ReversingLabs Malware Intelligence Enriches Splunk Data for Improved Correlation and Threat Detection

Accelerate decisions on threats with advanced visualization, integrated access to intelligence

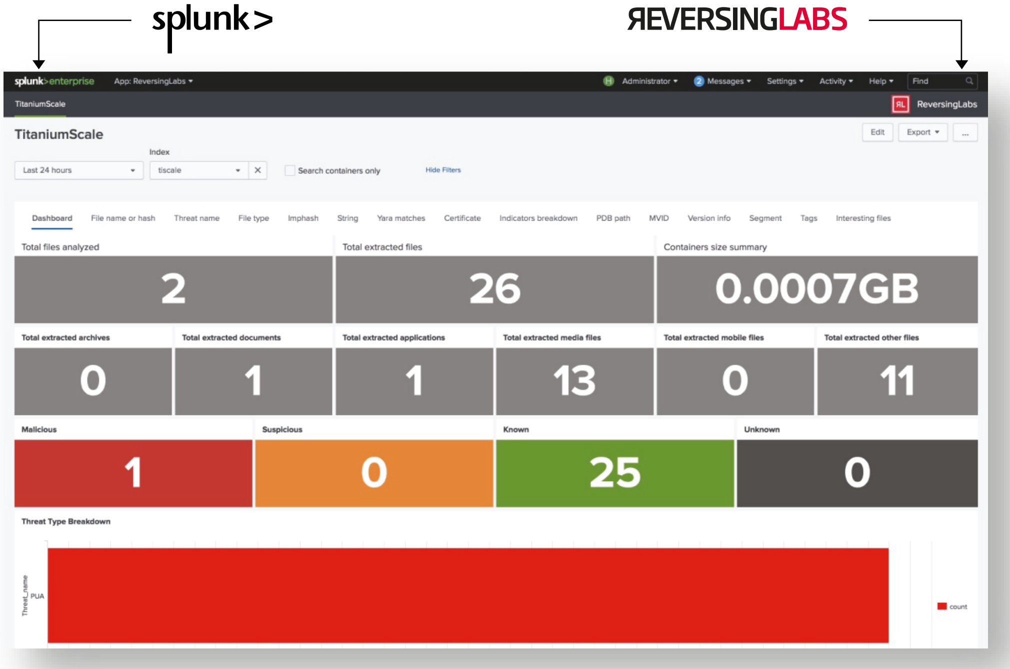
ReversingLabs has built an app that enriches Splunk data with next generation malware analysis and threat intelligence. Splunk ingests detailed malware analysis performed on every file by ReversingLabs' TitaniumScale platform to enhance threat hunting, identification, correlation and response. The app enables quicker malware identification and visualization in the Splunk dashboard by providing relevant data at analyst's fingertips. With 1-click, security teams can also seamlessly pivot to the ReversingLabs A1000 Malware Analysis Platform for detailed investigation of malware threats. Splunk's value lies in the vast amount of security data it correlates, analyzes and displays. Splunk's value increases with the relevance of the data collected. ReversingLabs provides comprehensive automated static analysis on the files entering an organization which generates a unique source of threat intelligence and consolidated metadata which may be visualized in the Splunk dashboard, exposing undetected malware that evades security defenses. This rich, highly relevant threat intelligence enhances correlation and visibility of malware from any Splunk connected source and promotes more effective and efficient malware hunting, identification and response.

Using this integrated dashboard, security teams can now instantly make decisions on advanced threats without having to piece together malware data from multiple sources. Our TitaniumScale platform scales up to inspect millions of files per day and is proven in the largest global organizations for its effectiveness against advanced threats, including polymorphic and zero-day malware.

Solution Highlights

Correlate. Analyze.
Instantly Display.

- **Deep malware analysis results from files entering an organization can be searched, correlated and displayed in Splunk to catch advanced malware.**
- **ReversingLabs TitaniumScale platform extracts and stores metadata and objects from files to support advanced hunting based on file attributes.**
- **Automated static analysis enables file assessment at scales that are orders of magnitude larger than sandbox products (e.g. millions of files daily).**



TitaniumScale

Index

Last 24 hours ▾ | tiscale ▾ ✕ | □ Search containers only

Total files analyzed: 2

Total extracted files: 26

Containers size summary: 0.0007GB

Total extracted archives: 0

Total extracted documents: 1

Total extracted applications: 1

Total extracted media files: 13

Total extracted mobile files: 0

Total extracted other files: 11

Malicious: 1

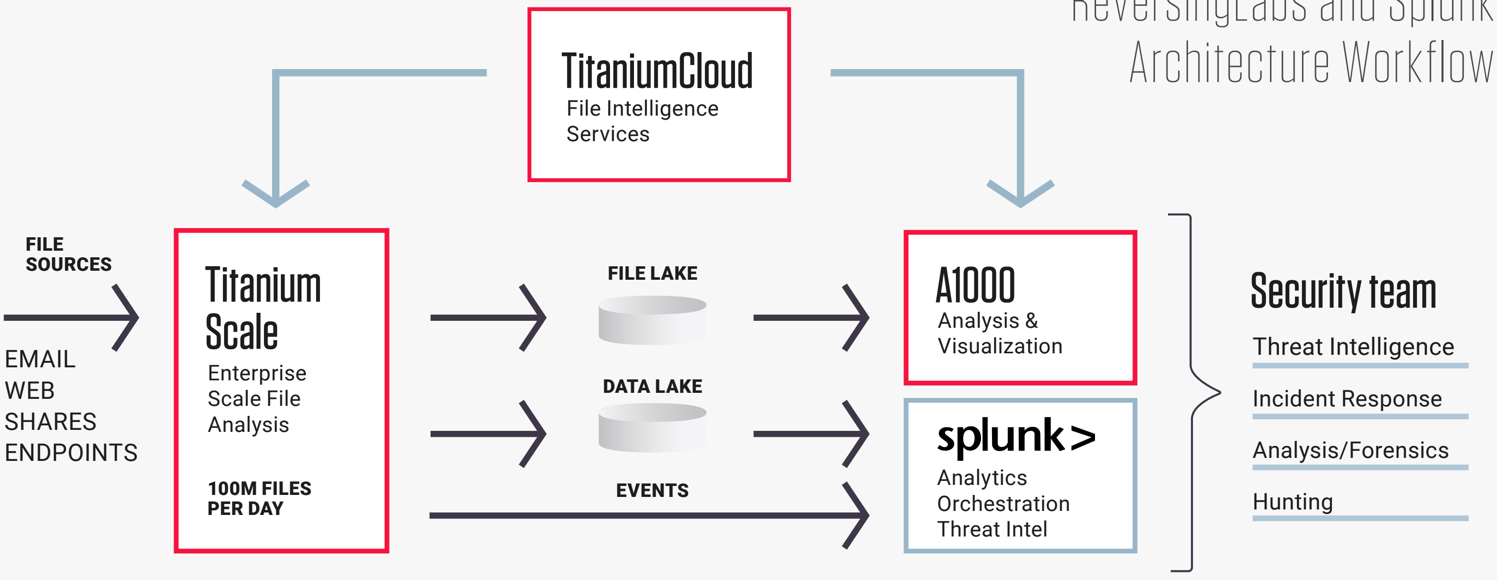
Suspicious: 0

Known: 25

Unknown: 0

Threat Type Breakdown

ReversingLabs and Splunk Architecture Workflow



How It Works

ReversingLabs created a plug-and-play app for Splunk to provide unprecedented visibility into SIEM events so security ops teams can rapidly identify malware embedded in files:

- All files are sent to TitaniumScale where static analysis is performed along with functional malware similarity analysis to expose threats. The results are enriched with data from RL's TitaniumCloud file intelligence platform and sent to Splunk.
- In Splunk, the TitaniumScale report is correlated with other available Splunk data and automatically generates an alert for suspicious or malicious activity.
- Extracted files and metadata are stored in a data/file lake to support advanced hunting, YARA matching and searching file profiles.
- When analysts receive alerts for suspicious files, they can click on the A1000 URL within the Splunk GUI to access detailed malware analysis which can be used for threat hunting and YARA rule generation.

The ReversingLabs A1000 is a high-speed automated static analysis platform and is the leading global solution for hunting, analyzing and investigating unknown malware. The A1000 automates malware analysis at enterprise scale by integrating external and internal intelligence into one place. The A1000 finds malware threat indicators and functionally similar malware by correlating incoming malware indicators with TitaniumCloud's in-the-wild file reputation intelligence to create in-depth, rich context and threat classification on over 7 billion files across all file types. It also detects functionally similar malware by visualizing malware status changes of malware families that have morphed over time via obfuscation and other techniques. It comes with API's to integrate with automated workflows, a dedicated database for malware search, global and local YARA Rules matching, as well as integration with 3rd party sandbox tools. The A1000 also accelerates analysis from the helpdesk to an 'analyst workbench' for deeper threat analysis for security teams that have various levels of experience.

ReversingLabs TitaniumScale is a high-volume file classification platform that assesses all files entering an enterprise to provide extensive visibility into embedded malicious code. TitaniumScale uses static analysis technology to automatically analyze millions of files pushed to it from web traffic, email gateways, file transfers, endpoints and storage to expose detailed malware metadata embedded in files. This data enables analysts to hunt for and expose unknown malware that enters organizations through cracks in their security infrastructure. It extracts thousands of internal and external indicators and classifies each file by reputation, threat level and severity status. All files are also checked against ReversingLabs' comprehensive file reputation database of 7 billion goodware and malware files for complete classification which are then automatically pushed to Splunk, orchestration and analytics platforms to accelerate response to current and past events.

REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com