Kaspersky Threat Data Feeds

kaspersky bring on the future

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

Cyberangriffe gibt es jeden Tag. Cyberbedrohungen werden immer häufiger, komplexer und schwerer erkennbar. Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger. Angreifer nutzen komplizierte Kill Chains, Kampagnen und individuell angepasste Taktiken, Techniken und Prozeduren (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu unterbrechen oder Ihren Kunden zu schaden. Umfassender Schutz muss über neue Methoden bereitgestellt werden, die auf Bedrohungsinformationen basieren.

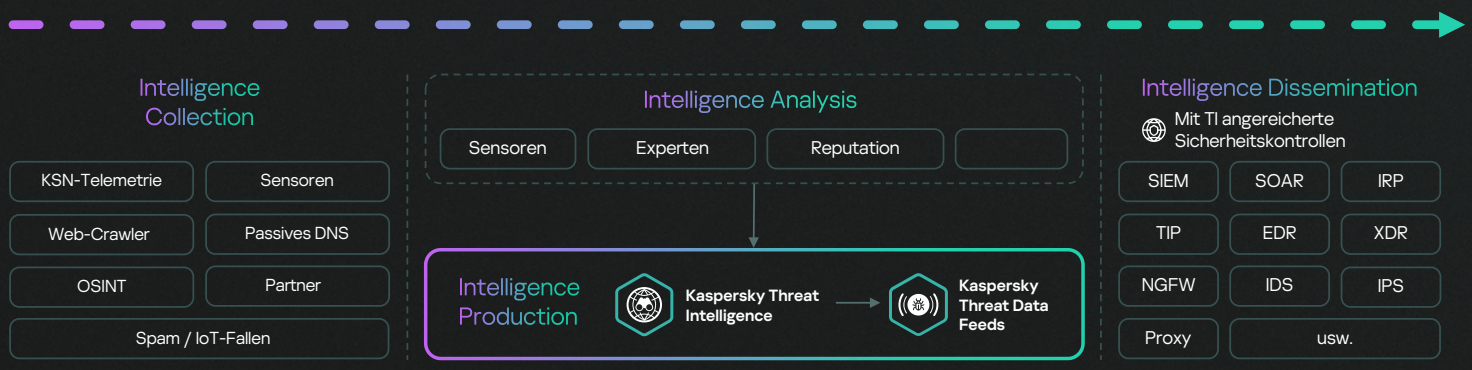
Durch die Integration aktueller Bedrohungsinformationen über verdächtige und gefährliche IP-Adressen, URLs und Datei-Hashes in bestehende Sicherheitssysteme wie SIEM-, SOAR- und Threat Intelligence-Plattformen, können Sicherheitsteams die Ersteinstufung von Warnmeldungen automatisieren. Darüber hinaus bieten sie den für die Ersteinstufung zuständigen Spezialisten genügend Kontext, um sofort zu erkennen, welche Warnmeldungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die Incident Response-Teams weitergeleitet werden müssen.

Kontextdaten

Die Einträge in den von Kaspersky bereitgestellten Feeds sind mit den folgenden Kontextdaten angereichert. So können Sie Bedrohungen schnell überprüfen und priorisieren:

- Bedrohungsnamen
- IP-Adressen und Domain-Namen schädlicher Web-Ressourcen
- Hashes von schädlichen Dateien
- Anfällige und gefährdete Objekte
- Taktiken, Techniken und Prozeduren von Angriffen gemäß der MITRE ATT&CK-Klassifizierung
- Zeitstempel
- Geostandort
- Verbreitung usw.

Funktionsweise



Kaspersky Threat Data Feeds werden von Kaspersky aus einer Vielzahl von äußerst zuverlässigen Quellen zusammengestellt:

Kaspersky SecurityNetwork

Eine hochentwickelte Cloud-Infrastruktur, die anonymisierte Cyber-Bedrohungsdaten von mehr als 400 Millionen freiwilligen Teilnehmern weltweit sammelt und analysiert, um mit Hilfe von Big-Data-Analysen, maschinellem Lernen und menschlichem Fachwissen schnell auf neue Bedrohungen reagieren zu können.

Web-Crawler

Erfassung neuer Malware-Programme und seriöser Stichproben aus einer Vielzahl von Quellen: OSINT, Untersuchungen von Kaspersky-Analysten sowie eigene automatische Verarbeitungs- und Analysesysteme, die URLs aus Malware extrahieren.

BotFarmen

Ein dediziertes Botnet-Forschungsteam extrahiert Bot-Konfigurationen, analysiert ihre Kommunikationsprotokolle durch Reverse Engineering und überwacht Befehle von Kommandozentralen, um wertvolle Informationen über Bedrohungen zu erhalten.

Spam-Fallen

Jedes Jahr blockieren unsere Anti-Phishing-Systeme mehr als 500 Millionen Klicks auf Phishing-Links und mehr als 160 Millionen bösartige E-Mail-Anhänge, aus denen wir zusätzliche Daten zur Anreicherung unserer Informationsquellen gewinnen.

Partner

Wir nehmen an Partnerschaften teil, um Malware Samples mit anderen Anbietern und Cybersicherheitsorganisationen auszutauschen.

Sensoren

Honeypots, Sinkholes und andere Methoden zur Abwehr von ITW-Angriffen. Zum Beispiel IoT-Geräte, anfällige Systeme, Software usw. Kaspersky-Analysten untersuchen Angriffsversuche und Methoden von Angreifern, extrahieren Gefährdungsindikatoren und bringen sie mit anderen Datenquellen in Verbindung.

Passives DNS

Diese Daten werden weltweit von vertrauenswürdigen Dritten wie Hosting-Organisationen und ISPs gesammelt.

OSINT

Daten über Gegner werden automatisch aus öffentlich zugänglichen Quellen bezogen, wie Nachrichtenagenturen, sozialen Medien, öffentlichen Berichten, dem Darknet usw. Anhand dieser Quellen suchen wir nach neuen Beispielen für schädliche Daten, indem wir die Infrastruktur des Gegners erforschen und unsere Wissensbasis kontinuierlich erweitern.

Jeder erkannte Indikator wird in einem mehrstufigen Prozess genau untersucht. Automatisierte Vertrauens- und Reputationstechnologien sowie lernfähige Systeme, die anhand von Hunderten Millionen vertrauenswürdiger und schädlicher Dateien trainiert wurden, arbeiten daran, Fehlalarme (False Positives) herauszufiltern. Jeder Indikator wird außerdem mehrmals in Sandboxes analysiert, in denen Dutzende zusätzlicher Attribute wie TTPs, Netzwerkverhalten, Betriebssystemverhalten und eine Vielzahl anderer Beziehungen extrahiert werden.

All dies macht Kaspersky Threat Intelligence zu einer leistungsstarken Quelle taktischer Informationen, die Ihre Bedrohungsüberwachung stärken und Angriffe auf Ihr Unternehmen frühzeitig erkennen kann.

Wichtigste Vorteile

Alle Feeds werden automatisch und in Echtzeit auf der Grundlage von Erkenntnissen aus der ganzen Welt generiert. Sie zeichnen sich durch hohe Erkennungsraten und Präzision aus.

Dank zusätzlicher Dokumentation, Beispielen, einem persönlichen Technical Account Manager und dem technischen Support von Kaspersky ist die Integration schnell und einfach.

Einfache Verteilungsformate (JSON, CSV, OpenIOC, STIX) über HTTPS, TAXII oder Ad-hoc-Bereitstellungsmechanismen ermöglichen eine unkomplizierte Integration der Daten in Sicherheitslösungen. Führende SIEM- und TI-Plattformen werden vollständig unterstützt.

Data Feeds mit vielen False Positives sind wertlos. Deshalb werden die Feeds vor ihrer Veröffentlichung umfassend getestet und gefiltert, um zu gewährleisten, dass nur vollständig überprüfte Daten bereitgestellt werden.

Hunderte von Experten tragen gemeinsam zur Bereitstellung dieser Feeds bei. Dazu gehören Sicherheitsanalysten aus der ganzen Welt sowie weltweit anerkannte Sicherheitsexperten aus unseren GREAT- und F&E-Teams. Sicherheitsbeauftragte erhalten kritische Informationen und Warnungen, die aus Daten höchster Qualität generiert werden, ohne dass die Gefahr besteht, von überflüssigen Indikatoren und Warnungen überflutet zu werden.

Sämtliche Feeds werden von einer hochgradig fehlertoleranten Infrastruktur generiert und beobachtet, die eine kontinuierliche Verfügbarkeit gewährleistet.

Vorteile

1. Verstärken Sie Ihre Abwehrlösungen, einschließlich SIEM, Firewalls, NGFW IPS/IDS, Sicherheitsproxys, DNS-Lösungen und APT-Abwehr, mit regelmäßig aktualisierten Gefährdungsindikatoren (Indicators of Compromise, IoCs) und praktisch verwertbarem Kontext. So erhalten Sie Einblicke in Cyberangriffe und können Zweck, Fähigkeiten und Ziele der Angreifer erkennen.

2. Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen, indem Sie die Ersteinstufung automatisieren. So erhalten Sicherheitsanalysten ausreichend Kontext, um sofort zu erkennen, welche Warnungen genauer untersucht oder zur weiteren Prüfung und Bearbeitung an die Incident Response-Teams weitergeleitet werden müssen.

3. Verhindern Sie, dass sensible Daten und geistiges Eigentum von infizierten Computern nach außen gelangen. Dank der schnellen Erkennung infizierter Assets können Sie den Ruf Ihres Unternehmens schützen, Ihren Wettbewerbsvorteil aufrechterhalten und Geschäftschancen sichern.

4. Bieten Sie Ihren Kunden branchenführende Bedrohungsinformationen als Premium Service und erweitern Sie so Ihr Business als MSSP.

5. Als CERT können Sie Ihre Fähigkeiten rund um die Erkennung und Identifizierung von Bedrohungen verbessern und erweitern.

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence bietet Zugang zu einer Vielzahl von Informationen, die von unseren weltweit anerkannten Analysten und Forschern zusammengestellt werden. Diese Daten helfen Ihrem Unternehmen, den Cyberbedrohungen von heute wirksam entgegenzutreten.

Unser Unternehmen verfügt über umfassendes Wissen, langjährige Erfahrung in der Erforschung von Cyberbedrohungen und einzigartige Einblicke in alle Bereiche der Cybersicherheit, die uns aktuelle taktische, operative und strategische Bedrohungsinformationen liefern. All dies macht uns zu einem verlässlichen Partner für Strafverfolgungsbehörden und Regierungsorganisationen weltweit, darunter Interpol und verschiedene CERT-Einheiten. Und all dieses Wissen steht auch Ihnen über das Kaspersky Threat Intelligence Portal **zur Verfügung – als Quelle für relevante und umsetzbare Informationen.**

Kaspersky Threat Intelligence

Mehr erfahren

www.kaspersky.de

© 2024 AO Kaspersky Lab.
Eingetragene Marken und Servicemarken sind Eigentum ihrer jeweiligen Rechtsinhaber.

#kaspersky
#bringonthefuture