SOLUTION BRIEF

REVERSINGLABS

Enrich Your SIEM / SOAR with Context-Rich File Intelligence

An ever-growing threat landscape and expanding attack surface, combined with a lack of people, expertise and budget has organizations searching for ways to increase SOC efficiency and maximize existing security investments, especially expensive SIEM / SOAR solutions.

Challenges

- Too many alerts creates information overload, making it difficult to filter out noise and focus on priorities
- Insufficient / incomplete file intelligence and lack of context hinders investigations and increases response times
- Lack of staff and expertise to operate and tune SIEM/SOAR platforms decreases value and return on investment

RL Benefits

- Triage alerts faster with instant file reputation lookups and verified threat classifications
- Improve analyst efficiency with human-readable file behavior indicators and easy-to-understand threat intelligence
- Feed high-confidence, context-rich indicators into SIEM and analytics platforms for more effective correlation
- Enhance automated, playbook-driven response by harnessing real-time, high-fidelity file and network intelligence
- Improve malware detection across the entire organization with highly scalable file analysis

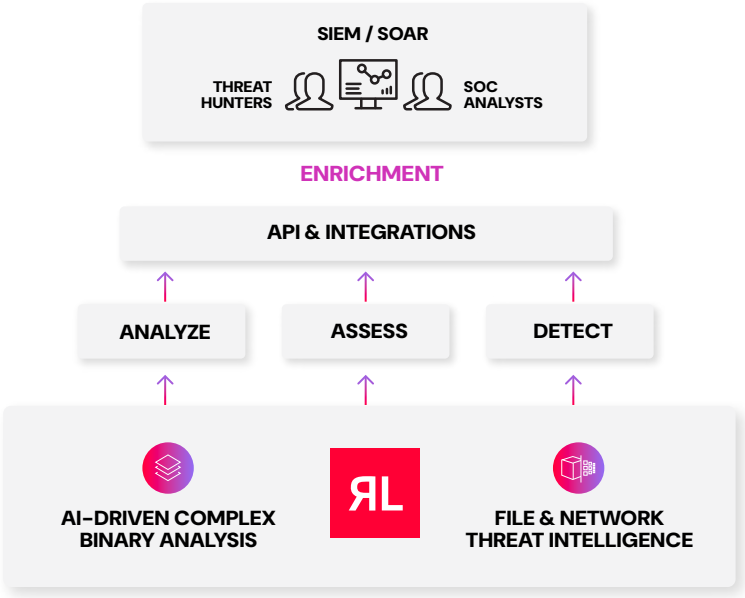
How ReversingLabs Can Help

One of the greatest unmet needs with SIEM and SOAR is obtaining threat intelligence with the necessary context and relevance to be truly actionable, in addition to having an effective level of automation to drive faster detection and response times.

ReversingLabs' helps organizations and under-resourced security teams drive up their operational efficiency by empowering them with the right intelligence, in the right place, at the right time. This starts with RL's AI-driven complex binary analysis, which can fully deconstruct any file or object down to its base components, extract all internal indicators and metadata, and provide definitive threat verdicts, in real time. Organizations get next-level malware and file intelligence with detailed threat context to enrich SIEM/SOAR platforms, enabling security teams to remediate threats faster. No other solution can match the speed or depth of ReversingLabs' proprietary analysis technology.

With ReversingLabs you can:

- Enrich SIEM and SOAR with context-rich metadata and verified threat intelligence from the industry's largest repository of continuously curated malware and goodware
- Leverage an extensive REST API and out-of-the-box integrations to plug into existing security tools and automated workflows with ease
- Aggregate and enrich multiple sources of data while performing real-time threat classification and simultaneously applying YARA rules at a massive scale



Benefits for SOC Analysts, Incident Responders, and Threat Hunters

Tier 1

Persona-based benefit

Tier 1 and junior analysts performing initial alert triage are empowered with automated malware analysis and decisive threat classifications that drastically reduce false positives and allows for more effective prioritization. Not only does this mean fewer alerts to chase down, but it also reduces what needs to be escalated for higher tier analysts for further investigation. And, with human-readable threat indicators and intelligence that's easy to interpret, ReversingLabs helps upskill and educate lower tier analysts.

Tier 2

Persona-based benefit

Tier 2 analysts and incident responders are enabled with verified file and network intelligence to rapidly assess an object's threat capability and risk impact. High-value threat indicators and contextual metadata can be automatically fed into the SIEM for better event correlation and faster investigations, which in turn enhance SOAR playbooks and response.

Tier 3

Persona-based benefit

Threat hunters benefit from advanced search and hunting techniques, including retro-hunting, to detect threats beyond SIEM capabilities. YARA rule matching can be performed across local datasets and RL's global threat data corpus of more than 40 billion goodware and malware samples. Hunters can import, build, test, and deploy rules with ease to provide another level of threat detection for the organization.

Use Case 1

Obtaining Enriched File Intelligence

Challenge:

Without enough context in file intelligence data, security teams are unable to understand the threat and take action in a timely manner. Analysts need to be able to quickly and accurately triage security events, prioritize the event based on severity, decide if the event needs further investigation or pass the event over to the response team. However, most of the time, the analyst does not have the information needed to make the determination.

Solution:

ReversingLabs provides much needed file intelligence to automatically enrich SIEM/SOAR platforms and drive faster, more informed response actions. With RL, analysts can immediately see if the underlying file is 'known good', so the event can be deprioritized. Similarly, if the file intelligence shows the malware type to be a simple form of adware, the analyst can deprioritize the event. If the threat level is high and the malware is verified and known (such as Trojan malware attack), the analyst can pass the event over to the response team for rapid containment and mitigation.

Use Case 2

Optimize Response And Containment

Challenge:

Incident responders need more in-depth information about events so the appropriate playbooks for both response and containment can be activated and produce a high degree of assurance that the threat has been mitigated. Pieces of the required information might come from the SIEM or other detection tools (EDR, NTA, etc.) or investigations. Regardless, the responder must bring together all disparate information to understand all aspects of the threat, including the malware type, infection process, and attack stages.

Solution:

ReversingLabs' integration with incident response tools creates a single and unifying view of all incident-related malware. If the incident response analysts find that they lack the details or context required to make accurate playbook activation decisions, the response tool can automatically query ReversingLabs' file reputation and intelligence service to instantly fill in any missing information. As a result, SOAR tools and response workflows are optimized, MTTR is significantly improved, and risk mitigation assurance is increased.

Use Case 3

Scalable Threat Classification and Orchestrated Response Processes

Challenge:

Large enterprises need to manage and secure an ever-growing volume of global traffic emanating from multiple sources and consisting of varying types of incoming files and objects. The volume, velocity, and variety of incoming traffic creates many ways for threats to enter the organization unchecked. In this situation, surfacing malware threats hidden within files becomes critical in the detection process.

Solution:

ReversingLabs' can automatically analyze and classify files and objects in real-time and at massive scale, with support for millions of files per day. Inputs to the RL threat classification engine include email, endpoints, cloud storage, network shares, web application data, and collaboration tools. The result is verified threat classification and rich, in-depth malware intelligence that can be delivered into a SIEM or SOAR solution via an extensive API and out-of-the-box integrations. Regardless of whether the input is threat classification, file or network reputation data, industry-specific threat intelligence, vulnerability information, or other malware details, ReversingLabs helps optimize the delivery of actionable information across detection and response workflows to increase operational efficiencies and threat surface coverage.

SIEM/SOAR Integrations

Additional Resources

Increase Your SIEM and SOAR Return on Investment with ReversingLabs

Read Blog

Better SOC/SOAR Efficiency with Better Threat Intelligence:
3 Ways to Get There

Watch Video

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.

Get Started!

We'll Show You How ReversingLabs
Detects and Analyzes More Hidden Threats

REQUEST A DEMO

reversinglabs.com

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com