

le cnam

Bretagne

Eric DUPUIS

`eric.dupuis@cnam.fr` `eric.dupuis@orange.com`

`http://www.cnam.fr`

Conservatoire National des Arts et Métiers
Chaire de Cybersécurité

Date de publication
13 décembre 2019



Sommaire

Sécurité opérationnelle

Lutte contre la menace

structure du cours

les métiers de la SECOPS

Contributions





Chapitre introductif de la Partie 3 du cours SEC 101 (VTI-INTRO) -oOo-

Après avoir construit une structure de sécurité cohérente sur les aspects de gestion des flux, de gestion des accès et des identités, et construit une gouvernance efficace sur la base de l'ISO27001, il est nécessaire maintenant de maintenir le niveau de sécurité de l'entreprise ou du système. On appelle quelque fois ce processus le « Maintien en Condition de Sécurité » que nous pourrions positionner dans le RUN en utilisant les termes anglo-saxons définissant le cycle des projets :

- **THINK/DESIGN** : Des risques évalués à la politique sécurité pensée ;
- **BUILD** : De la politique de sécurité déployée à la construction d'une sécurité implémentée ;

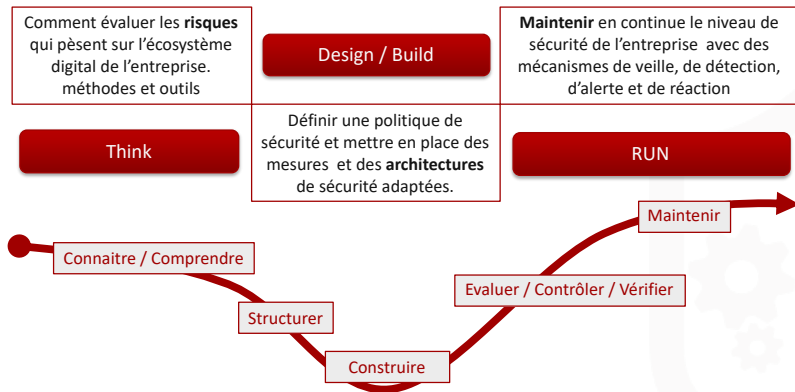


FIGURE – les phases du cycle de vie

Et nous classons donc dans la dernière phase du cycle de vie : les activités d'exploitation de la sécurité, **RUN** : Des évènements de sécurité gérés à une



cybercrise maîtrisée, que que certains appellent **SECOPS** : « Sécurité Opérationnelle ».

Ce modèle se développe bien entendu en fonction des finalités de l'entreprise.

- Soit nous sommes dans **une entreprise** et ces processus sont ceux mis en place pour s'assurer que l'ensemble de actions sont prises pour maîtriser les fragilités dont les vulnérabilités informatiques, détecter les menaces tant en anticipation que pendant des attaques (bruyantes, ou discrètes), et réagir pour maintenir l'activité et limiter l'impact.
- Soit nous sommes **fabricant d'un produit ou d'un service**, et au delà des engagements sécuritaire de toute entreprise (cf. ci-dessus) des processus de « maintien en condition de sécurité » des produits et services sont à ajouter pour maîtriser les vulnérabilités, les correctifs et leur cycle de vie (audit, communication, gestion des découvertes de fragilités par des tiers, rémunération de BugHunters ...)

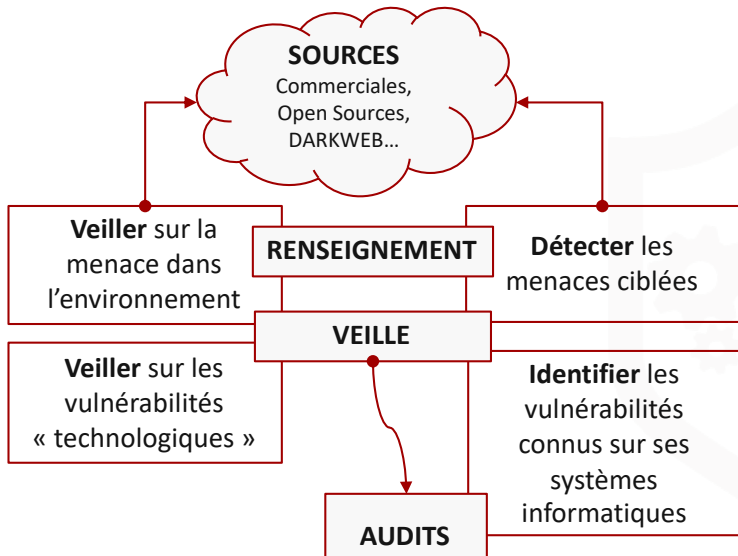


Sécurité opérationnelle

Une définition

Le terme de « sécurité opérationnelle », est relativement jeune dans l'histoire de la sécurité des technologies de l'information. Le terme de SSI (Sécurité des Systèmes d'Information) était né pour distinguer des disciplines qui s'attachaient à protéger l'information qui circulent dans les systèmes d'information de l'entreprise (cf. protection et classification de l'information) vis à vis de la sécurité des biens et des personnes. La sécurité des réseaux et la sécurité informatique ont été les précurseurs de la cybersécurité, le cyber recouvrant en un seul terme, les enjeux de sécurité liés au réseau et à l'informatique, mais plus largement à la sécurité de l'économie numérique.







Comme nous l'avons abordé, dans les chapitres précédents, la cybersécurité est un domaine vaste qui regroupe de nombreuses disciplines pouvant intervenir dans des cycles projets pour construire des systèmes sûrs et pour assurer la continuité d'activité et la protection des patrimoines dans l'entreprise. Il faut y ajouter aussi tout un espace de gestion des conformités (legislatives, réglementaires, normatives, contractuelles). C'est plutôt dans un contexte d'opération sécurité au quotidien que l'on parle de sécurité opérationnelle. Ces activités opérationnelles supportent donc le maintien en condition de sécurité au quotidien de l'entreprise. En France, au sein des armées, on parle de lutte informatique défensive permettant de différencier les activités des Cyber-défense des activités de Cyber-protection. Ces activités sont à opposer à la lutte informatique « offensive » qui ne sera pas abordé dans ce cours car elle relève de prérogative des états et non des entreprises. Nous aurons toutefois l'occasion d'aborder le **Hackback**, dans le chapitre sur la réponse à incident. La sécurité opérationnelle ajoute par ailleurs à son périmètre de surveillance de l'intérieur de la zone de responsabilité de l'entreprise SI, réseaux sociaux, services cloud ...), celle extérieure à l'entreprise via des mécanismes de veille sur la menaces et de surveillance des compromissions potentielles. Nous pourrions évoqué l'image d'une cité où



« Les murs sont épais et solides, les douaniers sont aux portes de la cité, la police doit toutefois veiller à la sécurité des biens et des citoyens dans la ville, car certains sont néanmoins des brigands. Quand à l'armée, elle veille aux frontières du pays informée pas des agents à l'étranger ».

On traitera donc cette partie avec une équivalence dans les terminologies suivantes :





Plusieurs terminologies, une dynamique

- Maintien en condition de sécurité (MCS) ;
- Sécurité opérationnelle (SECOPS) ;
- Lutte informatique défensive (LID) ;
- Cyberdéfense au sens de la cyberdéfense d'entreprise (CYBERDEFENSE).





Le but de cette sécurité opérationnelle est d'être au coeur de l'action de la sécurité de l'entreprise. En effet, la sécurité de l'entreprise est une propriété multiforme. Elle est d'abord statique dans la mesure où elle correspond à un niveau de confiance dans l'environnement pour conserver la disponibilité, la confidentialité et l'intégrité de l'entreprise. Cette forme statique est souvent liée à la conformité de l'entreprise aux différents référentiels sécuritaires (ISO27000, GDPR, LPM, NIS ...), mais surtout aux objectifs sécurité de l'entreprise face à ses risques et aux exigences de sécurité des clients souvent inscrites dans des plans d'assurance sécurité (Cf. PAS). Elle est aussi dynamique car c'est aussi une propriété systémique qui mesure la capacité à anticiper les menaces, identifier les fragilités, détecter en temps réel les attaques et réagir à temps ou au pire disposer des capacités de revenir dans un état de fonctionnement compatible avec la survie de l'entreprise (Modes dégradés par exemple). Le système évolue, faisant apparaître ici et là de nouvelles fragilités, l'entreprise se transforme, vit, suscitant de nouveaux potentiels d'attaques. L'entreprise doit s'organiser pour disposer de fonctions opérationnelles adaptées et dédiées à cette activité. Ces fonctions nécessitent des savoirs, des savoir-faire et de l'outillage. C'est l'ensemble de ces techniques que nous allons tenter d'aborder dans ce document.



Globalement, on peut remarquer que le cycle de vie est à prendre dans le sens inverse de notre présentation. Dans les entreprises moins matures en gouvernance de la sécurité, la dynamique de cette sécurité opérationnelle est la première visible et opérée. Dans l'entreprise va réagir le, plus souvent dans une dynamique de réponse immédiate aux problèmes de sécurité sans pour autant investiguer plus avant dans les fragilités globales. Les mécanismes de cybersécurité sont donc construits dans une entreprise peu mature dans le sens suivant :

- Répondre aux incidents de sécurité, tenter de répondre à la question : « qui nous attaque et pourquoi » ;
- Améliorer les filtrages ;
- Couvrir les vulnérabilités découvertes ;
- Rechercher les vulnérabilités existantes dans le périmètre de responsabilité ;
- Anticiper les attaques ;
- Anticiper les risques informatiques ;
- Anticiper les risques sur l'information ;
- Anticiper la menace.



La finalité de cette défense d'entreprise est de lutter contre ces attaques qui ne sont pas qu'informatique. L'attaquant peut utiliser des scénarii utilisant de nombreux vecteurs qui peuvent utiliser des fragilités organisationnelles ou humaines. On peut dire qu'une attaque est une fonction complexe, qui peut viser ou utiliser de nombreux facteurs internes et externes à l'entreprise. Ces facteurs constituent ce que certains nomment l'environnement numérique ou digital de l'entreprise. Cet environnement est globalement constitué de l'ensemble des outils, services, moyens informatiques ou réseaux utilisés par l'entreprise. Mai 2017 a été un tournant dans la prise de conscience de la menace de la part des entreprises. Le Rançon-logiciel WannaCry a plus fait trembler les médias que les entreprises, mais a permis de faire comprendre au grand public les enjeux des menaces informatiques.

(Paramètres d'une attaque)

$$\text{Attaque} = \text{Fonction} [\text{Fragilités HOT Entreprise} \otimes \text{Gains Escomptés PF}] \quad (1)$$

- Fragilités HOT : Humaines, Organisationnelles, Techniques
- Gains pour l'attaquant Idéologiques Politiques, Financiers, ...



On peut noter quatre grandes classes d'attaques informatiques¹ :



1. La majorité des attaques élémentaires peut être rangée dans ces classes



Grandes typologies des attaques numériques

- Attaques **d'interception** d'information, vols par écoutes passives ou actives dans les flux transitant entre un émetteur et un récepteur ;
- Attaques par **déni de services**, généralement sur le réseaux : Ce type d'attaque est un atteinte à la DISPONIBILITE du système, basé souvent sur la saturation d'une capacité de traitement. Le système saturé dans l'exécution de certaines de ses fonctions, ne peut plus répondre aux demandes légitimes, car il est occupé à traiter d'autres sollicitations ;
- Attaques par **exploitation de failles** logiciels : Ce type d'attaque va utiliser une vulnérabilité, d'un système d'exploitation ou d'un logiciel pour exécuter du code malveillant. Ce code réalisera alors sa mission ;
- Attaques par **exploitation de défauts** de configuration : Ce type d'attaque utilise simplement un ou des défauts de configuration pour que légitimement l'agresseur puisse dérouler un scénario, qui pourra lui donner par exemple des droits particuliers pour conduire des attaques.



Nous pourrions remarquer que ce nombre est relativement faible. Toutefois, la vraie difficulté réside dans la multiplicité des vulnérabilités, et des défauts de configuration. Les développeurs réalisent des logiciels possédant des failles (vulnérabilités), les utilisateurs ou les administrateurs déploient des systèmes en faisant des erreurs de configuration, ou ne les configurent que très rarement en pensant à la malveillance.

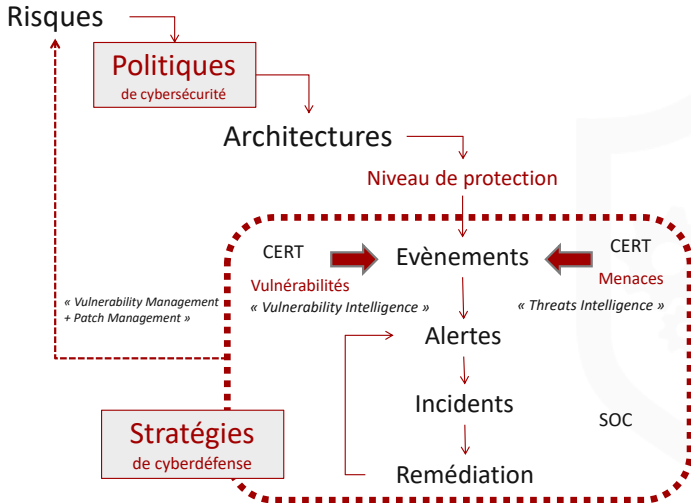
Les motivations des attaquants sont nombreuses, et leurs objectifs variés :

- obtenir un accès au système pour s'y maintenir en attendant une opportunité ;
- récupérer de l'information, secrets, données personnelles exploitables (en gros toutes les informations ayant de la valeur) ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler, couper, bloquer le fonctionnement d'un service (les rançongiciels entrent dans cette catégorie) ;
- utiliser le système d'un utilisateur, pour rebondir vers un autre système ;
- détourner les ressources du système d'un utilisateur (utiliser de la bande passante, utiliser de la capacité de calcul) ;



Bien entendu, il n'y a que très rarement un seul objectif, c'est la combinaison des méthodes d'attaques, des objectifs unitaires qui définissent globalement une mission ou un objectif final. L'exploitation de vulnérabilités au sein de l'entreprise va permettre le déploiement par l'attaquant d'un scénario.







A partir des risques identifiés, l'entreprise a posé des politiques de sécurité qui ont permis de mettre en place des mesures de sécurité. Ces mesures sont d'ordre techniques avec des systèmes de sécurité, ou des SI avec des architectures particulières, mais aussi d'ordre organisationnel avec des procédures et des mécanismes à respecter. L'ensemble de cette dynamique construit un niveau de sécurité qu'il va être nécessaire de maintenir dans le temps. Toutefois ce niveau de sécurité n'est pas suffisant pour une simple et bonne raison : la menace évolue, les vulnérabilités apparaissent (découvertes, ou créées), la valeur « marchande » des actifs d'une entreprise change aussi. Les occurrences de ces éléments de vie sont considérés comme des événements qu'il convient de détecter avec suffisamment d'avance sur l'attaquant pour pouvoir le plus rapidement les prendre en compte. La gestion des événements qui peuvent être une source de mesure de l'évolution du niveau de sécurité de l'entreprise est au cœur des stratégies de cyberdéfense. Ces événements sont corrélés avec des sources provenant de deux processus particuliers qui seront décrits dans ce document.

- Recherche des vulnérabilités : Processus qui permet de rechercher, découvrir, couvrir les vulnérabilités ou fragilités de l'entreprise ou ayant un impact sur l'entreprise que celles-ci soient techniques, humaines ou



organisationnelles ;

- Prévention de la menace : Processus qui permet de connaître les menaces directes sur l'entreprise ou potentielles afin d'anticiper et/ou se préparer à un type d'attaque.

C'est la confrontation entre les vulnérabilités, les menaces et la détection de l'activité de l'entreprise qui va permettre d'être efficace dans le processus de réponse. Il y a de nombreuses manières d'aborder la cybersécurité d'entreprise. Ce document présente donc une dynamique de cybersécurité en trois « volets » :

- Gestion des vulnérabilités (*Vulnerability Management and CERT*) : maîtriser ses vulnérabilités mais aussi surveiller l'environnement technologique.
- Surveillance, Détection de la menace (*Event and Threat Management*) : Analyser en temps réel l'environnement protégé mais aussi surveiller l'écosystème lié à la menace pour anticiper
- Gestion des incidents et réponse aux incidents (*Incident Response – CSIRT*) : Réagir en cas d'incident et assurer la remédiation

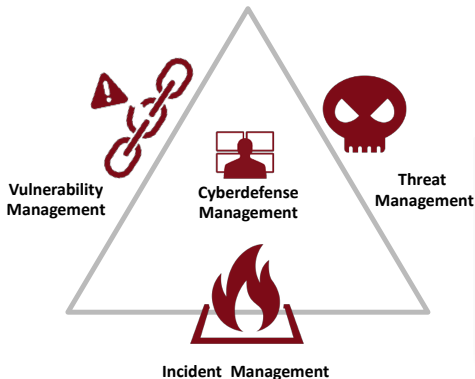


FIGURE – Des 3 des volets de la sécurité opérationnelle

Ces trois volets ne sont pas les seuls qui concourent à la cyberdéfense d'entreprise, mais ils en restent les trois faces principales. Il est à noter que ces



trois volets correspondent aussi en France à trois référentiels de qualification de l'ANSSI des prestataires de services de cybersécurité au profit des entreprises. Ces labels sont obtenus par les entreprises qui respectent un cahier des charges rigoureux sur le plan de l'éthique, du professionnalisme, et de la compétence des experts intervenants. Il y a trois cadres principaux de certifications sont :

- PASSI : Prestataire d'Audit de la sécurité des systèmes d'information ;
- PDIS : Prestataire de détection d'incident de sécurité ;
- PRIS : Prestataire de réponse à incident.

Ces trois référentiels définissent l'ensemble des exigences d'assurance pour « qualifier » des prestataires de services en cybersécurité sur ces trois thématiques. En effet, il serait en effet important de confier la recherche de ses vulnérabilités, leurs remédiations à des sociétés de confiance.

A ces 3 volets il ne faut pas oublier, le volet administration des briques informatique et de télécommunications de l'environnement de l'entreprise. C'est un volet que nous traiterons pas directement dans ce document pour se concentrer sur les mécanismes de maintien en continue le niveau de sécurité



Stratégies de l'action

de l'entreprise avec des mécanismes de veille, d'alerte et de réaction.

La cyberdéfense est un ensemble de mécanismes liés à une stratégie de l'action. Les outils de cyberdéfense sont construits pour aider à surveiller l'environnement, détecter des menaces et/ou des attaques mais surtout agir et réagir pour limiter les impacts. Si les outils de protection sont configurés à partir d'éléments de politique de sécurité (droits, accès, filtrage ...), les outils de défense sont basés sur les stratégies des attaquants. On distinguera donc ici trois grands mécanismes de Cyberdefense que les anglo-saxons appellent :

- Predictive Cyberdefense
- Active and Proactive Cyberdefense
- Reactive Cyberdefense



Nous aborderons, en particulier ces concepts quand nous évoquerons la notion de SOC (Security Operational Center) activité qui opère ce volet de cyberdéfense.

Il ne faut pas, par ailleurs, oublier le renseignement (*Intelligence*), qui reste une des grandes étapes de la cyberdéfense domaine que nous explorerons sous son volet cyber avec les sources de « threat intelligence », mais aussi avec le Renseignement d'Origine Cyber que les anglo-saxons nomme « intelligence cyber »

Dans les grandes organisations une autre stratégie globale de la cyberdéfense est de penser l'anticipation et la détection de manière globale à l'environnement digital de l'entreprise mais de structurer, la réaction de manière locale.

Nous avons positionné l'audit technique comme une des activités fondamentale de la gestion des vulnérabilités. En effet les techniques d'audit font partie des méthodes de référence pour disposer d'un état des fragilités de l'entreprise. On y trouvera donc les grands basiques des audits techniques que sont les tests d'intrusion, la sécurité applicative, l'audit de configuration, et le fuzzing.

Par ailleurs nous explorerons rapidement, les techniques de déception et de



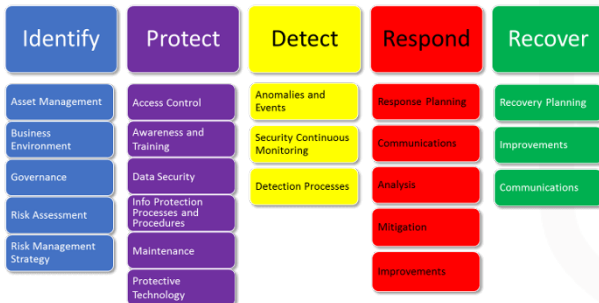
leurre qui font partie cette défense proactive avec les honeypots qui peuvent être couplés avec le *cyber-hunting*, technique de chasse aux codes malveillants dans l'entreprise.

Il existe de nombreux modèles de description de l'activité de Cyberdéfense dans un contexte de cybersécurité. Certains sont totalement intégrés au modèle de cybersécurité comme l'ISO 27K, ou le Cybersecurity Framework du NIST (Voir fig. 5 page 27) avec les activités **DETECT, RESPOND et RECOVER** ;





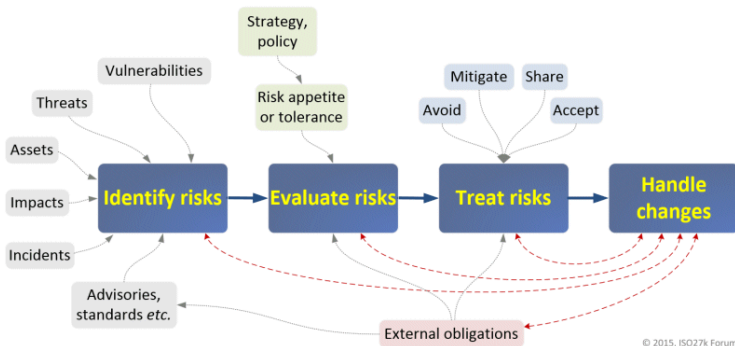
NIST Cyber Security Framework





Ce que l'on peut reprocher au modèle du NIST, c'est qu'il ne possède pas explicitement la gestion des fragilités / vulnérabilités, mais il apporte toutefois un modèle très détaillé, que nous utiliserons pour partie.
Dans l'environnement ISO 27000, le modèle est piloté par les risques (Voir fig. 6 page 29).







Nous avons fait le choix de positionner la présentation du volet sécurité opérationnelle en nous éloignant un peu des modèles pour présenter les 3 grands moteurs de la sécurité opérationnelle. En effet les modèles cités sont orientée sur un axe de cycle de vie. En sécurité opérationnelle ou cyberdéfense, l'objectif est de conduire en continue et de frond des processus de maitrise des risques cyber opérationnels.

- Les systèmes d'information évoluent en continue et des vulnérabilités peuvent s'insérer et/ou découvertes chaque jour au grès des modifications et évolutions,
- Des menaces se concrétisent quotidiennement par des attaques ciblées ou non, nécessitant de réagir vite et en cohérence avec des enjeux de l'entreprise
- Avoir la capacité de réagir, et d'assurer la continuité d'activité face à des attaques d'ampleur, ou à fort impact techniques ou médiatique.



Notre propos sera donc centré sur ces trois axes qui nous déclinerons dans trois chapitres. Le travail de fond d'une équipe de sécurité opérationnelle, ou simplement de l'activité SECOPS est de pouvoir gérer de front trois grandes tâches :





SECOPS en 3 thématiques

- maîtriser les fragilités numériques de l'entreprise (*Vulnerability Management*) quelles soient au sein du SI mais aussi dans l'environnement dit digital de cette entreprise (réseaux sociaux, partenaires, ...);
- anticiper les menaces et les scénarios associés (*Threat Management*), détecter les attaques et gérer au quotidien les événements de sécurité;
- réagir vite et en cohérence avec l'activité de l'entreprise en cas d'incident (*Incident Management*).



Nous aborderons aussi quelques compléments à ces processus SECOPS, comme la détection des fuites de données (Leak Detection), qui peut s'entendre comme un incident de sécurité externe, ou une détection d'évènement hors de périmètre du SI, mais dans le périmètre de surveillance.



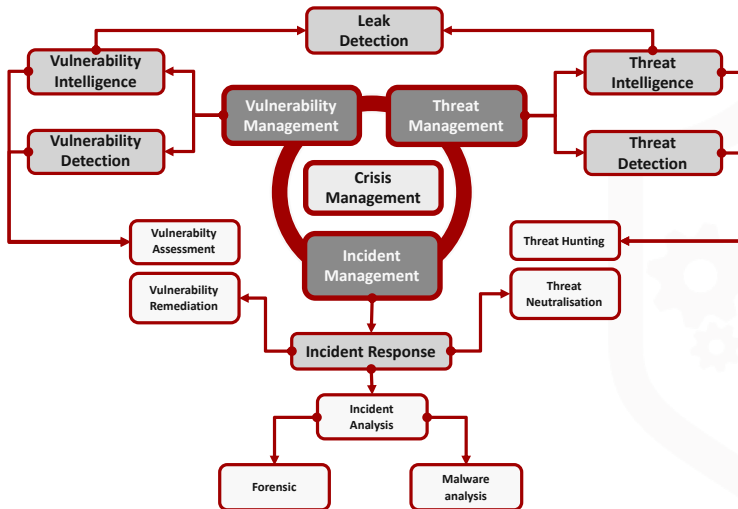


FIGURE – Synthèse des meta-processus SECOPS



Des activités qui nécessitent, pour être efficace, une symbiose parfaite entre les équipes qui gèrent l'activité digitale (Systèmes d'informations, réseaux sociaux, ...) et les équipes de sécurité opérationnelle.

Au delà des métiers de l'audit de sécurité qui existent depuis de nombreuses années, la sécurité opérationnelle est le champs de développement de nombreux métiers nouveaux ou en devenir. Nous en explorerons quelques-uns dans chacune des parties qui présentent les opérations de cette SECOPS.



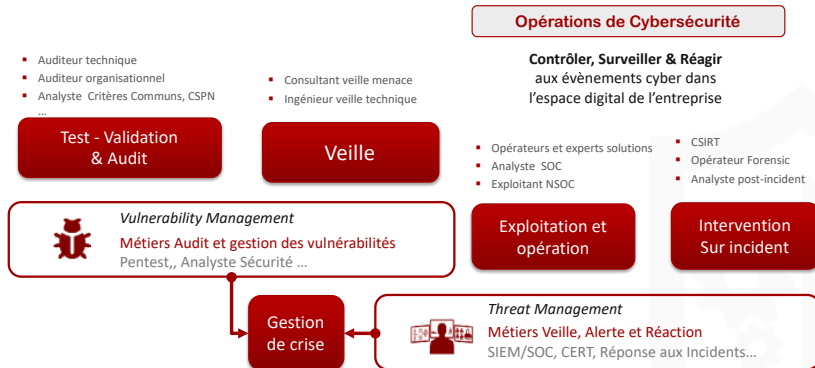


FIGURE – Des métiers SECOPS



Contributions

Les notes et les présentations sont réalisées sous $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$.

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.



Les fichiers sources sont publiés sur GITHUB dans l'espace :

(edufaction/CYBERDEF) ^a. Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes.

Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

a. <https://github.com/edufaction/CYBERDEF>