CROWDSTRIKE

FALCON X RECON

Gefahren für Marke, Mitarbeiter und sensible Daten erkennen – im öffentlichen Web, im Deep Web und im Darknet

ABKLÄRUNG DIGITALER RISIKEN IM DARK WEB UND DARÜBER HINAUS

Mit CrowdStrike Falcon X™ Recon können Unternehmen und Institutionen potenziell bösartige Aktivitäten im öffentlichen Web, im Deep Web und im Darknet aufdecken und ihre Marken, Mitarbeiter und sensiblen Daten besser schützen. Falcon X Recon dient dazu, Daten zu erfassen und die Aktivitäten von Millionen nicht öffentlicher Webseiten, krimineller Foren und verschlüsselter Messaging-Plattformen zu überwachen, also den versteckten Nischen im Internet, wo sich kriminelle Akteure versammeln und die digitale Wirtschaft im Untergrund floriert. Mit Falcon X Recon können Sicherheitsverantwortliche Untersuchungen in Echtzeit durchführen und Betrug, Datendiebstahl, Phishing-Kampagnen und andere Online-Bedrohungen proaktiv aufdecken.

WICHTIGE LEISTUNGSMERKMALE

ERFASSEN

Falcon X Recon eröffnet den Zugriff auf Daten, die in den vergangenen acht Jahren aus normalerweise schwer zugänglichen digitalen Kanälen im öffentlichen Web ebenso wie im Deep Web und Darknet gesammelt wurden. Falcon X Recon sammelt zudem proaktiv Rohdaten über betrügerische Aktivitäten, Datendiebstähle, Bedrohungen von Unternehmen und identifizierte Exploits und Tools im Arsenal der kriminellen Angreifer.

- **Sammeln umfangreicher Rohdaten:** Sie können Daten aus Millionen versteckter Webseiten und Tausenden von nicht öffentlichen Foren, Marktplätzen, Paste-Sites, IRC-Kanälen, Rogue-Apps, Phishing-Domains und offenen und geschlossenen Messaging-Anwendungen wie Telegram, QQ usw. überwachen.
- **Durchführen verdeckter Ermittlungen in Echtzeit:** Sie schwächen potenzielle Angreifer durch Zugriff auf Echtzeit-Rohdaten und schränken deren Angriffsmöglichkeiten ein. Sie führen Ermittlungen durch, indem Sie auf Daten von nicht öffentlichen Sites zugreifen, ohne Spuren zu hinterlassen. Falcon X Recon speichert historische Daten, sodass Angreifer ihre Spuren nicht durch Ändern oder Löschen von Beiträgen verwischen können.
- **Verfolgen krimineller Angreifer:** Sie analysieren und verfolgen Verhaltensänderungen von Angreifern im zeitlichen Verlauf und Identifizierung von Aktivitätssteigerungen, neuartigen Angriffe, neuen Ziele und weiterentwickelten Techniken und Tools, sodass Sie sich besser vor externen Bedrohungen schützen können.

DIE VORTEILE IM ÜBERBLICK

Unübertroffene Abdeckung von öffentlichem Web, Deep Web und Darknet

Automatisierte Extraktion von Daten aus Millionen von nicht öffentlichen Umgebungen und aus dem Untergrund

Verkürzung der Untersuchungszeit und Verbesserung von Effizienz und Reaktionsfähigkeit

Echtzeit-Überwachung anhand von Regeln, die auf die eigene Organisation abgestimmt sind

Sofortige Amortisierung – in wenigen Minuten einsatzbereit

Umfasst von CrowdStrike erstellte Angreiferprofile und Feeds mit Gefährdungsindikatoren

FALCON X RECON

UNTERSUCHUNG

Sie erhalten Echtzeit-Transparenz über potenzielle Bedrohungen und beschleunigen somit die Ermittlungen zu betrügerischen Angriffen auf Ihre Organisation. Falcon X Recon beendet Mutmaßungen zu möglichen Risiken und flankiert die Abwehr von Sicherheitsvorfällen, indem der nötige Kontext für fundierte und breit angelegte Untersuchungsberichte bereitgestellt wird.

- **Gezielte Bedrohungen identifizieren:** Überwachen Sie Umgebungen im Untergrund auf externe Bedrohungen, ohne komplexe Abfragen erstellen zu müssen. Die benutzerfreundlichen Assistenten von Falcon X Recon arbeiten mit vordefinierten Suchkriterien, wie beispielsweise Markennamen, Namen von Führungskräften, Domänen, Schwachstellen, E-Mail-Adressen usw. Erstellen und speichern Sie Ihre eigenen Überwachungsregeln oder teilen diese mit Ihrem Team, um Rohdaten proaktiv zu sichten.
- **Angreifer entlarven:** Die Ergebnisse von Untersuchungen werden in verständlichen Karten angezeigt. Sie können sich die Originalbeiträge des Bedrohungsakteurs mit zusätzlichem Kontext über den Akteur und die Website anzeigen lassen. Die Ergebnisse werden in der Originalsprache angezeigt, können aber unter Einbindung von Hacker-Slang-Wörterbüchern aus 18 Sprachen übersetzt werden.
- **Untersuchungen anreichern:** Gewinnen Sie ein vollständiges Verständnis der Bedrohung. Mit Universal Search korrelieren Sie die Ergebnisse von Falcon X Recon automatisch mit zusätzlichem Kontext, der aus anderen lizenzierten CrowdStrike Falcon-Modulen stammt. Sie maximieren die Effizienz und Effektivität Ihrer Reaktionen, denn Sie sehen die Beziehungen zwischen digitalen Bedrohungen und Endgeräte-Erkennungen, Hosts, Berichten zu Bedrohungsaufklärung, Schwachstellen usw.

BENACHRICHTIGUNG

Optimieren Sie den Workflow aus Untersuchungen und Reaktionsmaßnahmen anhand von Echtzeit-Benachrichtigungen, sobald potenzielle Bedrohungen identifiziert werden. So stellen Sie sicher, dass die für die Selektierung und Reaktion verantwortlichen Benutzer die benötigten Details sofort zur Hand haben.

- **Alarme priorisieren:** Legen Sie die Priorität des Alarms anhand der Kritikalität der externen Bedrohung fest. Hierzu können Sie auf Anhieb von Benachrichtigung zu den Alarmdetails wechseln.
- **Vollständige administrative Kontrolle:** Legen Sie fest, wie und wie häufig die Teammitglieder benachrichtigt werden. So kann die Benachrichtigung sofort oder nach einem Zeitplan erfolgen, beispielsweise täglich oder wöchentlich. Sie können die Benachrichtigungen ein- oder ausschalten, ohne dass davon die zugrunde liegende Überwachungsregel betroffen ist.
- **Das richtige Team informieren:** Mehr als nur Cybersicherheit – digitale Bedrohungen gefährden die Marke, den Ruf und die Sicherheit der Mitarbeiter einer Organisation. Mit Falcon X Recon können Sie auch andere Abteilungen außerhalb der Cybersicherheit schützen, wie beispielsweise Marketing, Recht, Personalwesen und Innenrevision.

EDITIONEN

Falcon X Recon ist in zwei Editionen erhältlich:

- **Falcon X Recon Express:** Für kleine und mittlere Unternehmen. Damit lassen sich auf Anhieb die verborgenen Bereiche im Internet untersuchen.
- **Falcon X Recon Enterprise:** Beinhaltet den gesamten Leistungsumfang von Express, plus:
  - Dynamische Ad-hoc-Suchfunktion für neuartige Untersuchungen
  - BIN-Codes von Kredit-/Bankkarten
  - CrowdStrike® Intelligence Actor Profiles und Feed mit Gefährdungsindikatoren

Testen Sie jetzt kostenlos den Virenschutz der neuesten Generation

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

AUFKLÄRUNG DIGITALER RISIKEN

Schutz der eigenen Marke: CrowdStrike Falcon X Recon erkennt betrügerische Interaktionen in Bezug auf Ihre Marke, wie beispielsweise gefälschte Social-Media-Konten, Domains und mobile Apps.

Aufdeckung von Datenlecks: CrowdStrike Falcon X Recon erkennt kompromittierte Anmeldeinformationen und den Diebstahl von sensiblen Daten, IP- und Kreditkarteninformationen aus Datenlecks im öffentlichen Web sowie im Deep Web und Darknet.

Überwachung der Lieferkette: CrowdStrike Falcon X Recon hilft bei der Identifizierung von Bedrohungen Ihrer Lieferanten durch Entlarven von Gerüchten, Phishing-Kampagnen, gefälschten Websites usw.

Schutz von Führungskräften: CrowdStrike Falcon X Recon überwacht Bedrohungen, Identitätsmissbrauch und Phishing-Versuche gegen VIPs und Führungskräfte.

ÜBER CROWDSTRIKE

CrowdStrike, 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, Cloudbasierte, schlanke Agentenarchitektur, die von künstlicher Intelligenz(KI) unterstützt wird und unternehmensweit für Schutz und Transparenz in Echtzeit sorgt. 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 5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cybersicherheit.