CrowdStrike Technology Partners

SWIMLANE

CROWDSTRIKE

Solution Brief

CROWDSTRIKE AND SWIMLANE INTEGRATION: EDR AND SOAR

Enabling collaboration between security and IT teams to reduce mean time to repair (MTTR)

CHALLENGE

Organizational silos, tailored response processes and continuous monitoring of endpoint indicators are important factors in securing and managing endpoints. In addition, collaboration between security and IT operations is crucial, especially when a critical incident occurs. Utilizing the power of the Swimlane Security, Orchestration, Automation and Response (SOAR) platform along with the CrowdStrike Falcon® platform endpoint detection and response (EDR) capabilities can help overcome these challenges by enabling machine-speed responses to any Falcon threat detection, custom alert or internal request for assistance.

SOLUTION

The joint integration of the Crowdstrike® Falcon and the Swimlane SOAR platforms boosts enterprises' response capabilities in three unique use cases. In addition to allowing companies to investigate, interact and enforce response and remediation directly with the endpoint at machine-speed, the combined solution also improves collaboration across teams and allows for better tracking of incidents, indicators and responses in disparate tools. Additionally, this allows security teams to gain insights into how they can reduce mean time to repair (MTTR) and the resources required when an incident occurs. Whether you encounter a detected, custom or internal alert, the combination of Swimlane and CrowdStrike will enable your security team to SOAR beyond endpoint security.

KEY BENEFITS

- Improve collaboration and response processes across teams
- Reduce MTTR and resources required when an incident occurs
- Investigate, interact and enforce response and remediation directly with the endpoint at machine-speed
- Ingest indicators from CrowdStrike for use within or to trigger an automated workflow

CROWDSTRIKE AND SWIMLANE INTEGRATION

BUSINESS VALUE

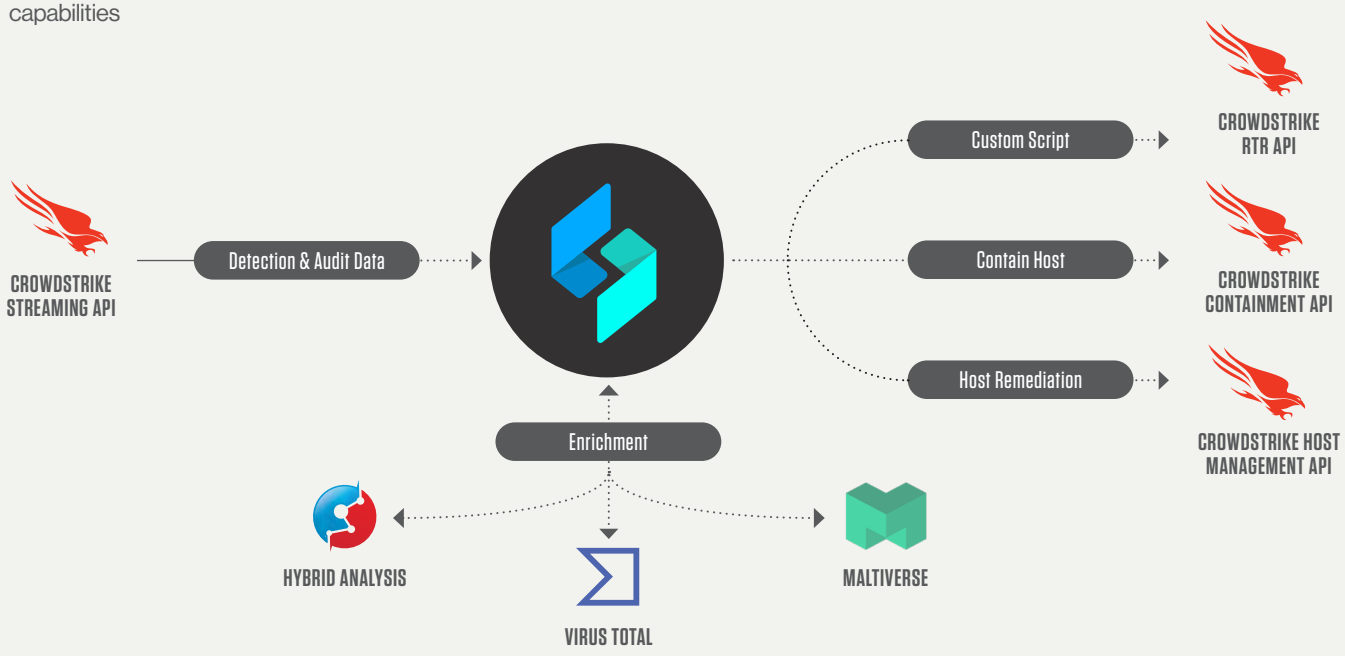
Use Case / Challenge	Solution	Benefit
Centralized Intelligence and Enrichment: When a security team gets an alert or an indicator, more context is often needed to decide on the next steps. This can lead to a team having to pivot across several different tools to find additional intelligence and enrichment. The result is an inefficient process and limited visibility between multiple tools.	This integration allows analysts and security teams to pull relevant details into Swimlane from CrowdStrike and other tools in their security stacks. This data can be centralized within the Swimlane platform for a more comprehensive view.	When all of this information is available in a single product, it becomes much easier for security teams to find the information they need and better understand the results for each investigation.
Automation: Today's cybersecurity teams often struggle to keep up with all of the alerts coming from their various tools, resulting in alert fatigue. Separating the alerts that need action from harmless alerts takes time, which can jeopardize a fast and accurate response to true threats.	When integrated with the CrowdStrike Falcon platform, Swimlane's automated workflows perform repetitive tasks such as intelligence gathering, enrichment and even remediation without needing an analyst's input. Workflows can be configured to automatically trigger these processes as soon as an alert comes in, ensuring a better response to incidents.	When automated workflows are utilized, security teams benefit from a significant reduction in time spent gathering the proper intelligence across each alert. This means analysts can spend more time on the alerts that really matter.

TECHNICAL SOLUTION

This integration was created to allow Swimlane to ingest indicators and intelligence from the CrowdStrike Falcon platform, powered by the CrowdStrike Security Cloud and world-class AI, so they can be utilized as part of a playbook or workflow. This integrated solution is capable of over 23 different actions that can all be configured in an automated or semi-automated fashion depending on the use case. For this integration to work, users will need a Swimlane license and a CrowdStrike Falcon Query API ID and API Key.

The CrowdStrike and Swimlane integration — how it works:

- Ingests alerts, indicators and intelligence
- Automates and optimizes security operations
- Implements superior protection through enhanced endpoint detection and response (EDR) and threat intelligence capabilities



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 CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**