



SEC 101

Analyse de risques
Politiques et architectures de sécurité
Sécurité opérationnelle

le cnam Bretagne

30 - SECOPS : Des événements de sécurité gérés à une cybercrise maîtrisée

Éléments de sécurité opérationnelle en cyberdéfense d'entreprise

Eric DUPUIS

eric.dupuis@lecnam.net eric.dupuis@orange.com

<http://www.cnam.fr>

Conservatoire National des Arts et Métiers
Chaire de Cybersécurité

Publication Notes de cours SECOPS 2022-2023 du
2 octobre 2023, 17 h 36 CEST



Abstract

⚙️ Hashtags : anticipation, veille, alerte, réponse

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.



Sommaire

1. Sécurité opérationnelle

2. Lutte contre la menace

3. Processus SECOPS

4. Les métiers de la SECOPS

5. Éléments Communs





sécurité opérationnelle

Dans le cycle de vie

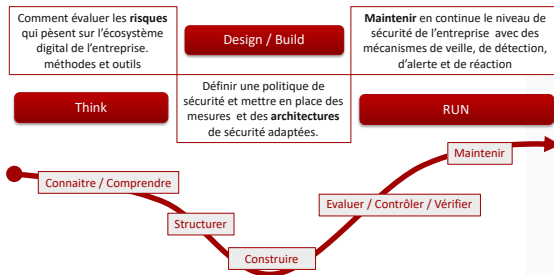
Dans certains ouvrages ce processus est dénommé « Maintien en Condition de sécurité ». En utilisant les termes anglo-saxons définissant le cycle des projets, nous pourrions positionner ses activités dans la phase dite de **RUN**. Les autres phases en amont pouvant être définies comme :

- **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 ;



sécurité opérationnelle

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 événements de sécurité gérés à une **Cybercrise** maîtrisée, ce que certains appellent **SECOPS** : « sécurité Opérationnelle ».



Objectifs adaptés aux finalités

de l'activité de l'entreprise

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 prises en compte 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 sécuritaires 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.



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).





Enjeux SECOPS

- 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.



Grandes typologies des attaques numériques

- Attaques **dinterception** 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 réseau : 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.



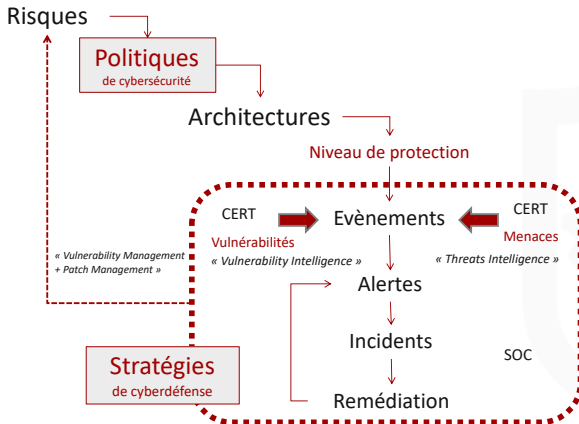
Motivations de l'attaquant

- obtenir un accès au système pour sy maintenir en attendant une opportunité ;
- récupérer de linformation, secrets, données personnelles exploitables (en gros toute information 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 entre dans cette catégories) ;
- utiliser le système dun utilisateur, pour rebondir vers un autre système ;
- détourner les ressources du système dun utilisateur (utiliser de la bande passante, utiliser de la capacité de calcul) ;



Politique vs stratégie

Positionnement de la sécurité opérationnelle





Politique vs stratégie

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.



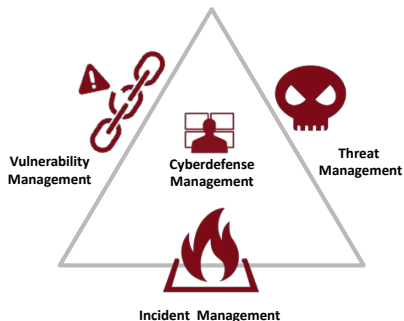
3 volets d'une cybersécurité

- 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



3 volets d'une cybersécurité

Des 3 des volets de la sécurité opérationnelle





Référentiels ANSSI

- 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.



Stratégies de l'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 :

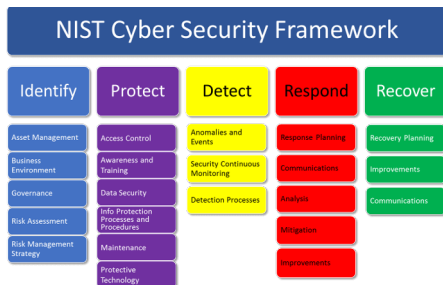
- Predictive Cyberdefense ;
- Active and Proactive Cyberdefense ;
- Reactive Cyberdefense.



Modèle NIST

modèle NIST

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 Framework du NIST ?? page ??) avec les activités **DETECT**, **RESPOND** et **RECOVER** ;

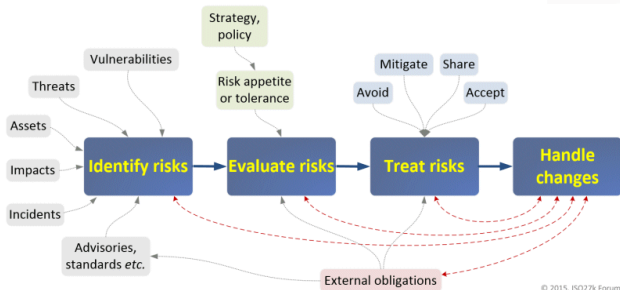




NIST vs ISO 27k

modèle ISO27 et risques

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.



© 2015, ISO27k Forum



SECOPS en 3 thématiques

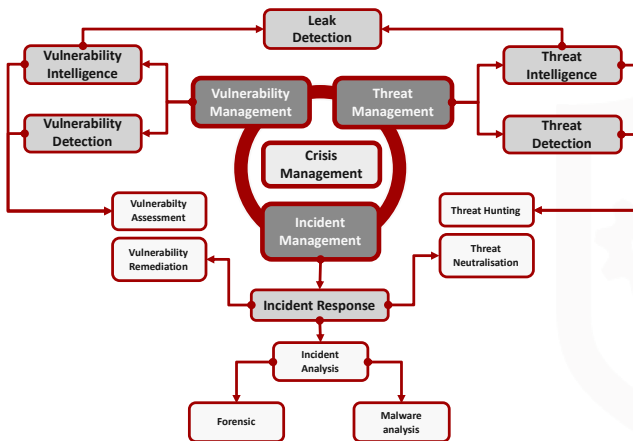
Notre propos sera donc centré sur ces trois axes qui nous déclinerons dans trois chapitres. Le travail de fond d'une équipe de sécurité opérationnelle, ou simplement de l'activité SECOPS est de pouvoir gérer de front trois grandes tâches :

- 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*).



Les processus SECOPS

Synthèse des méta-processus SECOPS





Les métiers SECOPS

Des métiers SECOPS

- Auditeur technique
- Auditeur organisationnel
- Analyste Critères Communs, CSPN

Test - Validation
& Audit

- Consultant veille menace
- Ingénieur veille technique

Veille



Vulnerability Management

Métiers Audit et gestion des vulnérabilités
Pentest,, Analyste Sécurité ...

Gestion
de crise



Threat Management

Métiers Veille, Alerte et Réaction
SIEM/SOC, CERT, Réponse aux Incidents...

Opérations de Cybersécurité

Contrôler, Surveiller & Réagir
aux événements cyber dans
l'espace digital de l'entreprise

- Opérateurs et experts solutions
- Analyste SOC
- Exploitant NSOC

- CSIRT
- Opérateur Forensic
- Analyste post-incident

Exploitation et
opération

Intervention
Sur incident



des questions ?

contacter eric.dupuis@lecnam.net

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 \LaTeX .

Vous pouvez contribuer au projet du cours CYBERDEF101. Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. A chaque session 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 vos expertises dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace :
(edufaction/CYBERDEF101) ^a.

a. <https://github.com/edufaction/CYBERDEF101>





Mises à jour régulières

Eduf@ction eric.dupuis@lecnam.net

Vérifiez la disponibilité d'une version plus récente de

CourseNotes-FR-SEC101-30-VTI-intro.prz.pdf sur GITHUB CYBERDEF ¹



2023 eduf@ction - Publication en Creative Common BY-NC-ND

