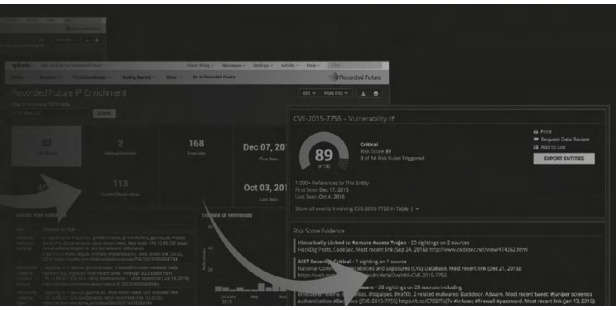
Recorded Future

DATA SHEET

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.

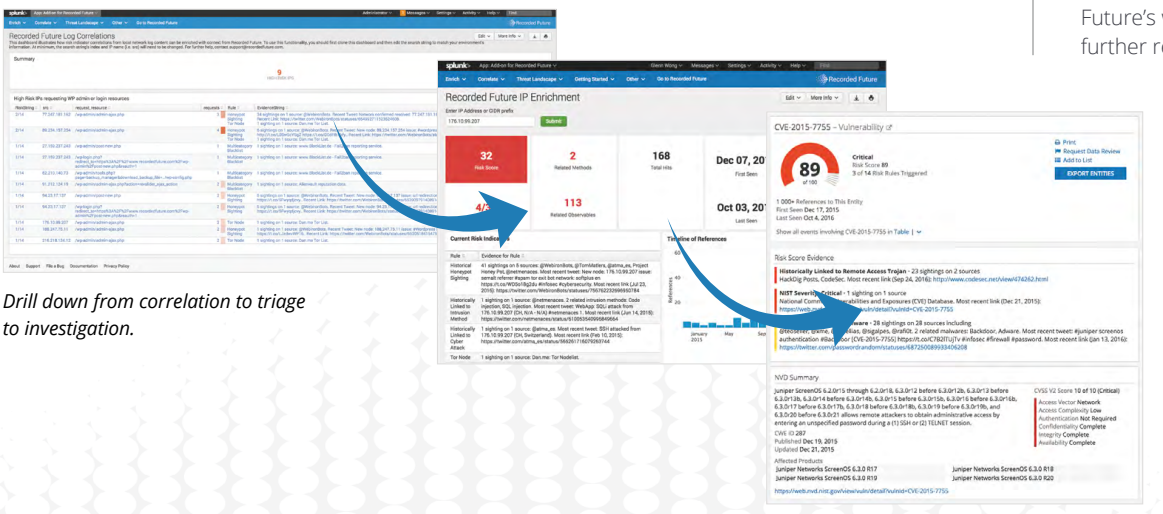
Security operations center (SOC) teams are inundated with alerts and events. Threat intelligence from Recorded Future creates clarity by adding rich context. We surface and deliver threat intelligence in real time from the widest breadth of open, technical and dark web sources, helping you make informed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



Drill down from correlation to triage to investigation.

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-certified Enterprise app** or our **Splunk-certified ES TA** from Splunk Base.

- Risk Lists to drive correlation rules
- Risk Lookups for event prioritization
- Enrichment dashboards for triage
- Intelligence Cards for IR investigation
- On-demand export to STIX and CSV
- Alerts on outside-the-network risks
- Sec Ops Access to Recorded Future's web application for further research

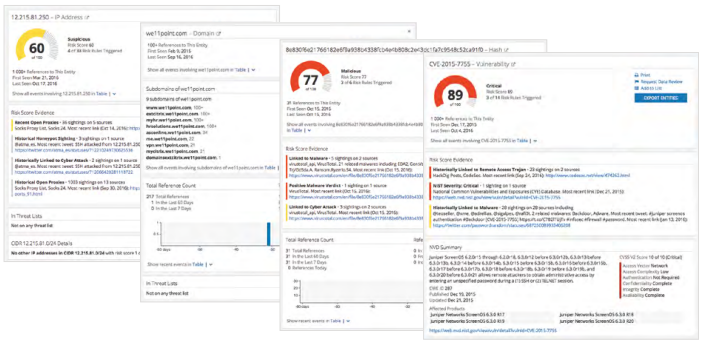
Threat Intelligence Powered by Machine Learning

We arm you with threat intelligence from open, technical, and dark web sources so you can proactively defend your organization from cyber attacks.

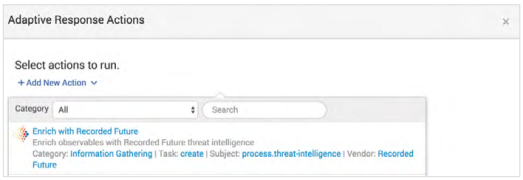
Every day organizations are blindsided by cyber attacks, and analysts risk missing external threats that impact their business. There are valuable sources of threat data out there, but analysts struggle to gain insights from it. As a result, organizations' risk of hacks and breaches increases alongside the data. Recorded Future delivers threat intelligence by applying machine learning and natural language processing to millions of data points collected from an unrivaled array of sources each day. Our technology makes sense of references to indicators of compromise, attack vectors, and emerging tactics.

More context for better insight.

To help organizations proactively defend against attackers, Recorded Future's threat intelligence provides analysts full context of emerging threats from the widest breadth of open, technical, and dark web sources. Recorded Future captures and structures this information for security analysis: billions of indexed facts over a eight year history, linked to sources and authors, and across multiple languages. We detect reporting of new vulnerabilities, exploits, IOCs, exposed company assets, and threat actors targeting organizations and industries. This threat intelligence can be readily filtered to an individual organization, its IT infrastructure, partners, and industry helping to reduce security risk.



Intel Cards deliver instant context on IPs, domains, hashes, and vulnerabilities.



Recorded Future's Adaptive Response Enrichment Action

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

Why Recorded Future

- **Faster Analysis:** Spend less time collecting data and supercharge your analytic capacity.
- **Cut Out the Middleman:** Direct access to real-time intel for monitoring and IR.
- **Always Relevant Intel:** Filtered to your corporate profile, environment, and infrastructure.

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.

About Recorded Future

Recorded Future delivers threat intelligence powered by machine learning, arming you to significantly lower risk. We enable you to connect the dots to rapidly reveal unknown threats before they impact your business, and empower you to respond to security alerts 10 times faster. Our patented technology automatically collects and analyzes intelligence from technical, open, and dark web sources to deliver radically more context than ever before, updates in real time so intelligence stays relevant, and packages information ready for human analysis or instant integration with your existing security systems.

Recorded Future, 363 Highland Avenue, Somerville, MA 02144 USA | © Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners. | 05/17