kaspersky

Kaspersky Endpoint Detection and Response

Les entreprises renforcent leurs stratégies de sécurité pour répondre aux menaces avancées et aux cyberattaques modernes. Alors que les terminaux restent des cibles privilégiées pour les cybercriminels, les menaces actuelles déjouent les mesures de sécurité des terminaux traditionnelles, perturbant ainsi les processus stratégiques tout en affectant la productivité et en augmentant les coûts opérationnels.

Les retards sont coûteux

Le lancement d'une récupération une semaine après la détection d'un incident coûte à une entreprise 200 % plus d'argent qu'une réponse immédiate.
Enquête de Kaspersky Lab sur les risques liés à la sécurité informatique pour les entreprises

Kaspersky EDR est un choix tout indiqué pour les entreprises qui souhaitent :

- Automatiser l'identification des menaces et la réponse à celles-ci, sans perturber leurs activités
- Améliorer la visibilité et la détection des menaces sur les terminaux, à l'aide de technologies avancées, incluant le machine learning, le sandboxing, l'analyse des indicateurs de compromission (IoC) et la surveillance des menaces
- Renforcer leur sécurité, en adoptant une solution de réponse aux incidents professionnelle et facile d'utilisation
- Établir des processus unifiés et performants de Threat Hunting, de gestion des incidents et de réponse.

Simplification de la mise en conformité :

Partage en temps réel des informations sur les menaces par le biais de la solution Kaspersky Private Security Network sur site.

- Aucune dépendance vis-à-vis du Cloud et des flux de données sortants, grâce à l'intégration de KPSN.
- Stockage centralisé sur l'environnement de l'entreprise de toutes les données de cyberdiagnostic avec Kaspersky EDR.

Recherche active des menaces :

En associant le service Kaspersky Managed Protection de Threat Hunting actif 24 heures sur 24, 7 jours sur 7 au déploiement de Kaspersky EDR, les entreprises obtiennent un accès à un réseau mondial de recherche sur les menaces. En outre, les chercheurs de Kaspersky Lab spécialisés dans les menaces peuvent :

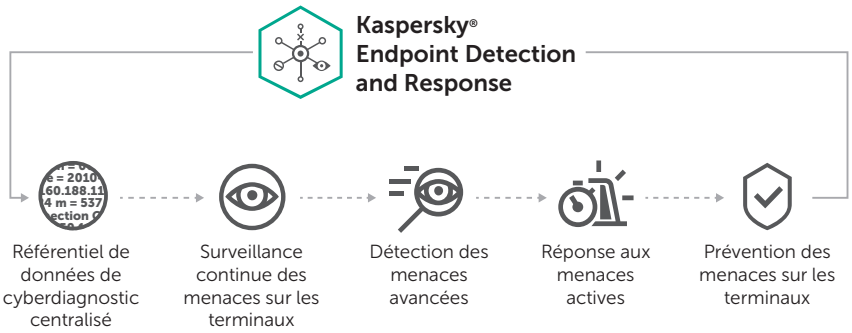
- Examiner les données collectées dans l'environnement de l'entreprise ;
- Avertir rapidement l'équipe de sécurité de l'entreprise en cas de détection d'une activité malveillante ;
- Fournir des conseils en matière de réponse et de résolution.

Points forts

Réponse adaptable aux menaces
Kaspersky EDR inclut un large éventail de réponses automatisées évitant aux entreprises d'utiliser les processus de résolution traditionnels, comme l'effacement et la création de nouvelles images, qui peuvent entraîner des interruptions coûteuses et une perte de productivité.

Threat Hunting proactive
Grâce à une recherche rapide exploitant une base de données centralisée, associée à la recherche d'indicateurs de compromission (IoC), Kaspersky EDR peut radicalement modifier les flux de travail de sécurité. Au lieu d'attendre l'émission d'alertes, votre équipe de sécurité peut traquer activement les menaces et analyser les terminaux de manière proactive en vue de détecter les anomalies et failles de sécurité.

Interface Web intuitive
L'interface sur navigateur facile d'utilisation de Kaspersky EDR procure au personnel de sécurité une visibilité et un contrôle unifiés des opérations de détection, d'enquête, de prévention, d'émission d'alertes et de génération de rapports. Grâce à la surveillance et au contrôle d'un large éventail de fonctions sur une même interface, votre équipe de sécurité peut effectuer les tâches de sécurité plus efficacement, sans avoir à composer avec plusieurs outils et consoles.



Détection et confinement rapides des menaces avancées

Kaspersky Endpoint Detection and Response (Kaspersky EDR) optimise les processus de détection, d'enquête et de réponse des entreprises :
- Augmentation de la visibilité sur les terminaux
- Automatisation des tâches de réponse manuelles
- Amélioration des fonctionnalités d'enquête

... et est compatible avec les solutions de sécurité des terminaux traditionnelles.

Kaspersky EDR aide l'équipe de sécurité et les responsables de la réponse les moins expérimentés à décortiquer un terminal avec la précision d'un spécialiste en cyberréponse. Avec Kaspersky EDR, votre entreprise peut :
- SURVEILLER efficacement les menaces ne se limitant pas aux programmes malveillants ;
- DÉTECTER précisément les menaces à l'aide de technologies avancées ;
- AGRÉGER de manière centralisée les données de cyberdiagnostic ;
- RÉPONDRE rapidement aux attaques ;
- EMPÊCHER les actions malveillantes issues des menaces détectées...

... le tout sur une interface Web performante, simplifiant les opérations d'enquête et de réaction.

Cas d'utilisation :

- Recherche proactive des preuves d'intrusion, notamment des indicateurs de compromission (IoC), sur l'ensemble d'un réseau, le tout en temps réel
- Détection et résolution rapide des intrusions, avant qu'elles ne causent des interruptions et des dégâts majeurs
- Intégration à un système SIEM, dans le but de mettre les alertes et les activités en corrélation sur le terminal
- Validation des alertes et des incidents potentiels détectés par d'autres solutions de sécurité
- Enquête rapide et gestion centralisée des incidents, sur des milliers de terminaux, par le biais de flux de travail parfaitement intégrés
- Automatisation des opérations de routine, afin de réduire les tâches manuelles, de libérer des ressources et d'éviter la « surcharge d'alertes ».

Sécurité avancée des terminaux

Kaspersky Lab prouve son leadership continuel en matière de protection des terminaux avec l'association de cinq éléments stratégiques dans une même solution :

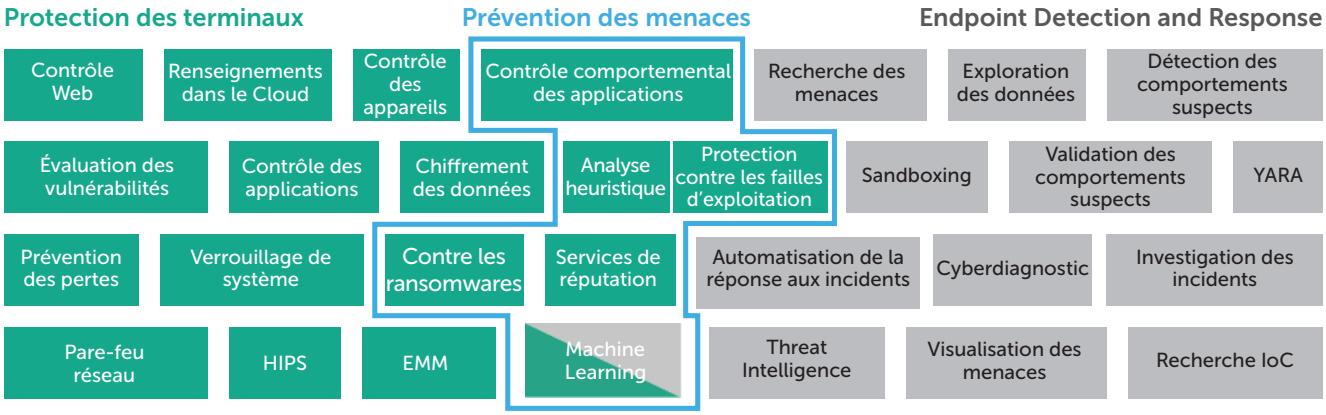
- Un moteur de protection contre les programmes malveillants de nouvelle génération intégrant le machine learning
- La solution Endpoint Detection and Response (Kaspersky EDR)
- Le service de Threat Hunting Kaspersky Managed Protection, actif 24 heures sur 24, 7 jours sur 7
- L'accès à des informations en temps réel sur les menaces avec Kaspersky Security Network
- Des contrôles de terminaux avancés (appareils/Web/applications, chiffrement, etc.).

Renforcement de la sécurité des terminaux traditionnelle

Du fait de sa compatibilité avec un large éventail de produits de sécurité traditionnels de différents fournisseurs, Kaspersky EDR peut également ajouter les éléments suivants à une solution de sécurité des terminaux existante :

- Fonctionnalités de détection et de prévention de nouvelle génération ;
- Processus d'enquête et de réponse centralisés.

... sans obliger l'entreprise à remplacer sa solution de sécurité actuelle.



Analyse d'objets dans un environnement virtuel isolé

Kaspersky EDR comprend une sandbox avancée sur site, qui permet l'extraction automatisée de tout fichier, sur n'importe quel terminal, à des fins d'analyse approfondie. Cette solution fournit un laboratoire d'analyse de virus interne à l'entreprise, sans l'obliger à envoyer des données à l'extérieur de son réseau.

Détection avancée offerte par le machine learning

Le moteur de machine learning de Kaspersky EDR, l'analyseur d'attaques ciblées (TAA, Targeted Attack Analyzer), établit une base de référence sur le comportement des terminaux. Il est ainsi possible d'utiliser un registre historique pour découvrir la genèse d'une violation. Par ailleurs, la mise en corrélation des données de cyberdiagnostic, des informations sur les menaces et des résultats du moteur de sécurité contribue à la détection des anomalies.

Avantages commerciaux dans toute l'entreprise :

Réduction des coûts

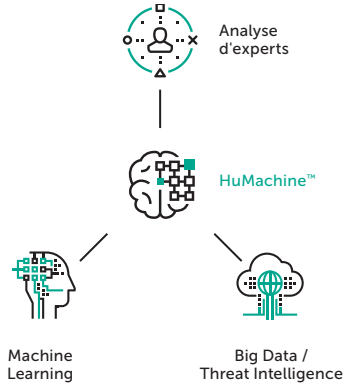
- Automatisation des tâches manuelles pendant la détection des menaces et la réponse
- Accélération du confinement des menaces, pour économiser de l'argent et des ressources
- Allègement de la charge de travail du personnel, lui permettant de se consacrer à d'autres tâches
- Réduction des interruptions d'activités pendant les enquêtes

Accélération du retour sur investissement

- Intégration de flux de travail efficaces
- Réduction du temps nécessaire à l'identification et au blocage des menaces
- Simplification de la mise en conformité (pour les normes PCI DSS et autres réglementations) par l'application de journaux de terminaux, l'examen des alertes et la documentation des résultats des enquêtes

Réduction des risques d'attaque

- Élimination des failles de sécurité et réduction des temps d'arrêt dus aux attaques
- Simplification de l'analyse des menaces et de la réponse aux incidents
- Renforcement de la sécurité existante à l'aide de la validation des menaces



Solutions de sécurité Kaspersky 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