Solution Brief

Mimecast and Palo Alto Networks Cortex XSOAR

Coordinated, Automated, and Efficient Incident Response

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

By integrating **Mimecast** with **Cortex XSOAR**, organizations gain search and correlation capabilities to detect and respond to cyberattacks from a central location - No needless pivoting between consoles. Cortex XSOAR is the perfect ally for security analysts, through a machine learning-powered platform which provides guidance based on past incidents and analyst actions, accelerates playbook development, and enables leaner, more efficient security operations.

The Security Challenge: Effective and Timely Response Across Multiple Tools

IT environments today stretch everywhere - the adoption of mobile devices and cloud services has signaled the shift from perimeter security.

Key Benefits:

- Automate email security processes, shorten the decision-making cycle, and drive resource efficiency through automation.
- Enrich email and network security threat intelligence with Mimecast and other security tools for coordinated incident response.
- Reduce email-threat alert fatigue and speed-up incident response with full orchestration using proactive playbooks and workflows.

With the next era of cloud adoption and the current work-from-home (WFH) population, the attack surface of all these new applications has vastly increased. Because this IT expansion happened over time, organizations addressed cybersecurity as latest trends emerged and evolved which left them 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 adds additional load upon an already overworked Security Operations (SecOps) team.

By way of illustration, a typical organization will employ somewhere between 10 and 45 different security tools, and a single incident requires coordination across an average of 19 of them. The deployed security tools will create approximately 17,000 alerts each week, to which SecOps teams must react. Of 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 low-level security tasks needed to investigate each alert are too tedious and numerous to be handled by human beings.

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 by the attacker. In addition, email attacks can generate a lot of alerts that have to be sifted through manually to determine malicious intent. These tasks, while essential to incident response, are repetitive and time-consuming, causing alert fatigue and taking analysts away from actual problem-solving.

In today's ever-changing threat environment, threat-related data from various disparate sources must be compiled and automate response actions to low level threats.
This is where security orchestration, automation, and response (SOAR) platforms play a key part in supercharging incident analysis and triage through a combination of human and machine learning.

Orchestration is achieved through the SOAR platform coordinating the security actions to support a process or workflow across multiple tool suites.

To aid in the alert and response issues, organizations are now focusing on quality over quantity with a mature approach that focuses on automation and the application of actionable intelligence to help monitor, detect, and respond to threats.

Integrated Solution

Mimecast and Palo Alto Networks provide an integrated solution to improve detection, stop threats, augment security insights, and centralize response across security functions. Email attack investigations usually require pivoting from one suspicious indicator to another to gather critical evidence, grabbing and archiving evidence, and finalizing a resolution - Running these commands traps analysts in a screen-switching cycle.
By integrating Mimecast with Cortex XSOAR, SecOps teams can standardize their incident response processes, execute repeatable tasks at scale, accelerate the time it takes to detect and protect against email-borne attacks and make more efficient use of limited security resources.

The Cortex XSOAR platform ingests rich Mimecast email-based information (URL lists, message content, attachments, logs, policies, sender info) into Cortex XSOAR for analyst investigation or automated playbook-driven response. Analysts can collaborate in real time, manage policies, and execute thousands of tasks from a single interface. With 850+ integrations and content packs, Cortex XSOAR makes it easy to coordinate responses across all security functions.

Together, Mimecast and Palo Alto Networks 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 ward against initial infection and lateral spread that can lead to downtime, ransom demands, lost data, and stolen passwords.

Mimecast + Palo Alto Networks Cortex XSOAR: 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 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 Palo Alto Networks
Cortex™ XSOAR is the industry's first extended security orchestration and automation platform that simplifies security operations by unifying automation, case management, real-time collaboration, and threat intelligence management. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case.

Learn more at **www.paloaltonetworks.com/cortex/cortex-xsoar**