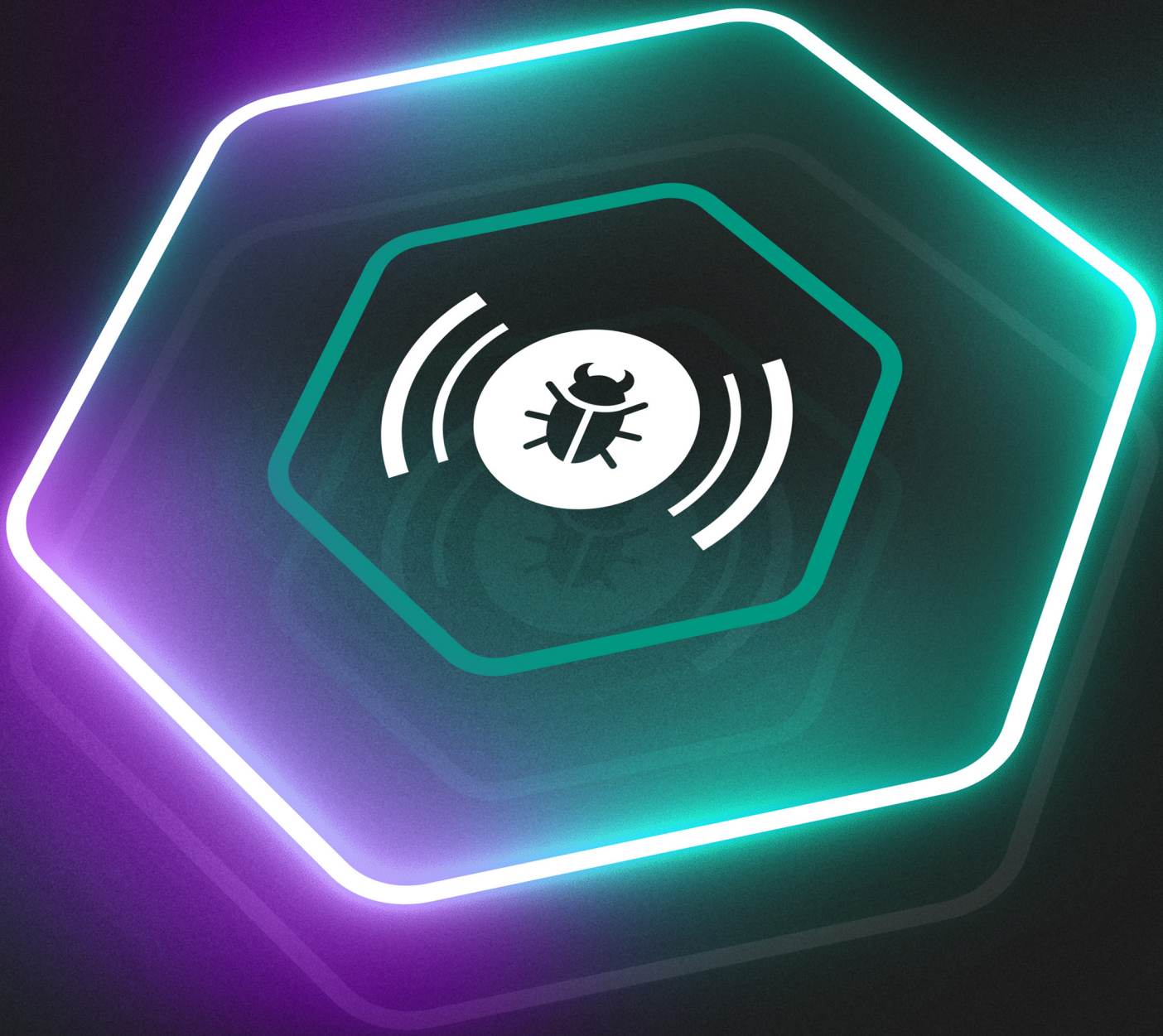


Kaspersky Threat Data Feeds

kaspersky BRING ON THE FUTURE

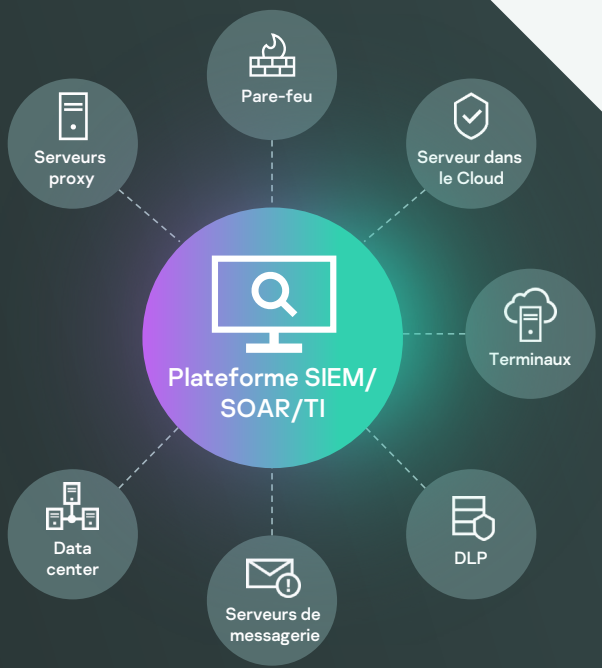
Kaspersky Threat Data Feeds

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 plate-formes 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.

- Informations sur la réputation des adresses IP
- INFORMATIONS SUR LES HASHES (WIN / *nix / MacOS / AndroidOS / iOS)
- INFORMATIONS SUR LES URL (malicieux, phishing et C&C)
- INFORMATIONS SUR LES URL DE RANSOMWARES
- INFORMATIONS SUR LES INDICATEURS DE COMPROMISSIONS APT
- INFORMATIONS SUR LA VULNÉRABILITÉ
- INFORMATIONS SUR LES DNS PASSIVES (pDNS)
- INFORMATIONS SUR LES URL IoT
- INFORMATIONS SUR LA LISTE BLANCHE
- INFORMATIONS SUR LES HACHAGES ICS
- ET BIEN PLUS ENCORE

Kaspersky Threat Data Feeds



Données contextuelles

Pour tous les flux d'informations, chaque dossier est enrichi avec un contexte exploitable (noms des menaces, horodatages, géolocalisation, adresses IP résolues de ressources Web infectées, hashes, popularité, etc.). Les données contextuelles permettent de pointer la situation globale, étayant et soutenant ainsi une large utilisation des données. Les données mises en contexte peuvent être plus facilement utilisées pour savoir qui, quoi, où et quand, afin d'identifier vos adversaires et de prendre des décisions et des mesures opportunes.

Bénéfices

Collecte et traitement

Les flux d'informations sont agrégés à partir de sources ultra-fiables, hétérogènes et fusionnées, comme Kaspersky Security Network et nos propres robots d'indexation, notre service de contrôle des botnets (qui surveille les botnets, leurs cibles et activités 24 h/24, 7 j/7, 365 j/an), les spam traps, les équipes de chercheurs et nos partenaires.

Toutes les données agrégées sont ensuite soigneusement analysées et affinées en temps réel à l'aide de plusieurs techniques de prétraitement : critères statistiques, sandbox, moteurs heuristiques, outils de similarité, profils de comportement, validation par des analystes et vérification de listes blanches.

Les flux d'informations sont générés en temps réel et de manière automatique dans le monde entier (le Kaspersky Security Network couvre une proportion considérable de l'ensemble du trafic Internet, avec des dizaines de millions d'utilisateurs dans plus de 213 pays), afin de garantir un taux de détection élevé et une bonne précision

Facilité de mise en œuvre. Une documentation complémentaire, des échantillons, un responsable commercial et technique dédié et l'assistance technique Kaspersky sont à votre disposition pour une intégration simple

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 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

Renforcez vos outils de défense du réseau, notamment les systèmes SIEM, les pare-feu, 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 qui informent sur les cyberattaques et les intentions, capacités et cibles de vos adversaires. Les principaux systèmes SIEM (y compris HP ArcSight, IBM QRadar, Splunk, etc.) et les plateformes TI sont totalement pris en charge

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

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 et des opportunités commerciales

Si vous êtes un MSSP, développez votre activité en proposant à vos clients un service de Threat Intelligence haut de gamme et leader. Si vous faites partie du CERT, optimisez et élargissez vos capacités de détection et d'identification des cybermenaces

www.kaspersky.fr