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 ApplInspect 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

Recorded Future for Splunk

Threat Intelligence Powered by Machine Learning, Tailored for Security Operations

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.
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.