REVERSINGLABS

SOLUTION BRIEF

How Advanced SOCs Optimize EDR and Threat Intelligence to Prioritize Hidden Malware

Challenges

- **Lack of file-level visibility on endpoints makes it difficult to find unknown malware.**
- **Dynamic analysis solutions do not analyze all file types, can be slow, and evaded by advanced malware.**
- **Malware hunting is a slow and manual process as hunters work to piece together IOCs.**

The lack of file-level visibility into suspicious files on Endpoint Detection and Response (EDR) tools often inhibit the risk reduction and event response objectives of security operations and incident response teams. Threat vectors like email and web apps force organizations to analyze files residing on endpoints to effectively defend against attacks, but manual processes are not fast enough to identify new malware, and do not provide adequate information. Analysts attempt to learn about suspicious files by uploading samples to public reputation services, but this practice exposes sensitive information to the public with less than actionable results. In addition, dynamic analysis solutions give enterprises another way to identify malware embedded in files, but cannot scale with large volumes, and are often evaded leaving significant gaps in file analysis.

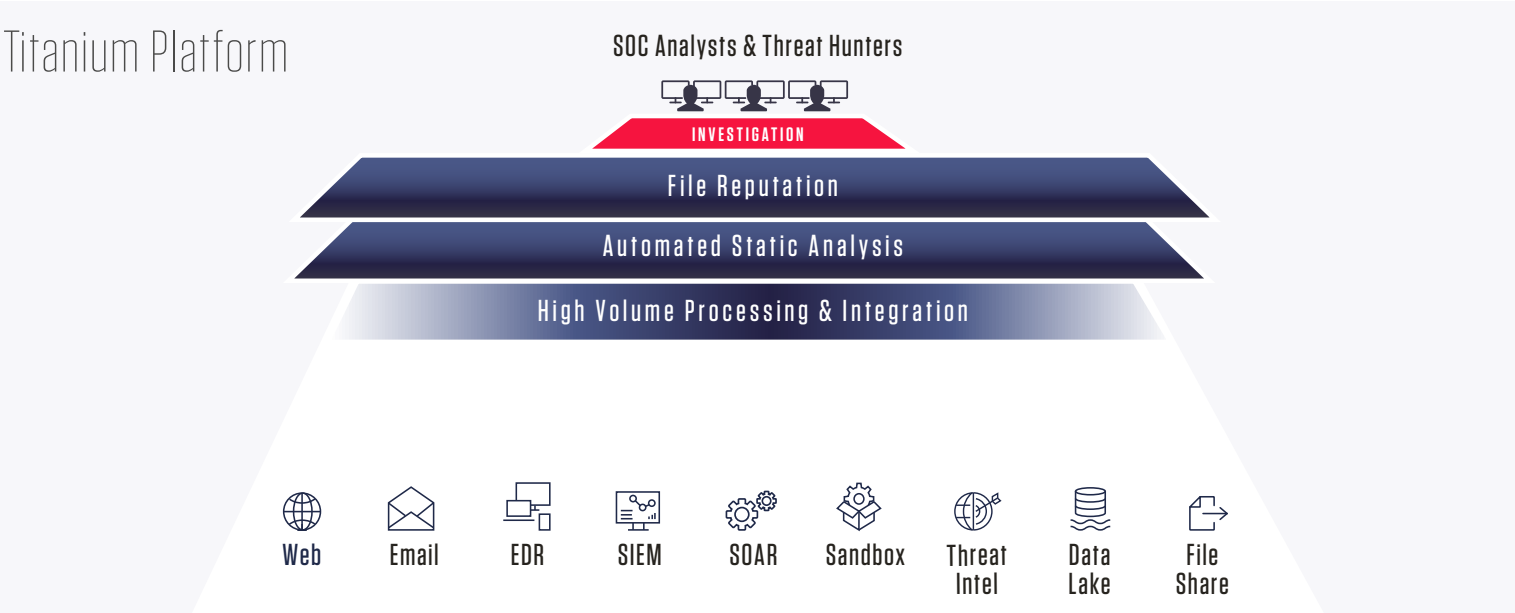
Benefits

- **Instantly analyzes files identified by EDR tools for malware information, results displayed in EDR console.**
- **Exposes malware and provides file intelligence to help determine the appropriate threat response.**
- **Increases analyst productivity by integrating file reputation into EDR dashboards and workflows.**

Solution

ReversingLabs Titanium platform integrates with EDRs to instantly and accurately identify files as Malicious, Known Good, or other classifications - giving much-needed visibility into suspicious files and exposing malware pre-execution. Within milliseconds, file hashes collected from all file types and objects across thousands of endpoints are automatically analyzed for severity level, threat classification (e.g. malicious), name (e.g. Trojan), and malware type (e.g. adware vs. ransomware).

The Titanium platform delivers threat intelligence results on files directly in the EDR user interface (UI). With 400% more files in ReversingLabs' authoritative goodware and malware database than the closest competitor, analysts have the best coverage to instantly, privately and accurately identify advanced malware on endpoints. Severity levels enable EDR administrators to prioritize and accelerate their responses to advanced threats across all objects for the broadest coverage available and the best possible protection.



Use Case | 1

INSTANTLY IDENTIFY AND PRIORITIZE FILES BY THREAT SEVERITY

Challenge: EDR administrators are often put in a difficult position when trying to respond quickly and accurately to threats. Too often, the contextual details of why files and objects have been flagged as suspicious are just not available, and high volumes of alerts create complexity. This is burdensome for EDR admins and poses real risks to their organizations. Response time increases. Files are missed due to incomplete coverage across all file types. Mean Time to Resolution (MTTR) increases. Incidents of compromise go up. All due to the lack of information that should be readily available to EDR admins.

Solution: ReversingLabs Titanium platform solves this problem by seamlessly integrating with EDR systems to display file reputation results from its authoritative reputation database. Files are instantly filtered by malware severity level and type. Results are displayed in the EDR's UI with clear and simple language and intuitive graphics. This clarity and simplicity enable EDR admins to inspect larger volumes of files and focus on the most critical threats. Because ReversingLabs provides more comprehensive reputation analysis coverage across all files and objects, advanced malware is exposed no matter how many evasion tactics are used. The processing can take place on-premises, or through a secure, private cloud API, without ever executing the actual malware.

Benefit: The speed and accuracy of deep file reputation analysis results displayed within the EDR console provide accelerated pre-execution triage of endpoint threats. The solution cuts down on the amount of traffic sent to sandboxes, and the EDR admin is put in a much better position to identify advanced malware, accelerate threat response and reduce time to resolution. All without wasting any time having to review 'known good' files.

Use Case | 2

KEEP FILE REPUTATION LOOK-UPS PRIVATE

Challenge: Privacy can be a major issue in today's file analysis process. Quite often when a file is flagged as suspicious by a SOC analyst or EDR administrator, the file is manually uploaded to a public/ crowdsourced file reputation service. The files are then compared against a global file reputation database to identify known malware indicators embedded within the file. Unfortunately for the analyst and the business, the content of the document along with the attack information is publicly exposed, risking the compromise of sensitive data.

Solution: The ReversingLabs global file reputation service alleviates these privacy concerns with the ability to keep data local or protect files from exposure when uploaded to the cloud. Customers choose the privacy level. If a customer wants a local repository of file reputation data, the ReversingLabs solution is deployed on-premise, preventing any files from being transferred offsite. If the customer prefers a cloud-based solution, ReversingLabs securely controls access to its APIs and data, even preventing its engineering team from having access to those files.

Benefit: The solution offers simple access to the file reputation information that security teams need to rapidly triage threats while maintaining the required privacy and security, which is often put at risk in public domains.

Use Case | 3

DIG DEEPER WITH PRE AND POST INCIDENT INVESTIGATION AND HUNTING

Challenge: Advanced, customized malware can adapt to and bypass organizations security defenses and enter anywhere across global networks, making it extremely challenging for threat hunters and incident responders to defend their environments. Threat hunters need context around attacks to proactively search out hidden malware before it attacks. Incident responders need accurate malware context and a speedy way to define new malware, and not wait for signature creation, across detection systems.

Solution: The ReversingLabs Titanium platform solves this problem through its YARA rule capability. YARA rules can be written by security analysts to match all extracted malware files and objects. These rules can be easily written and tested for efficacy in ReversingLabs Titanium Platform and then exported to EDR, firewall, and network security solutions for proactive threat detection. YARA rules also enhance the native search and hunt capabilities in EDR products enabling threat hunters to use these rules for further investigation and advanced searches.

Benefit: ReversingLabs bolsters the speed and effectiveness of EDR based threat hunting while reducing the time to create and test effective YARA rules that define advanced malware. The use of YARA rules also removes reliance on vendor created malware signatures and increases protection against customized malware.

REVERSINGLABS | TANIUM

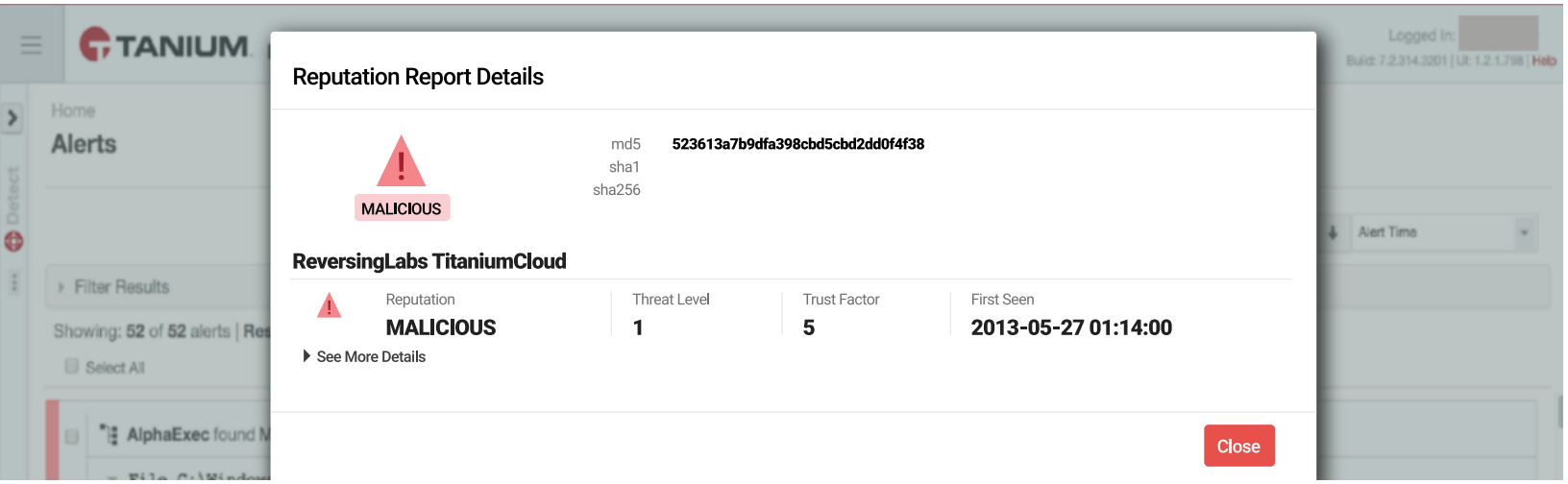
Case Study

A regional bank in the Midwest had a complete security infrastructure, but malware was still infecting their networks through their 20,000 endpoints. The bank implemented the Tanium platform for endpoint visibility and to flag suspicious activity to address the problem. Tanium collected all related suspicious files but provided no further information or context for the Tanium administrator to analyze, identify, and contain any advanced malware.

We rely on ReversingLabs analysis for threat level, severity, and malware identification. This classification is key to understanding the threat we're dealing with and deal with it fast by getting data instantly on the profile of the file, so my team knows how to respond.

SOC Manager, Regional Bank

The Tanium platform integrates with third-party file reputation services to help detect malicious files. This bank's third-party file reputation service displayed results in the Tanium UI, but only provided a thumbs up or thumbs down result. With no further information about severity level or malware type, it did not help the bank's team prioritize their activities or define effective containment strategies. There was also a privacy issue. In some cases, the actual files were being uploaded for file reputation analysis by members of the security team not understanding that with this service, the content of those files was exposed to and became accessible by other customers of the service.



Solution

ReversingLabs File Reputation and Intelligence platform were seamlessly integrated with their Tanium implementation. This enriched the bank's file analysis results with context and actionable file reputation intelligence information including severity level, threat classification (e.g. malicious), malware type, and more by using unique advanced high-speed static analysis. The ReversingLabs Titanium platform also cataloged known good files from trusted sources to assure analysts did not waste time on known safe files. ReversingLabs enhanced the bank's Tanium search results and user interface so that their security operations teams quickly saw analysis results of unknown files. The bank's analysts can then rapidly determine whether a file is malicious and initiate an appropriate response based on attack type.

Value Realized

The bank used the ReversingLabs and Tanium integration to run automated queries on their 20,000 endpoints every 24 hours to see newly downloaded files. Within seven days, 500 malware samples were found and classified by threat type, threat level, and severity. More than half the malware was known by the ReversingLabs Titanium platform but wasn't detected by the bank's AV scanners. With ReversingLabs enriched data results, the bank's analysts were able to increase their file review speeds by several orders of magnitude. Today, those analysts can quickly identify the highest severity risks and formulate the appropriate responses. They set rules that identify the highest severity level threats and automatically trigger escalated responses. For example, if 40 out of 40 AV products deem a file malicious in a crowdsourced reputation check, the security team will likely prioritize the incident response playbooks for that file. With ReversingLabs, the results will go beyond just reputation, and finding the file is simple adware (vs. ransomware), the security team will know de-prioritize that file in favor of more critical threats.

Conclusion

For EDR admins, the ever-increasing volume and variety of suspicious and malware-infected files is a real and pressing problem they face every day. Their existing security resources were not designed with the speed, comprehensiveness, and file evaluation capabilities needed to effectively combat today's evolving malware threats.

ReversingLabs bridges this gap with its Titanium platform. Through unmatched performance and coverage, the Titanium platform is the weapon security teams need to identify and contain advanced malware as well as finding destructive files hidden within their endpoints and networks and eliminate the threats they pose.

www.reversinglabs.com

Schedule Demo Here