



SECOPS : Des événements de sécurité gérés à une cybercrise maîtrisée

Eric DUPUIS^{1,2*}

🕒 Résumé

Ce document introduit le triptyque de la partie cyberdéfense de la sécurité opérationnelle : Anticiper, Détecter, Réagir et ceci sur les trois grands invariants des risques numériques : les vulnérabilités, les menaces et l'impact. Il donne les grandes lignes des trois chapitres qui suivent.

Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document final unique.

Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel au cours.

🔑 Mots clefs

anticipation, veille, alerte, réponse

¹Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France

²RSSI Orange Cyberdefense

*email : eric.dupuis@lecnam.net – eric.dupuis@orange.com

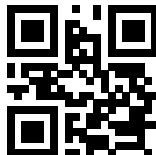
DRAFT NOTES S2 - 2020

Vérifiez la disponibilité d'une version plus récente de

SEC101-C3a-VTI-intro.doc.pdf sur GITHUB CYBERDEF ¹



2020 eduf@ction Publication en Creative Common BY-NC-ND



1. <https://github.com/edufaction/CYBERDEF/raw/master/Builder/SEC101-C3a-VTI-intro.doc.pdf>



1. SECOPS et cyberdéfense

Mettre en place des stratégies de cyberdéfense, c'est partir du principe que l'entreprise sera attaquée et que l'enjeu des équipes est de se préparer à des attaques pouvant violemment impacter l'entreprise. Pour cela, l'entreprise doit anticiper, détecter à temps et réagir vite pour réduire l'impact.

1.1 Des opérations de cyberdéfense d'entreprise

C'est dans ce contexte de sécurité que doit s'organiser cette cyberdéfense opérationnelle et se structurer autour des axes qui caractérisent une posture de cyberdéfense d'entreprise :

- ▶ Le renseignement :
 - sur les menaces : les attaquants et leurs intentions, leurs techniques et outils, les sources compromises,
 - sur les vulnérabilités : des logiciels, et des structures organisationnelles,
- ▶ La détection d'attaques ou de menaces dormantes ou cachées ;
- ▶ La mise en alerte, ou la réponse à incidents pour aller à la gestion de crise ;
- ▶ La neutralisation de sources malveillantes.

1.2 Veille et renseignement

Au cœur des opérations de cyberdéfense, le renseignement reste le moteur de l'anticipation. Une grande partie des attaques exploitent des failles ou des vulnérabilités. Être au plus tôt au courant de l'existence d'une vulnérabilité sur un système utilisé par l'entreprise est le premier stade d'une veille pour ANTICIPER une attaque potentielle basée sur cette faille.

Toutes les attaques ne sont pas liées à l'utilisation d'une faille technique, il existe d'autres marqueurs ou indicateurs qui peuvent être surveillés pour évaluer les risques. Nous verrons dans le chapitre sur la détection, que les marqueurs des menaces sont souvent des données techniques qui peuvent caractériser l'attaque, l'attaquant, les techniques utilisées... Par ailleurs le renseignement permet aussi de détecter des fuites de données, ou des informations sensibles compromises en surveillant les sites spécialisés. On peut citer le célèbre **'-have i been pwned?** ² qui indique si une adresse électronique utilisée comme identifiant de compte a été compromise lors d'un vol de données sur un site.

L'ensemble des informations liées aux menaces s'appelle de la *Threat Intelligence* ou *Cyber-Threat Intelligence (CTI)*, et celles liées aux vulnérabilités classées dans la dynamique *Vulnerability Intelligence*.

1.3 VTI

Le triptyque VTI (Vulnérabilités/Failles, Menaces/Attaques, Incidents/Alertes), est souvent présenté comme le cœur des activités de sécurité opérationnelle.

2. <https://haveibeenpwned.com>



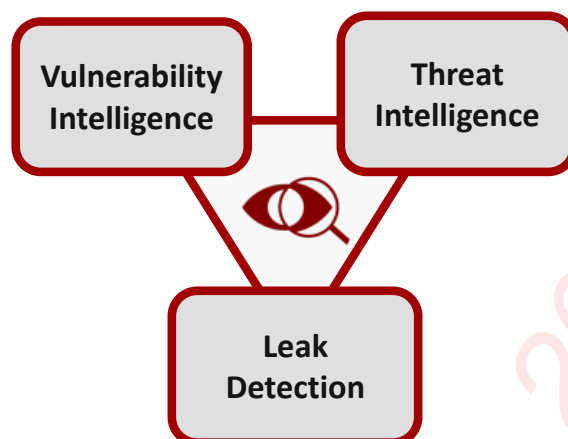


FIGURE 1. Les axes du renseignement cyber

La sécurité opérationnelle c'est l'ensemble des processus opérationnels qu'il faut mettre en place et évaluer au quotidien afin réduire la surface d'exposition du système d'information aux risques, mais aussi réduire l'impact en cas d'attaque.

On y trouve en particulier :

- ▶ Les audits techniques, pentest, scan : pour identifier, mais aussi la cartographie des actifs, des acteurs ...,
- ▶ Les systèmes de détection comme le SIEM, de chasse comme le Threat Hunting ...,
- ▶ Les mécanismes de remédiation, les techniques et outils de forensique.

Tous ces actions génèrent au sein de l'entreprise de l'information, souvent à destination d'acteurs différents mais participant globalement à l'objectif de cyberdéfense.

1.4 Fusion Center

Les préoccupations des responsables de cette sécurité opérationnelle restent encore l'accès et le partage de l'information car dans le cycle de gestion du risque et de réduction de la surface d'attaque. Le terme *Fusion Center* est historiquement liée au attentats au 11 septembre 2001, qui avaient montré les lacunes de partage de l'information entre les services de police et renseignements américains face à cette attaque. Repris par les experts de la cybersécurité, pour gérer les menaces La sécurité opérationnelle est gérée généralement par deux principales structures : le SOC, en charge de la détection, de la qualification et de la gestion des incidents ; et le CSIRT, responsable de la gestion de crise, de l'investigation numérique, de la veille et de la Threat Intelligence.

- ▶ Automatiser la **création de règles** basées sur des menaces avérées et détecter de manière avancée avec le *Machine Learning*
- ▶ Automatiser le **processus de management** des incidents avec en particulier les SOAR (Security Orchestration, Automation et Response) outils d'aide et d'automatisation de la réaction aux incidents de sécurité.



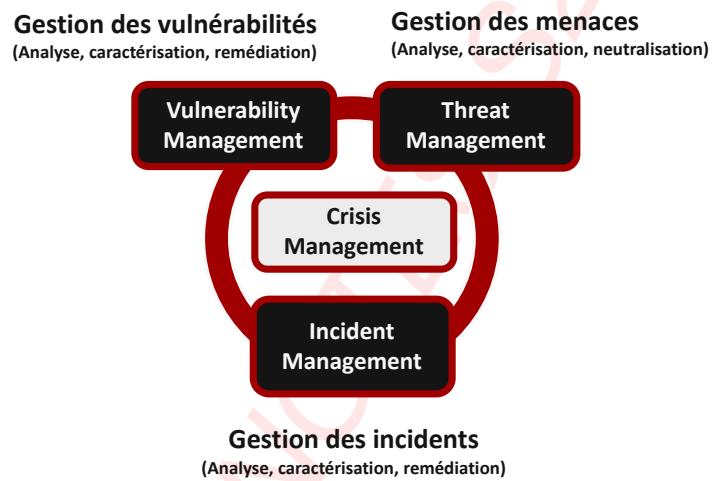


FIGURE 2. Les axes du renseignement cyber



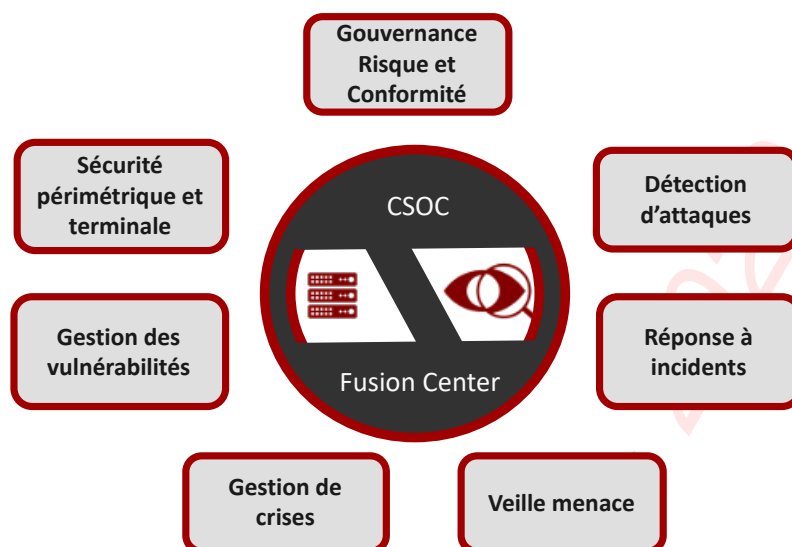


FIGURE 3. Fusion Center et CSOC

- Adapter l'**organisation** à cette automatisation
- et surtout automatiser la **collecte et la distribution** de l'information dans les différents services grâce à un « Centre de Fusion de l'information et du renseignement ».

1.5 Entraînement à la cyberdéfense

En matière de cybersécurité, les organisations sont confrontées à la persistance des cyberattaques, combinées à la montée en puissance de nouvelles menaces, ne sont pas suffisamment préparées à anticiper les incidents et à y apporter les réponses adéquates. De nombreuses études continuent à montrer que la formation du personnel demeure le défi premier, se traduisant par un investissement conséquent de la part des organisations.

L'entraînement répond à différents objectifs de l'entreprise :

- Sensibilisation des acteurs (salariés, décideurs, managers) aux risques « cyber ». Ces entraînements, relativement brefs et regroupant qu'une partie des acteurs permettent d'illustrer concrètement les menaces. Il permet en particulier de l'illustrer concrètement les impacts des cyberattaques sur une entreprise notamment pour les niveaux stratégiques ;
- Evaluation du dispositif de sécurité et de gestion de crise en particulier pour les évaluations autour des travaux de PCA/PRA avec l'ISO 22301. L'objectif est d'évaluer toute la chaîne opérationnelle, des équipes techniques informatiques et sécurité, aux top management sur l'ensemble de structures de la résilience ;
- Entraînement des équipes techniques, par exemple au sein des SOC (Security Operation Center). Cela suppose de s'appuyer sur des environnements de simulation informatique représentatif de la réalité pour s'adapter à l'évolution des attaques (Outils de Range en particulier) ;

Pour répondre à ces besoins, trois niveaux d'entraînement doivent donc être distingués :



- ▶ Des entraînements techniques au niveau des opérations. Ces entraînements peuvent intervenir dans le cadre de formations des équipes ;
- ▶ Des entraînements managériaux ou niveau des managers de proximité ou des COMEX. La durée de ces entraînements dépend des objectifs de montée en compétence. Pour une sensibilisation de COMEX, la durée doit être adaptée et courte (de l'ordre d'une demi journée). Les entraînements ou exercices peuvent/doivent être réguliers, une fréquence d'exercice annuelle est recommandée.
- ▶ Des entraînements mixtes associant des populations techniques et non techniques, afin de traiter l'inter-dépendance des différentes structures engagées.

1.6 Gestion de crise

Les opérations de sécurité opérationnelle doivent embarquer le processus de gestion de crise de l'entreprise, on trouvera dans le chapitre de gestion des incidents la manière donc les opérations de cybersécurité peuvent s'intégrer à des processus de gestion de crise existants ou comment créer des processus spécifiques à la cyber-crise. En effet, une des particularités des cyber-crises c'est que le système d'information et de communication peut lui aussi être compromis, et que la confiance dans les systèmes informatiques de gestion peut être altérée, ou ces systèmes totalement inopérants.

2. Range et Simulation

Les cyber-ranges, environnements de simulation informatique, dédiés non seulement à l'expérimentation des technologies, mais également à la formation par la pratique et à l'entraînement du personnel, constituent une réponse à l'enjeu de vision globale. Initialement développés dans un cadre militaire, les cyber-ranges intéressent aujourd'hui l'ensemble de l'écosystème de cybersécurité. Ils offrent des conditions d'entraînement proches du réel, tant dans les topologies réseau reconstituées que dans les technologies de sécurité déployées. Ils fournissent un environnement d'affrontement informatique permettant une nouvelle approche de la formation axée sur l'opérationnel.

Il existe de nombreux outils d'entraînements. La majorité sont construits sur des technologies de virtualisation. L'environnement de simulation technique est donc basé sur un « bac à sable » numérique (une sorte de pailleasse numérique) offrant notamment des capacités de :

- ▶ Virtualisation de postes de travail et de serveurs et de tout autres composants informatique ou réseaux. l'environnement de simulation informatique peut être « hybride » lorsqu'il permet également de connecter des équipements physiques (routeur, sonde, automate industriel...) ou des appliances ;
- ▶ Virtualisation des différents couches de transports, de stockage et de traitement (couche réseau pour les liens et les équipements, couches base de données et infrastructures de base : Annuaire, Infrastructure de gestion de clefs, ...) ;
- ▶ Création de scénarios pédagogiques ou de situation tactiques pour fournir des contextes d'entraînement et de formation ;



- Simulation et Génération de trafic pour donner de la vie au système.

L'entraînement est une solution pour dynamiser les activités de cyberdéfense.

CyberRange-Airbus



La CyberRange est utilisée par ses utilisateurs (administrateur, intégrateur, testeur, formateur) pour concevoir des réseaux virtualisés ou hybrides, émuler des activités unitaires comme des communications entre deux machines ou encore pour lancer des scénarios complexes reproduisant une activité réaliste (échange de fichier, email, trafic web et potentiellement de véritable cyber-attaques). CyberRange est disponible dans un caisson mobile, dans une baie ou accessible depuis un cloud.

⚙ Classe : **RANGE**, Site de référence : **CyberRange-Airbus** [↗](#)³

👤 Editeur : **airbus** 👁 Analyste : **eduf@ction**

Hynesim



hynesim, pour « HYbrid NETwork SIMulation », est une plateforme distribuée de simulation de systèmes d'information. hynesim est un ensemble logiciel s'appuyant sur des composants reconnus tels que Linux, Qt et libvirt. Grâce à une interface graphique simple d'utilisation (hyneview), mais néanmoins puissante, hynesim permet de simuler des réseaux complexes en seulement quelques clics. De plus les fonctionnalités hybrides de la plateforme offrent la possibilité de relier un réseau virtuel à des équipements réels.

⚙ Classe : **RANGE**, Site de référence : **Hynesim** [↗](#)⁴

👤 Editeur : **Diateam** 👁 Analyste : **eduf@ction**

3. <https://airbus-cyber-security.com/fr/produits-services/prevenir/cyberrange/>

4. <https://www.hynesim.org>



EDUYesWeHack



La plate-forme s'adresse aux promotions cybersécurité des écoles et université et plus largement à l'ensemble des promotions européennes en IT qui veulent accélérer le partage de jeux de données de qualité. L'approche pédagogique encourage d'abord l'émulation via la gamification et l'implication de chaque élève dans la sécurisation de son institution. Elle ouvre surtout des perspectives aux futurs développeurs vers des spécialisations porteuses telles que DevSecOps, Data Scientist, Security Analyst, etc. Enfin, YesWeHack EDU facilite la mise en place de projets collaboratifs et d'initiatives transversales entre les institutions académiques et le secteur privé.

Disponible partout en Europe, la plateforme YesWeHack EDU s'inscrit dans la ligne de l'initiative du consortium SPARTA, dont YesWeHack est un des membres fondateurs, qui vise à renforcer l'innovation et la recherche en matière de cybersécurité au niveau européen.

🔧 Classe : **RANGE**, Site de référence : **EDUYesWeHack** ⁵

👤 Editeur : **YesWeHack** 👁 Analyste : **eduf@ction**

Sur le plan humain, l'utilisation d'un cyber-range se construit autour de deux équipes que nous explorerons dans les chapitres sur la gestion des vulnérabilités et la gestion des menaces :

- ▶ La « Red-Team », composée de hackers éthiques professionnels (les PENTESTEURS). Ceux-ci reproduisent des attaques ciblées et d'ampleur et de complexité croissante, de nature à challenger la défense tout au long de l'entraînement ;
- ▶ La « Blue-Team », chargée de la défense des réseaux et systèmes d'information (le SOC), qui est donc constituée des apprenants participant au programme d'entraînement ou de formation.

3. Sécurité opérationnelle

En terme de gouvernance, 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 de maintenir le niveau de sécurité de l'entreprise ou du système. La dynamique de sécurité de l'entreprise est en exploitation nécessite une organisation et des politiques orientés vers cette efficacité de l'anticipation, de la détection et de la réaction que nous avons présenté comme le volet cyberdéfense de la cybersécurité de l'entreprise.

Dans certains ouvrages ce processus est dénommé « Maintien en Condition de sécurité ». En utilisant les termes anglo-saxons définissant le cycle des projets, nous pourrions positionner ses activités dans la phase dite de **RUN**. Les autres phases en amont pouvant être définies comme :

- ▶ **THINK/DESIGN** : Des risques évalués à la politique sécurité établie en fonction des risques ;
- ▶ **BUILD** : De la politique de sécurité déployée à la construction d'une sécurité implémentée ;

Et nous classons donc dans la dernière phase du cycle de vie : les activités d'exploitation de la sécurité, **RUN** : Des événements de sécurité gérés à une **Cybercrise** maîtrisée, ce que certains appellent **SECOPS** :

5. <https://www.yeswehack.com/edu/>



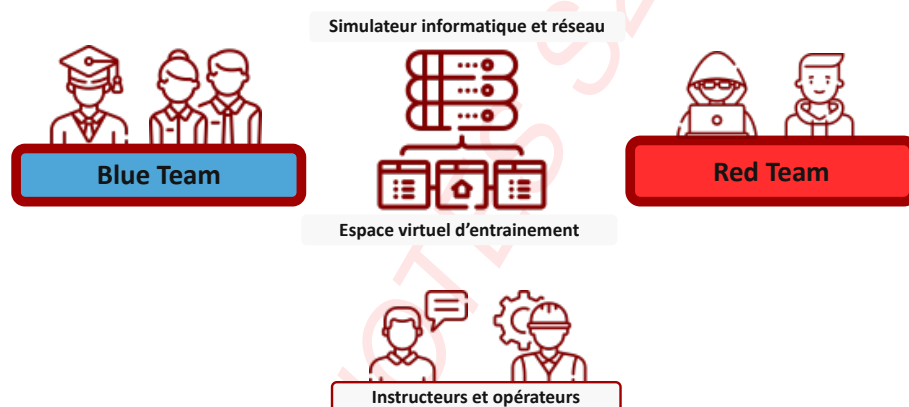


FIGURE 4. Entrainement



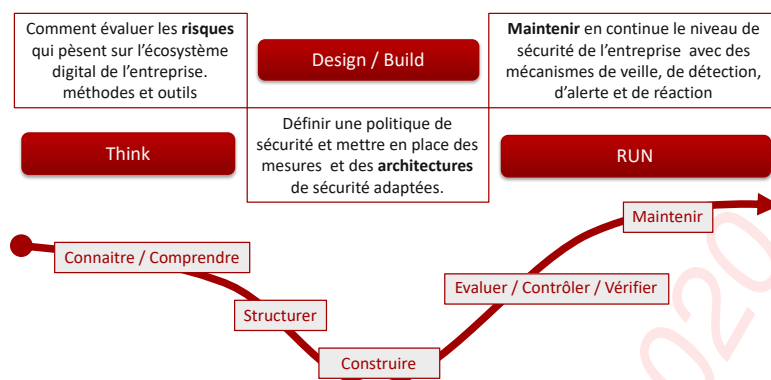


FIGURE 5. les phases du cycle de vie

« sécurité Opérationnelle ».

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

- Soit nous sommes dans **une dynamique entreprise** et ces processus sont ceux mis en place pour s'assurer que l'ensemble de actions sont pris 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 ...).

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 l'introduction et dans les chapitres précédents, la cybersécurité est un domaine vaste qui regroupe de nombreuses disciplines. Elle peuvent intervenir dans des cycles projets pour construire des systèmes sûrs ou pour assurer la continuité d'activité et la protection des patrimoines dans l'entreprise. Il faut aussi, penser à y ajouter aussi tout un espace de gestion des conformités (législatives, 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 :

- ▶ 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 immédiates 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.

4. Lutte contre la menace

La finalité de cette défense d'entreprise est de lutter contre ces attaques qui ne sont pas qu'informatiques. 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 :

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

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

On peut classer la majorité des attaques informatiques dans quatre grandes classes :

- ▶ 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 une 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.

4.1 Politiques et Stratégies

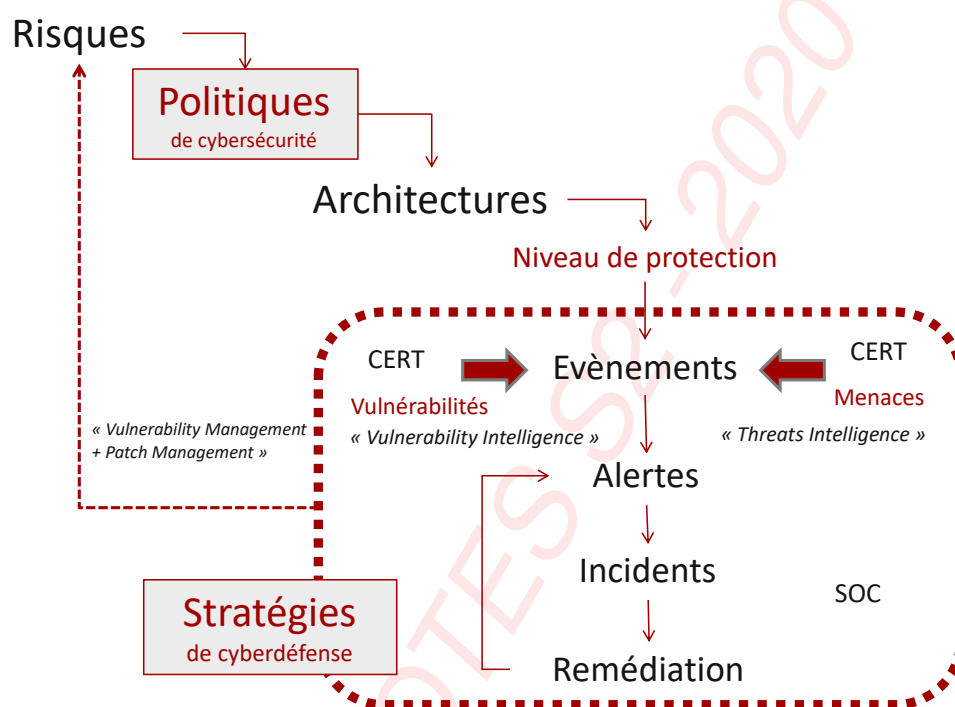


FIGURE 6. Positionnement de la sécurité opérationnelle

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.

Il est à noter qu'un attaquant ne raisonne pas en politiques d'attaque face à une politique de sécurité, mais par des stratégies auxquelles il faut opposer aussi par des stratégies de défense, dont

- 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 cyberdéfense d'entreprise.

Ce document présente donc une dynamique de cyberdéfense 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

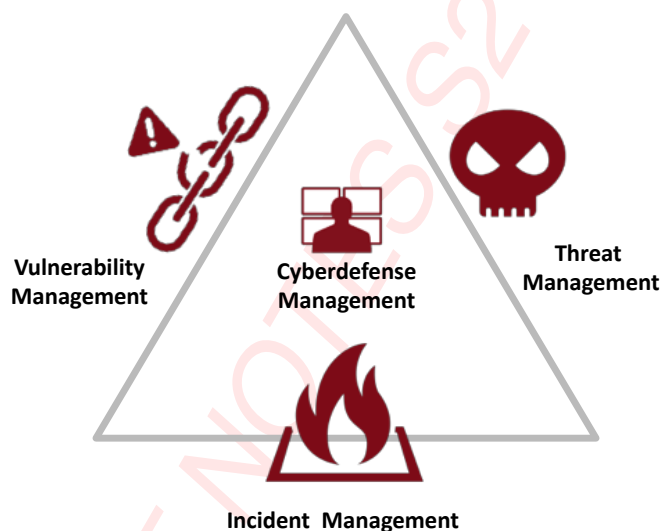


FIGURE 7. Des 3 des volets de la sécurité opérationnelle

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 :

- ▶ 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 trois volets il ne faut pas oublier, le volet administration des briques informatiques 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 de l'entreprise avec des mécanismes de veille, d'alerte et de réaction.

4.2 Stratégies d'action

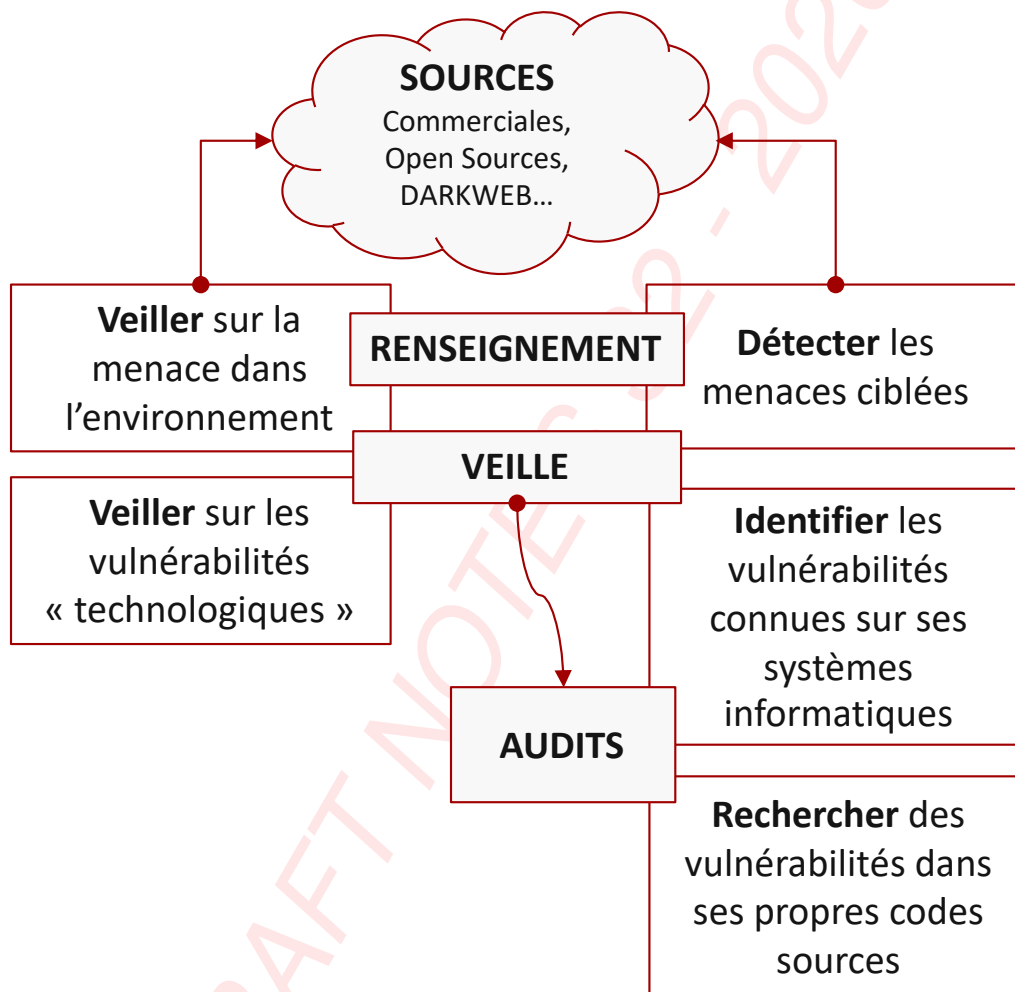


FIGURE 8. Les différentes actions de veille

La cybersécurité est un ensemble de mécanismes liés à une stratégie de l'action. Les outils de cybersécurité 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 Cybersécurité 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 mais la veille sur l'environnement numérique reste un axe important.

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 fondamentales 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.

4.3 Les modèles de cybersécurité

Les modèles ou framework de sécurité sont intéressants à plusieurs titres. Ils permettent en particulier, de disposer d'un ensemble d'exigences ou de bonnes pratiques organisées dans un référentiel connu et reconnu d'une communauté et offre un cadre pour :

- Passer en revue les pratiques des organisations en matière de cybersécurité ;
- Etablir ou améliorer son propre programme de cybersécurité ;
- Effectuer une auto-évaluation des risques en matière de cybersécurité ;
- Sensibiliser collaborateurs, partenaires, sous-traitants ;
- Améliorer la communication entre organisations grâce à un échange d'exigences cybersécurité entre les partenaires commerciaux, les fournisseurs et les régulateurs (ANSSI par exemple)

Il existe de nombreux modèles de description de l'activité de Cyberdefense dans un contexte de cybersécurité. Certains sont totalement intégrés au modèle de cybersécurité comme l'ISO 27K, ou le Cybersecurity Framework du NIST (Voir Framework du NIST fig. 9 page 17) avec les activités **DETECT, RESPOND et RECOVER** ;

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 l'bl-risk27 ?? page ??)

Nous avons fait le choix de positionner la présentation du volet sécurité opérationnelle en nous éloignant un peu des modèles pour présenter les trois 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 front des processus de maîtrise 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,



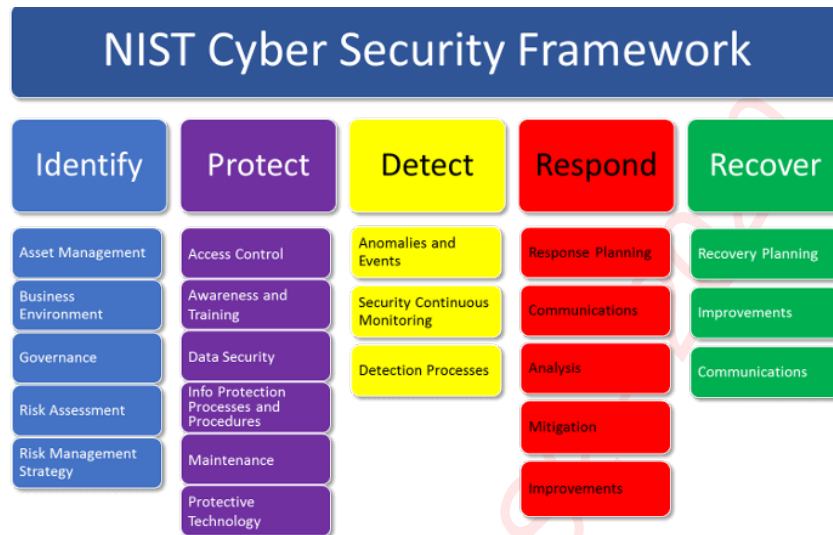


FIGURE 9. modèle NIST

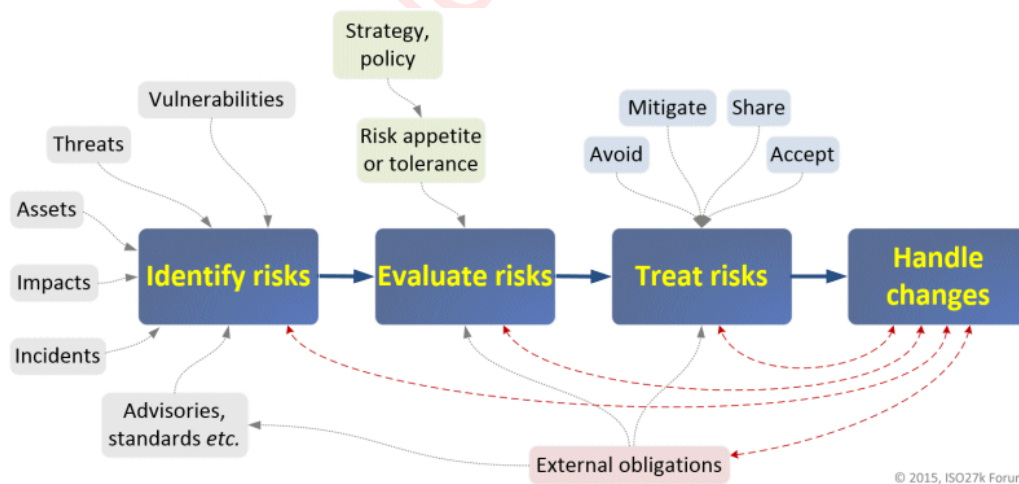


FIGURE 10. modèle ISO27 et risques



- ▶ 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.

DRAFT NOTES S2 - 2020



5. Processus SECOPS

Notre propos sera donc centré sur ces trois axes qui nous déclineront 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 :

- maîtriser les fragilités numériques de l'entreprise (*Vulnerability Management*) quelles soient au sein du SI ou 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'événements hors de périmètre du système informatique, mais dans le périmètre de surveillance.

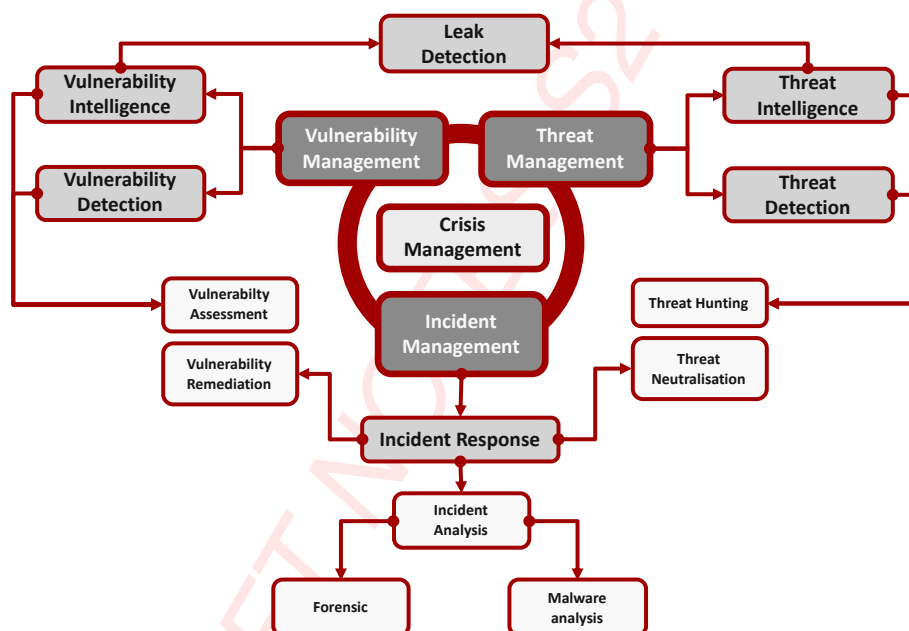


FIGURE 11. Synthèse des méta-processus SECOPS

Ces activités nécessitent, pour être efficace, une symbiose parfaite entre les équipes qui gèrent l'activité digitale (Systèmes d'informations, réseaux sociaux, communication...) et les équipes de sécurité opérationnelle. Il ne faut pas oublier bien entendu les mécanismes de gouvernance sécurité globale (ISO 27001 par exemple) dans lesquels s'inscrit la sécurité opérationnelle. On trouve souvent dans les entreprises un RSSI dédié cette activité relevant soit du RSSI de la DSI soit d'un DSSI (Directeur de la SS).

6. Les métiers de la SECOPS

Au delà des métiers de l'audit de sécurité qui existent depuis de nombreuses années, la sécurité opérationnelle est le champ 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.



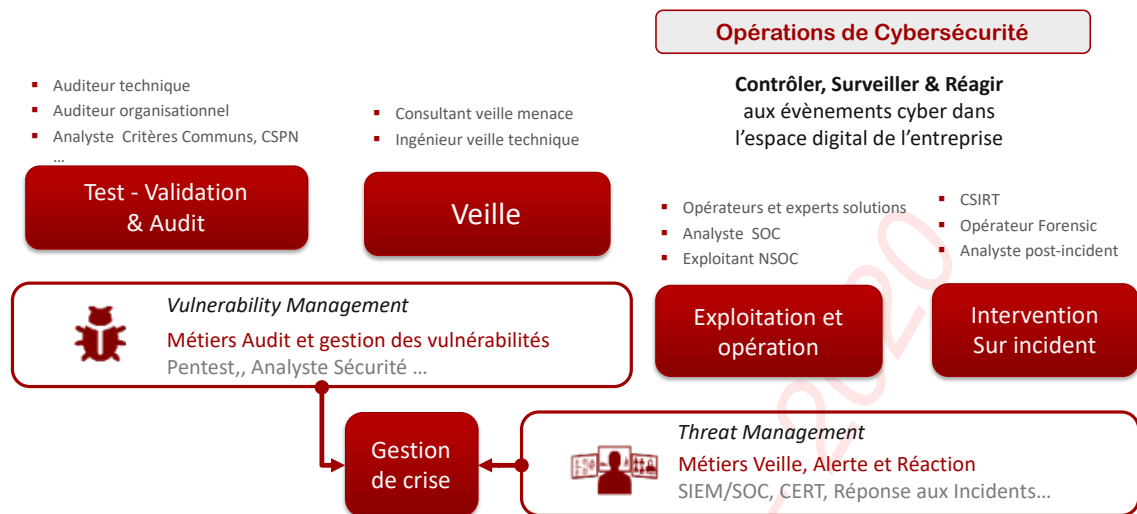


FIGURE 12. Des métiers SECOPS

7. Eléments Communs

Nous trouverez dans chacun des chapitres un petit condensé du processus avec :

- ▶ Les objectifs ;
- ▶ Les outils ;
- ▶ Les méthodologies et standards ;
- ▶ Les métiers et compétences.



8. Contributions

8.1 Comment contribuer

Les notes et les présentations sont réalisées sous \LaTeX .

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) [↗](https://github.com/edufaction/CYBERDEF)⁶. 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.

8.2 Les contributeurs/auteurs du cours

8.2.1 co-auteurs

(2019-2020) **David BATANY** - Cnam SEC101 : *Architecture et fonctionnement des Botnets*

8.2.2 contributeurs

(2020) **Celine JUBY** - Orange Cyberdefense : *Contributions d'amélioration et relectures*

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



Table des matières

1	SECOPS et cyberdéfense	2
1.1	Des opérations de cyberdéfense d'entreprise	2
1.2	Veille et renseignement	2
1.3	VTI	2
1.4	Fusion Center	3
1.5	Entraînement à la cyberdéfense	5
1.6	Gestion de crise	6
2	Range et Simulation	6
3	Sécurité opérationnelle	8
4	Lutte contre la menace	11
4.1	Politiques et Stratégies	13
4.2	Stratégies d'action	15
4.3	Les modèles de cybersécurité	16
5	Processus SECOPS	19
6	Les métiers de la SECOPS	19
7	Eléments Communs	20
8	Contributions	21
8.1	Comment contribuer	21
8.2	Les contributeurs/auteurs du cours	21
8.2.1	co-auteurs	
8.2.2	contributeurs	

Table des figures

