Travaux pratiques - Explorer le monde des professionnels de la cybersécurité

Objectifs

Découvrez les fonctionnalités déployées par des entreprises comme Google et Cisco pour sécuriser vos données.

Partie 1 : Protéger vos données

Partie 2 : Améliorer la sécurité de votre compte Google

Contexte/Scénario

Ce chapitre présente l'univers numérique aux participants. L'univers numérique est un véritable réservoir de données qui traite un nombre inimaginable d'informations personnelles et professionnelles. Pour les professionnels de la cybersécurité, il est important de comprendre les types de protections qu'une entreprise doit mettre en place afin de protéger les données qu'elle stocke, gère et protège. Lors de ces travaux pratiques, vous allez observer l'une des plus grandes entreprises de traitement de données au monde : Google. Vous regarderez deux vidéos, puis répondrez à une série de questions. Chaque vidéo présente un aspect différent de la défense en matière de cybersécurité chez Google. À la fin de ce chapitre, vous comprendrez mieux les mesures et services de sécurité que des entreprises comme Google mettent en place afin de protéger les informations et les systèmes d'information.

Vidéos :

Comment Google protège vos données

Clé de sécurité

Ressources requises

- Ordinateur personnel ou terminal mobile avec accès Internet

Partie 1 : Protéger vos données

Google, le plus grand référentiel de données personnelles au monde, stocke une énorme quantité de données. L'entreprise compte près de 50 % des activités de recherche sur Internet. Pour compliquer encore un peu plus les choses, Google possède et gère YouTube, le système d'exploitation Android et de nombreuses autres sources majeures de collecte de données. Durant cette activité, vous regarderez une courte vidéo et vous tenterez d'identifier plusieurs mesures prises par les professionnels de la cybersécurité chez Google pour protéger vos données.

Étape 1 : Ouvrez votre navigateur et regardez la vidéo suivante : Comment Google protège vos données

a. Comment Google s'assure-t-il que les serveurs qu'il installe dans ses data centers n'ont pas été infectés par des malwares provenant des fournisseurs de matériel ?

b. Comment Google se prémunit-il des accès physiques aux serveurs situés dans ses data centers ?

c. Comment Google protège-t-il les données client sur un système de serveurs ?

Étape 2 : Identifiez les vulnérabilités en matière de données.

a. Comme l'indique la vidéo, les données sont bien protégées dans les data centers de Google. Cependant, lorsque vous utilisez Google, toutes vos données ne se situent pas dans le data center de Google. À quels autres endroits pouvez-vous trouver vos données lorsque vous utilisez le moteur de recherche Google ?

b. Pouvez-vous prendre des mesures pour protéger vos données lorsque vous utilisez le moteur de recherche Google ? Quelles sont les quelques mesures que vous pouvez prendre pour protéger vos données ?

Partie 2 : Améliorer la sécurité de votre compte Google

Lorsque vous utilisez des services web comme Google, le plus important est de protéger les informations de votre compte personnel (nom d'utilisateur et mot de passe). Pour compliquer la donne, ces comptes sont généralement partagés et utilisés pour vous authentifier sur d'autres services web, tels que Facebook, Amazon ou LinkedIn. Vous disposez de plusieurs options pour améliorer la gestion de vos identifiants de connexion Google. Ces mesures comprennent la création d'une vérification en deux étapes ou un code d'accès contenant votre nom d'utilisateur et votre mot de passe. Google prend également en charge les clés de sécurité. Pendant cette activité, vous regarderez une courte vidéo et tenterez d'identifier les mesures qui peuvent être prises pour protéger vos informations d'identification lorsque vous utilisez des comptes web.

Étape 1 : Ouvrez votre navigateur et regardez la vidéo suivante : Travailler mieux, plus rapidement et en toute sécurité

a. Qu'est-ce que la vérification en deux étapes ? Comment permet-elle de protéger votre compte Google ?

b. Qu'est-ce que la clé de sécurité et comment fonctionne-t-elle ? Pouvez-vous utiliser la clé de sécurité sur plusieurs systèmes ?

c. Cliquez ici pour consulter les questions fréquentes sur les clés de sécurité. Si vous configurez votre compte de manière à utiliser une clé de sécurité, pouvez-vous toujours y accéder sans disposer de clé physique ?

Étape 2 : Protégez l'accès à votre compte Gmail.

a. Les comptes Gmail sont devenus très communs. Google compte désormais plus d'un milliard de comptes Gmail actifs. L'une des fonctionnalités pratiques des comptes Gmail est la possibilité d'accorder l'accès à d'autres utilisateurs. Cette fonctionnalité de partage d'accès génère un compte e-mail partagé. Les hackers peuvent se servir de cette fonctionnalité pour accéder à votre compte Gmail. Pour vérifier votre compte, connectez-vous et cliquez sur la roue dentée dans le coin supérieur droit (Paramètres). Lorsque l'écran des paramètres s'ouvre, une barre de menu s'affiche sous le titre Paramètres. (Général – Libellés – Boîte de réception – Comptes et importation – Filtres et adresses bloquées…)

b. Dans la barre du menu, cliquez sur **Comptes et importation**. Vérifiez l'option **Déléguer l'accès à votre compte**. Supprimez tout utilisateur non autorisé de la fonctionnalité de partage de votre compte.

Étape 3 : Vérifiez l'activité de votre compte Gmail.

a. Les utilisateurs de Gmail peuvent également vérifier l'activité du compte afin de s'assurer qu'aucun autre utilisateur n'a accédé à leur compte Gmail personnel. Cette fonctionnalité permet d'identifier les personnes qui ont accédé au compte, ainsi que leur emplacement géographique. Utilisez l'option **Dernière activité sur le compte** pour vérifier si une autre personne a accédé à votre compte. Pour accéder à cette option, suivez ces étapes :

   1) Connectez-vous à votre compte Gmail.

   2) Sélectionnez **Dernière activité sur le compte**, tout en bas de la page. La dernière heure à laquelle l'utilisateur non autorisé a accédé au compte s'affiche, ainsi que son emplacement géographique.

   3) Juste en dessous de ce message se trouve un lien « Détails ». Cliquez dessus.

b. Regardez l'activité de votre compte. Si vous identifiez un utilisateur non autorisé, vous pouvez le déconnecter en cliquant sur le bouton **Se déconnecter de toutes les autres sessions web** en haut à gauche. Modifiez votre mot de passe pour empêcher l'utilisateur non autorisé d'accéder à votre compte.