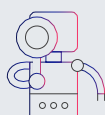


Swimlane and Arcanna.ai

AI-assisted cybersecurity and automation

Benefits



Improve Strategic Decision Making



Time Savings



Faster Response



Improve Accuracy



Seamless Integration

Challenge

The cybersecurity industry is confronted with a multitude of challenges, including an overwhelming influx of threats, alert fatigue, and high turnover rates among professionals. With a projected shortage of 3 million cybersecurity roles by 2030, nearly 70% of cyber professionals attribute enterprise vulnerability to staffing shortages. To make matters worse, many cybersecurity analysts predict that by 2025, over half of significant cyber incidents will result from these shortages and human fatigue. The proliferation of IT tools further exacerbates the issue, as organizations use an average of 40 tools, leading to alert duplication and cumbersome manual workflows. The Security Operations Center (SOC), which is tasked with managing security infrastructure, experiences turnover rates exceeding 50% and struggles to recruit and train new talent efficiently. Addressing these challenges requires a focus on automating routine tasks and leveraging cutting edge technologies such as AI to enhance SOC efficiency and facilitate quicker, higher-quality decision-making.

Solution

By combining Swimlane Turbine, AI-enhanced, low-code security automation platform, with Arcanna.ai's decision intelligence AI platform, we offer an integrated system that unifies security teams, tools, and telemetry, both within and beyond the SOC. This unified platform reduces process and data fatigue, augments human decision-making, and continuously improves through human feedback via a patented learning approach.

Our joint solution ensures quantifiable business value, enhanced security effectiveness, and a seamless evolution toward autonomous decision-making, transforming how security operations are managed and optimized.

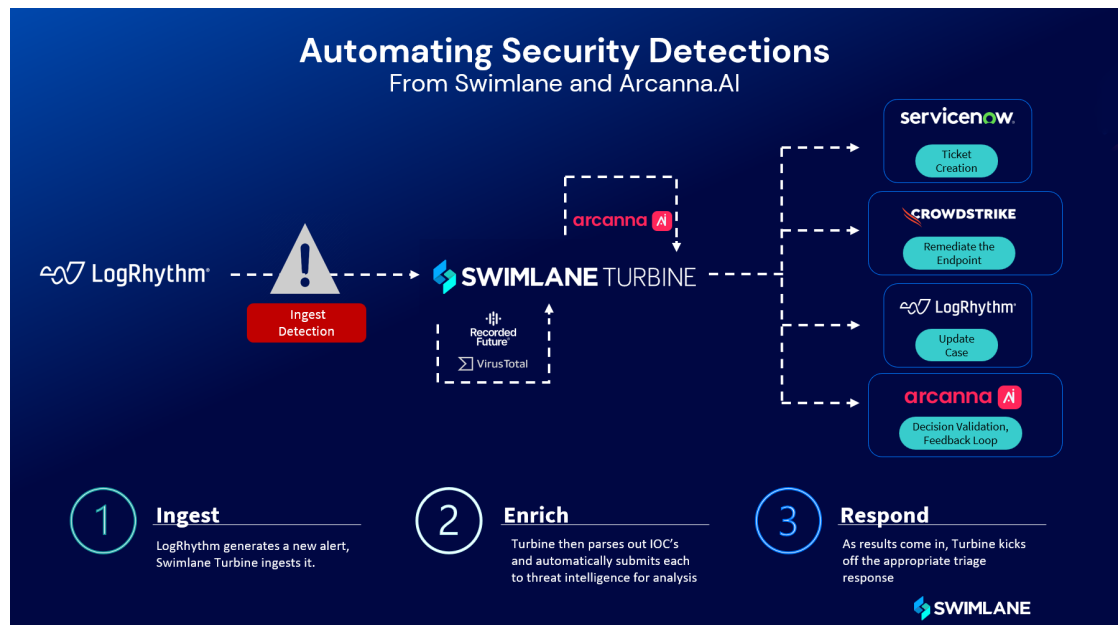
Features

- Swimlane Turbine Hero AI
- Arcanna AI
- Continual AI improvement
- Workflow Management

How It Works

The use case gets started with the endpoint downloading a suspicious file. LogRhythm SIEM creates a new alert containing the file hash. Swimlane Turbine ingests the alert and submits the hash to threat intelligence tools. Results on the hash are pulled back into Turbine, where Arcanna then ingests them for AI analysis. As results come back from Arcanna, the verdict on the file hash is confirmed as malicious. It looks to be malware. Turbine then automatically kicks off 4 actions to begin to triage the threat.

- All of the findings are sent to ServiceNow and a ticket created there
- CrowdStrike is instructed to isolate the endpoint until the hash is removed.
- Turbine then reaches back to LogRhythm to update the case there.
- When the Swimlane case closes in Turbine, it will trigger the Arcanna feedback loop for continual feedback and optimization.



Corporate Headquarters
363 Centennial Pkwy Suite 210
Louisville, CO 80027
1-844-SWIMLANE

Better Together

About Swimlane

Swimlane delivers automation for the entire security organization. Swimlane Turbine is the AI-enabled, low-code security automation platform that unifies security teams, tools, and telemetry in-and-beyond the SOC into a single system of record to reduce process and data fatigue while quantifying business value and ensuring overall security effectiveness. Learn more at swimlane.com

About Arcanna.ai

Arcanna.ai empowers Security Operations Centers (SOCs) with AI-driven decision intelligence. By automating tasks and offering predictive recommendations, it enhances SOC efficiency, reduces analyst fatigue, and fosters an increasingly autonomous SOC for efficient threat detection and response. Additional information is available at <https://www.arcanna.ai>