mimecast® | Datasheet

CyberSponse

Mimecast Integration

In today's modern security environment, time is a critical factor when it comes to analyzing, as well as remediating critical cyber security threats. A Security Operations Center (SOC) must be able to quickly analyze, process, and act on the emerging threats that their organization is facing. In addition to this, a SOC must be able to accurately identify true and immediate threats, to improve their cyber resilience.

To realize the full benefit of SOAR investments, SOC teams must be able to integrate their security tools with 3rd party platforms. This becomes even more vital with email, given that it's attacker's number one platform to target. The ability to integrate with various security products expands the range of responses to the array of threats, which can be discovered by security teams throughout an organization.

Therefore, Cybersponse's Security Orchestration, Automation, and Response (SOAR) tool has been integrated with Mimecast's email security data. Through its robust Automation Framework and Playbook Engine, which seamlessly integrates with hundreds of security tools, CyberSponse Operations Platform (CyOPs™), enables modeling of security automation workflows, and thus aids analysts to make more discerning decisions in far lesser time. It supports the entire gamut of Incident Management with its user-friendly and configurable case-management and best-in-class enterprise reporting.

Features of CyOPs:

- Role Based Incident Management
- Visual Playbook Designer
- Multi-Tenancy for MDRs/MSSPs
- Role Based Dashboards
- Metrics and Reporting features
- Queue Management for Security teams
- Comprehensive OOB playbook library
- Extensive integration library with over 260+ OOB integrations

CyOPs™ integrates with Mimecast Email Security products *(both Email Security- S1 and Email Security & Remediation-S2 product bundles)* and enriches the threat intel pouring into a security teams' environment, filtering out false positives and enabling teams to act faster and more accurately. The integration provides a comprehensive set of actions ranging from actions such as search message (searching through Mimecast's email logs instantly), get message details, get message list of a specified user etc. to response and containment actions such as blacklisting/whitelisting a URL, blocking a sender, create incident etc. for allowing to build an effective automation workflow.

Mimecast is a cybersecurity and compliance provider that helps thousands of organizations worldwide make email safer, restore trust and strengthen cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, compliance risk, human error and technical failure.

Various Actions Available As Part Of This Deep Integration

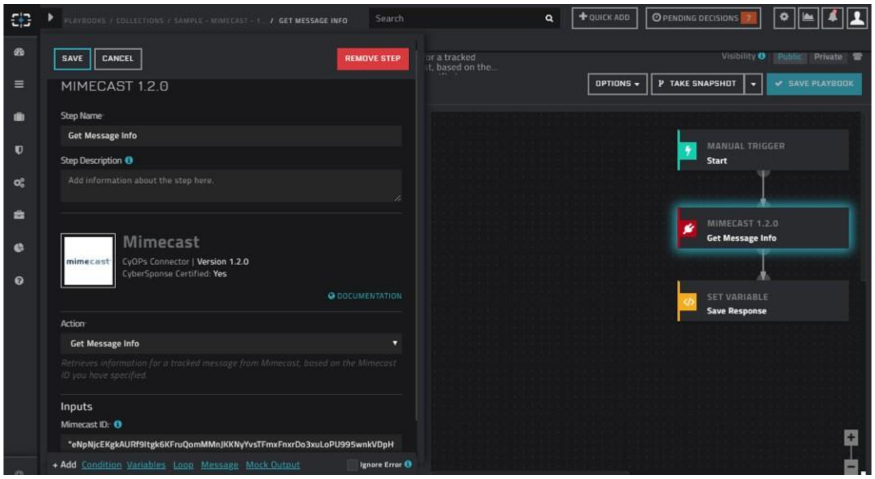
Block Sender	Adds a sender to the blocked sender list on the Mimecast server.
Unblock Sender	Adds a sender to the permitted sender list on the Mimecast server.
Blacklist URL	Adds a URL to be blacklisted on the Mimecast server.
Whitelist URL	Adds a URL to the targeted threat protection whitelist on the Mimecast server.
Get Managed URL	Retrieves a list and details of managed URLs from the targeted threat protection blacklist or whitelist on the Mimecast server.
Get Message List	Retrieves a list of messages for a specified user or the logged in user from Mimecast.
Get Archive Search Message Details	Retrieves metadata for a message from the Mimecast archives, based on the message ID you have specified.
Get Message Info	Retrieves information for a tracked message from Mimecast, based on the Mimecast ID you have specified.
Archive Search	Retrieves a list of messages from Mimecast that match the search criteria that you have specified.
Message Search	Tracks messages across the Mimecast platform, based on the input parameters you have specified
Create Blocked Sender Policy	Creates a policy for blocking senders on the Mimecast server.
Get Blocked Sender Policy	Retrieves a list and details of all blocked sender policies for a Mimecast account from the Mimecast server, or retrieves the details of a specific policy based on the policy ID you have specified.
Update Blocked Sender Policy	Updates an existing blocked sender policy from a Mimecast account on the Mimecast server, based on the policy id, action, and other input parameters you have specified.
Delete Blocked Sender Policy	Deletes an existing blocked sender policy from a Mimecast account on the Mimecast server, based on the policy id you have specified.
Create Group	Creates a new group on the Mimecast server.

Various Actions Available As Part Of This Deep Integration

Deleted Group	Deletes an existing group from the Mimecast server.
Find Groups	Retrieves details of existing Mimecast groups from the Mimecast server, based on the input parameters (filter criteria) you have specified.
Update Groups	Updates a group on the Mimecast server, based on the input parameters you have specified.
Add Group Member	Adds members (users) to the specified group on the Mimecast server, based on the csv list of email addresses or domains of the users you have specified.
Get Group Member	Retrieves details of the members of a specific group on the Mimecast server, based on the group ID you have specified.
Remove Group Member	Removes a member from the specified group on the Mimecast server, based on the email address or the domain of the user you have specified.
Get Aliases	Retrieves the alias address(es) associated with a user from the Mimecast server, based on email address specified .
Create Incident	Creates a remediation or restore incident in the Mimecast S2 platform, based on the input parameters you have specified.

Integration Screenshots

With other 260+ integrations available to be used OOB, CyOPs allows SOC teams an ability to visualize and implement enriched investigation processes, thereby building a comprehensive automated incident response life-cycle management solution. To know more about the solution, visit **CyberSponse.com.**



MIMECAST 1.2.0

Step Name: Get Message Info

Step Description: Add information about the step here.

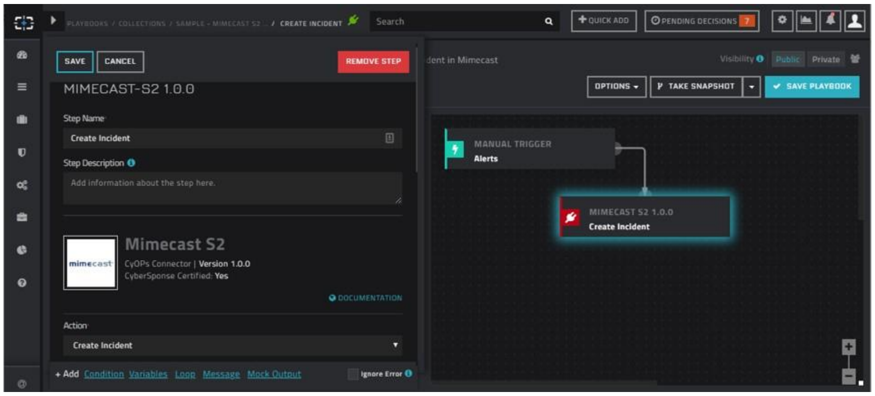
Mimecast
CyOPs Connector | Version 1.2.0
CyberSponse Certified: Yes

Action: Get Message Info

Retrieves information for a tracked message from Mimecast, based on the Mimecast ID you have specified.

Inputs

Mimecast ID: "eNpNjcEKgkAURf9Itgk6KFruQomMMnJKKNyYvsTFmxFnxrDo3xuLoPU995wnkVDpH



MIMECAST-S2 1.0.0

Step Name: Create Incident

Step Description: Add information about the step here.

Mimecast S2
CyOPs Connector | Version 1.0.0
CyberSponse Certified: Yes

Action: Create Incident