KB4-CON

Get in Position to Disposition

(what the heck is PhishER and how it works)

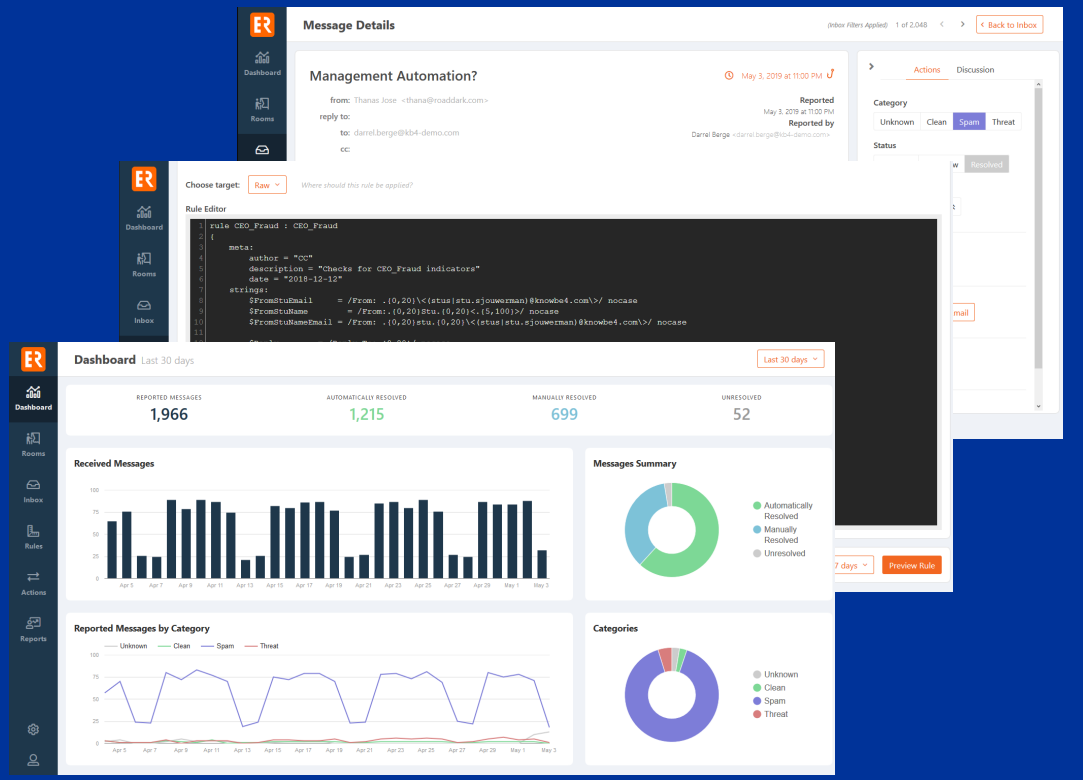
Greg Kras, Chief Product Officer

Chris Cline, Product Manager

KnowBe4

KnowBe4

PhishER



What is PhishER

- New product made available on Dec 17th 2018.
- A hosted platform which helps you identify and respond to user-reported messages.
- Helps you differentiate between the threats and the benign messages - quickly.
- Rules and Actions allow you to categorize messages and automate responses.
- Simply put, it saves time.

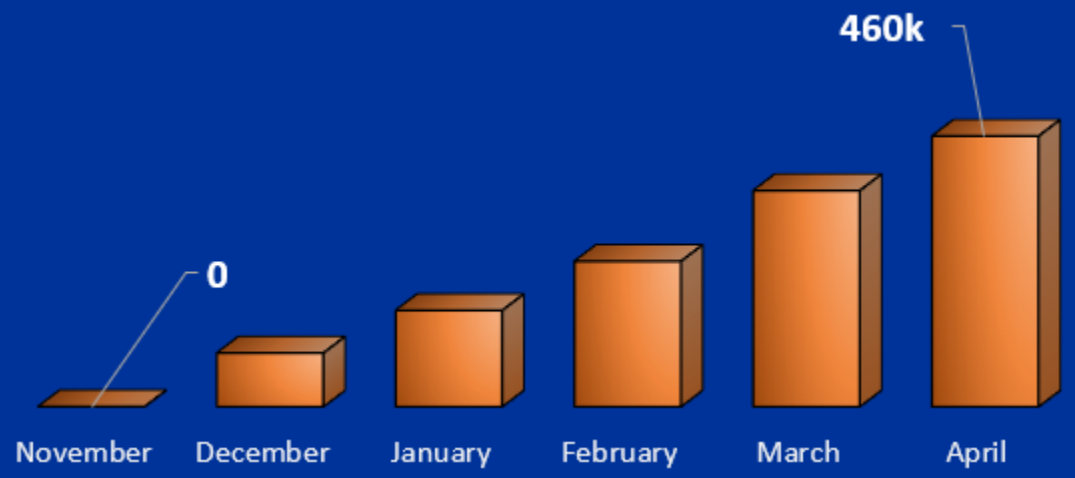
KnowBe4

PhishER

How does PhishER work?

1. Users report an email via the Phish Alert Button (PAB) or forward an email to unique address.
2. PhishER receives the message and prepares it for processing and analysis.
3. Rules run over the messages and enrich the information about the messages in the form of tags.
4. Automated actions trigger based upon criteria such as tags.

PhishER



PhishER stats so far

- 460k PhishER reporters
- 500 PhishER accounts
- 1.5 million emails since launch
  - Tens of thousands every day, and growing quickly
- 1 million YARA rules matched
- .5 million actions run

KnowBe4

PhishER

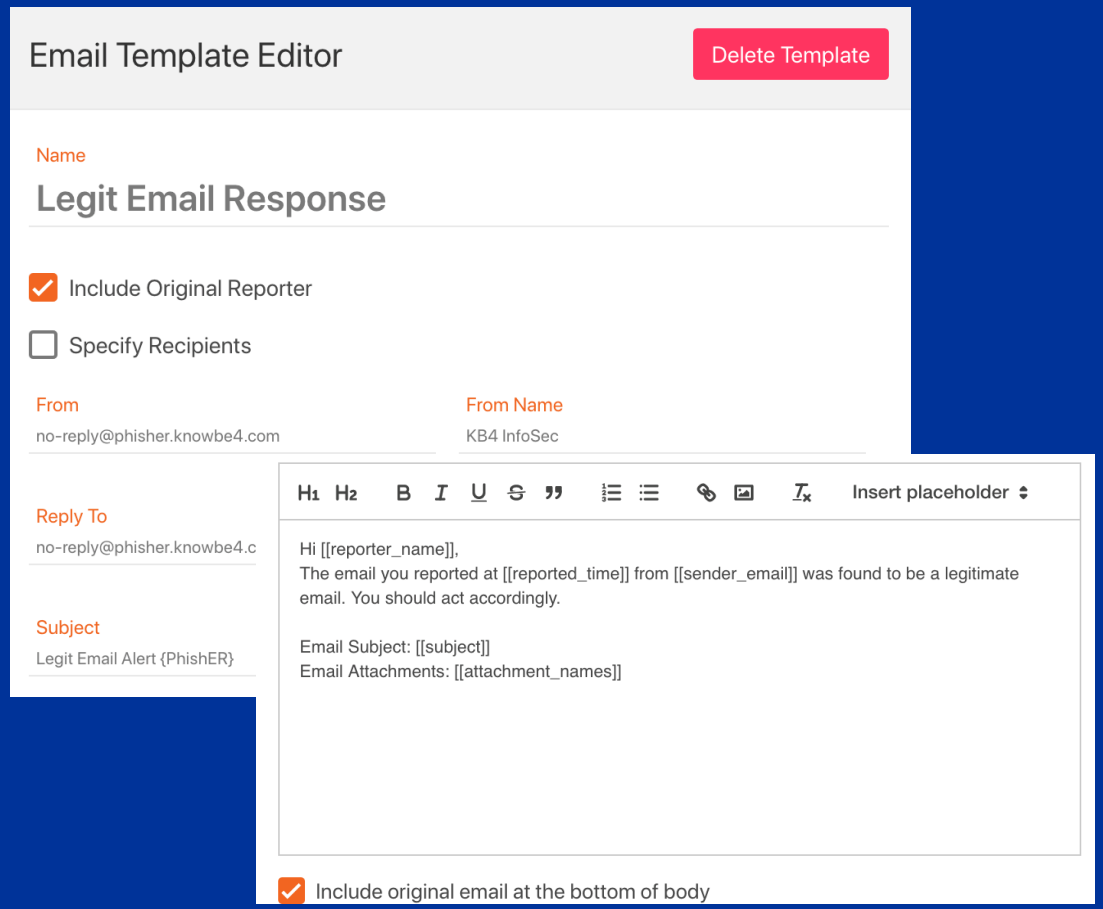
(these are all the master updates since launch)

Improvements since launch

- ~1000 merges to master branch
- Constant enhancements (and fixes)
  - Data retention policies
  - Bulk tagging
  - Quick filtering
  - Quick actions
  - Message history
  - Email Templates
  - YARA rule preview
  - Dozens of minor enhancements

KnowBe4

PhishER



Better Responses

- Email Templates

As people began to use PhishER it became obvious that admins wanted to send a lot of emails from the platform.

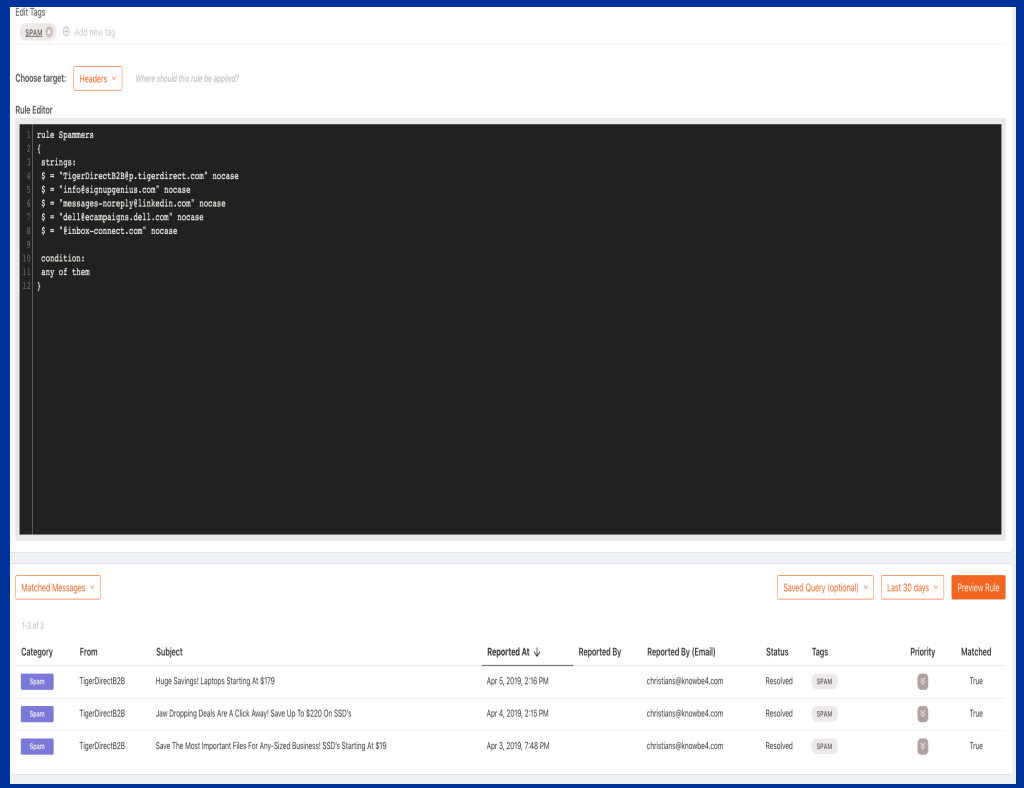
- Placeholders

Email Template Editor allows you to insert placeholders to help personalize and legitimize emails sent from PhishER.

These emails are being used to acknowledge the users reporting messages, alter them to final disposition, and create escalation chains within organizations.

KnowBe4

PhishER



Better Workflows

- Rules Preview
- QuickActions
- Live Updates

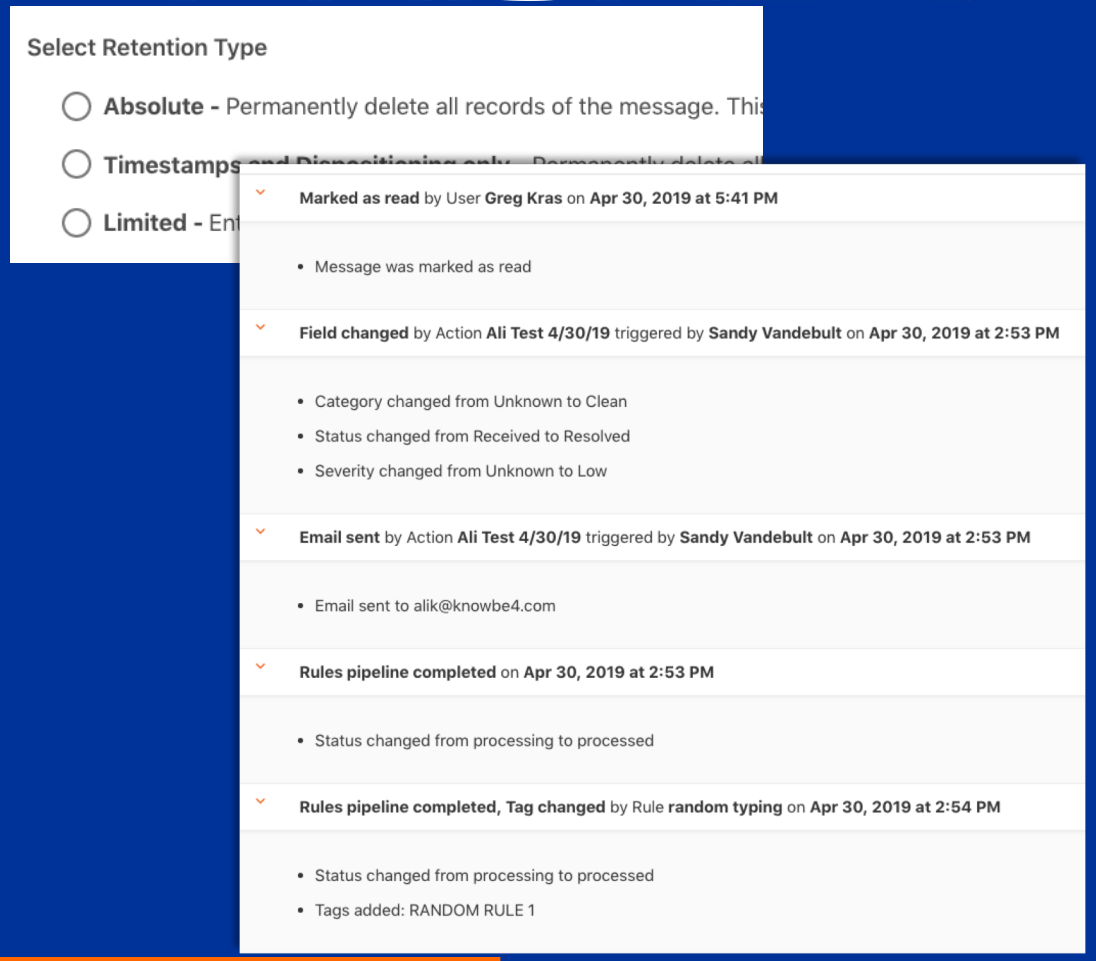
YARA is powerful but can be complex. Rules Preview allows you to verify that the Rule you've spent time building actually matches the expected messages before releasing it to the wild.

Some organizations want fine controls and others employ rougher dispositioning. With QuickActions, you can fire the actions you need faster.

Live Updates are easy! Who wants to refresh?

KnowBe4

PhishER



Better Auditing

- Data Retention

Sometimes it's more important NOT to have data. Depending on how sensitive your data is, you can select anything from a limited obfuscation up to permanent and complete deletion.

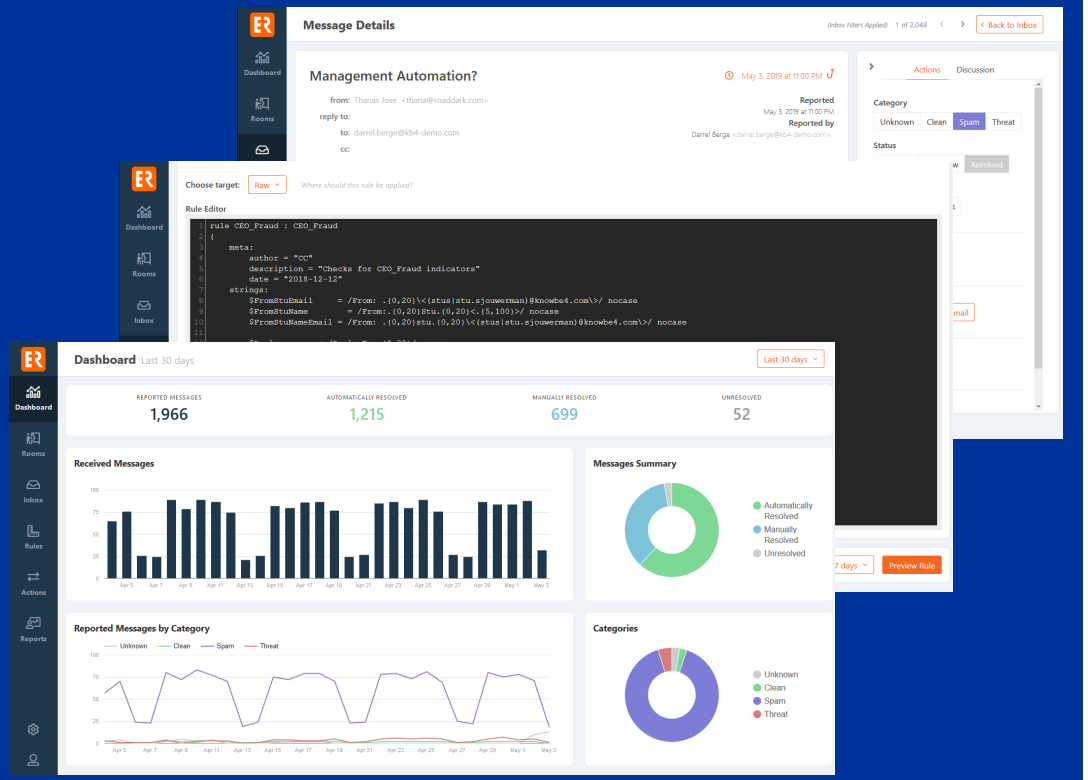
- Message History

Auditing is a big deal for most organizations.

Now everything that happens to a message is timestamped. You can see who did what when.

KnowBe4

PhishER

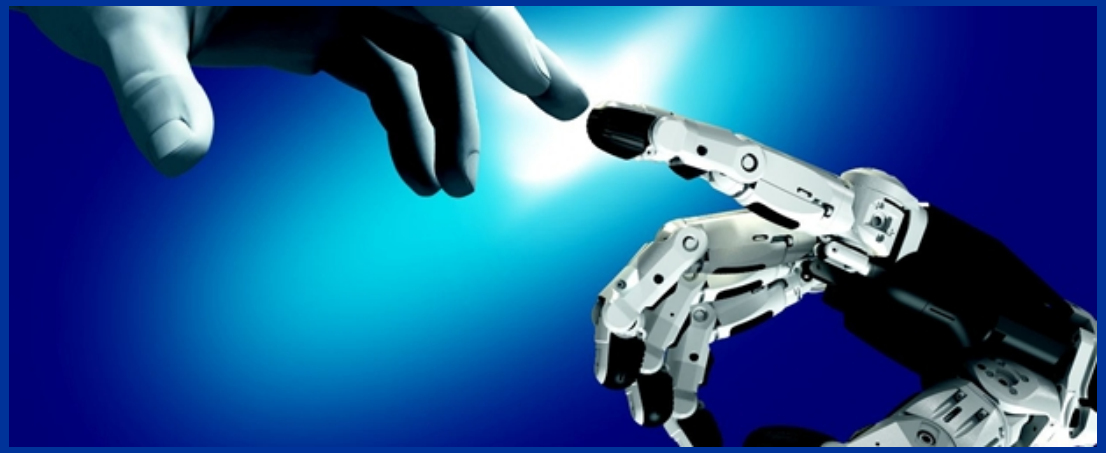


Let's do a demo

Launch it!

KnowBe4

PhishER



Right Around the Corner

- VirusTotal hash scans automated

-- The PhishER pipeline is important to keep speedy. A slow pipeline means that potentially dangerous messages stay in your IR inbox longer.

-- Sending just the hash to VT will allow us to push this back to an automated task during the pipeline.

- Apply rules on existing messages

--Sometimes it takes a few iterations to get your YARA *just right*. With the Rule Replay function you'll be able to keep your data clean for longer term reporting.

PhishER

Q&A

Closing / Q & A

Make sure you come to Lifting the Veil Tomorrow at 2:30-3:15p at SABAL

Visit us in the labs if you want to get into more detail

And with that, we'd like to open up the floor for Q&A

KnowBe4

Thank You!

KnowBe4

KnowBe4