Surveillance du Dark Web
Guide d’onboarding des employés

Dans le cadre de notre engagement en faveur de la sécurité et de la confidentialité, nous avons mis en place un nouveau service de surveillance du Dark Web. Ce guide vous aidera à comprendre ce qu'est la surveillance du Dark Web, comment elle fonctionne et comment elle vous affecte.

Pourquoi est-il vital pour nous de lutter contre les menaces du Dark Web ?

Le Dark Web constitue une menace importante pour notre sécurité, principalement en raison de l'utilisation abusive des informations d'identification des utilisateurs volées. Dans cette partie obscure d’Internet, les hackers peuvent acheter ou vendre des informations d’identification obtenues lors de brèches de données internes et tierces, leur permettant ainsi d’accéder à des comptes personnels et d’entreprise. Cet accès peut conduire à d’autres failles de sécurité, au vol financier, au vol d’identité et même à l’espionnage industriel.

Les identifiants volés sont la principale méthode utilisée par les hackers pour pirater une entreprise.
(DBIR Verizon 2023)

50%

des brèches proviennent d’informations d’identification volées ou compromises, comme les mots de passe des utilisateurs.
(DBIR Verizon 2023)

62%

des brèches (sans erreur humaine) impliquaient l’utilisation d’identifiants volés, la force brute ou le phishing.
(Héros)

- Aide à la détection précoce des brèches de données, réduisant ainsi les dommages potentiels.
- Nous tient informés de notre empreinte numérique et de nos vulnérabilités.
- Aide à se conformer aux réglementations sur la protection des données.
- Protège la réputation de notre marque en réduisant l’impact des fuites de données.

Surveillance du Dark Web – Une couche de sécurité supplémentaire

Chacun de nous joue un rôle crucial dans la protection contre les menaces du Dark Web. En adhérant à des protocoles de sécurité, comme l'utilisation de mots de passe forts et le signalement d'activités suspectes, nous pouvons réduire considérablement le risque que nos données soient compromises et se retrouvent sur le Dark Web. Pour renforcer notre résilience, l'entreprise a mis en place un service interne de surveillance du Dark Web pour nous aider à protéger la réputation de notre entreprise et à assurer la sécurité de l'entreprise et de nos informations personnelles.

Notre service de surveillance du Dark Web – Comment ça marche

1 Analyser

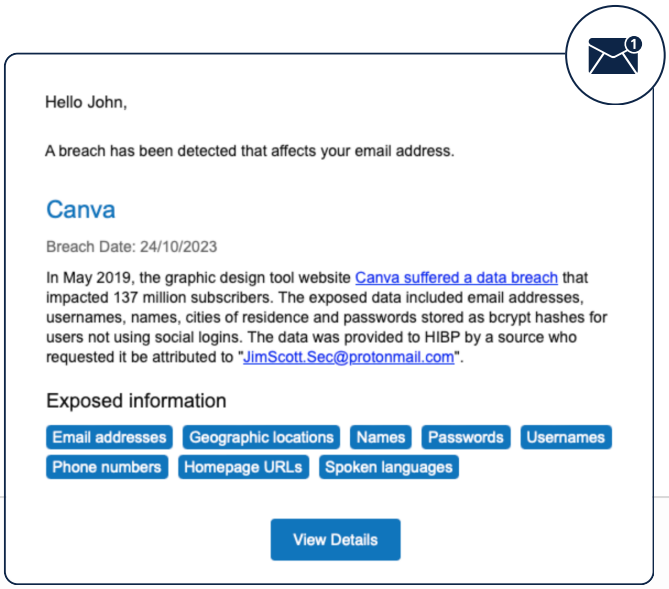
Une vaste base de données de sources de brèches sera analysée, identifiant si l'une de vos données d'entreprise (par exemple votre mot de passe de messagerie professionnelle) est présente dans une brèche de données.

Une surveillance continue du Dark Web aura alors lieu, analysant en permanence les nouvelles brèches de données pour identifier si vous êtes en danger.

Où se trouvent souvent les données volées ?

- Salons de discussion sur le Dark Web – salons secrets où les brèches sont discutées
- Sites de piratage et de vidage – sites Web où les données piratées sont partagées
- Forums de vol cachés – communautés de piratage où les données piratées sont publiées
- Fuites de fichiers P2P – fuite de données via des réseaux peer-to-peer

Quelles données trouve-t-on couramment ? Mots de passe | Détails de compte en banque | Adresses | Numéro de téléphone



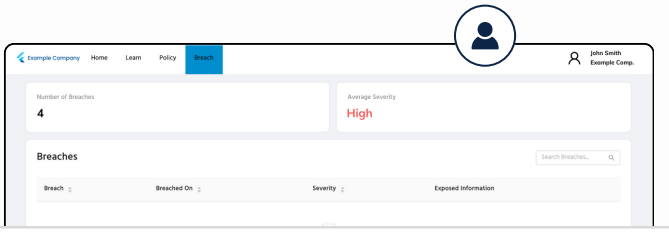
2 Alerte

Si, à un moment donné, vos données ou informations d'identification sont détectées dans une brèche, vous recevrez une alerte par e-mail (exemple, à gauche) qui comprend :

- Liste des brèche qui vous concernent
- Origine et date des brèches
- Types de données exposées
- De plus, un lien pour voir plus de détails

Vos données ont été découvertes lors d'une brèche, et maintenant ?

Si vous êtes informé par notre service de surveillance du Dark Web que vos données ont été découvertes lors d'une brèche, il est important d'agir rapidement pour protéger vos informations et réduire votre score de risque humain dans votre portail d'utilisateur final (exemple ci-dessous).



Voici quelques conseils pour réduire vos risques :

- Modifier les mots de passe : mettez immédiatement à jour les mots de passe de tous les comptes concernés. Utilisez des mots de passe forts et uniques pour chaque compte.
- Contactez votre banque : si des informations financières sont impliquées, contactez rapidement votre banque ou votre société de carte de crédit.
- Comptes de messagerie sécurisés : pour les comptes de messagerie compromis, mettez à jour vos paramètres de sécurité et activez l'authentification à deux facteurs si vous ne l'utilisez pas déjà.
- Surveillez vos comptes : vérifiez régulièrement vos relevés bancaires et de carte de crédit pour détecter toute transaction suspecte.