Kaspersky Threat Intelligence

kaspersky

Kaspersky Threat Intelligence

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 Cybersecurity Services

Das Kaspersky Threat Intelligence

Threat Data Feeds
CyberTrace
APT Intelligence Reporting
Digital Footprint Intelligence
Threat Lookup
Cloud Sandbox
Financial Threat Intelligence
Reporting,

Das Kaspersky Threat Hunting

Kaspersky Security Training

Kaspersky Incident Response

Das Kaspersky Security Assessment

Die Threat Intelligence Services von Kaspersky bieten Ihnen Zugriff auf alle Informationen, die Sie zur Abwehr dieser Bedrohungen benötigen. Sie werden von unserem erfahrenen 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. Auch Sie können dieses Wissen für Ihr Unternehmen nutzen.

Die Threat Intelligence Services von Kaspersky beinhalten:

- Threat Data Feeds
- CyberTrace
- APT Intelligence Reporting
- Digital Footprint Intelligence
- Threat Lookup
- Cloud Sandbox
- Financial Threat Intelligence Reporting,

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 in Systeme einzudringen und 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 Sicherheitskontrollen, wie z. B. SIEM-Systeme, können Sicherheitsteams die Ersteinstufung von Warnmeldungen automatisieren. Außerdem bieten sie den Tier 1 Analysts so ausreichend Kontext, um umgehend ermitteln zu können, welche Warnungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die Incident Response (IR) Teams übergeben werden müssen.

Andere Sicherheitsanbieter und Unternehmen nutzen KasperskyThreat Data Feeds, um eigene Sicherheitslösungen zu entwickeln oder **ihr Unternehmen zu schützen**.

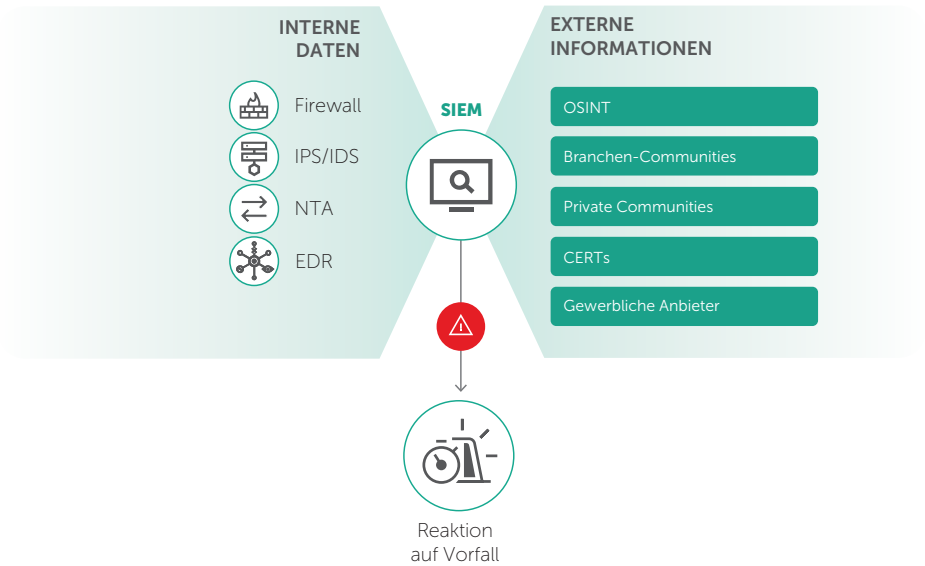


Abbildung 1. Operationalisierung externer Bedrohungsinformationen

Kontextdaten

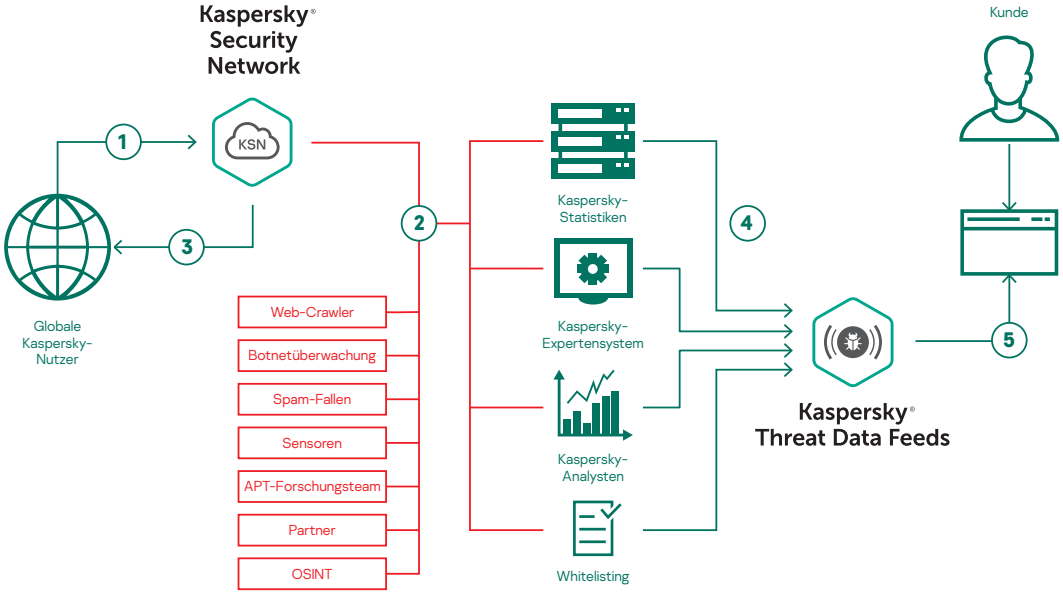
Jeder Datensatz in jedem Data Feed wird mit **umfangreichem Kontext** angereichert (Bezeichnungen von Bedrohungen, Zeitstempel, Geolokalisierungsdaten, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.). Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die 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 rechtzeitig Entscheidungen treffen und die **richtigen Maßnahmen für Ihr Unternehmen** finden können.

Die Data Feeds

Die Feeds umfassen Folgendes:

- **IP Reputation Feed** – Gruppen von IP-Adressen mit Kontext zu verdächtigen und schädlichen Hosts;
- **Malicious and Phishing URL** – Enthält schädliche bzw. Phishing-Links und -Websites;
- **Botnet C&C URL Feed** – Enthält C&C-Server für Desktop-Botnets sowie zugehörige schädliche Objekte;
- **Mobile Botnet C&C URL Feed** – Enthält C&C-Server für mobile Botnets, um infizierte Geräte zu erkennen, die mit C&C-Servern kommunizieren;
- **Ransomware URL Feed** – Enthält Links, die Ransomware-Objekte hosten oder auf die Ransomware-Objekte zugreifen;
- **Schwachstellen-Daten-Feed** – Eine Reihe von Sicherheitslücken mit verbundener Threat Intelligence (Hashes anfälliger Apps/Exploits, Zeitstempel, CVEs, Patches etc.);
- **APT IoC Feeds** – Enthält schädliche Domains, Hosts, IP-Adressen und Dateien, die Cyberkriminelle bei APT-Angriffen verwenden;
- **Passiver DNS (pDNS) Feed** – Eine Reihe von Datensätzen, die die Ergebnisse von DNS-Lösungen für Domänen in entsprechenden IP-Adressen enthalten;
- **IoT URL Feed** – Betrifft Websites, die verwendet wurden, um Malware herunterzuladen, die IoT-Geräte infiziert;
- **Malicious Hash Feed** – Umfasst die gefährlichste, am weitesten verbreitete und neu aufkommende Malware;
- **ICS Hash-Datenfeeds** – Satz von Hash-Werten mit entsprechendem Kontext zur Erkennung von schädlichen Objekten, die in ICS (Industrial Control Systems) verwendete Geräte befallen;
- **Mobile Malicious Hash Feed** – Unterstützt die Erkennung schädlicher Objekte, die mobile Android- und iOS-Plattformen infizieren;
- **ICS Hash-Datenfeeds** – Satz von Hash-Werten mit entsprechendem Kontext zur Erkennung von schädlichen Objekten, die in ICS (Industrial Control Systems) verwendete Geräte befallen;
- **P-SMS Trojan Feed** – Unterstützt die Erkennung von SMS-Trojanern, über die Angreifer SMS-Nachrichten stehlen, löschen oder beantworten und Sondergebühren für mobile Nutzer erheben können;
- **Whitelisting Data Feed** – Stellt für Lösungen und Services von Drittanbietern systematische Informationen zu legitimer Software bereit;
- **Kaspersky Transforms for Maltego** – Liefert Maltego-Nutzern eine Reihe von Transformationen, mit denen auf Kaspersky Threat Data Feeds zugegriffen werden kann. Mit Kaspersky Transforms for Maltego können Sie URLs, Hashes und IP-Adressen mithilfe der Feeds von Kaspersky überprüfen. Die Transformationen können die Kategorie eines Objekts bestimmen und nützlichen Kontext bereitstellen.

Abbildung 2. Quellen der Kaspersky Threat Intelligence



Service-Highlights

- 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.
- 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** garantiert.
- Sämtliche Feeds werden über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die **dauerhafte Verfügbarkeit** gewährleistet.
- Die Feeds ermöglichen die **umgehende Erkennung von URLs**, die für Phishing, Malware, Exploits, Botnets und andere schädliche Inhalte genutzt werden.
- **Malware** in allen Arten von Datenverkehr (Web, E-Mail, P2P, IM usw.) sowie gezielte mobile Malware kann **sofort erkannt** und identifiziert werden.
- Einfache **Verteilungsformate** (**JSON, CSV, OpenIOC, STIX**) über **HTTPS** oder Ad-hoc-Bereitstellungsmechanismen ermöglichen die einfache Integration der Daten in Sicherheitslösungen.
- Hunderte von Experten, darunter **Sicherheitsanalysten** aus der ganzen Welt, weltweit anerkannte **Sicherheitsexperten aus unserem GReAT-Team** und führenden 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.
- **Einfache Implementierung.** Dank ergänzender Dokumentation, Beispielen, einem persönlichen technischen Account Manager sowie dem technischen Support von Kaspersky geht die Integration schnell und einfach vonstatten.

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 alle aggregierten Daten in Echtzeit sorgfältig untersucht und verfeinert. Dazu kommen verschiedene Vorverarbeitungstechniken zum Einsatz, wie statistische Kriterien, Sandboxes, heuristische Engines, Multiscanner, Similarity Tools, Behavior Profiling, Analystenvalidierung und Whitelisting-Verifizierung:

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.) werden vollständig unterstützt.
- Entwickeln oder verbessern Sie den **Malware-Schutz für Geräte am Netzwerkrand** (wie z. B. Router, Gateways und UTM-Appliances).
- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Fähigkeiten**, indem Sie Ihren Sicherheits- bzw. SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe gezielter Angriffe bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit, und unterbrechen Sie die Kill Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- **Stellen Sie Unternehmensnutzern Bedrohungsinformationen bereit**. Nutzen Sie Informationen aus erster Hand zu aufkommender Malware und anderen Bedrohungen, um Ihre Verteidigung **präventiv zu stärken und Vorfälle zu vermeiden**.
- **Helfen Sie bei der Abwehr gezielter Angriffe**. Verstärken Sie Ihre Sicherheitsstellung durch taktische und strategische Bedrohungsinformationen, indem Sie Verteidigungsstrategien an die spezifischen Bedrohungen anpassen, mit denen Ihr Unternehmen konfrontiert ist.
- Verwenden Sie Threat Intelligence, um **schädliche Inhalte aufzudecken, die auf Ihren Netzwerken und Datenzentren gehostet werden**.
- **Verhindern Sie die Extraktion vertraulicher Assets und geistigen Eigentums** über infizierte Geräte an Personen außerhalb des Unternehmens. Dank der schnellen Erkennung infizierter Assets vermeiden Sie den Verlust von Wettbewerbsvorteilen und Geschäftschancen und schützen den Ruf Ihres Unternehmens.
- Durchsuchen Sie Gefährdungsindikatoren, wie z. B. C&C-Protokolle, IP-Adressen, schädliche URLs oder Datei-Hashes mit von Experten validiertem Bedrohungskontext. Dieser ermöglicht es Ihnen, Angriffe zu priorisieren, vereinfacht Entscheidungen zu IT-Ausgaben und -Ressourcenverteilung und **unterstützt Sie dabei, sich auf die Abwehr der Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen**.
- Nutzen Sie unsere Expertise und praktisch umsetzbaren Kontextinformationen zur **Verbesserung Ihrer Produkte und Services**, wie z. B. Inhaltsfilterung, Blockierung von Spam/Phishing usw.
- **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

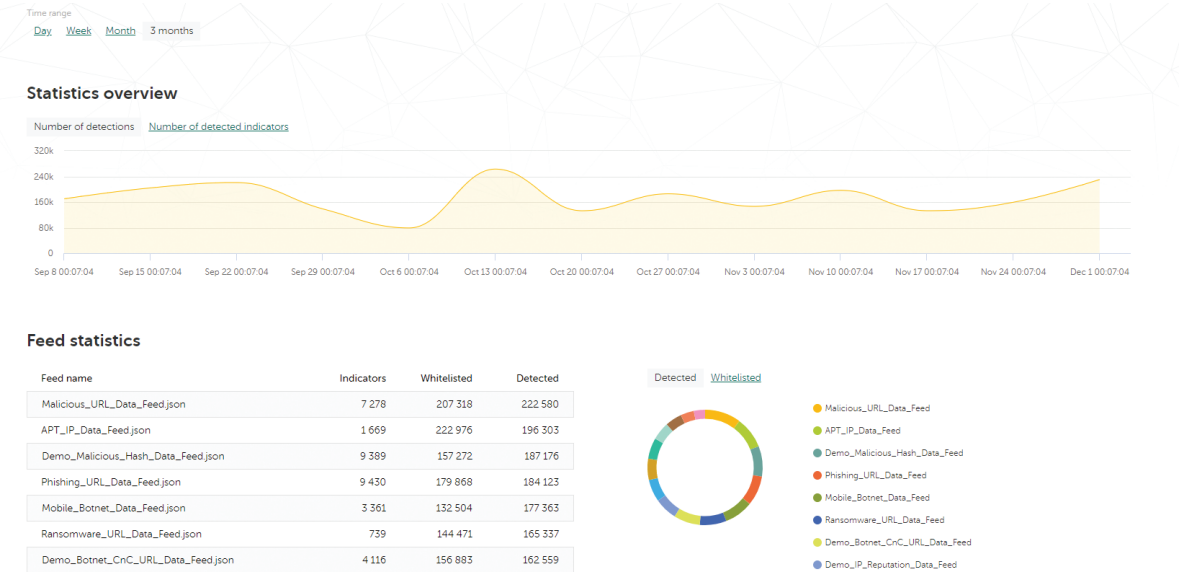
Die Anzahl der Sicherheitswarnungen, die Analysten in Security Operations Centers (SOC) täglich bearbeiten müssen, wächst exponentiell. Angesichts dieser riesigen Datenmengen ist eine effektive Priorisierung, Auswahl und Validierung der Warnungen nahezu unmöglich. Permanent zeigen die zahlreichen Sicherheitsprodukte neue Benachrichtigungen an – bis zu dem Punkt, an dem wichtige Alarme in der Masse untergehen und Analysten überfordert sind. SIEM-Systeme, also Tools zur Protokollverwaltung und Sicherheitsanalyse, die Sicherheitsdaten zusammenführen und Beziehungen zwischen den verschiedenen Warnungen finden, können die Anzahl der Sicherheitsbenachrichtigungen, die näher untersucht werden müssen, reduzieren. Analysten an vorderster Front – sogenannte Tier 1 Analysts – sind jedoch auch mit entsprechenden Systemen oft völlig überfordert.

Effektive Auswahl und Analyse von Sicherheitswarnungen

Durch Integration topaktueller maschinenlesbarer Bedrohungsinformationen in bestehende Systeme, wie z.B. SIEM-Systeme, können Security Operation Centers die Erstauswahl automatisieren. Außerdem bietet sie den Tier1 Analysts so ausreichend Kontext, um umgehend ermitteln zu können, welche Warnungen näher untersucht oder zur weiterenÜberprüfung und Bearbeitung an die an die Incident Response (IR) Teams übergeben werden müssen. Durch die steigende Anzahl von Threat Intelligence Feeds und verfügbaren Bedrohungsinformationen können Unternehmen jedoch 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 ein Threat Intelligence Tool zur Zusammenführung und Analyse von Bedrohungsinformationen, das die nahtlose Integration von Threat Intelligence Feeds in SIEM-Lösungen ermöglicht. So können Analysten die Bedrohungsinformationen in ihren bestehenden Sicherheitsworkflows nutzen. Die Lösung kann jeden Threat Intelligence Feed im JSON-, STIX-, XML- oder CSV-Format integrieren, den Sie verwenden möchten. Hierzu zählen Feeds von Kaspersky, von anderen Anbietern, Open Source-Informationen (Open Source Intelligence, OSINT) sowie benutzerdefinierte Feeds. Darüber hinaus unterstützt CyberTrace zahlreiche SIEM-Lösungen und Protokollquellen ohne Konfigurationsaufwand. Durch automatische Abstimmung der Protokolle mit den Bedrohungsfeeds bietet Kaspersky CyberTrace zu jedem Zeitpunkt eine Echtzeitübersicht der aktuellen Sicherheitssituation, damit Tier 1 Analysts schneller fundiertere Entscheidungen treffen können.

Abbildung 3. Statistiken von Kaspersky CyberTrace



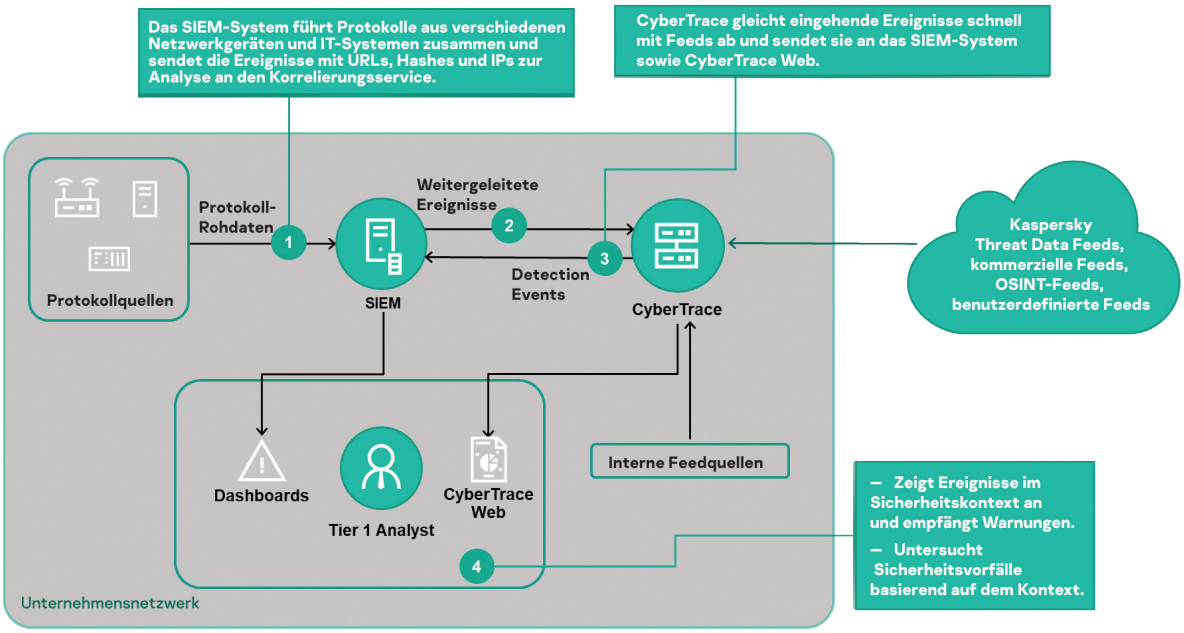
Kaspersky CyberTrace bietet verschiedene Tools, um Bedrohungsinformationen optimal zu nutzen und eine effektive Auswahl von bzw. Reaktion auf Sicherheitswarnungen zu ermöglichen:

- Bereits enthaltene Demo-Bedrohungsfeeds von Kaspersky sowie OSINT-Feeds
- SIEM-Konnektoren für verschiedenste SIEM-Lösungen zur Visualisierung und Verwaltung von Bedrohungsdaten
- Feed-Nutzungsstatistiken zur Messung der Effektivität integrierter Feeds
- On Demand-Suche nach Indikatoren (Hashes, IP-Adressen, Domains, URLs) für eingehende Untersuchungen

- Weboberfläche für Datenvisualisierungen, Konfigurationszugriff sowie zur Verwaltung von Feeds, Syntaxanalyse-Regeln, Blacklists und Whitelists
- Erweiterte Feed-Filter (basierend auf dem Kontext des jeweiligen Indikators, einschließlich Bedrohungstyp, Geostandort, Beliebtheit, Zeitstempel und weiteren Informationen) sowie Protokollereignisse (basierend auf benutzerdefinierten Bedingungen)
- Export von Suchergebnissen aus Datenfeeds im CSV-Format zur Integration in andere Systeme (Firewalls, Netzwerk- und Host-IDS, benutzerdefinierte Tools)
- Batch Scans von Protokollen und Dateien
- Befehlszeilenschnittstelle für Windows- und Linux-Plattformen
- Standalone-Modus, bei dem Kaspersky CyberTrace nicht in ein SIEM-System integriert wird, sondern die Protokolle von verschiedenen Quellen, wie z.B. Netzwerkgeräten, empfängt und analysiert
- Installation in DMZs, die vom Internet isoliert sein müssen

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:

Abbildung 4. Integrationsschema von Kaspersky CyberTrace



Kaspersky CyberTrace und die Kaspersky Threat Data Feeds können zwar separat verwendet werden, verbessern jedoch in Kombination deutlich die Bedrohungserkennung und ermöglichen einen sicheren Betrieb mit umfassendem globalem Einblick in Cyberbedrohungen. Kaspersky CyberTrace und die Kaspersky Threat Data Feeds bieten SOC-Analysten folgende Vorteile:

- Effektive Analyse und Priorisierung von Sicherheitswarnungen
- Verbesserung und Beschleunigung der Auswahl und Erstreaktion
- Umgehende Erkennung kritischer Warnungen und fundiertere Entscheidungen hinsichtlich der Eskalation von Warnungen an Vorfallsreaktionsteams
- Vorausschauende informationsbasierte Abwehr

Kaspersky APT Intelligence Reporting bietet Folgendes:

- **Exklusiver Zugriff** auf die technischen Details aktueller Bedrohungen noch während der Untersuchung und vor der Veröffentlichung.
- **Einblicke in nicht öffentliche APTs:** Nicht alle komplexen Bedrohungen werden öffentlich bekannt gemacht. Einige von ihnen werden aufgrund der Angriffsziele, der Vertraulichkeit der Daten, der Art und Weise, auf die die Schwachstellen geschlossen werden, oder der zugehörigen Strafverfolgungsmaßnahmen nie veröffentlicht. Aber die Details werden unseren Kunden mitgeteilt.
- **Detaillierter Zugriff auf technische Daten.** Dies beinhaltet eine umfangreiche Liste von Gefährdungsindikatoren (Indicators of Compromise, IOCs), die in Standardformaten wie OpenIOC oder STIX bereitgestellt werden, sowie Zugriff auf unsere Yara-Regeln.
- **Profile von Bedrohungsakteuren** mit zusammengefassten Informationen zum jeweiligen Bedrohungsakteur, einschließlich vermutetem Herkunftsland und Hauptaktivität, verwendeter Malware-Familien, angegriffener Branchen und Regionen sowie Beschreibungen aller verwendeten HTTP-Adressen und deren Zuordnung zum MITRE ATT&CK-Framework.
- **MITRE ATT&CK.** Alle in den Berichten beschriebenen HTTP-Adressen werden dem MITRE ATT&CK-Framework 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.
- **Kontinuierliche Überwachung von APT-Kampagnen:** Zugriff auf praktisch nutzbare Informationen noch während der Untersuchung (Information über die APT-Verteilung, IOCs, C&C-Infrastruktur).
- **Nachträgliche Analyse:** Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Abolaufzeit.
- **RESTful-API** für nahtlose Integration und Automation Ihrer Sicherheitsworkflows.

APT Intelligence Reporting

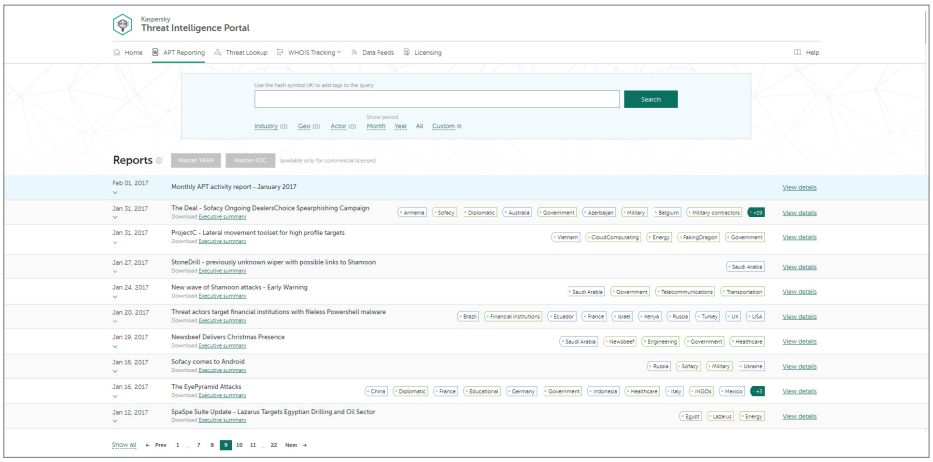
Verbessern Sie das Bewusstsein für und Wissen über hochentwickelte Cyberspionage-Kampagnen durch umfassende, praxisorientierte Berichte von Kaspersky.

Mit den Informationen in diesen Berichten können Sie schnell auf neue Bedrohungen und Schwachstellen reagieren, indem Sie Angriffe über bekannte Vektoren abblocken, den durch hoch entwickelte Angriffe angerichteten Schaden reduzieren und Ihre Sicherheitsstrategie oder die Ihrer Kunden erweitern.

Kaspersky hat einige der bedeutendsten APT-Angriffe aller Zeiten entdeckt. Nicht alle neu entdeckten APTs werden umgehend gemeldet– viele von ihnen werden sogar nie veröffentlicht.

Als Abonnent von Kaspersky APT Intelligence Reporting erhalten Sie exklusiven Zugang zu unseren Forschungsergebnissen und Erkenntnissen, einschließlich der vollständigen technischen Details in unterschiedlichen Formaten zu jedem APT, noch während dieser aufgedeckt wird – inklusive aller Bedrohungen, die nie veröffentlicht werden. Jeder der Berichte enthält 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 Informationen für eine präzise Reaktion auf entsprechende Bedrohungen.

Unsere Experten, die zu den erfolgreichsten APT-Jägern der Branche zählen, halten Sie zudem über Änderungen in der Taktik von Cyberkriminellen auf dem Laufenden. Außerdem erhalten Sie Zugriff auf unsere vollständige Datenbank mit APT-Berichten – eine weitere effektive Recherche- und Analysequelle, die Sie zur Verteidigung Ihres Unternehmens nutzen können.



Hinweis – Einschränkung von Abonnenten

Aufgrund der Tatsache, dass einige der in den Berichten enthaltenen Informationen äußerst vertraulich und spezifisch sind, können wir diese Services nur vertrauenswürdigen staatlichen sowie börsennotierten bzw. privat geführten Unternehmen zur Verfügung stellen.

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 aus der Optimierung ihrer Prozesse, erhöhter Produktqualität, einem besseren Kundeneindruck und einer gestärkten Wettbewerbsposition 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 etc. 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 Sie abgesehen hat, zur Verfügung? Ist Ihre Infrastruktur bereits gefährdet?

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

Das Modul wurde auf der Grundlage von OSINT-Techniken in Kombination mit automatisierten und manuellen Analysen des öffentlichen Internets, Deep Web und Dark Web entwickelt. Zusammen mit der internen Kaspersky-Wissensdatenbank bieten die daraus resultierenden maßgeschneiderten Berichte praktisch umsetzbare Einblicke und Handlungsempfehlungen, mit denen Sie die Zahl der potentiellen Angriffsvektoren und das Risiko einer digitalen Gefährdung minimieren können. Dazu zählen:

- Netzwerkperimeter-Bestandsaufnahme ohne Störung des laufenden Betriebs, um zu ermitteln, welche kundenseitigen Netzwerkressourcen und offen zugänglichen Services potentielle Angriffspunkte bieten. Dazu gehören unter anderem versehentlich im Perimeter belassene Management Interfaces 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, sozialen Netzwerken, 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.

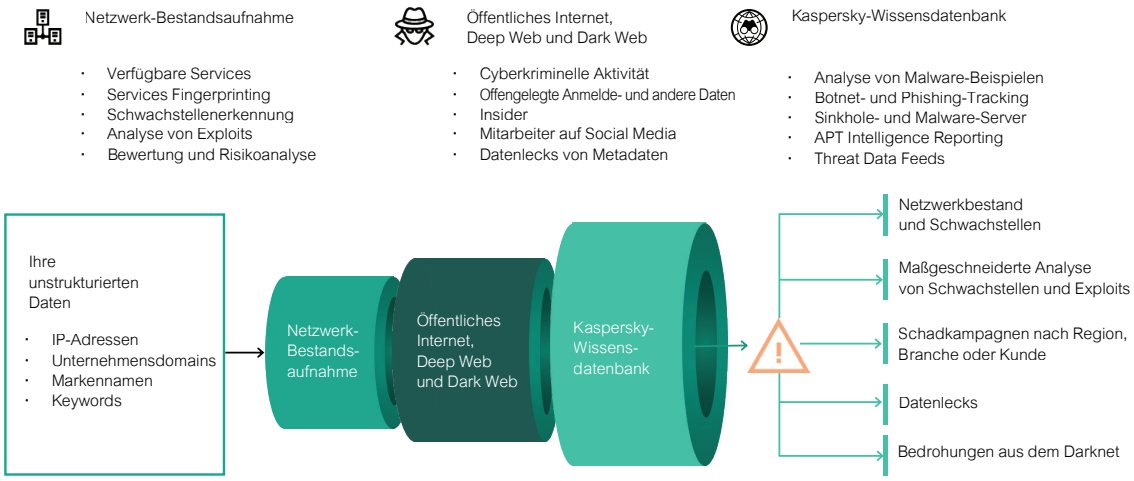
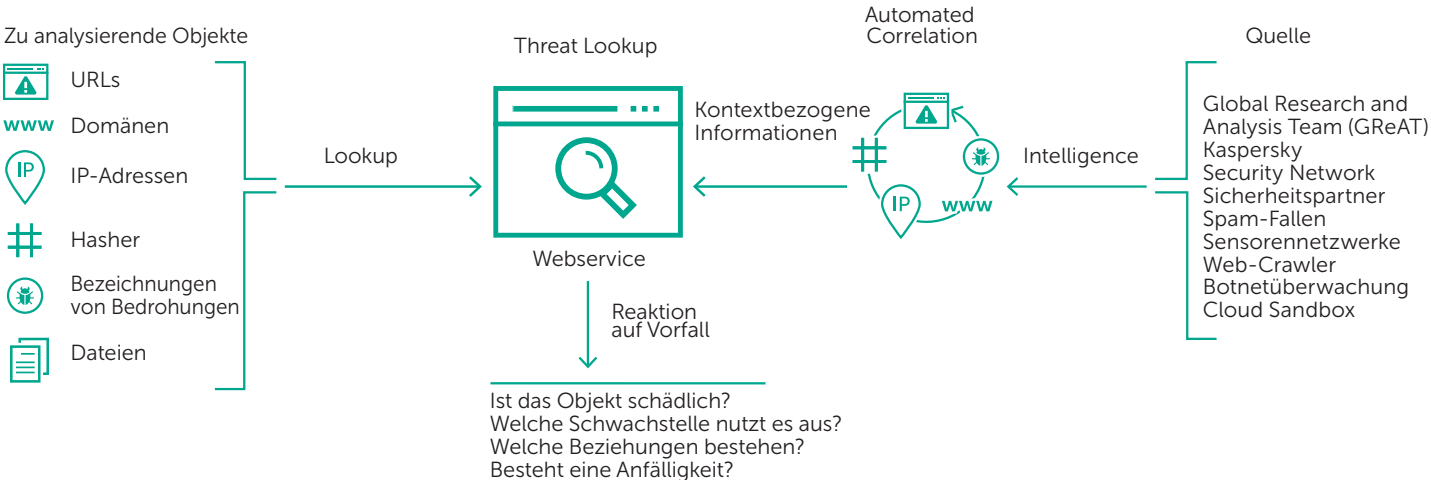


Abbildung 1. Kaspersky Digital Footprint Intelligence

Schneller Einstieg – einfache Anwendung – keine Ressourcen erforderlich

Kaspersky Digital Footprint Intelligence hat keinerlei Auswirkungen auf die Integrität und Verfügbarkeit Ihrer Netzwerkressourcen und -services. Die Berichte werden im Kaspersky Threat Intelligence Portal bereitgestellt, wo wir alle Bedrohungsdaten aus mehr als 20 Jahren gesammelt haben. Darüber hinaus werden Sie sofort benachrichtigt, sobald neue Informationen zur Verfügung stehen. Per API lässt sich Kaspersky Digital Footprint Intelligence auch in die Task Management-Systeme von Drittanbietern integrieren, was den zur Workflow-Verwaltung erforderlichen zeitlichen Aufwand erheblich reduziert.

Threat Lookup



Service-Highlights

- **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 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.
- **Sandbox-Analyse:** Dabei werden unbekannte Bedrohungen durch die Ausführung von verdächtigen Objekten in einer abgesicherten Umgebung erkannt sowie das gesamte Bedrohungsverhalten mitsamt der Artefakte in leicht verständlichen Berichten überprüft.
- **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, um alle Vorteile von Bedrohungsinformationen nutzen zu können, betriebliche Workflows zu automatisieren oder eine Integration in bestehende Sicherheitskontrollen, z. B. SIEMs, zu ermöglichen.
- **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.

Cyberkriminalität entwickelt sich mit dem technologischen Fortschritt und kennt heute 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.

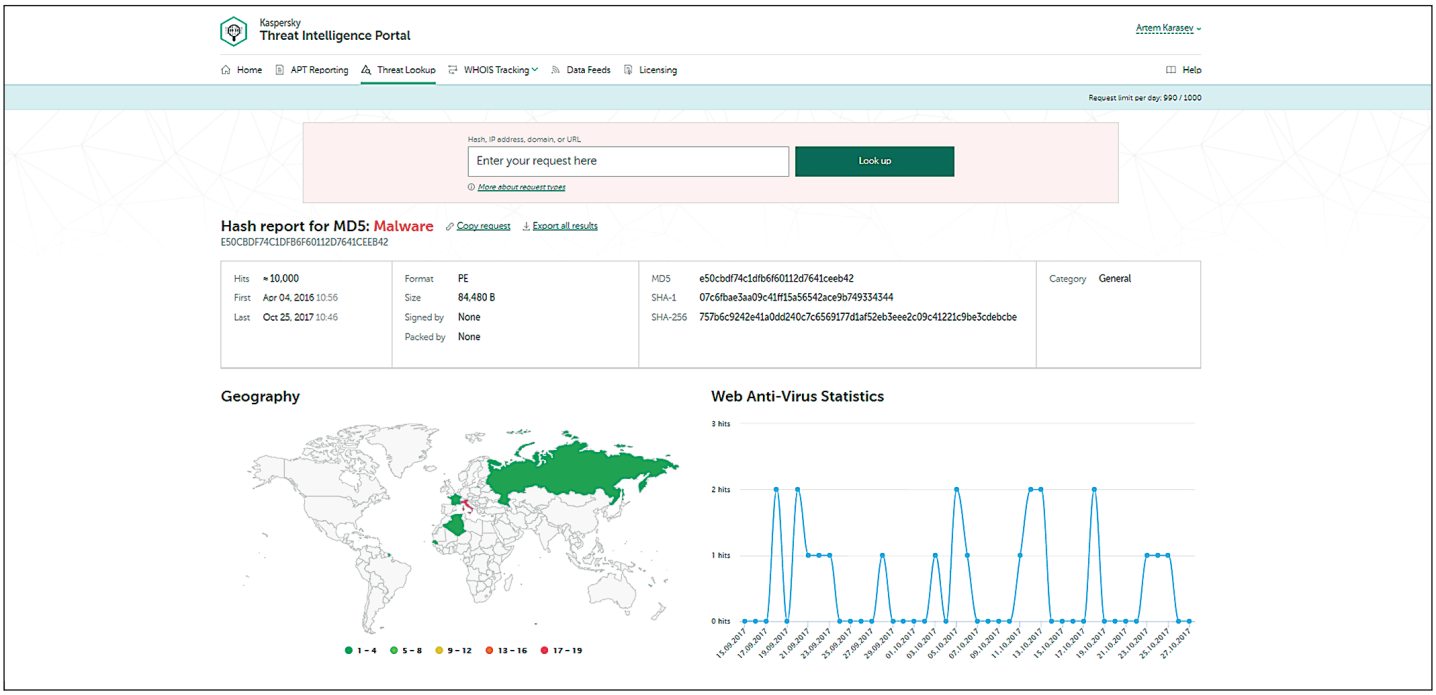
Kaspersky Threat Lookup bietet unser gesamtes Wissen über Cyberbedrohungen und ihre Verflechtungen in einem einzigen, leistungsstarken Webservice. Das Ziel ist es, Sie und Ihre Sicherheitsteams mit so vielen Informationen wie möglich zu versorgen, damit Cyberangriffe schon im Vorfeld abgewendet werden 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.

Die durch KasperskyThreat Lookup erhaltene Threat Intelligence wird von einer sehr fehlertoleranten Infrastruktur in Echtzeit überwacht so dass die dauerhafte Verfügbarkeit und einheitliche Leistung sichergestellt sind. Hunderte von Experten, darunter Sicherheitsanalysten aus der ganzen Welt, international anerkannte Sicherheitsexperten aus unserem GReAT-Team und führende Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung von wertvollen und praxisnahen Bedrohungsinformationen bei.

Hauptvorteile

- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen**, indem Sie Ihren Sicherheits-/SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe von gezielten Angriffen bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit und unterbrechen Sie die Kill Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- **Führen Sie anhand hochzuverlässiger Bedrohungskontexte detaillierte Suchabfragen innerhalb der Bedrohungsindikatoren aus**, z. B. in IP-Adressen, URLs, Domänenoder Datei-Hashes, um Angriffe zu priorisieren, Entscheidungen über Personal- und Ressourcenzuteilungen zu verbessern und sich auf die Abwehr derjenigen Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen.
- **Wehren Sie gezielte Angriffe ab.** Verbessern Sie mithilfe taktischer und strategischer Bedrohungsinformationen Ihre Sicherheitsinfrastruktur, indem Sie die richtigen Verteidigungsstrategien einsetzen.

1 http://www.kaspersky.com/top3



Jetzt können Sie...

- Über eine webbasierte Benutzeroberfläche oder die RESTful-API nach Bedrohungsindikatoren suchen.
- Nachvollziehen, warum ein Objekt als schädlich eingestuft wird.
- Überprüfen, ob ein entdecktes Objekt weit verbreitet ist oder nur vereinzelt vorkommt.
- Zusätzliche Details überprüfen, darunter Zertifikate, häufig genutzte Bezeichnungen, Dateipfade oder zugehörige URLs, um neue verdächtige Objekte zu ermitteln.

Dies sind nur einige Beispiele. Es gibt noch eine Vielzahl weiterer Möglichkeiten, diese relevanten und fein abgestuften Sicherheitsinformationen zu nutzen.

Kenne deine Feinde und deine Freunde. Erkennen Sie nachgewiesen unschädliche Dateien, URLs und IP-Adressen und beschleunigen Sie den Untersuchungsvorgang. Wenn jede Sekunde zählt, sollten Sie keine Zeit mit der Analyse von vertrauenswürdigen Objekten verlieren.

Unser Ziel ist es, alle Arten von Cyberbedrohungen abzuwehren und die digitale Welt unserer Kunden sicherer zu machen. Um das zu erreichen und die Nutzung des Internets sicher zu machen, müssen Bedrohungsinformationen in Echtzeit weitergegeben und verwendet werden können. Ein zeitnaher Zugriff auf Informationen ist für einen effektiven Schutz Ihrer Daten und Netzwerke unerlässlich. Jetzt können Sie mit Kaspersky Threat Lookup effizienter und einfacher denn je auf diese Daten zugreifen.

Hauptfunktionen:

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

Hauptvorteile:

- Fortschrittliche Erkennung von APTs, gezielten und komplexen Bedrohungen
- Ein Workflow, der die Durchführung hocheffektiver und komplexer Vorfallsuntersuchungen ermöglicht
- Skalierbarkeit, ohne dass Sie kostspielige Hardware erwerben oder viele Systemressourcen einsetzen müssen
- Nahtlose Integration und Automatisierung Ihrer Sicherheitsabläufe

Cloud Sandbox

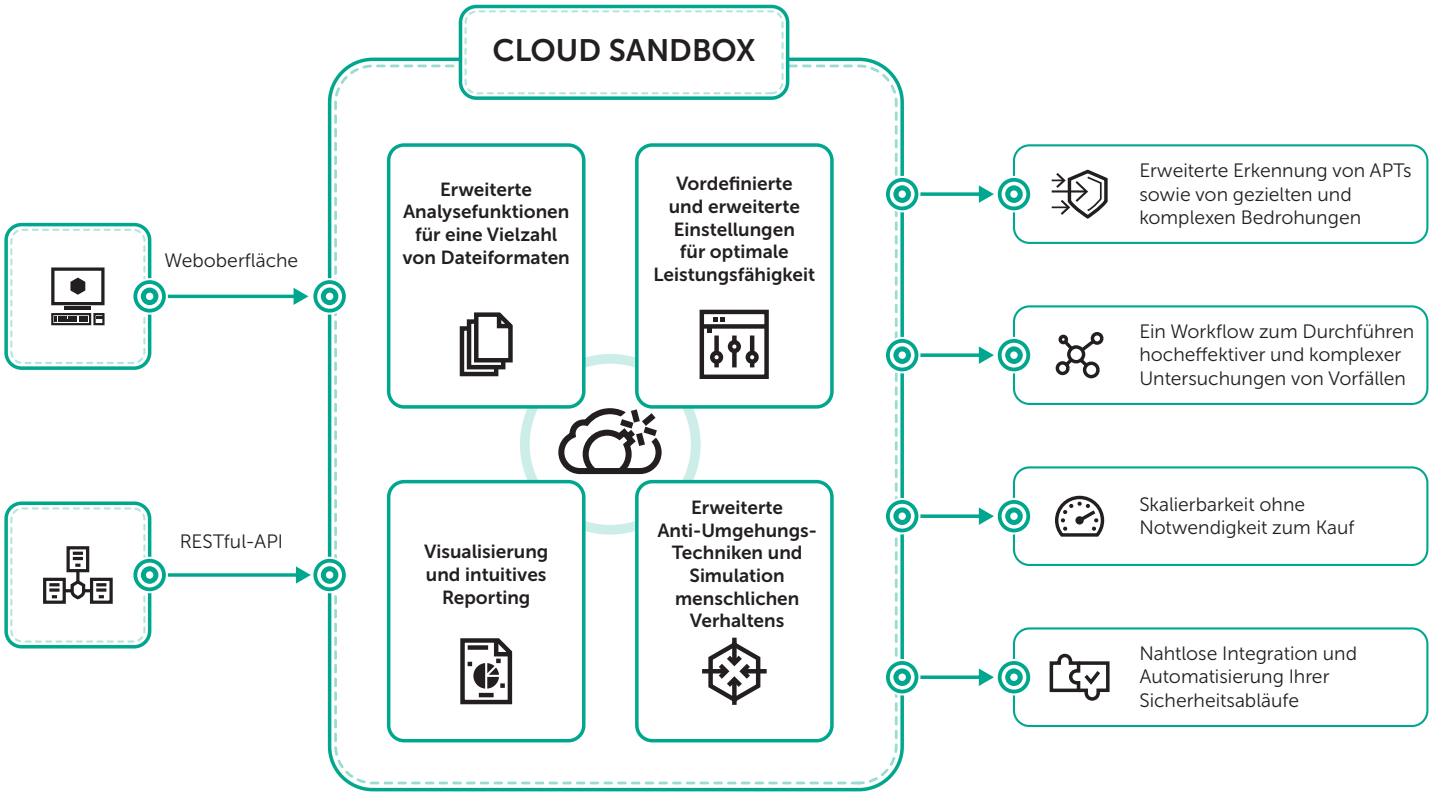
Herkömmliche Antiviren-Tools reichen heutzutage nicht mehr aus, um gezielte Angriffe zu verhindern. Virenschutz-Engines können nur bekannte Bedrohungen in verschiedenen Varianten abwehren. Versierte Bedrohungsakteure nutzen jedoch alle ihnen zur Verfügung stehenden Mittel, um eine automatische Erkennung 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 ausgeklügelte, gezielte und maßgeschneiderte Bedrohungen von heute 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.

Proaktive Abwehr von Bedrohungen, die Sicherheitsbarrieren umgehen

Heutzutage kommt bei Malware eine Vielzahl von Methoden zum Einsatz, um die Ausführung des eigenen Codes zu vermeiden, wenn dies zur Aufdeckung der schädlichen Aktivität führen könnte. 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 Ergebnis ist eine optimale Umgebung für die Erkennung unbekannter Bedrohungen.



Dieser Service geht unmittelbar aus unserem hauseigenen Sandboxing-Komplex hervor, den wir seit über 10 Jahren stetig weiterentwickeln. Diese Technologie beinhaltet das gesamte Wissen über das Malware-Verhalten, das wir uns während 20 Jahren kontinuierlicher Bedrohungsforschung angeeignet haben. So können wir täglich über 350.000 neue schädliche Objekte erkennen und branchenführende Sicherheitslösungen für unsere Kunden bereitstellen.

Kaspersky Cloud Sandbox ist Teil des Kaspersky Threat Intelligence Portal und ergänzt Ihren Threat Intelligence Workflow. 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 ausfallen, insbesondere bei mehrstufigen Angriffen. Kaspersky Cloud Sandbox ist ein ideales Tool zur Beschleunigung der Reaktion auf Zwischenfälle sowie forensische Aktivitäten. So profitieren Sie von Skalierbarkeit für die automatische Verarbeitung von Dateien, ohne kostspielige Hardware zu erwerben oder sich Gedanken über Systemressourcen zu machen.

Was Sie in den Berichten erhalten

- **Zusammenfassung**
  - Bewertung der {Dringlichkeit der Bedrohung} / {Schwere der Schwachstelle}
  - Beschreibung der Bedrohung/ Schwachstelle
  - Timeline
  - Verbreitung in Regionen, Ländern, Branchen
  - Empfehlungen zur Risikominderung
- **Detaillierte Beschreibung der Analyseergebnisse**
- **Für Berichte zu Bedrohungen:**
  - Angriffsmethoden
  - Verwendete Exploits (falls zutreffend)
  - Beschreibung(en) der Malware
  - Beschreibungen der C&C-Infrastruktur und Protokolle
  - Opferanalyse
  - Analyse der Daten-Exfiltration
  - Zuordnung
- **Für Berichte zu Schwachstellen:**
  - Öffentliche Verfügbarkeit von Exploits
  - Anzeichen für eine Ausnutzung in realen Angriffen
  - Für die Ermittlung der Schwachstelle verwendete Methodik
  - Technische Analyse der Sicherheitsvorfälle, die die Ausnutzung der Schwachstelle ermöglicht haben
  - Mögliche Angriffsvektoren (möglicherweise in Verbindung mit anderen Schwachstellen und Sicherheitslücken)
  - Bewertung von betroffenen Produkten/ Produktversionen
  - Schätzungen der Verbreitung anfälliger Produkte in Regionen/Ländern/Branchen
- **Fazit**
- **Appendix**
  Technische Analyse, wichtige IOCs und alle weiteren relevanten Informationen

Industrial Control Systems (ICS) Threat Intelligence Reporting

Der **Kaspersky ICS Threat Intelligence Reporting Service** liefert dem Kunden 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.

Berichtsarten, die Sie mit dem Abonnement erhalten

1. **APT-Berichte.** Berichte zu neuen APT- und umfangreichen Angriffskampagnen mit Ausrichtung auf Unternehmen sowie Updates zu aktiven Bedrohungen.
2. **Bedrohungslage.** 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 durchdachte und praktisch umsetzbare Empfehlungen von Kaspersky-Experten, um Schwachstellen in Ihrer Infrastruktur zu ermitteln und zu mindern.

Wofür Sie Threat Intelligence-Daten einsetzen können

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.

Gleichen Sie schädliche und verdächtige Aktivitäten, die Sie in Branchenumgebungen ermitteln, mit den Recherche-Ergebnissen von Kaspersky ab, um Ihre Feststellung den gemeldeten schädlichen Kampagnen zuzuordnen, ermitteln Sie Bedrohungen und reagieren Sie unverzüglich auf Vorfälle.

Führen Sie ein Vulnerability Assessment Ihrer Branchenumgebung 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.

Nutzen Sie Informationen zu Angriffstechnologien, Taktiken und Verfahren, kürzlich entdeckten Schwachstellen und anderen wichtigen Veränderungen der Bedrohungslandschaft, die von uns gemeldet wurden, um:

- die Risiken, die von den berichteten Bedrohungen und anderen ähnlichen Bedrohungen ausgehen, zu ermitteln und zu bewerten;
- Änderungen der Branchen-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;
- informierte strategische Entscheidungen zu treffen, um in Cybersicherheit zu investieren und die Resilienz der Betriebsabläufe sicherzustellen.

Servicevorteile

Exklusiv

- **Einblick in nicht öffentliche Informationen:** als Experte für Cybersicherheit erhalten Sie Informationen, die für die Planung und Durchführung von Aktivitäten im Rahmen der Cybersicherheit wichtig sein können, die aber aufgrund der anwendbaren Offenlegungsrichtlinien nicht öffentlich zur Verfügung stehen.
- **Einfacher Zugang zu technischen Informationen zu Bedrohungen** während die Recherche und Untersuchung noch im Gange sind und bevor die Informationen veröffentlicht werden.
- **Exklusiver Zugang zu Informationen**, die möglicherweise niemals veröffentlicht werden, da sie arglistige Akteure missbräuchlich verwenden könnten (umfasst keine Software, die ausschließlich an Verkäufer zur Demonstration von Schwachstellen versandt wurde).

Nutzbar

- **Frühzeitige Reaktion auf entstehende Bedrohungen:** mit den bereitgestellten Informationen und Tools können Sie schnell auf neue Bedrohungen und Schwachstellen reagieren, um die Risiken zu mindern, die mit fortschrittlichen Bedrohungen verbunden sind und mit denjenigen, die bekannte Vektoren verwenden.
- Technische Informationen für ICS-Cybersicherheits-Maßnahmen: das Abonnement umfasst einen **Zugang zu technischen Artefakten**, wie Indicators of Compromise (IOCs), die in die automatisierten Tools des Kunden integriert und zur Unterstützung des Vulnerability Assessment, der Vorfallerkennung, der Reaktion wie auch von Untersuchungsaktivitäten integriert werden können.

Vollständig

- **Retrospektive Analyse:** Zugang zu allen zuvor veröffentlichten privaten Berichten während des Abonnementzeitraums.
- **Kontinuierliche Überwachung schädlicher Kampagnen:** Zugang zu praktisch umsetzbaren Informationen während einer Untersuchung und Updates zu neuen Feststellungen, einschließlich TTP-Änderungen und IOCs neuer ermittelter Toolsets.

Einfache Verwendung

- **Automatisierung:** Berichtsinformationen können automatisch analysiert und in automatisierte Prozesse zur Cybersicherheit integriert werden.
- **Unterstützung für mehrere Branchenstandards:** IOCs werden in branchengängigen Formaten bereitgestellt, wie OpenIOC, STIX, YARA und SNORT-Regeln.

Testen Sie unseren Service

Sie können einen **Demo-Zugang** zum Kaspersky ICS Threat Intelligence Reporting unter folgender Adresse anfordern: **https://tip.kaspersky.com**. Die Demo-Version enthält **rund 10 Beispielberichte**, die Daten zu Angriffen auf Branchenunternehmen, die Ergebnisse der Untersuchung von Schwachstellen in Branchenlösungen wie auch Informationen zur Bedrohungslandschaft angesichts industrieller Automatisierungssysteme enthalten.

Weitere Informationen erhalten Sie unter **ics-cert-query@kaspersky.com**.

Cyber Threats News: https://de.securelist.com/
IT Security News: business.kaspersky.de/

www.kaspersky.de

kaspersky BRING ON THE FUTURE