SWIMLANE

mimecast

JOINT SOLUTION BRIEF

Mimecast and Swimlane

Coordinated, Automated and Efficient Incident Response

The Security Challenge: Effective and Timeous Response Across Multiple Tools

IT environments today stretch far and wide - adoption of mobile devices and cloud services has signalled the shift from perimeter security. With the next era of cloud adoption and the current work from home population (WFH), the attack surface of all these new applications has vastly increased. Because this IT expansion happened over time, organizations addressed cybersecurity as new trends emerged and evolved which ultimately left them burdened with a collection of disjointed architectures and siloed components leading to complexity, technical debt, blind spots, and time-sensitive security events not being met, which adds additional load upon an already overworked Security Operations (SecOps) team.

A typical organization will employ somewhere between 10 and 45 different security tools, and a single incident requires coordination across an average of 19 of them. The deployed security tools will create approximately 17,000 alerts each week, to which SecOps teams have to react. From the alerts generated, approximately 16% are considered reliable, however; investigating this huge volume of false positives can take up to 21,000 hours per year. The low-level security tasks needed to investigate each alert are too tedious and numerous to be handled by human beings.

When responding to email threats, time is of the essence as these attacks usually target multiple users simultaneously across the organization, often leading to multiple points of infiltration by the attacker. In addition, email attacks can generate a lot of alerts that have to be sifted through manually to determine malicious intent. These tasks, while essential to incident response, are repetitive and time-consuming, causing alert fatigue and taking analysts away from actual problem-solving.

Key Benefits

- Save time by using Swimlane Turbine to automate email security processes, shorten decision making cycles, and drive resource efficiency through automation
- Gain actionable insights with enriched intelligence from Mimecast and other security tools for coordinated response
- Accelerate your mean-time-to-resolution with full orchestration capabilities using proactive playbooks and workflows

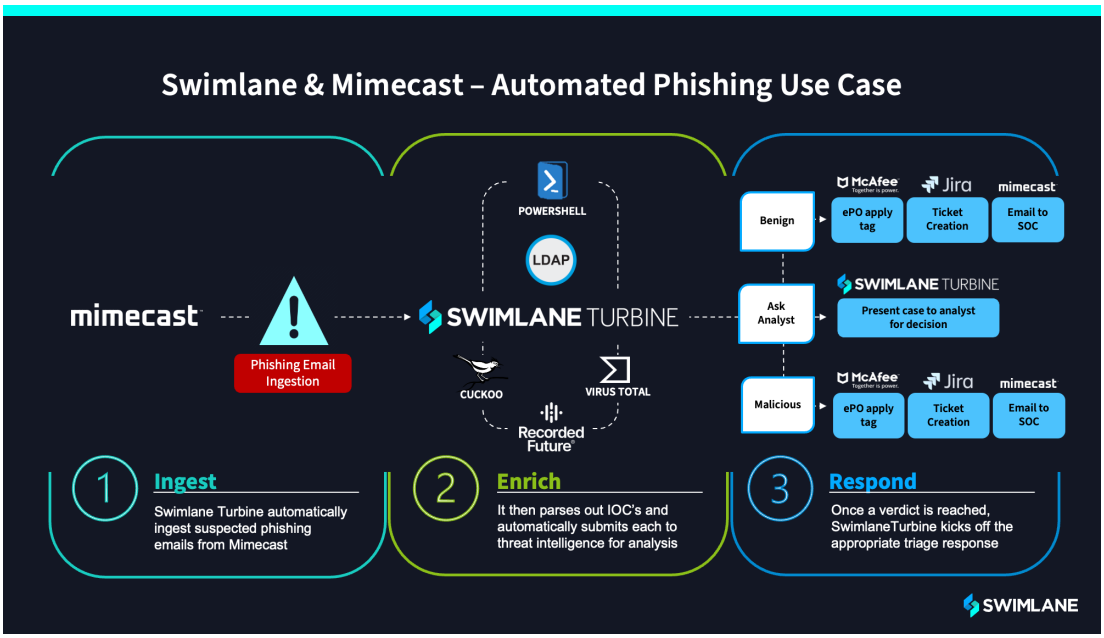
Integrated Solution

To mitigate the pain of alert fatigue and speed the detection, investigation, response process when email threats occur, security teams need to leverage low-code security automation. Together, Mimecast and Turbine provide an integrated solution to improve detection, stop threats, augment security insights and centralize response across security functions. Email attack investigations usually require pivoting from one suspicious indicator to another to gather critical evidence, grabbing and archiving evidence and finalizing a resolution - running these commands traps analysts in a screen-switching cycle.

The Mimecast and Turbine integration ensures that SecOps teams can standardize their incident response processes, execute repeatable tasks at scale, accelerate the time it takes to detect and protect against email-borne attacks and make more efficient use of limited security resources.
The Mimecast and Turbine integration ensures that SecOps teams can standardize their incident response processes, execute repeatable tasks at scale, accelerate the time it takes to detect and protect against email-borne attacks and make more efficient use of limited security resources.

Turbine ingests rich Mimecast information into a single system of record for security. This combines human data with machine data like Mimecast Actions (URL lists, message content, attachments, logs, policies, queue management, sender management and email removal) so that actionable insights are available for analyst investigation and automated playbooks can be triggered from a single interface.

As a result, Mimecast and Turbine help analysts quickly and accurately identify the root cause of an attack and remediate the threat. This ensures that SecOps teams ward against initial infection and lateral spread that can lead to downtime, ransom demands, lost data and stolen passwords.



Mimecast + Turbine Use Case - Automated Email Threat Enrichment & Phishing Response

1. Turbine ingests in all suspected phishing emails from an abuse inbox.
2. Parses out the email and submits IOCs to your threat intelligence provider for analysis.
3. Once a verdict is reached, Turbine will kick off a number of remediation actions if the email is malicious. Otherwise it will mark the email as benign if a false positive.
4. If the malicious score is unsure, it will be to an analyst for further manual review

Integration Features

Actionable Investigation and Reports
Turbine orchestrates and automates a variety of critical but repeatable Mimecast commands during incidents to accelerate response times.

Complex Email Threat Investigation
Analysts leveraging Turbine gain greater visibility and new actionable information about the attack through integrated Mimecast commands, with documentation per step and artifact reporting

Email Alert Prioritization
Increase efficiency and effectiveness by prioritizing the most pressing threats. This is enabled via automated enrichment and IOC score aggregation.

Low-code Playbooks
This integration enables customizable workflows and automation via Turbines low-code approachable automation.

Centralized Case Management
Turbine enables users to connect all of their security tools through integration and webhooks, enabling a centralized case management approach.

SWIMLANE

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

Learn more at: swimlane.com

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.

About Mimecast

For organizations concerned about cyber risk and struggling to attract and retain sufficient cybersecurity expertise and budget, Mimecast delivers a comprehensive, integrated solution that protects the No. 1 cybersecurity attack vector: email.

Mimecast also reduces the time, cost and complexity of achieving more complete cybersecurity, compliance and resilience through additional modules, all while connecting seamlessly with other security and technology investments to provide a coherent security architecture. Learn more at: mimecast.com