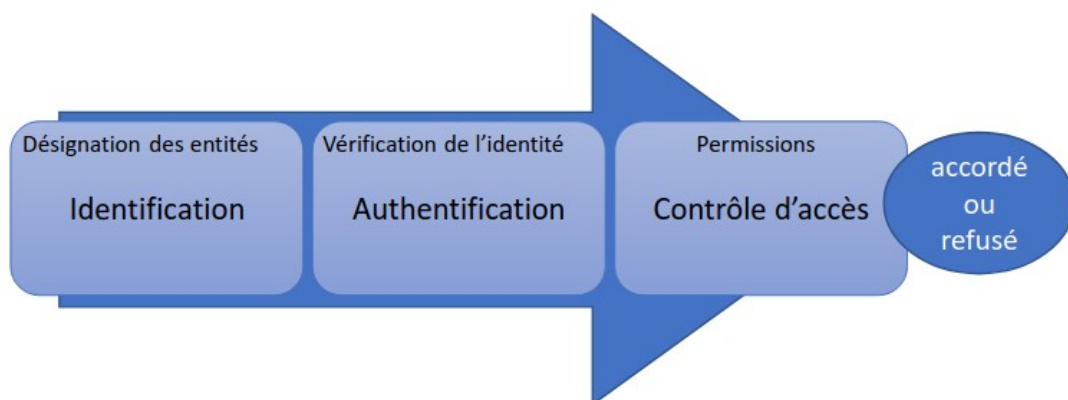
Séance 1:

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



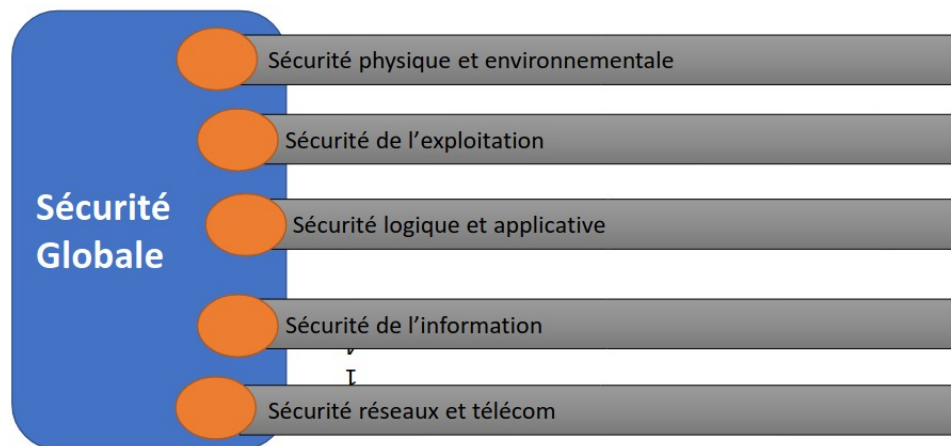
Cyberspace → Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. (autre nom d'internet)

Cybersécurité → État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace 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

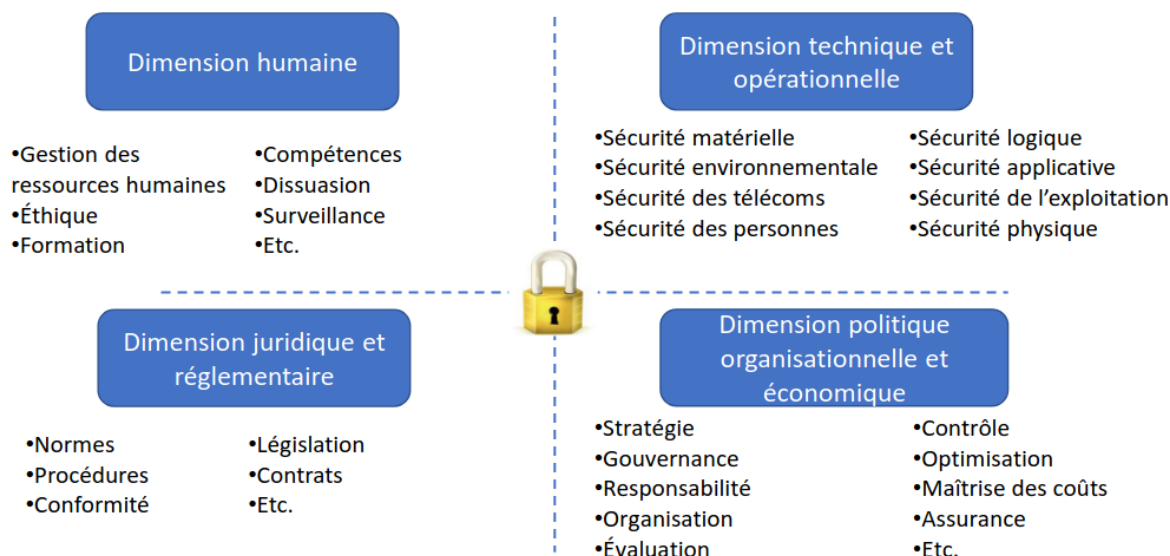
cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cybergdéfense.

Cybergdéfense → Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberspace 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



Physique et environnement intérieur, exploitation matériel dedans



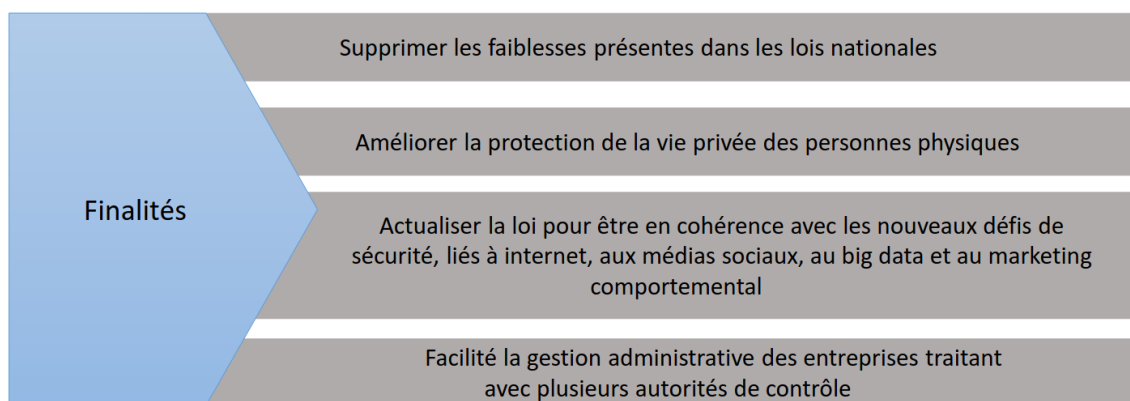
Identité numérique:

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

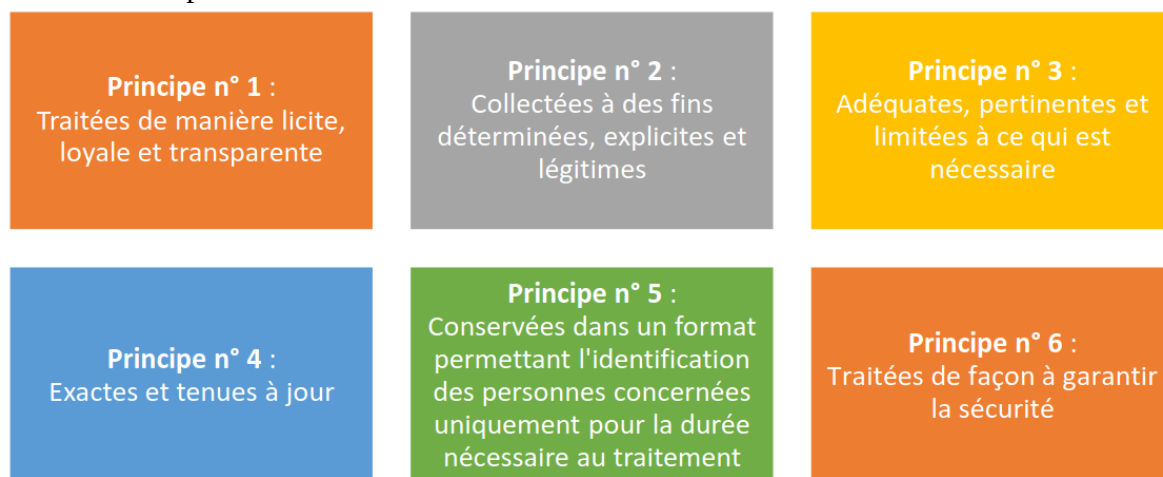
Ce n'est pas un droit constitutionnel

RGPD (européen) 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

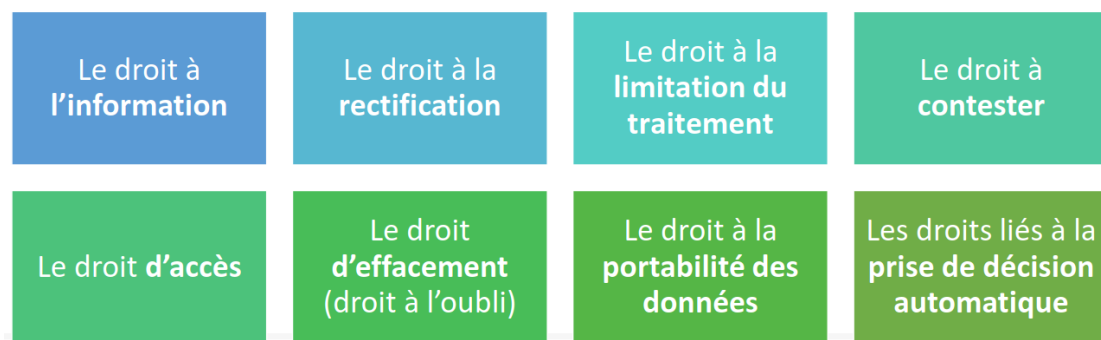


Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel 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 :



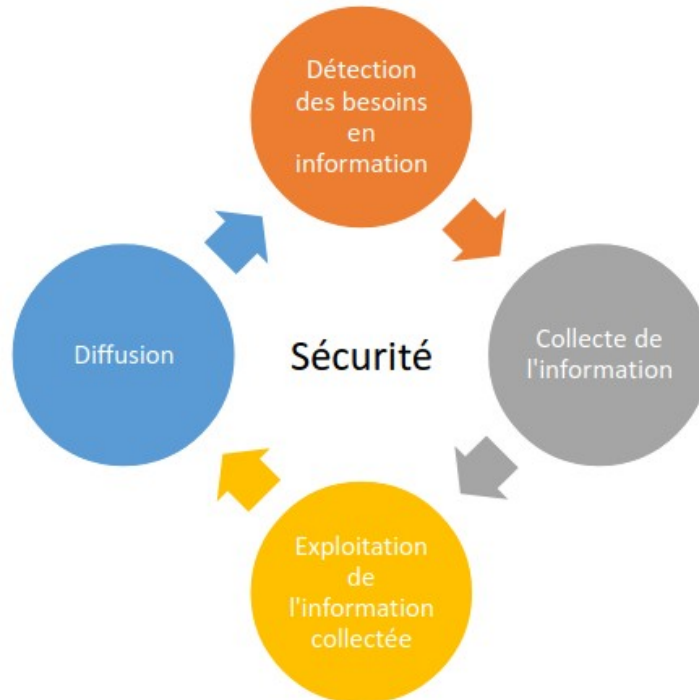
Séance 2:

Intelligence économique, géopolitique

Les états ont intérêt à ce que le business se passe bien entre eux. Besoin de confiance

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



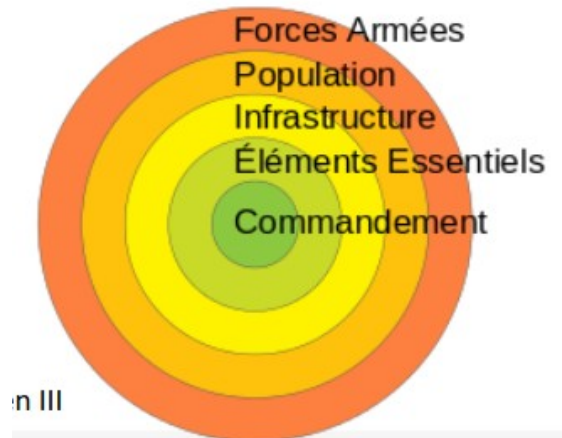
Le niveau de protection de l'ensemble est égal à son élément le moins protégé.

Agir sur l'attitude et le comportement du public: La méthode employée pour façonner l'opinion se nomme «relations publiques».

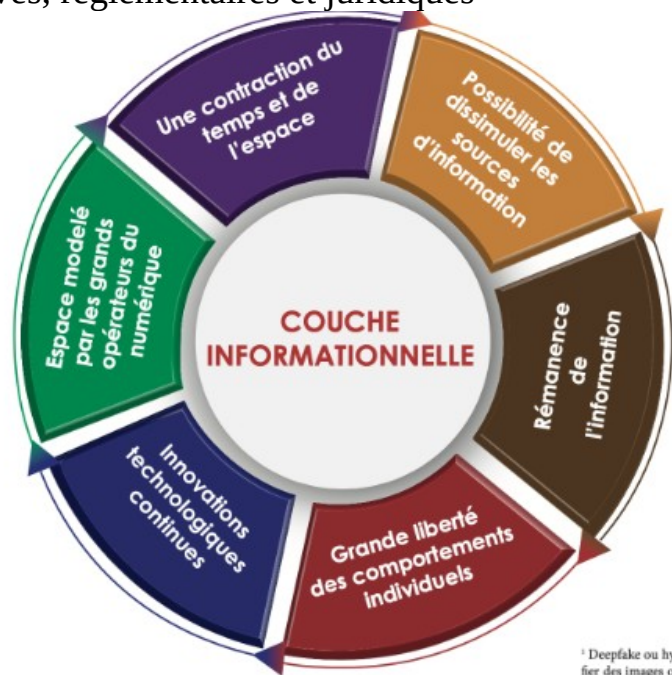
Processus d'influence: identification des cibles → définition du message et identification des relais → choix du moment d'action → surveillance et ajustement



Théorie des cinq cercles de John A.Warden: le cyberspace 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 (directive européenne)

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 être soumis à des contrôles de sécurité

RGS → Référentiel Général de Sécurité fournit 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

$T \rightarrow A$: « Authentification »

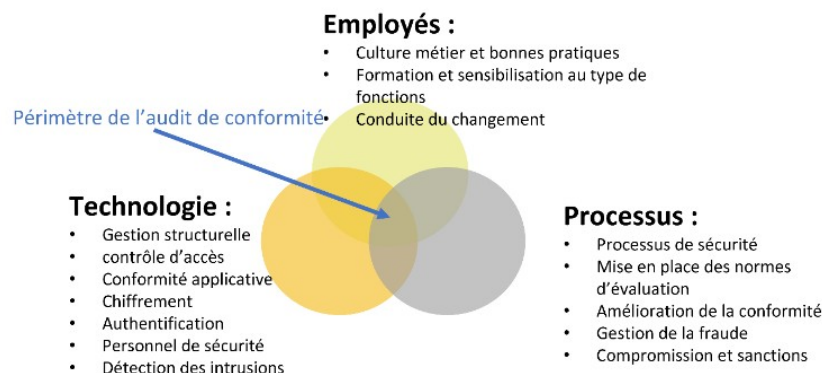
$C \rightarrow T$: $Data, \{Data\}_{K_B^{-1}}$

$T \rightarrow A$: « Code ? »

$A \rightarrow T$: 3456

$T \rightarrow C$: 3456

$C \rightarrow T$: ok



Référentiel de sécurité PCI-DSS

Séance 3:

Norme ISO 27000

Norme de sécurité de l'information

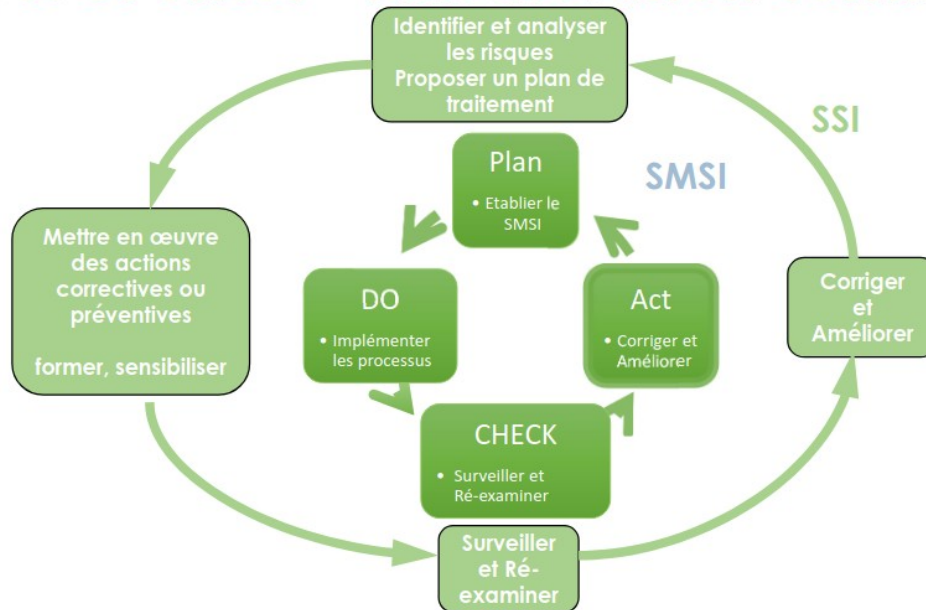
La sécurité est un processus

Les décisions doivent être prises au plus haut niveau

Norme ISO 27001 management de la sécurité et sécurité. Convient à toutes les organisations

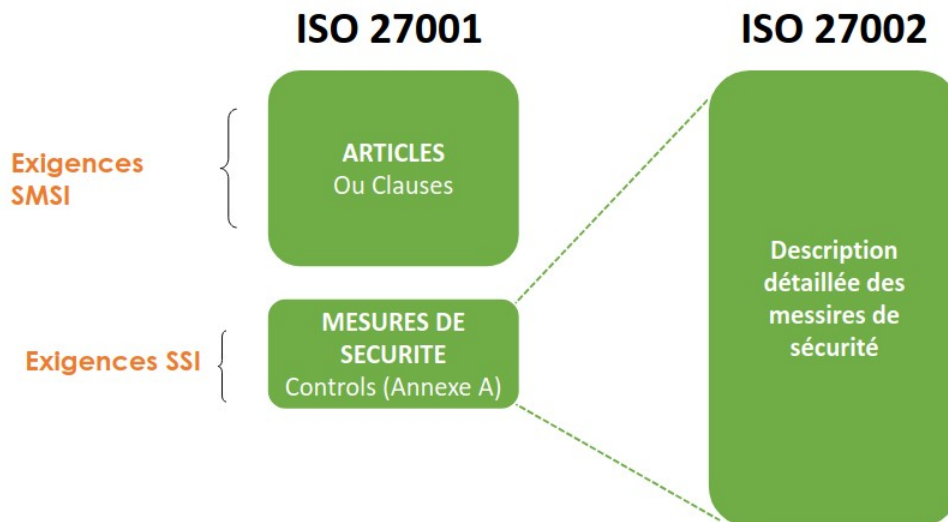
PDCA → Modèle de gouvernance Plan → Do → Check → Act

SSI et SMSI – Amélioration continue



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

Approche ISO 27001

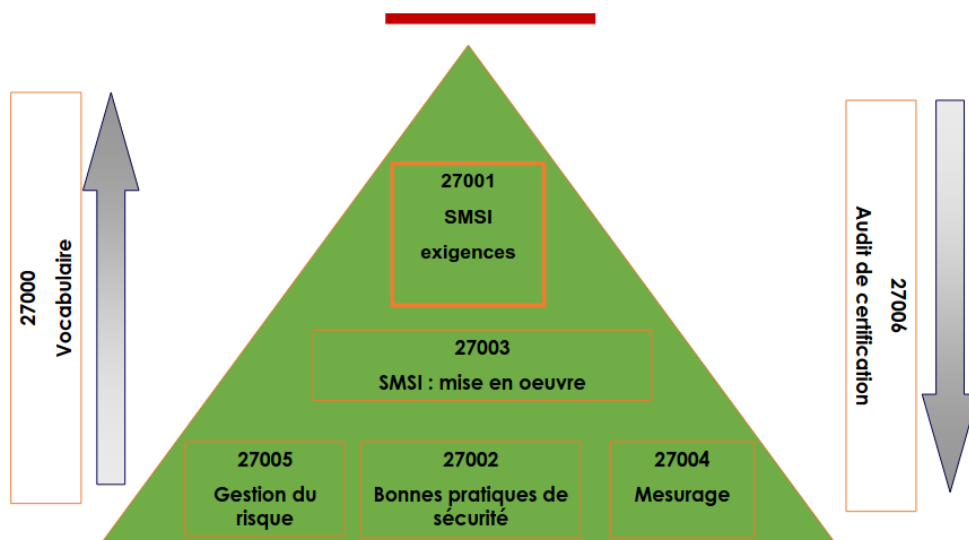


Qu'est-ce qu'un SMSI ? Un système de management de la sécurité de l'information que votre entreprise met en place pour protéger son contenu, réduire les risques et assurer la continuité de votre activité même en cas de faille du système.

- 27007 : Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
- 27008 : Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

- 27010 ~27001 : Gestion de la sécurité de l'information des communications intersectorielles et inter-organisationnelles
- 27011 ~27002 : Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002
- 27031 : Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité
- 27033 : Sécurité Réseau
- 27035 : Gestion des incidents de sécurité de l'information

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

SMSI – Dans la pratique



Démarche globale 27001

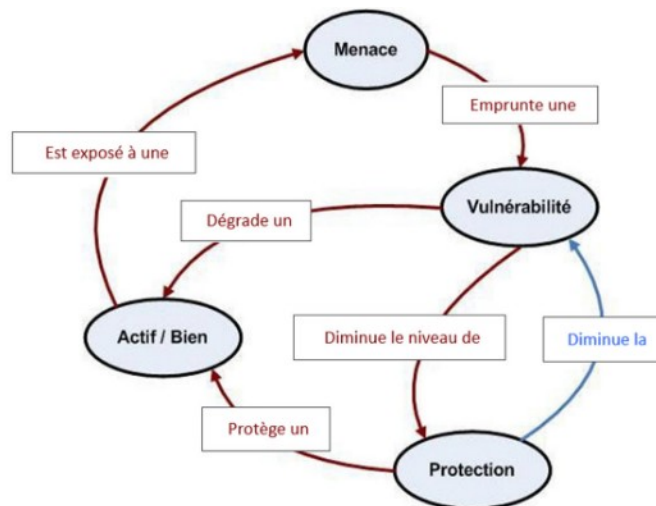
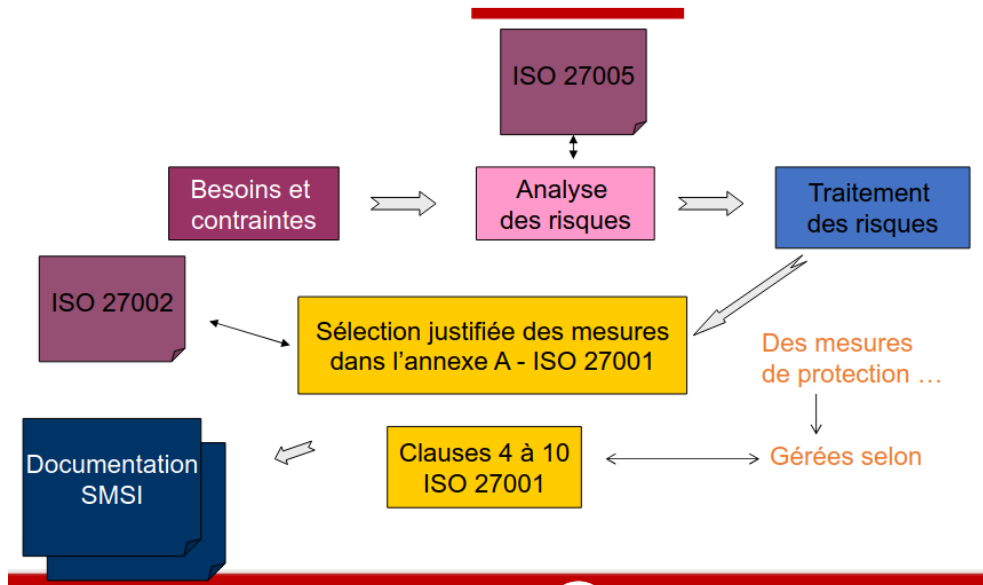
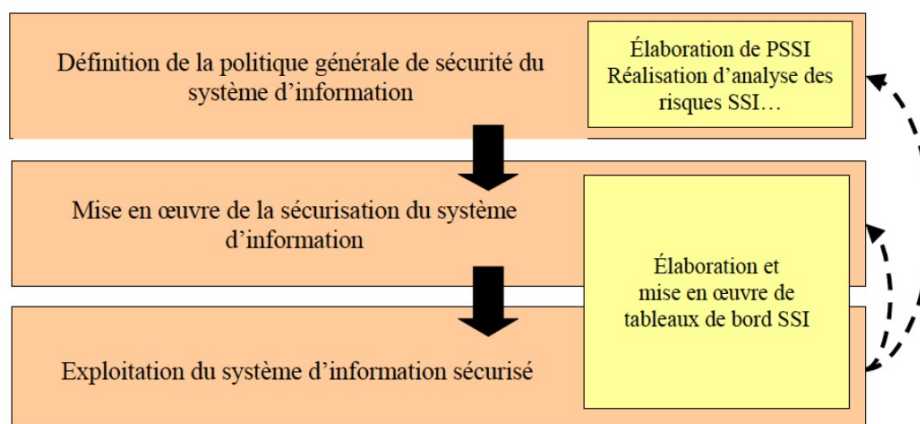


Diagramme de flux du Risque (Source AFAI)



Elaboration SMSI :

1. Concevoir l'organisation du SMSI
2. Concevoir la politique de sécurité
3. Développer les plans opérationnels et les procédures
4. Planifier les revues de management
5. Concevoir les programmes de formation, sensibilisation et compétences
6. Concevoir la sécurité du système d'information
7. Concevoir les exigences d'enregistrements du SMSI, et le contrôle de la documentation
8. Produire le plan d'implémentation du SMSI

CLOISONNEMENT RESEAUX !!! RUMEURS !!!

Exemples indicateurs :

- Niveau de mise en œuvre du SMSI
- Niveau de formation des parties prenantes au SMSI
- Niveau de sensibilisation à la sécurité de l'information
- Avancement des projets/chantiers sécurité
- Qualité des mots de passe
- Couverture du processus de vérification du SMSI
- Gestion des incidents de sécurité
- Efficacité du processus
- Mise en œuvre des actions correctives
- Niveau d'engagement de la Direction
- Niveau de protection contre les codes malveillants
- Efficacité des contrôles d'entrée physiques
- Efficacité de l'examen des logs
- Efficacité de la gestion de la maintenance périodique
- Efficacité de la sécurité dans les accords avec les tiers fournisseurs

Tableaux de bord SSI

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

Audit interne, audit externe

Accréditation (ISO-17000) : Reconnaissance de la compétence d'un organisme à évaluer la conformité et à certifier des produits, des systèmes ou des personnes.

Preuves d'audit : Preuves objectives - Faits

- Informations, enregistrements, déclarations
- Peuvent être quantitatives ou qualitatives
- Doivent se rattacher à un critère d'audit
- Basée sur l'observation, la mesure ou le test
- Peuvent être vérifiées

Audit de sécurité de l'information - Objectifs

- Valider le degré d'implémentation du SMSI

- Valider l'efficacité des politiques, procédures et instructions
- Identifier des failles de sécurité
- Fournir des opportunités d'amélioration
- Assurer un contrôle régulier

Rôle du Responsable d'audit

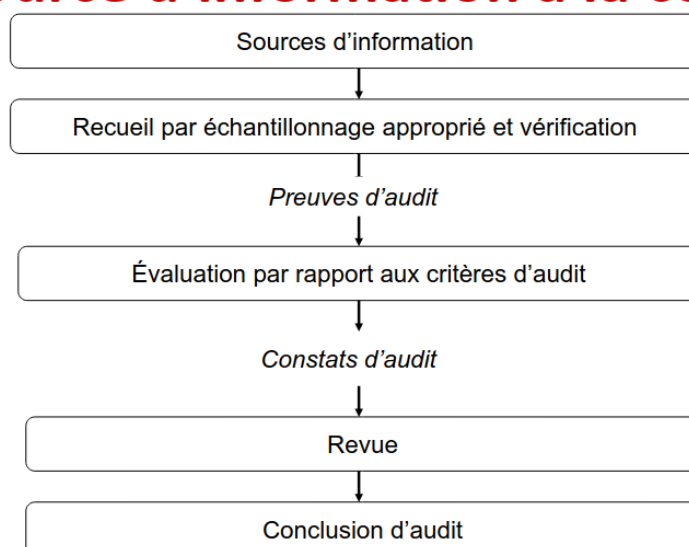
- Planifier et diriger l'audit
- Et utiliser efficacement les ressources au cours de l'audit
- Représenter l'équipe d'audit
- Lors des communications avec le commanditaire et l'audité
- Organiser l'équipe d'audit
- Et diriger ses membres
- Amener l'équipe d'audit à élaborer les conclusions
- Décider de l'issue d'une non-conformité
- Prévenir et résoudre les conflits
- Reporter les résultats de l'audit
- Préparer et établir le rapport d'audit

Ne pas mettre de nom de personne dans les non conformités

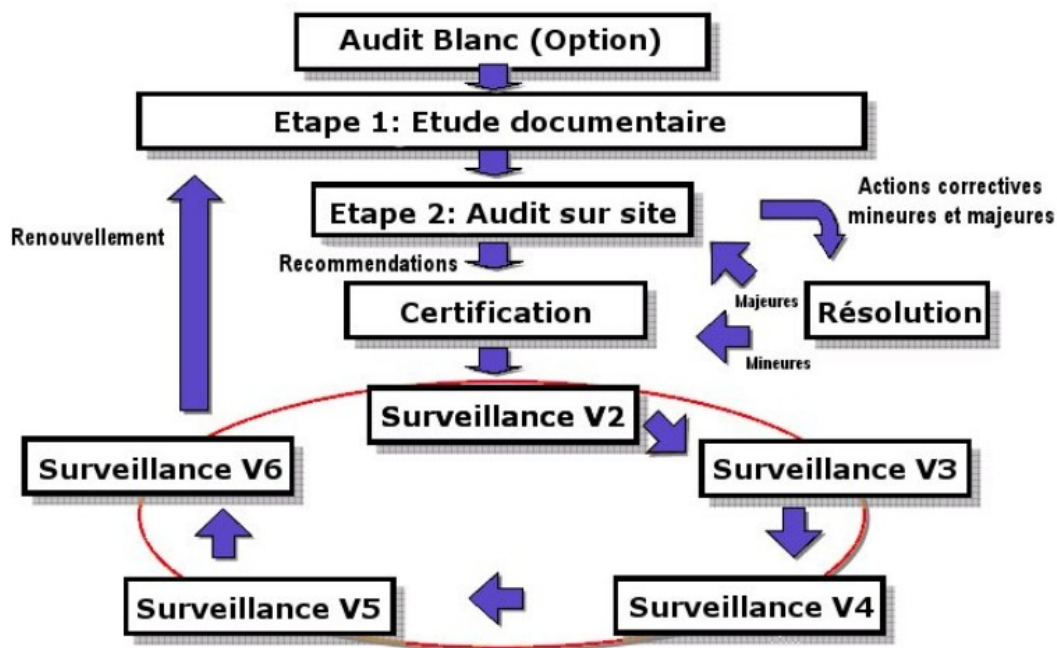
Etablir la responsabilité [titre de l'emploi plutôt que le nom de la personne]

- Non-conformité Majeure : Non-respect d'au moins une exigence et qui fait courir un risque direct et significatif au système
- Non-conformité mineure
- Remarque
- Une non-conformité non traitée dans les délais prescrits est considérée en « récurrence »
- La récurrence implique une augmentation de son niveau de gravité, une remarque en récurrence devient un écart mineur, un écart mineur en récurrence devient un écart majeur

De la source d'information à la conclusion



Certification ISO 27001



EVALUATION

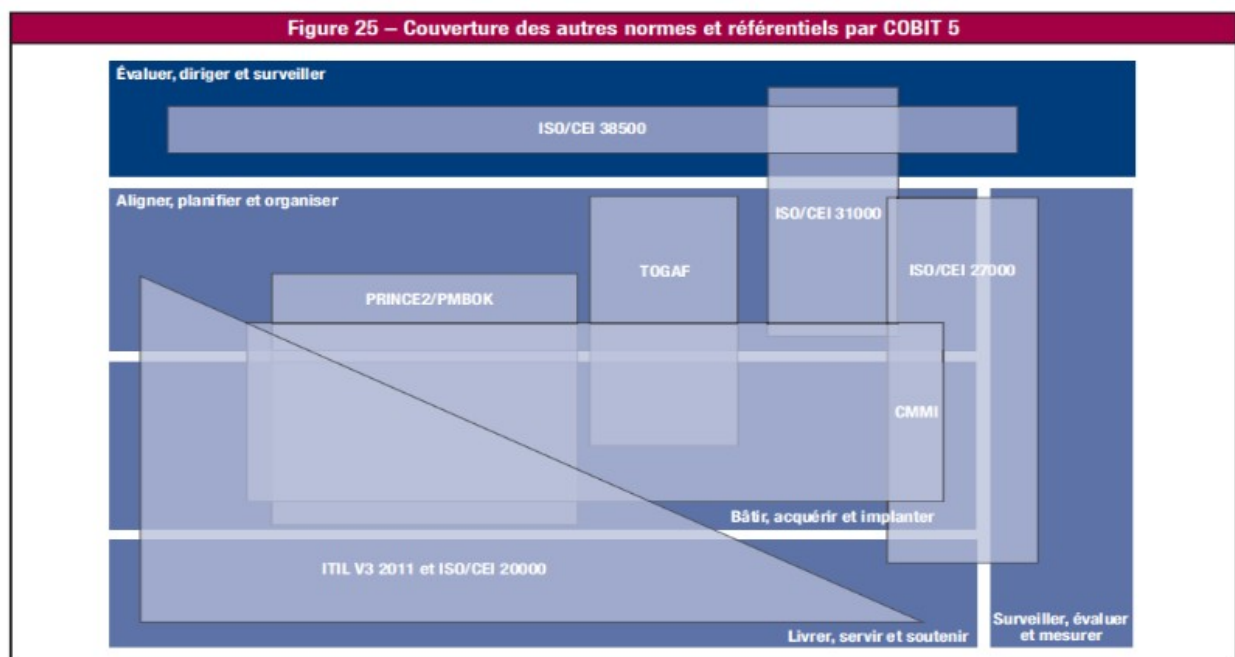
OBJECTIFS

PRIORISATION/DECISIONS

CONTROLE PERFORMANCE ET CONFORMITE SELON OBJECTIFS

ISACA 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.



Cobit : principes en sécurité de l'information



1. Soutenir les affaires

Intégrer la SI dans les activités d'affaires essentielles;
Evaluer et traiter les risques de sécurité;
Promouvoir une culture d'amélioration continue en SI



2. Sécuriser les actifs

Définir une approche formelle pour gérer les risques;
Catégoriser/classifier les actifs;
Adopter des développements sécuritaires



3. Sensibiliser les ressources

Sensibiliser afin d'obtenir des réflexes de sécurité;
Implication de la haute direction

!!Séance 4:

Gouvernance de système informatiques

Un projet en sécurité informatique est une suite d'actions et d'activités entreprises dans le but de répondre à un besoin défini et dans des délais fixés et dans la limite d'une enveloppe budgétaire allouée

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) (cahier des charges), 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 :

- o La préparation du projet
- o L'élaboration de la solution
- o Le déploiement de la solution
- o La validation pré-opérationnelle
- o Le démarrage opérationnel et sa stabilisation
- o 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

Le terme gouvernance désigne la capacité d'une organisation à être en mesure de contrôler et de réguler son propre fonctionnement. L'un des objectifs étant d'éviter les conflits d'intérêts liés à la séparation entre les ayants droit (actionnaire, Direction d'entreprise, Conseil d'Administration, État) et les acteurs (employés, fournisseurs, clients, banques, environnement, etc.).

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

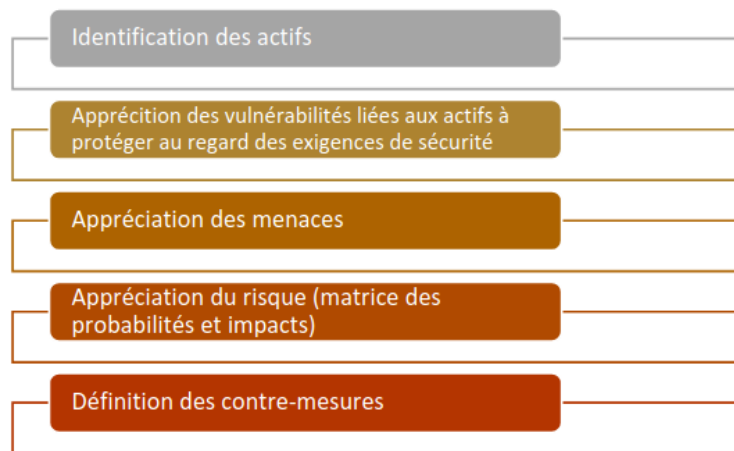
Évaluation du risque : processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance du risque

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

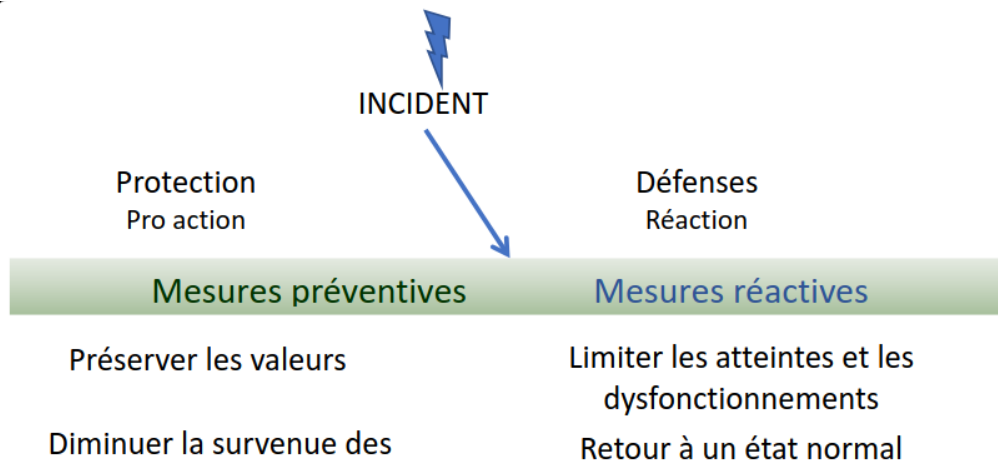
Gestion du risque : activités coordonnées visant à diriger et à piloter une organisation vis-à-vis des risques et à maintenir les risques sous contrôle

Éléments constitutifs d'une démarche de gestion du risque informationnel

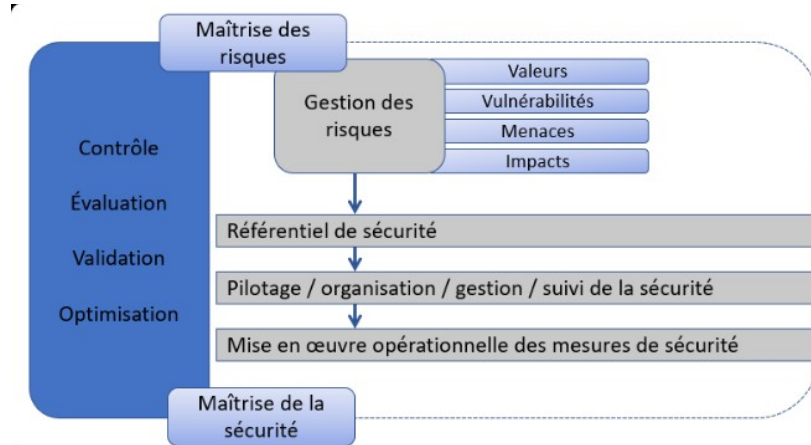


	Impacts				
Probabilité	Catastrophique 5	Majeur 4	Modéré 3	Mineur 2	Insignifiant 1
Très forte 5	10	9	8	7	6
Forte 4	9	8	7	6	5
Moyenne 3	8	7	6	5	4
Faible 2	7	6	5	4	3
Très faible 1	6	5	4	3	2

Risque extrême	Risque élevé	Risque moyen
----------------	--------------	--------------



DÉMARCHE D'INTELLIGENCE ÉCONOMIQUE



ROSI : Le retour sur investissement en matière de sécurité (ROSI) mesure spécifiquement le retour sur investissement dans les initiatives de cybersécurité. L'investissement dans la sécurité est essentiel pour une organisation, mais de nombreuses équipes de sécurité ont du mal à quantifier les avantages qui en découlent.

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.

!!!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,)

► Zone ressource

o Regroupement des systèmes dédiés 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 – Îlot 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.

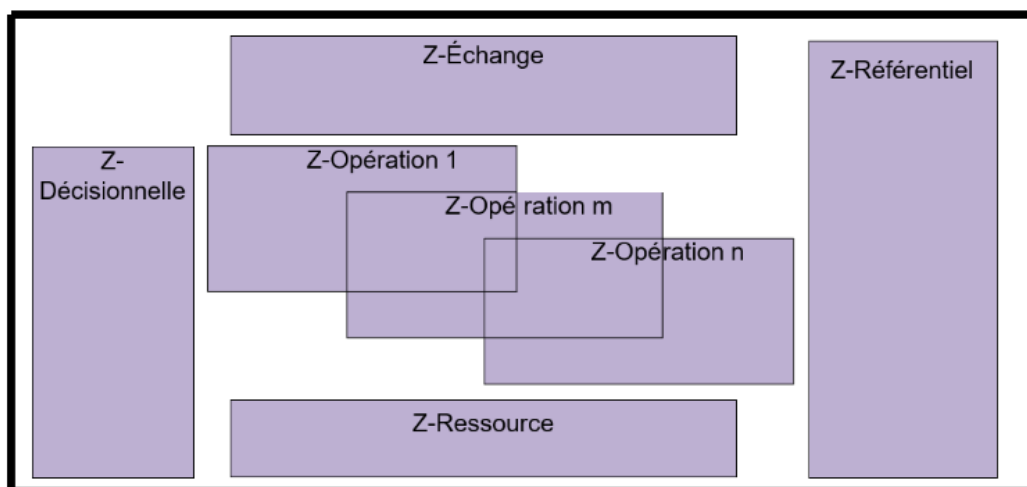
Un îlot émet des résultats normalisés exploitables par d'autres îlots

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...)



Architecture technique

Démarche en 7 étapes (urbanisation)

1 Appliquer les règles de bonnes pratiques pour définir les différentes zones composant la division fonctionnelle : échanges, référentiel de données et de règles, décisionnel, opération, ressource

2 Exploiter les processus métier afin d'identifier les classes concepts.

- Une classe concept est une classe de substance portant la notion essentielle du concept métier correspondant.

- Une classe secondaire complète la définition du concept métier auquel elle se rapporte (sous ensemble fonctionnel du concept rattaché)

3 Recadrage de l'ébauche d'architecture fonctionnelle en fonction des objectifs stratégiques du SI

4 Identification des services des différents blocs fonctionnels composant l'architecture fonctionnelle

5 Vérification - rapprochement des activités du processus métier par rapport aux blocs fonctionnels devant les services nécessaires

6 Rebouclage par rapport aux objectifs stratégiques du SI

7 Dernière vérification du respect des règles d'urbanisme

Séance 5:

Réponse à incident (ISO 27035)

- 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.

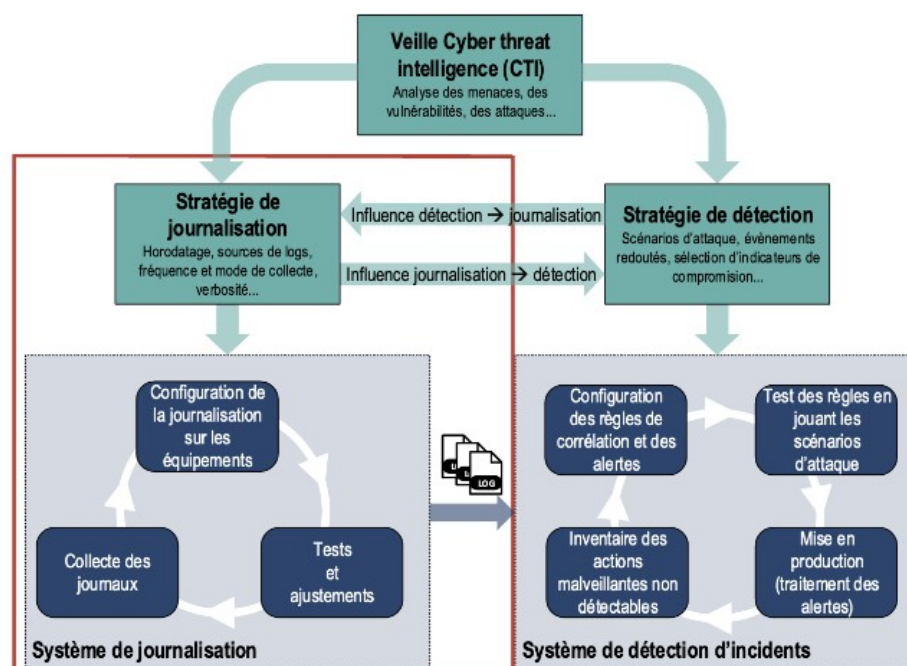
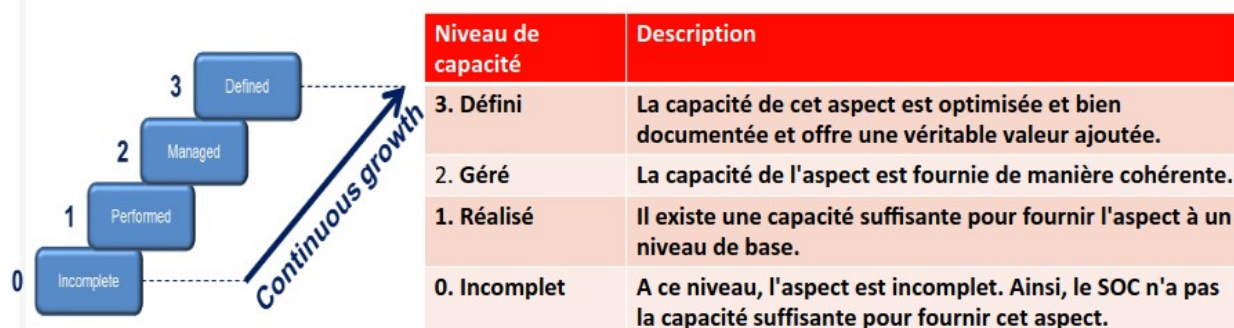
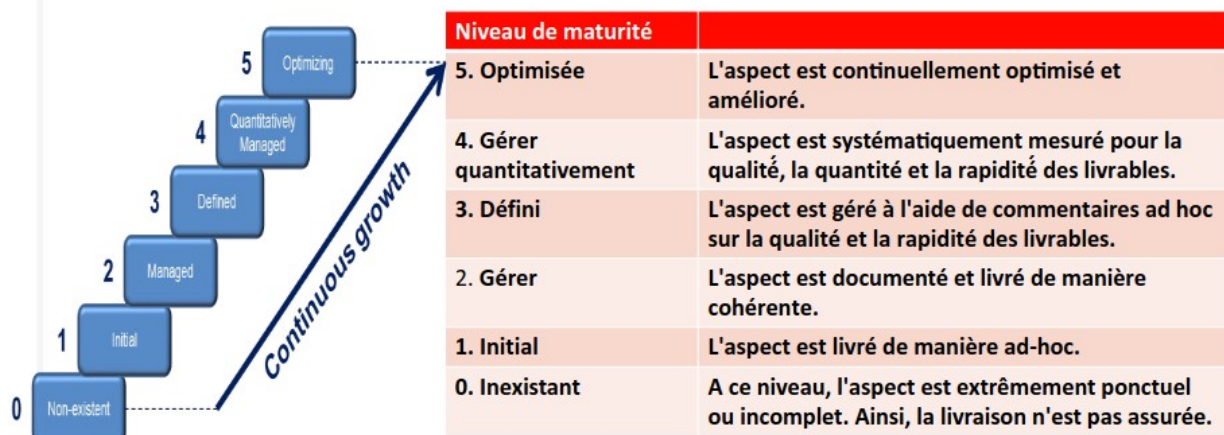
Les organisations s'assurent que les incidents de sécurité de l'information sont documentés, catégorisation, classés et partagés, afin que les métriques soient dérivées de données agrégées sur une période donnée. Ceci facilitera le processus de prise de décision stratégique.

Investiger traces réseau et système

Dans le meilleur des mondes, le niveau de maturité du SOC ou CERT permet procéder à une réponse graduée garantissant la continuité de service et la remédiation rapide. Concomitamment, le service juridique est averti et les forces de l'ordre sauront réagir

SOC : les SOC sont des centres d'expertise où les connaissances et les compétences en matière de cybersécurité sont agrégées. Le SOC est l'endroit où les informations de journal collectées dans toute l'entreprise sont collectées, traitées et analysées par des personnes qualifiées pour trouver des indicateurs de cybermenaces dans l'infrastructure. Ainsi, le SOC ajoute de la valeur à l'entreprise en augmentant la résilience de l'organisation contre les cybermenaces et en minimisant les dommages résultant des cyberattaques.

La mesure de la maturité des capacités est un outil de gestion du SOC qui peut être utilisé pour déterminer les forces et les faiblesses du SOC. En outre, il fournit un moyen de mesurer la croissance du SOC, démontrant ainsi le retour sur investissement. Le SOC-CMM est un outil d'auto-évaluation sur la maturité de leur capacités permettant aux SOC de mesurer et de se développer.



Périmètre de ce guide

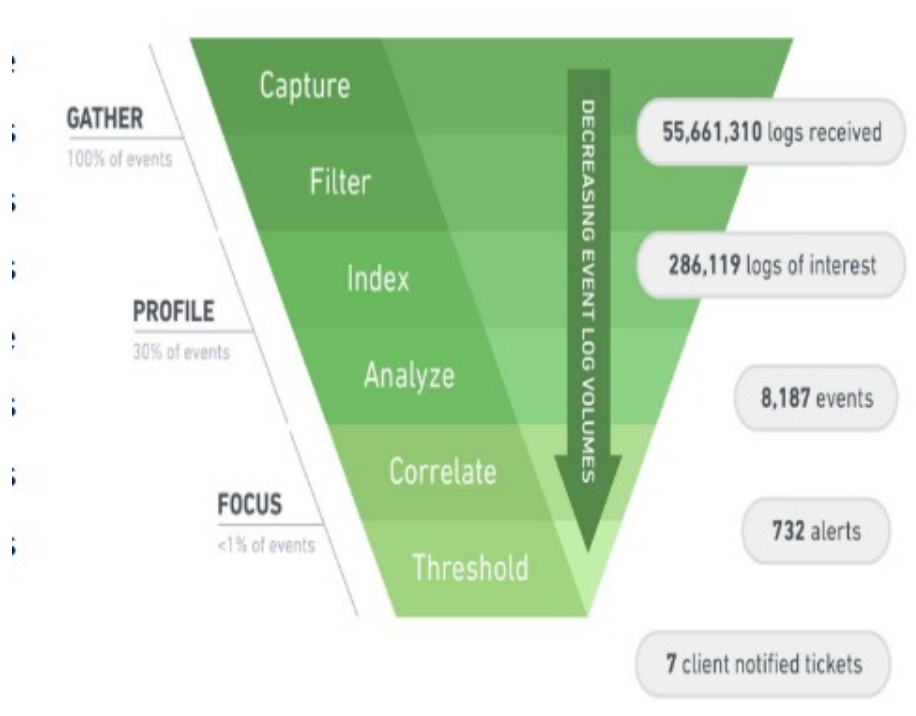
En ce qui concerne les logs on cherche à collecter le minimum nécessaire pour ne pas avoir trop à gérer et être noyé, mais pour ne rien rater non plus.

Production de logs : Sur Windows : via la politique de gestion de log (GPO) plus précisément dans les Global Policies Preference (GPP) Sur Linux : AuditD Sur les EAR : réseau, FW, Pix

Security Information et Event Manager, le graal pour la gestion des log en masse. Pour les experts, les bidouilleurs, les puristes, la suite ELK (Elastic, Loglogic, Kibana) est la solution opensource. Splunk

5 étapes pour mettre en place :

- Planifier et préparer
- Détection et signalement
- Evaluation et décision
- Réponses
- Leçons apprises



Acteurs et responsabilités :

Au niveau local la chaine SSI se décline suivant les préconisations nationales donnant lieu à une structure dont les acteurs sont :

L'autorité hiérarchique qualifiée en SSI (chef d'organisme : AQSSI, chef d'établissement : Personne Juridiquement Responsable) est juridiquement responsable de la sécurité des systèmes d'information de ses entités ou de son entité et du respect des réglementations.

Sur le plan décisionnel et juridique, chaque service déconcentré, chaque établissement est responsable et décideur dans son périmètre.

L'autorité hiérarchique est personnellement responsable, par convention.

Le responsable d'une entité déconcentrée agit sous l'autorité de l'AQSSI.

L'AQSSI est assisté par un responsable de la sécurité des systèmes d'information (RSSI) qu'il nomme et mandate pour définir et veiller à la bonne réalisation de la politique sécurité qu'il a lui-

même impulsée. C'est cette position de rattachement direct auprès de l'AQSSI qui lui confère toute sa légitimité et qui lui permet d'assurer pleinement sa mission. Il s'appuie lui-même sur une chaîne de correspondants de Sécurité (CR) qu'il organise et dont il est le référent.

Acteurs étatiques :

Cybermalveillance.gouv.fr

ANSSI

Sous-direction de lutte contre la cybercriminalité

DGSI

Préfecture de Police

La brigade de lutte contre cybercriminalité (BL2C)

La brigade des fraudes aux moyens de paiement (BFMP)

La brigade de répression de la délinquance astucieuse (BRDA)

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 cyberspace (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 (Tactiques, Techniques et procédures)

MD5, SHA256, SHA512

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 de A à M

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

OTX est une plate-forme de sécurité informatique participative.

- Elle compte plus de 180 000 participants dans 140 pays partageant quotidiennement plus de 19 millions de menaces potentielles.
- Utilisation libre sans contrepartie.

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.

Temp-mail.org

fakenamegenerator.com

generated.photos

Recherche personne :

- <https://whatsmyname.app/>
- <https://checkusernames.com>

Outils E-mail tracking :

- Simple email reputation
- Mxtoolbox
- EmailSherlock
- Isit phishing

Outils mot de passe :

- Intelligence x
- Dehashed
- thejavasea.com
- BugMeNot
- ‘;-- have i been pwned ?

Outils threat Intelligence Plateforme :

- MISP
- OPENCTI
- ThreatQuotient