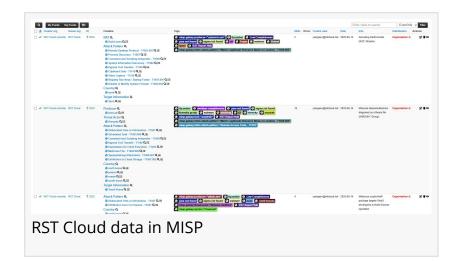# RST Cloud Brings Threat Intelligence from Blogs and Reports Straight into Your MISP

SYDNEY, AUSTRALIA, June 24, 2025 /EINPresswire.com/ -- Security and threat intelligence (TI) teams are increasingly overwhelmed by the volume and complexity of threat data published daily across research blogs, technical articles, and PDF reports - often in multiple languages. Manually processing and integrating this information into platforms like MISP (Malware Information Sharing Platform) consumes valuable analyst time and can lead to missed insights.

RST Cloud data in MISP

RST Cloud announces an automated integration solution that brings clarity and efficiency to this challenge - seamlessly importing multilingual, high-quality threat intelligence into MISP. To support global coverage, the platform automatically translates articles from languages such as Chinese, Russian, Korean, Italian, French, Japanese and many more into English. It extracts summaries, key facts, and core insights, which are then included in MISP as event descriptions and analyst notes, giving users clear context and fast readability. Indicators of Compromise (IoCs) from these reports are intelligently filtered, with noisy indicators labeled to reduce the risk of false positives in detection pipelines.

"

Our mission is to eliminate the noise and effort that stand between analysts and the insights they need"

Yury Sergeev, Director of RST Cloud

Powered by automation, machine learning, and large language models, RST Cloud's engine continuously collects, classifies, and filters threat reports and blog posts from public sources. Using a decision-tree-based classifier, the system ensures only original and relevant content is ingested - excluding duplicates and rewritten material unless it offers new intelligence, such as additional IoCs or novel TTPs.

Each report is converted into a comprehensive STIX 2.1 graph, preserving all critical threat

objects and their relationships. These are then translated into MISP's native format, including event tagging and Galaxy mapping where applicable. A PDF copy of each original report is archived and attached to ensure traceability and offline access.

To further enhance the value of MISP, RST Cloud offers two powerful extensions:
- RST Threat Feed delivers a constant stream of IoCs, providing security teams with near real-time visibility into emerging threats. The feed is customisable, allowing teams to ingest only high-risk or attributed IoCs, ensuring focus and relevance.
- RST Threat Library enriches MISP with structured definitions of threat actors, malware, campaigns, TTPs, vulnerabilities, and more. Delivered as a dedicated Galaxy with four clusters - Threat Actors, Malware, Campaigns, and Tools - this extension enables improved context, threat clustering, and more actionable intelligence.

"Our mission is to eliminate the noise and effort that stand between analysts and the insights they need," said Yury Sergeev, Director of RST Cloud. "With our integration, MISP users can finally automate the ingestion of public threat research and spend their precious time on analysis, not manual data processing."
Organisations looking to maximise the value of their threat intelligence platforms can now rely on RST Cloud to automate the operationalisation of threat intelligence from research blogs, technical articles, and PDF reports. The platform unifies multilingual sources, eliminates manual entry, and delivers timely, relevant, and high-fidelity intelligence directly into existing MISP environments.

Learn More
RST Cloud Website: https://rstcloud.com
Integration Details on GitHub: https://github.com/rstcloud/rstcloud-import2misp

Marketing
RST Cloud
+61 2 8006 4567
email us here