DATASHEET

Mimecast Email Incident Response

Remediate email-based threats and elevate your SOC's focus with Email Incident Response.

The Problem

Security teams are inundated with alerts. Email-based threats in particular represent a massive security challenge due to their volume and complexity. With many employees now empowered to report suspicious emails, there's a never-ending backlog of security alerts that still require expert human analysis. Many of these reported emails are benign, but it takes careful attention to cut through the noise and identify real threats before they result in a successful attack. Unfortunately, this noise diverts analysts from investigating more serious alerts.

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

- **Accelerate Threat Response**
  Lowers the dwell time of email threats with rapid response and remediation, typically in 30 minutes or less.
- **Safeguard every inbox**
  Protects your entire organization by remediating known threats across all employee inboxes.
- **Expert Security Insights**
  Strengthens your security posture with Mimecast expert email security analyst recommendations.

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 landscape, you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.

Feature	Details
Employee Experience	• One-click suspicious email reporting through 'Outlook End-User reporting' integration • Positive reinforcement and feedback for reporting suspicious emails • No additional training or new interfaces required for end users • Immediate protection when threats are identified • Automated removal of threats from all employee inboxes
Administration	• Seamless integration with existing Mimecast email infrastructure • Comprehensive metadata enrichment including employee reporting accuracy and email risk scoring • Expert SOC analyst investigation with response times under 30 minutes, improving MTTD and MTTR metrics • 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 • Full visibility through administrative dashboard with complete service control

Use Cases

Phishing Campaign
Multiple employees report suspicious emails that appear to be part of a coordinated phishing campaign attempting to harvest credentials. Using Mimecast Email Incident Response, end-user reported messages are inspected using the latest threat intelligence, and the email metadata is enriched to help with later analyst investigation. The analyst receives contextual information focused on reporting accuracy, number of reports of similar emails, and email risk scores. This aids in quickly identifying all related phishing emails across the organization. The analyst automatically removes malicious messages from all affected inboxes and blocks the malicious indicators to prevent further compromise. Security and IT teams are also included in the communication workflow and receive valuable forensic information when an incident is closed, helping with any further internal investigation. Finally, Mimecast threat intelligence is updated, and future instances of the same threat will be prevented from reaching recipients.

Phish Testing
A company implements a phishing simulation program where employees who successfully identify and report test phishing emails are rewarded. When an employee correctly flags a simulated phishing test email by reporting it through Mimecast's reporting button, they receive positive reinforcement and recognition. This helps drive engagement with security awareness training, encourages vigilant email behavior, and allows security teams to track improvements in phishing awareness over time while identifying areas needing additional focus.