Recorded Future for Splunk Phantom
Disrupt Adversaries in Real Time with Elite Threat Intelligence

Today’s ever-changing security landscape makes it nearly impossible for time-strapped security operations and incident response teams to mitigate every potential threat to their organization. Overwhelmed by manual processes and high alert volume, they’re unable to take advantage of the breadth of intelligence available, instead they focus only on internal logs and data. Security teams need a platform that centralizes intelligence in real time and harnesses that information to drive action across security infrastructures.

To meet these challenges, Recorded Future empowers security teams with improved threat visibility and accelerated incident response. Integrating comprehensive, real-time intelligence into the security orchestration and automation features of Splunk Phantom solves for the following use cases:

**Alert Triage**: Automatically retrieve external data and context on IOCs to prioritize alerts, quickly discount false positives, identify the most significant threats, and take immediate action.

**EXAMPLE**: When a Splunk IOC alert is passed to Splunk Phantom, a playbook can be automatically invoked to get Recorded Future risk scores and associated risk rules for those IOCs. The playbook’s decision logic can immediately escalate the IOC to an analyst if deemed risky.

**BUSINESS IMPACT**: Prioritize analysts’ time to make quicker decisions on the highest-risk threats and discover threats faster.

**Threat Detection**: Identify relationships between internal activity logs in Splunk and external security intelligence. Splunk Phantom will initiate a playbook based on the correlation of the data, empowering security teams to automate responses and reduce risk for the organization.

**EXAMPLE**: Based on suspicious log data, Splunk issues a Breach-IOC alert to Splunk Phantom. The playbook enhances the IOC. If the risk score is greater than 80 and the risk string contains ransomware, then the playbook will look for and add the offending IOC into an internal list, create a feedback loop into Splunk, and send an email notification to the analyst. Other actions may be added to block or quarantine the threat via other products available in the security stack.

**BUSINESS IMPACT**: Proactive intelligent blocking can lower risk profile and prevent breaches.
Threat Monitoring: Use Recorded Future alerts to stay on top of security news, events, and risk factors important to your organization and respond faster with more real-time context.

EXAMPLE: Recorded Future provides alerts on potential threats to the organization. A Splunk Phantom playbook can be used to automate and orchestrate precautionary and remediation actions based on the alert name or validation actions.

BUSINESS IMPACT: Earlier warnings of threats empower analysts to take faster preventive actions.

Threat Hunting: Proactively and iteratively search through networks to detect and isolate advanced threats that evade existing security solutions. Enable analysts to quickly pull together related evidence to reveal a larger threat.

EXAMPLE: From a suspicious event generated by Splunk, use Recorded Future and Splunk Phantom to gather risk scores on IOCs and expand the investigation to include related entities.

BUSINESS IMPACT: Deploy an informed hunting capability to allow analysts to spend more time on analysis rather than data collection.