kaspersky BRING ON THE FUTURE

Kaspersky EDR Optimum

Réduire le risque que votre entreprise subisse des menaces ciblées et sophistiquées n'est plus un luxe mais une nécessité. Notre ambition est de rendre ce processus simple et économique, tout en assurant la sécurité de chacun.

Kaspersky Endpoint Detection and Response (EDR) Optimum est un outil automatisé et centralisé qui répond aux attaques avancées et ciblées de manière à soulager votre personnel et vos ressources informatiques.

Avantages

- Réduit le risque d'être victime d'une attaque ciblée ou avancée
- Offre une visibilité approfondie sur vos terminaux
- Détecte les menaces complexes
- Fournit à votre équipe de sécurité informatique les outils et informations nécessaires à l'analyse des causes profondes
- Permet de créer et d'importer des IoC et d'analyser des hôtes à cet effet
- Intègre une multitude d'options de réponses automatisées et par simple clic
- Peu exigeant et efficace
- Est hautement automatisé, mais laisse la place nécessaire au facteur humain et à l'expertise humaine

Les problèmes actuellement rencontrés par les entreprises

Les menaces sophistiquées sont devenues monnaie courante

Les attaques ciblées et sophistiquées sont de plus en plus simples à mener et moins coûteuses. Cela signifie que les États et les grandes entreprises ne sont plus les seules entités potentiellement menacées. Les entreprises qui pensaient autrefois ne pas être concernées par de telles attaques doivent désormais protéger leurs arrières et rechercher une solution de protection adéquate ; **91 %**[1] des entreprises ont subi des cyberattaques au cours d'une même année, et **1 entreprise sur 10**[1] a été touchée par une attaque ciblée.

Le coût moyen d'une attaque ne cesse d'augmenter d'année en année

Les attaques ciblées et sophistiquées ont des conséquences économiques réelles. Actuellement, le coût moyen d'une violation de données s'élève à environ **1,41 million de dollars**[2], tandis que celui d'une infection, par un programme malveillant, d'un terminal dans une entreprise tourne autour de **2,73 millions de dollars**[2]. Ces coûts comprennent l'enquête, les mesures correctives, les indemnisations, les campagnes de presse et toutes les autres mesures nécessaires pour atténuer les conséquences d'une attaque.

En revanche, l'expertise et les outils appropriés permettant d'éviter que de telles attaques ne se produisent ne représentent qu'une infime partie de ces coûts.

Les entreprises disposent de ressources limitées

Le nombre de professionnels formés en sécurité de l'information que vous pouvez embaucher et le temps qu'ils peuvent consacrer à une tâche spécifique ne sont pas illimités. Ce problème est loin d'être nouveau, mais pour espérer le résoudre, encore faut-il agir. L'automatisation des tâches de sécurité constitue l'un des moyens les plus efficaces pour y parvenir. À l'heure actuelle, **2 entreprises sur 3**[3] pâtissent d'un manque de personnel dédié à la sécurité des informations ; et d'après les prévisions, d'ici 2021, **3,5 millions**[4] de postes en cybersécurité seront à pourvoir.

Par ailleurs se pose la question des ressources informatiques nécessaires pour exécuter les solutions de sécurité. Le budget que les entreprises consacrent à leurs besoins informatiques est souvent morcelé. Il convient par conséquent de privilégier des solutions légères, ou dont les coûts sont minimes.

Nos solutions pour y faire face

Kaspersky EDR Optimum a été développé afin de répondre au besoin d'une solution de sécurité de qualité, capable de faire face aux menaces actuelles complexes malgré les ressources limitées. Il est conçu pour détecter les menaces de manière robuste, y répondre de façon proactive, et simplifier les opérations quotidiennes.

1 – Le rapport Kaspersky sur les risques informatiques mondiaux, Kaspersky, 2019
2 – Rapport sur l'économie de la sécurité informatique en 2019, Kaspersky
3 – Étude sur le personnel du secteur de la cybersécurité, (ISC)², 2019
4 – Rapport annuel officiel sur les emplois dans la cybersécurité, Cybersecurity Venture, 2019

Robuste

Pour vous protéger contre une attaque, encore faut-il en avoir connaissance ; c'est pourquoi toute solution EDR digne de ce nom doit disposer de capacités de détection et d'enquête robustes.

Kaspersky EDR Optimum s'appuie sur une multitude de techniques capables de détecter la moindre trace d'une attaque, par exemple :

- Les attaques sans programme malveillant
- Les mouvements latéraux
- Les comportements suspects
- et bien d'autres

Proactif

Détecter une menace n'est pas suffisant : vous devez pouvoir la contrer le plus rapidement possible, aussi bien sur l'hôte infecté que sur les autres hôtes du réseau. Kaspersky EDR Optimum vous permet de répondre aux nouvelles menaces de plusieurs façons :

- Isolement de l'hôte
- Exécution d'une analyse de l'hôte
- Suppression de fichiers (en quarantaine)
- Arrêt de processus
- Empêchement de l'exécution du processus

Pratique

Le temps et les efforts que votre équipe de sécurité consacre à l'analyse des menaces et aux réponses à apporter sont aussi importants que les taux de détection et les techniques de réponse. Avec Kaspersky EDR Optimum, nul besoin d'une expertise poussée, d'une grande équipe ou d'une journée complète de travail pour rester protégé. Il fournit des données détaillées, est hautement automatisé et ménage vos ressources informatiques. Vous bénéficiez ainsi de solides avantages :

Visibilité

- Informations complètes sur les incidents
- Visualisation de la chaîne de frappe
- Historique des incidents et analyse des causes profondes

Automatisation

- Options de réponse d'un simple clic
- Création automatique d'IoC à partir d'un incident (ou importation)
- Recherche d'IoC dans les hôtes et réponse automatisée aux menaces

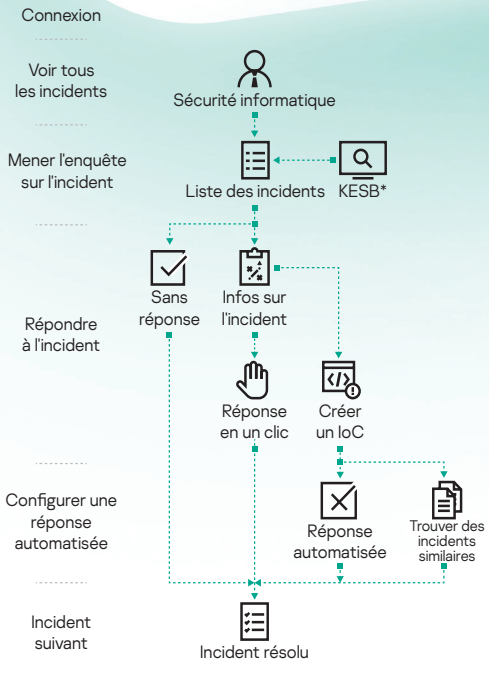
Performance

- Pas de frais supplémentaires
- Intégration avec Kaspersky Endpoint Security
- Contrôle à partir de la console Kaspersky Security Center

Cas d'utilisation

Voici quelques exemples de situations où Kaspersky EDR Optimum est capable de détecter une multitude de menaces, de mener l'enquête à leur sujet et d'y répondre.

Détecter	Enquêter	Répondre
Détection d'un fichier malveillant, placé dans la liste des événements	La visualisation de la chaîne de frappe montre que ce fichier a été déposé par un processus non signé.	Empêcher le processus de s'exécuter d'un simple clic, mettre le fichier déposé en quarantaine.
Détection d'une injection de processus	Les informations complètes de l'incident présentent les détails sur l'hôte, la date de création et de modification du fichier, l'auteur et la signature, etc. Sur la base de ces informations et de la chaîne de frappe, le fichier est considéré comme suspect.	Isoler cet hôte et rechercher des incidents similaires sur d'autres hôtes du réseau.
Détection d'une connexion suspecte	Les données de l'incident révèlent l'adresse avec laquelle la connexion a été établie. La visualisation de la chaîne de frappe associe cette connexion à une modification de la clé de registre ; toutes deux ont été lancées par le même processus.	Isoler cet hôte. Créer un IoC afin de réaliser des recherches périodiques sur d'autres hôtes et configurer une réponse automatisée : mettre le fichier en quarantaine et lancer une analyse de l'hôte.



*Kaspersky Endpoint Security for Business

Comment ça fonctionne ?

Kaspersky EDR Optimum améliore la solution EPP actuelle (Kaspersky Endpoint Security for Business) en y ajoutant une plus grande visibilité, des capacités d'analyse des causes profondes et des réponses automatisées, tout en utilisant le même agent.

Les données sont rassemblées et analysées à partir de ces hôtes, puis les rapports, les informations détaillées sur les incidents et les options de réponse aux incidents sont fournis via la console Kaspersky Security Center.

Les réponses aux incidents peuvent être gérées de façon automatisée ou d'un simple clic. Une réponse automatisée est configurée pour répondre à des incidents similaires sur plusieurs hôtes sans la moindre intervention humaine, et celle-ci est déclenchée après qu'un indicateur de compromission (IoC) créé par l'utilisateur ou importé a été détecté sur ces hôtes.

Nous avons veillé à rendre le fonctionnement de Kaspersky EDR Optimum aussi simple que possible. Une fois le déploiement réalisé, votre équipe informatique aura uniquement besoin de consulter la console de temps à autre, afin de traiter les nouveaux incidents, de procéder à l'analyse des causes profondes et de répondre à ces incidents.

Avec un tel degré d'automatisation et de visibilité, le responsable de la sécurité n'a plus besoin de passer du temps à consulter de grandes quantités de données chaque jour. Il peut à la place se concentrer sur les activités suspectes, en disposant de toutes les informations nécessaires.

Pour en savoir plus sur la façon dont Kaspersky EDR Optimum répond aux cybermenaces tout en ménageant votre équipe et vos ressources de sécurité, rendez-vous sur la page : http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Actualités dédiées aux cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : kaspersky.fr/business
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise

www.kaspersky.fr

Nous sommes reconnus. Nous sommes indépendants. Nous sommes transparents. Nous nous engageons à construire un monde plus sûr où la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/about/transparency

Reconnu.
Transparent.
Indépendant.