ANOMALI mimecast™

KNOW YOUR ADVERSARIES, AND THE EMAIL THEY RODE IN ON

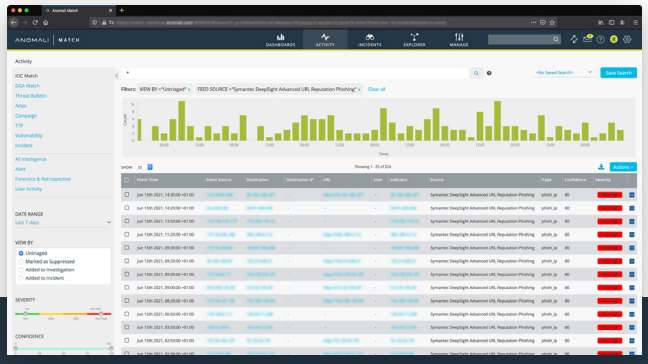
Detect and respond to email-based threats with Anomali and Mimecast

ANOMALI AND MIMECAST JOINT SOLUTION FEATURES

- Enhanced detection and remediation with Mimecast threat feed augmenting Anomali Threat Stream and integrated with your existing security estate.
- High Fidelity indicators of compromise from Mimecast's global locations, ensuring every region and industry vertical is served.
- Bi-lateral threat sharing to remove resource constraints through security automation tasks to reduce investigation and triage process.

IMMEDIATE TIME-TO-VALUE

- Threat coverage from the number 1 attack vector — email
- Strengthen risk-based decision making from verified indicators
- Ingestion of non-email-based threat indicators into Mimecast for pro-active defense



SHARED INTELLIGENCE

Email remains the most common and widely utilized attack vector for the delivery of malware, from commodity mass-delivered to custom-built and highly targeted instances. Mimecast and Anomali have partnered to provide bi-lateral threat sharing of high-fidelity indicators to ensure perimeter technologies are aware of the latest malware-based threats, protecting the organization against infection, lateral spread, associated downtime and potential data loss.

CRITICAL INTELLIGENCE

Up to the minute intelligence of the latest email-based threats

REDUCED RISK

Protect the security estate as threats are discovered

PROACTIVE PROTECTION

Ingestion of multi-vector threats into email gateway

MALWARE DELIVERY

CHALLENGE

Malware remains the preferred methodology for access to your corporate infrastructure by malicious actors, and it is constantly evolving as attackers attempt to stay ahead of the security ecosystem and their detection capabilities.

SOLUTION

Malware-based email threats stopped by Mimecast, are shared across your ecosystem from the endpoint, to network, and cloud solutions.

CUSTOMER BENEFIT

Increased protection, reduced resource utilization and enhanced malware analysis and knowledge.

DEEPER UNDERSTANDING

CHALLENGE

Threat correlation is challenging when looking across the vast number of security technologies deployed within an organization. Obtaining a view of the initial deployment methodology, characteristics and subsequent access attempts is time consuming, involves multiple toolsets and requires a high amount of manual effort.

SOLUTION

Threat intelligence feeds from external sources, and organizational toolsets combined into a single platform with analysis capabilities to view the entire attack chain, and subsequent vulnerabilities which require remediation.

CUSTOMER BENEFIT

Reduced risk through enhanced understanding of threats across the security estate including email.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI