

ENTERPRISE SECURITY

WWW.ENTERPRISESECURITYMAG.COM

ISSN 2691-4034

EUROPE SPECIAL

THREAT
INTELLIGENCE
EDITION



RST Cloud

TOP
THREAT
INTELLIGENCE
SOLUTIONS
PROVIDERS
IN EUROPE
2023

Recognized by
ENTERPRISE
SECURITY



RST Cloud

The Art of Cyber Threat Intelligence: Managing Unstructured Data

Threat Intelligence requires a careful handling of large amounts of unstructured data at every stage, from consolidation and normalization to enrichment, false positive reduction, and prioritisation. Filtering out noise is an art by itself. The massive volume of information can make it challenging for cybersecurity professionals to quickly process and analyse all available cyber threat intelligence. But with the right approach and the support of a trusted threat intelligence partner like RST Cloud, these challenges can be overcome to uncover valuable insights and stay ahead of potential threats.

“
Our key objective is to relieve the stress of collecting and compiling threat intelligence and make it simple and accessible for consumption and application
”

RST Cloud provides flexible and scalable threat intelligence and data enrichment solutions that assist businesses of all sizes in their day-to-day cybersecurity operations. Using its smart solutions, cybersecurity professionals can easily and efficiently access a comprehensive collection of globally available cyber threat intelligence. This includes capabilities for consolidation, normalization, enrichment, filtering, and scoring, providing a streamlined and trustworthy method for staying ahead of potential threats.

“One of our key objectives is to alleviate the burden of collecting and aggregating threat intelligence for our clients. We aim to comprehensively gather this information, contextualize it to the fullest extent possible, and deliver it to our customers in a convenient format,” says Anna Mikhaylova, the Director of Business Development at RST Cloud.

Context makes difference. It can be daunting for cybersecurity professionals to assess the threat level of observed indicators of compromises (IoC) in the absence of any context and swiftly determine an appropriate course of action. RST Cloud's threat intelligence engine aggregates data from numerous sources, sandboxes, RST Cloud honeypot network, analyses TI reports, and uses a combination of proprietary methods to consistently and reliably contextualise them. IoCs are enriched with information on threat

categories, attributed malware families and threat actors, common vulnerabilities. By utilizing algorithms to assign scores based on source confidence, context, and relevance, the engine prioritizes indicators and helps users identify the most important threats. Additionally, the engine eliminates irrelevant data, reducing the risk of false positives and negatives in IoCs. With this comprehensive and methodical approach to consolidate, verify, contextualize, and score threat data, cybersecurity professionals can make informed decisions and streamline their workflow while accurately evaluating the threat level of each IoC match.

RST Cloud offers RST Threat Feed via API, with seamless integrations into popular security infrastructure and workflows, including SIEM, SOAR, NGFW, and TIP. This convenience allows users to effortlessly integrate threat data into their existing security environment. In addition, TI analysts can have access to the RST Report Hub, a library of public CTI reports from various sources, even if the original source is deleted. The reports come complete with a wealth of metadata, including threat names, geodata, hacker tool names, affected software, APT groups, and many more details. Users can also download a PDF version of a report and view related indicators of compromise (IoCs) for deeper analysis.

In the current scenario, businesses are between a rock and a hard place regarding cybersecurity as threats come from every direction, putting each aspect of their IT operations at risk. RST Cloud goes above and beyond in providing an accurate and contextualised understanding of cyber threats. Its team of highly experienced professionals has developed a solution that enables a calculated and systematic approach to ingest high-fidelity threat data, analyse that data, interpret context, develop proactive strategy, and respond to alerts in tune with their priority and thus accelerate incident prevention and response.

In today's rapidly evolving threat landscape, businesses are facing increasing pressure to protect their IT operations from a variety of cyber threats. RST Cloud rises to the challenge with its unparalleled threat intelligence solutions. The RST Cloud's experts have crafted a comprehensive approach to collecting, analysing, and contextualising threat data. This enables organisations to proactively develop strategies, prioritize alerts, and accelerate incident prevention and response with a calculated and systematic approach. **ES**

Anna Mikhaylova, ▶
Director of Business Development



RST Cloud



The annual listing of 10 companies in Europe that are at the forefront of providing Threat Intelligence solutions and impacting the marketplace