CISCO
SECURE

Présentation
Document public

Simplifiez les opérations de sécurité avec Cisco XDR

Détectez davantage de menaces, agissez plus rapidement et améliorez la productivité

Cisco XDR change la façon dont les équipes de sécurité envisagent la détection et la réponse. Notre solution cloud est conçue pour simplifier les opérations de sécurité et permettre aux équipes de détecter et hiérarchiser les menaces les plus sophistiquées afin de les neutraliser. Parce qu'elle s'intègre à la vaste gamme de solutions de sécurité Cisco et à un ensemble d'offres tierces clés, Cisco XDR est l'une des solutions les plus complètes et les plus flexibles du marché.

Conçue par des professionnels de la sécurité pour les professionnels de la sécurité, Cisco XDR permet aux analystes d'agréger et de mettre en corrélation les données de plusieurs sources dans une vue unifiée pour simplifier les enquêtes, réduire le nombre de faux positifs, hiérarchiser les alertes et prendre le chemin le plus court entre la détection et la réponse.

L'automatisation intégrée, l'orchestration et les recommandations de remédiation assistée permettent aux analystes d'automatiser les tâches répétitives et de maîtriser les menaces plus efficacement, libérant du temps et des ressources pour se concentrer sur d'autres tâches de sécurité essentielles.

L'approche de Cisco XDR axée sur les données permet aux équipes du SOC de définir les événements liés à la sécurité les plus importants et d'y appliquer en priorité les stratégies de remédiation, renforçant ainsi la sécurité globale de l'entreprise et la résilience de ses systèmes.

Bénéfices

Unifiez la visibilité, quels que soient le fournisseur ou le vecteur, pour bénéficier d'une visibilité inégalée

Gagnez en visibilité et identifiez les menaces sur le réseau, le cloud, les endpoints, la messagerie et les applications pour une sécurité efficace dans les environnements multifournisseurs et multivecteurs.

En mettant en corrélation les données issues de plusieurs technologies de détection dans une vue unifiée, Cisco XDR simplifie et accélère le processus d'investigation, et rationalise la réponse aux incidents.

Accélérez la détection et l'élimination des menaces pour agir aux niveaux les plus importants

Mettez en corrélation les détections entre 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 aligne efficacement les risques pour la sécurité sur les risques pour l'entreprise.

Automatisez la réponse avec des recommandations étayées par des preuves pour minimiser l'impact

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

En réduisant les délais d'enquête et de réponse, Cisco XDR stoppe les remontées aux équipes du SOC et renforce la résilience.

Des fonctionnalités de détection des menaces et des actions de réponse complètes grâce à des informations étayées par les données

Détectez les menaces complexes plus tôt

- Cisco XDR offre la plus large gamme d'intégrations prédéfinies du marché : endpoint, messagerie, réseau, cloud, pare-feu et bien plus encore, ainsi que des intégrations tierces pour vous proposer la stratégie XDR la plus flexible, la plus évolutive et la plus efficace.
- Tirez parti des données télémétriques des réseaux sur site et des clouds publics et privés pour détecter les menaces sur les équipements gérés et non gérés, et obtenir des informations contextuelles essentielles pour la mise en corrélation des événements, notamment sur le point de départ des attaques et la façon dont elles se propagent sur le réseau.
- La Threat Intelligence de Talos renforce les capacités de détection. Les analystes profitent de fonctionnalités inégalées de collecte d'informations exploitables pour exposer les menaces connues et émergentes avec un contexte plus précis et une meilleure appréciation du comportement des menaces dans le monde réel.

Hiérarchisez les menaces en fonction de leur impact et agissez plus rapidement sur ce qui compte le plus

- La hiérarchisation basée sur les risques permet aux analystes du SOC de se concentrer sur les alertes représentant la plus grande menace : ils peuvent ainsi prendre des mesures rapides et efficaces. Cette approche unique permet d'avoir une vue unifiée des alertes, classées par ordre de gravité concret.
- Réduisez le délai moyen de réponse (MTTR) grâce à des recommandations pour l'identification, l'isolation, l'éradication des menaces et la récupération suite à une attaque, et à des actions de réponse intégrées, qui se combinent pour permettre une prise de décision cohérente et efficace.

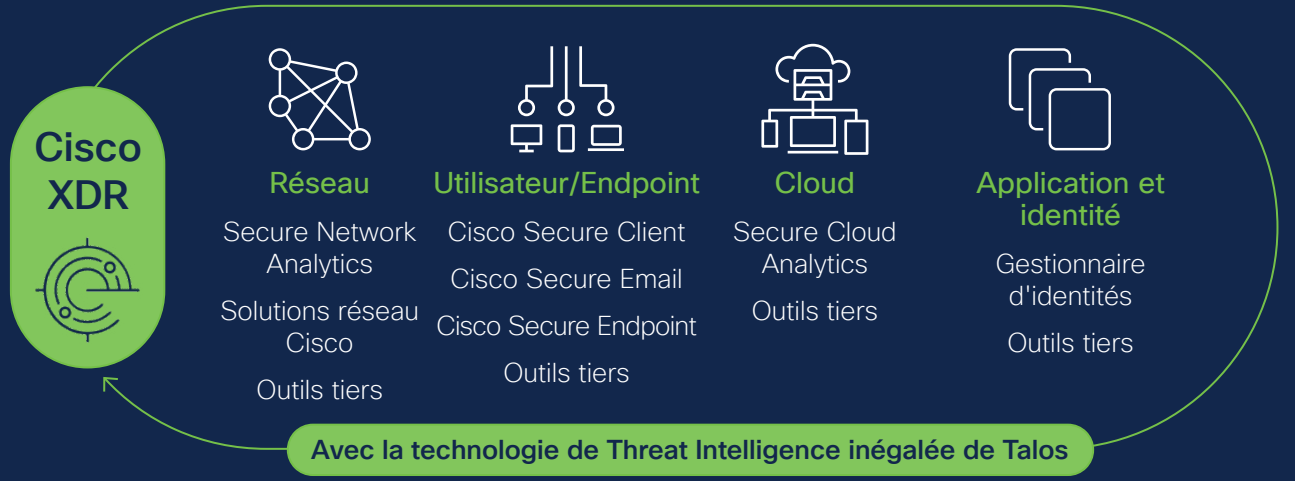
Accélérez les délais de réponse

- Corrigez rapidement les menaces grâce à des actions de réponse et à une orchestration intégrées. Avec Cisco XDR, les équipes du SOC peuvent tirer parti d'une gamme de guides d'orchestration prédéfinis ou personnalisables pour stopper les menaces et maîtriser les risques en quelques clics.
- Optimisez vos ressources limitées pour une valeur ajoutée maximale en automatisant les tâches répétitives et chronophages et en fournissant aux équipes du SOC des bonnes pratiques prêtes à l'emploi. Lorsque l'automatisation n'est pas adaptée, Cisco XDR fournit des suggestions et des recommandations de réponse guidées pour aider les analystes du SOC à prendre des mesures efficaces.
- Appliquez rapidement des actions de réponse à un large éventail d'outils de sécurité grâce à des intégrations poussées avec divers points de contrôle de la sécurité, qu'il s'agisse de solutions Cisco intégrées ou tierces. Jouez un rôle proactif dans la chasse aux menaces en analysant les différents journaux d'alertes à mesure que vous découvrez de nouvelles tactiques, de nouvelles techniques et de nouveaux 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 fournit aux analystes les informations dont ils ont besoin pour effectuer les tâches en cours sans les inonder de données superflues qui gêneraient leurs analyses. En cas de besoin, un seul clic suffit pour obtenir davantage d'informations et étayer leurs enquêtes.
- Les analystes du SOC peuvent regrouper les alertes, les informations globales et le contexte local pour comprendre la cause première et l'étendue des répercussions, afin d'être toujours prêts à agir.

Déployer la technologie XDR sur l'ensemble de votre environnement



Tirer parti de Cisco Security Cloud : toutes les fonctionnalités de base, notamment une expérience fluide, un écosystème ouvert et extensible et l'automatisation

En savoir plus sur Cisco XDR : cisco.com/go/xdr