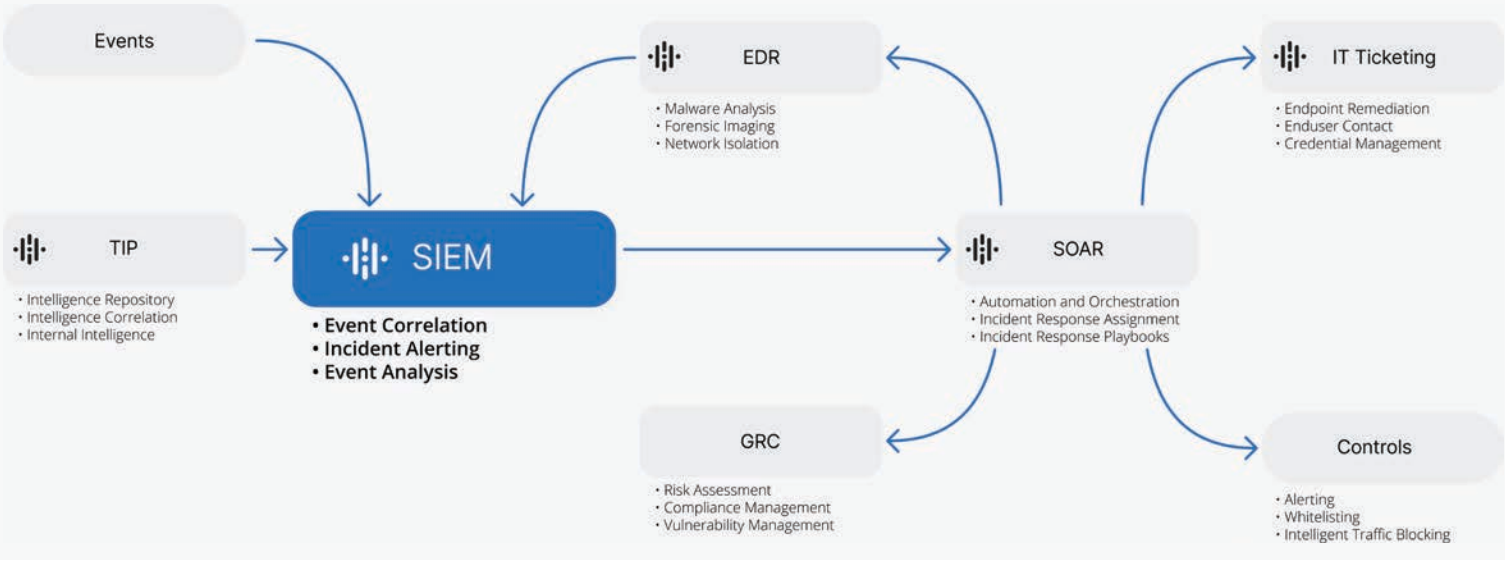


Supercharging SOAR Solutions With Threat Intelligence

The Challenge With SOAR: Automation Requires Actionable Data

Orchestration and automation are key drivers for digital transformation, enabling organizations to optimize existing processes, lower costs, fill personnel gaps, and gain a competitive edge. Recognizing these clear benefits, security teams have started to embrace security orchestration, automation, and response (SOAR) technology to collect and analyze threat data from multiple sources and automate repeatable incident response (IR) tasks. Many early adopters are using SOAR to augment existing SIEM systems and empower their security teams to drive down mean time to detection (MTTD) and mean time to response (MTTR) by working smarter and faster.

For SOAR solutions to work effectively, they require a series of defined playbooks designed to describe threats and how to handle them using repeatable, automated security workflows. But these playbooks are only as smart and effective as the data used to construct them. Without actionable, real-time data on active and emerging threats, security teams face the following challenges with their SOAR technology:

- **Information Overload:** Numerous security technologies feed the SOAR thousands of security alerts a day. While this information is necessary for decision-making and task automation, it's typically not delivered in a way that's contextual, actionable, or programmable. Studies show that on average, it takes analysts over four days to manually resolve such alerts. As a result, many security breaches go undiscovered for months, giving hackers free rein and time to wreak havoc.

Integration Partners

Recorded Future has existing SOAR integrations with the following security software partners, enabling organizations to reduce attacker dwell time and make better decisions.

splunk> SWIMLANE

IBM Security insightConnect

paloalto NETWORKS sumo logic

- **Lack of Context From Internal Systems:** Logs and events feeding the SOAR are often riddled with false positives or missing the vital information that's necessary to make the best decision. To act effectively on these alerts and properly triage them, analysts often need to spend hours performing research and analysis. The decision for how to respond needs to not only be good enough for that event or incident at that moment, but also consider the threat's historical context and ability to stand the test of time.
- **Limited View of External Threats:** In order for the SOAR to provide meaningful data for analysis and automated decision-making, it requires a full, integrated view of external threat information. Without a broad set of contextualized and relevant data, the IR team — and the SOAR playbooks — won't have a full picture of what is happening, leaving organizations unaware of external threats that could be targeting them.

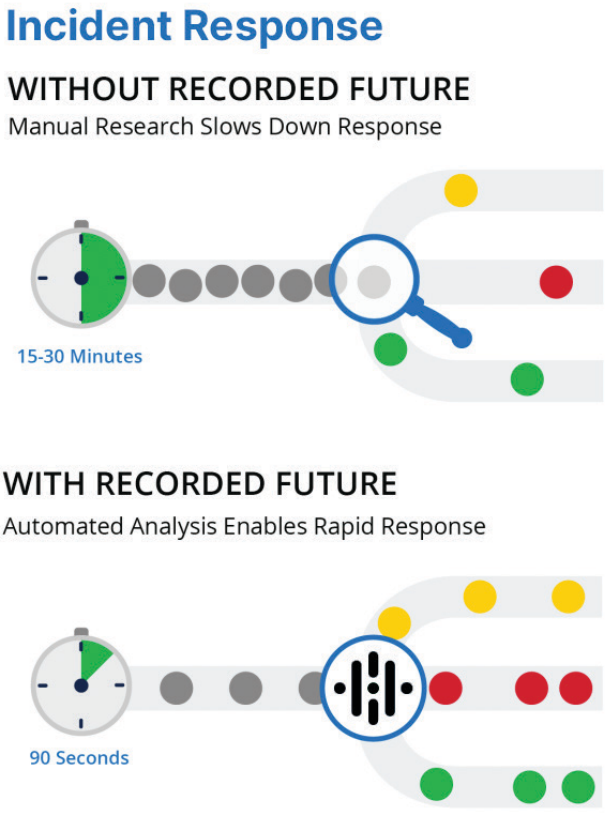
As alert volumes surge and the attack surface continues to grow, IR teams are increasingly challenged to gather the information needed to develop playbooks and automate security processes. While threat feeds can aid in uncovering new threats, the varying quality of feeds and lack of context often create unnecessary manual work. When trying to integrate external threat data into SOAR, analysts are often forced to follow a series of manual tasks to respond to an incident type and make decisions at specific points of query during the playbook execution. This is counterintuitive to the value of a SOAR solution, and it impedes the incident response team's ability to focus on high-value work. Analysts need a way to prioritize alerts so they can optimize their efforts and effectively and proactively reduce risk.

Contextualized Threat Intelligence, Accelerated Investigation, Seamless Integration

Properly contextualized threat intelligence that correlates with internal alerts is a vital component of any proactive security strategy. Relevant insights updated in real time give security operations analysts, incident responders, and vulnerability management professionals the insights they need, when they need them, to make faster, more confident security decisions. Real-time threat intelligence from Recorded Future is machine readable for frictionless integration with existing SOAR solutions, empowering analysts to investigate and respond faster, reduce false positives, and make more confident decisions.

Using Real-Time Intelligence in SOAR Technology

- **Contextualize threat intelligence.** When an alert is passed to SOAR, a playbook can be automatically invoked to obtain associated Recorded Future Risk Scores and Evidence to inform the decision-making logic.
- **Rapidly identify critical threats.** Recorded Future can speed the identification and escalation of an IOC to an IR analyst if it's deemed high risk — helping analysts detect threats earlier and resolve incidents faster.
- **Increase security team efficiency.** Actionable threat intelligence and direct access to source material gives security teams the context needed to streamline investigations and quickly determine how to contain and mitigate threats — boosting workforce efficiency and engagement.



Faster Investigation and Response

Analysts are inherently limited by how much research they can perform on any given alert. There are only so many sources they can consult and so much time they can spend before needing to come to a verdict. Recorded Future supplies SOAR solutions with vital information in real time, by using an automated approach to threat intelligence collection. We gather data from the broadest set of sources and use natural language processing and analytics to connect disparate data points across the web and aggregate them into intelligence that's surfaced in real time. This dramatically reduces MTTD and MTTR and empowers analysts to resolve incidents quickly and decisively.

Fewer False Positives With High-Confidence Data

Recorded Future's unique combination of automated data collection and human analysis generates high-quality intelligence that can be seamlessly integrated into SOAR solutions. Recorded Future provides real-time Risk Scores for each IP address, domain, URL, hash, and vulnerability based on risk rules determined from the widest breadth of sources. This adds valuable context to internal network observables and enables automated processes to rank indicators of compromise (IOCs) by threat severity. And it helps IR teams to quickly identify high-risk security events, rule out false positives, and address low-level events through automation. With the right intelligence from the broadest set of sources, you can trust that your SOAR has all the information it needs to automatically make real-time decisions that strengthen your organization's security.

> **"I have used Recorded Future at multiple companies now, and it has made a major impact ... Currently the IOC enrichment is my number one use case that helps our orchestration and automation flow."**

Global Threat Intelligence Manager
Gartner Peer Insights Review

Recorded Future: More Confident Decision-Making

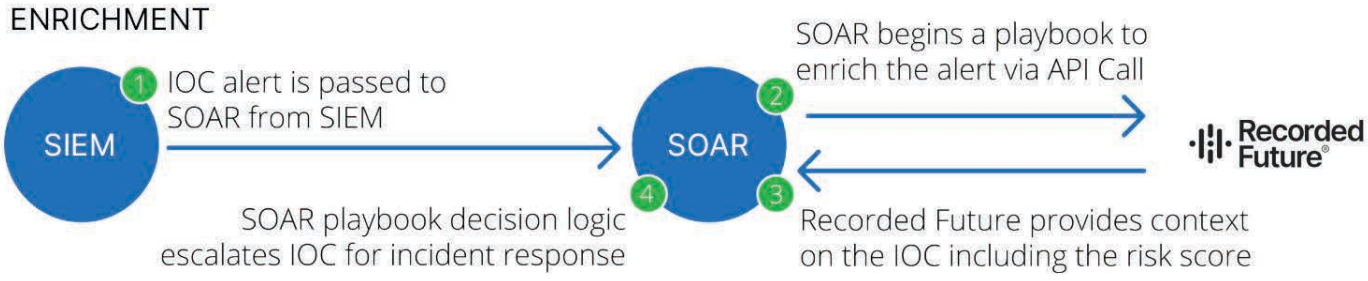
Recorded Future helps organizations reduce risk with the industry's only complete threat intelligence solution for SOAR powered by patented machine learning and artificial intelligence. The solution delivers more context than threat feeds, updates in real time so intelligence stays relevant, and integrates seamlessly with SOAR solutions to support four primary use cases:

Enrichment. Rapidly contextualize alerts by enriching them in SOAR with the broadest set of external data sources — technical, open web, and dark web sources — simplifying workflows and ensuring all detection gaps are closed.

Correlation. Identify correlations between internal activity logs and external risk and threat intelligence to initiate playbooks and drive rapid response — reducing the burden on IT security.

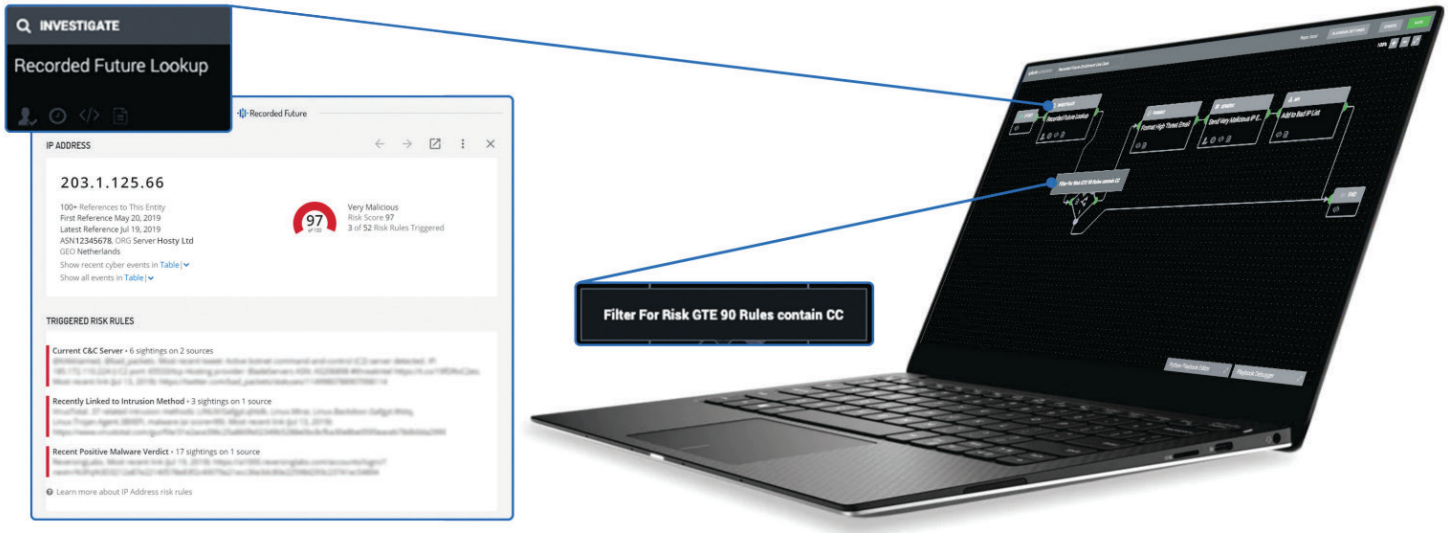
Monitoring. Continuously monitor for intelligence directly relevant to the organization and receive contextualized, risk-prioritized alerts in real time. IR playbooks can then automate and orchestrate precautionary and remediation actions.

Threat Hunting. Proactively and iteratively search through your organization's networks to detect and isolate advanced and emerging threats relevant to your organization with Recorded Future intelligence in your SOAR solution.



Recorded Future SOAR Integration in Action: Splunk Phantom

1. Your Endpoint Detection and Response tool (EDR) identifies a suspicious hash on one of your internal servers, and initiates a Splunk Phantom playbook for further investigation.
2. Splunk Phantom enriches the hash with Recorded Future intelligence to then discover it is malicious and used by several threat actors.
3. Splunk Phantom pulls the entities related to this hash, including IP addresses, from Recorded Future and uses the information in a search against the SIEM.
4. Several IP addresses related to the malicious hash are identified communicating with the internal server, corroborating the threat.
5. With this information, Splunk Phantom sends the IP address directly to MineMeld and blocks it at the perimeter, thus blocking the threat actor from achieving objectives.



Don't Take Our Word for It

A global threat intelligence manager explains how integrating Recorded Future into the company's security stack speeds up alert triage, subsequent investigation, and decision-making:

"I have used Recorded Future at multiple companies now, and it has made a major impact... Currently the IOC enrichment is my number one use case that helps our orchestration and automation flow."

Key Benefits

By integrating existing SOAR solutions with Recorded Future, organizations can:

- Improve MTTD by identifying threats **10X** faster
- Improve MTTR by resolving threats **63%** quicker
- Increase overall efficiency by **32%** before impact

EXPLORE OTHER RECORDED FUTURE INTEGRATIONS | RECORDEDFUTURE.COM/INTEGRATIONS