Gardez une longueur d'avance
sur vos adversaires

Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

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 CERT majeurs. Kaspersky Threat Intelligence vous donne un accès instantané à une solution de Threat Intelligence tactique, opérationnelle et stratégique.

La Threat Intelligence offre une vision complète du paysage mondial des menaces, en combinant des sources de renseignements, des flux de données sur les menaces et des recherches internes, le tout analysé par notre équipe d'experts dans le but de fournir des informations exploitables afin d'aider les organisations à se protéger contre les cybermenaces.

Kaspersky Threat Intelligence vous accompagne

Identifiez et prévenez les menaces de manière proactive

Kaspersky Threat Intelligence vous tient informé des dernières menaces et vulnérabilités, ce qui vous permet de prendre des mesures proactives pour protéger vos systèmes avant qu'une attaque se produise.

Gagnez en visibilité sur votre empreinte numérique

Kaspersky Threat Intelligence offre une vue d'ensemble de votre empreinte numérique, y compris de toutes les ressources qui peuvent être exposées à une attaque ou à une compromission.

Améliorez votre capacité de détection des menaces

Kaspersky Threat Intelligence vous aide à compléter vos solutions de sécurité existantes avec les dernières informations sur les menaces, améliorant ainsi votre capacité à détecter et à bloquer les menaces avancées.

Améliorez votre réponse aux incidents

Kaspersky Threat Intelligence fournit des informations en temps réel au sujet des menaces émergentes et des indicateurs de compromission, de sorte que vous puissiez répondre rapidement et efficacement aux incidents.

Respectez les réglementations et les normes

Toutes les entreprises sont soumises à diverses réglementations et normes au sein de leur industrie. Kaspersky Threat Intelligence facilite la mise en conformité en vous aidant à répondre à ces exigences.

Enrichissez votre expertise interne

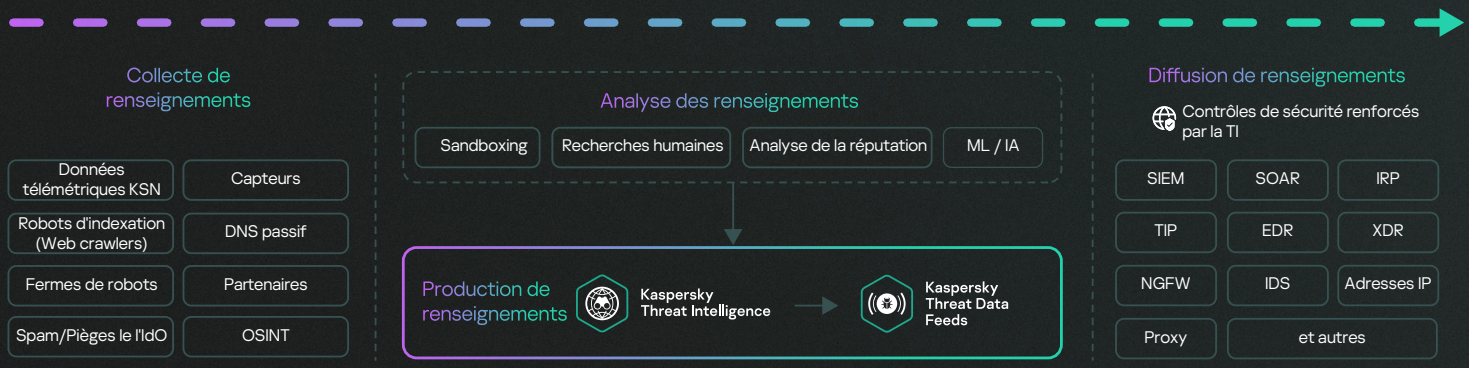
L'équipe d'experts de Kaspersky figure parmi les chercheurs les plus expérimentés et les plus respectés de l'industrie, apportant une richesse de connaissances et d'expertise à vos équipes de sécurité industrielle.

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. Une protection efficace 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.

Kaspersky Threat Data Feed fournit des informations de Threat Intelligence en temps réel pour vous aider à protéger vos réseaux et systèmes contre les menaces. Les flux de données comprennent des informations sur les programmes malveillants connus, les sites Internet de phishing, les dernières vulnérabilités et exploits, ainsi que d'autres types de cybermenaces. Ces informations vous aideront à bloquer le trafic malveillant, à mettre à jour votre logiciel de sécurité et à prendre d'autres mesures pour vous protéger contre les cyberattaques.



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.

Comment ça fonctionne ?

1

Les données sont collectées à partir d'une grande variété de sources fiables, notamment Kaspersky Security Network et nos propres robots d'exploration, le service de surveillance des menaces des botnets (qui suit les botnets et leurs cibles 24h24, 7j/7), les pièges à spam, les données des groupes de recherche, les partenaires et bien d'autres choses encore.

2

Toutes les informations collectées sont soigneusement vérifiées et nettoyées en temps réel à l'aide de diverses méthodes de prétraitement : sandboxing, analyse statistique et heuristique, outils de similarité, profilage comportemental et analyse d'experts.

3

Les flux de données permettent de collecter des informations liées aux menaces concernant une alerte ou un incident, et de les examiner en détail. Ils permettent également de répondre aux questions « Qui ? Quoi ? Where? Pourquoi ? » et de déterminer la source d'une attaque, ce qui permet de prendre rapidement des décisions pour protéger l'entreprise contre les menaces, quelle que soit leur complexité.

Les entrées des flux fournis par Kaspersky contiennent des données contextuelles 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.

Avantages liés à Kaspersky Threat Data Feeds

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.

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 sur les cyberattaques et les intentions, capacités et cibles de vos adversaires. Les principaux systèmes SIEM (y compris ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) et les plateformes TI sont totalement pris en charge.

Empêchez toute fuite de ressources sensibles et de propriété intellectuelle

en dehors de votre organisation à partir de 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.

Développez votre activité de MSSP

en offrant à vos clients un service de pointe en matière de Threat Intelligence. Si vous faites partie du CERT, optimisez et élargissez vos capacités de détection et d'identification des cybermenaces.

Kaspersky CyberTrace

La croissance continue du nombre de flux de données sur les menaces et de sources de Threat Intelligence complique singulièrement la tâche des entreprises, qui peinent à identifier les informations pertinentes. En même temps, les données de Threat Intelligence, fournies dans différents formats et comprenant une quantité phénoménale d'indicateurs de compromission, sont particulièrement indigestes pour les SIEM et d'autres contrôles de sécurité du réseau.

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.

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.

Outils

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 le contexte

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

Le balisage des IOC simplifie la gestion des IOC. Créez 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

Le 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 vous permet d'exporter des ensembles d'indicateurs vers les contrôles de sécurité, comme les listes de politiques (listes de blocage) ainsi que de partager des données de menaces entre les instances Kaspersky CyberTrace ou avec d'autres plateformes TI

La fonctionnalité de corrélation historique (analyse rétrospective) vous permet d'analyser des éléments observables issus d'événements déjà vérifiés en utilisant les flux les plus récents pour trouver des menaces précédemment identifiées

Cas d'usage des prises en charge multi-clients des MSSP et des grandes entreprises

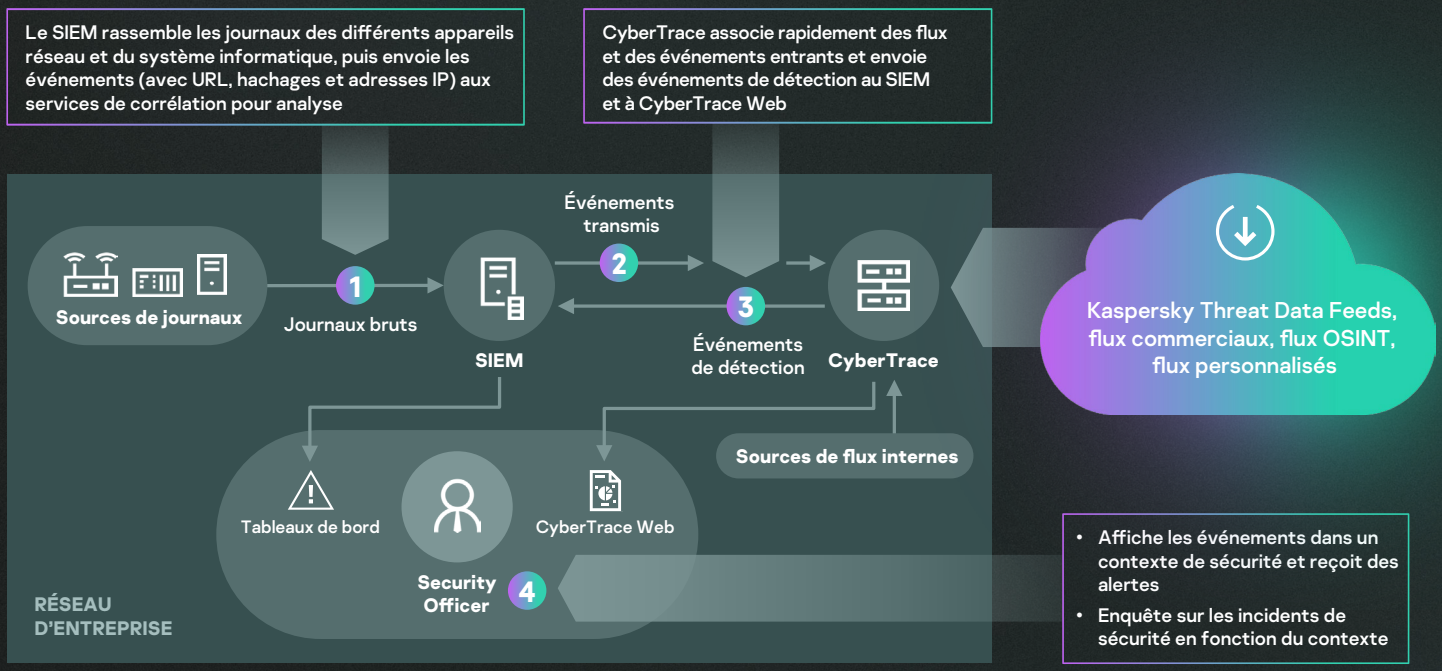
Un filtre envoie des événements de détection vers les solutions SIEM, réduisant ainsi la charge sur ces dernières et sur les analystes

HTTP RestAPI vous permet de gérer et de faire des recherches au sein de la Threat Intelligence

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

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.

Architecture



Kaspersky CyberTrace et Kaspersky Threat Data Feeds permettent à vos analystes de sécurité de :

Traiter et hiérarchiser efficacement d'énormes volumes d'alertes de sécurité

Améliorer et accélérer les procédures de tri et de réponse initiale

Élaborer une défense proactive basée sur la veille stratégique

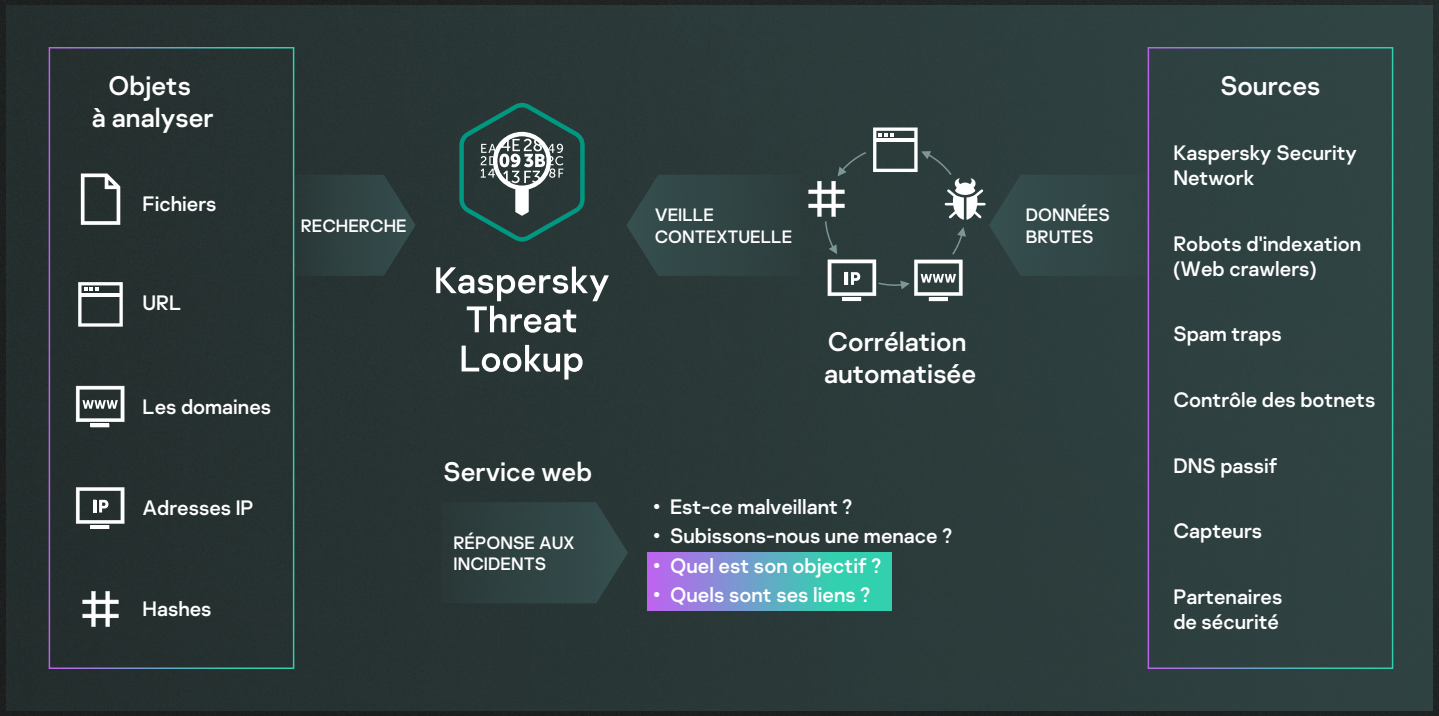
Identifier immédiatement les alertes critiques pour votre entreprise et prendre des décisions mieux informées sur les alertes à faire remonter aux équipes de réponse aux incidents

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.

Comment ça fonctionne ?



Bénéfices

Informations de confiance

un des principaux atouts de Kaspersky Threat Lookup est la fiabilité de nos données sur la surveillance des menaces, enrichies d'un contexte exploitable, ce qui peut donner lieu à des actions. Les produits de Kaspersky arrivent en tête dans les tests anti-malware 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

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 découvrez une menace, moins il y a de dommages potentiels et plus rapides sont les réparations ainsi que le retour à la normale des opérations de réseau.

Facile à utiliser

Interface Web ou API RESTful. 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 actionnable 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 liés à Kaspersky Threat Lookup

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

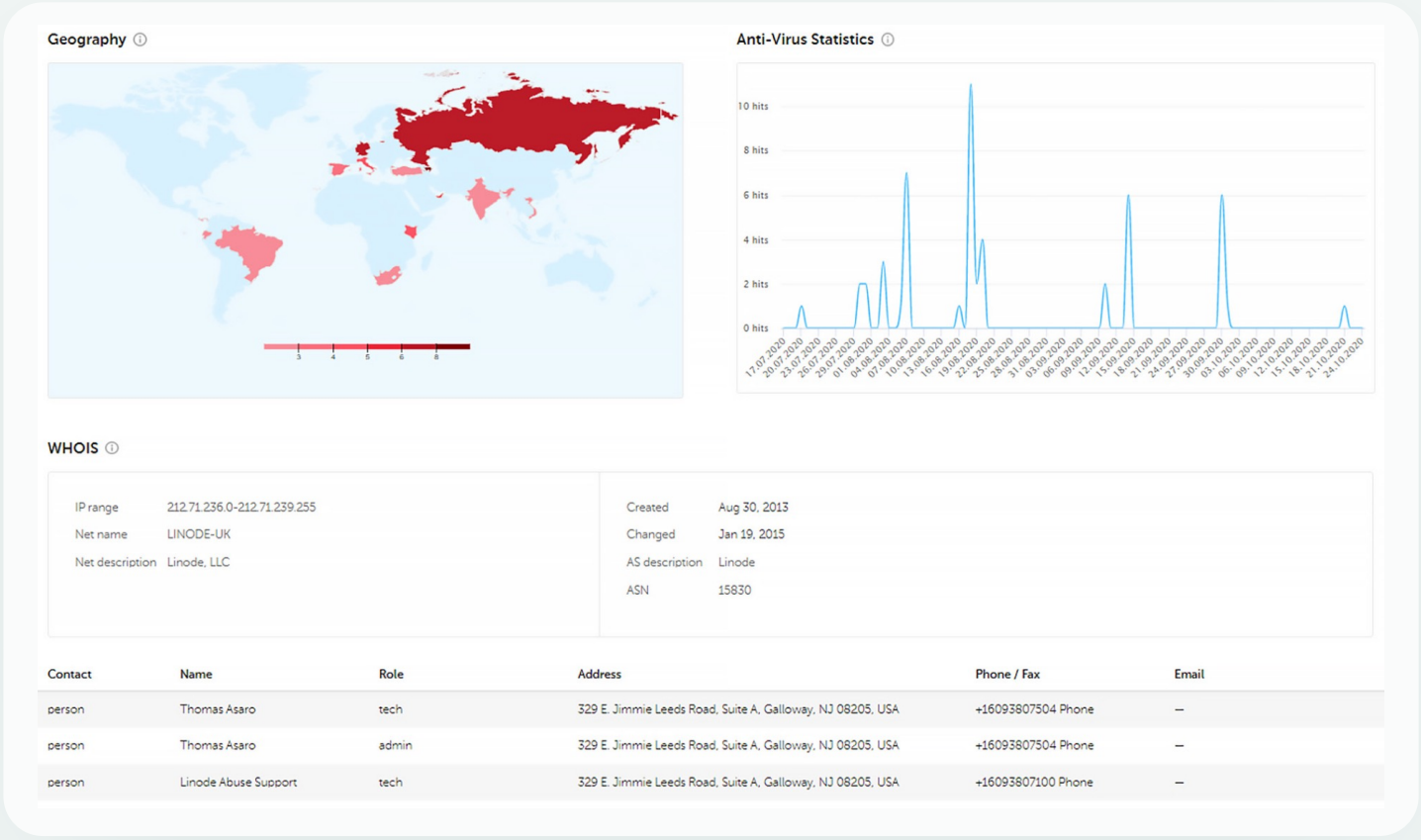
Diagnostiquer et analyser les incidents de sécurité sur les hébergeurs et le réseau plus efficacement, et hiérarchiser les signaux des systèmes internes contre des menaces inconnues

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

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 découvert est courant ou unique et comprendre pourquoi un objet doit être considéré comme malveillant

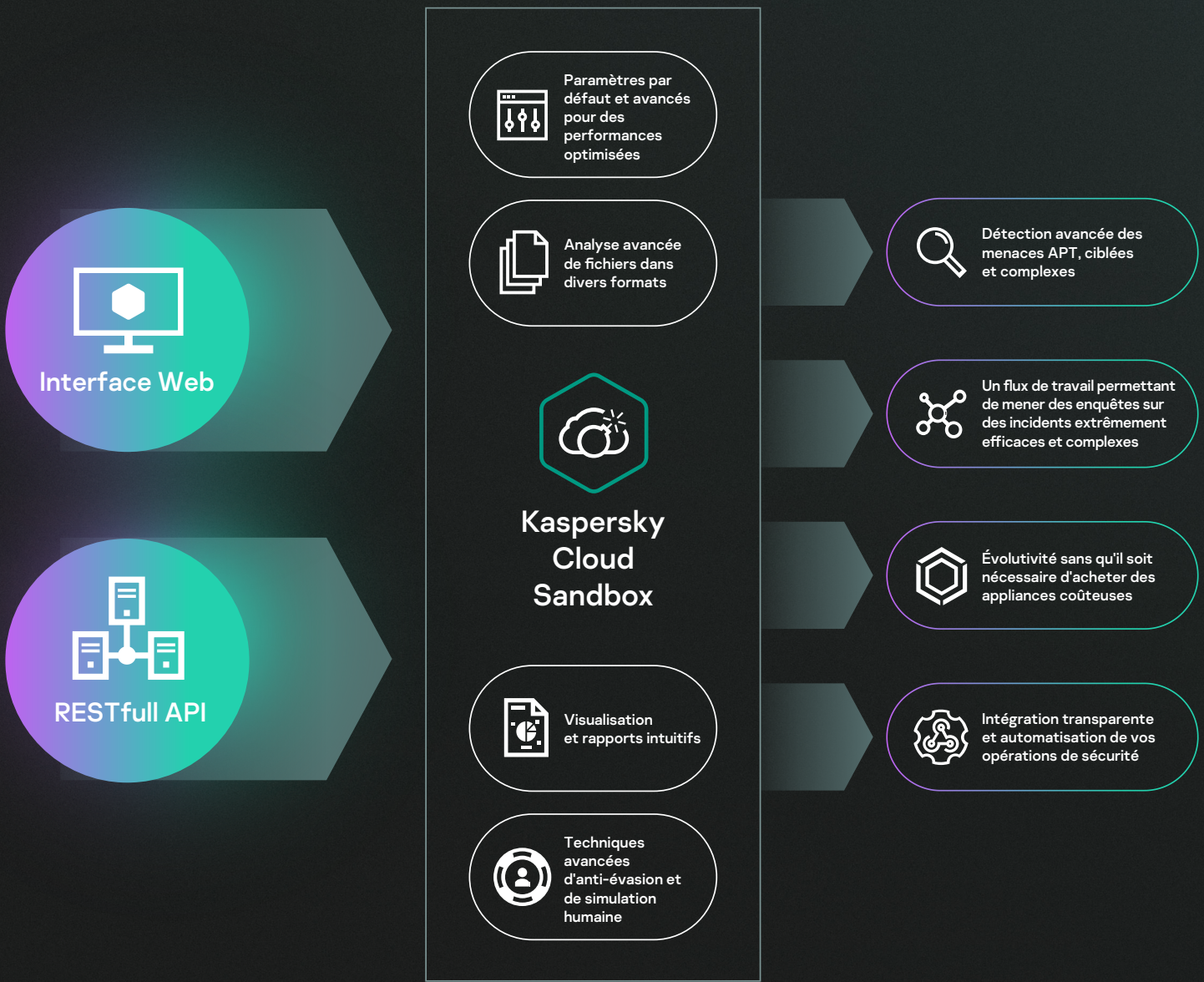


Kaspersky Research Sandbox

Il est impossible d'éviter les attaques ciblées uniquement avec les outils antivirus traditionnels. Les moteurs antivirus ne peuvent arrêter que les menaces connues et leurs variantes, tandis que les auteurs de menaces sophistiquées utilisent une grande variété de techniques pour échapper à la détection automatique. Les pertes dues à des incidents de sécurité informatique continuent de se multiplier, ce qui souligne l'importance des capacités de détection immédiate des menaces pour garantir une réponse rapide et la capacité de contrer les menaces avant qu'elles ne causent des dommages.

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.

Kaspersky Research Sandbox vous permet d'enquêter sur les origines des échantillons de fichiers, de collecter des IOC basés sur l'analyse comportementale et de détecter des objets malveillants qui n'ont jamais été vus auparavant. La solution offre une approche hybride combinant la Threat Intelligence recueillie 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.



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 Research Sandbox offre une approche hybride combinant la Threat Intelligence recueillie 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 service a été développé dans notre laboratoire sandbox interne, pendant plus d'une décennie. La technologie intègre toute notre connaissance des comportements malveillants gagnée pendant 25 ans de recherche continue sur les menaces. Cela nous permet de détecter plus de 400000 nouveaux objets malveillants chaque jour et d'offrir à nos clients des solutions novatrices en termes de sécurité.

La solution Sandbox de Kaspersky Research peut être gérée à partir d'une plateforme de gestion centralisée basée dans le cloud ainsi que depuis une console hors ligne dans les environnements isolés. Cet agent exploite la Threat Intelligence et intègre les analyses personnalisables.

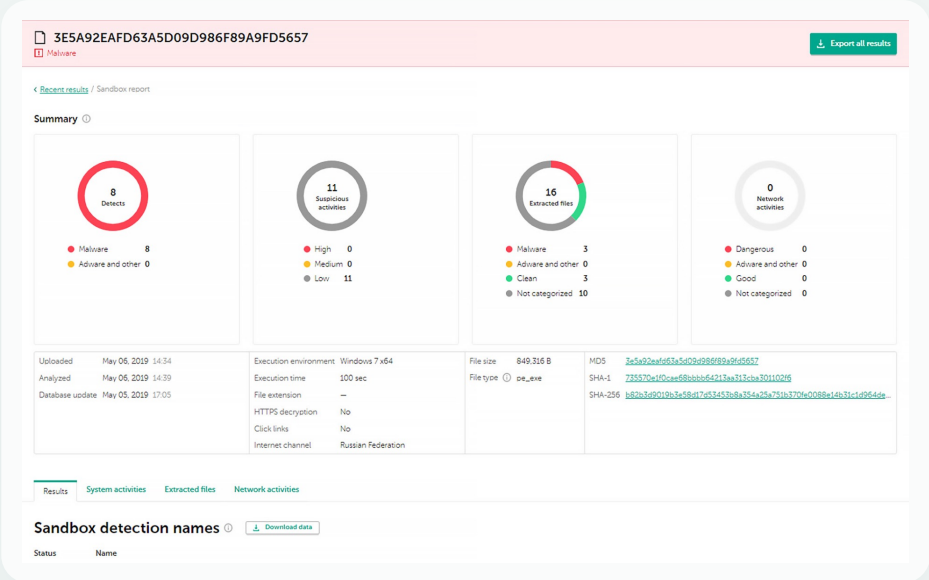
Dans le cadre de notre Threat intelligence Portal, Kaspersky Research Sandbox est le composant final dans votre flux de travail pour la Threat Intelligence. Tandis que le portail récupère les dernières informations détaillées de Threat Intelligence sur les URL, les domaines, les adresses IP, les hachages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

Rapport complet

- Score de menace unifié
- Activités suspectes du système avec descriptions détaillées
- Chargement et exécution des DLL
- Création, modification et suppression de fichiers
- Décharges de mémoire de processus et de trafic réseau (PCAP)
- Création d'extensions mutuelles (mutex)
- Modification et création des clés du registre
- Processus créés par le fichier exécuté
- Activités réseau (SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, sessions SOCKS ; HTTP(s), demandes et réponses)
- Informations détaillées de Threat Intelligence avec contexte exploitable pour chaque indicateur de compromission révélé (IoC)
- Carte d'exécution détaillée avec mise en évidence des techniques MITRE ATT&CK
- YARA détecte et déclenche des règles IDS (y compris des règles personnalisées)
- Téléchargement et analyse d'un fichier hébergé sur une certaine URL
- Clic sur des liens dans des documents pour Microsoft Office (Word, Excel, PowerPoint, Publisher et Outlook) et Adobe Reader
- Possibilité d'exporter les détails de l'analyse aux formats STIX, JSON, CSV
- Variété d'environnements, y compris les systèmes d'exploitation mobiles (Android) et les capacités de personnalisation de l'environnement
- Paramètres d'exécution des fichiers personnalisés
- Différents canaux Internet, possibilité d'acheminer le trafic via un canal VPN personnalisé
- API compatible REST
- Captures d'écran et bien plus encore

Avec Kaspersky Research Sandbox, 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 Research Sandbox stimule la réponse aux incidents et les activités de cyber-diagnostic, 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 Threat Attribution Engine

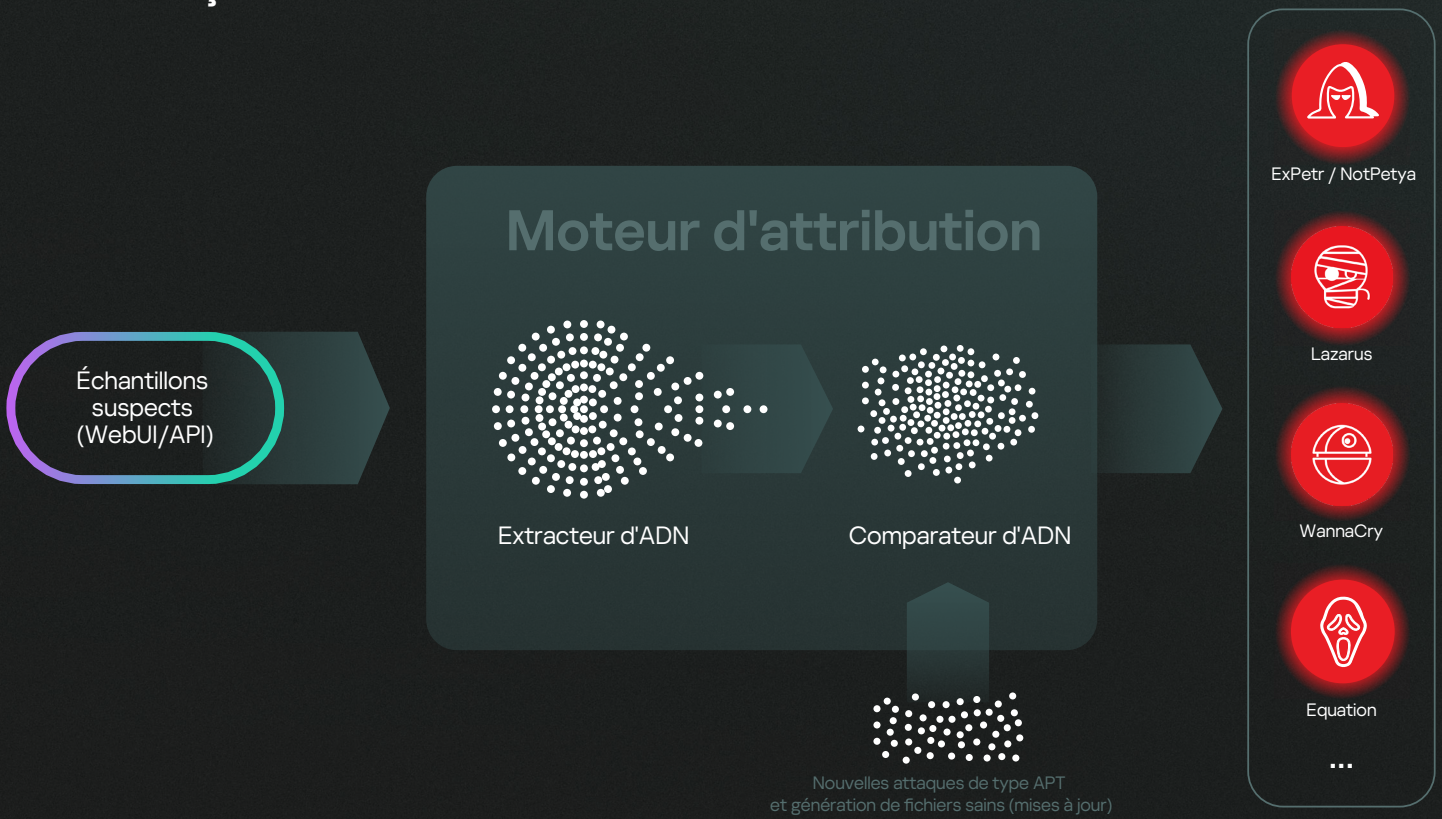
Ce n'est pas pour rien que l'attribution des menaces joue un rôle aussi important dans le domaine de la cybersécurité. Le délai moyen entre la détection et la réponse à des menaces hautement sophistiquées peut être frustrant et prolongé, en raison des processus complexes d'enquête et de rétro-ingénierie impliqués. Dans de nombreux cas, ce délai peut donner aux pirates informatiques suffisamment de temps pour atteindre leurs objectifs. Une attribution correcte et rapide permet non seulement de réduire le temps de réponse aux incidents de plusieurs heures à quelques minutes, mais aussi de réduire le nombre de faux positifs.

Identifier une attaque ciblée, établir le profil des attaquants et créer des facteurs d'attribution pour les différents acteurs de la menace est un travail long et complexe, qui peut prendre des années. Pour pouvoir créer une attribution fonctionnelle, il faut également accumuler une grande quantité de données au fil du temps et disposer d'une équipe de chercheurs hautement qualifiés possédant l'expérience nécessaire en matière d'enquêtes. Ces chercheurs suivront généralement l'activité de différents groupes, et alimenteront une base de données avec toutes les informations accumulées. Cette base de données devient alors une ressource précieuse pouvant être partagée sous forme d'outil.

Kaspersky Threat Attribution Engine intègre une base de données d'échantillons de programmes malveillants APT et de fichiers sains collectés par les experts Kaspersky au cours des 25 dernières années, et plus. Nous surveillons plus de 1 100 acteurs et campagnes de menaces et publions plus de 120 rapports de Threat Intelligence par an. Notre recherche en cours soutient une collection d'APT qui contient quelque 83 000 fichiers. Cela améliore la détection des faux drapeaux et, en conjonction avec l'utilisation d'outils automatisés, permet d'obtenir des niveaux d'attribution d'une précision exceptionnelle.

Le produit offre une approche unique pour comparer des échantillons similaires tout en garantissant un taux de faux positifs proche de zéro. Toute nouvelle attaque peut être rapidement associée à des programmes malveillants APT connus, à des attaques ciblées antérieures et à des groupes de pirates informatiques, ce qui vous permet de distinguer les menaces à haut risque des incidents moins graves. Vous pouvez ainsi prendre des mesures de protection appropriées pour empêcher un pirate de prendre pied dans votre système.

Comment ça fonctionne ?



Pour établir un lien entre les programmes malveillants et les entités d'attribution, Kaspersky Threat Attribution Engine utilise une méthode propriétaire unique de recherche de similitudes entre les fichiers. Cette méthode prévoit :

1

L'analyse de la génétique d'un échantillon grâce à l'extraction des éléments suivants de son code :

- Génotypes – des morceaux distincts de code binaire.
- Chaînes – des chaînes de caractères distinctes.

2

La recherche automatique dans les fichiers analysés des génotypes et des chaînes de caractères qui sont similaires aux génotypes et aux chaînes de caractères des échantillons d'APT précédemment analysés, ou déjà associés à des entités d'attribution.

3

En fonction des chaînes et des génotypes similaires trouvés dans les échantillons d'APT, la création d'un rapport sur l'origine de l'échantillon analysé, les entités d'attribution connexes ainsi que toute similitude entre cet échantillon et les échantillons d'APT connus.

Le produit peut être déployé dans un environnement sécurisé, à l'abri des regards indiscrets, empêchant toute tierce partie d'accéder aux informations traitées et aux objets soumis. Une API connecte le moteur à d'autres outils et frameworks afin de mettre en œuvre l'attribution dans l'infrastructure existante et les processus automatisés.

Caractéristiques principales du produit

- Fournit un accès instantané à une base de données structurée concernant des milliers d'acteurs APT, d'échantillons et de menaces plus larges (via le moteur anti-virus).
- Permet une hiérarchisation automatique ou manuelle efficace des menaces et un triage des alertes.
- Permet d'ajouter des acteurs et des échantillons privés pour un produit évolutif qui apprendra à détecter les échantillons qui sont similaires aux fichiers de votre collection privée.
- Permet le téléchargement manuel d'échantillons et offre une fonctionnalité API REST améliorée pour l'intégration avec des flux de travail automatisés.
- Prend en charge les déploiements sur Amazon Web Services (AWS), ce qui permet une configuration rapide du produit ainsi qu'une réduction des coûts puisqu'il n'est pas nécessaire d'investir dans du matériel au départ.
- Exportation facile vers des règles YARA pour une recherche/analyse automatisée plus poussée de fichiers similaires ou intégration avec des solutions tierces.
- Exportation facile au format STIX 2.1 (les formats TXT et JSON sont également pris en charge) pour une analyse automatisée plus poussée des journaux de sécurité ou une intégration avec des solutions/contrôles de sécurité tiers.
- Permet de déballer des archives protégées par un mot de passe personnalisé.
- Permet d'accéder rapidement à la documentation et au Contrat de licence utilisateur final (EULA) dans l'interface Web.
- Envoie les attributs dans des fichiers parallèles pour analyse en une seule demande.

Avantages liés à Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine calcule le score de réputation

de l'échantillon et révèle sa génétique et l'attribution du code. Ces informations donnent un aperçu de l'origine de l'échantillon et peuvent permettre de l'attribuer à des auteurs potentiels.

Votre équipe de sécurité peut ajouter ses propres entités d'attribution

et échantillons à la base de données de Kaspersky Threat Attribution Engine. L'équipe peut ensuite instruire l'application pour attribuer les échantillons envoyés à ces entités et échantillons d'attribution privés.

Le processus d'attribution ne prend que quelques secondes

Grâce à Kaspersky Threat Attribution Engine, le processus d'attribution ne prend que quelques secondes, alors que ce processus prenait des mois et des années par le passé.

Kaspersky Threat Attribution Engine étend et renforce

le portefeuille de Kaspersky pour les centres d'opérations de sécurité (SOC) commerciaux et les agences nationales de cybersécurité en les aidant à mettre en place un processus efficace de gestion des incidents.

Kaspersky APT Intelligence Reporting

Les clients de Kaspersky APT Intelligence Reporting 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.

Plus de 300

acteurs de menaces

Plus de 160

rapports privés par an

Plus de 12 000

IoC

Plus de 400

de cyber-espionnage

Plus de 700

Règles Yara

Kaspersky APT Intelligence Reporting fournit

Profils de criminels

Application du cadre MITRE ATT&CK

Résumé analytique

Informations pour les cadres supérieurs

Analyse technique approfondie

- Méthodes d'attaque
- Vulnérabilités utilisées
- Description(s) des programmes malveillants
- Descriptions de l'infrastructure C&C et du protocole
- Analyse des victimes
- Analyse de l'exfiltration de données
- Attributions

Conclusion et recommandations

Indicateurs de compromission (IoC) et règles YARA

Avantages liés à Kaspersky APT Intelligence Reporting

Information sur les APT privées

Pour différentes raisons, toutes les menaces les plus graves ne sont pas révélées publiquement, mais nous les partageons avec vous

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

Renseignements sur les profils des acteurs des menaces

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

Intégration et automatisation fluides

Intégration transparente et automatisation de vos flux de travail avec l'API RESTful

Une surveillance continue des campagnes d'APT

Accédez aux informations exploitables au cours des enquêtes grâce à des informations sur la distribution des menaces APT, les indicateurs IoC, les infrastructures de commande et de contrôle, etc.

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

Kaspersky Crimeware Intelligence Reporting

La cybercriminalité motivée par des raisons financières ne se limite pas à des secteurs particuliers. Les attaques contre les infrastructures financières, comme les distributeurs automatiques de billets et les appareils de point de vente se poursuivent, toutes les entreprises, quel que soit leur secteur, sont menacées par les ransomwares. Au cours des dernières années, les frontières entre les différents types de menaces et les différents types de cybercriminels se sont estompées. Mentionnons notamment l'émergence des campagnes de menaces ciblées avancées (APT), qui se concentrent non pas sur le cyber-espionnage, mais sur le vol d'argent pour financer les autres activités du groupe APT. Il ne faut pas sous-estimer la complexité croissante des menaces liées aux crimewares.

Kaspersky Crimeware Intelligence Reporting renforce vos stratégies défensives grâce à des informations pertinentes sur les campagnes de programmes malveillants et les attaques visant les institutions financières, ainsi que des informations sur les outils de crimewares utilisés pour attaquer les banques, les entreprises de traitement des paiements et les infrastructures qui leur sont propres.

Kaspersky Crimeware Intelligence Reporting fournit

- Des descriptions détaillées de programmes malveillants populaires, répandus et très médiatisés
- Des notes de chercheurs et des avertissements précoces, y compris des informations sur les menaces récentes liées aux programmes malveillants
- Des informations sur les campagnes dangereuses et répandues de programmes malveillants
- Des descriptions détaillées des menaces visant les infrastructures financières et des outils de pirate informatique correspondants développés ou vendus par les cybercriminels sur le Dark Web dans différentes régions du monde

Avantages liés à Kaspersky Crimeware Intelligence Reporting

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

Intégration et automatisation fluides

Intégration transparente et automatisation de vos flux de travail avec l'API RESTful

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

Renseignements sur les profils des auteurs de crimewares

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

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 le portail Kaspersky Threat Intelligence Portal, ce qui signifie que vous pouvez commencer à exploiter le service immédiatement.

Toutes les recherches de Threat Intelligence liées aux ICS sont menées par une équipe dédiée, Kaspersky ICS CERT :

- Société fondée en 1988
- La première équipe CERT créée par une organisation commerciale
- Près de 20 experts hautement qualifiés en recherche de menaces et de vulnérabilités, en réponse aux incidents et en analyse de sécurité pour les ICS

Rapports inclus dans votre abonnement

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.

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.

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.

Évolution de l'univers des menaces

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.

Les données de Threat Intelligence vous permettent de

Détecter et anticiper

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.

Évaluation des vulnérabilités

Évaluation des 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

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.

Exploiter les informations

Exploiter 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 aux infrastructures industrielles 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 du personnel 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 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 d'être en mesure de suivre ses changements et de réagir aux menaces externes visant les ressources numériques divulguées.

Les entreprises utilisent un vaste éventail d'outils de sécurité dans leurs opérations de sécurité, mais restent exposées à des menaces numériques qui se profilent et qui nécessitent des capacités très particulières pour détecter et atténuer les fuites de données, ainsi que surveiller les plans et les schémas d'attaque des cybercriminels présents sur les forums du Dark Web, etc. Pour aider vos analystes de la sécurité à voir les ressources de votre entreprise auxquelles les criminels ont accès, à découvrir rapidement les vecteurs d'attaque potentiels à leur disposition et à ajuster vos moyens de défense en conséquence, Kaspersky a créé Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence fournit

Reconnaissance du réseau

Identification des ressources du réseau du client et des services exposés qui constituent un point d'entrée potentiel pour une attaque. 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).

Protection de la marque

Contrôle et blocage de l'utilisation non autorisée de la marque d'une entreprise en ligne. Identification de faux comptes et d'applications de réseaux sociaux, de sites Internet de phishing et d'autres activités frauduleuses susceptibles de nuire à la réputation d'une entreprise et/ou de tromper les clients. Démantèlement de faux comptes de réseaux sociaux et de fausses applications sur les places de marché mobiles.

Surveillance du Dark Web

Surveillance continue des ressources du Dark Web (forums, blogs de ransomwares, messageries, sites Tor, etc.) permettant de détecter toute mention et menace relative à votre entreprise, à vos clients et à vos partenaires. Analyse des attaques ciblées actives ou planifiées, des campagnes APT ciblant votre entreprise, votre secteur d'activité et la zone des opérations.

Découverte de fuites de données

Détection des identifiants compromis d'employés, de partenaires et de clients, mais également des cartes bancaires, des numéros de téléphone et d'autres informations confidentielles qui peuvent être utilisées pour mener une attaque ou présenter des risques pour la réputation de votre entreprise.

Sources de renseignements

Il est essentiel que vous compreniez clairement la situation de votre entreprise sur le plan de la sécurité externe. Pour fournir ces informations, les analystes en sécurité de Kaspersky collectent et agrègent des informations provenant des sources de renseignements suivantes :

Vos données non structurées

- Adresses IP
- Domaines de sociétés
- Noms de marques
- Mots clés

Inventaire externe du périmètre réseau

Web surfacique, deep Web et dark Web

Base de connaissances Kaspersky

Rapports analytiques

Alertes de menace

10 demandes par an

Recherche en temps réel dans les données de Kaspersky, dans des renseignements Open Source ainsi que dans des sources du Web de surface et du Dark Web

Comment ça fonctionne ?

Configurer	Collecte	Filtre	Réagir
Recherche d'informations sur les ressources numériques de l'entreprise	Collecte automatisée de données à partir des sites Web de surface, profonds et sombres, et de la base de données de renseignements sur les menaces de Kaspersky	Détection, analyse et hiérarchisation des menaces gérées par des analystes	Remise des renseignements complétés

Valeurs commerciales

Kaspersky Digital Footprint Intelligence offre des avantages solides et une valeur considérable à votre organisation :

Protégez votre marque

Détectez les menaces en temps réel pour protéger la réputation de votre marque, préserver la confiance de vos clients, réduire les risques de pertes financières et les dommages causés aux activités de l'entreprise.

Réduisez les cyberrisques

Fournissez aux principales parties prenantes (directeur de l'expérience client et conseil d'administration) des informations sur l'orientation des dépenses en matière de cybersécurité en mettant en évidence les lacunes des structures actuelles et les risques qu'elles comportent.

Réagissez plus rapidement

Un contexte supplémentaire pour les alertes de sécurité améliore la réponse aux incidents et réduit le temps moyen de réponse (MTTR)

Réduisez la surface d'attaque

Gérez la présence numérique de votre entreprise et contrôlez les ressources réseau externes afin de minimiser les vecteurs d'attaque et les vulnérabilités susceptibles d'être utilisées dans le cadre d'une attaque.

Identifiez vos adversaires

Mieux vaut prévenir que guérir – les cybercriminels planifient et débattent au sujet de votre entreprise sur le Dark Web, donc il vaut mieux être préparé.

Apprenez à reconnaître l'inconnu

Améliorez votre capacité à résister aux cyberattaques et à reconnaître les menaces qui ne relèvent pas des compétences de vos équipes de sécurité internes.

Kaspersky Takedown Service

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.

Le service Kaspersky Takedown Service 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 fait gagner un temps précieux aux clients et leur fait réaliser des économies. Le service est disponible à l'échelle internationale.

Kaspersky bloque plus de 15 000 URL de phishing/scam et empêche plus d'un million de tentatives de cliquer sur de telles 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.

Visibilité complète

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

Gestion intégrale

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

Protection mondiale

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

Intégration avec Kaspersky Digital Footprint Intelligence

Kaspersky Takedown Service peut être acheté séparément, mais son intégration à Kaspersky Digital Footprint Intelligence permet de tirer le meilleur parti de la synergie naturelle entre ces services. Kaspersky Digital Footprint Intelligence fournit des notifications en temps réel à propos des domaines de phishing et de programmes malveillants qui peuvent être immédiatement envoyés à Kaspersky Takedown Service en vue d'un blocage ultérieur.

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 Kaspersky Takedown Service 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.

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.

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.

La 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.

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 Intelligence de Kaspersky à vos besoins particuliers, vous permettant ainsi de mettre en place des défenses résilientes contre les menaces visant votre organisation.

Livrables du service Kaspersky Ask the Analyst (abonnement unifié sur demande)

APT et crimeware

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

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)

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

Renseignements sur le Dark Web

- 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

Analyse des programmes malveillants

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

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 votre demande acceptée, vous serez informé du délai estimé pour sa prise en charge.

Cas d'utilisation

1. Clarifier tout détail dans les rapports de Threat Intelligence publiés précédemment
2. Obtenir des renseignements supplémentaires pour les IoC déjà fournis
3. Obtenir des détails sur les vulnérabilités et des recommandations sur la manière de se protéger contre leur exploitation
4. Recevoir des détails supplémentaires sur les activités particulières du Dark Web qui vous intéressent
5. 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
6. 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
7. Demander de l'aide pour déterminer si l'activité inhabituelle détectée est liée à une APT ou à un acteur de crimeware
8. Envoyer des fichiers de logiciels malveillants pour une analyse complète afin de comprendre le comportement et la fonctionnalité du ou des échantillons fournis

Avantages liés à Kaspersky Ask the Analyst

Développement 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.

Élargissez vos connaissances et 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 d'étendre vos capacités existantes grâce à nos connaissances et ressources uniques.

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 cette Threat Intelligenece et l'identification des contre-mesures les plus efficaces exigent 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, nous travaillons dur pour aider nos clients en leur proposant des renseignements 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.

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

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 permet de concentrer votre stratégie de défense sur des domaines identifiés comme cibles de choix des cyberattaques

Évite aux analystes de subir un burn-out et aide vos effectifs à se concentrer sur de véritables menaces

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

Kaspersky Threat Intelligence

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture