COFENSE

Intelligent Email Security

Powered by CROWDSOURCED INTELLIGENCE + MACHINE LEARNING

New PhishMe Client Kickoff

The Customer Experience

Agenda

- Introductions
- Customer Journey
- PhishMe Overview
- PhishMe Implementation
- Resources
- Q&A

Copyright © 2023, Cofense All Rights Reserved.

Introductions

Who we are & how we’ll work together

Introductions

Cofense Roles	Name	Email
Customer Experience Owner		
Account Executive		
Sales Engineer		

Customer Roles	Name	Email
Executive Sponsor		
Implementation Project Owner		
PhishMe Admin		
Reporter Admin		
Triage Admin		

Copyright © 2023, Cofense All Rights Reserved.

Customer Journey

Let’s talk next steps

Kickoff

Introduction call with Customer Experience representative to discuss business objectives and goals for success.

Implementation

Cofense guides you through the implementation and configuration of PhishMe features and development of a phishing defense program plan to include phishing simulation and awareness resources.

QA

Final implementation QA and conclusion, support procedures are outlined, and PhishMe is confirmed production-ready.

Reporting

Customer Experience representative will monitor progress, measure and drive program success through scenario reporting, and ensure customer is seeing value in the product.

Growth

Share success stories with Executive leadership. Follow up with end users for continuous engagement throughout the program.

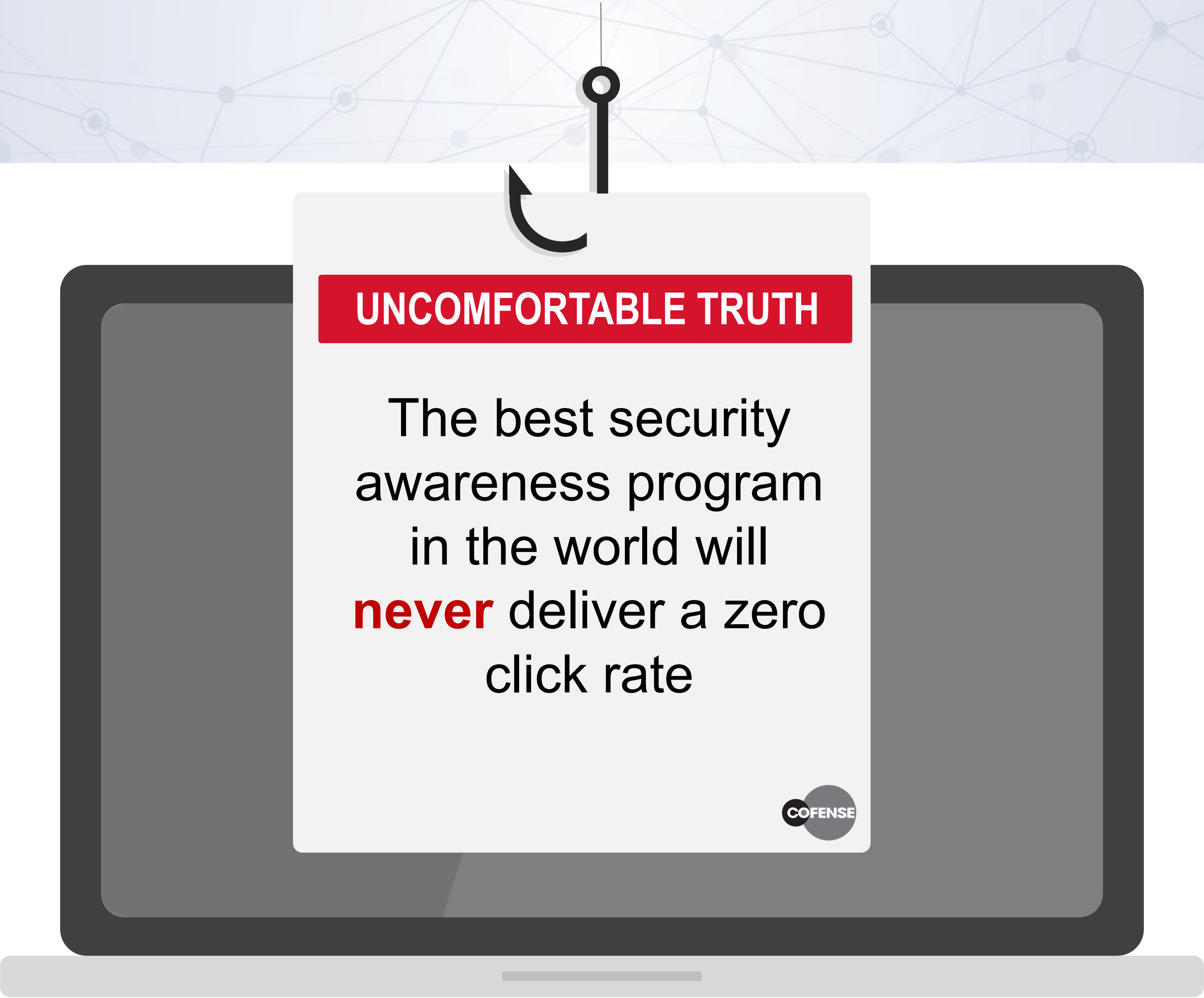
Review/Renewal

Continuously mature your phishing defense program and build resiliency to phishing threats for the business to reduce their risk of breach.

Copyright © 2023, Cofense All Rights Reserved.

PhishMe Overview

Getting to know the product

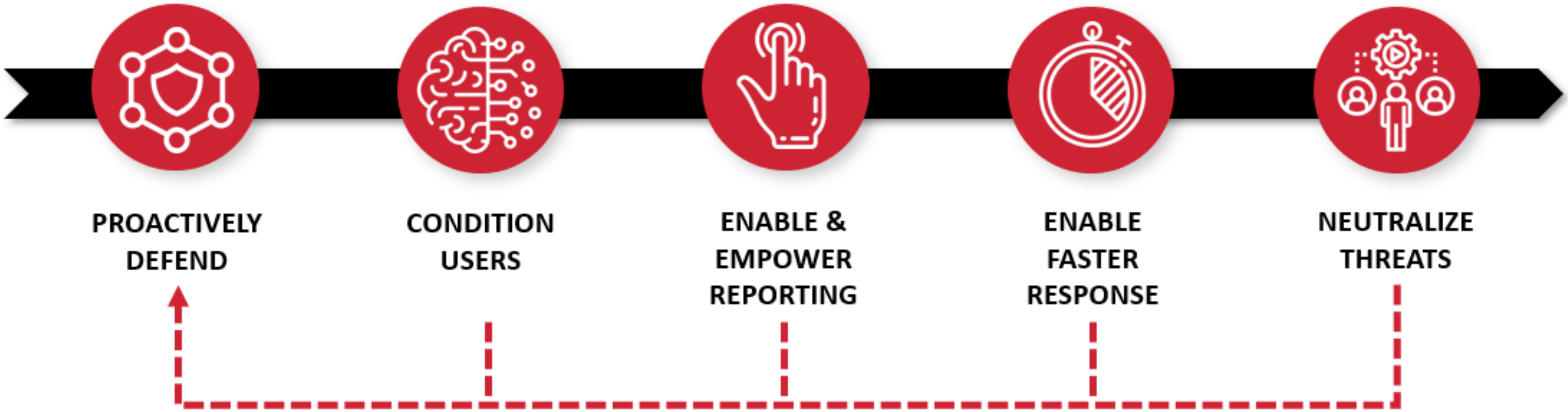


UNCOMFORTABLE TRUTH

The best security awareness program in the world will **never** deliver a zero click rate

Copyright © 2023, Cofense All Rights Reserved.

End to End Phishing Defense



PROACTIVELY DEFEND

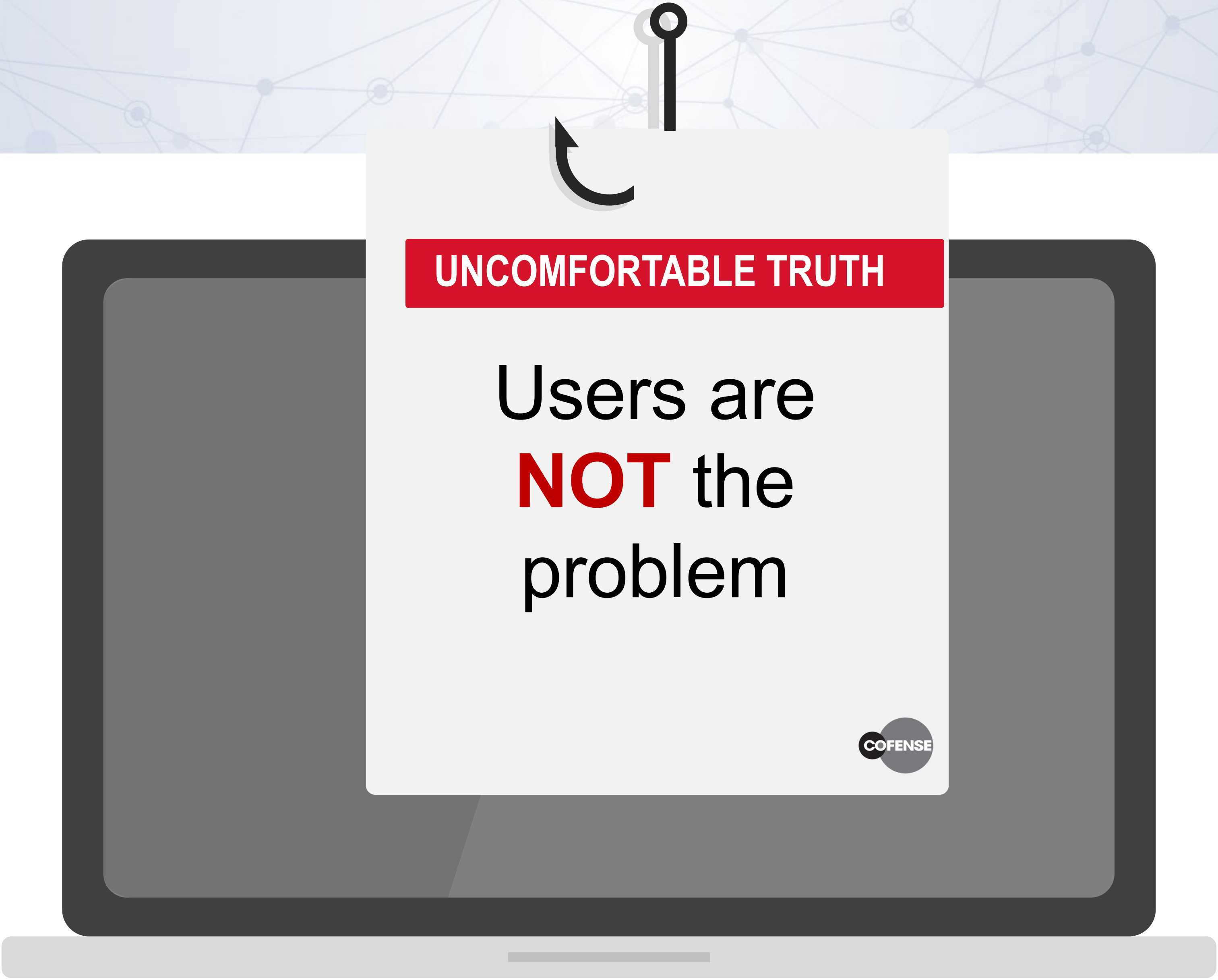
CONDITION USERS

ENABLE & EMPOWER REPORTING

ENABLE FASTER RESPONSE

NEUTRALIZE THREATS

Copyright © 2023, Cofense All Rights Reserved.



UNCOMFORTABLE TRUTH

Users are **NOT** the problem

Copyright © 2023, Cofense All Rights Reserved.

Phishing Defense Program Goals & Best Practices

Goals:

1 Change user behavior to make your organization more resilient to phishing.

2 Condition end users to report suspicious emails to mitigate organizational risk of breach.

Best Practices:

1 Announce the phishing defense program to all users in advance.

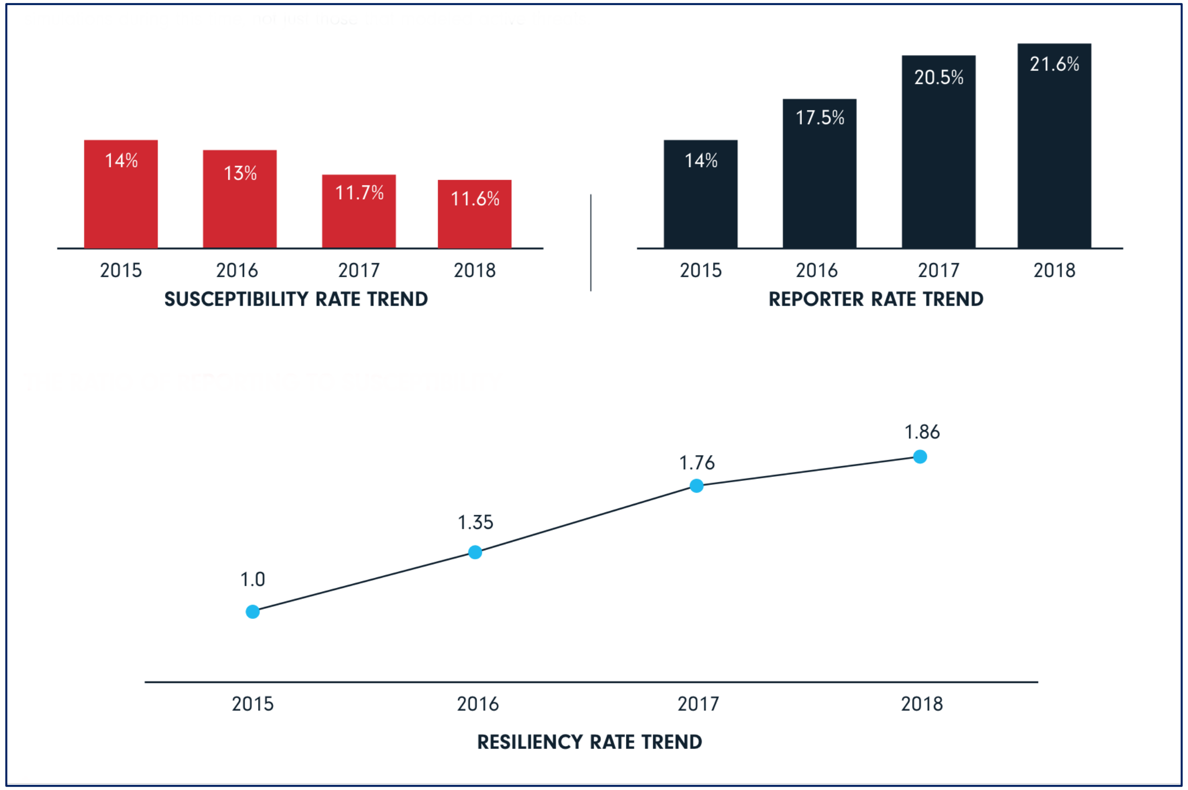
2 Build a program plan so **all** users are exposed to training exercises

3 Infuse current threat intelligence to expose users to real-world threats.

4 Baseline, benchmark and retest. Share program successes and recognize your reporters.

Copyright © 2023, Cofense All Rights Reserved.

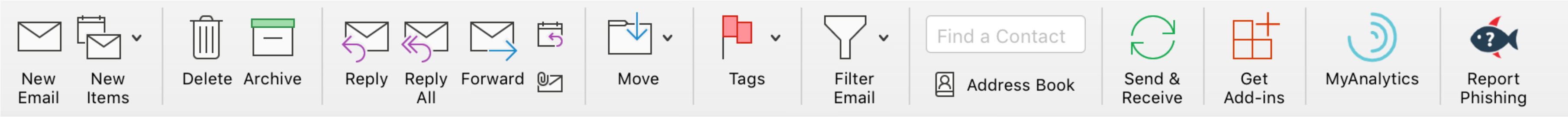
Resiliency – Metrics that Matter



- Resiliency is the ratio of the number of users whose only action was to report the simulation email / the number of users who fell susceptible to the simulation.
- When resiliency is greater than 1.00, there is a high probability that the attack will have been mitigated before your business was compromised.

Copyright © 2023, Cofense All Rights Reserved.

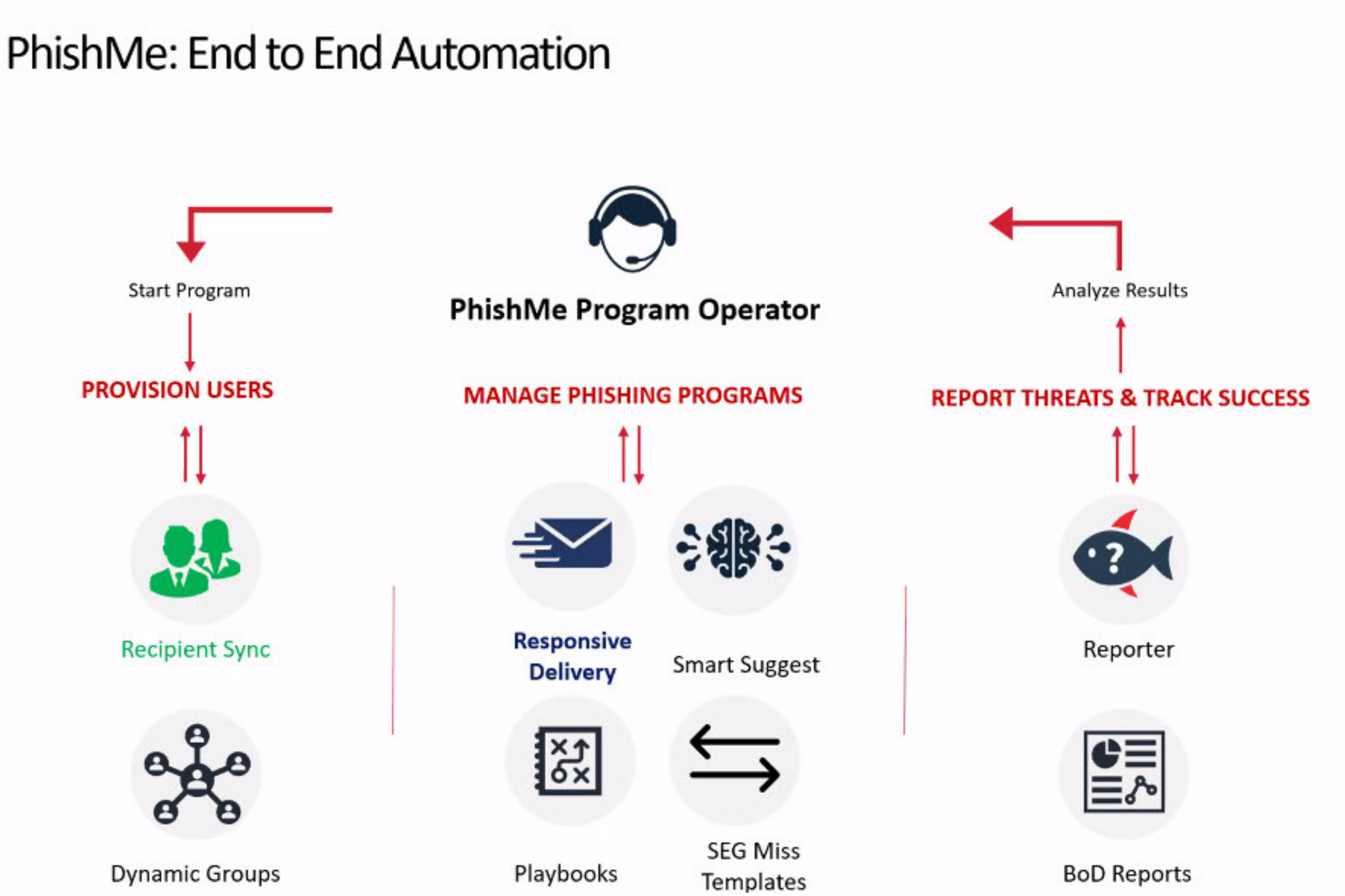
Cofense Reporter



- **Standardize** and **Organize** user reporting
- **Detect** and **Respond** to email-based threats faster
- **Minimize** impact of breaches with proactive response and improved visibility
- **Customize** user feedback to encourage employee reporting
- **Analyze** URL and malware attachments using third-party integrations
- **Desktop** and **Mobile** compatibility

Copyright © 2023, Cofense All Rights Reserved.

Program Success Through Automation



PhishMe: End to End Automation

Copyright © 2023, Cofense All Rights Reserved.

Recipient Sync

Recipient Sync

✓

Automatically sync user information to your account

Dynamic Groups

✓

Define a set of criteria to dynamically group email recipients

Copyright © 2023, Cofense All Rights Reserved.

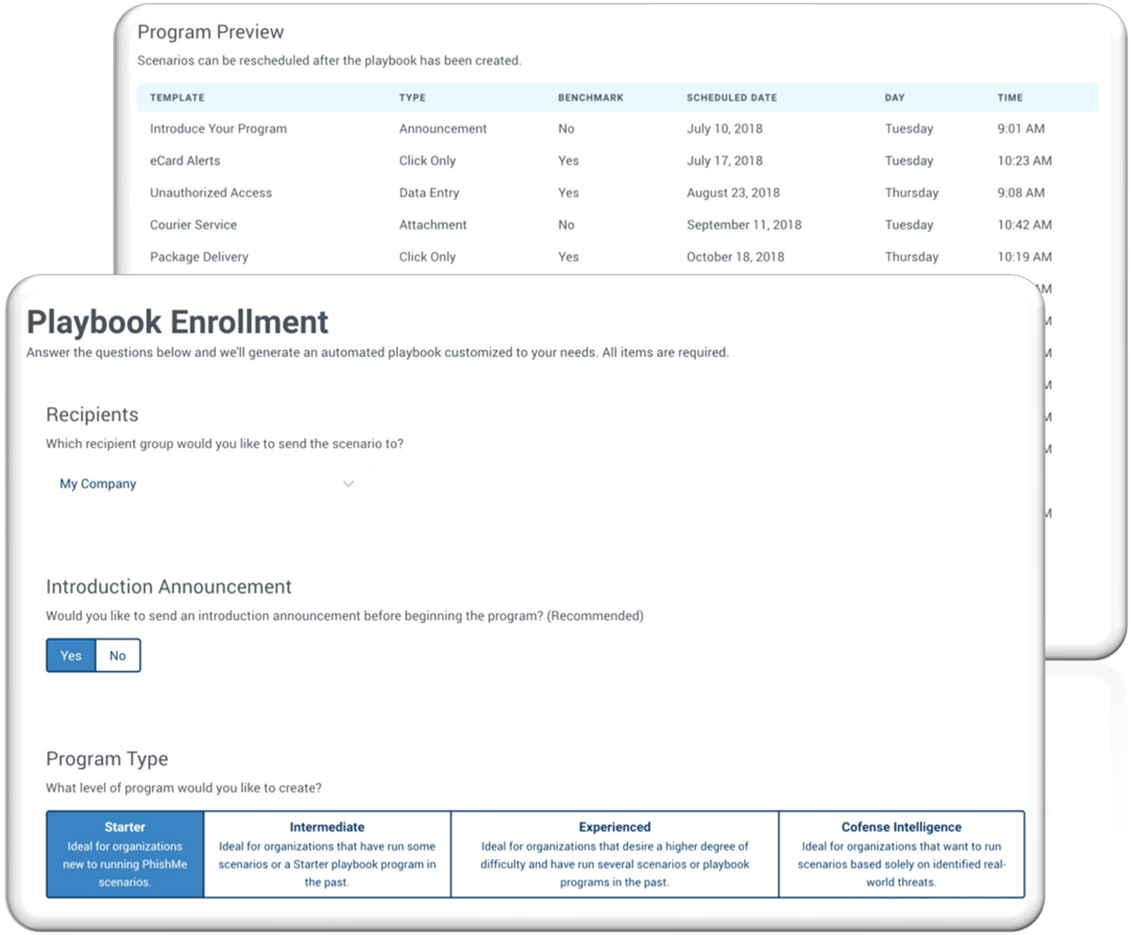
Responsive Delivery

- Eliminate time-zone and global scenario scheduling restrictions
- Eliminate technical complications
- Ensure simulation delivery only when users are <u>**active**</u> in their email client
- Flexible, efficient scenario delivery
- Simple, easy setup
- Mobile, tablet, and desktop application compatibility

Copyright © 2023, Cofense All Rights Reserved.

Playbooks

- Automated scenario selection and scheduling
- Scheduled reminders before scenarios run
- Great for clients new to phishing simulations
- “Set and forget” capability



Program Preview

Scenarios can be rescheduled after the playbook has been created.

TEMPLATE	TYPE	BENCHMARK	SCHEDULED DATE	DAY	TIME
Introduce Your Program	Announcement	No	July 10, 2018	Tuesday	9:01 AM
eCard Alerts	Click Only	Yes	July 17, 2018	Tuesday	10:23 AM
Unauthorized Access	Data Entry	Yes	August 23, 2018	Thursday	9:08 AM
Courier Service	Attachment	No	September 11, 2018	Tuesday	10:42 AM
Package Delivery	Click Only	Yes	October 18, 2018	Thursday	10:19 AM

Playbook Enrollment

Answer the questions below and we'll generate an automated playbook customized to your needs. All items are required.

Recipients

Which recipient group would you like to send the scenario to?

My Company

Introduction Announcement

Would you like to send an introduction announcement before beginning the program? (Recommended)

[✓ Yes] No

Program Type

What level of program would you like to create?

[✓ **Starter** Ideal for organizations new to running PhishMe scenarios.]	**Intermediate** Ideal for organizations that have run some scenarios or a Starter playbook program in the past.	**Experienced** Ideal for organizations that desire a higher degree of difficulty and have run several scenarios or playbook programs in the past.	**Cofense Intelligence** Ideal for organizations that want to run scenarios based solely on identified real-world threats.

Copyright © 2023, Cofense All Rights Reserved.

Integrated Learning

PhishMe’s Integrated Learning allows customers to enroll recipients into training courses for additional education

- One solution to manage both simulations and training
- Manage a single recipient list
- Select from a variety of courses and languages
- Multi-level reporting insights

Copyright © 2023, Cofense All Rights Reserved.

PhishMe Implementation

Achieving positive business outcomes

Implementation

- Conduct kickoff meeting and PhishMe overview
- Understand customer business objectives and goals
- Review agenda and timeline of deployment
- Customer should identify and engage technical resources and encourage stakeholder participation

Training & Program Planning

- PhishMe navigational walk-through
- PhishMe training
- Program planning
- Reporter deployment
- Ensure IPs are allowed through the gateway
- PhishMe feature adoption
- Discuss reporting options

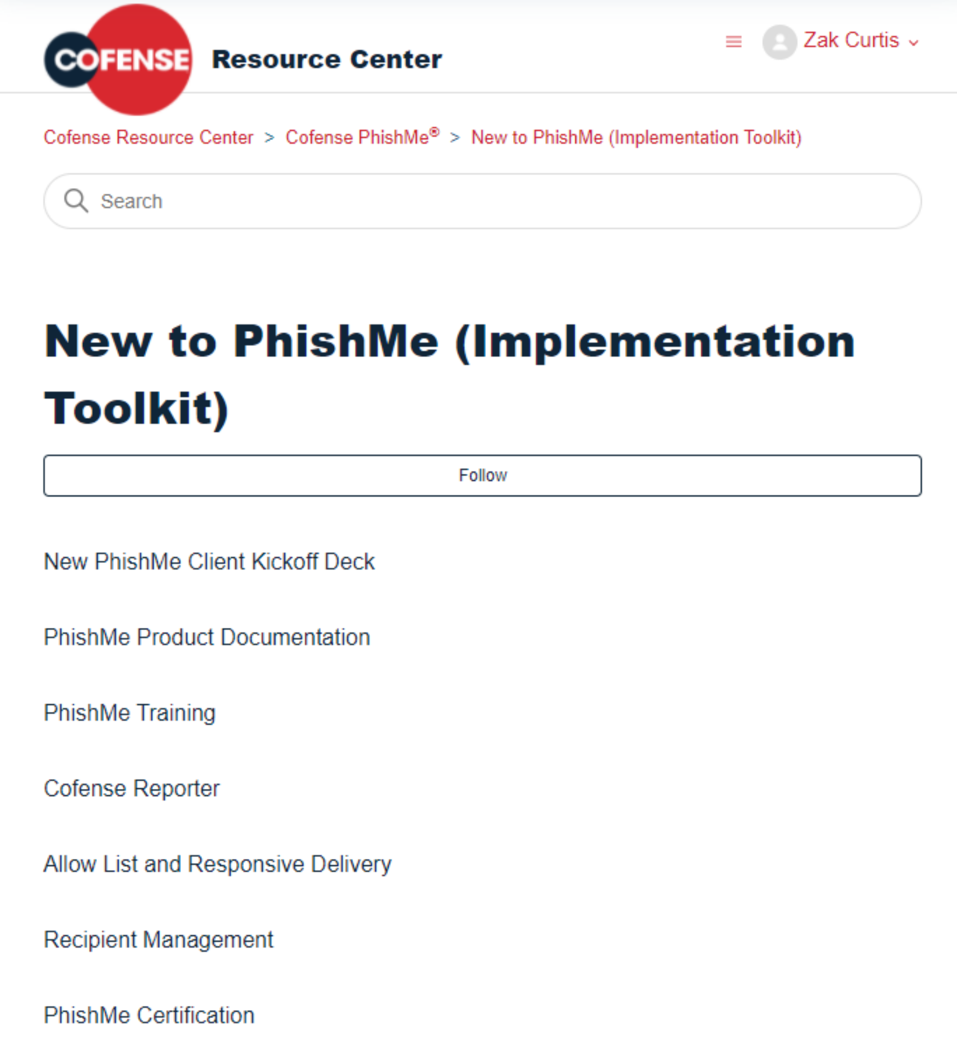
QA & Production

- Ensure successful simulation email delivery
- Outline support procedures and confirm production-ready

Copyright © 2023, Cofense All Rights Reserved.

Resources

New PhishMe Client Toolkit



Cofense Resource Center > Cofense PhishMe® > New to PhishMe (Implementation Toolkit)

Search

New to PhishMe (Implementation Toolkit)

Follow

New PhishMe Client Kickoff Deck

PhishMe Product Documentation

PhishMe Training

Cofense Reporter

Allow List and Responsive Delivery

Recipient Management

PhishMe Certification

Register for the Cofense Resource Center for on-demand implementation resources!

Register for the Cofense PhishMe Navigational Tour Training Workshop!

Copyright © 2023, Cofense All Rights Reserved.

Q&A