SEC 101

Analyse de risques
Politiques et architectures de sécurité
Sécurité opérationnelle

le cnam Bretagne

Introduction : CybersÃ©curitÃ© Objectifs, politiques et dÃ©ploiement

ElÃ©ments de sÃ©curitÃ© opÃ©rationnelle en cyberdÃ©fense d'entreprise

Eric DUPUIS

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

http://www.cnam.fr

Conservatoire National des Arts et MÃ©tiers
Chaire de CybersÃ©curitÃ©

Publication DRAFT NOTES 2020-2021 du
12 novembre 2020, 23 h 25 CET

Sommaire

CybersÃ©curitÃ© : 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

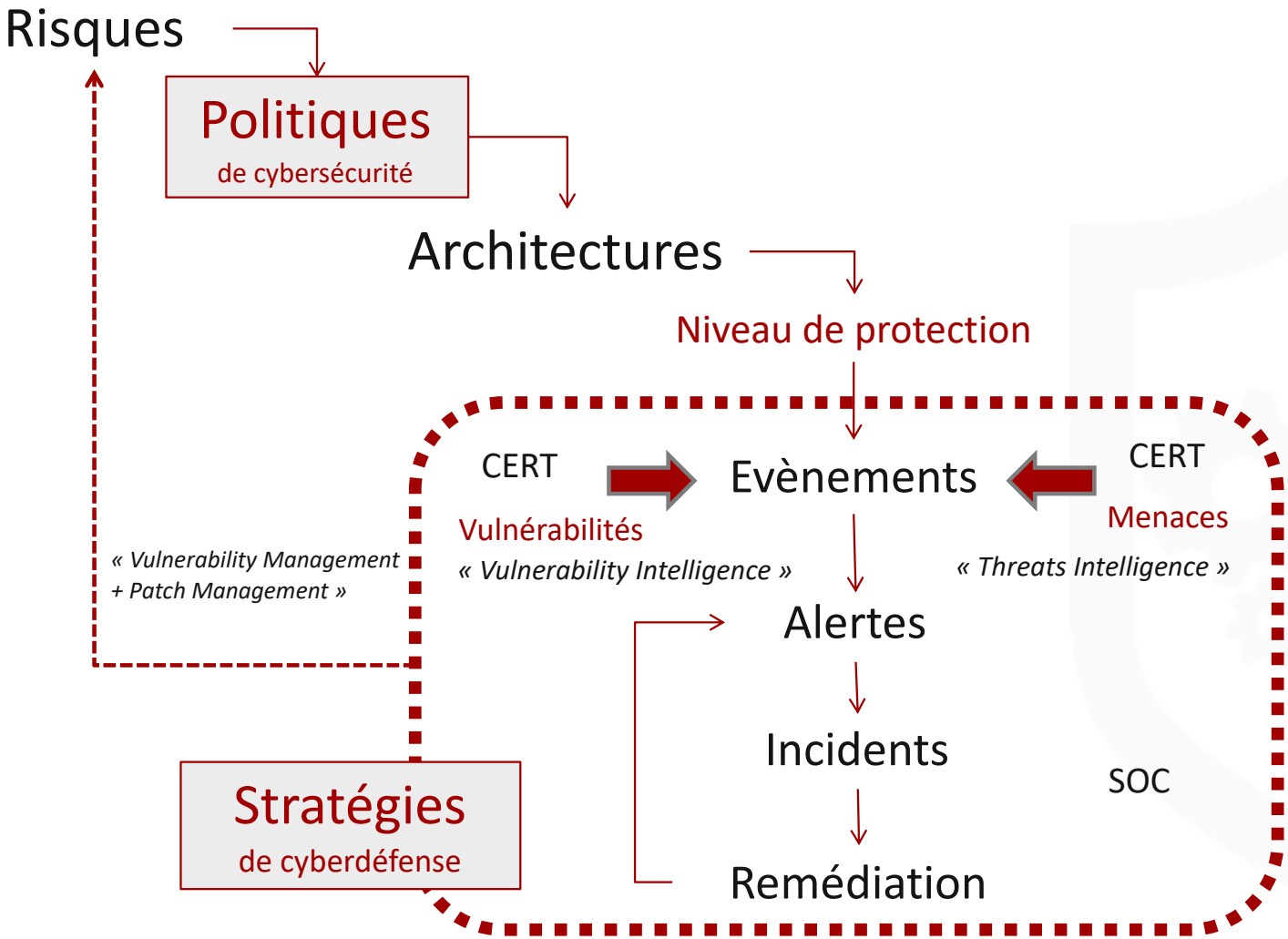
…de la détection de signaux faibles à la reprise sur incidents…

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

Les 3 axes de la cybersÃ©curitÃ©

- **l'analyse des risques** informatiques sur les actifs les plus sensibles de l'entreprise avec les difficultÃ©s d'identifier la sensibilitÃ© de ces actifs et les menaces qui pÃ¨sent sur l'environnement ;
- la structuration d'une gouvernance efficaces avec des **politiques de sÃ©curitÃ©** des systÃ¨mes d'information pour des architectures de sÃ©curitÃ© de confiance, dans des systÃ¨mes d'informations complexes, intÃ©grant des services dans le cloud, des technologies obsolÃ¨tes et des politiques de sÃ©curitÃ© sÃ©dimentÃ©es ;
- la construction et lâorganisation d'une **sÃ©curitÃ© opÃ©rationnelle** vue sous un angle d'anticipation et de veille, de dÃ©tection, et enfin d'alerte et de rÃ©ponse aux attaques, nÃ©cessitant une activitÃ© continue avec des ressources de plus en plus expertes et avec des outils plus « pointus ».

Processus Cyber d'entreprise



Une dÃ©finition de la cybersÃ©curitÃ©

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

La cybersÃ©curitÃ© est l'enchaÃ®nement opÃ©rÃ©, organisÃ©, documentÃ©, pilotÃ©, optimisÃ© de trois environnements d'actions :

- **ProtÃ©ger** l'environnement par les mesures et solutions technologies adaptÃ©es au niveau de risque que l'entreprise est prÃªte Ã prendre ;
- **DÃ©fendre** les actifs les plus sensibles de l'entreprise en surveillant et combattant la menace (y compris l'image de l'entreprise) ;
- assurer **la continuitÃ© et la reprise d'activitÃ©** de l'entreprise face Ã tout incident rendant indisponible tout ou partie d'une fonction essentielle de celle-ci.

le cyber-risque

Probabilité

Impact P/E	1	2	3	4
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

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

SSI : ResponsabilitÃ©s

les mÃ©tiers

- **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 suretÃ© / sÃ©curitÃ©** gÃ©nÃ©ralement responsable de la sÃ©curitÃ© physique ou sein de l'entreprise (vol, intrusion physique, contrÃ´le d'accÃ¨s). Il endosse le plus souvent la responsabilitÃ© des biens et des personnes ;
- **L'audit et le contrÃ´le** : Au sein des grandes organisations, il peut exister un service « indÃ©pendant » dont la mission est d'auditer et de contrÃ´ler les activitÃ©s des services ;
- **Les RSSI** : Responsables de la sÃ©curitÃ© des SystÃ¨mes d'Information ;
- **Les DSSI** : Au sein des grandes entreprises, les RSSI globaux ne dÃ©pendent plus trop de DSI, et possÃ¨dent le rang de directeur ;
- **Le DPO** : la derniÃ¨re responsabilitÃ© apparue dans l'environnement de la sÃ©curitÃ© (En France successeur du CIL , Correspondant Informatique et LibertÃ©) (*Data Protection Officer*).

Fonctions RSSI

diffÃ©rents mÃ©tiers

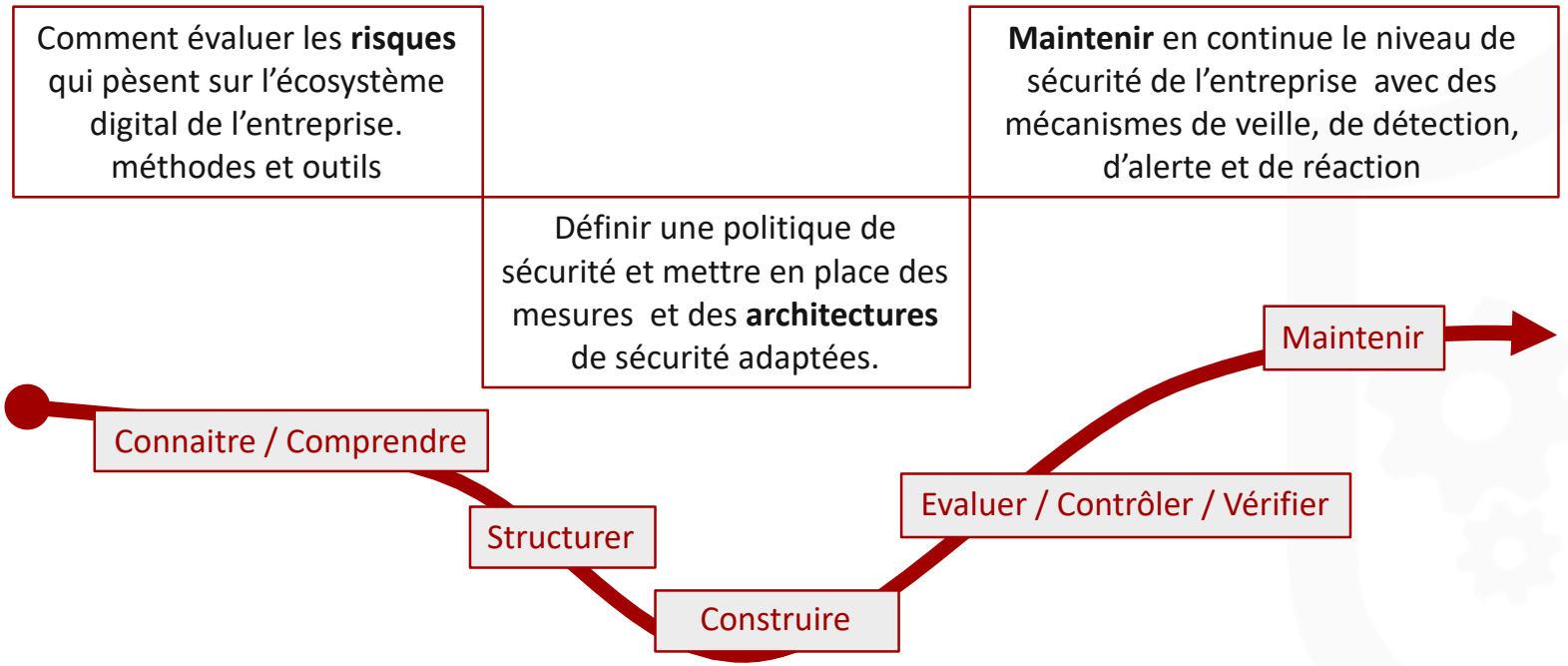
- **RSSI d'entreprise** : Responsable de la sÃ©curitÃ© de sa structure.
- **RSSI d'un dÃ©partement, d'une organisation intermÃ©diaire** : A l'image d'un RSSI d'entreprise, il assure toute les tÃ¢ches de gouvernance, il applique et fait appliquer les directives et politique de sÃ©curitÃ© aux Ã©quipes du dÃ©partement / division / structure intermÃ©diaire, il dÃ©ploie les actions dÃ©cidÃ©es dans la chaÃ®ne fonctionnelle sÃ©curitÃ©
- **RSSI d'un contrat, d'un projet contractualisÃ© (Security Manager)** : Responsable de la sÃ©curitÃ© du dÃ©roulement d'un contrat. Souvent liÃ© Ã un plan d'assurance sÃ©curitÃ©, le RSSI contrat se doit d'assurer pour le client ou pour le fournisseur le suivi des exigences de sÃ©curitÃ© du contrat.

Fonctions RSSI

suite

- **RSSI Projet** : La responsabilitÃ© sÃ©curitÃ© couvre le projet, on parle souvent de « security by design ». La responsabilitÃ© dans ce type de poste recouvre l'intÃ©gration de la sÃ©curitÃ© dans le systÃ¨me, le suivi des indicateurs dÃ©finis (contractuels, ou rÃ©glementaires), la remontÃ©e des indicateurs de suivi de sÃ©curitÃ© Ã la MOA (Maitrise d'ouvrage), la prise de dÃ©cision autour des choix de sÃ©curitÃ© ....
- **RSSI Produit / Service** : Au delÃ de ce qui est fait pour un projet, le RSSI produit a en charge de gÃ©rer la sÃ©curitÃ© opÃ©rationnel c'est Ã dire Maintenir la sÃ©curitÃ© de son produit ou de son service.
- **RSOP** : Le responsable sÃ©curitÃ© opÃ©rationnelle, est souvent un RSSI dÃ©pendant d'une DSI, il est gÃ©nÃ©ralement et dans beaucoup de d'entreprise de taille moyenne le RSSI technique. Il assure opÃ©rationnellement la mise en place technique des politiques de sÃ©curitÃ© et maintien en condition de sÃ©curitÃ© l'ensemble de l'environnement informatique. Il est aujourd'hui au coeur de la sÃ©curitÃ© opÃ©rationnelle face aux attaques et aux crises cyber.

Cycle de vie sÃ©curitÃ© dans les projets



Cadres normatifs

3 modÃ¨les du cadre

- Identifier ses cyber-risques sur la base de mÃ©thodologies que lâon retrouve dans lâenvironnement ISO/CEI 27001/27005 mais aussi sur la mÃ©thodologie Expression des Besoins et Identification des Objectifs de SÃ©curitÃ© (EBIOS) de lâANSSIÂ (MÃ©thode EBIOS RM en particulier) ;
- Elaborer une politique de cybersÃ©curitÃ© sur la base des cadres ISO/CEIÂ Â 27001 et 27002, en nâoubliant pas les architectures de sÃ©curitÃ© et la sÃ©curitÃ© des architectures associÃ©es ;
- Â DÃ©tecter en amont des attaques et savoir rÃ©agir Ã ses cyber-incidents en se basant sur ISO 27035 et sur la continuitÃ© dâactivitÃ© avec lâISO 22301 et 27031.

des questions ?

contacter eric.dupuis@lecnam.net

CYBERDEF

101

Tous les documents publiÃ©s dans le cadre de ce cours sont perfectibles, ne pas hÃ©siter Ã m'envoyer vos remarques !

Contributions

Les notes et les prÃ©sentations sont rÃ©alisÃ©es sous LaTeX.
Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- Corriger, amender, amÃ©liorer les notes publiÃ©es. Chaque semestre et annÃ©e des modifications et Ã©volutions sont apportÃ©es pour tenir compte des corrections de fond et de formes.
- Ajouter, complÃ©ter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines Ã©voquÃ©s.

Les fichiers sources sont publiÃ©s sur GITHUB dans l'espace : (edufaction/CYBERDEF) [a]. Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribuÃ© Ã ces notes.
Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les dÃ©tails de contributions.

a. `https://github.com/edufaction/CYBERDEF`

Mises Ã jour rÃ©guliÃ¨res

Eduf@ction eric.dupuis@lecnam.net

VÃ©rifiez la disponibilitÃ© d'une version plus rÃ©cente de

SEC101-C0a-Intro.prz.pdf sur GITHUB CYBERDEF [1]