RAPID7 + SWIMLANE

INTEGRATION BRIEF

Rapid7 Threat Command + Swimlane = Automated IOC Enrichment

Enabling Powerful Alert Investigation at Scale

The Challenge

As large enterprises look across their cybersecurity posture, it can be a bit daunting to think about how to further scale IOC enrichment and triage. There is little doubt that these large players have seen alert volumes grow over the last several years, and the sheer number of alerts today is very difficult to keep up with, even with a large team. As the world continues to go digital and move online, these large volumes of alerts will continue to grow, and security teams need to think about how they can increase their capacity.

One way organizations can look to add scale is through hiring more security analysts. However, Gartner has predicted that "By 2025, "labor volatility" will cause 40 percent of organizations to report a material business loss, forcing a shift in talent strategy from acquisition to resilience." Hiring and retaining cyber talent may become even more difficult in the coming years.

Security grows more complex by the day. The average large enterprise leverages many different point products aimed at addressing specific problems or vulnerabilities. Many of these tools are manual, forcing users to jump between products to gain a good understanding of potential threats. All of these steps make it even more challenging for security teams to stay ahead of attackers.

The Solution

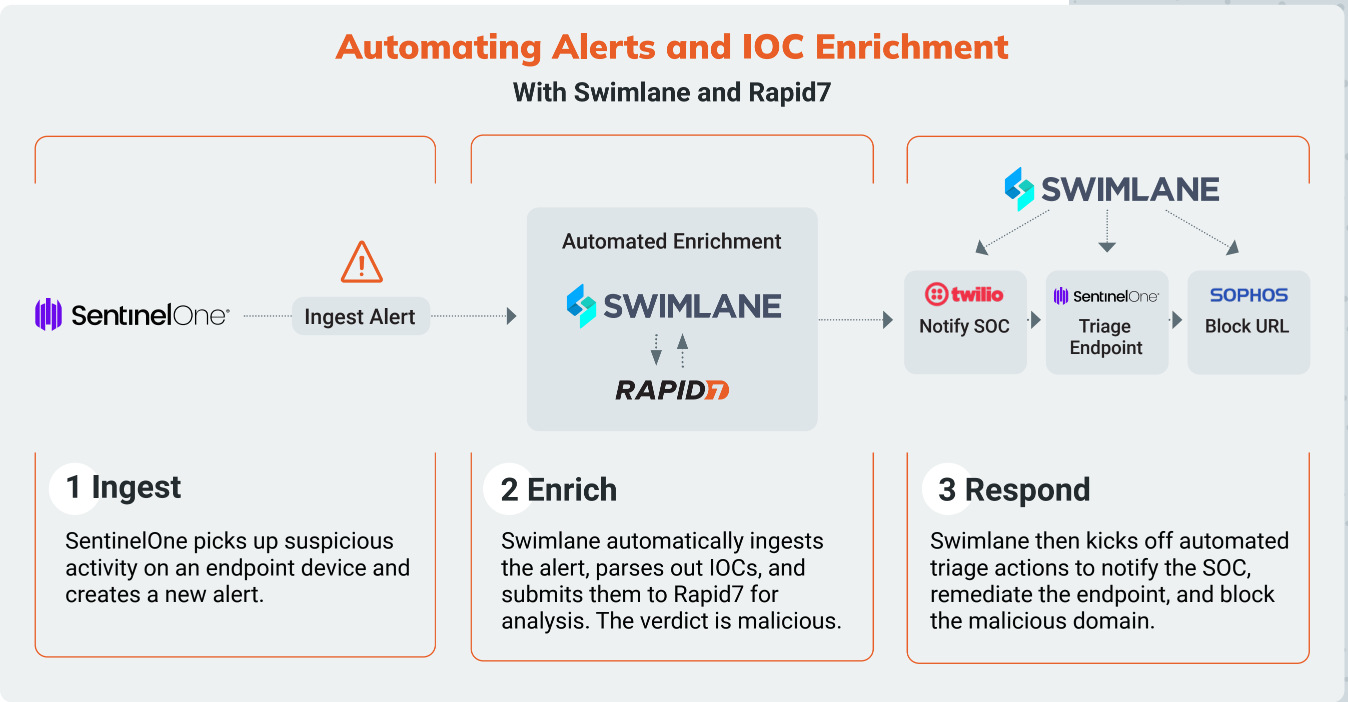
Security teams must leverage more automation. Rapid7 and Swimlane have teamed up to offer mutual customers an integration that can be leveraged for added scale through a highly customizable automation solution. Rapid7 delivers world-class external threat detection and remediation capabilities. Swimlane, a leader in low-code security automation, brings powerful workflows to the table and the ability to easily centralize enrichment results across multiple integrated tools. By combining these tools through this integration, users can enable automated enrichment across new alerts and one central location where results from several tools can be populated before the analyst even lays eyes on the alert.

> **By 2025, "labor volatility" will cause 40 percent of organizations to report a material business loss, forcing a shift in talent strategy from acquisition to resilience.**
>
> Gartner

Customer Benefits

- Speed mean-time-to-respond to new alerts and threats.
- Centralize enrichment and case management to reduce manual work across every alert.
- Add automated responses using Swimlane workflows to speed triage and reduce noise.
- Leverage defined business logic via workflows to remove human error and increase alert accuracy.

How It Works



Automating Alerts and IOC Enrichment

With Swimlane and Rapid7

1 Ingest

SentinelOne picks up suspicious activity on an endpoint device and creates a new alert.

2 Enrich

Swimlane automatically ingests the alert, parses out IOCs, and submits them to Rapid7 for analysis. The verdict is malicious.

3 Respond

Swimlane then kicks off automated triage actions to notify the SOC, remediate the endpoint, and block the malicious domain.

Featured Use Case

Step 1: SentinelOne identifies suspicious activity on a corporate endpoint and generates a new threat for analysts to investigate.

Step 2: The threat is automatically ingested into Swimlane. Once the threat is ingested, Swimlane parses out IOCs.

Step 3: Swimlane then automatically submits each IOC to Threat Command for enrichment.

Step 4: Swimlane kicks off actions based upon the results.

Step 5: Swimlane orchestrates other products to notify the SOC, triage the endpoint, and block the URLs within the firewall.

Integration Features

- Centralized Case Management and result aggregation
- Automated workflows to speed enrichment and response
- World-class threat intelligence data from Rapid7

For more information on this integration, please navigate to the Swimlane website at www.swimlane.com.

Ready to Get Started?

Get a demo today

Better Together

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps overcome process and data fatigue, chronic staffing shortages, and quantifying business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. Learn more at swimlane.com.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**