kaspersky BRING ON THE FUTURE

Kaspersky CyberTrace

Le nombre d'alertes de sécurité traitées par les analystes en sécurité augmente chaque jour de manière 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. Malgré les SIEM, les outils de gestion des journaux et d'analyse de sécurité et la mise en corrélation des alarmes associées, qui permettent de réduire le nombre d'alertes à examiner, les analystes sont surchargés.

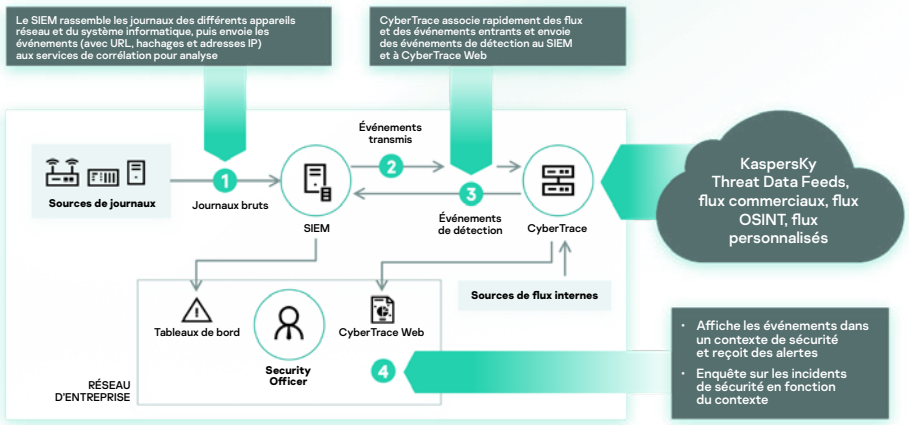
Les données de Threat Intelligence, fournies dans différents formats et comprenant une quantité phénoménale d'indicateurs de compromission, sont particulièrement indigestes pour les SIEM ou les contrôles de sécurité du réseau.

Trier et analyser efficacement les alertes

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 SOC peuvent automatiser le processus de tri initial tout en fournissant aux 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. Il s'intègre à tous les flux de Threat Intelligence que vous pourriez utiliser (flux de Kaspersky ou d'autres fournisseurs, flux OSINT, flux personnalisés, aux formats JSON, STIX, XML ou CSV) et propose donc une intégration prête à l'emploi avec la plupart des solutions SIEM et des sources de journaux.

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 :

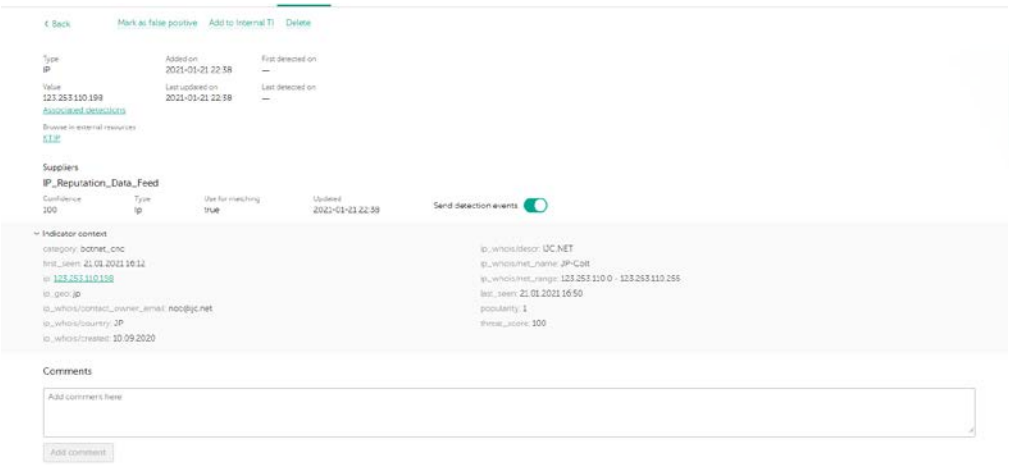


Graphique 1. Plan d'intégration de Kaspersky CyberTrace

Caractéristiques produit

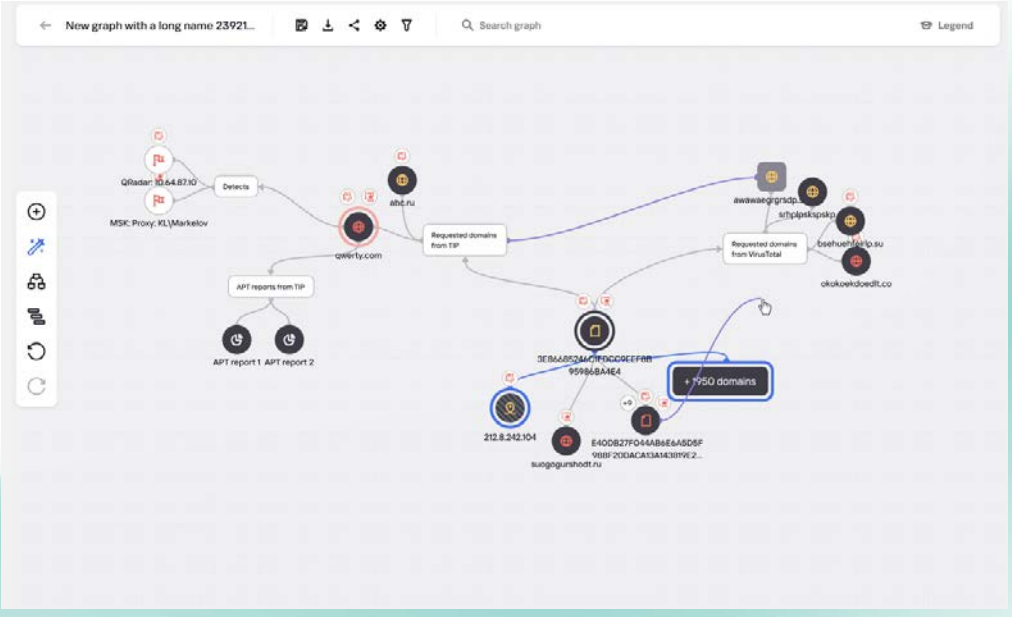
Kaspersky CyberTrace offre un ensemble d'instruments pour rendre les données de Threat Intelligence opérationnelles, procéder à un tri efficace et apporter une réponse initiale :

- 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 simplifie le processus d'analyse 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 Threat Intelligence 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.



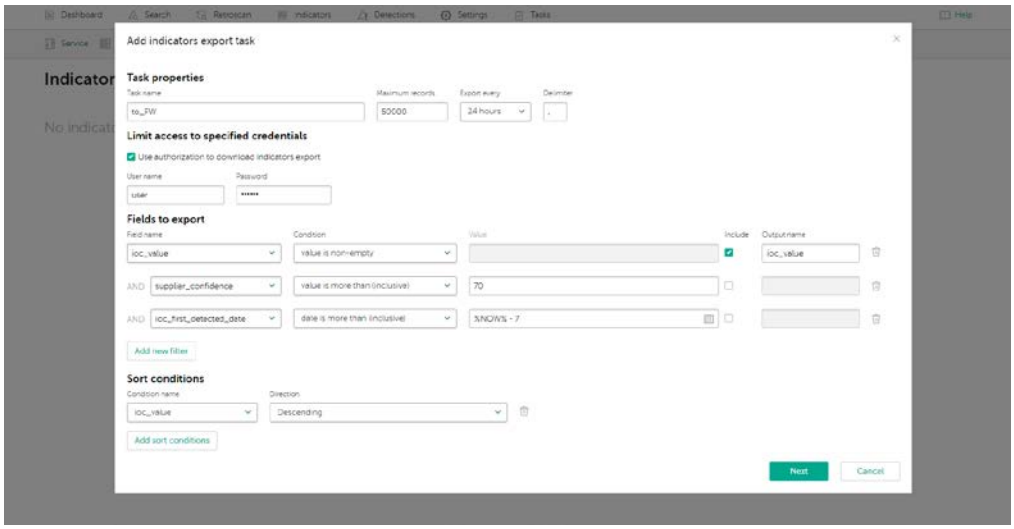
Graphique 2. Informations détaillées d'un indicateur provenant de tous les fournisseurs de Threat Intelligence

- 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.



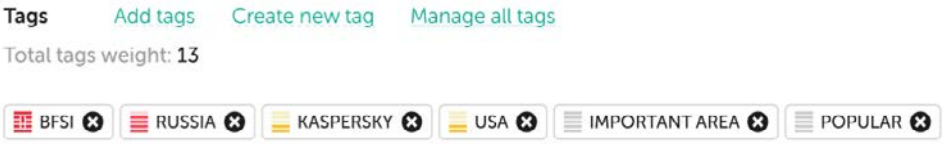
Graphique 3. Graphique de recherche

- 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.



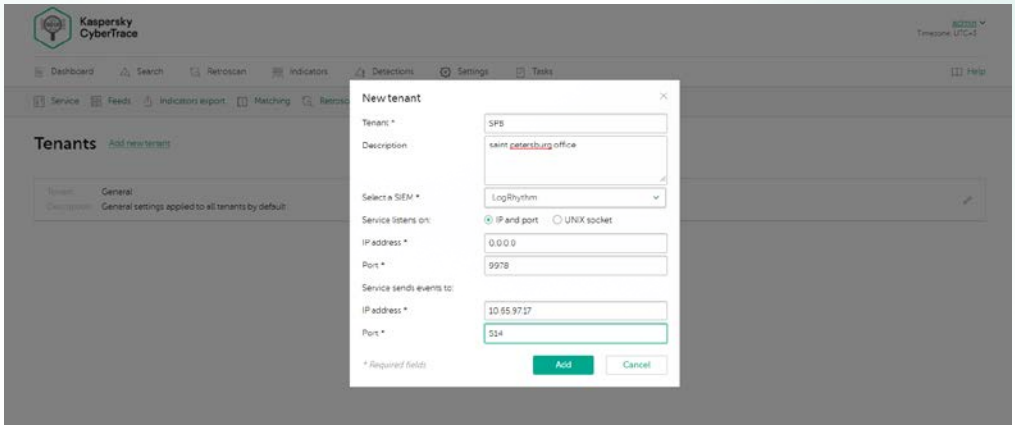
Graphique 4. Tâche d'exportation des indicateurs

- 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.



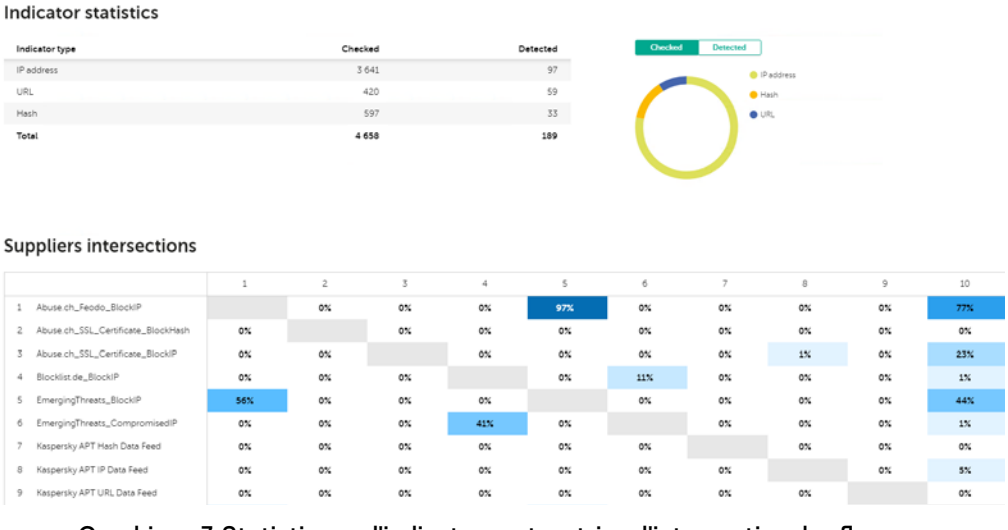
Graphique 5 : Étiquettes IOC

- 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.
- 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.
- 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 évènements 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.



Graphique 6. Création d'un nouveau locataire

- 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.



Graphique 7. Statistiques d'indicateurs et matrice d'intersection des flux

- HTTP RestAPI vous aide à gérer et à faire des recherches au sein de la Threat Intelligence. En utilisant l'API REST, la solution Kaspersky CyberTrace peut être facilement intégrée à des environnements complexes pour favoriser l'automatisation et l'orchestration.
- L'intégration avec Kaspersky Unified Monitoring and Analysis Platform (KUMA) est prise en charge, y compris l'intégration de l'interface utilisateur Web (interface utilisateur unique).

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,

- 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.

Autres caractéristiques 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.

Actualités sur les cybermenaces : www.securelist.fr
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security
Portail de Threat Intelligence : opentip.kaspersky.com

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr où la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/transparency

Proven.
Transparent.
Independent.