kaspersky prêts pour l'avenir

Kaspersky
Threat Intelligence

Kaspersky Données sur les menaces Flux

Présentation

Que contiennent les flux ?

Les entrées des flux fournis par Kaspersky contiennent des données contextuelles qui vous permettent de confirmer rapidement les menaces et de les classer par ordre de priorité :

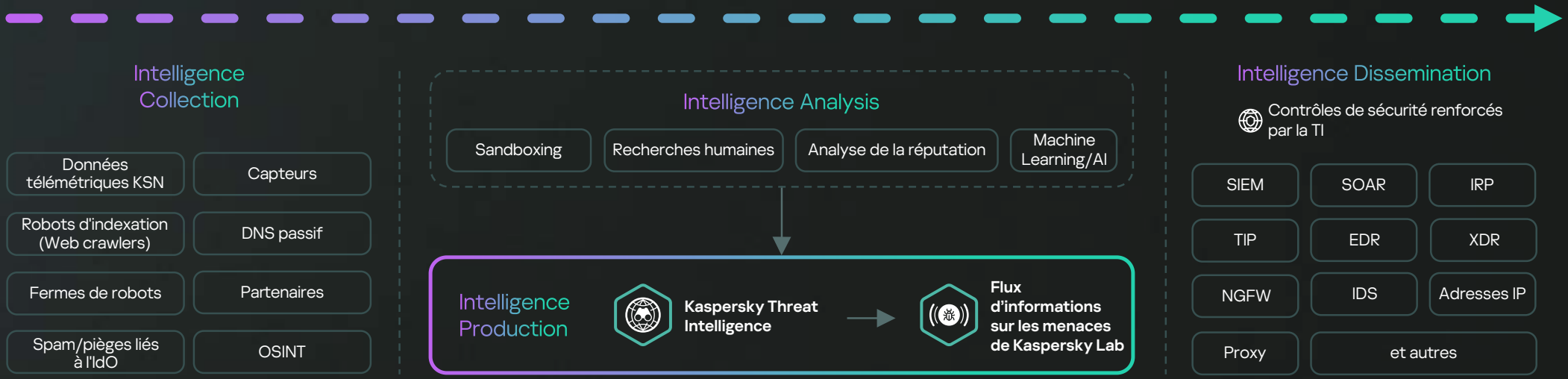
- noms des menaces
- adresses IP établies et noms de domaine des ressources Internet malveillantes
- hachages de fichiers malveillants
- identifiants des objets vulnérables et compromis
- tactiques, techniques et procédures d'attaques selon la classification MITRE ATT&CK
- horodatage
- position géographique
- popularité, etc.

Le service Kaspersky Threat Data Feed fournit des informations de Threat Intelligence en temps réel pour aider les organisations à protéger leurs réseaux et systèmes contre les menaces. Les flux de données comprennent des informations sur les programmes malveillants connus, les sites Internet de phishing, les vulnérabilités et les exploits les plus récents, ainsi que d'autres types de cybermenaces. Les organisations peuvent utiliser ces informations pour bloquer le trafic malveillant, mettre à jour leurs logiciels de sécurité et prendre d'autres mesures pour se protéger des cyberattaques.

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 (surveillance 24/7 des réseaux de zombies, de leurs cibles et de leurs activités), les pièges à spam, les données des groupes de recherche et des partenaires.

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.

Les flux de données permettent de collecter des informations générales sur un événement et de les examiner en détail. Ils permettent également de répondre aux questions « Qui ? Quoi ? Où ? 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.



Comment utiliser les flux de données ?

Nom du flux	menaces	Détection	Enquête
Flux d'informations sur les URL malveillantes	•	•	•
Flux d'informations sur les URL de ransomwares	•	•	•
Flux de données des URL de phishing	•	•	•
Flux d'informations sur les URL de botnet C&C	•	•	•
Flux de données sur les URL de botnet C&C mobiles	•	•	•
Flux d'informations sur les hachages malveillants	•	•	•
Flux d'informations mobile sur les hachages malveillants	•	•	•
Flux d'informations sur la réputation des IP	•	•	•
Flux d'informations sur les URL IoT	•	•	•
Flux d'informations sur les vulnérabilités	•	•	•
Flux d'informations sur les vulnérabilités dans les ICS	•	•	•
Flux d'informations sur les vulnérabilités dans les ICS au format OVAL		•	
Flux d'informations sur les hachages ICS	•	•	•
Flux d'informations sur le pDNS			•

Nom du flux	menaces	Détection	Enquête
Flux d'informations sur les règles Suricata		•	
Flux d'informations sur l'agent de sécurité des accès au cloud (CASB)		•	
Flux d'informations sur le hachage d'APT		•	•
Flux d'informations sur les IP d'APT		•	•
Flux d'informations sur les URL d'APT		•	•
Flux d'informations Yara sur les APT		•	•
flux d'informations sur les menaces liées aux logiciels open source	•	•	•
Flux d'informations sur les hachages de crimewares		•	•
Flux d'informations sur les URL de crimeware			•
Flux d'informations Yara sur les crimewares			•
Flux de données sur les règles Sigma	•		
Flux de données sur les IP de la sécurité des réseaux	•	•	
Flux de données sur les URL de la sécurité des réseaux	•	•	
Flux de données sur le filtage Internet de la sécurité des réseaux	•	•	

La liste des flux de données sur les menaces de Kaspersky est en constante évolution.

Description des flux d'informations sur les menaces de Kaspersky

Flux commerciaux

Les flux commerciaux permettent d'accéder à la collection d'informations la plus complète disponible par abonnement. Les informations sont mises à jour régulièrement ; selon le type de flux, la régularité des mises à jour peut varier de quelques minutes à quelques heures. Outre les flux de données listés, vous pouvez demander la création d'un flux personnalisé adapté à vos besoins.

Nom du flux	Description du flux	Type d'indicateur	Cas d'utilisation
Flux d'informations sur les URL malveillantes	Ressources Internet à partir desquelles les programmes malveillants sont distribués	Mask	• Les systèmes de gestion de la sécurité de l'information sont ouverts à l'enrichissement par des sources d'information externes. La connexion de ces flux aux SIEM/SOAR/IRP permet aux utilisateurs de répondre aux menaces actuelles en temps opportun et d'établir un contexte supplémentaire lors d'une enquête sur un incident. • L'intégration aux systèmes de sécurité des réseaux et de protection des messageries (par exemple, NGFW/IDS/IPS/Mail/Web Security) permet de prévenir les cyberincidents en enrichissant les capacités natives de contrôle de la sécurité avec des IOC provenant des flux de données.
Flux d'informations sur les URL de ransomwares	Ressources Internet à partir desquelles les ransomwares sont distribués		
Flux de données des URL de phishing	Ressources Web de phishing		
Flux d'informations sur les URL de botnet C&C	Serveurs de botnet C&C et objets malveillants associés (bots)		
Flux de données sur les URL de botnet C&C mobiles	Serveurs de botnet C&C mobiles et objets malveillants associés (bots)		

#prévention

#détection

#enquête

Nom du flux	Description du flux	Type d'indicateur	Cas d'utilisation	
Flux d'informations sur les hachages malveillants	Hachages de fichiers malveillants courants	Hachage	• Intégration aux systèmes de sécurité de l'infrastructure (sécurité des terminaux, sécurité des serveurs, sécurité des emails et d'Internet) pour empêcher le téléchargement et l'exécution de programmes malveillants, ainsi que pour détecter les programmes malveillants déjà en cours d'exécution. • L'intégration aux systèmes SIEM/SOAR/IRP permet aux utilisateurs de répondre rapidement aux menaces actuelles et d'établir un contexte supplémentaire lors d'une enquête sur un incident.	#prévention #détection #enquête
Flux d'informations mobile sur les hachages malveillants	Hachages de fichiers malveillants courants pour les systèmes d'exploitation mobiles (Android et iOS)			
Flux d'informations sur la réputation des IP	Différentes catégories d'adresses IP suspectes et malveillantes	IP	• L'intégration aux systèmes de sécurité des réseaux et des emails (NGFW/Mail Security) permet de prévenir les cyberincidents en enrichissant la base de données native des indicateurs de compromission avec des données sur les menaces actuelles. • L'intégration aux systèmes de classe SIEM/ SOAR/IRP permet aux utilisateurs de répondre rapidement aux menaces actuelles et d'établir un contexte supplémentaire lors d'une enquête sur un incident.	#prévention #détection #enquête
Flux d'informations sur les URL IoT	Ressources Internet qui distribuent des programmes malveillants pour les appareils de l'IdO (caméras IP, aspirateurs intelligents, théières, cafetières, etc.)	Mask		
Flux d'informations sur les vulnérabilités	Failles des logiciels d'entreprise	CVE	• Identification des éléments d'infrastructure vulnérables grâce à l'intégration des analyseurs de vulnérabilités et des systèmes de gestion des ressources. • Intégration aux systèmes de protection des terminaux afin d'empêcher le lancement de logiciels contenant des vulnérabilités critiques. • Détection du lancement de logiciels vulnérables. • Aide aux enquêtes. • Recommandations pour l'atténuation des vulnérabilités.	#prévention #détection #enquête
Flux d'informations sur les vulnérabilités dans les ICS	Vulnérabilités dans les logiciels et le matériel SCI, ainsi que dans les logiciels d'entreprise utilisés dans l'infrastructure de contrôle des processus			

Nom du flux	Description du flux	Type d'indicateur	Cas d'utilisation	
Flux d'informations sur les vulnérabilités dans les ICS au format OVAL	Règles pour la recherche automatisée des vulnérabilités dans les logiciels SCI	Contrôle OVAL	• Enrichissement des analyseurs de vulnérabilités des logiciels les plus courants afin de détecter les logiciels SCI vulnérables.	#détection
Flux d'informations sur les hachages ICS	Fichiers malveillants courants qui constituent une menace pour les SCI	Hachage	• À la périphérie des réseaux TO, comme dans les scénarios d'utilisation des flux de données sur les hachages malveillants. • À l'intérieur des réseaux TO, pour détecter les fichiers potentiellement dangereux.	#prévention #détection #enquête
Flux d'informations sur le pDNS	Enregistrements des recherches DNS pour les domaines vers les adresses IP correspondantes au cours d'une période donnée	IP, FQDN	• Mise en contexte lors des enquêtes sur les cyberincidents	#enquête
Flux d'informations sur les règles Suricata	Règles pour la détection de diverses catégories de menaces dans le trafic réseau, comme les APT, les botnets C&C, les ransomwares, etc.	Règles Suricata	• Intégration aux systèmes NGFW/IDS/IPS/NTA/NDR afin d'enrichir les règles de détection des activités malveillantes.	#détection
Flux d'informations sur l'agent de sécurité des accès au cloud (CASB)	Domaines et hôtes liés aux services cloud les plus courants	Mask	• Établissement d'une solution CASB, en particulier, afin de mettre en place des politiques d'accès aux services cloud.	#détection

Nom du flux	Description du flux	Type d'indicateur	Cas d'utilisation	
Flux d'informations sur le hachage d'APT	Hachages de fichiers utilisés par les gangs APT pour mener des attaques ciblées	Hachage	• Intégration aux systèmes de sécurité de l'infrastructure (sécurité des terminaux et des serveurs) pour empêcher le téléchargement et l'exécution de programmes malveillants, ainsi que pour détecter les programmes malveillants déjà en cours d'exécution. • L'intégration aux systèmes de sécurité des réseaux et de protection des messageries (par exemple, NGFW/IDS/IPS/Mail/Web Security) permet de prévenir les cyberincidents en enrichissant les capacités natives de contrôle de la sécurité avec des IOC provenant des flux de données. • L'intégration aux systèmes de classe SIEM/SOAR/IRP permet aux utilisateurs d'établir un contexte supplémentaire lors d'une enquête sur un incident, ainsi que de répondre en temps opportun aux menaces actuelles liées aux attaques ciblées ou aux membres de groupes APT.	#détection #enquête
Flux d'informations sur les IP d'APT	Informations sur les éléments d'infrastructure utiles à la conduite d'attaques ciblées	IP		
Flux d'informations sur les URL d'APT		Mask		
Flux d'informations Yara sur les APT	Règles YARA pour l'identification des fichiers utilisés dans les attaques ciblées	Règles YARA	• Recherche proactive de signes d'attaques ciblées dans l'infrastructure d'une entreprise. • Utile lors des enquêtes sur les cyberincidents.	#détection #enquête
flux d'informations sur les menaces liées aux logiciels open source	Logiciels open source contenant des vulnérabilités, des fonctionnalités malveillantes ou des compromissions de fonctionnalités à des fins politiques (blocage dans certaines régions, slogans politiques, etc.)	Nom et version du paquet	• Conçu pour l'analyse des modules des logiciels développés dans le cadre du processus de développement sécurisé (DevSecOps) afin de protéger les logiciels des attaques contre la chaîne d'approvisionnement, la détection précoce et l'élimination des vulnérabilités, ainsi que pour empêcher l'utilisation de paquets contenant des fonctionnalités non déclarées à orientation politique (NDV).	#prévention #détection #enquête

Nom du flux	Description du flux	Type d'indicateur	Cas d'utilisation	
Flux d'informations sur les hachages de crimewares	Hachages de fichiers utilisés dans les campagnes frauduleuses décrites dans les rapports sur les crimewares de Kaspersky	Hachage	• Détection des activités malveillantes associées aux actions frauduleuses des intrus. • Contribution à la résolution des incidents en fournissant des informations supplémentaires contenues dans les flux de données sur les menaces.	#détection #enquête
Flux d'informations sur les URL de crimeware	Informations sur les éléments d'infrastructure liés aux campagnes frauduleuses décrites dans les rapports sur les crimewares de Kaspersky	Mask		
Flux d'informations Yara sur les crimewares	Règles YARA pour l'identification des fichiers utilisés dans les campagnes frauduleuses décrites dans les rapports sur les crimewares de Kaspersky	Règles YARA	• Recherche proactive de signes de campagnes frauduleuses dans l'infrastructure de l'entreprise. • Utile lors des enquêtes sur les cyberincidents.	#enquête
Flux de données sur les règles Sigma	Règles au format YAML pour la détection des activités malveillantes	Règles Sigma	• Intégration au SIEM/EDR pour détecter les activités malveillantes	#détection
Flux de données sur les IP de la sécurité des réseaux	Liste des adresses IP pour les listes d'alerte/de refus du NGFW	IP	• Intégration aux contrôles de sécurité des réseaux (NGFW) pour augmenter leur niveau de protection	#détection #prévention

Nom du flux	Description du flux	Type d'indicateur	Cas d'utilisation	
Flux de données sur les URL de la sécurité des réseaux	Liste des URL pour les listes d'alerte/de refus du NGFW	URL	• Intégration aux contrôles de sécurité des réseaux (NGFW) pour augmenter leur niveau de protection	#détection #prévention
Flux de données sur le filtage Internet de la sécurité des réseaux	Liste des domaines catégorisés pour les listes d'alerte/de refus du NGFW	URL	• Intégration aux contrôles de sécurité des réseaux (NGFW) pour augmenter leur niveau de protection	#détection #prévention

Flux de démonstration

Les flux de démonstration sont uniquement destinés à l'évaluation. Les données contiennent des échantillons limités avec des informations considérablement réduites et des mises à jour moins fréquentes.
La structure des flux est similaire au format des flux commerciaux, mais elle peut différer dans certains cas.

- Flux d'informations de démonstration sur la réputation des IP
- Flux d'informations de démonstration sur les URL de botnet C&C
- Flux d'informations de démonstration sur les hachages malveillants
- Flux d'informations de démonstration sur les IP d'APT
- Flux d'informations de démonstration sur les URL d'APT
- Flux d'informations de démonstration sur les règles Sigma
- Flux d'informations de démonstration sur le hachage d'APT
- Flux d'informations de démonstration sur les règles Suricata
- Flux d'informations de démonstration sur les règles Suricata
- Flux d'informations de démonstration sur les vulnérabilités dans les ICS
- Flux d'informations de démonstration sur les vulnérabilités dans les ICS au format OVAL
- Flux d'informations de démonstration sur les hachages de crimewares
- Flux d'informations de démonstration sur les URL de crimeware

Demander une démo

Kaspersky Threat Intelligence

Votre contexte riche en informations

Kaspersky Threat Data Feeds améliore les capacités de détection de vos contrôles de sécurité existants, notamment les systèmes SIEM, les systèmes de détection des intrusions, les proxies de sécurité, etc.

En savoir plus

www.kaspersky.fr