

Mimecast for Swimlane

Integrate security tools and processes, automate routine tasks and work smarter: respond faster and strengthen cyber resilience.

In an ever evolving, fast moving threat landscape, every organization is under threat. It's a landscape that has pitted security teams against cyber criminals in an escalating technology arms race. But the race to keep up with emerging threats has driven a proliferation of security solutions, which has left often under-resourced security teams struggling with a growing array of point products and independent static security controls with no orchestration between them.

This is where Swimlane comes into play, by allowing Security Operation Center's (SOC) to act against identified threats attempting to attack an organization. Swimlane is a Gartner recognized SOAR (Security Orchestration, Automation and Response), with many adaptable and flexible functions, used to identify and remediate against found threats automatically.

Security Orchestration & Security Automation:

Swimlane does a phenomenal job of combining these two solutions into an easy to use, fully capable SOAR. Security Orchestration is achieved by integrating 3rd party security tools, such as Mimecast, into their platform. By doing this, they can enable Security Automation, which is the ability to execute a sequence of tasks related to a security workflow without human intervention. It allows a security analyst to build out a custom workflow to address the simple everyday tasks such as, blocking a malicious sender. Although a simple task, these common attacks can pile up, and take hours out of a SOC's work day, leaving an organization vulnerable to more advanced attacks.

Key Benefits:

- Integration allows for an easy to use platform, performing Mimecast functions at the click of a button
- Automate simple security processes, freeing up the security analyst's time to address more advanced threats
- Increase Mimecast and Swimlane ROI by giving security teams access to a more complete SOAR platform
- Achieve full orchestration capabilities using proactive playbooks and workflows

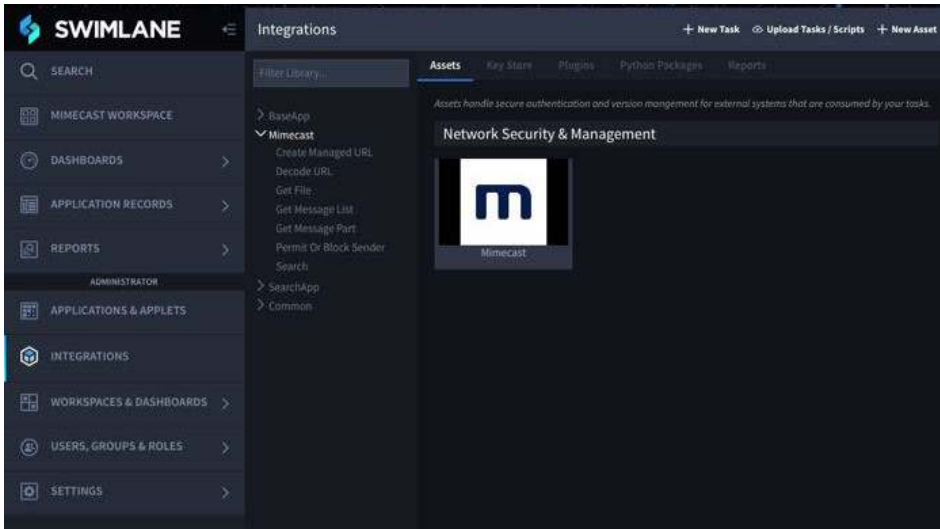
The screenshot shows a 'NEW SECTION' configuration window for an 'Integration'. It contains several fields for setting up the connection:

- Smash:** 15e175a999ac29edbe468cd99047d6168e8f01d5
- Received Date:** 2019-11-26T12:20:00+0000
- Display From:** Domain postMaster address
- ID:** eNotj01rg0AYhP_LXIXYd82qG0_FpmAo0qahYCSi3NdoXT_YzZqG0v_eNGVOMzCHZ5gFwCyGltJ1sS-TO9sKKq53kzQqIPuj_
- Status:** ARCHIVED
- Display To:** Test User
- Attachment Count:** 0
- Size:** 62017
- Subject:** You have new held messages

Retrieve All the necessary data from a message to allow for an accurate response from a SOC

Integrating Mimecast

Swimlane's platform, much like Mimecast, was built from the ground up. Allowing for custom features and flexibility when being faced with each enterprise's individual needs, accelerating time-to-value and delivering powerful collaborative capabilities.



Mimecast can be seamlessly integrated into the Swimlane platform, allowing for automated incident response, leveraging many of Mimecast's core functions. The integration has produced API generated, custom Mimecast workspaces and dashboards. This provides the user with an easy to use platform, making it extremely simple to perform actions such as blocking or permitting a sender.

Swimlane – Mimecast Integration

Custom Integration Functions:

Swimlane – Mimecast Integration

- **Mimecast Create Managed URL:** Add a URL to the Targeted Threat Protection
- **Mimecast Decode URL:** Decode Protect URL's
- **Mimecast Get File:** Returns a File Attachment from an archived message
- **Mimecast Get Message List:** Returns a list of messages for a given user
- **Mimecast Get Message Part:** Retrieve a specific part of a selected message
- **Mimecast Permit Or Block Sender:** Permit or Block a Sender through Mimecast
- **Mimecast Search:** Search through Mimecast Email Logs and Archives

For more Information Regarding This Integration

Check out Swimlane's [AppHub](#) or [Tech Connect](#)

Swimlane is a leader in security orchestration, automation and response (SOAR). By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real-time dashboards and reporting from across your security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations. Swimlane is headquartered in Denver, Colorado with operations throughout North America and Europe.