Recorded Future®

DATA SHEET

Recorded Future for Splunk SOAR

splunk>

Recorded Future helps security teams understand attackers and their intent, what tools they are using, and who they are targeting. We do this by modeling 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
- Delivering insights optimized for both user and technology workflows

The Recorded Future integration with Splunk SOAR is designed to make it easy for security teams to build workflows and playbooks that take advantage of our robust intelligence. Combining Recorded Future's real-time external context with playbooks in Splunk SOAR enables users to create customized, repeatable, and automated security workflows.

Enrich Playbooks with Intelligence for Quick, Confident Decisions

An indicator like an IP address, a server domain, or a list of hashes can be useful information when responding to an incident, but actionable context on each indicator can enhance prioritization and speed up triage. Real-time risk scores, based on specific risk rules for each IP address, domain, URL, hash, and vulnerability add valuable context to Splunk SOAR playbooks, and speed up investigation time. For example, when an IOC is passed to Splunk SOAR, a playbook can be automatically invoked to obtain risk scores and associated context for those IOCs from Recorded Future. Then the playbook's decision logic can immediately escalate the IOC to a human analyst if it's deemed risky, or deprioritize if not.

KEY BENEFITS

- Reduce manual research time
- Simplify incident response workflows
- Respond quickly with transparency and context
- Confidently take on real-time threats or alerts
- Maximize your investment in Splunk SOAR

USE CASES

Enrichment: Rapidly contextualize alerts by enriching them in Splunk SOAR with the broadest set of external data sources – open web, technical, and dark web sources – simplifying workflows and ensuring all detection gaps are closed

Correlation: Identify correlations between internal activity logs and external risk to initiate playbooks and drive rapid response – reducing the burden on IT security

Monitoring: Continuously monitor for intelligence directly relevant to the organization and receive contextualized, risk-prioritized alerts in real time. Playbooks can then automate and orchestrate precautionary and remediation actions

Threat Hunting: Proactively and iteratively search through your organization's networks to detect and isolate advanced and emerging threats relevant to your organization with Recorded Future Intelligence integrated into Splunk SOAR

Leverage Intelligence to Find Threats in Your Environment

In addition to providing high-fidelity indicators, Recorded Future can identify relationships between internal activity logs and external risk. For example, based on suspicious log data, your SIEM issues a Breach-IOC alert to Splunk SOAR. A playbook orchestrates the enrichment of the IOC. If the risk score is greater than 80, then the playbook will add the offending IOC into an internal threat list and send an email notification to the analyst. Other actions can then be taken to block or quarantine the threat to avoid future incidents.

Proactively Hunt for Malicious Activity

Proactively and iteratively search through networks to detect and isolate advanced threats that evade existing security controls to enable analysts to spend more time on analysis rather than data collection. For example, from a suspicious event generated by your SIEM, use Recorded Future intelligence in Splunk SOAR to gather risk scores on IOCs and expand the investigation to include related entities. Analysts can then quickly pull together evidence to uncover larger threats.

Powerful Alone, Unstoppable Together

Recorded Future helps organizations reduce risk with a complete intelligence solution for Splunk SOAR. Enriching playbooks with comprehensive intelligence on dangerous IOCs helps security analysts quickly identify high-risk security events, rule out false positives, and address low-level events through automation. With contextualized intelligence from the broadest set of sources, you can trust Splunk SOAR has all the information needed to automatically make real-time decisions that strengthen your organization's security posture.