The bridge to possible

Cisco Breach Protection Premier

Travaillez en toute confiance, assurez la pérennité de votre sécurité et réduisez le délai de rentabilisation

Cisco Breach Protection Suite unifie les solutions de détection, d'enquête, de maîtrise et de recherche des menaces en intégrant la gamme de solutions de sécurité de Cisco et certains outils tiers sur les points terminaux, la messagerie, le réseau et le nuage. Mais toutes les entreprises n'ont pas la capacité ou l'expertise pour déployer et gérer cette solution. Des services gérés pourraient être exactement ce dont votre entreprise a besoin.

Cisco Breach Protection Premier vous rejoint, vous et votre équipe, là où vous êtes maintenant, travaille avec les outils et les sources de télémétrie actuellement en place, applique notre expertise et nos conseils inégalés, et évolue avec vous tout au long de votre croissance en ajoutant des couches et des solutions à la stratégie de sécurité globale.

Niveau Cisco Breach Protection Premier

Le niveau de licence Cisco Breach Protection Premier fournit une solution de détection et d'intervention étendues (MXDR) optimisée par Cisco, fournie par une équipe d'élite d'experts en sécurité de Cisco. Cela comprend le soutien pour l'intégration des solutions de sécurité Cisco et les intégrations choisies par Cisco avec certains outils de sécurité tiers, le soutien de Cisco Software Support Services (SWSS) Enhanced, l'évaluation de la sécurité, la validation et l'amélioration par l'entremise de l'évaluation de sécurité technique de Cisco (CTSA) et de certains services de gestion des incidents Cisco Talos (Talos IR).

Le service Cisco Managed Extended Detection and Response (MXDR) fait appel à une combinaison de l'équipe d'élite de Cisco composée de chercheurs, d'enquêteurs et d'agents d'intervention, à la solution Cisco XDR, à des ensembles d'outils intégrés et à des technologies Cisco Security pour surveiller les possibles menaces et les violations de sécurité et intervenir.

Le service MXDR optimisé par Cisco XDR comprend ce qui suit :

- Surveillance continue des incidents de sécurité pour les événements et les alertes par l'entremise du centre des opérations de sécurité (SOC) de Cisco, 24 heures sur 24, 7 jours sur 7, 365 jours par année.
- Un analyste du SOC du service MXDR est responsable de l'analyse des données de la plateforme, de la corrélation, de l'enrichissement, de la hiérarchisation et de l'examen de tous les événements au moyen de guides établis.
- Signalement progressif des incidents de sécurité potentiels, au besoin.
- Interventions guidées pour vous aider à contenir, atténuer, corriger ou éradiquer les menaces. L'enquête et les mesures d'intervention seront effectuées en votre nom, selon des guides d'intervention préapprouvés.

- Une séance d'information trimestrielle sur les menaces fournira des mises à jour sur les modèles actuels de menaces, les volumes de détection et les tendances en matière d'événements.
- Les avis de menace identifient les menaces nouvellement découvertes, ce qui facilite la prévention proactive des incidents grâce à la mise en œuvre de contrôles d'atténuation.

CTSA offre une gamme de services proactifs pour évaluer votre état de préparation en matière de cybersécurité et fournir des conseils sur les menaces auxquelles vous êtes confronté, la probabilité qu'elles se concrétisent et l'incidence sur votre résilience opérationnelle, le cas échéant. Cela comprend, sans toutefois s'y limiter :

- Modélisation, atténuation et simulation des menaces
- Tests d'intrusion
- Équipes rouge, bleue et mauve
- Évaluations de l'architecture de sécurité
- Évaluations des applications, du centre des opérations de sécurité et des opérations de développement
- Examens de versions et de configurations

Talos IR fournit une suite complète de services proactifs et réactifs pour vous aider à vous préparer à un incident de cybersécurité et à intervenir et à récupérer plus rapidement si un tel incident survient.

Les heures de service de Talos IR et CTSA sont accumulées en fonction du nombre de licences Cisco Breach Premier achetées pour les utilisateurs couverts (UC). Des heures supplémentaires peuvent être achetées avec les offres à la carte de Talos IR et CTSA.

Service	Heures min.
Renseignements sur demande	5
Atelier sur la susceptibilité aux violations	5
Évaluation de l'empreinte numérique de l'entreprise	10
Atelier de réflexion sur la conception de la sécurité	20
Intervention d'urgence en cas d'incident*	40
Tests d'intrusion	40
Modélisation des menaces	40
Examen de configurations et de versions d'appareils	40
Plan d'intervention en cas d'incident	50
Guides d'intervention en cas d'incident	50
Simulation d'exercice sur maquette	50
Évaluation de l'architecture de sécurité	80
Évaluation de l'état de préparation d'intervention en cas d'incident	80
Évaluation des compromissions	80
Environnement de cyberdéfense	80
Recherche proactive de menaces	100
Simulation de menace de l'équipe rouge	160
Équipe mauve	160
Évaluation des opérations de sécurité	160

* Les clients disposant de 20 à 39 heures peuvent bénéficier de services limités d'intervention d'urgence en cas d'incident

Travaillez en toute confiance, assurez la pérennité de votre sécurité et réduisez le délai de rentabilisation grâce aux services gérés fournis par Cisco.

Pour en savoir plus : cisco.com/go/breach-protection