Recorded Future

Recorded Future for Splunk

Threat Intelligence Powered by Machine Learning, Tailored for Security Operations

splunk>

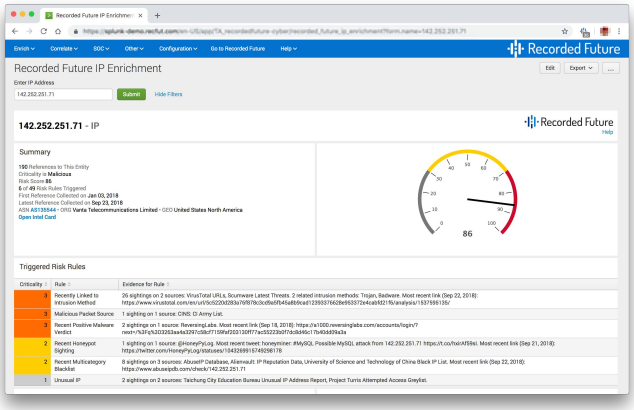
INTEGRATION WITH SPLUNK

Recorded Future for Splunk provides real-time intelligence for SOC teams with a Splunk® security solution.

Get started by downloading our Splunk Enterprise or Splunk ES AppInspect approved apps from Splunkbase

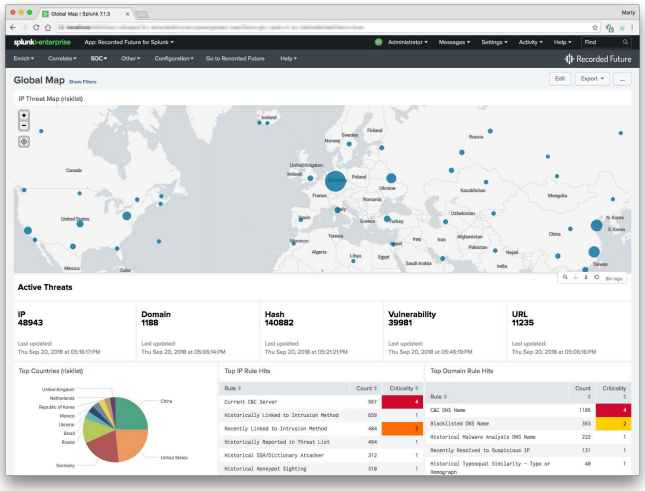
- Risk Lists to drive correlation rules
- Explore dashboard to test risklist correlations before setting up alerts
- Risk Lookups for event prioritization
- Enrichment dashboards for triage
- Intelligence Cards for incident response investigation
- On-demand export to STIX and CSV
- Alert Dashboard shows outside-the-network risks
- Access to Recorded Future's web application for further research

Dramatically increase your speed to "no" verdicts. Rapidly understand true incidents in context.



Security operations center (SOC) teams are inundated with alerts and events. Threat intelligence from Recorded Future creates clarity by adding rich context. We surface and deliver threat intelligence in real time from the widest breadth of open, technical, and dark web sources, helping you make informed verdicts. SOC analysts can efficiently dismiss false positives and capture threat context for true incidents.

Detect important incidents in your network that you would otherwise have missed.



Recorded Future identifies indicators with elevated risk by analyzing web reporting, threat lists, and our own novel methods. And unlike IP or domain reputation lists, we deliver rich context so you can selectively apply indicators that match your security needs in event correlation and detection rules.

SPLUNK ENTERPRISE AND SPLUNK ES

Add Recorded Future to your Splunk Enterprise or Splunk ES security solution. Augment your ES deployment with our threat intel content, drop our dashboards into your Enterprise deployment, or use our commands and lookups to configure the dashboards and alerts that precisely fit your needs.

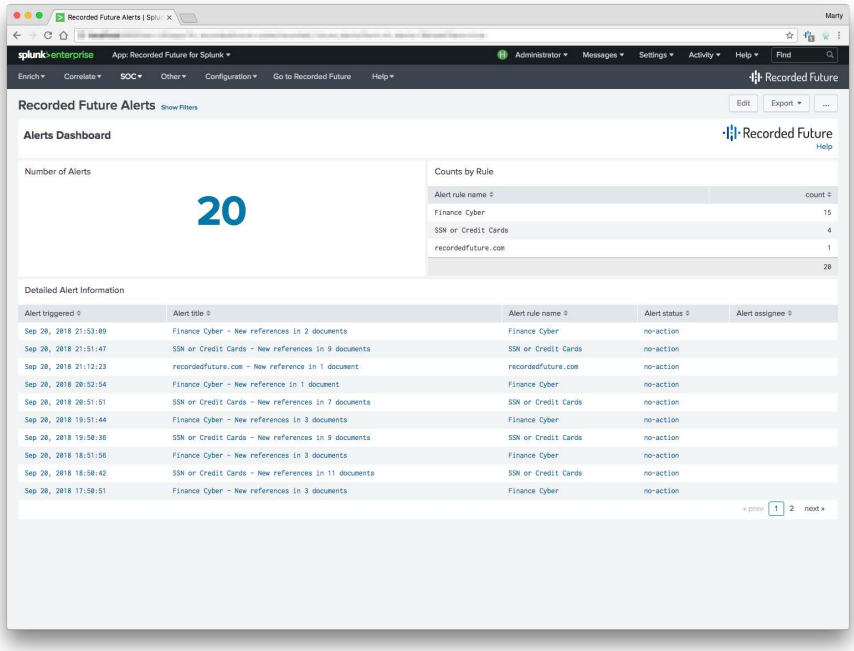
ADAPTIVE RESPONSE

Recorded Future for Splunk leverages the new Adaptive Response Framework, which provides greater integration with Splunk ES. If you have Splunk ES 4.5 (or higher), you can:

- Use Adaptive Response Actions to connect with Recorded Future manually or through automated processes.
- Enrich IOCs from any Notable Event with context from Recorded Future.
- View enrichment information in a custom dashboard.

Gain threat awareness beyond your network.

Be proactive with incident detection, as risks originate or are first reported outside your network. Monitor and alert on risks related to your IP ranges, domains, and company using Recorded Future as your sensor in the web. When alerting rules trigger, we deliver detailed notifications with provenance, links to sources, and cached access to ephemeral content.



For a demo or quote, email us at **splunk@recordedfuture.com.**

Recorded Future

About Recorded Future

Recorded Future arms security teams with threat intelligence powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context that's delivered in real time and packaged for human analysis or instant integration with existing security technology.