Recorded Future and Rapid7

PRODUCT OVERVIEW

Rapid7 InsightConnect is a security orchestration and automation response (SOAR) solution to accelerate, streamline, and integrate your teams and tools. When you use InsightConnect, you can run your multi-solution processes automatically, and free up your security team's bandwidth to tackle other challenges. InsightConnect workflows seamlessly map your security stack into automated processes with APIs, Insight products, and over 240 plugins. When you need to involve your team, InsightConnect centralizes data from your security tools so your team can take efficient action.

JOINT INTEGRATION DESCRIPTION

Recorded Future for Rapid7 Insight Connect allows organizations to quickly resolve security threats using external threat intelligence and rich context from Recorded Future directly on top of your workflows inside Insight Connect.

Analysts are able to view related external risk and evidence assigned to IPs, Domains, Hashes, CVE, and URLs for greater context as they investigate and respond to incidents. Full transparency is provided on the evidence applicable to any given IOC (indicator of compromise).

In addition, Recorded Future's risklist data is ingested Insight Connect to correlate internal telemetry data against high fidelity datasets from Recorded Future to detect threats faster. The integration makes use of the Recorded Future IP, Domain, Hash, and URL risk lists.

As a result, security and threat analysts can make quick and effective decisions at critical moments.

CHALLENGES OVERCOME THROUGH INTEGRATION

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.

USE CASES

Threat Detection: The explosive growth of indicators makes detecting real threats extremely resource-intensive for already overwhelmed security teams. Recorded Future connects the dots between the broadest range of sources across every language. This intelligence and critical context enables Rapid7 InsightConnect to automatically analyze and identify IOCs related to phishing attacks, malware, and command-and-control servers, empowering security teams to automate responses and reduce risk for the organization.

Alert Triage: With the Recorded Future and Rapid7 InsightConnect integration, analysts see which alerts should be prioritized based on a real-time risk score that is backed by transparent evidence. An enrichment playbook automatically prioritizes alerts, quickly discounts false positives, identifies the most significant threats, and takes immediate action.

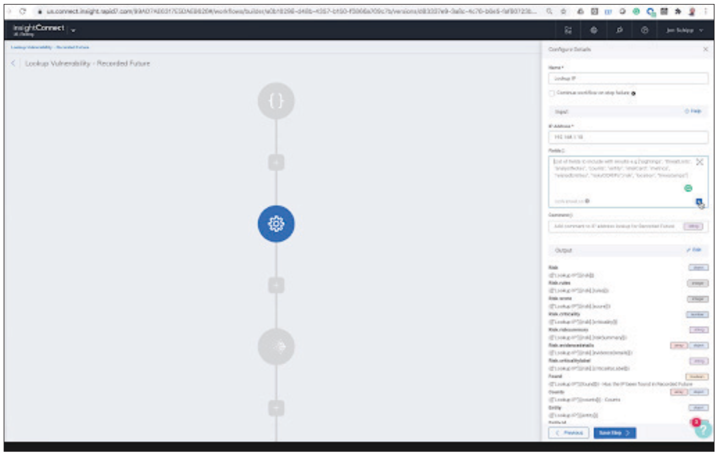
Threat Prevention: Armed with proprietary, evidence-based findings, organizations are able to automatically identify and block high-risk utilize IPs, URLs, hashes, and domains at the perimeter, minimize false positive blocking, automate incident response, and improve overall security posture.

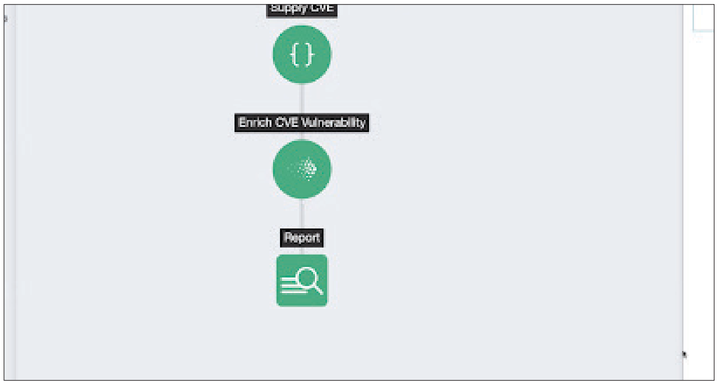
Vulnerability Prioritization: Recorded Future provides necessary, real-time context around disclosed vulnerabilities based on the organization's technologies, industry, company, and more. By positioning direct access to evidence on the new and exploited vulnerabilities impacting their assets within Rapid7 InsightConnect, organizations are enabled to produce deeper analysis and prioritize CVEs faster.

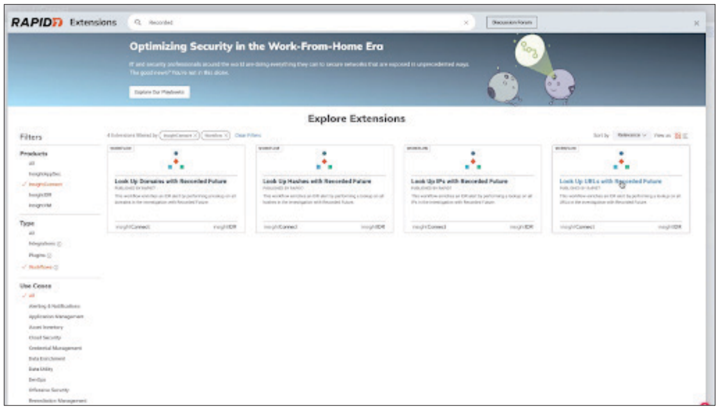
BENEFITS:

- Proactively block threats before they impact your business
- 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
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation
- Shorten your decision-making cycle by automating key tasks with analyst reviews

DATA SHEET






RAPID7 Extensions
Optimizing Security in the Work-From-Home Era
Explore Extensions
Filters
Products
Type
Use Cases
Look Up Domains with Recorded Future
Look Up Hashes with Recorded Future
Look Up IPs with Recorded Future
Look Up URLs with Recorded Future

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 hundreds of businesses and government organizations around the world.

About Rapid7

Rapid7 InsightConnect is a security orchestration and automation response (SOAR) solution to accelerate, streamline, and integrate your teams and tools. When you use InsightConnect, you can run your multi-solution processes automatically, and free up your security team's bandwidth to tackle other challenges. InsightConnect workflows seamlessly map your security stack into automated processes with APIs, Insight products, and over 240 plugins. When you need to involve your team, InsightConnect centralizes data from your security tools so your team can take efficient action.