2022

Powering up protection with KATA

kaspersky BRING ON THE FUTURE

Powering up protection with KATA

When the research institute of one of this country's power innovators wanted to strengthen its existing cybersecurity protection and standardize their network security, they turned to Kaspersky.

This customer in East Asia is a wholly-owned subsidiary of a highly innovative and competitive state-owned enterprise, tasked with developing the country's power system. It provides comprehensive expertise, support and services for the production, operation, management and development of its parent company.

The customer also serves the needs of society by exploring electric power development and working to expand universal power services in the area. They are developing the high-end of the value chain, with a fully integrated Internet ecosystem to serve and support its parent company's international expansion. Their expertise encompasses cloud computing, big data, mobile apps, smart grids and artificial intelligence to R&D, production and sales of chips and terminals, smart grid and digital technology transfer, consulting and testing services – and everything in between.

The aim? To become an outstanding, highly competitive energy Internet service operation.

Finding the right partner

In the wake of the pandemic, the number of security events affecting OT/ICS infrastructure increased sharply, with 50% of organizations experiencing an increase in incidents compared with 2019. And the estimated total financial costs of industrial infrastructure cybersecurity attacks are 59% higher than the average for other large businesses.

In the face of this very specific evolving threat landscape, the customer recognized the need to strengthen its existing cybersecurity protection and standardize their network security. After evaluating a number of international vendors – and already a user of Kaspersky Hybrid Cloud Security – they chose Kaspersky; specifically, Kaspersky Anti Targeted Attack Platform (KATA) and KATA Sandbox.

"We chose Kaspersky for its unmatched detection and low false positive rates", explained a company spokesperson. "We specifically wanted a vendor with an international reputation and an outstanding track record of longstanding, a partner that would work with us to establish a highly professional and efficient network security protection for our parent company's power monitoring system."

The Kaspersky solution

The Kaspersky Anti Targeted Attack (KATA) Platform, with Kaspersky EDR Expert at its core, is an extended solution that delivers all-in-one protection against complex and targeted attacks. It's powered by advanced threat intelligence and mapped to the MITRE ATT&CK framework.

By automating data collection and analysis, and allowing investigation and incident response tasks to be performed from a single web console, the customer has the ability to increase incident processing speeds while boosting their IT security team's productivity. And with every potential entry point centralized under their control, they have full visibility into their entire infrastructure - network, web, email, PCs, laptops, servers and virtual machines.

Security researchers at the customer's in-house SOC Center particularly appreciate the ability to automatically identify and analyze suspicious files in their electric tuning system, which Kaspersky's technologies makes possible. Of course, the solution integrates seamlessly with a number of other existing solutions.

Solution highlights

Since roll-out, the customer is more than satisfied with their Kaspersky implementation. They draw particular attention to the solution's advanced capabilities and accuracy levels – and mention KATA Sandbox's performance when it comes to detecting bad links. KATA detects malware hidden inside links, to ensure that malware doesn't reach their intranet, where it could cause untold damage.

Other highlights for the customer include traffic import and API docking, automatic import of suspicious files, and malware analysis, all of which save time and resources, and boost their efficiency.

Because traditional defenses alone can't handle sophisticated threats and targeted attacks, a layered approach using advanced detection technologies is needed. The KATA Platform uses basic methods, such as a unique set of IDS rules for traffic analysis based on APT research and the global threat landscape, as well as advanced machine learning and artificial intelligence technologies to determine 'normal' behavior, while integrated real-time threat intelligence and customizable threat detection tools help detect multi-vector, non-malware threats.

"Kaspersky's high detection rates and accuracy, advanced technologies, and high flexibility with support for API interfaces and third-party integration, really set them apart", says the customer spokesperson. "We recommend Kaspersky to any business anywhere, and especially to those in our industry. Nothing compares."

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
www.kaspersky.com/fraudprevention

www.kaspersky.com

kaspersky BRING ON THE FUTURE