Kaspersky Flux d'informations sur les menaces

kaspersky prêts pour l'avenir

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

Des cyberattaques ont lieu tous les jours. La fréquence, la complexité et l'obfuscation des cybermenaces ne cessent de croître, les cybercriminels tentant par tous les moyens d'affaiblir vos défenses. Ils utilisent des chaînes de frappe d'intrusion complexes, des campagnes et des TTP (Tactiques, Techniques et Procédures) personnalisées pour paralyser votre activité ou encore attaquer vos clients. Il apparaît clairement que la protection exige de nouvelles méthodes, basées sur la threat intelligence.

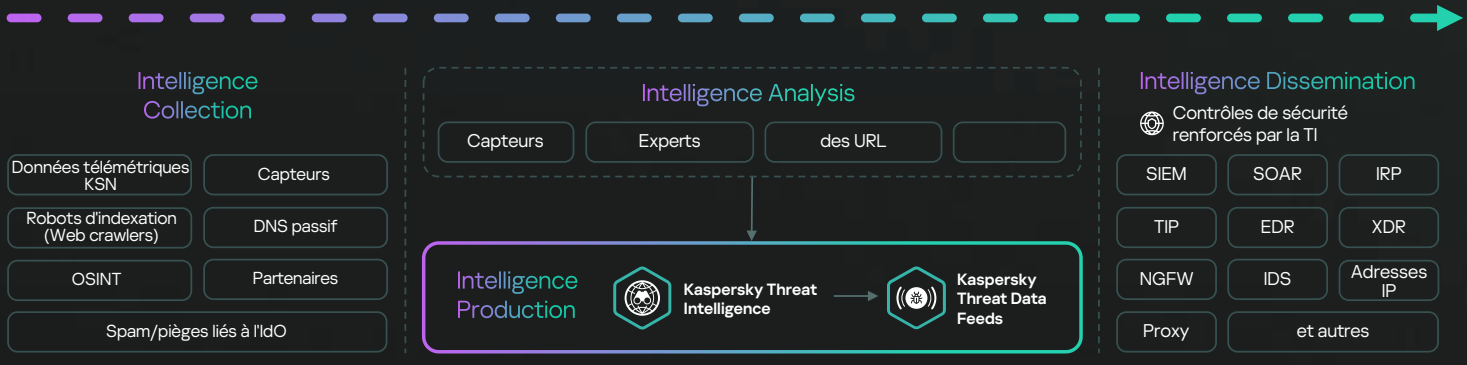
En intégrant aux contrôles de sécurité existants (ex. : systèmes SIEM, SOAR et des plateformes de Threat Intelligence) des données de Threat Intelligence mises à jour minute par minute contenant des informations sur des adresses IP, des URL et des hachages de fichiers suspects et dangereux, les équipes de sécurité peuvent automatiser le processus de tri initial tout en fournissant à leurs spécialistes un contexte suffisant pour identifier immédiatement les alertes qui doivent faire l'objet d'une enquête ou être remontées aux équipes de réponse aux incidents.

Données contextuelles

Les entrées des flux fournis par Kaspersky contiennent les données contextuelles suivantes qui vous aident à confirmer rapidement les menaces et à les classer par ordre de priorité :

- Noms des menaces
- Adresses Internet et noms de domaine des ressources Internet malveillantes
- Hachages de fichiers malveillants
- Objets vulnérables et compromis
- Tactiques, techniques et procédures d'attaques selon la classification MITRE ATT&CK
- Horodatage
- Géolocalisation
- Popularité, etc.

Comment ça fonctionne ?



Les flux d'informations sur les menaces de Kaspersky sont agrégés à partir de sources Kaspersky fusionnées, hétérogènes et hautement fiables :

Kaspersky SecurityNetwork

Infrastructure cloud sophistiquée qui collecte et analyse des données anonymes sur les cybermenaces provenant de plus de 400 millions de participants bénévoles à travers le monde entier, afin de fournir la réponse la plus rapide aux nouvelles menaces en tirant parti de l'analyse du Big Data, du machine learning et de l'expertise humaine.

Robots d'indexation

Collecte de nouveaux échantillons de programmes malveillants et légitimes à partir de diverses sources : OSINT, recherche par des analystes de Kaspersky, et nos propres systèmes de traitement et d'analyse automatiques extrayant les URL des programmes malveillants.

Bot farms

Une équipe spécialisée dans la recherche sur les botnets extrait les configurations des bots, procède à une rétroingénierie de leurs protocoles de communication, et surveille les instructions des centres de contrôle afin d'obtenir une Threat Intelligence précieuse.

Spam traps

Chaque année, nos systèmes anti-phishing empêchent plus de 500 millions de clics sur des liens de phishing et bloquent plus de 160 millions de pièces jointes malveillantes contenues dans des emails, et nous en extrayons par ailleurs des données supplémentaires afin d'enrichir nos flux de données.

Partenaires

Nous prenons part à des partenariats pour partager des échantillons malveillants avec d'autres fournisseurs et entreprises de cybersécurité.

Capteurs

Honeypots, sinkholes et autres méthodes d'interception des attaques ITW. Par exemple (y compris les appareils de l'IdO, les systèmes vulnérables, les logiciels, etc.) Les analystes de Kaspersky recherchent les tentatives d'attaques et les méthodes des pirates informatiques, extraient les indicateurs de compromission et les relient à d'autres sources de données.

DNS passif

Les données sont collectées à l'échelle mondiale par des tiers de confiance comme des services d'hébergement et des FAI.

OSINT

Les données adverses sont automatiquement collectées à partir de sources accessibles publiquement, comme les organes de presse, les réseaux sociaux, les rapports publics, le Dark Web, etc. Nous utilisons ces données pour chercher de nouveaux échantillons malveillants en explorant l'infrastructure des adversaires, afin d'enrichir en permanence notre base de connaissances.

Chaque indicateur détecté est soumis à un processus de filtrage en plusieurs étapes dans un système de traitement automatisé qui utilise des technologies fiables et réputées et des modèles de machine learning formés à partir d'échantillons de centaines de millions de fichiers fiables et malveillants afin d'éliminer les faux positifs. Chaque indicateur est également analysé dans plusieurs sandboxs, d'où sont extraits des dizaines d'attributs supplémentaires comme les TTP, le comportement des réseaux, le comportement des systèmes d'exploitation, et toute une série d'autres relations.

Tout cela fait de Kaspersky Threat Intelligence une source puissante de renseignements tactiques capable de renforcer vos centres de surveillance des menaces et de détecter les adversaires en première ligne de votre entreprise.

Bénéfices

Les flux d'informations sont automatiquement générés en temps réel en se basant sur des résultats recueillis dans le monde entier, ce qui fournit des taux de détection et une précision élevés.

La facilité de mise en œuvre et d'intégration est assurée par une documentation complémentaire, des échantillons, un responsable commercial et technique dédié et l'assistance technique de Kaspersky.

Les formats de diffusion simples et légers (JSON, CSV, OpenIoC, STIX) via le protocole HTTPS ou des mécanismes de distribution ad hoc simplifient l'intégration des flux dans les solutions de sécurité. Les principales plateformes SIEM et TI sont entièrement prises en charge.

Les flux d'informations remplis de faux positifs ne servent à rien, aussi appliquons-nous des filtres et des tests extrêmement complets pour garantir la diffusion de données intégralement vérifiées.

Des centaines d'experts – y compris des analystes en sécurité du monde entier, les experts en sécurité mondialement réputés de l'équipe GReAT, ainsi que nos équipes de R&D – contribuent à générer ces flux. Les agents de sécurité reçoivent des informations et des alertes critiques générées à partir de données optimales, sans être inondés d'indicateurs et d'avertissements superflus.

Tous les flux sont générés et surveillés par une infrastructure hautement tolérante aux pannes, assurant une disponibilité permanente.

Avantages

1. Renforcez vos outils de défense du réseau, notamment les systèmes SIEM, les pare-feu, les pare-feu de nouvelle génération, les IPS/IDS, les proxy de sécurité et les solutions DNS et anti-APT à l'aide d'indicateurs de compromission (IOC) constamment actualisés et d'informations concrètes sur les cyberattaques et les intentions, capacités et cibles de vos adversaires.

2. Améliorez et accélérez vos capacités de réponse aux incidents et d'investigation en automatisant la procédure de tri initial tout en fournissant suffisamment de contexte à vos analystes de données pour identifier immédiatement les alertes devant faire l'objet d'une enquête ou être transmises aux équipes d'intervention en cas d'incident, en vue de poursuivre les recherches et de réagir.

3. Empêchez l'exfiltration de propriété intellectuelle et de ressources sensibles stockées dans des machines infectées. Détectez rapidement ces dernières afin de protéger la réputation de votre marque et d'éviter de perdre un avantage concurrentiel ainsi que des opportunités commerciales.

4. Si vous êtes un MSSP, développez votre activité en proposant à vos clients un service de Threat Intelligence haut de gamme et leader.

5. Si vous faites partie du CERT, optimisez et élargissez vos capacités de détection et d'identification des cybermenaces.

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence donne accès à un large éventail d'informations recueillies par nos analystes et chercheurs de classe mondiale. Ces données aideront votre entreprise à lutter efficacement contre les cybermenaces actuelles.

Notre entreprise possède des connaissances approfondies, une grande expérience dans la recherche sur les cybermenaces et des connaissances uniques sur tous les aspects de la cybersécurité, fournissant ainsi une Threat Intelligence tactique, opérationnelle et stratégique à jour.
Cela a fait de nous un partenaire de confiance pour les organisations policières et gouvernementales du monde entier, y compris Interpol et diverses unités CERT. Et tout cela est accessible sous forme de données pertinentes et exploitables via le portail de Kaspersky Threat Intelligence.

Kaspersky Threat Intelligence

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture