The bridge to possible
(Et vos ambitions prennent vie)

Cisco Breach Protection Premier

Opérez en toute confiance, pérennisez votre sécurité et rentabilisez plus rapidement votre solution

La suite Cisco Breach Protection unifie les solutions de détection, d'analyse, d'éradication et de recherche des menaces en intégrant la gamme de solutions de sécurité Cisco ainsi qu'une sélection d'outils tiers pour les endpoints, les e-mails, le réseau et le cloud. Cependant, toutes les entreprises n'ont pas la capacité ni l'expertise nécessaires pour déployer et gérer cette solution. Et si votre entreprise avait besoin de services managés ?

Cisco Breach Protection Premier s'appuie sur les outils et les sources de télémétrie actuellement déployés dans votre infrastructure. Avec notre expertise inégalée et nos conseils avisés, nous accompagnons votre croissance et le développement de votre environnement au fur et à mesure que vous ajoutez des solutions et des couches de sécurité dans le cadre de votre stratégie globale.

Cisco Breach Protection niveau Premier

Le niveau de licence Cisco Breach Protection Premier propose une solution MXDR (Managed Extended Detection and Response) optimisée par Cisco et assurée par une équipe de nos experts en sécurité. Il inclut la prise en charge de l'intégration des solutions de sécurité Cisco et des intégrations approuvées par Cisco avec une sélection d'outils de sécurité tiers, les services d'assistance améliorée Cisco Software Support Services (SWSS), l'évaluation de la sécurité, un service de validation, l'évaluation technique de la sécurité Cisco (CTSA) et certains services de réponse aux incidents de Talos (Cisco Talos IR).

Notre service managé de détection et de réponse étendues (MXDR) associe les chercheurs, les enquêteurs techniques et les équipes d'intervention de Cisco, la solution Cisco XDR, des outils intégrés et des technologies de sécurité Cisco supplémentaires pour surveiller et traiter les menaces et les failles potentielles.

Le service MXDR optimisé par Cisco XDR inclut :

- La surveillance continue des incidents et des alertes via le centre opérationnel de sécurité (SOC) de Cisco, disponible 24 h/24, 7 j/7, 365 jours par an.
- Un analyste SOC MXDR est chargé d'analyser les données de la plateforme, de mettre en corrélation, d'enrichir, de hiérarchiser et d'examiner tous les événements via des guides établis.
- Le signalement des incidents potentiels, si nécessaire.
- Les actions de réponse guidée vous aident à contenir, à limiter, à éliminer ou à éradiquer les menaces. Les enquêtes et les interventions seront menées en votre nom, sur la base de guides d'intervention préapprouvés.

The bridge to possible
(Et vos ambitions prennent vie)

- Les briefings trimestriels sur les menaces fournissent des mises à jour sur les modèles de menaces actuels, les volumes de détection et les tendances.
- Les avertissements identifient les menaces nouvellement détectées, ce qui facilite la prévention proactive des incidents grâce à la mise en œuvre de mesures dédiées.

CTSA propose une suite de services proactifs pour évaluer votre niveau de préparation en matière de cybersécurité et fournir des conseils sur les menaces auxquelles vous faites face, la probabilité qu'elles se concrétisent et l'impact sur votre résilience opérationnelle, le cas échéant. Parmi ces services :

- Modélisation/atténuation/simulation des menaces
- Analyse des intrusions (test d'intrusion)
- Teaming rouge, bleu ou violet
- Évaluations de l'architecture de sécurité
- Évaluations applications/SOC/DevOps
- Vérifications des versions/configurations

Talos IR propose une suite complète de services d'urgence et proactifs pour se préparer aux incidents liés à la cybersécurité, les gérer et s'en remettre rapidement.

Les heures de service de Talos IR et CTSA sont comptabilisées en fonction du nombre de licences Cisco Breach Premier achetées pour les utilisateurs couverts. Vous pouvez acheter des heures supplémentaires avec les offres à la carte Talos IR et CTSA.

Services	Heures min.
Informations à la demande	5
Atelier sur la vulnérabilité aux failles	5
Évaluation de l'empreinte numérique de l'entreprise	10
Atelier de réflexion sur la conception de la sécurité	20
Réponse d'urgence aux incidents*	40
Test de pénétration	40
Modélisation des menaces	40
Configuration des équipements et vérification des versions	40
Planification de la réponse aux incidents	50
Guides de réponse aux incidents	50
Exercices de simulation	50
Évaluation de l'architecture de sécurité	80
Évaluation du niveau de préparation à la gestion des incidents	80
Évaluation des compromissions	80
Formation Cyber Range	80
Threat Hunting proactif	100
Simulation des menaces – Red Team	160
Purple Team	160
Évaluation des opérations de sécurité	160

* Les clients disposant de 20 à 39 heures peuvent bénéficier de services limités de réponse d'urgence aux incidents

Travaillez en toute confiance, pérennisez votre sécurité et rentabilisez plus rapidement vos investissements grâce aux services managés de Cisco.

En savoir plus : cisco.com/go/breach-protection