XDR

Plus puissant, plus performant, plus rapide

Le potentiel d'innovation du XDR

kaspersky BRING ON THE FUTURE

Une solution révolutionnaire ou banale ?

XDR : Extended Detection and Response

Cet acronyme est sur toutes les lèvres, mais comme pour toutes les technologies relativement récentes, tout le monde ne sait pas exactement de quoi il s'agit ni ce qu'elles peuvent signifier dans les entreprises. Une chose est sûre : le XDR implique un changement stratégique de la réactivité à la proactivité, car l'attentisme n'est pas de mise en matière de cybersécurité. Il est judicieux de considérer le XDR comme une stratégie plutôt que comme un simple produit.

Le XDR est-il une nouvelle technologie banale ou est-il susceptible de changer la donne ? Le potentiel est certainement présent en raison de la pénurie mondiale de compétences, de la surcharge de travail du personnel chargé de la sécurité informatique, des diverses menaces qui ne s'arrêtent jamais, du trop grand nombre d'alertes, des outils disparates, de la faiblesse de la Threat Intelligence et de l'expansion de la surface d'attaque. IDC estime que le XDR sera « une force perturbatrice qui aura un impact sur les ventes de plateformes SIEM, EDR, SOAR, d'intelligence réseau et d'analyse des menaces, ainsi que sur les fournisseurs de Threat Intelligence externe »[1], et Forrester pense que la technologie XDR différenciée « supplantera la détection et la réponse aux terminaux (EDR) à court terme et supplantera les SIEM à long terme »[2].

À qui le XDR s'adresse-t-il ?

Le XDR s'adresse aux organisations qui disposent d'une politique de sécurité bien établie et qui ont besoin d'une plateforme unique leur fournissant une image complète et cohérente de ce qui se passe dans l'ensemble de leur infrastructure.

Le XDR sera une force perturbatrice – IDC

Plus d'appareils, plus d'applications, plus de trafic réseau, plus de données, plus de menaces…

À qui s'adresse le XDR et quels sont les défis qu'il permet de relever ?

Le XDR s'adresse aux organisations qui disposent d'une politique de sécurité bien établie et qui ont besoin d'une plateforme unique leur fournissant une image complète et cohérente de ce qui se passe dans l'ensemble de leur infrastructure.

Les défis auxquels ces organisations sont confrontées en matière de cybersécurité sont constants et bien connus. ESG Research a interrogé des professionnels de l'informatique et de la cybersécurité[3] dans des organisations comptant 100 employés ou plus, dans de multiples secteurs verticaux. Voici quelques-unes des principales conclusions :

Difficultés pour répondre aux exigences opérationnelles des technologies SOC

La gestion des opérations de sécurité est plus difficile aujourd'hui qu'elle ne l'a jamais été au cours des deux dernières années, en raison des difficultés à suivre les besoins opérationnels des technologies SOC – extensibilité du pipeline de données, équilibrage des charges des moteurs de traitement, augmentation de la capacité de stockage, etc.

[1] Source : Analyse des produits de sécurité mondiaux de l'IDC : From Power Point to Power Product, Where Is XDR Right Now? 2022

[2] Source : Forrester, Extended Detection and Response (XDR) – A Battle Between Precedent and Innovation, Allie Mellen, Senior Analyst, 2021

[3] Source : ESG Research Report, SOC Modernization and the Role of XDR, 2022

La surface d'attaque croissante et en constante évolution, et le paysage des menaces dans son ensemble

Plus d'appareils, plus d'applications, plus de trafic réseau, plus de données, plus de menaces. Le paysage des menaces ne cesse de changer, et les cybermenaces évoluent sans cesse en volume et en complexité à mesure que de nouveaux outils prolifèrent. Dans le même temps, les programmes malveillants n'ont jamais été aussi accessibles pour les pirates informatiques, avec d'un côté des acheteurs peu qualifiés de menaces bon marché sur le Dark Web, et de l'autre des pirates hautement qualifiés et patients qui élaborent des attaques complexes. Sans oublier les menaces internes et les vulnérabilités liées à la chaîne d'approvisionnement.

Le nombre élevé de processus manuels nécessaires à la gestion de la sécurité

Les données de sécurité à collecter et à traiter sont de plus en plus nombreuses, et le traitement manuel de ces données est inefficace. Il en résulte une situation explosive qui a un impact sur l'évolutivité, entraîne une dépendance excessive à l'implication humaine directe et réduit l'efficacité de la gestion des menaces en général.

Une incapacité à développer des règles de détection

Une incapacité à développer des règles de détection, affiner les contrôles de sécurité et identifier et traiter les menaces rapidement et efficacement, en raison d'un manque de temps, de ressources et de compétences. Les organisations ne disposent pas toujours des compétences ou du personnel nécessaires pour suivre l'évolution des analyses et des opérations de sécurité. Cette situation nous amène directement au problème suivant.

La pénurie mondiale de compétences

Bien que la main-d'œuvre mondiale dans le domaine de la cybersécurité a atteint un niveau record de 4,7 millions de professionnels, un déficit de 3,4 millions de personnes doit encore être comblé, en vain pour l'instant. Cet écart se creuse deux fois plus vite que l'augmentation de la main-d'œuvre, avec une augmentation de 26,2 % par an.[4]

[4] Source : (ISC)², Cybersecurity Workforce Study, 2022

Les outils existants peinent souvent

à détecter et à étudier les menaces avancées, et des compétences spécialisées sont nécessaires pour les utiliser et les gérer.

88 %

des organisations dépenseront davantage cette année pour améliorer les SecOps

66 %

déclarent que la consolidation des outils est une priorité

Outils inadaptés

Lorsque les outils eux-mêmes deviennent une partie du problème, quelque chose doit changer. Les outils existants peinent souvent à détecter et à étudier les menaces avancées, et des compétences spécialisées sont encore nécessaires pour les utiliser et les gérer. Des études[5] montrent que les outils actuels sont souvent inefficaces pour corréler les alertes et que le personnel chargé de la sécurité informatique est confronté à de multiples outils déconnectés et disparates traitant des données différentes. Ce processus est inefficace, lourd, désordonné et coûteux. Un autre défi est que les outils actuels ne sont pas adaptés à l'expansion de la surface d'attaque et qu'il existe de grandes lacunes dans les capacités de détection et de réaction dans le cloud[6].

Faut-il s'étonner que votre RSSI ait l'air stressé ?

La bonne nouvelle est que l'amélioration des opérations de sécurité (SecOps) est une priorité, et qu'elle est financée – 88 % des organisations dépenseront davantage cette année, 66 % déclarent que la consolidation des outils est une priorité, et le développement et le déploiement d'applications modernes se sont accélérés, ce qui appelle de nouvelles compétences[7].

Que fait le XDR ?

Voici comment le XDR peut relever ces défis.

Le XDR détecte mieux les menaces avancées

Les capacités de détection des menaces du XDR couvrent les terminaux, les réseaux et les environnements cloud. Cette technologie utilise des algorithmes de machine learning et d'analyse comportementale pour détecter les menaces complexes, notamment les programmes malveillants, les ransomwares et les menaces persistantes avancées (APT).

Réponse et correction automatisées

Le XDR automatise les réponses et les corrections, permettant aux organisations de contenir les menaces rapidement et de minimiser les dommages potentiels. Il permet de mettre automatiquement en quarantaine les terminaux compromis ou de les isoler, de bloquer les activités malveillantes et de remédier aux vulnérabilités, en réduisant les efforts manuels ainsi que le temps de réponse.

Intégration avec les outils de protection des terminaux

L'intégration avec l'EPP est un aspect essentiel, et le XDR exploite les données télémétriques et l'analyse comportementale des terminaux pour fournir des informations détaillées sur les activités de ces derniers. Elle utilise des algorithmes avancés de machine learning pour identifier les comportements suspects et les indicateurs d'attaques (IOA), facilitant ainsi la détection précoce des menaces complexes.

[5] Source : ESG Research Report, SOC Modernization and the Role of XDR, May 2022

[6] Source : ESG Research Report, SOC Modernization and the Role of XDR, 2022

[7] Source : ESG Research Report, SOC Modernization and the Role of XDR, May 2022

La place du XDR dans l'écosystème EDR, MDR, SOAR et SIEM

La réponse est dans le X — « extended », ou étendu. Le XDR étend les capacités offertes par l'EDR pour détecter de manière proactive des menaces complexes à plusieurs niveaux d'infrastructure, et pour répondre automatiquement à ces menaces et les contrer.

Une approche intégrée est essentielle

En intégrant de multiples outils et applications de sécurité, et en surveillant les données sur les terminaux, les réseaux, le cloud, les serveurs Internet, les serveurs de messagerie, etc. le XDR permet de détecter et d'éliminer les menaces tout en simplifiant la gestion de la sécurité de l'information grâce à l'automatisation de l'interaction entre les produits.

Forrester estime que, dans la plupart des cas, le XDR ne remplacera pas totalement les plateformes d'analyse de la sécurité, notant que « le XDR est en plein essor et [nous] prévoyons qu'au cours des cinq prochaines années, les plateformes d'analyse de la sécurité et le XDR se rencontreront ».

Le système SIEM a des cas d'utilisation qui vont au-delà de la détection des menaces, et la personnalisation du SOAR est utile, mais lorsqu'il s'agit de détecter et de répondre aux menaces, les analyses avancées de la protection renforcée du XDR sont inégalées.

Offre une visibilité en temps réel

Le XDR offre une visibilité en temps réel de la sécurité de votre organisation. Il recueille et analyse des données provenant de diverses sources, comme les terminaux, les serveurs, les pare-feux et les plateformes cloud, afin de fournir des informations complètes sur les menaces en cours et les activités suspectes dans une console unique. Il s'agit donc d'une solution véritablement proactive, qui permet de détecter les menaces de manière efficace et de réagir plus rapidement en cas d'incident. Une vision globale permet aux équipes de sécurité de détecter plus précisément les activités suspectes et les incidents de sécurité potentiels.

Contextualisation des données et de la Threat Intelligence

Lorsqu'il exploite une Threat Intelligence de haute qualité et une base de données complète, le XDR fournit des informations contextuelles très utiles sur les menaces et les pirates informatiques. Cette Threat Intelligence enrichie simplifie les alertes et le traitement des incidents, et aide les équipes de sécurité à comprendre les tactiques, les techniques et les motivations des acteurs de la menace, permettant ainsi de répondre plus efficacement aux incidents et de mettre en place des mesures de défense proactives.

Permet de rationaliser les opérations de sécurité

Correctement intégrées, les meilleures solutions s'insèrent sans effort dans votre infrastructure actuelle afin de produire les meilleurs résultats en matière d'automatisation, et offrent une visibilité et une sensibilisation totales sans avoir à remplacer les solutions de sécurité tierces déjà utilisées. Et n'oubliez pas qu'en fournissant une vue d'ensemble des incidents de sécurité et du comportement des utilisateurs, l'intégration favorise la conformité.

Il est clair que le XDR est en mesure d'offrir ce qu'il promet : contrôle, stabilité et ce petit plus. Mais toutes les offres de XDR ne se valent pas… Comment choisir celle qui vous convient le mieux ?

5 éléments clés à prendre en compte pour comparer les fournisseurs et les solutions de XDR

Voici comment le XDR peut relever ces défis.

1

Il existe un lien direct entre la qualité d'une solution XDR et la synergie entre l'EPP et l'EDR du fournisseur

Une solution EDR pour la détection avancée et la réponse aux cybermenaces complexes au niveau des terminaux est un élément central du XDR. Parallèlement, l'EDR a besoin d'une plateforme de protection des terminaux (EPP) robuste pour trier automatiquement un grand nombre de menaces de masse. Il est important d'examiner attentivement les fonctions de protection des terminaux et de vérifier qu'elles prennent en charge tous les types de terminaux – PC, ordinateurs portables, machines virtuelles, appareils mobiles et divers systèmes d'exploitation.

2

Une Threat Intelligence à jour et une vision complète des tactiques et techniques des cybercriminels sont essentielles pour contrer les cybermenaces

Ce n'est pas sorcier – toute solution XDR digne de ce nom offrira ces deux capacités, ainsi qu'une fonction supplémentaire permettant d'améliorer et d'accélérer les enquêtes et la réponse aux incidents.

3

L'intégration avec des solutions tierces est plus durable et plus rentable

La qualité de l'intégration d'une solution XDR avec des tiers est une autre question cruciale, car l'interopérabilité fait de l'achat un investissement plus durable dès le départ. Une solution XDR qui offre de nombreuses et véritables options d'intégration collectera davantage de sources de données et fournira une image plus complète de la situation dans votre infrastructure.

4

Des avis indépendants, une reconnaissance mondiale et des résultats de tests indépendants comptent

Lorsque vous investissez dans un domaine aussi important pour votre entreprise que la cybersécurité, ne négligez pas les évaluations indépendantes. Demandez des résultats de tests indépendants. Vérifiez la reconnaissance internationale par des organismes, comme Forrester, IDC et autres. Les solutions sont-elles mises en œuvre dans le monde entier ? Demandez des études de cas.

5

Votre investissement est-il évolutif ?

La technologie n'est pas figée et, surtout pour un produit comme le XDR, qui est encore une technologie relativement jeune, il convient de se renseigner sur la politique du fournisseur en ce qui concerne le développement continu du produit.

Pourquoi Kaspersky ?

La protection la plus testée et la plus récompensée.

Kaspersky est une entreprise mondiale de cybersécurité bien établie, qui a donné les preuves de son expertise en matière de cybersécurité. Nous protégeons des organisations dans le monde entier depuis plus de 25 ans et avons reçu d'innombrables prix et distinctions pour nos produits et services. Entre 2013 et 2022, les produits Kaspersky :

587

ont réussi à obtenir 587 premières places

685

ont réussi à se classer 685 fois parmi les trois premiers

827

ont participé à 827 études et avis indépendants

En 2023, Kaspersky a été désigné leader du marché des solutions XDR par le cabinet mondial de recherche et de conseil en technologies ISG. ISG définit les « leaders » comme des entreprises proposant une offre complète de produits et de services et faisant preuve d'innovation et de stabilité concurrentielle.

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture