CROWDSTRIKE

INCIDENT RESPONSE SERVICE

Cybersicherheitsvorfälle schnell und präzise erkennen, eindämmen und beheben

CROWDSTRIKE INCIDENT RESPONSE

Das CrowdStrike® Incident Response (IR) Team sorgt in einer unter Umständen gefährlichen und chaotischen Lage für Kontrolle, Stabilität und Ordnung. Angesichts der aktuellen Bedrohungslage werden die meisten Unternehmen und Institutionen irgendwann einen Sicherheitsvorfall erleiden, auf den sie reagieren und den sie wirksam bewältigen müssen. Wer folgenschwere Verluste vermeiden will, die sich auf mehrere Hunderttausend oder sogar Millionen Euro an direkten und indirekten Kosten belaufen können, muss schnell, effizient und kompetent handeln können.

Das IR-Team von CrowdStrike arbeitet mit Unternehmen und Institutionen gemeinsam daran, kritische Sicherheitsvorfälle zu bewältigen, Probleme unverzüglich zu beheben und eine langfristige Lösung zur Vermeidung neuer Vorfälle zu implementieren.
Bei seinen Untersuchungen verfolgt das IR-Team einen auf künstlicher Intelligenz basierenden, teamorientierten Ansatz. Die umfangreichen Erfahrungen aus der realen Welt werden dabei mit modernsten Technologien über die cloudbasierte CrowdStrike Falcon®-Plattform kombiniert. Mit Falcon identifiziert das Team den Angreifer schnell und präzise und beseitigt ihn aus Ihrer Umgebung. Methode und Konzept decken alle Aspekte eines Vorfalls ab. Hierzu zählen Erkennung, Untersuchung, Eindämmung, Beseitigung und Dokumentation der gewonnenen Erkenntnisse.
Das CrowdStrike-Team konzentriert sich gezielt darauf, die normale Geschäftsfähigkeit schnell wiederherzustellen und die Folgen eines Sicherheitsvorfalls zu mindern.

INCIDENT RESPONSE SERVICE VON CROWDSTRIKE BIETET UNTERNEHMEN FOLGENDE VORTEILE:

Technologie
Größe und Effizienz der cloud-nativen Falcon-Plattform ermöglicht es uns, Angreifer schnell und präzise zu identifizieren und aus Ihrer Umgebung zu beseitigen

Erfahrung und Expertenwissen
CrowdStrike rekrutiert ausschließlich Spitzenkräfte für Cybersicherheit, Incident Response und digitale Forensik. Dadurch entsteht ein Team mit unübertroffenen Fachkenntnissen und Fähigkeiten.

Enge Partnerschaft
CrowdStrike geht individuell vor und erarbeitet mit Ihrem Team einen Reaktions- und Abhilfeplan, der die geschäftlichen und sicherheitstechnischen Anforderungen des jeweiligen Unternehmens in Einklang bringt.

Positive Ergebnisse
Das IR-Team hilft Ihnen bei der Bewältigung der jüngsten Angriffe und leitet daraus Erkenntnisse ab, die Ihnen helfen, Ihre Sicherheitslage in Zukunft zu verbessern.

INCIDENT RESPONSE SERVICE

WICHTIGE LEISTUNGSMERKMALE

- **Incident Response in Echtzeit:** Wenn ein Sicherheitsvorfall eintritt, hängt alles von einer schnellen Behebung ab. Die IR-Methodik von CrowdStrike und die Falcon-Plattform bieten viele Vorteile gegenüber herkömmlichen IR-Ansätzen. CrowdStrike bringt Ihr Unternehmen schneller wieder ins Geschäft – in Tagen oder Wochen statt in Monaten. Und wir mindern die Auswirkungen eines Cyberangriffs. Das bedeutet für Sie:
  - Schnellere Transparenz und Behebung bei entsprechend geringeren forensischen Kosten
  - Weniger Verluste durch Geschäftsunterbrechung, da der normale Geschäftsbetrieb schneller wiederhergestellt ist
  - Weniger Auswirkungen aufgrund kürzerer Verweildauer der Angreifer
- **Erfahrung und Expertenwissen:** Das IR-Team von CrowdStrike wirkte bereits an einigen der weltweit wichtigsten Cyber-Untersuchungen mit. Die Teammitglieder verbessern ständig ihre Fertigkeiten und Kenntnisse, während sie Unternehmen und Institutionen im Kampf gegen versierte Angreifer unterstützen.
- **Hohe Qualität, hoher Geschäftswert:** Die Technologie und Methodik von CrowdStrike in Verbindung mit überlegenen Fertigkeiten und Erfahrungen ermöglichen es dem Team, schneller und effizienter zu reagieren und Vorfälle zu lösen. Das Ergebnis: weniger Zeitaufwand und geringere Kosten für Sie.
- **Maßgeschneidertes Konzept:** CrowdStrike arbeitet mit Ihrem Team zusammen und entwickelt einen Reaktions- und Abhilfeplan, der sowohl Ihre betrieblichen Anforderungen als auch Ihre bereits vorhandenen Investitionen und Ressourcen berücksichtigt. Dies gewährleistet eine eingehende Untersuchung und ermöglicht es dem Team, einen individuellen Plan für Abhilfemaßnahmen zu entwickeln, der die Geschäfts- und Sicherheitsanforderungen Ihres Unternehmens miteinander in Einklang bringt.
- **Positive Ergebnisse:** CrowdStrike dokumentiert die Ergebnisse und strategischen Empfehlungen des Teams zur Verbesserung Ihrer Sicherheitslage. Diese Empfehlungen sind auf Ihre vorhandene Technologieumgebung ausgelegt und werden Ihren wirtschaftlichen Zielen ebenso gerecht wie Ihren Sicherheitsanforderungen. Als erfahrene Experten für Incident Response und Bedrohungsaufklärung betrachtet das Serviceteam diese Erkenntnisse aus einer einzigartigen Perspektive und erstellt eine priorisierte Liste von Änderungsvorschlägen, die Ihre Fähigkeit verbessern, selbst besonders versierte und motivierte Angreifer zu erkennen, darauf zu reagieren und diese aktiv abzuwehren.

ÜBER CROWDSTRIKE SERVICES

CrowdStrike Services stattet Unternehmen und Institutionen mit dem nötigen Schutz und Know-how zur wirksamen Reaktion auf Sicherheitsvorfälle aus. Das Team von CrowdStrike Services unterstützt Kunden dabei, Angreifer in Echtzeit zu identifizieren, zu verfolgen und zu blockieren. Dabei nutzt es die cloudbasierte Plattform CrowdStrike Falcon® mit integriertem Endgeräteschutz der neuesten Generation, Erfassung von Cyber-Bedrohungsdaten, Berichterstattung und proaktiver Bedrohungssuche rund um die Uhr. Dank diesem einzigartigen Konzept kann CrowdStrike unbefugte Zugriffe schneller unterbinden und weitere Datenschutzverstöße verhindern. Darüber hinaus bietet CrowdStrike proaktive Services an, mit denen Unternehmen ihre Fähigkeit verbessern können, Bedrohungen zu antizipieren, Netzwerke abzusichern und Datenschutzverstöße letztlich zu unterbinden.

Erfahren Sie mehr unter www.crowdstrike.de/services/
E-Mail: services@crowdstrike.com

ABDECKUNG WICHTIGER VORFALLSTYPEN

Diebstahl von geistigem Eigentum
Darunter fällt der Diebstahl von Ideen, Erfindungen, kreativen Werken, Geschäftsgeheimnissen oder anderen sensiblen Informationen bei Angriffen, die oft von versierten nationalstaatlich unterstützten Akteuren durchgeführt werden.

Finanziell motivierte Kriminalität
Beispiele für diese Art von Angriffen sind gefälschte geschäftliche E-Mails, Diebstahl von Kreditkartendaten, Erpressung/Ransomware, Kryptojacking usw.

Zerstörerische Angriffe
Dies kann ein breites Spektrum von Angriffen umfassen: von gezielt eingesetzter Malware bis hin zu Malware, die auf Betriebsunterbrechungen ausgelegt ist.

Datendiebstahl
Dies schließt den Diebstahl von personenbezogenen Daten ein, durch den eine Person oder ein Kunde Ihres Unternehmens bloßgestellt werden könnte.

Insider-Bedrohungen
Hierbei handelt es sich um böswillige Übergriffe, die von Personen aus dem Unternehmen ausgehen, wie z. B. Mitarbeitern, ehemaligen Mitarbeitern, Auftragnehmern oder Geschäftspartnern.