CASE STUDY

CUSTOMER:
Global Investment Firm

HEADQUARTERS: United States

EMPLOYEES: 1,300

INDUSTRY: Financial Services

Global Investment Firm: Streamlining YARA Rule Management with Spectra Analyze

A leading global investment fund selected ReversingLabs Spectra Analyze to help its team streamline their YARA workflows and ruleset management.

With a growing number of YARA rulesets from multiple sources, they needed to implement a solution that would drive higher quality rulesets with the most impact – quality vs quantity.

A More Impactful YARA Workflow

YARA plays a large role in the company's threat detection and hunting efforts. The company harvests YARA rulesets from various sources, then publishes rules to multiple third-party security tools. However, its existing workflow of testing and validating rules for deployment was becoming inefficient and less effective.

> **" Makes the workflow very 'set and forget' in most cases. "**
>
> Sr. Threat Researcher

CHALLENGES:

- Maintaining YARA rulesets from multiple sources
- Lack of integration between disparate YARA repos
- Difficulty validating YARA rules

SOLUTION:

- Spectra Analyze provides powerful YARA capabilities for developing, testing, deploying, and managing advanced rulesets with ease

ReversingLabs provided a better way. With Spectra Analyze, the company's security team can easily and automatically import, update, and sync YARA rulesets from third-party sources, then quickly validate rules against RL's global threat intelligence data corpus – all from a single interface.

This has not only simplified the management and administration of their multi-source YARA rulesets, but has also resulted in greater workflow efficiencies and more effective malware detection.

Learn More About RL Solutions

CONTACT US TODAY

RESULTS:

- Spectra Analyze centralized and simplified YARA rule management
- Allowed for easy integration with third-party repositories
- Enabled security team to automatically track and store rulesets from multiple sources
- Significantly improved YARA rule validation in efficacy and speed

RL PRODUCTS:

- Spectra Analyze

ABOUT REVERSINGLABS

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com