The bridge to possible

Guide d’achat des solutions de XDR

Évoluer en pro dans le marché émergent de la détection et de l’intervention étendues (XDR)

Comprendre la détection et l'intervention étendues (XDR)

Pourquoi le monde a-t-il besoin d'une autre approche de sécurité?

Même les équipes de sécurité les plus confiantes et les mieux financées savent qu'elles sont confrontées à des pressions externes écrasantes. Le récent passage au télétravail ou au travail ou hybride a introduit de nouveaux niveaux de complexité. La surface d'attaque est en expansion constante. Les alertes sont sans fin. Les outils de sécurité sont incompatibles. En raison de toutes les frictions entre les personnes et la technologie, il n'est pas étonnant que l'efficacité de la sécurité stagne et que les durées moyennes d'intrusion demeurent autour de 280 jours[1].

Cette nouvelle normalité exige de la résilience en matière de sécurité, la capacité de protéger l'intégrité de chaque aspect de votre entreprise pour résister aux menaces ou aux changements imprévisibles, et en sortir plus forte. Et la résilience en matière sécurité exige plus que ce que le passé a offert.

Principales raisons d'explorer la XDR :

- Réduire la fatigue liée aux alertes
- Accélérer la détection
- Augmenter la visibilité sur l'ensemble des outils
- Obtenir un meilleur contexte sur les menaces

[1] La recherche du Ponemon Institute présentée dans le rapport d'IBM sur le coût d'une violation de données de 2020

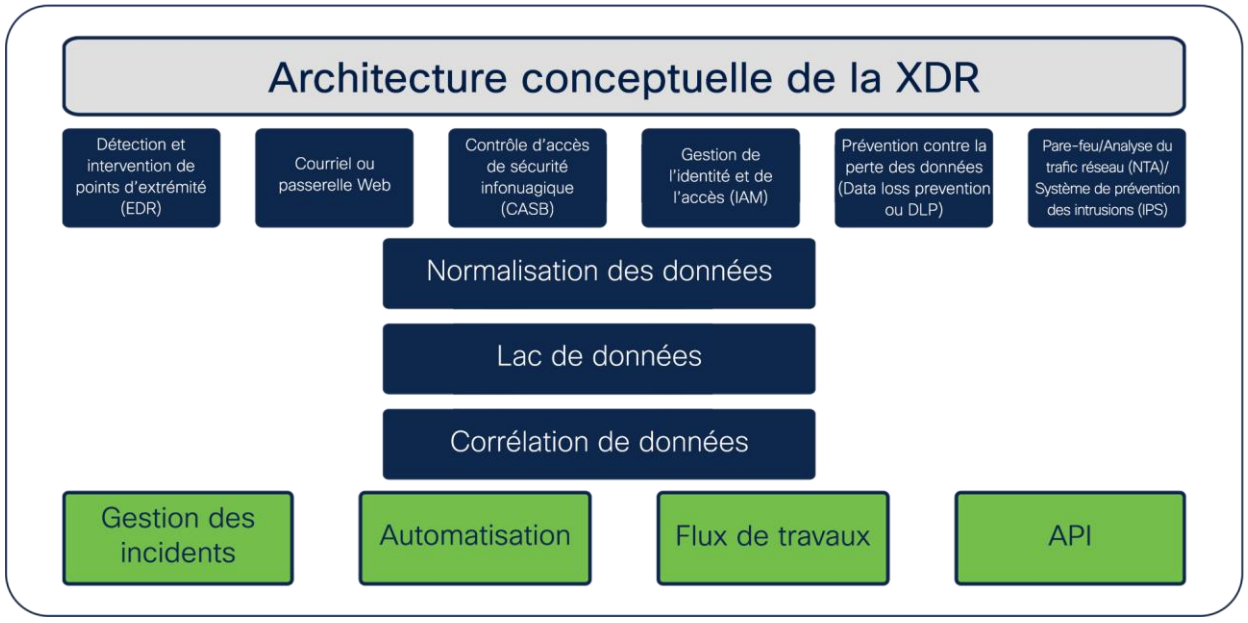
Qu’est-ce que la XDR exactement et pourquoi m’y intéresser?

Bien que l’intégration avec les solutions de points de sécurité natives au sein de la solution de XDR soit extrêmement bénéfique, il est également essentiel pour une plateforme de XDR d’exploiter et de se connecter facilement aux technologies tierces existantes afin d’offrir un meilleur rendement du capital investi et un contexte plus riche pour toutes les sources de données. Il s’agit d’un changement de paradigme important par rapport aux stratégies existantes où la détection et l’intervention se font principalement au sein des équipes et des silos de produits individuels. L’unité qu’offre la XDR a une incidence sur plusieurs domaines clés pour chaque équipe de sécurité :

Tout d’abord, elle offre une valeur rapide pour les équipes avec peu ou pas d’étalonnage. Pour les équipes qui ont déjà configuré des solutions d’information de sécurité et de gestion des événements (SIEM) ou une orchestration, automatisation et intervention de sécurité (SOAR), les plateformes de XDR tirent parti de ces avantages.

Deuxièmement, elle atténue la fatigue liée aux alertes qui afflige tant d’équipes, car la plateforme regroupe et met en corrélation tous les événements disparates causés par le même incident d’intrusion.

Troisièmement, il offre des éléments d’automatisation et d’orchestration prêts à l’emploi qui aident les équipes à éliminer les tâches de routine pour leurs activités quotidiennes.



Cinq éléments clés d'une détection et d'une intervention étendues (XDR) appropriées

1. Télémétrie coordonnée de n'importe où dans votre environnement

L'étendue de la visibilité et la profondeur des informations doivent être essentielles à la solution de XDR. À l'heure actuelle, les fournisseurs positionnent leurs produits existants en tant que composants clés de la XDR. Or, la véritable XDR doit relier non seulement les données, mais aussi la télémétrie de la plus grande variété de catégories de contrôle de sécurité, de référentiels de données et de fournisseurs d'informations sur les menaces pour déterminer la probabilité d'intentions malveillantes. Grâce à la XDR, les entreprises peuvent combler les lacunes et mettre en place une défense omniprésente dans l'ensemble de l'écosystème grâce à une plateforme ouverte et intégrée sur le campus, le centre de données, le nuage et la périphérie du nuage. Grâce au riche contexte tiré de chacune de ces solutions intégrées dans la XDR, vous pouvez trouver les vulnérabilités et les corriger plus rapidement.

Principales fonctions	Questions à poser
Informations complètes sur l'environnement	Comment votre solution m'offre-t-elle plus qu'une simple visibilité sur mon réseau?
Télémétrie exploitable	Utilisez-vous un lac de données pour fournir des informations ou autre chose qui offre une télémétrie plus percutante?
Sources fiables de données	Comment votre solution assure-t-elle que je reçois le contexte dans tous les terminaux, les périphériques et le trafic entrant et sortant de mon réseau?

2. Tirez parti de la fonctionnalité de détection de vos investissements existants, quel que soit le fournisseur

Bien que Gartner mentionne les composants propriétaires dans sa définition de la XDR, il est essentiel qu'une solution de XDR soit conçue selon une approche de plateforme ouverte qui se connecte facilement aux technologies tierces. Chaque composant de votre pile de sécurité possède des éléments de détection uniques (détection des indicateurs de compromission [IoC], apprentissage automatique, analyse comportementale, etc.) et chacun devient plus puissant lorsqu'ils sont réunis. Les signaux faibles des silos deviennent des signaux forts dans l'ensemble. La collaboration entre les fonctions de détection est essentielle à la XDR. Assurez-vous donc que la plateforme que vous choisissez fonctionne avec l'ensemble de votre pile.

Principales fonctions	Questions à poser
Tirez parti de vos solutions	Sur combien de mes investissements existants votre approche de XDR peut-elle tirer parti?
Indépendance des fournisseurs	En quoi vos technologies de détection diffèrent-elles des autres technologies sur le marché?
Intègre des analyses tierces	Lesquelles de vos solutions ont des intégrations prêtes à l'emploi les unes avec les autres?

3. Un contexte unifié à partir de sources fiables qui prennent en charge une intervention rapide et précise

L'unification des informations provenant du réseau, des points d'extrémité et des courriels (pour n'en nommer que quelques-uns) permet de comprendre plus précisément ce qui s'est passé, comment cela a progressé et quelles mesures doivent être prises pour éliminer la menace. Une solution de XDR efficace nécessite des capacités d'intervention et de correction natives, comme l'isolation d'un hôte ou la suppression d'un courriel malveillant de toutes les boîtes de réception. Idéalement, ces mesures seraient possibles en un clic ou deux. La XDR doit également faciliter la création de mesures d'intervention personnalisées afin que les équipes puissent faire évoluer leur sécurité au fil du temps.

Principales fonctions	Questions à poser
Informations contextuelles	Puis-je utiliser votre XDR pour comprendre l'effet d'une menace et l'étendue de la violation et prendre des mesures en un seul clic à partir d'une seule interface?
De multiples sources de vérité	Quel type d'informations sur les menaces alimente votre détection et d'où proviennent-elles?
Améliorer le délai médian de détection (MTTD)	Comment validez-vous les sources de données que vous utilisez dans votre solution?

4. Possibilités continues d'automatisation et d'orchestration pour les problèmes à l'échelle de la machine

Faire le suivi de flux de travail compliqués, manuels et obsolètes expose votre entreprise à des menaces et à des erreurs humaines. La bonne plateforme de XDR aura de fortes capacités d'orchestration, et d'automatisation et rendra les tâches de sécurité répétitives plus faciles et plus efficaces sans une importante courbe d'apprentissage pour que l'équipe soit opérationnelle. L'automatisation des flux de travail essentiels aide l'équipe à réagir plus rapidement aux alertes, ce qui laisse plus de temps et d'énergie pour les tâches essentielles comme la recherche de menaces.

Principales fonctions	Questions à poser
Plus d'automatisation	Pour vos intégrations tierces, les modifications apportées par les fournisseurs à l'interface API interrompent-elles vos scripts d'automatisation?
Voir à travers le bruit de sécurité	Comment pouvez-vous m'aider à orchestrer et à automatiser les flux de travail dans mes solutions existantes?
Surmonter les limites à l'échelle humaine	Comment votre solution prend-elle en charge la surveillance vers et depuis les charges de travail en nuage?

5. Un point de vue d'enquête unique qui simplifie l'isolement et la correction

La XDR doit élargir les outils essentiels dans la trousse d'une équipe de gestion des incidents, en offrant une visibilité sur la télémétrie supplémentaire au-delà du point d'extrémité. Une console unique permet une correction directe, un accès aux informations sur les menaces et des outils pour fournir une vue unifiée d'une alerte. De plus, une XDR qui facilite la recherche de menaces, grâce à des modèles tels que MITRE ATT&CK, rendra accessible la recherche de menaces basée sur des hypothèses pour les personnes novices avec le processus, et facilitera l'anticipation de la prochaine étape.

Principales fonctions	Questions à poser
Réduire le délai moyen de correction (MTTR)	Où votre solution aide-t-elle ou accélère-t-elle la correction?
Permettre plus de recherche de menaces	Comment votre solution aide-t-elle mon équipe dans ses efforts de recherche des menaces?

Aller de l'avant avec la XDR

Nous vous recommandons de travailler avec les parties prenantes de la XDR pour déterminer quelle stratégie de XDR vous convient. Assurez-vous que les fournisseurs potentiels donnent la priorité à l'automatisation et à l'intégration.

Commencez par ces questions, mais assurez-vous de bien comprendre les différentes fonctions et exigences de votre pile actuelle afin d'obtenir des résultats mesurables et d'améliorer le rendement du capital investi.

1. Votre offre de XDR couvre-t-elle la détection et l'intervention du réseau, ainsi que d'autres couches de sécurité comme la messagerie, le nuage et le pare-feu?
2. Comment m'aiderez-vous à prendre des mesures de sécurité plus efficaces et plus éclairées?
3. Comment votre XDR m'aide-t-il à automatiser le blocage ou la correction?
4. Lesquelles de vos solutions ont des intégrations prêtes à l'emploi les unes avec les autres?
5. Comment votre approche de XDR s'articule-t-elle avec d'autres initiatives de sécurité comme le service d'accès sécurisé en périphérie (SASE) ou la vérification systématique?

La XDR et la résilience en matière de sécurité

De nos jours, l'incertitude est une garantie, des opérations aux finances en passant par la chaîne logistique. Les entreprises investissent dans la résilience, c'est-à-dire la capacité de résister à des chocs imprévus et à en sortir plus fortes. Mais cela sera insuffisant sans investissement dans la résilience en matière de sécurité.

Il y a cinq dimensions de la résilience en matière de sécurité :

1. Activez des milliards de signaux dans votre écosystème
2. Anticipez la suite grâce à des informations partagées
3. Hiérarchisez les alertes grâce à l'analyse du contexte basée sur les risques
4. Comblez les lacunes dans l'écosystème grâce aux intégrations
5. Devenez plus fort grâce à l'orchestration et à l'automatisation

La bonne plateforme de XDR répond à chacune de ces dimensions. De nos jours, seule Cisco tient les promesses de la solution de XDR grâce à un contexte unifié, à des détections corrélées et à des interventions plus rapides.

SecureX, notre plateforme de sécurité intégrée, est un droit fourni avec tous les produits de sécurité Cisco et s'intègre facilement aux solutions de votre environnement à l'aide d'interfaces API ouvertes. Cette couche unifiée de détection et d'intervention met en corrélation la télémétrie de tous les points de contrôle en un seul point de vue d'enquête et simplifie considérablement la hiérarchisation et la prise de mesures. En outre, l'orchestration intégrée vous permet d'automatiser les interventions et de décharger les tâches de routine pour libérer les équipes pour des tâches plus proactives, comme la recherche de menaces.

Courir sur place, c'est terminé. Il est temps d'avancer.

Feuille de travail de validation de fournisseur de XDR

Utilisez ce format de tableau et les questions fournies précédemment dans ce document pour vous préparer aux conversations avec les fournisseurs de XDR. Choisissez les 8 à 10 questions les plus pertinentes pour votre environnement et copiez-collez-les ci-dessous.

Question et remarques	Réponses convaincantes
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	
Question :	
Remarques :	

En savoir plus

Pour en savoir plus sur l'approche de Cisco en matière de XDR, communiquez avec votre représentant commercial dès aujourd'hui!

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose. CA

Siège social en Asie-Pacifique
Cisco Systems (USA) Pad Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de télécopieur sont répertoriés sur le site Web de Cisco, à l'adresse **www.cisco.com/go/offices**.

Imprimé aux États-Unis C07-3236254-00 11/22