CROWDSTRIKE

FALCON INTELLIGENCE RECON

Découvrez les menaces qui pèsent sur votre marque, vos employés et vos données sensibles sur le Web, le Deep Web et le Dark Web

RECONNAISSANCE DES RISQUES NUMÉRIQUES SUR LE DARK WEB ET AU-DELÀ

CrowdStrike Falcon Intelligence™ Recon expose les activités potentiellement malveillantes provenant du Web, du Deep Web et du Dark Web, permettant ainsi aux entreprises de mieux protéger leur marque, leurs employés et leurs données sensibles. Falcon Intelligence Recon collecte des données et surveille l'activité de millions de pages web à accès restreint, de forums cybercriminels et de plateformes de messagerie chiffrées, autrement dit les recoins cachés de l'Internet où les cybercriminels se retrouvent et où les économies numériques souterraines prospèrent. En offrant aux équipes de sécurité la possibilité de mener des investigations en temps réel, il leur permet de découvrir de manière proactive les fraudes, les compromissions de données, les campagnes de phishing et autres menaces en ligne qui ciblent leur entreprise.

PRINCIPAUX AVANTAGES

COLLECTE

Falcon Intelligence Recon offre un accès instantané à plus de huit ans de données provenant de canaux numériques difficiles d'accès du Web, du Deep Web et du Dark Web.
Falcon Intelligence Recon collecte de façon proactive des renseignements bruts sur les activités frauduleuses, les données volées, les menaces pour les entreprises, ainsi que les exploits et outils identifiés dans les arsenaux des adversaires.

- **Collecte de renseignements bruts à grande échelle** : Surveillez automatiquement les données issues de millions de pages web dissimulées et de milliers de forums à accès restreint, de marchés criminels, de sites pastebin, de canaux IRC, d'applications malveillantes, de domaines de phishing et d'applications de messagerie ouvertes et fermées telles que Telegram, QQ et bien d'autres.
- **Investigations secrètes en temps réel :** Perturbez les activités des cyberadversaires grâce à un accès à des renseignements bruts en temps réel, et limitez leurs opportunités d'attaque. Effectuez des investigations grâce à un accès indétectable aux données des sites à accès restreint. Falcon Intelligence Recon stocke les données historiques afin que les cyberadversaires ne puissent pas effacer leurs traces en modifiant ou supprimant leurs publications.
- **Suivi des cybercriminels :** Analysez et suivez les changements de comportement des cyberattaquants dans le temps, et identifiez les augmentations d'activité, les attaques émergentes, les nouvelles cibles ainsi que l'évolution des techniques et des outils, afin de mieux vous protéger contre les menaces externes.

PRINCIPAUX AVANTAGES

- Couverture inégalée du Web, du Deep Web et du Dark Web
- Automatisation de l'extraction des données de millions d'environnements clandestins et à accès restreint
- Réduction de la durée des investigations pour une efficacité et une réactivité accrues
- Surveillance en temps réel avec règles personnalisées adaptées à votre entreprise
- Efficacité immédiate — la solution est déployée et opérationnelle en quelques minutes seulement
- Profils des cyber-adversaires et flux d'indicateurs de compromission compris

INVESTIGATION

Bénéficiez d'une visibilité en temps réel sur les menaces potentielles, et accélérez les investigations liées aux activités frauduleuses ciblant votre entreprise. Falcon Intelligence Recon élimine les suppositions dangereuses et enrichit la réponse à incidents traditionnelle en fournissant un contexte étendu pour des rapports d'investigation et des analyses plus complets et approfondis.

- **Identification des menaces ciblées :** Surveillez en permanence les environnements clandestins à la recherche des menaces externes ciblant votre entreprise, sans devoir créer des requêtes complexes. Falcon Intelligence Recon met à disposition un assistant facile à utiliser qui inclut des critères de recherche prédéfinis tels que les noms de marque, les dirigeants, les domaines, les vulnérabilités, les adresses e-mail et bien d'autres encore. Créez et enregistrez vos propres règles de surveillance pour passer les renseignements bruts au crible de façon proactive, ou partagez-les avec votre équipe.
- **Exposition des cyberadversaires :** Examinez les résultats présentés dans des tableaux de bord personnalisables et faciles à lire. Les utilisateurs peuvent consulter les publications originales du cybercriminel avec du contexte supplémentaire sur ce dernier et sur le site. Les résultats sont affichés dans leur langue d'origine et peuvent être traduits à partir de 18 autres langues grâce à une fonctionnalité de traduction augmentée utilisant des dictionnaires d'argot cybercriminel.
- **Enrichissement des investigations :** Bénéficiez d'une compréhension approfondie de la menace. La fonctionnalité de recherche universelle permet aux utilisateurs de corréler automatiquement les résultats de Falcon Intelligence Recon avec le contexte supplémentaire fourni par d'autres modules CrowdStrike Falcon sous licence. Optimisez l'efficacité de la réponse en dévoilant les relations entre les menaces numériques et les détections sur endpoints, les hôtes, les rapports sur les cybermenaces, les vulnérabilités, etc.

NOTIFICATION

Optimisez l'investigation et la réponse grâce à des notifications en temps réel lorsque des menaces potentielles sont identifiées. Assurez-vous que les utilisateurs responsables du tri et de la réponse disposent des détails dont ils ont besoin à portée de main.

- **Priorisation des alertes :** Définissez la priorité de l'alerte en fonction de la criticité de la menace externe. Pivotez en un clic de la notification aux détails de l'alerte.
- **Contrôle administratif total :** Personnalisez le type de notification et leur fréquence de réception. Les équipes peuvent être notifiées immédiatement ou selon un calendrier établi, par exemple une fois par jour ou une fois par semaine. Activez ou désactivez les notifications sans affecter la règle de surveillance sous-jacente.
- **Notification des équipes concernées :** Ne vous limitez pas à la cybersécurité ; les menaces numériques affectent la marque, la réputation et la sécurité des employés d'une entreprise. Alertez tous les départements concernés : équipe marketing, service juridique, ressources humaines ou équipe de lutte contre la fraude.

ÉDITIONS :

Falcon Intelligence Recon est disponible dans deux éditions :

- **Falcon Intelligence Recon Express:** conçu pour les petites et moyennes entreprises.
- **Falcon Intelligence Recon Enterprise :** inclut toutes les fonctionnalités d'Express, ainsi que :
  - Fonctionnalité de recherche ponctuelle dynamique pour les investigations en constante évolution
  - Données BIN des cartes de crédit/débit
  - Profils des cyberadversaires et flux d'indicateurs de compromission fournis par CrowdStrike® Intelligence

Profiter d'une évaluation gratuite
de notre antivirus de nouvelle génération

Pour en savoir plus, consultez le site **crowdstrike.fr**.

© 2021 CrowdStrike, Inc. Tous droits réservés.

RECONNAISSANCE DES RISQUES NUMÉRIQUES

Protection de la marque : CrowdStrike Falcon Intelligence Recon identifie les cyberattaquants associés à des interactions frauduleuses avec votre marque, notamment les faux comptes de réseaux sociaux, domaines et applications mobiles.

Identification des fuites de données : CrowdStrike Falcon Intelligence Recon détecte les identifiants compromis et les données sensibles dérobées, ainsi que les informations de carte de crédit et les adresses IP dans les données divulguées sur le Web, le Deep Web et le Dark Web.

Surveillance de la supply chain : CrowdStrike Falcon Intelligence Recon vous permet d'identifier les menaces qui pèsent sur vos fournisseurs en exposant les discussions malveillantes, les campagnes de phishing, les sites web contrefaits, etc.

Protection des dirigeants : CrowdStrike Falcon Intelligence Recon surveille les menaces, les usurpations d'identité et les tentatives de phishing à l'encontre des dirigeants et des collaborateurs de premier plan de l'entreprise.

À PROPOS DE CROWDSTRIKE

CrowdStrike, leader mondial de la cybersécurité, redéfinit la sécurité pour l'ère du cloud en proposant une plateforme de protection des endpoints conçue spécifiquement pour empêcher les compromissions. L'architecture à agent léger unique de la plateforme CrowdStrike Falcon® s'appuie sur l'intelligence artificielle à l'échelle du cloud pour offrir une visibilité et une protection en temps réel au sein de l'entreprise et prévenir les attaques sur les endpoints, qu'ils soient connectés ou non au réseau. Optimisé par la base de données propriétaire CrowdStrike Threat Graph®, CrowdStrike Falcon met en corrélation en temps réel plus de quatre billions d'événements liés aux endpoints identifiés chaque semaine dans le monde, qui viennent enrichir l'une des plateformes de données les plus avancées au monde en matière de sécurité.