



**Human Firewall
Leaders Community**
powered by  sosafe

HACKPROOF HANGOUT



Agenda

Welcome

A warm welcome & football **trivia** to kick things off

Community Updates

New Community Ambassador Programme, First Community Spotlight, Signal Cologne

Speaker Spotlight + Q&A

"From the Dressing Room to the Organisation - How Attackers Use Pressure, Routine and Trust Against Us" by **Aljoscha Thelen**

Interactive Workshop

Build Your Winning Team for Full Awareness - Identify which lessons are mission-critical, optional, or left on the bench when responding to real-world scenarios by **Megan Carlin**

Closing



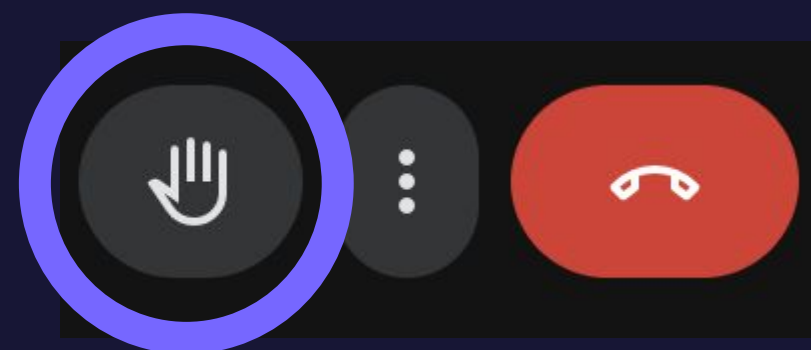
Melissa

Customer Community Manager

How to Participate 🙌

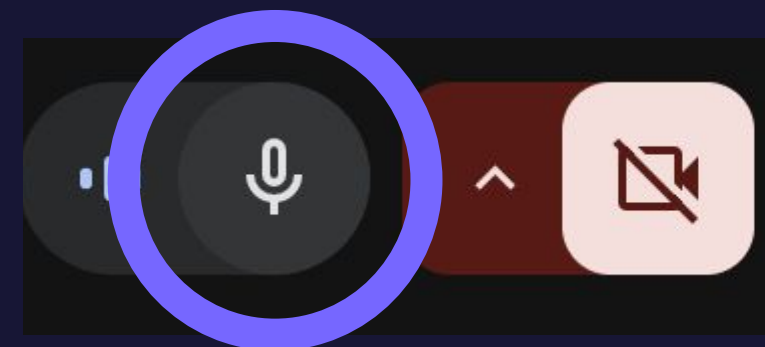
Hand Raise

Please use the **hand-raise feature** before speaking. We'll make sure to call your name in order to keep the flow structured and give everyone space to contribute.



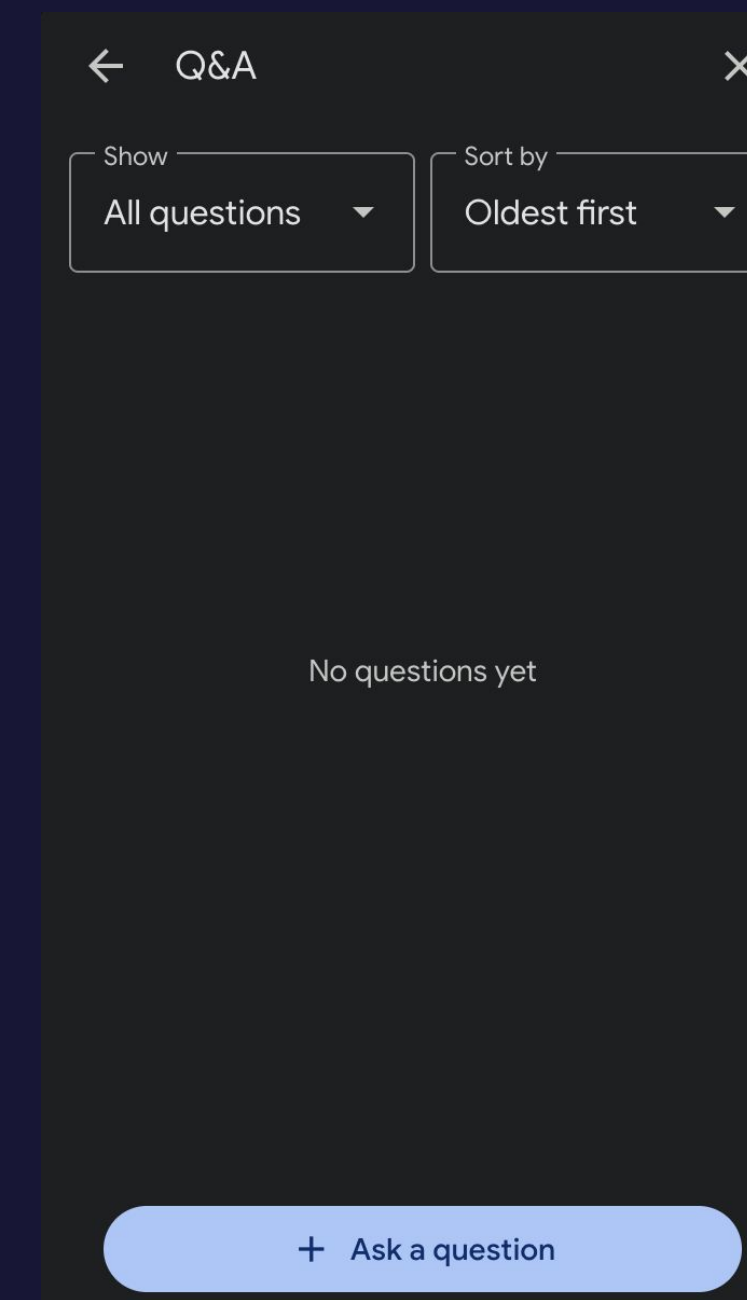
Unmute

Once your **name** is called, feel free to **unmute** and jump in. This helps maintain a clear and organized conversation.



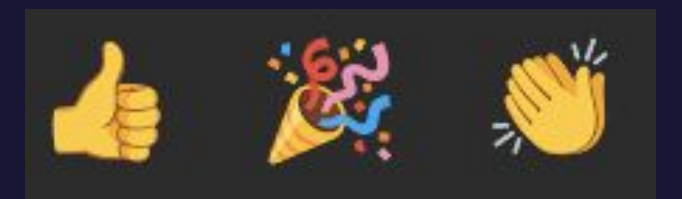
Q&A

You can also **submit questions via the Q&A section** in Google Meet. We'll moderate, read them out and mark them as resolved.

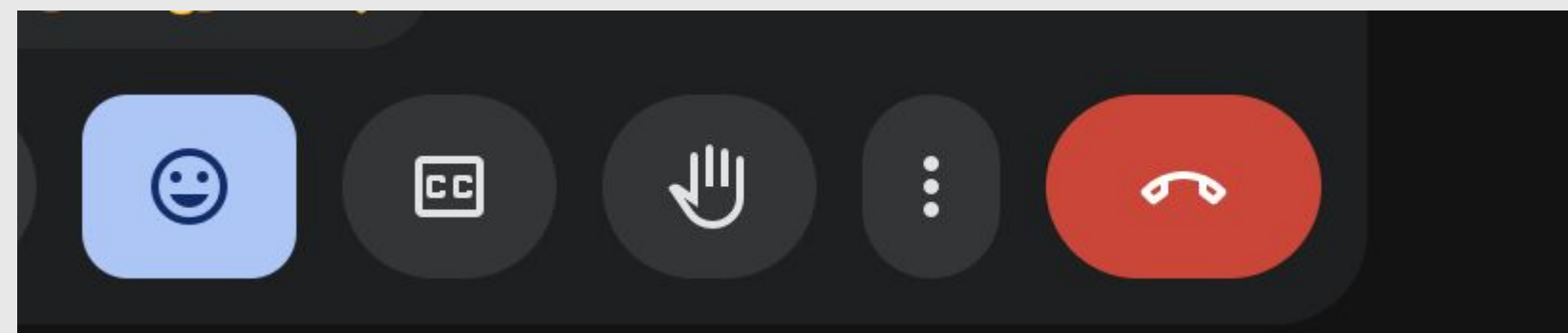


Emojis

Feel free to use emoji reactions to **show agreement or engagement** throughout the session – they're a great non-verbal way to participate.

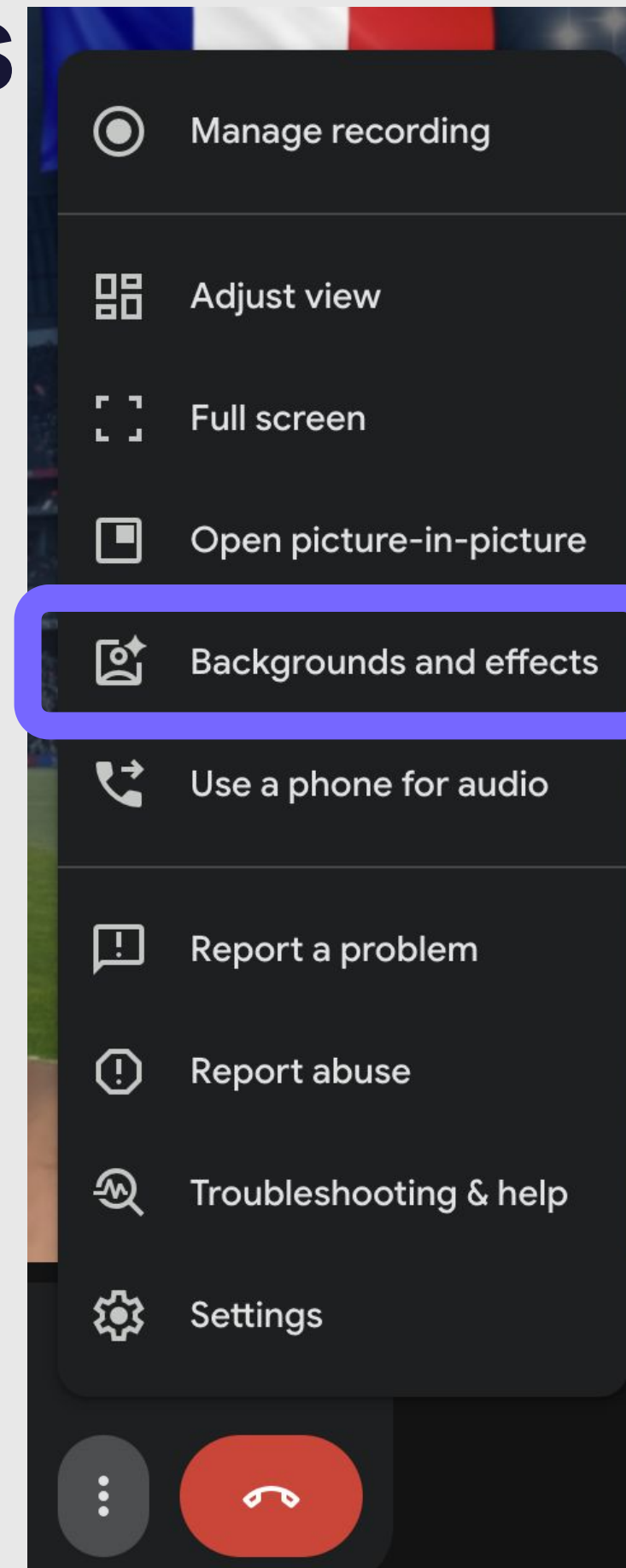


Google Meet Backgrounds



1

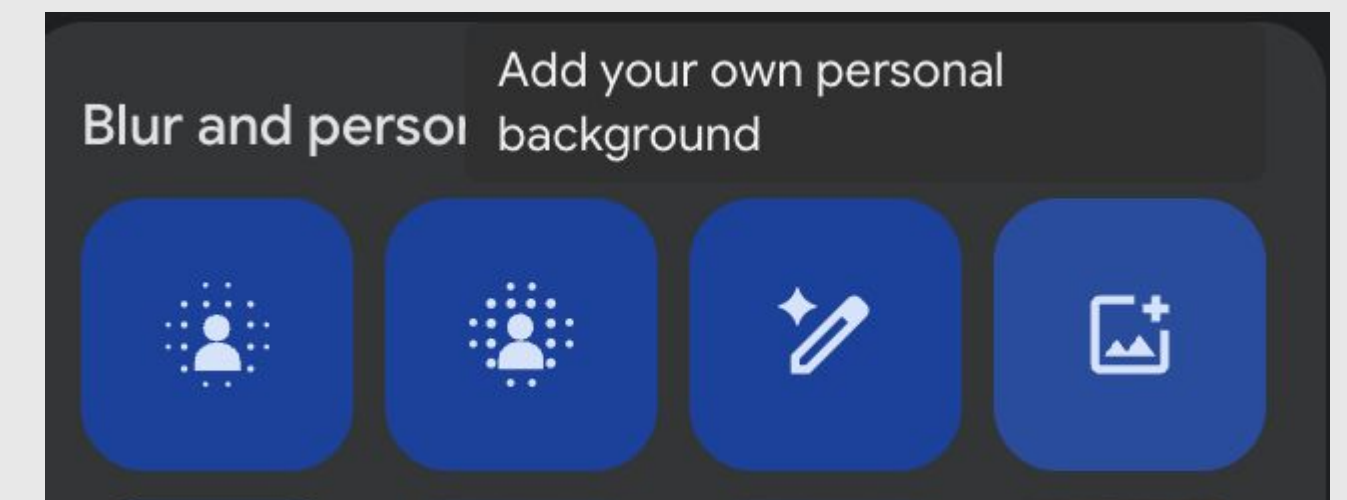
Start by selecting the **dotted line**.



2

Select “**Background and effects**”.

[Google Drive Link](#)



3

The **right button** will allow you to add **your own personal background**.
Simply upload and voilà, you're all set!

Q1: How would you rate your football knowledge?



A: Top of the league



B: Solid midfield



C: Let's see how I do!

Q3: Guess the Player

A: Lionel Messi

B: Jamal Musiala

C: Kylian Mbappé

D: Thomas Müller





Q3: Which of these songs was the official anthem of the 2010 FIFA World Cup?

A: Waka Waka (This Time for Africa) - Shakira

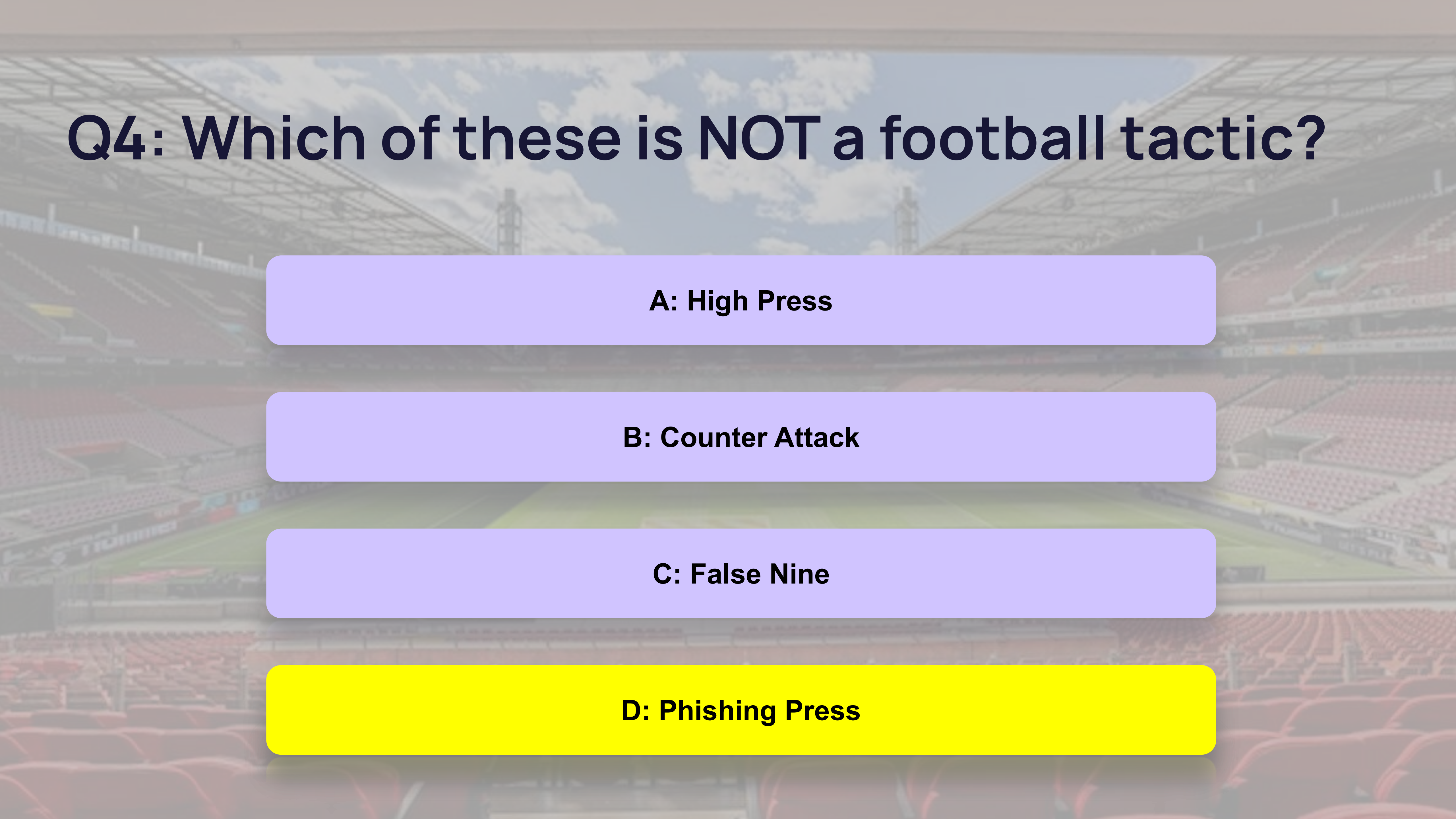
B: We Are the Champions - Queen

C: Wavin' Flag - K'naan

D: La Copa de la Vida - Ricky Martin

Q3: Which of these songs was the official anthem of the 2010 FIFA World Cup?





Q4: Which of these is NOT a football tactic?

A: High Press

B: Counter Attack

C: False Nine

D: Phishing Press

NEW Ambassador Programme: Meet Andrew Rose

Regular discussion starters

A facilitator, not just an expert

Practical lessons, best practices

Advice and peer exchange



Community Spotlight: Lars Schneider

Great communities aren't built on content - they're built on people

03_best-practices

Enhancing Reporting Rates: Ideas for a Wall of Fame Initiative

 [Lars S.](#) · Dec 02, 2025 03:40 PM ·  Share  Open with AI ^

Hi Community, I am currently planning to roll out additional measures to improve the reporting rate among my colleagues. One idea is a “wall of fame”, recognizing the department with the highest reporting rate as our Security Champions. Probably on a quarterly base.

Do you have any best practices or experiences (positive or negative) with this approach? It is not ground breaking but imho a good starting point. I am also planning some goodies/merchandise for the best department.

I would appreciate hearing your feedback or opinions. 😊

👍 1 🏆 1

Posted in 03_best-practices ·  [Lars S.](#) · 12 days ago · 

Using Positive Emotions Like Fun and Appreciation to Improve Security Behavior in the Workplace

[Andrew R.](#) Tbh, I'd go with this kind of approach. Using emotions is in my opinion the most effective way to change or push certain behaviours.

- I try to trigger "fun" by adding some gamification to our security campaigns like team rankings and challenges, for example on our Display in our bistro.
- I also try to trigger "curiosity" by having 1on1 dialogues with colleagues and showing them what is actually going on behind the scenes of our security measures like "how we secure our organization".
- And I trigger "appreciation/trust" by handing out mini lego fishermen with a handwritten card to colleagues who report really dangerous phishing emails or do really good in our e-learning.

I'd always try to avoid negative emotions more than necessary and focus on positive ones instead. But I think it heavily depends on the company culture. Highly regulated organisations might see things a bit differently. 😊

 0 Comments  2  Share

 MEMBER SPOTLIGHT



Lars Schneider

Information Security Officer
at Advanced UniByte GmbH

Member since Oct 2025

“If security never creates friction,
it’s probably not working.”

[Read the full story](#) and share
Kudos 🙌

03_best-practices

Resources and Tips for Preparing Business Continuity Management Against Ransomware Attacks

 [Lars S.](#) · Jul 01, 2026 06:38 AM ·  Share  Open with AI ^

I don't know if everybody has a similar challenge, but lately I had a longer discussion about ransomware groups, preparing for a ransomware attack, etc. The following source helped me a lot to get insights into ransomware negotiations and how to prepare. Maybe you are as curious as I am, or need to prepare your BCM for ransomware attacks:

[ransomware.live](#)

💡 1



[Lars S.](#) · about 1 month ago (edited) · 

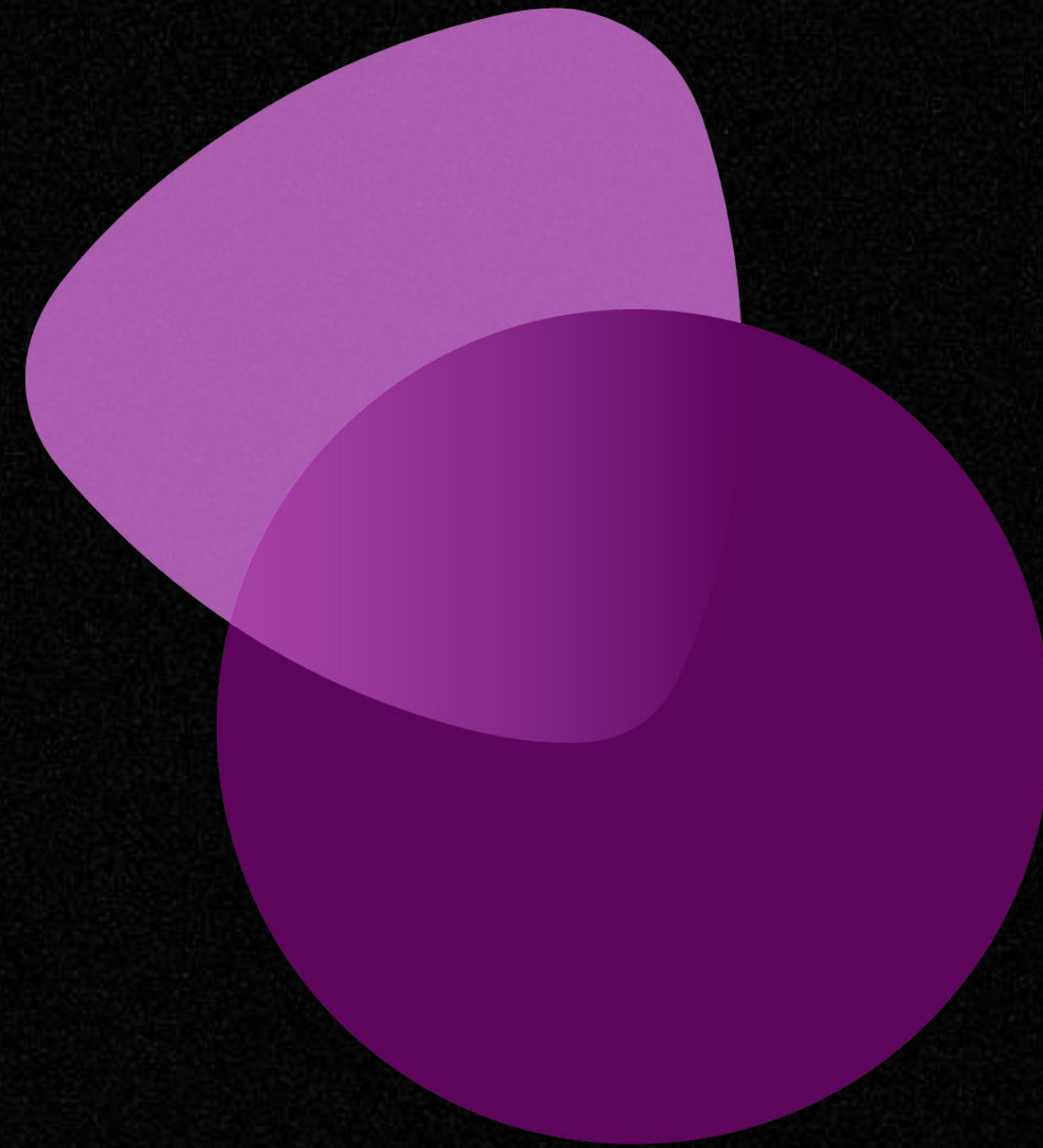
In my experience, it's important to "make security easy," be present, create opportunities for dialogue, and keep colleagues involved in security measures. At the same time, we need to utilize technology to "make insecure behavior hard."

"Trust but verify" never worked for me because if you know your organization and culture, you don't need to verify. You already know the security gaps, and the struggle is more about how to close them.

Edit:

Some thoughts: Trust ist important, but it has a time limit and requires to be regular renewed. Trust is subjective and cant really be measured and therefore cant be a base for decision makings.

👍 1 🗨️ 1



Signal Security Summit

by SoSafe

**The Security
Summit by
SoSafe**

November 18, 2026
Die Halle Tor 2, Cologne

Europe's leading security
event **focused on the
human factor.**

Save your seat



Signal Cologne.



The Security Summit by SoSafe

November 18, 2026

Die Halle Tor2, Cologne



1200+

ATTENDEES

35+

SPEAKERS

6

STAGES & BREAKOUTS

20+

SESSIONS

FEATURED SPEAKERS



Henry Coutinho-Mason

Future Trends & AI Strategist



Hans-Dieter Hermann

Sport Psychologist of the German National Football Team (2004-2024)



Dr. Niklas Hellemann

CEO and Co-founder, SoSafe



Dr. Christian Reinhardt

Director of Human Risk Management, SoSafe



Shannon Jaritz

SVP Customer Success, SoSafe

Speaker Spotlight



Aljoscha Thelen
Teamlead IT-Infrastructure, Deutz AG

From the Dressing Room to the Organisation - How Attackers Use Pressure, Routine and Trust Against Us

From the Dressing Room to the Organisation

How Attackers Use Pressure, Routine and Trust Against Us

- 1 Principle of **ClickFix**?
- 2 Boring Stuff, but important to know
- 3 **Our Incident**: From Attack to Defense
- 4 Lessons from the “First Game” – What went well, and what didn’t?
- 5 Preparing for the “Next Game” – Training & Awareness
- 6 The **Next Game**

1

Principle of ClickFix?

What is ClickFix?

- **ClickFix** is a **scam** used by cybercriminals in which employees are tricked into carrying out malicious actions themselves by following **seemingly harmless instructions**. .
- The attackers often pretend they want to “fix” a technical problem::
 - a supposed error on a website
 - a notice about a required login
 - a request to “fix” something
 - a supposed security check
- The danger here is that the malware doesn't always come in the form of a traditional attachment or link. That could be filtered out by Email gateways etc. Instead, victims are prompted to copy and paste commands or launch programs themselves
- See **Human Firewall Podcast** : [True Cyber Crime, Der Axios Hack](#)

2

**Some boring stuff, but
Important**

Background of Situation at DEUTZ AG

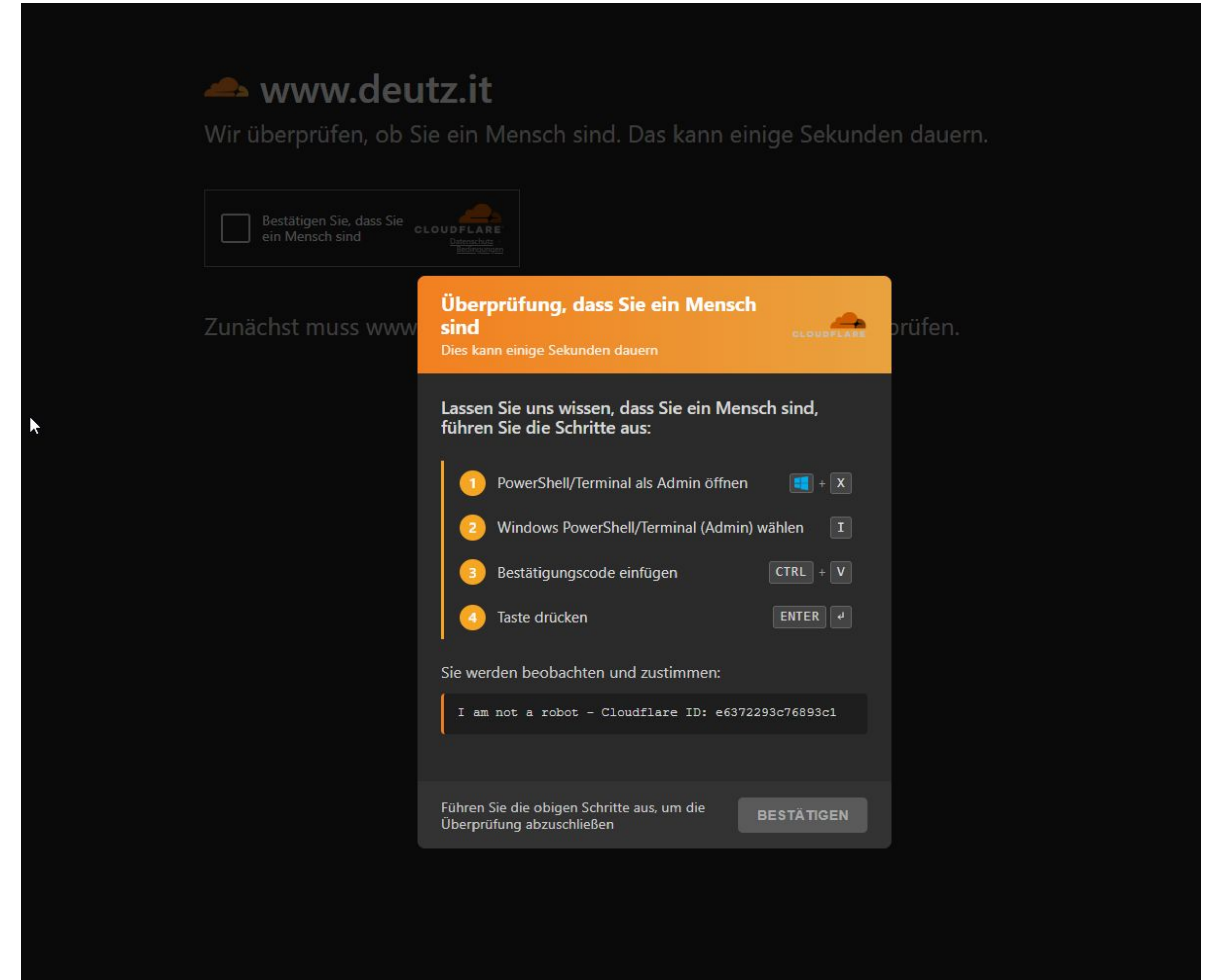
- 162 year old company, just in a **huge restructuring** (as every 25 Years ;))
- **Massively growing:**
 - **2016 Start of insourcing 2200 user, 80 server, 2500 Clients, one country**
 - **2022 3300 user, 400 server , 8 countries**
 - **2026 8000 user, 800 Server, 24 countries, 7500 Clients,**
 - **Expectations: in 2026 additional 1000 user, unknown number of devices and server.**
- Amount of people in IT Infrastructure **teams stabel since 2022**, no adjustments

2

Our Incident: From Attack to Defense

The Attack

- Compromised supplier/service website with a fake security prompt (Cloudflare screen / security check)
- "Vidar" information-stealing malware designed to extract sensitive data, particularly stored login credentials from browser profiles
- Employees follow the instructions from the Fake-Box—some with admin privileges



The Defense

- Technical Defense (Defensive Line)
- When the connection was established, the EDR system triggered an alert and reported it to the SOC.
- All outbound connections were automatically blocked.
- Immediate Measures:
 - Suspension of all accounts
 - Isolation of the affected clients
 - Change of all passwords
 - Forensic investigation



3

Lessons from the “First Game” – What went well, and what didn’t?

Game Analysis

What went well:

- A playbook for this type of incident was in place
- Everyone involved responded quickly and followed the guidelines
- Those affected actively cooperated
- The EDR system blocked the connections

What went wrong:

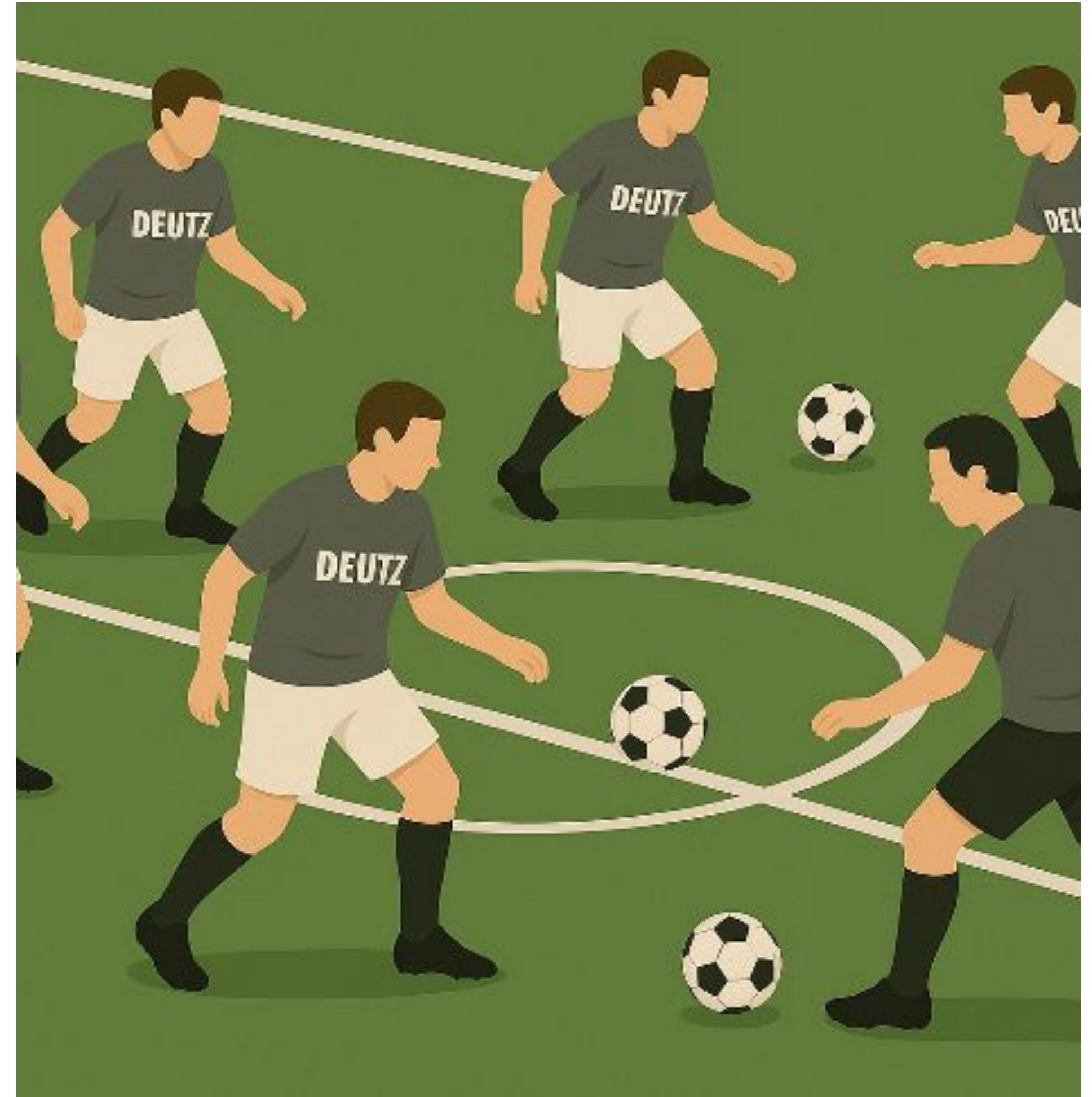
- Browsing the website “on the side” during a stressful work situation
- A colleague had temporarily obtained local admin rights for testing purposes
- The combination of isolating the PC from network and a USB lock made the forensic analysis more difficult. The Playbook and an analysis environment were still missing for this.

4

Preparing for the “Next Game” – Training & Awareness

Practice for the next game

- Organizational / Human Approach
- Root Cause Analysis: Why were the instructions carried out? Employee motivation and decision-making processes
- Involvement of Those Affected: An employee agrees to present the incident at a departmental meeting
- Development of training materials for employees (web-based training + newsletter)
- Development of test-phishing simulation and deploy it to our employees
- Updating the playbooks, setting up a forensic environment



5

The Next Game

The Next Game

A supplier's website was compromised; same type of attack

- Employees immediately blocked access
- The EDR system responded faster
- The entire process was completed significantly faster

Perceptions within the company have changed. IT security is a “team player”—not just a hindrance, a source of complications, or a monitor.

There is a high level of engagement and a willingness to openly address one's own mistakes, though this varies by country.

Thank you

DEUTZ AG

Ottostrasse 1

51149 Cologne, Germany

Phone: +49 (0) 221 822 0

Fax: +49 (0) 221 822 5850

Email: info@deutz.com

www.deutz.com





Interactive Workshop



Megan Carlin
Senior UX Researcher, SoSafe

***Build Your Winning Team for Full Awareness -
Identify which lessons are *mission-critical*,
optional, or *left on the bench* when
responding to real-world scenarios***

Research Session: Build Your Winning Team for Full Awareness



What we want to know

How do you choose your modules to build an awareness campaign? What are your decision-making criteria, and how do you figure out which information is relevant?



Why we want to know it

To support new joiners onto our platform and make module choice easier when they are faced with so many options when they join SoSafe.



How we will find it out

By playing through the activity together on the Miro board.



Join the Game

Miro board link:

<https://miro.com/app/board/uXjVHFbsfrw=/>

Password:

(Start with looking over the players 😊)

It's World Cup season, so let's build our teams

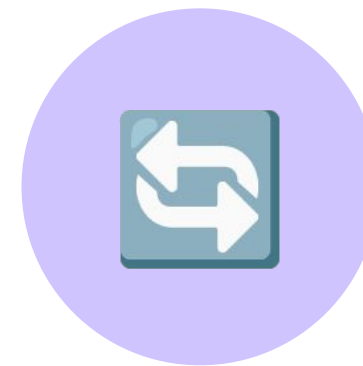


Your campaigns are the teams. The modules are your players. You're the manager: pick your squad and decide who makes the cut.



Starting line-up

The mission-critical modules. The lessons every new joiner has to play from day one.



On the bench

Optional or situational modules. Good to have, brought on when the scenario calls for it.



Left on the bench

Modules that don't make this squad. Tell us why they sit this one out.



For every pick, tell us why they made your line-up



How It Runs

Activity Guidelines



1

0 to 5 min

Vote for a challenger

- NIS2
- GDPR
- An upcoming audit
- Your latest Incident

2

5 to 10 min

Build your squad

- 3 minute rush to place your picks
- Vote to “Axe” anything you disagree with

3

10 to 20 min

Review the line-ups

- Go through the choices together
- Start with any disagreements

4

20 to 30 min

Repeat as Possible

We'll run another round if there is time and appetite

Times are a guide. The final block flexes to fit the room.



Stay Vigilant &
See You Soon 🏈👋