1. Une synthèse des fondamentaux

Comme nous l'avons vu dans cette dernière partie, la sécurité opérationnelle en Cyberdefense est un ensemble d'actions élémentaires dont l'objectif est de maintenir le niveau de continuité d'activité de l'entreprise en assurant la découvertes des vulnérabilités et leur remédiation , la détection des attaques et la mise en vigilance des activités de l'entreprise, et la réaction à incident pouvant conduire à la gestion de crise.

A titre de synthèse des éléments présentés dans les chapitres précédents, je vous propose une synthèse très macroscopique des éléments à retenir.

Les actions des sécurité opérationnelle sont structurées autour d'axes fondamentaux opérés par des métiers différents avec des compétences diverses. Dans une entreprise de faible maturité, la réaction aux incidents est le premier corpus d'action de cyberdéfense. Que ce dernier soit organisé ou pas, l'entreprise fasse à un incident perçu et considéré comme grave pour l'activité économique devra ré-agir et agir.

Dans l'ordre logique de leur rencontre, les 3 grandes fonctions de cyberdéfense de cette sécurité opérationnelle sont :

- **Répondre** au plus tôt aux incidents de sécurité afin de limiter l'impact des attaques (Equipe et compétences en réponse à incident, in-forensique, analyse post-mortem, qualification PRIS de l'ANSSI).
- **Détecter** au plus tôt les tentatives d'attaques et les attaques en cours afin d'y répondre de manière adaptée en corrigeant si nécessaire les fragilités ayant été utilisées ; (Analystes en cybersécurité, SOC, outillage Logs, SIEM, Référentiel PDIS de l'ANSSI)
- **Rechercher** des fragilités connues, et détecter des vulnérabilités intrinsèques et les corriger avant qu'un attaquant ne les utilisent. (Auditeurs, Pentesteurs, base de vulnérabilités, référentiel PASSI de l'ANSSI)

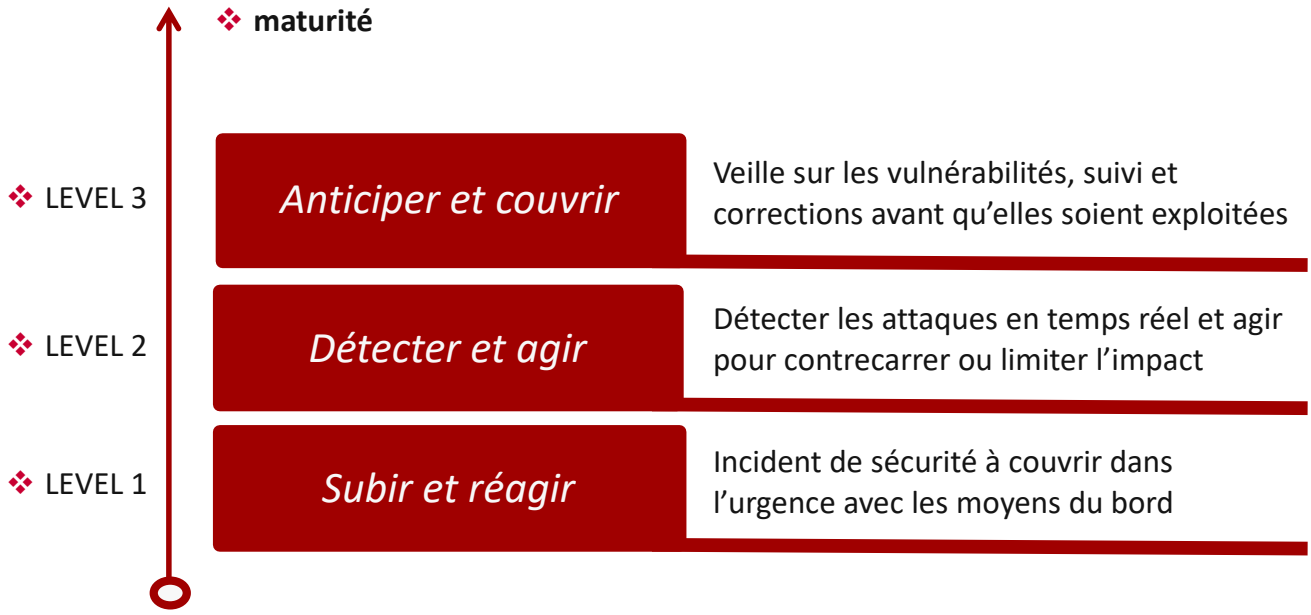

Figure 1. maturité et actions prioritaires

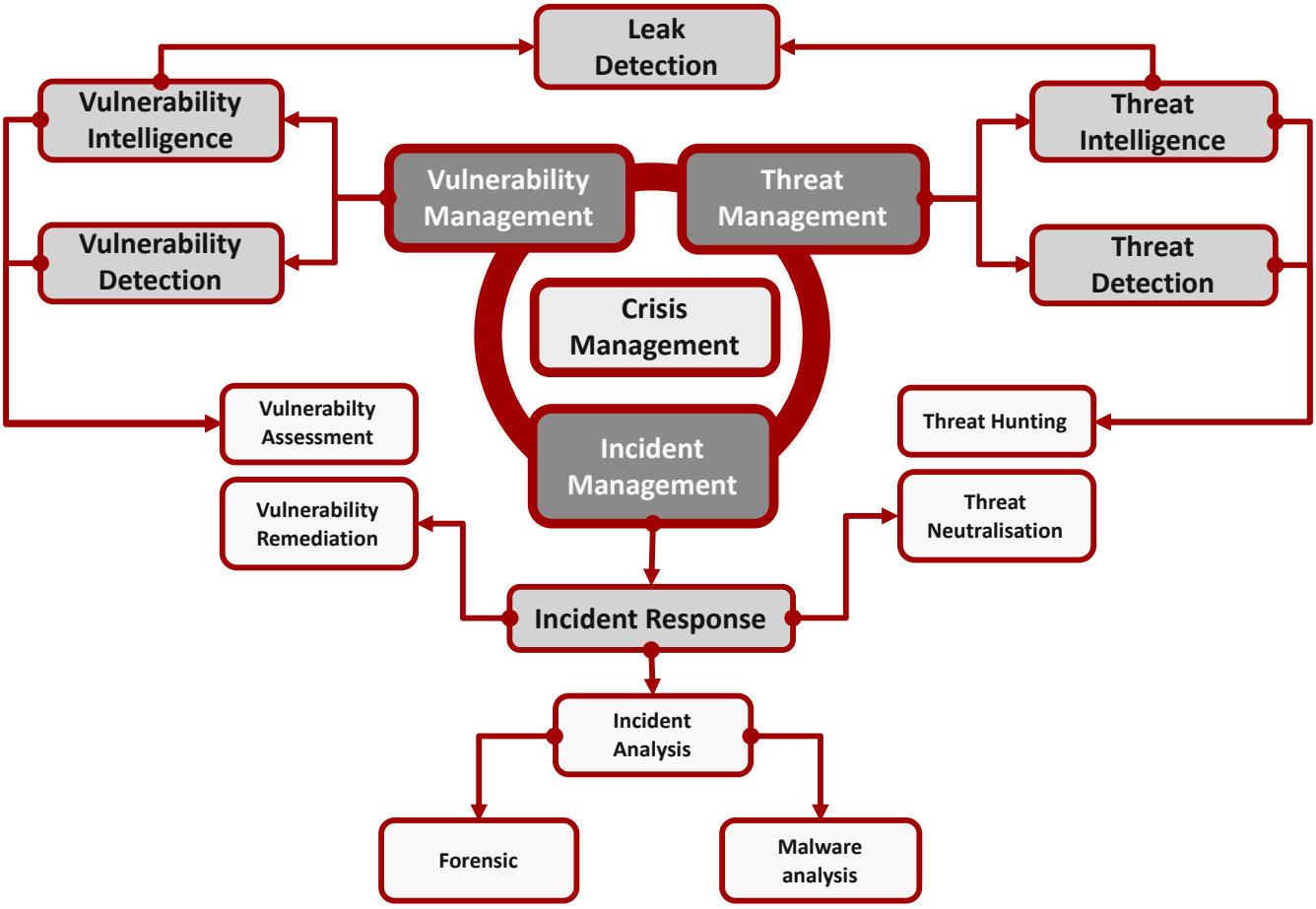

FIGURE 2. Eléments Secops

2. La réponse aux incidents

La réponse à incident est souvent la première activité qui est interpellée dans une entreprise. C'est aux équipes informatiques ou le cas échéant à un prestataire de service qu'incombe dans un premier temps le traitement de l'attaque. Généralement cette attaque est activité, et a concrètement déjà impacté le fonctionnement d'une partie de l'entreprise, ou si cela n'est pas directement le cas, le risque est élevé pour un impact non négligeable.

Les équipes informatiques doivent dont au plus tôt circonscrire l'attaque, déterminer les niveaux d'impact, les risques de propagation, et communiquer à l'environnement managerial les premiers impacts connus ou fortement probables. Par la suite le processus de réponse à incident pourra dérouler ses mécanismes, pour peu qu'il soit organisé et alerte.

A l'image d'un sinistre par le feux, les premières actions sauver ce qui doit l'être ou peu l'être dans le contexte de l'action (sécuriser les actifs) , sécuriser l'environnement pour le feu de se propage pas (limiter l'impact), éteindre le feu (circonscrire et bloquer l'attaque). Par la suite, il sera peut être nécessaire d'analyser les causes de l'incendie et d'identifier si le sinistre est intentionnel ou accidentel. Ves analyses sont plutôt du métier de l'enquêteur, sui se trouve le plus souvent du côté des forces de polices que des pompiers.

Les étapes du cycle de vie de la gestion d'incidents sont :

- **Caractériser** rapidement pour identifier les impacts (tout en continuant les investigations) ;
- **Répondre au plus tôt** pour limiter l'impact (tout en suivant les actions de remédiation et leurs effets) ;
- **Apprendre** de l'attaque (Analyse Malware, forensique, corriger les failles, corriger les postures et mécanismes de réaction) ;
- Mettre en place de nouvelles « contre-mesures », et rapidement adapter les processus de détection ;
- **Orienter ses capteurs** vers les menaces pour identifier si possible l'attaquant, et se préparer à d'autres actions de sa part ;
- **Neutraliser** les sources menaces avec les services spécialisés de l'état.

Il est important de pouvoir répondre aux incidents rapidement, avec efficacité avec une certaine forme de mode réflexe. Toutefois mettre en péril son entreprise à chaque attaque ou incident de sécurité et fonctionner en mode pompier n'est peut être pas la meilleure solution pour maintenir les équipes IT dans un fonctionnement normal et nominal. En effet tous les incidents, évènements ne sont pas du même niveau de gravité, et certain nécessite un analyse préalable afin de déterminer les forces à mettre en oeuvre pour couvrir l'incident. Il est peut être intéressant de regarder comment mettre. en oeuvre ces cyber-« vigiles » équipés de capteurs qui leur permettront de détecter et caractériser des alarmes et par la suite de préparer des interventions qui pourront aller jusqu'à l'activation d'équipes spécialisées.

3. La détection des attaques

La détection de l'attaque est au coeur du quotidien d'un ingénieur SECOPS, toutefois la veille sur la menace dont l'attaque est la concrétisation doit rester au coeur des préoccupation de la gestion des risques. C'est entre ce deux processus que se dessinne les scénario que l'on cherche à détecter. L'adage qui dit que l'on ne trouve que ce que l'on cherche, semble encore beaucoup fonctionner. L'anticipation grace au renseignement acquis par des outils de veille associée à des mécanismes de

remontées d'alertes de menaces peut permet de mettre les équipes SOC dans un état de vigilance (Etat d'alerte). L'ensemble de ces processus est dénommé **« THREAT MANAGEMENT »** .

Dans une activité normale, il y a généralement de nombreux évènements qui permettent de déterminer les écarts de fonctionnement de l'IT de l'entreprise (Nouvelles applications, déviances comportementales, nouveaux utilisateurs, ...). Des équipes de surveillance et de détection d'incident sont à organiser pour assurer cette tache de veille continu, de caractérisation des alarmes et de déclenchement des alertes **« THREAT DETECTION »** Elles doivent :

- Disposer des outils permettant de **voir ce qui se passe** dans l'environnement numérique de l'entreprise (Interne sur son SI, externe sur ses partenaires, clients et fournisseurs), mais aussi surveiller l'écosystème technologique et l'environnement de menaces. (Log Management pour son SI, et Veille sur l'externe) ; Ces outils doivent être alimenter d'informations, renseignements provenant de sources de **« THREAT INTELLIGENCE »**
- Disposer des moyens pour **détecter** dans les flots de données, d'informations, d'évènements les corrélations qui permettent de détecter la concrétisation d'une menace : une attaque (SIEM) ;
- Mettre en oeuvre les **mesures** d'analyse des évènements et de **remontée** des alertes au bon niveau de décision ;
- Disposer d'une équipe apte à **décider** ce qui doit passer mettre l'entreprise en alerte et engager une réponse à incident ;
- Disposer d'un ensemble de **compétences**, pour assurer la mise en place de nouveaux mécanismes, de **nouvelles règles** de détection face aux nouvelles menaces ou aux menaces spécifiques (SOC, expertises menaces).

4. La couverture des fragilités

Couvrir ou corriger ses vulnérabilités est certainement l'activité la plus visible de la gestion de sécurité opérationnelle. Elle fait appellent à toutes la panoplie des tests de sécurité dont l'objectif est de découvrir des fragilités Humaines, Organisationnelle, ou Technique qui permettent d'attaquer des actifs dans l'entreprise. Cette couverture des vulnérabilités s'organise autour d'un processus appelé **« VULNERABILITY MANAGEMENT »**

- Pentest, Bug Bounty, Fuzzing et autres techniques offrent un panel de métier dans le domaine de recherche et l'analyse des failles. La maturité des chaines de développement dans le domaine du logiciel est encore suffisamment faible pour que l'on continue à trouver des défauts de programmation connues conduisant à des vulnérabilités logicielles.
- La complexité des systèmes d'information induit aussi une complexité à maitriser le déploiement de politiques de sécurité sur l'ensemble du périmètre induisant des défauts de configuration laissant ouvertes des portes pour des attaques.
- La pression du DEVOPS devant rendre opérationnel des codes dont la conception et la vérification ne sont pas optimums, ne facilite pas le déploiement de systèmes robustes.

Le processus de gestion des vulnérabilités **« VULNERABILITY DETECTION »** s'organise donc autour de 2 axes REF BIB wang2009ovm :

- La **détection** de vulnérabilités dans ses actifs basés :

- sur des catalogues de vulnérabilités connues sur des actifs utilisants des codes externes (Codes Open-source, Progiciels ...) ;
- sur la mauvaise configuration de ses actifs dans le contexte de l'entreprise et sur des catalogues de mauvaises configurations. ;
- sur la non conformité aux politiques de sécurité de l'entreprise induisant des failles systémiques.

- La **recherche** des vulnérabilités utilisant :
  - des techniques de rétro-conception pour rechercher des failles d'implémentation ;
  - des techniques d'analyse de code (Basées ou non sur des outils d'analyse de code statique) pour rechercher des erreurs de conception ou de programmation.
  - des services de veille « **VULNERABILITY INTELLIGENCE** » pour accéder à ce que d'autres font en matière de recherche de vulnérabilités (CERT en particulier)

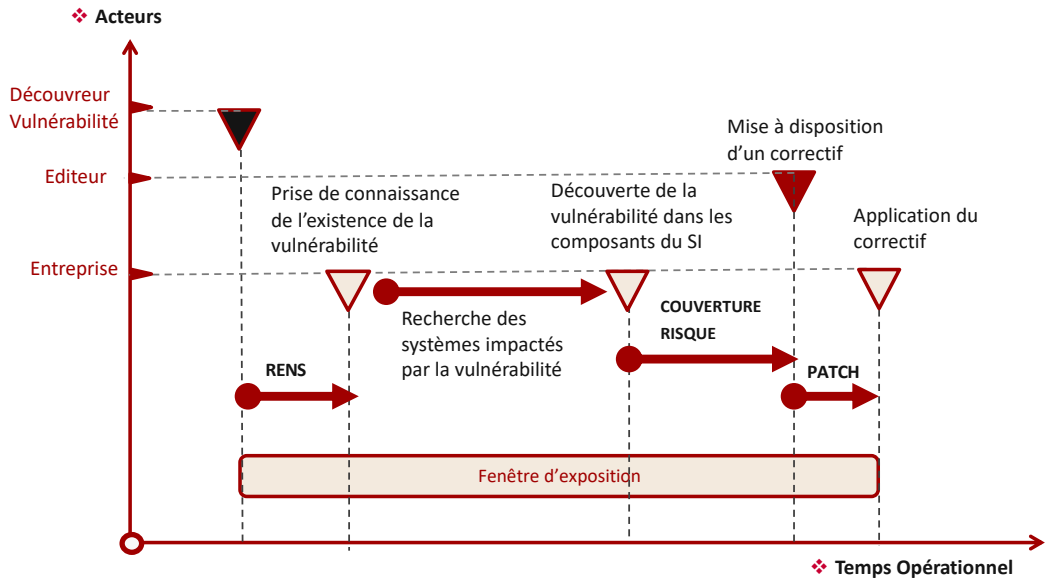

FIGURE 3. patch management en sécurité

5. La veille et l'anticiaption

La veille reste centrale dans la sécurité opérationnelle et permet d'alimenter les processus de SECOPS :

- **La veille sur les vulnérabilités** permet de connaitre les vulnérabilités apparaissant dans les logiciels ou codes connus que l'entreprise utilise (en ses murs, dans le cloud, ou chez des partenaires, fournisseurs ...) pour peu bien entendu que l'entreprise possède une cartographie exhaustive de ses logiciels. Sinon, elle aura à effectuer des audits ponctuels ou continus pour cartographier et corriger ces failles (en mettant à jour les logiciels ou en trouvant un mécanisme de couverture)
- **La veille sur les menaces** permet de disposer d'éléments pour alimenter les mécanismes de détection, il peut s'agir :

— d'adresses mail, d'adresses IP, de nom de domaines malveillants ;

— d'IOC indice de compromission sorte de signature comportemental d'un code malveillant ;

— de scénario complexe de nouvelle attaques ;

— de vulnérabilités « ZERODAY » c'est à dire n'ayant pas encore de « correctifs » disponibles.

La mise en place de mécanismes de veille ciblée sur l'entreprise se rapproche des techniques de renseignement dans l'espace militaire.

- On y trouve la **détection de compromission** ou de fuites de données en particulier la détection de couple Utilisateurs/Mots de passe sur la base d'adresse mail de l'entreprise, des bases de données clients piratées .... ;
- Le « **targeting** », c'est à dire la détection d'éléments ou d'information permettant d'alerter l'entreprise qu'une attaque se prépare contre elle ou contre les entreprises du secteur. On y trouve en particulier la lutte AntiDDOS, ou il es possible avec un renseignement suffisamment actifs de détecter avec un certains temps d'avance que des adresses IP, ou des noms de domaines particuliers vont être ciblées par des « BOTs ».

FIGURE 4. 4 axes à retenir

De manière générale après avoir engager les politiques sur la prévention et la protection, l'entreprise doit investir dans la détection et la réaction.

- Détecter pour identifier le plus en amont possible une tentative d'attaque, un comportement anormal sur ses réseaux ou une exfiltration de données.
- Répondre, en étant préparé à réagir en cas d'incident de sécurité (attaque virale, DDoS, phishing...) à travers un véritable processus de gestion et de réponse à incident qui va être piloté et mis en œuvre par un équipe de type CSIRT.

De nombreuses entreprises ne disposent pas encore systématiquement de ce type de compétences en interne ; souvent par manque de moyens. Certaines d'entre elles préfèrent faire appel à des CSIRT «commerciaux». Mais certains CSIRT internes font également appel à ces CSIRT commerciaux pour certaines parties des activités spécifiques (la veille vulnérabilités, par exemple).

6. Contributions

6.1 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) [1]. 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.

6.2 Les contributeurs/auteurs du cours

6.2.1 co-auteurs

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

6.2.2 contributeurs

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

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

Table des matières