Plateforme de
Threat Intelligence

Kaspersky CyberTrace

kaspersky bring on the future

Kaspersky CyberTrace

Une plateforme 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.

Trier et analyser efficacement les alertes

Le nombre d'alertes traitées par les analystes en cybersécurité augmente de façon exponentielle. Face à un tel volume de données, il est presque impossible de hiérarchiser, de trier et de valider efficacement les alertes.

Les alertes provenant des produits de sécurité se multiplient,au risque de voir les véritables menaces passer au travers des mailles du filet, sans même parler du risque d'épuisement des analystes. Les SIEM et les autres outils d'analyse de la sécurité permettent de corréler les événements et de réduire le nombre d'alertes, mais les analystes de la sécurité restent extrêmement surchargés.

Systèmes SIEM

En intégrant aux contrôles de sécurité existants (p. ex., systèmes SIEM) des données de Threat Intelligence mises à jour minute par minute et interprétables par une machine, les professionnels de la sécurité peuvent automatiser le processus de tri initial tout en obtenant 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.

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.

Intégration

Kaspersky CyberTrace peut être intégré à n'importe quel flux de données de Threat Intelligence aux formats JSON, STIX, XML et CSV :

1. Flux d'informations de Kaspersky Threat Intelligence
2. Flux d'informations d'autres fournisseurs
3. OSINT ou vos flux personnalisés

Pour simplifier la tâche des clients, CyberTrace propose une intégration prête à l'emploi avec la plupart des solutions SIEM et des sources de journaux.

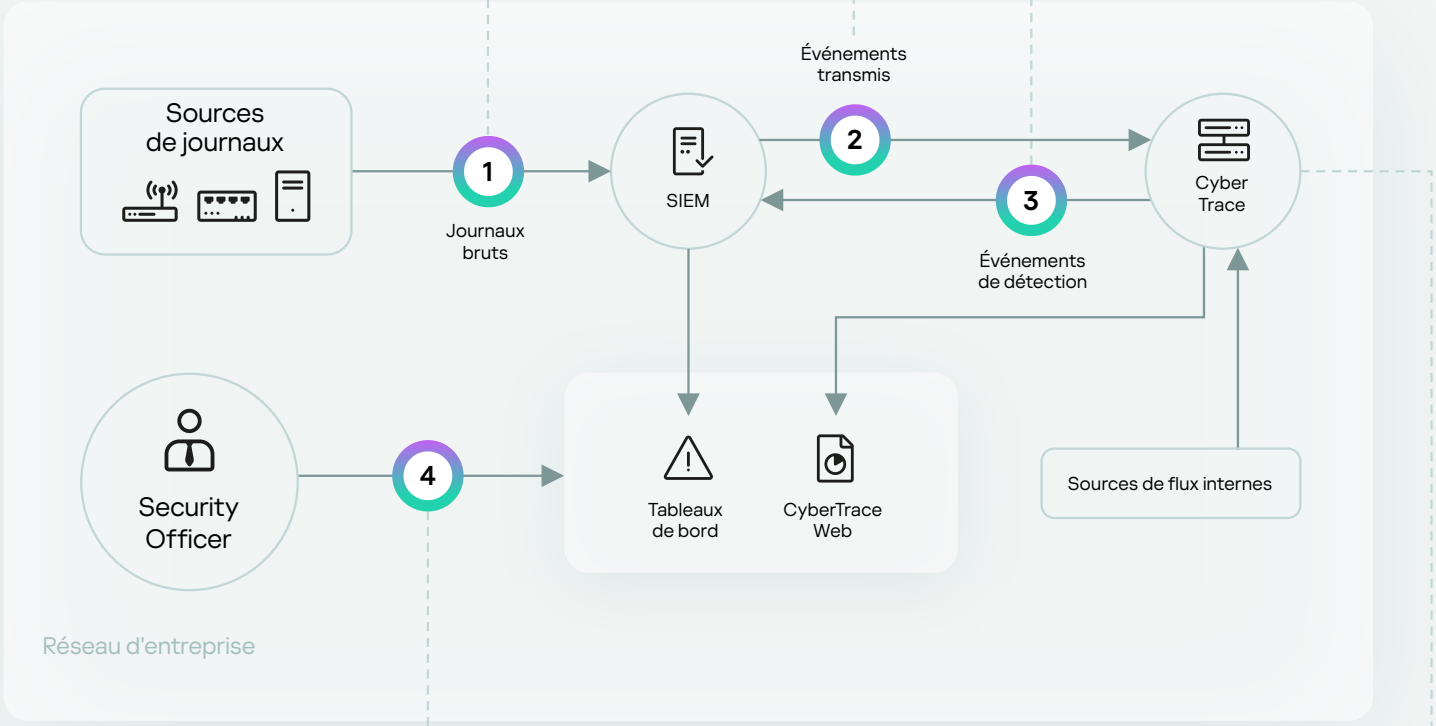
Plan d'intégration de Kaspersky CyberTrace

Kaspersky CyberTrace est capable d'améliorer la capacité du SIEM avec une couche supplémentaire d'analyse et de correspondance des données entrantes, réduisant ainsi de manière significative la charge de travail du SIEM. La mise en correspondance des événements avec les informations issues des flux d'informations permet d'identifier les menaces et de fournir un contexte précieux aux incidents détectés. L'illustration ci-dessous montre une architecture d'intégration de la solution de haut niveau.

Le SIEM regroupe les journaux d'événements provenant de différents appareils de réseau et systèmes informatiques

Les journaux contenant les URL, les hachages et les IP sont envoyés à CyberTrace pour une analyse supplémentaire

CyberTrace associe rapidement des flux et des événements entrants et envoie des événements de détection au SIEM et à CyberTrace Web



- Affiche les événements dans un contexte de sécurité et reçoit des alertes
- Enquête sur les incidents de sécurité en fonction du contexte

Kaspersky Threat Data Feeds, flux commerciaux, flux OSINT, flux personnalisés

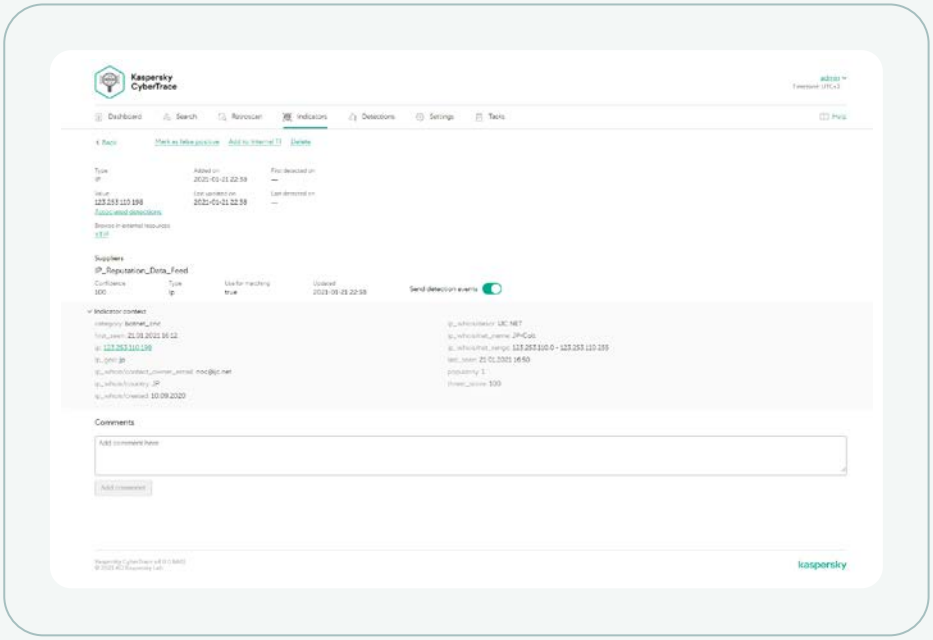
Caractéristiques produit

Kaspersky CyberTrace offre un ensemble d'instruments pour rendre les données de Threat Intelligence opérationnelles, procéder à un tri efficace et apporter une réponse initiale :

Informations détaillées d'un indicateur provenant de tous les fournisseurs de Threat Intelligence

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. Le filtrage des résultats selon le fournisseur de service de veille simplifie le processus d'analyse de la Threat Intelligence.

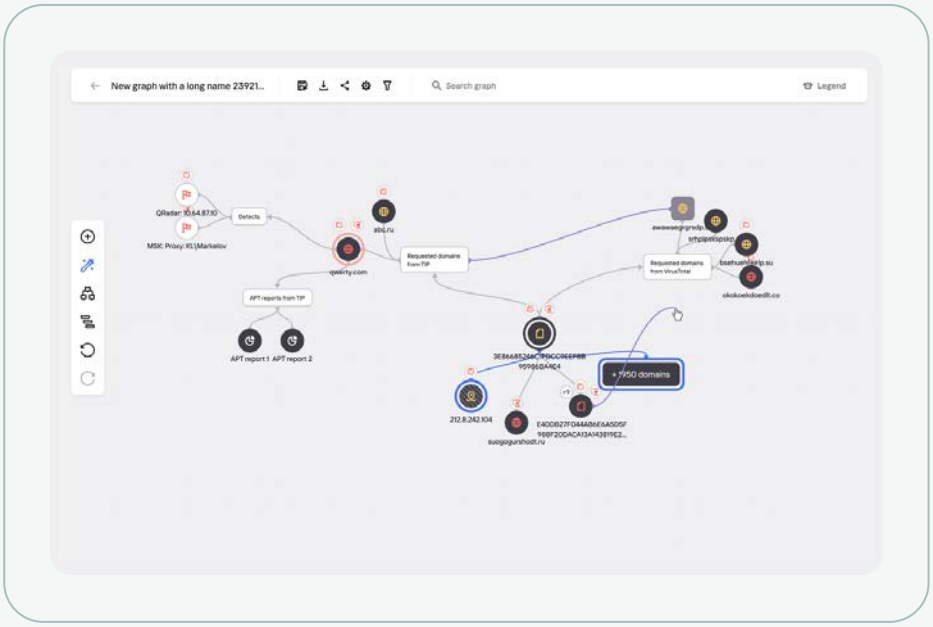
Les abonnements par email et les documents PDF des équipes d'intervention en cas d'urgence informatique (CERT) nationales/gouvernementales/financières, des fournisseurs de TI et des communautés pourraient être utilisés comme source d'IoC pour CyberTrace. L'extraction des IOC est possible à partir du corps de l'email et de la pièce jointe (XML, CSV, JSON, PDF). Les serveurs IMAP/POP3 et les dossiers locaux/partagés contenant une collection de fichiers PDF pourraient être utilisés comme source de flux.



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. Si l'indicateur a été détecté, les informations portant sur la date de la détection et les liens menant à la liste de détection seront disponibles.

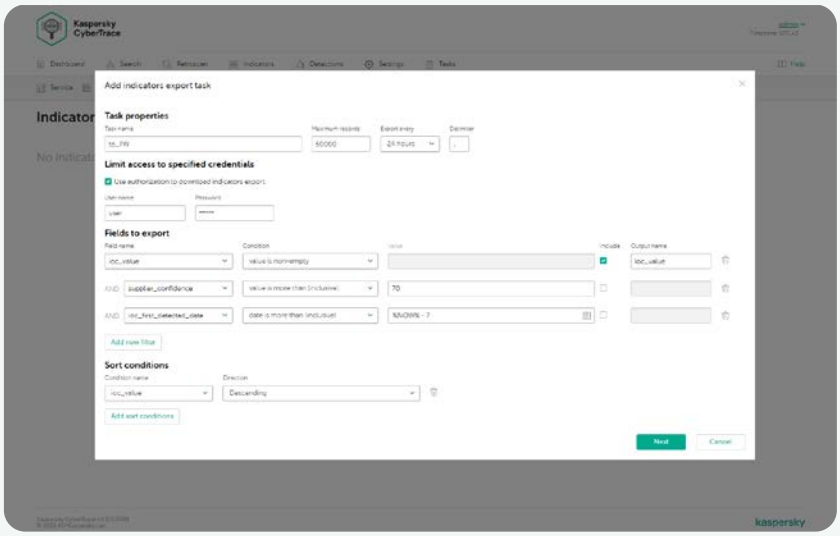
Graphique de recherche

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. Il permet la visualisation graphique de la relation entre les URL, les domaines, les adresses IP, les fichiers et autres contextes rencontrés lors de recherches. Le graphique inclut les caractéristiques suivantes : transformations, mini graphique, le regroupement de nœuds, ajout manuel de liens, ajout d'indicateurs et la recherche de nœuds sur le graphique. Il est possible d'enrichir les IoC sur le graphique de recherche à partir de VirusTotal.



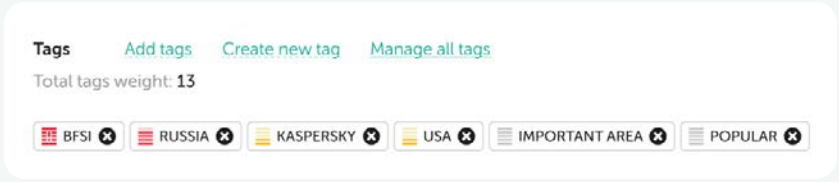
Tâche d'exportation des indicateurs

La fonctionnalité d'exportation des indicateurs prend en charge l'intégration native des IoC exportés avec des 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 de TI.



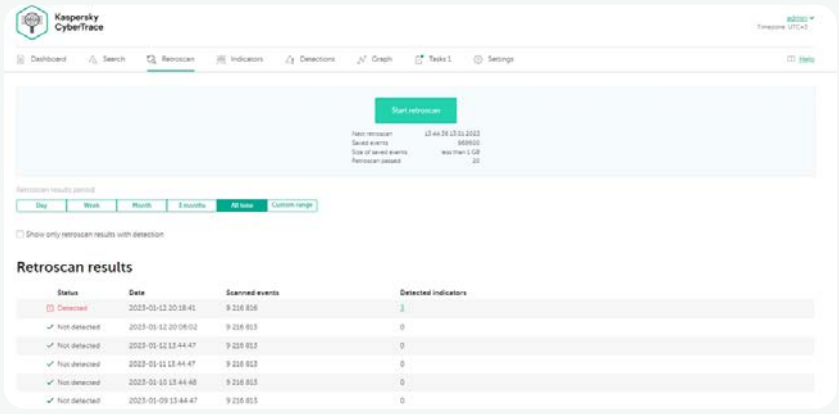
Étiquettes IoC (tags)

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.



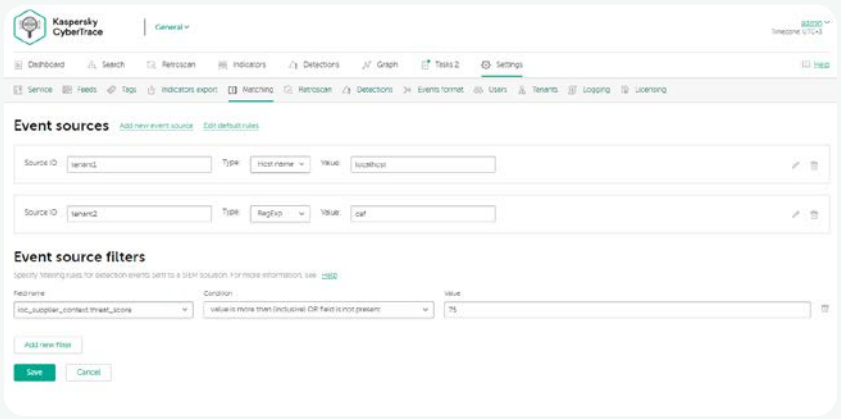
Fonctionnalité d'analyse rétrospective

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. Toutes les détections historiques sont incluses dans le rapport pour les futures investigations.



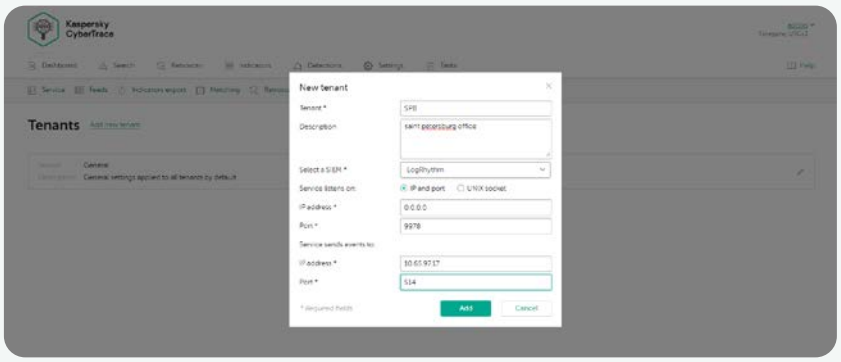
Filtres de sources d'événements

Un filtre permettant d'envoyer des événements de détection vers les solutions SIEM réduit la charge sur ces dernières ainsi que sur les analystes aux prises avec la fatigue à l'égard des alertes. Ce filtre vous permet d'envoyer aux solutions SIEM uniquement les détections des dangers les plus importants et devant être traités comme des incidents. Toutes les autres détections sont sauvegardées dans la base de données interne et peuvent être utilisées lors d'une analyse des causes profondes ou de threat hunting.



Prise en charge de la multilocation

La fonctionnalité multi-clients prend en charge les MSSP ou les cas d'utilisation de grandes entreprises lorsqu'un fournisseur de service (bureau central) a besoin de gérer des événements dans plusieurs succursales (locataires) séparément. Cela permet à une seule instance Kaspersky CyberTrace d'être connectée avec plusieurs solutions SIEM de différents locataires. Vous pouvez également configurer quels flux doivent être utilisés pour chaque locataire.



Statistiques d'indicateurs et matrice d'intersection des flux

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

En utilisant l'API Rest, Kaspersky CyberTrace peut être facilement intégré dans des environnements complexes pour l'automatisation et l'orchestration. Intégration à la plateforme de surveillance, d'analyse et de réponse aux incidents de Kaspersky.

Autres caractéristiques du produit

- Connecteurs SIEM pour une large gamme de solutions SIEM afin de visualiser et de gérer les données de détection des menaces
- Recherche à la demande des indicateurs (hachages, adresses IP, domaines, URL) pour une investigation en profondeur
- Filtrage avancé des flux
- Analyse groupée des journaux et des fichiers
- Interface à ligne de commande pour les plateformes Windows et Linux
- Mode autonome, dans lequel Kaspersky CyberTrace reçoit et analyse les journaux provenant de diverses sources, telles que les appareils réseau
- Etc.

Vous pouvez utiliser Kaspersky CyberTrace et Kaspersky Threat Data Feeds séparément, mais lorsqu'ils sont utilisés ensemble, ils renforcent considérablement vos capacités de détection des menaces et confèrent à vos opérations de sécurité une visibilité globale sur les cybermenaces.

Avec Kaspersky CyberTrace et Kaspersky Threat Data Feeds, les organisations peuvent :

Traiter et hiérarchiser efficacement les alertes de sécurité.

Réduire la charge de travail des analystes et éviter l'épuisement professionnel.

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 CyberTrace

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture