

ARE YOU READY FOR YOUR NEXT ATTACK?





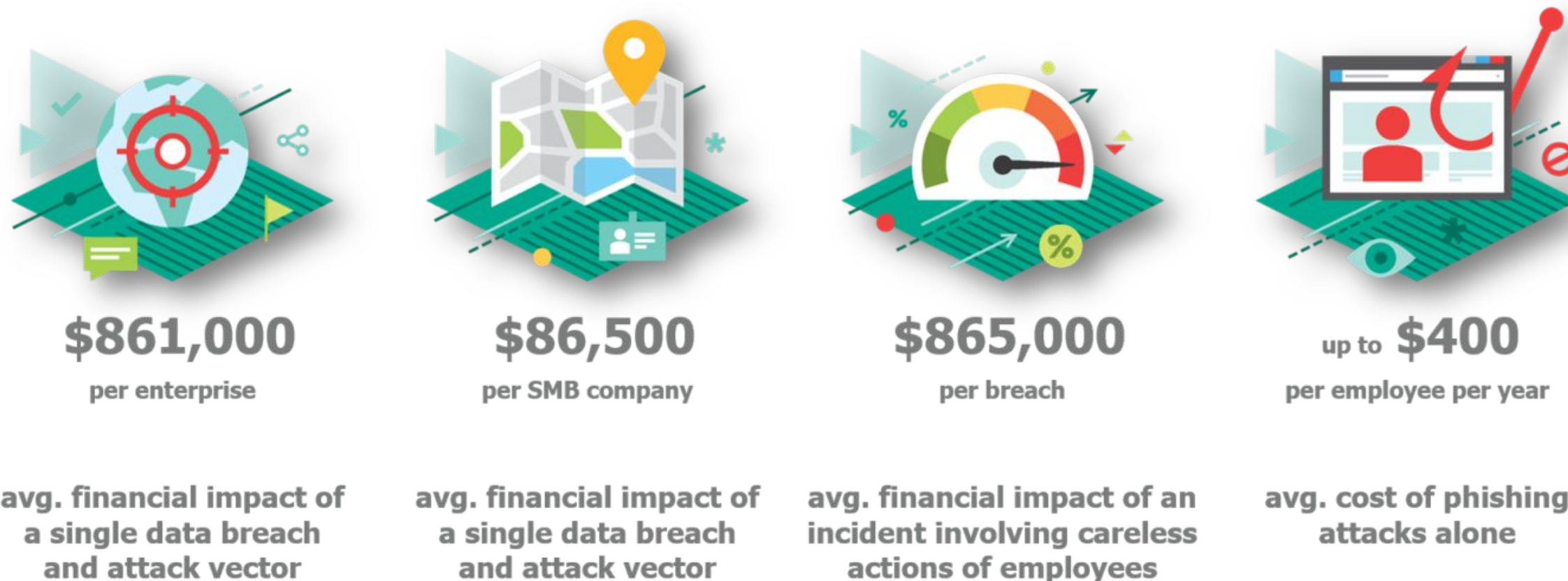
INCREASE AWARENESS AND
MINIMIZE YOUR EXPOSURE TO
CYBERATTACKS.

CYBER ATTACKS PRICE TAG

Cybersecurity awareness is more critical than you think.

Cyber incidents can come with a hefty price tag. If you're struggling to allocate a budget to cybersecurity training, tools or talent, you should think about it through risk management.

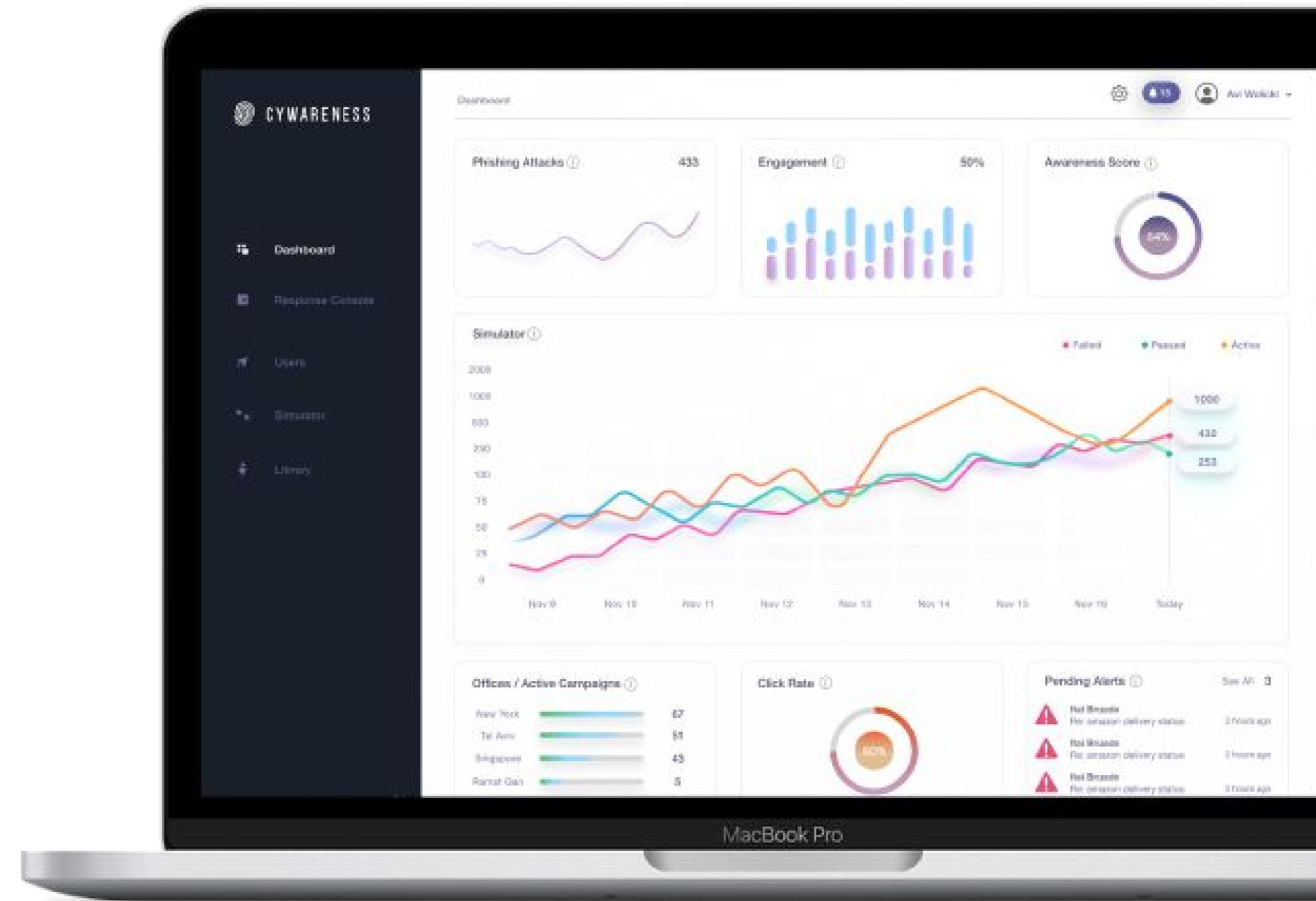
With an ever-rising number of cyber-attacks each year, the risk of not educating your employees on cybersecurity awareness only continues to grow.

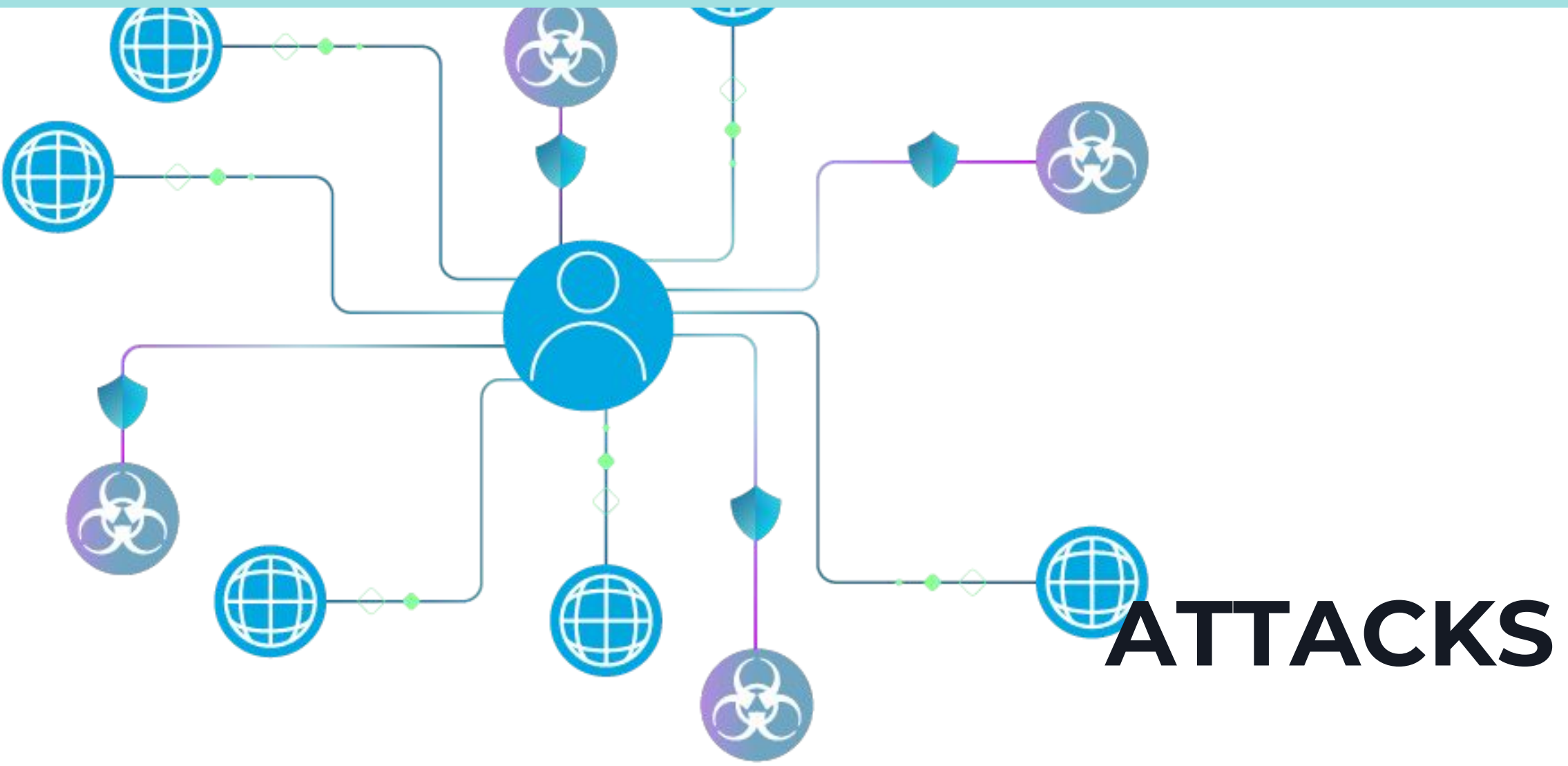


www.kenfil.com

PROTECT YOUR ORGANIZATION

Cywareness allows you to maximize your employees cybersecurity potential by exposing them to the most relevant cybercrime scenarios on an ongoing basis, with no additional requirements or resources from your IT team





200+ PHISHING EMAILS TEMPLATES & SMS's

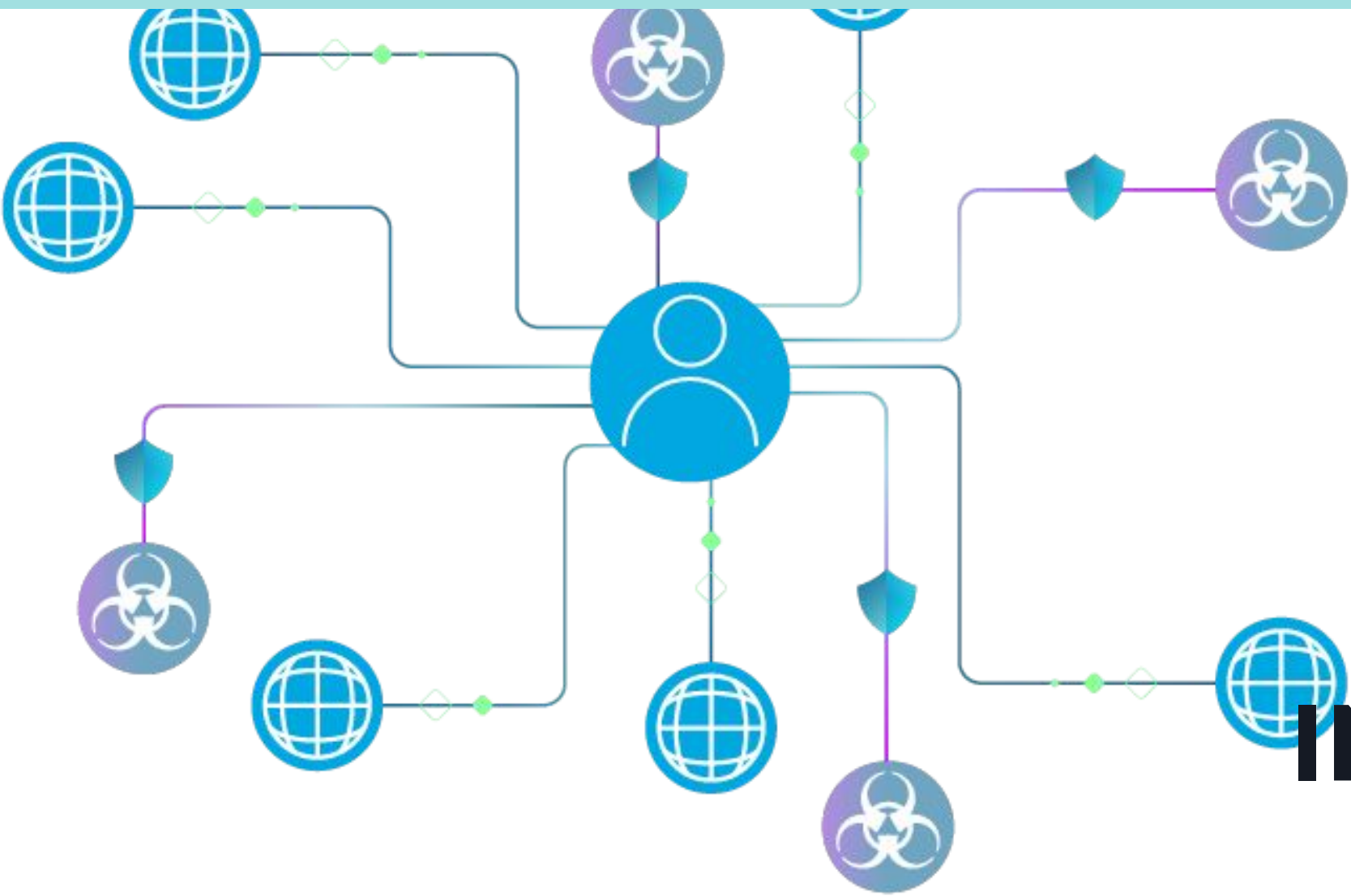
Phishing simulations are easier than ever



Cywareness allows you to deploy smart simulated attacks in multiple languages on your employees by both email and SMS

The platform includes micro-training sessions to teach the user how to identify future attacks

The screenshot displays the 'Campaign Details' section of the Cywareness platform. It shows a campaign named 'Phishing Templates Test' with recipients 'Niv Netanel', 'David Polevoy', and 'Yanon Hadad'. The start date is 'October 18th 02:37 pm' and the end date is 'October 25th 02:37 pm'. A checkbox 'Is it a test campaign?' is checked. Below this, there are tabs for 'Email Templates' and 'SMS Templates', with a search bar. Two templates are listed: 'LinkedIn new connection request' (Level 4) and 'OneDrive - Shared file reminder' (Level 5). To the right, a simulated Gmail inbox is shown with a phishing email titled 'You have a new sign-in' from 'Password <no-reply@pass.authenticationn.com>' received at 8:02 AM. The email content is partially obscured by a large blue information icon.



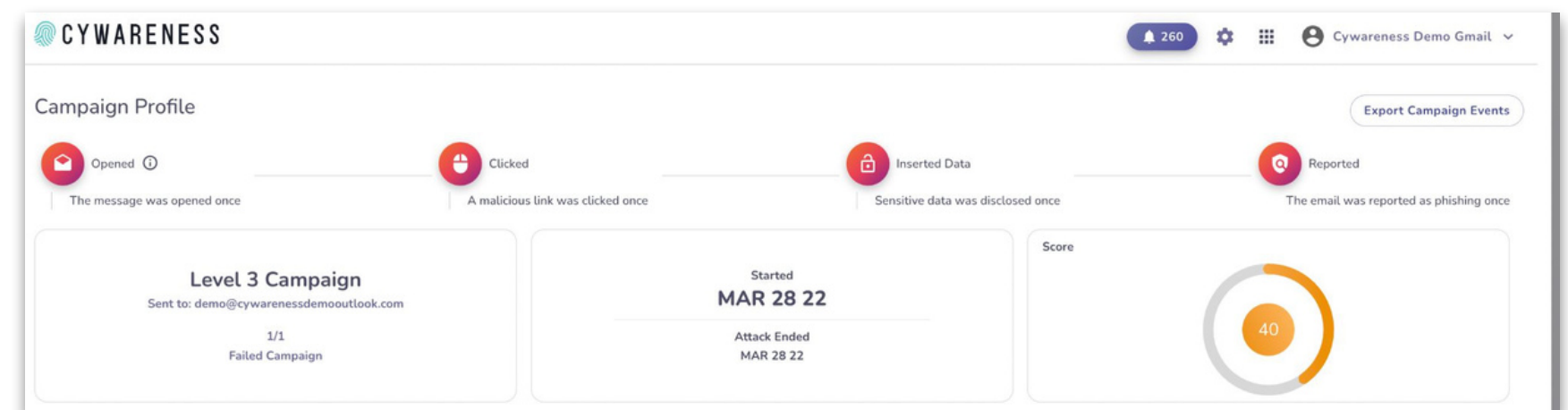
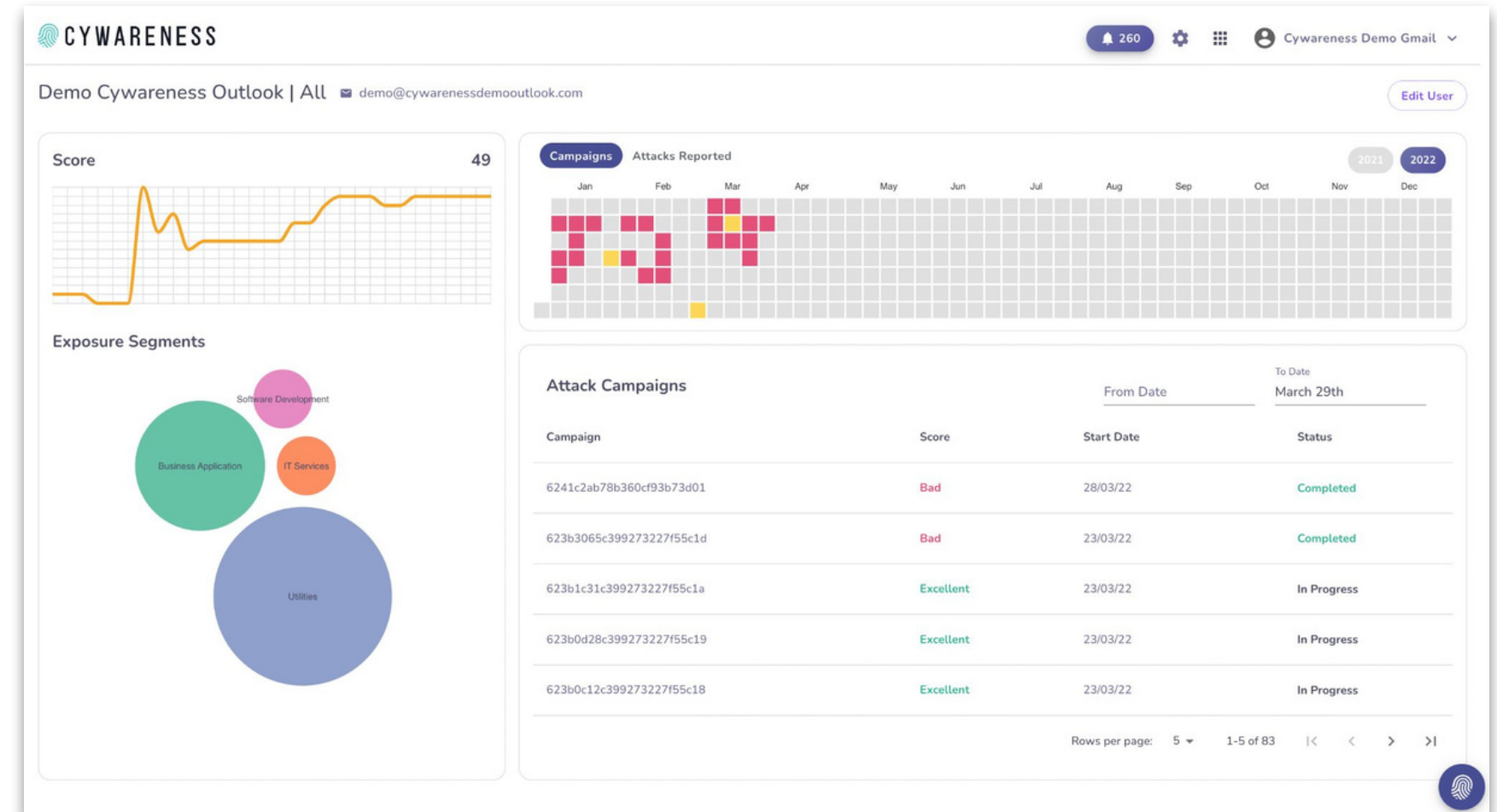
INSIGHTS

FULL VISIBILITY

Get a complete understanding of your employees strengths and weaknesses

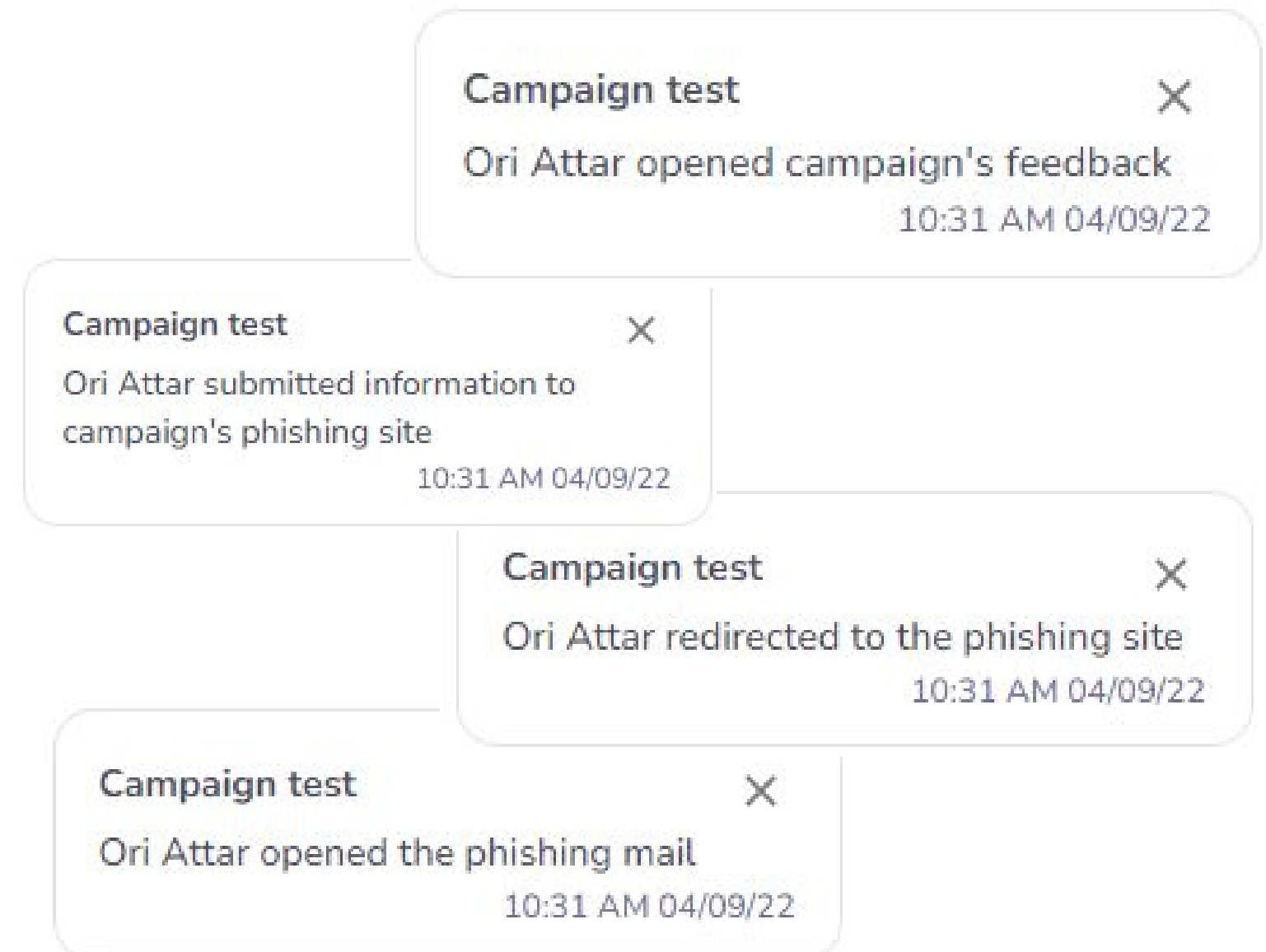
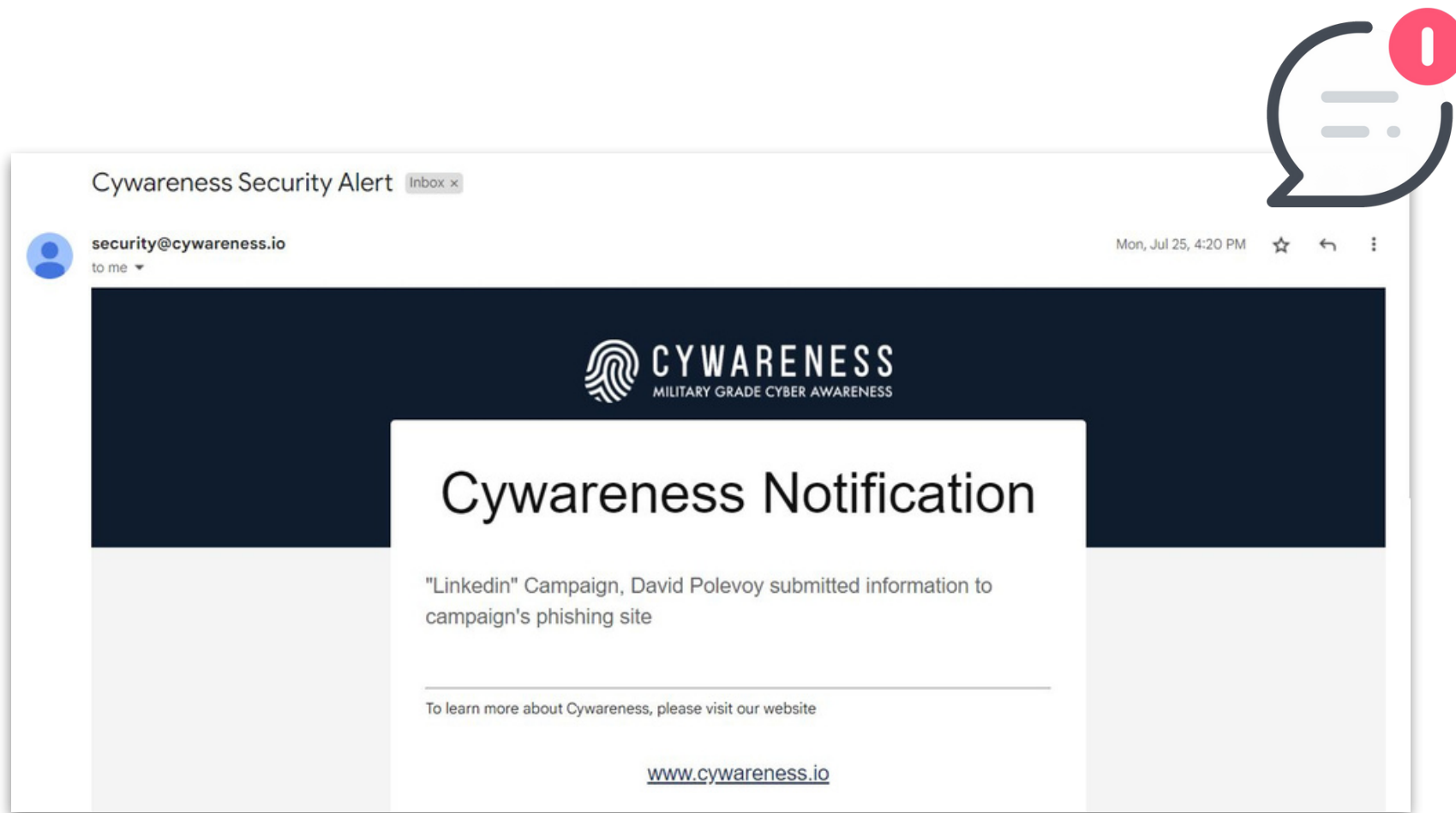
Get analytics of each simulated attack, from opening an email to inserting data into our phishing page. Full flexibility allows you to analyze the performance of each employee, team, department, or even office.

Our analytics give you a view of how your employees have done compared to previous campaigns.



GET PHISHING ALERTS

Real-time alerts when a user interacts with a campaign. These alerts can be viewed in our dashboard as well as be sent by email.



DATA ANALYZING & REPORT

ONE-STOP shop for all your insights

Campaign Profile | Buy Me Gift Card

28.92% Opened The message was opened 68 times

19.41% Clicked A malicious link was clicked 53 times

9.89% Inserted Data Sensitive data was disclosed 27 times

0% Reported

Level 3 Campaign
Sent to: Niv and +272 more
27/273 Failed Campaign

Started **JUN 26 22**
Attack Ended **JUN 28 22**

Awareness Level i

Bad Low Average Excellent

Campaign Users

Events by Groups & Offices

Attack Template

CYWARENESS™

PHISHING CAMPAIGN ASSESMENT SUMMARY

Company name Ltd.

CAMPAIGN SUMMARY

- Start date: 29th of July, 2022
- Duration: 72 Hours
- Vector: Mail | Type: Airline Points
- Difficulty level: ●●●●○
- Num. of participants: 5,257
- 2,519 (47.92%) Downloaded File

CAMPAIGN INSIGHTS

PERFORMANCE BY DEPARTMENT VULNERABILITY:

Department	Open link	Submitted data
Business Development	392	249
Finance	469	298
Sales	549	301
Customer Service	767	347

OFFICE COMPARISON

LINK CLICK RATE:

- A | level 3 | Buyme: 28.10%
- B | level 3 | Buyme: 18.68%
- A | level 4 | Airline Points: 47.92%

CAMPAIGN EMAIL

© Cywareness LTD - 2 HaNofar Street, Raanana, Israel

TRAINING





AUTOMATED TRAINING PROGRAM

No additional resources

Provide an automated cybersecurity educational experience based on real-life threats aimed towards every employee of all cyber awareness levels and technological background with no additional resources from your security team.

The goal of phishing training is to improve employee defense against phishing attempts.

Our phishing training includes quizzes and videos to show employees how to spot phishing emails and be aware of cybersecurity threats and respond to these risky threats.

From: office366@microvoft.com

Sent: john@companydomain.com



Total Held Email: 23 Contact Messages

Date: 09 - 23 - 2020

Please continue below in order to view your **important** contact messages.

Continue

23 contact email messages will be automatically deleted after 24 hours

Sincerely,
The Microsoft Online Services Team

2 Spelling Mistake

Spelling mistakes are common indicators of phishing email.



INSTANT MICRO TRAINING

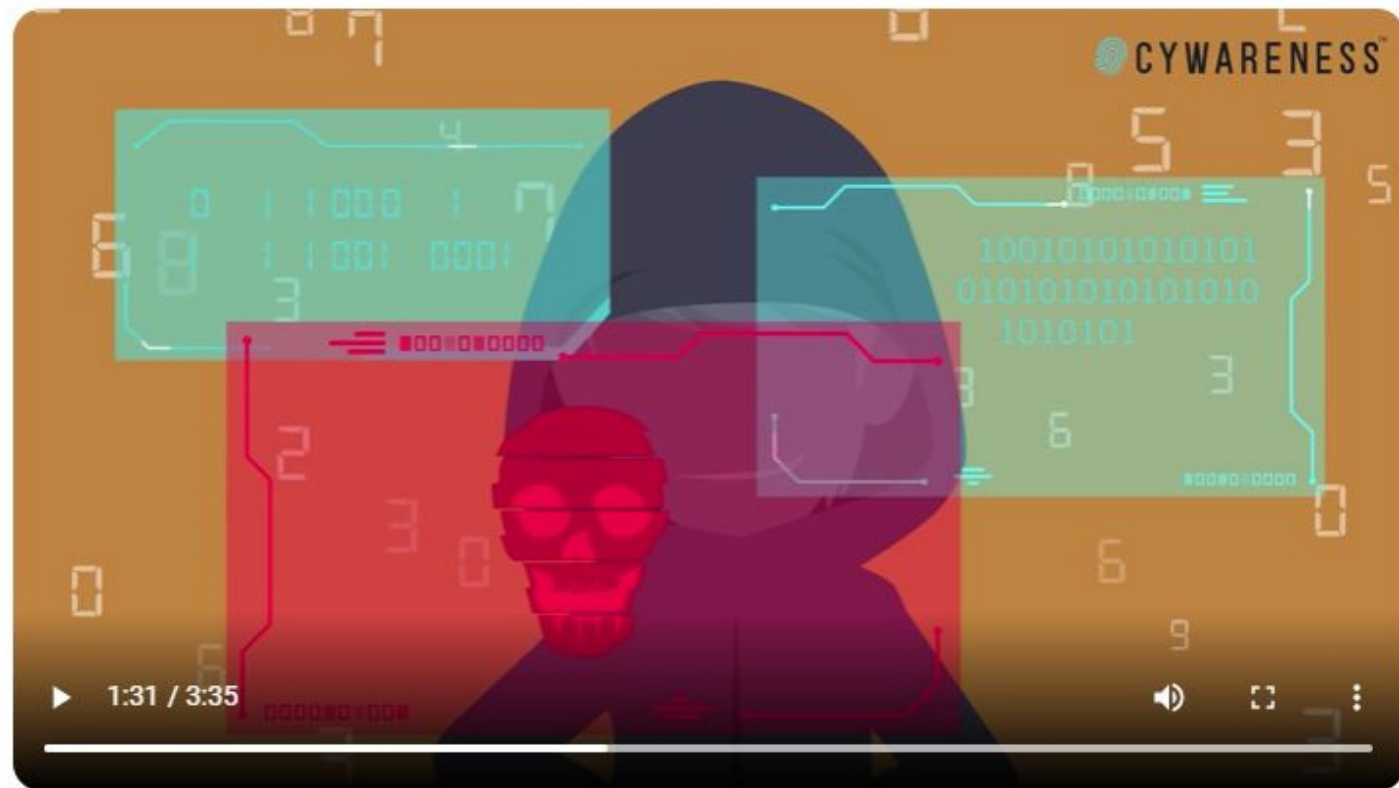
Have your employees identify the latest phishing vectors in no time

If an employee falls for a simulated attack, they will receive an instant micro training, showing them what they missed and what to look out for. The employee's awareness level will rise by providing the training instantly, ensuring the organization is in safe hands if they ever face a genuine phishing email.



Onboarding: Cybersecurity

Complete by 19/09/22



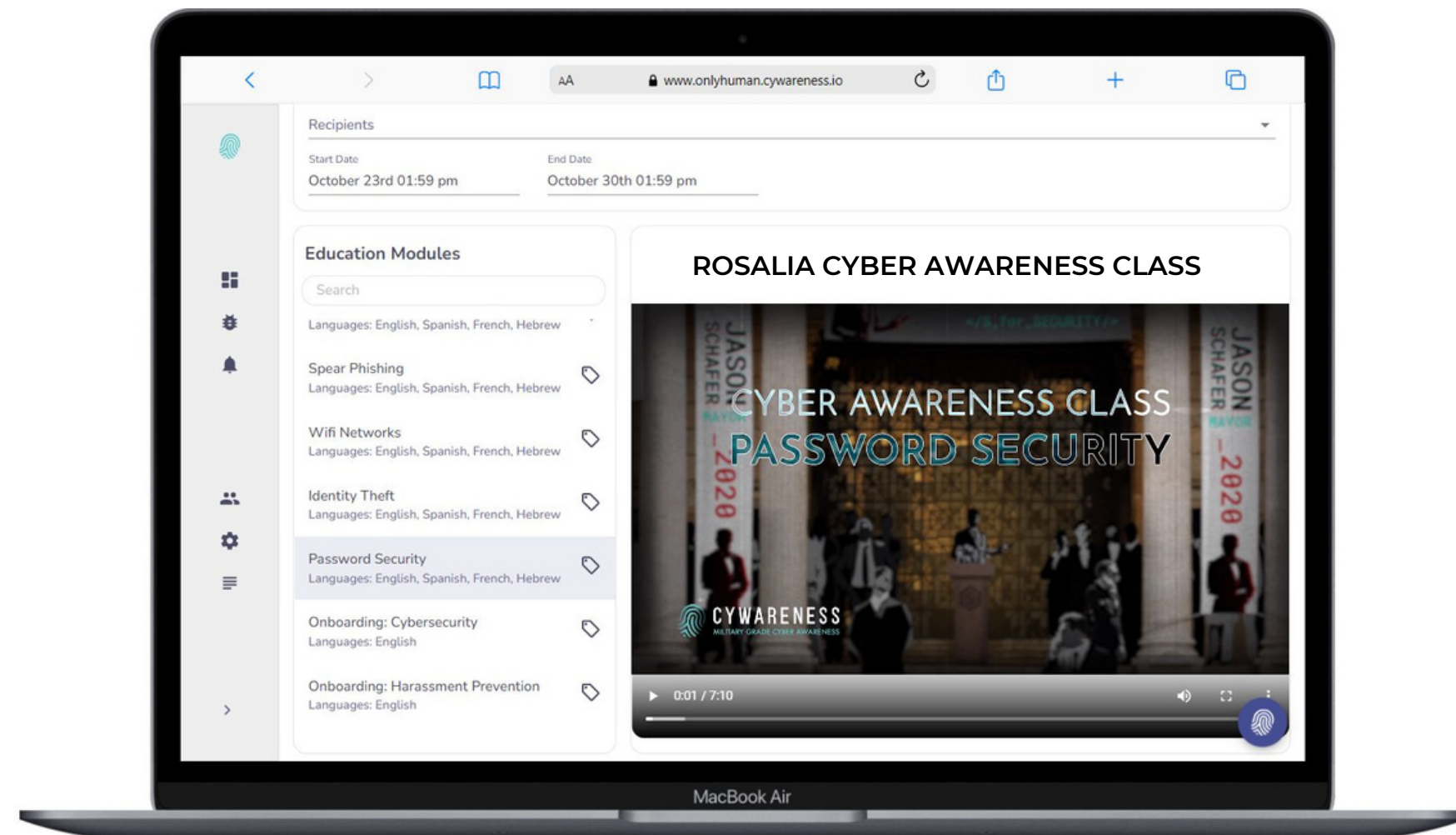
Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Complete Quiz

Multi Languages Quizzes

ONBOARDING & TRAINING VIDEOS

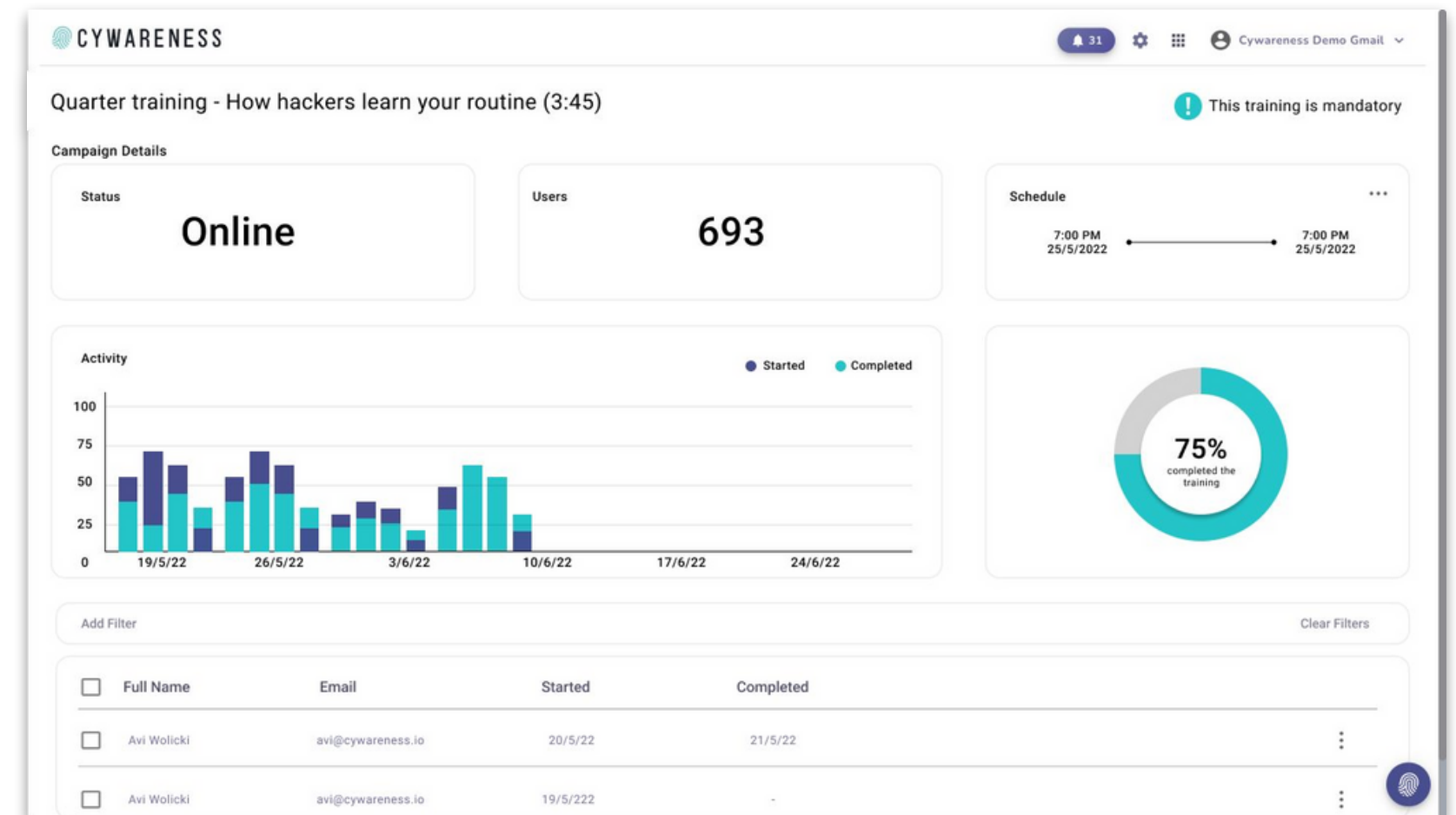
New Compliance Training Content Delivered Easily and Effectively including Rosalia and OnBoarding Videos



NEW TRAINING PROGRAM EXPERIENCE

Get a complete understanding of your employees strengths and weaknesses

cybersecurity awareness new training experience that uses engaging, micro-learning videos to empower individuals and organizations to become defenders against cyber threats.



SUPPORT MULTI-LANGUAGES QUIZZES

Our system supports numerous smart testing languages, allowing you to deliver them to your employees and educate them on the dangers of phishing.

How can a phishing email install malware on your computer?

- A Through links to malicious websites
- B Using infected files attached to an email
- C Through unwanted videos and pop-ups

All of the above

3 / 4 Continue

כיצד מייל פשינג יכול להתקין תוכנה זדונית במחשב שלך?

- A באמצעות קישורים לאתרי אינטרנט דדוניים
- B שימוש בקבצים נגועים המצורפים למייל
- C באמצעות סרטונים וחלונות קופצים לא רצויים

כל התשובות נכונות

3 / 4 המשך

¿Cómo puede un correo de phishing instalar malware en tu ordenador?

- A A través de enlaces a sitios web maliciosos
- B Utilizando archivos infectados adjuntos a un correo electrónico
- C A través de vídeos y ventanas emergentes no deseadas

Todo lo anterior

3 / 4 Continue

Language selection menu:

- Hebrew (selected)
- English
- Spanish
- Hebrew
- French

X

TRAINING SUMMARY

Get your employees results quickly and easy



Campaign Users (2)

Name	Email	Started	Completed	Score
Yanon Hadad	yinnon@cywareness.io	22/09/22	22/09/22	75
David Polevoy	david@cywareness.io	22/09/22	22/09/22	50

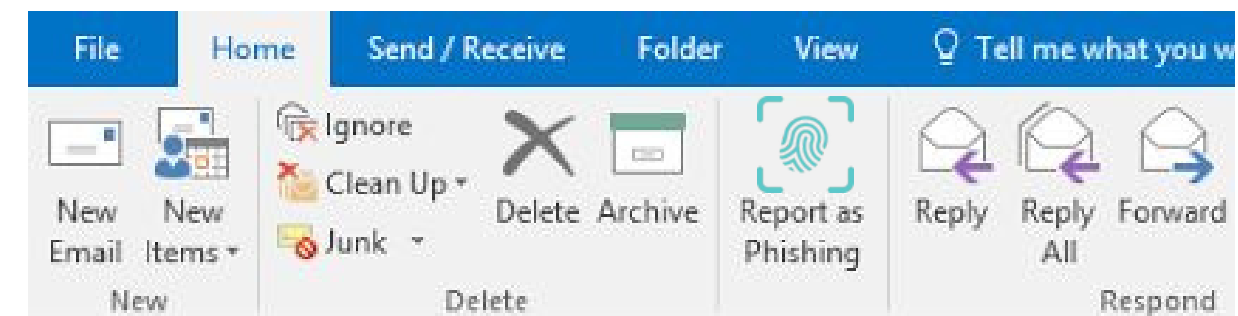
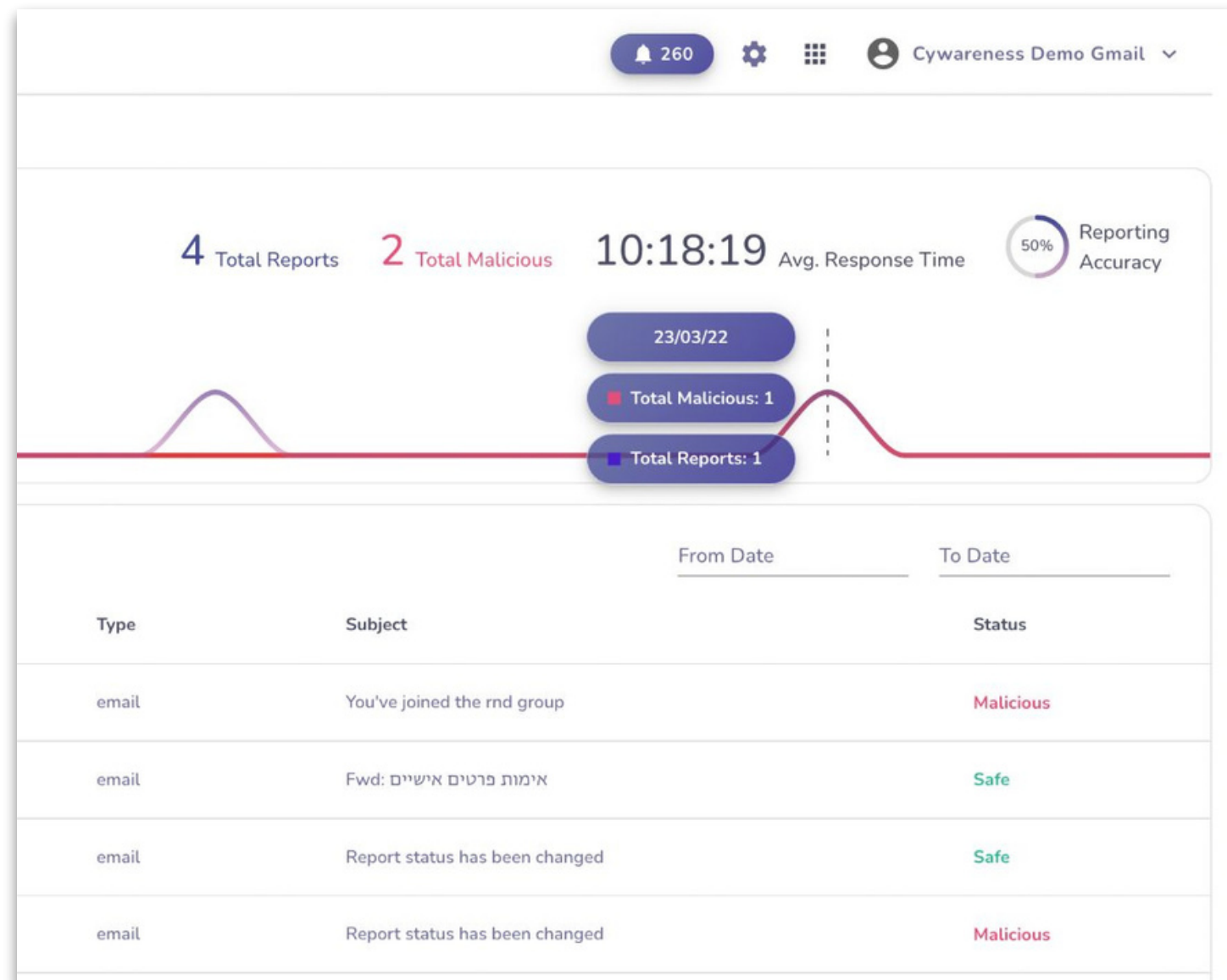


DEFENCE

YOUR EMPLOYEES ARE YOUR BEST DEFENSE LINE

Provide your employees with tools to protect against and manage cyber attacks

Imagine that your employees could be your strongest defense against cyber attacks, rather than a potential area of weakness. Employees must be able to spot the types of attacks that may compromise company networks and be ready to use best practices and available tools against cyber attacks like our report button:



MANAGE ANY POTENTIAL PHISHING ATTACK

Automate and scale your response process for a potential cyber attack

Get a fast understanding of every email that your employees report as suspicious with Cywareness security tool, you will be able to examine the email's code, hidden links and attachments to determine if the email is malicious or safe. All of the communication with the employees in this kind of an event will be automated by Cywareness, allowing fast response and scale for the security teams.

The screenshot displays the Cywareness interface for a suspicious email. It includes the following sections:

- Email Details:** Subject: Re: Amazon delivery failed; Sender: badbob@gmail.com; Received: 13:20 2/11/2020; Recipients (4): itai@cywareness.io.
- Timeline (3 Days):** A calendar view for November showing a report on Friday, Nov 6th, labeled 'Avi w Reported'.
- Cywareness Score:** A circular gauge showing a score of 8.
- Links (2):** Two links are listed: www.cnn.com/newsfake/uid23923 (score 3.5) and www.amaz.com/newsfake/uid23923 (score 8).
- Attachments (2):** Two attachments are listed: Installer.exe and howtoworkwithyour.pdf.



 **Witz**
Cybersecurity
Australia & New Zealand Partner

