SOLUTION BRIEF

ЯL REVERSINGLABS

Enhancing SOC Efficiency: Automating Incident Response and Mitigation through Real-Time File Analysis

Challenges Faced by SOC Teams

- **Talent Shortage and Skills Gap:** Finding and retaining skilled cybersecurity professionals is a significant challenge. The demand for qualified experts often exceeds the supply, leading to a shortage that can impact the SOC's ability to monitor and respond to threats effectively
- **Alert Fatigue:** SOC teams often deal with a high volume of security alerts, many of which can be false positives. This can overwhelm analysts, making promptly identifying and responding to genuine threats challenging
- **Integration and Interoperability of Security Tools:** SOCs use various security tools, such as SIEM systems, intrusion detection systems, and threat intelligence platforms. Ensuring these tools work seamlessly together can be challenging, impacting the SOC's overall efficiency and effectiveness

Benefits

- Automatically analyzes files identified by cybersecurity tools and provides real-time file reputation status and intelligence
- Uncovers hidden malware and provides verified threat classifications to drive the appropriate automated response actions
- Increases analyst productivity by integrating file reputation and threat context into SOC dashboards and workflows

Security operations tools are adept at identifying and flagging suspicious files for further investigation. However, uncovering malware within these flagged items is far from straightforward. It requires a combination of human resources and specialized skills to analyze and interpret the data thoroughly. Cybersecurity analysts must delve into the intricacies of the files, using their expertise to detect subtle signs of malicious activity that automated tools might miss. This involves understanding complex malware behaviors, reverse engineering code, and staying updated with the latest threat intelligence. Consequently, while automation significantly aids in the initial detection phase, malware identification and mitigation rely heavily on skilled professionals to ensure comprehensive security.

How ReversingLabs Can Help

ReversingLabs delivers industry-leading file analysis and malware intelligence that can be easily integrated into cybersecurity solutions. This enables organizations to fill in threat detection gaps that could harm the business.

Utilizing proprietary, AI-driven, complex binary analysis, ReversingLabs deconstructs files and objects down to their base elements to detect embedded threats in real time. This unique analysis technology recursively unpacks objects, extracts all metadata, and correlates it against billions of malware and goodware samples in our authoritative reputation database and threat intelligence repository.

With ReversingLabs, security teams can instantly assess files and get definitive threat verdicts backed by rich context, including severity level, threat name, malware family, malware type, MITRE ATT&CK mapping, and more. Results are displayed in the user interface with clear and straightforward language, giving visibility into suspicious files and exposing malware pre-execution. Analysts get all the information they need to prioritize and accelerate their responses to advanced file-based threats across the organization.

And, with support for more than 4800 file types and millions of new samples added daily to ReversingLabs' global threat repository of 40+ billion files, analysts can rest assured they're getting the most up-to-date intelligence with the broadest coverage in the industry to stay ahead of increasingly sophisticated malware threats.

Use Case 1

Make Email Triage Easier

Challenge:
End-users receive 100's of emails with attachments daily. And those attachments continue to increase in size and complexity. The best practice is to examine each file attachment for malware. Most email tools allow each attachment to be quarantined until examined, preventing users from opening malware on their machines. Unfortunately, this creates a vast and constant backlog, along with frustrated users bombarding the SOC team with requests to have their files released from quarantine.

In reality, many SOC teams will clear tickets without investigation to clear backlogs or because of user pressure to access files.

Solution:
Submit each suspicious file to ReversingLabs for high-speed, in-depth binary analysis to uncover malware or ransomware before it activates. Unlike other solutions, ReversingLabs can effortlessly analyze large, multi-layered files and objects with speed and scale to eliminate bottlenecks while ensuring evasive malware threats are exposed. The combination of our proprietary analysis engine and comprehensive file and network threat intelligence ensures that advanced malware can't hide.

Case Study

State-Level Cybersecurity Operations Center

A large state government cybersecurity operations center is actively combating ransomware attacks against the organization. State and local governments are now common targets for ransomware, often forced to pay millions in extortion. A best practice is to examine every file on every email attachment. Therefore, the SOC team quarantines each attachment for further examination. However, these files are critical for city operations, such as mortgages, insurance, and filing of statements. As a result, users constantly request the release of files from quarantine, creating a huge backlog.

Initially, The organization used a standard ticketing system, leading to thousands of backlog tickets. This clogged the entire system and prevented the SOC team from focusing on actual attacks and critical tasks. End-users complained that the security measures interfered with operations and escalated these concerns to leadership. The city needed a different solution.

Alternative automated workflow with ReversingLabs
All email attachments are quarantined and submitted to ReversingLabs for real-time, comprehensive binary analysis. This provides the SOC with immediate and definitive threat classifications so they know right away whether something is 'good' or 'bad'. These results, including the relevant context and threat details are then passed to cybersecurity tools to update incident reports. This process takes only a few seconds.

Automation tools either release goodware files to the user or delete the email and notify the end-user if malware is detected. In the rare case of an unknown file, the file hash is escalated to RL engineers if the SOC operator requests further analysis.

As a result, more than 99% of files are resolved in less than 5 seconds.

Benefits

- Allows every attachment to be examined in the same consistent manner regardless of size or format type
- Dramatically reduces user wait time to open attachments, so business productivity isn't hindered
- Improves SOC operations and morale by alleviating bottlenecks associated with scanning attachments

Use Case 2

Make Handling Endpoint Detection and Response (EDR) Incidents Easier

Challenge:
EDR tools detect unusual or suspicious activities on protected endpoints. The alerts are passed to the SOC team for analysis. These investigations can be time-consuming and require a high level of skill, but they are a best practice for preventing malware and ransomware outbreaks. This activity is a major drain on SOC teams.

In reality, most SOC teams do not have the time or resources to investigate each alarm. Instead, they will isolate the endpoint and schedule a re-imaging of the device without further investigation.

Solution:
Submit a file or hash to ReversingLabs for real-time reputation lookups and analysis from our authoritative threat intelligence repository of more than 40 billion goodware and malware samples. A result is received within seconds, enabling the investigator to very quickly make a correct decision about the status of the file. This dramatically reduces the SOC team's workload, improves accuracy in mitigation, and reduces the load on other tools, such as the sandbox.

Case Study

International Insurance Agency SOC Team

An international Insurance agency widely deployed an EDR solution on all endpoints within the organization and tuned it to detect suspicious files by activity. These endpoints would generate alerts, which were logged and marked for investigation.

While this is standard best practice, it quickly generated more alerts for the SOC team than they could process. The SOC team tried to use file hash matching tools, but with threat actors using new AI capabilities to create polymorphic malware for custom ransomware campaigns, these tools gave poor results. The SOC team investigators would then submit the unknown files to a sandbox, which was effective at uncovering behavior but was over-subscribed, thereby forcing a rationing of resources. Shortages of staff and skill level issues compounded the problem, resulting in the SOC's inability to investigate and close cases properly.

The result was a significant rise in isolating endpoints from the network and re-imaging them as the only way to address the massive backlog. This created frustration with both the SOC team and the end-users, who were inconvenienced by the re-imaging process, which took up to a week. This work interruption was especially concerning to executives and critical staff.

Alternative automated workflow with ReversingLabs
The EDR solution creates an alert because of a suspicious file, which creates an incident. The file is computed using the EDR tool, and the hash is submitted to ReversingLabs for enrichment and context. The enriched results are populated into case management, including:

- **File Reputation:** Determines whether the file is malicious, suspicious, known (benign), or unknown.
- **Static and Dynamic Analysis Results:** Offers a combination of high-speed static analysis plus optimized dynamic analysis for comprehensive, collective metadata.
- **File Metadata:** Includes file type, size, and various computed hashes (e.g., MD5, SHA256).
- **Threat Context:** Provides relevant context, such as malware family, threat level, and other related threat intelligence.
- **Similarity Analysis:** Utilizes the ReversingLabs Hashing Algorithm (RHA) to identify functionally similar files and provide their reputation information.

The investigator can review this information and make a quick decision with high confidence.

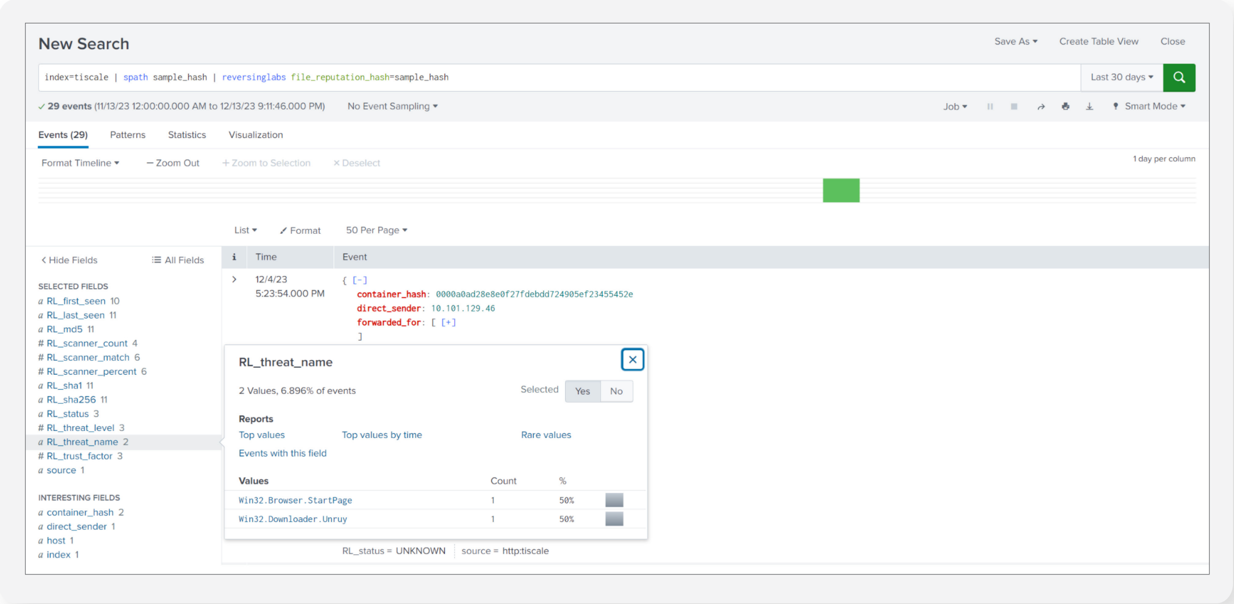
As a result, more than 99% of incidents have enough information for the investigator to resolve the case correctly within one minute.

Benefits

- Instantly analyzes files identified by EDR tools and provides real-time file reputation status
- Exposes malware and provides verified threat classifications and the necessary context to speed incident response
- Uplevels security analysts by providing them with the context to handle alerts that would otherwise need escalation

> “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 dealing with it fast by getting data instantly on the profile of the file, so my team knows how to respond.”

– SOC Manager, Regional Bank



```
index=tiscale | spath sample_hash | reversinglabs file_reputation_hash=sample_hash
```

✓ 29 events (11/13/23 12:00:00.000 AM to 12/13/23 9:11:46.000 PM) No Event Sampling ▾

SELECTED FIELDS
- a RL_first_seen 10
- a RL_last_seen 11
- a RL_md5 11
- # RL_scanner_count 4
- # RL_scanner_match 6
- # RL_scanner_percent 6
- a RL_sha1 11
- a RL_sha256 11
- a RL_status 3
- # RL_threat_level 3
- a RL_threat_name 2
- # RL_trust_factor 3
- a source 1

INTERESTING FIELDS
- a container_hash 2
- a direct_sender 1
- a host 1
- a index 1

i	Time	Event
>	12/4/23 5:23:54.000 PM	{ [-] container_hash: 0000a0ad28e8e0f27fdebdd724905ef23455452e direct_sender: 10.101.129.46 forwarded_for: [[+]]

RL_threat_name

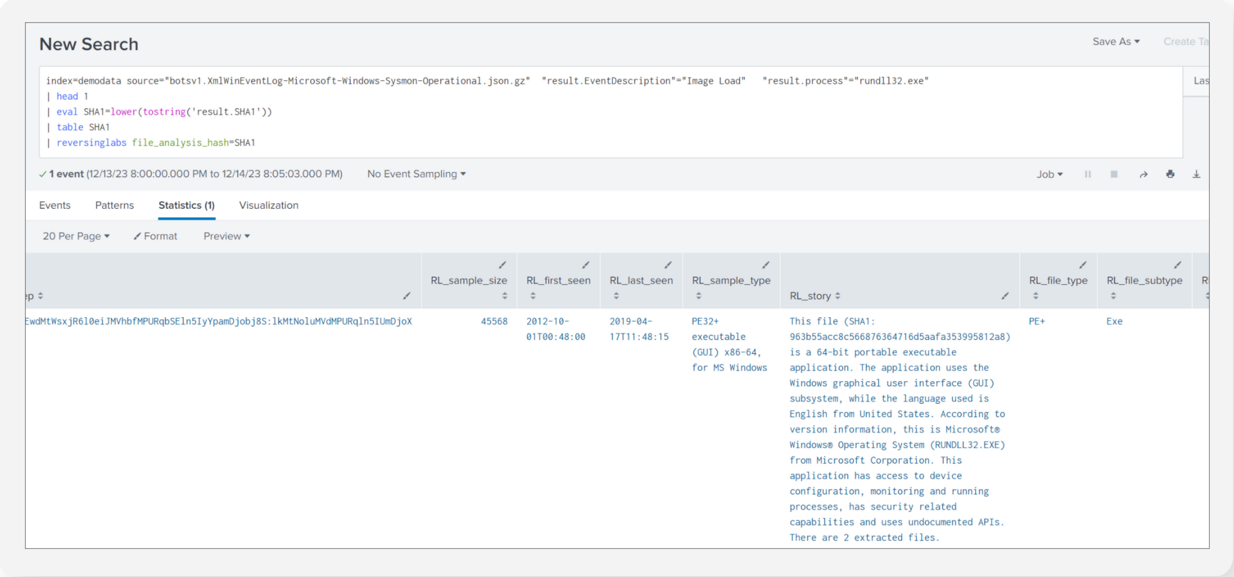
2 Values, 6.896% of events Selected [✓ Yes] No

Reports
Top values Top values by time Rare values
Events with this field

Values	Count	%
Win32.Browser.StartPage	1	50%
Win32.Downloader.Unruy	1	50%

RL_status = UNKNOWN source = http:tiscale

Example of retrieving file reputation information from a file hash showing malware

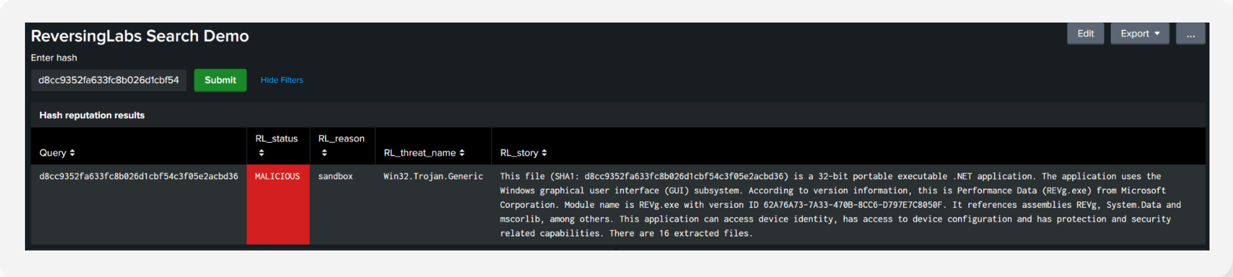


```
index=demodata source="botsv1.XmlWinEventLog-Microsoft-Windows-Sysmon-Operational.json.gz"  "result.EventDescription"="Image Load"  "result.process"="rundll32.exe"
| head 1
| eval SHA1=lower(tostring('result.SHA1'))
| table SHA1
| reversinglabs file_analysis_hash=SHA1
```

✓ 1 event (12/13/23 8:00:00.000 PM to 12/14/23 8:05:03.000 PM) No Event Sampling ▾

ep	RL_sample_size	RL_first_seen	RL_last_seen	RL_sample_type	RL_story	RL_file_type	RL_file_subtype	R
EwdMtWsxjR6l0eiJMVhbfMPURqbSEln5IyYpamDjobj8S:lkMtNoluMVdMPURqln5IUmDjoX	45568	2012-10-01T00:48:00	2019-04-17T11:48:15	PE32+ executable (GUI) x86-64, for MS Windows	This file (SHA1: 963b55acc8c566876364716d5aafa353995812a8) is a 64-bit portable executable application. The application uses the Windows graphical user interface (GUI) subsystem, while the language used is English from United States. According to version information, this is Microsoft® Windows® Operating System (RUNDLL32.EXE) from Microsoft Corporation. This application has access to device configuration, monitoring and running processes, has security related capabilities and uses undocumented APIs. There are 2 extracted files.	PE+	Exe	

Summary of file analysis of the file hash showing what data is returned to the SOAR



ReversingLabs Search Demo

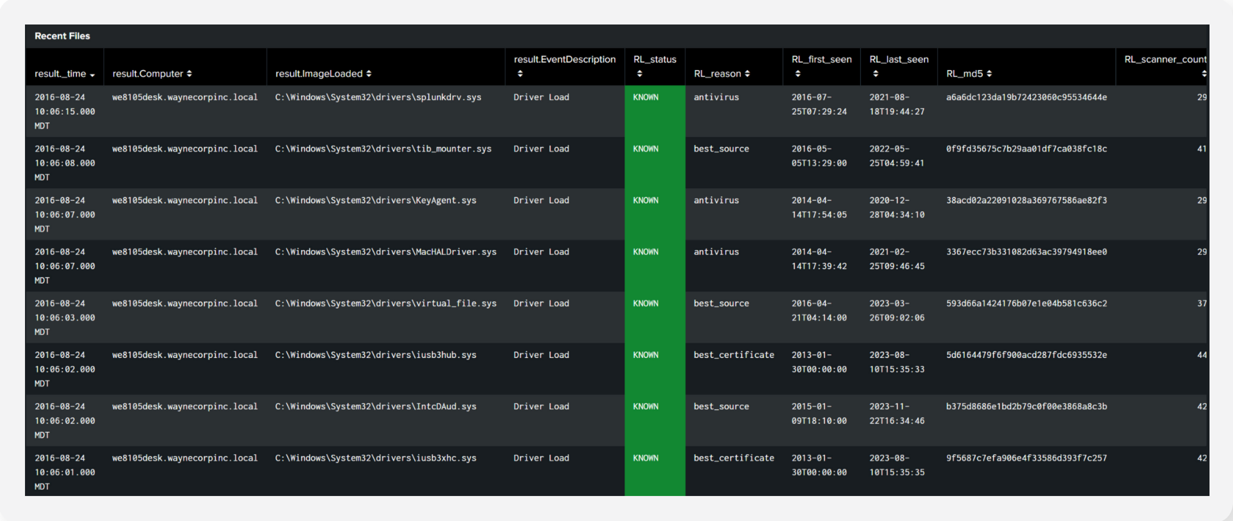
Enter hash

d8cc9352fa633fc8b026d1cbf54

Hash reputation results

Query	RL_status	RL_reason	RL_threat_name	RL_story
d8cc9352fa633fc8b026d1cbf54c3f05e2acbd36	MALICIOUS	sandbox	Win32.Trojan.Generic	This file (SHA1: d8cc9352fa633fc8b026d1cbf54c3f05e2acbd36) is a 32-bit portable executable .NET application. The application uses the Windows graphical user interface (GUI) subsystem. According to version information, this is Performance Data (REVg.exe) from Microsoft Corporation. Module name is REVg.exe with version ID 62A76A73-7A33-470B-8CC6-D797E7C8050F. It references assemblies REVg, System.Data and mscorlib, among others. This application can access device identity, has access to device configuration and has protection and security related capabilities. There are 16 extracted files.

Example of a custom dashboard showing an interactive example of examining a malicious file hash



Recent Files

result._time	result.Computer	result.ImageLoaded	result.EventDescription	RL_status	RL_reason	RL_first_seen	RL_last_seen	RL_md5	RL_scanner_count
2016-08-24 10:06:15.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\splunkdrv.sys	Driver Load	KNOWN	antivirus	2016-07-25T07:29:24	2021-08-18T19:44:27	a6a6dc123da19b72423060c95534644e	29
2016-08-24 10:06:08.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\tib_mounter.sys	Driver Load	KNOWN	best_source	2016-05-05T13:29:00	2022-05-25T04:59:41	0f9fd35675c7b29aa01df7ca038fc18c	41
2016-08-24 10:06:07.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\KeyAgent.sys	Driver Load	KNOWN	antivirus	2014-04-14T17:54:05	2020-12-28T04:34:10	38acd02a22091028a369767586ae82f3	29
2016-08-24 10:06:07.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\MacHALDriver.sys	Driver Load	KNOWN	antivirus	2014-04-14T17:39:42	2021-02-25T09:46:45	3367ecc73b331082d63ac39794918ee0	29
2016-08-24 10:06:03.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\virtual_file.sys	Driver Load	KNOWN	best_source	2016-04-21T04:14:00	2023-03-26T09:02:06	593d66a1424176b07e1e04b581c636c2	37
2016-08-24 10:06:02.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\iusb3hub.sys	Driver Load	KNOWN	best_certificate	2013-01-30T00:00:00	2023-08-10T15:35:33	5d6164479f6f900acd287fdc6935532e	44
2016-08-24 10:06:02.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\IntcDAud.sys	Driver Load	KNOWN	best_source	2015-01-09T18:10:00	2023-11-22T16:34:46	b375d8686e1bd2b79c0f00e3868a8c3b	42
2016-08-24 10:06:01.000 MDT	we8105desk.waynecorpinc.local	C:\Windows\System32\drivers\iusb3xhc.sys	Driver Load	KNOWN	best_certificate	2013-01-30T00:00:00	2023-08-10T15:35:35	9f5687c7efa906e4f33586d393f7c257	42

Example of an extended dashboard using the RL integration to gather trend analysis

Conclusion

Security Operation Centers (SOCs) face ever-increasing challenges due to the growing complexity and volume of cyber threats. The sheer number of security alerts, the need for more skilled cybersecurity professionals, and the integration of diverse security tools are significant hurdles. These challenges are compounded by the need to manage vast data and respond to sophisticated attacks in real-time. However, automation is transforming the security landscape by streamlining processes and reducing the manual workload on SOC teams. AI-driven solutions can quickly analyze large datasets, identify patterns, and detect anomalies that may indicate a threat. Automation also enables faster incident response and mitigation, allowing SOCs to focus on more strategic tasks. By leveraging these advanced technologies, SOCs can enhance their efficiency and effectiveness, ultimately improving their ability to protect organizational assets.

ReversingLabs bridges this gap with industry-leading file reputation services and malware intelligence, which provides the next-level coverage, accuracy, context, and performance security teams need to identify and contain advanced malware and find destructive files and objects hidden within their endpoints and network as quickly as possible.

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide a 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.

Get Started!

See How ReversingLabs' High-Speed File Analysis Can Accelerate Your Threat Detection And Response Workflows

REQUEST A DEMO

www.reversinglabs.com

ЯL ЯEVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com