SOLUTION BRIEF

Swimlane and Stellar Cyber

Together, we deliver an integrated automated detection and response platform across the entire IT infrastructure

WHY WE WORK BETTER TOGETHER

- The foundation for the next generation intelligent SOC is built on the promise of consolidation, automation and simplification to enable customers to radically improve the efficiency of their security operations and dramatically reduce both detection and response time.
- The joint solution through this partnership between Stellar Cyber and Swimlane delivers a seamless integration by feeding high-fidelity detections from the eXtended Detection and Response (XDR) security platform to Swimlane's security orchestration, automation and response (SOAR) platform.
- Powerful, yet easy-to-build playbooks leverage high-fidelity detections improving the SOC's efficacy and efficiencies.

BUSINESS CHALLENGE

Today, cyber security experts have a wealth of products at their fingertips, but all of these products are not created equal. There are many tools out there that are great for detecting anomalous activity, but these tools often require additional monitoring and investigation with all the alerts they produce. To add to this, many of these products are siloed, or disconnected from one another, making the investigation of each alert even more time intensive. This can lead security teams to fall behind or even to miss alerts as they don't have enough time to investigate them all fully.

Building visibility across cloud, endpoints, users, applications and the network is challenging with these silos and often means pulling together all the available tools or data feeds to be normalized for correlations. This can be an extremely manual task and is time-intensive for analysts. Even still, additional visibility challenges exist, including bridging virtual or containerized environments as well as remote workers and/or remote assets. Data now becomes fragmented and redundant, which add another layer to the SOC analysis inefficiencies. AI promises to improve the ability to piece together complex attacks and reduce alert fatigue, but there is more that can be done through integration and automation.

SOLUTION AT A GLANCE

Workflows or playbooks make ingestion and enrichment less time intensive

Open XDR has 20+ natively supported applications and finds detections you do not see with tools you already trust

Swimlane delivers a single, centralized response platform

Remove product silos with Swimlane's 270+ integrations

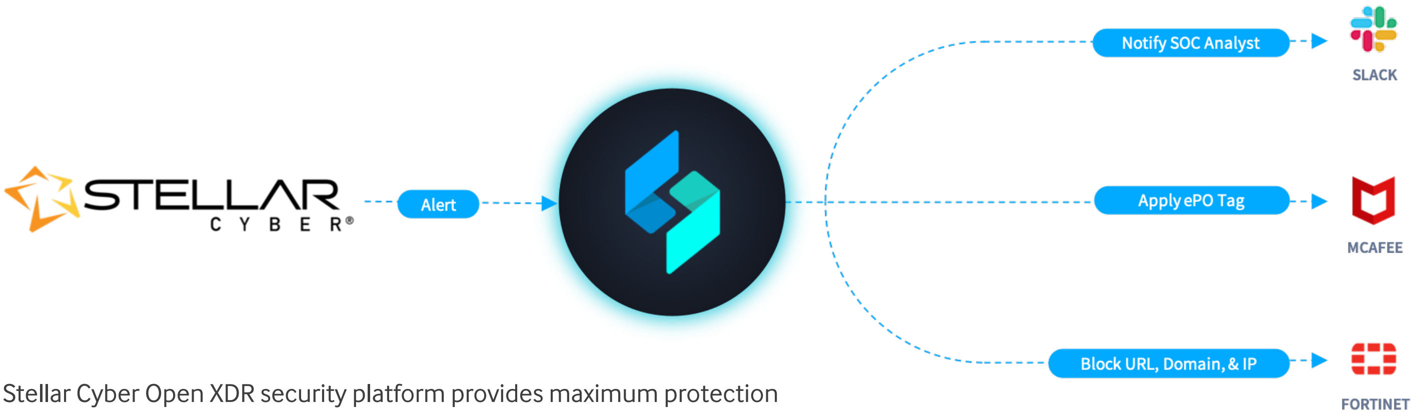
BENEFITS

- Quickly respond to high-fidelity detections across the entire kill chain, improving ROI.
- Stellar Cyber delivers pervasive visibility across cloud, SaaS, endpoint, users, applications and networks.
- Incorporating higher quality detections with Swimlane's SOAR improves mean-time-to-respond metrics.

SOLUTION OVERVIEW

This integration offers solutions to many of the challenges facing security teams today. With a single centralized platform for managing all of your integrated products, Swimlane helps to tear down silos and provides greater visibility across your security stack. Stellar Cyber's XDR platform provides a wealth of context around its alerts and allows you to ingest all of these details into Swimlane. Once ingested, Swimlane can then launch workflows to check on indicators and events with other intelligence tools in your network to correlate the findings into one actionable score. If the alert is found to be malicious or appears to be a true attacker, playbooks or customized workflows can be initiated to begin triage procedures and any additional escalations. This empowers teams to respond at machine speed when needed and connects previously siloed products, adding to visibility and preventing data redundancy.

HOW IT WORKS



Stellar Cyber Open XDR security platform provides maximum protection and improved analyst productivity by piecing together attacks from across the entire IT infrastructure while Swimlane integrates your people, processes, and technology for optimal response and remediation.

BETTER TOGETHER

About Swimlane
Swimlane is at the forefront of the growing market of security orchestration, automation and response (SOAR) solutions and was founded to deliver scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane's solution helps organizations address all security operations (SecOps) needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats — improving performance across the entire organization. Swimlane is headquartered in Denver, Colorado, with operations throughout North America and Europe. For more information, visit www.swimlane.com.

About Stellar Cyber
Stellar Cyber is the only cohesive security operations platform that provides maximum protection and improved analyst productivity by piecing together attacks from across the entire IT infrastructure. www.stellarcyber.ai