

Mimecast Email Incident Response

AI and Human Expertise for Better Incident Remediation

The Problem

Email-based threats account for a significant percentage of all security threats, highlighting a massive challenge for organizations due to growing volume and increasing sophistication. While many of these emails may be benign, distinguishing genuine threats from the noise requires meticulous attention and expertise.

The Solution

Mimecast's Email Incident Response service improves your security posture while reducing the burden on your security operations center (SOC). Elevate your SOC's focus by routing employee-reported, email-based threats directly to Mimecast. With advanced threat intelligence, Mimecast's automated triaging and expert human analysis capabilities provide you with a trusted partner for email incidents. By quickly investigating emails to accurately identify and remediate threats, Email Incident Response empowers your security analysts to focus on more than just email.

Mimecast Value

- **Enhanced Threat Detection and Response**

MEIR significantly improves the ability to detect and respond to email-based threats, combining AI-based analysis with world-class threat analysts.

- **Reduced Analyst Burden**

MEIR augments in-house analysts and alleviates the burden of analysis by filtering out benign reports and prioritizing real threats.

- **Comprehensive Reporting and Insights**

MEIR provides detailed reporting and insights into email threats and incidents, enabling customers to refine security strategies and improve overall resilience against future attacks.

Feature	Details
Submitted emails run through AI	<ul style="list-style-type: none"> Automation quickly triages real threats and benign emails. Insights into patterns and trends. Continuous retraining.
MEIR Analyst Skills	<ul style="list-style-type: none"> Extensive experience in security and threat intelligence. Proven Incident Response Framework. Visibility across all Mimecast reported messages aids threat response. Ability to decrease MTTD and MTTR metrics.
Analysis & Reporting	<ul style="list-style-type: none"> Seamless integration with existing Mimecast email infrastructure. Detailed forensic reporting including email analysis, attachment details, and threat assessment. Complete threat remediation and removal across all organizational inboxes. Preventive recommendations and complete audit trail of analyst actions.

Use Cases

Phishing Campaign

Multiple employees have reported suspicious emails linked to a phishing campaign aimed at harvesting credentials. With Mimecast Email Incident Response, these reported messages are analyzed using the latest threat intelligence and enriched with email metadata for analyst investigation. Analysts receive contextual information, including reporting accuracy, the number of similar reports, and email risk scores, enabling quick identification of all related phishing emails. Malicious messages are automatically removed from affected inboxes, and indicators are blocked to prevent further compromise. Security and IT teams are included in the communication workflow, receiving valuable forensic information upon incident closure for further internal investigation. Mimecast's threat intelligence is updated to prevent future occurrences of the same threat.

About Mimecast

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.