SECOPS : Des évènements de sécurité gérés à une cybercrise maitrisée

Eric DUPUIS[1,2]*

Résumé
Ce document introduit le triptype 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 suiv
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.

Mots clefs
anticipation, veille, alerte, réponse

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI 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-C3-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-C3-VTI-intro.doc.pdf

1. Sécurité opérationnelle

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 maintenant 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 l'efficience de l'anticipation, de la détection et de la réaction.

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 ;

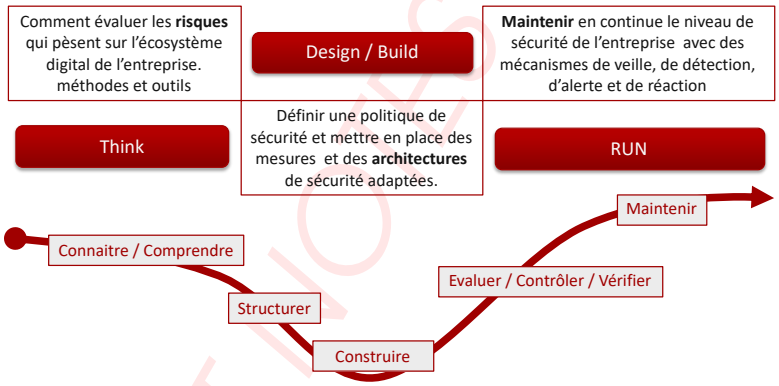

FIGURE 1. les phases du cycle de vie

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** maitrisée, ce que certains appellent **SECOPS** : « 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 soit pris pour maitriser 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

DRAFT NOTES S2 - 2020

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 différentier 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

DRAFT NOTES S2 2020

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 apparaitre 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 savoirs-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 a 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.

2. 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 scenarii 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

DRAFT NOTES 2020

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 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 vrai 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 un opportunité ;
- récupérer de l'information, secrets, données personnelles exploitables (en gros toutes information ayant de la valeurs)
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;

DRAFT NOTES 22 - 202

- troubler, couper, bloquer le fonctionnement d'un service (les rançongiciels entre dans cette catégories) ;
- 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.

2.1 Politiques et Stratégies

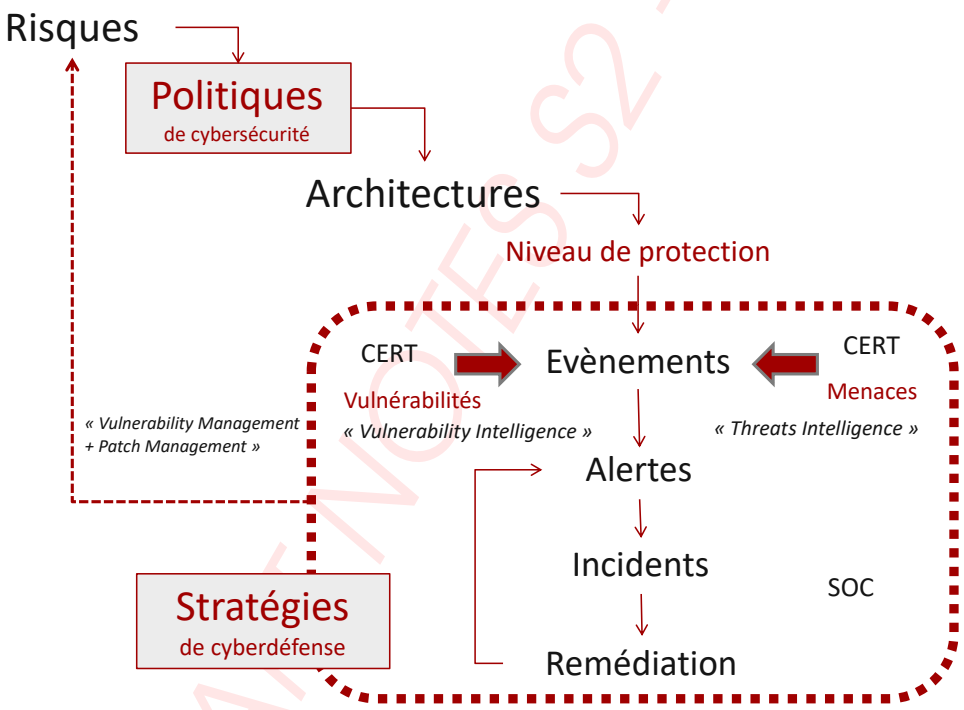

FIGURE 2. Positionnement de la sécurité opérationnelle

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 évènements qu'il convient de détecter avec

DRAFT NOTES S2 - 2020

suffisamment d'avance sur l'attaquant pour pouvoir le plus rapidement les prendre en compte.

La gestion des événements qui peuvent être un source de mesure de l'évolution du niveau de sécurité de l'entreprise est au coeur des stratégies de cyberdéfense. Ces évènements sont corrélés avec des sources provenant de deux processus particuliers qui seront décrit dans ce 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 connaitre 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 manière d'aborder la cyberdéfense d'entreprise.

Ce document présente donc une dynamique de cyberdéfense en trois« volets »

- Gestion des vulnérabilités (*Vulnerability Management and CERT*) : maitriser 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

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 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.

DRAFT NOTES S2 2020

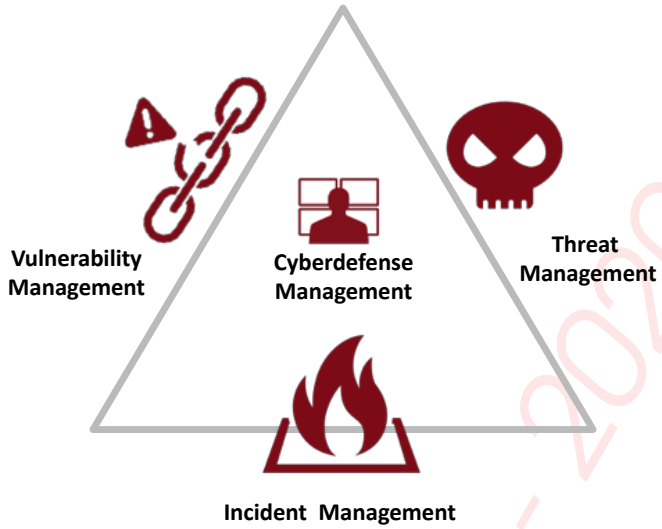

FIGURE 3. Des 3 des volets de la sécurité opérationnelle

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.

2.2 Stratégies d'action

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 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

DRAFT NOTES S2 - 2020

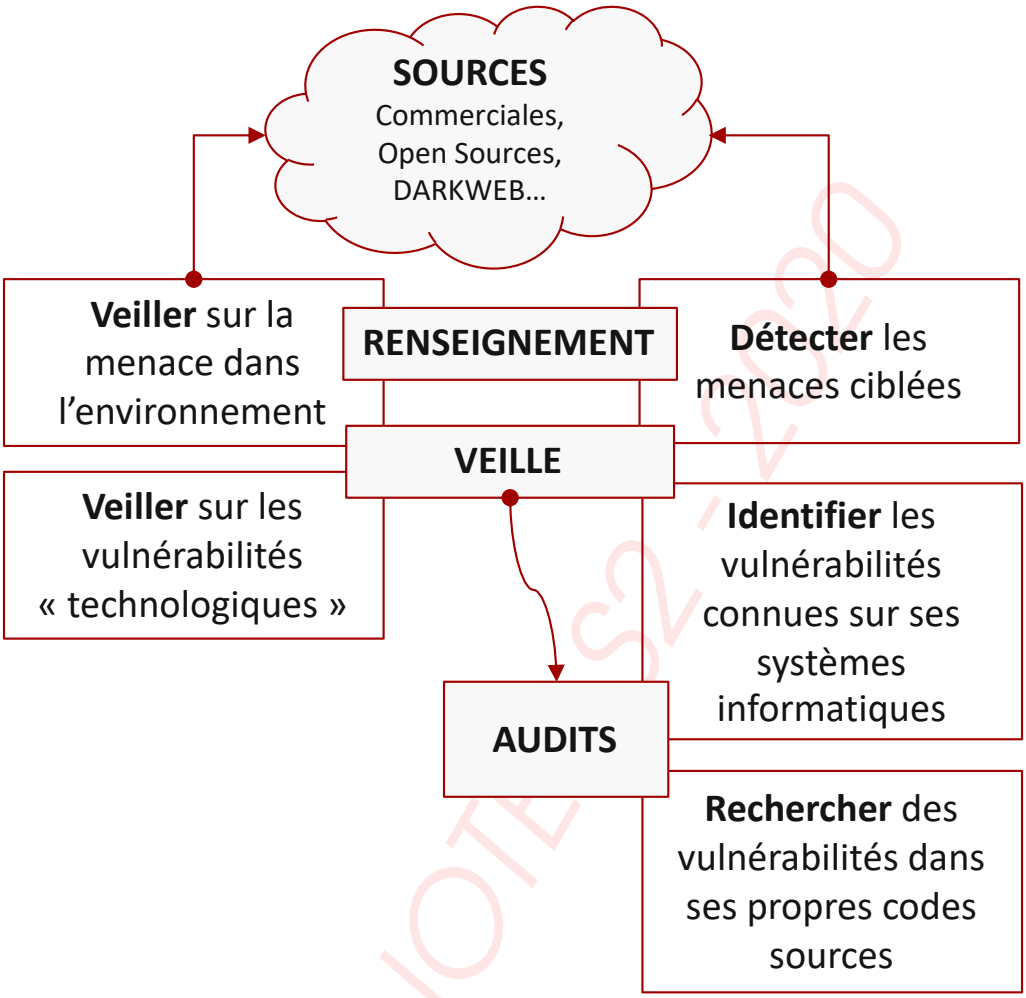

FIGURE 4. Les différentes actions de veille

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.

DRAFT NOTES 2 - 2020

2.3 Les modèles de cybersécurité

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. 5 page 10) avec les activités **DETECT, RESPOND et RECOVER** ;

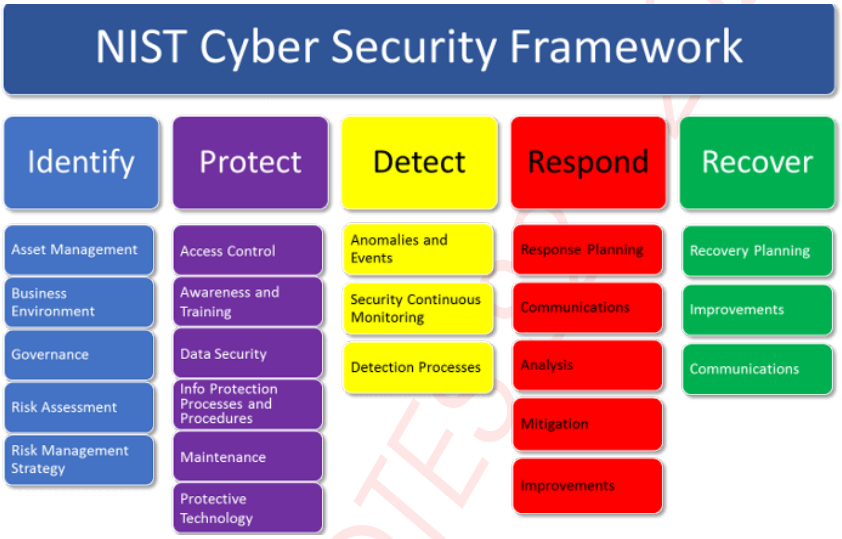

FIGURE 5. modèle NIST

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 lbl-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 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

DRAFT NOTES 2020

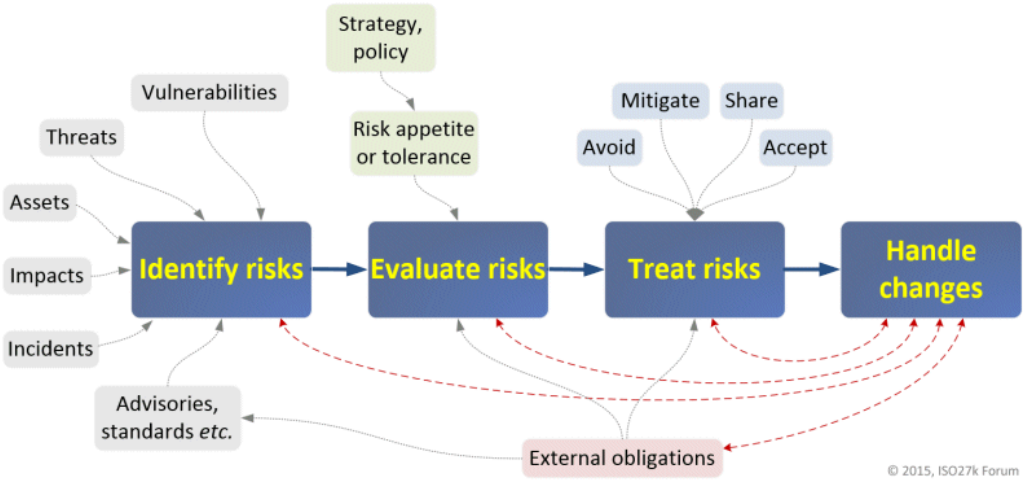

FIGURE 6. modèle ISO27 et risques

d'ampleur, ou à fort impact techniques ou médiatique.

DRAFT NOTES S2

3. Structure du cours

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 :

- maitriser 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'évènements hors de périmètre du système informatique, mais dans le périmètre de surveillance.

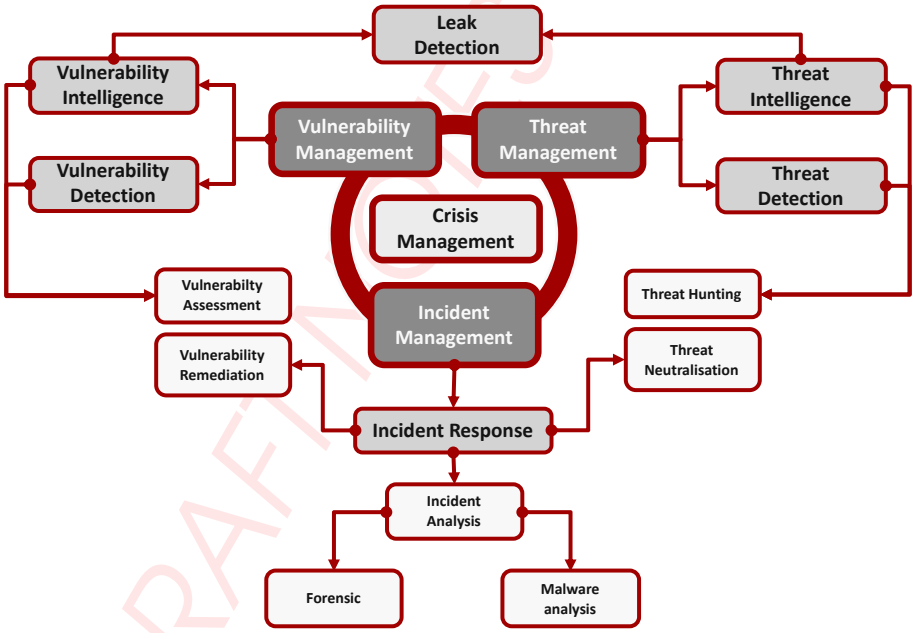

FIGURE 7. Synthèse des méta-processus SECOPS

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 SSI).

DRAFT NOV 2020

4. 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.

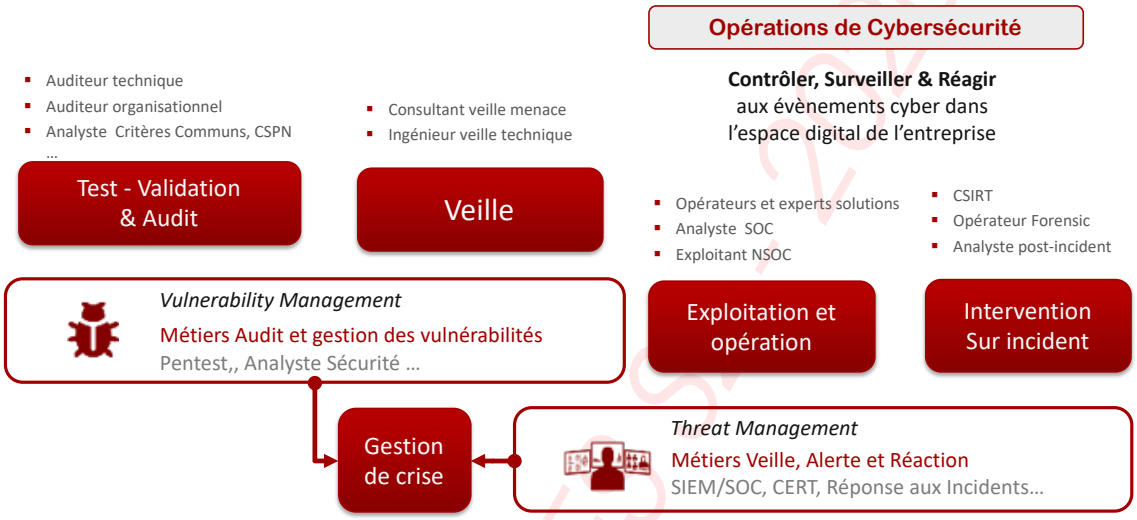

FIGURE 8. Des métiers SECOPS

DRAFT NOTES 2020

5. Contributions

5.1 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) [2] . 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.

5.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

5.2.1 Années 2020

- **David BATANY** (Contributeur LATEX) : BOTNET
- **Charly Hernandez** : User and Entity Behavior analytics, UEBA
- **Florian PINCEMIN (Orange)** : SIEM en quelques mots

5.2.2 Années 2019

- **François REGIS** (Orange) : CyberHunting

5.2.3 Années 2018

- **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

DRAFT NOTES S2 - 2020

2. https://github.com/edufaction/CYBERDEF

Table des matières

Table des figures

DRAFT NOTES S2 - 2020