Kaspersky Ask the Analyst

kaspersky BRING ON THE FUTURE

Kaspersky Ask the Analyst

Kontinuierliche Bedrohungsforschung

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

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

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

Leistungsumfang von Ask the Analyst

(vereinheitlichtes Abonnement, basierend auf Anfrage)

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

APT und Crimeware

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

Malware-Analyse

- Analyse von Malware-Proben
- Empfehlungen für weitere Eindämmungsmaßnahmen

Beschreibungen von Bedrohungen, Schwachstellen und relevanten IoCs

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

Dark-Web-Intelligence[2]

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

ICS-bezogene Anfragen

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

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

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

Servicevorteile

Zusätzliches Fachwissen

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

Schnellere Untersuchungen

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

Schnelle Reaktion

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

Funktionsweise

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

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

Anwendungsfälle für den Service:

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

Ergänzung Ihres Know-hows und Ihrer Ressourcen

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

www.kaspersky.de