SOLUTION BRIEF

Personalized Curated Threat Intelligence

Faster detection, prevention, and eradication of targeted threats

ReversingLabs Flexible Intel Feed

Threat intelligence is not one-size-fits-all. For threat hunters and incident responders, the most relevant and impactful threat intelligence comes from validated security incidents detected inside your enterprise, as well as targeted threat intelligence received from trusted sources like FS-ISAC or CISA for active adversaries and newly discovered, targeted threats. The biggest challenge most security teams face is not obtaining the latest threat intelligence but how to prioritize, contextualize, and operationalize this information in their detection and prevention infrastructure.

Solution Highlights

Flexible Intel Feed automates the process of:

- Identifying high priority IOCs from validated security incidents
- Correlating and contextualizing prioritized IOCs with curated threat intelligence
- Packaging the enriched intelligence into an easily consumable format for

Prioritize. Contextualize. Operationalize.

IOCs from Internal Security Incidents

As outlined in NIST 800-61, NIST's Incident Response Life Cycle recommends a feedback loop, where Detection and Analysis efforts are supplemented by new intelligence gained during Containment, Eradication, and Recovery.

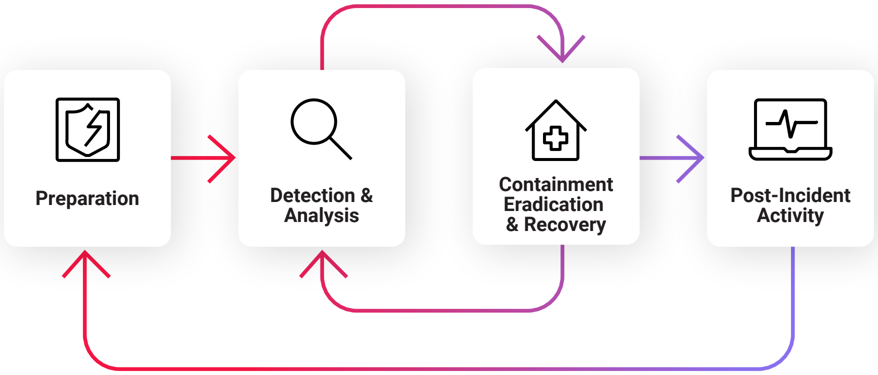

Figure 1: NIST 800-61 Incident Response Life Cycle

Critical indicators of compromise (IOCs) gathered during Containment and Recovery should be used to expand Detection and Analysis activities to document the full scope of the incident, provide validation of remediation, and fine tune detection infrastructure. Given the volume of data, metadata, and potential IOCs generated during an incident, many organizations struggle to identify which IOCs have the most value and to properly correlate and contextualize this raw data with curated intelligence. Even large organizations which have the expertise to enrich and correlate IOCs can struggle with operationalizing this content in their security infrastructure for detection and prevention.

Unstructured IOCs from External Sources

Threat intelligence on late breaking threats and active campaigns from sources like FS-ISAC, CISA, or other trusted sources often come in unstructured email, text, and/or PDF format. This creates a challenge for organizations to enrich, contextualize, and operationalize this content quickly and accurately to identify and prevent active threats. Speed of deployment and prioritization of the intelligence are critical in ensuring your organization remains protected during active campaigns and to prevent time lost to low-fidelity false positives.

Transforming Raw IOCs into Curated Threat Intelligence

Use Case 1

IOC Prioritization and Enrichment for Threat Hunting / Detection Engineering

Challenge:
Identifying and prioritizing IOCs from internal security events then correlating, enriching, and operationalizing high-priority IOCs to maximize threat hunting and detection engineering efforts.

Impact:
ReversingLabs Flexible Intel Feed automatically transforms your organization's Spectra Analyze activity into a private, curated threat intelligence feed delivered in STIX/TAXII format, making this easy to implement across a wide range of security solutions. Flexible Intel Feed provides a continuous feed of prioritized, contextualized, and enriched IOCs of all files and URLs submitted to Spectra Analyze by your organization. Flexible Intel Feed is prioritized by severity to reduce false positive alerts and enriched with the full breadth of threat intelligence ReversingLabs is known for. No more guesswork or manual effort to assign priorities, identify what is important, and correlate raw IOCs from observed behavior with the wider threat landscape.

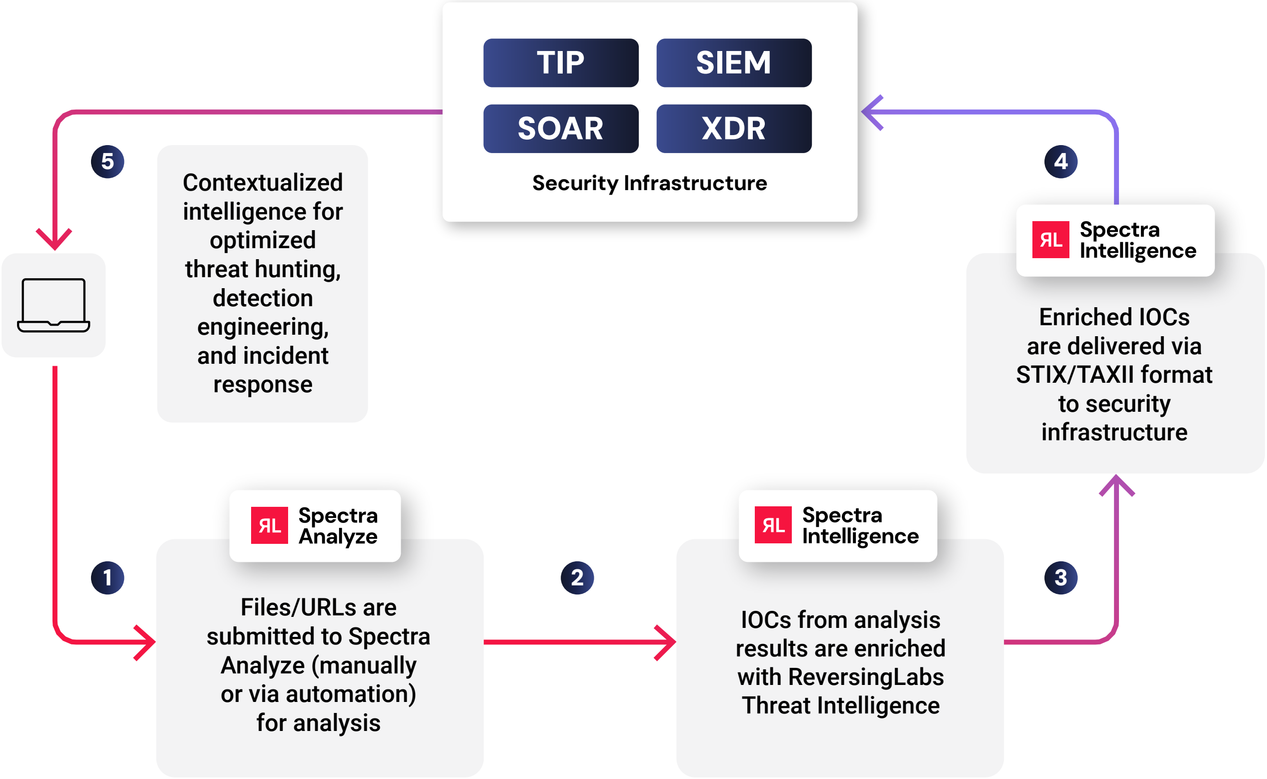
TIP
SIEM
SOAR
XDR
Security Infrastructure
5
Contextualized intelligence for optimized threat hunting, detection engineering, and incident response
4
Spectra Intelligence
Enriched IOCs are delivered via STIX/TAXII format to security infrastructure
1
Spectra Analyze
Files/URLs are submitted to Spectra Analyze (manually or via automation) for analysis
2
Spectra Intelligence
IOCs from analysis results are enriched with ReversingLabs Threat Intelligence
3

Figure 2: Flexible Intel Feed - Private Sample Analysis Workflow

Use Case 2

Targeted Campaigns and Unstructured Threat Intelligence

Challenge:
Processing unstructured IOC lists delivered in text, email, and/or PDF formats into prioritized, actionable threat intelligence to detect and prevent breaking threats.

Impact:
ReversingLabs Flexible Intel Feed easily transforms unstructured IOC lists into prioritized, curated, and actionable threat intelligence as easily as performing a copy / paste / search. Search results on IOCs of interest are queued for analysis by Spectra Analyze with the results automatically added to the Flexible Intel Feed for prioritization, enrichment, and implementation. Bulk actions can be accomplished via API for full automation of this process. Human effort that used to be spent processing unstructured threat intelligence can be refocused on other high impact tasks, providing direct and tangible ROI.

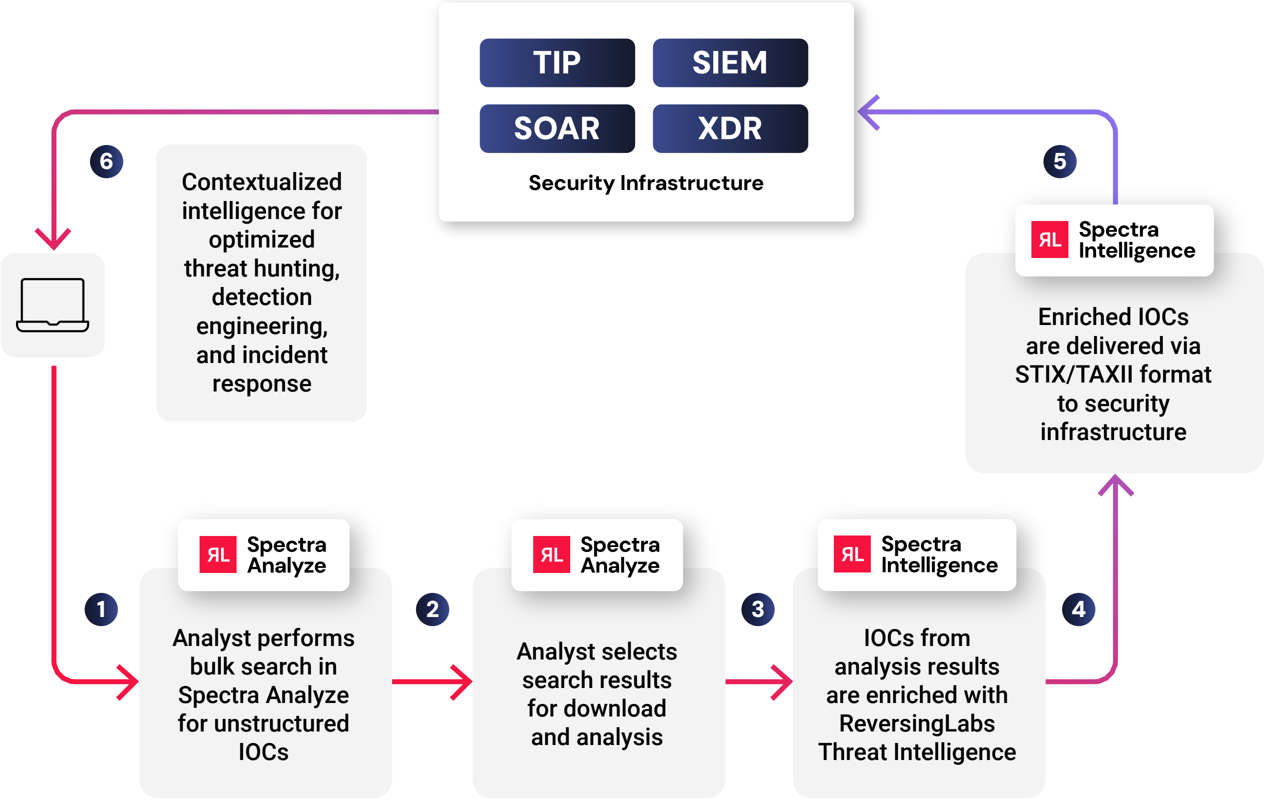
TIP
SIEM
SOAR
XDR
Security Infrastructure
6
Contextualized intelligence for optimized threat hunting, detection engineering, and incident response
5
Spectra Intelligence
Enriched IOCs are delivered via STIX/TAXII format to security infrastructure
Spectra Analyze
1
Analyst performs bulk search in Spectra Analyze for unstructured IOCs
2
Spectra Analyze
Analyst selects search results for download and analysis
3
Spectra Intelligence
IOCs from analysis results are enriched with ReversingLabs Threat Intelligence
4

Figure 3: Flexible Intel Feed - Unstructured IOC Enrichment Workflow

Conclusion

ReversingLabs Flexible Intel Feed takes the manual effort out of the crucial task of creating curated and contextualized threat intelligence from both internal security events and unstructured IOCs from trusted sources. Using ReversingLabs extensive threat intelligence repository, raw IOCs are transformed into contextualized, prioritized, and actionable threat intelligence which is easily and readily consumable by your security infrastructure. Flexible Intelligence Feed increases threat detection and prevention accuracy while reducing false positive alerts in one simple-to-deploy automated process.

Get Started!

Experience the ReversingLabs Difference

REQUEST A DEMO

www.reversinglabs.com

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, RL Spectra Core powers the software supply chain and file security insights, tracking over 422 billion searchable files 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.