CROWDSTRIKE

FALCON IDENTITY THREAT DETECTION

ERKENNUNG KOMPLEXER IDENTITÄTSBEDROHUNGEN

ANGRIFFE AUF DIE IDENTITÄT LIVE VERFOLGEN

Falcon Identity Threat Detection (ITD) macht identitätsbasierte Angriffe und Anomalien sichtbar. Dazu wird der Datenverkehr live mit Verhaltensgrundmustern und -regeln verglichen, um Angriffe und Seitwärtsbewegungen zu erkennen. Die Erkennung von Identitätsbedrohungen in Echtzeit warnt bei kompromittierten Zugangsdaten und infizierten Rechnern im Netzwerk oder in der Cloud oder bei sonstigem ungewöhnlichen Authentifizierungs-Traffic. 80 % der Datendiebstähle gehen mit kompromittierten Anmeldeinformationen einher. Die Automatisierung der Bedrohungserkennung und die Erstellung dynamischer Risikoprofile und Warnmeldungen zum Traffic von Identitätsdaten sind daher der beste Weg zur Absicherung aller Domänen in Ihrer Umgebung.

WICHTIGE PRODUKTMERKMALE

ECHTZEITWARNUNG BEI VERDÄCHTIGEM TRAFFIC

Erkennen Sie anomale Aktivitäten, ohne Protokolle einsehen zu müssen. Falcon ITD erkennt Bedrohungen, zeichnet sich durch eine niedrige False-Positive-Rate aus und bietet zudem die Möglichkeit, schwer erkennbare Bedrohungen durch logbasierte Sicherheitswerkzeuge nach dem Ereignis zu ermitteln.

VORBEREITET FÜR HYBRIDE IDENTITÄTSSPEICHER

Die Lösung funktioniert für Identitätsspeicher vor Ort oder in der Cloud sowie für alle Benutzer/Anwendungen, ohne dass Agents auf Endgeräten oder Servern außerhalb der Domänencontroller installiert werden müssen.

WESENTLICHE VORTEILE

- Untersuchung von Authentifizierungsereignissen und bedenklichem Benutzerverhalten über eine einfache grafische Oberfläche
- Eine Correlation Engine fasst Ereignisse nach Benutzer, Gerät, Aktivität usw. zusammen und erleichtert eine bessere Reaktion auf Vorfälle
- Einheitliche Darstellung des Zugriffsverkehrs für Anwendungen, Ressourcen und Identitätsspeicher
- Reduzierung der mittleren Erkennungs- und Behebungszeit (MTTD/R) sowie höhere Effizienz und kürzere Antwortzeiten von SOC-Analysten, da die mühsame und fehleranfällige Sichtung komplexer Protokolle entfällt
- Verbesserung der Alarmqualität und genauere Ergebnisse durch Erkennen der tatsächlich relevanten Ereignisse
- Geringere Kosten für die Protokollspeicherung, da nur relevante Authentifizierungsprotokolle gespeichert werden

VERHALTENSBASIERTE INDIKATOREN UND PROFILERSTELLUNG

IDT-Profile beruhen einerseits auf statischen Informationen aus Identitätsspeichern und andererseits auf dynamischen Informationen in Echtzeit. Dies dient dazu, Insider-Bedrohungen, Seitwärtsbewegungen und den Missbrauch von Privilegien oder Service-Konten abzufangen. So vermeiden Sie riskante Spekulationen und können sich auf die Authentifizierungsaufgaben konzentrieren, die auf über 100 Verhaltensanalysen und Risikobewertungen für jedes Konto basieren.

ANGRIFFE AUF IDENTITÄTSSPEICHER ERKENNEN

Sie erkennen Bedrohungen von Identitätsspeichern (und typische Angriffssimulationen), wie beispielsweise Bedrohungen von NTLM/LDAPS-Protokollen, Golden-Ticket-Angriffe, Pass-the-Hash und andere Credential-Diebstähle sowie Persistenztechniken.

WERKZEUGE FÜR DIE REAKTION AUF VORFÄLLE

Die in Falcon Identity Threat Detection integrierte Threat-Hunter-Funktion macht alle Credential-Angriffe und Reaktionen auf Vorfälle wie in einem Mini-SIEM sichtbar und zeigt die Aktivitätsketten sowie das Ergebnis der anschließenden Risikobewertung auf. Einfach zu bedienen: Für Betrieb und Administration sind keine CLI- oder eingehenden Sicherheitskenntnisse erforderlich. Die Lösung lässt sich in viele gängige Ticketing-Plattformen integrieren.

WEITGEHENDE INTEGRATION IN ANDERE SICHERHEITSWERKZEUGE

Export im CEF- oder LEEF-Format über API in jedes SIEM oder in SOAR-Tools möglich.

ERWEITERTE PROTOKOLLABDECKUNG

CrowdStrike Falcon Identity Threat Detection vermittelt einen granularen Einblick in Vorfälle unter Einbeziehung von Protokollen wie NTLM, RPC und LDAP/S, die mit herkömmlichen Tools wie NGFW und UEBA nicht oder nur schwer zu erkennen sind.

MEHRWERT DURCH GESCHWINDIGKEIT

Eine typische Installation dauert weniger als eine Stunde. Anschließend kann die Identifizierung von Anomalien sofort starten.

ÜBER CROWDSTRIKE

CrowdStrike ist der führende Anbieter beim cloudbasierten Endgeräteschutz. Die Plattform CrowdStrike Falcon® sorgt auf Anhieb für Transparenz und Schutz im gesamten Unternehmen und verhindert Angriffe auf Endgeräte innerhalb und außerhalb des Netzwerks – unterstützt durch verwaltete Bedrohungssuche rund um die Uhr. Es gäbe noch viel darüber zu sagen, wie CrowdStrike Falcon den Endgeräteschutz neu definiert. Aber unter dem Strich sollten Sie vor allem eines über CrowdStrike wissen: Wir stoppen Datendiebstahl.