Introduction à l'approche XDR : vers une simplification des opérations de sécurité

Sommaire

Introduction

Lorsque vous imaginez un centre opérationnel de sécurité (SOC), à quoi pensez-vous ? À une salle obscure où de mystérieux agents trient des alertes de sécurité ? À un grand bureau avec un écran géant affichant une carte des menaces ?

Les opérations de sécurité sont sans doute parmi les plus exigeantes du secteur. Ces dernières années, les SOC ont gagné en importance et en complexité, une conséquence naturelle de la transformation numérique et de l'adoption des nouvelles technologies.

Selon un récent rapport d'ESG, plus de la moitié des entreprises utilisent plus de 26 outils, qu'ils soient achetés, développés en interne ou open source, pour leurs opérations de sécurité[1]. L'adoption de nouvelles technologies devrait faciliter le travail de l'équipe SOC. Pourtant, ce n'est pas toujours le cas.

L'impact de la connectivité

Avec le travail hybride et l'adoption des technologies cloud, nous sommes plus connectés que jamais. Les entreprises fonctionnent comme des écosystèmes intégrés dans lesquels la frontière entre les équipes, les clients, les fournisseurs et les partenaires peut être floue. Cette nouvelle ère de l'interconnexion, bien que bénéfique pour nos entreprises et dans nos vies privées, augmente la surface d'exposition aux attaques et conduit au développement de cybermenaces plus sophistiquées que jamais.

Évidemment, il est tentant de se munir des dernières technologies pour répondre aux nouvelles préoccupations en matière de sécurité. Mais en réalité, sans une simplification de la pile de solutions de sécurité, se doter de nouveaux outils ne fait qu'ajouter à la confusion d'un environnement de sécurité déjà chaotique et peut augmenter le nombre de failles de sécurité qui ralentissent l'entreprise, quand l'objectif est au contraire d'accélérer la détection et de hiérarchiser les réponses.

« Pour être vraiment efficaces, les fournisseurs de solutions de cybersécurité doivent être ouverts au partage de données et de contexte afin que l'analytique avancée appliquée à un maximum de vecteurs permette de détecter et de contrer rapidement les groupes de hackers les plus sophistiqués au monde. »

AJ Shipley
Vice-président de la gestion des produits pour la détection et la réponse aux menaces

« Le temps, c'est de l'argent »

Un proverbe qui s'applique parfaitement à la cybersécurité. Une entreprise met en moyenne 277 jours pour détecter et contenir une faille. Cela signifie qu'un hacker pourrait déambuler librement et à votre insu dans votre entreprise, accéder à des applications internes et dérober des données privées tous les jours pendant près de 10 mois. C'est inacceptable !

Les analystes en cybersécurité font de leur mieux pour classer et hiérarchiser des milliers d'alertes chaque jour dans l'espoir de trouver l'approche la plus efficace pour détecter et neutraliser les menaces, mais c'est une véritable gageure pour la plupart des SOC. Pour vraiment résoudre ces problèmes, il convient d'examiner les causes premières de l'inefficacité des équipes de sécurité :

1. **Une intégration insuffisante avec les outils de sécurité existants**

   La plupart des entreprises s'appuient sur les outils de plusieurs fournisseurs pour développer l'intégralité de leur infrastructure de sécurité, ce qui signifie qu'elles disposent en général de plusieurs solutions autonomes avec peu ou pas d'intégration ou de télémétrie partagée. Lorsque les solutions ne coopèrent pas, un cercle vicieux s'enclenche.

   Une mauvaise intégration limite la quantité de données télémétriques et d'informations partagées. Impossible dès lors de bénéficier d'une visibilité unique et contextualisée. Si vous ne pouvez pas voir toutes les menaces dans l'ensemble de l'entreprise, comment limiter efficacement les risques à grande échelle ?

   AJ Shipley, vice-président de la gestion des produits pour la détection et la réponse aux menaces chez Cisco, le dit clairement : « Pendant des années, les cybercriminels ont exploité tout ce qu'ils ont pu pour faire avancer leurs objectifs, notamment le manque de partage des données entraînant l'incapacité à mettre en corrélation plusieurs signaux provenant de différents fournisseurs pour effectuer une détection précise. Pour être vraiment efficaces, les fournisseurs de solutions de cybersécurité doivent être ouverts au partage de données et de contexte afin que l'analytique avancée appliquée à un maximum de vecteurs permette de détecter et de contrer rapidement les groupes de hackers les plus sophistiqués au monde. » Les équipes de sécurité ont besoin d'une approche ouverte et extensible pour que leurs solutions fonctionnent mieux ensemble.

2. **Un trop grand nombre d'alertes**

   Selon une récente étude d'ESG sur la modernisation des SOC, 37 % des professionnels de l'IT et de la sécurité admettent que leurs opérations de sécurité sont plus difficiles à gérer que deux ans auparavant, en raison du volume toujours plus élevé et de la complexité croissante des alertes de sécurité. Les analystes ont du mal à trouver l'équilibre entre l'identification des menaces réelles et leur hiérarchisation afin de déterminer la meilleure stratégie de remédiation pour minimiser l'impact sur l'entreprise.

   Lorsque le SOC ne dispose pas d'informations suffisantes sur les menaces ni sur le contexte, il lui est presque impossible de hiérarchiser les risques en fonction de leur répercussion sur l'entreprise. Il croule sous un flot d'alertes et ne peut pas distinguer précisément celles qui risquent d'entraîner plusieurs millions d'euros de pertes de celles qui n'ont que peu ou pas d'impact.

3. **Une pénurie de compétences**

   La pénurie d'analystes disposant des compétences nécessaires pour un juste partage des responsabilités aggrave un peu plus les effets des systèmes cloisonnés et de la lassitude liée aux alertes sur les opérations de sécurité. Selon ESG, 81 % des professionnels de l'IT et de la cybersécurité reconnaissent que leurs opérations de sécurité ont été affectées par la pénurie mondiale de compétences dans ce secteur[2].

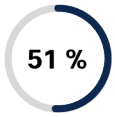
Les entreprises doivent trouver un moyen de renforcer les compétences de leurs analystes pour s'assurer que les bonnes informations exploitables sont détectées et mises en évidence afin que les menaces sophistiquées ne passent pas inaperçues ou ne soient pas négligées. Intégrer des informations sur les menaces mondiales et locales permet de combler cette lacune en fournissant le contexte supplémentaire nécessaire pour identifier et hiérarchiser avec précision les risques. Cela permet à chaque analyste de savoir quelles menaces sont à haut risque et doivent être traitées immédiatement pour se protéger, ce qui rend votre équipe plus efficace, indépendamment de son expérience.

Changer de paradigme avec l'approche XDR

Face à des menaces de plus en plus sophistiquées, l'ancien modèle de détection et de réponse reposant sur des solutions de sécurité ponctuelles et autonomes ne suffit plus. Les équipes se tournent vers des solutions telles que les systèmes SIEM et SOAR pour unifier les environnements cloisonnés et réduire les alertes, mais le problème persiste. Les SOC d'aujourd'hui ont besoin d'une solution qui transforme les données provenant d'un large éventail de sources en alertes fiables et en informations exploitables, afin de pouvoir agir rapidement en toute confiance.

Au cours des deux dernières années, la technologie de détection et de réponse étendues, mieux connue sous le nom de XDR, a pris de l'ampleur en tant que technologie émergente prometteuse, avec une approche ouverte et unifiée pour prévenir, détecter et répondre aux menaces rapidement et efficacement.

Mais qu'est-ce que la technologie XDR ? Pour résumer, il s'agit d'une solution qui collecte les données de télémétrie de plusieurs outils de sécurité au sein d'un référentiel de données central, analyse les données recueillies et homogénéisées pour détecter les comportements malveillants et accélère la réponse et la neutralisation de ces attaques. Avec un système XDR efficace, il est plus facile pour les analystes, quel que soit leur niveau, de se concentrer sur la détection des menaces, la gestion hiérarchisée des incidents en fonction des risques et l'amélioration de la productivité.



Selon ESG, 51 % des professionnels déclarent que les outils de sécurité qu'ils utilisent actuellement ont du mal à détecter et à analyser les menaces avancées[2].

Une solution XDR axée sur les risques tire parti de la Threat Intelligence à l'échelle mondiale et du contexte local pour quantifier, vérifier et hiérarchiser rapidement les menaces.

Mettre les données en corrélation pour détecter les menaces les plus sophistiquées où qu'elles soient

Il y a beaucoup à protéger si l'on considère toutes les données qui transitent par vos réseaux, vos endpoints, vos e-mails et vos applications.

Nous savons qu'une grande majorité des entreprises tirent parti d'une pile d'outils de sécurité multifournisseur pour analyser les menaces et les éliminer. Isolées, ces solutions n'offrent qu'une visibilité partielle sur ce qui se passe à un moment donné, mais quand elles sont réunies, leurs données se transforment en informations exploitables et utiles.

Agir plus rapidement sur les leviers qui font la différence

Chaque entreprise est différente. Selon les systèmes et les opérations les plus stratégiques pour votre entreprise, une menace infectant depuis trop longtemps le mauvais endroit peut entacher la réputation de votre marque ou la mener à la ruine. Et pour ne rien arranger, les analystes n'ont souvent pas le temps de hiérarchiser avec précision la multitude d'alertes qu'ils reçoivent chaque jour.

Cependant, une solution XDR axée sur les risques tire parti de la Threat Intelligence à l'échelle mondiale et du contexte local pour quantifier, vérifier et hiérarchiser rapidement les menaces en fonction de la probabilité de risque matériel. Essentiellement, la technologie XDR traduit le contexte mondial et local unifié pour visualiser le continuum complet des attaques et aider les analystes à comprendre à la fois la cause première et les répercussions.

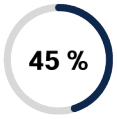
Cinq atouts clés d'une stratégie XDR

1. Des données de télémétrie hiérarchisées et exploitables, partout où vous en avez besoin
2. Une détection unifiée, quel que soit le vecteur ou le fournisseur
3. Une réponse rapide et précise aux menaces
4. Un point de vue unique pour une expérience d'utilisation simplifiée
5. L'opportunité d'augmenter la productivité et de renforcer la sécurité

Optimiser l'efficacité et accélérer les résultats

En dehors des hackers, les principaux ennemis de la sécurité sont le manque de contexte, de compétences et de temps. Mais avec une console XDR unifiée, même les équipes soumises à des contraintes de ressources et de temps peuvent réduire considérablement leurs délais de détection.

L'approche XDR agrège et centralise les données de sécurité, ce qui permet à vos équipes d'analyser, de hiérarchiser et de neutraliser les menaces les plus critiques avec rapidité et précision, indépendamment de leur expérience. L'orchestration et l'automatisation intégrées les aident à se décharger des tâches répétitives et à consacrer les ressources limitées là où elles sont le plus nécessaires.



Des entreprises qui disposent d'une mise en œuvre XDR mature ont constaté une amélioration de la résilience de leurs systèmes de sécurité par rapport aux autres[3].

Renforcer la résilience des systèmes de sécurité

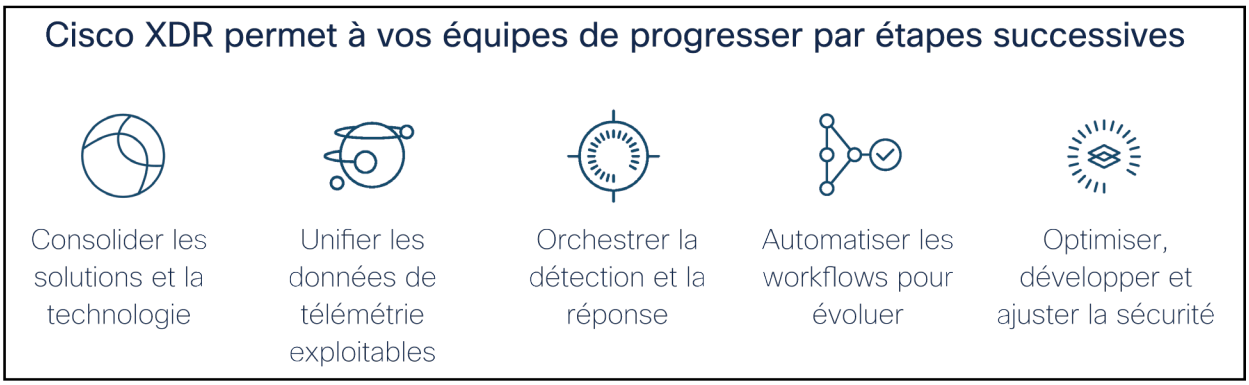
Aujourd'hui, l'incertitude est devenue la norme. En réponse, les entreprises investissent dans la résilience de tous les aspects de leur activité. Mais si elles ne renforcent pas la résilience de leurs systèmes de sécurité, elles restent vulnérables aux menaces et aux imprévus.

Dans le cadre de la plateforme ouverte et intégrée Cisco Security Cloud, notre solution XDR intègre la résilience de la sécurité, y compris dans les environnements multicloud hybrides les plus complexes. À mesure que de plus en plus de solutions se connectent à votre système XDR, vous pouvez renforcer la détection et apporter des réponses plus complètes sur tous les vecteurs nécessaires.

Pourquoi choisir Cisco XDR ?

Les clients sont au cœur de tout ce que Cisco entreprend. C'est pourquoi nous proposons une solution XDR complète avec une bibliothèque complète d'intégrations tierces des principaux fournisseurs de solutions de sécurité pour vous offrir une flexibilité maximale.

Nous savons également que vous n'avez pas besoin de plus de complexité. C'est pourquoi nous avons créé une console tout-en-un qui permet à vos analystes de sécurité et à votre SOC de détecter, d'analyser et d'éliminer les menaces en quelques clics seulement. Notre solution est ouverte, extensible et axée sur le cloud pour vous permettre d'optimiser vos investissements en matière de sécurité et d'unifier la détection des menaces dans l'ensemble de votre environnement.



[1] « Résultats complets de l'enquête d'ESG : la modernisation du SOC et le rôle de la technologie XDR », Enterprise Strategy Group (ESG), septembre 2022 https://www.esg-global.com/research/esg-complete-survey-results-soc-modernization-and-the-role-of-xdr

[2] « La modernisation du SOC et le rôle de la technologie XDR », Enterprise Strategy Group (ESG), juin 2022 https://www.cisco.com/c/en/us/products/security/soc-modernization-xdr

[3] « Rapport sur les objectifs en matière de sécurité, volume 3 », Cisco, décembre 2022 https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html

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

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. 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 de fax sont répertoriés sur le site web de Cisco, à l'adresse : **www.cisco.com/go/offices**.

Imprimé aux États-Unis C95-3551078-00 04/23