kaspersky

Kaspersky
Managed Detection
and Response

Nous arrêtons les incidents avant qu'ils ne paralysent votre activité

Renforcez votre résilience en matière de cybersécurité grâce à une protection gérée 24 h/24, 7 j/7

Le travail à distance, le développement rapide des échanges d'informations numériques, le fossé grandissant entre les compétences et le nombre croissant de cybermenaces capables de contourner les contrôles automatisés traditionnels font peser une pression constante sur les entreprises de toutes tailles. Dans ce contexte, il est essentiel de réagir rapidement et efficacement à chaque incident.

Kaspersky Managed Detection and Response est un service géré par des experts qui offre une surveillance, une détection, une analyse et une réponse rapide 24 h/24 aux cyberattaques complexes, renforçant vos contrôles de sécurité existants grâce à une détection humaine et à une Threat Intelligence mondiale. Ce service renforce immédiatement votre niveau de sécurité informatique et opérationnelle, quel que soit le secteur d'activité ou la taille de votre organisation.

Principaux avantages

Une protection avancée permanente sur l'ensemble de votre surface d'attaque (terminaux, réseau, cloud et au-delà) dès le premier jour.

Un SOC prêt à l'emploi, disponible 24 h/24 et 7 j/7, avec une équipe mondiale d'experts, qui vous évite d'avoir à mettre en place, à doter en personnel et à maintenir vos propres opérations de sécurité en interne.

Une charge de travail réduite pour votre équipe de sécurité interne, puisque vous nous confiez la surveillance, le triage et les enquêtes.

Une sécurité axée sur les résultats qui combine savoir-faire humain, Threat Intelligence et IA pour prévenir les incidents avant qu'ils n'aient un impact sur votre activité.

Aperçu des cybermenaces actuelles[1]

1 Vecteurs d'attaque initiaux

31 % comptes valides

13 % relation de confiance

39 % exploitation d'une application exposée sur Internet

2 Déplacez-vous et accomplissez vos tâches

Les pirates utilisent souvent des outils légitimes (comme Mimikatz, PsExec ou SoftPerfect Network Scanner) dans des infrastructures qui ne disposent pas de contrôles adéquats pour la configuration du système.

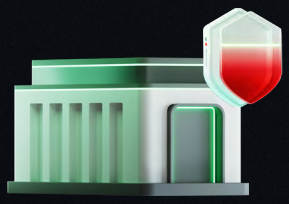
3 Impact

42 % fichiers chiffrés

17 % fuites de données

11 % persistance installée pour un impact ultérieur

Les données montrent que les pirates repassent souvent à l'action après une attaque réussie.



Durée de l'attaque

Rapide **45 %** — jusqu'à 1 jour

Moyenne **20 %** — 13 jours

Longue durée **35 %** — 253 jours

> Kaspersky MDR a détecté et contré efficacement une attaque zero-day qui aurait pu perturber gravement nos opérations.
>
> **Daniel Huerta Santos**
> Responsable de la cybersécurité, gouvernement de l'État de Guanajuato

En savoir plus

1 Rapport Kaspersky MDR et Incident Response

Ce que propose Kaspersky MDR

Protection continue contre les menaces avancées dès le premier jour

Kaspersky MDR s'active en quelques minutes sans infrastructure supplémentaire, grâce à nos analystes SOC et à notre Threat Intelligence, pour offrir une détection multicouche à travers plusieurs domaines. Grâce à des milliards de signaux télémétriques, il permet une recherche proactive des menaces, une enquête sur les causes profondes et une correction complète et rapide, offrant ainsi une protection contre les menaces connues et les menaces zero-day dès le premier jour.

Opérations de sécurité menées par des experts, renforcées par la Threat Intelligence

Avec Kaspersky MDR, vos opérations de sécurité sont gérées par des experts internationaux chevronnés, titulaires de certifications réputées dans le secteur. Leur travail est optimisé par des mécanismes avancés de Threat Intelligence et d'IA intégrés au service, qui enrichissent chaque alerte, accélèrent la détection et réduisent le temps moyen de réponse (MTTR).

Efficacité opérationnelle et prévisibilité des coûts

- Kaspersky MDR élimine la complexité et le coût liés à la mise en place d'un SOC interne de A à Z, une tâche susceptible de grever votre budget et de retarder de plusieurs mois, voire plusieurs années, une amélioration concrète de votre sécurité.
- Si vous disposez déjà de votre propre SOC, le service assure la surveillance 24 h/24, 7 j/7, le triage des alertes et la classification des incidents, ce qui permet à vos analystes de se concentrer sur des tâches stratégiques plus importantes.

Cas d'utilisation

- Protection clé en main 24 h/24, 7 j/7 pour les organisations sans SecOps
- SecOps cogéré pour renforcer les équipes internes chargées de la cybersécurité
- Protection avancée des infrastructures OT
- Protection continue dédiée des systèmes embarqués

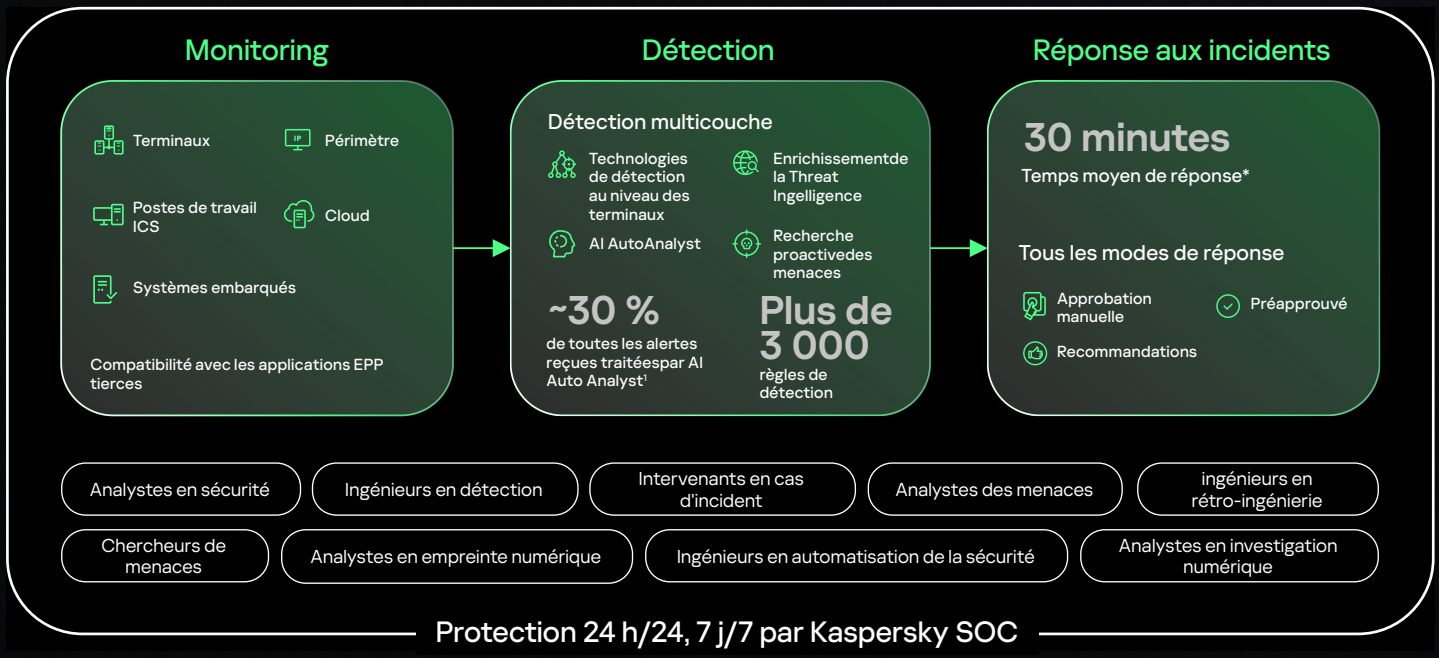
30 minutes
notre temps moyen de réponse [2]

30 %
de toutes les alertes reçues traitées par AI Auto Analyst [1]

jusqu'à 15 minutes
temps que prend l'activation de Kaspersky MDR

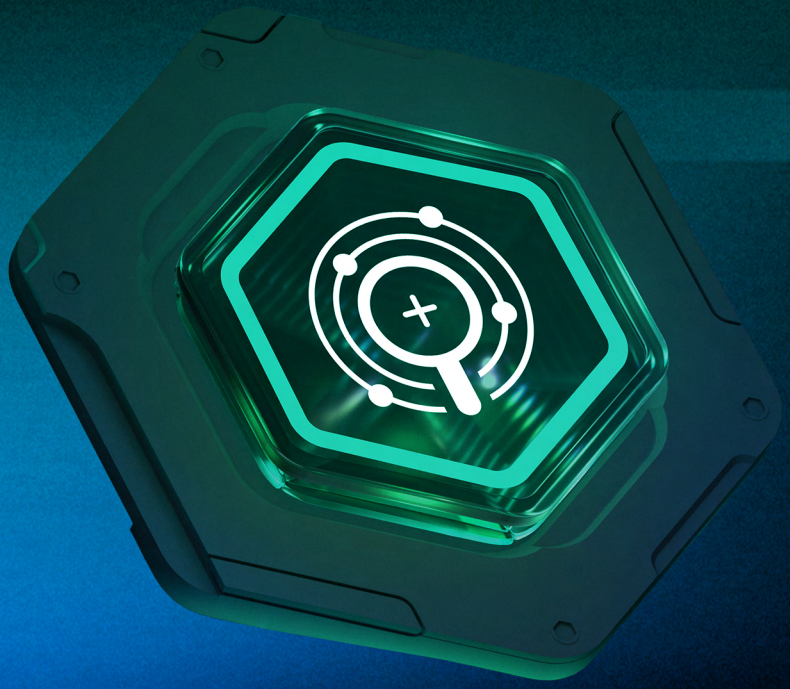
jusqu'à 2 ans
temps qu'il faut pour construire, en interne et à partir de zéro, ses opérations de sécurité.

70 %
des équipes de sécurité ont du mal à suivre le nombre d'alertes générées par leurs outils de sécurité [3]



2 Selon nos rapports annuels d'analystes MDR

3 Portrait du professionnel moderne de la sécurité de l'information, 2024



Kaspersky Managed Detection and Response

Demander une démonstration

www.kaspersky.fr

© 2026 AO Kaspersky Lab.
Les marques déposées et les marques de service sont la propriété de leurs détenteurs respectifs.

#kaspersky
#bringonthefuture