PHISHME COFENSE

6 KEYS TO FASTER PHISHING MITIGATION

Speed Matters in Email Security - How to Optimize Incident Response

IN THE HIGH-STAKES RACE AGAINST CYBER THREATS, SPEED AND PRECISION MAKE ALL THE DIFFERENCE

According to Verizon's *2024 Data Breach Investigations Report*, "*68% of breaches involved a non-malicious human element, like a person falling victim to a social engineering attack or making an error.*"

In a landscape where threat actors are exploiting increasingly sophisticated tactics to deceive not only technology but also the vulnerabilities of your workforce, a multifaceted, efficient approach must be adopted to optimize an organization's incident response.

YOU NEED TO MITIGATE FAST

When a malicious email evades your perimeter defenses, the race is on and the clock is ticking. Every minute adds to potential business losses. You need to triage the threat and get to mitigation fast.

In this e-book, we'll examine how you can win the race against email threats, and how Cofense® solutions such as our Phishing Threat Detection and Response (PDR) Platform can help you quickly mitigate attacks. You'll learn to accelerate your email threat triage and use fewer man-hours to optimize your incident response. Neutralize threats before they cross the finish line with these 6 key elements.

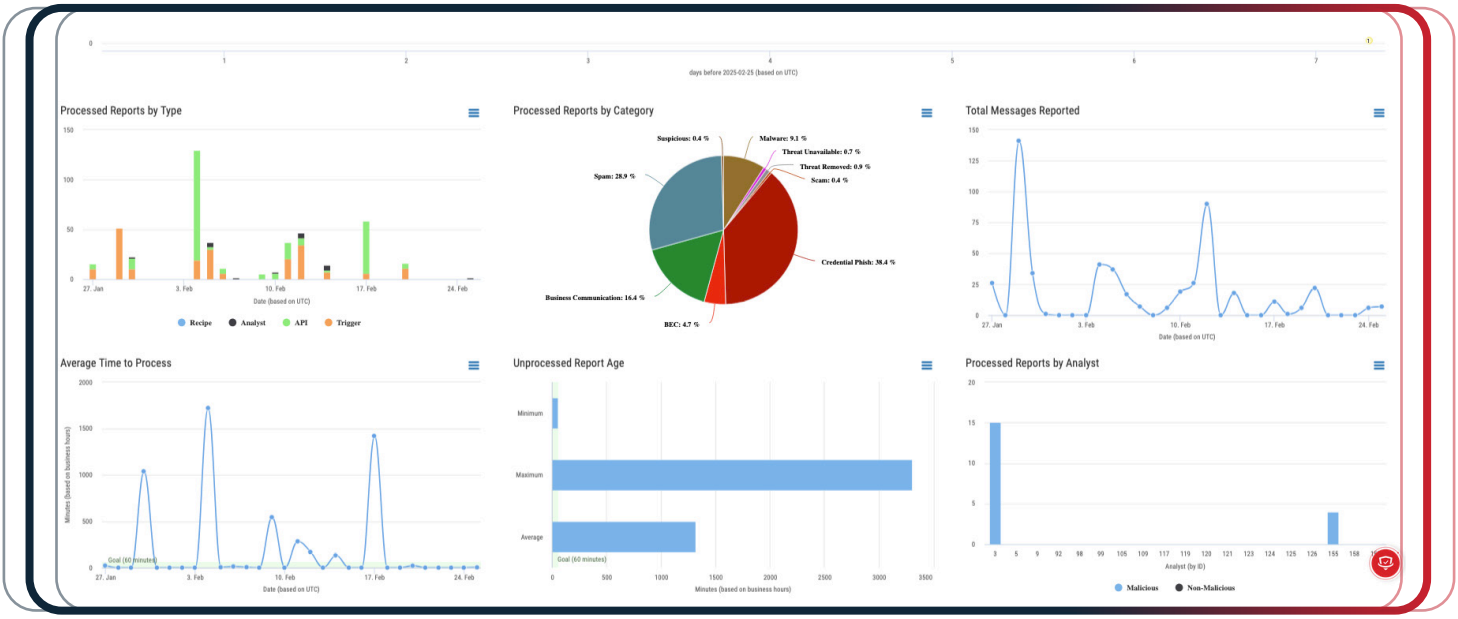
01

RESPOND TO EMAIL CLUSTERS, NOT EVERY SINGLE EMAIL

Automation is critical in achieving a speedy response to email threats that bypass traditional security defenses, so it's important to understand what your technology enables you to do. If your existing technology doesn't allow, by integrating Cofense PDR with your current security program, you're able to streamline email threat analysis by automatically clustering malicious emails by campaign.

Our platform finds key commonalities among reported emails. As these commonalities are discovered, a cluster report is created. These reports include indicators of what could be an email threat campaign.

Treating the email cluster as a unit alleviates you from having to sort through and try to match every single message that may be related. When you're responding to email threats in volume, as most companies do, this is much faster than executing a response to each and every instance.



Once a cluster has been identified, the work of the analyst begins. The analyst can look at the headers, along with the bodies of emails, and start to analyze what kind of threat a cluster is. Suspicious attachments can be sent to tools like Cuckoo, VirusTotal or Palo Alto Wildfire to determine if it contains malware. Threat intelligence feeds like Cofense Intelligence can be consulted for additional analysis on live and new email threats.

The aim is to allow analysts to determine malicious intent in one place, by increasing the speed this analysis can be completed, without sacrificing accuracy.

02

FURTHER AUTOMATE WITH PLAYBOOKS & TRIGGERS

Once you identify a threat, you need to get ahead of it. A playbook is a set of repeatable tasks that can be automated to reduce the work of the analyst; allowing you to beat the threat by acting fast and efficient.

A BASIC EXAMPLE

- Based upon the contents of the cluster, the playbook starts by assigning it a category
- Depending upon the category, the playbook knows the type of threat the messages represent and creates a ticket in your help desk system
- If you utilize a tool such as Cofense Triage, you can automate the analysis of a malicious URL or attachment
- The platform can notify the proxy team to block a URL or a domain
- And it sends a message to the employees who reported the messages to close the reporting loop

After you create a playbook, you can save it and reuse for other threats. You can then further automate by creating a trigger that executes the playbook when certain specific conditions are met. All of this is designed to reduce the load on your email analysts, again enabling accuracy and speed.

03

ORCHESTRATE AND INVOLVE THE RIGHT TEAMS AT THE RIGHT TIME

Enabling your security teams and technology to mobilize when needed, and most importantly in unison, is vital in orchestrating effective incident response. Cofense's out-of-the-box integrations enable analysts to work with all your existing security tools effectively. Our API automates the process of involving the right teams quickly, while Cofense Triage integrations keep your array of solutions in sync.

What's more, our customized AI spam filter helps to 'clear the noise' to free your people to focus on the genuine threats. The custom filter learns from the spam or legitimate business communications specific to your environment, making it uniquely effective for your organization's needs, and automatically filtering the 'noise' reported by end users. This custom approach ensures higher accuracy and more efficient spam management, increasing the efficiency and effectiveness of your analysts.

04

FIND AND QUARANTINE EMAILS THREATS

Let's stop for a moment and review what happens in an ideal world when you respond to an email threat alert.

- A bad email makes it past your security technology that should have caught it
- Your eagle-eyed workforce recognizes the threat and reports it
- If you deploy Cofense Triage, you automatically analyze it and use playbooks to prepare the response
- A security analyst kicks off the response to the email threat

But then your security team asks, "Where else does that email live on my network?"

ENTER COFENSE VISION

To find threats wherever they're hiding, Cofense Vision® stores, indexes, and enriches emails for faster querying and quarantine. How long does it typically take to search your email network? How many internal resources do you have to tap into to be able to do so? Does the mail team talk to the incident response team?

By utilizing playbooks you can automate your response, and Cofense Vision allows you to easily find the bad emails, dig deeper, and root out the whole phishing campaign.

One click allows you to quarantine emails across your entire email network such as Microsoft Exchange, Google, and Office365, then un-quarantine if further analysis proves an email to be harmless.

What's more, the auto-quarantine function of Cofense Vision helps to eliminate 'known' (previously seen and confirmed) threats, automatically removing them from your entire network the moment they arrive. This adds a vital layer of fast and efficient threat protection, mitigating any risk of your workforce engaging with confirmed threats.

05

AUTOMATE, YES. BUT WITH HUMAN CONTROL

While automation vastly improves efficiency, it doesn't erase the need for "eyes on." With the increasing use of AI in threat development, bad emails are not only increasingly more sophisticated at evading security controls, but also at being discernible from legitimate emails. Only humans have the contextual understanding to effectively identify and act against these emerging threats.

It's important to enable this human element throughout your layers of email security. Not only to enable your workforce to easily report suspected threats, but also so that security teams are able to effectively analyze and remediate the threats reported.

Cofense leaves the critical decision-making to human analysts. We give security teams access to vital and unique threat intelligence on clusters, complete with indicators of compromise (IOCs), so teams can apply the human touch as they respond decisively.

06

COMPLEMENT (AND IMPROVE) YOUR CURRENT ENVIRONMENT

When it comes to email threat response, your security program shouldn't be a drain or burden on your resources. It should enable your teams and empower them to act not only efficiently but proactively against threats.

Fortunately, the Cofense PDR Platform combines cutting-edge technology with battle-tested expertise to deliver consistent, race-winning results. It allows your teams to manage and respond to the onslaught of email threat alerts more effectively, with fewer man-hours and more accuracy.

The option of a fully managed service also allows you to deliver rapid incident response and effective email security for your organization 24/7, maximizing the team you have internally to focus on your organization's unique environment. The Cofense-managed PDR service gives you access to the skillset of a global team of forensic email threat experts, the Cofense Phishing Defense Center, enabling 24/7 protection and access to unique live global threat intelligence.

ABOUT COFENSE

Our solution is designed to allow your team to identify and mitigate cyber threats with maximum speed, increasing your organizational resilience and reinforcing your email security strategy.

Cofense provides the world's most effective business email threat detection and remediation solutions. The Cofense PhishMe® Email Security Awareness Training (SAT) Platform with Risk Validation and the Cofense Phishing Threat Detection and Response (PDR) Platform are powered by over 35 million Cofense-trained employees who report phishing and other dangerous email threats in real time. Exclusive to Cofense, our network detects and eradicates threats other email security systems miss and removes them from our customers' inboxes.

For more information, visit Cofense.com or connect with Cofense on X and LinkedIn.

To sign up for a live demo or to learn more, visit cofense.com.