

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 ransomware, 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 : 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 ransomware, qui a chiffré des fichiers critiques de l'entreprise.
Outils utilisés	Playbook
Les 5 W	<p><u>Qui a causé l'incident ?</u> Un groupe de cybercriminel</p> <p><u>Que s'est-il passé ?</u> Un ransomware a été déployé ce qui a chiffré des données critiques de l'entreprise.</p> <p><u>Quand l'incident s'est-il produit ?</u> Mardi matin vers 9 h 00</p> <p><u>Où l'incident a-t-il eu lieu ?</u> Dans une entreprise de santé Américaine</p> <p><u>Pourquoi l'incident est-il arrivé ?</u> 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 ransomware 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.</p>
Notes Additionnel	<p><u>Comment éviter que cela se reproduise ?</u> Mettre en place des entraînements contre le phishing, crée fréquemment des backup de donnée pour éviter la paralysie du système.</p>

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 : 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	<u>Qui a causé l'incident ?</u> Un individu externe non autorisé <u>Que s'est-il passé ?</u> 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. <u>Quand l'incident s'est-il produit ?</u> 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.

	<p><u>Où l'incident a-t-il eu lieu ?</u> L'incident s'est produit dans les systèmes de l'organisation. Les communications ont eu lieu par courriel externe.</p>
Notes Additionnel	<p><u>Comment éviter que cela se reproduise ?</u></p> <p>Il faut renforcer la formation pour sensibiliser davantage aux cyberattaques.</p> <p>Signaler l'incident à un analyste SOC de niveau 2.</p> <p>Mener l'enquête en utilisant un guide de procédures (playbook).</p>