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 : 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 Que s'est-il passé ? Un randsomware a été déployé ce qui a chiffré des données critiques de l'entreprise. Quand l'incident s'est-il produit ? Mardi matin vers 9 h 00 Où l'incident a-t-il eu lieu ? Dans une entreprise de santé Américaine 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.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.

Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.