Solution Brief

Mimecast and Rapid7 InsightConnect

Coordinated, Automated, and Efficient Incident Response

Cyberattacks can come from many different vectors, but they most commonly arrive via email. By using email to deliver phishing, business email compromise (BEC) attacks, brand impersonations, and more, attackers pursue an organization's weakest security link — its people. As a result, email is the No. 1 attack vector for security teams to secure.

By integrating **Mimecast** with **Rapid7 InsightConnect**, organizations gain search and correlation capabilities to detect and respond to cyberattacks from a central location. InsightConnect is designed to help the security team respond to cyberthreats with confidence, automate with intelligence and collaborate with consistency. It guides the team in resolving incidents by codifying established incident response processes into automated playbooks.

The Security Challenge: Effective and Timely Response Across Multiple IT and Security Systems

IT environments today stretch far and wide - the adoption of mobile devices and cloud services have signaled the shift from perimeter-centric security.

Key Benefits:

- Automate email security processes, shorten decision-making cycles, and drive resource efficiency with automation.
- Consume intelligence from Mimecast and other security tools for improved incident context and prioritization.
- Provide automation and consistent incident response using predefined security playbooks.

With the era of cloud adoption and the current work-from-home reality (WFH), the attack surface of these new applications has significantly increased. Because these and earlier changes have happened over time, organizations addressed cybersecurity as the new trends emerged. This left organizations burdened with a collection of disjointed architectures and siloed components leading to complexity, technical debt, blind spots, and time-sensitive security events not being met, which added additional load upon an already overworked Security Operations (SecOps) team.

By way of illustration, a typical organization employs somewhere between 10 and 45 different security controls, and a single incident typically requires coordination across an average of 19 of them. The deployed security systems will create approximately 17,000 alerts each week, to which SecOps teams must react. Of all the alerts generated, approximately 16% are considered reliable, however; investigating this huge volume of false positives can take up to 21,000 hours per annum.

The security steps needed to investigate each alert are typically too manual and numerous to be efficiently handled by humans.

When responding to email threats, time is of the essence as these attacks usually target multiple users simultaneously across the organization, often leading to multiple points of infiltration. In addition, email attacks can generate a lot of alerts that have to be sifted through manually to determine the intent. Threat hunting and remediation tasks, while essential to incident response, are manual, repetitive, and time-consuming, causing alert fatigue and taking analysts away from other priorities.

This is where security orchestration, automation, and response (SOAR) platforms play a key part in supercharging incident analysis and triage through a combination of full automation and analyst-driven decision-making. Orchestration is achieved through the SOAR platform coordinating the security actions to support a workflow across multiple IT and security systems.

Integrated Solution

Mimecast and **Rapid7** provide an integrated solution to improve detection, investigate threats, augment security insights and centralize response across security functions. Email attack investigations usually require pivoting from one indicator to another to gather critical evidence, grabbing and archiving evidence, and finalizing a resolution. By integrating Mimecast with InsightConnect, SecOps teams can standardize their incident response processes, execute repeatable tasks at scale, accelerate the time it takes to protect against email-borne attacks and make more efficient use of limited security resources.

The InsightConnect platform ingests rich Mimecast information to deliver context to threat investigation. The Mimecast Actions (URL management, message content, policies, and sender management) are available for analyst investigation or automated playbook-driven responses from a highly customizable, but easy-to-use platform. With more than 300 plugins to connect security and IT systems — and a library of customizable workflows —InsightConnect makes it easy to coordinate responses across all of the supporting IT and security functions.

Together, Mimecast and Rapid7 share high-fidelity indicators to help analysts quickly and accurately identify the root cause of an attack and remediate the threat. This helps SecOps teams better respond to the initial infection and lateral spread that can lead to downtime, ransom demands, lost data, and stolen passwords.

Mimecast + InsightConnect: Customer Use Cases

Automated email threat enrichment	Orchestrate and automate a variety of critical but repeatable Mimecast commands during incident response to improve response times.
Complex Email Threat Investigation	Analysts gain greater visibility and new actionable information about the attack through integrated Mimecast commands, with documentation per step and artifact reporting
Alert prioritization	Increase efficiency and effectiveness by prioritizing the most pressing threats.
Threat intelligence	Unifying aggregation, scoring, and sharing of threat intelligence with playbook-driven automation across the security and IT estate.

About Mimecast
For organizations concerned about cyber risk and struggling to attract and retain sufficient cybersecurity expertise and budget, Mimecast delivers a comprehensive, integrated solution that protects the No. 1 cybersecurity attack vector: email.

Mimecast also reduces the time, cost, and complexity of achieving more complete cybersecurity, compliance, and resilience through additional modules, all while connecting seamlessly with other security and technology investments to provide a coherent security architecture.

Learn more at **www.mimecast.com**

About Rapid7
At Rapid7, we believe in simplifying the complex through shared visibility, analytics, and automation that unite your teams around the challenges and successes of cybersecurity.

The Rapid7 Insight Platform collects data from across your environment, making it easy for teams to manage vulnerabilities, monitor for malicious behavior, investigate, and shut down attacks, and automate your operations.

Through automation and orchestration, you'll free up team members to focus on strategic priorities with the confidence to know that things are running smoothly in the background. We work together to make sure you're getting the right security outcomes based on your organization's business goals.

Learn more at **www.rapid7.com**