Journal du gestionnaire d'incidents

Instructions

Au fur et à mesure que vous poursuivez ce cours, vous pouvez utiliser ce modèle pour enregistrer vos découvertes après avoir terminé une activité ou pour prendre des notes sur ce que vous avez appris sur un outil ou un concept spécifique. Vous pouvez également utiliser ce journal pour consigner les principaux points à retenir sur les différents outils ou concepts de cybersécurité que vous rencontrez dans ce cours.

Date: 23/10/2025	**Entrée** Entry: 1
Description	Documentation d'un incident de cybersécurité
Outil(s) utilisé(s)	Répertoriez tous les outils de cybersécurité qui ont été utilisés.
Les 5 W	Capturez les 5 W d'un incident. ● **L'incident a été causée par un groupe d'acteur malveillant** ● **Un incident de sécurité de type Ransomware** ● **L'incident s'est produit le Mardi à 9 heures** ● **L'incident s'est produit à la clinique** ● **Les attaquants ont affiché sur les machines une somme de ranson à payer par l'organisation pour retrouver ses données. Il est sûr alors que l'attaque avait unbut financier.**
Notes complémentaires	Si l'entreprise a connaissance qu'un groupe de hacker a tendance à cibler les organisations de santé et de transport, pourquoi elle n'a pas mis en place une équipe de sécurité pour prévenir et répondre à ces genres de situations ?

Date: Enregistrez la date de l'écriture de journal.	**Entrée:** Entrée #2
Description	Description d'un incident de sécurité
Outil(s) utilisé(s)	Répertoriez tous les outils de cybersécurité qui ont été utilisés.
Les 5 W	Capturez les 5 W d'un incident. ● **Un acteur malveillant** ● **Une Ingénierie sociale de type phishing** ● **L'incident s'est produit au site** ● **L'incident s'est produit le Mercredi 20 Juillet 2022 à 09:30:14** ● **Un attaquant a envoyé au RH une email de phishing qui porte sur l'annonce de poste d'ingénieur publié sur le site web de l'organisation. L'attaquant s'est fait passé pour un potentiel candidat au poste et à envoyer une pièce jointe qu'il présente comme un CV et une lettre de motivation alors que c'est un fichier malveillant.**
Notes complémentaires	Quelles sont les mesures nécessaires qui doivent être prises pour ces genres de situations dans l'avenir?

Date: Enregistrez la date de l'écriture de journal.	**Entrée** Entrée #3
Description	Identification de problémes de sécurité
Outil(s) utilisé(s)	Splunk
Les 5 W	Capturez les 5 W d'un incident. ● Un utilisateur ou un acteur malveillant a causé l'incident ● L'incident concerne un échec de connexion par SSH ● L'incident s'est produit le Mardi 06 Mar 2023 à 01:39:51 ● L'incident s'est produit sur le serveur Mail de l'entreprise Buttercup Games ● L'incident a eu lieu car un utilisateur ou un acteur malveillant a essayé de se connecter sur le serveur en mode administrateur. Malheureusement, le mot avec lequel la personne a essayé de se connecter n'étais pas valide, ce qui causé l'enregistrement de l'événement dans le journal du serveur
Notes complémentaires	Est ce que l'utilisation d'une authentification multifactorielle ne serait pas plus adapté au serveur de mail ?

Date: Enregistrez la date de l'écriture de journal.	**Entrée:** Entrée #4

Description	Description d’un incident de sécurité
Outil(s) utilisé(s)	Chronicle
Les 5 W	Capturez les 5 W d'un incident. ● **Un acteur malveillant a causé l’incident** ● **Un email de phishing a été envoyé à de nos utilisateurs** ● **L’incident s’est produit le 31 janvier 2023 à 14H40** ● **L’incident s’est produit dans le boite mail de l’employé** ● **L’email contenait une adresse web** *signin.office365x24.com*. **identifiée comme malveillante aprés avoir effectuer des recherches dans crhonicle.**
Notes complémentaires	Ne pouvons nous pas effectuer des ateliers de sensibilisation pour permettre aux employés de mieux identfier des attaques de tel genre.

Date: Enregistrez la date de l’écriture de journal.	**Entrée:** Enregistrez le numéro de l’entrée de journal.
Description	Fournissez une brève description de l’entrée de journal.
Outil(s) utilisé(s)	Répertoriez tous les outils de cybersécurité qui ont été utilisés.
Les 5 W	Capturez les 5 W d'un incident. ● **OMS** qui a causé l'incident ?

	● **Quoi** arrivé? ● **Quand** l'incident s'est-il produit ? ● **Où** l'incident s'est-il produit ? ● **Pourquoi** l'incident s'est-il produit ?
Notes complémentaires	Incluez toute réflexion, question ou découverte supplémentaire.

Date: Enregistrez la date de l'écriture de journal.	**Entrée:** Enregistrez le numéro de l'entrée de journal.
Description	Fournissez une brève description de l'entrée de journal.
Outil(s) utilisé(s)	Répertoriez tous les outils de cybersécurité qui ont été utilisés.
Les 5 W	Capturez les 5 W d'un incident. ● **OMS** qui a causé l'incident ? ● **Quoi** arrivé? ● **Quand** l'incident s'est-il produit ? ● **Où** l'incident s'est-il produit ? ● **Pourquoi** l'incident s'est-il produit ?
Notes complémentaires	Incluez toute réflexion, question ou découverte supplémentaire.

Besoin d'un autre modèle d'entrée de journal ?

Si vous souhaitez ajouter d'autres écritures de journal, veuillez copier l'un des tableaux ci-dessus et collez-le dans le modèle pour l'utiliser pour les écritures futures.

Réflexions/Notes : Enregistrez des notes supplémentaires.