# Journal de gestions d’incidents

## Scenario 1 :

Une petite clinique de santé américaine, spécialisée dans la prestation de services de soins primaires, a subi un incident de sécurité un mardi matin, vers 9 h 00. Plusieurs employés ont signalé qu’ils n’étaient pas en mesure d’utiliser leurs ordinateurs pour accéder à des fichiers tels que les dossiers médicaux. Les activités de l’entreprise ont été interrompues, car les employés ne pouvaient plus accéder aux fichiers ni aux logiciels nécessaires à l’exécution de leur travail.

De plus, les employés ont également signalé qu’une demande de rançon s’affichait sur leurs ordinateurs. Cette demande indiquait que tous les fichiers de l’entreprise avaient été chiffrés par un groupe organisé de pirates malveillants, connus pour cibler les organisations dans les secteurs de la santé et du transport. Pour rétablir l’accès aux fichiers chiffrés, la note de rançon exigeait une grosse somme d’argent en échange de la clé de déchiffrement.

Les attaquants ont réussi à pénétrer dans le réseau de l’entreprise en utilisant des courriels d'hameçonnage ciblés, envoyés à plusieurs employés. Ces courriels contenaient une pièce jointe malveillante qui installait un logiciel malveillant sur l’ordinateur de l’employé dès qu’elle était téléchargée.

Une fois qu’ils ont obtenu l’accès, les attaquants ont déployé leur randsomware, qui a chiffré des fichiers critiques. L’entreprise n’a plus pu accéder à des données sensibles sur les patients, ce qui a entraîné de graves perturbations dans ses activités. Elle a été contrainte d’arrêter ses systèmes informatiques et de contacter plusieurs organisations pour signaler l’incident et obtenir une assistance technique.

| **Date :**<br>22/09/2025 | **Entrée : #1** |
|---|---|
| Description | Un groupe de cybercriminel a réussi à pénétrer dans le réseau de l'entreprise en utilisant des courriels d'hameçonnage ciblés, ils ont par la suite déployé leur randsomware, qui a chiffré des fichiers critiques de l'entreprise. |
| Outils utilisés | Playbook |
| Les 5 W | Qui a causé l'incident ? Un groupe de cybercriminel<br>Que s'est-il passé ? Un randsomware a été déployé ce qui a chiffré des données critiques de l'entreprise.<br>Quand l'incident s'est-il produit ? Mardi matin vers 9 h 00<br>Où l'incident a-t-il eu lieu ? Dans une entreprise de santé Américaine<br>Pourquoi l'incident est-il arrivé ? L'incident s'est produit lorsque les attaquants ont réussi à accéder au réseau de l'entreprise grâce à des courriels de phishing. Ces courriels contenaient des pièces jointes malveillantes qui ont été téléchargées par les employés. Peu de temps après leur téléchargement, le randsomware a été déployé (chiffrement de fichiers critiques), provoquant d'importantes perturbations dans le fonctionnement de l'entreprise. Les attaquants exigent désormais le paiement d'une certaine somme d'argent. |
| Notes Additionnel | Comment éviter que cela se reproduise ? Mettre en place des entrainements contre le phishing, crée fréquemment des backup de donnée pour éviter la paralysie du système. |

## Scenario 2 :

L'organisation a connu un incident de sécurité le 22 janvier 2024 à 19h20, au cours duquel un individu a réussi à obtenir un accès non autorisé à des PII ainsi qu'à des données financières de clients. Environ 50 000 enregistrements clients ont été affectés. L'impact financier de l'incident est estimé à 100 000 dollars, en coûts directs et pertes potentielles de revenus. L'incident est désormais clos et une enquête approfondie a été menée.

Le 20 janvier 2024, vers 15h13 (heure du Pacifique), un employé a reçu un courriel provenant d'une adresse externe. L'expéditeur affirmait avoir volé des données clients et exigeait un paiement en cryptomonnaie de 25 000 dollars pour éviter leur divulgation sur des forums publics. L'employé, pensant qu'il s'agissait de pourriel, a supprimé le message. Le 22 janvier 2024, le même employé a reçu un nouveau courriel du même expéditeur. Celui-ci contenait un échantillon des données volées et portait la demande de rançon à 50 000 dollars. C'est ce jour-là que l'employé a alerté l'équipe de sécurité, qui a immédiatement lancé une enquête.

| **Date :**<br>28/09/2025 | **Entrée : #2** |
|---|---|
| Description | Un individu non autorisé a réussi à accéder aux PII et aux données financières des clients. L'incident a été constaté lors de la phase de détection et d'analyse, ainsi que durant la phase de confinement, d'éradication et de rétablissement. |
| Outils utilisés | Playbook |
| Les 5 W | Qui a causé l'incident ? Un individu externe non autorisé<br>Que s'est-il passé ?<br>Un accès non autorisé aux données personnelles et financières a eu lieu. Une tentative d'extorsion a été faite avec une demande de rançon en cryptomonnaie. L'impact financier est estimé à cent mille dollars.<br>Quand l'incident s'est-il produit ?<br>Le premier message a été reçu le 20 janvier 2024 à 15h13. L'incident a été confirmé le 22 janvier 2024 à 19h20. Le second message a été reçu le même jour avec un échantillon de données volées.<br>Où l'incident a-t-il eu lieu ? L'incident s'est produit dans les systèmes de l'organisation. Les communications ont eu lieu par courriel externe. |

| | |
|---|---|
| Notes Additionnel | <u>Comment éviter que cela se reproduise ?</u><br>Il faut renforcer la formation pour sensibiliser davantage aux cyberattaques.<br>Signaler l'incident à un analyste SOC de niveau 2.<br>Mener l'enquête en utilisant un guide de procédures (playbook). |

## Scénario 3

Vous êtes analyste de niveau un au sein d'un centre des opérations de sécurité (SOC) dans une entreprise de services financiers. Vous avez reçu une alerte concernant un fichier suspect téléchargé sur l'ordinateur d'un employé.
Vous enquêtez sur cette alerte et découvrez que l'employé a reçu un e-mail contenant une pièce jointe. La pièce jointe était un fichier tableur protégé par mot de passe. Le mot de passe du tableur était fourni dans l'e-mail. L'employé a téléchargé le fichier, puis a saisi le mot de passe pour l'ouvrir.
Lors de l'ouverture du fichier, une charge utile malveillante s'est exécutée sur son ordinateur.Le hachage est une méthode cryptographique utilisée pour identifier de manière unique un logiciel malveillant, agissant comme l'empreinte digitale unique du fichier.
Maintenant que vous disposez du hachage du fichier, vous allez utiliser VirusTotal pour découvrir des IoC (Indicateurs de Compromission) supplémentaires associés au fichier.

| | |
|---|---|
| **Date :** | **Entrée : #3** |

| | |
|---|---|
| 30/09/2025 | |
| Description | Cet incident s'est produit lors de la phase de Détection et d'Analyse. Le scénario me permet d'enquêter sur un hachage de fichier suspect. J'ai analysé et déterminé si l'alerte représentait une menace réelle.<br><br>Hachage de fichier SHA256 :<br>54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b |
| Outils utilisés | VirusTotal : Outils d'investigation pour analyser des fichiers et des URL afin de détecter du contenu malveillant tel que des virus, vers, chevaux de Troie, etc. |
| Les 5 W | Qui a causé l'incident ? Un cybercriminel (acteur malveillant).<br>Que s'est-il passé ?<br>L'email contenait un fichier malveillant (le hachage du fichier est indiqué dans la description).<br>Quand l'incident s'est-il produit ?<br>À 13h20 : un système de détection d'intrusion a détecté les fichiers exécutables et a envoyé une alerte au SOC.<br>Où l'incident s'est-il produit ? Dans une entreprise de services financiers.<br>Pourquoi l'incident s'est-il produit ?<br>Après avoir reçu le contenu malveillant dans l'email, l'employé a téléchargé puis exécuté le fichier malveillant. |
| Notes Additionnel | Comment éviter que cela se reproduise ?<br>Ne jamais télécharger de fichiers suspects provenant d'emails.<br>Il faut renforcer la formation pour sensibiliser davantage aux cyberattaques<br>Dois-je signaler cela à un analyste SOC de niveau 2 ?<br>Oui. Selon le playbook utilisé par l'organisation, la gestion d'un tel incident peut varier. |

## Scénatio 4 :

| Ticket ID | Type d'alerte | Gravité | Détails | Status |
|---|---|---|---|---|
| A-AD3C0 | SERVER-MAIL<br><br>Tentative de phishing, possible téléchargement de malware | Moyenne | L'utilisateur a pu ouvrir un email malveillant et ses pièces jointes ou cliquer sur des liens. | Escaladé |

| **Commentaires du ticket :** |
|---|
| L'alerte a détecté qu'un employé avait téléchargé et ouvert un fichier malveillant provenant d'un email de phishing.<br>Le nom de l'expéditeur était trop beau pour être vrai. Le nom était "Security IT team" et l'adresse email était "kfdtjsdfjk@gmail.com |

| **Date :**<br>30/09/2025 | **Entrée : #3** |
|---|---|
| Description | Un Ticket d'incident a été émis. Tentative de phishing, possible téléchargement de malware |
| Outils utilisés | Playbook<br>Suivi du statut d'alerte (JIRA, etc.) |
| Les 5 W | Qui a causé l'incident ? Un individu externe non autorisé.<br>Que s'est-il passé ?<br>Après enquête, le ticket ID a été créé (A-AD3C0). L'alerte de message a été générée et signalée comme une tentative de phishing confirmée. La gravité du dommage est moyenne. L'utilisateur a ouvert un email malveillant et ses pièces jointes.<br>Quand l'incident s'est-il produit ?<br>Le 18 janvier 2024 (13h20).<br>Où l'incident s'est-il produit ? Dans une entreprise de services financiers. |

| | |
|---|---|
| | Pourquoi l'incident s'est-il produit ?<br>Après avoir reçu le contenu malveillant dans l'email, l'employé a téléchargé puis exécuté le fichier malveillant. |
| Notes Additionnel | Comment éviter que cela se reproduise ?<br>Ne jamais télécharger de fichiers suspects provenant d'emails inconnus .<br>Il faut renforcer la formation pour sensibiliser davantage aux cyberattaques<br>Dois-je signaler cela à un analyste SOC de niveau 2 ?<br>Oui. Selon le playbook utilisé par l'organisation, la gestion d'un tel incident peut varier. |