DATA SHEET

Recorded Future for Splunk

As the attack surface grows, security teams are seeing more and more events each day. However, with too little time and not enough context on the activity in their cloud environment, there's no way to connect the dots between data in their SIEM and the external risk of any detected threats. This slows responses and potentially enables relevant threats to slip through the cracks.

Contextualized Intelligence

Relevant insights, updated in real time, and integrated with your existing infrastructure drive faster, more informed security decisions. Recorded Future's intelligence reduces security risk by automatically positioning threat data in your Splunk environment. This empowers analysts to identify and triage alerts faster, proactively block threats, and reduce time spent on false positives to improve analyst efficiency.

Understand Alerts in Context

Recorded Future surfaces and delivers intelligence in real time from the widest breadth of open, technical, and dark web sources, helping Splunk users make informed verdicts. Evidence-driven risk scores backed by transparent sourcing and in-app Recorded Future Intelligence Cards enable analysts to confidently triage Splunk alerts and efficiently dismiss false positives.

Accelerate Threat Detection

Recorded Future enables analysts to spend less time researching and more time remediating by correlating external threat intelligence against internal telemetry data by layering real-time security intelligence on top of internal activity in Splunk. This provides analysts with visibility into technical indicators — and empowers them to make prioritization decisions based on a real-time Recorded Future risk score that is backed by transparent evidence.

Proactively Block External Threats

The ever-growing number and dynamic nature of threat indicators make it extremely difficult to confidently identify, block, and prevent real threats. By providing known malicious indicators identified across open, closed, and technical sources, Recorded Future security intelligence enables Splunk users to validate known risky indicators currently living on endpoints and proactively block threats in their environment.

BENEFITS

- Automatically detect risky IOCs in your environment
- Triage alerts faster with elite, real-time intelligence
- Respond quickly with transparency and context around internal telemetry data
- Proactively block threats before they impact the business
- Maximize your investment in Splunk

KEY FEATURES

- Risk lists to drive correlation rules
- Explore dashboard to test risk list 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 Portal for further research

FREE TRIAL

Start your free 30-day trial of Recorded Future's integration for Splunk today and dramatically reduce the amount of time it takes to detect, investigate, and respond to real threats:

https://go.recordedfuture.com/splunk-integration-trial

Results*

Resolve Security Threats 63% Faster

Relevant insights, updated in real time, and integrated with Splunk drive faster, more informed security decisions. Recorded Future eliminates laborious manual collection by providing contextual intelligence on internal telemetry data — empowering teams to quickly and confidently respond to incidents.

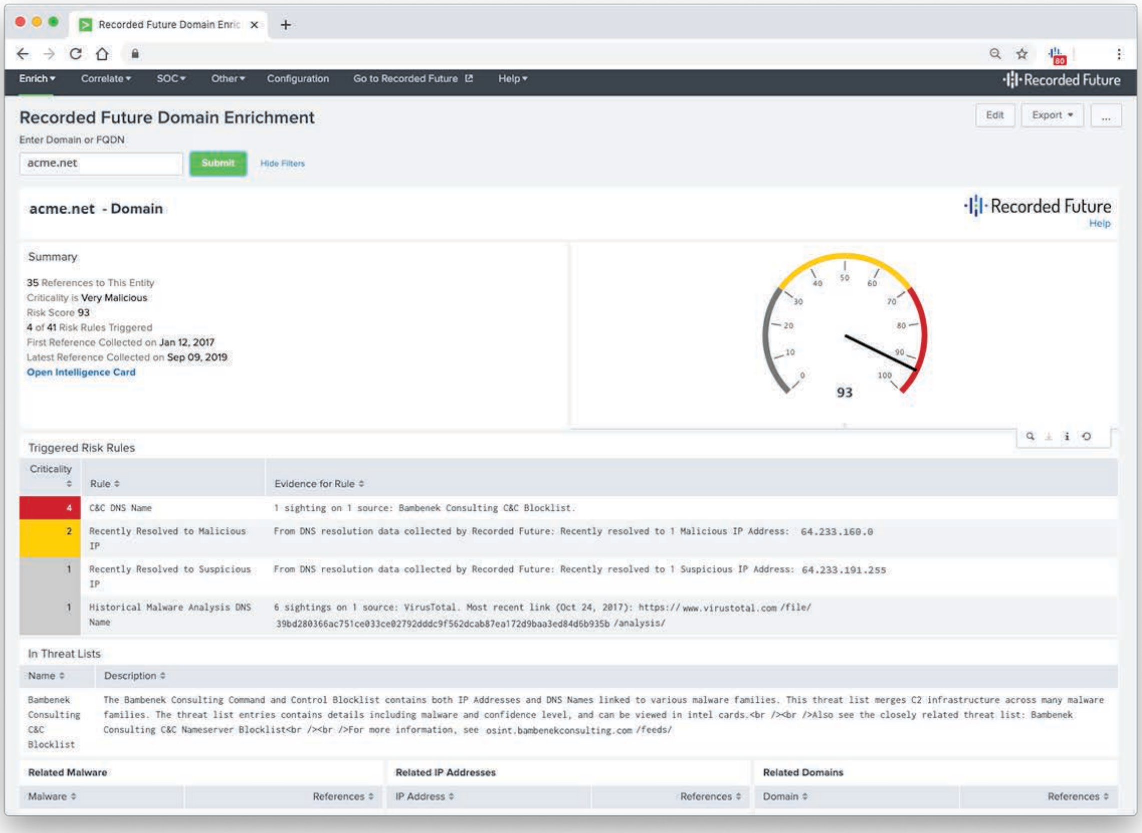
Identify 22% More Security Threats Before Impact

Using a sophisticated combination of patented machine and expert human analysis, Recorded Future fuses an unrivaled set of open source, dark web, technical sources, and original research to deliver relevant cyber threat insights in real time — empowering you to identify threats faster.

Improve Security Team Efficiency by 32%

Use the world's most advanced security intelligence platform to easily access the information you need, when you need it, to disrupt adversaries and reduce risk to your organization.

**Learn more about the business value Recorded Future brings to clients in our IDC Report, [Organizations React to Security Threats More Efficiently and Cost Effectively with Recorded Future]*



Recorded Future Domain Enrichment

Enter Domain or FQDN: acme.net

acme.net - Domain

Summary

35 References to This Entity
Criticality is Very Malicious
Risk Score 93
4 of 41 Risk Rules Triggered
First Reference Collected on Jan 12, 2017
Latest Reference Collected on Sep 09, 2019
Open Intelligence Card

Triggered Risk Rules

Criticality ⇕	Rule ⇕	Evidence for Rule ⇕
4	C&C DNS Name	1 sighting on 1 source: Bambenek Consulting C&C Blocklist.
2	Recently Resolved to Malicious IP	From DNS resolution data collected by Recorded Future: Recently resolved to 1 Malicious IP Address: 64.233.160.0
1	Recently Resolved to Suspicious IP	From DNS resolution data collected by Recorded Future: Recently resolved to 1 Suspicious IP Address: 64.233.191.255
1	Historical Malware Analysis DNS Name	6 sightings on 1 source: VirusTotal. Most recent link (Oct 24, 2017): https:// www.virustotal.com /file/ 39bd280366ac751ce033ce02792dddc9f562dcab87ea172d9baa3ed84d6b935b /analysis/

In Threat Lists

Name ⇕	Description ⇕
Bambenek Consulting C&C Blocklist	The Bambenek Consulting Command and Control Blocklist contains both IP Addresses and DNS Names linked to various malware families. This threat list merges C2 infrastructure across many malware families. The threat list entries contains details including malware and confidence level, and can be viewed in intel cards.<br /><br />Also see the closely related threat list: Bambenek Consulting C&C Nameserver Blocklist<br /><br />For more information, see osint.bambenekconsulting.com /feeds/

Related Malware

Malware ⇕	References ⇕

Related IP Addresses

IP Address ⇕	References ⇕

Related Domains

Domain ⇕	References ⇕

View Recorded Future risk scores and risk rules for any IOC within your Splunk environment

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