Kaspersky Digital Footprint Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky Digital Footprint Intelligence

À mesure que votre entreprise évolue, la complexité et la répartition de vos environnements informatiques ne cessent de croître, engendrant un problème de taille : la protection de votre présence numérique étendue sans contrôle direct ni propriété. Les environnements interconnectés et dynamiques permettent aux entreprises de tirer des avantages significatifs. Néanmoins, l'interconnectivité toujours croissante étend également la surface des attaques. Les attaquants étant de plus en plus compétents, il est crucial non seulement d'obtenir une image précise de la présence en ligne de votre entreprise, mais également de suivre ses changements et de réagir aux dernières informations sur les ressources numériques exposées.

Les entreprises utilisent un vaste éventail d'outils de sécurité dans leurs opérations de sécurité, mais restent exposées à des menaces numériques : la capacité à détecter et à atténuer les activités des initiés, les plans et les schémas d'attaque des cybercriminels situés sur les forums du Dark Web, etc. Pour aider les analystes de la sécurité à voir les ressources d'entreprise auxquelles les criminels ont accès, à découvrir rapidement les vecteurs d'attaque potentiels à leur disposition et à ajuster les moyens de défense en conséquence, Kaspersky a créé Kaspersky Digital Footprint Intelligence.

Quel est le meilleur moyen d'organiser une attaque contre votre entreprise ? Quel est le moyen le plus rentable de vous attaquer ? À quelles informations un attaquant qui cherche à cibler votre entreprise a-t-il accès ? Votre infrastructure a-t-elle déjà été compromise sans que vous ne le sachiez ?

Les rapports sur les menaces spécifiques au client proposés par Kaspersky répondent à toutes ces questions et à d'autres encore grâce au travail de nos experts. Ils offrent un aperçu complet de votre situation actuelle en termes de sécurité, identifient les failles susceptibles d'être exploitées et découvrent les preuves d'attaques passées, actuelles et prévues.

Le produit offre :

- Inventaire du périmètre réseau au moyen de méthodes non intrusives pour identifier les ressources réseau et les services exposés du client qui constituent un point d'entrée potentiel pour une attaque, comme les interfaces de gestion involontairement placées sur le périmètre ou les services mal configurés, les interfaces d'appareils, etc.
- Analyse sur mesure des vulnérabilités existantes avec notation supplémentaire et évaluation complète des risques à partir de la note de base CVSS, disponibilité des vulnérabilités publiques, expérience de test de pénétration et localisation des ressources réseau (hébergement/infrastructure).
- Identification, surveillance et analyse de toute attaque ciblée active ou de toute attaque planifiée, des campagnes APT ciblant votre entreprise, le secteur et la zone des opérations.
- Preuves de menaces et d'activités des botnets ciblant spécifiquement vos clients, partenaires et abonnés, dont les systèmes infectés pourraient ensuite être utilisés pour vous attaquer.
- Surveillance discrète de sites Pastebin, des forums publics, des blogs, des canaux de messagerie instantanée, des forums en ligne souterrains restreints et des communautés pour mettre la main sur des comptes compromis, des fuites d'informations ou des attaques planifiées et évoquées à l'encontre de votre entreprise.

Bénéfices

Kaspersky Digital Footprint Intelligence utilise des techniques OSINT combinées à une analyse automatisée et manuelle du Web surfacique, du deep Web et du dark Web, en plus de la base de connaissances Kaspersky interne, pour fournir des informations et recommandations exploitables.

Le produit est disponible sur le portail Threat Intelligence de Kaspersky. Vous pouvez acheter quatre rapports trimestriels avec des alertes de menaces en temps réel ou acheter un rapport unique avec des alertes actives pendant six mois.

Fouillez le web surfacique et le dark Web à la recherche d'informations presque en temps réel sur des événements de sécurité mondiaux qui menacent vos actifs et de données sensibles exposées dans des forums et communautés souterrains restreints. La licence annuelle inclut 50 recherches par jour dans les sources externes et la base de connaissances Kaspersky.

Kaspersky Digital Footprint Intelligence forme une solution unique avec le service de démontage Kaspersky Takedown Service. La licence annuelle inclut 10 demandes de démontage de domaines malveillants et de phishing par an.

Inventaire externe du périmètre réseau (cloud inclus)

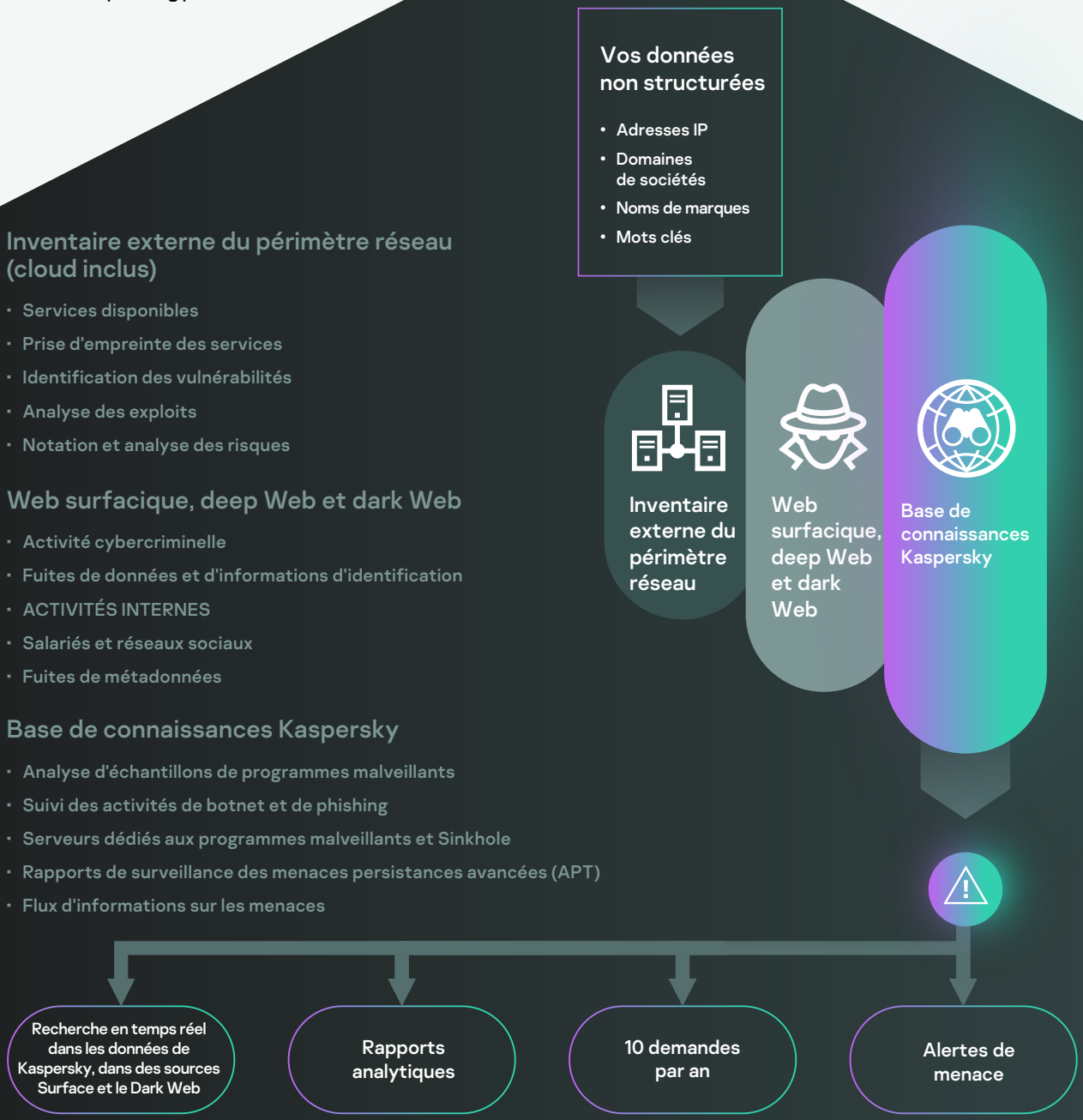
- Services disponibles
- Prise d'empreinte des services
- Identification des vulnérabilités
- Analyse des exploits
- Notation et analyse des risques

Web surfacique, deep Web et dark Web

- Activité cybercriminelle
- Fuites de données et d'informations d'identification
- ACTIVITÉS INTERNES
- Salariés et réseaux sociaux
- Fuites de métadonnées

Base de connaissances Kaspersky

- Analyse d'échantillons de programmes malveillants
- Suivi des activités de botnet et de phishing
- Serveurs dédiés aux programmes malveillants et Sinkhole
- Rapports de surveillance des menaces persistances avancées (APT)
- Flux d'informations sur les menaces



www.kaspersky.fr

© 2022 AO Kaspersky Lab.
Les marques déposées et les marques de service sont la propriété de leurs détenteurs respectifs.