



# SEC 101

Analyse de risques  
Politiques et architectures de sécurité  
Sécurité opérationnelle

# le cnam Bretagne

## Introduction Cybersécurité Objectifs, politiques et déploiement

Éléments de sécurité opérationnelle en cyberdéfense d'entreprise

Eric DUPUIS

[eric.dupuis@cnam.fr](mailto:eric.dupuis@cnam.fr) [eric.dupuis@orange.com](mailto:eric.dupuis@orange.com)

<http://www.cnam.fr>

Conservatoire National des Arts et Métiers  
Chaire de Cybersécurité

Date de publication  
25 février 2020



# Sommaire

Avant propos

Les axes d'une cybersécurité intégrée

Transformation numérique

sécurité du système d'information

les enjeux légaux

Contributions





# Cybersécurité : un domaine hollistique

...du contrôle des conformités  
à la gestion des relations  
institutionnelles...

...de l'intégration de solutions  
de sécurité aux architectures  
résilientes...



Normatif, contractuel,  
réglementaire,  
législatif

Technologique



Expérimentale

Méthodologique



...de la détection de  
signaux faibles  
à la reprise sur incidents...

...de l'analyse des risques  
à la gestion des crises...



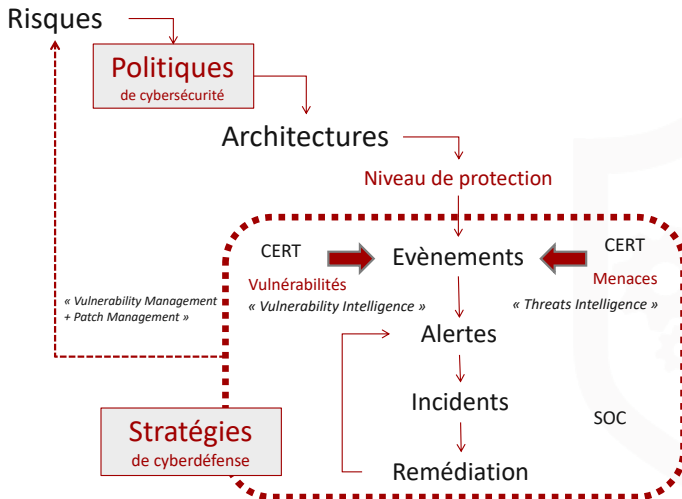
## Les 3 axes de la cybersécurité

- **l'analyse des risques** informatiques sur les actifs les plus sensibles de l'entreprise avec les difficultés d'identifier la sensibilité de ces actifs et les menaces qui pèsent sur l'environnement ;
- la structuration des **politiques de sécurité** des systèmes d'information pour des architectures de sécurité de confiance, dans des systèmes d'informations 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 « pointus ».



# Politiques et stratégies

Processus Cyber d'entreprise

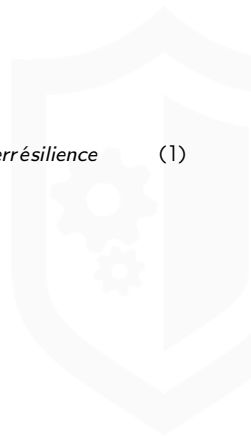


La figure ?? présente la dynamique avec laquelle nous avons structuré dans ce document



# 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'ingénierie :

- **Protéger** l'environnement par les mesures et solutions technologies adaptées au niveau de risque que l'entreprise est prêt 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



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





- **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 sûreté / 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*).



# des questions ?

contacter [eric.dupuis@cnam.fr](mailto: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<sup>A</sup>T<sub>E</sub>X.

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) <sup>a</sup>. 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>