

Kaspersky Threat Intelligence

Gardez une longueur d'avance
sur vos adversaires



kaspersky

Sources des données de Threat Intelligence Kaspersky

2



Kaspersky Threat Intelligence donne accès à un large éventail d'informations recueillies par **nos analystes et chercheurs de renommée mondiale** afin d'aider votre organisation à contrer efficacement les cybermenaces actuelles.

Threat Intelligence fondée sur une expertise et des connaissances uniques à l'échelle mondiale

3



Chaque centre contribue à faire évoluer les solutions et services de Kaspersky

● Recherche de menaces

● Investigation des incidents



Kaspersky Global Research and Analysis Team

- Recherche des menaces les plus complexes : APT, campagnes de cyberespionnage, cyberépidémies mondiales, etc.
- Sécurité des technologies d'avenir
- Enquête sur des cas de cybercriminalité financière complexe



Kaspersky Recherche de menaces

- Recherche de programmes malveillants
- Recherche de filtrage de contenu
- Méthodes de développement SSDLC et de sécurisation dès la conception



Kaspersky AI Technology Research

- Cybersécurité IA
- Recherche dans le domaine de l'IA générative
- Détection des menaces / solutions assistées par l'IA



Kaspersky Services de sécurité

- MDR
- Réponse aux incidents
- Security Assessment
- Conseil en matière de SOC
- Digital Footprint Intelligence



Kaspersky ICS CERT

- Analyse des menaces pesant sur les infrastructures critiques
- Recherche et évaluation de la vulnérabilité des SCİ
- Associations, analyses et normes technologiques

Faits marquants de Kaspersky Threat Intelligence Portal

4

Nos connaissances pointues, notre vaste expérience en matière de recherche sur les cybermenaces et notre vision unique de tous les aspects de la cybersécurité font de nous un partenaire de confiance pour les entreprises du monde entier et un allié précieux pour les forces de l'ordre et les organisations gouvernementales, y compris Interpol et de nombreux CERT.



Couverture des menaces mondiales et vaste expérience en matière de recherche sur les menaces dans les zones géographiques d'où proviennent la plupart des attaques



Contribution continue des experts de Kaspersky



Threat Intelligence pour les segments IT et OT



Faits marquants de Kaspersky Threat Intelligence Portal

5

Nous suivons :

Plus de
300



acteurs de menaces

Plus de
500



de cyber-espionnage

Plus de
200

rapports privés par
an sont produits

Plus de
170000

IoCs liés aux rapports

Plus de
2 500

règles YARA relatives
aux rapports

Niveaux de données de Threat Intelligence

6



Tactique

Informations de bas niveau, hautement périssables, qui soutiennent les opérations de sécurité et la réponse aux incidents. Un exemple de renseignements tactiques est l'IOC lié à la conduite d'une attaque nouvellement découverte.

Fonctions:

Analyste SOC

Systems:

SIEM

NGFW

SOAR

Adresses IP

IDS

Processus:

Threat Hunting

Contrôle



Opérationnelle

Ce niveau comprend généralement des données sur les campagnes et les TTP d'ordre supérieur. Il peut inclure des informations sur l'attribution d'acteurs particuliers, ainsi que sur les capacités et les intentions des adversaires.

Fonctions:

Analyste SOC L3

Analyste DFIR

Analyste IR

Systems:

SIEM

NTA

TIP

EDR / XDR

Processus:

Réponse aux incidents

Threat Hunting



Stratégie

Ce niveau soutient les cadres dirigeants et les conseils d'administration dans la prise de décisions importantes liées à l'évaluation des risques, à l'affectation des ressources et à la stratégie organisationnelle. Ces informations comprennent les tendances, les motivations des acteurs et leurs classifications.

Fonctions:

RSSI

CTO

CIO

PDG

Processus:

Élaboration d'une stratégie en matière de SI

Sensibilisation

Formats de diffusion de la Threat Intelligence

7



Threat Intelligence
interprétable par
une machine



Kaspersky
Threat Data
Feeds

Plus de 30 flux d'informations
sur les menaces répondant à
des besoins différents avec une
couverture IT et OT ainsi qu'une
plateforme TI



Threat Intelligence
interprétable par
un être humain



Kaspersky
Threat Intelligence
Portal

Le portefeuille principal de
Kaspersky Threat Intelligence pour
les environnements IT et OT avec
un point d'accès unique via
Kaspersky Threat Intelligence Portal



Support expert en
Threat Intelligence



Kaspersky
Takedown
Service



Kaspersky
Ask the Analyst

Des conseils de professionnels
chevronnés

Kaspersky Threat Intelligence

8



Flux d'informations sur les menaces de Kaspersky Lab

9



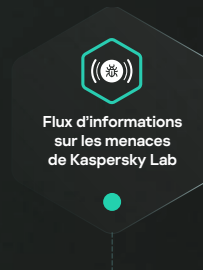
Plus de 30 flux d'informations sur les menaces prêts à l'emploi pour différentes tâches.

Des flux d'informations sur les menaces personnalisés en fonction de votre organisation sont également disponibles.

- TI tactique
- TI opérationnelle

Flux d'informations général sur les menaces

- URL malveillantes
- URL de ransomwares
- URL de phishing
- URL de botnet C&C
- Botnet mobile C&C de botnet mobiles
- Hachages malveillants
- Hachages malveillants mobiles
- Réputation des IP
- URL IoT
- Hachages d'ICS
- Hachage d'APT
- IP d'APT
- URL d'APT
- Hachages de crimewares
- URL de crimewares



Flux d'informations sur les menaces de Kaspersky Lab

SIEM, SOAR / IRP, TIP, EDR / XDR

Plateforme de TI

Rendez rapidement opérationnels vos différents flux de Threat Intelligence et réduisez la charge de travail des SIEM



Flux d'informations spécifique sur les menaces



Kaspersky Threat Intelligence Portal

10



Un point d'accès unique à Kaspersky Threat Intelligence au sein d'une interface utilisateur / API unifiée, où les services travaillent ensemble, s'enrichissent et se renforcent mutuellement. Rassemblant toute l'expertise et les connaissances de Kaspersky en matière de cybermenaces en un seul endroit, il permet de surveiller les menaces pertinentes pour chaque organisation grâce à des technologies propriétaires de traitement et de normalisation des données, et permet d'examiner des échantillons de programmes malveillants et leur attribution.

- TI tactique
- TI opérationnelle
- TI stratégique



Kaspersky
Threat Intelligence Portal :
version gratuite



Paysage des menaces sur Kaspersky Threat Intelligence Portal

11

Threat Intelligence propre à votre pays et à votre industrie pour comprendre les menaces exactes auxquelles votre organisation est confrontée

- Alignement MITRE ATT&CK
- Mises à jour en temps réel basées sur les recherches en cours de My Kaspersky
- Remplissage automatique des profils des adversaires et des logiciels
- Stockages des règles de détection

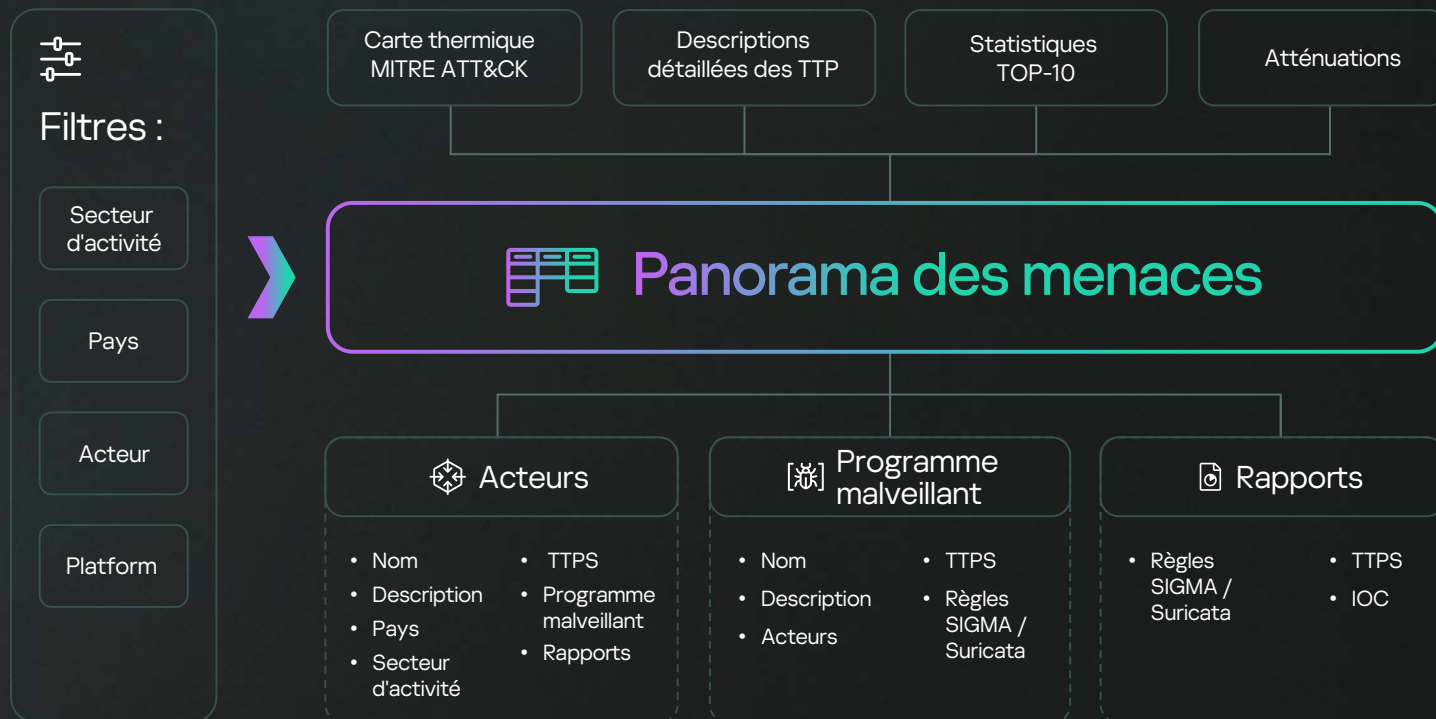


Plus de 400 000

Fichiers malveillants que nous détectons quotidiennement

Paysage des menaces – fonctionnement

12



Support par des experts de Kaspersky Threat Intelligence

13



Kaspersky Ask the Analyst

- TI opérationnelle
- TI stratégique

Le service Kaspersky Ask the Analyst vous permet **de demander des conseils et des informations sur des menaces spécifiques auxquelles vous êtes confronté** ou qui vous intéressent.

Nous vous donnons accès à un groupe de chercheurs de Kaspersky, au cas par cas. Ce service permet une communication complète entre experts afin de renforcer vos capacités existantes grâce à nos connaissances et ressources uniques.



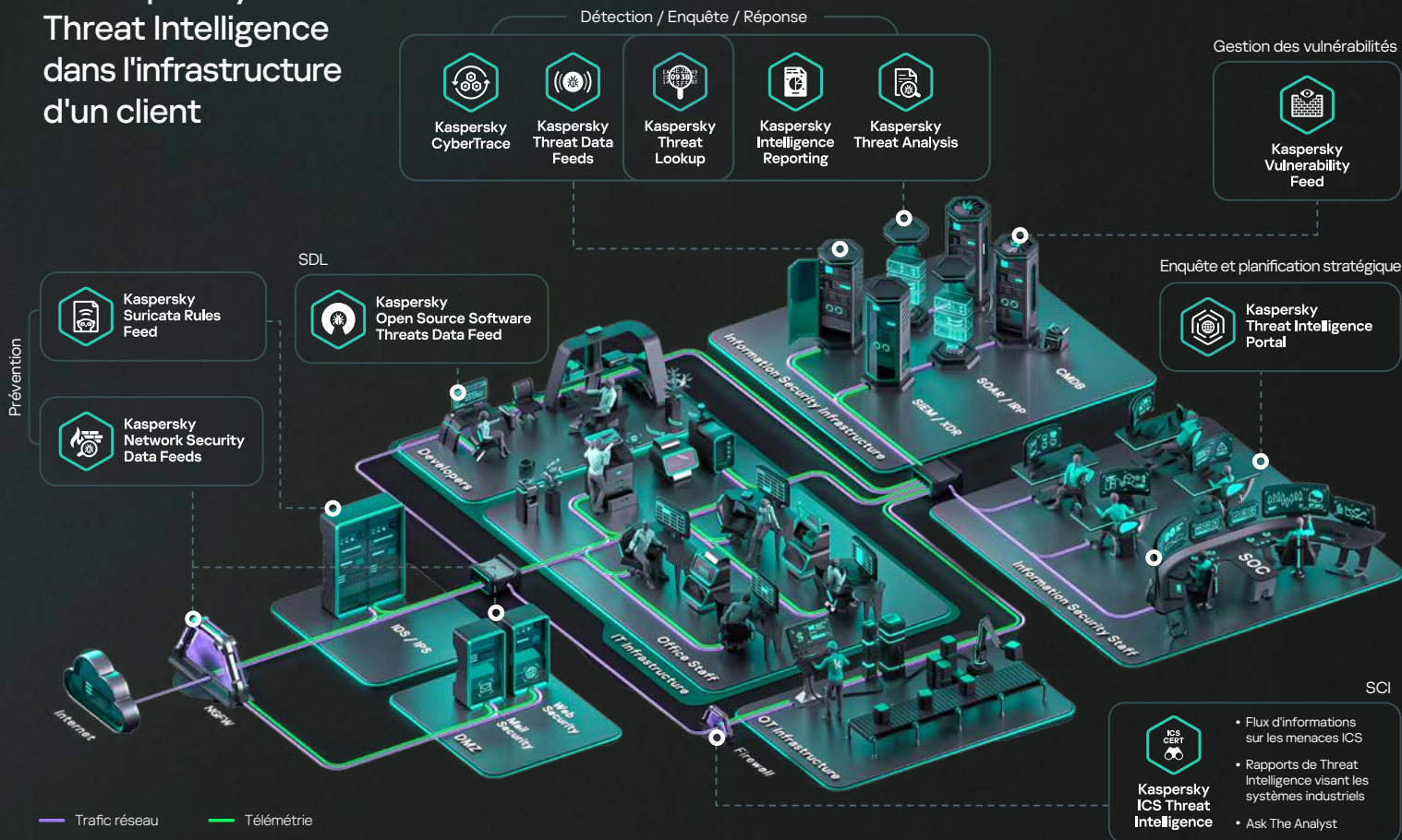
Kaspersky Takedown Service

- TI opérationnelle

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. Forts d'une grande expérience dans l'analyse des domaines, nous savons comment rassembler les preuves indiquant qu'il s'agit de domaines malveillants. Nous nous occupons de la gestion du démantèlement. Ce service est fourni à l'échelle mondiale en collaboration avec des organisations internationales et des organismes nationaux et régionaux chargés de l'application de la loi.

Exemple d'utilisation de Kaspersky Threat Intelligence dans l'infrastructure d'un client

14



Kaspersky Threat Intelligence Industrial

15

Threat Intelligence interprétable par une machine



Kaspersky Threat Data Feeds

Données lisibles par les machines sur les menaces et les vulnérabilités en matière de cybersécurité industrielle :

Flux d'informations sur les hachages de Kaspersky ICS Flux d'informations sur les vulnérabilités de Kaspersky ICS Flux d'informations sur les vulnérabilités de Kaspersky ICS au format OVAL

Threat Intelligence interprétable par un être humain



Kaspersky ICS Intelligence Reporting

Accédez à des publications régulières portant sur les menaces et les vulnérabilités en matière de cybersécurité industrielle sur le portail Kaspersky Threat Intelligence Portal

Soutien d'un expert en Threat Intelligence



Kaspersky Ask the Analyst

Consultez directement les experts de Kaspersky ICS CERT pour obtenir des conseils personnalisés sur les menaces et les vulnérabilités en matière de cybersécurité industrielle, les statistiques sur les menaces, le paysage des menaces, les normes de l'industrie et plus encore.

● Tactique

● TI opérationnelle

● TI stratégique

Pourquoi choisir Kaspersky Threat Intelligence

16



Une offre TI de premier plan reconnue par les analystes de l'industrie

Vérifié par des analystes de diverses entreprises mondiales de recherche comme Frost & Sullivan, Quadrant Knowledge Solutions, Forrester, IDC, etc.



Des sources multiples, crédibles et uniques pour produire une TI fiable

Notre infrastructure Kaspersky Security Network couvre plus de 100 millions de capteurs dans 200 pays, les plus grands stockages de fichiers malveillants et légitimes, le Dark Web, les activités TH et IR continues, les robots d'indexation web, les pièges à spam, etc.



Une expertise humaine reconnue dans les domaines IT et OT

Plus de 200 experts certifiés issus de 5 centres d'expertise, dont l'équipe GReAT et ICS-CERT, répartis dans le monde entier et parlant plus de 20 langues. Les experts de Kaspersky sont toujours parmi les premiers à découvrir les menaces les plus notoires, allant de Stuxnet et WannaCry à l'opération Triangulation.



Une présence mondiale

Notre forte présence dans les pays d'où proviennent la plupart des attaques (Russie/CEI, Chine, etc.) nous donne la possibilité unique de collecter, d'analyser et de distribuer une Threat Intelligence entièrement vérifiée pour les organisations de n'importe quel pays.



Expérience unique en matière de technologies de détection des programmes malveillants

En tant qu'éditeur de solutions de cybersécurité proposant les produits les plus primés, nous traitons chaque jour des millions de nouveaux échantillons de programmes malveillants à l'aide de nos technologies exclusives de détection des menaces.



Une expérience unique en matière de recherche sur les APT

Nous surveillons des centaines d'acteurs et de campagnes d'APT, publions plus de 200 rapports stratégiques approfondis sur les technologies de l'information chaque année et disposons de la plus grande collection de fichiers d'APT de l'industrie, qui comprend plus de 70 000 échantillons.



TI optimisée par l'IA en vue d'améliorer la détection, la réponse et les rapports sur les menaces

L'IA et le ML nous permettent d'extraire des informations exploitables, de générer des rapports personnalisés et d'automatiser les analyses, ce qui nous permet d'économiser beaucoup de temps et de ressources.



Un fournisseur robuste et sûr

Infrastructure transparente et résistante aux pannes, avec des accords de niveau de service et des fonctions de surveillance élevés, construite selon des méthodologies SDLC, avec des évaluations régulières par des tiers indépendants (SOC 2 Type 2 ou ISO 27001).

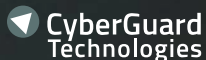
Études de cas publiques

17



Nous disposons ainsi d'une meilleure visibilité sur les menaces auxquelles nos clients sont confrontés. En cas d'alerte, il est vital de posséder ces informations spécialisées et référençables, avec toutes les données collatérales qui les accompagnent, pour obtenir une image complète de la situation et des enseignements que nous pouvons en tirer.

Paul Colwell
CyberGuard Technologies



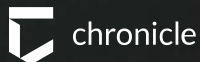
Lire l'étude de cas



Kaspersky est souvent la première entreprise à identifier l'émergence d'une nouvelle menace, avant même que les éditeurs de logiciels n'en soient informés.

Kaspersky dispose de l'expertise nécessaire pour m'informer au sujet des menaces nouvelles, tapies dans l'ombre et que nous ne connaissons pas, au lieu de simplement donner une foule d'informations recyclées qui ne nous apportent rien de plus.

Juan Andres Guerrero Saade
Chercheur, Chronicle Security



Lire l'étude de cas



Kaspersky a dépassé mes attentes par ses fonctionnalités et son souci de répondre à nos besoins. Nous avons fait confiance au produit et aux personnes qui l'ont développé, ce qui nous a permis de sécuriser davantage notre réseau.

Rashid AlNahlawi
Consultant en sécurité informatique,
Comité olympique du Qatar



Lire l'étude de cas

Kaspersky Threat Intelligence vous aide...

18



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 ne se produise.



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.



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.



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.



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.

Merci !

Kaspersky Threat Intelligence Portal –
le portail des connaissances en matière
de cybersécurité



Kaspersky
Threat Intelligence
Portal



En savoir plus



Demander une démonstration

