Medicare Network
More intelligent, More Secure

Crown Commercial Service Supplier

AI-Powered Self-Learning Email Security

Prevent | Detect | Respond | Predict

Real-World Email Threats

It's hard to overestimate how fundamental email has become to initiating cyber-attacks. While there are numerous ways for attackers to target organisations, email is almost-always the common denominator. Email phishing attack detection, analysis and rapid response is one of the biggest challenges email admins and security teams face today.

Enhance your phishing response strategy, with the next-generation automated email anti-phishing incident response, will dramatically accelerate detection-to-response time from days, weeks or months down to just minutes, or even seconds.

On average, it takes less than 82 seconds from attack detonation until the first click is lured.

Here is a step-by-step response to an attack without a self-learning email security mitigation solution:

- An employee reports a phishing attack to the SOC team, sending it to the bottom of an exhaustive list of tickets already submitted, regardless of priority
- Once the SOC team gets the report they must manually perform forensic analysis and reverse engineering
- The SOC team attempts to pinpoint the origin and nature of the attack to figure out the best way to contain it
- The SOC team compiles all reported alerts in order to analyse the situation.
- After the attack has been realised, the SOC team sends an email to all employees about the phishing event
- The SOC team quarantines and deletes suspected phishing emails

Introducing the Solution of Tomorrow

This comprehensive solution is the world's first and only anti-email phishing technology to combine human intelligence and leveraging award-winning technologies consisting of artificial intelligence (AI) powered and machine-based learning.

The self-learning platform helps where your email security is most vulnerable with post-delivery protection, detection, and remediation. Now you can defend against the full spectrum of phishing threats when and where they are most likely to cause damage, at the mailbox level.

Advanced Malware/URL Protection
Identify, flag and respond to malware and URL threats at scale

Mailbox-Level BEC Protection
Make smarter and faster decisions regarding suspicious emails already in users' mailboxes

AI-Powered Incident Response
Reduce manual email analysis and response by orders of magnitude (up to 90%)

Democratized Real-Time Threat Detection
Crowdsource the best threat analysis and detection from the world's leading SOCs

Virtual Security Analyst
Get AI-Powered machine learning to help humans do more with automated threat remediation

Gamified, Personalised Simulation and Training
Access customised micro-learning to help employees think and act like security analysts

"Without machine intelligence, there are no preventative measures to ensure the same attack won't happen again."

What the Platform Delivers

The technology vendor is constantly adapting the platform with their 'innovation as a service' approach to ensure you always have access to fast, easy and complete email security solutions in a single platform.

"The speed at which the platform identifies and remediates is the core of the product."

Platform Features

The platform helps you fight all sorts of known and unknown attacks such as malware, ransomware, credential/ID theft, business email compromise, brand forgery, polymorphic and zero-day attacks. The platform works in real-time, without writing a single script or rule to:

- Automatically scan malicious URL's and attachments on ALL inbound emails
- Detect all types of email threats, even impersonation, and non-signature based BEC attacks
- Automatically render verdicts on suspicious emails and respond without full mailbox scans
- Leverage thousands of analyst inputs at any moment, based on what's happening now
- Automatically claw back and cluster bad emails at scale instantly
- Interactively train each employee to think and act like a security pro, based on how they work

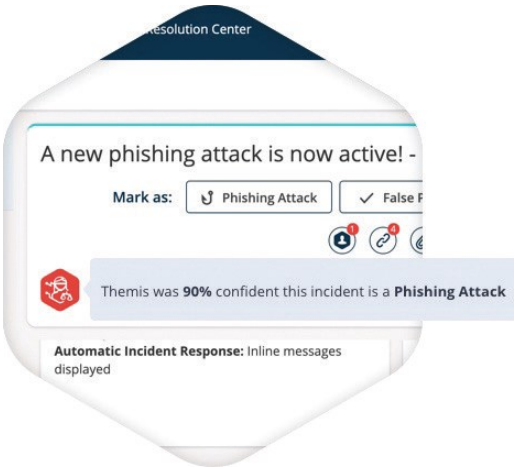
Key Benefits

- Reduces risk by resolving unknown phishing threats faster
- Mimics the decision process of 1000's of SOC teams in real-time for hard-to-read email threats
- Improves the efficiency of security teams with AI-Powered assisted email phishing classification
- Automates decisions without human intervention based on your thresholds and policies
- Provides a confidence level for all open email threats

A solution that works for you, not the other way around

Themis (the AI-Powered virtual security analyst) examines detected or reported incidents and provides a threshold of confidence for any recommendations based on all the collective verdicts made by customers using the platform such as phishing, spam and false positives. Themis then makes a recommendation to your security team based on dozens of data points.

As a fully autonomous solution, Themis can be set up to make and implement its decisions automatically without human intervention. With more than 90% accuracy, more and more customers are relying on Themis for the majority of their incident response decisions.



The Power of Now

For both security professionals and end-users, the solution offers a single platform with push-button protection, giving you simplicity and speed for accelerated visibility and control.

The platform works from the inside out to protect your organisation from any and all types of phishing attacks, especially those that get past traditional Secure Email Gateways (SEGs).

About Medicare Network

Medicare Network is an agile, forward-thinking Cyber Security and Risk Management company, product agnostic that offers a range of industry-leading and advanced secure solutions, leveraging award-winning AI and Machine Learning technologies to identify, respond and protect against sophisticated cyber-attacks.

20 Mortlake High Street | London | SW14 8JN | United Kingdom
UK +44 (203) 355 3785 | **US** +1 (702) 605 4601
www.mednetsec.com