CROWDSTRIKE

FALCON INTELLIGENCE PREMIUM

Bedrohungsaufklärung zur proaktiven Abwehr von Gegnern und Angriffen

WISSEN, WER IHR UNTERNEHMEN IM VISIER HAT

CrowdStrike® Falcon Intelligence™ Premium ist das führende Angebot von CrowdStrike zur Bedrohungsaufklärung. Anhand fundierter Aufklärungsdaten können Unternehmen und Institutionen damit Angriffe von nationalstaatlichen Akteuren, Cyber-Kriminellen und Hackern antizipieren und abwehren. Mit Falcon Intelligence Premium haben Teams aus den Bereichen Security Operation, Incident Response und Cyber-Aufklärung alles zur Hand, um die hochgerüsteten Gegner von heute schnell zu erkennen, zu durchschauen und zu schlagen.

Ganz gleich, ob sich Ihr Sicherheitsteam gerade erst einarbeitet oder bereits Erfahrung mit der Aufklärung von Cyber-Bedrohungen hat: Falcon Intelligence Premium beinhaltet alles Nötige zur Stärkung Ihrer Sicherheitsabwehr. Ihre Teams sind besser informiert und können effizienter und effektiver tätig werden.

WICHTIGE LEISTUNGSMERKMALE

DEN GEGNER UND SEINE ANGRIFFE KENNEN

- **Gegnerprofile:** Zugriff auf über 140 detaillierte Gegnerprofile. CrowdStrike ist ein Vorreiter bei der Analyse böswilliger Akteure. Ein globales Team von Aufklärungsexperten, Forschern und Experten für geopolitische Fragen erstellt wegweisende Recherchen zur Aufdeckung der Absicht, Motivation und Technik potenzieller Gegner.
- **Bedrohungswarnungen:** Verschaffen Sie sich auf Anhieb Einblick in neue und vorhandene Cyber-Bedrohungen. Mit Bedrohungswarnungen in Echtzeit, die Sie über die neuesten Datendiebstähle, Malware-Entwicklungen, Aktivitäten und Kampagnen von Angreifern auf dem Laufenden halten.
- **Technische Berichte:** Verbessern Sie das Lagebewusstsein Ihrer Sicherheitsteams und verringern Sie das Risiko von Kampagnen, die sich gegen Ihre Organisation richten. Unsere technischen Berichte enttarnen gegnerische Operationen, Ziele und Zeitpläne sowie deren Taktiken, Techniken und Verfahren (TTPs). Das verschafft Ihnen Zeit, Ihre Abwehrmaßnahmen zu verbessern.
- **Gezielte Aufklärung:** Durchsuchen Sie soziale Medien nach verdächtigen Aktivitäten in Online-Foren. Fahnden Sie nach DDoS- und Botnet-Angriffen, um Aktionen gegen die Infrastruktur Ihrer Organisation aufzudecken.

VON FALCON INTELLIGENCE PREMIUM PROFITIERT JEDES TEAM

Security Operations Centers (SOCs): Beschleunigt die Einordnung von Warnungen und vereinfacht die Untersuchung von Vorfällen

Reaktion auf Vorfälle: Verbessert die Priorisierung von Vorfällen und Strategien zur Risikoeindämmung

Informationen über Cyber-Bedrohungen: Erstklassige Rechercheergebnisse und verbessertes Gefahrenbewusstsein

Informationstechnologie: Verbessert die Wirksamkeit der Sicherheitsmaßnahmen

Management-Unterstützung: Risikomanagement und Sicherheitsent-scheidungen anhand fundierter Fakten

FALCON INTELLIGENCE PREMIUM

HÖHERE SICHERHEIT UND FUNDIERTE ENTSCHEIDUNGEN

- **Executive Reports:** Entscheidungsträger werden in die Lage versetzt, Auswirkungen von Cyber-Risiken auf ihre Organisation besser zu verstehen. Diese Berichte konzentrieren sich auf mittel- und langfristige Trends. Sie helfen der Leitung, sinnvolle Investitionen in die Sicherheit zu tätigen und die Aktivitäten der Sicherheitsverantwortlichen auf die Ziele und Strategien der Organisation auszurichten.
- **Vierteljährliche Berichte zur Bedrohungslage:** Gewinnen Sie mehr Einblick, indem Sie an den vierteljährlichen CrowdStrike-Webcasts zur aktuellen globalen Bedrohungslandschaft teilnehmen. Fachleute von CrowdStrike konzentrieren sich auf die jüngsten gegnerischen Kampagnen, die Zielregionen und -branchen sowie die neuesten TTP-Innovationen.
- **Informationsanfragen (RFIs):** Kunden von Falcon Intelligence Premium können RFI-Pakete erwerben. Über RFI-Pakete können Sie bis zu fünf Anfragen an einen CrowdStrike-Experten stellen. Der führt die entsprechenden Recherchen durch und liefert individuelle Antworten.

MALWARE ANALYSIEREN UND MASSNAHMEN ERGREIFEN

- **Malware-Analyse:** Dank der automatisierten Malware-Analyse-Sandbox von CrowdStrike werden Sie auch mit der raffiniertesten Malware fertig. Die Sandbox führt sowohl statische als auch dynamische Analysen durch und überwacht gleichzeitig bösartiges Verhalten und Systeminteraktionen. Hierbei wird nicht nur eine einzelne Malware-Probe analysiert, sondern auch geprüft, ob die verdächtige Datei mit einer größeren Kampagne, einer Malware-Familie oder einem Gegner in Verbindung steht.
- **Malware-Analyse von Experten:** Senden Sie Malware-Proben an einen CrowdStrike-Experten, um weitere Recherchen durchführen zu lassen oder eine zweite Meinung einzuholen. Sie können bis zu fünf Dateien pro Monat für diese Art von Analyse einreichen.
- **Endgeräteintegration:** CrowdStrike-Kunden können auch potenzielle Malware-Dateien analysieren, die direkt von Endgeräten stammen, die durch die CrowdStrike Falcon®-Plattform geschützt sind. Die Analyseergebnisse sind in der Falcon-Plattform sichtbar und werden zusammen mit der Bedrohungserkennung dargestellt. Dank der engen Verknüpfung von Erkennungs- und Bedrohungsinformationen können Ihre Mitarbeiter schnellere und bessere Entscheidungen treffen.

VERBESSERN SIE IHRE ABWEHR IN DER GESAMTEN SICHERHEITSINFRASTRUKTUR

- **Zugriff auf Gefährdungsindikatoren (IOC) 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.
- **YARA- und Snort-Regeln:** Verbessern Sie die Fähigkeit, versierte Angriffe aus Verhaltens- oder Infrastrukturperspektive zu erkennen. CrowdStrike erstellt und testet YARA- und Snort-Regeln, sodass Sie auch raffinierte Bedrohungen automatisch erkennen, klassifizieren und mit einem Minimum an Fehlalarmen zuordnen können.
- **Einfache Integration von Gegenmaßnahmen:** Schützen Sie sich mit Gefährdungsindikatoren und Sicherheitsregeln vor künftigen Angriffen. Die Integration in SIEM (Security Information and Event Management), Firewall, Netzwerkgeräte und Intrusion-Detection-Systeme ist problemlos machbar. Die umfangreiche Sammlung von APIs und vorkonfigurierten Tools erleichtert die Integration in bestehende Sicherheitslösungen.

MERKMALE VON FALCON INTELLIGENCE PREMIUM

- Automatisierte Malware-Analyse
- IOC-Feed in Echtzeit
- Tägliche Bedrohungsberichte
- Technische Berichte
- Strategische Berichte
- Angreiferprofile
- Individualisierte Intelligence-Informationen
- Snort-/YARA-Regeln
- Vierteljährliche Briefings zu Bedrohungen
- Malware-Analyse von Experten (bis zu 60 Malware-Dateien)
- APIs und vorkonfigurierte Integrationen
- Zugang zu RFI-Paketen (separat erhältlich)

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**

© 2020 CrowdStrike, Inc. Alle Rechte vorbehalten.