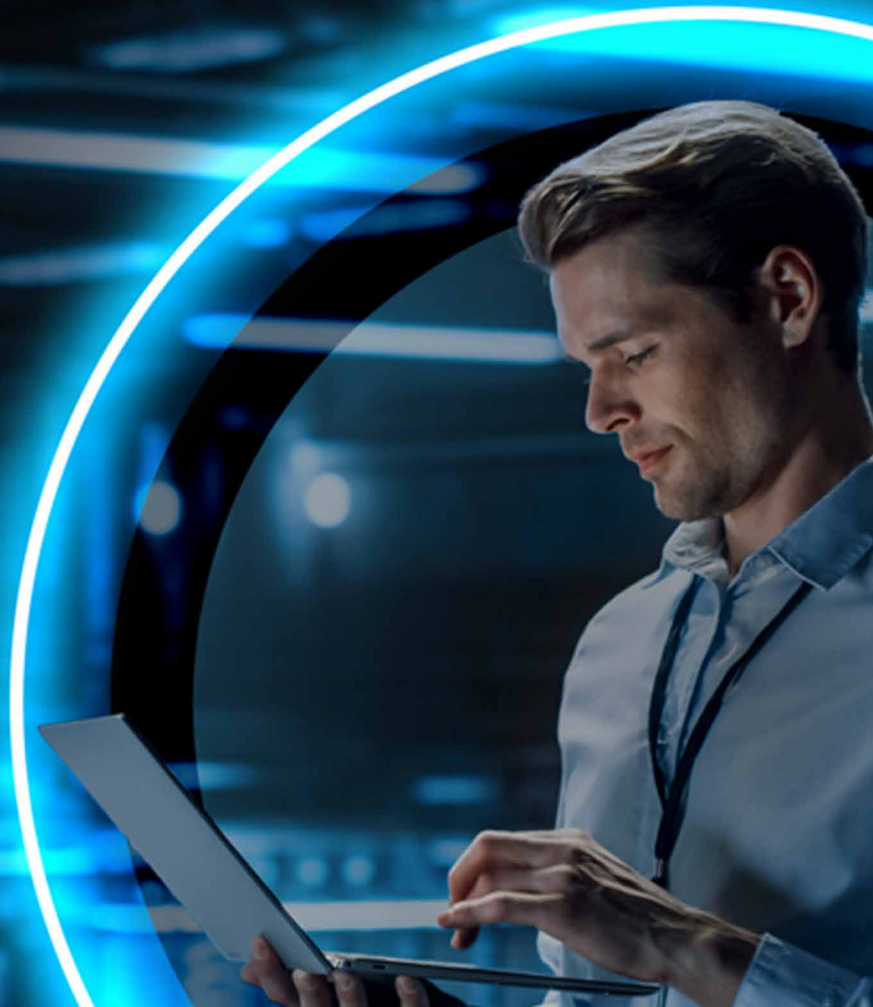
Le XDR expliqué : une approche stratégique de la gestion des menaces



Barracuda

La défense est difficile

La défense des systèmes d'entreprise devient chaque jour plus complexe. Votre réseau n'a plus de limite clairement définie. L'infrastructure informatique des entreprises évolue et s'étend en permanence, souvent sans la supervision des équipes informatiques ou de sécurité. De par leur nature même, les systèmes cloud et hybrides sont flexibles et peuvent être modifiés instantanément, souvent par les entreprises et non par les équipes informatiques.

Barracuda

Les attaques sont plus faciles

La barre pour lancer des attaques a également été abaissée. Les pirates n'ont plus besoin de savoir manier les outils de piratage ou un botnet : il leur suffit de s'abonner à une plateforme de ransomware-as-a-service et de spécifier une cible. Certaines de ces plateformes de piratage sont même disponibles sans frais initiaux en échange d'une part des bénéfices extorqués lors d'attaques réussies.

Les pirates ne dépendent pas d'un seul outil ou d'une seule stratégie pour attaquer leurs cibles. Les attaques se présentent désormais sous diverses formes, mettant à l'épreuve les défenses non seulement au niveau du périmètre, mais aussi à l'intérieur et à l'extérieur d'une organisation.

Les acteurs malveillants utilisent l'automatisation pour balayer en permanence les systèmes à la recherche de vulnérabilités. Les attaques sont de plus en plus intelligentes, multiformes, ciblées et sophistiquées. Avec l'aide de l'IA, les attaques par phishing et sur les réseaux sociaux visant à voler les identifiants d'accès aux systèmes sont décuplées. Les gangs organisés ne passent pas forcément à l'action immédiatement une fois qu'ils ont pénétré un réseau. Ils peuvent prendre leur temps pour observer la situation et planifier leurs prochaines étapes. Ils ont les moyens d'attendre, car ils sont souvent bien financés par le succès des attaques précédentes et, dans certains cas, par des États-nations.

Les compétences en matière de sécurité restent rares

Il subsiste une pénurie mondiale de professionnels formés et compétents en cybersécurité. Trouver et garder les bonnes personnes est coûteux et prend du temps pour tout responsable ou directeur informatique. Et le nombre de postes vacants en cybersécurité ne cesse de croître.

Une étude de l'ISC2 (PDF), l'association des professionnels de la cybersécurité, a révélé une pénurie considérable de professionnels de la cybersécurité dans le monde. « Nous estimons la taille des effectifs mondiaux en cybersécurité à 5,5 millions, soit une augmentation de 9 % par rapport à 2022, le chiffre le plus élevé que nous ayons jamais enregistré. À l'inverse, le déficit mondial de main-d'œuvre continue de se creuser encore plus rapidement : l'écart a augmenté de 13 % par rapport à 2022, ce qui signifie qu'en 2023, il faudra environ 4 millions de professionnels de la cybersécurité dans le monde. La profession doit presque doubler ses effectifs pour être à pleine capacité.

Surcharge d'alertes et fatigue

La sophistication de plus en plus poussée des outils et des défenses de cybersécurité s'accompagne de nouveaux défis. Alors que les équipes de sécurité n'avaient autrefois qu'une poignée de systèmes défensifs à gérer et à surveiller, elles ont désormais affaire à de multiples sources d'information. Ce sont davantage d'alertes à évaluer et davantage de décisions à prendre. Les équipes décident des dizaines de fois par jour si une alerte nécessite une action immédiate ou s'il s'agit d'un faux positif qui peut être ignoré en toute sécurité.

À terme, votre personnel s'épuise, le risque d'erreurs augmente et les problèmes de turnover se multiplient.

Les équipes de sécurité ont plus de travail et moins de temps pour réfléchir de manière stratégique à la façon de protéger l'entreprise. Vos collaborateurs très bien rémunérés se transforment en secouristes : ils s'emploie à combattre les incendies avant de penser à l'avenir.

Barracuda

Qu'est-ce que l'eXtended Detection and Response ?

L'Extended Detection and Response (XDR) ou détection et réponse étendues offre un référentiel unique pour les données de sécurité et la télémétrie, ainsi qu'une capacité d'analyse permettant d'exploiter ces données et d'accélérer la détection des menaces. Les détails peuvent varier légèrement selon l'analyste ou le fournisseur à qui vous posez la question, mais ce sont les grandes lignes. Le XDR fournit également des réponses automatisées aux incidents basées sur des playbooks et des plans préalablement convenus.

Une autre façon de considérer le XDR est de le voir comme une évolution du système Endpoint Detection and Response (EDR) qui enregistre les ordinateurs portables, les ordinateurs de bureau et les serveurs et collecte leurs données de sécurité pour rechercher des indicateurs de compromission.

Parallèlement, les systèmes de détection et de réponse du réseau vérifient et collectent les journaux des appareils sur le réseau et analysent le trafic entrant, sortant et interne du réseau de l'entreprise.

Le XDR utilise les données de sécurité générées par chacune de ces sources et potentiellement par d'autres, et aide les analystes de sécurité à les interpréter. Ils peuvent ainsi mieux comprendre la situation et distinguer les menaces réelles des fausses alarmes.

Barracuda

Quels sont les avantages de XDR ?

Comme le XDR rassemble tous vos instruments de sécurité en un seul endroit et automatise l'analyse, la détection et la réponse, les détections sont plus précoces et vos équipes peuvent réagir plus rapidement en cas d'attaque réelle.

Le XDR peut vous faire économiser de l'argent et du temps. Une étude d' Enterprise Strategy Group (ESG) montre que le XDR peut faire le travail de huit personnes à temps plein. Dans un monde où le recrutement et la fidélisation du personnel de sécurité est un défi, cela donne un coup de pouce à votre équipe.

Il permet de transformer la masse de données de sécurité et de télémétrie non structurées en une ressource utile et informative.

Le XDR exploite le fait que les attaques sont désormais menées sur plusieurs fronts : il ne s'agit plus seulement d'attaques de phishing contre votre service financier. Étant donné que les pirates observent l'ensemble de votre organisation, vous devez disposer de systèmes défensifs qui font de même. Les plateformes XDR bien connectées exploitent les points forts d'une attaque sur plusieurs fronts et les transforment en faiblesse. En repérant les anomalies dans les systèmes, elles peuvent réagir et contenir les attaques plus rapidement.

À quoi sert un système XDR ?

Si capacités de précision peuvent varier, la plupart des systèmes XDR présentent les mêmes fonctionnalités. Ils rassemblent toutes vos données de sécurité en un seul endroit, effectuent une analyse de ces données pour une détection rapide et automatisent les réponses si un incident nécessite une intervention.

Tout d'abord, ils offrent une surveillance de la sécurité des points de terminaison, une analyse du trafic réseau et des journaux système, et repèrent les connexions, les liens et les corrélations qui peuvent indiquer une attaque ou une autre activité inhabituelle.

Surtout, ces fonctionnalités incluent la télémétrie depuis le cloud, pas seulement votre réseau local. Le XDR intègre également la télémétrie des systèmes de messagerie, des firewalls et du trafic réseau. L'ensemble permet d'accélérer la détection et la réponse aux incidents et de réduire le temps passé à se connecter à des systèmes disparates pour l'instrumentation et la vérification des alertes.

Ensuite, le XDR offre un certain degré d'analyse intelligente des données qu'il rassemble. Il peut par exemple examiner le comportement des utilisateurs par rapport à une norme prédéfinie. Il peut repérer un accès utilisateur anormal ou des privilèges élevés indiquant un possible piratage de compte. Il examine le trafic réseau à la recherche d'exfiltrations de données.

Enfin, les systèmes XDR sont capables de répondre automatiquement aux attaques. Ils suivent généralement pour cela un protocole de réponse aux incidents établi qui prévoit, entre autres, le blocage des adresses IP suspectes.

Cette automatisation permet de garantir une réponse aussi rapide et efficace que possible. Elle permet également au personnel de se concentrer sur l'ensemble de la situation en cas d'incident et de ne pas s'enliser dans les tâches manuelles nécessaires au verrouillage et à la sécurisation des systèmes.

Mais le plus grand avantage du XDR est sans doute la visibilité qu'il procure.

Un système XDR correctement configuré offre une vue unique sur l'état de la sécurité de votre organisation en temps réel. Le personnel ne passe pas son temps à consulter les journaux d'accès, la télémétrie du réseau et les alertes de firewall puisque tout est rassemblé au même endroit, sur un seul écran.

Les équipes de sécurité peuvent ainsi anticiper le flot interminable d'alertes, ce qui leur laisse le temps et la capacité mentale de réfléchir sans se laisser happer par la réponse aux incidents.

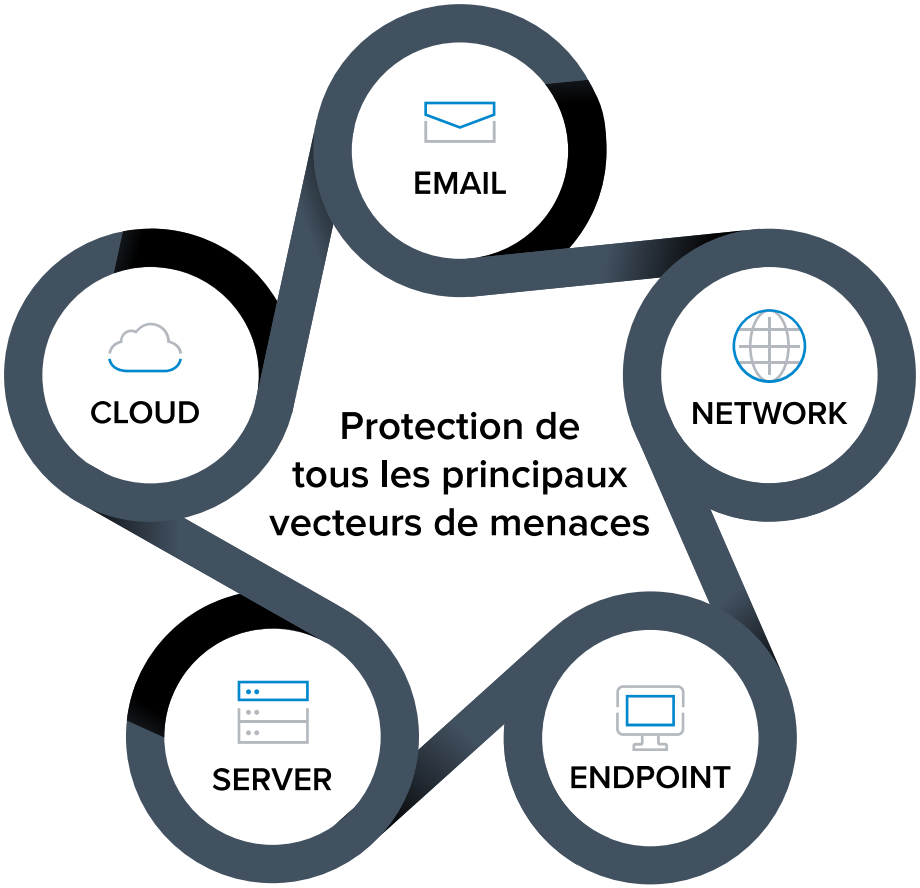
Choisir un fournisseur XDR

Le plus important est de ne pas considérer le XDR comme un simple complément à votre arsenal de sécurité. Il doit être central et entièrement intégré à tous les composants clés que vous utilisez.

Le point fort du XDR est la vue d'ensemble qu'il offre à votre équipe de sécurité sur l'ensemble de vos actifs numériques. Vous devez donc vous assurer que le système fonctionne avec les outils que vous avez.

Il doit aussi pouvoir se connecter facilement à d'autres sources de données et systèmes tiers, aujourd'hui et à l'avenir. Par conséquent, sa compatibilité et son développement futur doivent être clairement établis afin que vous puissiez planifier l'avenir de manière stratégique et sécurisée.

Face à un paysage de menaces en constante évolution et à l'essor des technologies et sources de données nécessaires pour assurer votre défense, votre fournisseur XDR doit posséder les compétences requises pour suivre le rythme d'un monde en mutation rapide.



Conclusion

Le XDR n'est pas une solution miracle. C'est cependant un outil essentiel pour aider vos équipes de sécurité à devancer les pirates et à utiliser au mieux les contrôles de sécurité existants. Il leur procure un moyen rapide d'exploiter les données que vous générez déjà et d'ajouter de nouvelles sources de télémétrie aisément. Il leur offre une meilleure visibilité en temps réel sur l'état de la sécurité des systèmes et accélère la détection des menaces et la réponse.

La solution Barracuda Managed XDR vous permet de bénéficier de toutes ces fonctionnalités, ainsi que du soutien de son centre des opérations de sécurité dont les analystes sont à votre disposition 24/7.

Notre équipe analyse en permanence les événements provenant de plus de 40 sources de données et les associent à des règles de détection des menaces pour assurer votre sécurité et celle de votre infrastructure.

En savoir plus sur Barracuda XDR.

Barracuda

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda. Nous pensons que chaque entreprise doit se doter de solutions cloud-first, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients. Plus de 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business. Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda