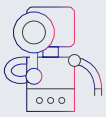
JOINT SOLUTION BRIEF

Swimlane and CYFIRMA – Combine Real-time External Threat Visibility with Rapid Response to Combat Threat Actors at Scale

Benefits



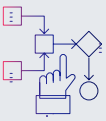
Enhanced Threat Detection

Contextualized Incident Analysis

Accelerated Incident Response

Proactive Threat Mitigation

Enriched Threat Intelligence Sharing



Tailored Workflows and Playbooks

Challenge

The constantly changing tactics, techniques, and procedures (TTPs) of threat actors make it challenging to stay ahead of emerging risks and vulnerabilities. Advanced Persistent Threat (APT) groups with sophisticated tools and techniques pose a significant challenge, as they often remain undetected for extended periods, causing severe damage before discovery. State-sponsored attacks and industrial espionage require deep analysis and understanding of geopolitical context to accurately assess potential threats. Security teams are swamped with alerts, making it tough for them to react quickly. Organizations face risks through vulnerabilities in third-party vendors and partners, which can be exploited by attackers to gain unauthorized access.

Solution

DeCYFIR threat intelligence models empower businesses to make informed decisions on threats and prioritize remediation activities DeCYFIR helps organizations uncover potential attack surfaces, deliver vulnerability and brand intelligence, monitor for digital risk, provide situational awareness and cyber-intelligence, all at scale, and at the speed of AI.

Swimlane Turbine is a AI-enabled, low-code security automation platform that combines human and machine intelligence to unify any workflow, telemetry source and team. It is approachable enough for those with no coding experience and sophisticated enough to satisfy the world's most demanding security operations. With Turbine, security teams can now respond to possible threats in real-time without the risk of human mistake.

The integration of DeCYFIR Threat Intelligence with the Swimlane Turbine low-code security automation platform enhances the capability of security teams to be alerted and proactively monitor, identify, assess, and respond to cyber threats. Swimlane Turbine ingests and enriches DeCYFIR real-time, context-rich threat intelligence data. This integration represents a critical step towards bolstering cyber defense mechanisms and maintaining a resilient security posture in an ever-evolving threat landscape.

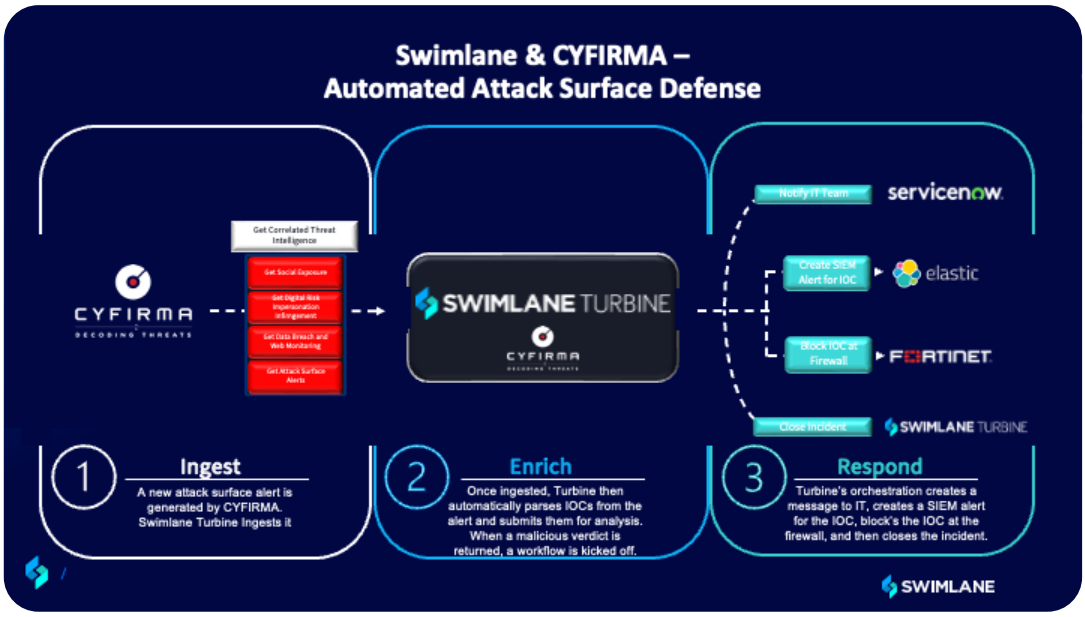
Integration Features

- Proactive Alerting
- Incident Correlation
- OCSF Conversion
- Adaptable Low-Code Workflows

How It Works

The combined Swimlane and CYFIRMA offering provides many use cases including identifying digital risk, vulnerabilities, and data exposures. The following illustrates one use case on how the solution identifies and mitigates the risk of a potential attack surface.

The Swimlane Turbine integrations with CYFIRMA uses an API integration to ingest alerts, leveraging CYFIRMA's correlated intelligence across the 7 pillars of threat intelligence. Once ingested, Swimlane Turbine is able to call upon other connected tools to provide enrichment around the information CYFIRMA has surfaced. As results come back from those tools, Turbine will take appropriate automated actions to triage the threat and keep users' attack surface as protected as possible.



SWIMLANE

Corporate Headquarters
363 Centennial Pkwy Suite 210
Louisville, CO 80027
1-844-SWIMLANE

Better Together

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps overcome process and data fatigue, chronic staffing shortages, and quantifying business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. Learn more at swimlane.com

About CYFIRMA

CYFIRMA combines cyber-intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. We have built the next generation of AI-powered threat intelligence platform called External Threat Landscape Management (ETLM) to provide cyber defenders with the hacker's view to help clients prepare for impending attacks. CYFIRMA is headquartered in Singapore with offices in Japan, India, the US, and the EU. Learn more at cyfirma.com