CROWDSTRIKE

FALCON INTELLIGENCE

Die in den Endgeräteschutz integrierte Bedrohungsaufklärung automatisiert die Untersuchung von Vorfällen und beschleunigt die Abwehr von Angriffen

ENDGERÄTESCHUTZ AUF HÖCHSTEM NIVEAU

Die Bedrohungslandschaft entwickelt sich ständig weiter. Sicherheitsverantwortliche benötigen daher jede erdenkliche Unterstützung, um Bedrohungen wirksam zu verhindern, zu erkennen und abzuwehren. Je besser Sicherheitsverantwortliche darüber informiert sind, wer sie angreift, warum sie ins Visier genommen werden und wie die Angriffe ablaufen, desto besser können sie sich verteidigen. Durch Integration der Bedrohungsinformationen in die Arbeitsabläufe der Sicherheitsteams lassen sich Bedrohungen erheblich schneller, effizienter und präziser untersuchen.

CrowdStrike® Falcon® Intelligence™ baut auf der CrowdStrike Falcon®-Plattform auf. Die Lösung gewährleistet einen Endgeräteschutz auf höchstem Niveau. Hierzu werden die maßgeblichen Bedrohungen analysiert, denen die Endgeräte ausgesetzt sind. Falcon Intelligence untersucht Vorfälle automatisch und beschleunigt damit die Alarmierung und Abwehr.
Die Bedrohungsaufklärung mit Falcon Intelligence ist Teil des Workflows. Aus ihr errechnet sich die Risikobewertung, woraus sich weitere wichtige Schritte ableiten: Priorisierung, Offenlegung der Absicht und der Vorgehensweise der Angreifer, Malware-Analyse zur Aufdeckung des Angriffsverhaltens und Ermittlung von Gefährdungsindikatoren zur Stärkung der Verteidigung und zur Implementierung von Gegenmaßnahmen.

Indem erkannte Vorfälle automatisch mit Informationen aus der Bedrohungsaufklärung ergänzt werden, können auch kleinere Sicherheitsteams ein hohes Schutzniveau erreichen. Größere Teams profitieren von einer deutlich effektiveren Vorgehensweise.

WESENTLICHE VORTEILE

- Automatisierte Untersuchung aller Bedrohungen an Endgeräten
- Ergänzung der von CrowdStrike Falcon erkannten Bedrohungen durch wichtige Informationen zur schnelleren und besseren Abwehr
- In die Falcon-Plattform integriert und innerhalb weniger Sekunden einsatzbereit
- Bereitstellung von Gefährdungsindikatoren zum proaktiven Schutz vor zukünftigen Bedrohungen und Malware-Infektionen
- Vorkonfigurierte Integrationen und Anwendungsprogrammier-schnittstellen (APIs) für branchenführende Sicherheitslösungen

FALCON INTELLIGENCE

WICHTIGE LEISTUNGSMERKMALE

AUTOMATISIERTE UND VEREINFACHTE UNTERSUCHUNG VON VORFÄLLEN

- **Nahtlose Integration der Endgeräte:** Sie analysieren die wirklich maßgeblichen Bedrohungen Ihrer Endgeräte, die durch die CrowdStrike Falcon-Plattform geschützt sind. Die Analyse mit Falcon Intelligence wird zusammen mit den Informationen über die Erkennung eines Endgerätevorfalls angezeigt. Ein Angriff auf die eigene Umgebung ist für Sicherheitsteams unabhängig von Mannstärke oder Kenntnisstand immer auch eine Chance, neue Erkenntnisse zu gewinnen.
- **Zeit, Aufwand und Geld sparen:** Sie automatisieren jeden Schritt der Bedrohungsanalyse und schließen Ihre Analyse innerhalb von Minuten statt in Tagen ab. Falcon Intelligence kombiniert Malware-Analyse, Malware-Suche und die Analyse von Bedrohungen in einer durchgängigen Lösung.
- **Bedrohungen sichtbar machen:** Der Indicator Graph von Falcon Intelligence zeigt Ihnen die Beziehungen zwischen Gefährdungsindikatoren (IOCs), Gegnern und Endgeräten in Ihrer Umgebung auf. So sehen Sie auf Anhieb, wie sich die Bedrohung ausgebreitet hat und welche Endgeräte betroffen sind.

DEN GEGNER KENNEN

- **Böswillige Akteure nachverfolgen und stoppen:** Die Bedrohungsdaten aus CrowdStrike lassen Rückschlüsse über die Akteure zu. So können Sie die Motivation, die Werkzeuge und die Verfahren der Angreifer aufdecken. Gleichzeitig erhalten Sie eine praxisorientierte Anleitung, damit Ihr Team Gegenmaßnahmen einleiten und künftigen Angriffen vorgreifen kann.
- **Wöchentlicher Bedrohungsbericht:** Sie erhalten per E-Mail wöchentlich eine Zusammenfassung der kürzlich beobachteten Aktivitäten in den Bereichen eCrime, Cyberspionage und Hacktivismus. Darin enthalten sind zudem aktuelle Infos zu Datendiebstählen, Sicherheitsverletzungen und mehr.

HÖHERE SICHERHEIT DURCH TEILEN VON GEFÄHRDUNGSINDIKATOREN

- **Schutz vor den wirklich maßgeblichen Bedrohungen:** Ihr Team konzentriert sich auf die Bedrohungen, denen Sie tatsächlich ausgesetzt sind. Falcon Intelligence stellt Gefährdungsindikatoren bereit, die aus der Malware-Analyse direkt von Ihren Endgeräten stammen. Weitere Indikatoren werden aus der Malware derselben Kampagne, der Malware-Familie oder desselben Autors erzeugt.
- **Zugriff auf Gefährdungsindikatoren von CrowdStrike:** Der globale IOC-Feed von CrowdStrike liefert hochwertige Gefährdungsindikatoren in Echtzeit, die das Team von CrowdStrike Intelligence erstellt und ausgewertet hat. Die Indikatoren im IOC-Feed sind mit Kontexten angereichert, wie beispielsweise Vertrauensniveau, Zuordnung, zugehörige Schwachstellen, Bedrohungsart und mehr.
- **Einfache Integration von Gegenmaßnahmen:** Schützen Sie sich vor künftigen Angriffen mit Gefährdungsindikatoren, die Ihre Sicherheitsinfrastruktur problemlos weiterverarbeiten kann. Die umfangreiche Sammlung von APIs und vorkonfigurierten Tools macht die Orchestrierung für bestehende Sicherheitslösungen einfach.

MERKMALE VON FALCON INTELLIGENCE

- In die CrowdStrike Falcon-Plattform integriert
- Erkennungen von Falcon werden mit Bedrohungsinformationen von CrowdStrike angereichert
- Automatisierte Malware-Analyse
- IOC-Feed in Echtzeit
- Indicator Graph
- Täterprofile
- Wöchentliche Updates zu Bedrohungen
- APIs und vorkonfigurierte Integrationen von Dritten

ÜBER CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die Plattform CrowdStrike Falcon® verfügt über eine einzigartige, Cloud-basierte, schlanke Agentenarchitektur, die von künstlicher Intelligenz (KI) unterstützt wird und unternehmensweit für Schutz und Transparenz in Echtzeitsorgt. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 3 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cyber- Sicherheit.

Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation

Erfahren Sie mehr unter **www.crowdstrike.de**