Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

Le défi

Le suivi, l'analyse, l'interprétation et la lutte contre les menaces informatiques, en perpétuelle évolution, représentent un travail considérable. Dans tous les secteurs, les entreprises manquent de données actualisées et pertinentes pour gérer les risques liés aux menaces informatiques.

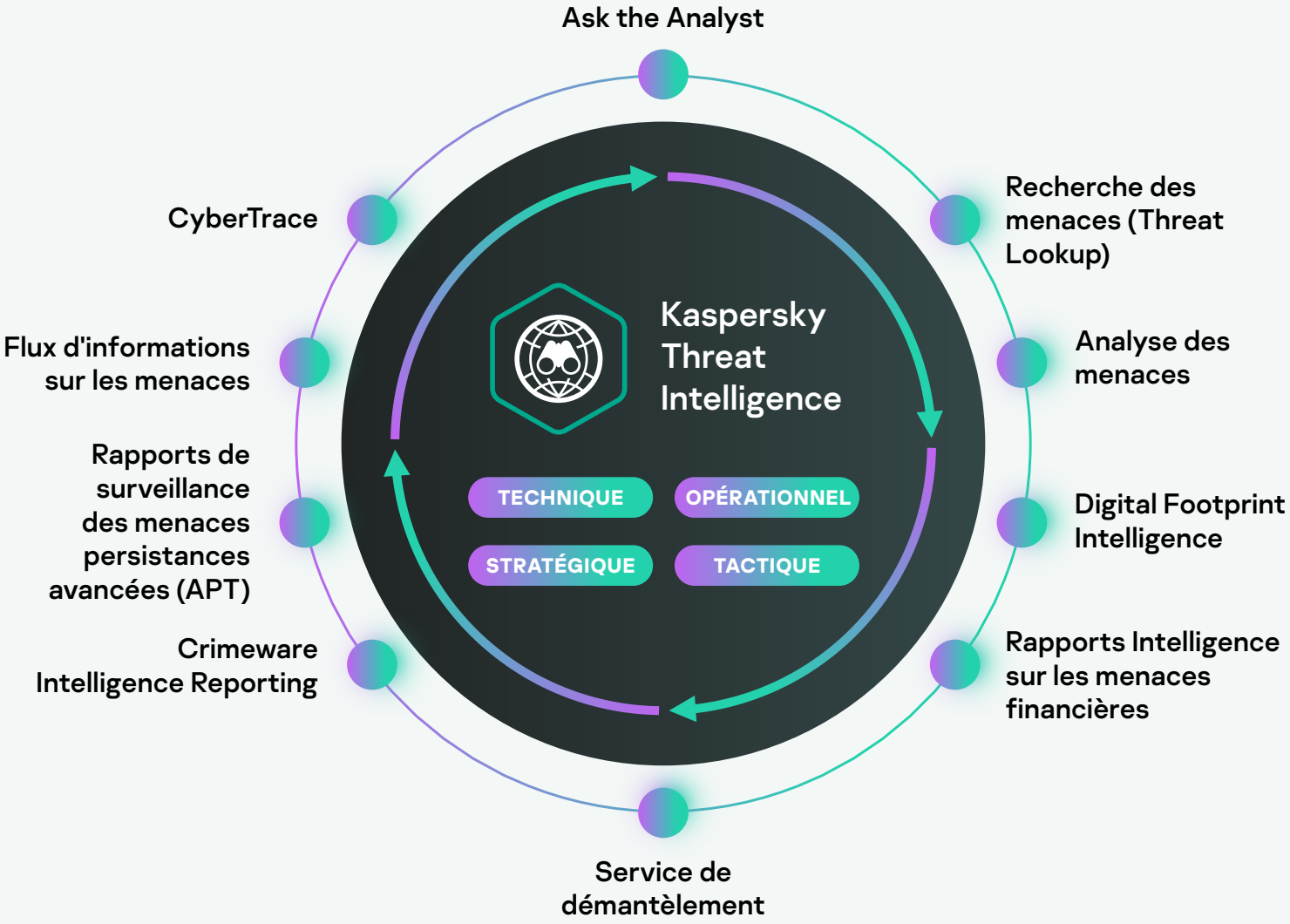
Kaspersky Threat Intelligence

Les services de Threat Intelligence (surveillance des menaces) de Kaspersky vous donnent accès aux informations nécessaires pour atténuer ces cybermenaces, fournies par notre équipe de chercheurs et d'analystes internationaux.

Les connaissances et l'expérience approfondies de Kaspersky dans tous les domaines de la cybersécurité en font le partenaire de choix des plus grandes autorités de police et administrations au monde, comme INTERPOL et les grands organismes CERT. Kaspersky Threat Intelligence vous donne un accès instantané à une solution Threat Intelligence technique, tactique, opérationnelle et stratégique.

Le portefeuille Threat Intelligence de Kaspersky inclut

Flux de données sur les menaces, CyberTrace (une plateforme Threat Intelligence), Threat Lookup, Threat Analysis (Cloud Sandbox et Cloud Threat Attribution Engine), une gamme d'options de rapport Threat Intelligence, et des services offrant une expertise de Threat Intelligence sur demande.



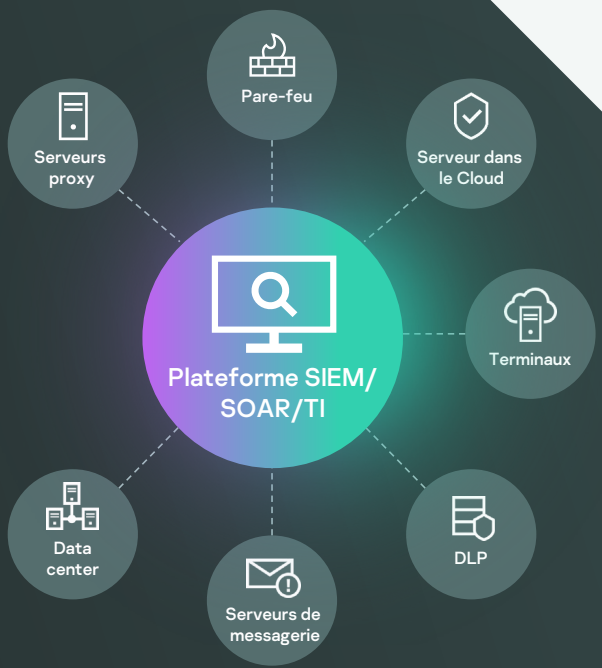
Kaspersky Threat Data Feeds

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

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

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

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 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

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

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

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

Kaspersky CyberTrace

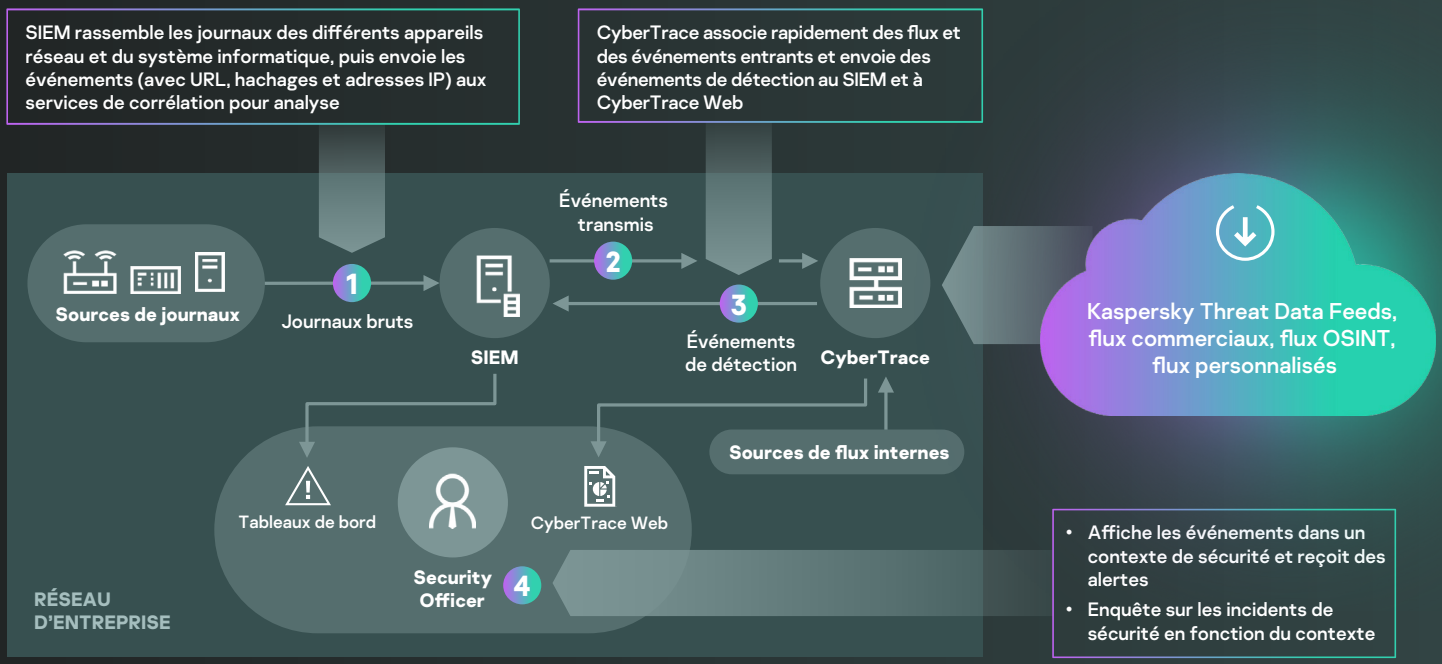
En intégrant aux contrôles de sécurité existants (ex : systèmes SIEM) des données de Threat Intelligence mises à jour minute par minute et interprétables par une machine, les centres de sécurité peuvent automatiser le processus de tri initial tout en fournissant aux spécialistes de niveau 1 un contexte suffisant pour identifier immédiatement les alertes qui doivent faire l'objet d'une enquête ou être remontées aux équipes de réponse aux incidents. Néanmoins, la croissance continue du nombre de flux de données sur les menaces et de sources de Threat Intelligence complique singulièrement la tâche des organisations, qui peinent à identifier les informations pertinentes. Les données de Threat Intelligence, fournies dans différents formats et comprenant une quantité phénoménale d'indicateurs de compromission, sont particulièrement indigestes pour les SIEM ou les contrôles de sécurité du réseau.

Kaspersky CyberTrace est un outil de fusion et d'analyse des données de Threat Intelligence qui assure une intégration transparente des flux de données sur les menaces dans les solutions SIEM afin d'aider les analystes à exploiter efficacement ces données dans le cadre de leurs opérations de sécurité. L'outil s'intègre à tous les flux de Threat intelligence (flux de Kaspersky ou d'autres fournisseurs, flux OSINT ou flux de vos propres clients) aux formats JSON, STIX, XML et CSV, et propose donc une intégration prête à l'emploi avec la plupart des solutions SIEM et des sources de journaux.

Kaspersky CyberTrace offre un ensemble d'outils pour mettre en œuvre la Threat intelligence de manière efficace :

- Une base de données d'indicateurs dotée de la recherche plein texte et la capacité de faire des demandes de recherche avancées rendent possibles des recherches complexes dans tous les domaines d'indicateurs, y compris les zones de contexte
- Des pages avec des informations détaillées à propos de chaque indicateur assurent une analyse encore plus approfondie. Chaque page présente toutes les informations issues de l'ensemble des fournisseurs de service de veille à propos d'un indicateur (déduplication) pour permettre aux analystes de discuter des menaces dans les commentaires et d'ajouter des éléments de Threat Intelligence internes à propos de l'indicateur
- Un graphique de recherche permet d'explorer visuellement les données et les détections stockées dans CyberTrace et de découvrir des points communs entre les menaces
- La fonctionnalité d'exportation des indicateurs prend en charge l'exportation des ensembles d'indicateurs vers les contrôles de sécurité, comme les listes de politiques (listes de blocage), ainsi que le partage des données de menaces entre les instances Kaspersky CyberTrace ou avec d'autres plateformes TI
- Identifier les indicateurs IOC simplifie leur gestion. Vous pouvez créer n'importe quelle étiquette et spécifier son poids (importance) et l'utiliser pour identifier les indicateurs IOC manuellement. Vous pouvez aussi trier et filtrer les indicateurs IOC selon ces étiquettes et leurs poids
- La fonctionnalité de corrélation historique (analyse rétrospective) vous permet d'analyser des éléments observables issus d'évènements déjà vérifiés en utilisant les flux les plus récents pour trouver des menaces précédemment non identifiées
- Un filtre envoie des événements de détection vers les solutions SIEM, réduisant ainsi la charge sur ces dernières et sur les analystes
- Cas d'usage des prises en charge multi-clients des MSSP et des grandes entreprises
- Les statistiques d'utilisation des flux visant à mesurer l'efficacité des flux intégrés et la matrice d'intersection des flux aident à sélectionner les meilleurs fournisseurs de Threat Intelligence
- HTTP RestAPI vous aide à gérer et à faire des recherches au sein de la Threat Intelligence

L'outil utilise un processus internalisé d'analyse et d'association des données entrantes qui réduit considérablement la charge de travail du SIEM. Kaspersky CyberTrace traite les journaux et les événements entrants, associe rapidement les résultats aux flux et génère ses propres alertes de détection des menaces. L'illustration ci-dessous montre une architecture d'intégration de la solution de haut niveau :



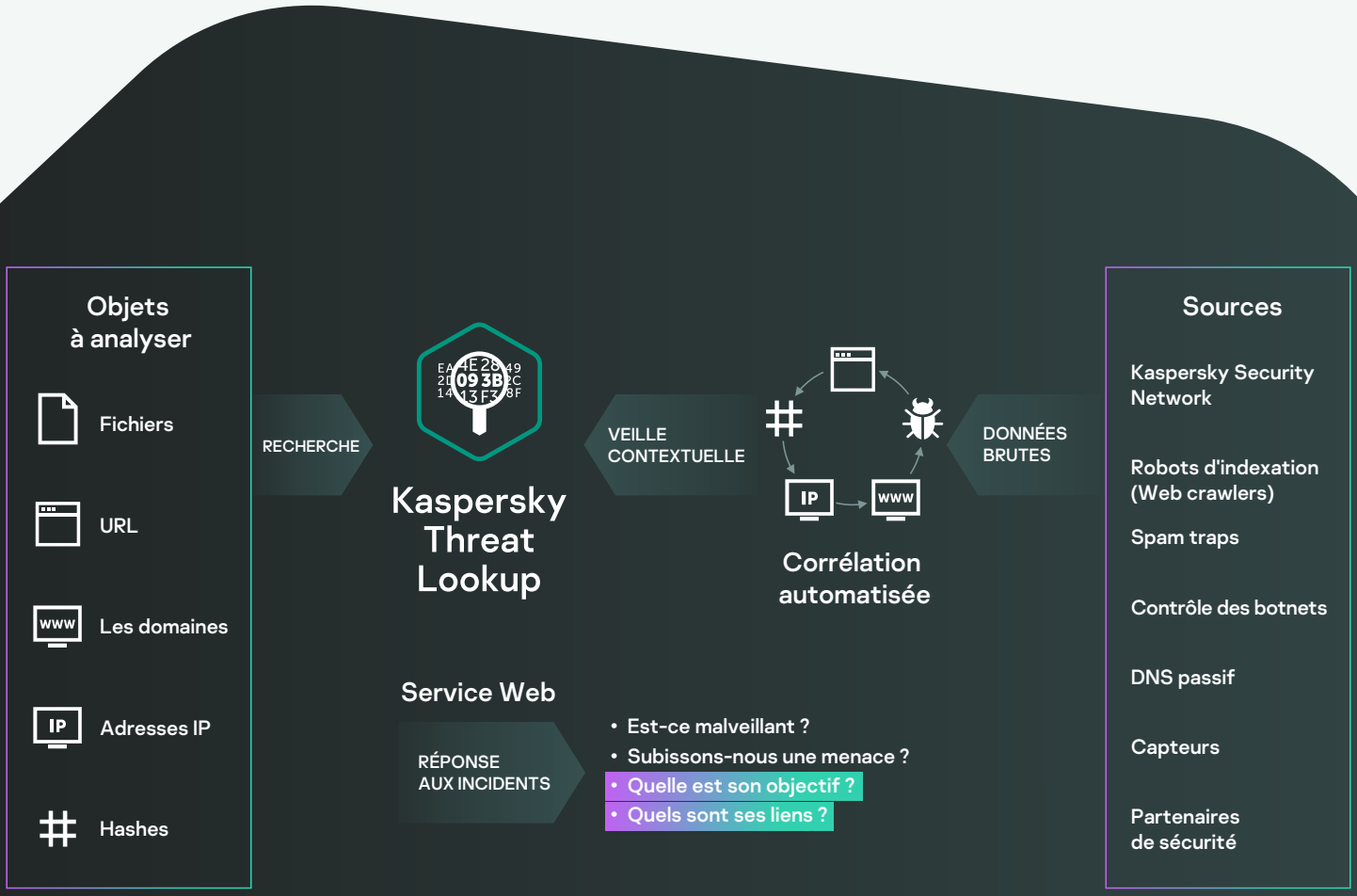
Avec Kaspersky CyberTrace et Kaspersky Threat Data Feeds, les analystes de sécurité peuvent :

- Traiter et hiérarchiser efficacement d'énormes volumes d'alertes de sécurité
- Améliorer et accélérer les procédures de tri et de réponse initiale
- Identifier immédiatement les alertes critiques pour l'entreprise et prendre des décisions mieux informées sur les alertes à faire remonter aux équipes de réponse aux incidents
- Élaborer une défense proactive basée sur la veille stratégique

Kaspersky Threat Lookup

La cybercriminalité ne connaît pas de frontières et les capacités techniques sur lesquelles elle s'appuie évoluent rapidement : nous assistons à des attaques qui sont de plus en plus sophistiquées, les cybercriminels ayant recours à des ressources du Dark Web pour menacer leurs cibles. La fréquence, la complexité et l'obfuscation des cybermenaces ne cessent de croître. Et les cybercriminels utilisent de nouveaux moyens pour affaiblir vos défenses. Chaînes de frappe complexes et TTP (Tactiques, Techniques et Procédures) personnalisées font désormais partie de leurs méthodes pour paralyser votre activité, dérober vos ressources et attaquer vos clients.

Kaspersky Threat Lookup fournit toutes les connaissances acquises par Kaspersky sur les cybermenaces et leurs liens, regroupées dans un service Web unique et efficace. Le but est de fournir à vos équipes de sécurité autant d'informations que possible, afin de contrer les cyberattaques avant qu'elles n'aient un impact sur votre entreprise. La plateforme récupère les dernières informations détaillées de Threat Intelligence sur les URL, les domaines, les adresses IP, les hachages de fichiers, les noms des menaces, les données statistiques/comportementales, les données WHOIS/DNS, les attributs de fichiers, les données de géolocalisation, les chaînes téléchargées, les horodatages, etc. Il en résulte une visibilité globale sur les menaces nouvelles et émergentes pour sécuriser votre entreprise et améliorer la réponse aux incidents.



Bénéfices

Informations de confiance : un des principaux atouts de Kaspersky Threat Lookup est la fiabilité de notre Threat Intelligence, ces informations sont enrichies d'un contexte exploitable, ce qui constitue un soutien pour des actions concrètes. Les produits de Kaspersky arrivent en tête dans les tests anti-malware[1] et démontrent la qualité inégalée de nos renseignements sur la sécurité en offrant les taux de détection les plus élevés, avec un nombre de faux positifs quasi nul

Recherche des menaces (Threat hunting) : faites preuve de proactivité dans la prévention, la détection et la réaction face aux attaques afin de minimiser leur impact et leur fréquence. Suivez et éliminez avec fermeté les attaques le plus tôt possible. Plus tôt vous détectez une menace, moins il y a de dommages et plus rapides sont les réparations ainsi que le retour à la normale des opérations de réseau

Investigations sur les incidents : un graphique de recherche dope les investigations sur les incidents en vous permettant d'explorer visuellement les données et détections stockées dans Threat Lookup. Il offre une visualisation graphique des relations entre les URL, les domaines, IPs, les fichiers et d'autres contextes afin que vous ayez une meilleure compréhension de la totalité de l'incident et de son origine.

Recherche maître : Cherchez des informations parmi tous les produits de threat intelligence actifs et les sources externes (notamment les IoC OSINT, le dark Web et le Web surfacique) dans une seule et puissante interface.

Interface Web conviviale ou API compatible REST : vous pouvez choisir d'utiliser le service en mode manuel par l'intermédiaire d'une interface Web (avec un navigateur Web) ou d'y accéder via une simple API compatible REST

Large éventail de formats d'exportation :exportez les indicateurs de compromission (IOC) ou le contexte exploitable dans des formats de partage largement utilisés et mieux organisés, interprétables par une machine, tels que STIX, OpenIOC, JSON, Yara, Snort ou même CSV, afin de profiter pleinement des avantages de la Threat Intelligence, d'automatiser les processus d'opérations, ou de les intégrer dans des contrôles de sécurité tels que SIEM

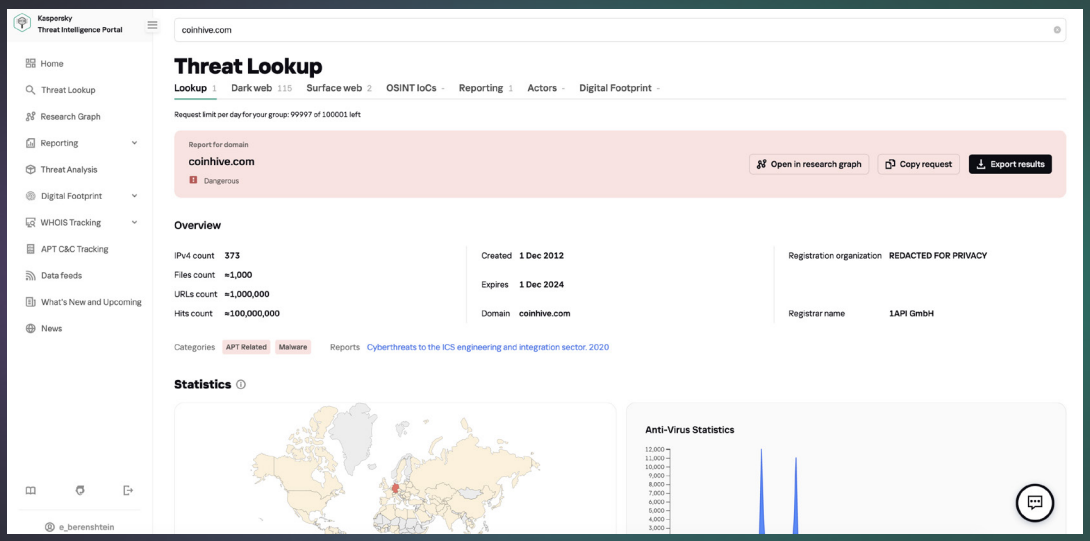
Avantages

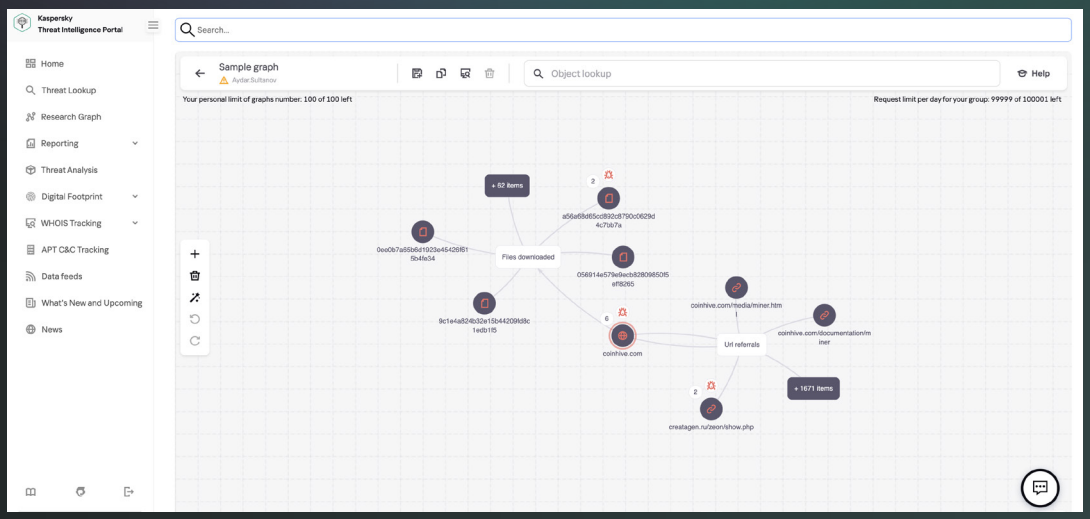
Examiner de manière approfondie les indicateurs de menace dotés d'un contexte hautement validé afin de hiérarchiser les attaques et de mettre l'accent sur l'atténuation des menaces les plus dangereuses pour votre entreprise

Diagnostiquer et analyser les incidents de sécurité sur les hébergeurs et le réseau plus efficacement, et hiérarchiser les signaux des systèmes internes contre des menaces inconnues

Doper vos capacités de réponse aux incidents et de recherche des menaces pour briser la chaîne de frappe avant que des données et des systèmes sensibles ne soient compromis

[1] kaspersky.fr/top3





Maintenant, c'est possible

Rechercher des indicateurs de menace via une interface Web ou une API compatible REST

Examiner les informations détaillées (certificats, noms couramment utilisés, chemins d'accès aux fichiers, URL associées) pour identifier de nouveaux objets suspects

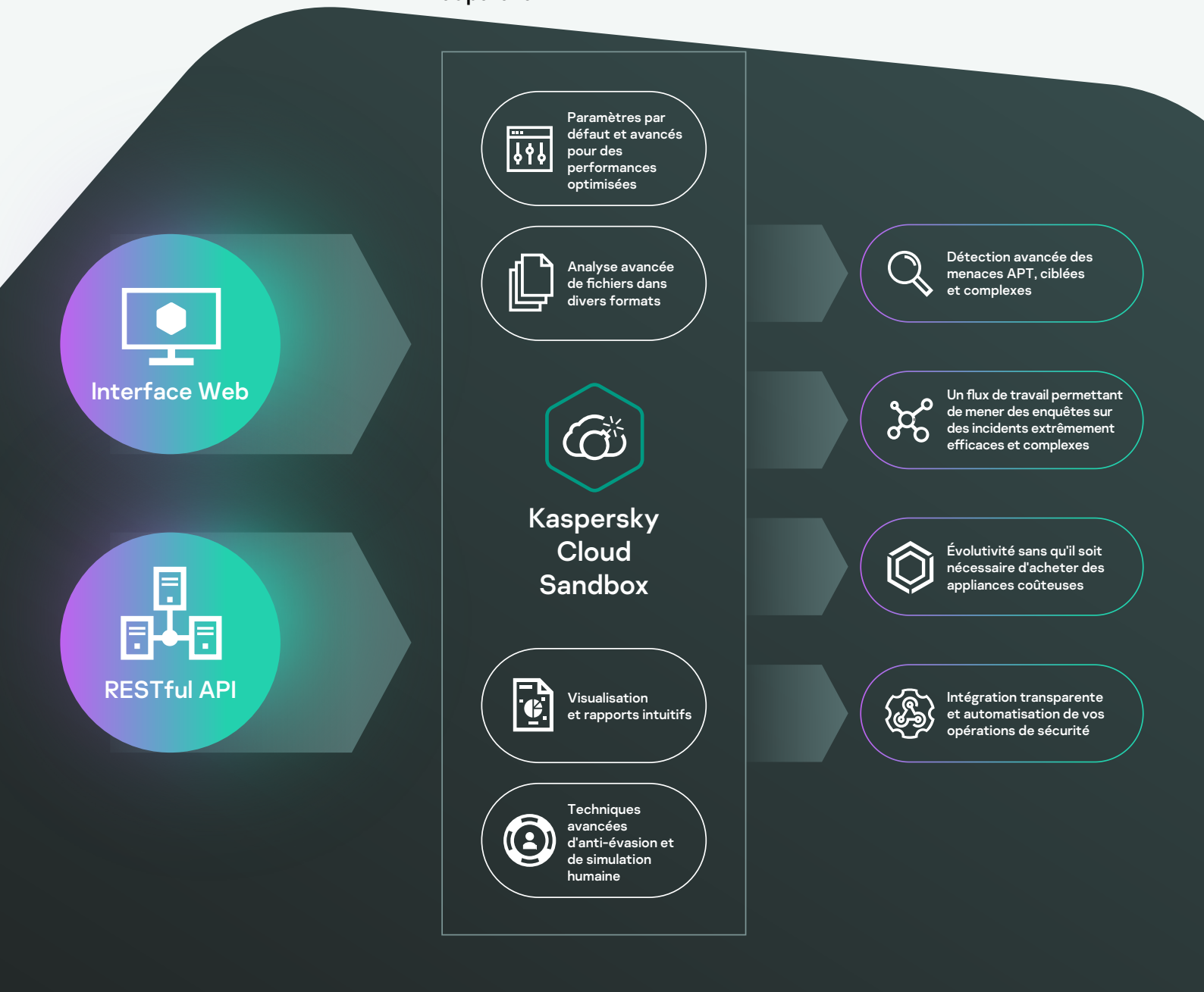
Vérifier si l'objet en question est répandu ou unique

Comprendre dans quelle mesure un objet particulier doit être considéré comme malveillant

Kaspersky Cloud Sandbox

Il est impossible d'éviter les attaques ciblées d'aujourd'hui uniquement avec les outils antivirus traditionnels. Les moteurs antivirus sont uniquement capables d'arrêter les menaces connues et leurs variations, tandis que d'ingénieux cybercriminels utilisent tous les moyens à leur disposition pour se soustraire à la détection automatique. Les pertes provenant d'incidents relatifs à la sécurité des informations continuent de croître de manière exponentielle, soulignant l'importance croissante des capacités de détection immédiate pour assurer une réponse rapide et contrer la menace avant que des dommages importants ne soient causés.

Prendre une décision intelligente basée sur le comportement d'un fichier tout en analysant simultanément la mémoire du processus, l'activité réseau etc. est l'approche optimale pour comprendre les menaces sophistiquées, ciblées et personnalisées les plus récentes. Alors que les données statistiques peuvent manquer d'informations sur les programmes malveillants récemment modifiés, les technologies de sandboxing sont des outils puissants qui permettent d'enquêter sur l'origine d'un échantillon de fichier, de collecter des indicateurs de compromission basés sur l'analyse comportementale et de détecter des objets malveillants qui n'avaient jamais été vus auparavant.



Génération de rapports complets

- Chargement et exécution des DLL
- Connectivités externes avec noms de domaine et adresses IP
- Création, modification et suppression de fichiers
- Informations détaillées de Threat Intelligence avec contexte exploitable pour chaque indicateur de compromission révélé (IoC)
- Décharges de mémoire de processus et de trafic réseau (PCAP)
- Requêtes et réponses HTTP et DNS
- Création d'extensions mutuelles (mutex)
- API compatible REST
- Modification et création des clés du registre
- Processus créés par le fichier exécuté
- Captures d'écran
- **etc.**

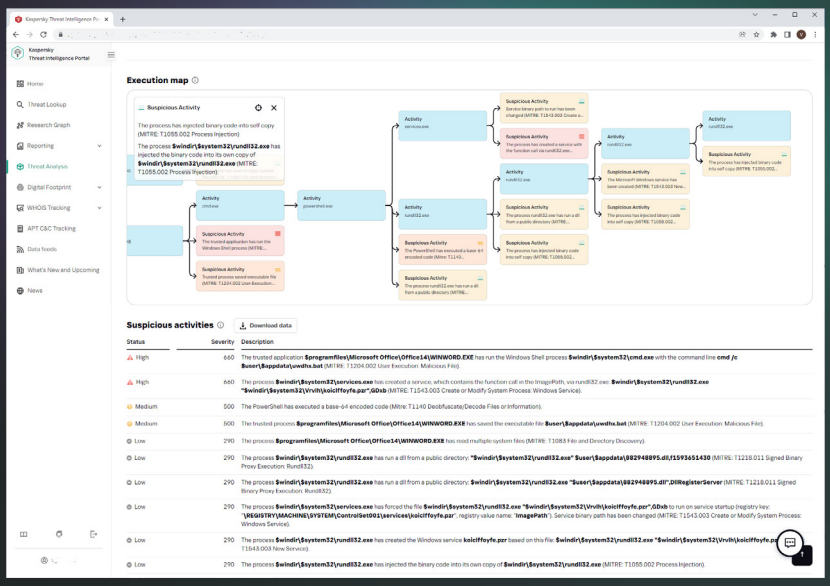
Détection et atténuation proactives des menaces

Les logiciels malveillants utilisent un large panel de méthodes pour attaquer sans être détectés. Si le système ne respecte pas les paramètres requis, le programme malveillant s'autodétruira certainement, ne laissant aucune trace. Pour que le code malveillant s'exécute, l'environnement de sandboxing doit être capable d'imiter avec précision le comportement normal de l'utilisateur final.

La Kaspersky Cloud Sandbox offre une approche hybride combinant la Threat Intelligence glanée à partir de pétaoctets de données statistiques (grâce à Kaspersky Security Network et à d'autres systèmes propriétaires), l'analyse comportementale et l'anti-évasion, avec des technologies de simulation humaine telles que le sélecteur automatique, le défilement des documents et des processus factices.

Ce produit a été développé dans notre laboratoire sandbox interne, pendant plus d'une décennie. La technologie intègre toute notre connaissance des comportements malveillants gagnée pendant 20 ans de recherche continue sur les menaces. Cela nous permet de détecter plus de 360 000 nouveaux objets malveillants chaque jour et d'offrir à nos clients des solutions novatrices en termes de sécurité.

Dans le cadre de notre Threat intelligence Portal, Cloud Sandbox est le composant important dans votre flux de travail pour la Threat intelligence. Tandis que le portail récupère les dernières informations détaillées de Threat Intelligence sur les URL, les domaines, les adresses IP, les hachages de fichiers, les noms des menaces, les données statistiques/comportementales, les données WHOIS/DNS, etc., la Cloud Sandbox permet de relier ces connaissances aux indicateurs de compromission générés par l'échantillon analysé.



Vous pouvez désormais mener des enquêtes très efficaces et complexes sur les incidents pour acquérir une compréhension immédiate de la nature de la menace, puis tirer des conclusions à mesure que vos recherches révèlent les indicateurs de menace interconnectés.

L'inspection peut être très gourmande en ressources, surtout lorsqu'il s'agit d'attaques à plusieurs niveaux. Kaspersky Cloud Research Sandbox stimule la réponse aux incidents et les activités de cyberdiagnostic, en vous offrant l'évolutivité nécessaire pour traiter automatiquement les fichiers sans avoir à acheter des appliances coûteuses ou à vous soucier des ressources système.

Kaspersky APT Intelligence Reporting

Les clients de rapports de surveillance des APT de Kaspersky accèdent à tout moment à nos enquêtes et découvertes, y compris aux données techniques complètes (sous plusieurs formats), sur chaque APT, dès sa découverte, ainsi que sur toutes les menaces qui ne seront jamais rendues publiques. Les rapports contiennent un résumé analytique offrant des informations faciles à comprendre destinées aux cadres supérieurs ainsi qu'une description détaillée de l'APT, des règles Yara et des indicateurs IOC associés pour fournir aux experts en sécurité, aux analystes de programmes malveillants, aux ingénieurs en sécurité, aux analystes de la sécurité des réseaux et aux experts en matière d'APT des conseils exploitables afin d'assurer une protection supérieure.

Nos experts vous alerteront de suite s'ils constatent une modification dans les stratégies des groupes de cybercriminels. Vous aurez également accès à tous les rapports des bases de données d'APT de Kaspersky, un autre outil de recherche et d'analyse puissant venant compléter votre arsenal de sécurité.

Avantages

Enrichi avec les données

Toutes les TTP décrites dans les rapports sont cartographiées dans le cadre MITRE ATT&CK, améliorant ainsi la détection et la réponse grâce au développement et à la hiérarchisation des cas d'utilisation de surveillance sécurisée correspondants, ainsi qu'aux analyses d'écarts et aux tests des moyens de défense actuels contre les TTP pertinentes

Information sur les APT privées

Pour plusieurs raisons, toutes les menaces les plus graves ne sont pas révélées publiquement. Mais nous les partageons toutes avec nos clients

Accès privilégié

Recevez des descriptions techniques sur les dernières menaces pendant les enquêtes, avant leur révélation au grand public

Analyse rétrospective

Accès garanti à tous les rapports privés précédents durant toute la période de votre abonnement

Un accès aux données de l'entreprise...

Une documentation technique détaillée, avec une liste complète d'IOC, dans des formats standard tels qu'OpenIOC ou STIX, en plus de l'accès à nos règles YARA

Profils de criminels

Notamment le pays d'origine et la principale activité suspectés, familles de programmes malveillants utilisées, secteurs et régions visés, et descriptions de toutes les TTP utilisées dans le cadre MITRE ATT&CK

Une surveillance continue des campagnes d'APT

Accès aux informations exploitables au cours de l'enquête avec (information sur la distribution des menaces APT, les indicateurs IOC, les infrastructures de commande et de contrôle, etc.

API compatible REST

Intégration transparente et automatisation de vos flux de travail de sécurité

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)

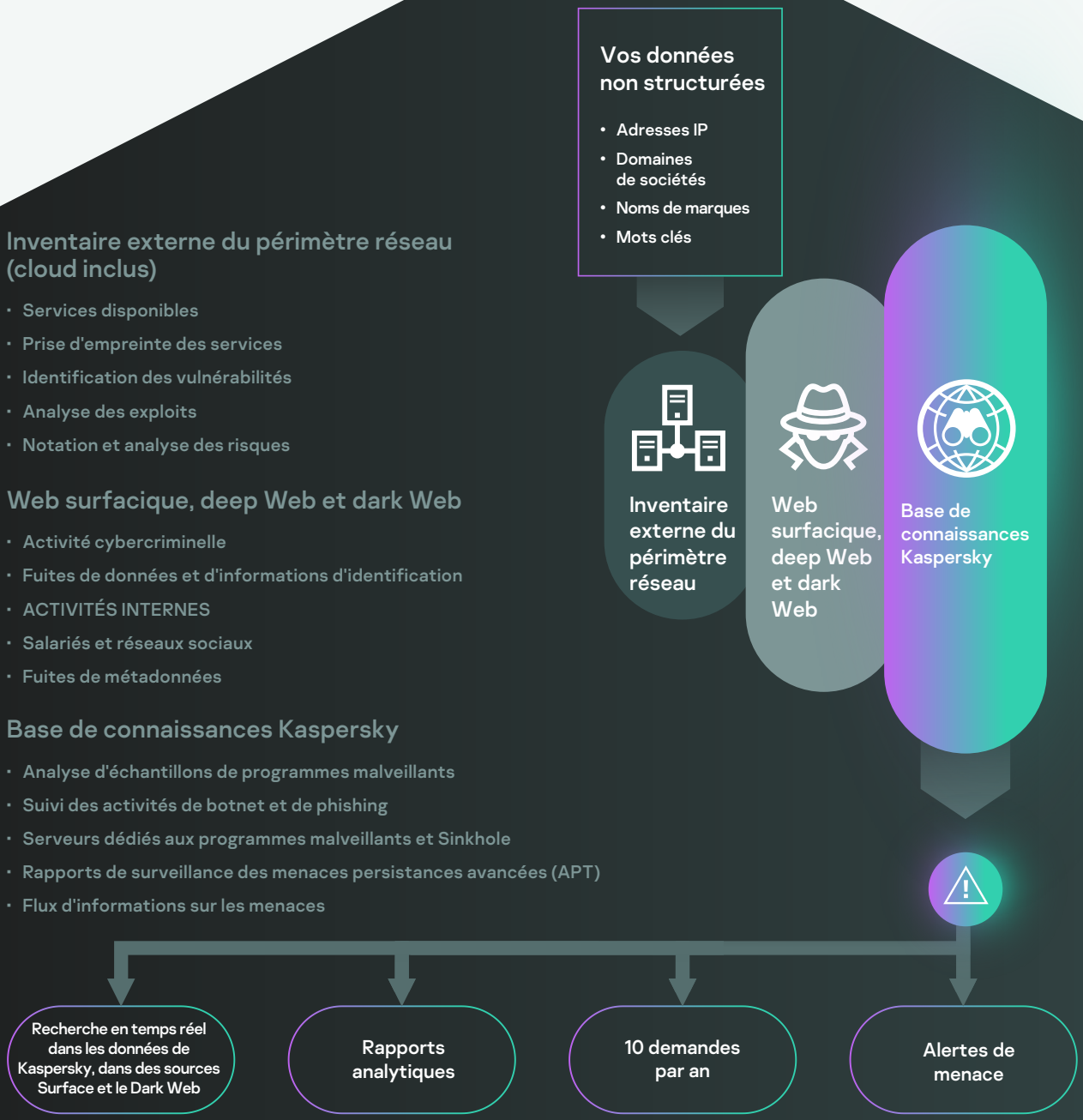
- Services disponibles
- Prise d'empreinte des services
- Identification des vulnérabilités
- Analyse des exploits
- Notation et analyse des risques

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



Rapports de Kaspersky Threat Intelligence sur les menaces financières

Kaspersky ICS Threat Intelligence Reporting fournit des données d'analyse et permet de prendre conscience des campagnes malveillantes ciblant les entreprises industrielles. Il fournit également des informations sur les vulnérabilités détectées dans les systèmes de contrôle industriel les plus courants et les technologies sous-jacentes. Les rapports sont transmis via un portail Web, ce qui signifie que vous pouvez commencer à exploiter le service immédiatement.

Rapports inclus dans votre abonnement

1. **Rapports sur les APT** Rapports sur les nouvelles APT et les campagnes d'attaque de grande ampleur ciblant des entreprises industrielles, mises à jour sur les menaces actives.
2. **L'environnement à risques.** Rapports sur les modifications majeures de l'environnement à risques pour les systèmes de contrôle industriel, derniers facteurs détectés affectant les niveaux de sécurité des ICS et leur exposition aux menaces, y compris des informations propres à la région, au pays et au secteur.
3. **Vulnérabilités détectées.** Rapports sur les vulnérabilités identifiées par Kaspersky dans les plupart des produits les plus utilisés dans les systèmes de contrôle industriel, L'Internet industriel des objets et les infrastructures dans différents secteurs.
4. **Analyse et atténuation des vulnérabilités.** Nos rapports fournissent des recommandations exploitables émanant d'experts Kaspersky visant à identifier et à atténuer les vulnérabilités dans votre infrastructure.

Les données de Threat Intelligence vous permettent de

Détecter et anticiper les

menaces signalées pour protéger les ressources critiques, y compris les composants logiciels et matériels, et garantir la sécurité et la continuité du processus technologique

Évaluer

les vulnérabilités de vos environnements industriels et de vos ressources sur la base d'évaluations précises de la portée et de la gravité des vulnérabilités et prendre des décisions éclairées sur la gestion des correctifs ou sur la mise en œuvre d'autres mesures préventives que nous recommandons

Mettre en corrélation

l'activité malveillante et suspecte que vous détectez dans les environnements industriels avec les résultats de l'étude Kaspersky pour attribuer votre détection aux campagnes malveillantes signalées, identifier les menaces et répondre rapidement aux incidents

Profiter

les informations sur les technologies, les tactiques et les procédures d'attaque, sur les dernières vulnérabilités découvertes et sur d'autres modifications majeures de l'environnement à risques pour :

- identifier et évaluer les risques inhérents aux menaces signalées et aux autres menaces similaires
- Planifier et concevoir des modifications à apporter à l'infrastructure industrielle pour garantir la sécurité de la production et la continuité du processus technologique
- Exécuter des activités de sensibilisation à la sécurité sur la base de l'analyse de cas réels pour développer des scénarios de formation personnelle et planifier des exercices équipe rouge contre équipe bleue
- Prendre des décisions stratégiques éclairées pour investir dans la cybersécurité et garantir la résilience des opérations

Kaspersky Ask the Analyst

Les cybercriminels développent constamment des moyens complexes d'attaquer les entreprises. Le paysage actuel des menaces, volatile et en pleine expansion, présente des fonctionnalités de plus en plus agiles en matière de cybercriminalité. Les organisations sont confrontées à des incidents complexes causés par des attaques sans programme malveillant, des attaques sans fichier, des attaques hors sol, des exploits de type zero-day ainsi que des combinaisons de tous ces éléments constitutifs des menaces complexes, des APT et d'attaques ciblées.

Recherche continue sur les menaces

permet à Kaspersky de découvrir, d'infiltrer, et de surveiller les communautés fermées et les forums obscurs du monde entier fréquentés par des adversaires et des cybercriminels. Nos analystes tirent parti de cet accès pour détecter et étudier de manière proactive les menaces les plus graves et les plus connues ainsi que les menaces conçues pour cibler des organisations particulières.

À une époque marquée par des cyberattaques dévastatrices ciblant les entreprises, les professionnels de la cybersécurité sont plus importants que jamais, mais il n'est pas facile de les trouver ni de les retenir. Même si vous disposez d'une équipe de cybersécurité bien établie, vous ne pouvez pas toujours attendre de vos experts qu'ils mènent seuls la guerre contre les menaces complexes. **Ils doivent pouvoir faire appel à l'aide de tiers experts.** Une expertise externe permet d'éclairer les voies probables d'attaques complexes et d'APT, et fournir des conseils exploitables sur la manière la plus déterminante de les éliminer.

Livrables de Ask the Analyst

(Abonnement unifié sur demande)

Le service **Kaspersky Ask the Analyst** étend notre portefeuille de Threat Intelligence, vous permettant de demander des conseils et des informations sur des menaces spécifiques auxquelles vous êtes confronté ou qui vous intéressent. Ce service adapte les puissantes capacités de recherche sur les menaces et de Threat Intlligence de Kaspersky à vos besoins particuliers, vous permettant ainsi de mettre en place des défenses résilientes contre les menaces visant votre organisation.

APT et crimeware

Informations supplémentaires sur les rapports publiés et les recherches en cours (en plus du service APT ou Crimeware Intelligence Reporting)[1]

Analyse des programmes malveillants

- Analyse d'échantillons des programmes malveillants
- Recommandations concernant d'autres mesures correctives

Descriptions des menaces, des vulnérabilités et des IoC connexes

- Description générale d'une famille particulière de programmes malveillants
- Contexte supplémentaire pour les menaces (hachages associés, URLs, CnCs, etc.)
- Informations sur une vulnérabilité particulière (son degré de criticité et les mécanismes de protection correspondants dans les produits Kaspersky)

Renseignements sur le Dark Web [2]

- Recherche sur le Dark Web d'artefacts particuliers, d'adresses IP, de noms de domaine, de noms de fichiers, d'emails, de liens ou d'images.
- Recherche et analyse d'informations

Requêtes liées aux ICS

- Informations supplémentaires sur les rapports publiés
- Information sur la vulnérabilité des ICS
- Statistiques de menaces ICS et tendances par zone géographique / secteur
- Information d'analyse des programmes malveillants ICS sur les réglementations ou les normes

[1] Disponible uniquement pour les clients ayant un rapport actif APT et/ou Crimeware Intelligence.

[2] Déjà inclus dans l'abonnement Kaspersky Digital Footprint Intelligence

Avantages du service

Renforcement de votre expertise

Profitez d'un accès sur demande à des experts du secteur sans avoir à chercher ni à investir dans le recrutement de spécialistes à plein temps difficiles à trouver

Accélération des enquêtes

Priorisez efficacement les incidents et définissez-en la portée en fonction d'informations contextuelles détaillées et adaptées

Réponse rapide

Répondez rapidement aux menaces et aux vulnérabilités en utilisant nos conseils pour bloquer les attaques via des vecteurs connus.

Comment ça fonctionne ?

Kaspersky Ask the Analyst peut être acheté séparément ou en complément de l'un de nos services de Threat Intelligence.

Vous pouvez envoyer vos demandes via Kaspersky Company Account, notre portail de support pour les entreprises clientes. Nous vous répondrons par email, mais en cas de besoin et avec votre accord, nous pouvons organiser une conférence téléphonique et/ou une session de partage d'écran. Une fois que votre demande est acceptée, vous serez informé du délai estimé pour sa prise en charge.

Cas d'usage des services :

- Clarifier tout détail dans les rapports de Threat Intelligence publiés précédemment
- Obtenir des renseignements supplémentaires pour les IoC déjà fournis
- Obtenir des détails sur les vulnérabilités et des recommandations sur la manière de se protéger contre leur exploitation
- Obtenir des détails supplémentaires sur les activités particulières du Dark Web qui vous intéressent
- Obtenir un rapport général sur la famille de programmes malveillants comprenant le comportement du programme malveillant, son incidence potentielle et des détails relatifs à toute activité connexe observée par Kaspersky
- Prioriser efficacement les alertes/incidents à l'aide de renseignements contextuels détaillés et d'une catégorisation des IoC connexes fournis par le biais de rapports succincts
- Demander de l'aide pour déterminer si l'activité inhabituelle détectée est liée à une APT ou à un acteur de crimeware
- Envoyer des fichiers de logiciels malveillants pour une analyse complète afin de comprendre le comportement et la fonctionnalité du ou des échantillons fournis

Élargissement de vos connaissances et de vos ressources

Kaspersky Ask the Analyst vous donne accès à un groupe restreint de chercheurs de Kaspersky, au cas par cas. Ce service permet une communication complète entre experts afin de renforcer vos capacités existantes grâce à nos connaissances et ressources uniques.

Avantages du service

Protection mondiale

Peu importe où est enregistré le domaine malveillant ou de phishing, Kaspersky demandera son démontage de l'organisation régionale avec l'autorité juridique pertinente.

Gestion intégrale

Nous nous occuperons de tout le processus de démontage et réduirons au maximum votre implication.

Visibilité complète

Vous serez informés à chaque étape du processus, de l'enregistrement de votre demande au démontage accompli.

Intégration avec Digital Footprint Intelligence

Le service s'intègre avec Kaspersky Digital Footprint Intelligence qui offre des notifications en temps réel sur des domaines malveillants et de phishing, conçus pour porter atteinte, malmener ou imiter votre marque / entreprise. Une solution unique est un composant important d'une stratégie complète de cybersécurité.

Kaspersky Takedown Service

Défi

Les cybercriminels créent des domaines malveillants et de phishing utilisés pour attaquer votre entreprise et vos marques. L'incapacité d'atténuer ces menaces rapidement une fois identifiées, peut conduire à une perte de revenus, à une atteinte à l'image de marque, à une perte de confiance des clients, à des fuites de données, et bien plus encore. Mais gérer les démontages de ce genre de domaines est un processus complexe qui requiert de l'expertise et du temps.

Solution

Kaspersky bloque plus de 15 000 URL de phishing/scam et empêche plus d'un million de tentatives de cliquer sur de tels URL chaque jour. Nos nombreuses années d'expérience dans l'analyse de domaines malveillants et de phishing nous permettent de savoir comment rassembler les preuves indiquant qu'il s'agit de domaines malveillants. Une gestion de bout en bout des tâches permettant une action rapide pour minimiser votre risque numérique afin que votre équipe puisse se concentrer sur d'autres tâches prioritaires.

Kaspersky fournit à ses clients une protection efficace de leurs services en ligne et de leur réputation en travaillant avec les organisations internationales et les services de police (INTERPOL, Europol, division Microsoft Digital Crimes Unit, NHTCU (National High Tech Crime Unit) aux Pays-Bas et City of London Police, par exemple) ainsi qu'avec les CERT (Computer Emergency Response Teams) du monde entier.

Comment ça fonctionne ?

Vous pouvez envoyer vos demandes via Kaspersky Company Account, notre portail de support pour les entreprises clientes. Nous préparerons toute la documentation nécessaire et enverrons la demande de démontage à l'autorité locale / régionale compétente (CERT, registraire, etc.) ayant les droits juridiques nécessaires pour fermer le domaine. Vous recevrez des notifications à chaque étape du processus jusqu'à ce que la ressource demandée soit démontée avec succès.

Protection sans effort

Le service de démontage Kaspersky réduit rapidement les menaces posées par des domaines malveillants et de phishing avant qu'un quelconque dommage soit causé à votre marque et à votre entreprise. La gestion de bout-en-bout du processus entier vous fait gagner du temps et de l'argent.

Principaux avantages

- Permet une visibilité mondiale des menaces, la détection rapide des cybermenaces, la hiérarchisation des alertes de sécurité et une réponse efficace aux incidents liés à la sécurité des informations
- Évite aux analystes de subir un burn-out et aide vos effectifs à se concentrer sur de véritables menaces
- Les aperçus uniques des tactiques, techniques et procédures utilisées par les acteurs de la menace parmi les différents secteurs et régions permettent une protection proactive contre les menaces ciblées et complexes
- Un aperçu complet de votre système de sécurité avec des recommandations exploitables sur les stratégies d'atténuation vous permettent de concentrer votre stratégie de défense sur des domaines identifiés comme cibles de choix des cyberattaques
- Une réponse améliorée et accélérée aux incidents et de meilleures capacités de recherche des menaces aident à réduire le temps d'arrêt des attaques et minimisent de manière significative les dommages potentiels

Conclusion

La lutte contre les cybermenaces d'aujourd'hui nécessite une vue à 360 degrés des tactiques et outils utilisés par les cybercriminels. La génération de ces renseignements et l'identification des contre-mesures les plus efficaces exige une implication constante et des niveaux élevés d'expertise. Avec plusieurs péta-octets de données sur les menaces à exploiter, des technologies avancées de machine learning et une équipe unique d'experts partout dans le monde, Kaspersky travaille dur pour aider ses clients en leur proposant les informations sur les dernières menaces du monde entier, et en leur permettant de préserver leur immunité, même en cas de cyberattaques qui ne sont pas encore détectables.

FORRESTER®

Kaspersky se positionne comme un leader dans le rapport Forrester New Wave : External Threat Intelligence Services, 2021.

www.kaspersky.fr