CROWDSTRIKE

COMPROMISE ASSESSMENT

Erkennung laufender und zurückliegender Angreifer-Aktivitäten

STELLEN SIE FEST, OB IHRE ORGANISATION OPFER EINES ANGRIFFS GEWORDEN IST

Das CrowdStrike® Services Compromise Assessment dient dazu, laufende oder vergangene Angreiferaktivitäten in der Umgebung einer Organisation zu identifizieren. Es nutzt die langjährige Erfahrung des Crowdstrike Services Teams bei der Abwehr versierter Angreifer in Verbindung mit der leistungsstarken CrowdStrike Falcon®-Plattform, branchenführender Threat Intelligence und 24/7 Threat Hunting. Diese Kombination liefert eine umfangreiche Bewertung der IT-Umgebung Ihres Unternehmens und die Antwort auf die entscheidende Frage: „Ist meine Organisation kompromittiert worden?"

Das Services-Team besitzt umfangreiche Erfahrungen mit großen und komplexen Incident-Response-Untersuchungen und gezielten Bedrohungen. Es ist damit in der Lage, Taktiken, Techniken und Verfahren (TTPs) offenzulegen, die heute von den versiertesten Angreifern eingesetzt werden. Die Kombination von Wissen, Expertise und der mehrfach ausgezeichneten, cloudbasierten Endgerätetechnologie der Falcon-Plattform erlaubt eine gründliche und umfassende Bewertung, die über eine herkömmliche indikatorbasierte Erkennung und punktuelle Überwachung hinausgeht und sowohl auf kompetenten Analysen historischer, forensicher Daten und auf der Bedrohungserkennung und -suche in Echtzeit basiert. Nur wenn Sie wissen, was in der Vergangenheit passiert ist und was derzeit auf Ihren Endgeräten vor sich geht, sind Sie in der Lage, Ihre Cyber-Umgebung in Zukunft wirksam zu verteidigen.

DIE VORTEILE IM ÜBERBLICK

DAS BIETET DAS CROWDSTRIKE COMPROMISE ASSESSMENT

Minimierte Verweilzeit: Sie erfahren, ob Angreifer Ihre Verteidigungsmaßnahmen durchbrechen konnten und sich unbemerkt in Ihrer Umgebung bewegen

Reduzierte Risiken: Eine gründliche Analyse reduziert das Risiko, dass Angreifer finanzielle Assets, Kundendaten oder geistiges Eigentum stehlen

Verbesserte Sicherheit: Ineffektive Sicherheitspraktiken, die Ihr Unternehmen gefährden, werden proaktiv identifiziert

COMPROMISE ASSESSMENT

WICHTIGE LEISTUNGSMERKMALE

EIN HOCHQUALIFIZIERTES TEAM

- Das Team von CrowdStrike Services verfügt über hervorragende Fachkenntnisse und Fähigkeiten zur Durchführung von Compromise Assessments. Es umfasst die besten Experten aus Cybersicherheit, Incident Response, Forensik und Operations, die Ihnen einzigartige Einblicke in die aktuellen Taktiken, Techniken und Verfahren (TTPs) der versiertesten Gegner bieten.

BRANCHENFÜHRENDE WERKZEUGE

- **Die Falcon-Plattform** verleiht Ihnen in Echtzeit Einblick in Ihre Umgebung. So können Sie potenzielle Schwachstellen erkennen und gezielt beseitigen. Dies ist ein erheblicher Vorteil gegenüber herkömmlichen Compromise Assessments auf der Grundlage klassischer forensikbasierter Konzepte, die lediglich nach Gefährdungsindikatoren (IOCs) suchen.
- **Falcon Insight™** ist die Lösung für Endpunktbasierte Detektion und Reaktion (EDR) von CrowdStrike und bietet modernsten cloud-nativen Schutz mit einem einzigen, schlanken Agent, der auf jedem Endgerät in Ihrer Umgebung bereitgestellt wird.
- **Falcon Forensics Collector (FFC)** ist ein plattformübergreifendes, nicht-persistentes und einmalig ausführbares Tool, das Daten von mehr als 45 forensisch signifikanten Artefakten auf jedem Endgerät sammelt. Die Daten werden in der CrowdStrike-Cloud aggregiert und verarbeitet. Dort können sie mit der CrowdStrike Intelligence zur Verfolgung und Identifikation gegnerischer TTPs abgeglichen werden.

EIN UMFASSENDER ANSATZ

- Die Bewertung kombiniert die fachliche Analyse historischer forensischer Beweise mit Bedrohungserkennung und -suche in Echtzeit. Auf dieser Grundlage kann CrowdStrike nach Aktivitäten von Angreifern am Endgerät und im Netzwerk suchen.
- Ein Compromise Assessment von CrowdStrike beginnt mit der effizienten Sammlung und Analyse forensischer Artefakte von Microsoft Windows, macOS und vielen Linux-basierten Betriebssystemen, ohne die Notwendigkeit von On-Premise-Anwendungen oder der aktiven Indikatorensuche. Parallel dazu bietet die CrowdStrike Falcon-Plattform Bedrohungserkennung und -überwachung Ihrer Umgebung in Echtzeit. Hierbei wird sowohl nach Malware als auch Malware-freien Bedrohungen sowie nach Angriffsindikatoren (Indicators of Attack, IOAs) gesucht.
- Die aussagekräftige Bewertung, ob es in Ihrer Umgebung bösartige Aktivitäten gegeben hat, setzt einen umfassenden, historischen und forensisch basierten Kontext in Verbindung mit einer dynamischen Beobachtung voraus. Jede Umgebung ist einzigartig. Daher arbeitet das Services-Team schnell und effizient mit Ihrem Team daran, Ihre Netzwerktopologie und die Systeme in Ihrer Umgebung kennenzulernen.

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.

FUNDIERTE ANALYSEN UND ERKENNTNISSE

Ein erfolgreiches Compromise Assessment setzt Erkenntnisse und Analyseberichte voraus, die für alle Beteiligten in den Bereichen IT-Sicherheit und Risikomanagement aussagekräftig und relevant sind. Die CrowdStrike Consultants stellen typischerweise folgende Unterlagen zur Verfügung:

Einen schriftlichen Bericht, aus dem hervorgeht, ob Beweise für ein gezieltes Eindringen in Ihre Umgebung entdeckt wurden, verbunden mit Empfehlungen für wirksame Verbesserungen Ihrer Sicherheitsaufstellung

Eine schriftliche Zusammenfassung mit maßgeblichen Ergebnissen, Schlussfolgerungen und Empfehlungen

Eine technische Dokumentation der vom CrowdStrike Services Team durchgeführten Bewertung. Ihr technisches Team hat damit die Informationen, die es zur Behebung und Entfernung der Probleme sowie zur Validierung der Ergebnisse des Services-Teams benötigt

Weiterführende Erkenntnisse über das Vorhandensein von Commodity-Malware, verdächtigen Skripten und Dateien, Dienstprogrammen für den Fernzugriff und riskanten Administrationspraktiken

Erfahren Sie mehr unter www.crowdstrike.de/services/
Email: services@crowdstrike.com