Shape

Description automatically generated

|  |
| --- |
| Sylvain Depasse  1-30-2023 |

|  |
| --- |
| Incident Response |
| Incident Response Plan |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **CYBERSECURITE** | | |
| **POLITIQUE** | **Incident Response Plan** | | | |
| **Policy** **ID:** | **Add ID Number** | **Date de création: 8/24/2022** | | |
| **Approved** **by:** |  | **Reviewed**  **(No changes made)** | **☐** | **Date** |
| **Approved** **by:** |  | **Revised**  **(Changes made)** | **☐** | **Date** |
| **Area:** | **Choose Area** | **Repealed**  **(No longer active)** | **☐** | **Date** |
| **Department:** | **Choose Department** | **Prior** **Policy: N/A** | | |
| **Applies** **to:** | **All Areas** |  | | |
|  | | | | |
| **Additional Approvals**  Additional reviews and approvals by internal and external stakeholders. | | | | |
| **Approver Title** | | **Area / State / Agency** | | |
|  | |  | | |
|  | |  | | |
|  | | | | |
| **Data** **Classification:** **Confidential** | | **Electronic Approvals are maintained in the Policy Repository** | | |
|  | | | | |
| **Additional** **Information:** | | | | |
|  | | | | |
|  | | | | |

Contents

[1 Introduction 3](#_Toc127177402)

[2 Définitions : 3](#_Toc127177403)

[3 Niveaux de gravités : 3](#_Toc127177404)

[4 Information De Contacts: 3](#_Toc127177405)

[5 Rôles et Responsabilités du personnel (CERT) Uniwan : 3](#_Toc127177406)

[6 Processus de réponse aux incidents : 3](#_Toc127177407)

[6.1 Planifier/Préparer 3](#_Toc127177408)

[6.2 Détecter/Signaler 3](#_Toc127177409)

[6.3 Evaluer et décider 3](#_Toc127177410)

[6.4 Répondre 3](#_Toc127177411)

[6.5 Revue Après Action 3](#_Toc127177412)

[7 Plan de communication spécifique en cas d’incident : 3](#_Toc127177413)

[8 Préparation appel au CCB : 3](#_Toc127177414)

[9 Références aux Régulation et Standards 3](#_Toc127177415)

[10 Références aux autres documents internes 3](#_Toc127177416)

[11 Autres références externes 3](#_Toc127177417)



**Important** :

Ce document doit être disponible à tout moment ainsi que ses annexes, une version papier devra être prévue auprès de chaque personne susceptible de devoir participer à la bonne exécution de ce même plan.

Aucune des étapes détaillées ci-dessus ne devra être délaissée ! Effectivement, même le fait de documenter votre avancée est primordiale. Il en va du maintien et de l’évolution de ce présent plan.

# Introduction

La cybersécurité est un enjeu majeur pour les entreprises de toutes tailles et de tous secteurs, et la protection des données sensibles est l'une des préoccupations les plus importantes pour les entreprises qui gèrent les informations de leurs clients.

Rappel : Confidentialité, intégrité et disponibilité sont les maîtres mots de la cybersécurité.

Ce plan de réponse aux incidents est étudié pour garantir que nous traitons systématiquement les événements de sécurité de l'information de manière efficace et efficiente. Ce faisant, nous pouvons minimiser les conséquences négatives pour l'organisation, notre personnel et nos clients.

Son contenu vous fournira un process pas à pas expliquant comment aborder un problème spécifique.

Il identifie et décrit les rôles et les responsabilités de l'équipe d'intervention en cas d'incident.

Vous y trouverez aussi un manuel vous guidant pour l’établissement des communications nécessaires, ainsi que les personnes de contacte concernées en fonction du type et du degré de l‘incident.

!!L'équipe d'intervention en cas d'incident est responsable de la mise en œuvre du plan !!

Quatre principes de base pour notre plan de réponse aux incidents. Ils sont appelés ici, dès le début, pour servir de rappel pour chaque incident :

* Affirmez ce que vous savez (ou croyez) être vrai d'une manière qui peut être prouvée (ne présumez pas !)  
  Exemple:  
  => Lors de l’analyse, vous aurez accès à l’itinéraire de l’attaquant. Les données aux quelle il aura eu accès pourront être présumée consultée.   
  => A l’inverse, si son itinéraire n‘indique pas d’accès à une certaine donnée, celle-ci ne sera pas considérée comme consultée car rien ne nous l’indique.
* Les affirmations fausses aident à exclure ce qui n'est pas, tout comme les affirmations correctes vous permettent de vous rapprocher d'une cause.  
  Exemple:  
  => Face à un incident de WebApp, lors de l’analyse, si vous questionner la victime et que celle-ci vous assure n’avoir divulgué aucun accès, c’est une affirmation fausse vous permettant de mettre hors de cause la victime, tout en gardant à l’esprit que celle-ci les aura peut-être donnés sans même s’en rendre compte.   
  => A l’inverse, si celui-ci nous affirme avoir divulguer ses accès, volontairement ou par mégarde, c’est une affirmation vraie qui nous permettra d’investiguer cette probabilité, sans en écarter aucunes autres.
* Cherchez la réponse la plus simple au problème.  
  => Vous êtes face à un parc de plus de 10-15 machines, un incident vous oblige à isoler l’infrastructure de l’internet extérieure. Que feriez-vous ?  
   - Déconnecter chacune des machines indépendamment ?  
   - Déconnecter à la source, de façon à agir vite de simultanément sur les machines de l’infrastructure.
* Garder à l’esprit qu’il n’y a pas de solution simple et universelle

En suivant ce plan nous augmentons considérablement nos chances de transformer un incident de catastrophe potentielle à success-story. Effectivement, plutôt que d’être seul et désarmé, vous aurez avec vous ce plan et ses AddOn, qui vous permettrons de garder votre calme, tout en répondant de façon optimale.

# Definitions:

* SOC : Security Operation Center
* SANS (SysAdmin, Audit, Network, Secure) : Est une organisation visant à mutualiser l’information concernant la sécurité des systèmes d’information.
* CERT (Computer Emergency Response Team) : Equipe de réaction aux incidents
* Revue après action (RAA) : Une revue après action est un processus d'examen structuré qui a lieu après un événement. Le processus décrit généralement ce qui s'est passé en détail, tente d'identifier les raisons pour lesquelles l'événement s'est produit et désigne les domaines à améliorer afin d'éviter ces événements ou les événements similaires à l'avenir.
* Cyber Security Event : Un changement de cybersécurité susceptible d’avoir un impact sur les opérations d’une organisation
* Adverse event (évènement indésirable) : Evènement avec des conséquences négatives.
* Security Incident : Violation ou menace imminente de violation des politiques de sécurité informatique, des politiques d'utilisation acceptable ou des pratiques de sécurité standard qui compromettent la confidentialité, l'intégrité ou la disponibilité des ressources d'information ou des opérations.
* Gestion des incidents de cybersécurité : La gestion des incidents se fera via un processus visant à se préparer, détecter, rendre compte, évaluer, réagir, tirer des enseignements de ces incidents.
* CIA (Confidentiality, Integrity, and Availability) : Confidentialité, Intégrité et Disponibilité : Ce sont les trois composants essentiels de la triade CIA, un modèle de sécurité de l'information destiné à guider les procédures et les politiques de sécurité d'une organisation
* Confidentialité : Le mot "confidentiel" est défini comme étant « le caractère d’une information confidentielle, secret ». En sécurité de l’information, le terme « confidentialité » signifie qu’une information, une donnée **n’est accessible que par des personnes autorisées**. Plus la donnée, plus l’information est de caractère sensible, plus la liste des personnes autorisées à y accéder doit être restreinte.
* Intégrité : Le Larousse défini le terme « intégrité » comme un “état de quelque chose qui a conservé sans altération ses qualités, son état originel”. En informatique, garantir l’intégrité des données signifie garantir que les données n’aient subi aucune modification non-autorisée, quelle qu’elle soit, durant la communication ou la conservation. Cela signifie qu’elles sont exactement les mêmes que lors de leur création
* Disponibilité : En informatique, la disponibilité a pour but de garantir l’accès à une application, un système, une donnée. Les conséquences d’une perte en disponibilité ne sont pas du tout les mêmes en fonction de la nature des activités de l’organisation touchée.

# Niveaux de gravités :

Pour rappel, les classifications de gravité se feront sur base de 5 niveaux différents : P1 (niveau de gravité/priorité les plus élevé), P2, P3, P4 et P5 (niveau de gravité/priorité le plus bas)

Plus en détails :

* P1 – HAUTE : Plus de 80 % du personnel est incapable de travailler, SYSTÈME CRITIQUE hors ligne sans résolution connue.   
  Risque élevé / violation définitive des données sensibles des clients ou des données personnelles.  
  Grave atteinte à la réputation - susceptible d'avoir un impact sur l'entreprise à long terme.
* P2 - MOYENNE : 50 % du personnel incapable de travailler.  
   Risque de violation de données personnelles ou sensibles, Systèmes non critiques affectés, ou SYSTÈME CRITIQUE affecté avec résolution connue (rapide).  
   Atteinte grave potentielle à la réputation
* P3 - BASSE : Petite équipe/équipe individuelle incapable de travailler.  
   Violation possible de petites quantités de données non sensibles.  
   Faible risque pour la réputation, Petit nombre de systèmes non critiques affectés par des résolutions connues
* P4 - FAIBLE : Aucun membre du personnel à l’arrêt.  
  Violation possible de petites quantités de données non sensibles.  
   Faible risque pour la réputation, Petit nombre de systèmes non critiques affectés par des résolutions connues
* P5 – Minime : Impacte minime, voir une ou deux machines non sensibles/non critiques affectées.

# Informations De Contacts:

CCB (division CERT) :   
Entièrement gratuit, joignable de 8h à 18h. Le CCB offre un soutien à la lutte contre les incidents, pas seulement, mais c’est ce qui nous intéresse ici.   
 Tel : +3227/90.33.85  
 Mail : [cert@cert.be](mailto:cert@cert.be)

Merci de se référer au chapitre portant sur la préparation pour l’appel au CCB.

Décisions légales :

En cas de prise de décision légale, contacter en premier lieu

* (CEO) :

En cas de non réponse, vous contacterez :



Décision systèmes :

Dans le cas d’une décision à prendre en rapport au fonctionnement système (arrêt du système complet, certains services) demande d’autorisations auprès de :

Voir utilité de préciser la personne à même de communIquer les infos tech aux organismes externes

Ajouter les personnes aux responsabilités et rôles fixe et leur contact dans cette partie du plan (voir Mr Vander Elst)

Incident P.5 et P.4:  
  
Pour ce type d’incident il vous faudra contacter l’équipe CERT SD1 :



Incident P.3 :  
  
Pour ce type d’incident il vous faudra contacter l’équipe CERT SD2 :



Incident P.2 :  
  
Etant donné que l’on peut parler ici de données sensibles ou personnelles, il vous faudra juger l’utilité de contacter les services autoritaires en rapport à l’incident et/ou le propriétaire des données impactées.  
   
Il vous faudra aussi contacter l’équipe CERT SD2 :

Pour ce type d’incident il est possible SD3 soit impliqué, dans ce cas contactez :

Incident P.1 :

Etant donné que l’on peut parler ici de données sensibles ou personnelles, il vous faudra juger de l’utilité de contacter les services autoritaires en rapport à l’incident et/ou le(s) propriétaire(s) des données impactées.

Il vous faudra aussi contacter l’équipe CERT SD3 :

# Rôles et Responsabilités du personnel (CERT) Uniwan :

Cette partie du plan vous permettra de retrouver facilement vers qui vous tourner en cas de.

Le gestionnaire d’incident ()

* Il détient toute autorité pour la gestion de l’incident. Son rôle principal sera de coordonner et gérer toute l’intervention de réponse.
* Il constitue l’équipe de réponse et distribue les rôles suivants selon le contexte d’occurence et temporel de l’incident

Le responsable technique ()

* En contact direct avec le gestionnaire d’incident, ceux-ci travailleront en étroite collaboration.  
  Il sera chargé de piloter l’équipe CERT et d’élaborer des théories sur les défaillances et leurs causes.
* L’une de ses responsabilités est aussi de décider de l’utilité en cas de besoin d’un expert externe afin d’arriver à une résolution optimale.
* Il devra suivre la bonne documentation de l’intervention et participer aux réunions post-mortem.

Responsable communications ()

* Son rôle principal sera d’être le lien entre les équipes CERT, la haute direction, et si besoin le client lui-même (afin d’informer ou de prendre des informations)

Responsable du support client ((si différent du responsable com.))

* Il se chargera de s’assurer que les tickets générés, les appels téléphoniques, les tweets... En rapport avec l’incident soit pris en charge et reçoivent une réponse au plus rapide.
* Il aura donc la charge de la bonne transmission des informations reçues

Secrétaire ()

* Il est chargé de consigner toutes les informations en rapport à l’incident et les efforts fournis.
* Son rôle consistera aussi à garder à jour le calendrier de réponse (« qui, quoi, quand » a participé de quelque manière qu’il soit.  
  Ce rôle est très important, notamment pour l’étude post-mortem afin d’évaluer les possible modification d’organisation qui pourraient être reconnu.

Gestionnaire des problèmes ()

* Son rôle sera d’aller au-delà de la résolution de l’incident et d’identifier les causes profondes et donc tous changements à apporter pour éviter la répétition d’un même ticket.

Haute direction : CEO

Incident response P1 : SD3

Incident response P2 : SD2 – SD3

* A la réception du ticket niveau 2, le SD2 procèdera à une première analyse d’évaluation afin d’éventuellement l’envoyer vers SD3 en cas de complexité trop importante.

Incident response P3 : SD2

Incident response P4 : SD1

Incident response P5 : SD 1

L’équipe CERT SD1 se compose de manière fix de :

L’équipe CERT SD2 se compose de manière fix de :

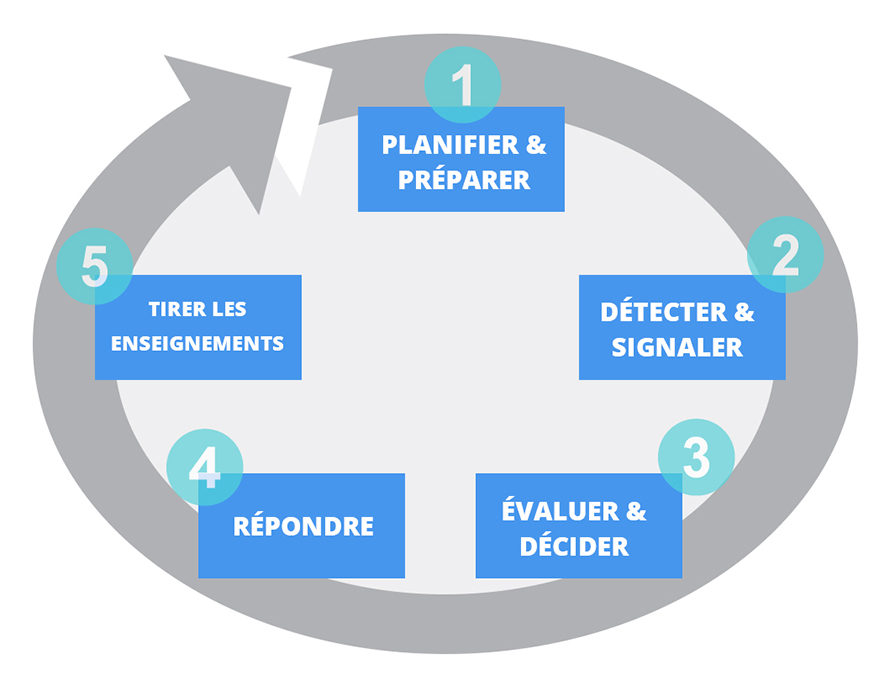
L’équipe CERT SD3 se compose de manière fix de :

# Catégorisation des incidents

Ce tableau représente les différents plan spécifique déjà mis en place par l’organisation.  
Il à pour but de facilité la recherche des plans nécessaire en cas de, mais aussi à avoir un bref aperçu de ce qui est déjà couvert aujourd’hui.

|  |  |  |
| --- | --- | --- |
| **Type d’incident** | **Incident Respons Plan** | **Incident Respons Diagramme** |
| Phishing | IR1 | DIR1 |
| Compromised Credentials | IR2 | DIR2 |
| WebApp | IR3 | DIR3 |
| Ransom | IR4 | DIR4 |
| DataBreach | IR5 | DIR5 |
| Android Compromis | IR6 | DIR6 |
| IOS Compromis | IR7 | DIR7 |

# Processus de réponse aux incidents :



# Planifier/Préparer

Notre équipe CERT doit être une machine bien rodée lorsque l’incident se produit, et cela demande du travail (mise en situation éventuelle, suivis de veilles technologiques, information continue,.. ). Définition d’une politique de sécurité d’entreprise (voir CSO) : elle porte sur l’utilisation acceptable des données de l’entreprise, les conséquences en cas de violation de la sécurité “et des définitions de ce que l’on entend par incident de sécurité (voir lexique ) » Voir Politique.   
Ce guide par étapes définit la façon dont l’équipe CERT doit gérer un incident de sécurité, y compris comment elle doit documenter les incidents et les communications internes et externes. Chacune des étapes de celui-ci se devront d’être respectées et appliquées du mieux qu’il soit.  
Effectivement cela nous permettra une réponse de qualité, idéalement au plus rapide mais aussi de tirer des leçons des incidents passés.

La procédure suivante est organisée en étapes logiques plus à des fins d'organisation qu'une chronologie stricte du moment où les choses doivent se produire. De nombreuses étapes du processus suivant peuvent se produire et se produiront simultanément, et ce n'est pas grave. S'il est logique d'effectuer une étape avant les autres, faites-le tant que toutes les actions pertinentes se produisent. Un exemple de ceci est que le confinement initial se produit généralement avant que l'identification ne soit terminée.

# Détecter/Signaler

* **Identification des signes d’un incident (signes précurseurs et indicateurs) :** les signes précurseurs et les indicateurs sont des signaux spécifiques indiquant qu’un incident est sur le point de se produire ou est déjà survenu.  
    
  Exemples :
  + Relevé de log
  + Contrôle des tâches planifiées
* **Analyse des indices découverts :** une fois ces signaux identifiés, l’équipe de réponse à incident doit déterminer si le signe précurseur ou l’indicateur fait partie d’une attaque ou s’il s’agit d’un faux positif.
* **Documentation de l’incident :** s’il s’agit d’une attaque avérée, l’équipe doit commencer à documenter tous les faits en rapport avec l’incident et continuer à consigner toutes les mesures prises tout au long de l’intervention. Cette étape est très importante et se doit d’être suivie avec rigueur.
* **Priorisation de l’incident :** L’équipe de réponse à incident ne peut pas se contenter de prioriser les incidents par ordre chronologique mais plutôt leurs attribuer un score en fonction de leur impact sur les fonctions métier (arrêt des effectifs), la confidentialité des informations concernées et la capacité à se remettre de l’incident.  
  Cette étape est, selon le NIST, la décision la plus importante du processus de réponse à incident.
* **Notification de l’incident :**après analyse et priorisation de l’incident, l’équipe doit avertir les personnes / départements internes concernés. Il vous suffira dès lors de vous tourner vers l’organigramme et personnes de contactes prévus afin que la délégation soit fluide et cohérente.

**Pour mener à bien votre détection et analyse il vous faudra par exemple :**

* **Surveiller les alertes** **:** Via les outils installés, alerte de détection de tentative d’énumération, de connexion, voir même une alerte antivirus...
* **Filtrer et analyser les logs : Relevé les logs de la machine, black liste si nécessaire, contrôler la présence d’anomalie...**
* **Relever les indicateurs de compromission (IoC) : Cred Invalid, Comportement anormale de la machine, changement de format des fichiers...**
* **Récupérer des preuves : Prélevez des échantillons, prenez des photos, prenez des captures d’écrans, ...**
* **Questionner des data base de hash : SiteGuarding, VirusTotal, AstraSecurity,..**
* **Check réputation IP : CriminalIp, Talosintelligence, ..**
* **Contrôle d’éventuelles persistances : En Vous référant à la cheatsheet pertinente, il vous faudra manipuler le système afin de détecter d’éventuelles tâches planifiées par l’attaquant (exécution de script).**

# Evaluer et décider

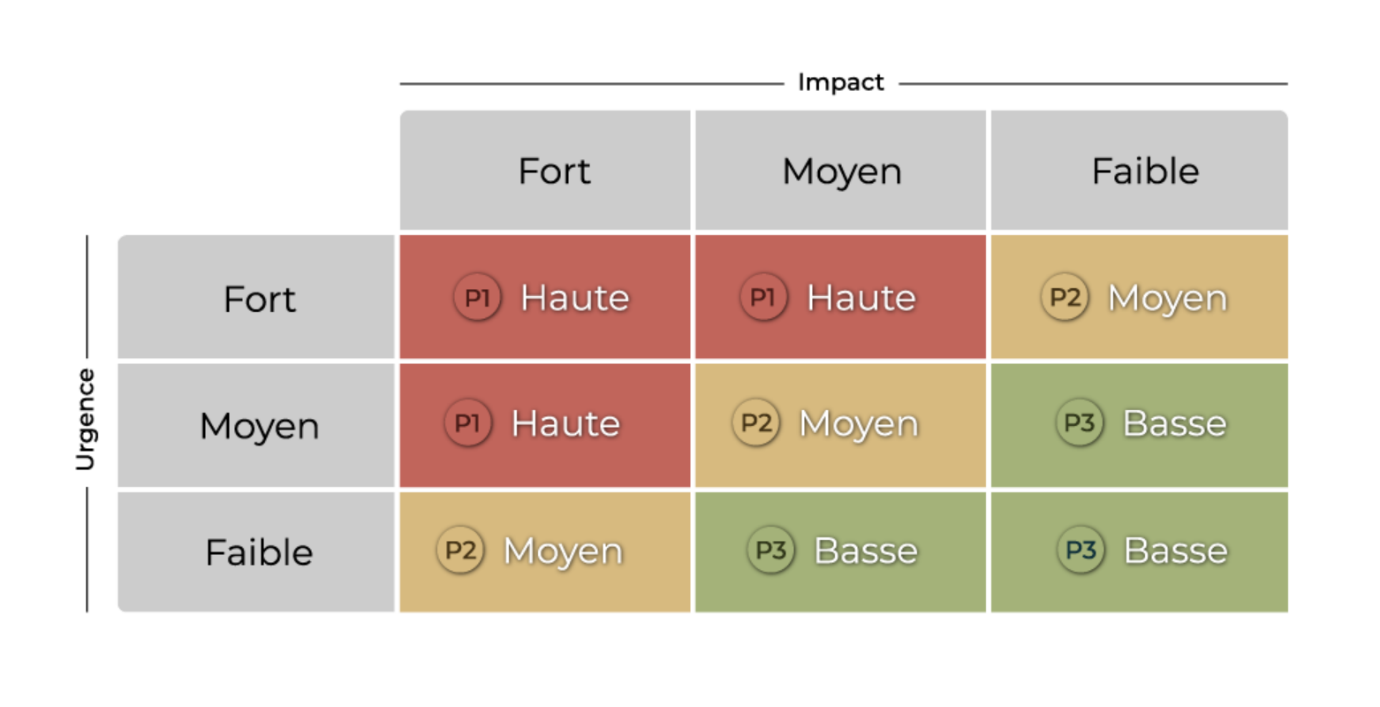
Évaluer l'impact et appliquer un niveau de gravité.

Une fois qu'un incident de cybersécurité a été détecté et validé, la prochaine étape est d'évaluer l'ampleur de la compromission et les dommages potentiels pour l'organisation. Cette étape est essentielle pour déterminer la meilleure approche à adopter pour contenir et éradiquer l'incident.

L'évaluation peut inclure les éléments suivants :

* Identification des systèmes et des données affectés : il est important d'identifier les systèmes et les données qui ont été compromis ou qui pourraient être compromis par l'incident. Cela peut aider à limiter la propagation de l'incident et à minimiser les dommages potentiels.
* Détermination de la cause de l'incident : il est important de comprendre la cause de l'incident afin de prévenir les futures attaques similaires. Il peut s'agir d'une erreur humaine, d'une vulnérabilité du système, d'un malware, d'une attaque par phishing, etc.
* Détermination de l'impact de l'incident : il est important de déterminer l'impact de l'incident sur l'organisation. Cela peut inclure des pertes financières, des violations de données, des perturbations du service, des problèmes de conformité réglementaire, etc.
* Classification de l'incident : en fonction de l'impact et de la gravité de l'incident, il peut être utile de le classer selon une échelle de gravité afin de déterminer la réponse appropriée.

En résumé, l'évaluation ou l'analyse de l'incident est une étape cruciale de la méthodologie de réponse aux incidents de cybersécurité du NIST, qui permet de comprendre l'ampleur de la compromission et les dommages potentiels pour l'organisation, afin de déterminer la meilleure approche à adopter pour contenir et éradiquer l'incident.  
En fonction des proportions de l’incident, mettre en place si besoin des canaux de communications via TEAMS de Microsoft (par exemple !) afin d’assurer une bonne gestion de l’incident en question.  
Cette phase d’évaluation est très importante car elle permettra de définir le niveau de priorité correct à attribuer aux tickets. Cependant, si vous avez un doute, choisissez le niveau d’évaluation supérieur.  
Effectivement, il est préférable d’envoyer un ticket P1 au niveau 2 que l’inverse, car cela pourrait influencer négativement la rapidité de réponse à l’incident en court.  
 !! se référer à la définition des niveaux de gravité. !!



# Répondre

La réponse à l’incident correspond au confinement et à l’éradication de la menace/incident, suivit de la reprise des activités.  
  
L’objectif ici est de stopper les effets d’un incident avant que celui-ci ne cause d’autres dommages. Une fois l’incident isolé, le CERT peut prendre le temps nécessaire pour peaufiner les étapes suivantes. Cela consiste notamment à prendre les mesures requises pour résoudre la cause de l’incident et rétablir le fonctionnement normal des systèmes.  
Ces décisions étant susceptibles d’impacter la productivité, le CERT doit faire preuve de prudence dans leur approche et aux besoins prendre contact avec les personnes concernées par ces impacts.

Nous parcourrons donc 3 étapes bien distinctes (confinement/ éradication/ reprise) durant lesquelles le CERT se devra d’opérer, par des actions comme :

1. Confinement :  
   =>Exemples :

* Isolement des systèmes (peut inclure des systèmes critiques, des machines virtuelles, des sites Web)
* Isoler ou mettre en quarantaine à distance des machines ou des parties du réseau
* Déconnecter complètement/arrêter les systèmes
* Réinitialisation des informations d'identification et possibilité de bloquer ou de verrouiller l'accès à distance
* Blocage du trafic

1. Eradication :  
   => Exemples :

* Suppression des fichiers malveillants (nettoyage ou reconstruction des machines, nettoyage des profils utilisateur, utilisation d'antivirus ou déploiement de scripts)
* Réinitialisation des comptes d'administrateur et de service du domaine, et réinitialisations à l'échelle du domaine
* Bloquer ou supprimer à distance les fichiers et/ou processus malveillants
* Bloquer ou alerter sur des modèles spécifiques (par exemple, des modèles de trafic)
* Stopper/kill des process
* Stopper/supprimer des sessions, utilisateurs
* Supprimer des persistances

1. Reprise :  
   => Exemples :

* Surveillance de l'activité du réseau et de l'hôte pour confirmer que les actions ont réussi
* Réimagé des machines
* Déployer un BackUp

Les stratégies de confinement, d’éradication et de reprise sont basées, entre autres, sur les critères suivants :

* Criticité des ressources impactées
* Type et gravité de l’incident
* Importance des systèmes touchés pour les processus métier critiques
* Ressources nécessaires pour mettre en œuvre la stratégie

Attention :   
  
Ces processus doivent être documentés et les preuves collectées en permanence. Deux raisons justifient une telle démarche : d’une part, pour en savoir plus sur l’attaque et améliorer l’expertise de l’équipe de sécurité et, d’autre part, pour se préparer à d’éventuels litiges.

Notez que :

La différence entre le confinement et l'éradication de la menace réside dans l'objectif de chaque étape et les actions qui en découlent.

Le confinement est une étape immédiate qui vise à empêcher la propagation de l'attaque et à isoler les systèmes affectés. L'objectif est de limiter les dommages causés par l'attaque en empêchant la propagation de l'attaque et en protégeant les données sensibles. Les actions qui en découlent peuvent inclure l'isolement des systèmes affectés, la restriction de l'accès aux données volées, l'analyse des données volées et la préservation des preuves pour une enquête ultérieure.

L'éradication de la menace, quant à elle, vise à supprimer complètement la menace de l'environnement de l'entreprise. L'objectif est de s'assurer que toutes les traces de l'attaque ont été supprimées et que l'entreprise est de nouveau en mesure de fonctionner normalement. Les actions qui en découlent peuvent inclure la suppression de tous les fichiers infectés, la mise à jour des logiciels de sécurité, la modification des mots de passe, etc.

En résumé, le confinement est une étape initiale qui vise à arrêter l'attaque et à limiter les dommages, tandis que l'éradication de la menace vise à supprimer complètement la menace de l'environnement de l'entreprise et à rétablir la sécurité. Les deux étapes sont essentielles pour une réponse efficace aux incidents de sécurité.

# Rapport

Dans un monde où les cyberattaques sont de plus en plus fréquentes et sophistiquées, les entreprises doivent être prêtes à faire face à ces menaces. C'est là que les SOC entrent en jeu, en surveillant en permanence les systèmes de sécurité pour détecter et répondre aux incidents de sécurité.

Lorsqu'une cyberattaque survient, il est essentiel pour le SOC d'établir un rapport détaillé sur l'incident. Le rapport doit inclure des informations sur la nature de l'attaque, les méthodes et techniques utilisées par l'attaquant, les vulnérabilités exploitées et les systèmes ou données compromis. En comprenant ces informations, le SOC peut prendre des mesures pour renforcer les mesures de sécurité et empêcher des attaques similaires à l'avenir.

En plus de renforcer la sécurité de l'entreprise, un rapport sur une cyberattaque est important pour répondre aux parties prenantes. Les clients, les partenaires commerciaux, les régulateurs et les actionnaires ont besoin de comprendre ce qui s'est passé, comment l'entreprise a réagi et comment elle va prévenir de telles attaques à l'avenir. Un rapport détaillé peut aider à rassurer ces parties prenantes et à renforcer la confiance dans l'entreprise.

Documenter l'incident est également important pour le suivi des progrès et l'analyse des risques. Les rapports sur les incidents de sécurité peuvent être utilisés pour établir des preuves dans le cadre d'une enquête criminelle ou d'un litige civil. Ils peuvent également être utilisés pour la formation des équipes de réponse aux incidents, pour améliorer les politiques de sécurité et pour sensibiliser les employés aux bonnes pratiques de sécurité.

En résumé, établir un rapport après une cyberattaque est essentiel pour comprendre l'attaque, améliorer la sécurité de l'entreprise, répondre aux parties prenantes et documenter l'incident. Les rapports détaillés peuvent aider les SOC à renforcer la sécurité des entreprises, à prévenir des attaques futures et à renforcer la confiance des parties prenantes.

# Revue Après Action

Chaque incident devrait être l’occasion d’apprendre et de s’améliorer, tout comme **chaque incident majeur devrait donner lieu à une réunion regroupant toutes les parties intéressées afin de tirer les leçons qui s’imposent de l’incident.** Une telle réunion devrait également être encouragée en cas d’incident de moindre gravité, avec pour objectif d’améliorer la sécurité en général et la prise en charge des incidents en particulier. Dans le cas d’attaques majeures, n’hésitez pas à faire intervenir tous les acteurs de l’entreprise concernés par l’incident et pensez tout particulièrement à inviter ceux dont la coopération sera nécessaire lors d’incidents futurs.

Au cours de cette réunion, passez en revue les points suivants :

* Ce qui s’est produit et quand
* Quelle a été la réactivité et l’efficacité de l’équipe de réponse à incident
* Si les procédures documentées ont été respectées
* Si ces procédures étaient adaptées
* Quelles informations manquaient, et dans quelles circonstances
* Quelles actions ont retardé la reprise
* Ce qui aurait pu être fait différemment
* Quelles sont les mesures à prendre pour prévenir de futurs incidents
* Quels sont les signes précurseurs ou indicateurs à rechercher

Consignez les points importants de la réunion, attribuez les tâches à accomplir ou les mesures à prendre et envoyez par la suite un procès-verbal de la réunion par courriel à ceux qui n’ont pas pu y assister.

Les conclusions de ces réunions peuvent devenir un outil de formation important pour les nouvelles recrues. Elles peuvent également servir à actualiser les politiques et les procédures, ainsi qu’à créer une base de connaissances formelles qui peut être utile pour gérer des incidents ultérieurs.

# Plan de communication spécifique en cas d’incident :

Rappel : La Politique de sécurité d’Uniwan en termes de communication sera suivie et ce même durant le process de réponse

Gardez à l’esprit qu’il n’est pas impossible que les moyens de communications habituelles aient été impactés. C’est pourquoi chacun des outils listés devra être utilisable à tout instant.

Voir présence d’un numéro de passerelle secourt si nécessaire.

Outils de communications :

* Téléphone
* Teams
* Mail
* Courriers électronique chiffrés (PGP par exemple)
* Sur papier
* En personne

Il est important de prendre connaissance des application et implication légales liées aux incidents possibles.

Effectivement, dans certains cas il sera nécessaire de prendre contact avec les institutions concernées, tel que la police ou à L’autorité De Protection Des Données Personnelles.

Par exemple, dans le RGPD, la loi impose de signaler toute brèche de données à caractères personnelle susceptible de présenter un risque élevé pour les personnes dont les données ont été piratées, à la fois à l’autorité de protection des données et aux personnes dont les données ont été piratées (délais de 72h après détection).

Aucun contact de publicité ne pourra être établit et aucune information ne devra être divulguée sans l’accord de la Haute Direction.

# Préparation appel au CCB:

Le fait de faire appel au CCB n’est aucunement payant.  
Lors de la prise de contact avec le CCB, plusieurs informations vous seront demandées. Cette liste vous permettra d’être près au moment de prendre contact.

1. Vos propres coordonnées (pour un rappel direct (sans intermédiaire))
2. Le type d’incident
3. La date de l’incident
4. L’incident est-il toujours en cours ?
5. Comment avez-vous constaté l’incident ?
6. Quel est l’impact de l’incident ?
7. Avez-vous déjà entrepris des actions ou pris des mesures ? Si oui, lesquelles ?
8. Disposez vus de journaux ou d’autres données utiles ?
9. Qui avez-vous déjà informé de l’incident ?
10. Qu’attendez-vous de ce signalement ? \*

\*Effectivement il est possible de ne les appeler que pour signaler un incident, sans pour autant attendre un soutient. Il vous sera donc demandé ce que vous attendez. Par exemple, un soutien technique, ou de simples conseils ou encore signaler un incident résolu (avec sa résolution), pour qu’il ait déjà une procédure dans leur base de données en cas d’attaque similaire.

# Références aux Régulation et Standards

Les références aux standards internationaux et régulation relatives au secteur de l’entreprise sont repris dans le tableau ci-dessous.

|  |  |  |
| --- | --- | --- |
| **ISO** **27001:2013** | **NIST SP 800-53** | **HIPAA** |
| A.8.1.3 Acceptable Use of Assets | AC-20, PL‑4, PS-6 | Workstation Use §164.310(b) |

# Références aux autres documents internes

Les références à d’autres politiques, standards, procédures ou documents internes sont listées dans le tableau ci-dessous.

|  |  |
| --- | --- |
| **Document Name** | **Document ID** |
| Non-discrimination and Anti-harassment Policy |  |

# Autres références externes

Les références utilisées ou citées durant la rédaction de ce document sont listées dans le tableau ci-dessous.

|  |  |  |  |
| --- | --- | --- | --- |
| **Référence** | **Titre** | **ID de Référence** | **Année** |
|  |  |  |  |