Enhance Your SIEM / SOAR with Context-Rich File Intelligence

Challenges

- Too many Alerts create information overload, making it difficult to filter out noise and focus on priorities.
- Insufficient actionable file intelligence context increases MTTR
- Finding the right people to operate and tune the SIEM, as well as to respond to incidents, is difficult.

Benefits

- Obtain more effective automated, playbook-driven response by harnessing rich, real-time threat intelligence.
- Triage alerts from anywhere in your environment using file reputation and file analysis in your SOAR workflows.
- Improve analyst efficiency by centralizing analysis and collaboration.
- Improve detection across multiple sources by classifying all files with enriched data at massive scale.

Security operations teams struggle to keep up with the deluge of alerts from an increasing arsenal of threat detection technologies. With today's challenges from a growing hostile landscape, combined with a lack of people, expertise and budget, organizations must drive toward optimizing their SIEM and SOAR solutions in order to get the most ROI out of their expensive investment.

One of the greatest areas of unmet need with SIEM and SOAR is obtaining the right intelligence, actionable rich context and effective level of automation to help you increase your detection of and response to targeted attacks and breaches.

Integration Features

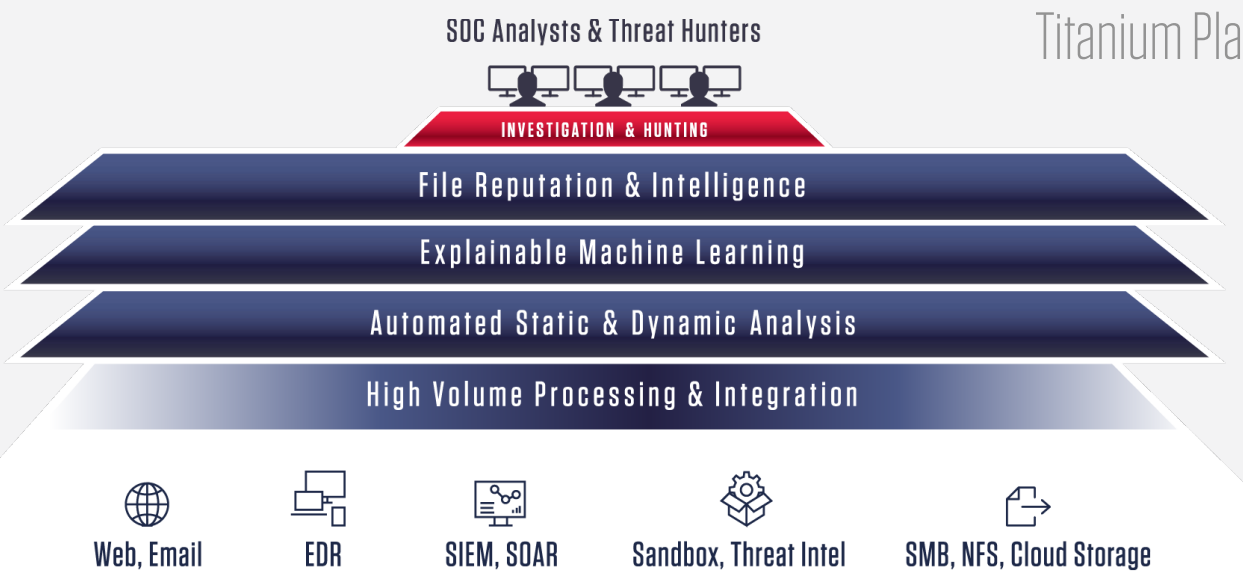
ReversingLabs provides comprehensive, automated static and dynamic analysis on files entering an organization which generates a unique source of threat intelligence and consolidated metadata for SIEM or SOAR solutions. This rich, highly relevant file intelligence enhances correlation and visibility of malware from any SIEM or SOAR connected source and promotes more effective and efficient malware identification and response.

With ReversingLabs you can:

- Automatically enhance SIEM or SOAR with rich file intelligence to quickly identify a file's threat level and severity, name, and type.
- Access the industry's most up-to-date, comprehensive intelligence on malware and goodware through a constantly curated database of over 25 billion samples.
- Aggregate and enrich multiple sources of data while performing near real-time classification and simultaneously applying YARA rules, at massive scale.

SIEM/SOAR Integrations

splunk>enterprise · Phantom · resilient an IBM Company · Azure Sentinel · Azure Logic Apps · CORTEX XSOAR BY PALO ALTO NETWORKS



ReversingLabs Simplified Block Diagram providing actionable intelligence to SIEM & SOAR solutions

Benefits for Malware Analysts and Threat Hunters

TIER 1

Persona based benefit

ReversingLabs malware analysis solutions enable Tier 1 analysts to accurately classify file reputation and reduce false positive alerts. Each file is unpacked and analyzed using static file analysis and multiAV scanners, enriched with dynamic analysis IOCs, providing a zero-trust approach. Files are classified as either goodware, potentially malicious, highly malicious or not seen before. Organizations are able to save time by escalating only files and objects that need additional investigation. Files and data are kept private unless organizations choose to share with the community. ReversingLabs also offers a solution for off-the-grid, fully air-gapped environments.

TIER 2

Persona based benefit

ReversingLabs malware analysis solutions provide seamless integrations with SOAR and sandbox solutions. Tier 2 analysts can quickly determine an object's threat capability and risk impact via 3000+ threat indicators generated by static and dynamic file analysis, in addition to file reputation provided by machine learning indicator correlation.

TIER 3

Persona based benefit

Threat hunters benefit from using ReversingLabs malware analysis solutions to perform advanced private searches and hunting techniques, including local, cloud, and retro yara hunting capabilities. ReversingLabs provides out-of-the box yara rules to accelerate threat hunting team maturity. A user-friendly interface enables teams to develop new yara rules specific to their needs, providing additional security measures to detect potentially malicious threats beyond SIEM (threats off of logs) and EDR capabilities. Hunting rules can be deployed and tested against ReversingLabs 25B+ file repository via retro hunting.

Use Case | 1

ENRICHING HASH METADATA FOR BETTER THREAT ANALYSIS

Challenge: Not enough context in file intelligence data to understand the threat and be actionable for security teams to be proactive in a timely manner.

Solution: ReversingLabs performs high-speed static analysis to classify files (good, malicious, suspicious, unknown), rank severity level and provide enriched context in near real-time. File reputation can be supplied from ReversingLabs with a query directly from the SIEM or SOAR console. Files requiring deeper investigation can be moved to the ReversingLabs Cloud Sandbox for dynamic analysis.

Benefit: Provides much needed file intelligence to SIEM and SOAR for highlighting malware that would normally go undetected or even classified. The enriched information helps analysts understand and prioritize threats. And with automation, analysis is faster with less resources and expertise required.

Use Case | 2

ANALYST WORKBENCH FOR ADVANCED PRIVATE SEARCH AND HUNTING

Challenge: There is no unified platform for advanced analysis on specific malware, or groups of malware, or to find functionally similar malware and perform pivots on IOCs to better understand threats. Analysts are forced to navigate between siloed security tools which are also not designed for collaboration, and in most cases, open to privacy concerns.

Solution: ReversingLabs Malware Analysis Workbench provides a seamless integration with a SIEM or SOAR. The workbench uses ReversingLabs file intelligence repository with over 25 billion samples of goodware and malware, holding rich context and continually updated with threats in-the-wild.

Benefit: In a single click, a user can switch to the ReversingLabs console and quickly determine relevant indicators to help prioritize threats and determine the next course of action, all in a safe and private environment.

Additional Resources

Get Started!

WE'LL SHOW YOU HOW REVERSINGLABS DETECTS AND ANALYZES MORE HIDDEN THREATS

www.reversinglabs.com

REQUEST A DEMO

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

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com