



Partnership for
Cyber Security
Innovation

Early Warning System Insider Attacks

Partnership for Cyber Security Innovation is a collaboration of



ING 

 ABN-AMRO

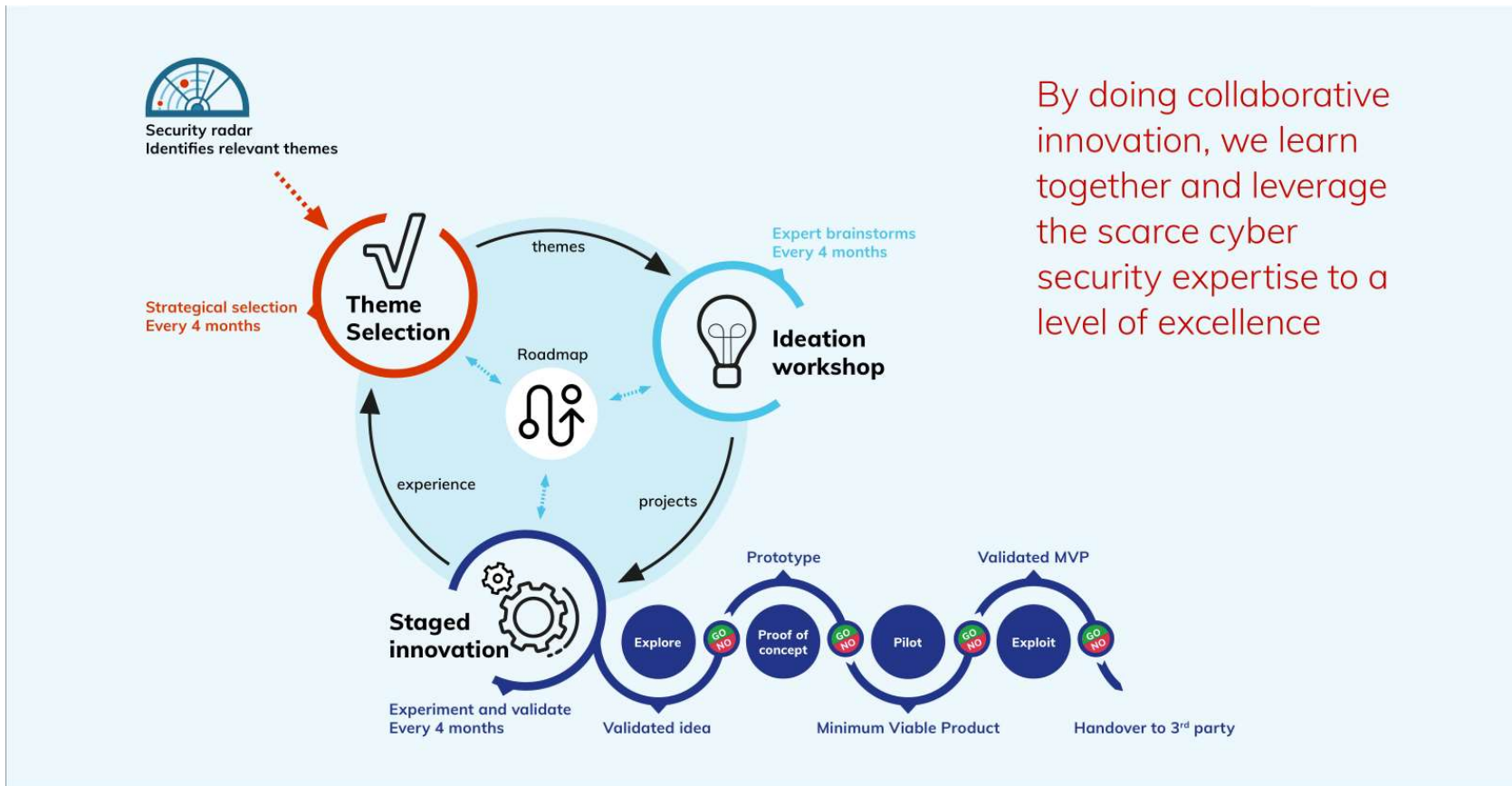
achmea 

TNO

de volksbank

ASML

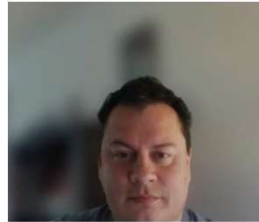
From Explore to Experiment



Who is our team?



Krista van Kan (de Volksbank)



Jeffrey Janssen (ABN AMRO)



Ellen van Bergen (TNO)



Tineke Hof (TNO)



Rick van der Kleij (TNO)



Age Kruijssen (TNO)

Business sponsors: Suzanne Janse (ING)

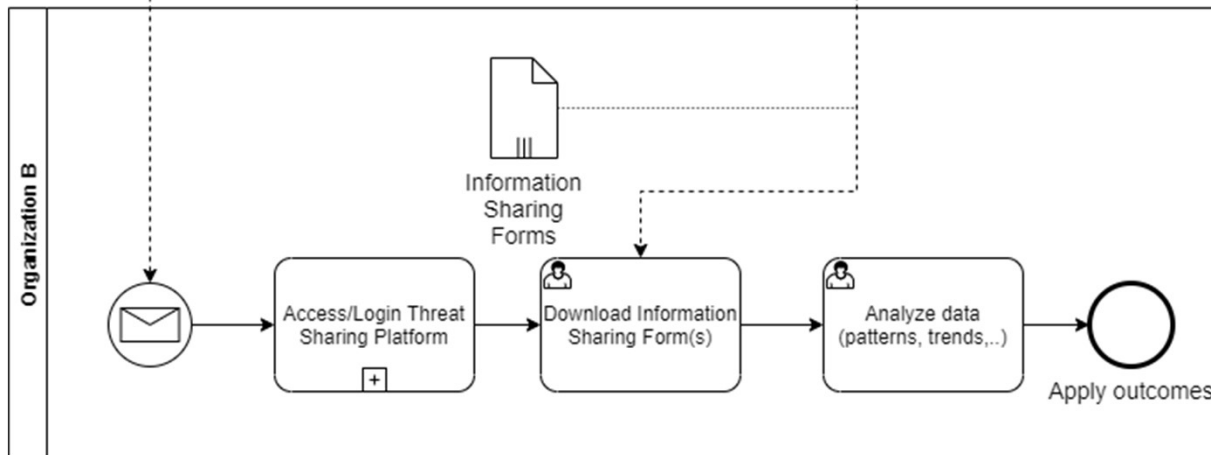
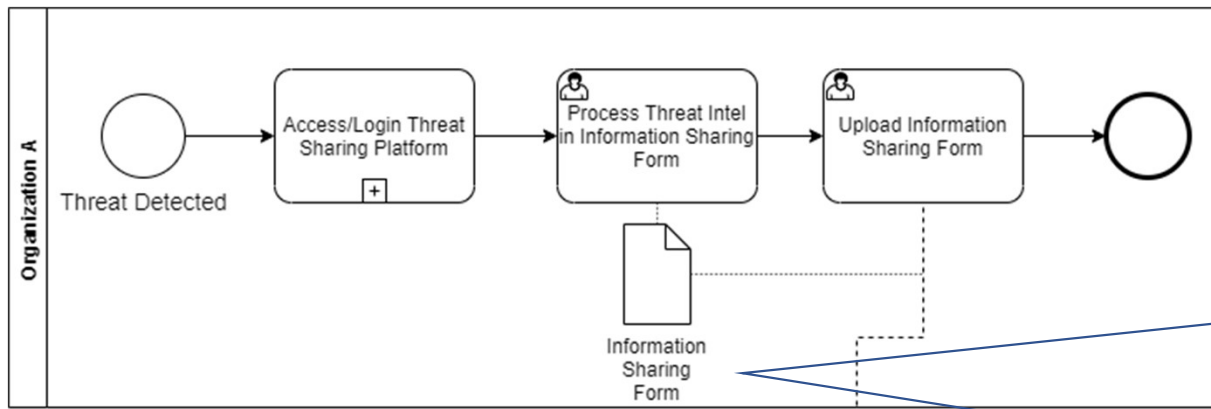
Scope & goal

- Solution for more collaboration **to prevent** or **to detect** an insider attack **in an early stadium**.
- Insider attack: Person **inside an organisation** with rightful access to an organisation's systems, data, and resources, who **deliberately** and **intentionally** abuses the organisation's assets
- New insider attack modus operandi emerge all the time and are replicated in other organizations shortly
- The earlier you know what to look for, the earlier an insider attack can be stopped
- On **early warning platform** parties can exchange information on actual modus operandi in a **rapid** and **secure** way



Animatiefilmpje project

- <https://youtu.be/fel9bxc2uZ0>



5. What type of damage did you identify *

- Theft of intellectual property
- Theft or trading (confidential) information
- Cashout activity
- Reputational
- Operational
- Other

6. Could you describe the beforementioned damage? *

Form



PCSI Insider Attack - Description Form

The form will take approximately 10 minutes to complete.

This form is used to gather information regarding new and/or upcoming modus operandi of insider attacks. An insider attack is an action with malicious intent from within the organization to the organization's network, system, or data for personal, financial or other form of gain, or to deliberately damage the organization. Insider attacks can be performed by full-time employees, independent contractors, interns, and other staff. Insiders are trusted and privileged (some more than others).

This form contains 5 sections: Actor, Script, Discovery, Impact, Corrective actions. Each section captures a different aspect of the insider attack narrative and will be used to get out an early warning to other financial organisations.

These sections summarise the incident narrative of "who did what to what (or whom) with what result" into a form suitable for analysis.

...

* Vereist

Incident summary

1. Please provide a brief summary of the incident *

Voer uw antwoord in

Volgende

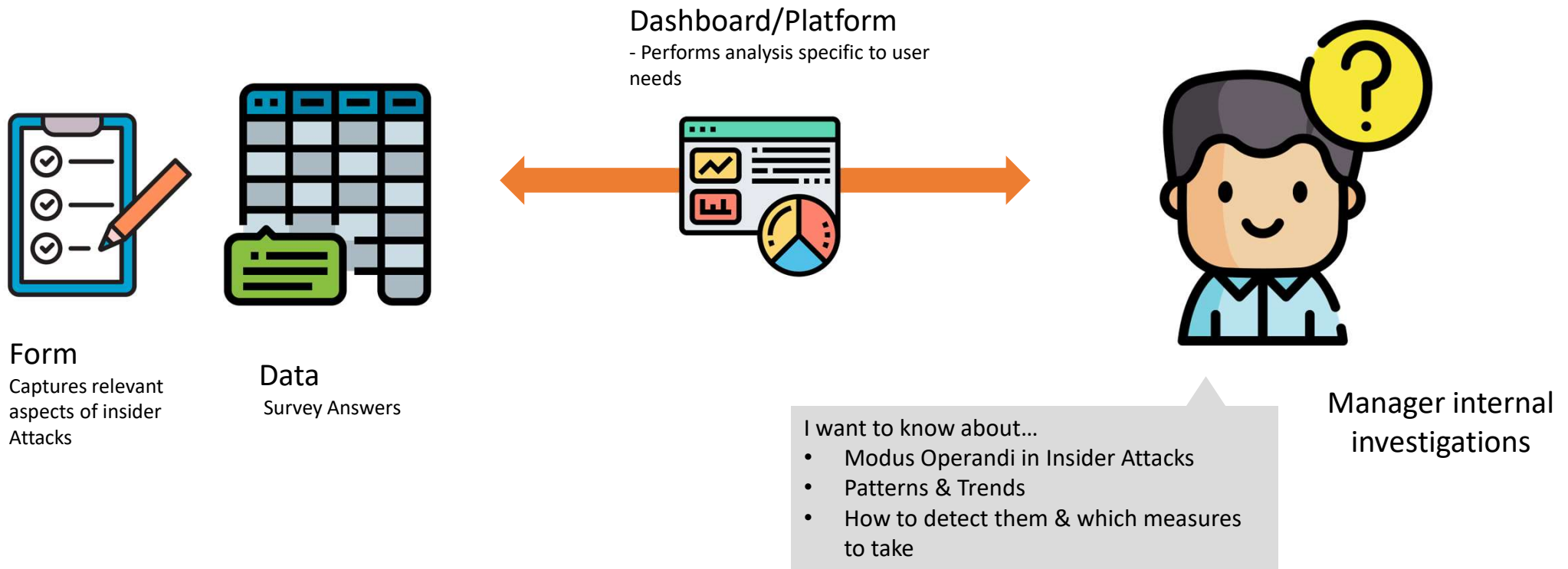
Geef nooit uw wachtwoord. [Misbruik melden](#)

Sections Form

1. Incident summary
2. Actor
3. Script of the incident – What happened when?
4. Discovery
5. Impact on the organisation
6. Corrective actions

Every section contains serveral questions

Dashboard Prototype



Dashboard Prototype



[HOME](#) [SEARCH](#) [PATTERNS AND TRENDS](#)



Early warning system insider attack

When an attack comes from the inside, the impact of an attack can be catastrophic, and could cause financial, reputational and regulatory consequences.



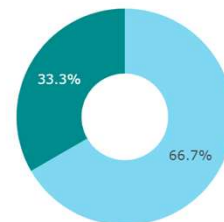
PCSI Insider Attacks - Dashboard

Motives



- Convenience of expediency, opportunistic
- Ignorance
- Financial or personal gain

Incident type



- Asset misappropriation / theft
- Financial Statement Fraud or reporting fraud

Discovery

- 🖥️ 50% Internal - IT audit or scan; Internal - HR sample survey
- 🔍 50% Internal - someone witnessed suspicious actions of the actor

Approach & Outcomes



APPROVAL TO SHARE DATA



FORM UPDATES



EXPLORED EXISTING
PLATFORMS: BKR, NVB,
TMNL, NDN



LEARNINGS FROM OTHER
SHARING COMMUNITIES



TALKS WITH PROVIDERS:
SIGNPOST SIX & UK
FINANCE



ANIMATION VIDEO



BRAINSTORMS WITH
BUSINESS SPONSOR

Process Learnings



Sharing information is a big challenge

Technical
Approvals
Time-wise



Exploration is never completed

“Have you spoken to this organisation?”



Parties further away still give valuable and new perspectives

Next phase

We have done:



Market scan



Form
improvements



Data analysis &
Dashboard



Identifying
collaboration
partners

We need to do:



INVOLVE THE RIGHT
STAKEHOLDERS



VALIDATE THE VALUE
OF THE SOLUTION



FURTHER IMPROVE OUR
SOLUTION (CONTINUOUS
LY)

Good advices?
Want to know more?
Visit us!