



Kaspersky Ask the Analyst

Kaspersky Ask the Analyst

Recherche continue sur les menaces

permet à Kaspersky de découvrir, d'infiltrer, et de surveiller les communautés fermées et les forums obscurs du monde entier fréquentés par des adversaires et des cybercriminels. Nos analystes tirent parti de cet accès pour détecter et étudier de manière proactive les menaces les plus graves et les plus connues ainsi que les menaces conçues pour cibler des organisations particulières.

Les cybercriminels développent constamment des moyens complexes d'attaquer les entreprises. Le paysage actuel des menaces, volatile et en pleine expansion, présente des fonctionnalités de plus en plus agiles en matière de cybercriminalité. Les organisations sont confrontées à des incidents complexes causés par des attaques sans programme malveillant, des attaques sans fichier, des attaques hors sol, des exploits de type zero-day ainsi que des combinaisons de tous ces éléments constitutifs des menaces complexes, des APT et d'attaques ciblées.



À une époque marquée par des cyberattaques dévastatrices ciblant les entreprises, les professionnels de la cybersécurité sont plus importants que jamais, mais il n'est pas facile de les trouver ni de les retenir. Même si vous disposez d'une équipe de cybersécurité bien établie, vous ne pouvez pas toujours attendre de vos experts qu'ils mènent seuls la guerre contre les menaces complexes. **Ils doivent pouvoir faire appel à l'aide de tiers experts.** Une expertise externe permet d'éclairer les voies probables d'attaques complexes et d'APT, et fournir des **conseils exploitables sur la manière la plus déterminante de les éliminer.**

Livrables de Ask the Analyst

(Abonnement unifié sur demande)



Le service **Kaspersky Ask the Analyst** étend notre portefeuille de Threat Intelligence, vous permettant de demander des conseils et des informations sur des menaces spécifiques auxquelles vous êtes confronté ou qui vous intéressent. Ce service adapte les puissantes capacités de recherche sur les menaces et de Threat Intelligence de Kaspersky à vos besoins particuliers, vous permettant ainsi de mettre en place des défenses résilientes contre les menaces visant votre organisation.



APT et crimeware

Informations supplémentaires sur les rapports publiés et les recherches en cours (en plus du service APT ou Crimeware Intelligence Reporting)¹



Analyse des programmes malveillants

- Analyse d'échantillons des programmes malveillants
- Recommandations concernant d'autres mesures correctives



Descriptions des menaces, des vulnérabilités et des IoC connexes

- Description générale d'une famille particulière de programmes malveillants
- Contexte supplémentaire pour les menaces (hachages associés, URLs, CnCs, etc.)
- Informations sur une vulnérabilité particulière (son degré de criticité et les mécanismes de protection correspondants dans les produits Kaspersky)



Renseignements sur le Dark Web ²

- Recherche sur le Dark Web d'artefacts particuliers, d'adresses IP, de noms de domaine, de noms de fichiers, d'emails, de liens ou d'images.
- Recherche et analyse d'informations



Requêtes liées aux ICS

- Informations supplémentaires sur les rapports publiés
- Information sur la vulnérabilité des ICS
- Statistiques de menaces ICS et tendances par zone géographique / secteur
- Information d'analyse des programmes malveillants ICS sur les réglementations ou les normes

¹ Disponible uniquement pour les clients ayant un rapport actif APT et/ou Crimeware Intelligence.

² Déjà inclus dans l'abonnement Kaspersky Digital Footprint Intelligence

Comment ça fonctionne ?

Avantages du service



Renforcement de votre expertise

Profitez d'un accès sur demande à des experts du secteur sans avoir à chercher ni à investir dans le recrutement de spécialistes à plein temps difficiles à trouver



Accélération des enquêtes

Priorisez efficacement les incidents et définissez-en la portée en fonction d'informations contextuelles détaillées et adaptées



Réponse rapide

Répondez rapidement aux menaces et aux vulnérabilités en utilisant nos conseils pour bloquer les attaques via des vecteurs connus.

Kaspersky Ask the Analyst peut être acheté séparément ou en complément de l'un de nos services de Threat Intelligence.

Vous pouvez envoyer vos demandes via [Kaspersky Company Account](#), notre portail de support pour les entreprises clientes. Nous vous répondrons par email, mais en cas de besoin et avec votre accord, nous pouvons organiser une conférence téléphonique et/ou une session de partage d'écran. Une fois que votre demande est acceptée, vous serez informé du délai estimé pour sa prise en charge.

Cas d'usage des services :



Clarifier tout détail dans les rapports de Threat Intelligence publiés précédemment



Obtenir des renseignements supplémentaires pour les IoC déjà fournis



Obtenir des détails sur les vulnérabilités et des recommandations sur la manière de se protéger contre leur exploitation



Obtenir des détails supplémentaires sur les activités particulières du Dark Web qui vous intéressent



Obtenir un rapport général sur la famille de programmes malveillants comprenant le comportement du programme malveillant, son incidence potentielle et des détails relatifs à toute activité connexe observée par Kaspersky



Prioriser efficacement les alertes/incidents à l'aide de renseignements contextuels détaillés et d'une catégorisation des IoC connexes fournis par le biais de rapports succincts



Demander de l'aide pour déterminer si l'activité inhabituelle détectée est liée à une APT ou à un acteur de crimeware



Envoyer des fichiers de logiciels malveillants pour une analyse complète afin de comprendre le comportement et la fonctionnalité du ou des échantillons fournis

Élargissement de vos connaissances et de vos ressources

Kaspersky Ask the Analyst vous donne accès à un groupe restreint 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 Ask the Analyst

[En savoir plus](#)

www.kaspersky.fr

© 2022 AO Kaspersky Lab.
Les marques déposées et les marques de service sont la
propriété de leurs détenteurs respectifs.