Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

Herausforderung

Die Überwachung, Analyse, Interpretation und Abwehr der sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist mit immensem Aufwand verbunden. Unternehmen aus allen Branchen verfügen oft nicht über die aktuellen und relevanten Daten, die für einen effektiven Umgang mit den Risiken der IT-Sicherheitsbedrohungen erforderlich sind.

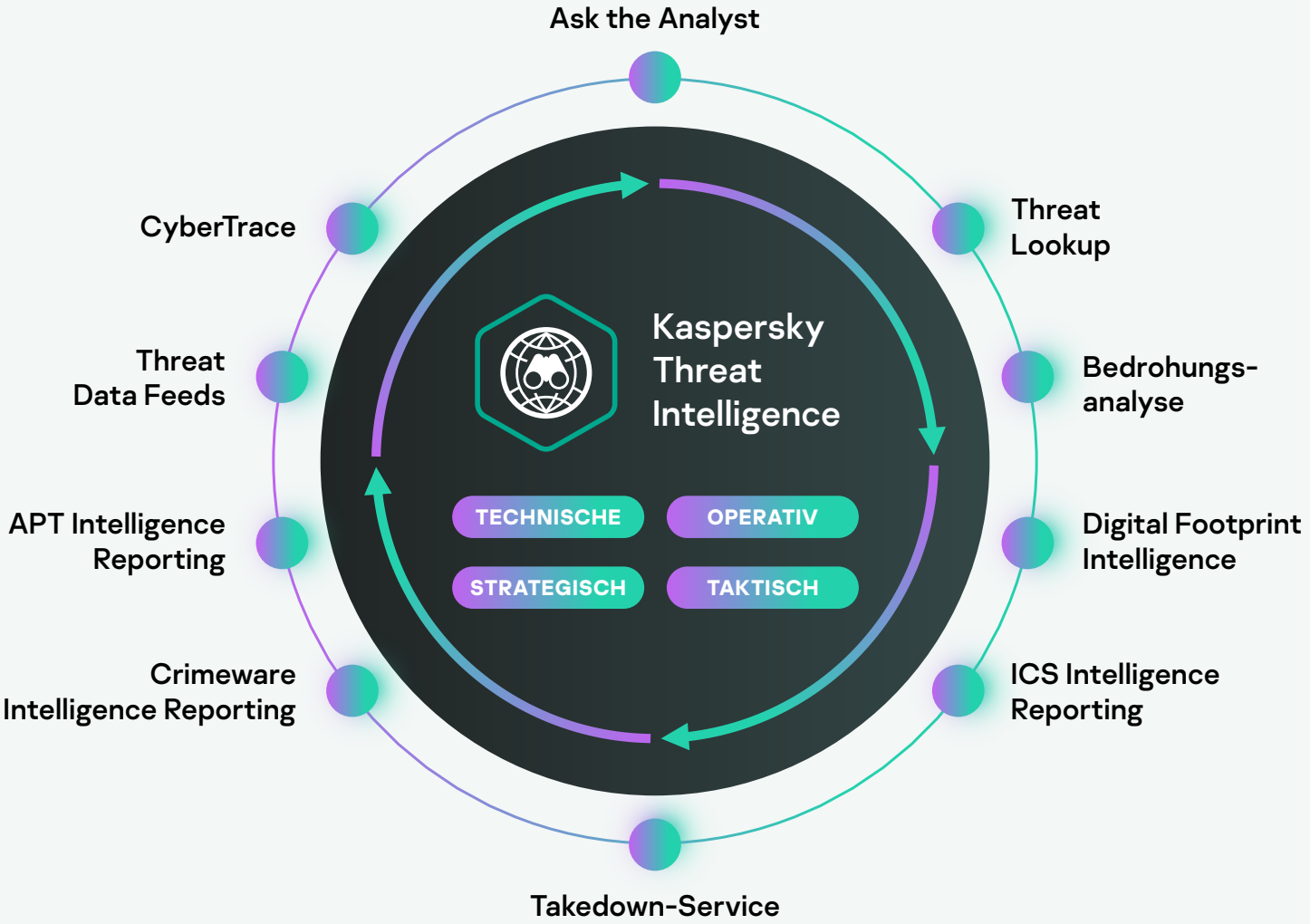
Kaspersky Threat Intelligence

Die Threat Intelligence von Kaspersky bieten Ihnen Zugriff auf alle Informationen, die Sie zur Abwehr von Cyberbedrohungen benötigen. Sie werden von unserem weltweit führenden Team aus Forschern und Analysten zur Verfügung gestellt.

Wissen, Erfahrung und umfassende Erkenntnisse über praktisch jeden Aspekt der Cybersicherheit haben Kaspersky zum vertrauenswürdigen Partner angesehener internationaler Strafverfolgungs- und Regierungsbehörden, darunter Interpol und CERTs, gemacht. Mit Kaspersky Threat Intelligence erhalten Sie einen direkten Zugang zu technischer, taktischer, operativer und strategischer Threat Intelligence.

Das Kaspersky Threat Intelligence-Portfolio beinhaltet:

Threat Data Feeds, CyberTrace (eine Threat Intelligence-Plattform), Threat Lookup, Threat Analysis (Cloud Sandbox und Cloud Threat Attribution Engine), eine Reihe an Threat Intelligence-Berichtsoptionen und Services, die bei Bedarf mit Fachwissen im Bereich Threat Intelligence beratend agieren.



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

Kaspersky Threat Data Feeds

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.

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.

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.

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

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.

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 CyberTrace

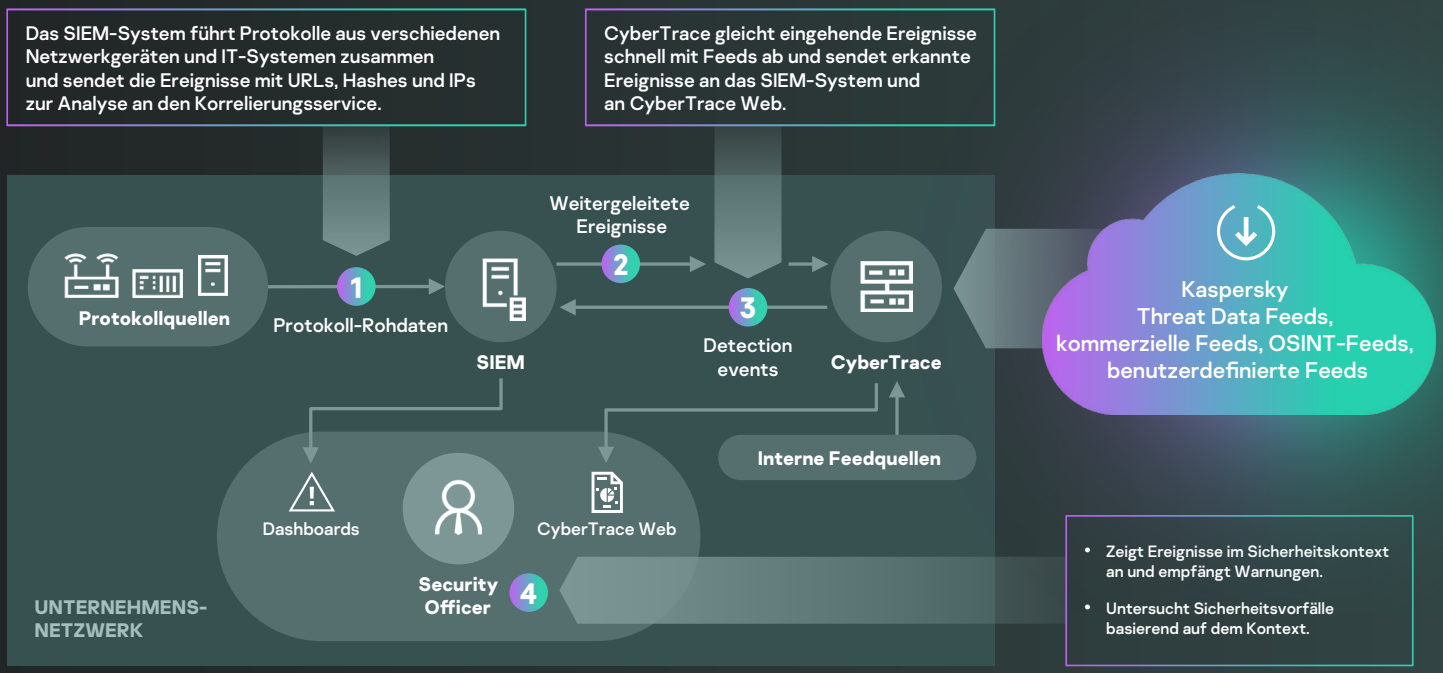
Durch Integration topaktueller maschinenlesbarer Bedrohungsinformationen in bestehende Systeme, wie z.B. SIEM-Systeme, können Security Operation Center die Ersteinstufung automatisieren. Außerdem bieten Sie den Sicherheitsanalysten so ausreichend Kontext, um umgehend ermitteln zu können, welche Warnungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die Teams für die Vorfallsreaktion übergeben werden müssen. Wegen der steigenden Anzahl von Threat Intelligence Feeds und verfügbaren Bedrohungsinformationen können Unternehmen aber nur schwer herausfinden, welche Informationen wirklich relevant sind. Bedrohungsinformationen werden in verschiedenen Formaten bereitgestellt und beinhalten viele Gefährdungsindikatoren (Indicators of Compromise, IOCs), die für SIEM-Systeme oder Sicherheitskontrollen nur schwer zu verarbeiten sind.

Kaspersky CyberTrace ist eine Threat Intelligence-Plattform zur Zusammenführung von Bedrohungsinformationen, die die nahtlose Integration von Threat Intelligence Feeds in SIEM-Lösungen ermöglicht. So können Analysten die Bedrohungsinformationen in ihren bestehenden Sicherheitsabläufen nutzen. Die Lösung kann jeden Threat Intelligence Feed (von Kaspersky Lab, anderen Anbietern, OSINT oder die Feeds Ihrer eigenen Kunden) im JSON-, STIX-, XML- oder CSV-Format integrieren und unterstützt zahlreiche SIEM-Lösungen und Protokollquellen ohne Konfigurationsaufwand.

Kaspersky CyberTrace bietet verschiedene Tools, um Bedrohungsinformationen effizient zu nutzen:

- Eine Datenbank mit Indikatoren und Volltextsuche sowie die Möglichkeit zur Nutzung erweiterter Suchabfragen ermöglichen komplexe Abfragen über alle Indikatorfelder hinweg, einschließlich der Kontextfelder.
- Seiten mit detaillierten Informationen zu jedem Indikator ermöglichen eine noch tiefere Analyse. Auf jeder Seite werden sämtliche Informationen zu einem Indikator aus allen Threat Intelligence-Quellen (ohne Dopplung) dargestellt. Analysten können die Bedrohungen in den Kommentaren diskutieren und interne Analysen zum Indikator hinzufügen.
- Mit einem Research Graph können Sie in CyberTrace gespeicherte Daten und erkannte Ereignisse visuell untersuchen und Gemeinsamkeiten von Bedrohungen erkennen.
- Mittels einer Exportfunktion lassen sich Indikatorensätze in Sicherheitssysteme wie Richtlinienlisten (Blocklisten) eintragen. Außerdem können die Daten zwischen Kaspersky CyberTrace-Instanzen oder mit anderen TI-Plattformen geteilt werden.
- Versehen Sie Gefährdungsindikatoren (IoCs) mit Tags, um ihre Verwaltung zu vereinfachen. Sie können einen beliebigen Tag erstellen, seine Gewichtung (Wichtigkeit) festlegen und dann IoCs manuell mit dem Tag versehen. Sie können IoCs auch basierend auf diesen Tags und deren Gewichtung sortieren und filtern.
- Mithilfe der Korrelationsfunktion zu früheren Verläufen (Retroscan) können Sie beobachtete Phänomene aus zuvor geprüften Ereignissen anhand der neuesten Feeds analysieren, um bisher nicht erkannte Bedrohungen aufzuspüren.
- Ein Filter sendet erkannte Ereignisse an SIEM-Lösungen und entlastet nicht nur diese sondern auch die Analysten.
- Mehrmandantenfähigkeit hilft MSSPs und bei Anwendungsfällen in großen Unternehmen.
- Anhand von Nutzungsstatistiken zur Messung der Effektivität integrierter Feeds sowie einer Feed-Überschneidungsmatrix kann man entscheiden, welche Threat Intelligence-Quellen am zuverlässigsten sind.
- Mit der HTTP Rest-API können Sie Bedrohungsdaten abrufen und verwalten.

Das Tool nutzt einen internen Prozess zum Abgleich und zur Analyse der eingehenden Daten, der die Arbeitslast der SIEM-Systeme deutlich reduziert. Kaspersky CyberTrace analysiert eingehende Protokolle und Ereignisse, gleicht die entsprechenden Daten schnell mit Feeds ab und erstellt bei Bedrohungen eigene Sicherheitswarnungen. Die übergeordnete Architektur der Lösungsintegration wird in der unten stehenden Abbildung dargestellt:



Kaspersky CyberTrace und die Kaspersky Threat Data Feeds bieten Sicherheitsanalysten folgende Vorteile:

- Effektive Analyse und Priorisierung von Unmengen an Sicherheitswarnungen
- Verbesserung und Beschleunigung der Auswahl und Erstreaktion
- Umgehende Erkennung kritischer Warnungen und fundiertere Entscheidungen hinsichtlich der Eskalation von Warnungen an Vorfallsreaktionsteams
- Aufbau einer vorausschauenden informationsbasierten Abwehr

Kaspersky Threat Lookup

Cyberkriminalität entwickelt sich mit dem technologischen Fortschritt und kennt kaum noch Grenzen. Wir beobachten Cyberangriffe, die immer raffinierter werden, und Cyberkriminelle, die für ihre Angriffe zunehmend Ressourcen aus dem Dark Web einsetzen. Cyberbedrohungen werden immer häufiger, komplexer und schwerer erkennbar. Zuverlässige Abwehrmaßnahmen zu finden, wird deshalb auch zunehmend schwieriger. Die Angreifer nutzen dabei komplizierte „Kill Chains“ und individuelle Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu stören, Ihre Vermögenswerte zu entwenden oder Ihren Kunden zu schaden.

Kaspersky Threat Lookup bietet das gesamte Wissen von Kaspersky über Cyberbedrohungen und ihre Interdependenzen in einem einzigen, leistungsstarken Webservice. Das Ziel ist es, Sie und Ihre Sicherheitsteams mit so vielen Informationen wie möglich zu versorgen, damit Cyberangriffe schon im Vorfeld abgewendet werden können. Die Plattform ruft die neuesten detaillierten Bedrohungsdaten ab zu URLs, Domänen, IP-Adressen, Hash-Werten, Namen von Bedrohungen, statistische/Verhaltensdaten, WHOIS/DNS-Daten, Dateiattribute, geographische Standortdaten, Downloadketten, Zeitstempel etc. Im Ergebnis erhalten Sie eine weltweite Übersicht über neue und sich entwickelnde Bedrohungen, damit Sie Ihre Organisation schützen und die Vorfallsreaktion beschleunigen können.

Wichtigste Vorteile

Vertrauenswürdige Informationen: Ein zentraler Bestandteil von Kaspersky Threat Lookup ist die Zuverlässigkeit unserer Bedrohungsinformationen, die durch einen praktisch umsetzbaren Kontext ergänzt werden. Kaspersky-Produkte zählen zu den führenden bei Anti-Malware-Tests[1]. Die hohen Erkennungsraten in Kombination mit False Positives, die praktisch gegen Null gehen, zeigen die Zuverlässigkeit unserer Sicherheitsinformationen.

Threat Hunting: Gehen Sie bei der Prävention, Erkennung und Reaktion auf Angriffe proaktiv vor, um deren Auswirkung und Häufigkeit zu minimieren. Erkennen und beenden Sie Angriffe so früh wie möglich. Je früher Sie eine Bedrohung entdecken, umso weniger Schaden entsteht, umso schneller können Korrekturmaßnahmen stattfinden und umso eher kann sich der Netzwerkbetrieb normalisieren.

Vorfallsuntersuchung: Ein Research Graph sorgt für eine effektivere Vorfallsuntersuchung, da sie Daten und erkannte Ereignisse visuell in Threat Lookup untersuchen können. Er bietet eine grafische Darstellung der Interdependenzen zwischen URLs, Domäen, IPs, Dateien und anderen Kontexten, damit Sie den Umfang eines Vorfalls besser verstehen und die Ursache identifizieren können.

Master-Suche: Suchen Sie nach Informationen in allen aktiven Threat Intelligence-Produkten und externen Quellen (einschließlich OSINT IoCs, Dark Web und öffentliches Internet) über eine einzige, leistungsstarke Oberfläche.

Benutzerfreundliche Weboberfläche oder RESTful API: Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über eine einfache RESTful-API zugreifen.

Breite Palette an Exportformaten: Exportieren Sie die Gefährdungsindikatoren (Indicators of Compromise, IOCs) oder den praktisch umsetzbaren Kontext in gängige, strukturiertere und computerlesbare Formate, z. B. STIX, OpenIOC, JSON, Yara, Snort oder sogar CSV. So können Sie alle Vorteile von Threat Intelligence nutzen, betriebliche Abläufe automatisieren oder eine Integration in bestehende Sicherheitskontrollen, z. B. SIEMs ermöglichen.

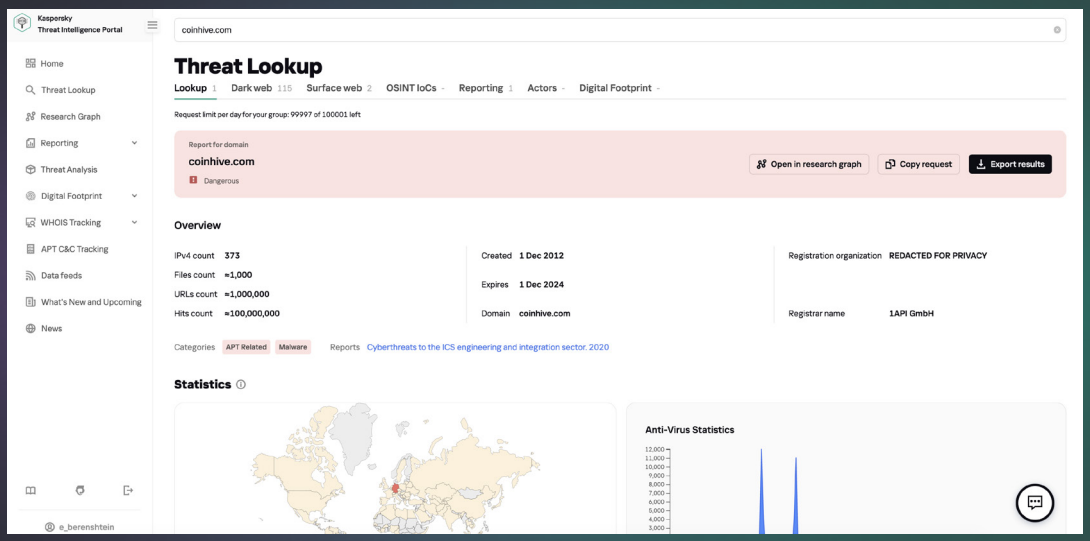
Vorteile

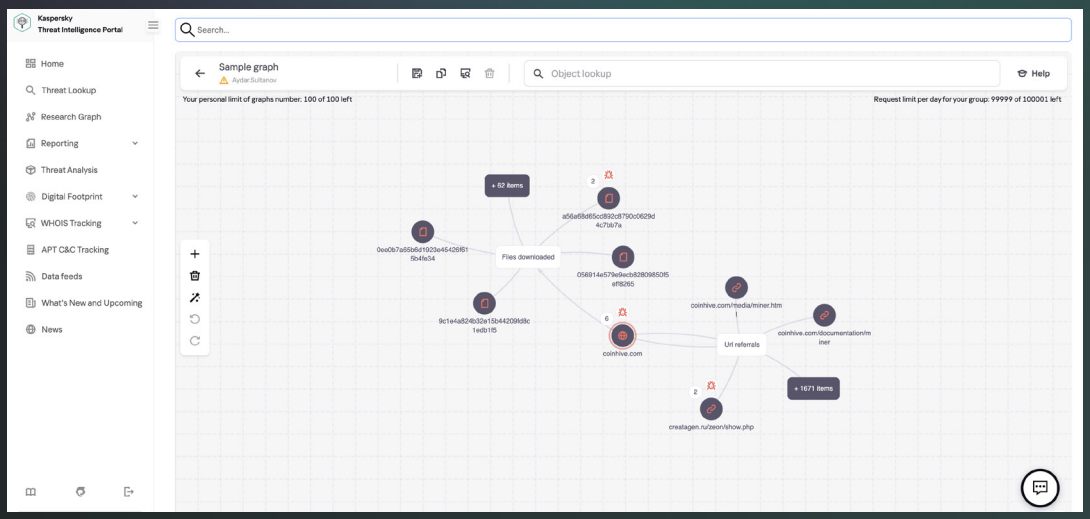
Führen Sie detaillierte Suchen innerhalb der Bedrohungsindikatoren anhand hochzuverlässiger Bedrohungskontexte durch, um Angriffe zu priorisieren und sich auf die Abwehr derjenigen Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen.

Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen.

Beschleunigen Sie Ihre Vorfallsreaktion sowie Ihre Threat Hunting-Funktionen, um die „Kill Chains“ zu durchbrechen, bevor kritische System und Daten in Mitleidenschaft gezogen werden.

[1] kaspersky.com/top3





Jetzt können Sie

Suchen Sie über eine webbasierte Benutzeroberfläche oder die RESTful-API nach Bedrohungsindikatoren.

Überprüfen Sie zusätzliche Details, darunter Zertifikate, häufig genutzte Bezeichnungen, Dateipfade oder zugehörige URLs, um neue verdächtige Objekte zu ermitteln.

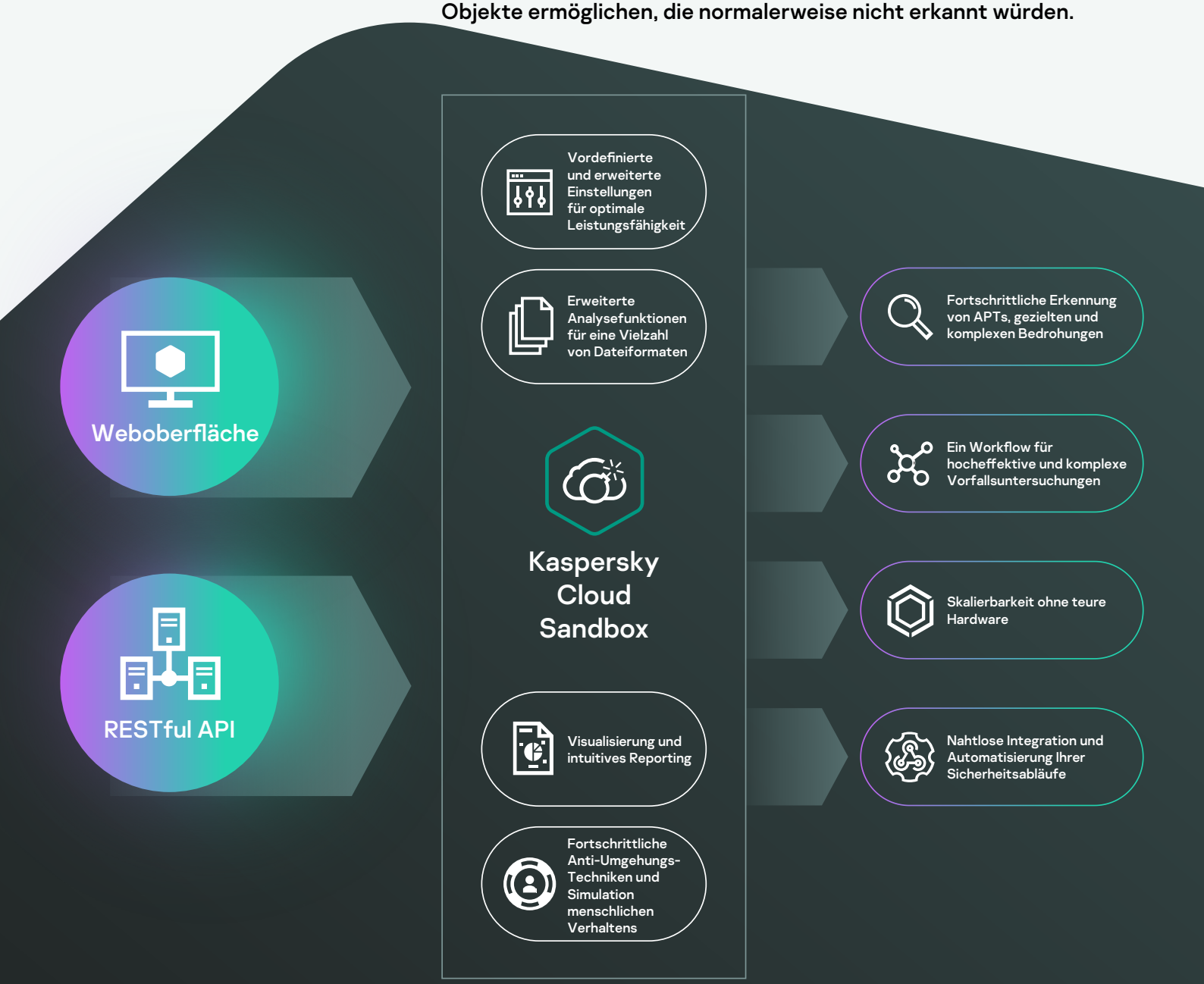
Überprüfen Sie, ob ein entdecktes Objekt weit verbreitet ist oder nur vereinzelt vorkommt.

Verstehen Sie, warum ein Objekt als schädlich eingestuft wird.

Kaspersky Cloud Sandbox

Herkömmliche Antiviren-Tools reichen heutzutage nicht mehr aus, um gezielte Angriffe zu verhindern. Virenschutz-Engines können nur bekannte Bedrohungen in verschiedenen Varianten abwehren. Versierte Bedrohungsakteure nutzen jedoch alle ihnen zur Verfügung stehenden Mittel, um eine automatische Erkennung zu umgehen. Verluste durch Zwischenfälle in der IT-Sicherheit steigen weiterhin exponentiell. Dadurch gewinnen Funktionen zur sofortigen Erkennung von Bedrohungen an Bedeutung, um eine schnelle Reaktionsfähigkeit aufzubauen und Bedrohungen entgegenzuwirken, bevor erhebliche Schäden entstehen können.

Intelligente Entscheidungen auf Basis von Dateiverhalten zu treffen und zugleich etwa den Prozess-Arbeitsspeicher, die Netzwerkaktivität usw. zu analysieren, ist der optimale Ansatz, um die neusten ausgeklügelten, gezielten und maßgeschneiderten Bedrohungen zu erfassen. Während es statistischen Daten häufig an Informationen zu kürzlich modifizierter Malware fehlt, bieten Sandboxing-Technologien leistungsstarke Tools, die die Untersuchung der Herkunft von Dateiproben, die Erfassung von IOCs auf Basis von Verhaltensanalysen sowie die Erkennung schädlicher Objekte ermöglichen, die normalerweise nicht erkannt würden.



Umfassendes Reporting

- Geladene und ausgeführte DLLs
- Externe Verbindungen mit Domainnamen und IP-Adressen
- Erstellte, geänderte und gelöschte Dateien
- Detaillierte Bedrohungsinformationen mit umsetzbarem Kontext für jeden aufgedeckten Gefährdungsindikator (IOC)
- Verarbeitete Speicherauszüge und Netzwerkverkehr-Dumps (PCAP)
- HTTP- und DNS-Anfragen und -Antworten
- Erstellte gemeinsame Erweiterungen (Mutexes)
- RESTful-API
- Geänderte und erstellte Registrierungsschlüssel
- Von der ausgeführten Datei erstellte Prozesse
- Screenshots
- **Und vieles mehr**

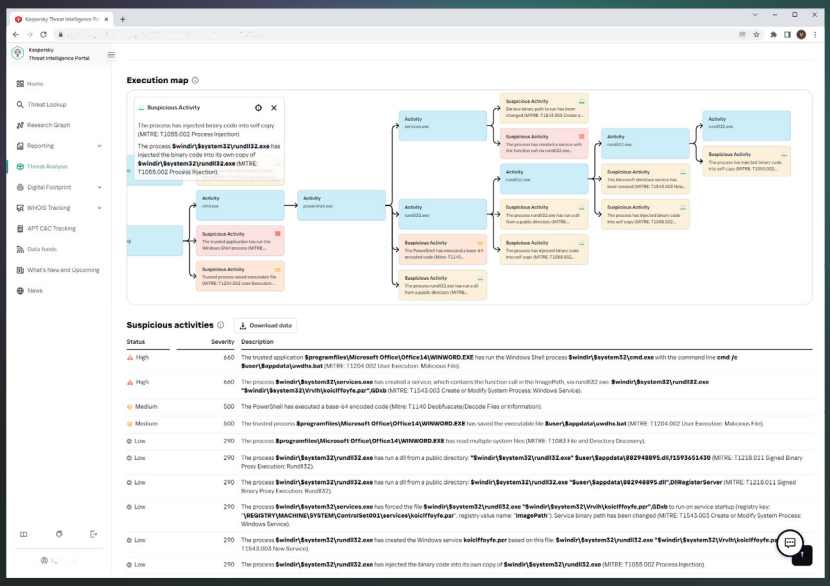
Proaktive Bedrohungserkennung und Risikominimierung

Malware verwendet eine Vielzahl von Methoden zur Verschleierung, damit sie nicht entdeckt wird. Wenn das System die erforderlichen Parameter nicht erfüllt, zerstört sich das schädliche Programm selbst, ohne Spuren zu hinterlassen. Damit der Schadcode ausgeführt werden kann, muss die Sandboxing-Umgebung daher in der Lage sein, ein normales Nutzerverhalten genau nachzuahmen.

Kaspersky Cloud Sandbox bietet einen hybriden Ansatz und kombiniert dabei Bedrohungsinformationen aus statistischen Daten im Petabyte-Bereich (dank des Kaspersky Security Network und anderen unternehmenseigenen Systemen), Verhaltensanalysen und besonders robuste Anti-Umgehungs-Techniken mit menschlichen Simulationstechnologien wie Auto-Clickern, Dokumentscrolling und Dummy-Prozessen.

Das Produkt wird bereits seit über 10 Jahren intern in unserem Sandbox Lab weiterentwickelt. Die Technologie vereint unser gesamtes Wissen hinsichtlich des Verhaltens von Malware, das wir uns in über 20 Jahren Bedrohungsforschung angeeignet haben. So können wir jeden Tag über 360.000 neue schädliche Objekte erkennen und unseren Kunden branchenführende Lösungen zur Verfügung stellen.

Cloud Sandbox ist Teil des Threat Intelligence Portals und ein wichtiger Bestandteil Ihres Threat Intelligence Workflows. Während Threat Lookup die neuesten detaillierten Bedrohungsdaten zu URLs, Domänen, IP-Adressen, Hash-Werten, Bedrohungsnamen, statistischen/Verhaltensdaten, WHOIS/DNS-Daten etc. abruft, können mit Cloud Sandbox diese Kenntnisse mit den von der analysierten Probe erzeugten IOCs verknüpft werden.



Jetzt können Sie hochwirksame und komplexe Vorfalluntersuchungen durchführen, um ein sofortiges Verständnis der Art der Bedrohung zu gewinnen und zusammenhängende Bedrohungsindikatoren aufzudecken.

Untersuchungen können äußerst ressourcenintensiv sein, insbesondere bei mehrstufigen Angriffen. Kaspersky Cloud Sandbox beschleunigt die Vorfallsreaktion sowie forensische Aktivitäten. So profitieren Sie von Skalierbarkeit für die automatische Verarbeitung von Dateien, ohne kostspielige Hardware erwerben oder sich Gedanken über Systemressourcen machen zu müssen.

Kaspersky APT Intelligence Reporting

Kunden von Kaspersky APT Intelligence Reporting erhalten exklusiven Zugriff auf unsere Untersuchungen und Entdeckungen, einschließlich vollständige technischen Daten (in verschiedenen Formaten) über jedes APT, sobald es entdeckt wird, sowie über Bedrohungen, die nie öffentlich gemacht werden. Die Berichte enthalten Zusammenfassungen, die sich an C-Level-Mitarbeiter richten und einfach verständliche Informationen zum entsprechenden APT enthalten. Der Zusammenfassung folgt eine ausführliche technische Beschreibung des APT mit zugehörigen IOCs und YARA-Regeln. So erhalten Sicherheitsforscher, Malware-Analysten, Sicherheitstechniker, Netzwerkanalysten und APT-Experten praktisch umsetzbare Daten, die eine schnelle und genaue Reaktion auf die Bedrohung ermöglichen.

Unsere Experten alarmieren Sie auch sofort, wenn sie Veränderungen in der Taktik von Cyberkriminellen feststellen. Außerdem erhalten Sie Zugriff auf die vollständige APT-Berichtsdatenbank von Kasperksy, einem weiteren leistungsstarken Forschungs- und Analysebestandteil Ihrer Sicherheitsstrategie.

Vorteile

MITRE ATT&CK-

Alle in den Berichten beschriebenen HTTP-Adressen werden MITRE ATT&CK zugeordnet. Dies ermöglicht eine verbesserte Erkennung und Reaktion durch die Entwicklung und Priorisierung der entsprechenden Anwendungsbereiche der Sicherheitsüberwachung, Schwachstellenanalysen und die Überprüfung der aktuellen Schutzmaßnahmen gegen relevante TTPs.

Informationen über nicht öffentliche APTs

Aus verschiedenen Gründen werden nicht alle komplexen Bedrohungen öffentlich bekannt gemacht. Wir teilen diese jedoch mit unseren Kunden.

Priorisierter Zugriff

Erhalt von technischen Beschreibungen der neuesten Bedrohungen während laufender Untersuchungen, bevor sie an die Öffentlichkeit gelangen

Nachträgliche Analyse

Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Abolaufzeit

Zugriff auf technische Daten

Dies beinhaltet eine umfangreiche Liste von IOCs, die in Standardformaten wie OpenIOC oder STIX bereitgestellt werden, sowie Zugriff auf unsere YARA-Regeln.

Profile von Bedrohungsakteuren

Einschließlich vermutetem Herkunftsland und Hauptaktivität, verwendeter Malware-Familien, angegriffener Branchen und Regionen sowie Beschreibungen aller verwendeten HTTP-Adressen und deren Zuordnung zu MITRE ATT&CK

Kontinuierliche Überwachung von APT-Kampagnen

Zugriff auf praktisch umsetzbare Informationen während der Untersuchung (Information über die APT-Verteilung, IOCs, C&C-Infrastruktur usw.)

RESTful-API

Nahtlose Integration und Automatisierung Ihrer Sicherheitsabläufe

Kaspersky Digital Footprint Intelligence

Ihr Unternehmen wächst. Aber gleichzeitig nimmt auch die Komplexität Ihrer verteilten IT-Umgebung zu; eine große Herausforderung, wenn es darum geht, Ihre weit verteilte digitale Präsenz ohne direkte Kontrolle oder entsprechende Zuständigkeiten zu schützen. Dank dynamischer und verbundener Umgebungen können Unternehmen erheblichen Nutzen ziehen. Gleichzeitig bietet die wachsende Konnektivität eine immer größer werdende Angriffsfläche. Und weil die Angreifer immer raffinierter werden, brauchen Sie nicht nur einen präzisen Einblick in die Online-Präsenz Ihrer Organisation, sondern müssen auch Veränderungen nachverfolgen und schnell entsprechend reagieren können.

Auch wenn Organisationen schon eine breite Palette an Sicherheitstools einsetzen, sind sie noch lange nicht vor jeder digitalen Bedrohung geschützt: Funktionen zur Erkennung und Eindämmung von Insider-Aktivitäten, Pläne und Angriffsszenarien von Cyberkriminellen in Darknet-Foren usw. Damit Sicherheitsanalysten Unternehmensressourcen aus dem Blickwinkel des Gegners betrachten, potentielle Angriffsvektoren schnell erkennen und ihre Verteidigungsstrategie entsprechend ausrichten können, hat Kaspersky die Kaspersky Digital Footprint Intelligence entwickelt.

Was wäre die beste Methode, einen Angriff gegen Ihr Unternehmen zu starten? Wie kann man Ihre Organisation am kosteneffizientesten angreifen? Welche Informationen stehen einem Angreifer, der es auf Ihr Unternehmen abgesehen hat, zur Verfügung? Wurde Ihre Infrastruktur bereits ohne Ihr Wissen angegriffen?

Kaspersky Digital Footprint Intelligence beantwortet diese und weitere Fragen. Unsere Experten erstellen dazu ein umfassendes Bild Ihrer Gefährdungslage, zeigen Schwachstellen auf, die mit großer Wahrscheinlichkeit genutzt werden, und weisen ggf. bereits stattgefundene bzw. geplante Angriffe nach.

Das Produkt bietet:

- Netzwerkperimeter-Bestandsaufnahme ohne Störung des laufenden Betriebs, um zu ermitteln, welche kundenseitigen Netzwerkressourcen und offen zugänglichen Services potentielle Angriffspunkte darstellen. Dazu gehören unter anderem versehentlich im Perimeter belassene Verwaltungsschnittstellen oder unzureichend konfigurierte Services, Geräteschnittstellen etc.
- Maßgeschneiderte Analyse der vorhandenen Schwachstellen mit Bewertung und umfassender Risikoeinstufung nach CVSS-Schweregrad, Verfügbarkeit von öffentlichen Exploits, Penetration Testing und Standort von Netzwerkressourcen (Hosting/Infrastruktur).
- Identifizierung, Überwachung und Analyse aller aktiven oder geplanten zielgerichteten Angriffe auf Ihr Unternehmen, Ihre Branche oder Region abzielende APT-Kampagnen.
- Die Erkennung von Bedrohungen, die sich speziell gegen Ihre Kunden, Partner und Abonnenten richten, deren infizierte Systeme dann für Angriffe auf Ihr Unternehmen genutzt werden könnten.
- Diskrete Überwachung von Pastebin-Seiten, öffentlichen Foren, Blogs, Instant-Messaging-Kanälen, im Untergrund tätige, geheime Online-Foren und -Communities; Ermittlung von möglicherweise gefährdeten Konten, Datenlecks oder Angriffen auf Ihre Organisation, die in diesen Foren geplant und diskutiert werden.

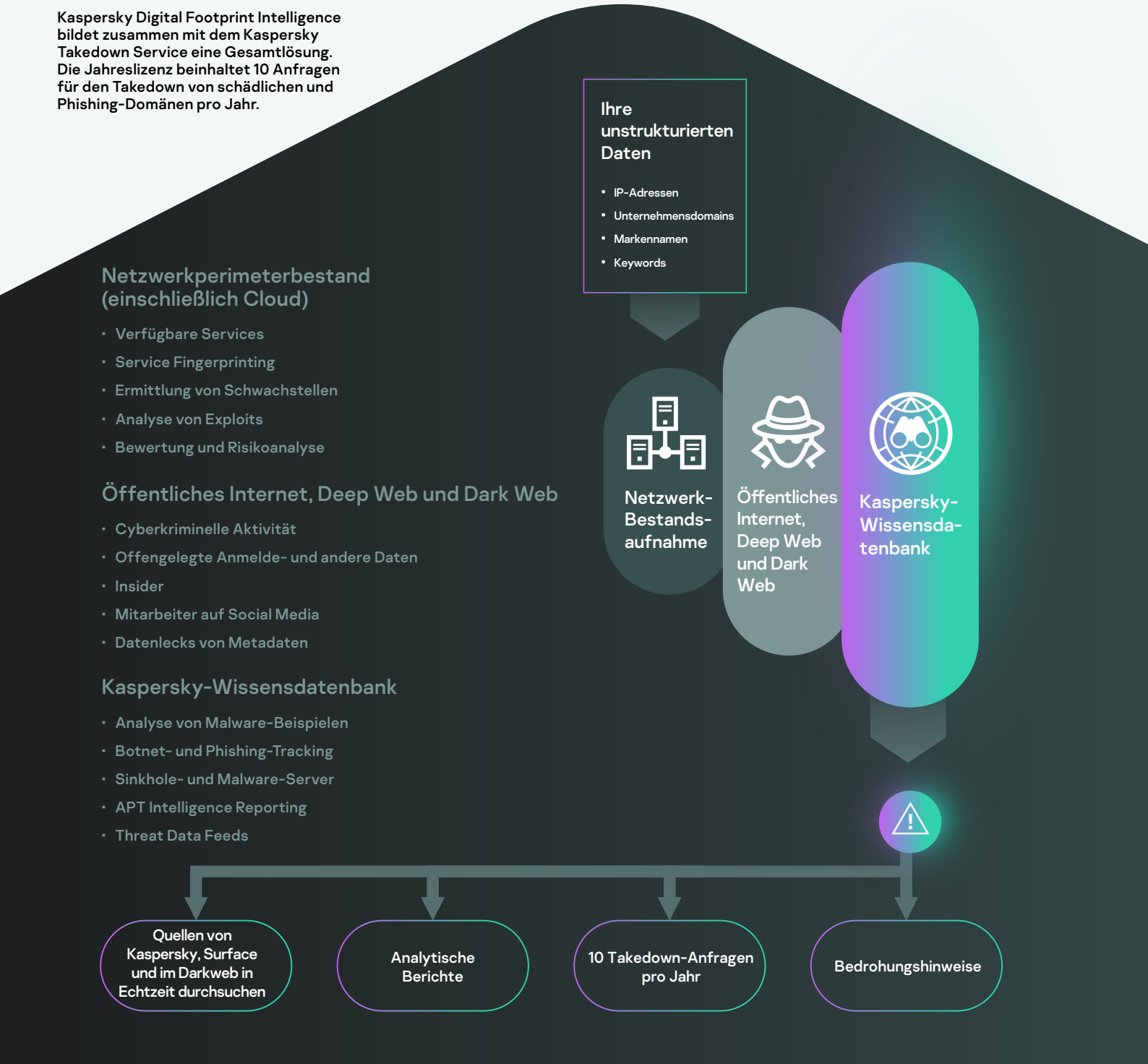
Wichtigste Vorteile

Kaspersky Digital Footprint Intelligence verwendet OSINT-Techniken in Kombination mit automatisierten und manuellen Analysen des öffentlichen Internets, Deep Web und Dark Web. Zusammen mit der internen Wissensdatenbank von Kaspersky erhalten Sie praktisch umsetzbare Einblicke und Handlungsempfehlungen

Das Produkt ist auf dem Kaspersky Threat Intelligence Portal verfügbar. Sie könnnen vier Quartalsberichte mit jährlichen Warnmeldungen zu Bedrohungen in Echtzeit oder einen Einzelbericht mit Warnungen, der sechs Monate lang aktiv ist, kaufen.

Durchsuchen Sie das öffentliche Internet und Dark Web nach Informationen in Echtzeit zu globalen Sicherheitsereignissen, die Ihre Assets bedrohen, sowie nach sensiblen Daten in geheimen Untergrund-Communities und Foren. Die Jahreslizenz umfasst 50 Suchen pro Tag über externe Quellen und die Wissensdatenbank von Kaspersky hinweg.

Kaspersky Digital Footprint Intelligence bildet zusammen mit dem Kaspersky Takedown Service eine Gesamtlösung. Die Jahreslizenz beinhaltet 10 Anfragen für den Takedown von schädlichen und Phishing-Domänen pro Jahr.



Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting liefert tiefgehende Informationen und ein größeres Bewusstsein für schädliche Kampagnen, die sich an Unternehmen richten, wie auch über Schwachstellen, die in den populärsten branchenweiten Kontrollsystemen und zu Grunde liegenden Technologien gefunden wurden. Berichte werden über ein Web-basiertes Portal geliefert. Dies bedeutet, dass Sie den Service sofort in Anspruch nehmen können.

In Ihrem Abonnement enthaltene Berichte

1. **APT-Berichte** Berichte zu neuen APT- und umfangreichen Angriffskampagnen mit Ausrichtung auf Unternehmen sowie Updates zu aktiven Bedrohungen.
2. **Die Bedrohungslandschaft.** Berichte über wesentliche Änderungen der Bedrohungslandschaft für branchenweite Kontrollsysteme, neu entdecke kritische Faktoren mit Auswirkung auf ICS-Sicherheitsstufen und ICS-Risiko für Bedrohungen, einschließlich regionaler, länderspezifischer und branchenspezifischer Informationen.
3. **Schwachstellen gefunden.** Berichte zu Schwachstellen, die von Kaspersky in den populärsten Produkten ermittelt wurden, die in branchenweiten Kontrollsystemen, dem branchenweiten Internet der Dinge und Infrastrukturen in verschiedenen Branchen verwendet werden.
4. **Analyse und Minderung von Schwachstellen** Wir liefern praktisch umsetzbare Empfehlungen von Kaspersky-Experten, um Schwachstellen in Ihrer Infrastruktur zu ermitteln und zu mindern.

Bedrohungsdaten ermöglichen Ihnen:

Ermitteln und verhindern Sie

gemeldete Bedrohungen, um kritische Assets zu sichern, wie Software- und Hardware-Komponenten, und um die Sicherheit und Kontinuität des technologischen Prozesses sicherzustellen

Führen Sie

ein Vulnerability Assessment Ihrer industriellen Umgebung und Assets basierend auf genauen Bewertungen des Umfangs und der Schwere der Schwachstelle durch und treffen Sie informierte Entscheidungen zum Patch Management oder der Implementierung anderer von uns empfohlener Präventionsmaßnahmen

Gleichen Sie

schädliche und verdächtige Aktivitäten, die Sie in industriellen Umgebungen ermitteln, mit den Recherche-Ergebnissen von Kaspersky ab und ordnen Sie sie schädlichen Kampagnen zu, ermitteln Sie Bedrohungen und reagieren Sie unverzüglich auf Vorfälle

Nutzen Sie

Informationen zu Angriffstechnologien, Taktiken und Abläufen, kürzlich entdeckten Schwachstellen und anderen wichtigen Veränderungen der Bedrohungslandschaft, um:

- Risiken, die von den berichteten Bedrohungen und anderen ähnlichen Bedrohungen ausgehen, zu ermitteln und zu bewerten
- Änderungen der industriellen Infrastruktur zu planen und zu konzipieren, um die Sicherheit der Produktion und die Kontinuität des technologischen Prozesses sicherzustellen
- Aktivitäten zum Sicherheitsbewusstsein basierend auf Analysen realer Fälle auszuführen, um Schulungsszenarien für Mitarbeiter zu schaffen und Übungen zwischen Red Teams und Blue Teams zu planen
- Fundierte strategische Entscheidungen zu treffen, um in Cybersicherheit zu investieren und die Resilienz der Betriebsabläufe sicherzustellen

Kaspersky Ask the Analyst

Kontinuierliche Bedrohungsforschung

ermöglicht es Kaspersky, auf der ganzen Welt Darknet-Foren und geschlossene Communities aufzuspüren, zu infiltrieren und zu überwachen, in denen sich Cyberkriminelle und potenzielle Angreifer aufhalten. So können unsere Analysten die gefährlichsten und komplexesten Bedrohungen proaktiv erkennen und untersuchen – auch solche, die auf bestimmte Unternehmen abzielen.

Cyberkriminelle entwickeln kontinuierlich raffinierte Angriffsstrategien gegen Unternehmen. Dabei setzen sie immer agilere Technologien ein. Die Folge: Die aktuelle Bedrohungslandschaft ist unbeständig und wächst schnell. Unternehmen sehen sich mit komplexen Vorfällen konfrontiert, verursacht durch Angriffe ohne Malware, dateilose Angriffe, LOTL-Angriffe (Living off the Land), Zero-Day-Exploits – und komplexe Bedrohungen sowie APT-ähnliche und gezielte Angriffe, die alle diese Varianten kombinieren.

Im Zeitalter geschäftsschädigender Cyberangriffe sind Cybersicherheitsexperten wichtiger als je zuvor, allerdings nicht einfach zu finden und zu halten. Und selbst wenn Sie über ein gut eingespieltes Cybersicherheitsteam verfügen, können Sie nicht erwarten, dass es sich den raffinierten Bedrohungen von heute immer allein stellt **– es muss externe Experten zurate ziehen können.** Solche externen Experten können auf wahrscheinliche Ausbreitungspfade komplexer Angriffe oder APTs hinweisen und praktische Ratschläge geben, wie man sie durch gezieltes Handeln unterbinden kann.

Leistungsumfang von Ask the Analyst

(vereinheitlichtes Abonnement, basierend auf Anfrage)

Der Service **Kaspersky Ask the Analyst** erweitert unser Threat Intelligence-Portfolio und ermöglicht es Ihnen, Handlungsempfehlungen und Erkenntnisse zu spezifischen Bedrohungen anzufordern. Der Service stimmt die leistungsstarken Threat Intelligence- und Forschungskompetenzen von Kaspersky auf Ihre individuellen Anforderungen ab. So können Sie eine zuverlässige Verteidigung gegen Bedrohungen aufbauen.

APT und Crimeware

Weiterführende Informationen zu veröffentlichten Berichten und laufender Forschung (zusätzlich zu APT Intelligence Reporting oder Crimeware Intelligence Reporting)[1]

Malware-Analyse

- Analyse von Malware-Proben
- Empfehlungen für weitere Eindämmungsmaßnahmen

Beschreibungen von Bedrohungen, Schwachstellen und relevanten IoCs

- Allgemeine Beschreibung spezifischer Malware-Familien
- Zusätzlicher Kontext zu Bedrohungen (relevante Hashes, URLs, CnCs usw.)
- Informationen zu spezifischen Schwachstellen (Ausmaß und entsprechende Schutzmechanismen in Kaspersky-Produkten)

Dark-Web-Intelligence[2]

- Dark-Web-Recherche zu spezifischen Artefakten, IP-Adressen, Domänennamen, Dateinamen, E-Mails, Links und Bildern
- Informationssuche und -analyse

ICS-bezogene Anfragen

- Zusätzliche Informationen zu veröffentlichten Berichten
- Informationen zu ICS-Schwachstellen
- ICS-Bedrohungsstatistiken und Trends für die Region/Branche
- Informationen zur ICS-Malware-Analyse hinsichtlich Regulierungen und Standards

[1] Nur verfügbar für Kunden mit aktivem Abonnement für APT Intelligence Reporting und/oder Crimeware Intelligence Reporting.

[2] Bereits enthalten im Abonnement für Kaspersky Digital Footprint Intelligence.

Servicevorteile

Zusätzliches Fachwissen

Sie haben jederzeit Zugang zu Branchenexperten und müssen nicht erst auf dem Arbeitsmarkt nach teuren und schwer zu findenden Vollzeitspezialisten suchen.

Schnellere Untersuchungen

Maßgeschneiderte und detaillierte Kontextinformationen ermöglichen eine effiziente Bewertung und Priorisierung von Vorfällen.

Schnelle Reaktion

Mit unserer Hilfe können Sie schnell auf Bedrohungen und Schwachstellen reagieren und Angriffe über bekannte Vektoren abblocken.

Funktionsweise

Kaspersky Ask the Analyst kann separat erworben werden oder zusätzlich zu jedem unserer anderen Threat-Intelligence-Services.

Anfragen können über Kaspersky Company Account gestellt werden, unser Support-Portal für Unternehmenskunden. Wir antworten per E-Mail, können bei Bedarf und mit Ihrer Zustimmung aber auch gerne ein Meeting organisieren. Sobald Ihre Anfrage angenommen wurde, teilen wir Ihnen die geschätzte Bearbeitungsdauer mit.

Anwendungsfälle für den Service:

- Klärung von Details in zuvor veröffentlichten Threat Intelligence-Berichten
- Zusätzliche Informationen zu bereits bekannten IoCs
- Details zu Schwachstellen und Empfehlungen dazu, wie sich deren Ausnutzung verhindern lässt
- Zusätzliche Details zu spezifischen Dark-Web-Aktivitäten, die für Ihr Unternehmen interessant sind
- Berichte zu Malware-Familien mit Details zum Verhalten der Malware, ihren potenziellen Auswirkungen und allen Kaspersky bekannten Aktivitäten, die ihr zugeordnet werden
- Effektive Priorisierung von Warnungen/ Vorfällen dank kurzer Berichte mit detaillierten Kontextinformationen und einer Kategorisierung nach relevanten IoCs
- Anforderung von Unterstützung bei der Identifizierung, wenn erkannte ungewöhnliche Aktivitäten auf APTs oder Crimeware zurückzuführen sind
- Einsendung von Malware-Dateien zur umfassenden Analyse auf Verhalten und Funktionsweise

Ergänzung Ihres Know-hows und Ihrer Ressourcen

Mit Kaspersky Ask the Analyst haben Sie auf Fallbasis Zugang zu einem Kernteam von Kaspersky-Forschern. Der Service bietet umfassende Kommunikation zwischen Experten und ergänzt so Ihr firmeninternes Know-how um unser umfassendes Angebot aus Fachwissen und Ressourcen.

Kaspersky Takedown Service

Die Herausforderung

Cyberkriminelle erstellen schädliche und Phishing-Domänen, die für einen Angriff auf Ihr Unternehmen und Ihre Marken verwendet werden. Die Unfähigkeit, diese Bedrohungen schnell abzuwehren, sobald sie erkannt wurden, kann Umsatzverluste, Schäden für die Marke, Verlust des Kundenvertrauens, Datenlecks und vieles mehr zur Folge haben. Die Verwaltung der Takedowns dieser Domänen ist jedoch ein komplexer Prozess, der Fachkenntnis und Zeit erfordert.

Lösung

Kaspersky blockiert mehr als 15.000 betrügerische und Phishing-URLs und verhindert täglich über eine Million Versuche, solche URLs anzuklicken. Unsere jahrelange Erfahrung im Bereich der Analyse von schädlichen und Phishing-Domänen heißt, dass wir wissen, wie wir alle notwendigen Beweise sammeln müssen, um deren Schädlichkeit nachzuweisen. Wir kümmern uns um die Verwaltung des Takedown und ermöglichen eine schnelle Reaktion zur Minimierung Ihres digitalen Risikos, sodass sich Ihr Team auf andere wichtige Aufgaben konzentrieren kann.

Durch die Kooperation mit internationalen Organisationen, nationalen und regionalen Strafverfolgungsbehörden (z. B. INTERPOL, Europol, Microsoft Digital Crimes Unit, The National High-Tech Crime Unit (NHTCU) der niederländischen Polizei und der City of London Police) sowie Computer Emergency Response Teams (CERTs), bietet Kaspersky seinen Kunden wirksamen Schutz ihrer Online-Dienste und Reputation.

Funktionsweise

Anfragen können über Kaspersky Company Account gestellt werden, unser Support-Portal für Unternehmenskunden. Wir bereiten alle notwendigen Unterlagen vor und senden die Anfrage für den Takedown an die relevante lokale/regionale Behörde (CERT, Registrierungsstelle usw.), die über die notwendige rechtliche Befugnis verfügt, die Domäne zu deaktivieren. Sie werden über jeden Schritt benachrichtigt, bis die entsprechende Quelle erfolgreich deaktiviert wurde.

Müheloser Schutz

Der Kaspersky Takedown Service wehrt Angriffe durch schädliche und Phishing-Domänen schnell ab, bevor Ihre Marke und Ihr Unternehmen Schaden nehmen. Die umfassende Verwaltung des gesamten Prozesses spart Ihnen wertvolle Zeit und Ressourcen.

Servicevorteile

Weltweite Abdeckung

Es spielt keine Rolle, wo eine schädliche oder Phishing-Domäne registriert ist, Kaspersky wird bei der regionalen Organisation mit der entsprechenden rechtlichen Befugnis einen Takedown anfordern.

Umfassende Verwaltung

Wir kümmern uns um den gesamten Takedown-Prozess und minimieren Ihre Beteiligung.

Vollständige Sichtbarkeit

Sie werden in jeder Phase des Prozesses benachrichtigt, von der Registrierung Ihrer Anfrage bis hin zum erfolgreichen Takedown.

Integration mit Digital Footprint Intelligence

Dieser Service kann in Kaspersky Digital Footprint Intelligence integriert werden. So erhalten Sie Benachrichtigungen in Echtzeit über Phishing- und Malware-Domänen, die darauf ausgelegt sind, Ihre Marke/Organisation zu missbrauchen oder sich als solche ausgeben. Eine einzige Lösung ist ein wichtiger Bestandteil einer umfassenden Cybersicherheitsstrategie.

Vorteile

- Ermöglicht globale Transparenz von Bedrohungen, die rechtzeitige Erkennung von Cyberbedrohungen, die Priorisierung von Sicherheitswarnungen und die effektive Reaktion auf Vorfälle bzgl. der Informationssicherheit
- Verhindert die Überforderung von Analysten und hilft Ihren Mitarbeitern, sich auf echte Bedrohungen zu konzentrieren
- Die einzigartigen Einblicke in die von Bedrohungsakteuren in verschiedenen Branchen und Regionen eingesetzten Taktiken, Techniken und Abläufe ermöglichen einen proaktiven Schutz vor zielgerichteten und komplexen Bedrohungen
- Dank des vollständigen Überblicks über Ihre Sicherheitslage mit praktisch umsetzbaren Empfehlungen zu Abwehrstrategien können Sie Ihre Verteidigungsstrategie auf die Bereiche konzentrieren, die als vorrangige Ziele für Cyberangriffe ausgemacht wurden
- Verbesserte und beschleunigte Vorfallsreaktion sowie Threat Hunting-Funktionen verringern die Verweilzeit für den Angriff und minimieren einen möglichen Schaden erheblich

Fazit

Die Bekämpfung heutiger Cyberangriffe erfordert eine umfassende Sicht auf die von den Bedrohungsakteuren eingesetzten Taktiken und Tools. Diese Informationen zu generieren und die effektivsten Gegenmaßnahmen zu identifizieren, erfordert ständigen Einsatz und ein hohes Maß an Fachwissen. Mit Petabytes an aussagekräftigen Bedrohungsdaten, fortschrittlichen Machine-Learning-Technologien und einem einzigartigen Pool weltweit agierender Experten unterstützt Kaspersky seine Kunden mit der neuesten Threat Intelligence aus der ganzen Welt und hilft ihnen dabei, ihre Immunität auch gegen bisher unbekannte Cyberangriffe aufrechtzuerhalten.

FORRESTER®

Kaspersky ging im Rahmen der Bewertung „Forrester Wave: External Threat Intelligence Services 2021“ als „Leader“ hervor.

www.kaspersky.de