DEMISTO
A PALO ALTO NETWORKS® COMPANY

mimecast®

Automated Email Security and Incident Response

Benefits

- Shorten decision-making cycle by automating key tasks with analyst review
- Improve analyst efficiency by centralizing investigation, collaboration and documentation
- Enrich Mimecast with intelligence from other security products for coordinated response across security functions

Compatibility

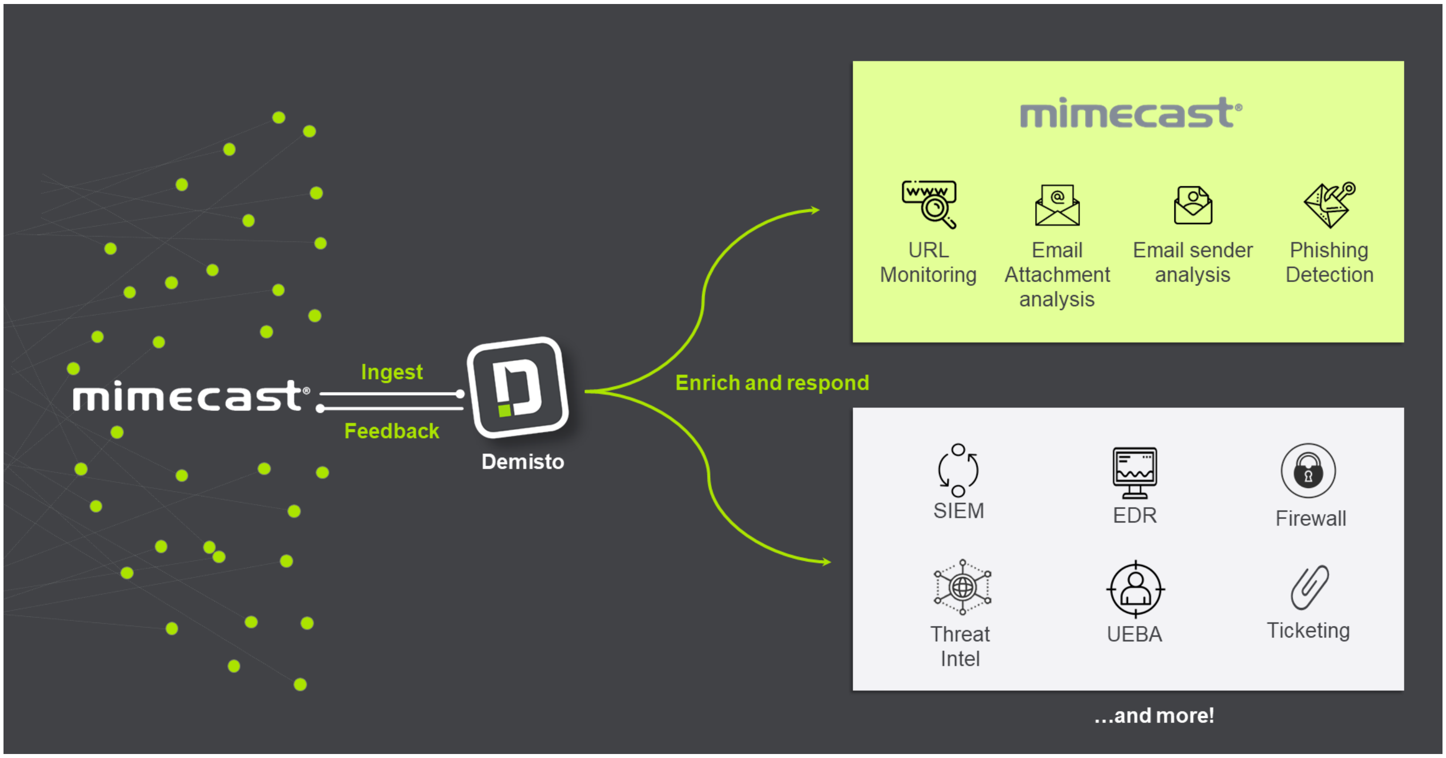
- Demisto Enterprise, Mimecast Secure Email Gateway

We all use email at work and at home. Not surprisingly, it is also a favorite application of cybercriminals for enabling malware delivery, impersonation fraud and phishing attacks. Because phishing attacks are easy to deliver and can be difficult to identify, an alarming 91% of hacking attempts today begin with some kind of phishing attack.

This integration combines Mimecast's comprehensive cloud-based email security capabilities with Demisto's security orchestration to help security teams standardize their incident response processes, execute repeatable tasks at scale, and accelerate time to detect and protect against email-borne attacks.

Integration Features

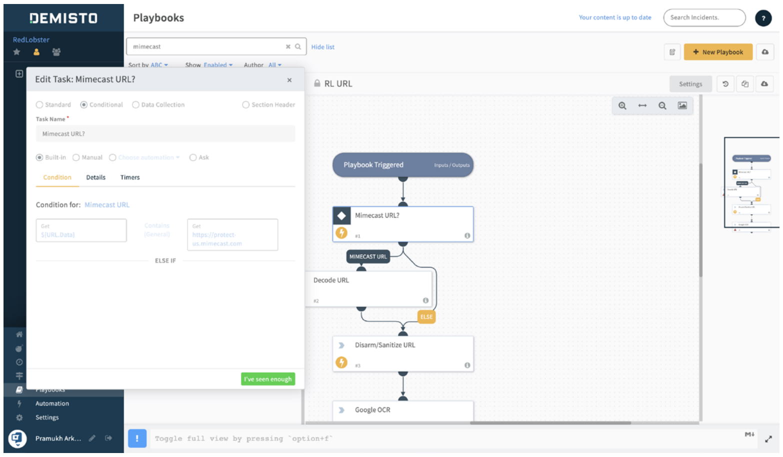
- Ingest rich Mimecast information (URL lists, message content, attachments, logs, policies, sender info) into Demisto for analyst investigation or automated playbook-driven response.
- Manage policies and users from within Demisto as automated playbook tasks or real-time actions
- Run thousands of commands (including for Mimecast) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.
- Leverage 100s of Demisto integrations to coordinate response across security functions.



USE CASE #1 AUTOMATED EMAIL THREAT ALERT ENRICHMENT AND RESPONSE

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

Solution: Demisto integrates with Mimecast to orchestrate and automate a variety of critical but repeatable actions during incident response. For example, if a suspect URL from a Mimecast alert is ingested into Demisto, the corresponding playbook gets automatically executed. This playbook looks up the URL, decodes it and if necessary disarms and sanitizes the URL.



Edit Task: Mimecast URL?

○ Standard ● Conditional ○ Data Collection ○ Section Header

Task Name *: Mimecast URL?

● Built-in ○ Manual ○ Choose automation ○ Ask

Condition | Details | Timers

Condition for: Mimecast URL

Get ${URL.Data} Contains (General) Get https://protect-us.mimecast.com

ELSE IF

Toggle full view by pressing `option+f`

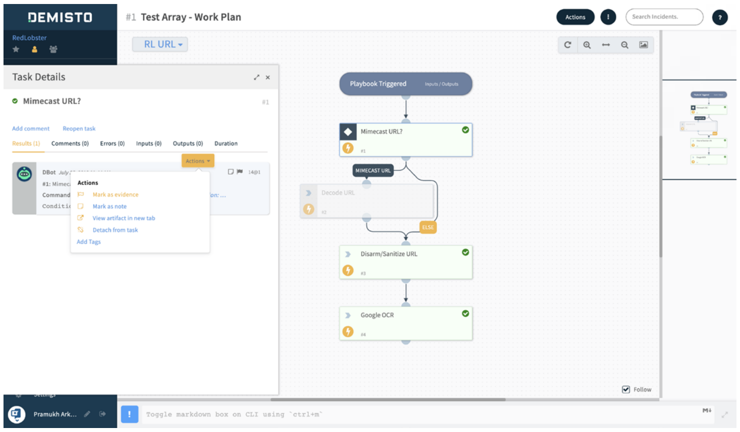
For other Mimecast alerts, playbooks can also be set up to enrich and extract malicious indicators or download and detonate suspicious payloads using an endpoint security sandbox.

Benefit: Demisto acts as the bridge between Mimecast and other security products that a SOC can use to speed incident resolution. This ensures standardized response and updates and reduced effort and time through automation.

USE CASE #2 INTERACTIVE INVESTIGATION FOR COMPLEX EMAIL THREATS

Challenge: Apart from running automated actions, attack investigations usually require additional real-time tasks such as pivoting from one suspicious indicator to another to gather critical evidence, grabbing and archiving evidence, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts can gain greater visibility and new actionable information about the attack by running Mimecast commands in the Demisto War Room. For example, if the analyst decides to block a sender, the analyst can run the Mimecast-manage-sender commands to block a sender in real-time without having to switch consoles. The War Room will document all analyst actions and analysts can mark artifacts as evidence for reporting.



Benefit: The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their environment from a common window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from a unified console. They will also prevent the need for collating information from multiple sources for documentation. Archived documentation can also be leveraged for future learning.

About Mimecast

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster 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, human error and technical failure. www.mimecast.com

About Demisto

Demisto, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit www.demisto.com.