Bleiben Sie den Angreifern immer einen Schritt voraus

Kaspersky Threat Intelligence

kaspersky bring on the future

Kaspersky
Threat Intelligence

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 uns zum vertrauenswürdigen Partner angesehener internationaler Strafverfolgungs- und Regierungsbehörden, darunter Interpol und CERTs, gemacht. Mit Kaspersky Threat Intelligence erhalten Sie einen direkten Zugang zu taktischer, operativer und strategischer Bedrohungsanalyse.

Kaspersky Threat Intelligence bietet einen umfassenden Überblick über die globale Bedrohungslandschaft durch die Kombination von Threat Intelligence-Daten, Bedrohungsdaten-Feeds sowie eigenen Untersuchungen, die alle von unserem Expertenteam analysiert werden, um Unternehmen im Kampf gegen Cyberbedrohungen zu unterstützen.

Taktisch

Kurzfristige Informationen mit niedriger Priorität zur Unterstützung von Sicherheitssystemen und der Reaktion auf Vorfälle. Ein Beispiel für taktische Threat Intelligence sind IoCs im Zusammenhang mit dem Verhalten eines kürzlich erst erkannten Angriffs.

Rollen:
- SOC-Analyst

Systeme:
- SIEM
- NGFW
- IPS
- IDS
- SOAR

Prozesse:
- Threat Hunting
- Monitoring

Operativ

Zu dieser Ebene gehören in der Regel Daten zu Kampagnen und übergeordnete TTPs. Kann Informationen zur Zuordnung zu bestimmten Akteuren sowie Fähigkeiten und gegnerischen Absichten enthalten.

Rollen:
- SOC L3-Analyst
- DFIR-Analyst
- IR-Analyst

Systeme:
- SIEM
- NTA
- EDR/XDR
- TIP

Prozesse:
- Incident Response
- Threat Hunting

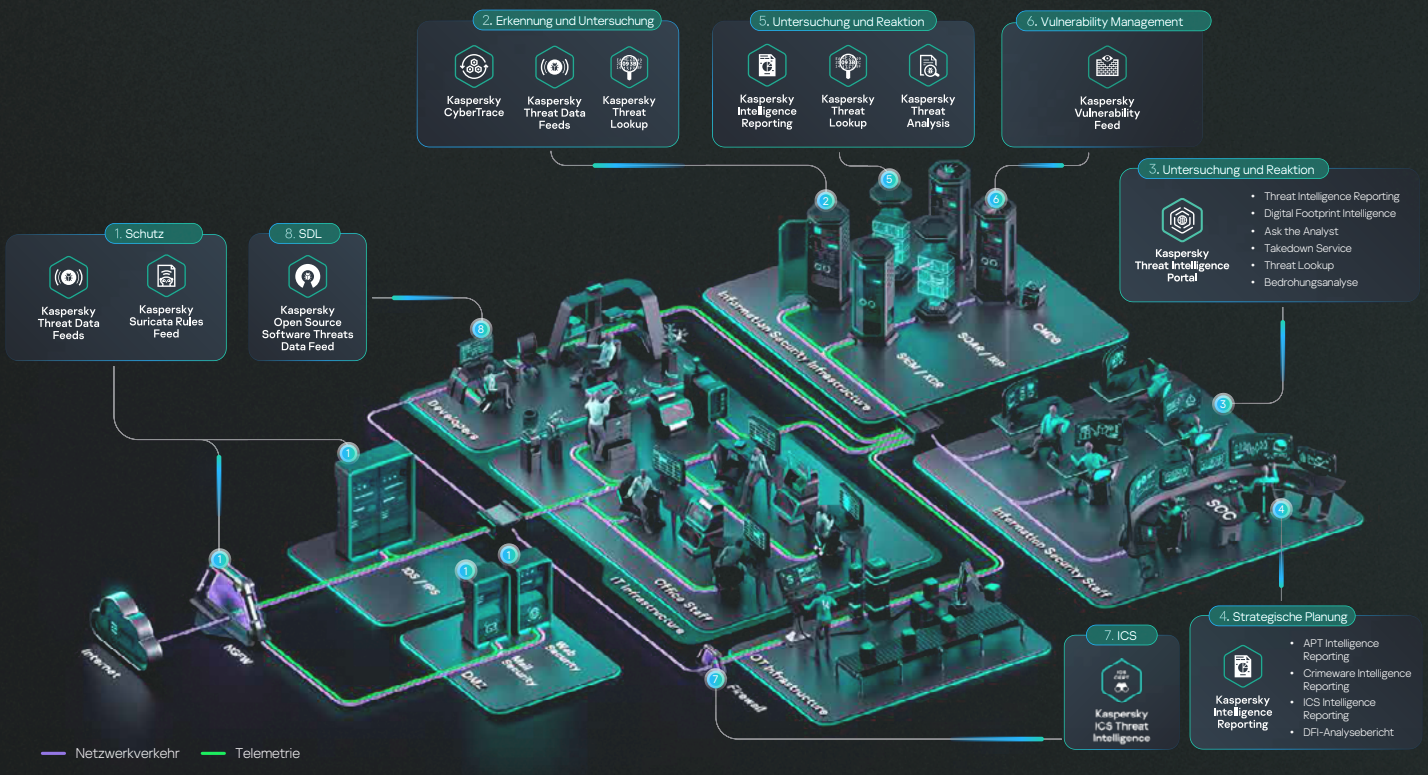
Strategisch

Auf dieser Ebene werden Vorstände und Aufsichtsräte bei wichtigen Entscheidungen zu Risikobewertung, Ressourcenverteilung und Unternehmensstrategie unterstützt. Bereitgestellt werden Trenddaten sowie Informationen zur Motivation der Akteure und deren Klassifizierung.

Rollen:
- CISO
- CTO
- CIO
- CEO

Prozesse:
- Aufbau einer IS-Strategie
- Stärkung des Bewusstseins

Kaspersky Threat Intelligence Anwendungsschema



Kaspersky Threat Intelligence gibt Ihnen die Möglichkeit,

Proaktiv Bedrohungen zu erkennen und zu verhindern

Kaspersky Threat Intelligence hält Sie über die neuesten Bedrohungen und Schwachstellen auf dem Laufenden. So können Sie proaktive Maßnahmen zum Schutz Ihrer Systeme ergreifen, bevor ein Angriff erfolgt.

Ihren digitalen Fußabdruck zu verstehen

Kaspersky Threat Intelligence bietet einen umfassenden Überblick über Ihren digitalen Fußabdruck, einschließlich aller Ressourcen, die für Angriffe oder Kompromittierung anfällig sein könnten.

Ihre Fähigkeiten zur Bedrohungserkennung zu erweitern

Kaspersky Threat Intelligence unterstützt Sie dabei, Ihre bestehenden Sicherheitslösungen mit neuesten Bedrohungsdaten zu füttern. So können Sie hochentwickelte Bedrohungen besser erkennen und abwehren.

Ihre Reaktionsfähigkeit zu verbessern

Kaspersky Threat Intelligence liefert Echtzeitdaten zu neuen Bedrohungen und Gefährdungsindikatoren, damit Sie schnell und effektiv auf Vorfälle reagieren können.

Gesetzliche Vorschriften und Normen einzuhalten

Alle Unternehmen unterliegen verschiedenen branchenspezifischen Vorschriften und Normen. Kaspersky Threat Intelligence unterstützt Sie bei der Erfüllung dieser Anforderungen.

Das firmeninterne Know-how auszubauen

Das Expertenteam von Kaspersky besteht aus den erfahrensten und angesehensten Forschern der Branche und stellt Ihren IT-Sicherheitsteams eine Fülle von Wissen und Expertise zur Verfügung.

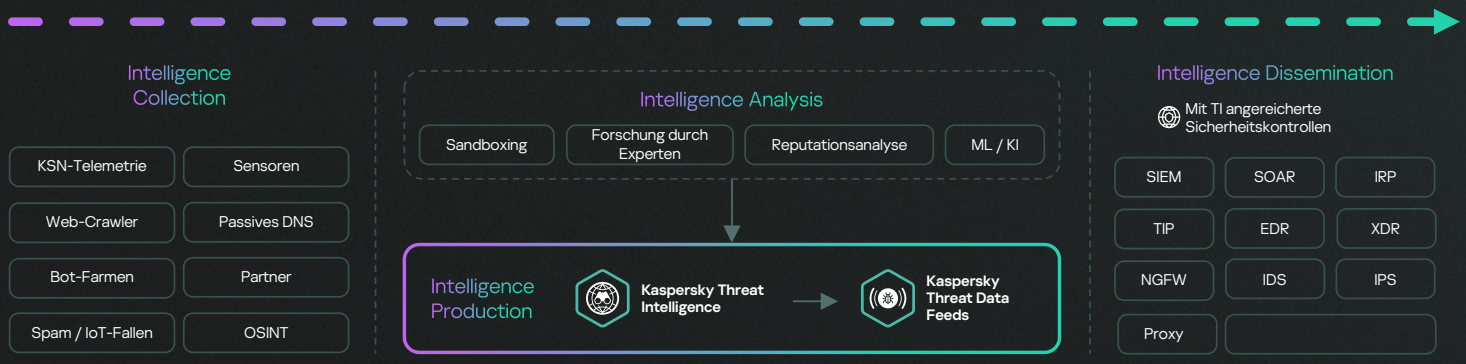
Kaspersky
Threat Data
Feeds

Kaspersky Threat Data Feeds

Cyberangriffe gibt es jeden Tag. Cyberbedrohungen werden immer häufiger, komplexer und schwerer erkennbar und versuchen, Ihre Abwehrmaßnahmen zu untergraben. Angreifer nutzen komplizierte Kill Chains, Kampagnen und individuell angepasste Taktiken, Techniken und Prozeduren (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu unterbrechen oder Ihren Kunden zu schaden. Effektiver Schutz benötigt neue Methoden, die auf Bedrohungsinformationen basieren.

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

Kaspersky Threat Data Feed liefert Bedrohungsdaten in Echtzeit, die Sie beim Schutz Ihrer Netzwerke und Systeme vor Cyberbedrohungen unterstützen. Die Datenfeeds enthalten Informationen über bekannte Malware, Phishing-Webseiten, die neuesten Schwachstellen und Exploits sowie weitere Arten von Cyberbedrohungen – Informationen, die Ihnen helfen, schädlichen Datenverkehr zu unterbinden, Ihre Sicherheitssoftware zu aktualisieren sowie weiterführende Maßnahmen zum Schutz vor Cyberangriffen zu ergreifen.



1

Die Daten werden aus einer Vielzahl von vertrauenswürdigen Quellen bezogen. Dazu zählen das Kaspersky Security Network und unsere eigenen Crawler, der Botnet Threat Monitoring Service (verfolgt rund um die Uhr Botnets und deren Ziele), Spam-Traps, Daten von Forschungsgruppen, Partnern und vieles mehr.

2

Alle gesammelten Informationen werden in Echtzeit sorgfältig geprüft und bereinigt. Dabei kommen verschiedene Vorverarbeitungsmethoden zum Einsatz: Sandboxing, statistische und heuristische Analyse, Ähnlichkeitstools, Verhaltensprofilierung und Expertenanalyse.

3

Datenfeeds sind ein wirksames Tool für die Erfassung von Bedrohungsinformationen zu einem Warnhinweis oder Vorfall und für die Suche nach weiteren Details. Sie helfen außerdem, die Frage nach dem „Wer? Was? Wo? Warum?“ und dem Ursprung des Angriffs zu beantworten. Dies erlaubt eine schnelle Entscheidungsfindung zum Schutz Ihres Unternehmens vor Bedrohungen jeglicher Komplexität.

Kontextdaten

Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die weitere Analyse und vielfältige Nutzung der Daten. Die Einträge in den von Kaspersky bereitgestellten Feeds sind mit den folgenden Kontextdaten angereichert. So können Sie Bedrohungen schnell überprüfen und priorisieren:

1. Bedrohungsnamen
2. IP-Adressen und Domain-Namen bösartiger Web-Ressourcen
3. Hashes von schädlichen Dateien
4. Anfällige und gefährdete Objekte
5. Taktiken, Techniken und Prozeduren von Angriffen gemäß der MITRE ATT&CK-Klassifizierung
6. Zeitstempel
7. Geostandort
8. Verbreitung usw.

Vorteile von Kaspersky Threat Data Feeds

Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen,

indem Sie die Ersteinstufung automatisieren. Darüber hinaus bieten Sie den Sicherheitsanalysten so genügend Kontext, um sofort zu erkennen, welche Warnmeldungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die Incident Response-Teams weitergeleitet werden müssen.

Verstärken Sie Ihre Abwehrlösungen,

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 Fähigkeiten und die Ziele der Angreifer erkennen. Führende SIEM-Systeme (einschließlich ArcSight, IBM QRadar, MS Sentinel, Splunk usw.) und TI-Plattformen werden vollständig unterstützt.

Verhindern Sie, dass sensible Werte und geistiges Eigentum

von infizierten Rechnern gestohlen werden und nach draußen gelangen. Dank der schnellen Erkennung infizierter Assets können Sie den Ruf Ihres Unternehmens schützen, Ihren Wettbewerbsvorteil aufrechterhalten und Geschäftschancen sichern.

Bauen Sie Ihr MSSP-Geschäft aus,

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

Kaspersky CyberTrace

Angesichts der steigenden Anzahl von Threat Intelligence Feeds und verfügbaren Bedrohungsinformationen können Unternehmen nur schwer herausfinden, welche Informationen wirklich relevant sind. Gleichzeitig gibt es Bedrohungsinformationen in verschiedenen Formaten. Diese beinhalten zahlreiche Gefährdungsindikatoren (Indicators of Compromise, IoCs), die für SIEM-Systeme und andere Sicherheitskontrollen nur schwer zu verarbeiten sind.

Durch Integration aktueller maschinenlesbarer Bedrohungsinformationen in bestehende Systeme, wie z. B. SIEM-Systeme, können Security Operations Center die Ersteinstufung automatisieren. Außerdem bieten Sie den Sicherheitsanalysten so genügend Kontext, um sofort zu erkennen, welche Warnmeldungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die Incident Response-Teams weitergeleitet werden müssen.

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, anderen Anbietern, OSINT oder die eigenen Feeds Ihrer Kunden) im JSON-, STIX-, XML- oder CSV-Format integrieren und unterstützt zahlreiche SIEM-Lösungen und Protokollquellen ohne Konfigurationsaufwand.

Wichtigste Vorteile

Detaillierte Informationen zu den einzelnen Indikatoren ermöglichen es, die Analyse noch weiter zu vertiefen. 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 zu jedem Indikator hinzufügen

Anhand von Nutzungsstatistiken zur Messung der Effektivität integrierter Feeds sowie einer Feed-Überschneidungsmatrix können Sie entscheiden, welche Threat Intelligence-Quellen am zuverlässigsten sind.

Versehen Sie Gefährdungsindikatoren (IoCs) mit Tags, um ihre Verwaltung zu vereinfachen. Erstellen Sie einen beliebigen Tag, legen Sie seine Gewichtung (Wichtigkeit) fest und versehen Sie dann IoCs manuell mit dem Tag. Sie können IoCs auch basierend auf diesen Tags und deren Gewichtung sortieren und filtern.

Mit einem Research Graph können Sie in CyberTrace gespeicherte Daten und erkannte Ereignisse visuell untersuchen und Gemeinsamkeiten von Bedrohungen erkennen.

Über eine Exportfunktion können Indikatorensätze in Sicherheitssysteme wie Richtlinienlisten (Blocklisten) eingetragen werden. Außerdem können die Daten zwischen Kaspersky CyberTrace-Instanzen oder mit anderen TI-Plattformen geteilt werden.

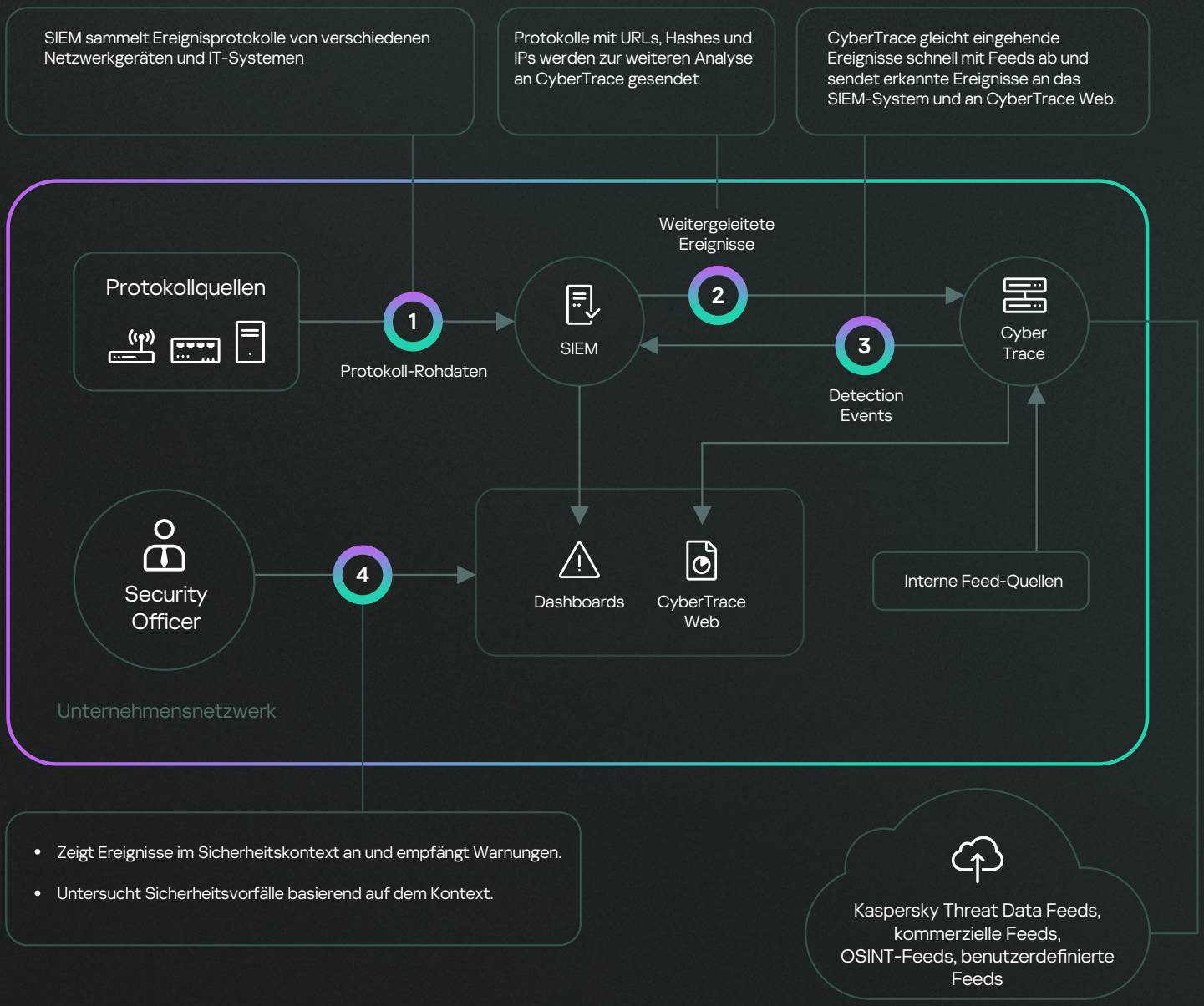
Die Korrelationsfunktion mit früheren Ereignissen (Retroscan) ermöglicht die Analyse von Phänomenen, die bei früher untersuchten Ereignissen beobachtet wurden, mit den neuesten Feeds, um bisher unerkannte Bedrohungen zu erkennen.

Mehrmandantenfähigkeit bietet Vorteile für MSSPs und für die Anwendung in großen Unternehmen.

Sendet erkannte Ereignisse an SIEM-Lösungen und entlastet nicht nur das SIEM sondern auch die Analysten

Mit der HTTP Rest-API können Sie Bedrohungsdaten abrufen und verwalten.

Funktionsweise



Kaspersky CyberTrace analysiert eingehende Protokolle und Ereignisse, gleicht die entsprechenden Daten schnell mit Feeds ab und erstellt bei Bedrohungen eigene Sicherheitswarnungen, was die SIEM-Arbeitslast erheblich reduziert.

Vorteile einer Kombination aus CyberTrace und Kaspersky Threat Data Feeds

Effektive Analyse und Priorisierung einer großen Anzahl von Sicherheitswarnungen

Verbesserung und Beschleunigung der Auswahl und Erstreaktion

Aufbau einer vorausschauenden und informationsbasierten Abwehr

Geschäftskritische Alarme werden sofort sichtbar und können an die IR-Teams eskaliert werden

Kaspersky
Threat Lookup

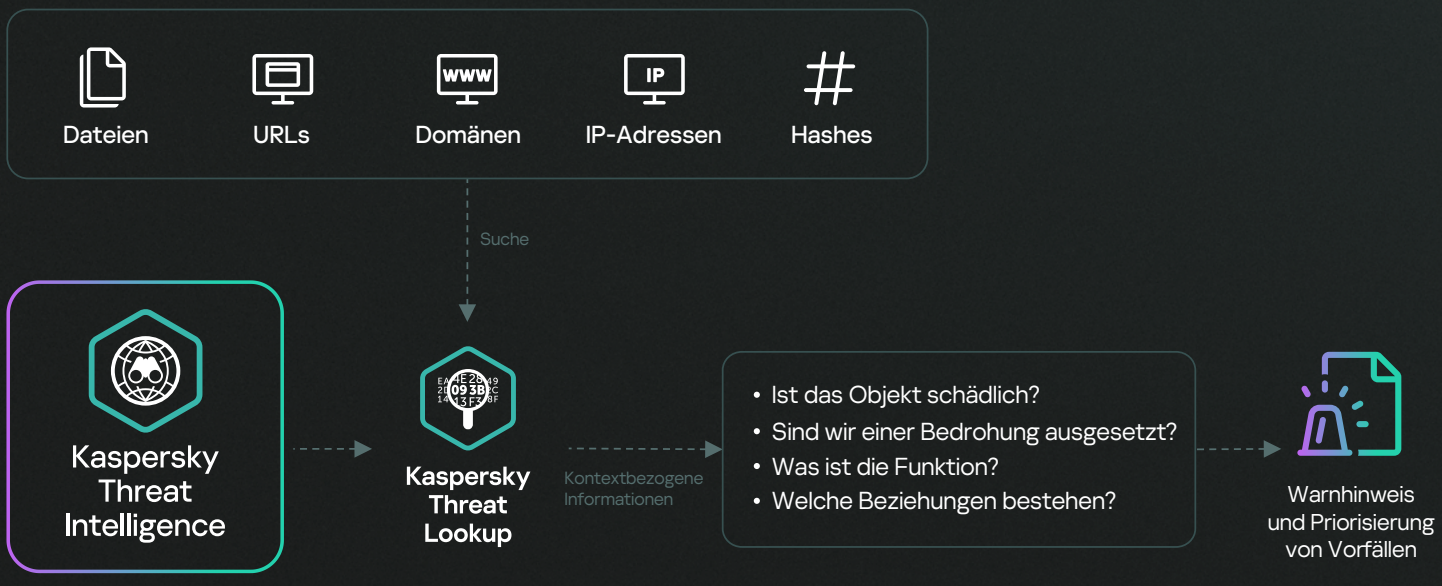
Kaspersky Threat Lookup

Cyberkriminalität kennt keine Grenzen und entwickelt sich rasant. Cyberangriffe werden immer raffinierter und Cyberkriminelle setzen für ihre Angriffe zunehmend Ressourcen aus dem Dark Web ein. Cyberbedrohungen werden immer häufiger, komplexer und schwerer erkennbar und versuchen, Ihre Abwehrmaßnahmen zu untergraben. 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 Zusammenhänge 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 zu URLs, Domänen, IP-Adressen, Hash-Werten, Namen von Bedrohungen, Statistik-/Verhaltensdaten, WHOIS/DNS-Daten, Dateiattributen, geographischen Standortdaten, Download-Ketten, Zeitstempel etc. ab. Im Ergebnis erhalten Sie eine weltweite Übersicht über neue und sich entwickelnde Bedrohungen. So können Sie Ihre Organisation schützen und die Vorfallsreaktion beschleunigen.

Funktionsweise

Zu analysierende Objekte



Wichtigste Vorteile

Zuverlässige Informationen

Ein zentraler Bestandteil von Kaspersky Threat Lookup sind unsere zuverlässigen Bedrohungsinformationen, die durch praktisch umsetzbaren Kontext ergänzt werden. Kaspersky-Produkte führen bei Anti-Malware-Tests. Die hohen Erkennungsraten in Kombination mit einer False-Positive-Rate, die praktisch gegen Null geht, beweisen 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 kann sie anrichten, umso schneller können Sie Gegenmaßnahmen ergreifen und umso eher kann sich der Netzwerkbetrieb normalisieren.

Einfache Verwendung

Webschnittstelle oder RESTful API-Zugang. Sie haben die Wahl: Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über eine einfache RESTful-API zugreifen.

Breites Spektrum an Exportformaten

Exportieren Sie die Gefährdungsindikatoren (Indicators of Compromise, IoCs) oder den praktisch umsetzbaren Kontext in gängige, strukturierte und computerlesbare Formate, z. B. STIX, OpenIoC, JSON, Yara, Snort oder sogar CSV. So nutzen Sie alle Vorteile von Threat Intelligence, automatisieren betriebliche Workflows oder ermöglichen die Integration mit bestehenden Sicherheitskontrollen, z. B. SIEMs.

Vorteile von Kaspersky Threat Lookup

1

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

2

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

3

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

4

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

5

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

6

Prüfen Sie, ob das entdeckte Objekt weit verbreitet ist oder ob es sich um einen Einzelfall handelt. Verstehen Sie, warum ein Objekt als schädlich eingestuft wird.

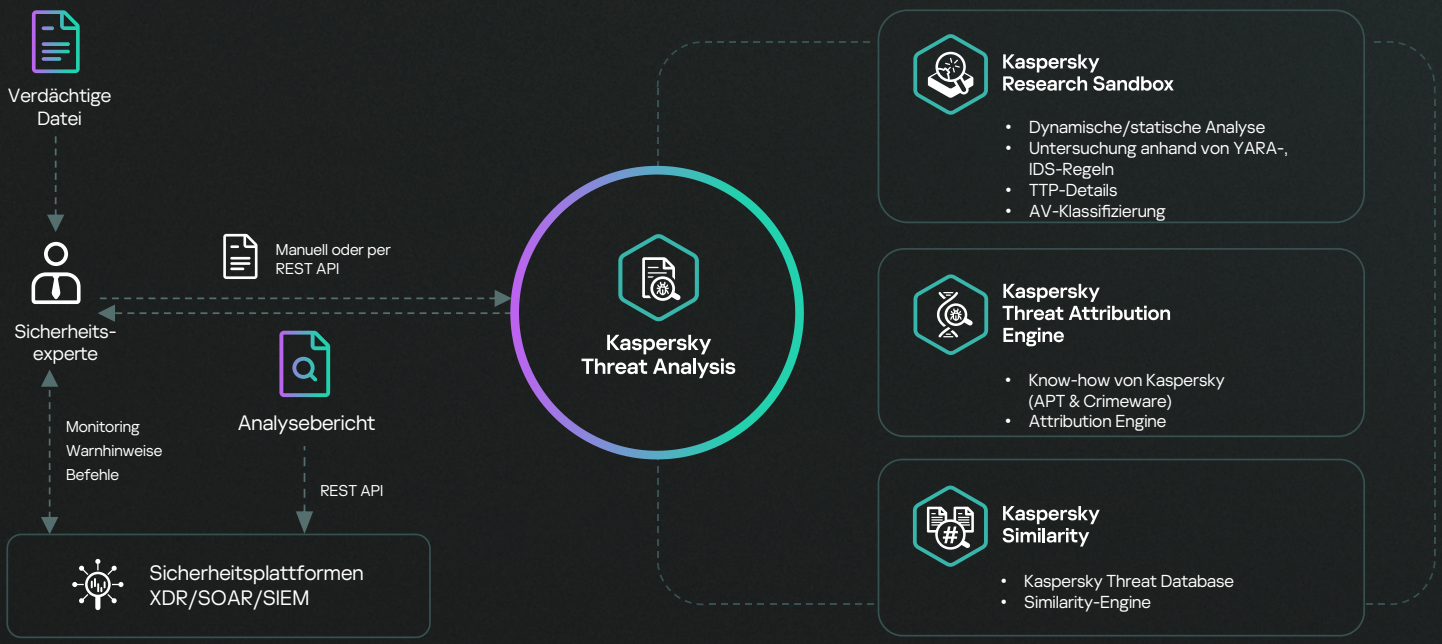
Kaspersky
Threat Analysis

Kaspersky-Bedrohungsanalyse

Wenn Sie mit einer potenziellen Cyberbedrohung konfrontiert sind, gilt es schnell und vor allem richtig zu handeln. Herkömmliche Antiviren-Tools allein reichen 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. Die Anzahl der Sicherheitswarnungen, die SOCs täglich bearbeiten müssen, wächst exponentiell. Angesichts der Vielzahl an Malware-Programmen, die jeden Tag generiert werden, ist eine effektive Priorisierung, Auswahl und Validierung der Warnhinweise nahezu unmöglich.

Damit Sicherheitsforscher über bestehende und neue Bedrohungen auf dem Laufenden bleiben, bietet Kaspersky eine zentrale, robuste Lösung, mit der sich die routinemäßige Analyse verdächtiger Dateien automatisieren lässt. Zusätzlich zu traditionellen Bedrohungsanalyse-Technologien wie Sandboxing verfügt Kaspersky Threat Analysis über hochmoderne Mapping- und Ähnlichkeitstools . Dieser hybride Ansatz ermöglicht eine effiziente Bedrohungsanalyse, damit Sie fundierte Entscheidungen treffen und Ihre Infrastruktur schützen können. Kaspersky Threat Analysis kann sowohl über eine einheitliche Web- als auch über eine RESTful-Schnittstelle bereitgestellt werden.

Komponenten von Kaspersky Threat Analysis



Kaspersky
Research Sandbox

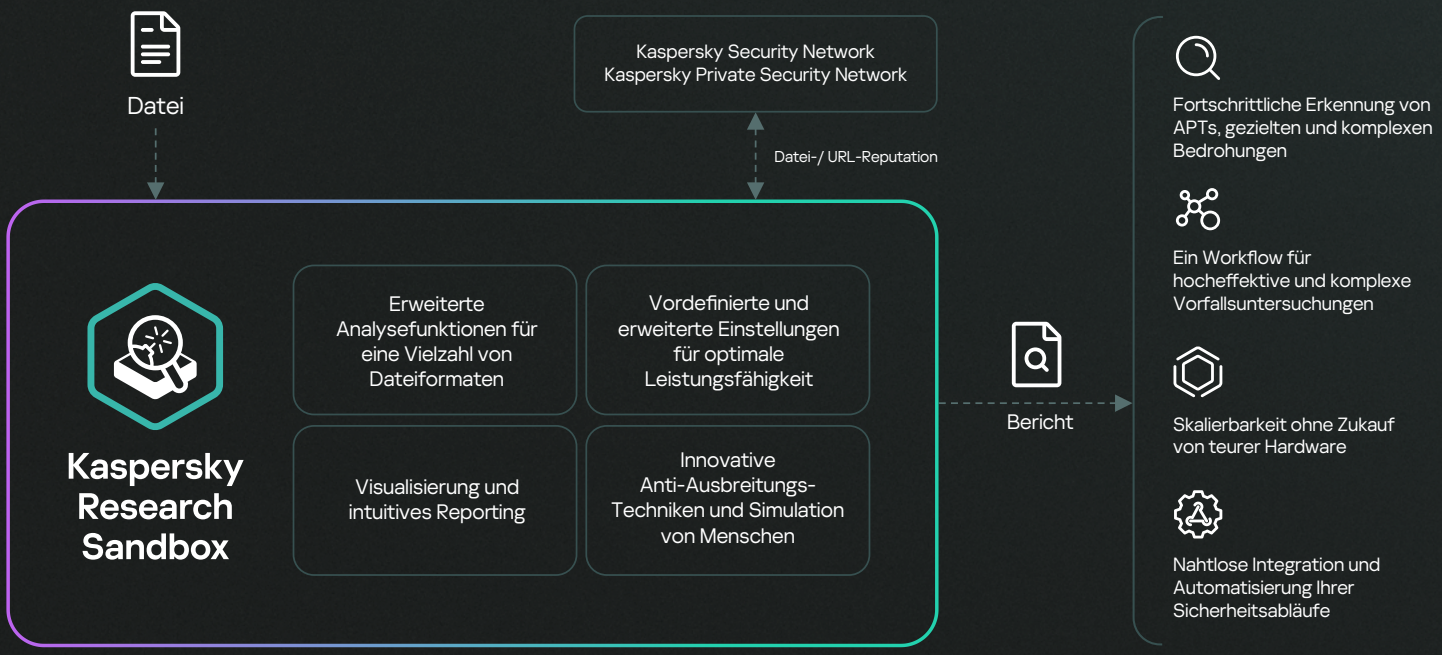
Kaspersky Research Sandbox

Die Kaspersky Research Sandbox geht unmittelbar aus unserem Sandboxing-Komplex hervor – eine Technologie, die wir seit über 20 Jahren laufend weiterentwickeln. Sie enthält das gesamte Wissen über das Verhalten von Malware, das wir im Rahmen unserer kontinuierlichen Bedrohungsforschung gesammelt haben. Täglich erkennen wir mehr als 420.000 neue schädliche Objekte.

Mit Kaspersky Research Sandbox können Sie die Herkunft von File Samples untersuchen, IoCs auf der Basis von Verhaltensanalysen sammeln und schädliche Objekte erkennen, die bislang unter dem Radar geblieben sind. In einem hybriden Ansatz werden Verhaltensanalysen und Anti-Umgehungstechniken mit Technologien zur Simulation menschlichen Verhaltens wie automatisches Klicken, Scrollen von Dokumenten und Dummy-Prozesse kombiniert.

Eine On-Prem-Bereitstellung verhindert, dass Daten außerhalb des Unternehmens offengelegt werden. Mit der lokalen Kaspersky Research Sandbox lassen sich außerdem benutzerdefinierte Ausführungsumgebungen für die Analyse erstellen und auf reale Umgebungen zuschneiden. Dies erhöht die Genauigkeit der Bedrohungserkennung und das Ermittlungstempo.

Funktionsweise



Produktvorteile im Überblick

- Patentierte Technologie
- Automatisierte Objektanalyse in Windows, Linux und Android
- Für mehr als 200 Dateitypen können Analysen durchgeführt und detaillierte Berichte erstellt werden
- 1.000+ einzigartige Bedrohungssuchen zum Auffinden und Extrahieren von Taktiken, Techniken und Verfahren (TTPs) gemäß MITRE ATT&CK
- Erweiterte Anti-Ausbreitungs-Techniken und Technologien zur Simulation menschlichen Verhaltens
- Der Bedrohungsscore, basierend auf den Metriken und Daten, die während der Ausführung der Datei gewonnen wurden, gibt den Bedrohungsgrad des analysierten Objekts an
- Mit vorkonfigurierten Suricata-Regeln lässt sich der bei der Ausführung von Dateien entstandene Netzwerkverkehr untersuchen
- Manueller Daten-Upload und eine verbesserte REST API zur Integration in automatisierte Workflows

Kaspersky
Threat Attribution
Engine

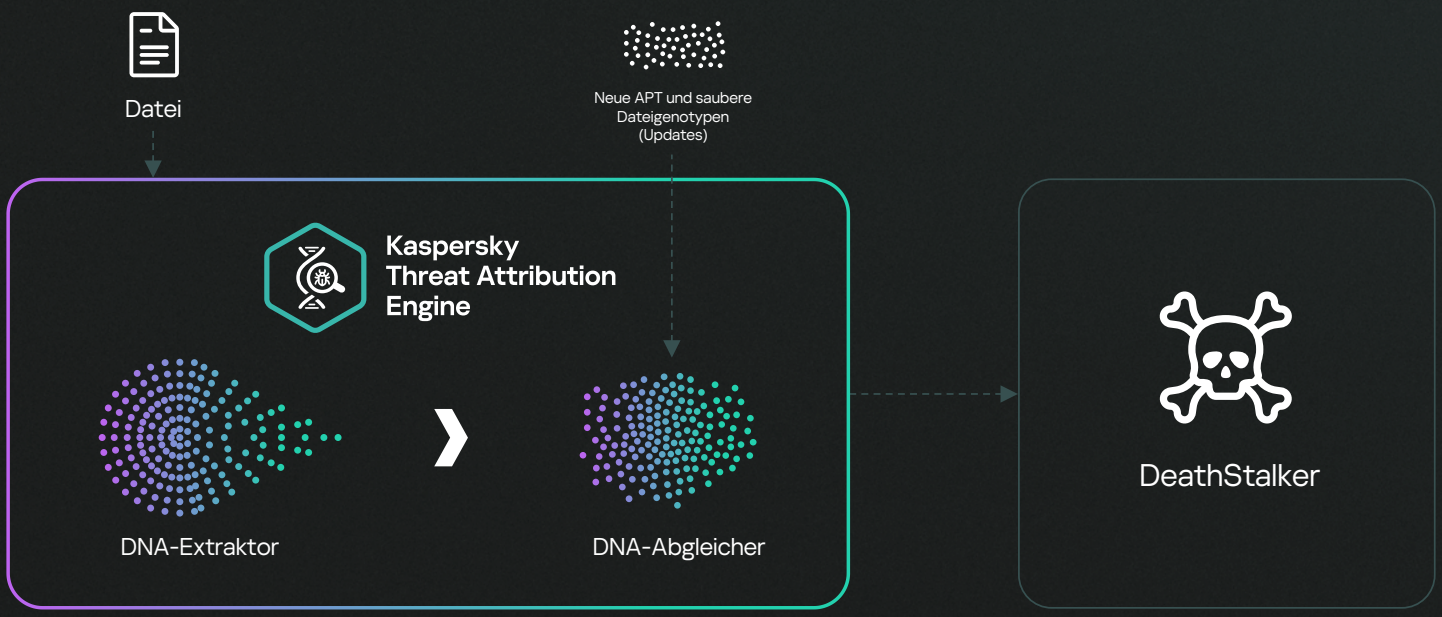
Kaspersky Threat Attribution Engine

Die Threat Attribution Engine von Kaspersky ist ein umfassendes und sehr spezifisches Malware-Analysetool, das automatisierte Einblicke in die Herkunft von Malware und deren mögliche Urheber bietet. Die Engine erkennt schnell Übereinstimmungen zwischen einer verdächtigen Datei und bekannten APT-Bedrohungen, -Akteuren und -Kampagnen. Dazu nutzt sie einen leistungsstarken Algorithmus und eine spezielle Datenbank, die APT-Malware-Samples und die branchenweit größte Sammlung sauberer Dateien enthält, die von Kaspersky-Experten in mehr als 25 Jahren gesammelt wurden.

Wir verfolgen mehr als 1100 Bedrohungsakteure und -Kampagnen und veröffentlichen mehr als 200 Threat Intelligence Reports pro Jahr. Im Rahmen unserer Bedrohungsforschung haben wir eine Sammlung von APTs mit mehr als 100.000 Dateien zusammengestellt, die in Verbindung mit automatisierten Tools eine sehr präzise Zuordnung ermöglicht.

Das Tool bietet einen einzigartigen Ansatz für den Vergleich ähnlicher Proben und gewährleistet eine Falsch-positiv-Rate von nahezu Null. Es kann neue Angriffe mit bekannter APT-Malware, vorausgehenden Angriffen und Hackern in Verbindung bringen. Das hilft Ihnen, Bedrohungen mit hohem Risiko aus der Vielzahl der weniger schwerwiegenden Vorfälle herauszufiltern. So können Sie zeitnah Schutzmaßnahmen treffen, um Angreifer am Eindringen in Ihr System zu hindern. Die Kaspersky Threat Attribution Engine kann in sicheren, isolierten Umgebungen bereitgestellt werden, in denen Dritte nur begrenzten Zugriff auf die verarbeiteten Informationen und die übermittelten Objekte haben. Bei lokaler Implementierung stehen weitere Funktionen zur Verfügung, wie das Hinzufügen eigener Akteure und Samples. Dies erlaubt den Abgleich von Dateien mit Ihrer privaten Sammlung, sowie den Export von YARA-Regeln für die weitere automatisierte Suche nach ähnlichen Dateien in Ihrer Infrastruktur und die Integration mit Drittanbieterlösungen.

Funktionsweise



Proprietäre Suchmethode

Die Kaspersky Threat Attribution Engine verwendet eine einzigartige, proprietäre Methode, um nach ähnlichen Genotypen und Strings zwischen Dateien zu suchen. Diese Methode beinhaltet:

1

Analyse der Genetik einer Probe durch Extraktion der folgenden Elemente aus dem Code:

- Genotypen – unverwechselbare Teile des binären Codes.
- Strings – unverwechselbare Zeichenketten.

2

Automatisches Durchsuchen der analysierten Dateien nach Genotypen und Strings, die den Genotypen und Strings von APT-Proben ähnlich sind, die bereits analysiert wurden oder mit Attributionsentitäten verknüpft werden konnten.

3

Auf der Grundlage ähnlicher Genotypen und Strings, die in APT-Proben gefunden wurden, wird ein Bericht über die Herkunft der analysierten Probe, die zugehörigen Attributionsentitäten sowie alle Ähnlichkeiten zwischen dieser Probe und den bereits bekannten Beispielen für APT erstellt.

Vorteile des Produkts im Überblick:

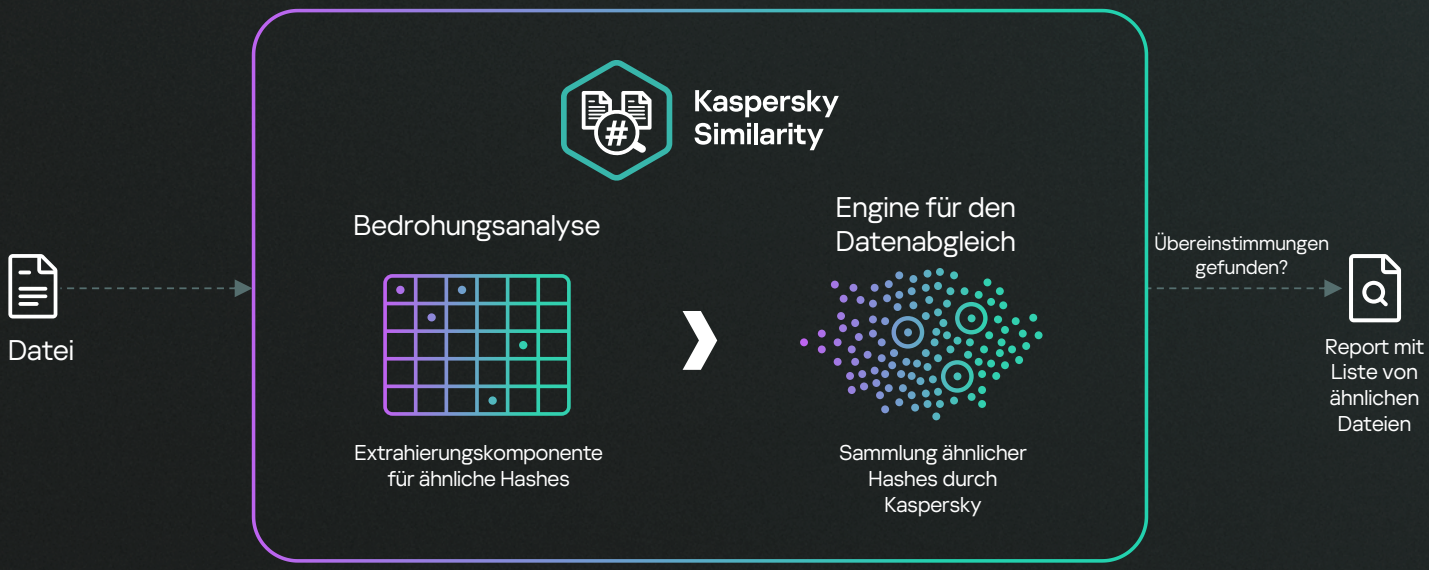
- Patentierte Technologie
- Sofortiger Zugang zu einem Repository an kuratierten Daten zu Tausenden von APT-Akteuren und -Kampagnen
- Manueller Daten-Upload und eine verbesserte REST API zur Integration in automatisierte Workflows
- Funktion zum Entpacken passwortgeschützter Archive mit benutzerdefinierten Passwörtern
- Export in das STIX 2.1-Format (TXT und JSON werden ebenfalls unterstützt) für die weitere automatische Analyse von Sicherheitsprotokollen oder für die Integration in Lösungen von Drittanbietern
- Unterstützt die Bereitstellung auf Amazon Web Services (AWS) und ermöglicht so eine schnelle Produkteinrichtung und Kosteneinsparungen, da keine Vorabinvestitionen in Hardware erforderlich sind

Kaspersky Intelligence Reporting

Kaspersky Similarity

Kaspersky Similarity ist ein praktisches Tool zur Identifizierung von Dateien mit ähnlicher Funktionalität. Das Modul basiert auf der von Kaspersky-Experten entwickelten Technologie zum Schutz vor unbekannten und versteckten Bedrohungen. Als Referenz werden mehr als 50 unterschiedliche Arten von speziellen Hashes sowie eine Datenbank mit Malware-Samples hinzugezogen, die Kaspersky im Laufe der letzten 25 Jahre gesammelt hat. Unsere Datenbank enthält Millionen von Schaddateien, um höchste Genauigkeit und Zuverlässigkeit der Ergebnisse zu gewährleisten.

Mit Kaspersky Similarity können Sie Ihre Infrastruktur nach ähnlichen (z. B. schwer zu erfassenden) Arten von Malware durchsuchen, damit eine potenzielle Gefahr auch bei geringfügiger Änderung des Angriffsmusters noch auf Ihrem Sicherheitsradar erscheint.



Similarity-Reports

Die Experten von Kaspersky haben eine Reihe von Hashes entwickelt, um anhand dieser Attribute Ähnlichkeiten zwischen verschiedenen Dateien festzustellen.

Kaspersky Similarity untersucht eine vom Nutzer vorgelegte verdächtige Datei und extrahiert die darin enthaltenen Hashes. Anschließend kann der Nutzer diese Hashes mit den Hashes von Dateien in der Kaspersky-Bedrohungsdatenbank vergleichen. Wenn Übereinstimmungen gefunden werden, wird eine Liste der Schaddateien mit der größten Ähnlichkeit erstellt, die Kaspersky bereits bekannt sind, sortiert nach dem Grad der Übereinstimmung. Der Bericht enthält außerdem zusätzlichen Kontext mit Metadaten für jede ähnliche Datei:

- Grad der Übereinstimmung
- Dateistatus (Malware, Adware oder Sonstiges)
- Bedrohungsname
- Zeitstempel der ersten und letzten Erkennung
- Anzahl der Treffer (Erkennungen)
- Datei-Hash
- Dateityp
- Dateigröße

Wichtigste Vorteile

- Patentierte Technologie
- Nutzt eine der umfangreichsten Datenbanken der Branche mit schädlichen und sauberen Dateien. Die Sammlung wurde über einen Zeitraum von mehr als 25 Jahren aufgebaut und umfasst ein sehr breites Spektrum an Vergleichsdaten.
- Manueller Daten-Upload und eine verbesserte REST API zur Integration in automatisierte Workflows
- Die Technologie wird seit langem von Kaspersky-Experten zur Erforschung neuer Bedrohungen eingesetzt, um einen noch besseren Schutz durch unsere Produkte zu bieten. Regelmäßige Spitzenwerte in unabhängigen Tests bestätigen dies:

Mehr erfahren

Vorteile von Kaspersky Threat Lookup

1

Die Kaspersky Research Sandbox unterstützt Sie bei der Reaktion auf Vorfälle und bei forensischen Aktivitäten. Sie bietet Ihnen eine hochmoderne dynamische Analyse verdächtiger Dateien mit der Fähigkeit, 0-Day-Bedrohungen zu erkennen, sowie Ergebnisse, die den MITRE ATT&ACK TTPs zugeordnet sind.

2

Dank der präzisen und zeitnahen Zuordnung durch die Kaspersky Threat Attribution Engine lassen sich passende TTPs für Bedrohungsakteure definieren, um Transparenz über den Angriffsvektor zu schaffen. Gleichzeitig erhalten Sie klare Hinweise zur bestmöglichen Schadensbegrenzung und die Reaktionszeit auf Vorfälle wird von Monaten auf Minuten verkürzt.

3

Entdecken Sie mit Kaspersky Similarity versteckte Bedrohungen und schädliche Dateien, die entwickelt wurden, um herkömmliche Anti-Malware-Technologien zu umgehen. Erkennen Sie selbst hoch entwickelte APT-Angriffe, die manchmal jahrelang unentdeckt bleiben.

Kaspersky Intelligence Reporting

Kaspersky Threat Intelligence Reporting

Die Bekämpfung moderner Cyberangriffe erfordert eine umfassende Sicht auf die von den Bedrohungsakteuren eingesetzten Taktiken, Techniken und Tools. Die für Angriffe genutzten Kontrollzentren und Tools ändern sich zwar häufig, nicht so einfach ist es aber für Angreifer, ihr Verhalten und ihre Methoden während der Durchführung von Angriffen zu ändern. Wenn diese Muster schnell identifiziert und aufgedeckt werden, können im Voraus effektive Verteidigungsmechanismen eingesetzt werden, um die Cyberkriminellen zu entwaffnen und die sogenannte Kill Chain zu unterbrechen.

Mit einem Abonnement von Kaspersky Threat Intelligence Reporting erhalten Sie kontinuierlichen und exklusiven Zugriff auf unsere Forschungsergebnisse mit aktuellen Informationen zu den gefährlichsten Bedrohungen. So können Sie und Ihr Sicherheitsteam proaktiv eine effektive Strategie entwickeln, um Angriffe frühzeitig zu erkennen und den Schaden durch ähnliche Bedrohungen zu minimieren.

Auch wenn nur ein kleiner Teil unserer Forschung öffentlich zugänglich ist, erhalten Sie mit Kaspersky Intelligence Reporting einen privilegierten Zugang zu den neuesten Entwicklungen in der Bedrohungslandschaft. Unsere Experten beobachten kontinuierlich die Aktivitäten von Cyberkriminellen und identifizieren besonders raffinierte und gefährliche zielgerichtete Angriffe, organisierte Cyberspionage, Beispiele für Malware und Verschlüsselung sowie die neuesten Trends der Cyberkriminalität weltweit.

Mehr als 200	Mehr als 300	Mehr als 500	Mehr als 2500	170.000+
private Berichte pro Jahr	Bedrohungsakteure	Kampagnen	YARA-Regeln	IoCs

Zu den analytischen Berichten gehören:

Profile von Bedrohungsakteuren

Zuordnung zu MITRE ATT&CK

Zusammenfassung (auf C-Ebene ausgerichtete Informationen)

Eingehende technische Analyse einschließlich:

- Angriffsmethoden
- Verwendete Exploits
- Beschreibung der Malware
- Beschreibungen der C&C-Infrastruktur und Protokolle
- Opferanalyse
- Analyse der Daten-Exfiltration
- Zuordnungen

Gefährdungsindikatoren (IoCs) und YARA-/SIGMA-/ Suricata-Regeln

Empfehlungen der Kaspersky-Experten

Wir bieten verschiedene Arten von Geschäftsberichten, die auf Ihren Bedarf und die Besonderheiten Ihres Unternehmens abgestimmt sind:

Kaspersky APT Intelligence Reporting

Bietet einen Einblick in hochentwickelte, zielgerichtete und langfristige Cyberbedrohungen, die häufig von gut organisierten und finanzkräftigen Gruppen ausgehen. Dieser Bericht enthält Informationen zu unterschiedlichen APT-Gruppen weltweit, deren Taktiken, Techniken und Vorgehensweisen (TTPs) und auf welche Branchen sie abzielen. Bei diesem regelmäßig erscheinenden Bericht liegt das Hauptaugenmerk auf Spionagetätigkeiten, von Angriffen auf die Lieferkette bis hin zu Hacktivismus und zerstörerischen Aktivitäten. Diese Berichte sind ideal, wenn es sich bei Ihrer Organisation um ein großes Unternehmen oder eine Regierungsbehörde handelt, bzw. wenn Sie im Bereich einer kritischen Infrastruktur tätig sind. Auch Organisationen, die sensible personenbezogene Daten speichern, für die sich andere Staaten interessieren, profitieren von diesen Informationen.

Kaspersky Crimeware Intelligence Reporting

Der Fokus liegt auf Angriffen und Kampagnen, bei denen die finanzielle Bereicherung im Vordergrund steht. Diese Berichte enthalten Informationen zu den neuesten Trends der Cyberkriminalität, wie der Handel mit gestohlenen Daten im Darknet, Finanzbetrug, Ransomware und Geldautomaten-/Kassensystem-Malware. Sie liefern Details über neue Crimeware-Varianten, Verbreitungsmethoden und die Art der Daten, auf die sie abzielen. Dieser regelmäßige Bericht ist besonders wichtig, wenn Ihr Unternehmen in großem Umfang Online-Geschäfte tätigt oder sensible Kundendaten verwaltet – wie z. B. ein Finanzinstitut oder eine E-Commerce-Plattform.

Kaspersky ICS Threat Intelligence

Bietet detaillierte Informationen und erhöht das Bewusstsein für böswillige Kampagnen, die auf Industrieunternehmen abzielen, sowie Informationen über Schwachstellen, die in den gängigsten industriellen Steuerungssystemen und den zugrunde liegenden Technologien gefunden wurden. Dieser regelmäßig erscheinende Bericht wird von Kaspersky ICS CERT erstellt, einem 2016 gegründeten Team aus über 30 hochqualifizierten Experten im Bereich der ICS-Bedrohungs- und Schwachstellenforschung, Vorfallsreaktion und Sicherheitsanalysen. Er bietet praktisch umsetzbare Erkenntnisse und Anleitungen zum Schutz Ihrer kritischen Bereiche, einschließlich Software- und Hardwarekomponenten, und gewährleistet so die Sicherheit und Verfügbarkeit Ihrer technologischen Prozesse.

In diesem Fall könnten auch die folgenden Kaspersky ICS Threat Intelligence-Dienste für Sie von Interesse sein:

Financial Threat Intelligence Reporting

Abonnieren Sie unsere regelmäßigen Veröffentlichungen zu industriellen Cybersicherheitsbedrohungen und potenziellen Schwachstellen:

- Warnhinweise zu Zero-Day-Bedrohungen
- Detaillierte technische Berichte
- Monatliche Bewertungen
- Empfehlungen zur Minimierung von Schwachstellen
- Statistiken und Trends

ICS Threat Data Feeds

Maschinenlesbare Informationsquellen über Cybersicherheitsbedrohungen in der Industrie sowie potenzielle Schwachstellen.

Einfache Formate zur Datenverteilung (JSON, CSV, OpenIOC, STIX) über HTTPS, TAXII oder spezifische Methoden der Bereitstellung zur nahtlosen Integration von Daten in Sicherheitslösungen.

Ask the Analyst

Beratung durch Kaspersky ICS CERT-Experten, die Sie individuell zu den für Sie relevanten Cybersicherheitsbedrohungen und Schwachstellen in der Industrie, statistischen Daten, Informationen zur Bedrohungslandschaft, Industriestandards usw. beraten.

Kaspersky Threat Intelligence bietet folgende Informationen:

Priorisierter Zugriff

Aus verschiedenen Gründen werden nicht alle komplexen Bedrohungen öffentlich bekannt gemacht. Diese Art von exklusiven Informationen stellen wir unseren Kunden jedoch bereits während der laufenden Forschung zur Verfügung, d.h. vor der offiziellen Veröffentlichung.

Zugriff auf technische Daten

Dazu gehört eine umfangreiche Liste von IoCs, die in Standardformaten wie OpenIoC oder STIX bereitgestellt werden, sowie Zugriff auf unsere YARA-/Sigma-/Suricata-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.

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 entsprechender Anwendungen der Sicherheitsüberwachung, Schwachstellenanalysen und die Überprüfung aktueller Schutzmaßnahmen gegen relevante TTPs.

Retrospektive Analyse

Zugriff auf alle verfügbaren privaten Berichte während der Abolaufzeit.

Unterstützung von RESTful-API

Nahtlose Integration und Automatisierung Ihrer Sicherheits-Workflows.

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

Ihr Unternehmen wächst. Gleichzeitig wird Ihre IT-Umgebung immer komplexer. Der Schutz Ihrer weit verstreuten digitalen Präsenz ohne direkte Kontrolle oder entsprechende Verantwortlichkeiten kann eine große Herausforderung darstellen. Dynamische und vernetzte Umgebungen bieten Unternehmen erhebliche Vorteile. Gleichzeitig vergrößert die zunehmende Konnektivität auch die Angriffsfläche. Die Angreifer werden immer geschickter. Deshalb ist es nicht nur wichtig, einen genauen Überblick über die Online-Präsenz Ihres Unternehmens zu haben; Sie müssen auch in der Lage sein, Änderungen zu tracken und auf externe Bedrohungen zu reagieren, die auf exponierte digitale Ressourcen abzielen.

Unternehmen setzen eine Vielzahl von Sicherheitstools ein, doch es gibt nach wie vor digitale Bedrohungen, die sehr spezifische Fähigkeiten erfordern: um Datenlecks aufzuspüren und einzudämmen, um Angriffspläne von Cyberkriminellen in Dark Web-Foren zu überwachen usw. Damit Ihre Sicherheitsanalysten Unternehmensressourcen aus dem Blickwinkel der Gegner betrachten, potentielle Angriffsvektoren schnell erkennen und Ihre Verteidigungsstrategie entsprechend ausrichten können, haben wir Kaspersky Digital Footprint Intelligence entwickelt.

Kaspersky Digital Footprint Intelligence bietet

Bedrohungserkennung

Überwachung betrügerischer Aktivitäten, die dem Ansehen eines Unternehmens schaden und/oder Kunden täuschen können.

Netzwerk-Erkundung

Identifizierung der Netzwerkressourcen des Kunden und der gefährdeten Dienste, die als Einstiegspunkt für einen Angriff missbraucht werden könnten. 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).

Dark Web Monitoring

Kontinuierliche Überwachung von Dark Web-Ressourcen (Foren, Ransomware-Blogs, Messenger, Tor-Websites usw.), um über alle Hinweise und Bedrohungen in Bezug auf Ihr Unternehmen, Ihre Kunden und Partner informiert zu sein. Analyse aller aktiven oder geplanten zielgerichteten Angriffe sowie von APT-Kampagnen, die auf Ihr Unternehmen, Ihre Branche oder Ihr Einsatzgebiet abzielen.

Erkennen von Datenlecks

Erkennung von kompromittierten Anmeldedaten, Bankkarten, Telefonnummern und anderen sensiblen Informationen von Mitarbeitern, Partnern und Kunden, die zur Durchführung eines Angriffs verwendet werden oder eine Rufschädigung für Ihr Unternehmen bedeuten könnten.

Mehrmandantenfähigkeit

Erweiterte Funktionen für Managed Security Services Provider (MSSP) und Großunternehmen mit mehreren Niederlassungen.

Informationsquellen

Es ist wichtig, dass Sie ein umfassendes Verständnis der externen Sicherheitslage Ihres Unternehmens haben. Um diese Informationen bereitzustellen, beziehen die Sicherheitsanalysten von Kaspersky Informationen aus den folgenden Quellen:

Ihre unstrukturierten Daten

- IP-Adressen
- Unternehmensdomains
- Markennamen
- Keywords
- IP-Adressbereich
- Bankleitzahlen/IIN-Kartennummern
- Arbeitnehmerinformationen

Netzwerk-Bestandsaufnahme

Suche im öffentlichen Internet, Deep Web und Dark Web

Suche in der Kaspersky-Wissensdatenbank

Bedrohungshinweise

Echtzeitsuche in den Bedrohungsinformationen von Kaspersky, im Internet und im Darkweb

Analytische Berichte*

Funktionsweise

Konfigurieren	Erfassen	Filtern	Nachrichten
Ermittlung von Informationen über die digitalen Ressourcen des Unternehmens	Automatisiertes Sammeln von Daten aus dem öffentlichen Internet, Deep Web und Dark Web sowie aus der Kaspersky-Wissensdatenbank	Von Analysten gesteuerte Erkennung, Analyse und Priorisierung von Bedrohungen	Unmittelbare Bereitstellung von Bedrohungsnachrichten im Kaspersky Threat Intelligence Portal oder über API

* Add-On-Service

Vorteile von Digital Footprint Intelligence für Unternehmen

Kaspersky Digital Footprint Intelligence bietet zahlreiche Vorteile und einen erheblichen Mehrwert für Ihr Unternehmen:

Bedrohungserkennung

Erkennen Sie potenzielle Bedrohungen in Echtzeit, um den Ruf Ihrer Marke zu schützen, das Vertrauen Ihrer Kunden zu wahren und das Risiko von finanziellen Verlusten und Schäden für den Geschäftsbetrieb zu senken.

Senken Sie die Cyberrisiken

Argumentieren Sie überzeugend gegenüber den wichtigsten Stakeholdern (CxO und Vorstand), wohin die Gelder für Cybersicherheit fließen sollten, indem Sie die Lücken im aktuellen System und die damit verbundenen Risiken aufzeigen.

Schneller reagieren

Zusätzlicher Kontext für Sicherheitswarnungen verbessert die Reaktion auf Vorfälle und verkürzt die MTTR (Mean Time To Respond).

Reduzieren Sie die Angriffsfläche

Verwalten Sie die digitale Präsenz Ihres Unternehmens und kontrollieren Sie externe Netzwerkressourcen, um Angriffsvektoren und Schwachstellen, die für Angriffe genutzt werden können, zu minimieren.

Den Gegner kennen

Vorbereitet sein, ist alles. Sie müssen wissen, was Cyberkriminelle planen und über Ihr Unternehmen im Darknet sagen.

Weiße Flecken beseitigen

Verbessern Sie Ihre Fähigkeit, Cyber-Angriffe abzuwehren und Bedrohungen zu erkennen, die über den Zuständigkeitsbereich Ihrer internen Sicherheitsteams hinausgehen.

Effizienz der Leistungserbringung

Der schnelle Einstieg und die Möglichkeit zur einfachen Skalierung im Mehrmandanten-Modus spart sowohl Managed Security Service Providern (MSSP) und deren Kunden als auch Großunternehmen mit mehreren Niederlassungen wertvolle Zeit.

Kaspersky Takedown Service

Kaspersky Takedown Service

Cyberkriminielle erstellen Malware- und Phishing-Domains, die für einen Angriff auf Ihr Unternehmen und Ihre Marken verwendet werden. Gegen diese Bedrohungen muss unmittelbar nach der Erkennung vorgegangen werden. Andernfalls kann es zu Umsatzverlusten, Rufschädigung, Verlust des Kundenvertrauens, Datenlecks und vielem mehr kommen. Allerdings ist ein solcher Domain-Takedown ein komplexer Prozess, der Fachkenntnis und Zeit erfordert.

Der Kaspersky Takedown Service wehrt Angriffe durch Malware- und Phishing-Domains schnell ab, bevor Ihre Marke und Ihr Unternehmen Schaden nehmen. Die umfassende Verwaltung des gesamten Prozesses spart Kunden wertvolle Zeit und Ressourcen. Der Service wird weltweit angeboten.

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 Malware- und Phishing-Domains 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.

Vollständige Sichtbarkeit

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

End-to-End-Management

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

Weltweite Abdeckung

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

Funktionsweise

Anfragen können über den 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 Domain zu deaktivieren. Sie werden über jeden Schritt benachrichtigt, bis die entsprechende Quelle erfolgreich deaktiviert wurde.

Müheloser Schutz

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

Kaspersky
Ask the Analyst

Kaspersky Ask the Analyst

Cyberkriminelle entwickeln ihre Angriffsstrategien gegen Unternehmen stetig weiter. Dabei setzen sie immer ausgefeiltere Technologien ein. Die Folge: Die aktuelle Bedrohungslage spitzt sich auch weiterhin zu. Unternehmen sehen sich mit komplexen Vorfällen konfrontiert, verursacht durch dateilose Angriffe, LOTL-Angriffe (Living off the Land), Zero-Day-Exploits – und komplexe Bedrohungen sowie APT-ähnliche und gezielte Angriffe, die all diese Varianten kombinieren.

Vor diesem Hintergrund sind Cybersicherheitsexperten wichtiger als je zuvor, allerdings nicht einfach zu finden und zu halten. Und selbst wenn Sie über ein gut eingespieltes Cybersicherheitsteam verfügen, sollte es externe Experten zurate ziehen können. Diese können auf wahrscheinliche Ausbreitungspfade komplexer Angriffe oder APTs hinweisen und praktische Ratschläge geben, wie man sie durch gezieltes Handeln unterbinden kann.

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.

Mit unserem Service Kaspersky Ask the Analyst können Sie Handlungsempfehlungen und Erkenntnisse zu spezifischen Bedrohungen anfordern. 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.

Leistungsumfang von Kaspersky Ask the Analyst (vereinheitlichtes Abonnement basierend auf Anfrage)

APT und Crimeware

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

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)

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

Dark Web Intelligence

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

Malware-Analyse

- Analyse von Malware-Proben
- Empfehlungen für weitere Eindämmungsmaßnahmen

Funktionsweise

Kaspersky Ask the Analyst kann separat erworben werden oder zusätzlich zu jedem unserer anderen Threat Intelligence Services. Anfragen können über den 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

1. Klärung von Details in zuvor veröffentlichten Threat Intelligence-Berichten
2. Zusätzliche Informationen zu bereits bekannten IoCs
3. Details zu Schwachstellen und Empfehlungen, wie sich ihre Ausnutzung verhindern lässt
4. Erhalten Sie zusätzliche Details zu den spezifischen Darkweb-Aktivitäten, die für Sie interessant sind
5. Sie erhalten Berichte zu Malware-Familien mit Details zum Verhalten der Malware, ihren potenziellen Auswirkungen und allen Kaspersky bekannten Aktivitäten, die ihr zugeordnet werden
6. Effektive Priorisierung von Warnungen/Vorfällen dank kurzer Berichte mit detaillierten Kontextinformationen und einer Kategorisierung nach relevanten IoCs
7. Fordern Sie Unterstützung bei der Identifizierung an, wenn erkannte ungewöhnliche Aktivitäten auf APTs oder Crimeware zurückzuführen sind
8. Einsendung von Malware-Dateien zur umfassenden Analyse auf Verhalten und Funktionsweise

Vorteile von Kaspersky Ask the Analyst

Erweitern Sie Ihr Fachwissen

Sie haben jederzeit Zugang zu Branchenexperten und müssen nicht 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.

Ausbau Ihres Know-how 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 erweitert so Ihr internes Know-how durch unser umfassendes Angebot an Expertise und Ressourcen.

Fazit

Die Bekämpfung heutiger Cyberbedrohungen erfordert einen 360-Grad-Blick 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 unterstützen wir unsere Kunden mit der neuesten Threat Intelligence aus der ganzen Welt. So helfen wir ihnen, auch gegen bisher unbekannte Cyberangriffe immun zu bleiben.

Die Vorteile auf einen Blick

Ermöglicht globale Transparenz von Bedrohungen, rechtzeitige Erkennung von Cyberbedrohungen, Priorisierung von Sicherheitswarnungen und effektive Reaktion auf Vorfälle

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 Maßnahmen auf die Bereiche konzentrieren, die als vorrangige Ziele für Cyberangriffe ausgemacht wurden

Verhindert die Überforderung von Analysten und hilft Ihren Mitarbeitern, sich auf echte Bedrohungen zu konzentrieren

Verbesserte und beschleunigte Vorfallsreaktion sowie Threat Hunting-Funktionen verringern die Verweilzeit für den Angriff und minimieren einen möglichen Schaden erheblich

Kaspersky Threat Intelligence

Mehr erfahren

www.kaspersky.de

#kaspersky
#bringonthefuture