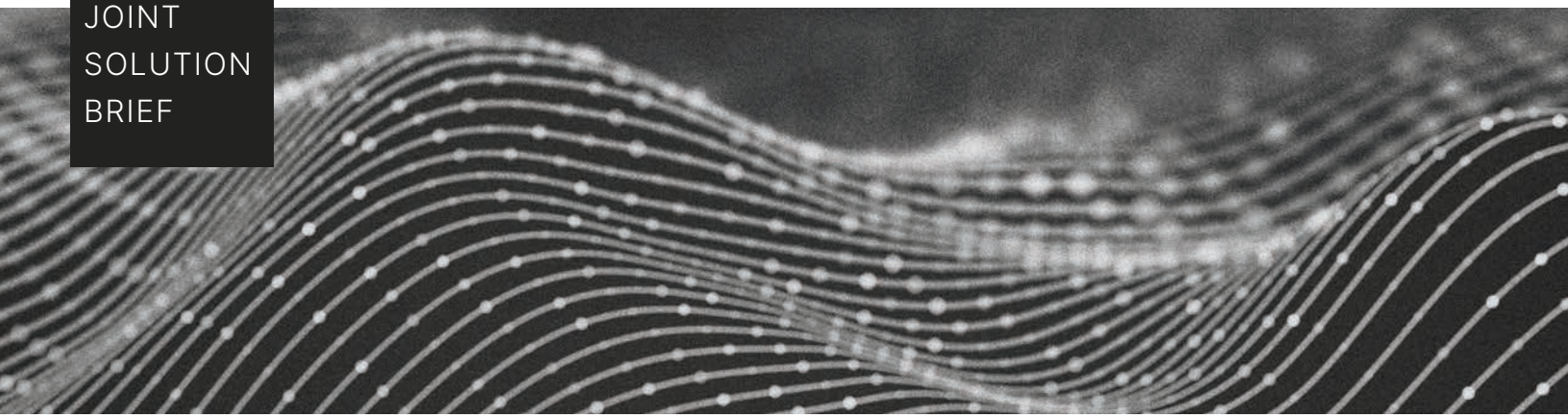
Recorded Future®

JOINT SOLUTION BRIEF



# Recorded Future and Splunk SOAR

splunk>®

**BENEFITS**

- Reduce manual research time
- Simplify incident response workflows
- Respond quickly with transparency and context
- Confidently take action on real-time threats or alerts
- Maximize your investment in Splunk SOAR

## Product Overview

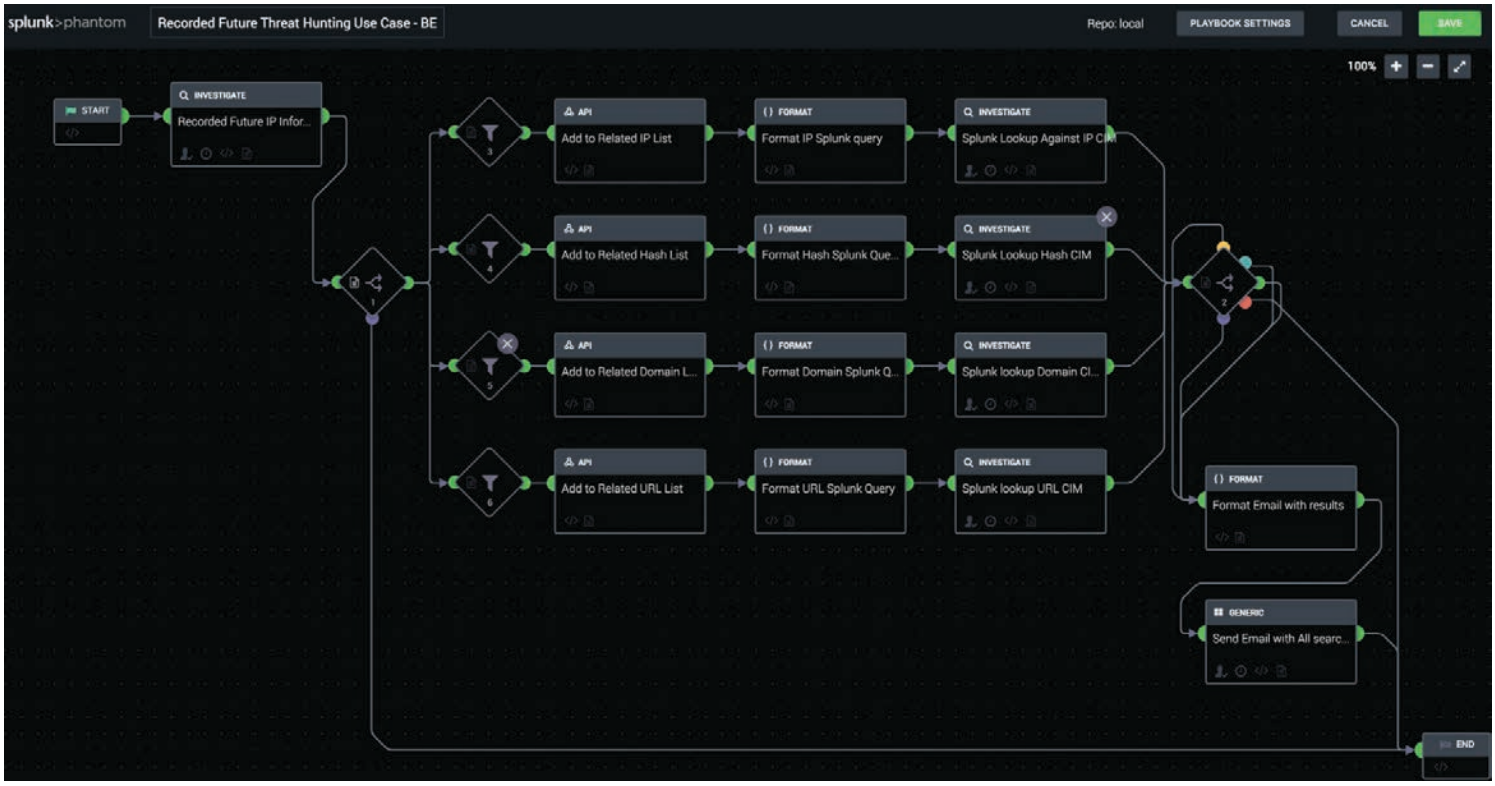
Orchestration and automation drive digital transformation by enabling organizations to optimize existing processes, reduce costs, fill personnel gaps, and gain a competitive edge. For SOAR solutions to work effectively, however, they require a series of defined playbooks designed to describe threats and how to handle them using repeatable, automated security workflows. 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 problems like an overload of information, a lack of context, and more.

## Joint Integration Description

The Recorded Future integration with Splunk SOAR improves security functions across the board by enriching data with threat intelligence and correlating internal and external data.

**Enrich Your Data with Threat Intelligence**

Recorded Future's integration with Splunk SOAR provides external details and context on indicators of compromise (IOCs). While an indicator can be useful information when responding to an incident, it can also be useless. Analysts need context in order to determine where to focus their time and energy - context like whether or not an IP address has already been associated with a phishing site, for example. Looking for this kind of context manually is a time-consuming process, which is where Splunk SOAR playbooks come into play. Automating this process with threat intelligence integrated into the process means that a playbook can be automatically invoked to get risk scores and associated context for these IOCs from Recorded Future. With this context, analysts can discover real threats faster and prioritize the highest-risk ones while ignoring the alerts that don't matter.




### Correlate Internal and External Data

It's not enough to just know what's going on in your organization. In today's world of aggressive uncertainty, it's essential to learn from attacks impacting other organizations. Given that threat actors are leveraging tools and tactics that already work, pattern recognition can give organizations an advantage in identifying suspicious activity and predicting attacks - if you have the right tools to do so. Recorded Future external threat context, correlated with your internal telemetry data through a SOAR correlation action, enables real-time detection of previously undetected threats within your environment. This proactive, intelligent, automatic blocking means that suspicious activity can be instantly cut off without needing human oversight, lowering your risk profile, and preventing breaches.

## Challenges Overcome through Integration

Numerous security technologies feed Splunk 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. In order for SOAR to provide meaningful data for analysis and decision-making, it requires a full, integrated view of external threat information. Without a broad set of contextualized and relevant data, the security 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.

## Use Cases

- **Alert Triage:** Automatically retrieve external data and context on IOCs to prioritize alerts and take immediate action
- **Threat Detection:** Initiate playbooks based on correlation of data, empowering security teams to automate responses and reduce risk
- **Threat Monitoring:** Use Recorded Future alerts to stay on top of security events and risk factors and respond faster with more real-time context
- **Threat Hunting:** Proactively and iteratively search through networks to detect and isolate advanced threats that evade existing security solutions

### ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

www.recordedfuture.com @RecordedFuture