

Analyst1 and ReversingLabs

Consolidated Malware Intelligence for Seamless Threat Operations

Meet Analyst1

- Analyst1 is an orchestrated threat intelligence platform that enables security teams to operationalize intelligence across their existing security ecosystem.
- With native integrations into leading SIEM, SOAR, and EDR solutions, Analyst1 allows teams to aggregate, enrich, and manage threat data for streamlined detection and response. By supporting content deployment directly from the platform, teams can proactively mitigate known threats – reducing response latency and eliminating manual processes.
- Analyst1 also centralizes intelligence workflows, minimizing noise and enabling analysts to rapidly answer critical questions across their infrastructure: who is targeting us, what tactics are being used, when were we impacted, and from where is the threat originating?

Key Use Cases for Analyst1

Use Analyst1 to:

- Centralize and operationalize threat intelligence across your tools
- Enrich detections with deeper context for faster decisions
- Break down workflow silos and reduce response times



A1DEFENDER
PARTNER PROGRAM

Meet ReversingLabs

ReversingLabs is the premier name in malware analysis and software security, trusted by the Fortune 500 and leading cybersecurity vendors.

With proprietary, high-speed, deep binary analysis, plus multi-mode threat classification, and support for over 4800 file types, ReversingLabs delivers the fastest, most accurate malware intelligence in the industry.

Use ReversingLabs to:

- Validate and prioritize alerts using definitive threat classifications and clear context.
- Support threat hunting and detection rule creation to identify and prevent attacks.
- Enrich security tools with real-time, high-fidelity intelligence on emerging and evolving threats.

Defense Based on Intelligence from Analyst1 and ReversingLabs

Deeper malware context for faster threat mitigation in your environment

ReversingLabs delivers malware intelligence directly into Analyst1, providing a consolidated view that helps analysts prioritize, detect, and respond to active threats. Additional context is provided from third-party sources and integrated into Analyst1 for deeper insights into emerging threats and attack patterns.

The Analyst1-ReversingLabs integration allows analysts to identify relationships between malware and adversary activity. This supports the detection of threats earlier and more decisive action, reducing exposure to potential attacks.

Direct Impact

- **Enhanced Threat Analysis:** Analyst1 and ReversingLabs deliver enriched malware context that allows for faster and more precise investigations.
- **Reduced Risk Exposure:** Faster detection and better clarity helps teams minimize disruption, improving operational resilience. Our integration helps close gaps in visibility and contain threats before they escalate into incidents.
- **Expanded Attack Surface Coverage:** By correlating third-party intelligence, teams using Analyst1 and ReversingLabs gain a comprehensive view across their full attack surface.