Kaspersky® CyberTrace

Le nombre d'alertes de sécurité traitées par les analystes de niveau 1 du centre de 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 spécialistes de niveau 1 sont surchargés.

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 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. Il s'intègre à tous les flux de Threat Intelligence que vous pourriez utiliser (flux de Kaspersky Lab 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. En comparant automatiquement les journaux aux flux de Threat Intelligence, Kaspersky CyberTrace fournit une « connaissance situationnelle » en temps réel et permet aux analystes de niveau 1 de prendre des décisions plus rapides et mieux informées.

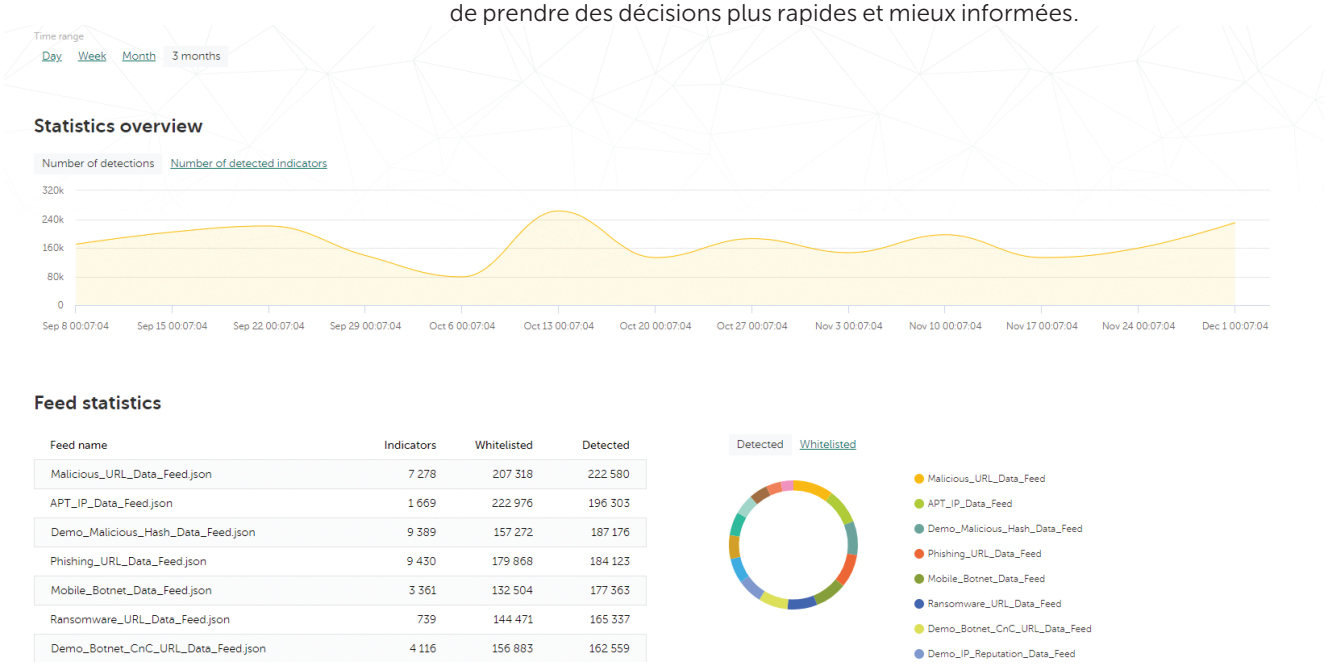


Figure 1. Statistiques Kaspersky CyberTrace

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 :

- Dès l'achat du produit, des flux OSINT et des flux de données sur les menaces de démonstration sont mis à disposition par Kaspersky Lab
- Connecteurs SIEM pour une large gamme de solutions SIEM afin de visualiser et de gérer les données de détection des menaces
- Statistiques d'utilisation des flux pour mesurer l'efficacité des flux intégrés
- Recherche à la demande des indicateurs (hachages, adresses IP, domaines, URL) pour une investigation en profondeur
- Interface utilisateur Web fournissant une visualisation des données, un accès à la configuration, une gestion des flux, des règles d'analyse des journaux et des listes noires et blanches
- Filtrage avancé des flux (selon le contexte fourni pour chacun des indicateurs : type de menace, géolocalisation, popularité, horodatage, etc.) et des événements des journaux (basé sur des conditions personnalisées)
- Exportation des résultats de recherche des flux de données au format CSV pour intégration avec d'autres systèmes (pare-feu, réseau, IDS hôte et outils personnalisés)
- Analyse groupée des journaux et des fichiers
- Interface à ligne de commande pour les plateformes Windows et Linux
- Mode autonome, dans lequel Kaspersky CyberTrace n'est pas intégré à un SIEM mais reçoit et analyse les journaux provenant de diverses sources telles que les appareils réseau
- Installation selon des scénarios compatibles DMZ, en complète isolation d'Internet.

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 :

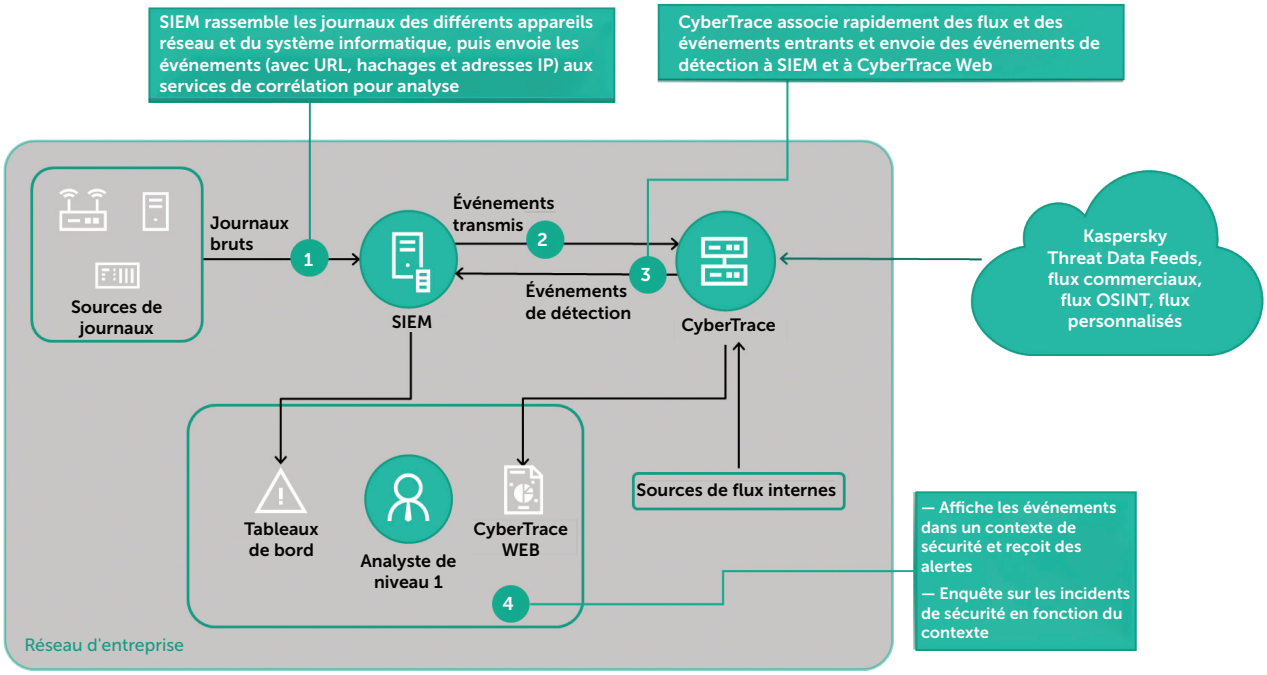


Schéma 2. Plan d'intégration de Kaspersky CyberTrace

Kaspersky Lab offre également des flux de données sur les menaces mis à jour en permanence qui peuvent être intégrés à Kaspersky CyberTrace pour une visibilité globale des menaces, une détection rapide des cybermenaces, une hiérarchisation des alertes de sécurité et une réponse efficace aux incidents liés à la sécurité des informations :

- Informations sur la réputation des adresses IP : ensemble d'adresses IP avec des données sur différentes catégories d'hôtes suspects et malveillants
- Informations sur les URL malveillantes et de phishing : liens et sites Internet malveillants et de phishing
- Informations sur les URL C&C de botnet : serveurs C&C de botnet d'ordinateurs de bureau et objets malveillants connexes
- Informations sur les URL C&C de botnet mobiles : serveurs C&C de botnet mobiles

- Informations sur les URL de ransomwares : liens hébergeant des ransomwares ou auxquels des ransomwares accèdent
- Informations sur indicateurs de compromissions APT : domaines, hôtes, adresses IP ou fichiers malveillants utilisés par des adversaires pour commettre des attaques APT
- Informations sur les DNS passives (pDNS) : ensemble de dossiers contenant les résultats de résolutions DNS pour les domaines en adresses IP correspondantes[1]
- Informations sur les URL IoT : sites Web utilisés pour télécharger un logiciel malveillant qui infecte les appareils IoT[2]
- Informations sur les hachages malveillants : nouveaux programmes malveillants les plus répandus et les plus dangereux
- Informations sur les hachages malveillants mobiles : objets malveillants qui infectent les plateformes mobiles Android et iPhone
- Informations sur le cheval de Troie P-SMS : chevaux de Troie SMS qui permettent de voler, de supprimer et de répondre à des SMS et de générer des frais via l'appel à des numéros surtaxés sur un mobile
- Informations sur les listes blanches : informations détaillées sur les logiciels authentiques destinées aux solutions et services tiers

Les flux d'informations sont agrégés à partir de sources ultra-fiables, hétérogènes et fusionnées, comme Kaspersky Security Network (plus de 100 millions d'utilisateurs qui partagent volontairement avec nous leurs données sur les cybermenaces), 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 spécialisées dans la recherche des menaces et nos partenaires de confiance.

Toutes ces données agrégées sont ensuite soigneusement analysées et affinées en temps réel à l'aide de plusieurs techniques de prétraitement : critères statistiques, systèmes spécialisés Kaspersky Lab (sandboxes, moteurs heuristiques, systèmes d'analyse multiples, outils de similarité, profils de comportement, etc.), validation par des analystes et vérification de listes blanches.

Pour tous les flux de données, chaque dossier est enrichi de contexte pouvant donner lieu à des actions (notation des menaces, géolocalisation, nom des menaces, horodatage, adresses IP résolues de ressources Web infectées, hachages, popularité, etc.).

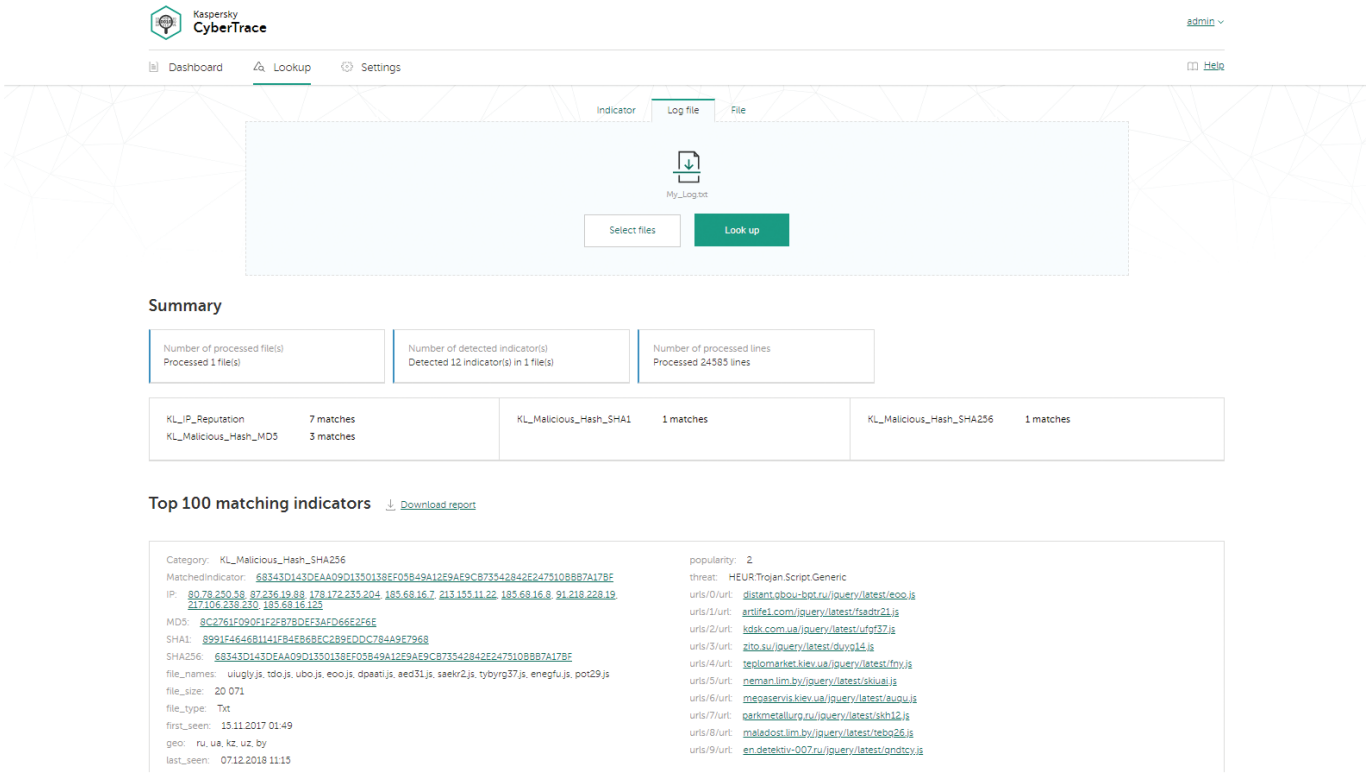


Schéma 3. Contexte de Kaspersky Threat Data Feeds

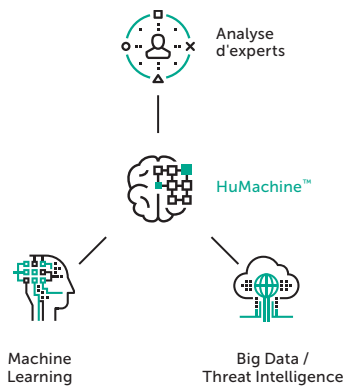
1 L'intégration sera prise en charge en 2019

2 L'intégration sera prise en charge en 2019

Ces 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 les bonnes décisions.

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 analystes du centre 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 Lab
Solutions de cybersécurité pour les entreprises :
www.kaspersky.fr/enterprise-security
Actualités dédiées aux cybermenaces : **www.securelist.fr**
Actualités dédiées à la sécurité informatique : **https://www.kaspersky.fr/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.fr