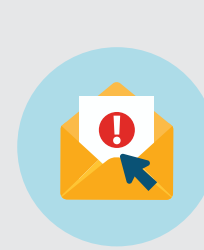
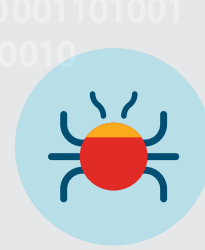


Bedrohungen rechtzeitig stoppen mit Incident Response Services



5

Möglichkeiten, wie Sie mit Cisco Incident Response Services Ihr Unternehmen sicherer machen

Ihr Draht zu den Experten

1



Das Cisco® Incident Response Team steht unter der Leitung professioneller Sicherheitsexperten und kann die Quelle von Bedrohungen durch Analyse und Synthese von Threat-Intelligence aus mehreren Quellen aufdecken. Diese gefragten Spezialisten können Probleme schneller lösen, damit Sie Ihren Geschäftsbetrieb wieder aufnehmen können.

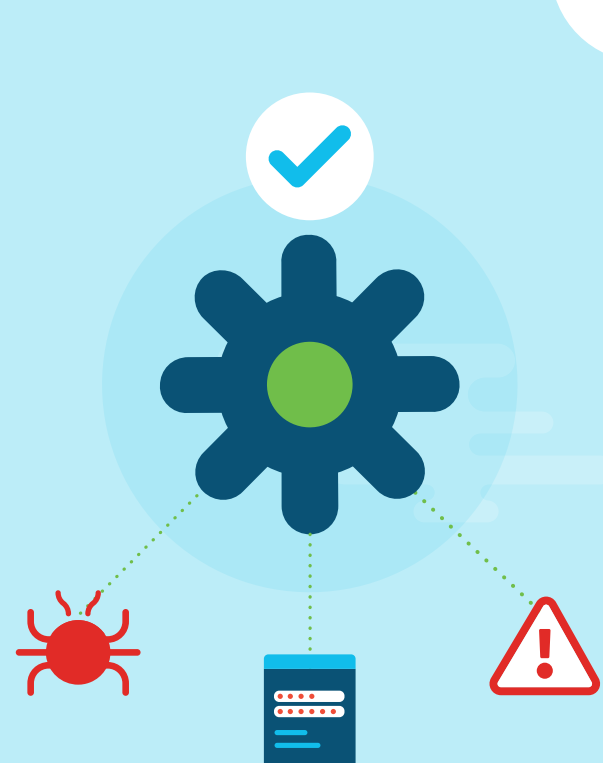
→ Incident-Response: die Grundlagen

Nutzen Sie das Potenzial der Threat-Intelligence

Die Talos™ Security Intelligence and Research Group (Talos) besteht aus über 300 branchenführenden Threat-Intelligence-Experten. Mit Talos erhalten Sie schnellen Zugriff auf die neueste Threat-Intelligence, und unser Incident Response Team arbeitet gemeinsam mit Experten aus der Sicherheitsforschung daran, Clients zeitnah vor einer Vielzahl bekannter und unbekannter Bedrohungen zu schützen. Das macht die Investition in Bedrohungserkennung, -analyse und -schutz lohnenswert für Sie.

→ Talos Intelligence

2



Umfassende Abwehr kritischer Bedrohungen

3



Der flexible Incident Response Retainer bietet proaktive Services zur Abwehr, wie etwa Bewertungen, Nachverfolgung von Bedrohungen und theoretische Übungen, und stellt Ihnen bei Sicherheitsverletzungen ein professionelles Cybersecurity-Team zur Seite, das auf Abruf verfügbar ist. Zur Unterstützung im Notfall sind unsere Experten innerhalb von 4 Stunden vor Ort und beheben jegliche Datensicherheitsverletzungen.

→ Incident Response Readiness and Retainer

Bedrohungen abwehren, bevor diese entstehen

Handeln Sie nicht erst bei einem Vorfall. Identifizieren Sie Schwachstellen, bevor diese sich auf Ihr Unternehmen auswirken. Unsere Experten spüren zusammen mit Ihrem Team vorhandene Angreifer in Ihrem Netzwerk auf und ergreifen entsprechende Maßnahmen.

Aus entgangenen Umsätzen infolge einer Sicherheitsverletzung ergeben sich Kosten von durchschnittlich 3,62 Millionen US-Dollar.

→ Proaktive Bedrohungsabwehr

4



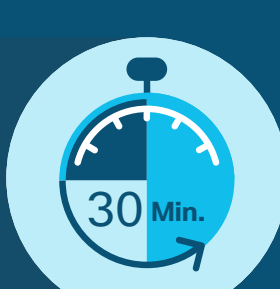
Bedrohungen schnell und effizient beseitigen

5



Im Falle einer Verletzung reagiert das Cisco Team sofort per Remote-Zugriff und ist innerhalb von 4 Stunden vor Ort. Wir bringen die erforderliche Ausrüstung mit und aktivieren zur schnelleren Problembeseitigung 60-Tage-Testlizenzen für **Cisco Advanced Malware Protection (AMP)**, **Umbrella** und **Stealthwatch**.

Unserer durchschnittliche Reaktionszeit: 30 Minuten. Der Branchenschnitt: 4 Stunden.



→ Emergency Incident Response Service

→ Cisco Umbrella

→ Cisco Advanced Malware Protection

→ Cisco Stealthwatch

Incident Response Services verbessern Ihre Vorbereitung und Reaktion auf Angriffe. Wie sicher ist Ihr Unternehmen?

Mehr Infos >