Recorded Future®

DATA SHEET

Recorded Future for Splunk

splunk>

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.

Recorded Future models relevant security information available from every corner of the internet by:

- Collecting and structuring adversary and victim data from text, imagery, and technical sources
- Using analytics to discover, analyze, and map associations across billions of entities in real time
- Including critical insights from our global team of world-class analysts that no machine could provide

Recorded Future's robust intelligence seamlessly integrated into Splunk's advanced streaming analytics empowers security teams to quickly and confidently react to alerts with detailed and validated threat intelligence.

Enhance Threat Detection

Recorded Future's intelligence from open, dark web, and technical sources combined with Splunk's powerful analytics enables analysts to correlate their internal telemetry logs with external risks to identify threats to their organization. The Recorded Future integration with Splunk surfaces malicious indicators alongside dynamically-updated risk scores to help analysts triage the most critical threats to their organization. This enables analysts to spend their time and energy on high-priority activities like investigating and remediating high risk threats, rather than manually researching alerts.

Accelerate Threat Investigation

Meaningful insights on potentially malicious IPs, domains, hashes, vulnerabilities, and more are available directly within Splunk. Analysts can pivot between correlation dashboards to drive rapid response on undetected threats, and enrich particular IOCs with comprehensive intelligence from Recorded Future for a holistic view of each threat. Minimizing the need to switch tools enables analysts to easily access the information required to prioritize and respond to threats.

BENEFITS

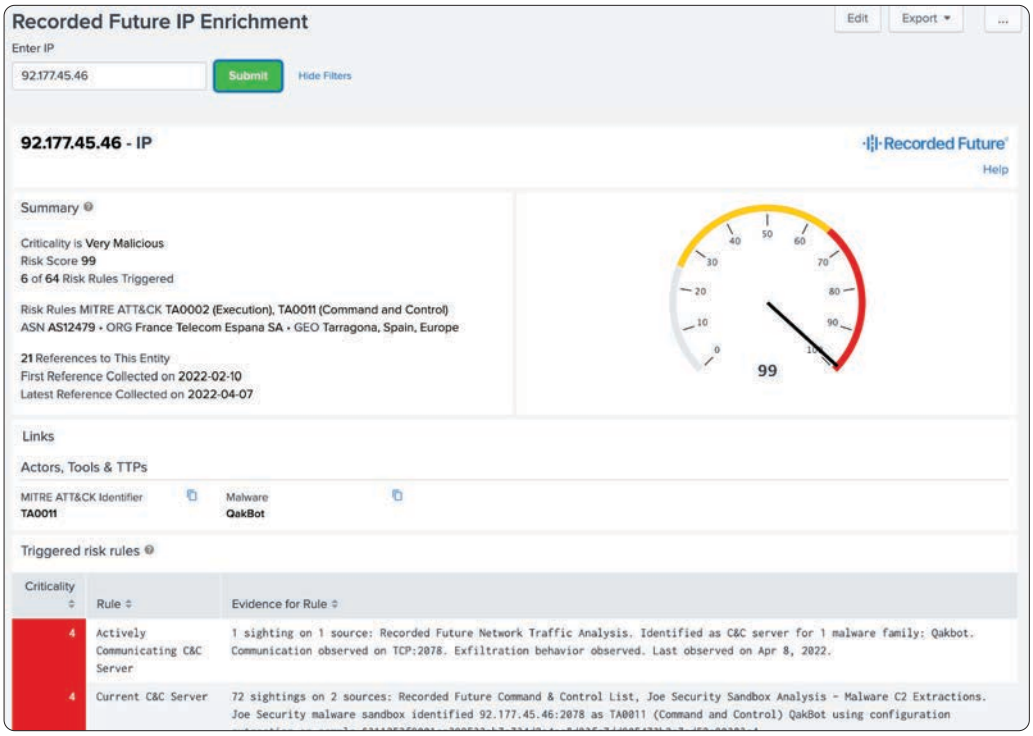
- Automatically detect risky IOCs in an environment
- Use real-time external intelligence to triage alerts faster
- Identify high risk alerts using Recorded Future Risk Scores, minimizing time it takes to identify threats in your environment and for you to act before they impact business
- Actionable context on threats seamlessly surfaced within Splunk

KEY 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
- On-demand export to STIX and CSV
- Alert dashboard for outside-the-network risk trends
- Access to Recorded Future's Portal for further research

Increase Analyst Confidence

With access to evidence-based risk scores, analysts can act with confidence to prioritize and respond to alerts. For example, Recorded Future intelligence integrated into Splunk helps users quickly determine the risk score of an IP address that triggered an alert, and further investigate to determine what rules caused the score to increase as well as gain additional evidence on who is attacking, what infrastructure they use, and the types of organizations they target. Recorded Future's proprietary intelligence graph scours an unprecedented quantity and variety of sources, maps relevant relationships between entities automatically, and includes critical insights from our global team of world-class analysts to help security teams make confident decisions.



Enrich IPs within your Splunk environment to gain meaningful insights on threats