Journal du gestionnaire des incidents

Instructions

Au fil de ce cours, vous pourrez utiliser ce journal pour noter vos conclusions à la fin d'une activité ou pour prendre des notes lorsque vous apprenez à maîtriser un outil ou un concept. Vous pourrez aussi y noter les points clés concernant les différents outils et concepts de cybersécurité abordés pendant la formation.

Date : 15/04/2024	Entrée : 1
Description	Incident de sécurité : hameçonnage par mail et ransomware
Outil(s) utilisé(s)	Aucun
QQQOP	Répondez aux questions principales concernant l'incident. ● Qui a causé l'incident ? Un groupe organisé de pirates informatiques qui est spécialisé dans les demandes de rançons pour les entreprises de santé et de transport. ● Que s'est il passé? Visiblement, plusieurs employés ont remarqué qu'il n'avait pas accès à leurs fichiers sur leurs ordinateurs, empêchant de faire leurs activités quotidiennes. Incident de sécurité impliquant un rançongiciel ● Quand a eu lieu l'incident ? L'incident a eu lieu mardi matin vers 9h. ● Où s'est produit l'incident ? L'incident s'est produit au sein de l'entreprise de santé. ● Pourquoi l'incident s'est-il produit ? Visiblement, les pirates ont utilisé un mail malveillant, incitant les employés à télécharger un logiciel malveillant, ce qui a bloqué tout accès aux fichiers dont les employés ont besoin pour

	travailler
Autres remarques	1. Comment l'entreprise pourrait éviter qu'un incident comme celui-ci ne se produise à nouveau? 2. L'entreprise doit-elle payer la rançon pour récupérer la clé de déchiffrement?

Date : 18/04/2024	Entrée : 2
Description	Incident de sécurité - Infection par un logiciel malveillant suite à l'ouverture d'une pièce jointe dans un email d'hameçonnage
Outil(s) utilisé(s)	- IDS - Virus Total
QQQOP	Répondez aux questions principales concernant l'incident. ● Qui a causé l'incident ? Un employé non identifié de l'entreprise de services financiers. ● Que s'est il passé? Ouverture d'une pièce jointe malveillante (feuille de calcul) menant à l'exécution d'une charge utile malveillante et la création de fichiers exécutables non autorisés. Elle contenait le code SHA-256 suivant : 54e6ea47eb04634d3e87fd7787e2136ccfbcc80a de34f246a12cf93bab527f6b ● Quand a eu lieu l'incident ? ○ Réception de l'email : 13h11 ○ Téléchargement et ouverture du fichier : 13h13 ○ Création de fichiers exécutables : 13h15 ○ Détection par l'IDS et alerte au SOC : 13h20 ● Où s'est produit l'incident ? Sur le poste de travail de l'employé du services financiers ● Pourquoi l'incident s'est-il produit ? Hameçonnage par email incitant l'employé à ouvrir une pièce jointe malveillante.

Autres remarques	Comment éviter cet incident à l'avenir ? La sensibilisation des employés à la sécurité n'est peut-être pas assez forte?

Date : 29/04/2024	Entrée : 3
Description	Analyse d'un fichier de capture de paquets.
Outil(s) utilisé(s)	- Wireshark : analyseur de protocole réseau qui utilise une interface utilisateur graphique
QQQOP	Répondez aux questions principales concernant l'incident. ● Qui a causé l'incident ? S.O ● Que s'est il passé? S.O ● Quand a eu lieu l'incident ? S.O ● Où s'est produit l'incident ? S.O ● Pourquoi l'incident s'est-il produit ? S.O
Autres remarques	Avec l'utilisation de Wireshark, j'ai pu voir comment analyser un fichier de capture de paquets. Il semble assez difficile à prendre en main au premier abord. Une fois que j'y serais familière, son utilisation sera plus facile pour moi.

Date : 30/04/2024	Entrée : 4
Description	Capture de mon premier paquet
Outil(s) utilisé(s)	- tcpdump : pour capturer et analyser le trafic réseau. Ici on utilise une ligne de commande contrairement à Wireshark.
QQQOP	Répondez aux questions principales concernant l'incident. ● Qui a causé l'incident ? S.O ● Que s'est il passé?S.O ● Quand a eu lieu l'incident ?S.O ● Où s'est produit l'incident ?S.O ● Pourquoi l'incident s'est-il produit ? S.O
Autres remarques	Là où il pouvait y avoir des codes couleurs sur Wireshark, ici on ne voit que les lignes de commandes. En suivant les instructions correctement, j'ai pu comprendre un peu le fonctionnement de tcpdump.