



How to reduce human risk with behavior change

NIS2 follow-up webinars

Welcome



Sacha Vekeman (Inetum's Host)
Specialized Sales Cybersecurity
Human Risk Practitioner



Jim Moliski (Guest speaker)
VP Strategy  **HOXHUNT**



AGENDA:

- Inetum's Webinar about **Human Risk**
- Practical session how to move from **Security Awareness** to **Behavior Change** and align with **NIS2** regulation
- How to achieve change with **Hoxhunt**

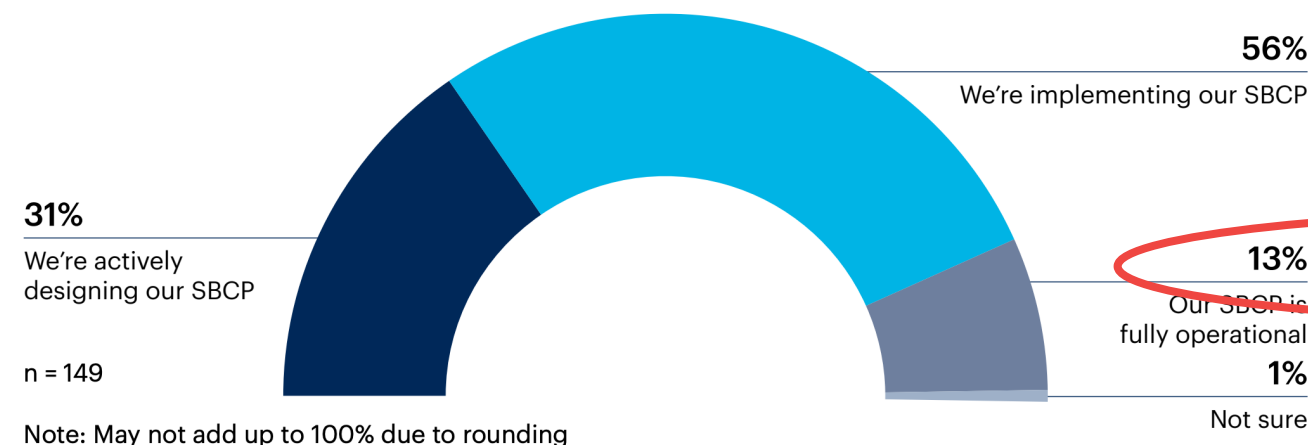
Practicalities

- Questions via chat
- Everybody is on mute
- Q&A after the presentation
- Evaluation with link to the slides will be sent after the webinar

Why Human Risk

Recent industry maturity: from SAT to Risk Adoption

- **2020** Hoxhunt published a Buyer's guide to "Modern **Phishing** Training" focusing on:
User experience, personalization, reporting metrics and automation to achieve behavior change!
- **2022** Gartner published: "Innovation Insights on Security **Behavior** & Culture Program Capabilities"
Security Awareness Computer-Based Training (SACBT) services offer a stable set of core capabilities, yet risky employee behavior persists. New, emerging capabilities apply **behavioral science principles, data analytics** and **automation** to help cybersecurity leaders reduce risk via **measurable** culture change
- **2023** Gartner updated research: Security Behavior & Culture Programs **Adoption** Strategies



Minority is at Human Risk

Majority is doing SAT

footer

Why Human Risk

Increasing customer maturity in Belgium

- **Situation in Belgium is changing fast**

1/3 Do nothing or classroom / video-based SAT (difficult to measure)

1/3 DIY phishing-test as once and a while (first measurement – fail rate baseline)

1/3 Phishing simulations done via a platform: e.g. Phished.io or Microsoft E5 licenses (first steps to compliance)

Minority is Running SBCP
Majority is doing SAT

- **Client maturity grows fast in large-scale or complex ecosystems – SAT doesn't work**

Port of Antwerp → start of a new "Cluster" with fast adoption (city of Antwerp, police zone, transport, railway, etc.) → driven by peer pressure

BPost + BEL20 companies + Critical Infrastructure (nuclear, energy, utilities, etc.) → today driven by NIS2, complexity & need for change

Healthcare → huge variation of people and skills, location of workers and cultural difference (languages, nationality, roles, etc.)

- **NIS2 is fast-tracking adoption – SAT is NOT the solution**

User awareness → **requires engagement!!!**

Reporting, reporting, reporting → **requires data** about your employees!!!

Focus on ransomware (→ 80% of attacks start with social engineering and phishing) → **requires behavior change** from people!!!

Why HOXHUNT

People-first approach – **Leveling your Executives** – Adoption

- **End-users** love it – high engagement rates (critical measurement) – critical for “Directie” en “RvB”
- Security defenders – fully automated (less work) – they love it as no overhead (IT / CIO)
- Security analysts – get more real malicious mails reported (no noise & no false-positives) (SoC)
- **Executives** – levels the cybersecurity playing field – shows the importance & URGENCY of cybersec.

Business case is made in less than 2 weeks – **Immediate data**

- **Engagement** rates → clear ROI to access platform and benefit from automation
- Fail rate versus **success rates** → phishing recognition (core to SAT)
- **Real-threat reporting rate** → visible risk-reduction: your own people become your most reliable security analysts

NIS2 stress tested – Easy to decide – Fast implementation – **Risk Reduction**

- Actionable data – clear metrics - real(-time) reporting – real visible progression of people!
- Continuous is in Continuous – change takes time but progression is measured day-to-day
- **Drives REAL THREAT REPORTING – Malicious emails are getting reported and handled!!!**



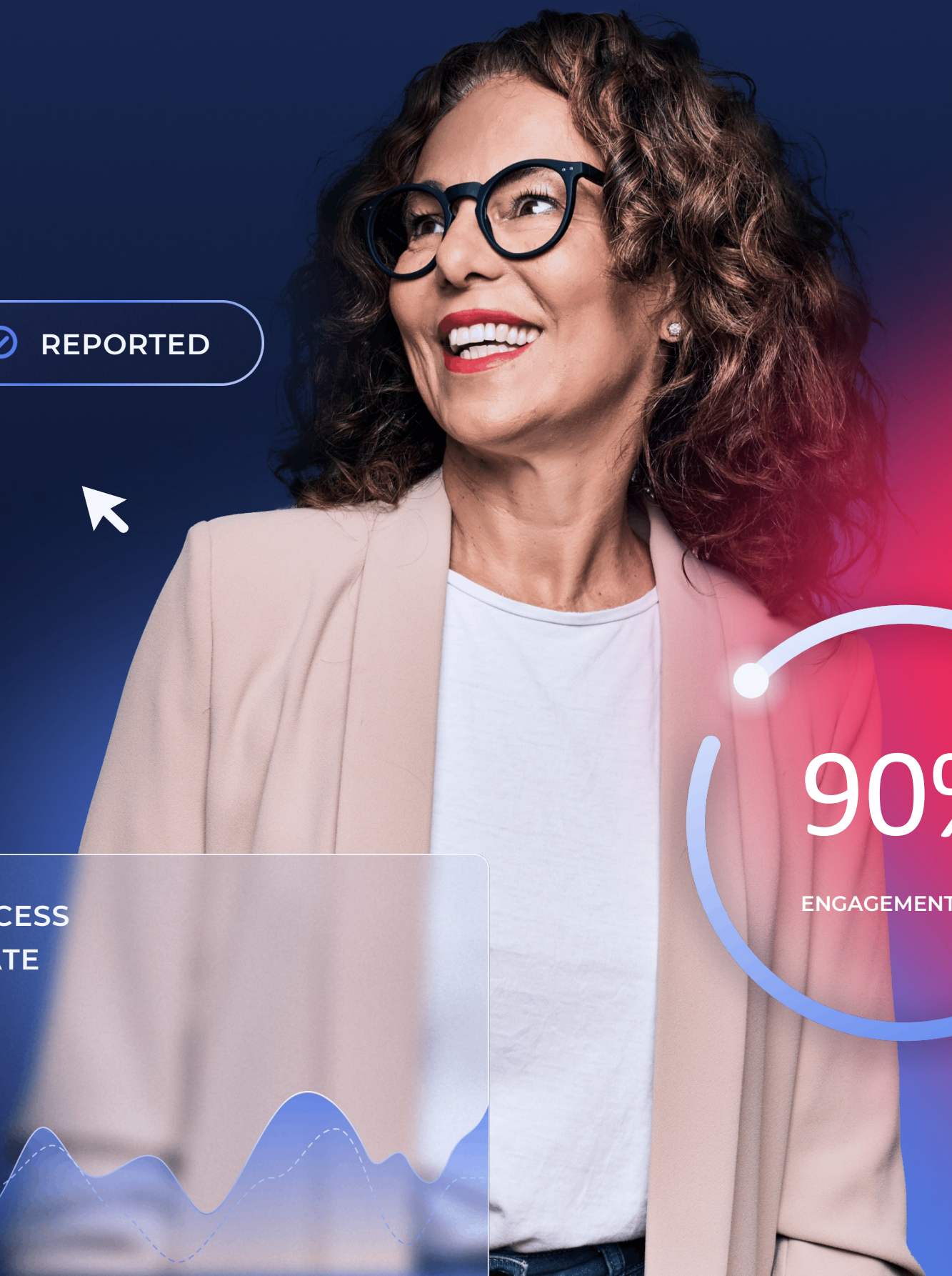
Reducing Human Risk with Hoxhunt

 REPORTED

SUCCESS
RATE
92%

90%

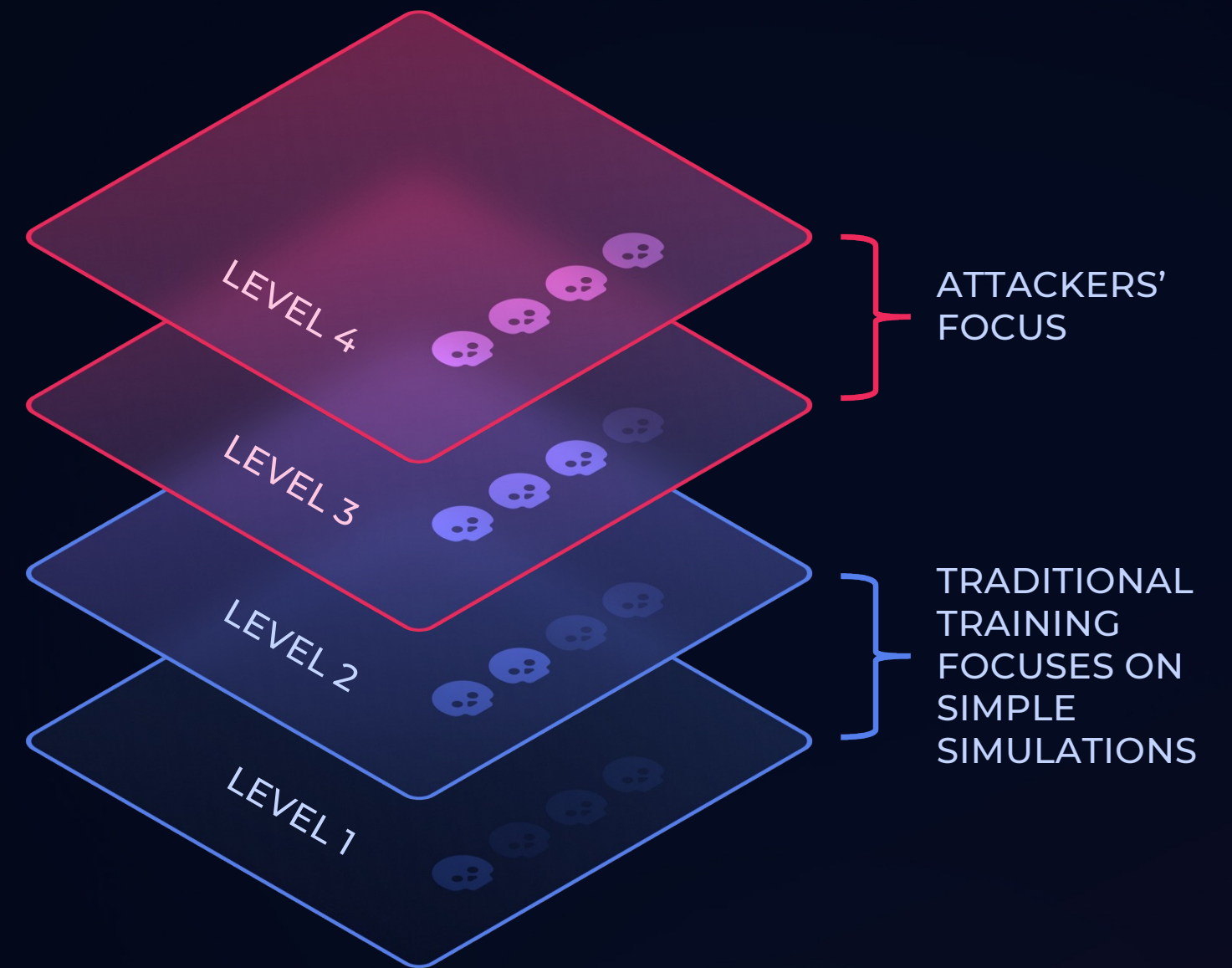
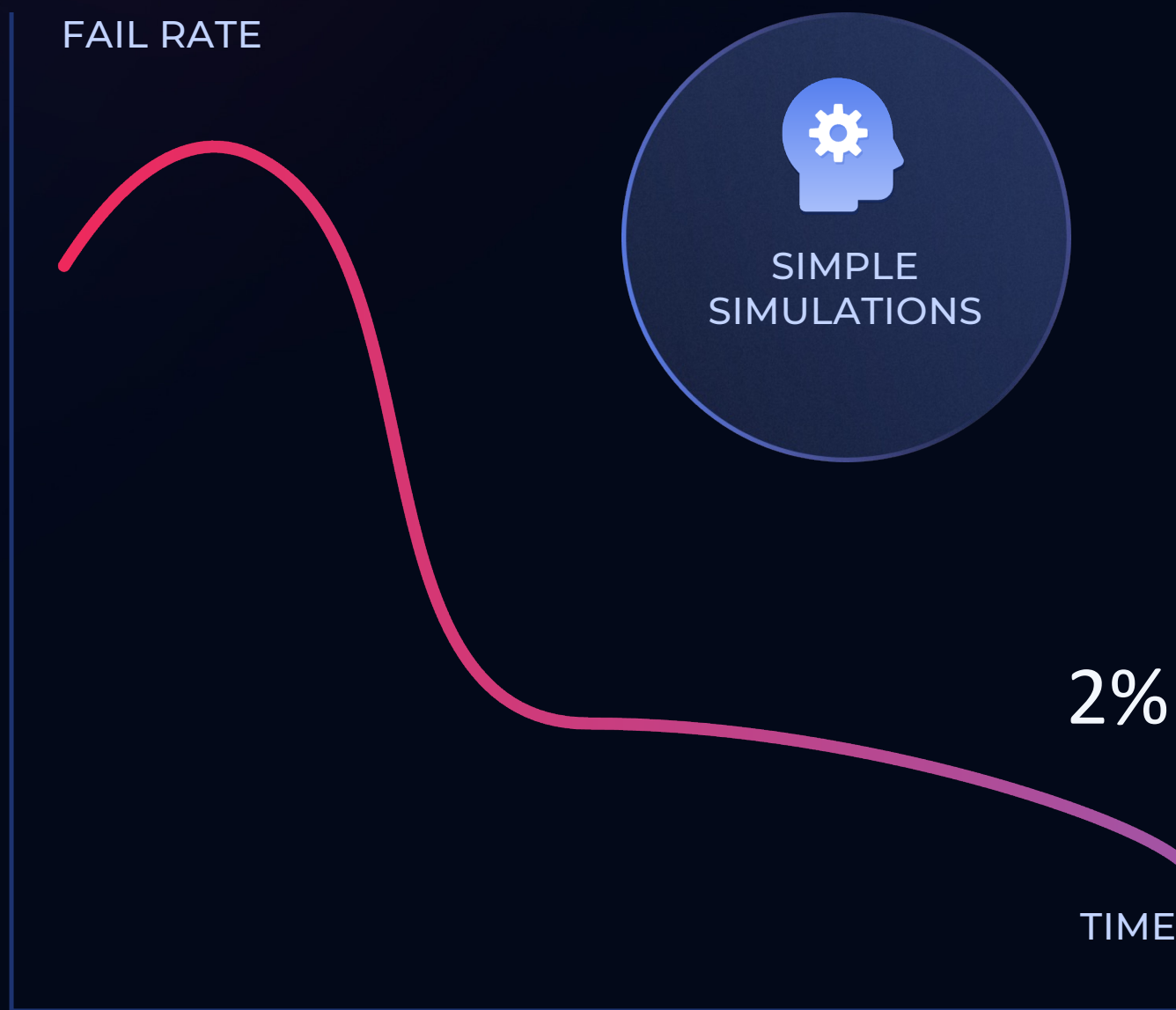
ENGAGEMENT RATE



People-first positive behavior change



Problem: Employees aren't prepared



Learning happens at the boundaries of knowledge



PETER'S SKILL PROFILE

HR Manager
Started training 3 months ago

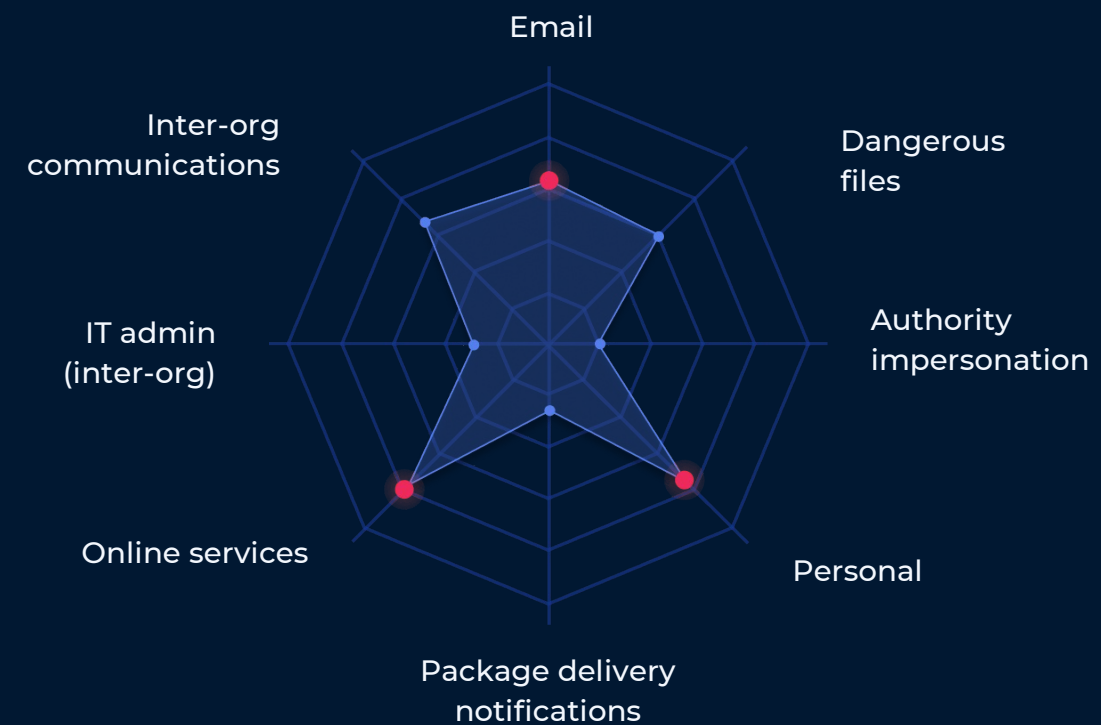
- SIMULATION REPORTED
- SIMULATION FAILED



JANE'S SKILL PROFILE

IT Admin
Started training 11 months ago

- SIMULATION REPORTED
- SIMULATION FAILED



Search

New Message Delete Archive Move Flag Mark as Read Sync Report this email


Demo

Today

External **Dirk via Dropbox**
Dirk Schiller wants to share folder "Summer p... 14.32
Dirk wants to share some files in a folder called "Summer..."

External **Dirk Schiller wants to share folder "Summer party pics" with you!**

Dirk via Dropbox <no-reply@dropbox.one> Today at 14.32
To: Olli Gunst



Hi there,

Dirk (dirk.schiller@hoxhunt.com) wants to share some files in a folder called "Summer Party Pics" with you via Dropbox.

[View folder](#)

Enjoy!
- The Dropbox Team

© 2022 Dropbox



Fantastic job!

You spotted a [Hoxhunt training](#) email. Keep up the great work with reporting!

Learn about the shady tricks used in this simulated phishing email and earn one more star!

Next





Dirk via

11/10/2022

Olli Gun:

Dirk Sch

Emotions

Curiosity is one of the most powerful emotions that social engineers exploit. By presenting something interesting or something mysterious, the attacker tries to get you to perform a wanted action.

Next

Hi there,

Dirk (dirk.schiller@hoxhunt.com) wants to share some files in a folder called "Summer Party Pics" with you via Dropbox.

View folder



Next

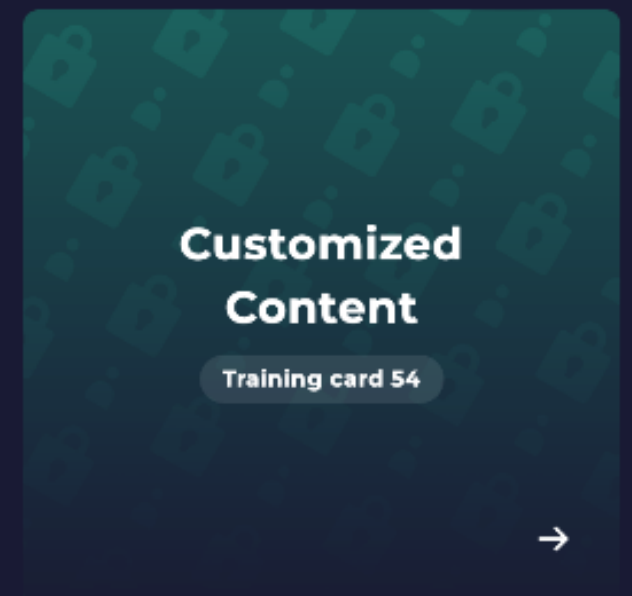


Prohibited Activities

Which of the following practices is allowed based on Hoxhunt Information Security Policy?

- Compromising confidential Information
- Introducing Malware
- Crashing an information system
- None of the above

Need a hint? Training card will help you out.



Customized Content
Training card 54

→





Iron

70



Bronze

90



Steel

115

133



Silver

145



Gold

160

Leaderboard

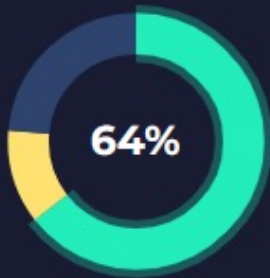
See all

Quarter 2 2023

Hoxhunt Sales All departments

88	Okko Parviainen	71%
89	Atso Puronen	71%
90	Jim Moliski	71%
91	Sacha Vekeman	71%
92	Eerik Murtta	70%

Overall Progress



- 38 reported
- 7 clicked
- 14 missed

Winning streaks

Current streak: 1

Best streak: 8

Achievements

See all

Next



Master of the Universe

Earn a total of 150 stars

133 / 150

Latest



One of these things is not like the other

Successfully report a spoofing simulation




[Hoxhunt Report] jane.doe@gmail.com sent you invoice2021.pdf



Jim Moliski
To Atso Puronen



Tue 13/09/2022 14.45

 If there are problems with how this message is displayed, click here to view it in a web browser.

jane.doe@gmail.com
sent you invoice2021.pdf

1 item, 22.3 KB in total · Expires on 30 August, 2021

[Get your files](#)

Download link

https://wetransfer.com/downloads/Mml4MWI3MDJiZWQ4ZTY2OTI4ZTc0ZDA2ZTYzNDA2Nj_cyMDIxMDgwOTA3/MzlxMWU4ZTRiNTEExZjYyOGFiYmQ3ODdkNjI1YTM0MWUyMDIxMDgwOTA3Mj_

[Hoxhunt Report] jane.doe@gmail.com sent you invoice2021.pdf



Jim Moliski
To Atso Puronen

Reply Reply All Forward

Tue 13/09/2022 14.45

If there are problems with how this message is displayed, click here to view it in a web browser.

jane.doe@gmail.com
sent you invoice2021.pdf

1 item, 22.3 KB in total · Expires on 30 August, 2021

Get your files

Download link

https://wetransfer.com/downloads/Mml4MWI3MDJiZWQ4ZTY2OTI4ZTc0ZDA2ZTYzNDA2NjcyMDIxMDgwOTA3/MzlxMWU4ZTRiNTEExZjYyOGFiYmQ3ODdkNjl1YTM0MWUyMDIxMDgwOTA3Mj_

Hoxhunt Report



Report email



Report as phishing

Suspicious content or sender with malicious intent? Report it for further analysis.



Report as spam

Unwanted content such as advertising or newsletters? Block the sender, and report this email for further analysis and move it to junk.

Go to Dashboard

19 other people also reported this email

Excellent job! You've caught a malicious email. Avoid any interaction with it.

What's going on?

We have rated this email as malicious with high confidence. The email includes a malicious attachment or link, or techniques practically only used by attackers to make you believe that you need to act upon the email.

The report has been forwarded to the Hoxhunt Demo security team.

What should I do?

It is very important that you avoid any interaction with the email. Do not click the links, download attachments, or reply.

Threat indicators

HOMOGLYPHS IN SENDER NAME

WETRANSFER MENTIONED IN BODY

MONEY TRANSFER KEYWORD MENTIONED

Homoglyphs are text characters with shapes that are near identical or similar to each other. Attackers use homoglyphs to impersonate a person without being caught by email filters.



Did you know that 84% of reported

From: Jane Doe <john.doe@nice-email1.com>

To: <jim.moliski@hoxhuntedemo.com>

9/13/2022

jane.doe@gmail.com sent you invoice2021.pdf



Reporting was successful

Thank you for reporting. You can close the window now.

Close



HOMOGLYPHS IN SENDER NAME

WETRANSFER MENTIONED IN BODY

MONEY TRANSFER KEYWORD MENTIONED

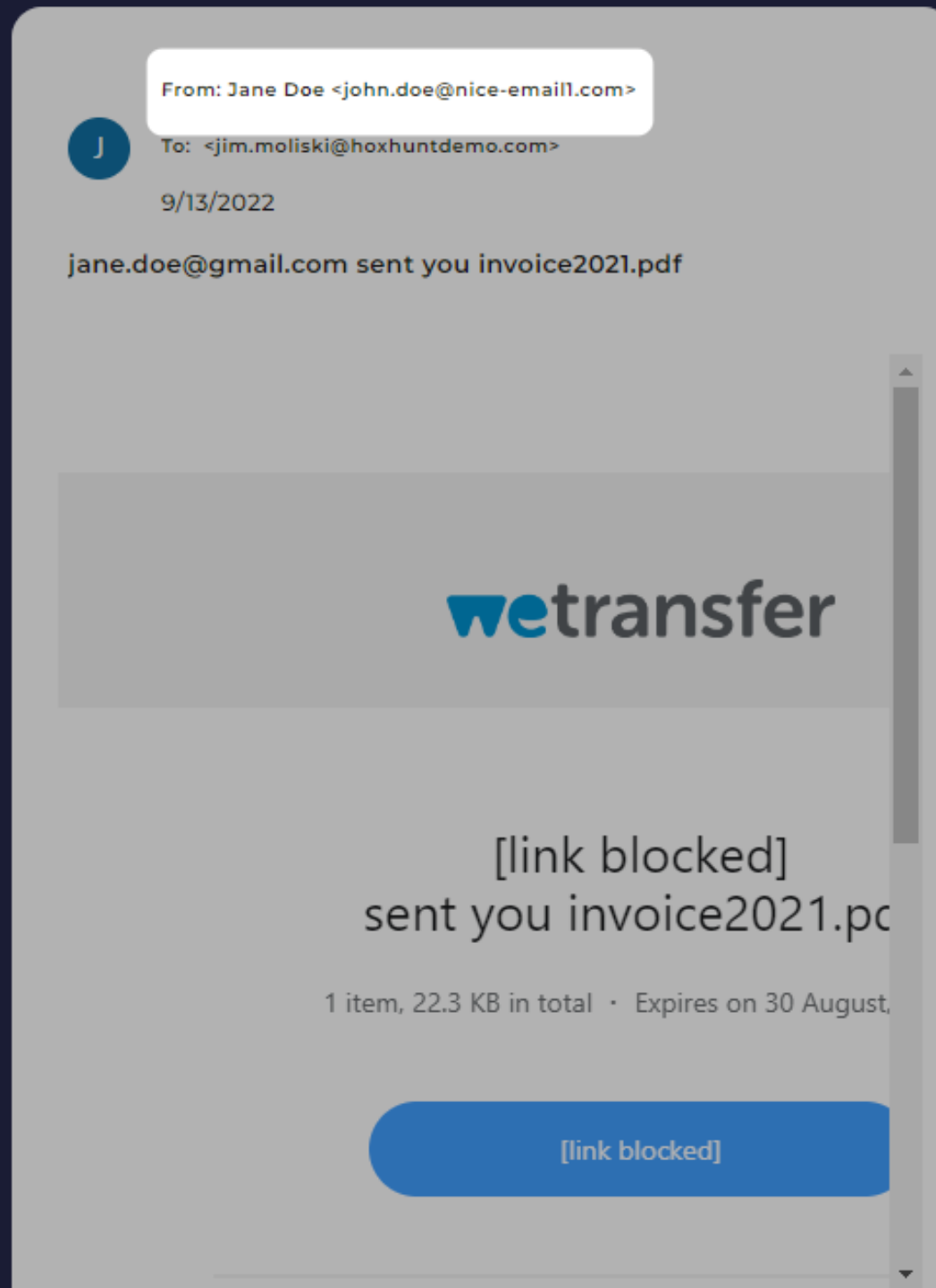
Homoglyphs are text characters with shapes that are near identical or similar to each other. Attackers use homoglyphs to impersonate a person without being caught by email filters.



Did you know that **84%** of reported emails with homoglyphs in the sender name were classified as malicious by our analysts?

👉 An attacker can impersonate Hoxhunt by claiming to be Hoxhunt. The former has a Latin "o" while the latter has a Cyrillic "o".

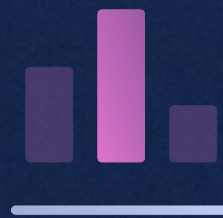
An observant user can spot homoglyphs, characters that appear identical, used in impersonation attacks.





60%

**Success rate
after 1 year**



60%

**Users reporting a real
threat after 1 year**



60

**Seconds to report a
real threat (top 5%
fastest users to report)**

WaterAid's Business Email Compromise (BEC) Attack



Business email of external partner is compromised



Fraudulent invoice issued to WaterAid



WaterAid pays the invoice

WaterAid: with Hoxhunt



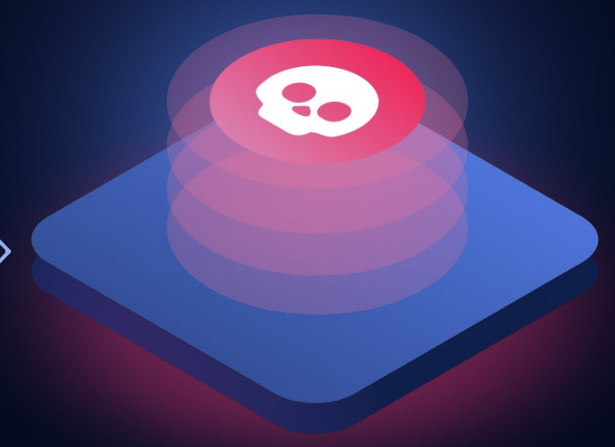
**2 employees
report a BEC
attack**



**Head of
Cybersecurity
notified**



**Operation team
finds the attack
was remediated
within minutes**



**Malicious emails
removed from 39
inboxes**



“I’m so confident in our staff now with Hoxhunt that if people ask me how many cybersecurity officers I’ve got, I say ‘2000’”

MARK SEDMAN
GLOBAL HEAD OF CYBERSECURITY





People are your greatest risk

Why Now

1. Maturity increases with our clients (CSATs)

- **Automation** requirements – main driver to reduce cost and balance the shortage of cybersec skills
- **Competition** is NOT up to par with Hoxhunt
- DIY is no longer an option

2. NIS2 directives are imminent

- Companies and private AND public sector starts to prepare – get started **before the summer!!!**
- POCS and POVS – we (have many to) handle many – **Hoxhunt** is skilled and scaled!
- **Data** output (with automation) is key to build the business case

3. People-Driven Solution

- Many **Belgian** references and examples
- Feedback **users** – we use it also at Inetum-Realdolmen – see G2
- **CISOs** can provide you with direct feedback!

No FUD please

Tot 10 miljoen boete voor onaangepaste cyberbeveiliging

24 APRIL 2024 - 12:50 | 4 MINUTEN LEESTIJD | [ACHTERGROND](#) | [GOVERNANCE & PRIVACY](#) | [EUROPESE COMMISSIE](#)



William Visterin

'NIS2 is NIS1 on steroids', aldus de Europese Commissarissen

De Belgische NIS2-wet is een feit. Zopas zette het federale parlement de Europese regelgeving daarover om in een wet. Zowat tweeduizend Belgische bedrijven en instellingen krijgen strengere normen voor cyberveiligheid. Met mogelijk miljoenenboetes tot gevolg. Maar wanneer treedt NIS2 in werking?



Kunnen ceo's persoonlijk aansprakelijk worden gesteld?

Zeker en vast. De nieuwe NIS2-wet heeft flink wat gevolgen voor managers en bestuurders van de bedrijven die onder NIS2 vallen. Zij zijn onder meer verplicht om een opleiding te volgen om cyberrisico's in te schatten. Verder moeten ze alle maatregelen goedkeuren om het bedrijf beter tegen aanvallen te beschermen en weerbaarder te maken. Managers en bestuurders zijn dus sowieso en bij wet betrokken partij.

Next step: Fast-track your human risk

What can you expect?

Fast intake & comparison of your measurements against our market intel

Free PoC after qualification with a Hoxhunt product specialist

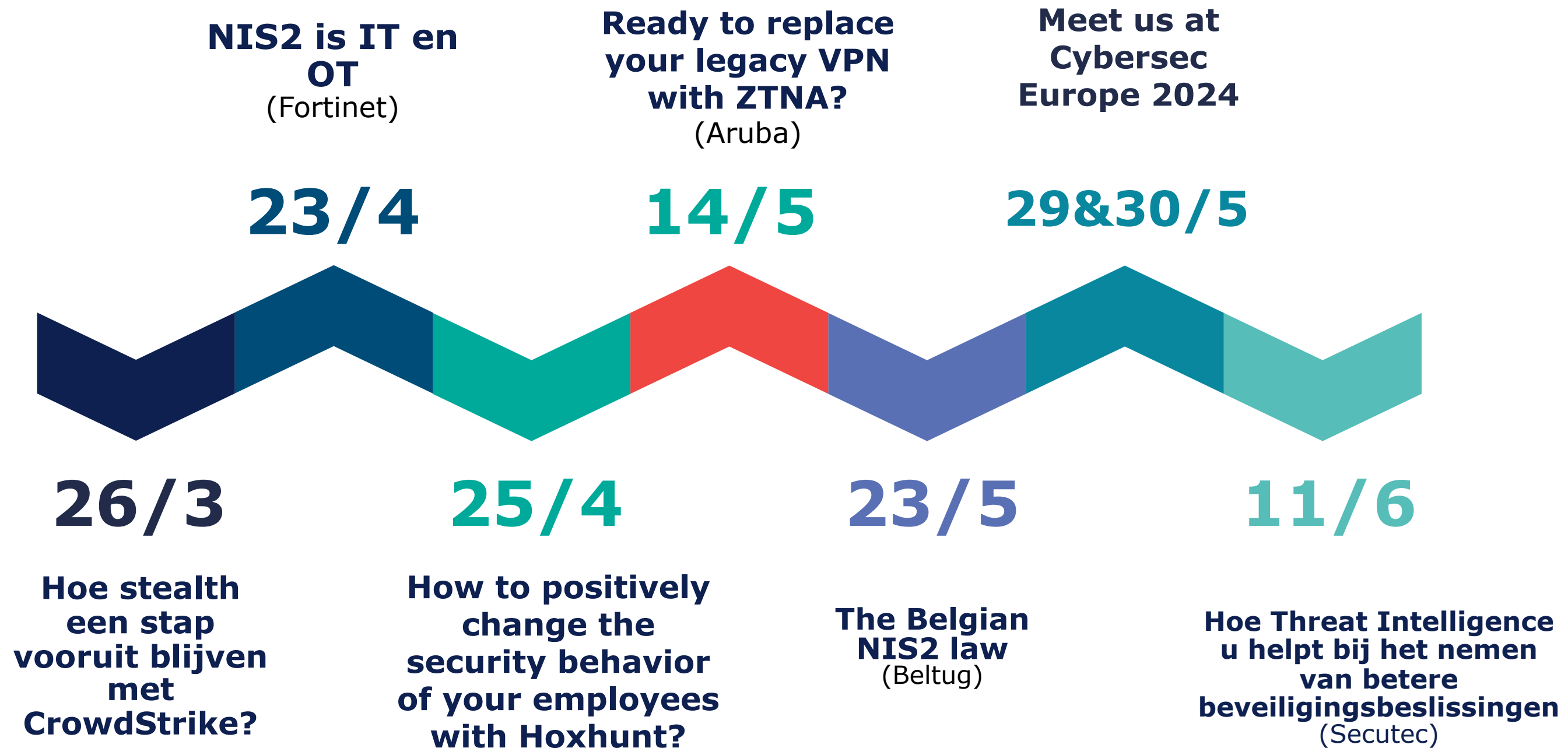
Comprehensive ROI & business case study prepared by human risk practitioner

Included is a 6-week onboarding service to get engagement above 60%

Free 1st QBR with customer success and human risk practitioner



Follow-up events NIS2



inetum 
realdolmen
Positive digital flow

Thank you