Les mégatendances de la cybersécurité et leurs implications pour la cyberprotection

Une nouvelle approche de l'EPP, de l'EDR et du XDR

kaspersky

Résumé analytique

Chaque année, les principaux analystes, commentateurs, associations professionnelles et autres mettent en lumière les « mégatendances » qui devraient façonner leur industrie à court terme.

La cybersécurité ne fait pas exception. Ces informations sont essentielles pour aider les cadres dirigeants à anticiper les grandes tendances et à planifier l'avenir de leur organisation, mais pour les directeurs des systèmes d'information (DSI), les responsables de la sécurité informatique (RSSI), les équipes d'informatique et de sécurité informatique, la manière dont elles peuvent être prises en compte et mises en œuvre en termes pratiques est tout aussi importante.

Pour vous aider sur cette voie, ce livre numérique résume certaines des tendances de sécurité les plus complexes de l'industrie informatique aujourd'hui. Il se penche en particulier sur leurs conséquences pour l'utilisation par les organisations de solutions comme les plateformes de protection des terminaux (EPP), la détection et la réponse étendues (XDR) ainsi que la détection et la réponse au niveau des terminaux (EDR).

Sommaire

Vous parlez de mégatendance. Je préfère surface d'attaque élargie

Même pour les personnes travaillant dans le secteur des technologies informatiques, il est parfois difficile d'apprécier pleinement l'importance vitale de la cybersécurité dans le contexte général du marché.

La Security Industry Association (SIA), par exemple, est la principale association commerciale des fournisseurs de solutions de sécurité au niveau mondial, avec plus de 1 400 membres. Dans l'introduction de l'édition 2023 de sa vision de l'industrie, la SIA note qu'« il n'est vraiment pas surprenant de voir la cybersécurité de la sécurité physique dominer à nouveau notre liste des mégatendances en sécurité 2023 ».

> « L'IA et la cybersécurité continuent à se disputer la première place parmi les tendances affectant l'industrie de la sécurité, mais les données sont claires : la cybersécurité est la priorité des dirigeants du secteur. » De plus, « l'IA et la cybersécurité devancent largement les tendances suivantes. »

Pour remettre l'information dans son contexte, les professionnels de l'industrie de la sécurité considèrent la cybersécurité et l'IA comme bien plus critiques que les mégatendances qui pourraient autrement être considérées comme dominant le secteur, comme le développement de la main-d'œuvre, l'évolution des conditions économiques et l'utilisation éthique/sécuritaire des données et de la technologie.

Qu'en est-il des tendances plus spécifiques à l'informatique ?

Penchez-vous sur des rapports similaires rédigés par des analystes de premier plan, comme Gartner, IDC et Frost & Sullivan, et vous trouverez des références à tous les aspects de la question, depuis le dynamisme accru des environnements de réseau, qui rend les vulnérabilités plus difficiles à défendre, jusqu'à l'accélération du volume et de la sophistication des cyberattaques qui exploitent ces vulnérabilités.

Dans Cybersecurity Megatrends 2022, par exemple, IDC met en évidence sept tendances en matière de cybersécurité :

- Transformation numérique, travail hybride et fin du périmètre
- Pénurie des professionnels de la sécurité des informations
- Sophistication des cybercriminels en hausse rapide
- Prolifération des outils de sécurité et plateformisation
- Augmentation continue des réglementations en matière de conformité
- Nouveaux acheteurs et anciens acheteurs avec de nouvelles priorités
- Fiabilité

Le rapport Top Trends in Cybersecurity 2023 de Gartner montre une reconnaissance accrue de l'importance de l'implication du personnel dans le programme de sécurité pour faire face aux risques de cybersécurité et maintenir une fonction de cybersécurité efficace. Le travail de plus en plus distribué amplifie le recours au cloud. En retour, la dépendance à l'égard de la visibilité totale des écosystèmes numériques en expansion et de la résilience des chaînes d'approvisionnement augmente. En outre, les DSI modifient leurs modèles d'exploitation informatique pour favoriser l'agilité de l'entreprise. L'environnement réglementaire continue d'évoluer, obligeant les conseils d'administration à jouer un rôle plus actif dans la gestion des risques de cybersécurité. Alors que les paiements liés aux ransomwares sont en baisse, les attaques par ransomware à grande échelle et les attaques contre les systèmes d'identité se poursuivent.

Ces tendances globales amènent les principaux responsables sécurité et gestion des risques (SRM) à concentrer leurs efforts sur les points suivants :

1. Mettre l'accent sur le rôle essentiel des individus dans la réussite et la durabilité des programmes de sécurité.
2. Mettre en œuvre des capacités techniques de sécurité pour accroître la visibilité et la réactivité dans l'ensemble de l'écosystème numérique de l'organisation.
3. Favoriser l'agilité sans compromettre la sécurité en restructurant son mode de fonctionnement. »

Voici les recommandations de Gartner aux responsables de la sécurité et de la gestion des risques (SRM) pour répondre à ces besoins :

- Se mettre dans la peau d'un pirate informatique pour donner la priorité aux efforts d'atténuation des cyberrisques en adoptant une vision intégrale de la surface d'attaque et consolider les portefeuilles de fournisseurs, le cas échéant.
- Optimiser l'alignement des capacités de cybersécurité sur les nouvelles méthodes de travail distribuées en adoptant de nouveaux modèles opérationnels de sécurité et des approches architecturales qui favorisent l'agilité et intègrent la sécurité dès la conception.
- Prioriser et optimiser les investissements dans l'amélioration du comportement des employés afin de renforcer et de maintenir l'efficacité de la sécurité de l'entreprise.

Toutes ces recommandations sont des conseils judicieux. Alors, comment les appliquer au sein de votre organisation ?

Pour y répondre, commençons par examiner plus en détail l'évolution du paysage des menaces et les conséquences dans le contexte de votre infrastructure, de vos outils et de vos contrôles de sécurité informatique existants.

« Les vulnérabilités de type zero-day sont rarement la cause première d'une violation. Autrement dit, les violations pourraient être évitées si les organisations corrigeaient leur exposition à une menace avant qu'un pirate informatique ne l'exploite. Toutefois, corriger toutes les vulnérabilités connues a toujours été impossible sur le plan opérationnel. »

Gartner : Top Trends in Cybersecurity 2023

L'influence des mégatendances sur le paysage des menaces

Le paysage des menaces évolue plus rapidement que jamais comparé à ces dernières années. Il est désormais rare, par exemple, de passer ne serait-ce qu'une semaine sans attaque par ransomware, escroquerie ou violation de données médiatisée, et ces cyberattaques sont non seulement plus nombreuses, elles sont aussi plus complexes, plus ciblées et plus difficiles à détecter.

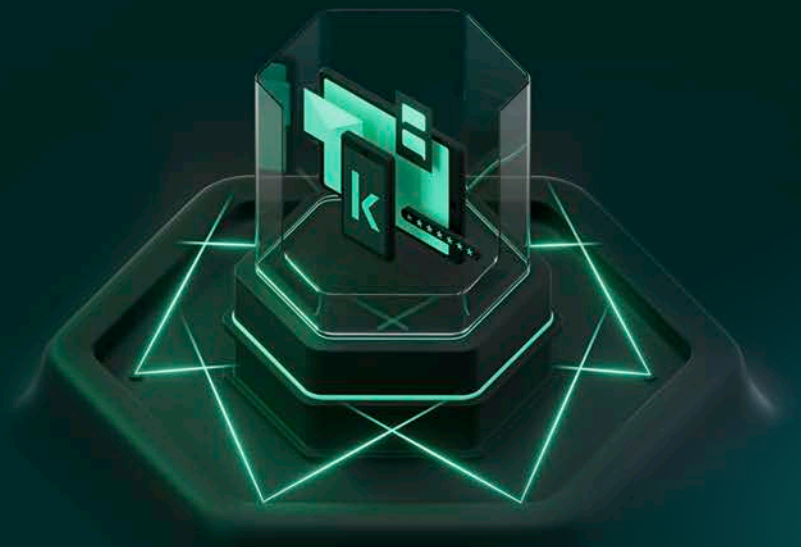
De nombreux individus derrière ces cyberattaques sont des criminels de carrière, et expérience rime avec succès. Le cliché du pirate informatique en guerrier numérique solitaire n'est plus d'actualité non plus.

Les groupes derrière les ransomwares, par exemple, se comportent de plus en plus comme des entreprises décentralisées, avec des réseaux complexes d'associés responsables des différentes étapes du processus, de la reconnaissance, l'accès, la création de programmes malveillants, la distribution et l'exfiltration de données, à la négociation de la rançon et la publication en ligne des données volées, en passant par le blanchiment des paiements.

La majorité des attaques par ransomware durent désormais quelques heures plutôt que quelques jours. Ces groupes proposent également des ransomwares sous forme de service et mènent des attaques plus proches des menaces persistantes avancées (APT) pour ce qui est de leur ampleur. D'autre part, les hacktivistes et les États-nations peuvent utiliser les ransomwares et d'autres techniques (comme les wipers) à des fins destructrices ou géopolitiques plutôt que purement commerciales.

En outre, les tactiques, techniques et procédures (TTP) utilisées par les cybercriminels sont de plus en plus sophistiquées, notamment l'utilisation de fonctionnalités d'autodiffusion et d'autopropagation, l'exploitation d'applications publiques, de comptes compromis et d'emails malveillants, et l'utilisation d'outils comme PowerShell, très répandue dans les opérations informatiques courantes, ce qui rend ces attaques beaucoup plus difficiles à repérer.

Par conséquent, il n'a jamais été aussi important d'établir le niveau de protection optimal pour votre organisation, que vous utilisiez l'EPP, l'EDR et/ou le XDR.



Comment sommes-nous passés de l'EPP à l'EDR puis au XDR ?

Traditionnellement, outre la défense de leur périmètre par des pare-feu et la protection des emails, les organisations ont concentré leurs efforts sur les terminaux, à savoir les ordinateurs de bureau, les ordinateurs portables, les serveurs (physiques et virtuels) et les postes de travail, pour se défendre contre les cybermenaces, à tel point que les plateformes de protection des terminaux (EPP) sont devenues incontournables dans la lutte contre les attaques complexes.

Plus récemment, les organisations ont renforcé ces mesures en déployant des outils plus avancés pour se défendre contre les attaques. Ceux-ci peuvent être utilisés pour identifier les comportements anormaux et y répondre, soit au niveau des terminaux, grâce à la détection et la réponse au niveau des terminaux (EDR), soit au niveau du réseau, avec la détection et la réponse au niveau des réseaux (NDR).

Toutefois, comme nous venons de le voir, les cybercriminels affinent leurs tactiques et développent sans cesse des méthodes plus sophistiquées pour cibler les entreprises. Les pirates informatiques d'aujourd'hui optent de plus en plus pour une approche multi-vectorielle des attaques, impliquant souvent plusieurs points d'entrée dans l'infrastructure et une série de tactiques et de techniques différentes.

Les acteurs malveillants utilisent des techniques avancées comme l'ingénierie sociale (dont le phishing et la compromission de la messagerie en entreprise), la compromission de comptes, les applications publiques et les exploits zero-day pour percer les défenses organisationnelles, complexifiant considérablement la protection des entreprises contre ces menaces en constante évolution.

Les APT, par exemple, contournent la détection traditionnelle des terminaux et peuvent rester actives pendant des semaines, voire des mois, en se déplaçant latéralement dans le réseau, en obtenant des autorisations, en exfiltrant des données et en recueillant des informations à partir des différentes couches de l'infrastructure informatique en vue d'une attaque à grande échelle ou d'une violation des données.

Les organisations ont de plus en plus de mal à garder une longueur d'avance face au volume et à la complexité de ces attaques. Et l'expansion constante de leur surface d'attaque, avec notamment les appareils mobiles, les environnements cloud, le travail à distance, les serveurs, ne fait qu'augmenter les difficultés.

En outre, les organisations doivent faire face aux menaces internes, aux vulnérabilités de la chaîne d'approvisionnement, aux exigences de conformité et de réglementation, dans un contexte de pénurie de professionnels qualifiés en matière de cybersécurité. S'ajoutent les dommages potentiels considérables causés aux systèmes, aux opérations et à la réputation des entreprises par les violations des données, les ransomwares, les attaques par déni de service distribué (DDoS), les APT, le cyberespionnage, etc.

Pour assurer une sécurité efficace contre ces menaces, il faut donc adopter une approche globale et proactive combinant technologies avancées, stratégies robustes, surveillance vigilante, formation continue et bien d'autres encore, c'est-à-dire la vision à 360 ° promise par l'XDR.

En décloisonnant les solutions ponctuelles propres à chaque couche, le XDR offre aux centres opérationnels de sécurité (SOC) et aux équipes de sécurité informatique la visibilité et l'intégration de bout en bout nécessaires pour identifier plus vite les menaces, y répondre plus rapidement, les résoudre plus efficacement et minimiser les dommages causés.

51 % des organisations ont du mal à détecter les menaces avancées et à mener des enquêtes sur celles-ci avec les outils actuels.

ESG Research Report, SOC Modernization and the Role of XDR, juin 2022

Quel type de sécurité pour qui ?

La solution idéale consiste à compléter la protection des terminaux par une sécurité de type EDR : plus on prévient de menaces, moins on reçoit d'alertes que les équipes de sécurité auront à examiner.

Depuis des années, les petites et moyennes entreprises (PME) et les très petites entreprises peuvent compter sur l'EPP pour se défendre contre une série de menaces courantes. Mais comme nous l'avons évoqué, les pirates informatiques d'aujourd'hui ciblent les organisations de toutes tailles, de tous secteurs et de tous niveaux de préparation, les PME et les petites entreprises étant de plus en plus exposées aux menaces évasives avancées, auparavant réservées aux grandes organisations.

En réaction, les équipes de sécurité informatique complètent leurs EPP avec des services EDR et/ou de détection et de réponse gérées (MDR) qui leur permettent de détecter et d'étudier les incidents de sécurité, de contenir la menace au niveau du terminal et d'y remédier au moyen d'une réponse et/ou recommandation automatisée.

La solution idéale consiste à compléter la protection des terminaux par une sécurité de type EDR : plus on prévient de menaces, moins on reçoit d'alertes que les équipes de sécurité auront à examiner. Les équipes informatiques peuvent alors optimiser les ressources clés et se concentrer sur l'activité informatique, au lieu de chasser les faux positifs et les énormes volumes d'alertes.

Juste au-dessus de l'EDR et du MDR, l'adjectif « étendues » dans « détection et réponse étendues » signifie que dans le XDR, une solution EDR est complétée et étroitement intégrée à une série d'autres outils de sécurité qui ne sont pas nécessairement conçus pour fonctionner ensemble. Plutôt que d'utiliser divers outils de sécurité comme solutions ponctuelles cloisonnées, le XDR permet aux organisations de créer un écosystème de sécurité complet, flexible et évolutif qui tire le meilleur des outils existants, s'adapte aux besoins de l'organisation, réduit les risques et augmente la sécurité.

Examinons maintenant cinq étapes clés pour vous aider à évaluer et à appliquer vos exigences en matière de sécurité sur ces points.

Pour répondre à la question « Qui a besoin de quel type de sécurité ? », il convient donc de garder à l'esprit les points suivants :

- Toutes les organisations ont besoin d'une base solide et moderne de sécurité des terminaux.
- Le ou les niveaux de sécurité supplémentaires nécessaires dépendront en grande partie des types de cyberattaques auxquelles l'organisation est potentiellement exposée et des compétences de l'équipe informatique chargée de mettre en œuvre et d'utiliser les outils nécessaires pour les prévenir.

Évaluer vos besoins de sécurité en constante évolution : EPP, EDR et MDR

Étape 1 :

Examinez la protection présente sur vos terminaux

Avec autant de solutions de cybersécurité avancées disponibles sur le marché, on oublie facilement le rôle vital que joue la protection des terminaux. En quoi les terminaux sont-ils si importants ? En plus de constituer les points d'entrée les plus communs dans l'infrastructure d'une organisation, ainsi que la principale cible des cybercriminels, ils représentent les sources clés des données nécessaires pour examiner efficacement les incidents complexes.

Par conséquent, chaque organisation doit choisir une solution EPP qui assure une protection automatisée contre un grand nombre d'incidents possibles causés par des menaces basiques, notamment les menaces sans fichiers et les ransomwares.

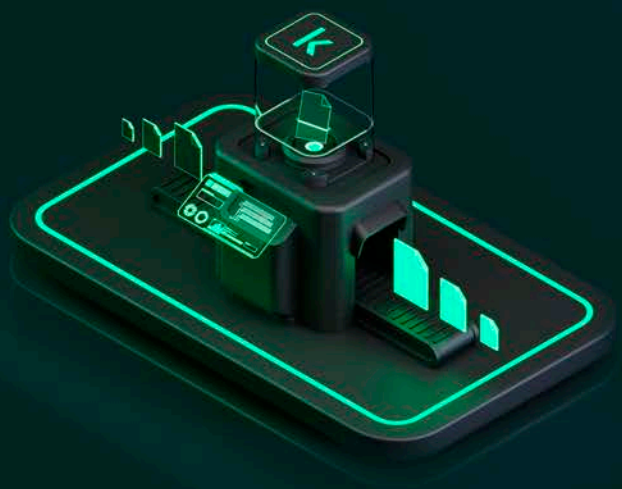
En raison du niveau relativement limité de connaissances ou d'employés spécialisés en sécurité qu'il exige, ce type de configuration répond aux besoins de sécurité des terminaux des PME ou des plus petites entreprises ne disposant pas d'une équipe de sécurité dédiée, ou des organisations dotées de faibles niveaux d'expertise en cybersécurité.

Il s'agit de même d'une étape fondatrice essentielle pour les entreprises moyennes et plus grandes où, en traitant automatiquement un grand nombre de menaces mineures, la solution ouvre la voie aux équipes de sécurité qui peuvent alors se concentrer sur des défenses plus sophistiquées si nécessaire.

Principales observations

En examinant une solution EPP pour déterminer si elle fournit les capacités nécessaires ou attendues, demandez-vous :

- À quel point cette solution est-elle efficace ?
- Combien de faux positifs recevez-vous ?
- Offre-t-elle des capacités efficaces de réduction de la surface d'attaque comme l'antivirus pour les fichiers, Internet et les emails, la protection du réseau, l'interface d'analyse anti-programmes malveillants (AMSI), la protection contre les exploits, la correction, la détection comportementale et la prévention des intrusions (HIPS) ?
- Permet-elle d'automatiser les tâches routinières ?
- Est-elle simple à faire fonctionner et aide-t-elle à minimiser les coûts et les frais administratifs liés à votre équipe informatique ?
- Contribue-t-elle à des tâches essentielles comme l'évaluation des vulnérabilités, l'inventaire logiciel et matériel, le contrôle des pare-feu, des sites Internet, des appareils et des applications, et le Cloud Discovery ?



Étape 2 :

Identifiez toute éventuelle faille critique au niveau des défenses de vos terminaux

Pourquoi une solution EPP nécessite-t-elle des capacités d'EDR ?

Comme nous l'avons souligné dans cet e-book, l'évolution du paysage des menaces signifie qu'au fil du temps, des menaces de plus en plus sophistiquées ciblant auparavant uniquement les grandes organisations touchent progressivement les PME et les plus petites entreprises qui ne disposent pas des ressources internes nécessaires pour y répondre efficacement.

L'apparition de menaces évasives en particulier, avec leur recours aux outils légitimes dans les attaques, dont des scénarios prêts à l'emploi pour contourner l'EPP, leur faible coût et leur facilité d'accès sur le Dark Web, a considérablement augmenté les risques de cybersécurité pour les organisations qui optent pour des solutions EPP traditionnelles.

Ces problèmes sont encore aggravés par le manque de transparence des solutions EPP traditionnelles. En effet, ces solutions n'offrent qu'une information feu rouge/feu vert indiquant qu'une attaque est ou n'est pas en cours. Or, ce dont a besoin une équipe informatique ayant des compétences de base en matière de sécurité, c'est d'avoir une visibilité sur l'activité des différents terminaux, afin de pouvoir l'analyser plus en détail et mieux comprendre la menace.

Les solutions EPP modernes intégrant des fonctionnalités EDR simples constituent donc une étape importante entre l'EPP traditionnelle et les solutions EDR plus avancées et complètes.

Même si votre EPP vous protège contre un large éventail de menaces basiques, vous devez aussi réfléchir à votre défense contre les menaces nouvelles, inconnues et évasives qui contournent votre EPP.

La préparation d'une attaque revient de moins en moins cher, ce qui expose de plus en plus d'organisations aux risques. En plus de survenir plus fréquemment, ces types d'attaques ont énormément gagné en efficacité en raison des diverses techniques que les criminels combinent, testent et utilisent pour contourner efficacement la sécurité des terminaux.

Le besoin urgent de gérer ces menaces est devenu de plus en plus vital de par les changements tels que la dissolution du périmètre des entreprises découlant de la hausse du travail à distance. Ces tendances créent un besoin pour un EPP avec des capacités supérieures aux solutions EPP traditionnelles, notamment des capacités d'EDR de base, comme une analyse simple des causes profondes.

Principales observations

Voici les signes avant-coureurs indiquant qu'il est temps d'étendre vos défenses au-delà d'une solution EPP traditionnelle :

- Votre solution EPP ne parvient pas à bloquer un nombre croissant de menaces nouvelles, inconnues et évasives.
- Vous disposez d'une visibilité limitée sur ce qui se passe au niveau de vos terminaux. Cela inclut l'incapacité de réaliser une analyse des causes profondes, une enquête et une réponse en temps réel aux menaces, ou l'obligation de devoir le faire manuellement au moyen d'outils de systèmes d'exploitation (OS) standard au cas par cas. Un processus long, complexe et source d'erreurs.
- Vous ne disposez pas des compétences ou capacités spécialisées en sécurité informatique nécessaires pour gérer des menaces toujours plus sophistiquées.
- Les amendes potentielles ou les atteintes à la réputation de votre entreprise résultant d'un incident de sécurité majeur vous inquiètent.

Pour mettre en œuvre une solution efficace capable de vous défendre contre ces menaces, vous devrez également prendre en compte les aspects de votre organisation comme sa taille, son profil d'entreprise, son degré de préparation à la sécurité, ses ressources et son expertise existantes et plus particulièrement les compétences en matière de sécurité de votre infrastructure informatique ou équipe de sécurité informatique.

Étape 3 :

Identifiez clairement l'objectif à atteindre

Bon nombre d'organisations disposent de peu de temps et de ressources (ou d'un petit service de sécurité informatique sans aucun projet d'agrandissement), mais doivent comprendre ce qui se passe dans leur infrastructure et être capables de répondre aux menaces évasives avant qu'elles ne puissent leur nuire.

L'ajout de fonctionnalités EDR appropriées à une solution EPP peut fournir une défense très efficace contre les menaces plus sophistiquées et évasives. On devrait ainsi pouvoir envoyer des réponses « en un seul clic » automatisées et/ou rapides et précises (mise en quarantaine de fichiers, isolation de l'hôte, interruption d'un processus, suppression d'un objet, etc.). En outre, si votre entreprise compte des spécialistes de la sécurité informatique, votre solution doit également fournir les informations, les connaissances et les outils nécessaires à une enquête efficace, comme l'analyse des causes profondes, la création d'indicateurs de compromission (IOC) personnalisés, l'importation d'IOC et l'analyse de ces derniers sur tous les terminaux.

Vous aurez également besoin d'une solution qui utilise de façon optimale toutes les fonctions qui vous sont vraiment nécessaires, au lieu de payer pour un grand nombre de fonctions dont vous ne voulez pas vraiment et de devoir recruter des experts en sécurité informatique possédant les compétences requises pour s'en servir.

5 idées fausses à propos de l'EDR

1 Notre protection des terminaux est suffisante, nous n'avons pas besoin d'EDR

Idée fausse : Les cybercriminels ne s'intéressent pas aux entreprises comme la nôtre ; nous passons inaperçus pour le type d'attaques contre lesquelles l'EDR nous protège.

Réalité : S'il est facile de penser que les cybercriminels ont tendance à ne pas cibler les petites entreprises, la réalité est que les PME sont confrontées aux mêmes menaces que les grandes entreprises. Bien que la grande majorité des cyberattaques soient des menaces courantes, une grande partie des autres sont des attaques nouvelles, inconnues et évasives qui contournent les solutions EPP traditionnelles. Ces menaces sont difficiles à détecter en raison de l'éventail de techniques d'évasion adoptées, en particulier l'utilisation d'outils légitimes et intégrés au système. En restant dissimulées pendant plus longtemps, elles disposent du temps nécessaire pour explorer votre infrastructure, s'y implanter et provoquer le plus de dégâts possible, qu'il s'agisse d'une violation de données, d'une attaque de ransomware ou de logiciel espion ou du contournement direct de vos opérations.

2 Nous avons besoin de l'EDR pour compenser la faiblesse des solutions EPP

Idée fausse : Notre solution EPP n'est pas assez efficace, nous avons donc besoin de l'EDR pour la renforcer.

Réalité : Essayer de renforcer la sécurité de vos terminaux en investissant dans une solution EDR sans régler les problèmes de votre EPP revient à construire une tour sur des sables mouvants. Une solution EPP faible peut en réalité nuire à l'EDR et l'empêcher d'atteindre les résultats escomptés. De plus, si la solution EDR est surdimensionnée par rapport à vos besoins réels, elle peut aussi être trop coûteuse, et difficile à appréhender et à utiliser pour votre équipe.

3 Pour utiliser l'EDR, il est nécessaire d'avoir une équipe de sécurité informatique composée d'experts

Idée fausse : Les PME et les entreprises à faible chiffre d'affaires ne disposent pas d'un nombre suffisant de spécialistes de la sécurité ayant les compétences nécessaires pour comprendre et utiliser les outils requis pour détecter les menaces, enquêter sur elles et y répondre.

Réalité : Lorsque l'EDR a été introduit, les systèmes étaient compliqués et difficiles à utiliser. Cependant, grâce aux solutions modernes, chaque fois que vous recevez une alerte, l'EDR vous renseigne sur l'origine de la menace, sa mise au point, ses causes profondes, les autres hôtes qu'elle a touchés et, par conséquent, son ampleur. Elle doit aussi vous guider à travers un simple processus de gestion des incidents qui comprend des étapes telles que l'identification, le confinement, l'élimination, le rétablissement et l'analyse des leçons apprises pour anticiper les futures attaques.

4 On ne peut pas combiner EDR et MDR

Idée fausse : Si vous voulez une sécurité de type EDR, vous devez soit investir dans l'EDR pour que votre équipe interne l'utilise, soit confier la détection et la réponse gérées (MDR) à un fournisseur spécialisé.

Réalité : Le choix d'une sécurité de type EDR ne se pose pas vraiment. L'EDR et le MDR présentent chacun leurs propres avantages, et la meilleure option consiste souvent à combiner les deux. Ainsi, par exemple, une PME ou une entreprise à faible chiffre d'affaires peut utiliser le MDR pour renforcer instantanément son niveau de sécurité informatique et se protéger contre les menaces évasives, sans avoir à investir dans du personnel ni des ressources supplémentaires, tandis qu'une plus grande entreprise peut l'utiliser pour se décharger des processus de triage des incidents et d'enquêtes sur ceux-ci 24h/24, 7j/7, et mobiliser plus efficacement ses ressources internes de sécurité informatique en utilisant l'EDR pour des enquêtes et des réponses détaillées.

5 L'EDR entraîne une lassitude vis-à-vis des alertes et ne justifie pas les efforts demandés

Idée fausse : L'EDR est réputé pour générer un grand nombre d'alertes et de faux positifs que les équipes informatiques n'ont ni le temps ni les ressources pour traiter ou résoudre.

Réalité : Les solutions EDR modernes ne se contentent pas d'automatiser de nombreuses tâches, l'EDR et/ou le MDR ont le pouvoir de vous faire passer d'une situation où vous êtes soumis à un risque important d'attaque évasive, à une situation où vous reprenez confiance dans la sécurité de vos terminaux. Au lieu de ne pas savoir exactement ce qui se passe dans votre environnement, vous aurez une visibilité et un contrôle sur tous vos terminaux. Et plutôt que de rechigner à mettre à niveau votre sécurité pour des raisons de complexité, vous disposerez d'une solution simplifiée et consolidée qui optimisera vos ressources.

Essayez notre jeu interactif de simulation de ransomware pour découvrir comment mieux protéger votre infrastructure informatique :
https://www.kaspersky.com/response-game/fr

Étape 4 :

Pensez à vos cas d'utilisation

Avant de pouvoir identifier la protection qui convient le mieux à vos besoins, vous devez définir des exigences précises à cet égard. Ceci implique de prendre en compte les aspects critiques des performances et de l'utilisation régulière de la solution, comme les cas d'utilisation qu'elle doit exécuter et les résultats qu'elle est censée donner.

À titre d'exemple, quand vous recevez une alerte de sécurité, la solution EDR et/ou MDR doit vous permettre de répondre à des questions clés telles que :

- Dans quel contexte l'alerte a-t-elle été lancée ?
- Quelles mesures ont déjà été prises à la suite de l'alerte ?
- La menace détectée est-elle toujours active ?
- D'autres hôtes font-ils l'objet d'une attaque ?
- Quel chemin l'attaque a-t-elle emprunté ?
- Quelles sont les causes profondes de la menace ?

Elle doit aussi vous aider à visualiser l'ampleur de la menace. Par exemple :

- Si une menace globale pèse sur votre entreprise, vos dirigeants voudront sûrement s'assurer que vous n'êtes pas actuellement la cible d'une attaque, auquel cas vous devrez être capable de trouver un indicateur de compromission (IoC) en ligne, d'exécuter une analyse et de répondre correctement à leurs préoccupations.
- Si les autorités réglementaires vous demandent d'exécuter l'analyse d'un IoC spécifique, vous devez pouvoir importer des IoC issus de sources fiables et exécuter des analyses régulières pour identifier tout signe d'attaque.
- Si vous avez examiné en détail une alerte et créé un IoC sur la base des menaces identifiées, vous devez faire automatiser l'exécution des analyses sur l'ensemble du réseau afin de découvrir si d'autres hôtes ont été impactés au lieu de vous en charger vous-même.

De même, vous devez être capable de répondre rapidement à des menaces prolifiques en constante évolution :

- En contenant la menace par l'isolation de l'hôte, la mise en quarantaine du fichier ou la prévention de l'exécution des fichiers pendant l'enquête.
- En utilisant une réponse automatisée entre les points d'accès basée sur des analyses IOC, vous permettant de répondre aux menaces évasives dès leur découverte, ou des scénarios de réponse guidée et à distance si vous utilisez le MDR.

Voici quelques-uns des principaux résultats que vous pouvez attendre de votre solution :

- Protection contre les menaces évasives plus fréquentes et plus perturbatrices.
- Économie de temps et de ressources grâce à un outil automatisé et simplifié.
- Évaluation de la portée d'une attaque en recherchant les IoC sur tous les terminaux.
- Compréhension des causes profondes de chaque menace et de son origine.
- Éviction des dommages préjudiciables par le biais d'une réponse rapide et automatisée.

5 idées fausses à propos du MDR

1 Le MDR n'est qu'un autre service de sécurité managé

Idée fausse : Le MDR est comme tout autre service de sécurité géré (MSS) impliquant une gestion de votre infrastructure informatique par le fournisseur.

Réalité : Les MSS (Managed Security Service) couvrent généralement une gamme de services généraux de cybersécurité, comme l'évaluation de la conformité réglementaire, ou encore de technologies, comme les VPN et les pare-feu, les tests de pénétration, les recommandations d'offres, etc. Le MDR, quant à lui, se concentre sur la détection avancée et la réponse rapide aux menaces nouvelles, inconnues et évasives qui contournent les EPP, en combinant la recherche, la détection et l'analyse des menaces basées sur les TTP.

2 Le MDR est réservé aux grandes entreprises

Idée fausse : Étant donné que le MDR traite des techniques de sondage complexes, comme la recherche des menaces et les indicateurs d'attaque (IoA), il n'est adapté qu'aux besoins des grandes entreprises.

Réalité : Le MDR n'est pas une solution universelle. Il offre différentes solutions pour différents types d'organisations. Une PME ou une entreprise à faible chiffre d'affaires pourrait utiliser le MDR pour améliorer instantanément sa sécurité informatique et se protéger contre les menaces évasives, tandis qu'une grande entreprise pourrait l'utiliser pour se décharger des enquêtes sur les incidents et leur triage, et pour mieux concentrer ses ressources internes en matière de sécurité informatique.

3 Le MDR basé sur l'IA peut se passer d'experts humains

Idée fausse : L'intelligence artificielle (IA) et le Machine Learning (ML) ont progressé au point que le recours aux experts humains dans le domaine du MDR appartiendra bientôt au passé.

Réalité : L'IA, le ML et les IoA propriétaires permettent de traiter automatiquement un grand nombre d'alertes : en automatisant le triage initial des incidents, en minimisant le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR) par une augmentation considérable du rendement des analystes MDR, et en assurant une protection continue contre les menaces non malveillantes les plus innovantes. En revanche, pour les TTP inconnues jusqu'alors ou d'origine humaine qui ne sont pas automatiquement détectées, la recherche des menaces gérée repose toujours sur des efforts minutieux, proactifs et pratiques de la part d'experts dans la recherche de menaces.

4 Le MDR est difficile à mettre en œuvre

Idée fausse : Le MDR est souvent vendu comme offrant les capacités d'un SOC fonctionnant en permanence, on pense donc qu'il est compliqué à utiliser.

La réalité : Comme nous l'avons souligné plus haut, le MDR peut servir à tout, de la prévention des menaces qui contournent les cyberdéfenses existantes à la fourniture d'un deuxième avis ou à la libération des experts internes pour qu'ils se consacrent à des tâches plus importantes. Il s'agit d'un service clé en main facile à mettre en œuvre, qui permet d'améliorer considérablement le MTTD et le MTTR. Plus le MTTD et le MTTR sont courts, moins il y a de perturbations causées par les incidents et plus les coûts sont bas.

5 Même avec le MDR, vos équipes ont encore beaucoup de travail

Idée fausse : Le travail des services MDR s'arrête après l'enquête sur l'incident, laissant aux clients des rapports et des recommandations techniques à appliquer à leurs systèmes, ce qui accroît encore la pression sur les ressources de sécurité informatique.

Réalité : Si c'était certainement le cas dans le passé, avec les services modernes de MDR, vous pouvez choisir d'autoriser le fournisseur à répondre automatiquement pour vous, de lancer vous-même les actions de réponse recommandées (comme l'isolement de l'hôte, la mise en quarantaine de fichiers, la suppression de fichiers, l'interruption de processus, la demande de fichiers d'un hôte ou l'exécution d'un programme sur celui-ci, l'analyse des IoC, etc.), ou de tirer parti de scénarios de remédiation gérés que vous pouvez pré-approuver ou approuver manuellement pour chaque alerte.

Le centre des opérations de sécurité (SOC) et l'équipe GERT (Global Emergency Response Team) de Kaspersky ont analysé un an d'incidents de sécurité dans tous les secteurs pour développer un aperçu inégalé du paysage des menaces.

Accéder aux rapports : https://go.kaspersky.com/mdr-and-ir-reports-2022.html

Étape 5 :

Choisissez la protection la plus adaptée à vos besoins

De nombreuses entreprises n'ont pas d'expert de la sécurité dédié. Certaines d'entre elles commencent peut-être tout juste à créer leur service de sécurité informatique, tandis que d'autres disposent sans doute déjà d'équipes de sécurité informatique pleinement formées et compétentes.

De nombreuses entreprises n'ont pas d'expert de la sécurité dédié. Certaines d'entre elles commencent peut-être tout juste à créer leur service de sécurité informatique, tandis que d'autres disposent sans doute déjà d'équipes de sécurité informatique pleinement formées et compétentes. La qualité de l'expertise disponible de ces organisations en matière de défenses contre les menaces varie donc énormément, à l'instar du temps qu'elles peuvent consacrer à cette tâche.

Pour gérer ces circonstances différentes, les organisations dépourvues de personnel de sécurité informatique dédié ou dont celui-ci est surchargé par les tâches routinières devront utiliser l'automatisation de façon stratégique pour contrer les nouvelles menaces évasives.

Ceci implique de combiner leur EPP avec des outils EDR supplémentaires qui, en plus de protéger contre ces menaces, intègrent des niveaux appropriés d'automatisation (complète ou partielle).

Alternative possible : au lieu d'investir dans une solution EDR excessivement complexe pour laquelle elles n'ont ni le temps ni les compétences nécessaires, les organisations peuvent, grâce au MDR, accéder à des fonctionnalités comme la surveillance sécurisée 24 h/24, 7 j/7 par des experts, la recherche de menaces automatisée et gérée et les scénarios de réponse à distance guidés, que ce soit auprès d'un fournisseur, d'un fournisseur de services gérés (MSP) ou d'un fournisseur de services de sécurité gérés (MSSP).

En troisième option, il est possible de combiner l'EDR avec une solution MDR. Puisque de nombreuses organisations ne disposent pas de l'expertise requise pour la recherche de menaces, l'idéal consiste souvent à externaliser cette tâche tout en mettant en œuvre les fonctionnalités de détection et de réponse en interne. Ceci peut s'avérer particulièrement bénéfique pour les entreprises qui souhaitent élaborer leur propre équipe de cybersécurité, mais ne possèdent pas les ressources, le personnel et/ou les compétences nécessaires pour prendre en charge la détection et la réponse spécialisées.

Que faire si vos ressources internes sont limitées ?

Supposons que vos ressources internes en matière de sécurité informatique soient limitées, ou que vous disposiez d'une petite équipe composée d'un ou deux spécialistes de la sécurité. Supposons également que vous deviez déterminer la nécessité de compléter votre EPP par une solution EDR et/ou MDR. Quels types d'avantages pouvez-vous attendre et quelle solution vous conviendrait ?

Si vous préférez une approche plus pratique (et que votre équipe informatique possède des compétences suffisantes en matière de sécurité informatique), l'EDR peut empêcher les interruptions d'activité et les dommages en éliminant les risques inhérents aux menaces nouvelles, inconnues et évasives et en donnant à votre personnel de sécurité la visibilité nécessaire pour enquêter sur les menaces, analyser leurs causes profondes et y répondre.

Cette solution favorise les économies en permettant à votre équipe de sécurité de travailler plus efficacement sans avoir à jongler avec plusieurs outils et consoles et optimise la capacité de travail en automatisant un grand nombre de processus. Vous aurez également l'esprit tranquille, car il vous sera alors plus facile de surveiller et de détecter les menaces, ainsi que de répondre aux attaques et de les prévenir.

Si vous cherchez à étendre vos capacités de sécurité informatique en interne en déléguant les tâches principales de détection et de réponse, le MDR peut vous offrir une protection avancée et continue contre les menaces qui peuvent contourner les barrières de sécurité automatisées. Cette solution contribue à résoudre la problématique de recrutement de talents dans le domaine de la cybersécurité et apporte tous les avantages principaux d'un SOC, 24 h/24, 7 j/7.

La technologie MDR peut également vous permettre de réaliser des économies en réservant les ressources internes aux tâches critiques qui requièrent vraiment l'implication de votre équipe informatique ou de sécurité informatique, et optimiser la capacité en exploitant des modèles de ML avancé pour augmenter de manière significative le rendement des analystes et minimiser le MTTR. De plus, cette solution vous assure une surveillance sécurisée continue par des experts, ainsi qu'une recherche de menaces automatisée et gérée. Ceci inclut l'analyse de menaces non malveillantes complexes et les menaces dangereuses difficiles à détecter à l'aide d'outils OS légitimes dans les attaques.

En parallèle, la combinaison de solutions EDR et MDR vous permet de personnaliser leurs fonctionnalités selon vos propres besoins, par exemple en externalisant la recherche de menaces (pour laquelle vous ne disposez peut-être pas de l'expertise requise) tout en mettant en œuvre les fonctionnalités de détection et de réponse au niveau des terminaux en interne.

Comment évaluer vos nouveaux besoins en matière de sécurité – XDR

40 % des organisations auront déployé une plateforme de XDR d'ici 2027, contre 5 % en 2021

Selon l'étude Cyber Resilient Organization Study 2021 d'IBM, 32 % des organisations ont déclaré utiliser 21 à 30 outils de sécurité individuels pour répondre à chaque menace, et 13 % ont déclaré utiliser au moins 31 outils.

Les menaces avancées sont trop longues à identifier et à contenir à cause du nombre d'outils impliqués.

Le rapport d'IBM « Cost of a Data Breach » 2022 a révélé qu'il fallait en moyenne 277 jours pour détecter et résoudre une violation des données. Une violation survenue le 1er janvier ne serait donc pas maîtrisée avant le 4 octobre.

Le XDR en résumé

Si vous êtes une moyenne ou grande entreprise et que votre SOC ou votre équipe de sécurité informatique ne vous parle pas constamment de XDR, cela ne saurait tarder.

Comme le note CRN (15/02/23), « lorsqu'il s'agit de détecter les menaces et d'y répondre, il ne suffit plus d'examiner le terminal ou le réseau. L'approche adoptée par de nombreuses grandes entreprises de cybersécurité dans ce domaine est le XDR, ou détection et réponse étendues. L'une des catégories les plus dynamiques en cybersécurité aujourd'hui, le XDR vise à renforcer la sécurité en mettant en corrélation les données provenant de l'ensemble des environnements et des dispositifs d'une organisation, puis répondant en priorité aux menaces les plus sérieuses.

« Indépendamment de leur propre définition, les plateformes XDR ont toutes pour objectif de donner un coup de pouce aux équipes de sécurité en manque de personnel, afin d'améliorer la qualité de la détection des menaces tout en réduisant la surcharge d'alertes. »

Avec le XDR, des solutions de sécurité qui ne sont pas nécessairement conçues pour fonctionner ensemble peuvent interagir de manière transparente sur la prévention, la détection, l'enquête et la réponse aux menaces. En outre, combler le manque de visibilité entre les outils et les couches de cybersécurité avec le XDR permet aux équipes de sécurité surchargées de détecter et de résoudre les menaces plus rapidement et plus efficacement, et de capturer des données contextuelles plus complètes pour les aider à prendre de meilleures décisions en matière de sécurité et à prévenir de futures attaques.

Alors, que fait exactement le XDR, quels sont ses avantages et pourquoi est-ce potentiellement l'un des investissements les plus importants en matière de sécurité pour votre organisation ?

EDR, MDR ou XDR

EDR
Endpoint Detection and Response

- Identifie les menaces nouvelles, inconnues et furtives qui contournent la protection des terminaux et automatise les tâches de sécurité de routine

MDR
Managed Detection and Response

- Décharge la détection des menaces, la recherche des menaces et les enquêtes sur les incidents, ou complète les mesures existantes en fournissant une protection avancée permanente contre les menaces

XDR
Extended Detection and Response

- Détecte de manière proactive les menaces complexes dans plusieurs niveaux de l'infrastructure et y répond automatiquement pour les contrer

Comment ça fonctionne ?

- Améliore la visibilité et la visualisation des menaces
- Fournit des mécanismes de détection avancés (p. ex. IOC, IoA)
- Simplifie l'analyse des causes profondes et soutient la recherche des menaces
- Délivre une réponse rapide et automatisée

- Fournit une protection experte en continu, même contre les menaces d'origine non malveillante les plus complexes et les plus innovantes

- S'intègre à de nombreux outils et applications de sécurité ainsi qu'à l'infrastructure de cybersécurité existante
- Surveille des données de sources multiples afin de détecter et éliminer les menaces complexes

Valeur commerciale

- Permet aux équipes de sécurité informatique de travailler de manière plus efficace, sans avoir à jongler entre plusieurs outils et consoles
- Automatise de nombreux processus pour éviter de dépendre des processus de correction traditionnels qui pourraient entraîner des temps d'arrêt
- Facilite la surveillance et la détection des menaces, l'agrégation centralisée des données de cyberdiagnostic, la réponse aux attaques et leur prévention

- Concentre les ressources internes coûteuses sur les tâches critiques qui requièrent réellement l'implication d'une équipe de sécurité informatique
- Exploite des modèles de machine learning propriétaires pour augmenter considérablement le rendement des analystes et réduire les temps moyens de détection (MTTD) et de réponse (MTTR)
- Résout le problème du manque de talents dans le secteur de la cybersécurité
- Fournit tous les avantages principaux d'un SOC 24/7

- L'approche par écosystème optimise l'efficacité des outils de cybersécurité mis en œuvre, économise des ressources et réduit le risque
- Simplifie le travail des spécialistes de la sécurité informatique et leur procure le contexte supplémentaire nécessaire pour enquêter sur les attaques perpétrées avec plusieurs vecteurs
- Minimise les temps moyens de détection et de réponse (MTTD et MTTR), ce qui est essentiel pour combattre les menaces complexes et les attaques ciblées
- Fournit une protection globale contre le paysage des menaces en évolution

Pour qui est-ce le mieux adapté ?

- Entreprises avec une approche conservative de la technologie, qui souhaitent éviter tout risque et gagner en visibilité au niveau de la protection automatique
- Public général souhaitant développer des processus de réponse aux incidents
- Organisations qui utilisent l'informatique comme avantage concurrentiel et ont besoin de permettre aux experts de trouver et neutraliser des menaces complexes

- Sociétés cherchant à développer leur capacité de sécurité informatique interne en se déchargeant des tâches principales de détection et de réponse
- Organisations qui ne disposent peut-être pas du budget ou de l'équipe de spécialistes pour élaborer leur propre centre d'opérations de sécurité (SOC)

Organisations disposant d'importantes ressources en matière de sécurité et recherchant une plateforme unique avec ce qui suit :

- Une image cohérente de ce qui se passe d'un bout à l'autre de leur infrastructure
- Recherche des menaces et Threat Intelligence intégrées
- Hiérarchisation des incidents supérieure et moins d'alertes de faux positifs

Capacités et avantages propres aux plateformes de XDR

Intègre plusieurs outils de sécurité en une plateforme unique

Avec le XDR, des solutions de sécurité qui ne sont pas nécessairement conçues pour fonctionner ensemble peuvent interagir de manière transparente sur la prévention, la détection, l'enquête et la réponse aux menaces.

- Il pourrait s'agir, par exemple, de solutions conçues pour protéger les emails, Internet, le réseau, l'infrastructure cloud, les applications, l'identité, etc., permettant de détecter et d'étudier de nouveaux types de scénarios d'attaque et de renforcer le processus de lutte contre les menaces complexes.
- Le XDR peut également intégrer des outils de Threat Intelligence, comme des flux de données sur les menaces et la plateforme utilisée pour gérer ces données, afin de fournir aux équipes SOC le contexte supplémentaire si important lors d'enquêtes sur des cyberincidents complexes.
- De plus, en fonction du secteur et des exigences d'une organisation, le XDR peut intégrer des outils de sécurité de technologies opérationnelles (TO) et de l'Internet des objets (IdO), et ainsi déployer un cadre de sécurité complet sur les environnements informatiques/de TO.

Réunit plusieurs types de télémétrie

En permettant une analyse comportementale et télémétrique en temps réel à travers plusieurs couches de sécurité, y compris les terminaux, le réseau et le cloud, les analystes de sécurité peuvent mieux visualiser les cybermenaces, les cibler et les éliminer en fonction de la gravité de leur impact sur l'infrastructure informatique de l'organisation.

Offre une visibilité des menaces de bout en bout

En décloisonnant les solutions ponctuelles propres à une couche, le XDR offre aux SOC et aux équipes de sécurité informatique la visibilité et l'intégration de bout en bout nécessaires pour identifier plus vite les menaces, y répondre plus rapidement, les résoudre plus efficacement et minimiser les dommages causés.

Le XDR peut relier chaque étape de la chaîne d'exécution et la présenter sous forme d'alerte unique avec le contexte complet de l'attaque, ce qui réduit les volumes d'alerte, améliore leur qualité et permet une orchestration ainsi qu'une réponse de bout en bout.

Rationalise et centralise la collecte des données, améliore l'efficacité

Un data lake unique permet une collecte, une gestion et un stockage complets des journaux, en fournissant une plateforme centralisée pour collecter, indexer et analyser les journaux provenant de diverses sources, y compris les solutions de sécurité (EPP, FW, NGFW, IAM, SIEM, SOAR, etc.), les systèmes opérationnels, les applications d'entreprise (systèmes RH, outils bureautiques), la sécurité physique (systèmes de contrôle d'accès automatisés) et d'autres appareils.

Cela permet aux équipes SOC et de sécurité informatique d'obtenir des informations précieuses, de détecter des anomalies et d'identifier des incidents de sécurité potentiels en exploitant des données de journaux riches, couvrant à la fois les événements passés et présents (en temps réel). L'intégration avec d'autres outils et plateformes de sécurité améliore également l'efficacité opérationnelle en centralisant la gestion de la sécurité et en fournissant une vue unifiée des événements et des incidents de sécurité.

Accélère la détection des menaces, les enquêtes et la réponse

En éliminant les écarts de visibilité entre les outils et les couches de cybersécurité, le XDR permet aux équipes de sécurité surchargées de détecter et de résoudre les menaces plus rapidement et plus efficacement, et de capturer des données plus complètes et contextuelles pour les aider à prendre de meilleures décisions en matière de sécurité et à prévenir de futures attaques.

En automatisant les tâches de routine, comme le tri, le confinement et l'élimination des menaces, les entreprises peuvent optimiser leurs ressources de sécurité et se concentrer sur des activités plus stratégiques.

Réduit les MTTD et MTTR

Le XDR contribue à réduire le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR), ce qui est essentiel pour lutter contre les menaces complexes et les attaques ciblées, où les actions rapides des experts en sécurité informatique réduisent le temps d'attente et les chances des pirates informatiques d'atteindre leur objectif de nuire financièrement ou à la réputation de l'organisation.

Améliore la recherche des menaces

En exploitant les flux de Threat Intelligence les plus récents, le XDR améliore la recherche et la découverte de menaces, tandis que l'automatisation des tâches de routine, les processus d'enquête guidés et les détections personnalisables favorisent une résolution rapide des incidents. Les menaces avancées sont détectées et neutralisées plus rapidement et plus précisément, un atout indispensable pour lutter contre les attaques complexes et de type APT.

Contribue à remédier à la pénurie mondiale d'experts en sécurité informatique

Dans un contexte de pénurie mondiale d'experts en sécurité informatique, le XDR assure la protection globale d'une infrastructure informatique en expansion et en mutation face à un paysage de cybermenaces en évolution rapide. Le XDR simplifie le travail de ressources précieuses et rares (les spécialistes de la sécurité informatique), réduit leur rôle dans les tâches routinières et leur permet de se consacrer au traitement d'incidents complexes.

Permet la conformité réglementaire et la gestion des risques

Grâce à une visibilité complète, la Threat Intelligence et des rapports, les organisations peuvent démontrer leur conformité avec les réglementations et cadres de l'industrie, comme le RGPD, la norme PCI DSS, l'HIPAA et bien d'autres. Cela permet d'atténuer les risques juridiques et financiers liés à la non-conformité.

La gestion des journaux joue également un rôle crucial dans la mise en conformité avec les normes et réglementations industrielles ou régionales, en facilitant le stockage et la conservation des données et des journaux pendant la durée prescrite, et en permettant aux organisations de récupérer et d'analyser facilement les journaux si besoin.

Offre une gestion conviviale grâce à une console unique

Les solutions XDR conviviales fournissent des informations complètes sur les menaces en cours et les activités suspectes via une console unique. Cette approche permet une recherche proactive des menaces et une réponse plus rapide aux incidents, et offre une vue holistique qui aide les équipes SOC à identifier plus efficacement les activités suspectes ainsi que les incidents de sécurité potentiels.

Options de plateformes ouvertes et natives

Un XDR ouvert prend en charge les intégrations tierces pour collecter des formes spécifiques de données télémétriques afin de permettre la détection des menaces, la recherche et l'enquête à travers différentes sources de données et de mettre en place des actions de réponse. Cette approche permet aux organisations de ne pas être limitées à un seul fournisseur, de tirer parti de leurs outils de sécurité tiers déjà déployés et de choisir les produits les plus appropriés de différents fournisseurs.

Un XDR natif est une solution élaborée par un seul fournisseur et conçue pour fonctionner avec les produits de ce fournisseur.

Se déploie dans le cloud et/ou sur site

Bien que la grande majorité des plateformes de XDR soient ouvertes et basées dans le cloud, le déploiement sur site est idéal pour les organisations qui souhaitent garantir la souveraineté totale de leurs données et s'assurer de respecter les exigences réglementaires et de conformité.

S'intègre avec Zero Trust

Combinés, le XDR et Zero Trust constituent une défense efficace contre les cybermenaces. Zero Trust permet d'empêcher l'accès non autorisé aux ressources et aux applications ou de révoquer l'accès déjà accordé si les conditions ont changé, tandis que le XDR permet de détecter et de répondre aux menaces qui parviennent à contourner ces contrôles d'accès initiaux.

Comparaison entre XDR, SIEM et SOAR

XDR
Extended Detection and Response

SIEM
Security information and event management

SOAR
Security orchestration and automated response

Comment ça fonctionne ?

- Détecte de manière proactive les menaces complexes dans plusieurs niveaux de l'infrastructure et y répond automatiquement pour les contrer
- Intègre plusieurs outils et applications de sécurité
- Surveille les données sur les terminaux, les réseaux, les clouds, les serveurs Web, les serveurs de messagerie, etc. pour détecter et éliminer les menaces complexes

- Collecte, agrège, analyse et stocke les données de journaux de l'ensemble de l'infrastructure informatique en vue de divers cas d'utilisation, notamment la gestion et la conformité, ainsi que la correspondance des corrélations basée pour les activités suspectes
- Recherche de modèles ou d'événements susceptibles d'indiquer un comportement suspect et génère une alerte pour l'équipe SOC ou l'équipe de sécurité informatique

- Intègre des données provenant de diverses sources de l'infrastructure, notamment des systèmes de gestion et des plateformes de Threat Intelligence, et fournit une analyse de la priorité
- Permet aux équipes de sécurité de configurer des réponses automatisées en plusieurs étapes et multi-solutions aux menaces entrantes
- Utilise des guides pour automatiser un large éventail de flux de travail comme l'analyse de la vulnérabilité et des journaux, la gestion de l'accès des utilisateurs, le tri des menaces, etc.
- Organise plusieurs outils et processus disparates en un flux de travail plus large, en rassemblant toutes les données pertinentes sur une plateforme unique pour des informations consolidées et exploitables

Alors, quelles sont les différences ?

- L'approche par écosystème optimise l'efficacité des outils de cybersécurité mis en œuvre, économise des ressources et réduit le risque
- Simplifie le travail des spécialistes de la sécurité informatique et leur procure le contexte supplémentaire nécessaire pour enquêter sur les attaques perpétrées avec plusieurs vecteurs
- Minimise les temps moyens de détection et de réponse (MTTD et MTTR), ce qui est essentiel pour combattre les menaces complexes et les attaques ciblées
- Fournit une protection globale contre le paysage des menaces en évolution

- Immense quantité de données fournies par le SIEM, ce qui peut entraîner un trop grand nombre d'alertes à filtrer, traiter et analyser manuellement
- Ne fournit pas le contexte nécessaire pour faire face à des attaques nouvelles, complexes ou sophistiquées
- Solution passive sans capacités de blocage, de mise en quarantaine ou de réponse
- Optimal en parallèle à des solutions d'enquête et de réponse proactives comme le XDR ou le SOAR

- Nécessite un effort continu de la part d'un SOC hautement qualifié et mature pour maintenir une plateforme SOAR bien configurée qui s'intègre avec les outils des partenaires
- Sans ces personnels de maintenance qualifiés et vigilants, les analystes SOAR peuvent se retrouver avec un trop grand nombre d'alertes de faible priorité, de faux positifs, et d'un ensemble de données généralement incohérentes provenant des divers outils indépendants qui alimentent la plateforme, ce qui est exactement ce qu'ils cherchent à éviter

Comment justifier l'investissement dans le XDR ?

Outre les avantages techniques, il existe de bonnes raisons commerciales d'investir dans le XDR, comme l'atténuation des attaques, la détection des menaces internes, le cloud et la conformité, l'enquête et la réponse aux incidents, etc.

Atténuation des attaques

Si une organisation a été victime d'une attaque par ransomware qui a entraîné le chiffrement de données critiques et l'arrêt des opérations, les capacités de détection proactive des menaces du XDR auraient permis d'identifier et de prévenir ce type d'attaque avant qu'elle ne fasse des ravages, grâce à la capacité de détecter les comportements suspects, d'isoler les terminaux infectés et de fournir une réponse à incidents en temps réel, réduisant ainsi considérablement l'impact de l'attaque et rétablissant rapidement la continuité des activités.

Détection des menaces en interne

Les menaces internes, intentionnelles ou non, sont une préoccupation majeure pour la plupart des organisations. Mais comme le XDR offre une visibilité complète sur les terminaux, les réseaux, les applications et le cloud, elle peut détecter les signes révélateurs de menaces internes, comme les comportements anormaux des utilisateurs, les tentatives d'exfiltration de données et les accès non autorisés. En corrélant et analysant des données provenant de sources multiples, le XDR peut donc aider à identifier et à atténuer les menaces internes, à protéger les informations confidentielles et à maintenir l'intégrité des données.

Cloud et conformité

Alors que de plus en plus d'entreprises adoptent les technologies dans le cloud, garantir une sécurité et une conformité solides est plus important que jamais. En offrant une visibilité unifiée et une détection des menaces dans les environnements hybrides et multiclouds, le XDR permet aux entreprises de surveiller les charges de travail dans le cloud, de détecter les mauvaises configurations et d'identifier les activités suspectes, et ainsi de maintenir une infrastructure cloud sécurisée et conforme, tout en atténuant les risques associés aux attaques dans le cloud.

Réponse aux incidents et enquêtes

Des réponses rapides et des enquêtes approfondies sont essentielles pour minimiser les dommages et prévenir de futurs incidents. Le XDR simplifie les processus de réponse aux incidents en automatisant la détection des menaces, le tri des alertes et les procédures d'enquête, et en fournissant aux équipes de sécurité une vue d'ensemble des incidents leur permettant de réagir rapidement et efficacement. Les économies de temps et de ressources résultant des capacités de réponse automatisée du XDR changent la donne en matière de gestion des incidents.

Extension de l'EPP, de l'EDR, du SIEM etc.

La prévention des menaces décrites ci-dessus justifie amplement l'investissement dans le XDR, et pour les utilisateurs d'EPP, d'EDR, de SIEM et autres, le XDR renforce les performances de toutes ces solutions.

- Pour l'EPP, le XDR renforce les capacités de protection des terminaux en offrant une détection avancée des menaces, une automatisation des réponses et une meilleure visibilité sur les environnements réseau et cloud, ce qui en fait la suite logique des feuilles de route de sécurité et permet aux organisations d'atteindre un niveau de protection plus élevé contre les menaces en constante évolution.
- Pour l'EDR, le XDR (souvent construite sur l'EDR) étend les capacités de la solution au-delà de la détection et de la réponse centrées sur les terminaux, en fournissant une visibilité holistique et une détection des menaces à travers l'infrastructure protégée, y compris le réseau, les machines virtuelles, les applications et les environnements cloud, et en permettant une réponse aux incidents plus efficace et des capacités de recherche des menaces améliorées.
- Pour le SIEM, le XDR complète la solution en fournissant une détection des menaces en temps réel, des capacités de réponse avancées, ainsi qu'une visibilité et une corrélation améliorées des événements de sécurité sur les terminaux, les réseaux et le cloud, permettant une réponse plus rapide aux incidents et une réduction des délais d'enquête.

Pour ceux susceptibles d'investir prochainement dans la technologie XDR, la facilité d'utilisation est, de loin, l'avantage perçu le plus important pour leur organisation, qu'il s'agisse d'intégrer la technologie à leurs outils de sécurité existants ou de mettre en place une infrastructure d'un seul fournisseur prête pour le XDR. Les répondants ont également indiqué que les autres investissements à court terme dans des solutions permettant d'unifier la détection et la réponse et d'améliorer la visibilité des produits/services de sécurité concerneraient très probablement la détection et la réponse au niveau des terminaux (EDR), la détection et la réponse au niveau des réseaux (NDR), la gestion des informations et des événements de sécurité (SIEM) ainsi que la Threat Intelligence.

CRA Business Intelligence, XDR Poised to Become a Force Multiplier for Threat Detection, mars 2022

S'attaquer à l'ensemble des menaces

Dans de nombreuses organisations, les analystes de la sécurité passent aujourd'hui plus de la moitié de leur temps à trier les faux positifs au lieu d'identifier les menaces et d'y répondre de façon proactive, rallongeant ainsi considérablement les délais de détection.

Threat intelligence

Pour de nombreuses organisations, en particulier celles qui sont vulnérables aux attaques ciblées et aux menaces persistantes avancées (APT), la Threat Intelligence (TI) est un outil essentiel pour assurer une défense proactive contre les menaces. Cependant, si les utilisations et les avantages de la TI sont nombreux et variés, il en va de même pour leurs sources, ce qui signifie que déterminer ce qui conviendra le mieux à une organisation particulière peut constituer un défi en soi.

Dans de nombreuses organisations, les analystes de la sécurité passent aujourd'hui plus de la moitié de leur temps à trier les faux positifs au lieu d'identifier les menaces et d'y répondre de façon proactive, rallongeant ainsi considérablement les délais de détection. Alimenter vos opérations de sécurité avec une TI inexacte ou inappropriée augmentera le nombre de fausses alertes et aura une incidence négative importante sur vos capacités de réponse ainsi que sur votre sécurité dans son ensemble. Alors, comment éviter cette situation ?

Bien qu'il n'existe pas de critères universellement reconnus pour évaluer les offres commerciales de TI, les aspects à prendre en compte sont les suivants :

- Parmi un large éventail de fournisseurs, les organisations devraient rechercher une TI qui leur permette de mieux comprendre leur propre paysage de menaces, par exemple grâce à une analyse détaillée des menaces historiques et émergentes ciblant leur secteur d'activité ou leur zone géographique, afin d'améliorer les performances telles que la gestion des vulnérabilités, la recherche de menaces, la réponse aux incidents etc.
- Pour combiner efficacement la TI avec les outils, les contrôles et les processus de sécurité qu'une organisation utilise et connaît déjà, celle-ci doit trouver des méthodes, des mécanismes d'intégration et des formats pour une intégration harmonieuse de la TI dans ses opérations de sécurité existantes.
- Il est également important d'identifier une TI ayant une portée mondiale. Sachant que les attaques ne connaissent pas de frontières, le fournisseur recherche-t-il des informations au niveau mondial et rassemble-t-il des activités à première vue distinctes en campagnes cohérentes ? Ce type de renseignements permettra de prendre des mesures plus appropriées.
- Les organisations à la recherche d'un contenu plus stratégique pour éclairer leur planification de la sécurité à long terme devraient rechercher un fournisseur de TI ayant fait ses preuves en matière de découverte et d'enquête continues de menaces complexes dans leur zone géographique et/ou leur secteur d'activité.
- La faculté du fournisseur à adapter ses capacités de recherche aux particularités de chaque organisation est également cruciale.

La Threat Intelligence (TI) est une ressource en constante évolution. Pour être efficaces, les programmes internes de TI qui l'utilisent doivent l'être également. Comparez vos performances actuelles avec notre outil interactif d'évaluation de la TI et obtenez des recommandations d'amélioration personnalisées en fonction de vos réponses : https://go.kaspersky.com/ti_tool_2023.html

En outre, l'utilisation de Kaspersky Threat Intelligence Portal permet à une organisation de regrouper, de gérer et de rendre opérationnelle la TI, ce qui est essentiel lorsque les outils de sécurité utilisent la TI provenant de plusieurs sources. Plus concrètement, Kaspersky Threat Intelligence Portal doit permettre à l'organisation de :

- Répondre plus efficacement aux menaces en vérifiant tout indicateur de menace jugé suspect, qu'il s'agisse d'un fichier, d'un hachage de fichier, d'une adresse IP ou d'une adresse Internet.
- Analyser les fichiers pour détecter les menaces complexes, évasives et de type APT.
- Envoyer des adresses IP, des hachages de fichiers des adresses Internet ou des domaines jugés suspects, afin de valider et de hiérarchiser rapidement les alertes et les incidents à l'aide de niveaux de risque et d'informations contextuelles permettant de déterminer quelles sont les menaces réelles.
- Recevoir des rapports réguliers relatifs au fonctionnement de certains fichiers ou de certaines adresses Internet spécifiques.
- Automatiser les flux de sécurité en connectant les applications correspondantes à Kaspersky Threat Intelligence Portal.

Plus de 80 % des cyberincidents sont dus à l'erreur humaine

Sensibilisation à la sécurité

Plus de 80 % des cyberincidents sont dus à une erreur humaine, notamment parce que les solutions de cybersécurité se développent rapidement et s'adaptent à des menaces complexes, ce qui complique la vie des cybercriminels qui se tournent vers l'élément le plus vulnérable de la cybersécurité, le facteur humain. Voici quelques exemples des conséquences de cette situation :

- 52 % des membres de la direction déclarent que les employés constituent la plus grande menace pour la sécurité opérationnelle.
- 43 % des petites entreprises ont subi un incident de sécurité à la suite d'une violation des politiques de sécurité informatique par des employés.
- 60 % des employés ont des données confidentielles sur leur appareil professionnel (données financières, base de données de messagerie, etc.).
- 30 % des salariés reconnaissent qu'ils partagent l'identifiant et le mot de passe de leur PC professionnel avec des collègues

Une culture de la cybersécurité ainsi que des compétences fondamentales et une sensibilisation à la cybersécurité de toute l'organisation sont donc essentielles pour réduire la surface d'attaque et le nombre d'incidents auxquels l'équipe informatique doit faire face.

Comment Kaspersky peut vous aider

Kaspersky Next EDR Foundations

Kaspersky Next EDR Foundations offre une puissante protection des terminaux basée sur le ML, des contrôles de sécurité flexibles ainsi que des outils d'analyse EDR des causes profondes qui permettent aux organisations de construire facilement une base solide pour leur cybersécurité. Une console simple, un déploiement dans le cloud ou sur site, et diverses fonctionnalités favorisant la qualité de vie au travail réduisent la complexité et augmentent l'efficacité.

Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum offre une protection solide des terminaux, des contrôles améliorés, des formations, une gestion des correctifs et bien plus encore, le tout renforcé par des fonctionnalités EDR essentielles. La visibilité, l'enquête et la réponse aux menaces sont simples, rapides et guidées pour aider les équipes informatiques et de sécurité à repousser les attaques rapidement et avec un minimum de ressources.

Kaspersky Next XDR Expert

Kaspersky Next XDR Expert s'intègre notamment de manière transparente à l'infrastructure de sécurité existante d'une organisation, offrant une visibilité en temps réel et une connaissance approfondie de l'évolution des cybermenaces afin de fournir une détection avancée des menaces ainsi qu'une réponse automatisée, avec les fonctionnalités XDR essentielles décrites dans cet e-book.

Kaspersky Managed Detection and Response

Kaspersky MDR fournit une protection avancée 24h/24 contre le volume grandissant de menaces qui contournent les barrières de sécurité automatisées et soulage ainsi les organisations qui peinent à trouver du personnel spécialisé ou qui disposent de ressources limitées en interne. Ses fonctionnalités avancées de détection et de réponse s'appuient sur l'une des équipes de Threat Hunting les plus efficaces et expérimentées du secteur. Contrairement aux solutions similaires, Kaspersky MDR repose sur des modèles de ML brevetés, une Threat Intelligence (TI) continue et unique ainsi qu'une expérience éprouvée de recherche sur les attaques ciblées. Cette solution renforce automatiquement la résilience de votre entreprise face aux cybermenaces, tout en optimisant vos ressources existantes et vos futurs investissements de sécurité informatique.

Kaspersky Threat Intelligence

Le portefeuille de TI de Kaspersky couvre une gamme complète de scénarios de sécurité, notamment la prévention, la détection, l'enquête, la réponse et les rapports stratégiques, qui peuvent tous être adaptés aux besoins des organisations. Notre équipe Global Research and Analysis Team (GReAT) est un groupe d'élite d'experts qui, grâce à l'infiltration de communautés fermées et de forums obscurs dans le monde entier, a découvert et disséqué plus de 50 attaques ciblées parmi les plus sophistiquées au monde. Par ailleurs, nos connaissances et notre expérience approfondies dans tous les domaines de la cybersécurité font de nous le partenaire de choix des plus grandes autorités de police et administrations, comme INTERPOL et les CERT majeurs.

Parmi les exemples de nos solutions et services TI innovants, citons plus de 20 types de flux de données sur les menaces, une vaste gamme de rapports TI, une sandbox développée en interne pour détecter les menaces complexes et évasives, un portail ouvert de Threat Intelligence et des services, comme l'analyse personnalisée du paysage des menaces et Kaspersky Digital Footprint Intelligence, qui analyse les données de l'empreinte numérique pour identifier les menaces et les vulnérabilités potentielles.

Kaspersky Security Awareness

Kaspersky Security Awareness offre une gamme de solutions de formation attrayantes et efficaces qui renforcent la sensibilisation à la cybersécurité des employés à tous niveaux et les aident à jouer leur rôle dans la cybersécurité globale. Comme les changements de comportement durables prennent du temps, notre approche implique la mise en place d'un cycle d'apprentissage continu avec de multiples composantes, notamment des simulations de protection interactives couvrant une série de scénarios, des outils d'évaluation ludiques, une plateforme automatisée de sensibilisation à la sécurité proposant des simulations de campagnes de phishing, une formation pour les dirigeants etc.

Kaspersky Professional Services

Le portefeuille de services professionnels de Kaspersky comprend des services d'évaluation, de mise en œuvre, de maintenance et d'optimisation qui aident les organisations à relever leurs défis, à minimiser leurs risques de sécurité, à maximiser le retour sur investissement, à limiter la pression sur leurs ressources, à répondre rapidement aux nouvelles menaces de sécurité et à tirer le meilleur parti de leurs solutions Kaspersky.

Fiabilité

Proven. Transparent. Independent.

En 2017, Kaspersky a lancé l'initiative de transparence mondiale. Ainsi, contrairement à tout autre fournisseur concurrent, si vous avez des doutes concernant nos produits, vous êtes libre de consulter notre code source, nos mises à jour logicielles et nos règles de détection des menaces, ainsi que nos processus sécurisés de cycle de vie de développement et nos stratégies d'atténuation des risques liés aux logiciels et aux chaînes d'approvisionnement. Pour soutenir cette initiative, nous avons ouvert plus de 10 centres de transparence dans le monde, qui ont notamment reçu la visite de régulateurs, de fournisseurs d'infrastructures critiques, de clients, de partenaires et de médias. Enfin, pour répondre aux attentes de nos clients, notre entreprise a fait l'objet d'un audit SOC2, et nos produits sont certifiés ISO/IEC 27001.

Kaspersky Next EDR Foundations — En savoir plus

Kaspersky Next EDR Optimum — En savoir plus

Kaspersky Next XDR Expert — En savoir plus

Actualités des cybermenaces : securelist.fr
Actualités dédiées à la sécurité informatique : kaspersky.fr/blog/category/business
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security

kaspersky.fr

Pour en savoir plus à propos de Kaspersky Next, consultez le site : https://go.kaspersky.fr/next

Choisissez le niveau qui vous convient le mieux en répondant à un bref questionnaire dans notre outil interactif : https://go.kaspersky.com/Kaspersky_Next_Tool