LOGPOINT

SWIMLANE

SOLUTION BRIEF

Swimlane and LogPoint

Automate alert handling to accelerate incident detection and response

WHY WE WORK BETTER TOGETHER

LogPoint and Swimlane help security staff respond to and resolve incidents faster. Our combined solution reduces the number of alerts that security and IT staff need to analyze, leaving more time to respond to the most critical matters. We help businesses reduce costs thanks to the automation of alerts and incident handling.

BUSINESS CHALLENGE

Alert triage is traditionally a manual process. When faced with a high volume of alerts, security analysts are bound to make mistakes and suffer from alert fatigue. Security operations centers (SOCs) are also under pressure to comply with a growing number of legal and regulatory requirements.

With limited security budgets, SOCs need a way to automate the alert handling process to respond quickly to incidents.

BENEFITS

- Quicker response time thanks to automated alert handling
- Reduced alert fatigue
- Lower costs by reducing the number of manual tasks needed to investigate and respond
- Easy to use with one central interface to control the entire alert handling process

SOLUTION AT A GLANCE

Collects and correlates data from devices across the organization

Detects potential security incidents and automatically triggers alerts

Identifies and eliminates false positives, while escalating valid threats

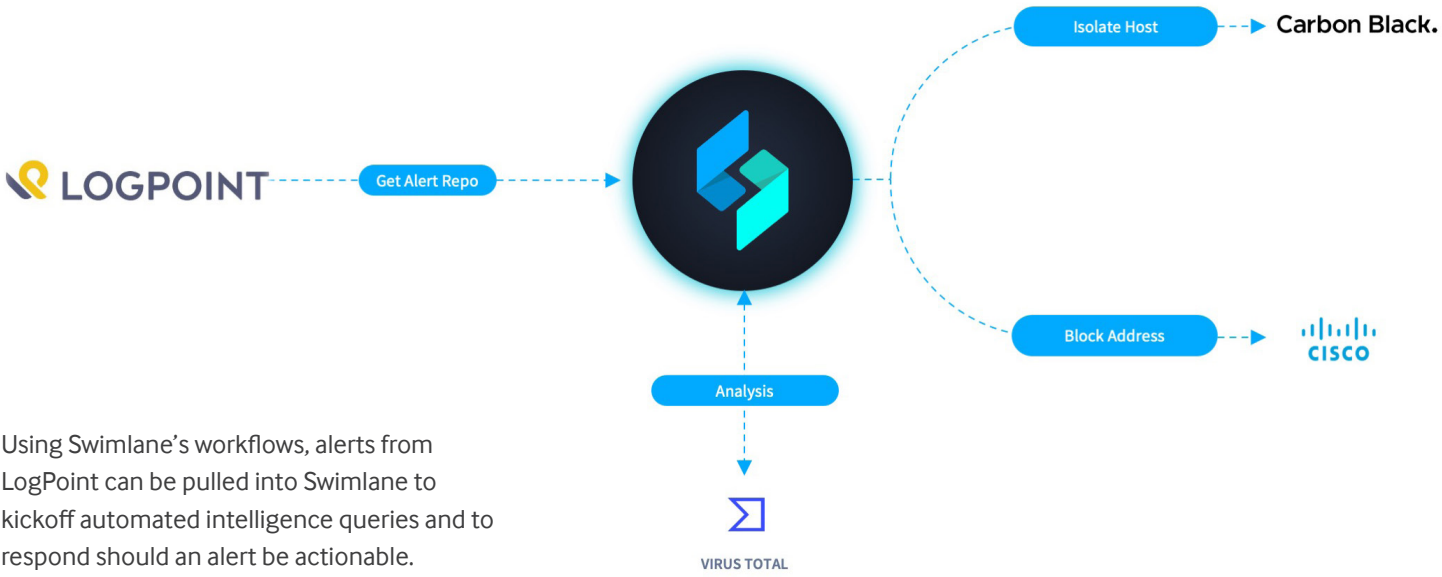
Automatically responds to alerts and takes remediation steps when needed

SOLUTION OVERVIEW

LogPoint is a modern security information and event management (SIEM) solution that collects and analyzes event data from any device or application within your infrastructure. LogPoint automatically identifies and sends alerts about any critical incidents or abnormalities in your system.

Swimlane is layered on top to manage the incident response process to each alert, automating and orchestrating the mundane and repetitive tasks which would otherwise take hours to complete. This allows users to take back the time they would otherwise spend on repetitive tasks and enables them to work on more pressing or complex issues. Additionally, the automation capabilities within the Swimlane platform mean a faster mean time to resolution (MTTR) and a much greater ability to respond to threats at machine speeds.

HOW IT WORKS



Using Swimlane's workflows, alerts from LogPoint can be pulled into Swimlane to kickoff automated intelligence queries and to respond should an alert be actionable.

BETTER TOGETHER

About LogPoint

LogPoint is committed to creating the best SIEM in the world. We enable organizations to convert data into actionable intelligence: supporting cybersecurity, compliance, IT operations, and business analytics.

About Swimlane

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market and was founded to deliver scalable security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages.