Proactive cybersecurity solutions for a threat intelligence expert

2024

kaspersky BRING ON THE FUTURE

Kaspersky provides this market-leading threat intelligence and analytics expert with infallible protection. With no room for error, they and their clients expect – and receive – only the best.

Cybersecurity

- Pennsylvania, United States
- Using Kaspersky APT Intelligence Reporting, Kaspersky Threat Data Feeds, and Kaspersky Threat Infrastructure Tracking.
- A depth of visibility that enables a holistic understanding of the threat landscape – crucial for the organization's cybersecurity posture.

0
security incidents

10,000+
threat actors identified thanks to the protection provided by Kaspersky

1,000,000,000+
telemetry data records to protect

About the customer

Risk surveillance is intrinsic to this American cyber threat intelligence and data analytics expert. Its clients must have absolute faith in its ability to handle 650,000+ sources of data at any one time.

Challenges

This cybersecurity company has been using Kaspersky for over five years to shield thousands of endpoints from an ongoing and ever-evolving array of threats, viruses, and ransomware attacks.

The company faces unique challenges and priorities when securing its operations. It must work tirelessly to keep up-to-date with the latest cybersecurity threats and trends, and adapt its security measures based on the dynamic threat landscape.

To do this, it needs timely and accurate information on emerging threats and vulnerabilities from around the world to proactively secure its operations. As cyber threats continue to evolve and target a wide range of platforms and operating systems, it requires a partner capable of providing a robust, versatile approach to cross-platform security.

The organization's cybersecurity requirements demand a deep level of technical analysis to understand the intricacies of actor TTPs and malware, so it needs a partner with the expertise to perform thorough and sophisticated technical analyses of both incidents and vulnerabilities.

The solution needed to provide comprehensive visibility over all the endpoints in the entirety of the company's network and give their security analysts real-time threat detection, investigation, and response capabilities. It also had to be able to handle the growing number of endpoints and the complexity of the organization's IT environment.

The Kaspersky solution

To meet the company's challenges, Kaspersky offered a fully integrated Threat Intelligence solution that delivered a comprehensive view of the global threat landscape, combining intelligence sources, threat data feeds, and in-house research to help protect against cyber threats. The full solution offered included **Kaspersky APT Intelligence Reporting, Kaspersky Threat Data Feeds, and Kaspersky Threat Infrastructure Tracking**.

Kaspersky APT Intelligence Reporting monitors even the most sophisticated targeted attacks and other cybercriminal activity, offering the organization customized and timely insights into high-profile cyber espionage campaigns.

Additionally, continuously updated Kaspersky Threat Data Feeds detects malicious activity on the company's enterprise network.

The implementation was managed centrally at the organization's Pennsylvania headquarters but covers 650,000+ sources of data and billions of records of telemetry data.

Security
When offering data analytics, there is no room for error

Detection
Kaspersky solutions boost detection rates and speed up response times

Compliance
Compliant with regional, national, and international regulations

Confidence
Well-researched products, timely intelligence, and data feeds

Kaspersky APT Intelligence Reporting

- Thanks to Kaspersky APT Intelligence Reporting, the company has access to exclusive intelligence on advanced persistent threats from over 200 threat actors in over 85 countries, which helps them to detect the most sophisticated and dangerous targeted attacks, cyber espionage campaigns, major malware, ransomware, and cybercriminal activity.
- Kaspersky tracks 1100+ threat actors and provides detailed descriptions on more than 200 through the Threat Intelligence Portal.
- Only a small number of Kaspersky's investigations are announced publicly, but all are reported to its active customers, such as this threat intelligence company. This helps them proactively deploy effective threat detection and risk mitigation controls for the associated campaigns.
- Each report provides an overview of the campaign, outlining industries and regions affected, probable attribution and objectives, as well as detailed technical analysis with a list of corresponding IoCs and YARA rules.

Kaspersky Threat Data Feeds

- The organization's threat intelligence is aggregated from fused, heterogeneous, and highly reliable sources such as Kaspersky Security Network (KSN) and Kaspersky's web crawlers, Botnet Monitoring service (24/7/365 monitoring of botnets, as well as their targets and activities) and spam traps.
- Kaspersky receives data from research teams, the deep web, partners and two decades of historical data about malicious objects.
- This aggregated data is carefully inspected and refined in real-time using multiple preprocessing techniques, such as statistical criteria, Kaspersky Expert Systems (sandboxes, heuristics engines, similarity tools, behavior profiling, etc.), analyst validation, and listing verification. All this means that this company's Kaspersky Threat Data Feeds contains thoroughly vetted threat indicator data sourced from the real world, in real time.

Kaspersky Threat Infrastructure Tracking

- This service delivers IP addresses of infrastructure connected to advanced threats. This helps security analysts working in CERTs, National SOCs, and National Security Agencies monitor the deployment of new malware so that they can take the required measures to mitigate ongoing and upcoming attacks.
- The service is updated daily with recent findings of Kaspersky Global Research and Analysis Team (GReAT) who have a proven track record in discovering APT campaigns across the world.
- For each IP address, there is a name of an APT group, operation, or malware it is associated with, Internet service provider, and autonomous system, collection of associated IP addresses hosting information, and dates when this was first and last seen.
- The IP addresses can be downloaded in a machine-readable format and can be uploaded to existing security solutions to automate detection.

"Kaspersky demonstrates a level of threat visibility that exceeds our expectations. They provide us comprehensive insights into a wide spectrum of cyber threats."

Chief Research Officer

"Kaspersky's main strengths lie in its global visibility and team of highly skilled technical analysts. Its extensive network of sensors and data sources ensures it can monitor and analyze threats on a global scale. This broad view allows it to identify emerging threats, trends, and vulnerabilities from around the world, helping clients like us stay ahead of evolving cybersecurity challenges.

We know we're getting well-researched products, alongside timely intelligence and data feeds. Being able to reach out to great researchers to dive deeper has been extremely beneficial to our organization."

Director of Technical Research

Outcomes

Kaspersky demonstrates a level of threat visibility that exceeds the company's expectations. Kaspersky provides comprehensive insights into a wide spectrum of cyber threats, ranging from common malware attacks to highly sophisticated and targeted threats.

This depth of visibility allows the organization to gain a holistic understanding of the threat landscape, which is crucial for its cybersecurity posture.

In the realm of cybersecurity and intelligence gathering, the detailed technical analysis provided in Kaspersky reporting has proven to be a pivotal tool in supporting its client's priority intelligence requirements.

By scrutinizing network traffic data using enrichment sourced from KSN, analysts can discern patterns and anomalies that point to potential threats or malicious activity. These findings are translated into signatures, which are subsequently deployed to network sensors to automate the detection and alerting process.

This approach not only enhances the timeliness of threat detection but also ensures a proactive stance to safeguard our client's critical systems and data. Furthermore, the integration of the shared YARA signatures plays a vital role in hunting for related host-based artifacts in its platform.

As a result, it can identify related binaries that share code with artifacts of high interest. The synergy between protocol analysis on the network level and YARA signature deployment at the host level forms a comprehensive approach to threat detection and mitigation.

Ultimately, the resulting telemetry generated from these processes yields invaluable insights, leading to the identification of new threat actors' TTPs that would not be possible without Kaspersky. This, in turn, allows for intelligence assessments to be continuously refined and strengthened, bolstering the organization's overall cybersecurity posture and enhancing its ability to address any emerging threats impacting its clients.

The company says that in its experience, one of the most crucial aspects of the Kaspersky solutions is the ability to provide timely and actionable intelligence. This means it receives real-time insights into potential threats and vulnerabilities, alongside clear and practical recommendations for mitigation.

While creating a polished product for distribution can take some time, the company adds that Kaspersky's "Threat Researcher Notes" publications have been both informative and timely, and have meant that information gets into its hands quicker.

Kaspersky has built its trust and confidence as a security partner through its commitment to transparency, technical excellence, and a rigorous approach to threat research. The client has said that Kaspersky's reports are not based solely on analytical conjecture but are backed by concrete technical data and analysis, which it has found to be hugely beneficial: **"Kaspersky's dedication to researching region-agnostic threats sourced from around the globe is a testament to its global perspective on cybersecurity."** – Chief Research Officer

The company concludes that the comprehensive threat intelligence provided by Kaspersky's solutions has played a critical role in helping it maintain a strong security posture.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

kaspersky BRING ON THE FUTURE