The bridge to possible

Cisco Breach Protection Premier

Sorgenfreier Betrieb, zukunftssicherer Schutz und beschleunigte Amortisierung

Die Cisco Breach Protection Suite vereint die Erkennung, Untersuchung, Abwehr und Nachverfolgung von Bedrohungen durch die Integration des Cisco Security-Portfolios und ausgewählter Drittanbietertools für Endpunkte, E-Mails, Netzwerk und Cloud. Aber nicht jedes Unternehmen verfügt über die Kapazität oder das Know-how, um diese Lösung bereitzustellen und zu managen. In diesem Fall kann eine Managed-Services-Lösung genau das sein, was Ihr Unternehmen braucht.

Cisco Breach Protection Premier passt sich an die Anforderungen Ihres Unternehmens und Ihrer Teams an. Es arbeitet mit den Tools und Telemetriequellen, die aktuell verwendet werden, stellt Fachwissen und Unterstützung bereit, wächst mit Ihrem Unternehmen mit und kann der allgemeinen Security-Strategie zusätzliche Schichten und Lösungen hinzufügen.

Cisco Breach Protection Premier-Lizenzstufe

Die Lizenzstufe Cisco Breach Protection Premier bietet Managed Extended Detection and Response (MXDR) powered by Cisco, ein Service, der von einem exklusiven Cisco Sicherheitsexpertenteam bereitgestellt wird. Der Service umfasst Integrationssupport für Cisco Security-Lösungen und von Cisco ausgewählte Integrationen mit Security-Tools von Drittanbietern, erweiterten Support durch Cisco Software Support Services (SWSS), Sicherheitsbewertungen, Validierungen und Verbesserungen durch Cisco Technical Security Assessment (CTSA) sowie ausgewählte Cisco Talos Incident Response Services (Talos IR).

Der Cisco Managed Extended Detection and Response Service (MXDR) nutzt eine Kombination aus dem exklusiven Cisco Expertenteam (aus den Bereichen Forschung, Ermittlung und Reaktion), der Cisco XDR-Lösung, integrierten Toolsets und weiteren Cisco Security-Technologien, um potenzielle Sicherheitsbedrohungen und -verletzungen zu überwachen und auf diese zu reagieren.

Der von Cisco XDR unterstützte MXDR-Service umfasst folgende Aspekte:

- Kontinuierliches Monitoring von Sicherheitsvorfällen im Hinblick auf Ereignisse und Warnungen über das Cisco Security Operations Center (SOC) rund um die Uhr
- Analyse von Plattformdaten sowie Korrelation, Anreicherung, Priorisierung und Überprüfung aller Ereignisse anhand bewährter Playbooks durch eine/n MXDR SOC AnalystIn
- Eskalation potenzieller Sicherheitsvorfälle nach Bedarf
- Begleitete Reaktionsmaßnahmen zur Eindämmung, Minderung, Behebung und Beseitigung von Bedrohungen; Untersuchungen und Reaktionsmaßnahmen werden basierend auf vorab genehmigten Playbooks in Ihrem Namen durchgeführt

The bridge to possible

- Vierteljährliche Briefings zur Bedrohungslage mit aktuellen Informationen zu Bedrohungsmustern und -trends sowie Zahlen zu erkannten Bedrohungen
- Identifizierung neuer Bedrohungen, Unterstützung bei der proaktiven Prävention von Vorfällen durch die Implementierung von Kontrollmechanismen zur Bedrohungseindämmung

CTSA bietet verschiedene proaktive Services zur Bewertung Ihrer Ausgangslage für die Cybersicherheit sowie Beratung zur aktuellen Bedrohungslage, zur Auftretenswahrscheinlichkeit einer Bedrohung und zu den möglichen Auswirkungen auf Ihren Betrieb. Dies umfasst unter anderem folgende Aspekte:

- Modellierung/Abwehr/Simulation von Bedrohungen
- Penetrationstests
- Red/Blue/Purple Teaming
- Bewertung der Sicherheitsarchitektur
- App-/SOC-/DevOps-Bewertungen
- Build-/Konfigurationsüberprüfungen

Talos IR bietet eine umfassende Suite an proaktiven Services und Notfalldiensten, mit der Sie sich besser auf einen Cybersicherheitsvorfall vorbereiten, darauf reagieren und Systeme wiederherstellen können.

Die Talos IR- und CTSA-Servicestunden richten sich nach der Anzahl der Cisco Breach Premier-Lizenzen, die für vertraglich abgedeckte User erworben wurden. Zusätzliche Stunden können über individuelle Angebote von Talos IR und CTSA erworben werden.

Service	Mindestanzahl in Stunden
Intel On Demand	5
Workshop zur Anfälligkeit für Sicherheitsverletzungen	5
Bewertung des digitalen Fußabdrucks im Unternehmen	10
Design-Thinking-Workshop zum Thema Security	20
Emergency Incident Response*	40
Penetrationstests	40
Bedrohungsmodellierung	40
Überprüfung von Gerätekonfiguration und Build	40
IR-Plan	50
IR-Playbooks	50
Theoretische Planspiele	50
Bewertung der Sicherheitsarchitektur	80
Bewertung der IR-Bereitschaft	80
Kompromittierungsbewertung	80
Cyber Range	80
Proaktive Nachverfolgung von Bedrohungen	100
Red Team-Bedrohungssimulation	160
Purple Teaming	160
Bewertung der Sicherheitsverfahren	160

* Kunden mit 20 bis 39 Stunden können eingeschränkte Emergency Incident Response Services nutzen

Mit den Managed Services von Cisco profitieren Sie von sorgenfreiem Betrieb, zukunftssicherem Schutz und beschleunigter Amortisierung.

Weitere Informationen finden Sie unter www.cisco.com/site/de/de/products/security/breach-protection/index.