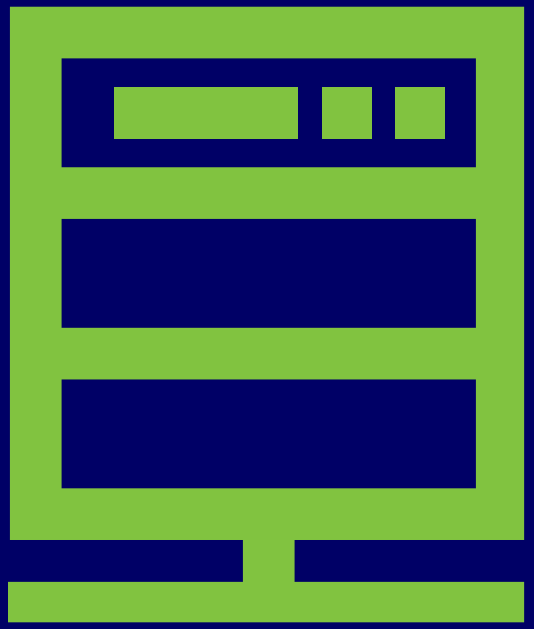
mimecast



White Paper

How Does Mimecast Help Improve the Performance of Security Operations Centers?

What is the Role of a Security Operations Center?

Organizations with a SOC understand that the security game is not about stopping everything from getting in, but making sure that the business keeps running and that sensitive data does not fall into the wrong hands. Whether created in-house, provided by a 3rd-party, or structured using a hybrid combination of the two, the role of a SOC is critical to the success of a security program.

A well run SOC must efficiently operationalize their people, use repeatable and efficient processes, and operate with the right automation and computer aided analysis to accelerate their people and processes. Given that diving into the details of people and processes of a SOC is beyond the scope of this paper, this paper will focus on the software and systems that SOCs typically use and how Mimecast services and data can make them more efficient and effective.

The primary role of the SOC can be framed using the NIST – **Cyber Security Framework (CSF)** as the model. The CSF categorizes security activities and controls into 5 core categories:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

In most organizations the SOC has primary responsibility for the systems, people, and processes which deliver the "Detect" and "Respond" portion of the NIST CSF. This is not to say that the SOC doesn't have influence and involvement in the other 3 control areas, they often do! If nothing else the SOC usually wants access to the data generated from these other domains to better enable them to monitor and improve the security posture of the organization.

Goals of a SOC

For a SOC to do its job effectively it is critical that all necessary security relevant data are collected, centralized, and available for normalization, correlation, alerting, investigation, threat hunting, and reporting.

It is hard to conduct effective and timely threat detection and response without the necessary data being available for automated analysis and to be at your analysts' fingertips for investigation! Mimecast services and data have an important role to play in helping SOCs with precisely this.

Common Functions of a SOC

- Security event monitoring, detection, investigation, and alert triage
- Security incident response management, including malware analysis, forensic analysis, & root cause analysis
- Threat intelligence management (collection, fusion, and dissemination)
- Threat hunting and vulnerability management
- Remediation of security issues
- Reporting (contributing to compliance and general proof of control)
- Working with 3rd-party SOC service providers when appropriate

Common Metrics for a SOC

How do you know if your SOC is doing a good job or even the right job? What are some common metrics and reports on which a SOC depends? This can be quite an expansive list, but usually at the core, metrics revolve around tracking the SOC's effectiveness and efficiency of detection, investigation, and response to security incidents that are hitting the organization.

What Software Tools do SOCs Use?

There is no shortage of technologies that are in common use by SOCs. The most common of these systems include Security Information and Event Management systems (SIEMs), Security Orchestration, Automation, and Response systems (SOARs), Endpoint Detection and Response systems (EDRs), Threat Intelligence Management platforms, as well as various types of commercial and open source threat intelligence feeds. These systems as well as others are used to help automate and support the SOCs primary roles of threat detection, investigation, and response.

Preventive security systems such as endpoint security systems, secure email gateways, firewalls, web gateways/ proxies, and directories (such as Active Directory for user authentication), that are primarily deployed to prevent bad things from happening, are key data sources for the SOC to help drive detections, provide data and context for investigations, and to enable faster threat blocking.

Given that data is the lifeblood of the SOC, integration with these preventive systems are critical to the efficiency and effectiveness of the SOC. But integration can go beyond one-way, inbound data flows. In fact, bidirectional integration between a SOCs' systems and these preventive security systems (having the SOC drive changes directly into the preventive system) is becoming much more common.

Using Metrics Such As:

- Number of security incidents investigated and escalated in a period
- Dwell Time from detection to containment and eradication (Mean-time-to-detect and respond)
- Percentage of incidents escalated from Tier-1 to Tier-2 analysts
- Percentage of recurring incidents
- Number of systems with known vulnerabilities yet unpatched
- False positive detections
- Time to investigate incidents
- Number of declared incidents in a period
- Reports of most attacked people, applications, and business units

Introducting Mimecast's Security Services

Mimecast is a cloud-based cybersecurity service provider that helps tens-of-thousands of organizations make their email safer, restore trust in employees, partners & customers and bolster their organization's cyber resilience. Known for helping customers safeguard their organization from email-borne threats, Mimecast's expanded cloud suite enables organizations to implement a more comprehensive cyber resilience strategy.

The primary security services provided by Mimecast are:

Mimecast Secure Email Gateway with Targeted Threat Protection

Mimecast's cloud-based Secure Email Gateway protects organizations and employees using any cloud or on-premises email platform. It defends against inbound spear-phishing, malware, spam and zero-day attacks by combining innovative applications and policies with multiple detection engines and intelligence feeds.

Mimecast Awareness Training

helps security organizations deliver effective online security training to employees in roughly three minutes a month. Each monthly training module is anchored on a short video in the contemporary workplace and driven by scenarios employees will recognize all too well.

Mimecast Web Security

The Mimecast Web Security service protects against malicious and business inappropriate web activity, and provides visibility and control over employee cloud application use. A fully cloud-based service, it adds strong security at the DNS level, is quick to setup, and straightforward to manage.

Mimecast Brand Exploit Protect

Block brand attacks before they can launch and stop live attacks in their tracks with Mimecast Brand Exploit Protect. This innovative service uses a combination of machine learning and quadrillions of targeted scans to identify even unknown attack patterns at an early stage, blocking compromised assets before they become live attacks. When active attacks are discovered, they can be remediated quickly to minimize damage.

Mimecast DMARC Analyzer

Using DMARC (Domain-based Message Authentication, Reporting and Conformance) to stop direct domain spoofing is an effective defense against brand abuse and scams that can tarnish your reputation and lead to direct losses for your organization, your customers and partners. Mimecast DMARC Analyzer is designed for simple and effective self-service to reduce the time, effort and cost of stopping domain spoofing attacks.

How Mimecast Helps SOCa with Threat Detection, Investigation and Response

It is no secret that most cyberattacks attacks start with email-borne threats. But the malicious use of the web at various stages of attack execution also occurs regularly. Given that email and the web are central to the execution of most attacks, it follows that data from those preventive security systems are critical to enable the SOC's threat detection, investigation, and response functions. After a threat is detected this same data is critical in helping a security investigator determine the root cause of an incident and to determine the optimal response.

Tables 1-7 on the following pages map the Common Functions of a SOC introduced above, and lays out in opposing cells the different ways that the Mimecast services and related data help SOCs deliver on those functions.

Tables 1-7 – Common Functions of a SOC and How Mimecast's Security Services & Data Help Improve the Performance of Those Functions

TABLE 1 - MONITORING

Security event monitoring, detection, investigation, and alert triage make up the single most important set of security functions of a SOC. Collectively these functions require timely and accurate data to be collected, centralized, analyzed, and fed to a SOC's systems and analysts. As a key security system in an organization, the data provided by the Mimecast service can play a key part in improving the priority for threat detections and the speed of investigations.

Common functions of a SOC	How Mimecast helps improve the performance

• Security event monitoring
• Detection
• Investigation
• Alert triage
	• Provides data from the email gateway and email & web threat analysis, including:
	  • Unblocked/blocked emails
	  • Inbound, outbound, & internal logs of email traffic from the Mimecast MTA
	  • Blocked malicious URLs & files
	  • Unblocked/blocked Web requests
	  • Malware origin by geo-location
	  • Sender IP & email address
	  • Post-delivery remediated emails & files
	  • Most targeted users
	  • Searches for malware file hashes
	  • Security policy audit events
	  • In-depth data on malware detected
	  • Source of likely brand spoofing emails being directed to customers and partners
	  • Listing of potential brand exploiting domains
	  • Evidence of live brand exploiting web sites
	• API & SIEM integrations (examples of out-of-the-box integrations - Splunk, IBM QRadar, LogRhythm. Current integrations can be found here). Details on Mimecast logging can be found here.
	• Data can be used in SIEM correlation rules - correlated with other security logs - to suppress or increase the priority of alerts and to add more context in support of investigations. Covering the detection of:
	  • Compromised user credentials
	  • Command & Control communications
	  • Data exfiltration
	  • Lateral movement
	• Provides security investigators with access to the organization's email archive, including individual mailboxes or all mailboxes in the organization.
	• Access to logs of blocked emails that violate DLP policies for including sensitive or otherwise restricted content.

TABLE 2 - INCIDENT RESPONSE

Data from the Mimecast system is critical to incident response management. Some threats are harder to truly understand than others. In these more difficult cases, the ability to efficiently conduct malware and other forensic investigations to track down the infection entry point is critical to understanding the root cause as well as the goal of the attack. This analysis is critical to improving an organizations' defenses. Data generated by the Mimecast service can play an important part of the analysis.

Common functions of a SOC	How Mimecast helps improve the performance
• Security incident response management • Malware analysis • Forensic analysis • Root cause analysis	• Track email messages as they entered and traversed the organization. • Track recipient & sender email addresses to follow the path of suspected threats. • Search for email via To:/From: email addresses & Mimecast message IDs. • Use Mimecast sourced data (listed in Table 1 above) to enrich investigations and to help drive response management . • Search for file hashes of suspected malware (MD5, SHA1, SHA256) to see if they have been directed at the organization. • Mimecast Internal Email Protect expands the visibility (reducing blind spots) into internal-to-internal emails which helps to detect threats spreading via internal emails (resulting from the use of RATs or the attacker's use of stolen credentials). • Leverage the Threat Intelligence API for access to details of Mimecast generated malware related detections. • Access to email and malware analysis logs generated by Mimecast AV engines, static file analysis, and sandboxing results with details on malware detections. Includes data on file structure & detailed threat indicators. • Data can be fed into SOAR based Run Books (or Playbooks) to provide context for the investigation process.

TABLE 3 - THREAT INTELLIGENCE MANAGEMENT

Without timely and accurate intelligence, it is difficult for a SOC to operate intelligently. Given that Mimecast analyzes billions of emails each month and given the prevalence of email-borne threats in their various forms are the primary attack vector used, threat intelligence provided by Mimecast can be an extremely valuable feed into an organization's threat management system.

Common functions of a SOC	How Mimecast helps improve the performance
Threat intelligence management: • Collection • Fusion • Disseminations	• STIX & CSV formatted threat data feeds of Mimecast security & message data (as described in Table 1 above) for feeding into Threat Management or SIEM/SOAR systems of your choosing via an API. • Mimecast provided Threat Intelligence Dashboard for direct access to the data via the Mimecast Administrative Console. Provides a summary of email-borne malware directed at your organization as well as geographic cuts, so you can compare your organization anonymously to thousands of others using the Mimecast service.

TABLE 4 - THREAT HUNTING & VULNERABILITY MANAGEMENT

A well run SOC generally wants to move from being almost exclusively reactive to providing more proactive protections. Instead of just reacting to threats that have unfortunately landed, important information can be gleaned from unsuccessful attacks to better understand what and who the attackers are after. The ability to better understand your organizations' most targeted people and systems can help the security team improve defenses where they matter the most.

Common functions of a SOC	How Mimecast helps improve the performance
• Threat hunting • Vulnerability management	• View most attacked users in the organization. • View blocked and visited web sites. • See recently observed indicators of compromise. • Mimecast Threat Center provides organizations with threat advisories, analysis of certain threat trends & deep dives into new threats and vulnerabilities that have been observed by Mimecast. • Benchmark the organization versus their industry/geography. • View malware rejection trends. • Discover and track brand spoofing emails and web sites on attacks directed to customers, partners, and to anyone else who would know and trust the organization's online brand.

TABLE 5 - REMEDIATION

Once threats are detected, triaged, and understood, the next logical step is to fix them. Mimecast helps by automating the removal of malicious or unwanted emails as well as updating blacklisted domains. With API initiated remediation SOCs can directly fix an issue that they discover, if that fits the preferred workflow, without needing to open tickets and waiting for other parts of the IT organization to act. The SOC alternatively can direct the team responsible for messaging security to take the necessary remediation actions.

Common functions of a SOC	How Mimecast helps improve the performance
• Remediation of security issues	• Leverage the Remediation API to remove malicious/unwanted/inappropriate emails as well as to block domains based on threat intelligence sourced elsewhere. Can also be done directly from within the Mimecast Administrative Console. • Automate the takedown of malicious, brand spoofing email and web domains.

TABLE 6 - REPORTING

The ability to demonstrate control to both internal as well as external auditors and regulators easily and accurately is also a key part of the responsibilities of a SOC. Mimecast data can be pulled directly into the reporting system to surface all relevant data that a SOC might need to provide this proof of control.

Common functions of a SOC	How Mimecast helps improve the performance
• Reporting	• Customer Service Reports containing historical email flow and threat data. • Integration with SIEMs for email & web security data for report generation. • Mimecast data available for searching in the reporting system of the organization's choosing. • Ongoing tracking of the successful and failed delivery of legitimate email coming from the organization's domains.

TABLE 7 - 3rd PARTY SOCs

Not all organizations run all aspects of their SOC functions in-house. Many organizations choose to outsource some common SOC functions to 3rd party service providers. Mimecast sourced data can be consumed by multiple systems and service providers even if certain SOC functions are outsourced.

Common functions of a SOC	How Mimecast helps improve the performance
• Working with 3rd-party SOC providers if the organization is running in hybrid mode	• Provide access to Mimecast administration console and/or APIs to 3rd-party SOC analysts and systems of the customer's choosing. • Mimecast has over 50 API functions to enable 3rd-parties to configure Mimecast policies, automate manual tasks and enable integration of Mimecast admin capabilities into 3rd-party tools in use by SOC providers.

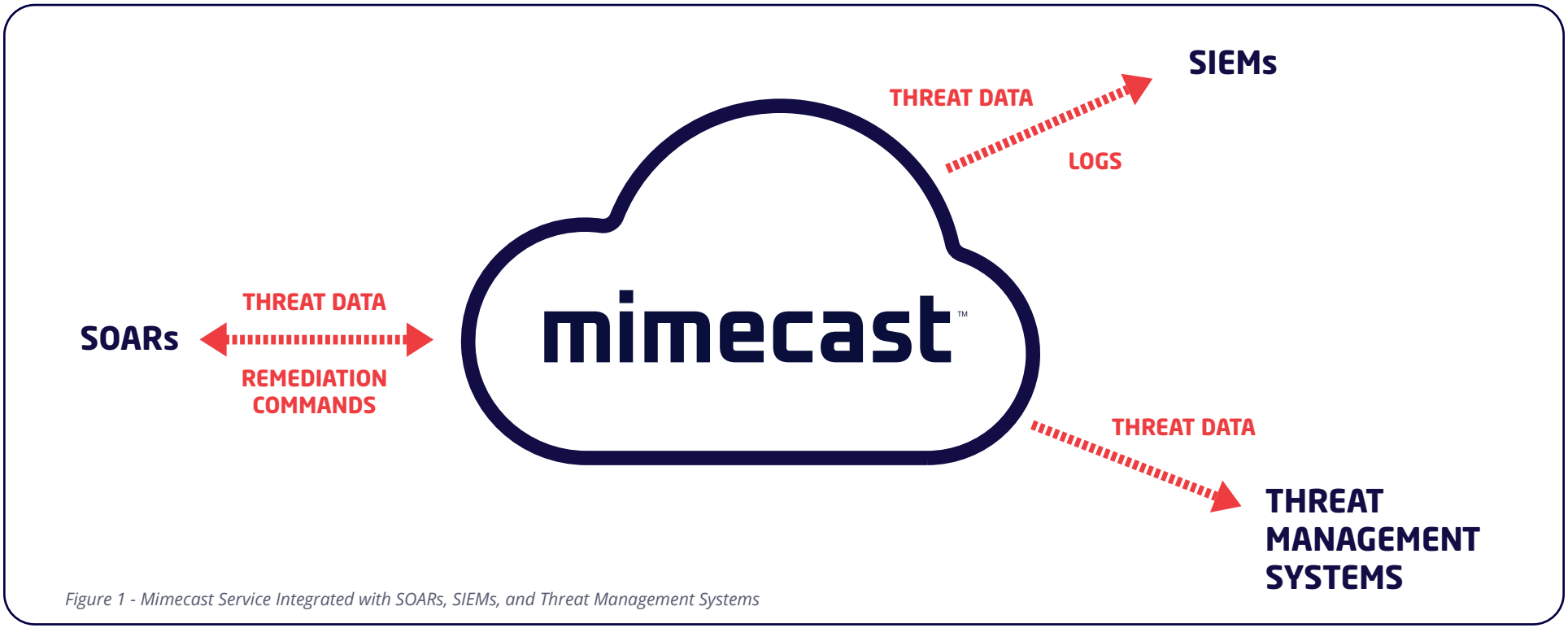


Figure 1 - Mimecast Service Integrated with SOARs, SIEMs, and Threat Management Systems

Conclusion

The creation and ongoing development of a SOC is pivotal to the maturation of an organization's security program. A high functioning SOC almost literally becomes the central nervous system of an organization's security system, sensing threats and rallying a response. To do this the SOC's systems and analysts need access to the most complete, accurate, and timely data, analysis, and intelligence from both inside and outside the organization.

Mimecast's security services are literally on the frontlines of an organization's security defenses and as such must provide critical data to the SOC to help them deliver on their primary functions: **Detection, Investigation, & Response.**

Mimecast understands this need and the critical role our security services and associated data can play in helping SOCs deliver these functions both efficiently and effectively.

Mimecast was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together.

We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.