IRONSCALES
THE POWER OF NOW

SWIMLANE

SOLUTION BRIEF

Swimlane and IRONSCALES

Together, we provide a faster approach to manage increasing threats and accelerate response.

WHY WE WORK TOGETHER

SOC teams are continuously looking to get a full view across their security stack in a single dashboard; this has become more and more of a priority as security tool proliferation has added many new tools to environments that must be monitored. Many of these tools provide alerts when they pick up malicious or anomalous activity and that means security teams have had more and more to investigate. With only so much time in the day and security professionals being in high demand, the current manual process for building a case or implementing remediation seem unsustainable without more help.

Swimlane and IRONSCALES have teamed up to take this problem on and have created an integration together that addresses many of these issues. Through this integration, incident alerts, statistics and details can automatically be ingested directly into the Swimlane dashboard, providing analysts with the ability to change classification of the incident right from within the dashboard. This intelligence can then be combined with additional enrichment from other integrated security tools to provide a single dashboard for full visibility of their alerts and events. From there, users will have options for automated or single click remediation at their fingertips.

CHALLENGE

An average Security Operations Center can have over 80 tools from 40 vendors. Between alert overload, complex security stacks and a lack of skilled personnel – it is harder for them to keep up with the increased threats. To add to these issues, many of these tools across the security stack are disconnected or siloed from other tools. This makes it difficult for analysts to see the larger picture and connect disparate pieces of evidence coming in across multiple tools. All of these challenges also work against security teams by adding to the amount of time it takes to resolve or remediate an alert.

SOLUTION AT A GLANCE

- Simplify remediation of incidents using automation
- Add efficiency for Security Analysts by reducing alert fatigue
- Enable easy correlation and classification of incidents
- Centralized Case Management

JOINT SOLUTION BENEFITS

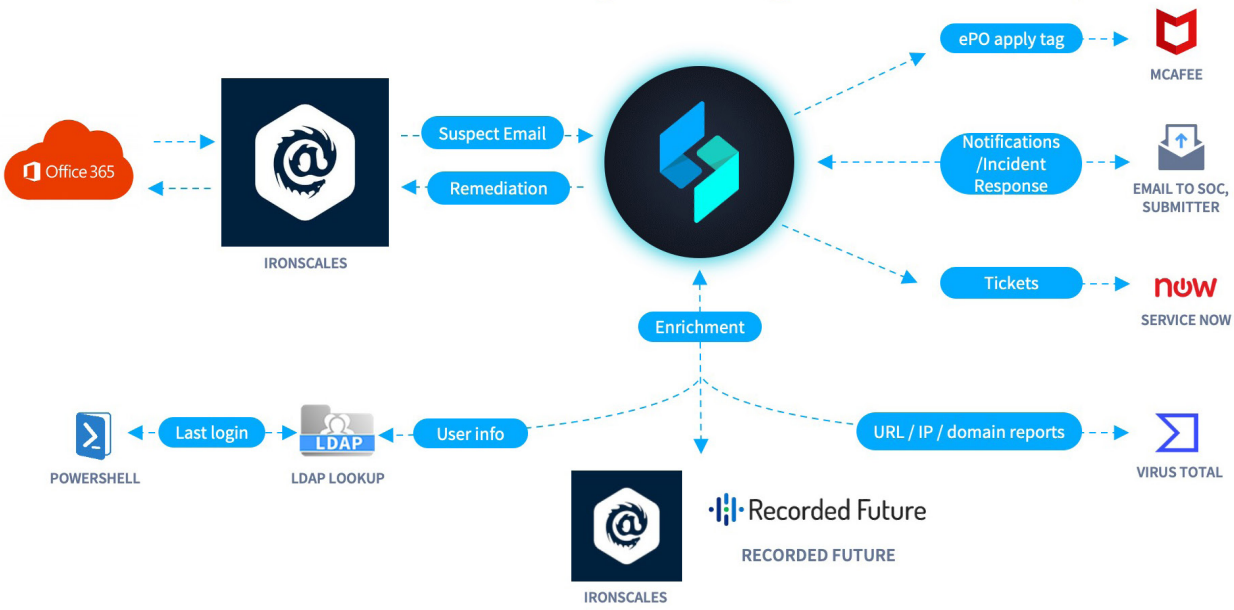
- Respond and triage incidents at machine speed with automated workflows
- Unifies view of alerts for easy management and incident correlation
- Decreases human inaccuracies of transposing data across tools
- Automation frees up time for more proactive threat hunting

SOLUTION OVERVIEW

IRONSCALES provides a self-learning email security platform that operates at the mailbox level and has visibility into many different data points within a company's email and messaging capabilities. This visibility, and the enrichment that comes with it, are items that can be ingested into Swimlane through this integration. That, in turn, provides users with a centralized view of all alerts and incidents they have pulled in from across their integrated tools making it easier to spot connected events. This enrichment also enables analysts to make decisions with a single click or to trigger automated workflows for automated remediation.

With this integration, Swimlane and IRONSCALES provide a better way for the SOC team to manage increasing threats and accelerate response, especially as it applies to managed email, phishing alerts, and incident response.

HOW IT WORKS



BETTER TOGETHER

About IRONSCALES

IRONSCALES offers security professionals and end users an AI-driven, self-learning email security platform that provides a comprehensive solution to stop tomorrow's phishing attacks today.

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.