Recorded Future®

DATA SHEET

Recorded Future for Splunk

Operationalize Threat Intelligence in Your SIEM

Security Operations teams rely on Splunk Enterprise and Splunk Enterprise Security to detect complex threats in their environment with advanced security analytics. Optimized for both user and technology workflows, intelligence from Recorded Future provides real-time context on who is attacking, what their motivations and capabilities are, and what indicators of compromise to look for without ever having to leave your Splunk environment.

With this integration you can:

- Automatically detect risky IOCs in your environment with real-time context from the Recorded Future Intelligence Cloud
- Use real-time threat intelligence to reduce alert triage time
- Identify high-risk alerts using Recorded Future Risk Scores, minimizing the time it takes to identify threats in your environment and for you to act before they impact business
- Operationalize threat intelligence in your SIEM with detection rules, written in Sigma format, by our Insikt research group, which can be launched directly in Splunk, eliminating the need to write or translate rules yourself.
- For Enterprise Security users, align Recorded Future intelligence to your Risk Based Alerting Framework to identify relevant threats and minimize alert fatigue

FEATURES

- Risk lists to drive correlation rules
- Use case specific correlation dashboards
- Risk lookups for event prioritization
- Enrichment dashboards for faster triage
- Intelligence Cards for informed incident response investigation
- Alert dashboard for outside-the-network risk trends
- Access to Recorded Future's Portal for further research
- Automated threat hunting with Sigma rules
- Alignment to Splunk's Risk-based Alerting framework

SPLUNK COMPATIBILITY

- Splunk Enterprise
- Splunk Enterprise Security

USE CASES

- Log Enrichment & Correlation
- Alert Triage
- Threat Detection
- Alert Monitoring

How Recorded Future client's use Recorded Future for Splunk to operationalize threat intelligence in their SIEM:

Save Time by Enriching Splunk Logs with Intelligence

A European MSSP has experienced 20-50% time savings in investigations using threat intelligence from Recorded Future and enriching their information in Splunk. Due to this time savings they are able to focus their resources on other critical areas.

Use Detection Rules to Put Yourself in Your Adversaries Shoes

A US-based health care system uses Recorded Future's Sigma Rules to consider how adversaries might evade security defenses they put in place and take a proactive approach to implementing security measures in Splunk.

Gain More Context with Actionable Queries

A Japanese eCommerce company has found the Sigma rules from Recorded Future to be a significant time saver, especially when implemented in their Splunk environment providing them with actionable queries to gain more context.

Quickly See High-Confidence Information on IOCs

A global automotive company uses Recorded Future intelligence to enrich Splunk logs to quickly see high-confidence contextual information for IOCs and notable events, allowing them to make sure they are focused on legitimate issues.

Improve Daily Workflows Through Seamless Integration with Splunk

An American biotech company uses our integration to improve their analyst's daily workflows through log enrichment from Recorded Future directly inside of Splunk, freeing up time for other tasks since they don't need to log into another portal other than Splunk, which is their main tool for security operations.

Create a Source of Truth with Recorded Future and Splunk

A global application software company uses the Recorded Future integration in their daily routines as the source of truth to ensure no critical threats were missed, for passing information along to relevant teams, and for reviewing IOCs that were flagged as bad by analysts in Splunk.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture