CrowdStrike Services

CROWDSTRIKE

INCIDENT RESPONSE UND PROACTIVE SERVICES

Vorbereitung und Training für die schnelle und effektive Behebung von Sicherheitsvorfällen

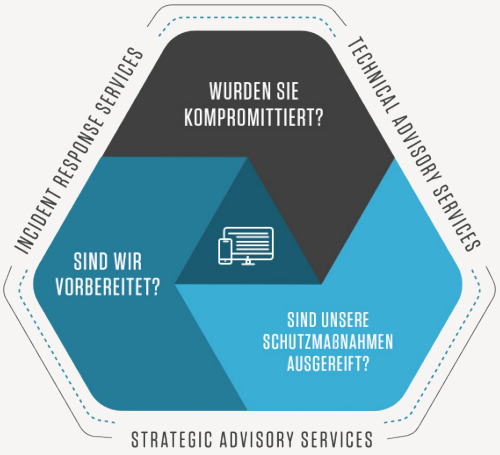
CROWDSTRIKE INCIDENT RESPONSE UND PROACTIVE SERVICES

WÄHLEN SIE DIE ZU IHREN ANFORDERUNGEN PASSENDEN SERVICES

Die CrowdStrike® Services umfassen sowohl Dienstleistungen zur Behebung von Vorfällen als auch proaktive Angebote. Diese spielen eine entscheidende Rolle, wenn es darum geht, die Sicherheitsaufstellung Ihrer Organisation zu verbessern und Datendiebstähle zu stoppen. Die spezifische Konzeption dieser Services ermöglicht eine schnelle und wirksame Reaktion auf Cybersicherheitsvorfälle. Kunden profitieren zudem von einer Reihe proaktiver Services, die darauf ausgelegt sind, die Cybersicherheitsreife zu verbessern.

Zur Durchführung dieser Maßnahmen steht CrowdStrike Services ein schlagkräftiges Team von Experten zur Verfügung. Es umfasst Sicherheitsfachleute aus den Bereichen Aufklärung, Strafverfolgung und Industrie ebenso wie IT-Architekten und Techniker international führender Technologieunternehmen sowie Sicherheitsberater, die bereits einige der weltweit anspruchsvollsten Untersuchungen geleitet haben.

Das Team arbeitet in erster Linie mit der CrowdStrike Falcon®-Plattform. Diese bietet wegweisenden Endgeräteschutz und ermöglicht eine Reaktion auf Vorfälle in Echtzeit sowie detaillierte forensische Analysen und Aufklärungsmaßnahmen. So ist gewährleistet, dass keine Bedrohung unentdeckt bleibt. CrowdStrike Services unterstützt Unternehmen dabei, sich auf Sicherheitsvorfälle und ausgefeilte Cyberangriffe vorzubereiten und diese abzuwehren. Besonders wichtig ist hierbei der Aufbau gezielter Maßnahmen zur Abwehr künftiger Angriffe.



Incident Response (IR) und Proaktive Services von CrowdStrike lassen sich einzeln oder kombiniert nutzen und über einen Services-Retainer abrechnen. Die Nutzung des Retainers ist flexibel: Wenn Sie keine CrowdStrike IR-Services benötigen, können Sie Ihr vorhandenes Stundenkontingent für Proactive Services nutzen, um so Ihre Sicherheitsaufstellung insgesamt weiter zu verbessern.

CROWDSTRIKE SERVICES AUF EINEN BLICK

Die Angebote von CrowdStrike Services helfen Unternehmen und Institutionen dabei, ihre Sicherheitsaufstellung zu stärken und zu optimieren, durch die Beantwortung von drei grundlegenden Fragen:

WURDEN WIR KOMPROMITTIERT?

- Incident Response Services für die Reaktion auf Vorfälle
- Endpoint Recovery Services für die Wiederherstellung von Endgeräten
- Compromise Assessment zur Integritätsbewertung
- Network Security Monitoring zur Überwachung der Netzwerksicherheit

SIND UNSERE SCHUTZMASSNAHMEN AUSGEREIFT?

- Bewertung der Cybersicherheitsreife
- Bewertung der Active-Directory-Sicherheit
- Bewertung der Cloud-Sicherheit
- Security Operations Center (SOC) -Bewertung
- Bewertung der IT-Hygiene
- Programm zur Verbesserung der Cybersicherheit
- Detaillierte Betrachtung des Sicherheitsprogramms
- Programm-Entwicklung für den effizienten Einsatz von Threat Intelligence

SIND WIR VORBEREITET?

- Tabletop-Übung
- Live-Übung eines Ernstfalls
- Angriffsemulation
- „Red Team / Blue Team"-Übung
- Penetrationstest

VERWALTETE SERVICES, SUPPORT UND VERFÜGBARKEIT

- Falcon Complete™
- Falcon Operational Support
- Falcon Training (CrowdStrike University)

CROWDSTRIKE INCIDENT RESPONSE UND PROACTIVE SERVICES

WURDEN WIR KOMPROMITTIERT?

INCIDENT RESPONSE (IR) SERVICES FÜR DIE REAKTION AUF VORFÄLLE

- Beschleunigen Sie die Behebung von Sicherheitsverletzungen und Datendiebstählen dank eines umfassenden Überblicks über die gegnerischen Aktivitäten, damit Sie Ihren Geschäftsbetrieb schneller wieder aufnehmen können. Das IR-Team von CrowdStrike arbeitet mit Ihnen gemeinsam daran, kritische Sicherheitsvorfälle zu bewältigen, Probleme anhand forensischer Analysen unverzüglich zu beheben und eine langfristige Lösung zur Vermeidung neuer Vorfälle zu implementieren.
- Das IR-Team verfolgt bei seinen Einsätzen einen auf Aufklärungsdaten basierten Ansatz. Dieser verbindet Praxiserfahrung mit forensischen Untersuchungen, Remediationserfahrung und modernste Technologie durch den Einsatz der cloudbasierten Falcon-Plattform. So können Angreifer schnell und präzise identifiziert und aus der Umgebung entfernt werden. Das CrowdStrike-Team konzentriert sich gezielt darauf, den Geschäftsbetrieb schnell wieder herzustellen und die Folgen eines Cybervorfalls so weit wie möglich zu reduzieren.

ENDPOINT RECOVERY SERVICES ZUR WIEDERHERSTELLUNG VON ENDGERÄTEN

- Die Endpoint Recovery Services von CrowdStrike helfen Ihnen, sich schnell und ohne Betriebsunterbrechung von APTs (Advanced Persistent Threat) und Angriffen zu erholen.
- Dieser Service vereint CrowdStrikes branchenführende Technologieplattform mit Daten aus der Bedrohungsaufklärung und einem Team von sehr erfahrenen Sicherheitsexperten. Diese Fachleute helfen bei der Erkennung, Analyse und Behebung bekannter Sicherheitsvorfälle und ermöglichen eine schnelle Wiederherstellung des Betriebs.

COMPROMISE ASSESSMENT ZUR INTEGRITÄTSBEWERTUNG

- Das Compromise Assessment Team von CrowdStrike identifiziert laufende oder vergangene Aktivitäten von Angreifern in Ihrer Umgebung. Es beantwortet die entscheidende Frage: „Wurde meine Organisation kompromittiert?“
- Das Team greift dabei auf jahrelange Erfahrung in der Abwehr versierter Angreifer zurück. In Kombination mit der leistungsstarken CrowdStrike Falcon®-Plattform, branchenführender Bedrohungsaufklärung und -suche rund um die Uhr ensteht so die umfassendste Integritätsbewertung Ihrer Umgebung.

NETWORK SECURITY MONITORING ZUR ÜBERWACHUNG DER NETZWERKSICHERHEIT

- Dieser Service bietet eine umfangreiche Überwachung Ihrer Netzwerksicherheit um aktive Bedrohungen in Ihrer Umgebung zu erkennen.
- Diese umfassende Überwachung der Netzwerksicherheit dient der Erkennung, Reaktion und Bedrohungssuche. Neben dem Know-how von CrowdStrike Services kommt hierzu eine Netzwerk-Appliance zum Einsatz, die vorhandene Bedrohungen in der Umgebung erkennt.

WARUM CROWDSTRIKE?

Ausgewiesenes Expertenwissen:
IR- und Malware-Spezialisten sowie Fachleute für Cyberaufklärung reagieren schnell und wirksam auf Vorfälle, führen forensische Analysen durch, stellen Endgeräte wieder her und ergreifen proaktive Maßnahmen.

Bedrohungsaufklärung:
Sie profitieren von minutengenauen Recherchen und Berichten über Bedrohungsakteure und deren Taktiken, Techniken und Verfahren, die auf Ihre Umgebung abzielen.

Konkurrenzlose Bedrohungssuche:
Die proaktive Suche nach Bedrohungen rund um die Uhr ergänzt die Suche nach Aktivitäten von Angreifern in Ihrer gesamten Umgebung.

Überlegene Technologie:
Die wegweisende CrowdStrike Falcon-Plattform schützt Ihre Endgeräte. So können Sie Angreifer schnell erkennen, bekämpfen und dauerhaft aussperren.

CROWDSTRIKE INCIDENT RESPONSE UND PROACTIVE SERVICES

SIND UNSERE SCHUTZMASSNAHMEN AUSGEREIFT?

CYBERSECURITY MATURITY ASSESSMENT

- Wer die Compliance-Auflagen erfüllt, ist noch lange nicht geschützt. Statt sich ausschließlich auf Compliance zu konzentrieren, bewertet unser Services-Team, wie ausgereift der Schutz zur Abwehr von Bedrohungen ist. Hierzu greifen wir auf jahrelange Erfahrung zurück.
- Die Methodik des Teams geht weit über ein übliches Audit hinaus. Die Bewertung der Cybersicherheit gibt Antwort auf die Frage, wie gut eine Organisation auf die Vermeidung, Erkennung und Abwehr von komplexen Angriffen vorbereitet ist.

ACTIVE DIRECTORY SECURITY ASSESSMENT (AD-SICHERHEITSBEWERTUNG)

- Die Konfiguration Ihres Active Directory (AD) sowie die dort hinterlegten Richtlinien werden einer eingehenden Prüfung unterzogen, um mögliche Schwachstellen in der AD Infrastruktur und Fehlkonfigurationen zu ermitteln, die von Angreifern ausgenutzt werden könnten.
- Diese Bewertung beinhaltet eine Überprüfung der Dokumentation, Gespräche mit Ihren Mitarbeitern, die Ausführung proprietärer Tools und eine manuelle Überprüfung Ihrer AD-Konfiguration und -Einstellung. Das Ergebnis ist ein detaillierter Bericht zu den erkannten Problemen und deren möglichen Folgen zusammen mit Empfehlungen zur Risikominimierung und Problembehebung.

CLOUD SECURITY ASSESSMENT / BEWERTUNG DER CLOUD-SICHERHEIT

- Das Cloud Security Assessment von CrowdStrike vermittelt Einblick in fehlerhafte sicherheitskritische Konfigurationen und Abweichungen von der empfohlenen Cloud-Sicherheitsarchitektur.
- In Verbindung mit der Erfahrung von CrowdStrike bei der Abwehr von Sicherheitsvorfällen und dem Engagement von anerkannten Fachleuten aus dem Bereich der Cloud-Sicherheitsarchitektur erhalten Sie mit dieser Bewertung einen Katalog an vorrangig durchzuführenden Maßnahmen, die darauf abzielen, Sicherheitsvorfälle in der Cloud zu vermeiden, zu erkennen und zu beheben.

IT HYGIENE ASSESSMENT ZUR BEWERTUNG DER IT-HYGIENE

- Entdecken Sie Schwachstellen proaktiv und schützen Sie Ihr Netzwerk, bevor es zu einem Datendiebstahl kommt.
- Das IT- Hygiene Assessment von CrowdStrike verschafft Ihnen einen verbesserten Einblick in Anwendungen, Zugangsmechanismen und die Kontenverwaltung in Ihrem Netzwerk. So erhalten Sie umfassende Informationen zum Netzwerkverkehr und über Sicherheitslücken. Da hierbei auch Schwachstellen identifiziert und fehlende Patches erkannt werden, ist es Ihnen möglich, Ihr Netzwerk proaktiv zu schützen, bevor es zu einem Datendiebstahl kommt.

CYBERSECURITY ENHANCEMENT PROGRAM ZUR VERBESSERUNG DER CYBERSICHERHEIT

- Entwickeln und implementieren Sie ein Programm zur Verbesserung der Cybersicherheit nachdem es zu einer Sicherheitsverletzung gekommen ist. Schließen Sie Sicherheitslücken und verhindern Sie weitere Datendiebstähle.
- Das Cybersecurity Enhancement Program von CrowdStrike richtet sich an Organisationen, die kürzlich einen Datendiebstahl erlitten haben und Unterstützung bei der Entwicklung eines strategischen Plans zur Verbesserung ihrer Cybersicherheit benötigen, damit weitere Datendiebstähle oder Sicherheitsverletzungen vermieden werden.

ZUSÄTZLICHE ANGEBOTE

SOC-Bewertung:
Verbessern Sie den Reifegrad Ihres SOC (Security Operations Center), indem Sie verbesserungswürdige Bereiche ermitteln und priorisieren.

Detaillierte Betrachtung des Sicherheitsprogramms:
Bestimmen Sie den Reifegrad Ihres Informations-sicherheitsprogramms durch die eingehende Untersuchung Ihrer Cybersicherheitsprozesse, -tools und -ressourcen.

Entwicklung eines Programms zur Bedrohungsaufklärung (Threat Intelligence Program Development)
Entwickeln Sie ein Programm zur Aufklärung von Bedrohungen, die von einer dynamischen Bedrohungslandschaft, globalen Bedrohungsakteuren und den neuesten Taktiken, Techniken und Verfahren ausgehen.

CROWDSTRIKE INCIDENT RESPONSE UND PROACTIVE SERVICES

SIND WIR VORBEREITET?

TABLETOP-ÜBUNG

- Die Erfahrung des Services-Teams von CrowdStrike mit der Durchführung von Ermittlungen zu komplexen Cyberbedrohungen gewährleistet, dass die Tabletop-Übungen unter realistischen Annahmen durchgeführt werden.
- Die Übungen simulieren einen gezielten Angriff. Hierbei werden Ihre Mitarbeiter – Führungskräfte oder Techniker – durch einen realistisch simulierten Sicherheitsvorfall geleitet. Auf diese Weise machen Sie sich mit allen Aspekten eines Angriffs vertraut, ohne die damit verbundenen Störungen und Schäden zu erleiden.

LIVE-ÜBUNG EINES ERNSTFALLS

- Im Rahmen dieser Übung werden einzelne Personen innerhalb der Organisation daraufhin getestet, ob sie mit ihrer Rolle in einem IR-Szenario vertraut sind.
- Anstatt der Besprechung eines hypothetischen Angriffs in der Gruppe, testet das Services-Team Ihre Tools und Prozesse in einer realistischen Übung. Bestimmte Informationen werden an einzelne Personen weitergegeben; so wie bei der tatsächlichen Untersuchung eines Vorfalls. Dann sind Ihre Mitarbeiter gefordert, die die Informationen bestmöglich nutzen müssen. Schwächen in Ihren Prozessen lassen sich durch diese Übung klar aufdecken.

ANGRIFFSEMULATION

- Dieser Test ermöglicht es Ihnen Ziel eines echten ausgefeilten und gezielten Angriffs zu werden, ohne dass Ihnen daraus der Schaden eines echten Vorfalls entsteht.
- Ein erfahrener Berater von CrowdStrike ahmt hierzu aktuelle Angriffstechniken nach, um sich Zugang zu Ihrem Netzwerk zu verschaffen und bestimmte Ressourcen zu kompromittieren. Nachdem dies gelungen ist, bespricht das Team von CrowdStrike mit Ihnen, wie es hierbei vorgegangen ist. Gemeinsam mit Ihnen werden dann mögliche Taktiken zur Vermeidung künftiger Angriffe ermittelt.

„RED TEAM / BLUE TEAM"-ÜBUNG

- Bereiten Sie Ihr Cybersicherheitsteam unter Anleitung von Experten auf den Ernstfall vor: Das rote Team greift Ihre Umgebung an, das blaue Team übernimmt die Verteidigung.
- Diese Übung arbeitet mit realen, gezielten Angriffsszenarien und dient dazu, das Know-how Ihrer Mitarbeiter zur Bedrohungssuche und zur Reaktion auf Vorfälle zu erweitern und zu verbessern.

PENETRATIONSTEST

- Das Services-Team arbeitet nach den Grundsätzen von „Ethical Hacking", um Sicherheitslücken aufzuspüren. Hierzu führt es mit Ihrem Einverständnis simulierte Angriffe und Penetrationstests für verschiedene Komponenten Ihrer Systeme, Netzwerke und Anwendungen durch.
- Sie können aus einer Vielzahl von Testoptionen wählen, die Ihren Anforderungen gezielt entsprechen.

VERWALTETE SERVICES, SUPPORT UND TRAINING

- **FALCON COMPLETE™:** Diese umfassende Lösung zum Schutz von Endgeräten und zur Bedrohungssuche wird als sofort einsatzbereiter, vollständig verwalteter Service bereitgestellt, der auf der Leistungsfähigkeit der Falcon-Plattform basiert.
- **FALCON OPERATIONAL SUPPORT:** Der operative Support unterstützt Sie bei der Konfiguration und Verwaltung der Falcon-Plattform zur Optimierung Ihrer Cybersicherheitsabläufe.
- **FALCON TRAINING:** Die professionellen Schulungs- und Weiterbildungsservices der CrowdStrike University (CSU) vertiefen und erweitern das Know-how Ihres Cybersicherheitsteams. So holen Sie das Beste aus Ihrer Investition in die Falcon-Plattform heraus.

ÜBER CROWDSTRIKE SERVICES

CrowdStrike Services stattet Unternehmen und Institutionen mit dem nötigen Schutz und Know-how zur wirksamen Reaktion auf Sicherheitsvorfälle aus. Das Sicherheitsteam 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 Services unbefugte Zugriffe schneller unterbinden und weitere Datenschutzverstöße verhindern.

Darüber hinaus bietet CrowdStrike strategische Beratung an, damit Unternehmen ihre Fähigkeit verbessern können, Bedrohungen zu antizipieren, Netzwerke abzusichern und Kompromittierungen letztlich zu stoppen.

Erfahren Sie mehr unter **www.crowdstrike.com/services/**

Email: **services@crowdstrike.com**