CNAM Bretagne, Cybersécurité SEC101, eduf@ction
Notes de cours éditées le 12 mai 2020, 23 h 24 CEST

Réagir : De l'évènement de sécurité à la crise

Eric DUPUIS[1,2]*

Résumé
Ce document donne les grands principes de la gestion des incidents, et la conduite de gestion de crise.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document final unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique.

Mots clefs
Incidents, forensic, crise

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@lecnam.net – eric.dupuis@orange.com

DRAFT NOTES S2 - 2020

Vérifiez la disponibilité d'une version plus récente de

SEC101-C3-IncidentMan.doc.pdf sur GITHUB CYBERDEF [1]

2020 eduf@ction Publication en Creative Common BY-NC-ND

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/SEC101-C3-IncidentMan.doc.pdf

1. GERER les incidents

1.1 Réponse à incident

la réponse sur incident de sécurité pose de nombreuses questions sur les aspects aussi bien techniques que juridiques ou organisationnels. Nous allons tenter d'aborder ces éléments dans ce chapitre. La réponse à incident, doit s'inscrire dans une organisation cohérente permettant de gérer l'ensemble de la chaine de traitement d'un incident. On parle de Gestion des incidents (Incident Management). Cette gestion des incidents est par ailleurs à cheval entre les processus de surveillance et de détection et de réponse à incident. Dans ce document nous nous focaliserons sur cette réponse à incident au sens du traitement d'un incident lié à une menace avérée.

1.2 Terminologie

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 nécessité des moyens techniques important ou pas, et mettre en isolation tout ou partie d'un système d'information.

La gouvernance de la réponse aux incidents consiste à planifier à l'avance et de disposer un plan d'opération avant qu'il ne soit nécessaire. Plutôt que d'être un processus axé sur l'informatique, il s'agit d'une fonction globale qui permet à une organisation de prendre des décisions rapides avec des informations fiables dans un contexte où la continuité d'activité ou l'image de l'entreprise est menacée. Non seulement le personnel technique des services informatiques et de sécurité est impliqué, mais aussi des représentants d'autres aspects clés de l'entreprise. La réponse à incident interpelle dans son mode d'opération, la gestion des plans de continuité et de reprise d'activité, la gestion de crise, l'interaction juridique et contractuelle ainsi que l'a gestion des relations avec les services de l'état (CNIL, ANSSI, Police et Gendarmerie ...).

Quelques éléments de terminologies avec la correspondance anglo-saxonne afin de se repérer dans les usages et trouver de l'information pertinentes lors de vos recherches sur Internet.

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

1.3 Définitions

Incident

Un incident de sécurité, correspond donc à la conséquence d'un ou plusieurs évènements de sécurité ou un évènement de sécurité majeur. Pour un **événement**, il n'y a pas de conséquence alors que pour un **incident** il y a un impact sur l'un des critères de sécurité DICA (Disponibilité, Intégrité, Confidentialité, Auditabilité).

Cette distinction a toujours existé, en effet l'ISO/IEC 27001 l'a reprise de l'ISO TR 18044 :2004 (aujourd'hui remplacée par l'ISO/IEC 27035) qui l'avait elle-même reprise de l'ISO TR 13335-2 :1997. Cela remonte donc à la création de la normalisation en sécurité informatique en 1991. 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.

Un événement peut donner lieu à un **traitement préventif,** dans la mesure où aucun impact n'a été identifié, par exemple la découverte d'une vulnérabilité. Un incident donne quant à lui obligatoirement lieu à un « traitement curatif »car un impact a été identifié. Ce qui motive la requalification d'un événement en incident doit impérativement être basé sur une décision humaine en fonction d'une estimation de l'impact. Néanmoins avant de s'engager dans la descriptions des activités liées à la réponse à incident cybersécurité, je souhaitais évoquer les bonnes pratiques ITIL qui donnent des pistes sur l'organisation de la gestion d'incident. Il ne faut en effet pas considérer la réponse à attaque comme une activité que technique bien que l'urgence nécessite le plus souvent de passer outre les processus classiques de traçabilité.

1.4 Sources Incidents

Il existe différents types d'incidents de sécurité et des moyens de les classer. Ce qui peut être considéré comme un incident pour une organisation peut ne pas être aussi critique pour une autre. tous les incidents ne proviennent pas de SIEM. En effet le déclenchement d'incident peut avoir différentes sources.

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 ;

FIGURE 1. Les axes de la gestion des cyber-Incidents

- Perte ou vol, d'un ordinateur portable non chiffré avec des informations sensibles ;
- découverte sur internet (Darkweb) de données sensibles appartenant à l'entreprise.

Selon le SANS Institute, la réponse est construit 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** : recherche de 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.

1.5 Parcours

La gestion de l'incident au quotidien

Réagir Mécanismes et processus compétences outils

Enquêter

Mécanismes et processus compétences outils

Anticiper

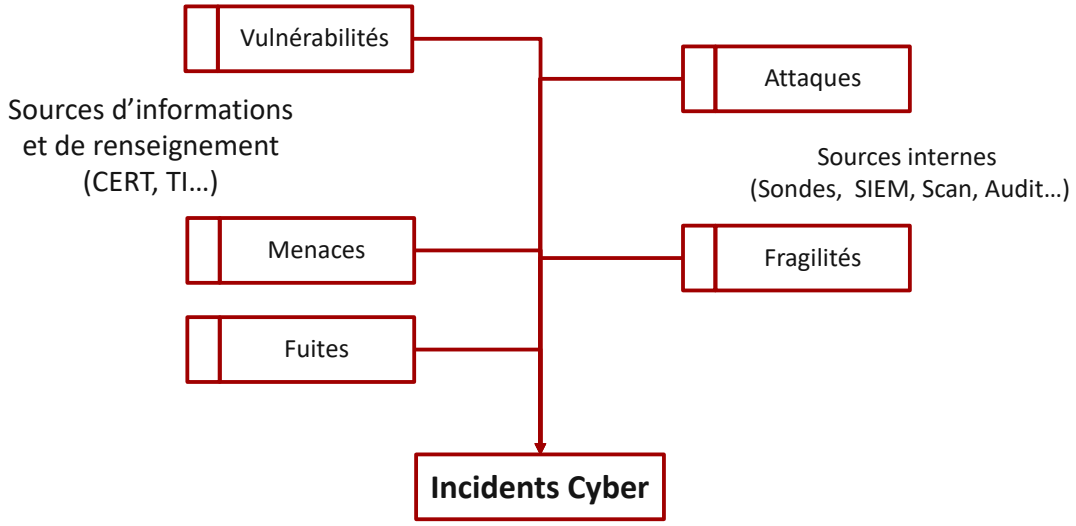

FIGURE 2. Les axes de la gestion des cyber-Incidents

Organiser sa réponse (moyens et compétences)

l'intégration dans ITIL

(aller plus loin) Organiser processus de réponse : CSIRT

2. ANTICIPER

2.1 Etablir un processus de management

2.1.1 Résilience

On ne peut pas parler de réponse à incident dans un contexte d'attaque informatique sans parler de résilience.

La cyber-résilience ou la résilience numérique est la capacité d'un système d'information à résister à une panne ou une cyber-attaque et à revenir à son état initial après l'incident, ou bien comme la faculté d'une structure quelconque à retrouver ses propriétés initiales après une altération significative. La notion peut s'appliquer aussi bien à un système physique ou un système d'information, qu'à un individu ou une organisation.

Elle se traduit pour cette organisation par sa capacité de continuer à fonctionner et de résister à des agressions internes comme externes, volontaires ou non.

Le niveau de résilience se mesure avec des critères tels que la structure de l'organisation mise en place, les ressources humaines consacrées au fonctionnement du système, la redondance et le durcissement des systèmes et des équipements, les procédures en place, des compétences acquises à travers une formation et un entrainement dédiés, la connaissance fine de l'état de fonctionnement du système et la capacité à diagnostiquer une défaillance potentielle.

Sur le cyber-espace, la cyber-résilience implique donc de se préparer et de prendre les mesures adaptées pour assurer le rétablissement d'un système. Par ailleurs, dans le monde cyber dans l'entreprise l'incertitude peut régner dans l'usage :

- sur la sécurité des systèmes (virus déployés dont les effets ne sont pas maîtrisés),
- l'intégrité du système n'est plus garantie,
- l'activité du système peut être dégradée (données corrompues ou altérées) ou inopérante (communications inactives),
- les risques de propagation des menaces sont augmentés si les interconnexions entre systèmes restent ouvertes,

Cette résilience peut nécessiter des bascules vers des modes dégradés, avec l'isolation ou l'arrêt de certaines sous-systèmes. Ce type de décision nécessite de circuit de décision rapide et court.

C'est dans un cadre de cette continuité d'activité que se situent la majorité des référentiels de management de l'incident de de sécurité.

Résilience et continuité d'activité

La capacité d'un système à résister à une panne ou une cyber-attaque et à revenir à son état initial après l'incident sera indifféremment appelé dans e cours résilience ou continuité d'activité.

2.2 L'intégration dans la gestion des incidents ITIL

ITIL (« Information Technology Infrastructure Library »pour « Bibliothèque pour l'infrastructure des technologies de l'information ») est un ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») du management du système d'information.

La Gestion des incidents vue du côté d'ITIL inclut tout événement qui perturbe, ou pourrait perturber, un service. Ceci inclut les événements communiqués directement par les utilisateurs, via le Centre de services, une interface web ou autrement. Ce processus appartient au sens ITIL à l'étape Service Operation(SO) du cycle de vie d'un SI.

Même si les incidents et les demandes de service sont rapportés au Centre de services, cela ne veut pas dire qu'ils sont de même type. Les demandes de service ne représentent pas une perturbation de service comme le sont les incidents. Voir le processus Exécution des requêtes pour plus d'information sur le processus qui gère le cycle de vie

Les objectifs du processus de Gestion des incidents sont :

- Veiller à ce que des méthodes et des procédures normalisées soient utilisées pour répondre, analyser, documenter, gérer et suivre efficacement les incidents.
- Augmenter la visibilité et la communication des incidents à l'entreprise et aux groupes de soutien du SI.

- Améliorer la perception des utilisateurs par rapport aux TI via une approche professionnelle dans la communication et la résolution rapide des incidents lorsqu'ils se produisent.
- Harmoniser les activités et les priorités de gestion des incidents avec ceux de l'entreprise.
- Maintenir la satisfaction de l'utilisateur avec la qualité des services du SI.

Généralement, cette gestion d'incident s'inscrit dans une chaine d'outillage avec des processus permettant de définir l'état ou le statut de l'incident.

- **Nouveau** : un incident est soumis, mais n'a pas été assigné à un groupe ou une ressource pour résolution.
- **Assigné** : un incident est assigné à un groupe ou une ressource pour résolution.
- **En traitement** : l'incident est en cours d'investigation pour résolution.
- **Résolu** : une résolution a été mise en place.
- **Fermé** : la résolution a été confirmée par l'utilisateur comme quoi le service normal est rétabli.

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).

Dans ces processus le cycle de vie de l'incident suis un cycle connu et reconnu :

- **Identification** : détecter ou rendre compte d'un incident ;
- **Enregistrement** : les incidents sont enregistrés dans le système de gestion des incidents ;
- **Classement** : les incidents sont classés par priorité ;
- **Priorisation** : l'incident est classé par ordre de priorité, sur la base de son impact et de son urgence, pour une meilleure utilisation des ressources et du temps disponible par l'équipe de support ;

- **Escalade** : l'équipe de support doit-elle obtenir de l'aide de la part d'un autre service ? Si oui, on engage une procédure de demande de service sinon, la résolution de l'incident s'effectue au niveau du support initial.
- **Diagnostic** : révélation du symptôme complet de l'incident ;
- **Résolution et rétablissement** : une fois que la solution est trouvée et que la correction est apportée alors l'incident est résolu ; La solution peut alors être ajoutée à la base des erreurs connues dans l'optique de résoudre plus rapidement un incident similaire dans le futur.
- **Clôture de l'incident** : l'enregistrement de l'incident dans le système de gestion du management est clôturé en appliquant le statut « terminé » à celui-ci.

2.3 La gestion des incidents 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.

C'est ce que l'on retrouve dans l'ISO 27035, une norme de l'ISO qui structure une organisation sur la réponse à incident autour d'une **politique** de gestion des incidents de sécurité

Ce document de politique définit les éléments structurants. Il doit être pragmatique et adapté aux enjeux et à la taille de l'entité. Une bonne appropriation de cette politique par les salariés est indispensable.

La norme donne un guide des incontournables de ce document :

- Organisation générale (rôles et responsabilités, processus, équipes internes et externes, service de l'état, régulateurs ou agences nationales,...) ;
- Grandes définitions (en particulier événement, incident, alerte et vulnérabilité) ;
- Sources (techniques, informationnelles et humaines) de remontée d'événements ;
- Catégorisation et priorisation des incidents suivant des critères à préciser ;
- Analyse post-mortem et analyse des retours d'expérience ;
- Activation et fonctionnement de la cellule de réponse aux incidents (CSIRT - Cybersecurity Incident Response Team) comprenant les modalités de notification des incidents majeurs et d'activation de la cellule de crise.

- Sensibilisation des collaborateurs et formations dédiées.

Les phases de qualification et de décision reposent sur des expertises techniques très diverses en fonction des incidents.

Se lancer dans la construction d'un processus de gestion des incidents en interne ou pour un client en mode service, il est important d'être conscient des expertises nécessaire pour opérer :

Les **expertises techniques** liées à la **« surveillance détection »**qui s'appuient sur les solutions et équipements disponibles (IPS/IDS : intrusion detection / Prevention System, Security Information and Event Management : SIEM, logs locaux, analyseurs réseaux, supervision. . .), les clients, partenaires et fournisseurs (CERT : Computer Emergency Response Team privés ou étatiques, opérateurs...).

Les expertises dépendent des caractéristiques techniques et fonctionnelles **des systèmes d'information** (technologies, logiciels, architectures, services cloud...). Le niveau de compétence des équipes internes ou externes qui assurent la maintenance conditionne la qualification d'un événement dit incident.

Des **expertises plus orientées vers la réaction** pour traiter la réaction nécessitent des expertises pointues en sécurité (analyse du mode de propagation d'un code malveillant, analyse « forensic » d'un poste de travail compromis. . .).

Le **niveau de capacité de support technique** ou de gestion de crise (Helpdesk) détermine le temps et la qualité de la réaction à l'incident et sa capacité de limiter les impacts. Les mauvaises décisions prises dans l'urgence pendant un incident sont souvent dues à un manque d'expertise ou d'organisation dans la phase d'organisation de ces plans de réaction à incidents. Ces mauvaises décisions peuvent amplifier les impacts de l'incident voire faire basculer l'entité en crise.

Le champ d'application de la norme est une approche planifiée et structurée :

- De la détection, de l'analyse et du reporting des incidents de sécurité,
- De la réponse et du management des incidents de sécurité,
- De la détection, de l'analyse et du management des vulnérabilités de la sécurité de l'information,
- De l'amélioration continue de la sécurité de l'information et de la gestion d'incident, dans le cadre plus global du management de « l'incidentologie » et des vulnérabilités.

2.4 Continuité d'activité avec l'ISO 22301

Autour de la gestion de la résilience, il existe un cadre normatif qui permet d'organiser les plans de continuité d'activité qui sont le pendant opérationnel de la DSI de la gestion de l'incident de cybersécurité. La vocation des plans de continuité d'activité (Business Continuity Plans) est donc de répondre à des situations critiques, souvent rares mais pouvant avoir des impacts graves pour l'entreprise. Ces plans prennent en compte (inondation, incendie, accident industriel), on intègre de plus en plus souvent des risques

de conflit social, des attaques cyber de grande ampleur, des ruptures de service d'un prestataire ou sous-traitant. La démarche pour concevoir son système de management de la continuité d'activité est l'objet de la norme ISO 22301. Une étape initiale consiste à analyser les impacts métiers (Business Impact Analysis) pour identifier les activités critiques et les besoins de reprise. La norme ISO 22317 fournit un cadre et des bonnes pratiques pour réaliser cette analyse. La norme ISO 22301 est intitulée « Sécurité sociétale — Systèmes de management de la continuité d'activité — Exigences ». Elle constitue un outil des organisations « pour anticiper et gérer la continuité de leurs activités » et « délivre des lignes directrices pour la mise en place d'un système de management spécifique et efficace ». Elle a été publiée dans sa première version en 2012, puis révisée en 2019. Cette norme remplace des standards qui étaient jusque-là nationaux, comme celui par exemple britannique (BS-25999).

En effet, lorsque toutes les stratégies de défense ont échoué et que la crise survient il est important de définir une cadre de résilience : Comment l'entreprise peut-elle continuer à fonctionner, rétablir ses activités le plus rapidement possible et essayer de minimiser son impact ?

C'est pour répondre à ces questions que cette norme ISO 22301 a été construite. Aujourd'hui encore, de nombreuses PME qui subissent une cyberattaque incapacifiante ne survivent pas . C'est souvent par un manque de en place d'une gestion de la continuité d'activité. La cyber résilience encore un parent pauvre de la cybersécurité, non pas le manque travaux, mais simplement pas la non prise de conscience du risque de rupture totale de l'activité par des attaques informatiques.

La norme ISO 22301 se fixe comme objectif de spécifier les exigences pour planifier, établir, mettre en place et en œuvre, contrôler, réviser, maintenir et améliorer de manière continue un système de management documenté afin de se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et de s'en rétablir lorsqu'ils surviennent.

En résumé, elle aide les organisations « à se montrer mieux préparées et plus solides face à des interruptions de toutes sortes » grâce notamment à la création d'un système de management de la continuité d'activité. Ce système de management de la continuité permettra également de s'assurer que les objectifs de la continuité soient alignés avec ceux de l'entreprise et de la direction .

Cette norme a été rédigée de façon générique pour englober le plus de situations possibles et pouvoir être appliquée dans des organisations de tous types et de toutes tailles . Les exigences spécifiées dans la norme le sont de manière « relativement brève et concise » afin de pouvoir servir de base pour la certification. Pour avoir un peu plus de détaille, vous pouvez consulter la norme ISO 22313 donne les bonnes pratiques de la Continuité d'activité.

3. REAGIR

3.1 La gestion de l'incident au quotidien

3.1.1 De l'alerte à l'incident

Comme nous avons vu dans le chapitre sur la détection des attaques certains événements peuvent conduire à des alertes. Le terme alerte est ici synonyme d'alarme. Ces alertes doivent être analysées par des analystes (Ingénieur SOC par exemple) pour caractériser si un événement ayant atteint à un niveau d'alerte doit être traité comme un incident de sécurité. L'alerte positionne les équipes dans un état de vigilance toutefois l'enregistrement d'un événement en incident engage les processus de réponse à incident. La question majeure est de savoir qui mobiliser pour gérer l'incident. A l'image d'une alarme incendie, l'analyse de l'évènement qui à lever cette alarme doit être rapidement effectuée afin de valider l'événement comme devant être pris en charge par un processus dédié. Ce processus de vérification, est important pour éviter des FAUX POSITIF qui risquent de mobiliser des équipes de manière inadaptée.

Tout incident qui n'est pas correctement confiné et traité peut, et généralement, dégénérer en un problème plus important qui peut finalement conduire à une violation de données dommageable, à des dépenses importantes ou à l'effondrement du système. Une réponse rapide à un incident aidera une organisation à minimiser les pertes, à atténuer les vulnérabilités exploitées, à restaurer les services et les processus et à réduire les risques que posent les incidents futurs.

3.1.2 L'incident

La problématique de la réaction à un incident dit « cyber » c'est que ce type d'incident peut mettre en doute la confiance que l'on peut avoir dans son propre système système d'information. Comme ce SI risque d'être utiliser dans les mécanismes pour opérer la réaction, il est aussi important de gérer les critères de confiance et d'usage en mode dégradé. Dans un premier dans nous allons donc partir de principe que le système d'information dispose de mécanisme permettant d'avoir confiance dans les systèmes qui opèrent pendant la réponse à incident. Nous allons aborder la réaction à incident suivant les 3 volets :

- Remédier et reconfigurer pour limiter l'impact ;
- Enquêter sur l'incident ;
- Neutraliser les sources de menaces ;

Il est à noter que la norme donne des éléments d'organisation mais manque d'aspect pratique avec par exemple des fiches reflexes.

3.1.3 Priorisation de l'évènement

Comme un événement est un changement observable du comportement normal d'un système, d'un environnement, d'un processus, d'un flux de travail, il est important de classifier ce changement dans un mécanisme de priorisation. Il existe trois types de classification de base :

- **Normal** : un événement normal n'affecte pas les composants critiques ni ne nécessite de contrôle des modifications avant la mise en œuvre d'une résolution. Les événements normaux ne nécessitent pas la participation du personnel supérieur ou la notification de la direction de l'événement. **Escalade** - un événement escaladé affecte les systèmes de production critiques ou nécessite la mise en œuvre d'une résolution qui doit suivre un processus de contrôle des modifications. Les événements escaladés nécessitent la participation du personnel supérieur et la notification des parties prenantes de l'événement. **Urgence** - une urgence est un événement qui peut :
  - avoir un impact sur la santé ou la sécurité humaine ;
  - enfreindre les contrôles primaires des systèmes critiques ou sensibles de l'entreprise ;
  - affecter matériellement les performances des composants ou en raison de l'impact sur les systèmes de composants empêcher les activités qui protègent ou peuvent affecter la santé ou la sécurité des individus ;
  - être considéré comme une urgence par la politique de sécurité de l'entreprise .

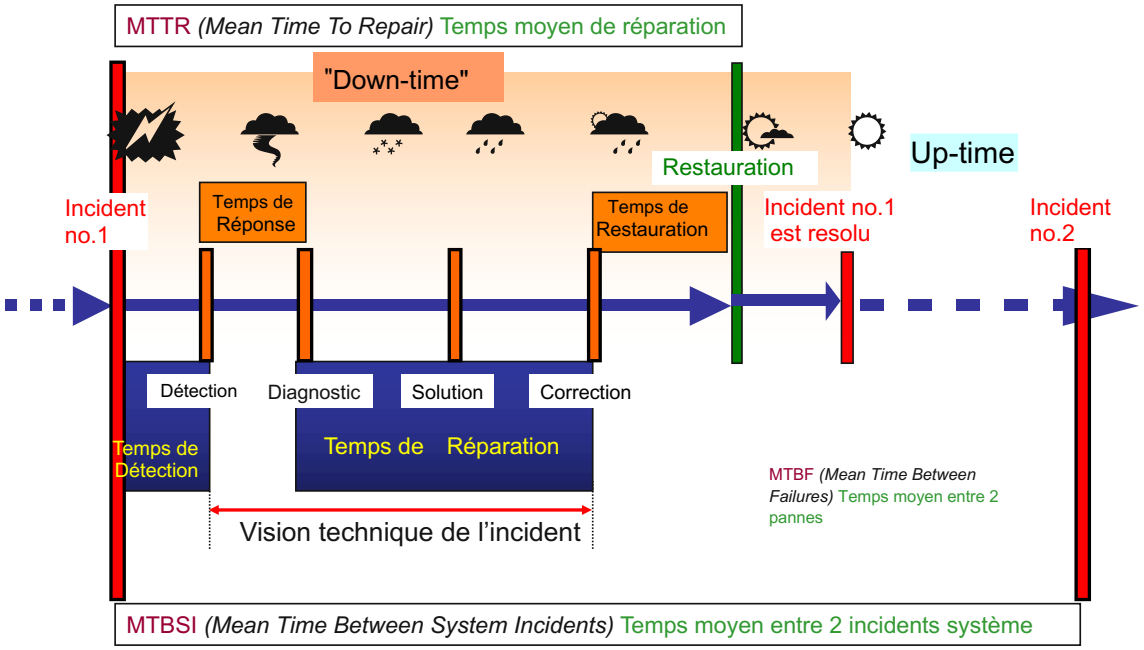

FIGURE 3. Incidents

3.2 Remédiation

Une question qui se pose lors d'une reprise d'activité est la confiance que nous avons dans le système. La difficultés après une attaque informatique ou une compromission, ou tout simplement une suspicion c'est la simple question de savoir si nous savons enlever toute la source de l'attaque. Reste-t-il des résidus.

FIGURE 4. Incidents

3.3 Aspect juridique de la réaction

4. ENQUETER

4.1 Analyse de l'attaque

Les enquêtes sur les intrusions visent à vérifier les modes d'attaque à l'œuvre dans les cyber-incidents, à déterminer les activités réseau postérieures aux événements, et à détecter les points terminaux et les comptes utilisateurs additionnels qui ont été compromis. Il est essentiel à la tenue d'une enquête sur une intrusion de tenter de comprendre l'étendue potentielle d'un incident.

4.2 Evaluation détaillée des dommages

Les évaluations des dommages consistent pour l'essentiel à identifier les données qui ont été infiltrées ou exposées, ainsi qu'à tenter de comprendre les motivations des cyber-adversaires et la suite possible des événements. Les évaluations peuvent mettre en lumière des enjeux qu'il importe de soulever et renseigner votre entreprise sur les conséquences éventuelles de la perte, de la fuite ou de l'exfiltration de données.

4.3 Se préparer et s'entrainer

4.4 Forensic

5. Techniques et Organismes connexes

5.1 Threats Hunting

Mettre place une interaction entre l'attaque et la défense, pour provoquer une continuité de l'attaque avec des objectifs qui peuvent aller du maintien de l'attaque pour découvrir les scénarios

Exemple se mettre en proxy et modifier les fichiers ex-filtrées pour les corrompre et faire

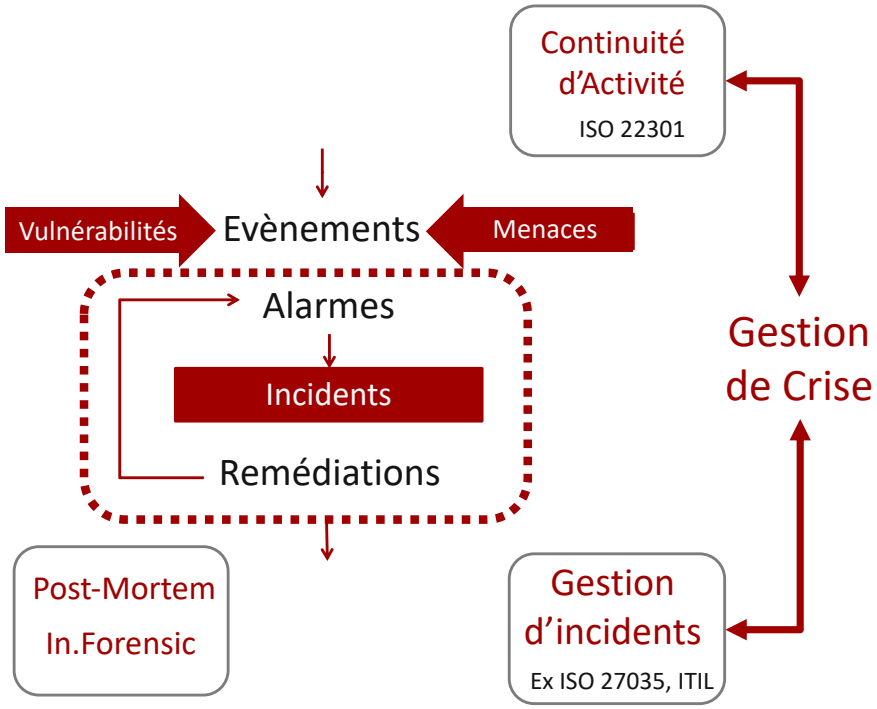

FIGURE 5. Incidents

en sort que l'attaquant reste plus longtemps. Réagir, gestion de crise, à quel moment géré t'on la crise.

5.2 HoneyPots

5.3 Hackback

5.4 CERT et CSIRT

Idéalement, les activités de réponse aux incidents sont menées par l' équipe de réponse aux incidents de sécurité informatique de l'organisation (CSIRT), un groupe qui a été précédemment sélectionné pour inclure la sécurité de l'information et le personnel informatique général . L'équipe peut également comprendre des représentants des services juridique, des ressources humaines et de la communication. L'équipe de réponse aux incidents suit le plan de réponse aux incidents (Cyber Incident Plan) de l'organisation, qui est un ensemble d'instructions écrites qui décrivent la réponse de l'organisation aux événements du réseau, aux incidents de sécurité et aux violations confirmées.

5.4.1 Un peu d'histoire

un peu d'histoire, dans les années 80, au coeur du réseau IP les plus célèbre ARPANET, un étudiant de CORNELL UNIVERSITY implanta, sur le réseau, un ver qui se propageait, se répliquait et exploitait les failles de sécurité UNIX de l'époque. Afin d'exterminer ce ver

internet, une équipe d'analyse, en compagnie d'experts MIT, a été créée pour identifier et corriger les failles d'une part, et d'autre part développer des solutions d'éradication. A la suite de cet incident, le DARPA (Defense Advanced Research Projects Agency), maitrise d'ouvrage d'ARPANET, décida la mise en place d'une structure dédiée, le CERT coordination Center, pour résoudre tous types d'incidents sécurité. Le terme CERT est le plus utilisé et le plus connu mais il s'agit d'une marque américaine qui appartient à l'université Carnegie Mellon. Les CSIRT peuvent demander l'autorisation d'utiliser le nom de « CERT ». En 2019, environ 80 CSIRT sont affiliés et autorisés à utiliser cette marque CERT.

Ces CSIRTs peuvent être internes à l'entreprise ou externes de type publique ou commercial.

Dans bien des entreprises, il y a des moments où il est indispensable de faire intervenir des équipes experts externes généralement nécessaires pour faire face à une crise évoluant rapidement. Ces équipes fournissent une assistance d'expertise en fonction de l'étendue et de la gravité de l'incident et de la charge nécessaire à sa remédiation.

Ces équipes de type CSIRT peuvent rapidement apporter les ressources et l'expertise adapté au contexte de l'incident.

Mais il y a beaucoup à faire par retirer tous les bénéfices de ce type de services. Et cela commence par une compréhension claire de la manière dont fonctionne le processus de réponse aux incidents, et ce que l'on attend d'une équipe externe dans une telle situation.

Un CSIRT est généralement une équipe de sécurité opérationnelle, composée d'experts de différents domaines (malwares, test d'intrusion, veille, lutte contre la cybercriminalité, forensics...). Elle est chargée de prévenir et de réagir en cas d'incidents de sécurité informatique.

- En **prévention**, elle assure notamment une veille sécurité (les nouvelles attaques, les nouveaux logiciels malveillants, les dernières vulnérabilités) pour « connaître » l'état de la menace et évaluer les propres vulnérabilités de son organisation.
- En **réaction**, elle analyse et traite les incidents de sécurité en aidant à leur résolution.

Le travail de fond d'un CSIRT est de centraliser la réponse à incident toutefois il sert de relais vers l'intérieur de l'organisation (pour prévenir les menaces en informant et sensibilisant) et surtout vers l'extérieur à destination des autres CSIRT et CERT mondiaux et de la communauté cybersécurité.

5.4.2 Les missions d'un CSIRT,

Les missions d'un CSIRT sont nombreuses, mais il est intéressants de prendre les 5 principales définies par le CERTA (CERT de l'Administration Française).

- Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;

- Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CSIRT, contribution à des études techniques spécifiques ;
- Etablissement et maintenance d'une base de données des vulnérabilités ;
- Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;
- Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CSIRT nationaux et internationaux.

Il existe plusieurs types de CSIRT :

- Le CSIRT interne (d'entreprise ou d'une administration / université / Etat...) que l'on trouve dans de grandes entrerprises bancaires comme par exemple (Le monde bancaire ayant été précuseurs dans l'utilisation de CERT). Le CSIRT a alors un rôle d'«alerte» et de « cyber pompier », prêt à intervenir pour aider et conseiller l'ensemble du groupe, ses filiales voire ses clients en cas d'incident de sécurité.
- Les CSIRT «commerciaux». Ce sont des équipes d'experts appartenant à des prestataires de services qui proposent des offres de veille, des réponses à incidents à leurs clients. cela peut être considéré un CSIRT externalisé et mutualisé.

5.5 Faire intervenir un CSIRT commercial

5.5.1 Phase d'analyse

La première chose à laquelle souhaite accéder un CSIRT est un présentation de situation la plus clair et concise que possible.

Les organisations qui sont la cible d'une attaque par logiciel malveillant à plusieurs couches, ou d'une intrusion réseau, n'ont souvent pas une idée complète de l'origine ou de l'étendue du problème. Pourtant, il est vital de pouvoir fournir autant de détails que possible. « Normalement, lorsqu'un client entre en contact avec un spécialiste de la réponse à incident, la première chose que l'on veut savoir, est ce qui est en train de se passer », relève ainsi Bob Shaker, directeur des opérations stratégiques, préparation cyber et réponse, chez Symantec.

Un spécialiste de la réponse à incident va vouloir des informations sur ce qui conduit son client à penser qu'il a été compromis, quand et comment il l'a découvert, et encore s'il l'a fait grâce à une source interne ou externe, des autorités locales, par exemple, ou encore un émetteur de cartes bancaires.

Durant la phase d'établissement de l'étendue du problème, il est vital de disposer de personnes internes à l'organisation sachant quelles informations il est possible de fournir au prestataire, qu'il s'agisse de journaux d'activité ou de tout autre élément de preuve,

explique Jim Aldridge, directeur de l'activité de conseil et Mandiant, l'unité de réponse aux incidents de FireEye.

Le prestataire va utiliser l'information qui lui est fournie pour évaluer l'étendue des dégâts et déterminer le type de ressources – y compris les experts à dépêcher sur place – nécessaires. « Lorsqu'une organisation contacte un prestataire de services de réponse à incident, il faut engager une discussion sur l'étendue du problème pour s'assurer que le prestataire comprend la situation sur laquelle il va intervenir », relève Aldridge.

5.5.2 La phase de contractualisation

Une fois que le prestataire a eu l'opportunité d'évaluer la situation, il pourra fournir une estimation de ce dont il aura besoin pour son intervention. Le contrat proposer doit généralement contenir des explications détaillées des services qui seront apportés, précisant au passage s'il aidera effectivement à remédier à l'incident, ou s'il ne fera que fournir les informations permettant à son client d'assurer seul la remédiation.

Dans cette phase, il est important de bien comprendre quelle documentation, accès et savoirs seront nécessaires au prestataire. Christopher Pierson, RSSI de Viewpost, une plateforme de paiement en ligne, estime qu'il est « crucial de s'assurer que les bonnes ressources seront fournies ». Les entreprises utilisant des applications et des services en mode Cloud sont parfois limitées dans le choix des tiers d'investigation qu'elles peuvent solliciter. Il est donc important d'examiner ces points avant de signer le contrat.

En outre, il est vital d'identifier les compétences que peut apporter le prestataire, ainsi que ses ressources technologiques, ses outils ou encore ses renseignements sur les menaces.

Signer pour un engagement de longue durée avec un prestataire, avant le premier incident, peut s'avérer profitable : ainsi, il n'est pas nécessaire de consacrer un temps critique en plein incident aux détails du processus de contractualisation, ou d'expliquer ses processus internes de réponse aux incident au milieu d'une crise. De fait, souligne Bob Shaker, « en pleine crise, la personne susceptible de signer un contrat est généralement sur le pont au centre de crise ». Réussir à l'en extraire peut s'avérer difficile. . .

5.5.3 Enquêter sur l'incident

Le CSIRT aura besoin de toute l'information possible : logs systèmes et réseau, diagrammes de topologie réseau, images systèmes, rapports d'analyse du trafic réseau, etc.

Souvent, il est tentant de céder à la panique et d'arrêter les systèmes dans la précipitation. Mais pour Shaker, c'est une mauvaise idée : « la première chose importante est de ne pas éteindre les systèmes. Une fois qu'un système est éteint, une quantité considérable d'éléments de preuve peuvent être effacés, en particulier tout ce qui réside en mémoire vive ».

Les équipes d'investigation utilisent les informations fournies par les entreprises clients, ainsi que celles qu'elles collectent elles-mêmes sur leurs points de terminaison et d'autres

sources, via des outils propriétaires, pour identifier des indicateurs de compromission, relève Kevin Strickland, consultant réponse à incident sénior chez Dell SecureWorks.

C'est après cela que le prestataire est généralement en mesure d'informer son client sur ce qui s'est passé, sur la manière dont l'intrusion est susceptible d'avoir commencé, ou comment le logiciel malveillant a été introduit sur le réseau, et sur quoi faire pour contenir l'incident : « nous allons fournir cette information et indiquer où des actions sont requises », explique Stickland. Et si les options recommandées sont difficiles à mettre en œuvre, il peut y avoir alors quelques aller-retour.

5.5.4 Contrôle et remédiation

L'équipe responsable de la remédiation travaille souvent en tandem avec l'équipe chargée de l'investigation, selon Aldridge. « Nous avons deux flux de travail. Le premier est lié à l'enquête et vise à identifier quels systèmes, comptes et données ont été compromis ; le second touche à la remédiation ». Et dès que la première équipe trouve des éléments relatifs à l'incident, elle les transmet à la seconde qui travaille avec le client à la mise en œuvre des mesures correctrices.

Mais discrétion peut s'avérer essentielle. Pour Strickland, il n'est pas question de laisser les attaquants savoir que l'on est sur leurs traces : « il est très important de comprendre ce qui se passe avant d'effectuer des changements drastiques ».

5.6 Création de son équipe CSIRT

Quelles sont les motivations pour créer un CSIRT dans son entreprise :

- Une augmentation exponentielle du nombre d'incidents sécurité ;
- Une augmentation du nombre et type d'organisations affectées par des incidents sécurité ;
- Un focus de la part des entreprises sur le besoin de politiques sécurité dans le cadre de leur management du risque
- Nouvelles lois et régulations impactant les entreprises en terme de protection des données ;
- Réaliser que les administrateurs systèmes et réseaux ne peuvent pas protéger l'entreprise à eux seuls.

Un CSIRT est composé de plusieurs experts dans différents domaines de la sécurité (intrusions, forensics, malwares, crytpo, etc..) qui préviennent mais surtout réagissent en cas d'incident. Ces experts sont en constante mise à jour des nouveaux vecteurs d'attaques (nouveaux malwares, nouvelles vulnérabilités), tout ceci afin de traiter les incidents de la manière la plus aboutie qui soit. Une véritable équipe CSIRT dans une entreprise à un coût non négligeable, il convient d'en étudier les modalités de de fonctionnement et de couverture.

Création d'un CSIRT

La création d'un CSIRT dans son entreprise, n'est pas chose facile, c'est un vrai sujet de RSSI dans le sens ou des choix sont a faire tant sur les compétences, les moyens, les procédures de travail. C'est un vrai sujet de mémoire pour la fiche techno.

5.7 Gestion de crises

PCA et PRA

reprise d'activité ...

6. Contributions

6.1 Comment contribuer

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.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) [2] . 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.

6.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

6.2.1 Années 2020

- **David BATANY** (Contributeur LATEX) : BOTNET
- **Charly Hernandez** : User and Entity Behavior analytics, UEBA
- **Florian PINCEMIN (Orange)** : SIEM en quelques mots

6.2.2 Années 2019

- **François REGIS** (Orange) : CyberHunting

6.2.3 Années 2018

- **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

2. https://github.com/edufaction/CYBERDEF

Table des matières