



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

Eric DUPUIS<sup>1,2\*</sup>

## 🕒 Résumé

Ce document donne quelques grands principes de la gestion des incidents, et la conduite de gestion de crise. Cette partie est préliminaire, en plein travaux, et risque d'évoluer rapidement.

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 unique, mais édité par chapitre dans le cadre de ce cours.

Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101 (SEC101 du Cnam). Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

## 🔑 Mots clefs

Incidents, forensic, crise

<sup>1</sup>Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France

<sup>2</sup>Directeur Orange Campus Cyber

\*email : eric.dupuis@lecnam.net – eric.dupuis@orange.com

## Notes de cours SECOPS 2025-2026

Vérifiez la disponibilité d'une version plus récente de

**CourseNotes-FR-SEC101-33-incidentman.doc.pdf** sur GITHUB CYBERDEF <sup>1</sup>



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



1. <https://github.com/edufaction/CYBERDEF/raw/master/Builder/CourseNotes-FR-SEC101-33-incidentman.doc.pdf>



## Table des matières

<b>1</b>	<b>GERER les incidents</b>	<b>3</b>
1.1	Réponse à incident	4
1.2	Terminologie	4
1.3	Définitions	5
1.4	Sources Incidents	6
1.5	Parcours	6
<b>2</b>	<b>ANTICIPER</b>	<b>7</b>
2.1	Les bons reflexes	8
2.2	Etablir un processus de management	8
2.2.1	Résilience	
2.3	L'intégration dans la gestion des incidents ITIL	9
2.4	La gestion des incidents avec l'ISO 27035	10
2.5	Et avec la NIST 800-61	11
2.6	Continuité d'activité avec l'ISO 22301	12
<b>3</b>	<b>REAGIR</b>	<b>13</b>
3.1	La gestion de l'incident au quotidien	13
3.1.1	De l'alerte à l'incident	
3.1.2	L'incident	
3.1.3	Priorisation de l'évènement	
3.2	Remédiation	14
3.3	Aspect juridique de la réaction	14
<b>4</b>	<b>ENQUETER</b>	<b>14</b>
4.1	Analyse de l'attaque	14
4.2	Evaluation détaillée des dommages	15
4.3	forensique	15
4.3.1	Cadre juridique	
4.3.2	Cadre non-juridique	
4.3.3	Outils	
<b>5</b>	<b>CERT et CSIRT</b>	<b>16</b>
5.0.1	Un peu d'histoire	
5.0.2	Les missions d'un CSIRT,	
5.1	Faire intervenir un CSIRT commercial	17
5.1.1	Phase d'analyse	
5.1.2	La phase de contractualisation	
5.1.3	Enquêter sur l'incident	
5.1.4	Contrôle et remédiation	
5.2	Création de son équipe CSIRT	18
5.3	Gestion de crises	19
5.4	Anticiper les crises	19
<b>6</b>	<b>Méthodes et techniques connexes</b>	<b>19</b>
6.1	Sécurité Offensive vs Défensive	19
6.2	Threats Hunting	19
6.3	HoneyPots	20
6.4	Hackback	20

## Table des figures

1	Les axes de la gestion des cyber-Incidents	6
2	Les axes de la gestion des cyber-Incidents	6
3	Incidents	7
4	Incidents	14



## 1. GERER les incidents

La réponse aux incidents est une approche organisée pour traiter et gérer les conséquences d'une violation de la sécurité ou d'une cyberattaque, également appelée incident informatique ou incident de sécurité (informatique). L'objectif d'une réponse à incident est de gérer la situation de manière à limiter les dommages et à réduire le temps et les coûts de récupération des informations, et de reprise d'activité et de retour à la normale.

La réponse aux incidents de sécurité informatique est devenue un axe majeur de la gestion de la sécurité en entreprise. De nouveaux types d'incidents émergent régulièrement avec des manières d'agir et de réagir différents. Il est important de distinguer les incidents liés à des phénomènes accidentels à ceux liés à des atteintes intentionnelles. Nous distinguerons donc ici la notion d'incident de sécurité d'incident informatique, en nous concentrant sur le volet incident de sécurité considéré comme lié à des attaques informatiques. Les activités préventives basées sur les résultats des évaluations des risques peuvent réduire le nombre d'incidents de sécurité à impact, mais tous ces incidents ne peuvent pas être évités. Une capacité de réponse aux incidents de sécurité est donc nécessaire pour traiter rapidement les incidents, minimiser les impacts, réduire les pertes et destructions, couvrir les faiblesses qui ont été exploitées et restaurer les services numériques.

Idéalement pour des attaques, les activités de réponse aux incidents sont menées par l'équipe de réponse aux incidents de sécurité informatique de l'organisation (« aCSIRT ») car elle nécessite des postures particulières. L'équipe peut également comprendre des représentants des services juridique, des ressources humaines, de la communication, et des risques. L'équipe de réponse aux incidents suit normalement un plan de réponse aux incidents (IRP) 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 impacts confirmés.

Cette réponse planifiée aux incidents est une entreprise complexe, l'établissement d'une capacité de réponse aux incidents réussie nécessite une planification et des ressources importante. La surveillance continue des attaques est essentielle en avant phase. Il est essentiel d'établir des procédures claires pour hiérarchiser le traitement des incidents, tout comme la mise en œuvre de méthodes efficaces de collecte, d'analyse et de communication des données. Il est également essentiel d'établir des relations et d'établir des moyens de communication appropriés avec d'autres groupes internes (par exemple, les ressources humaines, les services juridiques) et avec des groupes externes (par exemple, d'autres équipes de réponse aux incidents (CERT, CSIRT..), les forces de l'ordre).

L'établissement d'une capacité de réponse aux incidents doit comprendre les actions suivantes :

- ▶ Création d'une politique et d'un plan de réponse aux incidents ;
- ▶ Élaboration de procédures pour effectuer le traitement et le signalement des incidents ;
- ▶ Définir des lignes directrices pour communiquer avec des tiers sur les incidents ;
- ▶ Sélection d'une structure d'équipe et d'un modèle de dotation ;
- ▶ Établir des relations et des voies de communication entre l'équipe d'intervention en cas d'incident et d'autres groupes, à la fois internes (par exemple, le service juridique) et externes (par exemple, les forces de l'ordre) ;
- ▶ Déterminer quels services l'équipe d'intervention devrait fournir en cas d'incident ;
- ▶ Recruter et former l'équipe d'intervention en cas d'incident.

Les organisations doivent généralement être prêtes à gérer tout incident, mais elles doivent se concentrer sur leur préparation à gérer les incidents qui utilisent des vecteurs d'attaque courants. Les incidents peuvent se produire de nombreuses façons, il est donc impossible d'élaborer des instructions étape par étape pour gérer chaque incident. Cette publication définit plusieurs types d'incidents, basés sur des vecteurs d'attaque courants ; ces catégories ne sont pas destinées à fournir une classification définitive des incidents, mais plutôt à être utilisées comme base pour définir des procédures de manipulation plus spécifiques. Différents types d'incidents méritent différentes stratégies d'intervention.



Les vecteurs d'attaque les plus courants :

- ▶ Support Media externe / amovible : attaque exécutée à partir d'un support amovible (par exemple, un lecteur flash, un CD) ou un périphérique ;
- ▶ Attrition : attaque qui utilise des méthodes de force brute pour compromettre, dégrader ou détruire des systèmes, des réseaux ou des services ;
- ▶ Web : attaque exécutée à partir d'un site Web ou d'une application Web ;
- ▶ Courriel : une attaque exécutée via un message électronique ou une pièce jointe ;
- ▶ Utilisation incorrecte : tout incident résultant d'une violation des politiques d'utilisation acceptables d'une organisation par un utilisateur autorisé, à l'exclusion des catégories ci-dessus ;
- ▶ Perte ou vol d'équipement : la perte ou le vol d'un appareil informatique ou d'un support utilisé par l'organisation, tel qu'un ordinateur portable ou un smartphone ;

## 1.1 Réponse à incident

La réponse sur incident de sécurité pose de nombreuses problèmes « d'opérationnalité » tant sur les aspects techniques que juridiques ou organisationnels. Dans ce chapitre, nous allons tenter d'aborder les différentes méthodologies et outils qui permettent de répondre aux enjeux de la réactivité en cas d'incident cyber. La réponse à incident, doit s'inscrire dans une organisation cohérente permettant de gérer l'ensemble de la chaîne de traitement d'un incident. On parle de « Gestion des incidents » (*Incident Management*). Cette gestion des incidents est en outre à cheval entre les deux grands processus de la SECOPS, la surveillance-détection et la 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 ayant un impact sur les systèmes d'information, et non les événements de sécurité qui ne réclament pas d'action immédiate. Ces derniers ne sont bien évidemment pas à négliger.

Un événement est donc toute occurrence observable dans un système ou un réseau. Les événements incluent un utilisateur se connectant à un partage de fichiers, un serveur recevant une demande de page Web, un utilisateur envoyant un e-mail et un pare-feu bloquant une tentative de connexion. Les événements indésirables sont des événements ayant une conséquence négative, tels que les pannes du système, les inondations de paquets, l'utilisation non autorisée des privilèges système, l'accès non autorisé aux données sensibles et l'exécution de logiciels malveillants qui détruisent les données. Ce guide ne traite que des événements indésirables liés à la sécurité informatique, pas ceux causés par des catastrophes naturelles, des pannes de courant, etc.

Un incident de sécurité informatique est une violation ou une menace imminente de violation des politiques de sécurité informatique, des politiques d'utilisation acceptables ou des pratiques de sécurité standard ou simplement une menace active ayant un impact sur l'activité de l'entreprise, on peut citer des cas classiques comme : Exemples d'incidents2 :

- ▶ Un attaquant pilote botnet pour générer un DDOS sur un site WEB important de l'entreprise ;
- ▶ Les utilisateurs sont amenés à ouvrir un document envoyé par e-mail contenant un malware ou utilisant une vulnérabilité pour exécuter un outil qui infecte leurs ordinateurs pour établir des connexions avec un hôte externe ou pour chiffrer des fichiers pour réclamer une rançon ;
- ▶ Un attaquant obtient des données sensibles et menace que les détails soient rendus publics si l'organisation ne paie pas une somme d'argent désignée.
- ▶ Un utilisateur fournit ou expose des informations sensibles à des tiers via des services de partage de fichiers poste à poste, ou en utilisant des services non déclarés (Shadow IT)

## 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 nécessiter des moyens techniques importants 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 la gestion des relations avec les services de l'état (CNIL, ANSSI, Police et Gendarmerie ...).

Je vous propose quelques éléments de terminologie avec la correspondance anglo-saxonne afin de se repérer dans les usages et trouver de l'information pertinente lors de vos recherches sur Internet :

- ▶ **Investigations Numériques:***Digital Investigation* ;
- ▶ **Analyse légale:***forensique (Infoforensique)* ;
- ▶ **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 événements de sécurité ou un événement 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.

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 ;

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 description 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.



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

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.

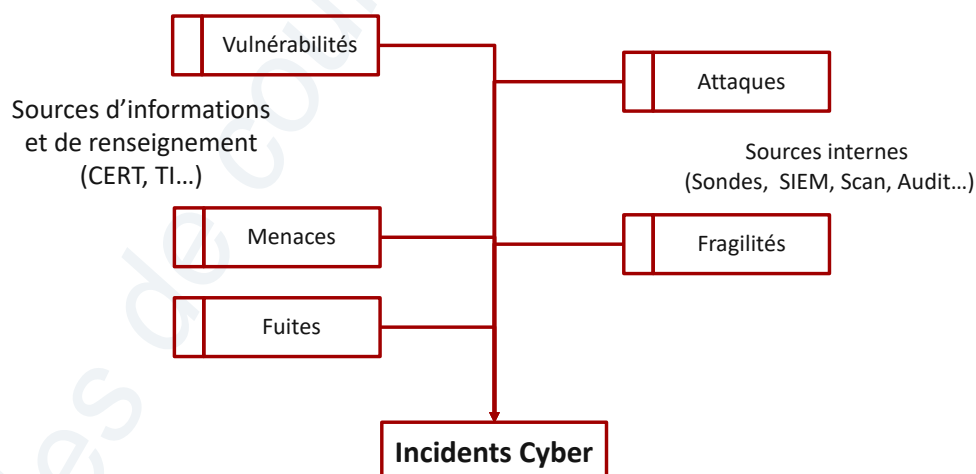


Figure 2. Les axes de la gestion des cyber-Incidents

## 1.5 Parcours

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.

Nous allons toutefois explorer la gestion de l'incident au quotidien sur la base de trois actions fondamentales qui dans l'ordre correspondent au niveau de maturité d'une entreprise en terme de réponse à incident :

- ▶ **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 complétée 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-mortem et le forensique.
- ▶ **Anticiper** : organiser ses mécanismes de réponse (moyens et compétences), intégrer le processus de réponse à incident Cyber dans les mécanismes ITIL de gestion des incidents, organiser une cellule de CSIRT.

## MAINTENIR LA CONTINUITE D'ACTIVITE

### Incidents

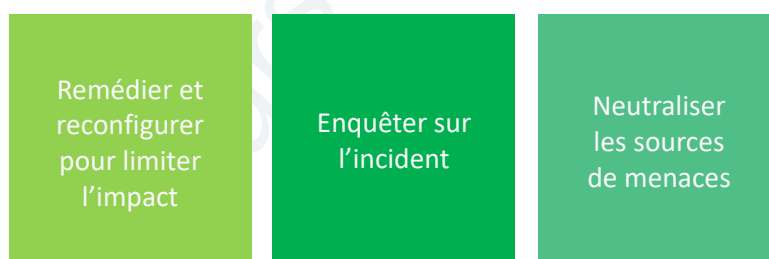


Figure 3. Incidents

Dans certains ouvrages, le cycle des gestions d'incidents informatiques peut être présenté en sept phases : Préparation, Détection, Identification, Isolement, Éradication, Restauration et Activités Post-Incident.

Il est important de différencier les phases de Détection et d'Identification des autres. La première étape consiste à découvrir la présence d'une cyberattaque ce que j'ai présenté pour ma part dans la partie « Threat Detection » alors que la deuxième est composée de l'ensemble des investigations et analyses forensiques permettant de déterminer le type d'attaque et son étendue, d'identifier l'ensemble des systèmes et comptes infectés, ainsi que de préparer un plan d'action pour répondre activement à la cyberattaque (Isolation, Éradication et Restauration). Ce sont ces phases que nous traiterons comme le processus de gestion des incidents.

## 2. ANTICIPER





## 2.1 Les bons reflexes

Anticiper la réponse à incident, c'est s'organiser pour assurer rapidement un certain nombre d'actions rapides :

- ▶ Conduire une levée de doute rapide pour s'assurer qu'il ne s'agit pas de faux positifs.
- ▶ Mobiliser une équipe d'investigation afin de déterminer la cause de l'incident, d'identifier les vecteurs d'infection et de propagation de l'attaquant,
- ▶ Qualifier les impacts immédiats et à venir, construire un plan de défense le cas échéant ;
- ▶ Mettre en sûreté des systèmes critiques (cœur de confiance serveur de sauvegarde, etc.) qui seront nécessaires pour assurer la survie métier en particulier en cas d'incident lié à un impact destructeur comme les rançons logiciel activer les plans de contournement et des procédures en mode dégradé
- ▶ et enfin mobiliser surtout les bonnes compétences, notifier les agences et les régulateurs et déclencher le cas échéant les assurances Cyber.

Cela ne s'improvise pas, et nécessite d'avoir structuré sa réponse à incident.

## 2.2 Etablir un processus de management

### 2.2.1 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 cyberattaque 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 entraînement 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 certains sous-systèmes. Ce type de décision nécessite un 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 cyberattaque et à revenir à son état initial après l'incident sera indifféremment appelé dans ce cours résilience ou continuité d'activité.

## 2.3 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'informations 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 chaîne 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 suit 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.

Les standards de gestion d'incidents (NIST 800-61 et ISO/IEC 27035) recommandent d'isoler les systèmes infectés directement après leur détection ce qui n'est pas toujours facile en contexte opérationnel. Cependant, avec des APT, il doit être supposé que de nombreux systèmes informatiques peuvent avoir été compromis. Ainsi, un confinement trop précoce sans analyse concrète de cette présence aura pour conséquence unique d'informer le cyber-criminel qu'il est potentiellement découvert. Le cyber-attaquant pourra donc réagir et prendre des contre-mesures telles qu'installer de nouveaux logiciels malveillants, détruire les traces numériques liées à son attaque (méthodes anti-forensiques) ou encore endommager l'environnement. Il faut donc dans la mesure du possible identifier intégralement la menace avant d'isoler les systèmes infectés et d'éradiquer les souches malveillantes.

## 2.4 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 nécessaires 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 compétences 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 « forensique » 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.

## 2.5 Et avec la NIST 800-61

Ce référentiel du NIST dénommé « Computer Security Incident Handling Guide » donne des recommandations intéressantes. Contrairement aux normes ISO, l'intérêt des documents de NIST c'est qu'ils sont accessibles et concrets. [GUIDE 800-61](#) <sup>2</sup>

Entre ISO 27035 et NIST 800-61, Les deux normes fondent la gestion des incidents sur une approche cyclique assez comparable :

Cycle de gestion des incidents dans NIST SP 800-61 :

- ▶ Préparation
- ▶ Détection et analyse
- ▶ Confinement, éradication et récupération
- ▶ Activité post-incident

2. <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>



Cycle de gestion des incidents dans ISO / IEC 27035 :

- ▶ Planifier et préparer
- ▶ Détection et signalement
- ▶ Évaluation et décision
- ▶ Réponses
- ▶ Leçons apprises

Les deux normes fournissent des recommandations détaillées sur l'équipe d'intervention en cas d'incident et les politiques et procédures de gestion des incidents. À mon avis, ces deux éléments sont essentiels pour une gestion efficace des incidents - pas les outils techniques. Donc, si vous commencez à développer des capacités de gestion des incidents dans votre organisation, concentrez-vous d'abord sur ces deux. Des procédures opérationnelles standard constamment améliorées aideront votre équipe à être efficace. Ils peuvent également aider à automatiser une partie des tâches. Le NIST 800-61 propose une liste de contrôle de gestion des incidents, avec 9 phases simple à appréhender. Cette liste de contrôle est le premier stade de ce qui doit être maîtrisé, et les personnes en charge de réponses aux incidents doit savoir comment exécuter les étapes contenues dans cette liste. L'ISO / CEI 27035 se concentre davantage sur une organisation elle-même que les bonnes pratiques et le partage. C'est la combinaison des deux qui permet de se préparer correctement. Je conseille aussi la lecture d'un document assez ancien (décembre 2006) mais intéressant pour organiser une petite équipe issu de l'ENISA [Guide de création d'un CSIRT pas à pas](https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-french) <sup>3</sup>

## 2.6 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 incapacitante 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.

3. <https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-french>



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'évènement 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 .

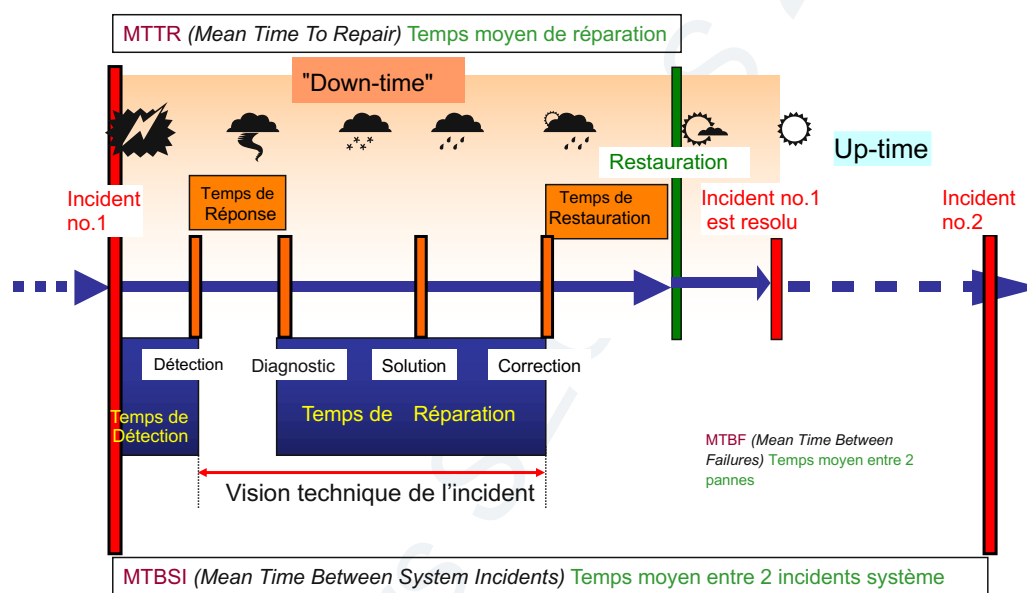


Figure 4. Incidents

## 3.2 Remédiation

Une question qui se pose lors d'une reprise d'activité est la confiance que nous avons dans le système. La difficulté 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.

## 3.3 Aspect juridique de la réaction

⚙ En cours de rédaction, DRAFT non publiable ⚙

# 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 forensique

### 4.3.1 Cadre juridique

L'analyse forensique est une science qui s'intéresse à la recherche de preuves sur des supports numériques pour comprendre un comportement, remédier à un incident et aider à prendre des décisions éclairées. Ces preuves sont des traces, des artéfacts numériques qui fournissent des informations qui, mises bout-à-bout, permettent de dégager un scénario factuel d'événements et d'apporter des réponses aux questions que peut se poser le demandeur. L'analyse forensique est encore appelée investigation numérique, digital forensiques, infoforensique ou informatique légale.

Dans une affaire judiciaire impliquant des supports numériques perquisitionnés pour des enquêtes, le juge peut faire appel à un expert judiciaire pour "faire parler" ces supports, pour l'aider dans sa prise de décision. L'expert judiciaire est une personne physique ou morale, professionnelle dans un domaine technique particulier, spécialement habilitée à exercer son expertise dans des dossiers judiciaires sur sollicitation d'un juge. Son avis ne s'impose pas au juge, qui reste libre dans l'appréciation des éléments fournis.

### 4.3.2 Cadre non-juridique

C'est ce que l'on retrouve le plus souvent avec les entreprises dans un contexte de réponse à incident à la suite d'une attaque du système d'information. Le cas plus fréquent est par exemple l'infection par un ransomware du parc d'une entreprise.

Dans ce type de situation aussi, il y a des sujets sur lesquels se focalisent les analystes en fonction des souhaits du client. Il peut s'agir de trouver qui a fait quoi, comment et quand, et à l'aide de ces éléments, comprendre comment contenir l'incident et surtout comment remédier à la situation au plus vite pour que l'activité reprenne sereinement, si possible.


Tout comme dans le cadre juridique, tout élément trouvé dans les investigations et qui est pénalement répréhensible est à communiquer au commanditaire. Il en est de même de tout écart par rapport à la charte informatique de l'entreprise.

### 4.3.3 Outillage

Il existe de nombreux outillages pour assister un analyste forensique dans la collecte, les analyses, l'interprétation, le stockage et la notarisation.

Les techniques de forensique sont en particulier :

- ▶ La recherche d'information dans les systèmes de fichiers, les bases de données, les réseaux, les systèmes d'exploitation. Ces techniques font appel à des connaissances sur les formats de données, les techniques de stockage et de codage de l'information.
- ▶ L'analyse de ces informations, pour y trouver des traces d'actions, d'intentions ou de phénomènes indiquant un événement recherché.

Je vous engage à aller voir du côté du SANS, avec [SIFT Workstation](https://digital-forensiques.sans.org) <sup>4</sup>

---

4. <https://digital-forensiques.sans.org>





## 5. 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.

### 5.0.1 Un peu d'histoire

Un peu d'histoire, dans les années 80, au cœur 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), maîtrise 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, forensiques...). 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.

### 5.0.2 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 entreprises bancaires comme par exemple (Le monde bancaire ayant été précurseurs 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.

## 5.1 Faire intervenir un CSIRT commercial

### 5.1.1 Phase d'analyse

La première chose à laquelle souhaite accéder un CSIRT est une présentation de situation la plus claire 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.

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.

### 5.1.2 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 proposé 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. 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.

### 5.1.3 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.

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.

### 5.1.4 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.

## 5.2 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 réglementations 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, forensiques, malwares, crypto, 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 fonctionnement et de couverture.

#### **Sujet de mémoire SECOPS : CSIRT**

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



## 5.3 Gestion de crises

Les cyberattaques sont généralement pilotées par les équipes IT, toutefois la majorité des crises associées à des incidents cyber interpellent toutes les activités de l'entreprise.

## 5.4 Anticiper les crises

L'objectif de l'anticipation est de réduire le risque de survenue et de préparer en amont tout ce qui peut l'être. Cela permet de limiter au maximum les impacts négatifs et d'éviter le risque de sur-accident. Cela se met en place avec les mécanismes de PCA/PRA organisés autour par exemple de la norme ISO 22301.

# 6. Méthodes et techniques connexes

## 6.1 Sécurité Offensive vs Défensive

### Sujet de mémoire SECOPS : Offensive Security

Un sujet intéressant pour une fiche TECHNO.

La sécurité offensive est une approche de la sécurité qui vise à identifier et à exploiter les vulnérabilités et les faiblesses d'un système de sécurité dans le but de le compromettre. Elle est souvent utilisée par les entreprises et les organisations pour évaluer la robustesse de leurs systèmes de sécurité et pour identifier les faiblesses qui pourraient être exploitées par des attaquants malveillants.

- ▶ Tests d'intrusion : Les tests d'intrusion consistent à élaborer un scénario d'attaque contre un système dans le but de réaliser un objectif malveillant. Ces tests sont réalisés par des équipes de sécurité (audit, redteam) qui utilisent des outils et des techniques similaires à celles des attaquants malveillants.
- ▶ Recherche de vulnérabilités : La recherche de vulnérabilités consiste à identifier les faiblesses et les points faibles d'un système et en particulier des systèmes de sécurité dans le but de d'inclure ces vulnérabilités dans une chaîne d'attaque.

La sécurité offensive est un peu controversée, car elle implique de simuler en profondeur des attaques malveillantes contre les systèmes et les systèmes de sécurité eux-mêmes. Cependant, elle est considérée comme un moyen efficace d'identifier et de corriger les vulnérabilités avant qu'elles ne soient exploitées par des attaquants malveillants.

## 6.2 Threats Hunting

### Sujet de mémoire SECOPS : Chasse et ATP

Un sujet intéressant pour une fiche TECHNO.

Le Threat Hunting est une technique qui consiste à rechercher activement des menaces cachées au sein d'un système. Il s'agit d'une approche proactive de la sécurité qui vise à identifier les menaces qui ont réussi à passer inaperçues des outils de sécurité traditionnels et à les éliminer avant qu'elles ne causent des dommages.

Il implique généralement l'utilisation de différentes techniques et outils pour analyser les données de sécurité et rechercher des anomalies ou des comportements suspects qui pourraient indiquer la présence d'une menace. Les équipes de Threat Hunting travaillent souvent en collaboration avec les équipes de sécurité de l'information et de l'analyse de données pour identifier et éliminer les menaces cachées.

Le Threat Hunting fait partie des expertises de plus en plus demandées ces dernières années en raison de l'augmentation des attaques de malware avancées et des menaces ciblées, qui peuvent passer inaperçues des



outils de sécurité traditionnels. Il est considéré comme un moyen efficace de renforcer la sécurité d'un système et de protéger contre les menaces qui pourraient autrement échapper aux défenses.

Ces métiers vont au delà de la simple "chasse" aux menaces discrètes et s'élargie vers les techniques mises en place pour gérer les interactions entre l'attaquant et les équipes de défense comme par exemple provoquer une continuité de l'attaque avec des objectifs qui peuvent aller du maintien de l'attaque pour découvrir les scénarios pensés par l'attaquant.

### 6.3 HoneyPots

#### **Sujet de mémoire SECOPS : HoneyPots**

Un sujet intéressant pour une fiche TECHNO.

Les honeypots sont des systèmes de sécurité particulier. Ils visent à attirer et à identifier les attaquants en simulant des cibles vulnérables ou attractives au sein d'un réseau ou d'un système d'information d'entreprise. Ils sont conçus pour ressembler aux systèmes existants ou à des données sensibles plausibles. Toutefois, ils sont isolés du système sensibles et ne contiennent pas d'informations ou de données sensibles pour l'entreprise. Ils sont équipées pour permettre de facilement maintenir le contact avec l'attaquant pour le pousser à dévoiler ses techniques et objectifs.

Lorsqu'un attaquant pénètre un honeypot, il lui est laissé la latitude de conduire son attaque, ses actions sont enregistrées, ce qui permet aux équipes de sécurité de comprendre comment des attaques sont menées et de développer des stratégies pour se protéger contre elles. Les honeypots peuvent également être utilisés pour détourner l'attention des attaquants et les empêcher de cibler des cibles réelles.

Il existe différents types de honeypots, tels que les honeypots de réseau, les honeypots de système et les honeypots de données. Ils sont utilisés en combinaison avec d'autres technique de sécurité, tels que les pare-feux et les systèmes de détection... Ce sont des techniques utilisées soit par les équipes de détection et de réponse soit par les équipes de protection. En fonction de l'usage les méthodes et les concepts d'usage peuvent être différents.

### 6.4 Hackback

#### **Sujet de mémoire SECOPS : Hackback**

Un sujet intéressant pour une fiche TECHNO.

Le hackback est une réponse à une attaque qui consiste à attaquer un système informatique qui a été utilisé pour mener une attaque contre un autre système. Il s'agit d'une approche controversée de la sécurité qui implique de prendre l'initiative et de mener une attaque contre un attaquant malveillant plutôt que de se contenter de se défendre contre lui.

Le hackback est souvent utilisé pour collecter des informations sur l'attaque initiale et sur l'attaquant, qui peuvent être utilisées pour mieux se protéger contre les futures attaques. Cependant, il est également controversé en raison des risques qu'il pose, notamment en termes de dommages potentiels causés aux systèmes ciblés et de la possibilité de violer les lois et les réglementations en matière de sécurité de l'information.

Il est important de noter que le hackback est considéré comme étant à la limite de la légalité dans la majorité pays et qu'il peut entraîner des poursuites judiciaires si utilisé de manière inappropriée. La réponse externe d'une entreprise est généralement judiciaire.

En France, en particulier, l'article 21 du chapitre IV "Dispositions relatives à la protection des infrastructures vitales contre la cybermenace" stipule bien que l'État, et seul l'État, peut "répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. Par ailleurs ce droit à la réponse active ne s'improvise pas. Car avant d'estimer avoir une



réponse active à réaliser, encore faut-il être certain de l'identité de son assaillant numérique, ce qui n'est pas encore spécialement facile, si ce n'est même extrêmement complexe.

