SWIMLANE

Swimlane Architecture

1 Swimlane can be deployed as one or more instances on physical hardware, virtual machines and/or cloud-based IaaS platforms. It scales vertically and horizontally, with full HA and DR capabilities.

2 Swimlane's web tier can be load balanced or distributed across a content delivery network (CDN) to maximize front end performance and availability.

3 Swimlane's backend database infrastructure is built on a combination of NoSQL and Graph components. NoSQL leverages sharding for scalability and replica sets to allow for HA and DR deployments. Graph DB components use clustering for scalability, HA and DR.

4 Task Engines manage integrations, data ingestion, and data enrichment. Additional Task Engines can be easily and rapidly deployed to support added scalability.

5 Swimlane integrates with internal infrastructure to gather relevant user, hosts, and network information, as well as security solutions to update rules, gather alarms, generate tickets and notify analysts.

6 Swimlane can leverage cloud-based services such as threat intelligence, whois, malware detonation and other cloud-based or SaaS services.

Swimlane has helped numerous government CIOs, CISOs, SOC managers and security analysts rapidly identify and respond to cyber threats to agencies and citizens using intelligent SOAR solutions.

Ask us how we can do the same for your agency or department

Automatically identify and respond to emerging cyber threats to government agencies.

Security Orchestration, Automation and Response (SOAR) Platform

Swimlane's architecture meets the stringent requirements of the U.S. Federal Government and its security operations centers. It is designed for the maximum deployment flexibility and resiliency that government agencies need to keep security operations performing to meet mission requirements. Swimlane supports granular multitenancy, and full high availability (HA) and disaster recovery (DR).