**Journal du gestionnaire d'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 rencontrés pendant la formation.

|  |  |
| --- | --- |
| **Date :** 23 juillet 2024 | **Entrée :**  n° 1 |
| Description | Documentation d'un incident de cybersécurité  Cet incident est survenu en deux phases :   1. **Détection et analyse**: le scénario décrit la façon dont l'entreprise a détecté l'incident de ransomware et l'a analysé. Pour l'étape d'analyse, l'entreprise a contacté plusieurs entités pour obtenir une assistance technique. 2. **Confinement, Éradication et Récupération** : le scénario détaille certaines mesures prises par l'entreprise pour confinement de l'incident. Par exemple, l'entreprise a arrêté ses systèmes informatiques. Cependant, comme elle ne pouvait pas travailler seule pour éradiquer l'incident et s'en remettre, elle a contacté plusieurs autres entités pour obtenir de l'aide. |
| Outil(s) utilisé(s) | Aucun |
| QQQOP | * **Qui**: un groupe organisé de hackers non éthiques * **Quoi**: un incident de sécurité impliquant un ransomware * **Où**: dans une entreprise du secteur de la santé * **Quand**: mardi à 9 h * **Pourquoi**: l'incident a été causé par des hackers non éthiques qui ont réussi à accéder aux systèmes de l'entreprise par le biais d'une attaque par hameçonnage. Ensuite, ils ont déployé leur ransomware au sein des systèmes de l'entreprise et chiffré des fichiers critiques. L'argent semble être le mobile dans cette attaque, car la demande de rançon exigeait une grosse somme d'argent en échange de la clé de déchiffrement. |
| Autres remarques | 1. Comment l'entreprise pourrait-elle éviter qu'un tel incident ne se produise à nouveau ? 2. L'entreprise devrait-elle payer la rançon afin de récupérer la clé de déchiffrement ? |

|  |  |
| --- | --- |
| **Date :** 25 juillet 2024 | **Entrée :**  n° 2 |
| Description | Analyse d'un fichier de capture de paquets |
| Outil(s) utilisé(s) | Pour cette activité, j'ai utilisé Wireshark pour analyser un fichier de capture de paquets. Wireshark est un analyseur de protocole réseau qui utilise une interface utilisateur graphique. L'intérêt de Wireshark en cybersécurité est qu'il permet aux analystes sécurité de capturer et d'analyser le trafic réseau. Cela peut aider à détecter les activités malveillantes et à enquêter à leur sujet. |
| QQQOP | * **Qui** : S.O. * **Quoi**: S.O. * **Où** : S.O. * **Quand** : S.O. * **Pourquoi** : S.O. |
| Autres remarques |  |

|  |  |
| --- | --- |
| **Date :** 25 juillet 2024 | **Entrée :**  n° 3 |
| Description | Capture de mon premier paquet |
| Outil(s) utilisé(s) | Pour cette activité, j'ai utilisé tcpdump pour capturer et analyser le trafic réseau. Tcpdump est un analyseur de protocole réseau auquel on accède par l'interface de ligne de commande. À l'instar de Wireshark, la valeur de tcpdump en cybersécurité réside dans le fait qu'il permet aux analystes sécurité de capturer, de filtrer et d'analyser le trafic réseau. |
| QQQOP | * **Qui** : S.O. * **Quoi**: S.O. * **Où** : S.O. * **Quand** : S.O. * **Pourquoi** : S.O. |
| Autres remarques | Je n'ai pas encore l'habitude d'utiliser l'interface de la ligne de commande, et l'utiliser pour capturer et filtrer le trafic réseau a donc été un véritable défi. Je me suis retrouvé dans une impasse à plusieurs reprises parce que j'ai utilisé les mauvaises commandes. Mais après avoir suivi attentivement les instructions et refait certaines étapes, j'ai pu venir à bout de cette activité et capturer le trafic réseau. |

|  |  |
| --- | --- |
| **Date :** 27 juillet 2024 | **Entrée :**  n° 4 |
| Description | Enquêter sur un hachage de fichier suspect |
| Outil(s) utilisé(s) | Pour cette activité, j'ai utilisé VirusTotal, un outil d'investigation qui analyse les fichiers et les URL à la recherche de contenus malveillants tels que des virus, des vers, des chevaux de Troie, etc. Il s'agit d'un outil très utile pour vérifier rapidement si un indicateur de compromission, tel qu'un site web ou un fichier, a été signalé comme malveillant par d'autres membres de la communauté de la cybersécurité. Pour cette activité, j'ai utilisé VirusTotal pour analyser le hachage d'un fichier, qui a été signalé comme malveillant.  Cet incident s'est produit au cours de la phase **de détection et d'analyse**. Le scénario me mettait à la place d'un analyste sécurité d'un SOC enquêtant sur un hachage de fichier suspect. Après que le fichier suspect a été détecté par les systèmes de sécurité en place, j'ai dû procéder à une analyse et à une enquête plus approfondies pour déterminer si l'alerte constituait une véritable menace. |
| QQQOP | * **Qui** : un acteur malveillant inconnu * **Quoi** : un courrier électronique envoyé à un employé contenait une pièce jointe malveillante dont le code SHA-256 est 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. * **Où** : l'ordinateur d'un employé d'une société de services financiers * **Quand** : à 13 h 20, une alerte a été envoyée au SOC de l'entreprise après que le système de détection d'intrusion a détecté le fichier * **Pourquoi** : un employé a pu télécharger et exécuter une pièce jointe malveillante par courrier électronique. |
| Autres remarques | Comment éviter cet incident à l'avenir ? Devrions-nous envisager d'améliorer la formation pour sensibiliser les employés à la sécurité afin qu'ils fassent attention à ce sur quoi ils cliquent ? |

|  |
| --- |
| Réflexions/remarques :   1. **Y a-t-il eu des activités spécifiques qui vous ont posé problème ? Pourquoi ou pourquoi pas ?**   Au début, je me suis senti très frustré parce que je n'obtenais pas le bon résultat. J'ai refait l'activité et j'ai compris où je m'étais trompé. Ce que j'ai appris de cette expérience, c'est qu'il faut lire attentivement les instructions et procéder graduellement.   1. **Votre compréhension de la détection et de la réponse aux incidents a-t-elle changé après avoir suivi ce cours ?**   Après avoir suivi ce cours, ma compréhension de la détection aux incidents et de la réponse aux incidents a définitivement évolué. Au début du cours, j'avais quelques notions de base sur ce qu'impliquaient la détection et la réponse, mais je ne comprenais pas entièrement la complexité en jeu. À mesure de ma progression dans le cours, j'ai découvert le cycle de vie d'un incident, l'importance des plans, des processus et des personnes, ainsi que les outils utilisés. Dans l'ensemble, j'ai l'impression que ma compréhension a évolué et que j'ai acquis davantage de connaissances et de compréhension en matière de détection et de réponse aux incidents.   1. **Y avait-il un outil ou un concept qui vous a particulièrement plu ? Pourquoi ?**   J'ai vraiment apprécié le fait de me familiariser avec l'analyse du trafic réseau et d'appliquer ce que je venais d'apprendre à l'aide des outils des analyseurs de protocole réseau. C'était la première fois que je m'initiais à l'analyse du trafic réseau, c'était donc à la fois difficile et passionnant. J'ai trouvé vraiment fascinant de pouvoir utiliser des outils pour capturer le trafic réseau et l'analyser en temps réel. Je suis définitivement plus intéressé à en apprendre davantage sur ce sujet, et j'espère un jour devenir plus compétent dans l'utilisation des outils des analyseurs de protocole réseau. |