



SEC 101

Analyse de risques
Politiques et architectures de sécurité
Sécurité opérationnelle

le cnam
Bretagne

0.1 - Introduction à la cyberdéfense d'entreprise SEC101

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
13 septembre 2023, 22 h 11 CEST



Abstract

⚙️ Hashtags : SEC101, Cybersécurité, Cyberdéfense, PSSI, ISO27001, Analyse de risques

Ce document fournit les éléments d'introduction au cours SEC101 du CNAM et d'Orange Campus Cyber.



Cybersécurité, un domaine hollistique



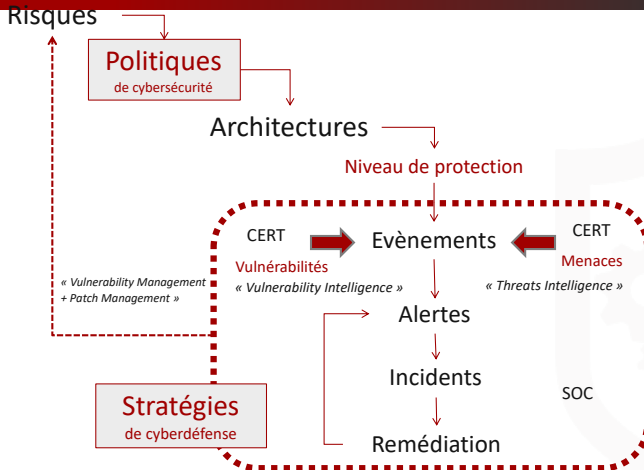


Les 3 axes de la cybersécurité d'entreprise

- **l'analyse des risques** informatiques sur les actifs les plus sensibles de l'entreprise avec les difficultés d'identifier ces actifs ainsi que leur sensibilité et les menaces qui pèsent sur ceux-ci ou sur l'environnement ;
- la structuration d'une gouvernance efficace avec des **politiques de sécurité** des systèmes d'information pour des architectures de sécurité de confiance, dans des systèmes d'information complexes, intégrant des services dans le cloud, des technologies obsolètes et des politiques de sécurité sédimentées ;
- la construction et l'organisation d'une **sécurité opérationnelle** vue sous un angle d'anticipation et de veille, de détection, et enfin d'alerte et de réponse aux attaques, nécessitant une activité continue avec des ressources de plus en plus expertes et avec des outils plus « hyperspécialisés » et de plus en plus complexe à déployer.



Processus Cyber d'entreprise





Une définition de la cybersécurité

$$\text{Cybersécurité} \cong \text{Cyberprotection} \oplus \text{Cyberdéfense} \oplus \text{Cyberrésilience} \quad (1)$$



La cybersécurité est l'enchaînement opéré, organisé, documenté, piloté, optimisé de trois environnements d'actions :

- **Protéger** l'environnement par les mesures et solutions technologies adaptées au niveau de risque que l'entreprise est prête à prendre ;
- **Défendre** les actifs les plus sensibles de l'entreprise en surveillant et combattant la menace (y compris l'image de l'entreprise) ;
- assurer **la continuité et la reprise d'activité** de l'entreprise face à tout incident rendant indisponible tout ou partie d'une fonction essentielle de celle-ci.



le cyber-risque

| | | Probabilité | | | | |
|--------|---|-------------|---|---|---|---|
| | | P/E | 1 | 2 | 3 | 4 |
| Impact | 1 | | | | | |
| | 2 | | | | | |
| | 3 | | | | | |
| | 4 | | | | | |

$$\text{Risque} = \frac{\text{Impact}(\text{Evènement, Entreprise}) \times \text{Proba}(\text{Evènement})}{\text{Moyens}(\text{Protection})}$$



La menace, une vision de l'attaquant



$$M_{\text{ menace }} = \frac{\text{Valeur(Cible)} \times \text{Fragilités (Entreprise)}}{\text{Moyens(Attaque)} \times \text{Risques(Attaquant)}}$$





SSI : Responsabilités

les métiers

- **Le gestionnaire de risque** ou *Risk Manager* qui porte l'animation de la gestion des risques dans les projets ou dans l'entreprise ;
- **Le responsable sureté / sécurité** généralement responsable de la sécurité physique ou sein de l'entreprise (vol, intrusion physique, contrôle d'accès). Il endosse le plus souvent la responsabilité des biens et des personnes ;
- **L'audit et le contrôle** : Au sein des grandes organisations, il peut exister un service « indépendant » dont la mission est d'auditer et de contrôler les activités des services ;
- **Les RSSI** : Responsables de la sécurité des Systèmes d'Information ;
- **Les DSSI** : Au sein des grandes entreprises, les RSSI globaux ne dépendent plus trop de DSI, et possèdent le rang de directeur ;
- **Le DPO** : la dernière responsabilité apparue dans l'environnement de la sécurité (En France successeur du CIL , Correspondant Informatique et Liberté) (*Data Protection Officer*).



Fonctions RSSI

différents métiers

- **RSSI d'entreprise** : Responsable de la sécurité de sa structure.
- **RSSI d'un département, d'une organisation intermédiaire** : A l'image d'un RSSI d'entreprise, il assure toute les tâches de gouvernance, il applique et fait appliquer les directives et politique de sécurité aux équipes du département / division / structure intermédiaire, il déploie les actions décidées dans la chaîne fonctionnelle sécurité
- **RSSI d'un contrat, d'un projet contractualisé (Security Manager)** : Responsable de la sécurité du déroulement d'un contrat. Souvent lié à un plan d'assurance sécurité, le RSSI contrat se doit d'assurer pour le client ou pour le fournisseur le suivi des exigences de sécurité du contrat.



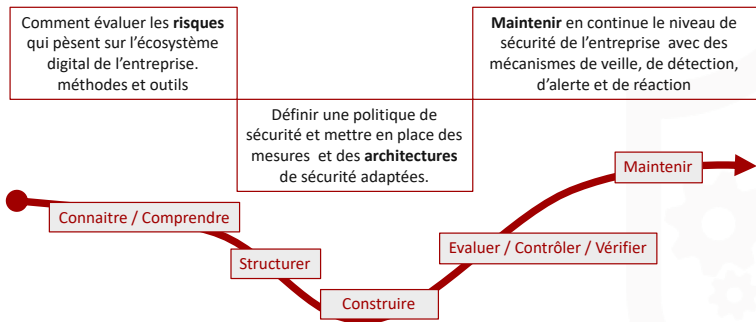
Fonctions RSSI

suite

- **RSSI Projet** : La responsabilité sécurité couvre le projet, on parle souvent de « security by design ». La responsabilité dans ce type de poste recouvre l'intégration de la sécurité dans le système, le suivi des indicateurs définis (contractuels, ou réglementaires), la remontée des indicateurs de suivi de sécurité à la MOA (Maitrise d'ouvrage), la prise de décision autour des choix de sécurité
- **RSSI Produit / Service** : Au delà de ce qui est fait pour un projet, le RSSI produit a en charge de gérer la sécurité opérationnel c'est à dire Maintenir la sécurité de son produit ou de son service.
- **RSOP** : Le responsable sécurité opérationnelle, est souvent un RSSI dépendant d'une DSI, il est généralement et dans beaucoup de d'entreprise de taille moyenne le RSSI technique. Il assure opérationnellement la mise en place technique des politiques de sécurité et maintien en condition de sécurité l'ensemble de l'environnement informatique. Il est aujourd'hui au coeur de la sécurité opérationnelle face aux attaques et aux crises cyber.



Cycle de vie sécurité dans les projets





Cadres normatifs

3 modèles du cadre

- Identifier ses cyber-risques sur la base de méthodologies que l'on retrouve dans l'environnement ISO/CEI 27001/27005 mais aussi sur la méthodologie EBIOS de l'ANSSI (Méthode EBIOS RM en particulier) ;
- Elaborer une politique de cybersécurité sur la base des cadres ISO/CEI 27001 et 27002, en n'oubliant pas les architectures de sécurité et la sécurité des architectures associées ;
- Détecter en amont des attaques et savoir réagir à ses cyber-incidents en se basant sur ISO 27035 et sur la continuité d'activité avec l'ISO 22301 et 27031.



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-SEC101-00-IntroSEC101.prz.pdf sur GITHUB CYBERDEF ¹



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

