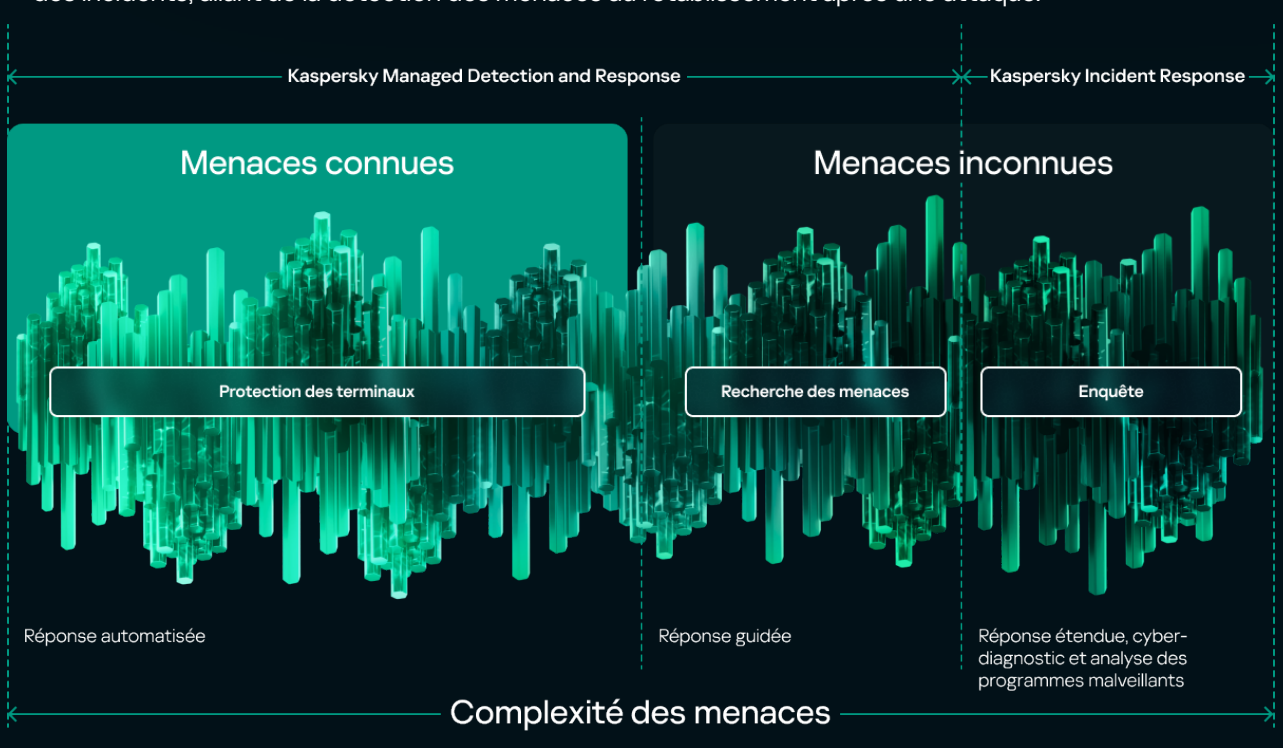
Approche holistique en matière de cybersécurité : Analyse du MDR et de la réponse aux incidents pour l'année 2022

Avec l'évolution des technologies informatiques, les risques de cyberattaques au sein des organisations vont s'accroître. Les données des rapports Kaspersky Managed Detection and Response (MDR) et Kaspersky Incident Response de 2022 confirment que les entreprises subissent une pression de plus en plus forte. Dans ces rapports, les experts Kaspersky partagent des statistiques et des informations obtenues grâce à notre service MDR et lors d'enquêtes sur des incidents de sécurité.

Les services Kaspersky MDR et Kaspersky Incident Response couvrent l'ensemble du cycle de gestion des incidents, allant de la détection des menaces au rétablissement après une attaque.



Grâce à Kaspersky MDR, vous pouvez détecter les menaces durant toutes les phases d'attaque et assurer une protection managée de votre infrastructure informatique 24h/24 et 7j/7 .

Grâce à Kaspersky Incident Response, vous pouvez répondre rapidement et efficacement aux incidents de sécurité informatique, dresser un tableau complet des attaques et en éliminer les conséquences.

En cas d'une utilisation combinée, vous pouvez analyser en détails un incident particulier afin d'obtenir une image complète des événements et d'appliquer par la suite une série de mesures de réponse étendues. Il s'agit généralement d'incidents critiques de haut niveau liés à une implication directe de l'ennemi et ayant une incidence négative importante sur les activités de l'entreprise.

La synergie entre les services Kaspersky MDR et Kaspersky Incident Response est très efficace. Dans ce cas, la sécurité informatique est gérée par une équipe d'experts qui surveillent votre infrastructure informatique et sont prêts à intervenir 24h/24 et 7j/7.

Vous pouvez utiliser les services Kaspersky MDR et Kaspersky Incident Response en tandem ou en tant que services distincts.

Les secteurs les plus attaqués

Les attaques en bref

Principales causes d'incidents de gravité élevée en 2022

Red team

Programme malveillant

Menaces persistantes avancées (APT)

Méthodes de base pour infiltrer l'infrastructure d'une organisation

Exploitation d'applications destinées au public

Comptes compromis

E-mails malveillants

Conséquences d'attaques les plus courantes

Chiffrement des fichiers

Fuites de données

Présence prolongée dans le système

Les outils de prédilection des pirates informatiques

PsExec

PowerShell

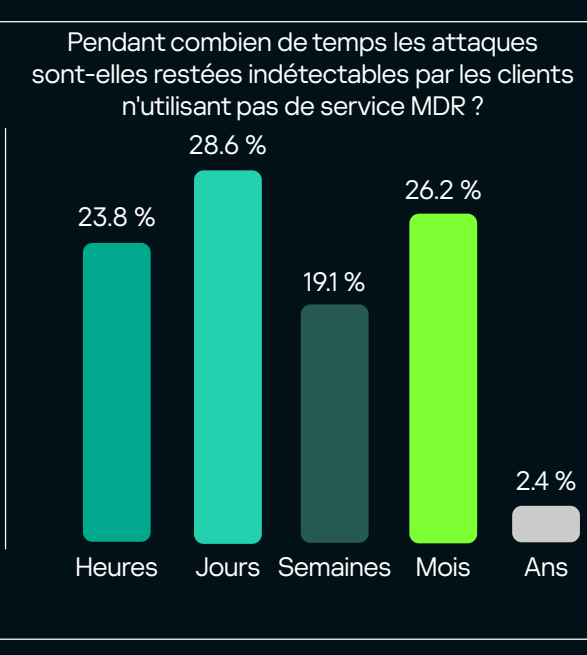
Cobalt Strike

Mimikatz

Kaspersky MDR détecte **plus de trois incidents critiques par jour**

Temps de détection des incidents

Les actions malveillantes des utilisateurs peuvent rester inaperçues pendant **des jours, des mois, voire des années** dans les organisations qui ne mettent pas en œuvre de système MDR



Le service MDR détecte automatiquement les menaces éventuelles avant qu'une attaque potentielle ne puisse causer de graves dommages

Équipes d'experts

Le **centre des opérations de sécurité (SOC)** de Kaspersky assure une surveillance 24h/24 et 7j/7 ainsi que des services d'analyse continue des données en vue d'une détection rapide et précise des attaques, de services de réponse instrumentale et de recommandations.

Depuis plus de dix ans, l'équipe **Global Emergency and Response Team (GERT) de Kaspersky**, composée d'experts certifiés au niveau international, enquête sur des incidents de cybersécurité complexes pour des organisations de divers secteurs et marchés.

Téléchargez nos rapports MDR et Incident Response, et obtenez les recommandations de Kaspersky sur les différentes façons de minimiser les risques de cybersécurité

Télécharger le rapport MDR

Télécharger le rapport Incident Response

kaspersky

www.kaspersky.fr