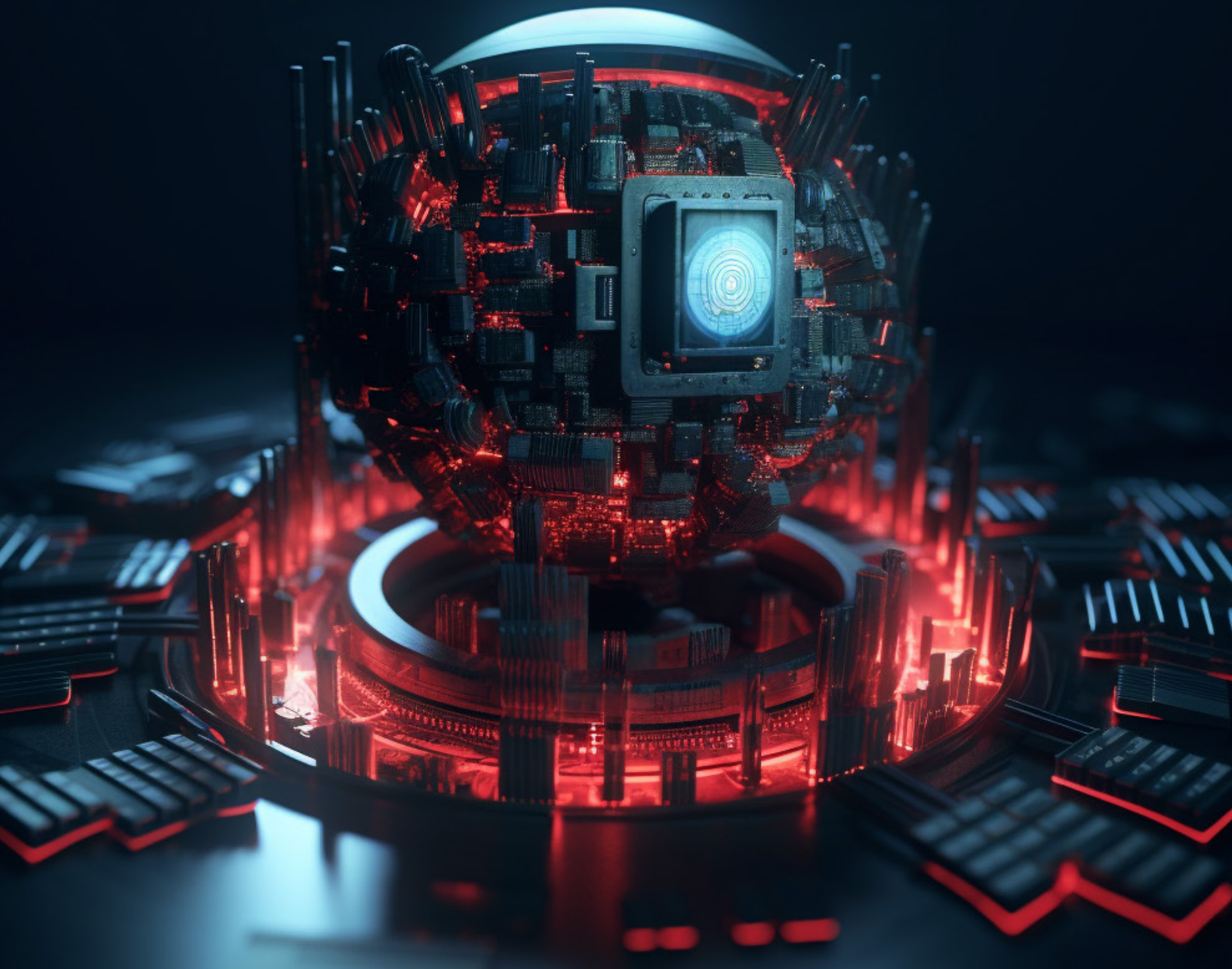
EBOOK

REVERSINGLABS

How to Evaluate Threat Intelligence Feeds

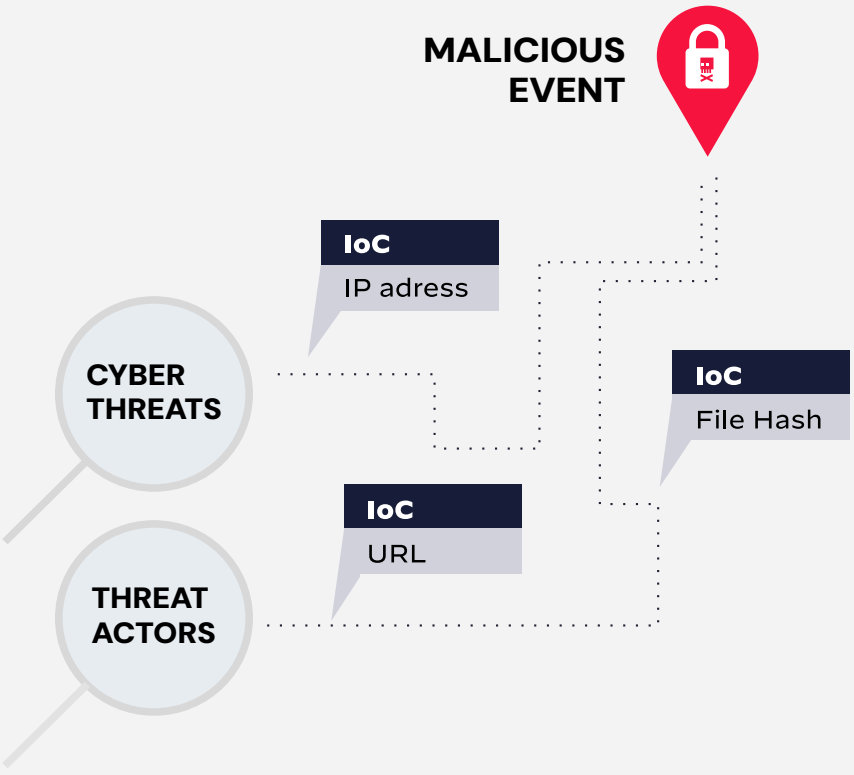


What Are Threat Intelligence Feeds?

Threat intelligence is information about cyber threats (malware, ransomware, etc.) and threat actors that help identify malicious events.

This information can be referred to as indicators of compromise or (IoC). It consists of objects such as IP addresses, file hashes, and URLs which can be used to identify an attack.

Threat Feeds and Search/Query APIs automate processing, correlation, analysis, and threat status information gathering to enable orchestration to build the foundation of a threat informed defense.



What to Look for in Trustworthy Threat Intelligence Feeds

Threat intelligence solutions should provide up-to-date file and network reputation services, threat classification and rich context over a wide array of malware and goodware samples.

REVERSINGLABS PROVIDES

historical detection information from an extensive threat repository to identify threats, determine how those threats behave over time and deliver trusted, up-to-date insights on file and network reputation.

High-fidelity threat intelligence feeds from ReversingLabs

1. Use the world's largest private repository of malware and goodware, with over 400 billion samples, to locate threats
2. Curate specific threat categories and collections such as ransomware, APT, CVEs, financial, retail, and other industry-specific information
3. Deliver file and malware intelligence for threat identification, analysis, intelligence development, and threat hunting services with a powerful set of REST API query and feeds
4. Generate alerts based on threat level changes for previously seen files to discover emerging threats in previously secure components
5. Enable advanced search by file context and threat indicators, even on large sample datasets to simplify threat hunting activities

Threat Intelligence Feeds Need to Be:

RELEVANT

Source: CISA & JHU APL

APPLICABLE

Is it a threat of interest? What/who are the sources of threat for the provider?

ACCURATE

How noisy is the information? How confident are they? Do you know how they derive certain content?

TIMELY

How long does it take to generate the information? Generate the information?

USABLE

MACHINE READABLE

What is the sharing infrastructure? Can you access in an automated manner?

CONSUMABLE

Can you access and inject into operational processes in an automated manner? Is the information consistent in usage?

ACTIONABLE

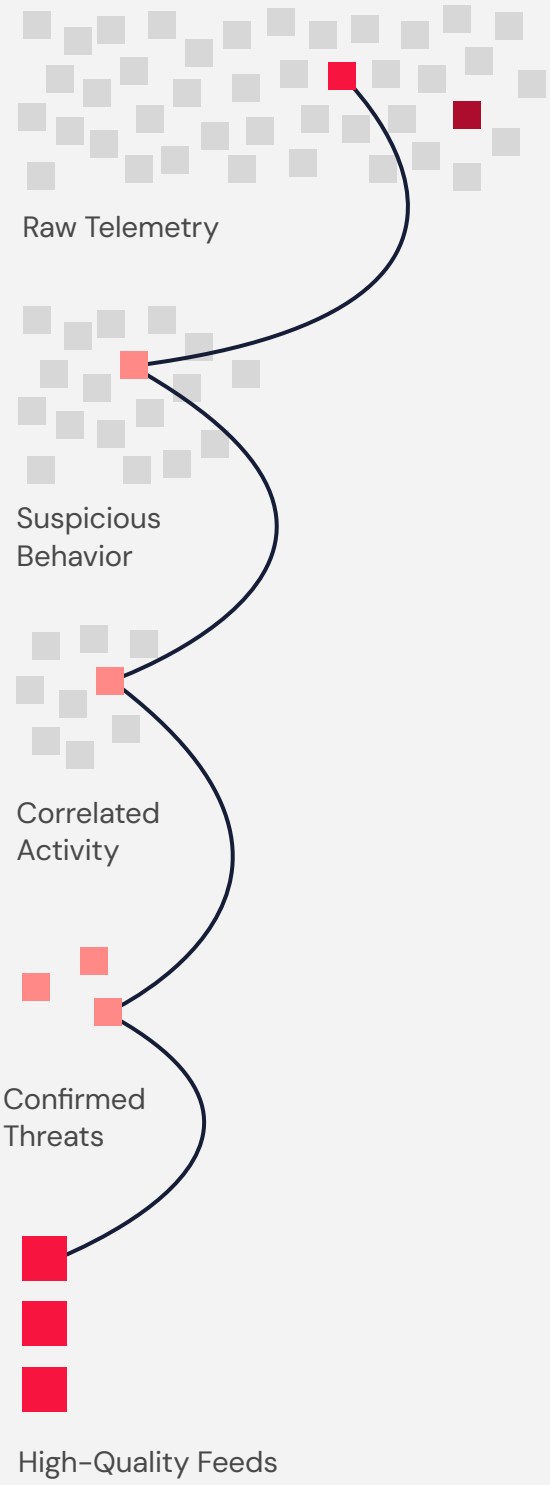
Can you use the information to make operational decisions in a timely fashion?

Quality Over Quantity: Scaling with High Quality Feeds Over Raw Telemetry

Constantly receiving a large number of low-quality alerts from threat intelligence feeds results in an overload of information for security operations teams, who then must spend an extensive amount of time on triaging these alerts. Today, SOC members spend nearly one-third (32%) of their day investigating incidents that don't actually pose a real threat to the business.[1]

Hiring additional expertise to scale up analysis as the threat landscape evolves is cost prohibitive for most organizations. Instead of ingesting large volumes of raw telemetry, threat hunters and SOC teams should consider automating that triage effort by demanding higher quality data from their feed providers. By automating the analysis of suspicious behavior and correlating activities, feed providers can filter out the noise for your teams while still providing the details to explain why they can trust that the alerts delivered are actually confirmed threats.

Obtaining high-quality threat intelligence feeds enables organizations to reduce alert fatigue, mitigate talent shortages and improve threat isolation and response.



Source: [1] https://securityintelligence.com/articles/socs-spend-32-percent-day-incidents-pose-no-threat/

Evaluate Feed Quality in Three Steps

STEP 1

Validate feed usability: Solutions must adhere to accepted data standards for describing and sharing threat intelligence.

QUESTIONS TO ASK

A **Is the feed STIX compliant?**

I What version is it compliant with?
II What STIX fields are provided?
III Is the data properly formatted in the provided fields?

B **Does the feed support the TAXII protocol?**

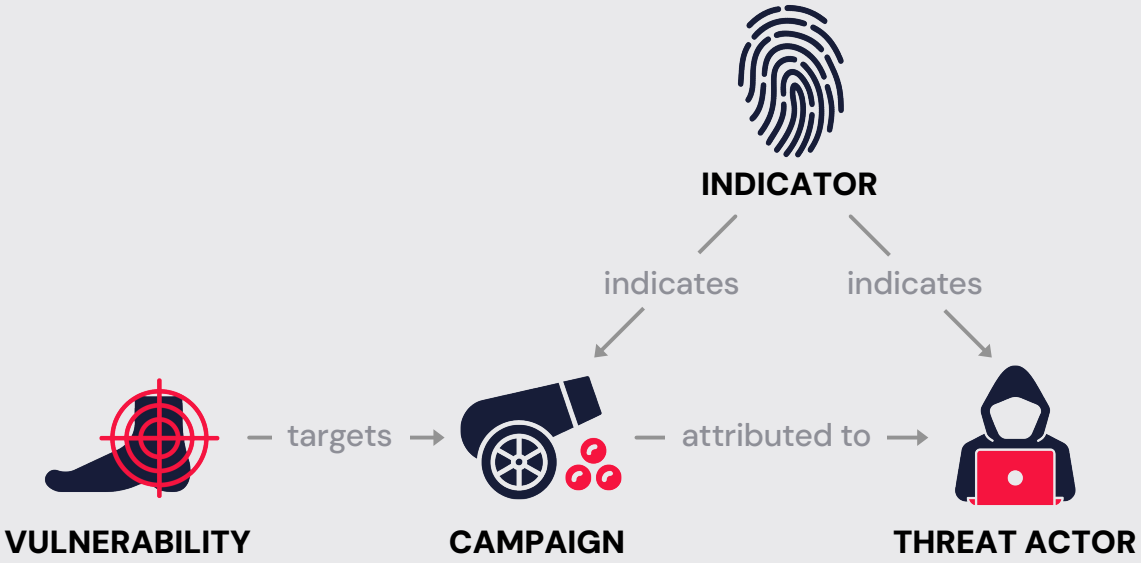
I What version(s) of the TAXII protocol does the feed support?
II How many collections/channels are available? Are collections organized in a manner that makes sense?

C **Are other formats provided?**

I Can you export to CSV?

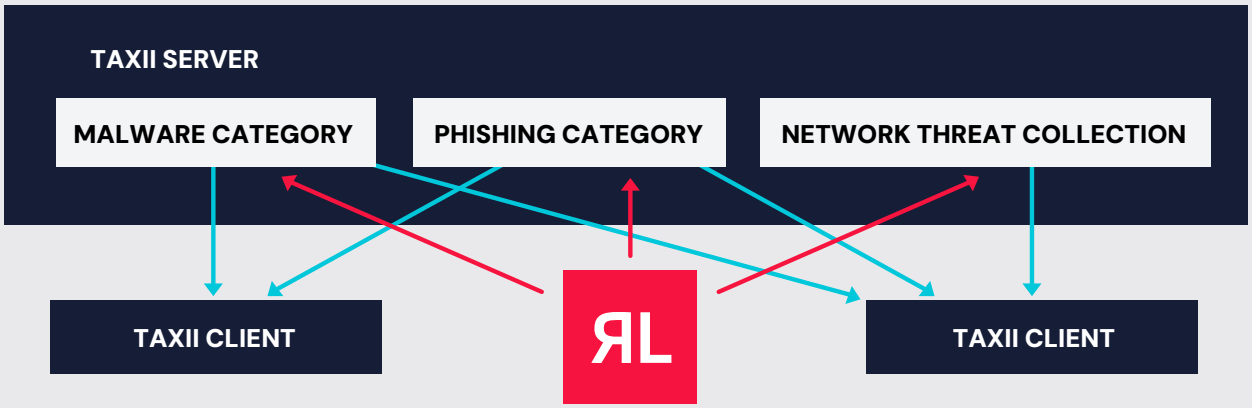
D **Does the vendor provide documentation for integration with SIEMs/TIPs?**

E **Is the vendor responsive to customer requests?**



ACTION ITEMS

- Review vendor documentation for the above guidelines
- Enable the feed in a development environment
- Compare a subset of the incoming data with standards



STIX — Standard data format to describe cyber threats

TAXII — A communication protocol to push and pull threat intelligence from different sources.

STEP 2

Validate feed quality: Typically, when more indicators are available for a specific threat, your detection logic can be more accurate and reduce the amount of noisy alerts that must be manually triaged. Additionally, threats can evolve very rapidly in some situations, and timely updates maximize your detection coverage.

QUESTIONS TO ASK

A **Does the feed include a variety of indicator types?**
(IPs/Domains/URLs/FileHashes/Email address/etc.)

B **Are there a variety of threats covered?**
How many malware families are represented?

C **Does your TIP/SIEM/SOAR support the indicator types and/or have data that can make use of the indicator types?**

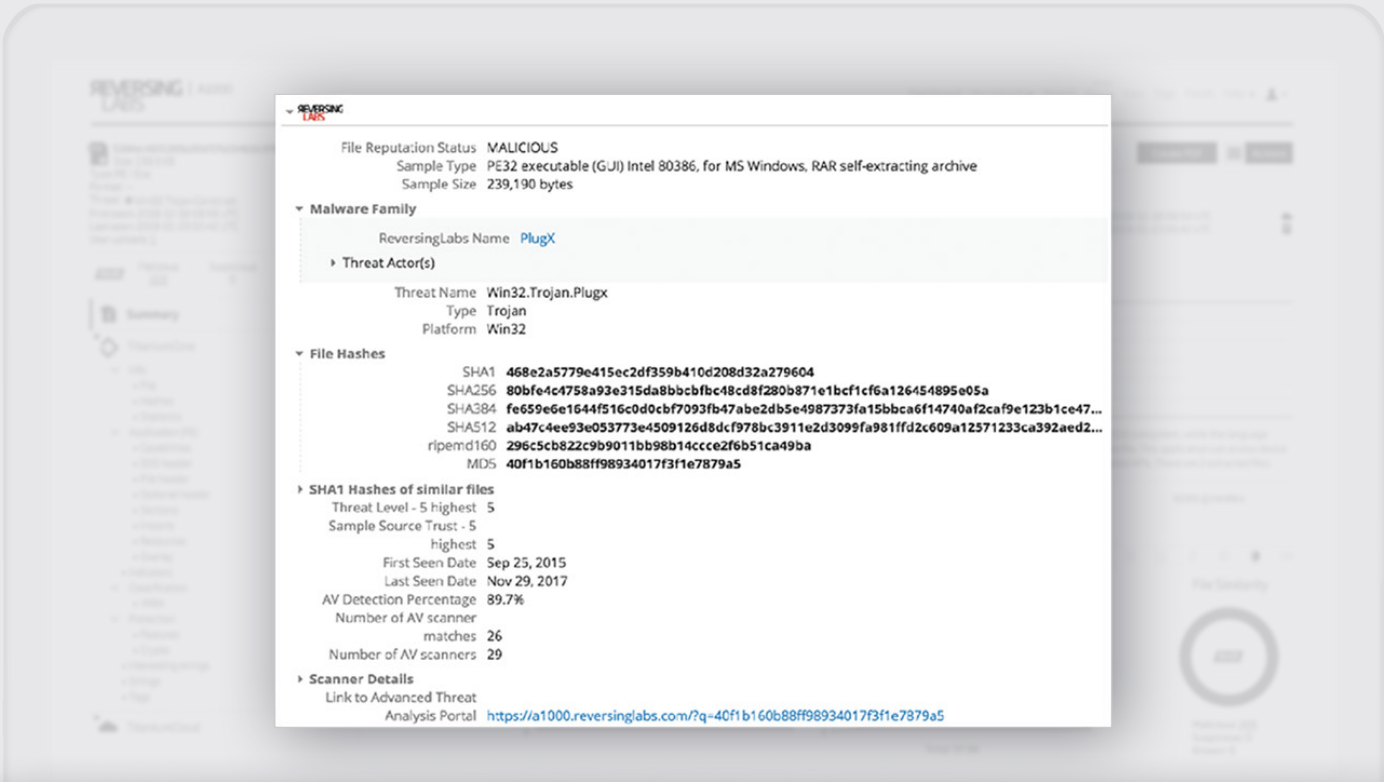
D **Are there any duplicate indicators?**

E **Are new indicators delivered in a timely manner?**
What frequency does the feed offer new updates?

F **Are indicators routinely updated?**

ACTION ITEMS

- Review vendor documentation for included indicator types
- Ensure that your tools have data inputs that can make use of the indicators (e.g. email security tool for email addresses)
- Monitor incoming indicators over a period of time and summarize average volume
- Compare created vs. modified timestamps



STEP 3 Validate indicator quality:

QUESTIONS TO ASK

A

Does every indicator include a useful description?

Indicators of Attack (IOAs) reveal the attack's goals and the chain of actions signaling that the early stages of MITRE's ATT&CK framework are underway (e.g. phishing emails, or new application behaviors that unnecessarily gather host or network information). IOAs are used to halt an attack's progress and mitigate weaknesses. Indicators of Compromise (IOCs) are signs that an attack has already taken place or is on-going. IOCs are used during incident response to assess the attack's scope and the degree of any data breaches.

B

Do indicators include external references?

C

Do indicators include relevant kill chain phases?

D

Validate IP address quality – do indicators provide enough information to avoid blocking legitimate traffic?

Indicators are generally ineffective when the majority of IP addresses are from Cloud or CDN services (Azure, AWS, Cloudflare, etc.) unless additional context. For example, cloud/CDN addresses can represent shared infrastructure, and blocking these addresses can prevent your business from accessing critical services. Similarly, Cloud/CDN providers may reuse IP addresses for future customers, and those organizations could be blocked from using your services.

E

Validate Domains/URLs – do indicators provide enough information to avoid blocking legitimate traffic?

In some cases, malicious actors use legitimate cloud storage services (OneDrive, Google Drive, etc.) to store and serve up their malware samples. Indicators must include additional context to identify and block this traffic effectively.

Three Ways to Improve SOC or DevOps Workflows with High-Quality Feeds

1. Threat intelligence feeds and APIs integrate with Threat Intelligence Platforms (TIPs), connecting actionable malware indicators with existing workflows across EDR, IPS, firewalls, and software supply chain security solutions to automate containment in TIP-managed security controls.

2. Integrating high-quality threat intelligence feeds that improve efficiency by minimizing false positives and removing the toil of manual triage.

3. With automated scanning and trusted intelligence, mean time to detect (MTTD) is reduced to minutes or hours rather than days or weeks, ***protecting enterprises from zero-day, ransomware and software supply chain attacks.***

Five ways threat hunters get value from high-quality feeds

There are several ways to effectively leverage your selected threat intelligence feeds to determine the location, severity, and behaviors of threats across their systems.

1. Apply IPs against egress/ingress logs to see if any are communicating with hacker infrastructure to show the ROI for your CTI feed focused on early-stage detection against threats like ransomware.

2. Apply hashes to other antivirus or endpoint logs to determine how well network and edge defenses are working to understand how well your AV/EDR tools are performing.

3. Review domains and run them against proxy logs or check IP/Domains against logs in your SIEM to locate what your risk exposure is and its prominence.

4. Export URLs to SNORT to view against malicious network activity to protect against unknown signatures and weaknesses across networks.

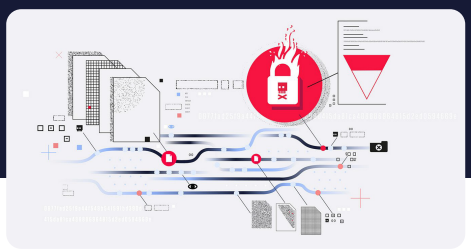
5. Prioritize potential threats by scanning files against open source, community, and government feeds to identify and address the right issues at the right times.

Additional Resources:

Do More With Your SOAR

Leverage ReversingLabs threat intelligence to enrich existing security tools and SOC workflows.

Read Blog



How to Use Threat Intelligence Indicator Feeds with Microsoft Sentinel

Learn how ReversingLabs threat intelligence indicator feeds can enhance Microsoft Sentinel. Plus, get a free trial of Early Detection of Ransomware for Sentinel.

Read Blog

ReversingLabs At-A-Glance

ReversingLabs provides the industry's most advanced and largest file threat intelligence database.

400B+
Largest Repository of Malware & Goodware

20M
Files Analyzed Daily

3M
Malware Identified Daily

4800
Files Types Supported

FASTEST
Binary File Deconstruction

60+
Cybersecurity Companies Trust RL

CONTACT US TO LEARN MORE

eB-Rev-03.28.25

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com