REVERSINGLABS

ReversingLabs Enhances Tanium with Industry-Leading File Reputation

ReversingLabs Accelerates Identification and Response to Threats

ReversingLabs is the industry leader in advanced malware analysis and file threat intelligence. Tanium is a single point of control to manage and secure endpoints. The two companies have developed a joint solution that seamlessly integrates ReversingLabs' file reputation data and context-rich intelligence with Tanium output so security teams have the latest malware insights to accelerate triage and response.

By providing authoritative file intelligence to Tanium Threat Response in real time, it's now significantly easier to quickly detect suspicious and malicious files on endpoints. This means security teams can better prioritize and accelerate their response to advanced threats.

Solution Highlights

- Reduces noise and speeds triage by accurately detecting suspicious files and malware on endpoints
- Analyzes all file hashes from endpoints in real time to provide timely and accurate endpoint data
- Leverages the world's largest authoritative reputation database of goodware and malware from ReversingLabs' 40+ billion file repository
- Enables SOC teams to more effectively prioritize and respond utilizing Tanium Threat Response

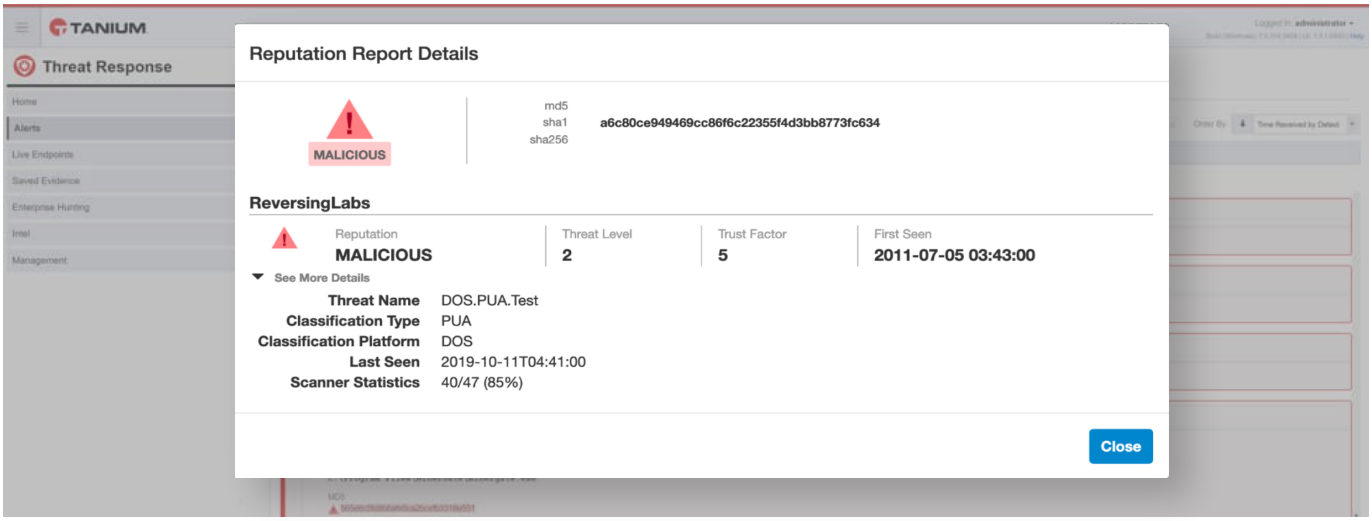
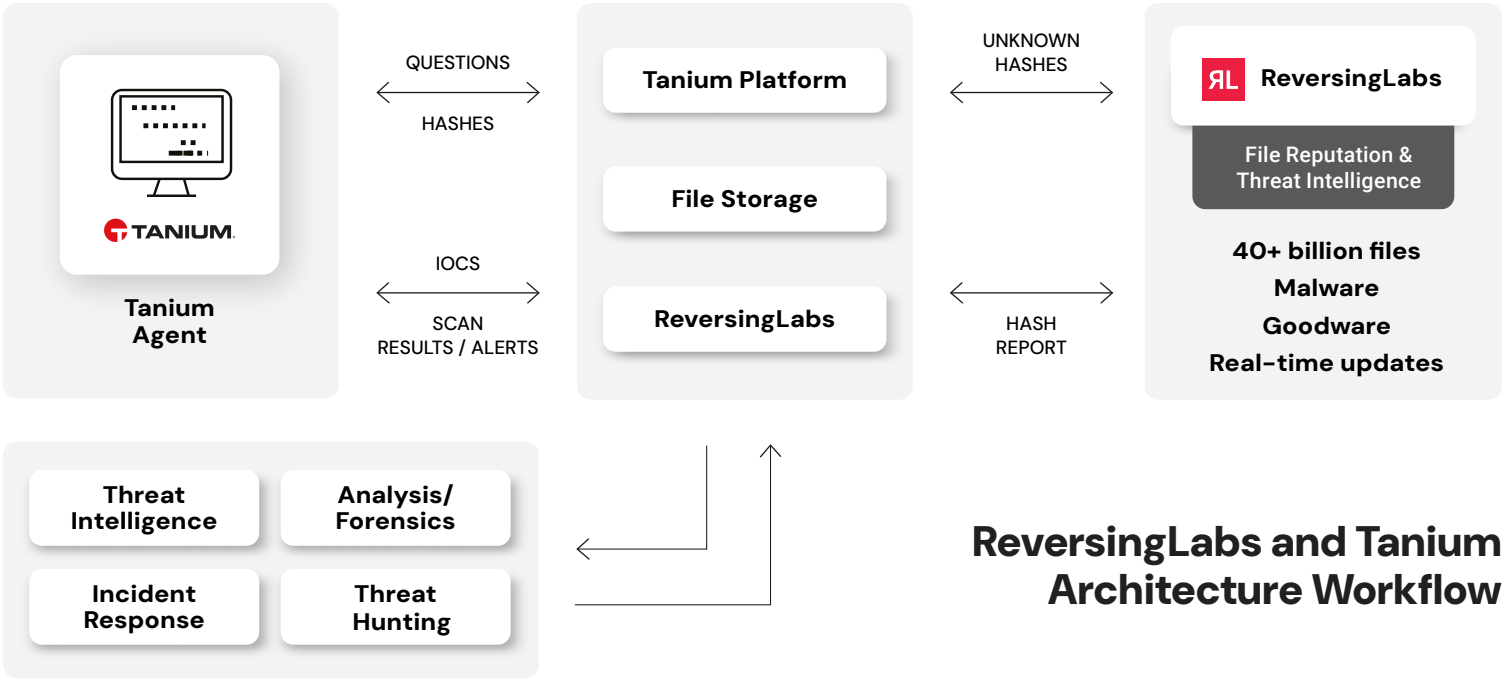


Figure 1: File reputation details from ReversingLabs displayed in Tanium UI to speed response



ReversingLabs and Tanium Architecture Workflow

How It Works

ReversingLabs integrates with Tanium Threat Response to determine file reputation and support deep file analysis for threat hunting. Our plug-and-play integration allows SOC teams to instantly determine reputation and obtain critical metadata through automatic file submissions. As a result, analysts are able to gain a clear and in-depth understanding of files that are of particular interest.

- File hashes are forwarded from Tanium Threat Response to ReversingLabs to automatically identify both goodware and malware
- ReversingLabs' threat intelligence service looks up hashes against its authoritative database that includes reputation information on over 40 billion files
- Tanium uses the results supplied by ReversingLabs to identify malware present on endpoints and to enrich data to accelerate triage and response
- In addition to reputation checks, files can be submitted to ReversingLabs' malware analysis platform for deep binary analysis, providing detailed classification and rich metadata, including thousands of unique file behavior indicators

WORLD'S MOST TRUSTED FILE REPUTATION SOURCE

OVER 40 BILLION SEARCHABLE FILES

LARGEST DATABASE OF MALWARE & GOODWARE

20K FILE BEHAVIOR INDICATORS

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.

PB-Rev-11.13.24

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com