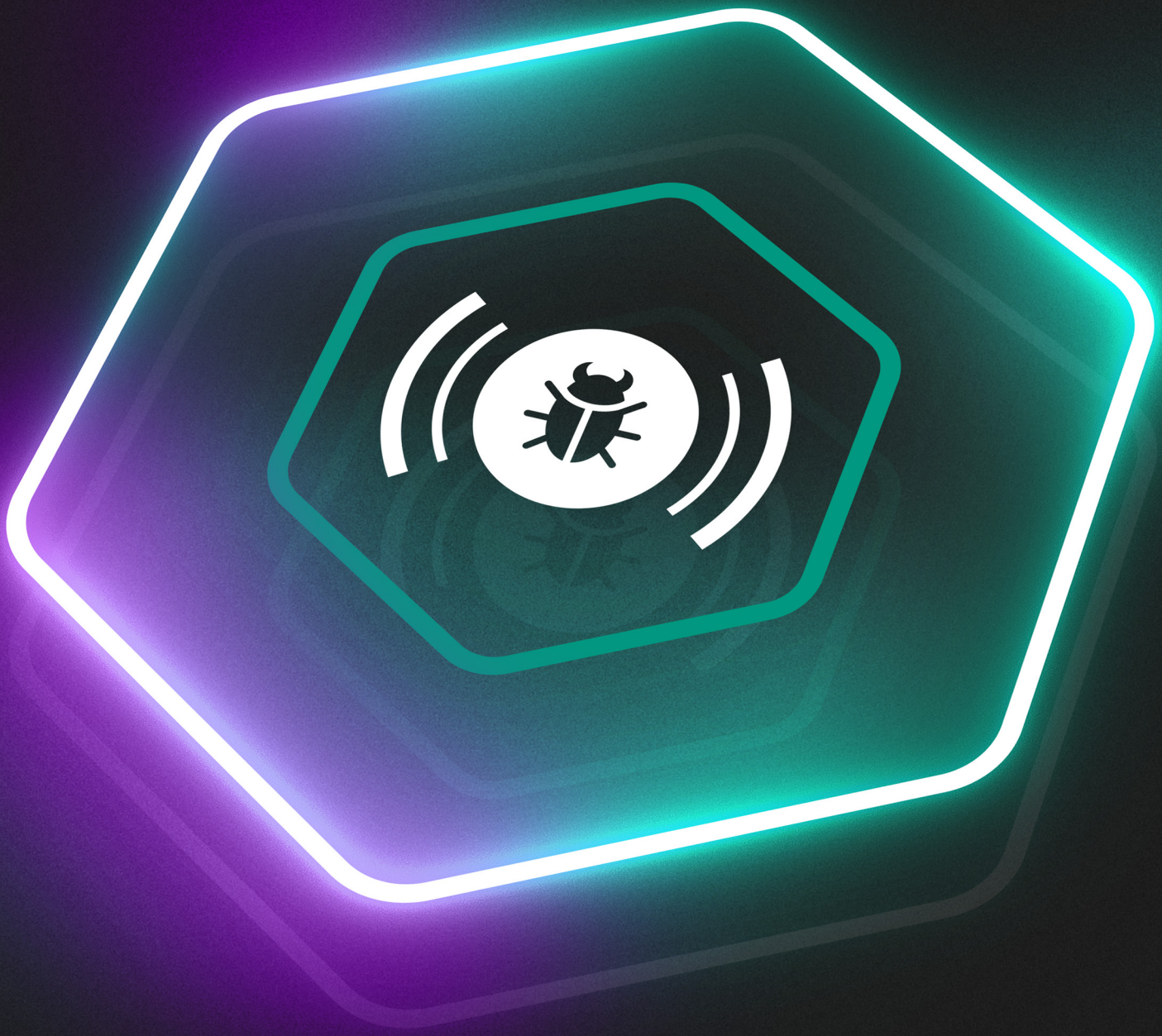

Kaspersky Threat Data Feeds

kaspersky BRING ON THE FUTURE

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 angepasste Taktiken, Techniken und Abläufe (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 Integration topaktueller Feeds mit Bedrohungsinformationen zu verdächtigen und gefährlichen IPs, URLs und Datei-Hashes in bestehende Sicherheitssysteme, wie z. B. SIEM-, SOAR- und Threat Intelligence-Plattformen, können Sicherheitsteams die Ersteinstufung von Warnmeldungen automatisieren. Außerdem bieten sie den Spezialisten für die Ersteinstufung so ausreichend Kontext, um umgehend ermitteln zu können, welche Warnungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die Teams für die Vorfallsreaktion übergeben werden müssen.

- IP-REPUTATION-FEED
- HASH-FEED (WIN/*nix/ MacOS/AndroidOS/iOS)
- URL-FEEDS (Malicious, Phishing und C&C)
- RANSOMWARE-URL-FEED
- APT-IOC-FEEDS
- SCHWACHSTELLEN-FEED
- PASSIVE DNS (pDNS)-FEED
- IoT-URL-FEED
- ALLOWLISTING-FEED
- ICS-HASH-FEED
- UND MEHR

Kontextdaten

Jeder Datensatz in jedem Data Feed wird mit praktisch umsetzbarem Kontext angereichert (Bezeichnungen von Bedrohungen, Zeitstempel, Geolokalisierungsdaten, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.). Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die weitere Analyse und vielfältige Nutzung der Daten. Wenn die Daten in einen Kontext gesetzt werden, liefern sie schneller Antworten auf die Fragen „Wer?“, „Was?“, „Wo?“ und „Wann?“. Außerdem geben sie Aufschluss über Ihre Gegner, sodass Sie schnell Entscheidungen und Maßnahmen treffen können.

Wichtigste Vorteile

Die Data Feeds werden automatisch in Echtzeit generiert – basierend auf den weltweit vom Kaspersky Security Network erfassten Daten, die einen Einblick in einen signifikanten Anteil des gesamten Internetdatenverkehrs und alle möglichen Datentypen von Millionen von Endbenutzern in mehr als 213 Ländern gewähren. So werden hohe Erkennungsraten und Genauigkeit garantiert.

Einfache Implementierung. Dank ergänzender Dokumentation, Beispielen, einem persönlichen technischen Account Manager sowie dem technischen Support von Kaspersky geht die Integration schnell und einfach vonstatten.

Hunderte von Experten, darunter Sicherheitsanalysten aus der ganzen Welt, weltweit anerkannte Sicherheitsexperten aus unserem GReAT- und Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung dieser Feeds bei. Sicherheitsbeauftragte erhalten kritische, aus zuverlässigen Daten generierte Informationen und Benachrichtigungen, ohne Gefahr zu laufen, von unnötigen Anzeigen und Warnungen überflutet zu werden.

Erfassung und Verarbeitung

Unsere Data Feeds werden aus zusammengeführten, heterogenen und äußerst zuverlässigen Quellen bezogen, darunter das Kaspersky Security Network, unsere eigenen Webcrawler, unser Service zur Botnet-Überwachung (Überwachung von Botnets und ihrer Ziele und Aktivitäten rund um die Uhr, das ganze Jahr) sowie Spam-Fallen, Forschungsteams und Partner.

Dann werden sämtliche zusammengefassten Daten in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren präzisiert, z. B. durch statistische Kriterien, Sandboxes, heuristische Engines, Similaritätstools, Erstellung von Verhaltensprofilen, die Validierung durch Analysten und die Verifizierung anhand von Whitelists.

Einfache Verteilungsformate (JSON, CSV, OpenIOC, STIX) über HTTPS, TAXII oder Ad-hoc-Bereitstellungsmechanismen ermöglichen die einfache Integration der Daten in Sicherheitslösungen.

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

Sämtliche Feeds werden über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die dauerhafte Verfügbarkeit gewährleistet.

Vorteile

Verstärken Sie Ihre Lösungen zur Netzwerkverteidigung, einschließlich SIEMs, Firewalls, IPS/IDS, Sicherheits-Proxys, DNS-Lösungen und APT-Abwehr, mit regelmäßig aktualisierten Gefährdungsindikatoren (Indicators of Compromise, IOCs) und praktisch umsetzbarem Kontext. So erhalten Sie Einblicke in Cyberangriffe und können den Zweck, die Funktionen und die Ziele der Angreifer ermitteln. Führende SIEM-Systeme (einschließlich HP ArcSight, IBM QRadar, Splunk usw.) und TI-Plattformen werden vollständig unterstützt.

Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen, indem Sie die Ersteinstufung automatisieren. Außerdem bieten Sie den Sicherheitsanalysten so ausreichend Kontext, um umgehend ermitteln zu können, welche Warnungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die Teams für die Vorfallsreaktion übergeben werden müssen.

Verhindern Sie die Extraktion vertraulicher Assets und geistigen Eigentums über infizierte Geräte an Personen außerhalb des Unternehmens. Dank der schnellen Erkennung infizierter Assets können Sie den Ruf Ihres Unternehmens schützen, Ihren Wettbewerbsvorteil aufrechterhalten und Geschäftschancen sichern.

Erweitern Sie als MSSP Ihr Business, indem Sie Ihren Kunden branchenführende Bedrohungsinformationen als Premiumservice bieten. Als CERT, können Sie Ihre Fähigkeiten rund um die Erkennung und Identifizierung von Bedrohungen verbessern und erweitern.

Kaspersky Threat Data Feeds

Weitere informationen

www.kaspersky.de