Kaspersky Ask the Analyst

kaspersky BRING ON THE FUTURE

Continuous threat research

enables Kaspersky to discover, infiltrate and monitor closed communities and dark forums worldwide frequented by adversaries and cybercriminals. Our analysts leverage this access to proactively detect and investigate the most damaging and notorious threats, as well as threats tailored to target specific organizations

Access unequaled expertise

Cybercriminals are constantly developing sophisticated ways of attacking businesses. Today's volatile and fast-growing threat landscape features increasingly agile cybercrime techniques. Organizations face complex incidents caused by non-malware attacks, fileless attacks, living-off-the-land attacks, zero-day exploits — and combinations of all of these built into complex threats, APT-like and targeted attacks.

In an age of business-crippling cyberattacks, cybersecurity professionals are more important than ever, but finding and retaining them isn't easy. And even if you have a well-established cybersecurity team, your experts can't always be expected to fight the war against sophisticated threats alone **— they need to be able to call on expert third-party assistance.** External expertise can shed light on the likely paths of complex attacks and APTs, and deliver actionable advice on the most decisive way to eliminate them.

Ask the Analyst Deliverables

(Unified request-based subscription)

The **Kaspersky Ask the Analyst** service extends our Threat Intelligence portfolio, enabling you to request guidance and insights into specific threats you're facing or interested in. The service tailors Kaspersky's powerful threat intelligence and research capabilities to your specific needs, enabling you to build resilient defenses against threats targeting your organization.

APT and Crimeware

Additional information on published reports and ongoing research (on top of APT or Crimeware Intelligence Reporting service)[1]

Malware Analysis

- Malware sample analysis
- Recommendations on further remediation actions

Descriptions of threats, vulnerabilities and related IoCs

- General description of a specific malware family
- Additional context for threats (related hashes, URLs, CnCs, etc.)
- Information on a specific vulnerability (how critical it is, and the corresponding protection mechanisms in Kaspersky products)

Dark Web Intelligence[2]

- Dark Web research on particular artefacts, IP addresses, domain names, file names, e-mails, links or images
- Information search and analysis

[1] Available to customers with active APT and/or Crimeware Intelligence Reporting only

[2] Already included in the Kaspersky Digital Footprint Intelligence subscription

Service benefits

Augment your expertise

Get on-demand access to industry experts without having to search for and invest in hiring hard to find full-time specialists

Accelerate investigations

Effectively scope and prioritize incidents based on tailored and detailed contextual information

Respond fast

Respond to threats and vulnerabilities fast using our guidance to block attacks via known vectors

How it works

Kaspersky Ask the Analyst can be purchased separately or on top of any of our threat intelligence services.

You can submit your requests via Kaspersky Company Account, our corporate customer support portal. We will respond by email, but if necessary and agreed on by you, we can organize a conference call and/or screen sharing session. Once your request has been accepted, you'll be informed of the estimated timeframe for processing it.

Service use cases:

- Clarify any details in previously published threat intelligence reports
- Get additional intelligence for already provided IoCs
- Obtain details on vulnerabilities and recommendations on how to protect against their exploitation
- Get additional details on the specific Dark Web activities you're interested in
- Get an overview malware family report including the malware behavior, its potential impact and details about any related activity Kaspersky has observed
- Effectively prioritize alerts/ incidents with detailed contextual information and categorization for related IoCs provided via short reports
- Request assistance in identifying if detected unusual activity relates to an APT or a crimeware actor
- Submit malware files for comprehensive analysis to understand the behavior and functionality of the provided sample(s)

Extend your knowledge and resources

Kaspersky Ask the Analyst gives you access to a core group of Kaspersky researchers on a case-by-case basis. The service delivers comprehensive communication between experts to augment your existing capabilities with our unique knowledge and resources.

Learn more

Kaspersky Threat Intelligence

www.kaspersky.com