Simplifiez les opérations de sécurité avec Cisco XDR

Renforcez la détection, agissez plus rapidement et augmentez la productivité

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 vaste gamme de solutions de sécurité de Cisco et à un ensemble d'offres tierces clés, 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 les faux-positifs, hiérarchiser les alertes et parcourir le chemin le plus court entre la détection et la réponse.

L'automatisation intégrée, l'orchestration et les recommandations de correction guidées aident les analystes à automatiser les tâches répétitives et à atténuer 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 plusieurs technologies de détection différentes dans une vue unifiée, Cisco XDR permet de réaliser des enquêtes plus rapides et plus simplifiées, et simplifie la réponse aux incidents.

Accélérez la détection et la réponse aux menaces pour intervenir 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 la réponse avec des recommandations fondées sur des preuves pour réduire au minimum les effets

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'investigation et en accélérant les réponses, Cisco XDR permet aux équipes du centre des opérations de sécurité de s'améliorer et de renforcer leur résilience.

Offrez des mesures complètes de détection des menaces et de réponse 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 points terminaux, les courriels, le réseau, le nuage, le pare-feu et plus encore, ainsi que des intégrations tierces sélectionnées pour la stratégie XDR la plus flexible, évolutive et efficace.
- Tirez parti de la télémétrie des réseaux sur site et des nuages publics et privés pour détecter les menaces sur les appareils gérés et non gérés et obtenir un contexte crucial lors de la corrélation des événements, y compris l'endroit 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'une collection inégalée d'informations exploitables pour exposer les menaces connues et nouvelles 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 de réponse grâce à des interventions guidées permettant l'identification, le confinement, l'éradication et la reprise après les menaces, de même que des actions d'intervention intégrées, qui se combinent pour permettre une prise de décision cohérente et efficace.

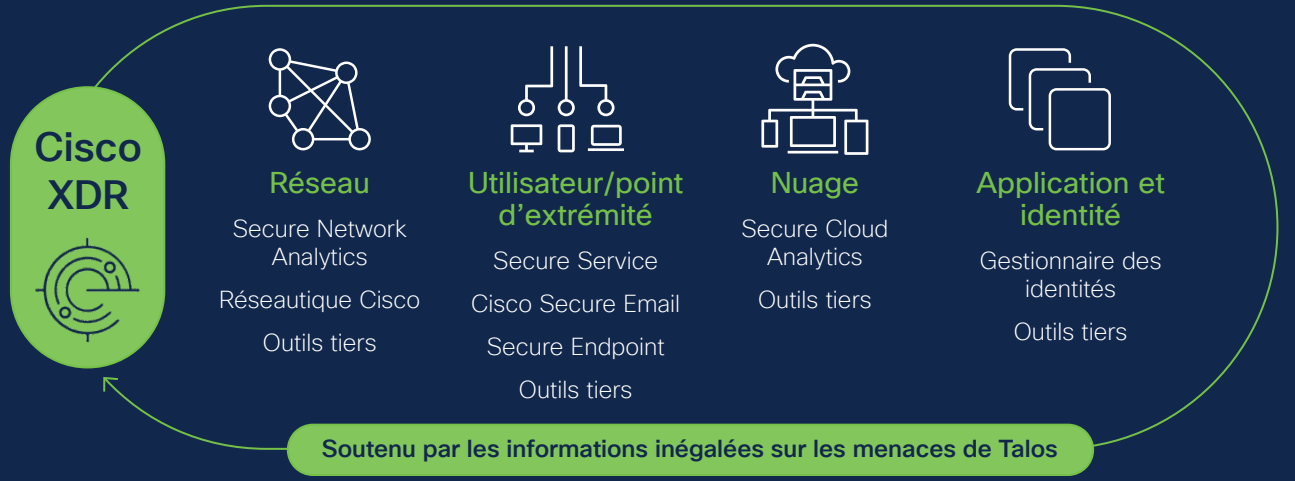
Accélérez les délais de réponse

- Éliminez rapidement les menaces grâce à des actions d'intervention 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 ou personnalisables pour aider à arrêter les menaces et à atténuer les risques en quelques clics.
- Stimulez les ressources limitées pour assurer une valeur maximale en automatisant les tâches répétitives et chronophages et en fournissant aux équipes de du centre des opérations de sécurité des pratiques exemplaires 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 actions d'intervention dans un large 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.

Simplifiez les enquêtes :

- 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 pour effectuer les tâches en cours sans les inonder de données superflues, ce qui entraînerait une paralysie de l'analyse. Au besoin, plus d'informations pour enrichir les enquêtes sont toujours à portée de clic.
- Afin d'être toujours prêts à l'action, les analystes du centre des opérations de sécurité peuvent regrouper les alertes, les renseignements mondiaux et le contexte local pour comprendre la cause première et l'étendue de l'effet.

XDR vous accompagne là où vous êtes



Tirer parti du nuage de sécurité de Cisco : combiner les fonctionnalités de base, y compris une expérience sans friction, un écosystème ouvert et extensible et l'automatisation.

Apprenez-en plus à propos de Cisco XDR : cisco.com/go/xdr