# Services de Threat Hunting de Kaspersky Lab

www.kaspersky.fr
#truecybersecurity

# Services de Threat Hunting de Kaspersky Lab

Dans tous les secteurs, les équipes de sécurité travaillent d'arrache-pied pour concevoir des systèmes qui protègent intégralement contre des cybermenaces évoluant rapidement. Cependant, face aux incidents de cybersécurité, la plupart d'entre elles adoptent une approche fondée sur les alertes et n'interviennent qu'une fois que l'incident est survenu. Une récente étude a révélé qu'un grand nombre d'incidents de sécurité passaient encore inaperçus. Ces menaces échappent aux radars, donnant littéralement aux entreprises un faux sentiment de sécurité. Par conséquent, elles sont de plus en plus nombreuses à reconnaître la nécessité de rechercher proactivement les menaces non détectées, mais pourtant actives au sein de leurs infrastructures. Les services de recherche de Kaspersky Lab contribuent à déceler les menaces avancées qui se dissimulent au sein de l'entreprise à l'aide de techniques proactives appliquées par des professionnels hautement expérimentés et qualifiés.

**Avantages du service**

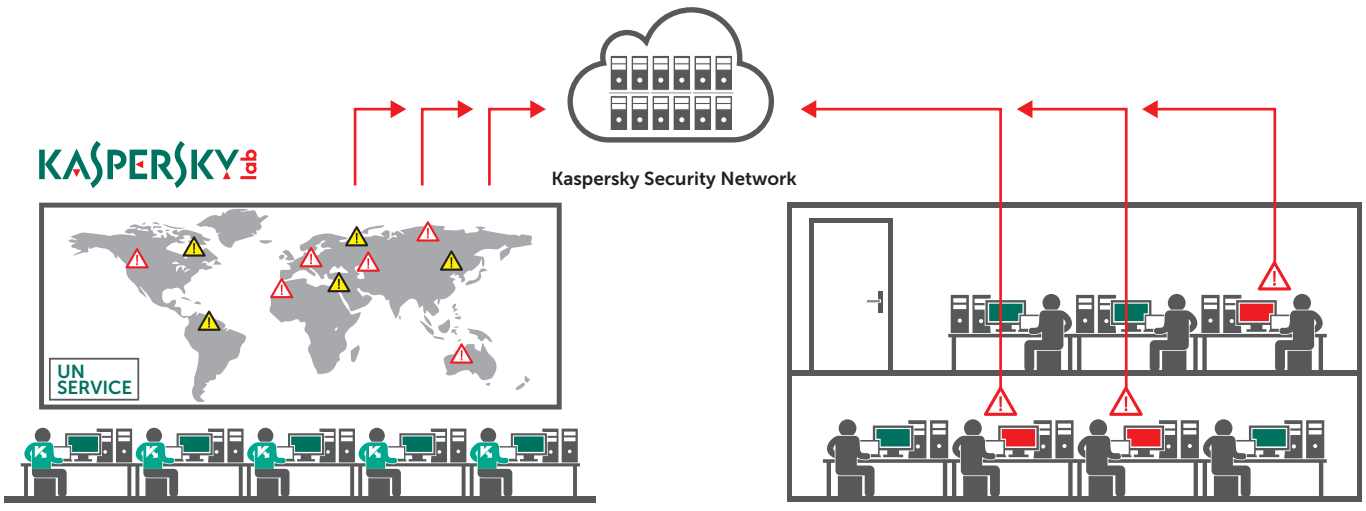
- Une détection rapide et efficace pour une atténuation et une résolution encore plus rapides et plus efficaces
- Absence de faux positifs synonymes de perte de temps grâce à une identification et à un classement clairs et immédiats de toute activité suspecte
- Une réduction du coût total relatif à la sécurité. Aucune nécessité de recruter et de former tout un tas de spécialistes internes
- La certitude rassurante d'être protégé en permanence, même contre les menaces d'origine malveillante les plus complexes et les plus innovantes
- Des informations sur les cybercriminels, sur leurs mobiles, leurs méthodes et leurs outils, ainsi que sur les dommages éventuels qu'ils pourraient provoquer, en vue de l'élaboration d'une stratégie de protection efficace et parfaitement étayée

## Kaspersky Managed Protection

Le service Kaspersky Managed Protection est un service entièrement géré qui offre aux utilisateurs de Kaspersky Endpoint Security et de la plate-forme Kaspersky Anti Targeted Attack un éventail unique de mesures techniques avancées pour détecter et prévenir les attaques ciblant leur entreprise. Ce service inclut un contrôle 24 h/24, 7 j/7 par des experts de Kaspersky Lab et une analyse constante des données de cybermenaces, offrant une détection en temps réel des campagnes de cyberespions et de cybercriminels – aussi bien nouveaux que notoires – visant les systèmes d'information critiques.

## Les points forts du service

- Un niveau constamment élevé de protection contre les attaques ciblées et les programmes malveillants, avec une équipe dédiée d'experts de Kaspersky Lab hautement qualifiés qui s'appuient sur une veille continue des menaces pour assurer une surveillance et une assistance 24 h/24, 7 j/7.
- La détection précise et opportune des attaques d'origine non malveillante, des attaques impliquant des outils jusqu'alors inconnus ou des attaques exploitant des vulnérabilités de type « zero-day »
- Une protection immédiate contre toute menace détectée grâce à des mises à jour automatiques des bases de données antivirus
- L'analyse rétrospective des incidents et la recherche des menaces, et notamment des méthodes et des technologies utilisées par les cybercriminels contre votre entreprise
- Une approche intégrée. Kaspersky Lab offre tous les services et technologies nécessaires à la mise en œuvre d'un cycle complet de protection contre les attaques ciblées : Préparation – Détection-Investigation – Analyse de données – Protection automatisée.




Centre de contrôle

* Pour les infrastructures isolées : Kaspersky Private Security Network

# Détection des attaques ciblées

Les experts de Kaspersky Lab proposent un service proactif de détection des attaques ciblées afin de véritablement protéger vos ressources.

Grâce à ce service, vous pourrez identifier les activités de cybercriminalité et de cyberespionnage à l'œuvre au sein de votre réseau, comprendre les mobiles et les sources potentielles de ces incidents, et planifier efficacement des mesures d'atténuation pour vous prémunir contre toute attaque similaire à l'avenir. Si vous craignez des attaques visant votre secteur, si vous avez constaté des comportements potentiellement suspects au sein de vos systèmes ou si votre entreprise est tout simplement consciente des avantages qu'elle peut tirer de contrôles préventifs réguliers, faites appel aux services Kaspersky Targeted Attack Discovery. Vous saurez ainsi :

- Si vous êtes en train de subir une attaque et, si oui, quelles en sont les caractéristiques et qui en est l'auteur
- En quoi cette attaque affecte vos systèmes et quelles sont les possibilités qui s'offrent à vous
- Comment éviter au mieux d'autres attaques

## Comment fonctionne le service

Nos experts indépendants mondialement reconnus identifieront et analyseront tous les incidents, menaces APT et attaques de cybercriminalité et de cyberespionnage affectant votre réseau. Ils vous aideront à repérer les éventuelles activités malveillantes, à comprendre quelles peuvent être les sources des incidents et à planifier les mesures correctives les plus efficaces.

Notre approche consiste à :

- Analyser les sources d'informations sur les menaces afin de comprendre le paysage de menaces propre à votre entreprise
- Étudier en détail votre infrastructure informatique et vos données (telles que les fichiers journaux) afin de repérer d'éventuels signes de compromission
- Analyser vos connexions réseau sortantes à la recherche d'une quelconque activité suspecte
- Découvrir les sources probables de l'attaque et d'autres systèmes susceptibles d'être compromis

## Les résultats

Nos conclusions sont regroupées dans un rapport détaillé incluant :

**Nos découvertes générales** : confirmation de l'existence ou de l'absence de signes de compromission dans votre réseau

**Une analyse approfondie** : analyse des données sur les menaces recueillies et des indicateurs de compromission mis en évidence

**Une description détaillée** : description des vulnérabilités exploitées, des sources potentielles de l'attaque et des composantes du réseau affectées

**Les mesures correctives préconisées** : mesures suggérées pour atténuer les répercussions de l'incident détecté et protéger vos ressources contre des attaques similaires à l'avenir

## Services complémentaires

Vous pouvez également demander à nos experts d'analyser les symptômes d'un incident, de réaliser un cyberdiagnostic approfondi de certains systèmes, d'identifier un programme malveillant binaire (le cas échéant) ou encore d'analyser les programmes malveillants. Ces services optionnels donnent lieu à des rapports distincts contenant des recommandations supplémentaires en matière de mesures correctives.

Nous pouvons par ailleurs, sur demande, déployer la **plate-forme Kaspersky Anti Targeted Attack (KATA)** sur votre réseau, de façon permanente ou à titre de démonstration. Cette plate-forme combine les technologies les plus récentes à des solutions d'analyse mondiales dans le but de détecter des attaques ciblées, d'y répondre rapidement et de les contrer à toutes les étapes du cycle de vie de votre système.

**À propos du service**

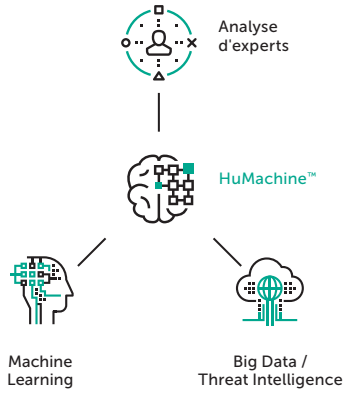
Le service Kaspersky Targeted Attack Discovery se compose de plusieurs activités, à savoir :

**Collecte et analyse d'informations de Threat Intelligence.** L'objectif consiste à obtenir un instantané de votre surface d'attaque, c'est-à-dire des menaces et attaques de cybercriminalité et de cyberespionnage visant potentiellement ou activement vos ressources. Nous puiserons dans les sources d'informations externes comme internes, y compris les communautés souterraines de fraudeurs et les systèmes de surveillance internes de Kaspersky Lab. L'analyse de ces informations nous permettra par exemple d'identifier les faiblesses de votre infrastructure qui risquent fortement d'intéresser les cybercriminels, ou encore les comptes compromis.

**Collecte de données sur place et réponse rapide aux incidents.** Parallèlement à la surveillance des menaces réalisée dans nos propres laboratoires, les experts de Kaspersky Lab collecteront sur place des artefacts réseau et système, ainsi que toutes les informations SIEM disponibles. Nous pourrons également effectuer une rapide évaluation des vulnérabilités afin de mettre en évidence les failles de sécurité les plus critiques et de les corriger sans attendre. Au cas où un incident se serait déjà produit, nous réunirons des éléments de preuve pour procéder à une investigation. À ce stade, nous vous exposerons les mesures correctives à court terme que nous préconisons.

**Analyse de données.** Pour nous permettre de comprendre exactement ce qui se passe dans votre système, les artefacts réseau et système collectés seront analysés en laboratoire au moyen de la base de connaissances Kaspersky Lab sur les indicateurs de compromission, des listes noires de serveurs C&C, des technologies de sandbox, etc. Si, à cette étape, nous identifions par exemple un nouveau programme malveillant, nous vous conseillerons et vous fournirons les bons outils (c'est-à-dire les règles Yara) pour le détecter immédiatement. Nous resterons en contact tout au long du processus et travaillerons à distance sur vos systèmes le cas échéant.

**Création de rapports.** Enfin, nous rédigerons un rapport formel exposant nos résultats sur la détection d'attaques ciblées et les mesures correctives que nous préconisons.




Solutions de cybersécurité de
Kaspersky Lab pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

**www.kaspersky.fr**