Les solutions EDR : vers l'automatisation et la simplification

kaspersky

Plus d'informations sur kaspersky.fr
#bringonthefuture

Introduction

À moins que vous n'ayez passé ces dernières années complètement isolé du reste du monde, vous avez dû faire face à une recrudescence des discours alarmistes au sujet de la croissance exponentielle et de la complexité toujours plus inédite des cybermenaces.

Rien n'est plus vrai. Mais il n'y a rien de nouveau là-dedans. Les cybercriminels mettent au point des mécanismes d'attaque, les fournisseurs développent des solutions de défense, les cybercriminels élaborent des moyens pour les contourner, nous controns ces derniers à l'aide de nouvelles technologies, et le cercle se répète ainsi sans fin. C'est aussi simple que ça.

Vous avez également dû entendre de toutes parts que la technologie de détection et de réponse au niveau des terminaux (EDR) représente désormais une nécessité, et non un luxe.

Et c'est le cas. Mais, comme pour tous les sujets relatifs à la cybersécurité, il faut trouver le juste équilibre. Quelle est la probabilité que votre entreprise soit attaquée, par quelles formes de menaces, et combien de temps, d'argent et de ressources devriez-vous allouer pour lutter contre ces menaces ? Les réponses à ces questions dépendent de la nature, de la taille et de la zone géographique de votre organisation, ainsi que des ressources dont vous disposez.

Alors, est-ce le bon moment pour investir dans une technologie EDR si vous ne l'avez pas déjà fait ? Au cours des dernières semaines, et même des derniers mois, de nombreuses organisations ont dû mettre en place le télétravail pour leurs salariés, au-delà de leur périmètre informatique et de la protection offerte par leur passerelle. Cette situation sans précédent nous a ouvert les yeux sur l'importance du partage sécurisé et continu des informations professionnelles et des canaux de communication, ainsi que sur notre dépendance vis-à-vis de l'efficacité de la sécurité au niveau des terminaux. Les organisations de toutes tailles, quel que soit leur secteur d'activité et leur niveau de compétence en cybersécurité, doivent envisager une détection avancée, une meilleure visibilité et une réponse instantanée aux menaces complexes.

Mais vous devez savoir ce que cela vous apporte, et comment l'exploiter.

Qu'est-ce que la technologie EDR ?

Le terme « Endpoint Threat Detection and Response » (ETDR, Détection et réponse aux menaces au niveau des terminaux) a été inventé en 2013 par Anton Chuvakin (Gartner), et défini comme « les outils principalement axés sur la détection et l'investigation des activités suspectes (et des signes) d'autres problèmes au niveau des hôtes/terminaux ». Le mot « Threat » (menace) a été abandonné plus tard, ETDR devenant ainsi « EDR ».

« Une solution EPP[1] faible détruira la valeur d'un outil EDR »

IDC, Sécurité des terminaux 2020 :
La résurgence de la protection des terminaux et le destin de l'EDR, Doc n° US45794219, 2020

La technologie EDR (Endpoint Detection and Response) est un élément de protection au niveau des terminaux, qui surveille en permanence et apporte une réponse aux menaces avancées au niveaux des terminaux, contrairement aux antivirus (AV) et aux protections contre les programmes malveillants, qui se concentrent essentiellement sur l'arrêt des menaces au cours de la phase de pré-exécution. Bien que la technologie EDR élargisse la gamme des plateformes de protection des terminaux (EPP) « classiques », elle ne les remplace pas. Pour rentabiliser votre investissement dans une technologie EDR, vous devez être sûr de disposer de bonnes bases en matière de protection. Si vous souhaitez consolider vos performances insatisfaisantes en matière de protection des terminaux par le biais de l'achat d'une solution EDR, vous devriez d'abord chercher à mettre à niveau votre EPP.

Tous les produits EDR ont le même objectif : identifier, examiner et répondre plus rapidement aux menaces avancées et complexes. Pour y parvenir, la majorité, voire l'ensemble, des outils suivants sont utilisés :

- Un moteur de détection, qui utilise des techniques telles que l'analyse structurelle basée sur le Machine Learning et le Sandboxing imitatif pour détecter et prévenir les programmes malveillants.
- Un moteur d'analyse en temps réel, qui sonde la mémoire et recherche des schémas comportementaux, ce qui lui permet de détecter les vulnérabilités et de diagnostiquer rapidement les menaces plus complexes auparavant inconnues.
- La Threat Intelligence, dont les renseignements peuvent provenir de différentes sources.
- La visibilité via les terminaux, essentielle pour détecter les activités malveillantes.
- La surveillance et l'enregistrement des données d'évènements en temps réel, et leur utilisation à des fins d'analyse.
- Des outils d'investigation pour examiner les précédentes violations et localiser les éventuelles menaces non identifiées au niveau d'un terminal.
- La réponse aux incidents : la génération d'alertes automatiques et les réponses apportées.
- Le filtrage des incidents, afin de prévenir les « faux positifs » (une surcharge d'alertes inutiles).

Tous les outils EDR ne fonctionnent pas de la même façon. Certains entreprennent une analyse plus approfondie de l'agent, tandis que d'autres se concentrent sur l'infrastructure back-end via une console d'administration. Le calendrier et le périmètre de la collecte des données peuvent varier, tout comme la qualité et les sources de la Threat Intelligence. Par ailleurs, tous les outils disponibles sur le marché ne sont pas nécessairement pertinents pour

1 EPP – Endpoint Protection Platform

vos opérations de cybersécurité. Le Threat hunting, par exemple, requiert des ressources et une expertise spécifique dont la majorité des services informatiques ne dispose pas.

De fait, plutôt que d'évaluer chaque solution EDR par rapport à chacune des fonctionnalités qu'elle offre, il est important d'identifier et de cibler ce dont vous avez réellement besoin. Il n'y a aucun intérêt à payer pour une fonctionnalité dont vous ne vous servirez jamais et qui ajoute une complexité inutile. Cherchez un produit sur lequel vous pouvez compter pour réaliser efficacement le travail à votre place, sans augmenter vos frais ni votre charge de travail, et qui s'intègre parfaitement à votre EPP existante.

Contre quelles menaces luttent les solutions EDR, et comment ?

Indicateurs de compromission (IoC)
Un IoC correspond à un ensemble de données forensiques, qui identifie toute activité malveillante potentielle sur un système ou un réseau, et qui peut se révéler être le fil d'Ariane menant à la détection d'une activité malveillante aux prémisses d'une séquence d'attaque.

De manière générale, une approche multi-niveaux est la meilleure façon de résister aux cybermenaces. Une série de filtres permet ainsi de lutter contre des formes de menaces toujours plus difficiles à déceler.

Au moment où la menace pénètre dans l'hôte, un moteur de protection des terminaux utilise tout un éventail d'approches, telles que les modèles de ML structurels, l'analyse comportementale et d'autres techniques de détection complexes, afin d'identifier et de neutraliser la grande majorité de la menace résiduelle.

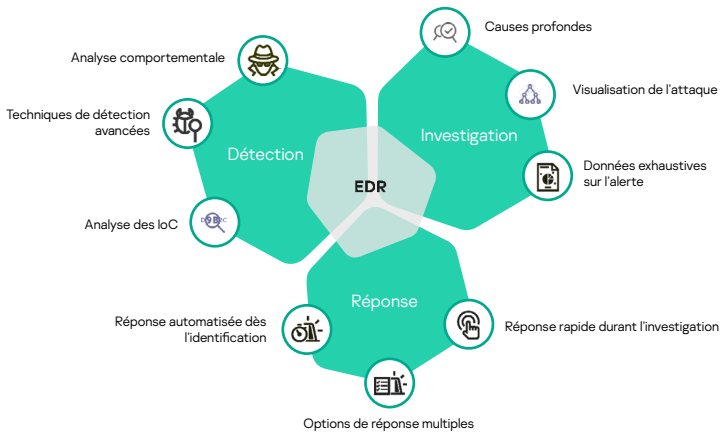
Une fois cette dernière exfiltrée par le biais de ces processus simples et hautement automatisés, les ressources peuvent être concentrées sur l'infime partie restante. Ces menaces non décelées comprennent les attaques complexes, évasives et avancées, qui, bien entendu, peuvent être les plus destructrices de toutes.

Et c'est là que la technologie EDR entre en jeu.

L'une des principales fonctions de la technologie EDR est de vous offrir de la **visibilité**, et d'aider votre équipe à voir ce qui se passe réellement au niveau de vos terminaux. Un accès rapide aux données relatives aux incidents, des informations exhaustives et une analyse des incidents de compromission (IoC) sont des éléments essentiels au contrôle de la sécurité des terminaux.

Une autre composante clé de la mission de la technologie EDR est l'**investigation.** Même si votre EPP a réagi, par exemple, à une suppression de fichier, ou à une injection de processus dans un processus existant (une attaque sans logiciel malveillant), cela ne signifie pas toujours que la menace a été éloignée, notamment dans le cas des attaques plus complexes. Comprendre les causes profondes d'une menace implique d'éradiquer l'intégralité de ces composantes. Par exemple, la seule suppression d'un fichier malveillant n'empêchera pas nécessairement le hacker de se connecter à l'hôte par d'autres moyens, et venir à bout d'un unique processus ne suffira probablement pas à prévenir une nouvelle attaque si les causes profondes n'ont pas été identifiées et traitées.

Pour finir, un grand nombre des menaces actuelles se développe très rapidement. En conséquence, une détection inefficace des composantes d'une menace pourrait être dévastatrice (les ransomwares ne sont qu'un exemple). Une **réponse rapide et de préférence automatisée** est donc essentielle. Détecter et comprendre la menace ne suffit pas, il faut aussi la neutraliser.



Graphique 1. Principales fonctionnalités EDR

À propos des ressources

Le nombre de postes vacants dans le domaine de la sécurité informatique a désormais dépassé les quatre millions à l'échelle du globe, selon (ISC)[2].

Cybersecurity workforce study, 2019 (ISC)[2]

Toute solution EDR doit correspondre aux ressources que vous pouvez, de façon réaliste, allouer à son déploiement et à sa maintenance. Trouver le budget pour l'achat de matériels et de logiciels est une chose, disposer d'un personnel aux compétences adaptées en est une autre.

Le recrutement de personnel qualifié dans le domaine de la sécurité informatique est en pleine crise à l'échelle mondiale. Au moment de la rédaction de ce document, le nombre de postes vacants dans le monde s'élève à 4,07 millions, contre 2,93 millions à la même période l'année précédente. Par conséquent, si vous ne disposez pas d'un personnel spécialisé dans la sécurité au complet, ne comptez pas être en mesure de le recruter facilement. Vous devez trouver un autre moyen.

À quel point une solution EDR peut-elle être automatisée et simplifiée ?

L'une des façons les plus efficaces d'utiliser une solution EDR avec des ressources limitées est d'automatiser les processus qui peuvent l'être en toute sécurité, et de simplifier les processus pour lesquels l'automatisation est inappropriée ou impossible. L'automatisation fait gagner du temps, des ressources et de l'argent. De plus, étant donné que les machines représentent une source d'erreurs moindre par rapport aux humains, elle vous permettra d'accroître l'efficacité de votre sécurité. Plus votre solution EDR est facile à utiliser par votre équipe sous pression, plus cette dernière accomplira ses missions en toute rapidité et précision. Pour les plus chanceux qui comptent dans leurs rangs des professionnels de la sécurité informatique, l'automatisation et la simplification libèrera ces derniers des tâches manuelles fastidieuses. Ils pourront ainsi consacrer davantage de leur temps précieux sur les aspects stimulants et enrichissants de leur mission.

Quels processus EDR peuvent être automatisés de façon efficace, et comment les processus manuels peuvent-ils être simplifiés ?

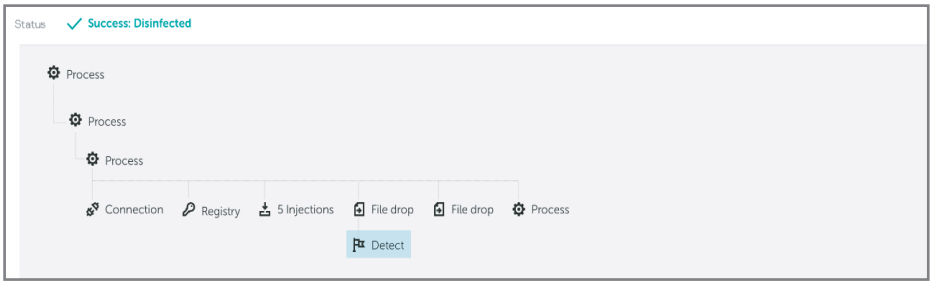
Pré-filtrage

Avant toute chose, votre solution de protection des terminaux doit être performante à 100 % pour ce qui est du pré-filtrage des incidents, avant que la technologie EDR n'entre en action. Plus tôt la grande majorité des menaces d'une chaîne de frappe peut être identifiée et contrée automatiquement, moins significatif est l'impact sur les ressources. La plupart des incidents de sécurité peuvent être immédiatement bloqués par une bonne solution EPP. Votre solution EDR et votre personnel dédié à la sécurité peuvent ainsi se concentrer sur les menaces plus avancées, qui sont aussi plus dangereuses. Nous allons nous répéter, mais assurez-vous de disposer d'une solution EPP de taille.

Simplification de l'analyse des incidents

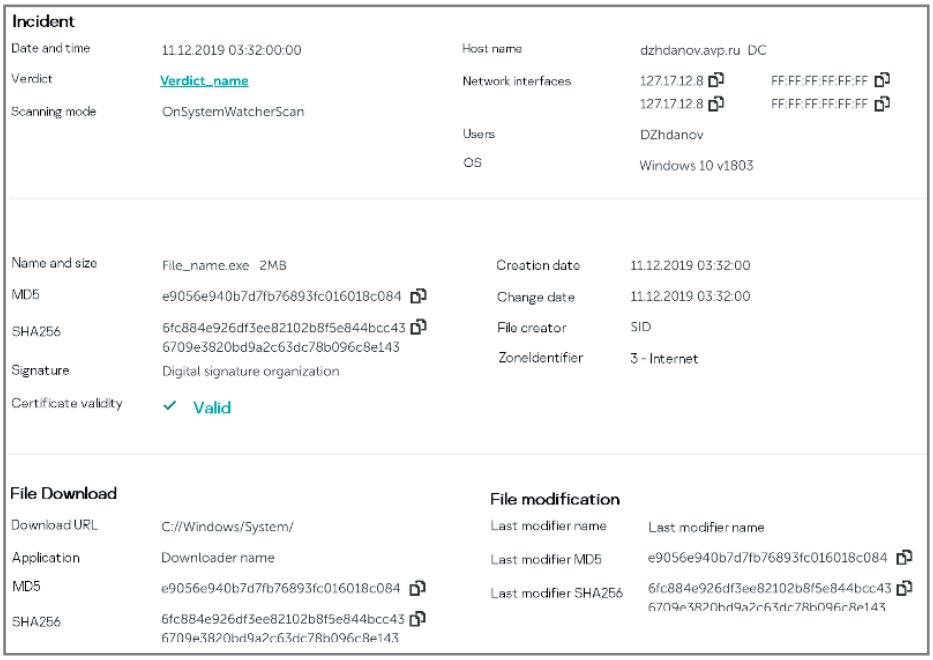
L'analyse des causes profondes, ou RCA, est simplement un processus consistant à découvrir ce qui est survenu, afin d'identifier la faille, s'assurer que l'incident a été entièrement traité et garantir qu'il ne se reproduira plus.

La visibilité sur ce qui se passe à un instant T est également primordiale. Une représentation visuelle claire, générée automatiquement, de chaque étape de l'avancée de l'incident (qui peut impliquer davantage d'éléments, dont des composantes ayant déjà pénétré dans votre système, que ceux détectés par votre EPP) est pour vous un moyen de disposer de toutes les données nécessaires à l'investigation.



Graphique 2. Une façon de visualiser le chemin emprunté par la menace et les connexions établies

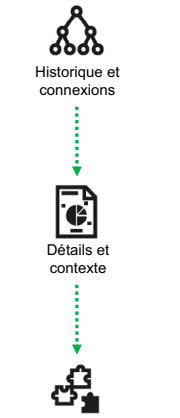
La seconde étape est la création automatisée d'une carte d'alerte regroupant toutes les informations requises à un seul et même endroit, afin de simplifier et d'accélérer le processus d'investigation. Parmi ces informations doivent figurer l'ensemble des détails et le contexte de l'incident : le moment précis, l'hôte infecté, les comptes utilisateurs utilisés, et diverses informations relatives à toute modification de fichiers, processus, clés de registres ou connexions associées.



Graphique 3. Un exemple de carte d'alerte présentant toutes les informations nécessaires

Utilisation

En cliquant sur une alerte, le responsable de la sécurité ouvre la carte d'alerte et visualise toutes les informations nécessaires, à commencer par les données de fichier et les données hôte, les éléments détectés et les actions entreprises par les différents niveaux de détection. Cela lui permet d'en savoir plus sur la façon dont les divers évènements sont reliés au niveau de l'hôte. À l'aide de ces données unifiées, il est bien plus simple d'examiner l'alerte et de comprendre si des composantes de la menace sont toujours actives ou sommeillent dans le système, et si le périmètre de la menace est plus étendu que ce qui avait été supposé. De cette façon, le responsable de la sécurité peut s'assurer qu'aucun résidu de l'attaque ne demeure dans le système.

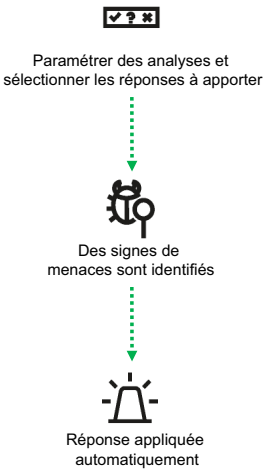


Création simplifiée et analyse automatisée des IoC

L'analyse des causes profondes d'un incident peut déclencher la création d'un indicateur de compromission (IoC) basé sur les activités associées à la menace détectée. L'analyse des IoC constitue, comme nous l'avons dit, un mécanisme de défense important de l'EDR. Elle vous aide à identifier les hôtes qui peuvent être infectés ou la localisation d'une menace. Les IoC connus (par exemple, ceux qui vous sont communiqués par les autorités réglementaires locales ou via une newsletter ou une liste de diffusion spécifique) peuvent être automatiquement importés dans la solution. Une analyse automatisée périodique des IoC importés et récemment créés est essentielle pour garantir l'intégrité du système. L'analyse périodique des IoC créés à partir d'une menace identifiée est précieuse, car il est fort probable que la même menace se représente. Et, si vous avez connaissance d'une attaque spécifique ciblant les organisations similaires à la vôtre et que des IoC associés sont disponibles, des analyses périodiques effectuées sur la base de ces IoC importés vous permettront d'identifier et de répondre à cette menace dans les plus brefs délais.

Utilisation

Vous obtenez des informations indiquant qu'une attaque cible les entreprises de votre secteur. Cela signifie que vous devez rechercher des IoC spécifiques. Plutôt que de procéder à des opérations manuelles, il vous suffit d'importer ces IoC et de paramétrer une analyse programmée.



Réponse automatisée

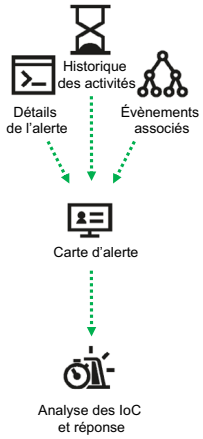
Les solutions EDR doivent être capables de réagir rapidement et de façon automatisée et efficace, de l'une des façons suivantes : via l'automatisation (lorsque, par exemple, une analyse des IoC a été exécutée et que des menaces ont été identifiées, exigeant une réponse immédiate) ou directement à partir de la carte d'alerte si, par exemple, le responsable de la sécurité doit isoler l'hôte durant l'analyse.

Les options de réponse peuvent inclure : empêcher l'exécution d'un fichier (par ex., créer une règle pour bloquer un fichier, au moyen d'un hachage spécifique à exécuter sur les hôtes), isoler l'hôte infecté, supprimer un fichier, et analyser automatiquement d'autres hôtes pour déceler tout signe d'infection à l'aide de l'EPP.

Utilisation

Au cours d'une investigation, le responsable de la sécurité découvre qu'un fichier ou une application particulière (par exemple, un RAT [Outil d'administration à distance] légitime d'origine inconnue) est une composante d'une cyberattaque potentiellement source de nombreuses activités malveillantes. Les circonstances (l'outil a été détecté sur une machine où sont stockées des données sensibles) préconisent d'isoler immédiatement l'hôte par précaution, jusqu'à ce que l'incident soit entièrement analysé et l'attaque complètement résorbée.

Une fois fait, le responsable peut initier une analyse des IoC afin d'identifier des fichiers similaires sur l'ensemble des terminaux, et paramétrer une réponse automatisée (telle que la suppression du fichier ou, mesure plus radicale, l'isolement de l'hôte du réseau dans l'attente d'une investigation plus approfondie). Il assure ainsi une réponse instantanée à toute menace identifiée sur le réseau.



Console unifiée

Basculer entre plusieurs outils est une perte de temps précieux, sans compter le risque d'erreurs généré par une visibilité tronquée. Votre personnel doit pouvoir mener des investigations et des analyses des causes profondes, répondre aux menaces et visualiser tout ce qui se passe à un instant T par le biais d'une seule console. Si votre solution EPP utilise la même console et le même agent, c'est encore mieux.

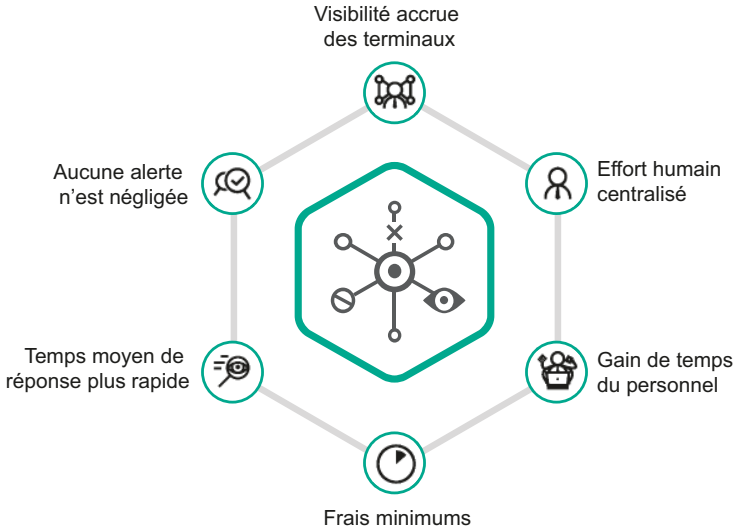
Utilisation

À la suite de l'identification d'une activité malveillante ou suspecte, vous n'avez pas besoin d'ouvrir toute une panoplie d'outils ou de vous rendre dans le terminal lui-même pour analyser des logs, des évènements associés, l'historique des activités des solutions EPP ou EDR, de réaliser des analyses des IoC ou de mener des actions de réponse avec un énième outil. Vous pouvez effectuer tout cela à partir d'une seule et même console.

Résultats de la mise en œuvre d'une solution EDR performante, avec automatisation intégrée

L'automatisation et la simplification des processus est synonyme de gain de temps et de ressources, tout en étant le gage d'une sécurité renforcée. Ce à quoi vous pouvez vous attendre :

- Aucun résidu d'attaque potentiellement dévastateur : élimine toute ambiguïté sur la présence éventuelle d'une menace dans votre réseau.
- Un temps moyen de réponse (MTTR) aux incidents plus rapide : un paramètre essentiel pour certaines attaques, telles que les ransomwares.
- Des incidents traités rapidement à chaque fois : un niveau d'automatisation élevé garantit que rien n'est mis de côté ou survolé à la suite d'une « baisse de vigilance par rapport aux alertes ».
- Davantage d'attention portée à ces incidents exigeant actuellement une intervention humaine, accompagnée d'une visibilité accrue et de données exhaustives sur les incidents.
- Ne pas avoir à investir dans une formation supplémentaire ou des experts en sécurité hautement qualifiés afin de gérer votre solution EDR au quotidien, mais seulement de façon ponctuelle.
- Une équipe plus enthousiaste qui, libérée des tâches de routine et dotée d'un kit d'outils EDR simples, est plus productive et moins vulnérable au phishing.



Graphique 4. Principaux résultats d'une implémentation EDR performante

Découvrez Kaspersky Endpoint Detection and Response Optimum

Sur la base de ces éléments, nous avons, chez Kaspersky, créé notre nouveau produit EDR : Kaspersky Endpoint Detection and Response (EDR) Optimum.

Kaspersky EDR Optimum vous aide à ériger une véritable défense en profondeur contre les menaces complexes, sans aucun frais supplémentaires.

En associant un kit d'outils de détection et de réponse convivial et hautement automatisé aux fonctionnalités inégalées de détection avancée et de protection des terminaux de Kaspersky Endpoint Security for Business au sein d'une offre unifiée, nous vous proposons aujourd'hui un niveau de sécurité extrêmement performant pour vos terminaux.

Avec un flux de travail rationalisé, des fonctionnalités d'automatisation et l'absence de frais supplémentaires, notre solution traite les incidents rapidement et de façon efficace, tout en préservant le temps et l'énergie de votre personnel de cybersécurité.

Prochaines étapes

Chaque organisation est unique. Nous vous recommandons donc d'examiner attentivement les fonctionnalités EDR dont vous avez véritablement besoin en fonction de votre activité.

Vous êtes à la recherche de meilleures fonctionnalités de détection et de réponse aux menaces, qui minimise les interventions de votre personnel surchargé à l'aide d'un outil simple et automatisé ? Dans ce cas, **Kaspersky Endpoint Detection and Response Optimum** pourrait être la solution idéale.

Vous avez plutôt besoin de fonctionnalités de détection des menaces avancées, de recherche proactive des menaces et de réponse aux incidents centralisée, afin d'armer votre équipe d'experts contre les attaques ciblées les plus complexes et les plus dangereuses ? Alors, vous serez peut-être intéressé par la solution **Kaspersky Endpoint Detection and Response**, pourquoi pas englobée dans la plateforme **Kaspersky Anti-Targeted Attack Platform**.

Vous souhaitez que votre organisation soit protégée 24 h/24, 7 j/7, tout en rendant votre personnel et vos ressources disponibles pour d'autres tâches ? **Kaspersky Managed Detection and Response** est précisément ce dont vous avez besoin.

Pour toute question sur la façon dont Kaspersky peut contribuer à la sécurité de votre entreprise, rendez-vous sur **https://www.kaspersky.fr/enterprise-security**.

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : https://www.kaspersky.fr/blog/

www.kaspersky.fr

kaspersky BRING ON THE FUTURE