LOGPOINT

LogPoint and Swimlane solution brief

Automate alert handling to accelerate incident detection and response

Accelerate threat detection and response with LogPoint SIEM

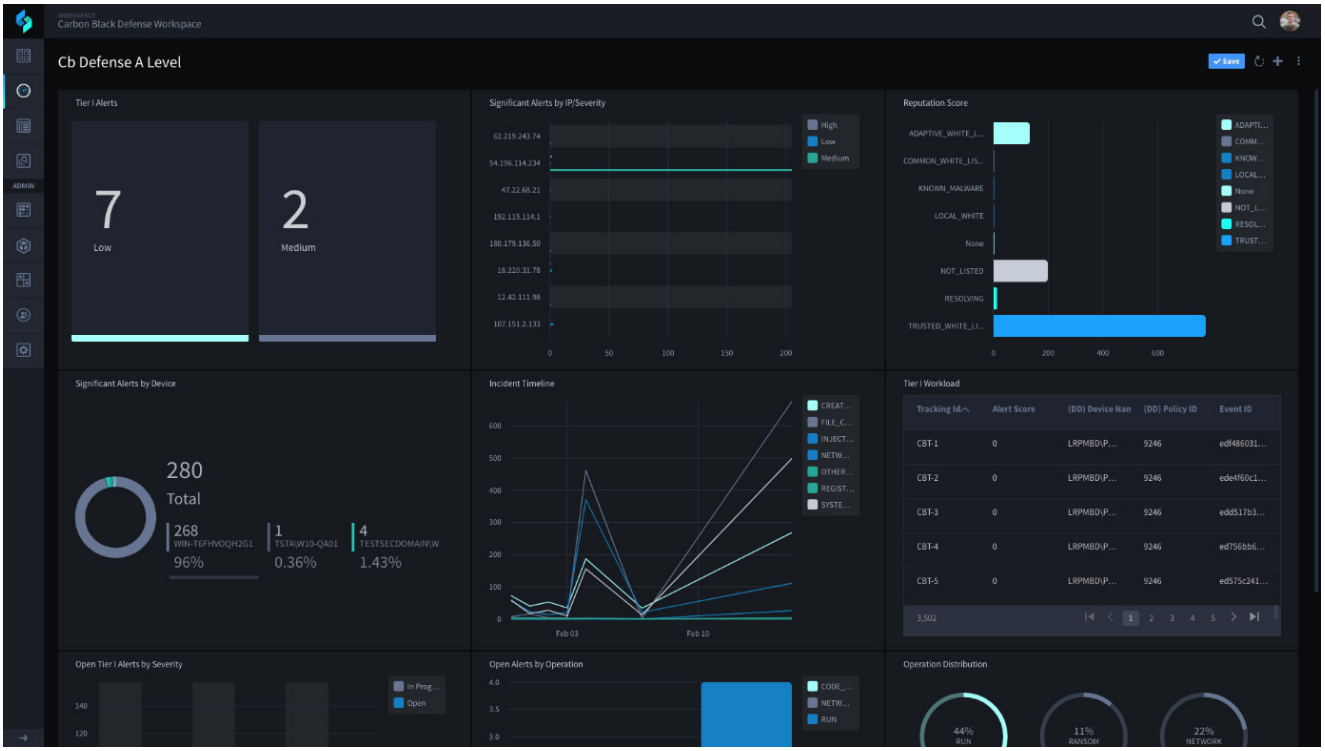
LogPoint collects, stores, and analyzes log data from your entire IT infrastructure to detect suspicious activities and respond to threats. LogPoint is a security information and event management (SIEM) solution that gives a complete view of the threat landscape by automatically identifying and sending alerts about any critical incidents or abnormalities in your system.

Automate incident response with machine-speed decision making

Swimlane is a security, automation, orchestration, and response (SOAR) that can be configured to automatically perform time-consuming security tasks, including responding to threats. Swimlane cuts down response time from hours to seconds. It executes incident response tasks allowing highly skilled security analysts to leverage their expertise better.

Helping 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. Security teams get lowered costs, reduced workload, and increased efficiency. Integrating LogPoint with Swimlane makes it possible to automate and orchestrate mundane and repetitive tasks, resulting in a faster mean time to resolution.

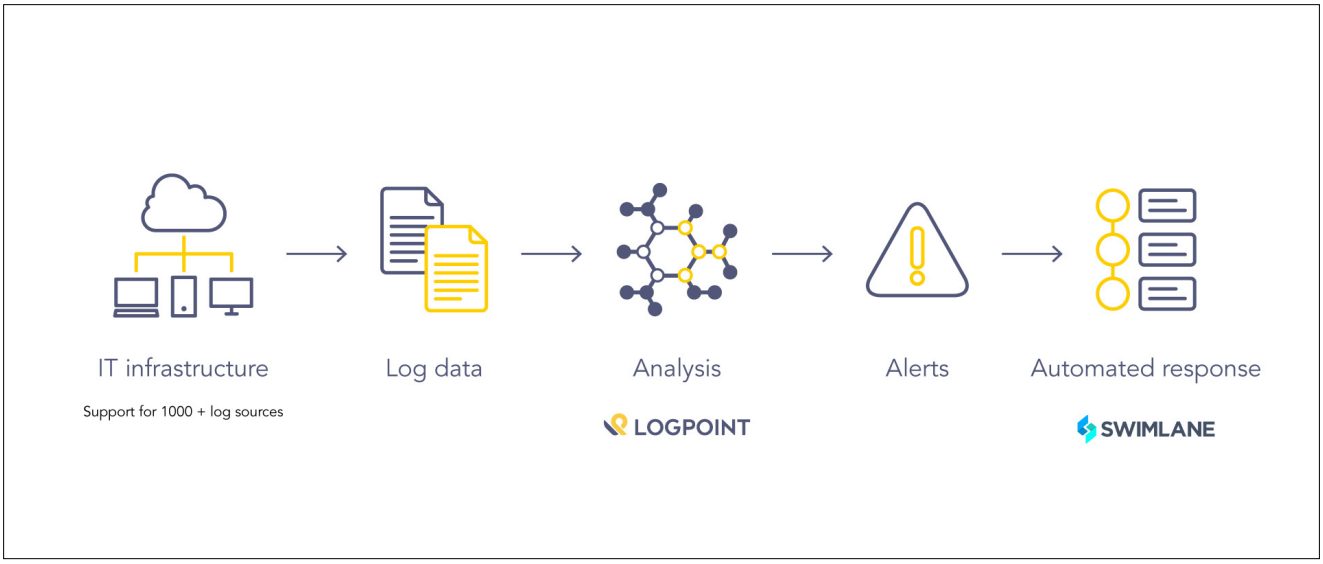


Lower costs and reduce alert fatigue

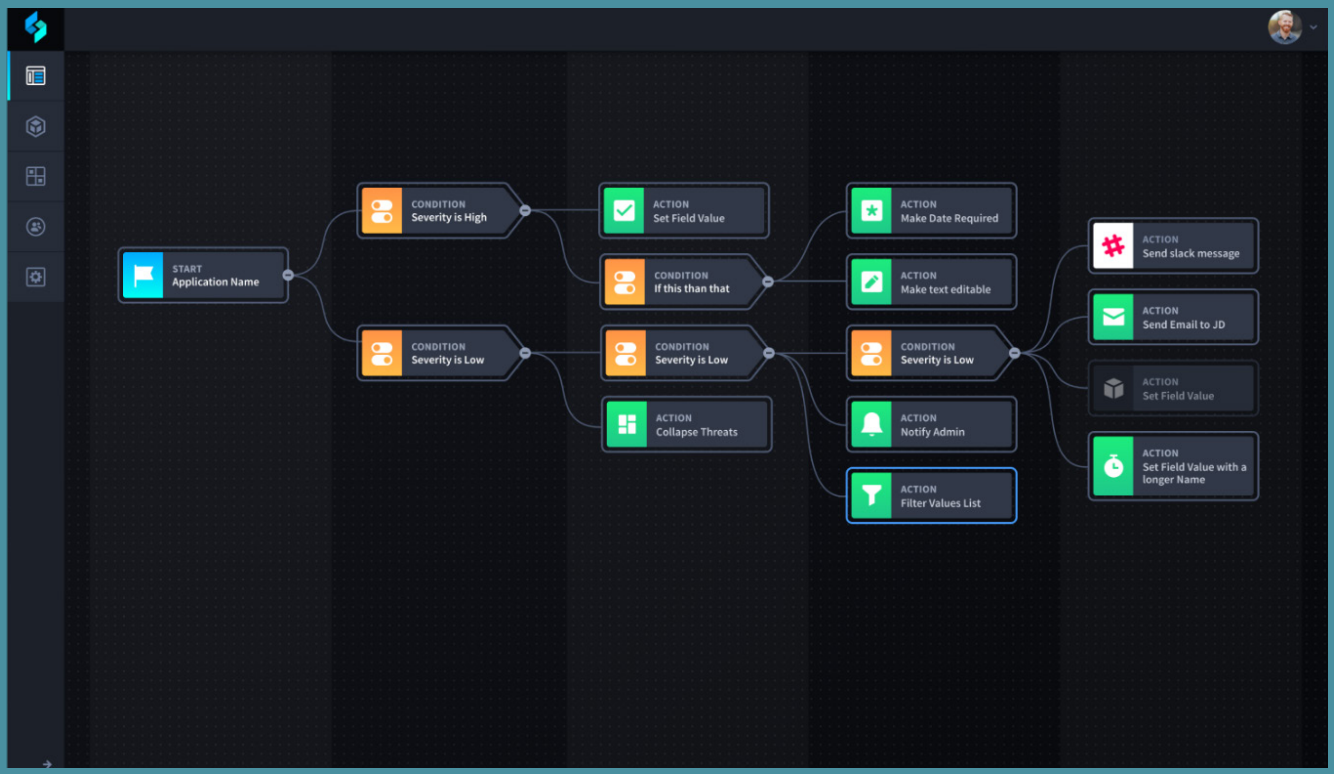
Responding to threats is traditionally a manual process. However, manual investigation of possible security incidents leads to overwhelmed security analysts and wastes time and money. When faced with a high volume of alerts, security analysts are bound to make mistakes and suffer from alert fatigue. With limited security budgets, security teams need to automate the alert handling process to respond quickly to incidents.

How it works

LogPoint collects and correlates data from devices across the organization. LogPoint detects potential security incidents, automatically triggers alerts, and prioritizes alerts based on risk. Swimlane automatically responds to alerts and initiates remediation steps when needed.



Using workflows, Swimlane pulls alerts from LogPoint to kick off automated threat responses.



Key benefits

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

About LogPoint

LogPoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value. Our advanced next-gen SIEM, UEBA and Automation and Incident Response solutions, simple licensing model, and market-leading support organization empower our customers to build, manage and effectively transform their businesses.

We provide cybersecurity automation and analytics that create contextual awareness to support security, compliance, operations, and business decisions. Our offices are located throughout Europe and in North America. Our passionate employees throughout the world are achieving outstanding results through consistent customer value-creation and process excellence. With more than 50 certified partners, we are committed to ensuring our deployments exceed expectations.

Contact LogPoint

If you have any questions or want to learn more about LogPoint and our next-gen SIEM solution, don't hesitate to contact us at www.logpoint.com/en/contact/

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.

SWIMLANE

Swimlane is a market-leading SOAR platform. Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations.