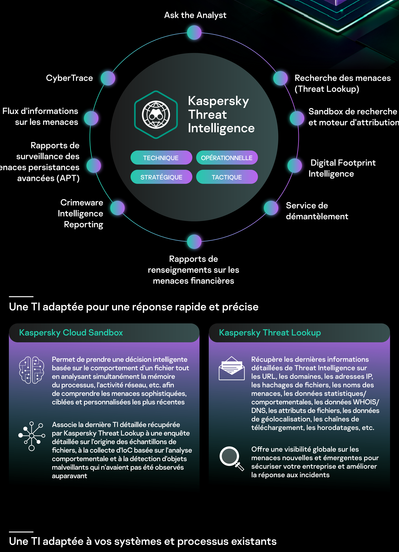
# De quel type de Threat Intelligence votre organisation a-t-elle besoin ?

## Une Threat Intelligence sur mesure




## Une TI adaptée pour une réponse rapide et précise

### Kaspersky Cloud Sandbox

Permet de prendre une décision intelligente basée sur le comportement d'un fichier tout en analysant simultanément la mémoire du processus, l'activité réseau, etc. afin de comprendre les menaces sophistiquées, ciblées et personnalisées les plus récentes

Associe la dernière TI détaillée récupérée par Kaspersky Threat Lookup à une enquête détaillée sur l'origine des échantillons de fichiers, à la collecte d'IoC basée sur l'analyse comportementale et à la détection d'objets malveillants qui n'avaient pas été observés auparavant

### Kaspersky Threat Lookup

Récupère les dernières informations détaillées de Threat Intelligence sur les URL, les domaines, les adresses IP, les hachages de fichiers, les noms des menaces, les données statistiques/ comportementales, les données WHOIS/ DNS, les attributs de fichiers, les données de géolocalisation, les chaînes de téléchargement, les horodatages, etc.

Offre une visibilité globale sur les menaces nouvelles et émergentes pour sécuriser votre entreprise et améliorer la réponse aux incidents

## Une TI adaptée à vos systèmes et processus existants

### Kaspersky CyberTrace

Le portail Threat Intelligence Portal assure l'intégration transparente des flux de données sur les menaces avec les solutions SIEM et aide vos analystes à exploiter plus efficacement la Threat Intelligence dans le cadre de leur flux de travail actuel sur les opérations de sécurité

Réduit considérablement la charge de travail des SIEM en traitant les journaux et les événements entrants, en associant rapidement les résultats aux flux et en générant ses propres alertes de détection des menaces

Intégration avec n'importe quel flux TI aux formats JSON, STIX, XML et CSV, et intégration prête à l'emploi avec de nombreuses solutions SIEM et sources de journaux

La combinaison de Kaspersky CyberTrace et de Kaspersky Threat Data Feeds permet à vos analystes de sécurité de traiter efficacement et de prioriser d'énormes quantités d'alertes de sécurité, d'améliorer et d'accélérer le triage et la réponse initiale, d'identifier immédiatement les alertes graves, de prendre des décisions éclairées sur celles qui doivent être transmises aux équipes de réponse aux incidents (RI) et de mettre en place une défense proactive fondée sur les renseignements

## Une TI adaptée à votre paysage de menaces individuel

### Kaspersky Threat Data Feeds

Intègre des flux TI actualisés contenant des informations sur les adresses IP, les URL et les hachages de fichiers suspects et dangereux dans les systèmes de sécurité existants tels que SIEM, SOAR et les plateformes de Threat Intelligence (TIP)

Automatise le triage initial des alertes et fournit à vos spécialistes du triage le contexte nécessaire pour identifier immédiatement les alertes qui doivent faire l'objet d'une enquête ou être transmises aux équipes chargées des incidents de réponse en vue de mener une enquête plus approfondie et d'apporter une réponse

Accès à des enregistrements enrichis d'un contexte exploitable (noms de menaces, horodatages, géolocalisation, adresses IP résolues des ressources Web infectées, hachages, popularité, etc.) répondant aux questions « qui, quoi, où, quand » afin d'identifier les adversaires, de prendre des décisions rapides et d'agir

### Kaspersky APT Intelligence Reporting

Offre un accès unique aux enquêtes et découvertes de Kaspersky, y compris des données techniques complètes sur chaque APT au fur et à mesure de sa découverte, ainsi que sur des menaces qui ne seront jamais rendues publiques

Les rapports offrent des informations faciles à comprendre et adaptées aux cadres dirigeants, ainsi que des descriptions techniques détaillées des APT et des règles YARA et IoC correspondants, afin de fournir aux chercheurs en sécurité, aux analystes de programmes malveillants, aux ingénieurs en sécurité, aux analystes de la sécurité des réseaux et aux chercheurs d'APT des données exploitables permettant une réponse rapide et précise aux menaces

### Rapports de Kaspersky Threat Intelligence sur les menaces industrielles

Fournit des données d'analyse et permet de prendre conscience des campagnes malveillantes ciblant les entreprises industrielles. Il fournit également des informations sur les vulnérabilités détectées dans les systèmes de contrôle industriel les plus courants et les technologies sous-jacentes

Les rapports incluent de nouvelles campagnes d'attaques APT et de gros volumes ciblant les organisations industrielles, des changements considérables dans le paysage des menaces ICS, des vulnérabilités récemment découvertes et des recommandations exploitables visant à atténuer ces menaces, y compris des informations régionales, nationales et sectorielles

### Kaspersky Crimeware Intelligence Reporting

Permet aux organisations d'étayer leurs stratégies défensives en fournissant des informations pertinentes sur les campagnes de programmes malveillants et les attaques visant les institutions financières, ainsi que des informations sur les outils de crimewares utilisés pour attaquer les banques, les entreprises de traitement des paiements et les infrastructures qui leur sont propres

Fournit des descriptions détaillées des programmes malveillants populaires, répandus et très médiatisés, des informations sur les campagnes de programmes malveillants dangereux et répandus, ainsi que des notes de recherche et des avertissements préalables, y compris des informations sur les menaces nouvelles et récentes en matière de programmes malveillants

## TI sur mesure pour votre équipe de sécurité

### Kaspersky Ask the Analyst

Vous permet de vous faire conseiller et d'obtenir des informations au cas par cas par les chercheurs de Kaspersky sur des menaces particulières auxquelles vous êtes confronté ou qui vous intéressent

Adapte les puissantes capacités de Threat Intelligence et de recherche sur les menaces à vos besoins particuliers, vous permettant ainsi de mettre en place des défenses résilientes contre les menaces visant votre organisation

### Kaspersky Digital Footprint Intelligence

Aide vos analystes de sécurité à explorer la façon dont un acteur malveillant perçoit les ressources de votre organisation, à découvrir les vecteurs d'attaque potentiels dont il dispose et à ajuster vos défenses en conséquence

Dresse un aperçu complet de votre situation sur le plan de la sécurité, identifie les failles susceptibles d'être exploitées et découvrent les preuves d'attaques passées, actuelles et prévues

Peut être combiné pour former une solution unique avec le service de démontage Kaspersky Takedown Service

### Kaspersky Takedown Service

La gestion des démantèlements de domaines malveillants et de phishing utilisés pour pirater votre organisation et vos marques étant un processus complexe nécessitant de l'expertise et du temps, le service permet d'atténuer rapidement les menaces posées par ces domaines avant qu'aucun dommage ne puisse être causé

## Couverture des scénarios de sécurité

Scénarios de sécurité — Kaspersky Threat Intelligence

| Prévention | Détection | Enquête | Réponse | Reporting stratégique |
|---|---|---|---|---|
| Kaspersky Threat Data Feeds | Kaspersky Threat Data Feeds<br>Kaspersky CyberTrace<br>Kaspersky Ask the Analyst | Kaspersky Threat Lookup<br>Kaspersky Research Sandbox<br>Kaspersky Threat Attribution Engine<br>Kaspersky CyberTrace<br>Kaspersky APT Intelligence Reporting<br>TTP de Kaspersky Crimeware Intelligence Reporting<br>TTP de Kaspersky ICS Reporting<br>Kaspersky Ask the Analyst | Kaspersky Takedown Service | Kaspersky Digital Footprint Intelligence<br>Résumés analytiques de Kaspersky APT Intelligence Reporting<br>Résumés analytiques de Kaspersky Financial Threat Intelligence Reporting<br>Kaspersky ICS Rapports personnalisés |

## Pourquoi Kaspersky Threat Intelligence ?

- Un large éventail de sources de données fournissant des informations sur les menaces actuelles dans le monde entier, y compris un inventaire des fichiers malveillants détectés par Kaspersky depuis plus de 25 ans
- Un accès direct aux informations techniques, tactiques, opérationnelles et stratégiques fournies par notre équipe de chercheurs et d'analystes de renommée mondiale
- Plus de 20 types de flux de données sur les menaces ; une sandbox développée en interne qui détecte les menaces sophistiquées et évasives ; et un moteur d'attribution des menaces qui fournit des informations détaillées sur les acteurs des menaces, nécessaires à la recherche des menaces APT
- Une équipe dédiée d'experts en cybersécurité industrielle
- Formation spécifique pour le personnel chargé de la sécurité informatique
- Contributeur principal au programme de protection active de Microsoft pour la recherche de vulnérabilités

Kaspersky Threat Intelligence

En savoir plus

www.kaspersky.fr