JOINT SOLUTION BRIEF

Elastic Security and Swimlane Turbine Deliver Real-Time Data for Real-Time Security Automation

Reduce the friction highly-distributed security operations teams experience during investigations and threat containment processes

The Challenge

Modern Security Operations Center (SOC) teams are challenged by the volume of data and alerts coming from the disparate detection tools they need to keep their organization safe. This leads to increasingly complex environments and noise, making it difficult to discover what information is most important. When analysts triage a critical alert they will often need to jump back and forth between several different products in order to remediate the host, policy or vulnerability that was found. To make matters worse, many of the alerts analysts triage aren't useful by themselves.

The Solution

Analysts need the ability to quickly connect the dots via logs or intelligence, so that they don't misdiagnosed alerts as benign. When security teams have an automation solution that connects disparate tools they are able to ensure no alert, event, detection, or anomaly gets by without being thoroughly inspected. Swimlane Turbine and Elastic Security work together to deliver a solution that provides real-time data for automated action at the point of inception. Their integrated solutions speeds the mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) by leveraging critical capabilities like the ability to:

- Automate enrichment of detections from Elastic and execute response and remediation
- Ability to add automation to any security playbook or observability use case
- Enhance collaboration by sharing reports, data, even an entire case with other stakeholders'
- Customize playbooks using Turbine's low-code workflow builder

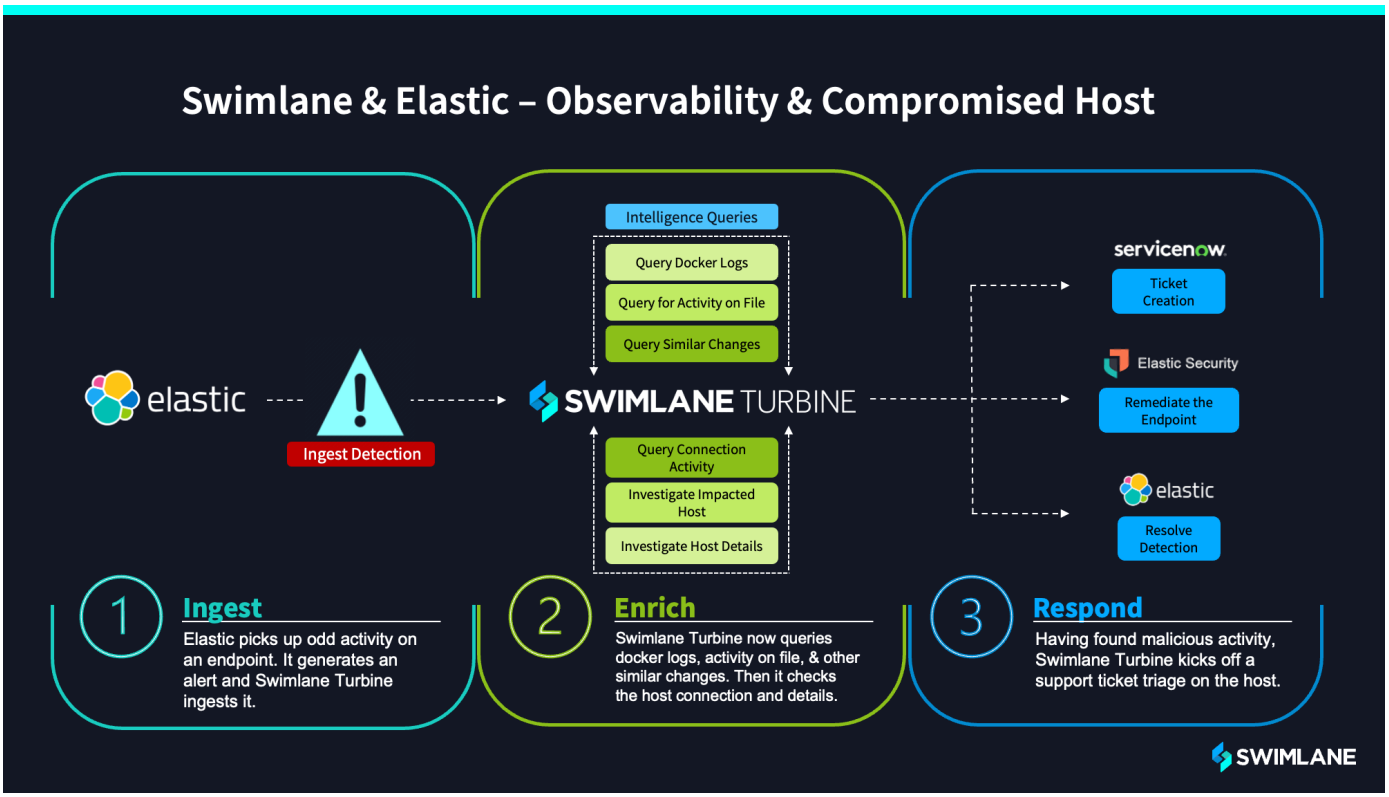
Customer Benefits

- Accelerate MTTD by automatically enriching disparate detection sources
- Speed MTTR with low-code playbooks for automated incident response
- Gain actionable intelligence for stakeholders with reports and case management
- Reduce alert fatigue and burnout for SOC analysts

How It Works

The Swimlane Turbine and Elastic Security integration applies automation to a large percentage of the alerts that SOC analysts would normally need to investigate manually. The integration leverages a push connector so that Turbine is able to ingest Elastic alerts and detections in real time. The Turbine and Elastic connector provides SOC teams with a force multiplier so they can reduce alert fatigue while also responding at machine speed to threats.

Swimlane Turbine and Elastic Security's joint solution also automates observability use cases. Swimlane's low-code methodology makes it easy for analysts to customize workflows and playbooks in order to access centralized data needed for any use case. This capability helps analysts see and work through the entire case management lifecycle and execute any necessary actions based on results or findings from any integrated tool. As a result, analysts find this solution easy to use so they are able to expand their automation use cases beyond the standard SOC use cases. This means that Swimlane and Elastic customers gain the ability to do more than the typical SIEM and SOAR combination can achieve.



Featured Use Case

Step 1: Elastic observes high CPU usage on an endpoint that normally doesn't require this much, alert generated and ingested by Swimlane

Step 2: Swimlane Turbine kicks off enrichment with a query of Docker, an error is noted while reading the file.

Step 3: Run a query for all activity on that file to diagnose the error. We see an unusual change logged 8 hours ago

Step 4: Query for all activity in that timeframe, results show many different files were accessed and/or modified.

Step 5: SwimlaneTurbine kicks off automated enrichment, finding all details it can about the odd host connection.

Step 6: Host is Identified as malicious or compromised, Turbine kicks off automated responses to create a case, pull in appropriate parties for containment or triage, creates an Elastic timeline, and resolves the detection in Elastic.

Integration Features

Bi-Directional Integration
This integration features a push connector that enables bi-directional integration between Swimlane Turbine and Elastic

Centralized Case Management
Swimlane Turbine enables users to connect all of their security tools through integration and webhooks, enabling a centralized case management approach

Collaboration Center
Swimlane Turbine's embedded Collaboration Center leverages automated workflows to foster greater cross-functional alignment and communication

Observability
Elastic offers powerful capabilities around observibility. Its' alerts can be directly ingested into SwimlaneTurbine for threat hunting or insider threat investigations

Real-Time Data & Response
Elastic offers real-time data capabilities within its SIEM and this integration with Swimlane Turbine's extends that real-time data to real-time response via automated workflows

Elastic Timelines
Automate the generation of Elastic Timelines using Swimlane Turbine's automated workflows to capture timing of important events and chronological history

Low-Code Workflow Customization
With Swimlane Turbine's low code workflow builder, it's easy to adapt automated workflows to fit your exact process, even for non-coders. This empowers SOCs to put security first when designing their business logic, rather than attempting to mold it into a rigid pre-made playbook

SWIMLANE

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

Learn more at: swimlane.com

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.

About Elastic

Elastic is a search company built on a free and open heritage. Anyone can use Elastic products and solutions to get started quickly and frictionlessly. Elastic offers three solutions for enterprise search, observability, and security, built on one technology stack that can be deployed anywhere. From finding documents to monitoring infrastructure to hunting for threats, Elastic makes data usable in real time and at scale. Thousands of organizations worldwide, including Cisco, eBay, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia, and Verizon, use Elastic to power mission-critical systems. Founded in 2012, Elastic is a distributed company with Elasticians around the globe and is publicly traded on the NYSE under the symbol ESTC.
Learn more at: elastic.co