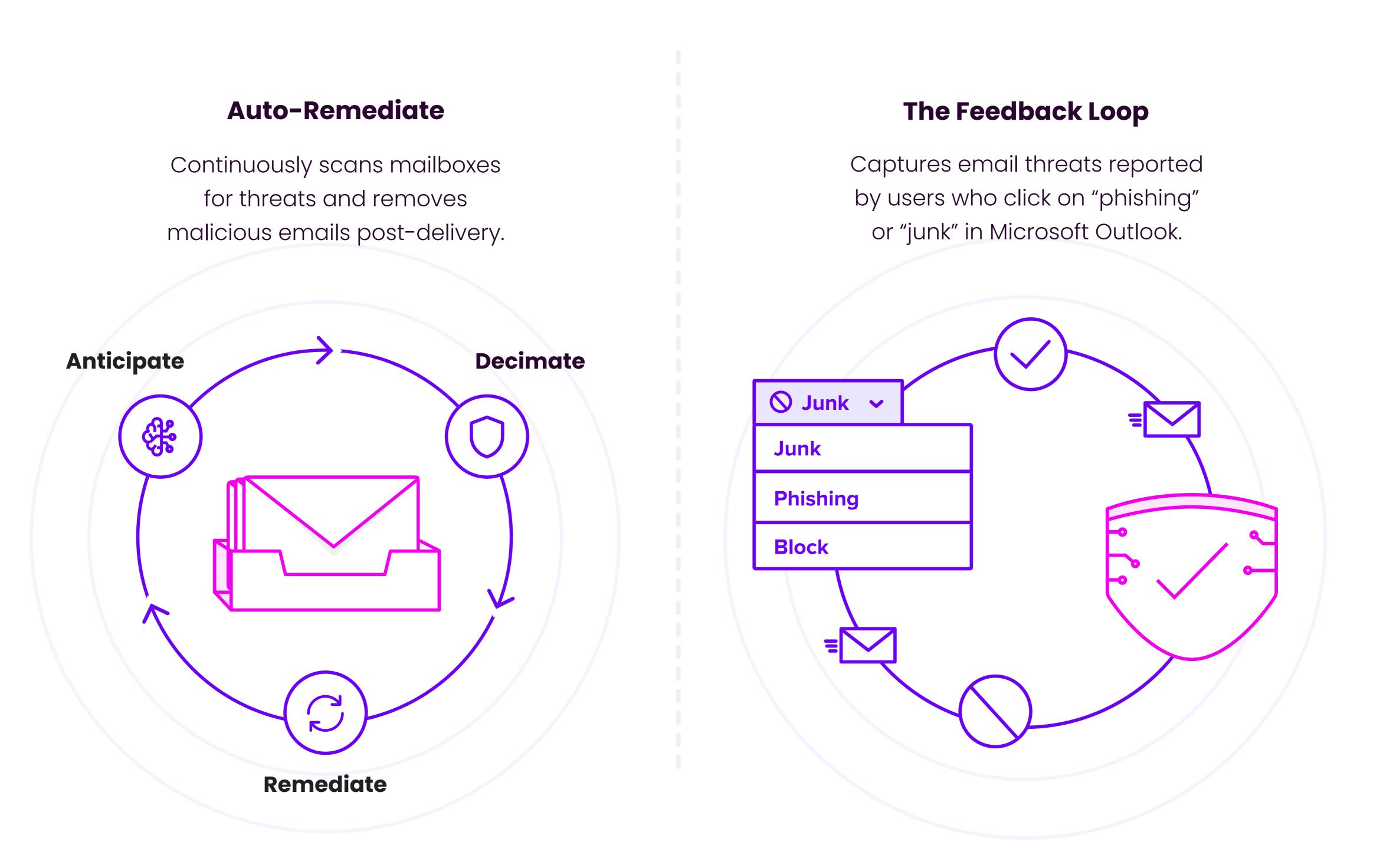




An integrated feature of Vade for M365, Vade Threat Coach delivers automated phishing awareness training to users who engage with phishing emails. Personalized at the user level, Threat Coach training features real phishing samples, contextualized by brand and delivered at the moment of need.

Vade Threat Coach is powered by two integrated tools that combine artificial intelligence and user feedback reports.



How does Vade Threat Coach work?

Unlike most phishing awareness training platforms that feature generic templates and simulations, Threat Coach training is personalized at the user level.

•••		
	To: update@sharepoint.ms	
	Subject: Notification - Review Doc	
	You have received a new shared document on OneDrive and it is said to b	pe important
	Click here	
	Your document is ready	
	ConeDrive	
	Concorrive for Business	



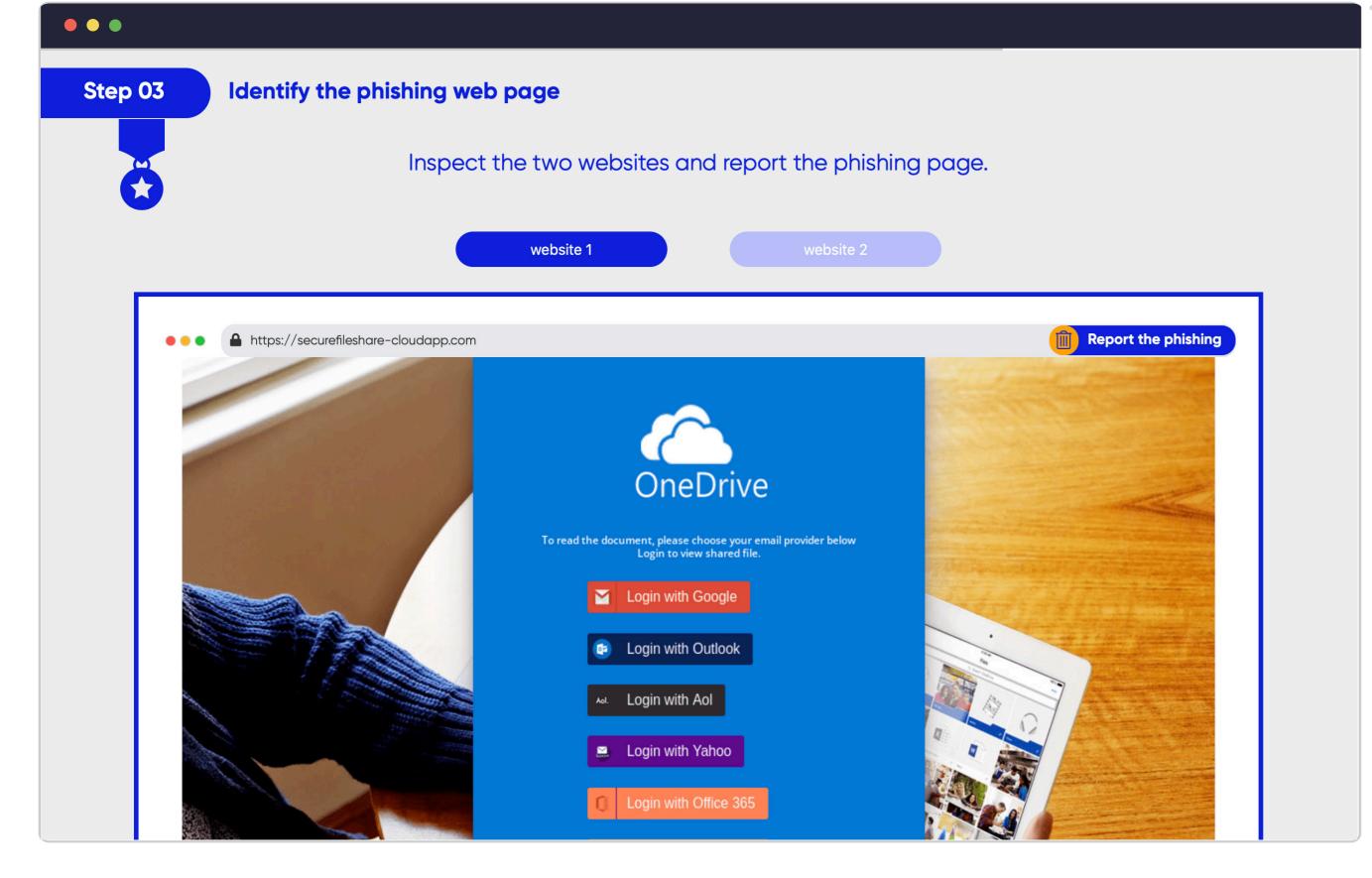


If Auto-Remediate detects a phishing email, any user who engaged with the email prior to remediation is alerted and invited via email to complete Threat Coach training. Unlike periodic training, this on-the-fly approach catches users at the moment of need.

Shelley Black <shelleymblack@yahoo.com></shelleymblack@yahoo.com>		Select the phishing email and repo	ort it!
Shelley Black <shelleymblack@yahoo.com> Me DocuSigne Your Signed Document VIEW DOCUMENT</shelleymblack@yahoo.com>		Email 1 Email 2	2
S 13.37 Me DocuSion: Vur Signed Document VIEW DOCUMENT	Completed Business_Pdf docume	nt Received	Report the phishing
Your Signed Document	S 13:37	.com>	<¬ <¬
	Docu <i>Sign</i>		
		Your Signed Document	
Microsoft OneDrive		VIEW DOCUMENT	
		Microsoft OneDrive	



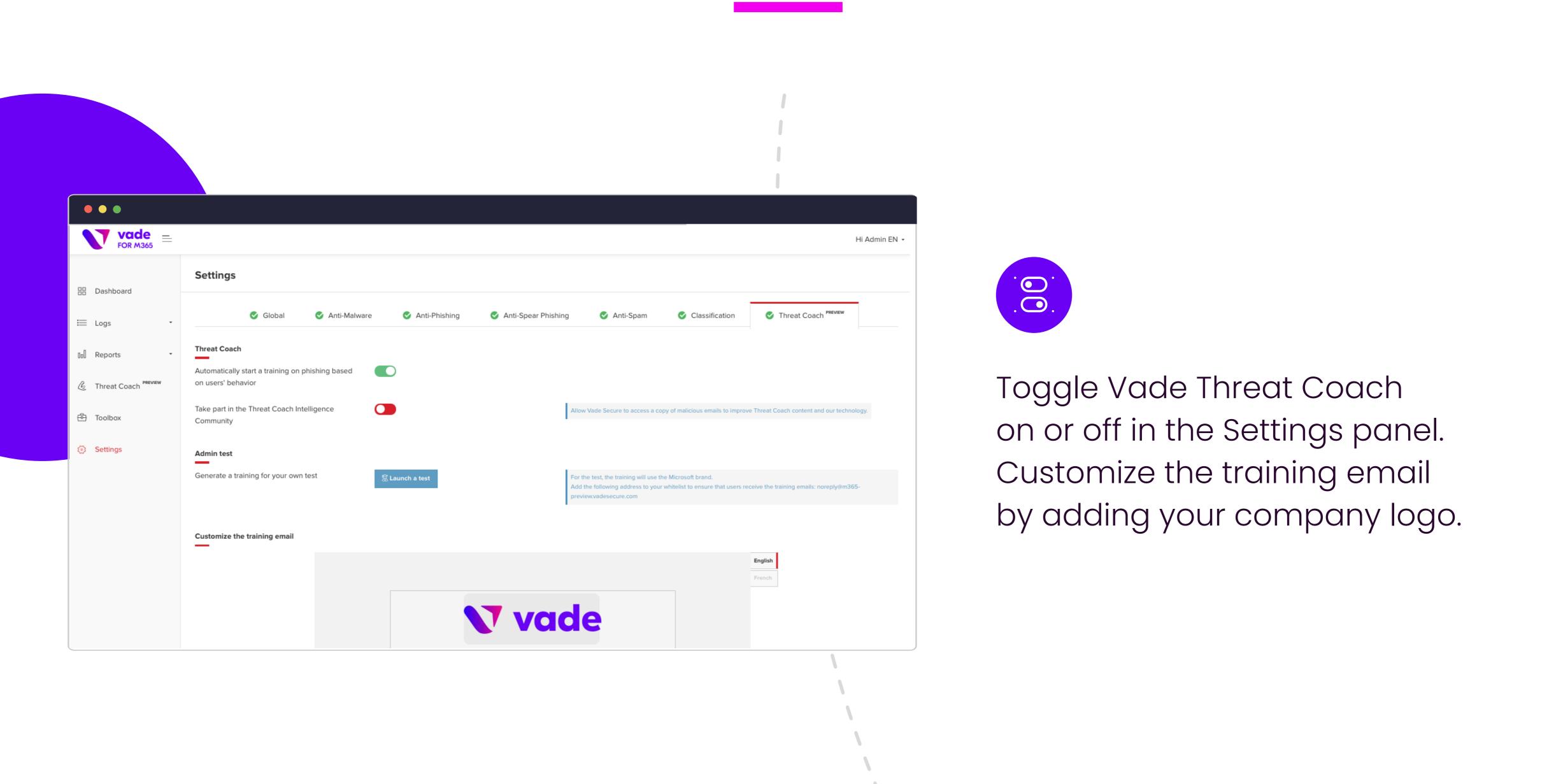
Users test their phishing awareness by taking a brief interactive quiz. It features real phishing emails and webpages captured by Auto-Remediate and the Feedback Loop.



Unlike generic templates and simulations, training content is contextualized by brand. For example, if the user clicked on a Microsoft phishing email, training samples will feature Microsoft phishing.

New phishing samples are continuously captured by Auto-Remediate and the Feedback Loop to train users on the latest phishing threats and techniques.

How do I manage Vade Threat Coach?





View details of all campaigns and trainings from the Threat Coach dashboard. Here, you can see the brands represented in trainings and users who failed training.

•••								
FOR M365 =								Hi Admin EN 👻
🗄 Dashboard	Threat Coach							忆 Launch campaign
E Logs .	Overview							7 DAYS 30 DAYS
Reports •	8 Campaigns i	8 Trainings (i)		5 Started (i)	62.5 % 4 Compl	leted (i)	50 % 3	37.5 % i
🖻 Toolbox	Recent campaigns							Export to CSV
Settings	DATE & TIME	BRAND	ТҮРЕ	TRAININGS	STARTED	COMPLETED	FAILED	DETAILS
	04/08/2021 6:23 AM	Microsoft	Admin	1	1	1	1	000
	04/07/2021 2:21 AM	Microsoft	Admin	1	1	0	0	000

Time-of-Click

Time-of-Click

Time-of-Click

 \ll

1

Microsoft

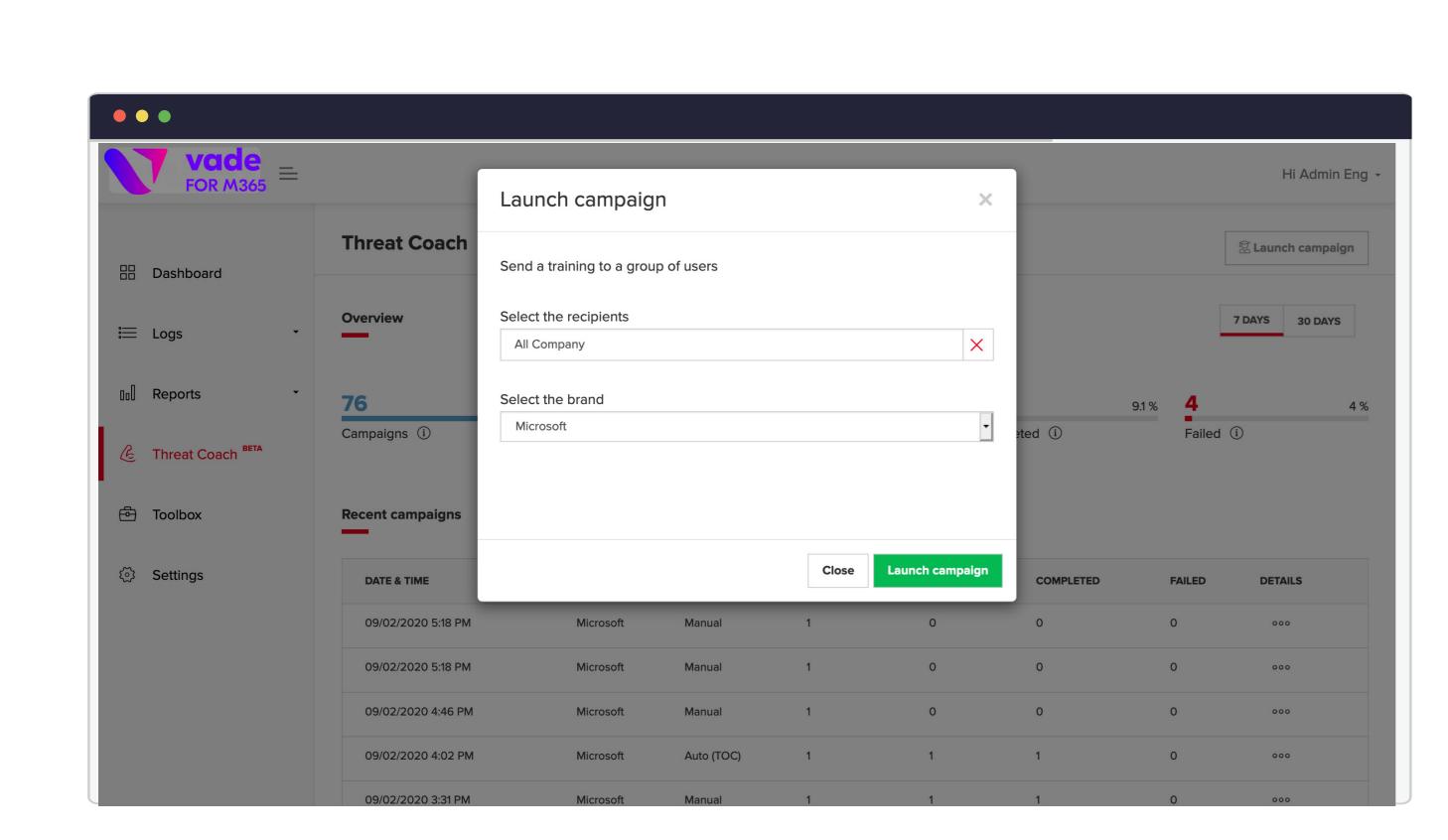
Microsoft

Microsoft

04/06/2021 3:50 PM

04/06/2021 1:19 PM

04/06/2021 12:24 PM



Manually send a campaign to at-risk users or users who fail training by clicking "Launch campaign" from the Threat Coach dashboard. Select a brand from the dropdown list to choose a brand for the training.

0

0

0

0

0

0

0

000

000

Fully automated, on-the-fly phishing awareness training.

No templates. No scheduled trainings. No complex setup or configurations.

