



SEC 101

Analyse de risques
Politiques et architectures de sécurité
Sécurité opérationnelle

le cnam Bretagne

Synthèse SECOPS

Éléments de sécurité opérationnelle en cyberdéfense

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
19 janvier 2020



Sommaire

Une synthèse

Réponse aux incidents

Détection des attaques

la couverture des fragilités

La veille

Contributions





Sécurité opérationnelle

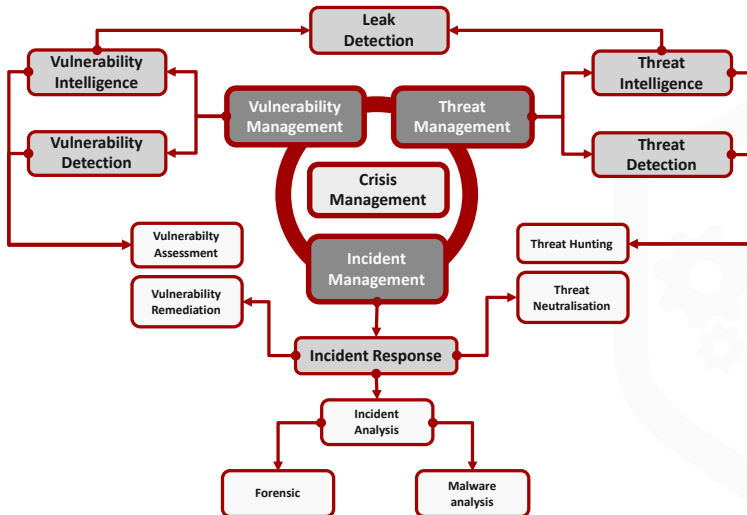
les 3 grandes fonctions

- **Répondre** au plus tôt aux incidents de sécurité afin de limiter l'impact des attaques (Equipe et compétences en réponse à incident, inforensic, 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)



3 fonctions = 3 processus SECOPS

Eléments Secops





Réponse à incidents

Étapes

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, Forensic, 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.



Détection d'attaques

les actions

- 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 alimentés d'information, renseignement 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).



Vulnerability Management

3 activités de la couverture des fragilités

- 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 maîtriser 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.



Fragilités

2 axes

- La **détection** de vulnérabilités dans ses actifs basée :
 - sur des catalogues de vulnérabilités connues sur des actifs utilisant 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 (Basé 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)



Veiller et Surveiller

Menaces et vulnérabilités

- **La veille sur les vulnérabilités** permet de connaître 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 ces logiciels. Sinon elle aura à effectuer des audits ponctuels ou continus pour cartographier puis 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 nouvelles attaques ;
 - de vulnérabilités « ZERODAY » c'est à dire n'ayant pas encore de « correctifs » disponibles.



Veiller et Surveiller

l'environnement de l'entreprise (darkweb)

- 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 ».



En quelques mots

4 axes à retenir





des questions ?

contacter eric.dupuis@cnam.fr

CYBERDEF



101

*Tous les documents publiés dans le cadre de ce cours sont perfectibles,
ne pas hésiter à m'envoyer vos remarques !*





Contributions


Les notes et les présentations sont réalisées sous L^AT_EX.

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>