SOLUTION BRIEF

Incident Response with Swimlane and Zscaler

AUTOMATED THREAT HUNTING

Most organizations today are not able to proactively identify and hunt for threats. They are stymied by lack of resources and manual processes that limit hunting frequency. Manually collecting artifacts from various point systems, sifting through logs or performing network packet captures isn't scalable in today's threat environment, where it is no longer enough to be passively vigilant.

Swimlane's integration with Zscaler gives analysts a centralized view into an organization's inbound and outbound traffic and allows the analyst to look at Zscaler artifacts, capture suspicious indicators and perform reputation checks or lookups all with a single click. This reduces the number of manual steps and time that an analyst would require to identify and hunt for threats. Once Zscaler deems an IOC as malicious, Swimlane can automatically have Zscaler enforce a block policy from within its UI, without requiring the analyst to log into multiple systems or switch screens.

INCIDENT TRIAGE, ENRICHMENT AND RESPONSE

Analysts are finding it difficult to act on the increasing volume of alerts and incidents. Incident response tasks involving identification, triage, and response actions involve switching between multiple screens, mundane and repeatable tasks, and lost time dealing with false positives.

Analysts can streamline security operations workflows by using Zscaler actions within Swimlane's playbooks. Swimlane can retrieve malware analysis results and indicator reputation, extracting wider context without the need for screen switching and manual repetition. For example, a Swimlane playbook can ingest an alert from a SIEM, extract a hash file and perform a reputation check for the hashes. If malicious hashes are found, Swimlane can call Zscaler to get a sandbox report which can then be used for further analyst investigation or playbook actions.

INTEGRATION FEATURES

Execute Zscaler actions – such as reputation checks, look ups and addition and deletion of indicators from custom blacklists for real-time enforcement across all users and devices within Swimlane's workflow tasks.

Leverage Zscaler's malware analysis and sandbox reputation results within Swimlane, either as an automated playbook task or as a stand-alone task.

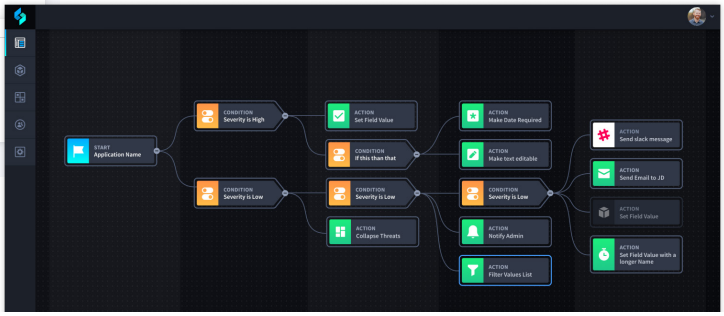
Leverage Swimlane's platform integrations to further enrich Zscaler data and coordinate response across various security endpoints.

BENEFITS

- Use Swimlane playbooks to orchestrate actions against web-proxy, next-generation firewall, and sandbox malware analysis
- Collect and centralize relevant forensic data for effective investigations and fast resolution
- Shorten security operations workflows by automating manual tasks and provide deep visibility into operational KPIs

INTEGRATION

The integration with Zscaler allows the analyst to keep on top of threats by performing security actions that go across Zscaler's access control, SSL inspection, advanced threat protection and data protection capabilities all from within Swimlane's UI. Playbooks automate a host of actions across products so that analysts have a wealth of information at their fingertips when starting an incident investigation. Conditional tasks within playbooks can help reduce false positives and ensure that analysts investigate incidents that have been confirmed as malicious.



BETTER TOGETHER

About Zscaler Security

Zscaler Internet Access (ZIA) delivers your security stack as a service from the cloud, eliminating the cost and complexity of traditional appliances. Zscaler operates over 100 datacenters worldwide to connect users to the closest gateway for faster access. Organizations can scale protection to all users regardless of location, without the need to add new appliances. ZIA sits between your users and the Internet giving unprecedented visibility to every byte, including SSL encrypted traffic which is inspected inline. Zscaler is a security cloud platform offering Cloud Sandboxing, Next-Generation Cloud Firewall, Data Loss Prevention (DLP), and Cloud Application Visibility and Control.

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.