Travaux pratiques – Identification des menaces

Objectifs

Découvrez quelles fonctionnalités les entreprises utilisent pour sécuriser leurs données.

Partie 1 : Découvrir les menaces liées aux cyberattaques

Partie 2 : La triade CID

Contexte/Scénario

Les menaces du monde numérique sont bien réelles. Dans un monde qui fonctionne en grande partie à l'aide des ordinateurs, ces menaces peuvent provoquer des ravages. Il est important que tout le monde comprenne ces menaces. Pour les combattre, nous avons besoin de personnes engagées qui sachent les reconnaître, les déjouer et devancer les hackers. Pour développer les compétences nécessaires, des entreprises telles que CompTIA, Cisco Systems et ISC2 ont créé des programmes pour former et certifier les professionnels de la cybersécurité.

Ressources requises

- Ordinateur personnel ou terminal mobile avec accès Internet

Partie 1 : Explorer les menaces des cyberattaques

Les cyberattaques sont en tête des menaces planant sur les états du monde entier. Lorsqu'on évoque des menaces pour la sécurité nationale ou mondiale, la plupart des gens pensent à des attaques physiques ou à des armes de destruction massive. Pourtant, les cybermenaces sont en tête de liste dans plus de vingt pays dans le monde. Ce classement en première place nous montre la manière dont la société a évolué. Les ordinateurs et les réseaux affectent notre manière d'apprendre, d'acheter, de communiquer, de voyager et de vivre. Les systèmes informatiques contrôlent presque tous les pans de notre vie. Une perturbation des systèmes informatiques et des réseaux pourrait avoir un impact dévastateur sur la vie moderne. La génération d'électricité, les systèmes de distribution, le traitement de l'eau, les systèmes d'approvisionnement, les transports et les systèmes financiers sont tous ciblés par les cyberattaques. Chacun de ces systèmes a déjà été victime d'une cyberattaque. Regardez la vidéo ci-dessous. Répartissez-vous en groupes de 3 à 4 personnes. Après avoir vu la vidéo, répondez aux questions ci-dessous.

Étape 1 : Rechercher les menaces.

Au cours de la première étape, vous rechercherez les menaces.

a. Cliquez ici pour regarder la vidéo. Selon la vidéo, quelle est l'arme la plus dangereuse au monde ? Pourquoi ? Êtes-vous d'accord ?

b. Répertoriez cinq manières d'enfreindre la loi pour un cybercriminel. L'une de ces infractions peut-elle vous affecter personnellement ? Est-ce que vous ou un membre de votre famille avez déjà été touché par l'une de ces infractions ?

c. Les menaces potentielles décrites dans la vidéo ont-elles déjà été mises à exécution ? Cliquez ici pour en savoir plus sur ces attaques.

Étape 2 : Découvrir les attaques récentes.

a. L'impact et l'étendue des cyberattaques récentes inquiètent nombre de hauts fonctionnaires et d'entreprises. Cliquez ici pour découvrir les dix cyberattaques les plus dévastatrices en 2015.

Combien de personnes la violation des données de l'Office of Personnel Management (Bureau de la gestion du personnel) américain a-t-elle touché ?

b. Décrivez l'attaque TalkTalk de 2015. Qui était responsable de cette attaque, et qu'est-ce que les cybercriminels ont volé ?

Partie 2 : La triade CID

Confidentialité, intégrité et disponibilité sont les trois principes fondamentaux de la cybersécurité. Ces trois principes forment la triade CID. Ce sont les trois éléments essentiels de la sécurité. Tous les professionnels de la cybersécurité doivent être familiers avec ces principes fondamentaux.

Étape 1 : Découvrez la triade CID.

a. Cliquez ici pour regarder la vidéo. Qu'est-ce que la confidentialité des données ? Pourquoi est-elle si importante aux yeux des personnes et des entreprises ?

b. Qu'est-ce que l'intégrité des données ? Citez trois manières dont l'intégrité ou la fiabilité des données peut être compromise.

c. Qu'est-ce que la disponibilité du système ? Que peut-il se passer si un système informatique essentiel n'est plus disponible ?

Étape 2 : Explorer les cyberattaques.

Cliquez ici pour regarder une vidéo. Qu'est-ce que les cybercriminels ont tenté de faire ? À quelle heure les attaques ont-elles eu lieu ? Les attaques réseau sont-elles susceptibles d'avoir lieu en dehors des heures de travail ? Pourquoi ?