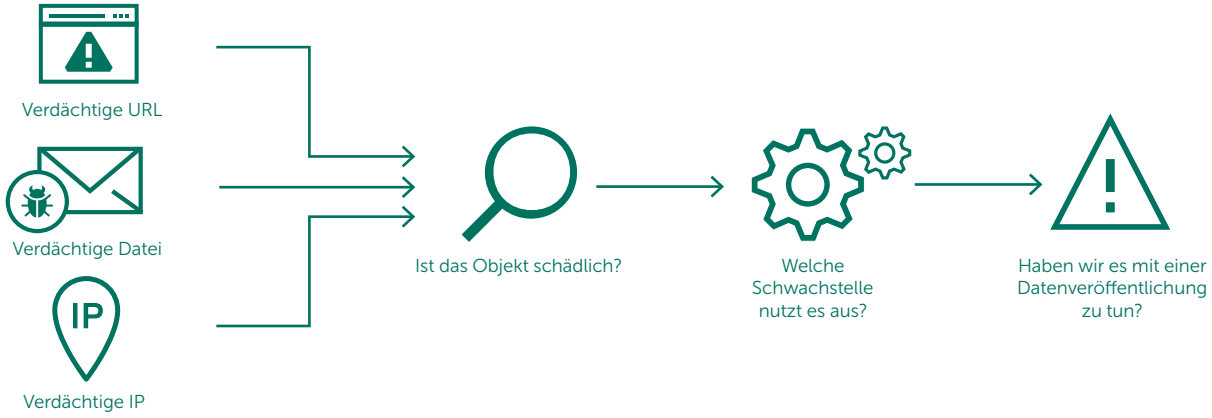
SCHLIESSEN SIE DIE LÜCKEN IN IHRER NETZWERKSICHERHEIT

KASPERSKY lab

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

Kaspersky Threat Lookup bietet Ihnen unmittelbar verlässliche Informationen über Cyberbedrohungen, legitime Objekte, deren gegenseitigen Abhängigkeiten und Indikatoren sowie praktisch umsetzbare Kontextinformationen, anhand derer sich die für die IT-Sicherheit zuständigen Mitarbeiter ein Bild über die Risiken und Folgen machen können. Dies ermöglicht eine effektivere Reaktion auf Bedrohungen und die Einleitung von Verteidigungsmaßnahmen noch vor dem Angriff.
Kaspersky Threat Lookup enthält unser gesamtes Wissen über Cyberbedrohungen und ihre Interdependenzen in einem einzigen, leistungsstarken Webservice. Das Ziel ist es, Sie und Ihre Sicherheitsteams mit so vielen Informationen wie möglich zu versorgen, damit Cyberangriffe schon im Vorfeld abgewendet werden können. Die Plattform ruft die aktuellen Bedrohungsinformationen zu URLs, Domänen, IP-Adressen, Datei-Hashes, Bezeichnungen von Bedrohungen, Statistik- und Verhaltensdaten, WHOIS/DNS-Einträge usw. ab. Hieraus ergibt sich ein umfassender Überblick über neue und aufkommende Bedrohungen, der Ihnen hilft, die Verteidigung und Vorfallsreaktion Ihres Unternehmens zu verbessern.



Funktionen:

- **Zuverlässige Sicherheitsinformationen:** Ein zentraler Bestandteil von Kaspersky Threat Lookup ist die Zuverlässigkeit unserer Bedrohungsinformationen, die durch einen praktisch umsetzbaren Kontext ergänzt werden. Produkte von Kaspersky Lab zählen zu den führenden bei Anti-Malware-Tests[1]. Die hohen Erkennungsraten mit Fehlalarmquoten, die praktisch gegen Null gehen, zeigen die Zuverlässigkeit unserer Sicherheitsinformationen.
- **Umfassender Schutz in Echtzeit:** Unsere Bedrohungsinformationen werden automatisch in Echtzeit generiert, und zwar basierend auf den weltweit von Kaspersky Security Network erfassten Daten, die einen Einblick in einen signifikanten Anteil des gesamten Internetdatenverkehrs und alle möglichen Datentypen von Millionen von Endbenutzern in mehr als 213 Ländern gewähren. Hierdurch entsteht umfassender Schutz und hohe Genauigkeit.
- **Aufspüren von Bedrohungen:** Gehen Sie bei der Prävention, Erkennung und Reaktion auf Angriffe proaktiv vor, um deren Auswirkung und Häufigkeit zu minimieren. Überwachen und eliminieren Sie Angreifer so früh wie möglich. Je früher Sie eine Bedrohung entdecken, umso weniger Schaden entsteht, umso schneller können Korrekturmaßnahmen stattfinden und umso eher kann sich der Netzwerkbetrieb normalisieren.
- **Umfassende Daten:** Die Bedrohungsinformationen von Kaspersky Threat Lookup decken eine große Bandbreite unterschiedlicher Datentypen ab, darunter Hash-Werte, URLs, IPs, whois-Einträge, pDNS, GeoIP, Dateiattribute, Statistiken und Verhaltensmuster, Downloadketten, Zeitstempel usw. Dank dieser Informationen erhalten Sie einen Überblick über die Bedrohungslage, mit der Sie konfrontiert sind.
- **Kontinuierliche Verfügbarkeit:** Unsere Bedrohungsinformationen werden durch eine hochgradig fehlertolerante Infrastruktur generiert und überwacht, die eine kontinuierliche Verfügbarkeit und ein gleichbleibendes Leistungsniveau sicherstellt.
- **Kontinuierliche Überprüfung durch Sicherheitsexperten:** Hunderte von Experten, darunter Sicherheitsanalysten aus der ganzen Welt, weltweit anerkannte Sicherheitsexperten aus unserem GReAT-Team und führenden Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung von wertvollen und praxisnahen Bedrohungsinformationen bei.

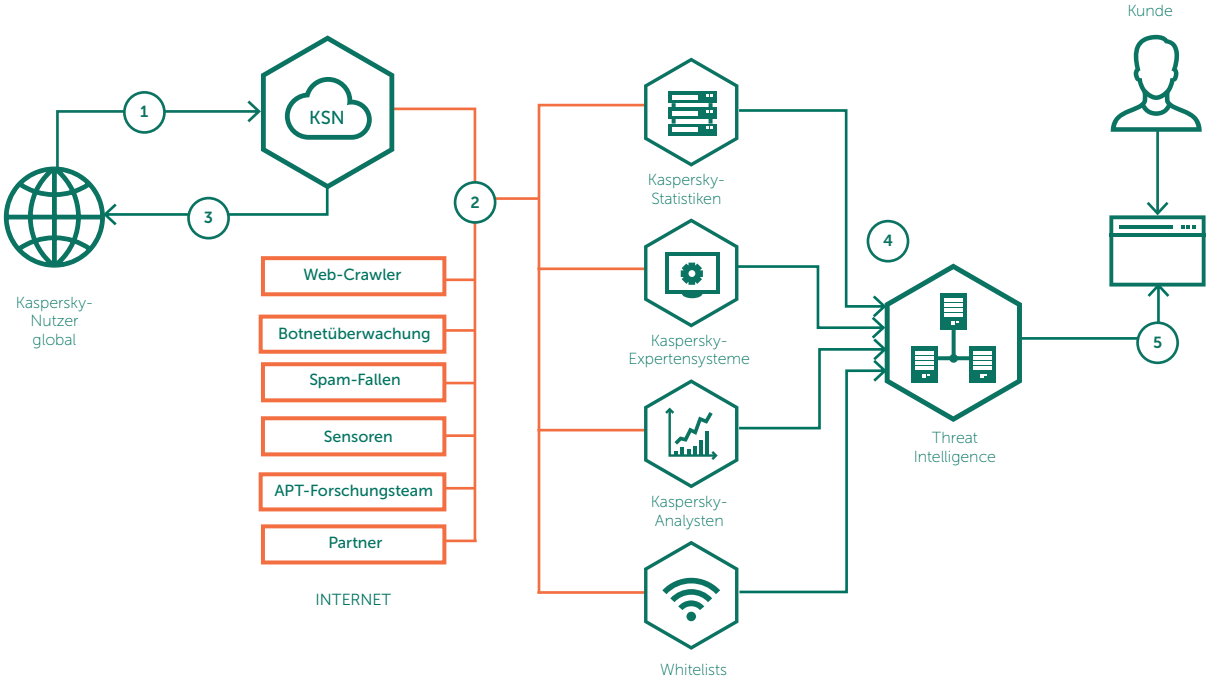
- **Sandbox-Analyse**[2] Dabei werden unbekannte Bedrohungen durch die Ausführung von verdächtigen Objekten in einer abgesicherten Umgebung erkannt sowie das gesamte Bedrohungsverhalten mitsamt der Artefakte in leicht verständlichen Berichten überprüft.
- **Breites Spektrum an Exportformaten:** Exportieren Sie die Gefährdungsindikatoren (IOCs = Indicators of Compromise) oder den praktisch umsetzbaren Kontext in gängige, strukturiertere und computerlesbare Formate, z. B. STIX, OpenIOC, JSON, Yara, Snort oder sogar CSV, um alle Vorteile von Bedrohungsinformationen nutzen zu können, betriebliche Workflows zu automatisieren oder eine Integration mit bestehenden Sicherheitskontrollen, z. B. SIEMs, zu ermöglichen.
- **Benutzerfreundliche Web-Oberfläche oder RESTful-API:** Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über ein einfaches RESTful-API zugreifen.

Hauptvorteile:

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

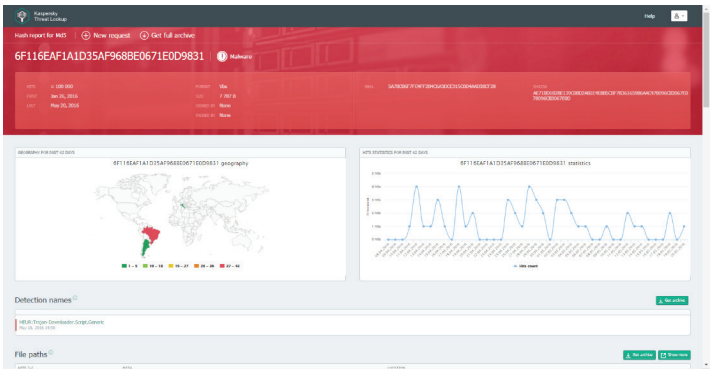
Threat Intelligence:

Unsere Bedrohungsinformationen (Threat Intelligence) werden aus heterogenen und höchst zuverlässigen Quellen wie dem Kaspersky Security Network (KSN) und unseren eigenen Web-Crawlern, unserem Botnet Monitoring Service (ununterbrochene Überwachung von Botnets sowie ihrer Ziele und Aktivitäten), Spam-Fallen, Forschungsteams, Partnern sowie anhand anderer historischer Daten zusammengestellt, die Kaspersky Lab in den vergangenen zwei Jahrzehnten erfasst hat. Dann werden sämtliche aggregierten Daten in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren verfeinert, z. B. durch statistische Kriterien, Kaspersky-Expertensysteme (Sandboxes, heuristische Engines, Similaritätstools, Erstellung von Verhaltensprofilen usw.), die Validierung durch Analysten und die Verifizierung anhand von Whitelists.



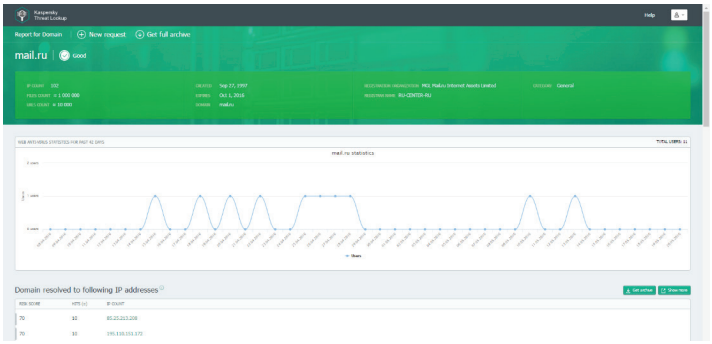
Kaspersky Threat Intelligence enthält sorgfältig geprüfte Daten zu Bedrohungsindikatoren, die in Echtzeit aus realen Datenquellen bezogen werden.

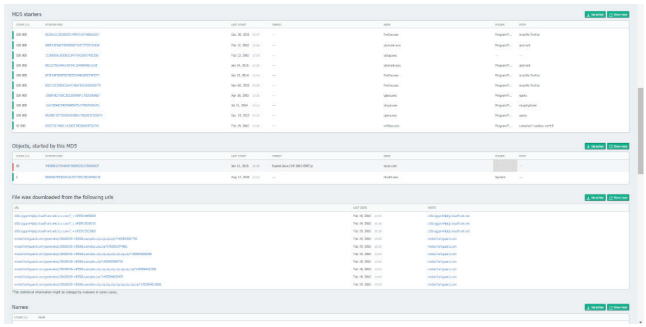
[1] http://www.kaspersky.com/top3
[2]. Die Funktion soll in der ersten Jahreshälfte 2017 veröffentlicht werden.



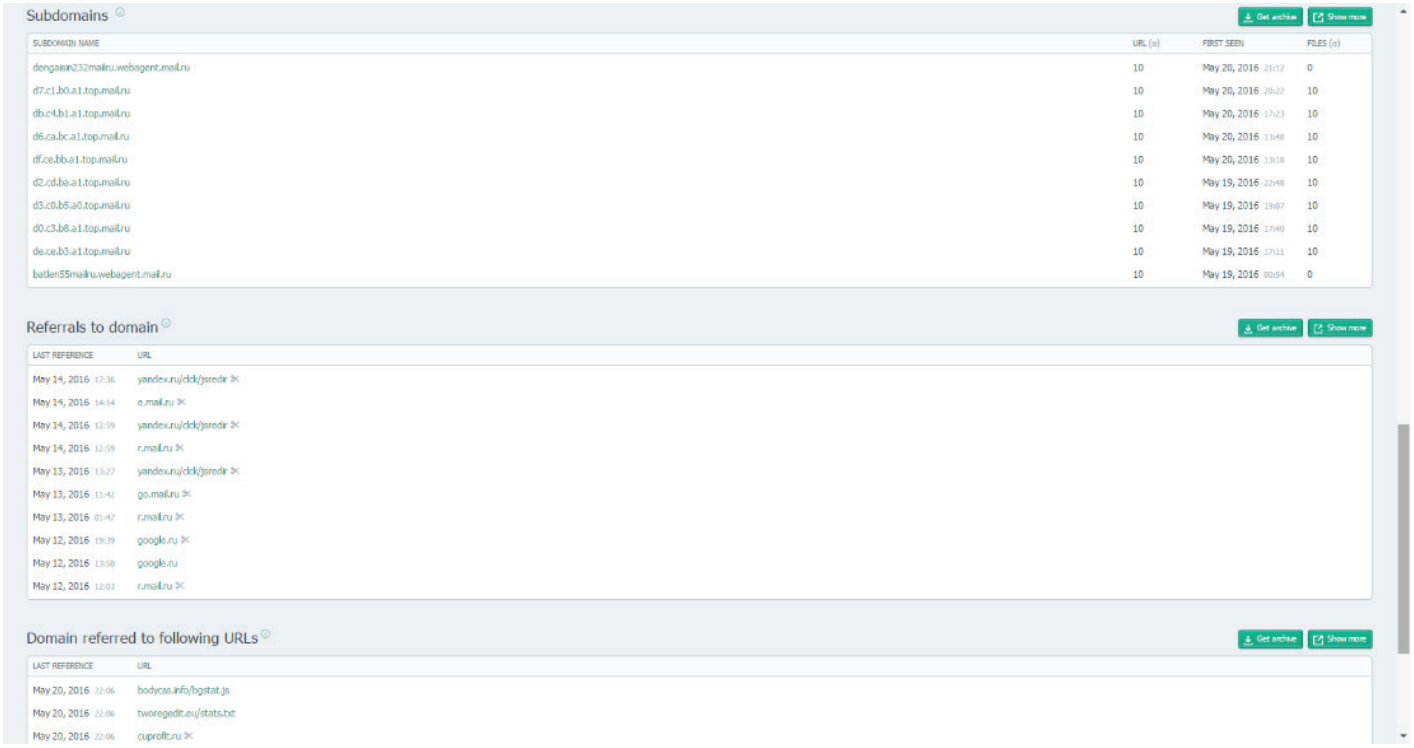
Jetzt können Sie:

- über eine webbasierte Benutzeroberfläche oder das RESTful-API nach Bedrohungsindikatoren suchen.
- nachvollziehen, warum ein Objekt als schädlich eingestuft wird.
- überprüfen, ob ein entdecktes Objekt weit verbreitet ist oder isoliert vorkommt.
- zusätzliche Details überprüfen, darunter Zertifikate, häufig genutzte Bezeichnungen, Dateipfade oder zugehörige URLs, um neue verdächtige Objekte zu entdecken. Dies sind nur einige Beispiele. Es gibt noch eine Vielzahl von Möglichkeiten, diese relevanten und fein abgestuften Sicherheitsinformationen zu nutzen.





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



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

KASPERSKY lab

THE POWER OF PROTECTION