Bleiben Sie den Angreifern immer einen Schritt voraus

Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

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, Threat Data-Feeds sowie eigenen Untersuchungen, die alle von unserem Expertenteam analysiert werden, um Unternehmen im Kampf gegen Cyberbedrohungen zu unterstützen.

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

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 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 Feeds liefern 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.

Kontextdaten

Jeder Datensatz in jedem Data Feed wird mit praktisch umsetzbarem Kontext angereichert (Bezeichnungen von Bedrohungen, Zeitstempel, Geolokalisierungsdaten, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.). Kontextdaten helfen, das große Ganze zu sehen, und ermöglichen eine weitere Analyse und vielfältige Nutzung der Daten. Wenn die Daten in einen Kontext gestellt werden, liefern sie schneller Antworten auf die Fragen „Wer?“, „Was?“, „Wo?“ und „Wann?“. Sie geben auch Aufschluss darüber, wer Ihre Gegner sind, so dass Sie schnell Entscheidungen treffen und handeln können.

Funktionsweise

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.

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

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

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

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 viele 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.

Werkzeuge

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

Eine Indikatorendatenbank mit Volltextsuche und erweiterten Suchmöglichkeiten erlaubt komplexe Abfragen über alle Indikatorfelder einschließlich der Kontextfelder.

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.

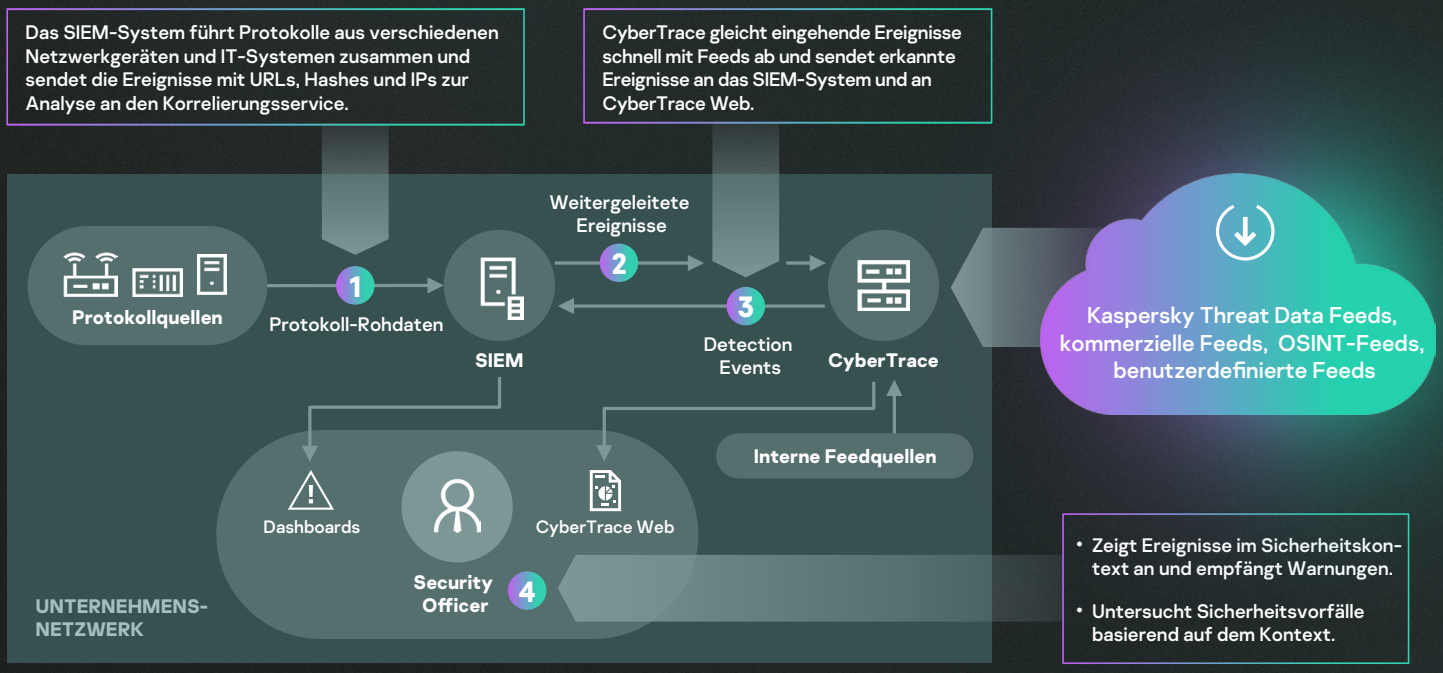
Ein Filter sendet erkannte Ereignisse an SIEM-Lösungen und entlastet nicht nur das SIEM sondern auch die Analysten.

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

Seiten mit detaillierten Informationen zu jedem Indikator ermöglichen eine noch tiefgreifendere Analyse. Auf jeder Seite werden sämtliche Informationen zu einem Indikator aus allen Threat Intelligence-Quellen (ohne Dopplung) dargestellt. Analysten können die Bedrohungen in den Kommentaren diskutieren und interne Analysen zum Indikator hinzufügen.

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.

Architektur



Kaspersky CyberTrace und Kaspersky Threat Data Feeds bieten Sicherheitsanalysten folgende Möglichkeiten:

Effektive Analyse und Priorisierung einer großen Anzahl von Sicherheitswarnungen

Verbesserung und Beschleunigung der Priorisierung und Erstreaktion

Aufbau einer vorausschauenden informationsbasierten Abwehr

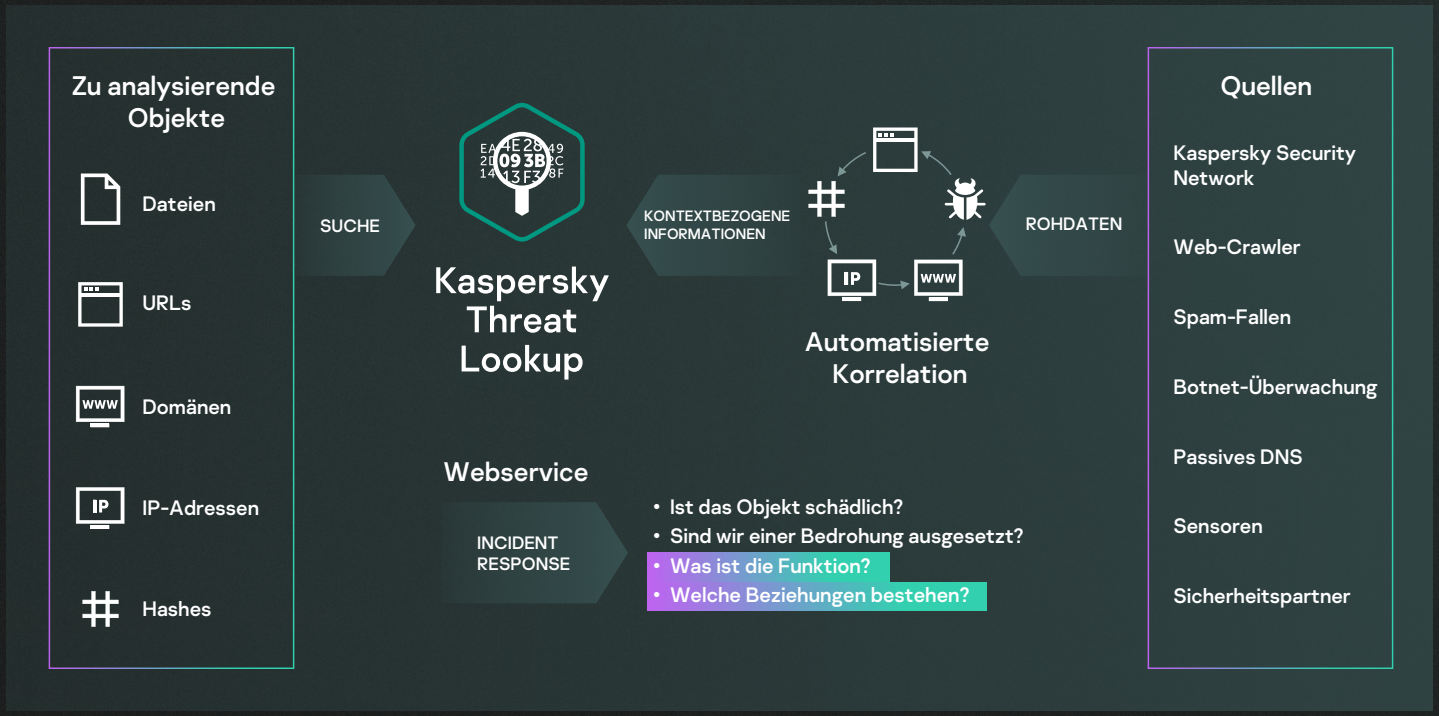
Sofortige Erkennung von Warnungen, die für Ihr Unternehmen kritisch sind, und fundierte Entscheidungen über die Eskalation von Warnungen an Incident Response-Teams

Kaspersky Threat Lookup

Cyberkriminalität kennt keine Grenzen und entwickelt sich rasant. Cyberangriffe werden immer raffinierter und Bedrohungsakteure 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



Highlights

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

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.

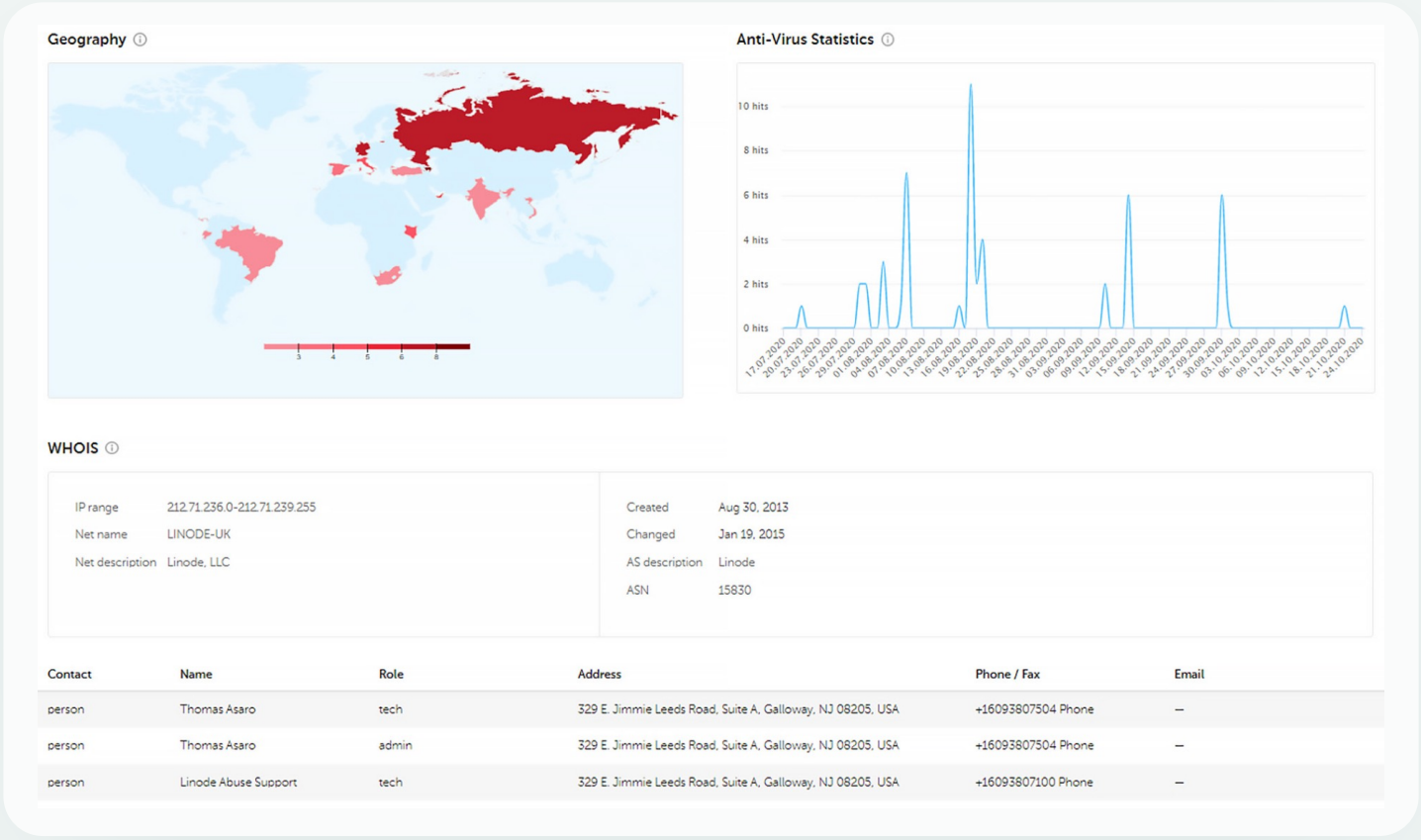
Suchen Sie über eine webbasierte Benutzeroberfläche oder die RESTful-API nach Bedrohungsindikatoren.

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

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

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.

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 Research Sandbox

Herkömmliche Antivirentools allein reichen nicht mehr aus, um gezielte Angriffe zu verhindern. Antiviren-Engines können nur bekannte Bedrohungen in verschiedenen Varianten abwehren. Versierte Bedrohungsakteure bedienen sich jedoch zahlreicher Techniken, um die automatische Erkennung zu umgehen. Schäden durch IT-Sicherheitsvorfälle nehmen ständig zu. Dadurch gewinnen Funktionen zur sofortigen Bedrohungserkennung an Bedeutung. So gewährleisten Sie eine schnelle Reaktionsfähigkeit und wirken Bedrohungen entgegen, bevor diese Schaden anrichten können.

Das Treffen intelligenter Entscheidungen auf der Grundlage des Dateiverhaltens bei gleichzeitiger Analyse z. B. des Prozessarbeitsspeichers, der Netzwerkaktivität usw. ist der optimale Ansatz, um die neuesten hochentwickelten, zielgerichteten und maßgeschneiderten Bedrohungen zu erkennen. Während statistische Daten oft keine Informationen über kürzlich modifizierte Malware enthalten, bieten Sandboxing-Technologien leistungsstarke Werkzeuge, um die Herkunft von Dateiproben zu untersuchen, IoCs auf der Grundlage von Verhaltensanalysen zu erfassen und schädliche Objekte zu erkennen, die normalerweise nicht erkannt würden.

Mit Kaspersky Research Sandbox können Sie die Herkunft von Beispieldateien untersuchen, IoCs auf der Grundlage von Verhaltensanalysen sammeln und schädliche Objekte erkennen, die Ihnen bislang entgangen sind. Die Lösung bietet einen hybriden Ansatz, der Bedrohungsinformationen aus Petabytes von statistischen Daten (dank Kaspersky Security Network und anderer proprietärer Systeme), Verhaltensanalysen und einen robusten Umgehungsschutz mit Technologien kombiniert, die menschliche Aktionen wie automatisches Klicken, Scrollen von Dokumenten und Dummy-Prozesse simulieren.

Proaktive Bedrohungserkennung und Risikominimierung

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

Kaspersky Research Sandbox bietet einen hybriden Ansatz, der Bedrohungsinformationen aus Petabytes von statistischen Daten (dank Kaspersky Security Network und anderer proprietärer Systeme), Verhaltensanalysen und einen robusten Umgehungsschutz mit Technologien kombiniert, die menschliche Aktionen wie automatisches Klicken, Scrollen von Dokumenten und Dummy-Prozesse simulieren.

Dieser Service wird seit über 10 Jahren intern in unserem Sandbox Lab weiterentwickelt. Die Technologie vereint unser gesamtes Wissen über das Verhalten von Malware, das wir uns in über 25 Jahren Bedrohungsforschung angeeignet haben. So können wir jeden Tag über 400.000 neue schädliche Objekte erkennen und unseren Kunden branchenführende Lösungen anbieten.

Kaspersky Research Sandbox verwendet einen einzigen Agenten, der über eine Cloud-basierte zentrale Verwaltungsplattform oder – in komplett isolierten Umgebungen – über eine Offline-Konsole verwaltet werden kann, wobei Threat Intelligence-Daten genutzt und anpassbare Analysen integriert werden.

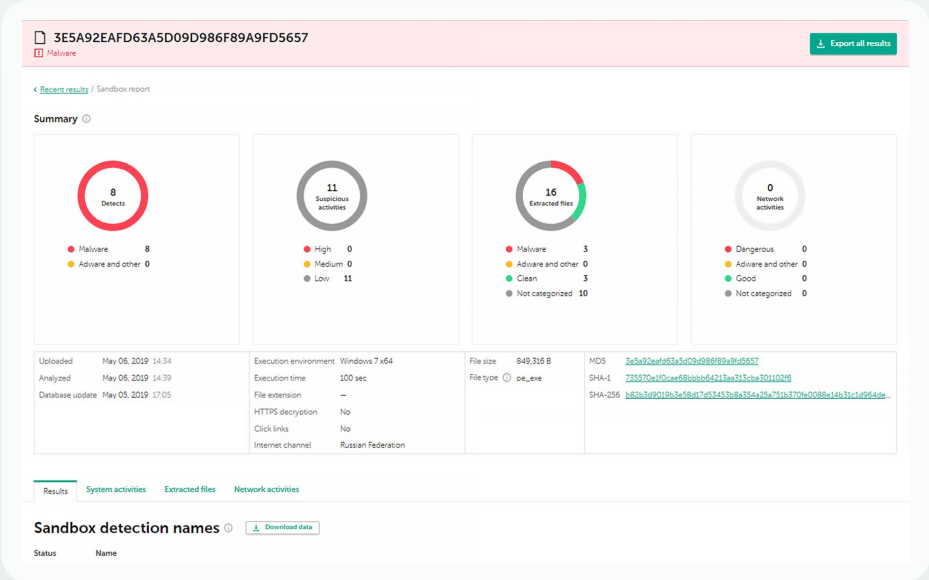
Kaspersky Research Sandbox ist Teil des Threat Intelligence-Portals und der letzte Baustein in Ihrem Threat Intelligence-Workflow. Während Threat Lookup die neuesten detaillierten Bedrohungsdaten zu URLs, Domänen, IP-Adressen, Hash-Werten, Bedrohungsnamen, statistischen/Verhaltensdaten, WHOIS/DNS-Daten etc. abruft, verknüpft Research Sandbox dieses Wissen mit den von der analysierten Datei erzeugten IoCs.

Umfassendes Reporting

- Vereinheitlichte Einstufung von Bedrohungen
- Verdächtige Systemaktivitäten mit detaillierten Beschreibungen
- Geladene und ausgeführte DLLs
- Erstellte, geänderte und gelöschte Dateien
- Verarbeitete Speicherauszüge und Netzwerkverkehr-Dumps (PCAP)
- Erstellte gemeinsame Erweiterungen (Mutexes)
- Geänderte und erstellte Registrierungsschlüssel
- Von der ausgeführten Datei erstellte Prozesse
- Netzwerkaktivitäten (SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, SOCKS-Sitzungen; HTTP(s), Anfragen und Antworten)
- Detaillierte Bedrohungsinformationen mit umsetzbarem Kontext für jeden aufgedeckten Gefährdungsindikator (IoC)
- Detaillierte Ausführungsübersicht mit hervorgehobenen MITRE ATT&CK-Techniken
- YARA erkennt und löst IDS-Regeln aus (aber auch benutzerdefinierte Regeln)
- Download und Analyse einer unter einer bestimmten URL gehosteten Datei
- Anklicken von Links in Adobe Reader- und Microsoft Office-Dokumenten (Word, Excel, PowerPoint, Publisher, Outlook)
- Möglichkeit zum Export der Analysedetails im STIX-, JSON- und CSV-Format
- Verschiedene Umgebungen, einschließlich Mobile OS (Android), sowie Anpassbarkeit der Umgebung
- Benutzerdefinierte Parameter für die Ausführung von Dateien
- Unterschiedliche Internet-Kanäle, die Möglichkeit, Datenverkehr über einen eigenen VPN-Kanal zu leiten
- RESTful-API
- Screenshots und vieles mehr

Mit Kaspersky Research Sandbox können Sie hochwirksame und komplexe Vorfalluntersuchungen durchführen. So gewinnen Sie ein sofortiges Verständnis der Art der Bedrohung und decken zusammenhängende Bedrohungsindikatoren auf.

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



Kaspersky Threat Attribution Engine

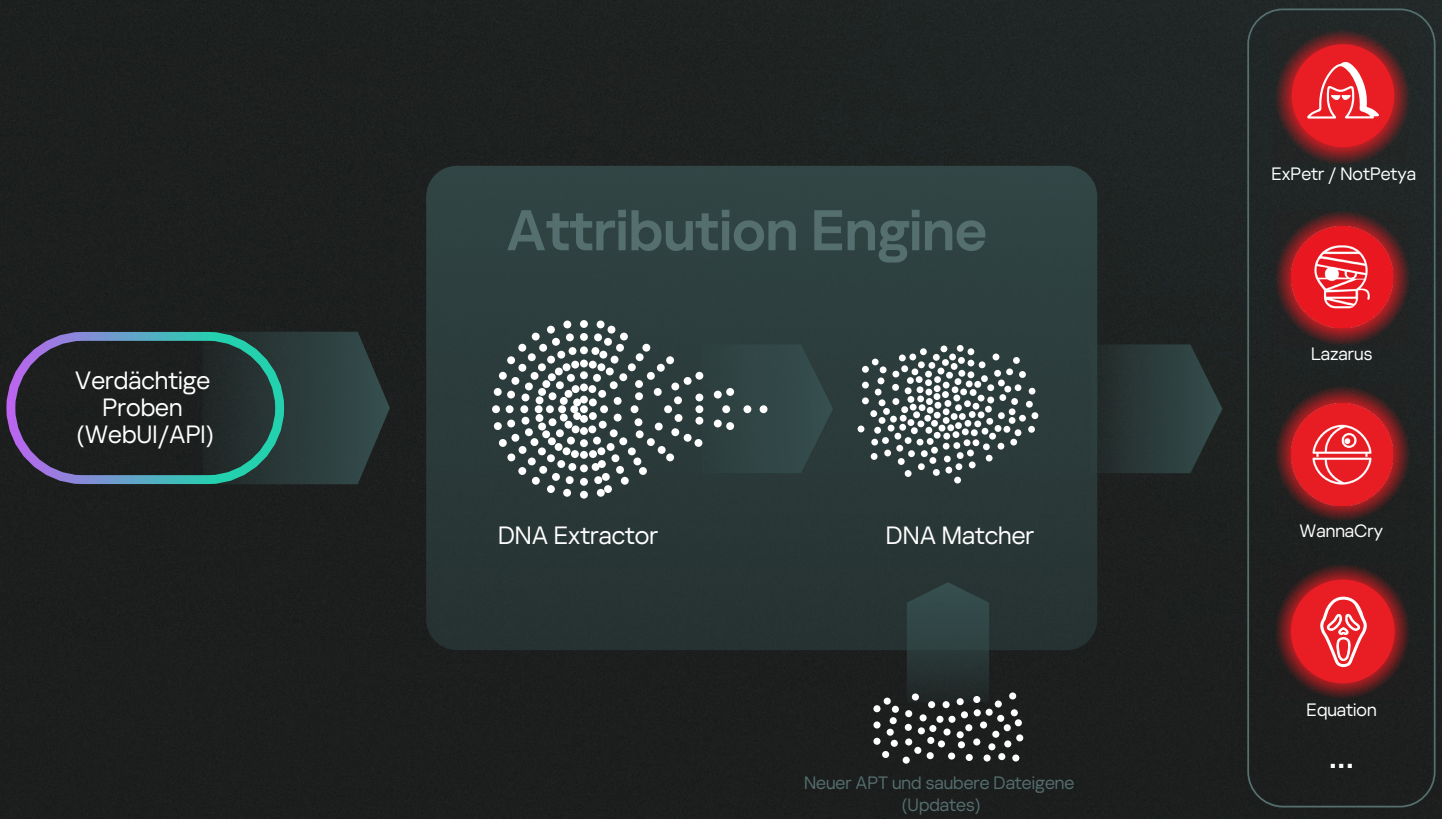
Es gibt gute Gründe dafür, dass Threat Attribution, also die Zuordnung von Bedrohungen, innerhalb der Cybersicherheit so wichtig ist. Die durchschnittliche Zeitspanne zwischen der Erkennung und der Reaktion auf hochentwickelte Bedrohungen kann sich aufgrund der komplexen Untersuchungs- und Reverse-Engineering-Prozesse dramatisch in die Länge ziehen. In vielen Fällen gibt diese Verzögerung den Angreifern genug Zeit, um ihre Ziele zu erreichen. Eine korrekte und zeitnahe Zuordnung hilft nicht nur die Reaktionszeiten von Stunden auf Minuten zu verkürzen, sondern auch die Zahl der Fehlalarme zu reduzieren.

Die Identifizierung eines zielgerichteten Angriffs, die Erstellung eines Angreiferprofils und der entsprechenden Attributionsfaktoren für die verschiedenen Bedrohungsakteure ist ein langer und komplexer Prozess. Dieser kann mitunter sogar Jahre dauern. Die Erstellung einer funktionierenden Zuordnung erfordert große Datenmengen, die über einen langen Zeitraum gesammelt werden, sowie ein hochqualifiziertes Team von Forschern mit einschlägiger Erfahrung. Diese Forscher verfolgen meist die Aktivitäten verschiedener Gruppen und sammeln alle Informationen in einer Datenbank. Diese Datenbank ist eine wertvolle Ressource, die als Tool freigegeben werden kann.

Die Kaspersky Threat Attribution Engine umfasst eine Datenbank mit APT-Malware-Proben und „sauberen“ Dateien, die von Kaspersky-Experten in mehr als 25 Jahren gesammelt wurden. Wir verfolgen mehr als 1100 Bedrohungsakteure und -Kampagnen und veröffentlichen mehr als 120 Threat Intelligence Reports pro Jahr. Im Rahmen unserer kontinuierlichen Forschung haben wir bereits eine beachtliche APT-Bibliothek gesammelt, die rund 83.000 Dateien umfasst. Damit lassen sich falsche Alarme wirksam vermeiden und in Verbindung mit dem Einsatz automatisierter Tools außerordentlich präzise Zuordnungen erreichen.

Das Tool bietet einen einzigartigen Ansatz für den Vergleich ähnlicher Proben und gewährleistet eine False-Positive-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.

Funktionsweise



Die Kaspersky Threat Attribution Engine verwendet eine einzigartige, proprietäre Methode zur Suche nach Ähnlichkeiten zwischen Dateien, um Malware mit zugehörigen Entitäten zu verknüpfen. 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.

Die 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. Eine API verbindet die Engine mit anderen Tools und Frameworks, so dass die Zuordnungsfunktion in bestehende Infrastrukturen und automatisierte Prozesse eingebunden werden kann.

Vorteile des Produkts im Überblick:

- Sofortiger Zugriff auf ein Repository mit kuratierten Daten zu Tausenden von APT-Akteuren, Mustern und allgemeineren Bedrohungen (über die Antiviren-Engine)
- Ermöglicht die effiziente automatisierte oder manuelle Priorisierung von Bedrohungen und Warnhinweisen
- Unterstützt die Eingabe von privaten Akteuren und Beispieldaten, damit das Produkt lernt, Daten zu erkennen, die Dateien in Ihrer privaten Sammlung ähnlich sind
- Ermöglicht das manuelle Hochladen von Daten und bietet eine verbesserte REST API zur Integration in automatisierte Workflows
- Unterstützt die Bereitstellung auf Amazon Web Services (AWS) und ermöglicht so neben einer schnellen Produkteinrichtung auch Kosteneinsparungen, da keine Vorabinvestitionen in Hardware erforderlich sind
- Exportiert problemlos in YARA-Regeln zur weiteren automatisierten Suche/Scannen nach ähnlichen Dateien oder zur Integration in Lösungen von Drittanbietern
- Exportiert problemlos in das STIX 2.1-Format (die Formate TXT und JSON werden ebenfalls unterstützt) zur weiteren automatischen Analyse von Sicherheitsprotokollen oder zur Integration in Lösungen/Sicherheitskontrollen von Drittanbietern
- Ermöglicht das Entpacken passwortgeschützter Archive mit benutzerdefinierten Passwörtern
- Bietet schnellen Zugriff auf Dokumentation und zum Endbenutzer-Lizenzvertrag (EULA) in der Weboberfläche
- Möglichkeit zum Senden von Attributen in parallelen Dateien zur Analyse in einer einzigen Anfrage

Vorteile der Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine berechnet den Reputationswert

der Probe und zeigt deren Zuordnung nach Genetik und Code an. Dies gibt Aufschluss über die Herkunft der Probe und ermöglicht die Zuordnung zu möglichen Urhebern.

Ihr Sicherheitsteam kann eigene Attributionsentitäten

und zugehörige Proben in die Datenbank der Kaspersky Threat Attribution Engine eintragen. Das Team kann das Programm dann so trainieren, dass es die eingereichten Proben diesen eigens erstellten Attributionsentitäten und Proben zuordnet.

Die Zuordnung erfolgt innerhalb von Sekunden.

Mit der Kaspersky Threat Attribution Engine ist die Zuordnung, verglichen zu Monaten und Jahren, die sie in der Vergangenheit in Anspruch genommen hat, innerhalb von Sekunden erledigt.

Die Kaspersky Threat Attribution Engine ergänzt und stärkt

das Kaspersky-Portfolio für kommerzielle Security Operations Centers (SOCs) und nationale Cybersicherheitsbehörden, indem es sie bei der Einführung eines effektiven Incident-Management-Prozesses unterstützen

Kaspersky APT Intelligence Reporting

Kunden, die Kaspersky APT Intelligence Reporting einsetzen, erhalten exklusiven Zugriff auf unsere Untersuchungen und Entdeckungen, einschließlich vollständiger technischer Daten (in verschiedenen Formaten) über jeden APT-Angriff, sobald dieser entdeckt wird, sowie über Bedrohungen, die nie öffentlich gemacht werden. Die Berichte enthalten Zusammenfassungen, die sich an C-Level-Mitarbeiter richten und leicht verständliche Informationen über die jeweiligen APTs enthalten. Der Zusammenfassung folgt eine detaillierte technische Beschreibung der APT mit den zugehörigen IoCs und YARA-Regeln. Auf diese Weise erhalten Sicherheitsforscher, Malware-Analysten, Sicherheitstechniker, Netzwerkanalysten und APT-Experten praktisch umsetzbare Informationen, die eine schnelle und präzise Reaktion auf die Bedrohung ermöglichen.

Unsere Experten alarmieren Sie sofort, wenn sie Veränderungen in der Taktik von Cyberkriminellen feststellen. Außerdem erhalten Sie Zugriff auf die vollständige APT-Berichtsdatenbank von Kaspersky, eine weitere leistungsstarke Forschungs- und Analysekomponente Ihrer Sicherheitsstrategie.

300+
Bedrohungsakteure

160+
private Berichte pro Jahr

Mehr als 12.000
IoCs

400+
Kampagnen

700+
Yara-Regeln

Vorteile von Kaspersky APT Intelligence Reporting

Profile von Bedrohungsakteuren

Zuordnung zu MITRE ATT&CK

Zusammenfassung

Auf C-Ebene ausgerichtete Informationen

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

Schlussfolgerungen und Empfehlungen

Gefährdungsindikatoren (IoCs) und YARA-Regeln

Vorteile von Kaspersky APT Intelligence Reporting

Informationen über nicht öffentliche APTs

Aus verschiedenen Gründen werden nicht alle komplexen Bedrohungen öffentlich bekannt gemacht – trotzdem informieren wir Sie darüber

Priorisierter Zugriff

Technische Beschreibungen der neuesten Bedrohungen während laufender Untersuchungen, bevor sie publik gemacht werden

Nachträgliche Analyse

Zugriff auf alle verfügbaren privaten Berichte während der Abolaufzeit

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-Regeln

Profildaten der Bedrohungsakteure

Einschließlich des vermuteten Herkunftslandes und der Hauptaktivität, der verwendeten Malware-Familien, der betroffenen Branchen und Regionen sowie Beschreibungen aller verwendeten HTTP-Adressen und ihrer Zuordnung zu MITRE ATT&CK

Nahtlose Integration und Automatisierung

Nahtlose Integration und Automatisierung Ihrer Sicherheits-Workflows mit RESTful API

Kontinuierliche Überwachung von APT-Kampagnen

Erhalten Sie Zugriff auf praktisch umsetzbare Erkenntnisse während der Ermittlungsphase mit Informationen über die APT-Verteilung, IoCs, C&C-Infrastruktur usw.

MITRE ATT&CK

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

Kaspersky Crimeware Intelligence Reporting

Finanziell motivierte Cyberkriminalität ist nicht auf bestimmte Branchen beschränkt. Und während Angriffe auf Finanzinfrastrukturen wie Geldautomaten und Point-of-Sale-Geräte nicht abreißen, sind alle Unternehmen in jedem Sektor durch Ransomware gefährdet. Seit einigen Jahren verschwimmen die Grenzen zwischen den verschiedenen Bedrohungsarten und den verschiedenen Typen von Bedrohungsakteuren. Dazu gehören APT-Kampagnen, die nicht auf Cyberspionage, sondern auf Diebstahl ausgerichtet sind – um an Geld zu kommen, das andere Aktivitäten der APT-Gruppe finanzieren soll. Crimeware wird immer ausgeklügelter und sollte nicht unterschätzt werden.

Kaspersky Crimeware Intelligence Reporting stärkt Ihre Abwehrstrategien durch zeitnahe Informationen über Malware-Kampagnen, Angriffe auf Finanzinstitute und Crimeware-Tools, die für Angriffe auf Banken, Zahlungsabwickler und deren spezifische Infrastrukturen eingesetzt werden.

Kaspersky Crimeware Intelligence Reporting bietet

- Detaillierte Beschreibungen gängiger, weit verbreiteter und in den Medien stark präsenter Malware
- Hinweise/Frühwarnungen, einschließlich Informationen über neue und aktualisierte Malware-Bedrohungen
- Informationen über gefährliche, weit verbreitete Malware-Kampagnen
- Detaillierte Beschreibungen der Bedrohungen für Finanzinfrastrukturen und der entsprechenden Angriffswerkzeuge, die von Cyberkriminellen in verschiedenen Regionen im Darknet entwickelt oder verkauft werden

Vorteile von Kaspersky Crimeware Intelligence Reporting

Priorisierter Zugriff

Technische Beschreibungen der neuesten Bedrohungen während laufender Untersuchungen, bevor sie publik gemacht werden

Nachträgliche Analyse

Zugriff auf alle verfügbaren privaten Berichte während der Abolaufzeit

Nahtlose Integration und Automatisierung

Nahtlose Integration und Automatisierung Ihrer Sicherheits-Workflows mit RESTful API

Zugriff auf technische Daten

einschließlich einer umfangreichen Liste von IoCs, die in Standardformaten wie OpenIoC oder STIX bereitgestellt werden, sowie Zugriff auf unsere YARA-Regeln

Profildaten zu Crimeware-Akteuren

Einschließlich des vermuteten Herkunftslandes und der Hauptaktivität, der verwendeten Malware-Familien, der betroffenen Branchen und Regionen sowie Beschreibungen aller verwendeten HTTP-Adressen und ihrer Zuordnung zu MITRE ATT&CK

Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting liefert detaillierte Informationen und erhöht das Bewusstsein für bösartige Kampagnen, die auf Unternehmen abzielen, sowie für Schwachstellen, die in den gängigsten branchenweiten Kontrollsystemen und den zugrunde liegenden Technologien identifiziert wurden. Berichte werden über das Kaspersky Threat Intelligence Portal bereitgestellt. Dadurch können Sie den Service sofort in Anspruch nehmen.

Alle ICS-bezogenen Bedrohungsanalysen werden von einem speziellen Team durchgeführt – Kaspersky ICS CERT:

- Gegründet im Jahr 2016
- Das erste CERT-Team, das von einer kommerziellen Organisation ins Leben gerufen wurde
- Ca. 20 hochqualifizierte Experten auf dem Gebiet der ICS-Bedrohungs- und Schwachstellenforschung, Vorfallsreaktion und Sicherheitsanalyse

In Ihrem Abonnement enthaltene Berichte

APT-Berichte

Berichte über neue APT- und umfangreiche Angriffskampagnen, die auf Unternehmen abzielen, sowie Updates zu aktiven Bedrohungen.

Identifizierte Schwachstellen

Berichte über Schwachstellen, die von Kaspersky in den gängigsten Produkten identifiziert wurden, die in industriellen Kontrollsystemen, im industriellen Internet der Dinge und in Infrastrukturen in verschiedenen Sektoren eingesetzt werden.

Schwachstellenanalyse und -minderung

Wir liefern praktisch umsetzbare Empfehlungen von Kaspersky-Experten, um Schwachstellen in Ihrer Infrastruktur zu ermitteln und zu mindern.

Entwicklung der Bedrohungslandschaft

Berichte über wesentliche Veränderungen in der Bedrohungslandschaft für branchenweite Kontrollsysteme, neu entdeckte kritische Faktoren mit Auswirkungen auf die ICS-Sicherheitsniveaus und das ICS-Bedrohungsrisiko, einschließlich regionaler, länderspezifischer und branchenspezifischer Informationen.

Diese Vorteile bieten Threat Intelligence-Daten

Erkennen und blockieren Sie

bekannte Bedrohungen, um kritische Assets wie Software- und Hardware-Komponenten zu sichern und die Sicherheit und Kontinuität des technologischen Prozesses zu gewährleisten.

Vulnerability Assessment

Bewerten Sie Ihre industrielle Umgebung und Ihre Anlagen auf der Grundlage einer genauen Einschätzung des Umfangs und der Schwere der Schwachstelle und treffen Sie fundierte Entscheidungen über das Patch-Management oder die Umsetzung anderer von uns empfohlener Präventivmaßnahmen.

Abgleich

schädlicher und verdächtiger Aktivitäten, die Sie in industriellen Umgebungen ermitteln, mit den Recherche-Ergebnissen von Kaspersky. Ordnen Sie diese schädlichen Kampagnen zu, ermitteln Sie Bedrohungen und reagieren Sie unverzüglich auf Vorfälle.

Gezieltes Einsetzen von Informationen

Zu Angriffstechnologien, Taktiken und Prozeduren, kürzlich entdeckten Schwachstellen und anderen wichtigen Veränderungen der Bedrohungslandschaft. Ziel ist es:

- Risiken, die von den bekannten Bedrohungen und anderen ähnlichen Bedrohungen ausgehen, zu ermitteln und zu bewerten
- Änderungen an industriellen Infrastrukturen zu planen und zu entwickeln, um eine sichere Produktion und die Kontinuität des technologischen Prozesses zu gewährleisten
- Aktivitäten zum Sicherheitsbewusstsein basierend auf Analysen realer Fälle durchzuführen, um Schulungsszenarien für das Personal zu entwickeln und Übungen für Red Teams und Blue Teams zu planen
- Fundierte strategische Entscheidungen zu treffen, um in Cybersicherheit zu investieren und die betriebliche Resilienz sicherzustellen

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

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).

Markenschutz

Monitoring und Blockierung der unbefugten Nutzung von Unternehmensmarken im Internet. Identifizierung von gefälschten Social Media-Konten und -Programmen, Phishing-Webseiten und anderen betrügerischen Aktivitäten, durch die der Ruf Ihres Unternehmens geschädigt und/oder Kunden getäuscht werden könnten. Takedown von gefälschten Konten in sozialen Netzwerken und gefälschten Apps auf den Marketplaces für Mobilgeräte.

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.

Quellen für **Bedrohungsdaten**

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

Netzwerk-Bestandsaufnahme

Öffentliches Internet, Deep Web und Dark Web

Kaspersky-Wissensdatenbank

Analysen

Bedrohungshinweise

10 Takedown-Anfragen pro Jahr

Echtzeit-Suche in den Quellen von Kaspersky, OSINT, Internet und Dark Web

Funktionsweise

Konfigurieren

Ermitteln von Informationen über die digitalen Ressourcen des Unternehmens

Erfassen

Automatisiertes Sammeln von Daten aus dem öffentlichen Internet, Deep Web und Dark Web sowie aus der Kaspersky Threat Intelligence-Datenbank

Filtern

Von Analysten gesteuerte Erkennung, Analyse und Priorisierung von Bedrohungen

Reagieren

Bereitstellung umfassender Bedrohungsdaten

Geschäftswerte

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

Schutz für Ihre Marke

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

Vorbereitung 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.

Kaspersky Takedown Service

Cyberkriminielle erstellen schädliche und Phishing-Domänen, die für einen Angriff auf Ihr Unternehmen und Ihre Marken verwendet werden. Diese Bedrohungen müssen sofort nach ihrer Entdeckung bekämpft werden. Andernfalls kann es zu Umsatzeinbußen, Rufschädigung, Verlust des Kundenvertrauens, Datenlecks und vielem mehr kommen. Allerdings ist ein solcher Domänen-Takedown ein komplexer Prozess, der Fachkenntnis und Zeit erfordert.

Der Kaspersky Takedown Service wehrt Angriffe durch schädliche und Phishing-Domänen schnell ab, bevor Ihre Marke und Ihr Unternehmen Schaden nehmen. Die umfassende Verwaltung des gesamten Prozesses spart 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 schädlichen und Phishing-Domänen heißt, dass wir wissen, wie wir alle notwendigen Beweise sammeln müssen, um deren Schädlichkeit nachzuweisen. Wir kümmern uns um das Takedown-Management und ermöglichen eine schnelle Reaktion zur Minimierung Ihres digitalen Risikos, damit 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 schädliche oder Phishing-Domäne registriert ist, Kaspersky wird bei der regionalen Organisation mit der entsprechenden rechtlichen Befugnis einen Takedown anfordern.

Integration mit Kaspersky Digital Footprint Intelligence

Der Kaspersky Takedown Service kann auch separat erworben werden. Hohe Synergieeffekte erzielen Sie aber durch die Integration mit Kaspersky Digital Footprint Intelligence. Mit Kaspersky Digital Footprint Intelligence werden Sie in Echtzeit über Phishing- und Malware-Domänen informiert und können diese direkt vom Kaspersky Takedown Service sperren lassen.

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 rechtliche Befugnis verfügt, die Domäne zu deaktivieren. Sie werden über jeden Schritt benachrichtigt, bis die entsprechende Quelle erfolgreich deaktiviert wurde.

Müheloser Schutz

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

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 baut so Ihr firmeninternes Know-how um unser umfassendes Angebot aus Fachwissen und Ressourcen aus.

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 dabei, ihre Immunität auch gegen bisher unbekannte Cyberangriffe aufrechtzuerhalten.

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