6 KEYS TO FASTER PHISHING MITIGATION

How Cofense™ Optimizes Incident Response

COFENSE

COFENSE.COM

Another day, another e-book. The world goes round and round. But one thing hasn't changed:

PHISHING IS STILL THE #1 CYBER-ATTACK VECTOR

According to Verizon's most recent Data Breach Investigations Report, email remains the most common way to launch a cyber-attack, used in 96% of socially engineered attacks.[1] What's more, phishing and pretexting represent 93% of all socially engineered data breaches[2]. (Pretexting involves a false narrative designed to trick the user.) And successful phishing attacks on average cost mid-sized companies $1.6 million per incident.[3]

WHEN MALICIOUS EMAILS INVADE YOUR NETWORK, YOU NEED TO MITIGATE ASAP

When a malicious email evades your "next-gen" perimeter defenses, the hunt is on and the clock is ticking. Every minute adds to potential businesses losses. You need to triage the threat and get to mitigation fast.

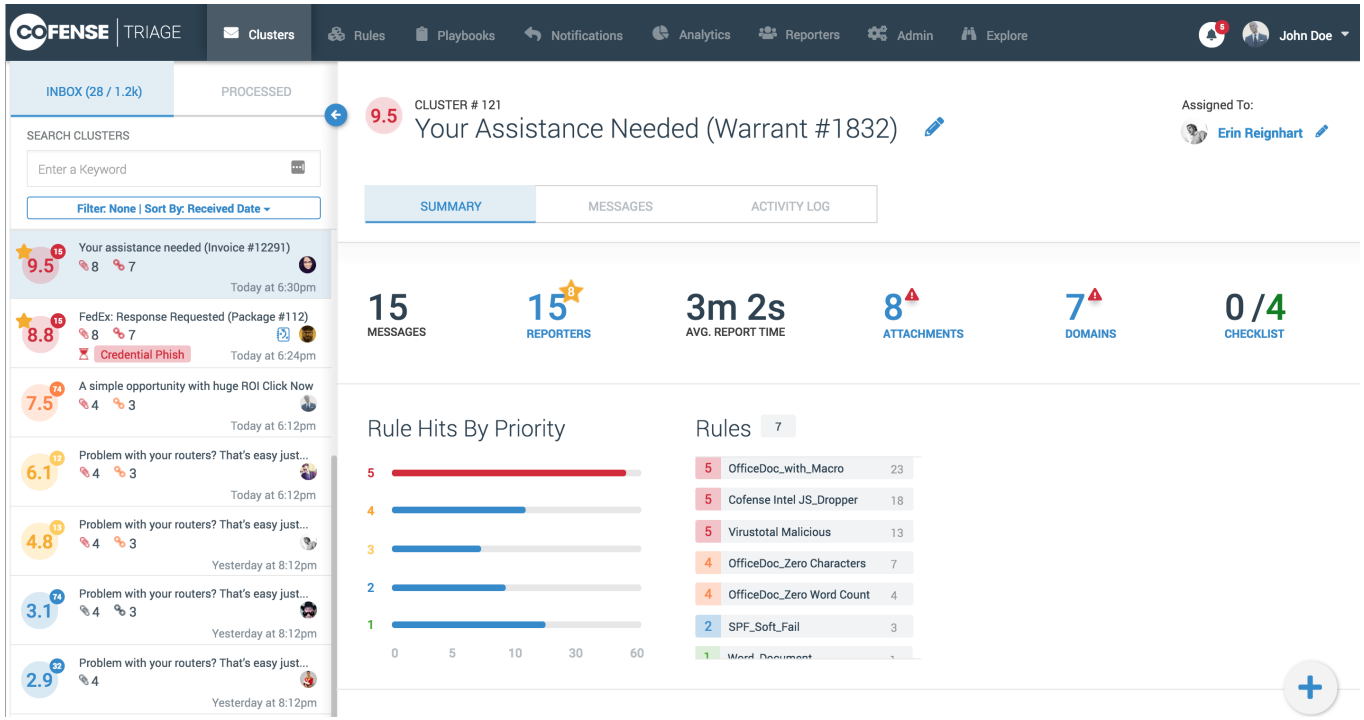
Cofense™ can help you do that. We're laser-focused on helping the world stop phishing attacks. In this e-book, we'll examine how Cofense adds the power of phishing Security Orchestration Automation and Response (SOAR) to Cofense Triage™ and Cofense Vision™, our comprehensive phishing incident response platform. You'll learn to accelerate your phishing triage and use fewer man hours. Following are 6 key elements.

#1. RESPOND TO EMAIL CLUSTERS, NOT EVERY SINGLE EMAIL

The 'A' in SOAR stands for automation. Cofense Triage streamlines phishing analysis by automatically clustering malicious emails by campaign.

Our platform finds key commonalities among reported emails. As these commonalities are discovered, Cofense Triage creates a cluster of reports. That cluster represents what could be a phishing campaign.

So, you treat an email cluster as a unit, instead of sorting through and trying to match every single message that may be related. When you're responding to phishing in volume, as most companies do, this is much, much faster than executing a response to this one, and this one, and this one... ad infinitum.



Once a cluster has been identified, the work of the analyst begins.

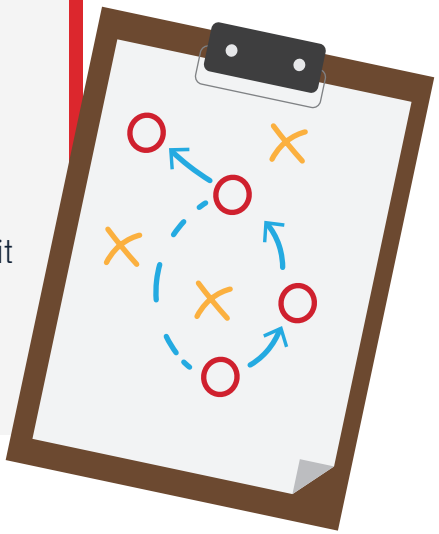
The analyst can look at the headers, along with the bodies of emails, and start to analyze what kind of threat a cluster is. Suspicious attachments can be sent to tools like Cuckoo, VirusTotal or Palo Alto Wildfire to determine if it contains malware. Threat Intelligence feeds like Cofense Intelligence™ can be consulted for additional analysis.

#2. FURTHER AUTOMATE WITH PLAYBOOKS

Once you identify a threat, you need to get ahead of it. Our platform uses playbooks to automate your response. A playbook is a set of repeatable tasks that can be automated to reduce the work of the analyst.

A Basic Example

- Based upon the contents of the cluster, the playbook starts by assigning a category to it
- Based upon the category, the playbook knows the type of threat the messages represent and creates a ticket in your help desk system
- Cofense Triage automates the analysis of a malicious URL or attachment
- It determines who else received a message in the cluster but did not report it
- The platform notifies the proxy team to block a URL or a domain
- And it sends a message to the employees who reported the messages



After you create a playbook, you can save it and reuse for other threats.

#3. ORCHESTRATE AND INVOLVE THE RIGHT TEAMS AT THE RIGHT TIME

Our out-of-the-box integrations enable analysts to work with all your existing security tools. This is the "orchestration" in SOAR. 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 Noise Reduction feature cuts through spam to free your people to collaborate on hunting genuine threats.

Just some of our integration partners:

View the full list.

#4. FIND AND QUARANTINE PHISHING EMAILS

Let's stop for a moment and review what happens when you respond to a phishing alert using Cofense Triage

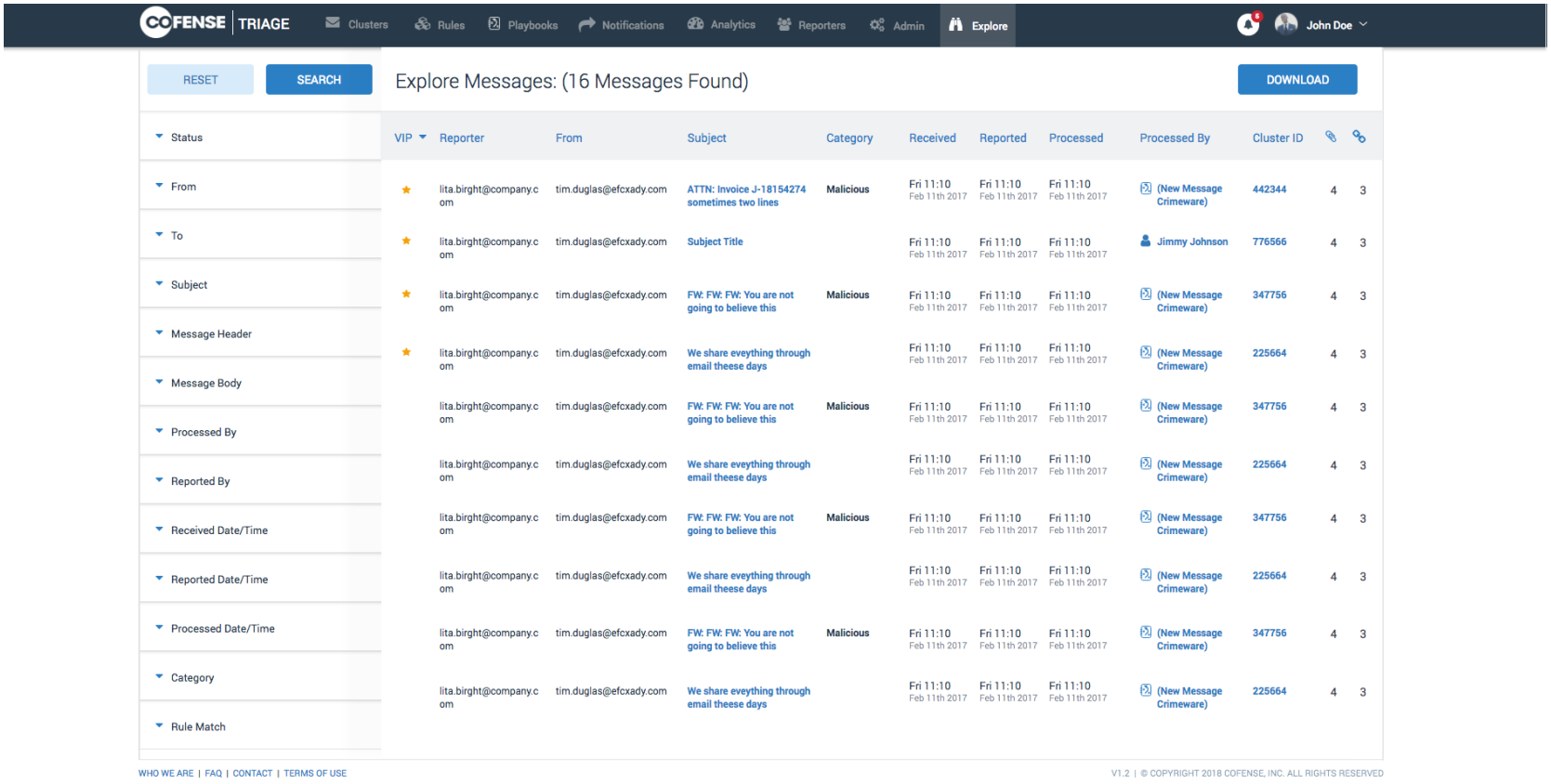
- A bad email makes it past the "next-gen" technology that should have caught it
- Your eagle-eyed workforce recognizes the threat and reports it
- Cofense Triage automates analysis and uses playbooks to prepare the response
- A security analyst kicks off the response

And he or she asks: "Where else does that email live on my servers? Uhhhh

ENTER COFENSE VISION™

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

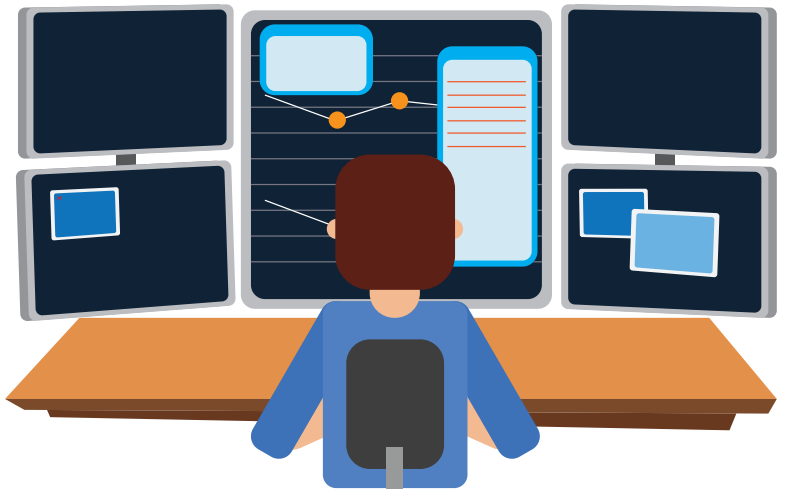
Cofense Vision allows you to easily find bad emails, dig deeper, and root out the whole phishing campaign. One click allows you to quarantine emails in Microsoft Exchange and Office365, then un-quarantine if further analysis proves an email to be harmless.



#5. AUTOMATE, YES. BUT WITH HUMAN CONTROL

While automation vastly improves efficiency, it doesn't erase the need for "eyes on glass." In a blog post titled "Security without Security People," Gartner Analyst Anton Chuvakin said, "If you think you can do security well without security people, you are deluded and probably breached, too. However, we need to really focus on making the available people work efficiently and effectively."[4]

As we continue to simplify phishing response by adding automation, Cofense leaves the critical decision-making to human analysts. We give security teams information on phishing clusters, complete with indications of compromise (IOC's), so teams can apply the human touch as they respond decisively.



#6. COMPLEMENT (AND IMPROVE) YOUR CURRENT SOAR ENVIRONMENT

When it comes to phishing response, Cofense Triage is more efficient than traditional SOAR platforms. You can respond to the tsunami of phishing alerts more effectively, with fewer man hours.

But let's be clear. A phishing-specific SOAR won't replace the need for a broader SOAR platform. Rather, it complements it by speeding response to threats from the #1 cyber-attack vector. Adding a quicker, smarter phishing response to your security stack gets you to mitigation, breach prevention, and peace of mind faster. Sometimes, 1 plus 1 adds up to 3.

LEARN MORE ABOUT COFENSE TRIAGE AND COFENSE VISION

So those are the ways Cofense helps mitigate phishing faster. But seeing is believing—view our platform for yourself.

Sign up for a live 1:1 demo now!

ABOUT COFENSE

Cofense™, formerly PhishMe®, is the leading provider of human-driven phishing defense solutions world-wide. Cofense delivers a collaborative approach to cybersecurity by enabling organization-wide engagement to active email threats. Our collective defense suite combines timely attack intelligence sourced from employees with best-in-class incident response technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organizations in defense, energy, financial services, healthcare and manufacturing sectors that understand how changing user behavior will improve security, aid incident response and reduce the risk of compromise. To learn more, visit https://cofense.com/.

SOURCES

1. Verizon Data Breach Investigations Report, 2018.
2. Ibid.
3. Vanson Bourne/Cloudmark, 2016.
4. Gartner Blog Network, 2017.