Recorded Future®

JOINT SOLUTION BRIEF

Recorded Future and Swimlane

SWIMLANE

ABOUT

Swimlane is a leader in security orchestration, automation and response (SOAR). By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real-time dashboards and reporting from across your security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations.

Product Overview

Orchestration and automation drive digital transformation by enabling organizations to optimize existing processes, reduce costs, fill personnel gaps, and gain a competitive edge. For SOAR solutions to work effectively, however, they require a series of defined playbooks designed to describe threats and how to handle them using repeatable, automated security workflows. These playbooks are only as smart and effective as the data used to construct them. Without actionable, real-time data on active and emerging threats, security teams face problems like an overload of information, a lack of context, and more.

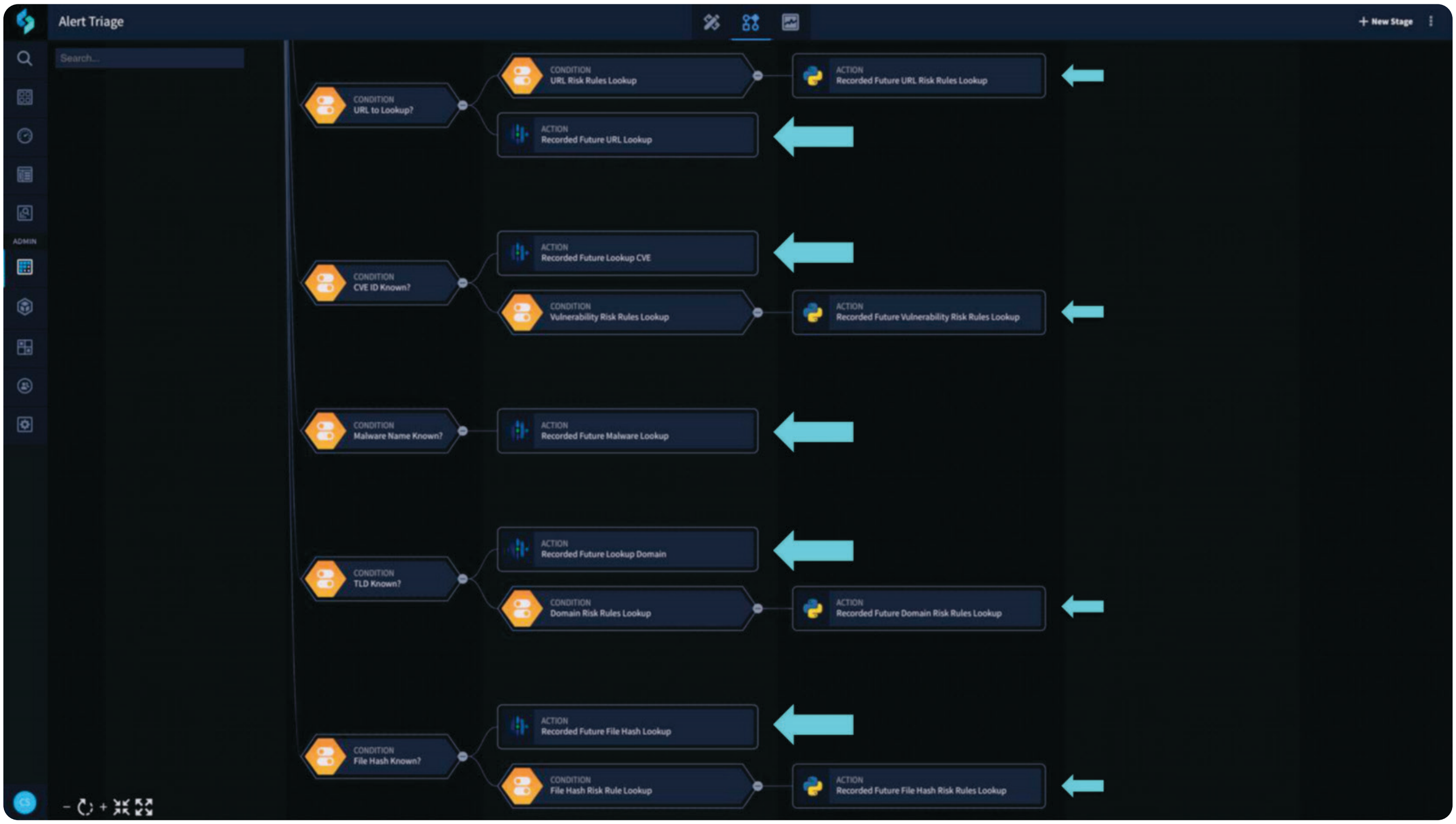
Joint Integration Description

The Swimlane and Recorded Future integration enables the Swimlane SOAR platform to quickly reference valuable threat intelligence and use it to immediately enrich, remediate and respond to security incidents. The integration also makes the Recorded Future data available in Swimlane case records saving valuable steps and time when analyst involvement is required.

Challenges Overcome through Integration

Automated Intelligence Gathering

With this integration between Swimlane and Recorded Future, workflows can be utilized to perform otherwise manual intelligence queries automatically or at the push of a button. This saves users time on every investigation and allows them to respond to critical alerts at a faster pace.


Alert Triage
Search...
ADMIN
+ New Stage
CONDITION
URL to Lookup?
CONDITION
URL Risk Rules Lookup
ACTION
Recorded Future URL Risk Rules Lookup
ACTION
Recorded Future URL Lookup
CONDITION
CVE ID Known?
ACTION
Recorded Future Lookup CVE
CONDITION
Vulnerability Risk Rules Lookup
ACTION
Recorded Future Vulnerability Risk Rules Lookup
CONDITION
Malware Name Known?
ACTION
Recorded Future Malware Lookup
CONDITION
TLD Known?
ACTION
Recorded Future Lookup Domain
CONDITION
Domain Risk Rules Lookup
ACTION
Recorded Future Domain Risk Rules Lookup
CONDITION
File Hash Known?
ACTION
Recorded Future File Hash Lookup
CONDITION
File Hash Risk Rule Lookup
ACTION
Recorded Future File Hash Risk Rules Lookup

False Positives

Many alerts coming from security tools are ultimately determined to be false positives. Without Recorded Future, analysts spend valuable time manually triaging these alerts until they have gathered enough data to indicate it is benign. Many of these lower level and repetitive false positives can be automatically enriched and closed using intelligence driven workflows that eliminate the need for analyst involvement.

Centralized Data

In today's cyber security world, many businesses and SOC's are using multiple products for intelligence and enrichment. With this integration, all of the data coming from Recorded Future can be correlated against data from adjacent tools. This allows users to see the bigger picture and saves time pivoting between multiple products.

Benefits

- Enables analysts to instantly enrich IOCs in the case record
- Tasks to quickly reference the available data and support condition-based subsequent actions
- Provide one-off tasks within the case record to avoid the time lost working multiple windows, systems, or sites

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 more than 1,000 businesses and government organizations around the world.

www.recordedfuture.com @RecordedFuture