Une introduction à XDR : la promesse d'une simplification des opérations de sécurité

Introduction

Quand vous pensez à un centre d'opérations de sécurité (SOC), qu'est-ce qui vous vient à l'esprit? Une salle remplie de ninjas qui trient les alertes? Ou bien une grande salle remplie de cartes de menaces massives?

Les opérations de sécurité sont sans doute parmi les tâches les plus difficiles du secteur. Au fil des ans, le SOC d'une entreprise n'a cessé de gagner en importance et en complexité sous l'effet de la transformation numérique et de l'adoption de technologies plus récentes.

Un récent rapport de l'ESG nous indique que plus de la moitié des entreprises utilisent plus de 26 différents outils commerciaux, maison ou en code source libre pour les opérations de sécurité[1]. L'adoption de nouvelles technologies devrait faciliter le travail de l'équipe SOC, mais ce n'est souvent pas le cas.

L'incidence de la connectivité

Nous sommes plus que jamais connectés grâce au travail hybride et à l'adoption du nuage. Les entreprises opèrent comme des écosystèmes intégrés où les frontières entre les entreprises, les clients, les fournisseurs et les partenaires s'estompent. Cette nouvelle ère d'interconnexion est certes bénéfique pour notre vie professionnelle et privée, mais elle a favorisé l'expansion de la surface d'attaque et l'augmentation du nombre de cyberattaques sophistiquées.

Nous savons qu'il est tentant d'acheter la plus récente technologie pour répondre aux nouvelles préoccupations en matière de sécurité. En réalité, sans une solution capable de rationaliser la pile de sécurité, l'ajout d'outils supplémentaires ne fait qu'accroître la confusion dans un environnement de sécurité déjà décousu. Cela peut conduire à des failles de sécurité supplémentaires qui vous ralentissent alors que l'objectif réel est d'accélérer la détection et de donner la priorité à l'intervention.

« Pour être vraiment efficaces, les fournisseurs de cybersécurité doivent être ouverts au partage des données et du contexte afin que les analyses avancées sur le plus grand nombre de vecteurs possible puissent rapidement détecter les groupes d'acteurs de menaces les plus sophistiqués du monde et y réagir. »

AJ Shipley
Vice-président de la gestion des produits pour la détection des menace et intervention

Le temps, c'est de l'argent

Soyons réalistes : en matière de sécurité, le temps, c'est de l'argent. Il faut en moyenne 277 jours à une entreprise pour découvrir et contenir chaque faille. Cela signifie que votre entreprise pourrait avoir un voleur qui se promène sans être détecté, qui accède aux applications internes et qui vole des données privées tous les jours pendant près de 10 mois. C'est inacceptable!

Les analystes en sécurité déploient tous leurs efforts pour trier et hiérarchiser des milliers d'alertes chaque jour, dans l'espoir de trouver l'approche la plus efficace pour détecter les menaces et y remédier, mais la plupart d'entre eux n'y parviennent pas. Afin de véritablement résoudre ces problèmes, nous devons examiner les causes premières de l'inefficacité de l'équipe de sécurité :

1. **Mauvaise intégration avec les investissements existants en matière de sécurité**

   La plupart des entreprises s'appuient sur des outils provenant de plusieurs fournisseurs pour mettre en place l'ensemble de leur infrastructure de sécurité, ce qui signifie qu'elles ont tendance à avoir plusieurs solutions autonomes avec peu ou pas d'intégration ou de télémétrie partagée. Un manque de coordination des solutions crée un effet boule de neige.

   Une mauvaise intégration a pour effet de limiter la quantité de données télémétriques et de renseignements partagés, ce qui rend impossible la création d'une vue unique et riche en contexte. Comment pouvez-vous atténuer efficacement les risques à grande échelle, voire les atténuer tout court, si vous ne pouvez pas voir toutes les menaces qui pèsent sur l'ensemble de l'entreprise?

   AJ Shipley, vice-président de la gestion des produits pour la détection des menaces et l'intervention de Cisco, a la réponse : « Pendant des années, les cybercriminels ont exploité tous les avantages possibles pour poursuivre leurs objectifs, y compris l'incapacité, en raison du manque de partage des données, de corréler efficacement plusieurs signaux de faible fidélité provenant de plusieurs fournisseurs pour obtenir une détection très précise. Pour être vraiment efficaces, les fournisseurs de cybersécurité doivent être ouverts au partage de données et de contexte afin que les analyses avancées sur autant de vecteurs que possible puissent rapidement détecter les groupes d'acteurs de menaces les plus sophistiqués au monde et y réagir. » Les équipes de sécurité ont besoin d'une approche ouverte et évolutive pour que leurs solutions fonctionnent mieux ensemble.

2. **Surcharge d'alertes**

   La récente étude de l'ESG sur la modernisation des SOC indique que 37 % des professionnels de l'informatique et de la sécurité reconnaissent que leurs opérations de sécurité sont plus difficiles à gérer en 2022 que deux ans auparavant en raison du volume et de la complexité croissants des alertes de sécurité. Les analystes s'efforcent de trouver un équilibre entre l'identification des bonnes menaces et leur hiérarchisation afin de déterminer la meilleure stratégie de correction pour atténuer les répercussions sur leur entreprise.

   Lorsque les analystes ne disposent pas de suffisamment d'information sur les menaces ou de connaissances contextuelles, il est pratiquement impossible de hiérarchiser les menaces en fonction de leur répercussion sur l'activité de l'entreprise. Il en résulte un flot d'alertes sans qu'il soit possible de distinguer avec précision celles qui risquent de coûter 5 millions de dollars à votre entreprise si elles sont négligées, et celles qui n'ont que peu ou pas de répercussions du tout.

3. **Pénurie de ressources humaines compétentes**

   La pénurie d'analystes possédant les compétences nécessaires pour équilibrer les responsabilités accentue encore les effets des systèmes cloisonnés et de la fatigue liée aux alertes sur les opérations de sécurité. Selon l'ESG, 81 % des professionnels des TI et de la cybersécurité reconnaissent que leurs opérations de sécurité ont été affectées par la pénurie mondiale de ressources humaines compétentes en cybersécurité[2].

Les entreprises ont besoin d'un moyen de perfectionner leurs analystes pour s'assurer que les bons renseignements exploitables sont découverts et mis en valeur afin que les menaces sophistiquées ne passent pas inaperçues ou ne restent pas sans réponse. Les informations sur les menaces mondiales et locales intégrées permettent de combler cette lacune en fournissant le contexte supplémentaire nécessaire pour signaler les menaces et les hiérarchiser avec précision pour votre équipe. Cela permet à chaque analyste de savoir quelles menaces présentent un risque élevé et doivent être traitées immédiatement afin d'améliorer l'efficacité de la sécurité, ce qui rend votre équipe plus efficace, quelle que soit son expérience.

XDR change le paradigme

Les menaces devenant de plus en plus sophistiquées, l'ancien modèle de détection et d'intervention fondé sur des solutions de sécurité ponctuelles autonomes ne suffit plus. Les équipes se sont tournées vers des solutions telles que le SIEM et la SOAR pour tenter d'unifier les environnements cloisonnés et de réduire les alertes, mais le problème demeure. Les équipes de sécurité actuelles ont besoin d'une solution qui convertit les données provenant d'un large éventail de sources en alertes et en informations pertinentes, afin qu'elles puissent agir rapidement et en toute confiance.

Ces deux dernières années, la détection et l'intervention étendues, mieux connues sous le nom de XDR, ont pris de l'ampleur en tant que technologie émergente permettant de combler le vide grâce à une approche ouverte et unifiée pour rapidement et efficacement prévenir et détecter les menaces et intervenir.

En quoi consiste exactement la XDR? En bref, il s'agit d'une solution qui recueille la télémétrie de plusieurs outils de sécurité dans un référentiel de données central, analyse les données collectées et homogénéisées pour parvenir à la détection de la malveillance, et accélère l'intervention et la correction de la malveillance détectée. Grâce à une XDR efficace, il est plus facile pour les analystes de tous niveaux de se concentrer sur la détection complète des menaces, la hiérarchisation de l'intervention aux incidents basée sur les risques et l'amélioration de la productivité.

D'après l'étude de l'ESG, 51 % des professionnels affirment que les outils de sécurité qu'ils utilisent à l'heure actuelle ont du mal à détecter et à analyser les menaces avancées[2].

Une solution de XDR axée sur les risques exploite la vigie des cybermenaces mondiales et le contexte local pour quantifier, vérifier et hiérarchiser rapidement les menaces.

Corrélez les données pour détecter les menaces les plus sophistiquées, où qu'elles soient

Il y a beaucoup à protéger lorsque l'on considère toutes les données qui se trouvent sur vos réseaux, vos terminaux, vos courriels et vos applications.

Nous savons que la plupart des entreprises s'appuient sur un système de sécurité multifournisseur pour enquêter sur les menaces et intervenir. Lorsqu'elles sont isolées, ces solutions ne peuvent fournir qu'une visibilité partielle de ce qui se passe à un moment donné, mais lorsqu'elles sont réunies, ces données se transforment en renseignements utiles et exploitables.

Agissez sur ce qui compte réellement, plus rapidement

Chaque entreprise est différente. En fonction des systèmes et des opérations qui sont les plus critiques pour votre entreprise, une menace qui se propage trop longtemps au mauvais endroit peut entacher la réputation de votre marque ou mener à la ruine. Pour compliquer les choses, les analystes n'ont souvent pas le temps de hiérarchiser avec précision la montagne d'alertes qu'ils reçoivent quotidiennement.

Cependant, une solution de XDR axée sur les risques exploite la vigie des cybermenaces mondiales et le contexte local pour quantifier, vérifier et hiérarchiser rapidement les menaces en fonction de la probabilité de risque important. Fondamentalement, la XDR traduit le contexte global et local unifié pour afficher le continuum complet de l'attaque et aider les analystes à comprendre à la fois la cause première et l'étendue complète des répercussions.

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

1. Fournir des données télémétriques hiérarchisées et exploitables, partout où vous en avez besoin
2. Permettre une détection unifiée, quel que soit le vecteur ou le prestataire
3. Prendre en charge une intervention rapide et précise aux menaces
4. Offrir un point de vue d'enquête unique pour une expérience utilisateur simplifiée
5. Offrir la possibilité d'augmenter la productivité et de renforcer la posture de sécurité

Optimisez l'efficacité pour maximiser la valeur et accélérer les résultats

À part les cybercriminels, les principaux ennemis de la sécurité sont le contexte, les compétences et le temps limités. Grâce à une console de XDR unifiée, même les équipes dont les ressources et le temps sont limités peuvent réduire considérablement la durée de présence.

L'approche de la XDR, qui consiste à regrouper les données de sécurité dans un emplacement central, permet à vos équipes d'analyser, de hiérarchiser et de réagir aux menaces les plus critiques avec rapidité et précision, quel que soit leur niveau d'expérience. L'orchestration et l'automatisation intégrées aident les équipes à se décharger des tâches répétitives et à affecter des ressources limitées là où elles sont le plus nécessaires.

Les entreprises dotées d'un système de XDR mature ont vu leur résilience en matière de sécurité s'améliorer par rapport à celles qui n'en disposaient pas[3].

Le parcours vers la résilience en matière de sécurité

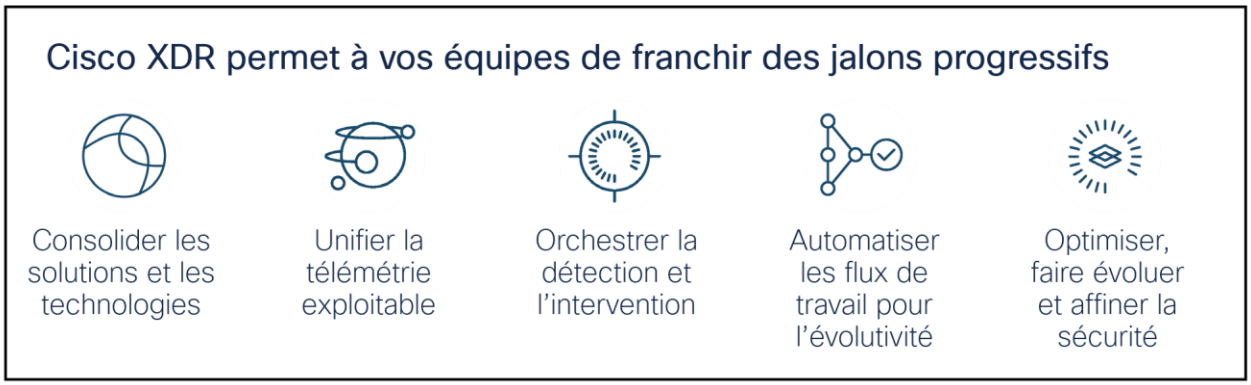
Aujourd'hui, l'incertitude est une garantie. Ainsi, les entreprises investissent dans la résilience à tous les niveaux de leur activité. Cependant, sans l'apport d'une résilience en matière de sécurité, votre entreprise peut être vulnérable à des menaces et à des changements imprévisibles.

Notre solution de XDR, intégrée à une plateforme ouverte appelée Cisco Security Cloud, garantit la résilience en matière de sécurité même dans les environnements multinuages hybrides les plus complexes. Au fur et à mesure que de nouvelles solutions sont intégrées à votre XDR, vous êtes en mesure de renforcer la détection et d'effectuer des interventions plus complètes sur tous les vecteurs nécessaires.

Pourquoi Cisco XDR?

Chez Cisco, nos clients sont au cœur de tout ce que nous faisons. C'est pourquoi nous proposons une solution de XDR complète avec une vaste bibliothèque d'intégrations tierces comprenant les principaux fournisseurs de sécurité afin d'offrir le plus de flexibilité possible.

Nous savons également que la complexité est la dernière chose dont vous avez besoin. C'est pourquoi nous avons créé une console tout-en-un qui permet à vos analystes de sécurité et du SOC de détecter, d'enquêter et de remédier aux menaces en quelques clics seulement. Notre solution est ouverte, extensible et axée sur le nuage, ce qui vous permet d'optimiser vos investissements existants en matière de sécurité et d'unifier la détection de la sécurité dans l'ensemble de votre environnement.



[1] « ESG Complete Survey Results: SOC Modernization and the Role of 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] « SOC Modernization and the Role of XDR », Enterprise Strategy Group (ESG), juin 2022
https://www.cisco.com/c/en/us/products/security/soc-modernization-xdr

[3] « Security Outcomes Report, 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 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 C95-3551078-00 23/04