SEC 101

Analyse de risques
Politiques et architectures de sécurité
Sécurité opérationnelle

le cnam Bretagne

REAGIR : De l'évènement de sécurité à la crise cyber

Eléments 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 DRAFT NOTES 2020-2021 du
26 janvier 2021, 20 h 55 CET

Sommaire

La réponse à incident

quelques éléments de définition

La réponse à incident est le processus qui permet de déployer les moyens nécessaires pour traiter un événement de sécurité classé comme incident de sécurité. Un incident de sécurité peut être enregistré en provenance de systèmes de sécurité, de veille ou d'audit. Le besoin d'intervention peut être immédiat comme différé. La réponse peut nécessiter des équipes de compétences larges comme expertes sur un domaine donné. L'intervention peut nécessiter des moyens techniques importants ou pas, et mettre en isolation tout ou partie d'un système d'information.

La réponse à incident

Terminologie

- **Investigations Numériques** : *Digital Investigation* ;
- **Analyse légale** : *forensique (Inforensique)* ;
- **CERT** : *Computer Emergency Response Team* ;
- **CSIRT** : *Computer Security Incident Response Team* ;
- **Gestion des Incidents** : *Incident Management* .

La réponse à incident

Evènement de sécurité

Concrètement, un événement peut donc être :

- soit la découverte d'une vulnérabilité ;
- soit la constatation d'une non-conformité ;
- soit une altération, une perte ou une atteinte à l'information ;
- soit une altération ou une perte d'un élément du système d'information, d'un élément de configuration du SI ou d'un actif non-IT ;
- soit un ensemble corrélé d'indicateurs avertissant d'un comportement non sollicité ou malveillant ;.

Les axes de la gestion des cyber-Incidents

ANTICIPER

Gouverner, Organiser, mesurer, architecturer

Mise en œuvre d'une cellule de gestion des incidents de sécurité disposant des capacités et de la légitimé pour répondre techniquement et piloter éventuellement une gestion de crise

REAGIR

Remédier, Isoler, Contenir, neutraliser

Intervention sur incidents pour réduire l'impact de l'attaque

ENQUETER

Identifier, Imputer, Evaluer Impact, Comprendre, modéliser

investigation numérique pour déterminer les caractéristiques de l'attaque (intentions et objectifs, sources, cibles, mécanismes

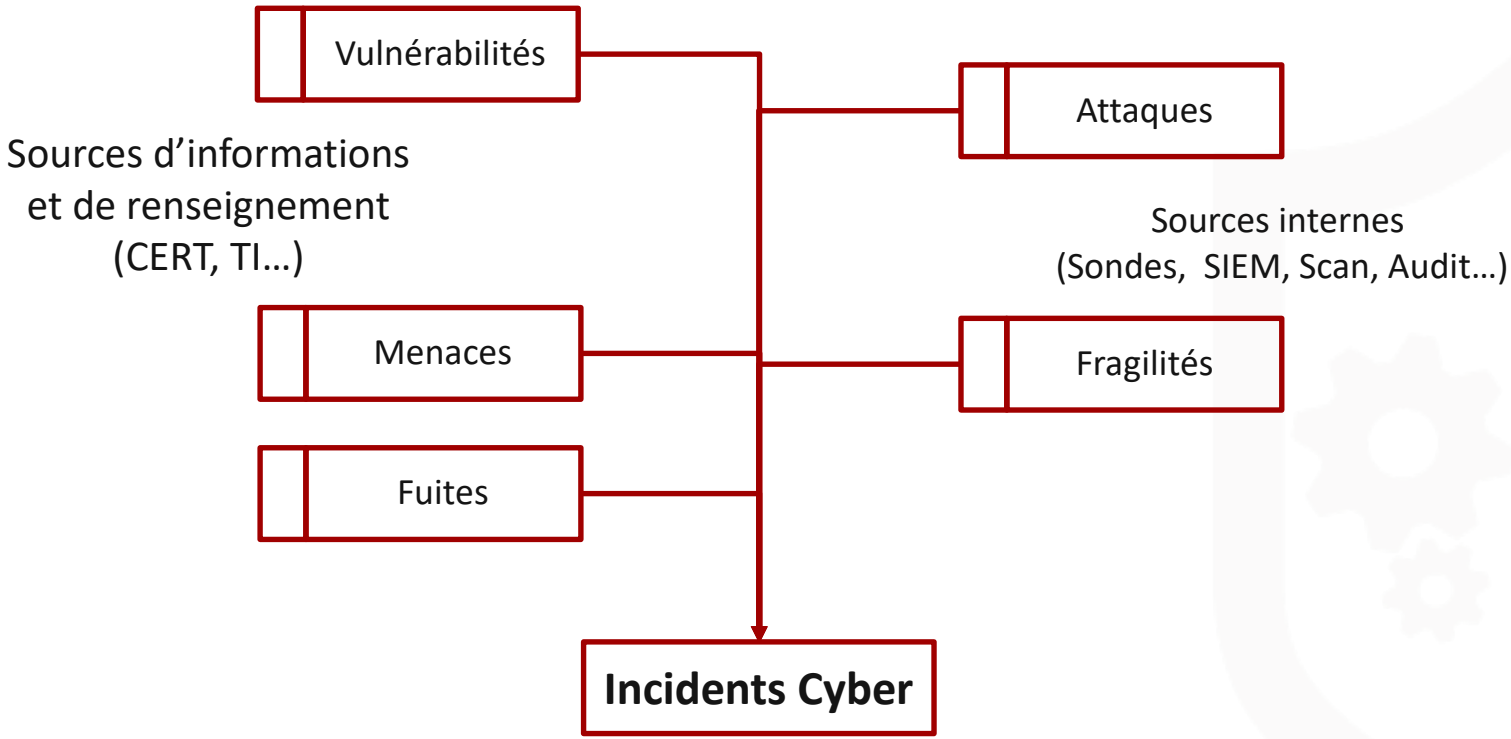
La réponse à incident

Incidents courants

Voici quelques exemples d'incidents relativement courants :

- Une attaque par déni de service distribué (DDoS) contre les services cloud critiques ;
- Infection par un logiciel malveillant ou un rançongiciel qui a chiffré des fichiers d'entreprise critiques sur le réseau de l'entreprise ;
- Une tentative de phishing réussie qui a conduit à la divulgation d'informations personnelles identifiables des clients ;
- Perte ou vol, d'un ordinateur portable non chiffré avec des informations sensibles ;
- Découverte sur internet (Darkweb) de données sensibles appartenant à l'entreprise.

Les axes de la gestion des cyber-Incidents



La réponse à incident

SANS Institute - Plan de réponse

Selon le SANS Institute, la réponse est construite autour de six phases clés d'un plan de réponse aux incidents :

- **Préparation** : préparer les utilisateurs et le personnel informatique à gérer les incidents potentiels en cas de survenance ;
- **Identification** : déterminer si un événement peut être qualifié d'incident de sécurité.
- **Confinement** : limiter les dommages de l'incident et isoler les systèmes affectés pour éviter d'autres dommages ;
- **Éradication** : rechercher la cause première de l'incident et suppression des systèmes affectés de l'environnement de production ;
- **Récupération** : autoriser les systèmes affectés à réintégrer l'environnement de production et garantir qu'aucune menace ne subsiste. ;
- **Leçons apprises** : remplir la documentation de l'incident, effectuer une analyse pour tirer des leçons de l'incident et potentiellement améliorer les efforts d'intervention futurs.

La réponse à incident

Evènement de sécurité

- **Réagir** : premier processus, si nous pouvons le nommer ainsi est la réaction immédiate en cas d'incident. Une entreprise peu ou pas organisée commence par découvrir les techniques de réponse à incident par cette première action. Cette réaction peut être compléter par des mécanismes (juridiques) de **neutralisation** de la menace, ou par exemple le déploiement d'un EDR pendant la phase de crise.
- **Enquêter** : si la réaction pour réduire l'impact ou neutraliser l'attaque est au coeur de la réponse à incident, il est nécessaire de rapidement lancer l'analyse des causes et origines de l'incident. Ce domaine d'action qui regroupe l'analyse post-morten et le forensique.
- **Anticiper** : organiser ses mécanismes de réponse (moyens et compétences), intégrer le processus de réponse à incident Cyber dans les mécanisme ITIL de gestion des incidents, organiser une cellule de CSIRT.

Incidents

MAINTENIR LA CONTINUITE D'ACTIVITE

Incidents

Remédier et reconfigurer pour limiter l'impact

Enquêter sur l'incident

Neutraliser les sources de menaces

La réponse à incident

ITIL

On ne peut toutefois pas oublier, que la gestion de la sécurité dans une entreprise mature, doit s'intégrer aux processus IT de l'entreprise et de remarquer que certaines activités de sécurité peuvent aussi s'intégrer dans un respect du référentiel ITIL.

- Le centre de services (service desk) cf le niveau 1 d'un « Security Operation Center » ;
- La gestion des incidents (incident management) ;
- La gestion des problèmes (problem management) ;
- La gestion des changements (change management) voir les mécanismes de couverture de vulnérabilités (patch management par exemple) ;
- La gestion des mises en production (release management) ;
- La gestion des configurations (configuration management).

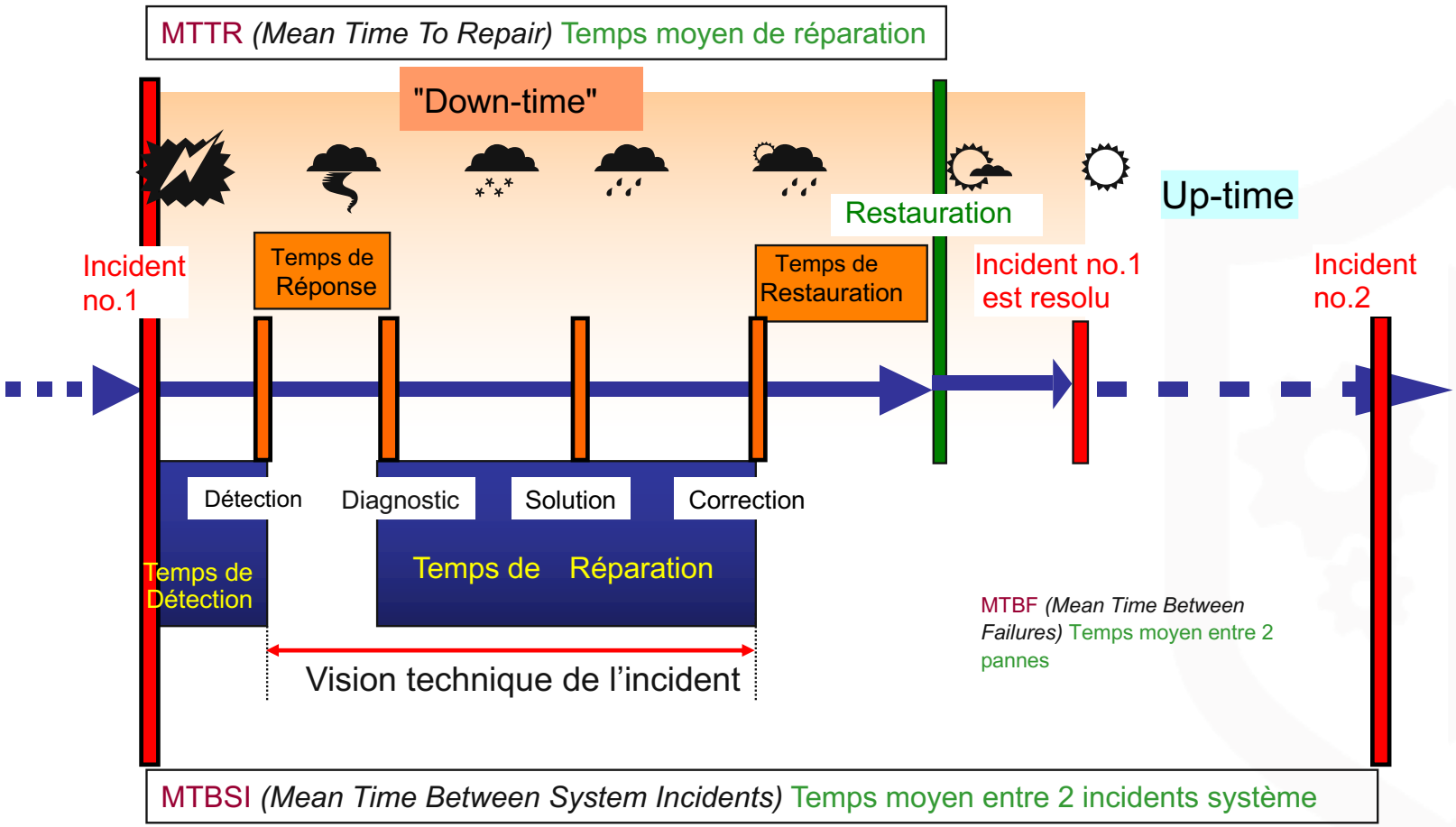
La réponse à incident

avec l'ISO 27035

La mise en place d'un processus de gestion d'incidents, qu'il soit totalement intégré à la DSI via ITIL, ou des processus ISO9001 est complexe en entreprise mais les enjeux sont toujours identiques :

- Améliorer la sécurité de l'information ;
- Réduire les impacts sur le business ;
- Renforcer la prévention d'incident ;
- Assurer le recevabilité des preuves ;
- Mettre à jour l'appréciation des risques ;
- Prévention et sensibilisation.

Incidents


MTTR (Mean Time To Repair) Temps moyen de réparation
"Down-time"
Restauration
Up-time
Incident no.1
Temps de Réponse
Temps de Restauration
Incident no.1 est resolu
Incident no.2
Détection
Diagnostic
Solution
Correction
Temps de Détection
Temps de Réparation
MTBF (Mean Time Between Failures) Temps moyen entre 2 pannes
Vision technique de l'incident
MTBSI (Mean Time Between System Incidents) Temps moyen entre 2 incidents système

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 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.

GitHub

Overleaf

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`

Mises à jour régulières

Eduf@ction eric.dupuis@lecnam.net

Vérifiez la disponibilité d'une version plus récente de

SEC101-C3c-IncidentMan.prz.pdf sur GITHUB CYBERDEF [1]