CROWDSTRIKE

CROWDSTRIKE FALCON SANDBOX MALWARE-ANALYSE

Die weltweit leistungsstärkste Malware-Sandbox

VOLLSTÄNDIGER EINBLICK IN NEUARTIGE UND UNBEKANNTE BEDROHUNGEN

Wenn ein Unternehmen oder eine Institution Opfer eines Cyberangriffs wird, muss die Absicht der Angreifer unverzüglich geklärt werden. Hierzu müssen Sie Arbeitsweise und Aktivitäten der Malware schnell ermitteln. Nur so können Sie mögliche Schäden begrenzen und sich vor weiteren Angriffen schützen. Doch die Malware-Analyse dauert heute in der Regel viel zu lange und liefert oft unvollständige Details über die Bedrohung. Folglich können Sicherheitsteams den Ergebnissen kaum trauen und müssen ständig weitere Analysen zur Absicherung durchführen. Zu allem Überfluss werden Angreifer immer geschickter und entwickeln ihre Malware ständig mit dem Ziel weiter, blinde Flecken in gängigen Tools und Techniken zur Malware-Analyse zu finden.

CrowdStrike® Falcon® Sandbox™ bezwingt selbst die gefährlichste Malware. Denn die Software wird im Kernel ausgeführt und nutzt ausgeklügelte Sandbox-Techniken. Das macht Falcon Sandbox nahezu unauffindbar. Die Lösung deckt die modernsten zielgerichteten Angriffe auf und übertrifft die übliche statische und dynamische Dateianalyse zur Überwachung aller bösartigen Verhaltensweisen und Systeminteraktionen. Damit liefert Falcon Sandbox den branchenweit umfangreichsten Satz an Gefährdungsindikatoren (Indicators of Compromise / IOC).

Falcon Sandbox spart nicht nur wertvolle Zeit. Die Sicherheitsteams arbeiten auch einfach effektiver – dank leicht verständlicher Berichte, fundierter Gefährdungsindikatoren und einer nahtlosen Integration. Die Malware-Analyseberichte von CrowdStrike geben praktische Hilfestellungen zur Priorisierung und Reaktion auf Bedrohungen. Gleichzeitig sind die forensischen Teams damit in der Lage, sich detailliert mit Speicheraufzeichnungen und Stack-Traces zu befassen. Die API zur Falcon Sandbox und vorkonfigurierte Integrationen ermöglichen eine einfache Orchestrierung zwischen bestehenden Sicherheitslösungen.

WESENTLICHE VORTEILE

- Detaillierter Einblick in alle Datei-, Netzwerk- und Speicheraktivitäten
- Führende Anti-VM-Erkennungstechnologie
- Intuitive Berichte mit forensischen Daten nach Bedarf
- Unterstützung des ATT&CK™- Framework von Mitre
- Orchestrierung von Workflows mit einer umfangreichen API und vorgefertigten Integrationen

WICHTIGE PRODUKTMERKMALE

UNBEKANNTE BEDROHUNGEN ERKENNEN

- **Hybride Analyse:** Hier werden Laufzeitdaten, statische Analyse und Speicherauszugsanalyse so kombiniert, dass alle denkbaren Ausführungswege auch der gefährlichsten Malware extrahiert werden. In Kombination mit einer umfangreichen Analyse vor und nach der Ausführung legt Falcon Sandbox mehr Gefährdungsindikatoren offen als jede andere konkurrierende Sandbox-Lösung. Alle aus der Hybrid-Analysis-Engine extrahierten Daten werden automatisch verarbeitet und in die Falcon Sandbox-Berichte integriert.

- **Anti-Evasion-Technologie:** Falcon Sandbox ist mit einer hochmodernen Anti-Sandbox-Erkennungstechnologie ausgestattet. CrowdStrike verwendet keine Agents, da diese von einer Malware leicht identifiziert werden könnten. Jedes Release wird kontinuierlich getestet, um sicherzustellen, dass Falcon Sandbox selbst unter Verwendung der ausgefeiltesten Sandbox-Erkennungstechniken praktisch nicht ermittelbar ist.

- **Anpassung an die Umgebung:** Übernehmen Sie die Kontrolle darüber, wie Malware unschädlich gemacht werden soll. Konfigurieren Sie allgemeine Einstellungen, mit denen Malware versucht, sich vor der Sandbox-Analyse zu verstecken, wie Datum/Uhrzeit, Umgebungsvariablen, Benutzerverhalten und mehr.

VOLLSTÄNDIGE TRANSPARENZ ERREICHEN

- **Analysberichte:** Leichtverständliche Berichte tragen dazu bei, dass jeder Analyst auf jeder Ebene seine Aufgaben effektiver wahrnehmen kann. Die Analyse ist mehrschichtig aufgebaut. Sie leistet den Sicherheitsteams praktische Hilfestellung für die Priorisierung und Reaktion auf Bedrohungen. Die Incident Response Teams können gezielt nach Bedrohungen suchen. Die forensischen Teams können Speicheraufzeichnungen und Stack Traces tiefgreifend analysieren.

- **Umfassende Dateiunterstützung:** Falcon Sandbox unterstützt die Betriebssysteme Windows, Linux und Android (nur statische Analyse). Darüber hinaus analysiert Falcon Sandbox über 40 verschiedene Dateitypen, darunter eine Vielzahl von ausführbaren Dateien, Dokumenten- und Bildformaten sowie Skript- und Archivdateien.

- **Malware-Suche:** Falcon Sandbox durchsucht die branchenweit größte Malware-Suchmaschine nach verwandten Mustern und weitet die Analyse innerhalb von Sekunden auf alle Dateien aus. Diese einzigartige Funktion verhilft Analysten zu einem besseren Verständnis des Angriffs und zu einem größeren Satz an Gefährdungsindikatoren, die zum besseren Schutz des Unternehmens verwendbar sind.

SCHNELLER REAGIEREN

- **Unverzügliche Erkennung:** Falcon Sandbox stellt Zusammenfassungen zur Bedrohungsbeurteilung und Reaktion auf Vorfälle mit dem Ziel bereit, Malware sofort zu erkennen und zu beseitigen. Darüber hinaus werden die Analyseberichte mit Informationen und Gefährdungsindikatoren von CrowdStrike Falcon MalQuery™ und CrowdStrike Falcon Intelligence™ ergänzt und bieten somit den notwendigen Kontext für schnellere und bessere Entscheidungen.

- **Einfache Integration:** Benutzerfreundliche REST-API, vorkonfigurierte Integrationen und Unterstützung von Formaten zum Teilen von Indikatoren, wie STIX, OpenIOC, MAEC, MISP und XML/JSON. So lassen sich die Ergebnisse von Falcon Sandbox über SIEMs, TIPs und Orchestrierungssysteme bereitstellen.

- **Flexible Einsatzszenarien:** Sie haben die Wahl zwischen einer Cloud-Version oder einer lokalen Version von Falcon Sandbox. Die Cloud-Option überzeugt durch sofortige Time-to-Value und geringere Infrastrukturkosten. Die lokale Version ermöglicht es, Muster ausschließlich der eigenen Benutzerumgebung zu sperren und zu verarbeiten. Beide Optionen stellen eine sichere und skalierbare Sandbox-Umgebung bereit.

STELLEN SIE FALCON SANDBOX AUF DIE PROBE

Falcon Sandbox unterstützt die größte Community für die Online-Analyse von Malware. D. h., diese Analyse wird täglich von Zehntausenden von Anwendern im praktischen Einsatz getestet. Probieren Sie Falcon Sandbox kostenlos unter www.hybrid-analysis.com aus. Wenn Sie mit den Ergebnissen zufrieden sind und Falcon Sandbox weiter verwenden möchten, können Sie problemlos auf eine Volllizenz aktualisieren.

Mit der standortgebundenen Lizenz von Falcon Sandbox können Unternehmen und Institutionen ihre Sandbox an ihre jeweiligen Anforderungen anpassen. Für eine gezielte Erkennung von Angriffen importiert Falcon Sandbox sogenannte „golden" Images für virtuelle Maschinen. Diese Images spiegeln das Betriebssystem, die Anwendungen und die Einstellungen der jeweiligen realen Umgebung wider. Darüber hinaus können das Benutzerverhalten emuliert und individuelle Verhaltensindikatoren definiert werden. Die standortgebundene Lizenz lässt sich ohne jegliche Netzwerkverbindung ausführen, sodass auch strengste Datenschutzrichtlinien eingehalten werden.

ÜBER CROWDSTRIKE

CrowdStrike ist der führende Anbieter von cloudbasiertem Endgeräteschutz der neuesten Generation. CrowdStrike hat den Endgeräteschutz revolutioniert. Ein einziger, schlanker Agent vereint nahtlosen Virenschutz der nächsten Generation mit erstklassiger Endgeräteerkennung und Reaktion (EDR), IT-Hygiene und einer verwalteten Bedrohungssuche rund um die Uhr.