REVERSINGLABS

TANIUM.

ReversingLabs Enhances Tanium with Industry-Leading File Reputation

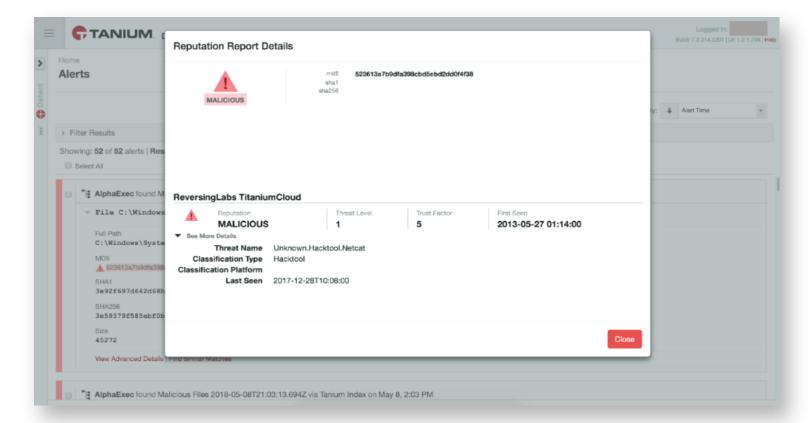## ReversingLabs Accelerates Identification and Response to Threats
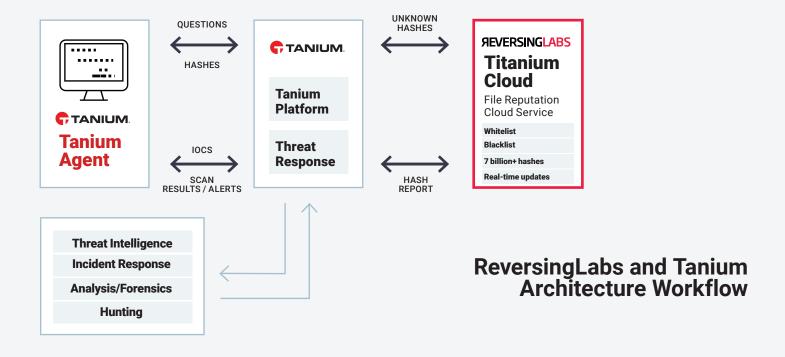
Solution Highlights

- **Reduce noise and triage effectively 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**

- **Comprehensive view powered by RL's 7 billion authoritative file reputation cloud that includes the world's largest whitelist and blacklist**

- **Analysis helps SOC teams prioritize and respond effectively utilizing Tanium Threat Response**

ReversingLabs is the industry leader in enterprise scale file intelligence, hunting and analysis. Tanium is a single point of control to manage and secure enterprises.

The two companies have developed a joint solution that seamlessly integrates file reputation intelligence with Tanium output so security teams have the latest malware data 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.

ReversingLabs and Tanium Architecture Workflow

WORLD'S BEST FILE REPUTATION SOURCE

7B+ Hashes

Whitelist & Blacklist

8M daily reputation updates

How It Works

ReversingLabs integrates with Tanium Threat Response, the combined plug-and-play integration automatically submits file hashes from an endpoint to ReversingLabs to instantly determine reputation status and obtain critical metadata.

- Hashes of suspicious files are forwarded from Tanium Threat Response to ReversingLabs TitaniumCloud to automatically identify goodware and malware.

- TitaniumCloud's file intelligence service looks up hashes against the authoritative whitelist and blacklist database that includes reputation information on over 7 billion files and returns file reputation intelligence.

- Tanium uses the results supplied by ReversingLabs to identify malware present on endpoints and to enrich data to accelerate triage and response.

ReversingLabs File Reputation Service

Industry-leading authoritative file intelligence solution with up-to-date threat classification and rich context on over 7 billion goodware and malware files. ReversingLabs does not depend on crowdsourced collection but instead curates the harvesting of goodware directly from the source and malware files from diverse malware intelligence sources. All files are processed using unique ReversingLabs' File Decomposition technology and augmented with data from 3rd party dynamic analysis and A/V products to provide industry reputation consensus. TitaniumCloud supports a powerful set of query and feed functions through REST APIs for threat identification, analysis, intelligence development and hunting.