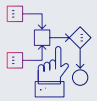


Signal, Speed & Scale for the Modern SOC

Get the best Attack Signal Intelligence and Low-code Security Automation outcomes with Swimlane and Vectra AI

Customer Benefits



70% of SecOps tasks are automated



360-degrees of attack context is available at analysts' fingertips



20x increase in SecOps actionability



Cover >90% of MITRE ATT&CK techniques with integrated signal



80% reduction in alert noise



>50% reduction in MTTD and MTTR

The Challenge

Organizations are struggling to get visibility, accurate attack signals, and easily orchestrate response across their siloed attack surface. Security teams are understaffed and overburdened with contextless alerts and manual processes.

The Solution

The Swimlane Turbine low-code security automation platform and the Vectra AI Platform integrate to deliver the intelligence, efficiency and performance that a modern security operations center (SOC) requires. Together, the platforms provide integrated signal and flexible automation solutions for hybrid environments. With Swimlane and Vectra AI, organizations are able to extend AI-driven security automation beyond the SOC in order to increase cyber resilience and prepare for advanced attacks.

The Vectra AI Platform is the integrated signal powering extended detection and response (XDR) that provides hybrid attack surface coverage across identity, public cloud, SaaS and data center networks while integrating with best-of-breed endpoint solutions. The platform's AI-driven Attack Signal Intelligence prioritizes real attacks in real-time. It arms human intelligence by giving analysts the coverage, clarity, and control they need to investigate and respond at the speed and scale of hybrid attackers.

Swimlane Turbine is a cloud-native low-code security automation platform that combines human and machine intelligence to unify any workflow, telemetry source and team. It is approachable enough for those with no coding experience and sophisticated enough to satisfy the world's most demanding security operations. This enables security teams to extend automation beyond the security operations center (SOC). With Turbine, security teams can now respond to possible threats in real-time without the risk of human mistake.

How it Works

The Vectra AI platform combines data science and machine learning to provide hybrid and multi-cloud threat detection. It leverages AI-driven prioritization to correlate, score and rank incidents by urgency level across public cloud, identity, SaaS and data center networks.

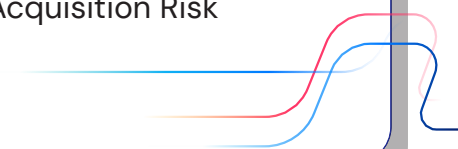
As a result, alert noise in customer environments is reduced by more than 80%. Integrated intelligence automatically associates all malicious behaviors and scores the entity (host and accounts) in terms of its overall risk. Once the Vectra AI platform identifies an infected entity, its IP address and threat certainty are ingested into Turbine over an API-first architecture, which centralizes information from the Vectra AI platform and other systems.

From here, Turbine triggers automated response workflows across the customer's hybrid environment to take action such as notify users, dynamically segment or quarantine the infected device, stop communication with a C&C server or prevent data exfiltration across all device types and network tiers.

Turbine's low-code playbook building experience, modular case management application and human-readable dashboards bring humans-in-to-the-loop of automation. These features help to unify siloed workflows, telemetry sources and teams so that automation can extend beyond foundational SOC use cases.

The Vectra AI and Turbine integration offers a new class of AI-driven defense, replacing manual incident response processes with machine-speed detection and decision making. Together, Vectra AI and Swimlane deliver automated and actionable intelligence to stop threats faster.

Top Use Cases

- Ransomware
 - Insider Threat
 - Supply Chain Attacks
 - Critical Infrastructure Risk
 - OT Environment Risk
 - Merger and Acquisition Risk
- 



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

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 reduce process and data fatigue, overcome chronic staffing shortages, and quantify business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit swimlane.com.

About Vectra AI

Vectra AI is the leader in AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signals across public cloud, SaaS, identity, and data center networks in a single platform. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.