Simplifiez les opérations de sécurité avec Cisco XDR

Renforcez la détection, agissez plus rapidement et augmentez la productivité

Table des matières

Cisco XDR change la façon dont les équipes de sécurité envisagent la détection et l'intervention. Notre solution en nuage est conçue pour simplifier les opérations de sécurité et permettre aux équipes de sécurité de détecter, de hiérarchiser et de répondre aux menaces les plus sophistiquées. S'intégrant à la plus vaste gamme de solutions de sécurité de Cisco et à certaines offres tierces, Cisco XDR est l'une des solutions les plus complètes et les plus flexibles sur le marché aujourd'hui.

Conçu par des praticiens de la sécurité pour les praticiens de la sécurité, Cisco XDR aide les analystes à agréger et à corréler les données de plusieurs sources en une vue unifiée pour simplifier les enquêtes, réduire le nombre de faux positifs, hiérarchiser les alertes et parcourir le chemin le plus court entre la détection et l'intervention.

L'automatisation intégrée, l'orchestration et les recommandations de correction guidées aident les analystes à automatiser les tâches répétitives et à maîtriser les menaces plus efficacement, libérant ainsi des ressources et du temps qui peuvent être consacrés à d'autres tâches de sécurité essentielles.

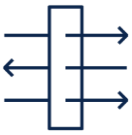
L'approche Cisco XDR basée sur les données permet aux équipes SOC de définir les événements les plus percutants et de cibler les stratégies de correction en premier lieu, renforçant ainsi la posture de sécurité globale de l'entreprise et augmentant la résilience.

Avantages

Pour éviter les angles morts, unifiez la visibilité, quel que soit le fournisseur ou le vecteur

Gagnez en visibilité et identifiez les menaces sur le réseau, le nuage, les points terminaux, les courriels et les applications pour assurer une sécurité efficace dans un environnement comportant de multiples fournisseurs et de multiples vecteurs.

En corrélant les données provenant de nombreuses technologies de détection différentes dans une vue unifiée, Cisco XDR permet de réaliser des enquêtes plus rapides et plus simplifiées, et simplifier les interventions.



Accélérez la détection des menaces et l'intervention pour agir sur ce qui est vraiment important

Mettez en corrélation les détections de plusieurs sources de télémétrie pour hiérarchiser les menaces en fonction du risque le plus élevé.

En tirant parti de l'intelligence artificielle et de l'apprentissage automatique, Cisco XDR permet une détection corrélée haute fidélité, réduit l'encombrement et harmonise efficacement les risques de sécurité avec les risques commerciaux.

Automatisez les interventions à l'aide de recommandations fondées sur des preuves pour réduire au minimum les conséquences.

Éliminez les menaces en toute confiance à l'aide de l'automatisation et de recommandations d'intervention guidées pour tous les points de contrôle pertinents.

En réduisant le temps d'enquête et en accélérant les interventions, Cisco XDR permet aux équipes du centre des opérations de sécurité de s'améliorer pour renforcer leur résilience.

Offrez des mesures complètes de détection des menaces et d'intervention avec des informations étayées par des données

Détectez plus rapidement les menaces complexes

- Cisco XDR offre la plus vaste gamme d'intégrations intégrées pour les terminaux, les courriels, le réseau, le nuage, le pare-feu et plus encore, ainsi que certaines intégrations tierces pour la stratégie de XDR la plus flexible, évolutive et efficace qui soit.
- Tirez parti de la télémétrie des réseaux sur place et des nuages publics et privés pour détecter les menaces sur les appareils gérés et non gérés, et obtenez un contexte crucial lors de la corrélation des événements, y compris où les attaques commencent et la façon dont elles se propagent sur le réseau.
- Les informations sur les menaces de Talos renforcent les capacités de détection, de sorte que les analystes disposent d'un ensemble inégalé d'informations exploitables pour exposer les menaces connues et émergentes dans un contexte plus approfondi et avec une meilleure connaissance du comportement des menaces dans le monde réel.

Hiérarchisez les menaces par effet et agissez sur ce qui compte le plus, plus rapidement

- La hiérarchisation reposant sur les risques aide les analystes du centre des opérations de sécurité à se concentrer sur les alertes les plus dangereuses, leur permettant de prendre des mesures rapides et efficaces. Cette approche unique fournit une vue unifiée des alertes, hiérarchisées selon leur gravité réelle.
- Réduisez le délai moyen d'intervention grâce à des interventions guidées pour l'identification, le confinement, l'éradication et la reprise. Cela, combiné à des interventions intégrées, permet une prise de décision cohérente et efficace.
- Simplifiez et réduisez les délais d'enquête grâce à un contexte unifié et à des techniques de divulgation progressives. Cisco XDR montre aux analystes les informations dont ils ont besoin sans les inonder de données superflues, ce qui entraînerait une paralysie de l'analyse. Au besoin, de plus amples renseignements pour enrichir les enquêtes sont toujours à portée de clic.

Accélérez les délais d'intervention

- Éliminez rapidement les menaces grâce à des interventions et à une orchestration intégrées. Avec Cisco XDR, les équipes du centre des opérations de sécurité peuvent tirer parti d'une gamme de manuels d'orchestration prédéfinis et personnalisables pour aider à arrêter les menaces et à maîtriser les risques en quelques clics.
- Stimulez les ressources limitées pour obtenir une valeur maximale en automatisant les tâches répétitives et chronophages et en fournissant aux équipes du centre des opérations de sécurité des bonnes pratiques prêtes à l'emploi. Lorsque l'automatisation n'est pas appropriée, Cisco XDR fournit des suggestions et des recommandations d'intervention guidées pour aider les analystes du centre des opérations de sécurité à prendre des mesures d'intervention efficaces.
- Poussez rapidement les interventions dans un vaste éventail d'outils de sécurité grâce à des intégrations approfondies avec différents points de contrôle de sécurité, à la fois des solutions Cisco intégrées et des solutions tierces. Jouez un rôle proactif dans la recherche de menaces en parcourant des journaux d'alertes disparates à mesure que vous découvrez de nouvelles tactiques, techniques et indicateurs de compromission.

XDR vous accompagne là où vous êtes

Options flexibles pour chaque entreprise

Cisco XDR est offert en trois niveaux de licence :

- **Cisco XDR Essentials** offre toutes les fonctions de XDR et s'intègre à l'ensemble de la gamme de produits de sécurité de Cisco.
- **Cisco XDR Advantage** s'appuie sur les capacités offertes dans Essentials en ajoutant des intégrations avec certains outils de sécurité tiers choisis par Cisco.
- **Cisco XDR Premie**r offre toutes les capacités d'Advantage en tant que service géré fourni par les experts en sécurité de Cisco, y compris la validation de la sécurité au moyen de tests d'intrusion, des services de gestion des incidents Cisco Talos et des services d'évaluation de sécurité technique de Cisco.

Apprenez-en plus à propos de Cisco XDR :
https://www.cisco.com/site/ca/fr/products/security/xdr/index.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 C45-3799269-00 23/08