

Automate Security Workflows

Enhance security operations with the context needed to identify and mitigate critical threats

Problem

Security teams are buried in alerts, burdened with manual workflows, and lacking sufficient context, leaving them scrambling to stay ahead of attackers.

Many alerts received by security operations teams are non-critical, creating noise that leads to critical alerts not being investigated and leading to potential risks slipping through the cracks.

Given the current threat landscape, speed is both your greatest adversary and biggest advantage. As adversaries continue to pick up their pace, it's more important than ever to fuse intelligence within your tools and workflows to separate the signal from the noise and ensure you can focus on critical alerts before they impact the business.

Solution

Recorded Future enables security teams to respond to threats faster and more efficiently by automating the collection and distribution of intelligence in an actionable format. Integrated into your security tools and workflows, Recorded Future correlates and enriches internal data with external insights to reduce noise, improve detection and response time, and enhance analyst efficiency.



SOC teams are able to investigate only

33%

of alerts received



Drivers

Dynamic Threat Landscape

Cybersecurity Skills Shortage

Security Stack Complexity

Challenge

Dynamic indicators

Lack of context

Alert fatigue

Threat Intelligence Outcomes

Reduce noise

Improve detection and response time

Enhance Analyst efficiency

Benefits

Focus on what matters

Empower security teams to efficiently prioritize alerts for investigation, eliminate the need to navigate between multiple tools, and streamline workflows to make informed decisions with ease.

Context at your fingertips

Get the information you need integrated into the tools your team uses today, including the severity of an indicator, related IOCs, linked malware, and expert research on the indicator in question.

Enhance efficiency and take proactive action

Achieve reliable and trusted outcomes with intelligence as the foundation of your security operations automation strategy. Reduce the burden of manual tasks, whether it involves automating file detonation, conducting threat hunts, or by setting alerts to prevent future attacks.

The screenshot shows the Splunk Enterprise Correlations interface. At the top, there are navigation tabs: Alert Center, Enrichment, Search, Data, Configuration, and Docs. The main heading is "Correlations". Below this, there are filters for IOC Type (set to IP), Correlation, and BadIPs. A large red number "150" indicates the "Number of ip IOCs". To the right, a "Top Ip Rule Hits" list includes items like "Recently Reported C&C Server", "Previously Validated C&C Server", and "Historically Linked to Intrusion Method". Below this is a table titled "High Risk Ip IOCs" with columns for Risk, IOC, Count, Rules, and Evidence.

Risk	IOC	Count	Rules	Evidence
99	45.61.186.	1	13/72	Validated C&C Server: 3 sightings on 1 source: Recorded Future Command & Control Validation. Recorded Future analysis validated 45.61.186. as a command and control server for Cobalt Strike on May 10, 2023
99	92.53.90.	1	10/72	Validated C&C Server: 1 sighting on 1 source: Recorded Future Command & Control Validation. Recorded Future analysis validated 92.53.90. as a command and control server for SystemBC on May 11, 2023

Client Proof

"Recorded Future has significantly improved our organization's security operations. We automated 70% of manual workflows, cutting investigation times by 50%. This led to a 40% increase in threat detection efficiency and a 30% reduction in response times, enhancing our overall security posture."

- Sr. SOC & Threat Intelligence Analyst, Air Freight & Logistics Company

Metrics*

Increase Capacity

43%

increase in security team's capacity

Save Time

15.9 hours

saved per week on alert investigation, triage, and response efforts

Accelerate Threat Identification

65%

increase in speed to identify a new threat

Request a Demo recordedfuture.com/demo

*User Evidence