Partnership for
Cyber Security
Innovation

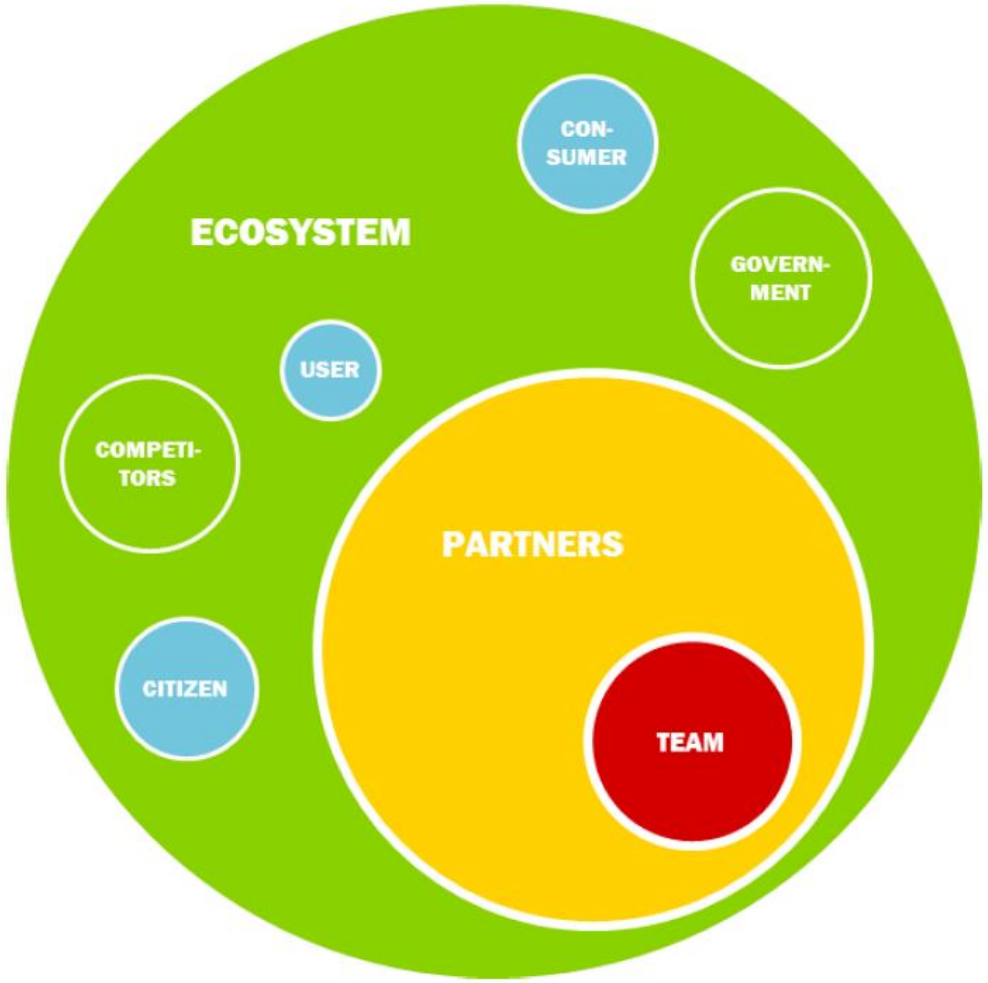
# Orchestrating Innovation for Cyber Security

# Partnership for Cyber Security Innovation - PCSI

Reinder Wolthuis
June 2022

# ORCHESTRATING INNOVATION

- Increasingly innovation and entrepreneurship transcend the boundaries of individual organizations
- They take place in so-called business ecosystems consisting of local communities, SMEs, large corporations, NGOs, and governments.



# ORCHESTRATING INNOVATION

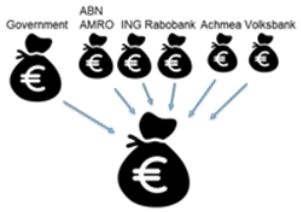

- Orchestrating Innovation is the way of working that is applied to start, shape manage and expand innovation in an ecosystem.
- The ultimate goal is to create value for the actors involved and society at large.
- https://orchestratinginnovation.nl/

The Partnership for Cyber Security Innovation - PCSI is an example of such an ecosystem, focussing on cyber security innovation

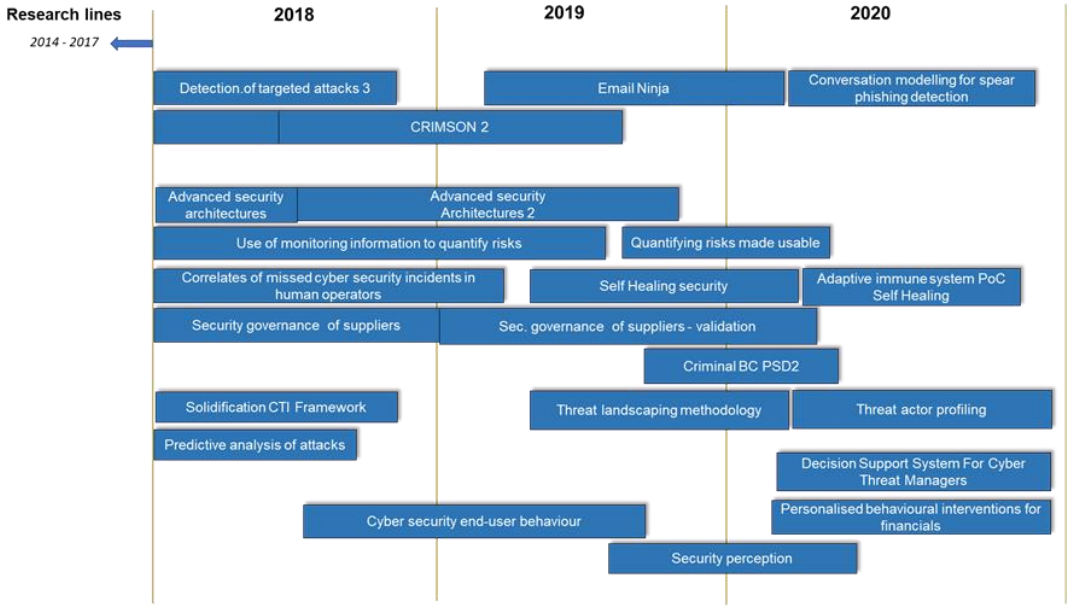
# PCSI predecessor: Shared Research Program Cyber Security (2014-2020)

Shared working

Sharing data




Shared funding




Shared Research Program cyber security
2014 - 2020 (and possible extension)
Yearly 1 million euro to innovate on cyber security

ABN·AMRO Rabobank ING achmea de volksbank TNO innovation for life

https://www.tno.nl/srpcybersecurity


Direct application of results by partners and increase resilience society by publications, presentations, spin-offs etc.

PCSI is a collaboration of

ABN·AMRO achmea ASML ING TNO de volksbank

Our mission

# With a volatile threat landscape developing at an alarming pace, we have partnered up to join forces and create a holistic cyber security approach with a focus on innovation

Shared workload

Shared learnings

Shared funding

Isolated protection | Leaves gaps


lack of innovation | isolated efforts

Shared innovation | Creates bonds


focus on innovation | joint effort

PCSI is a collaboration of

ABN·AMRO achmea ASML ING TNO de volksbank

# Craftmanship development

Collaborative workforce that speeds up craftmanship development

- Working collaboratively on an innovation with peer experts
- Opportunity to deepen existing knowledge by working in innovative projects
- Cooperation between operational oriented people and scientific oriented people (TNO) leads to interesting results
- Knowledge transfer from TNO to PCSI partners (presentations, webinars)

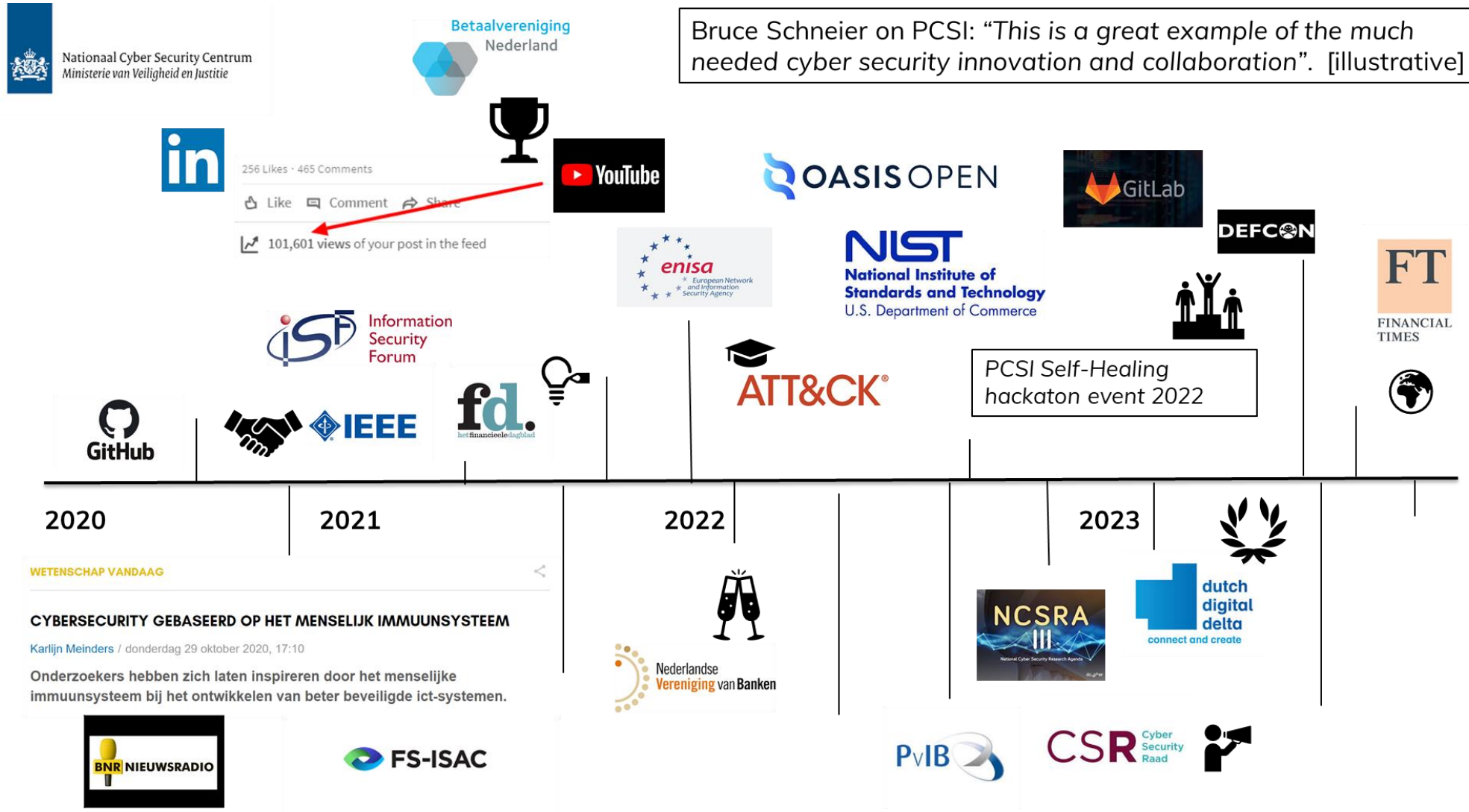
# Employee engagement

Step out of the day-to-day, build new capabilities and enhance employee engagement

- Stepping out of the daily operational job to work on innovative ideas
- High energy creative sessions to Ideate from selected trend to project pitch
- Competence development (brainstorming, Dragon's Den pitching, etc.)
- Opportunity to present results to the cyber security community (webinars, events, articles, website)
- Building networks of experts


The PCSI innovation process is facilitated by professional coaches

# Our ambition (1) Roadmap to impact




Bruce Schneier on PCSI: "*This is a great example of the much needed cyber security innovation and collaboration*". [illustrative]

PCSI is a collaboration of

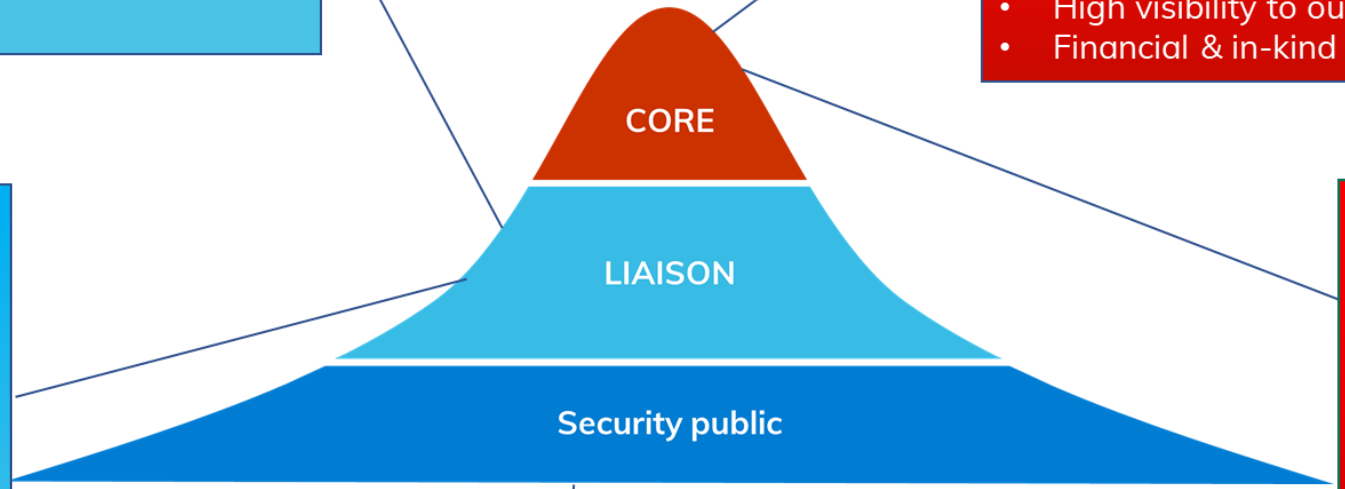
ABN·AMRO achmea ASML ING TNO de volksbank

Our ambition (2)

# Building the cybersecurity innovation ecosystem

- Closely informed on progress & results
- Provide feedback and suggestions
- Occasional involvement in projects when mutual beneficial
- Some in-kind contribution

- Steering Strategic direction
- Participating in projects
- Pilot experience
- Profiting from all results
- Full learning experience
- High visibility to outside world
- Financial & in-kind contribution




Current:
- Connect2Trust
- Gemeente Amsterdam-CTO innovation team
- Crowdstrike
- Security academy
- Ordina
- ONVZ
- Rabobank
- Securify
- Orange Cyber defense
- Niagara networks
- Cybertrap
- DTACT

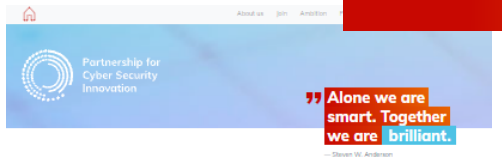
- Access to information via website, webinars and social media

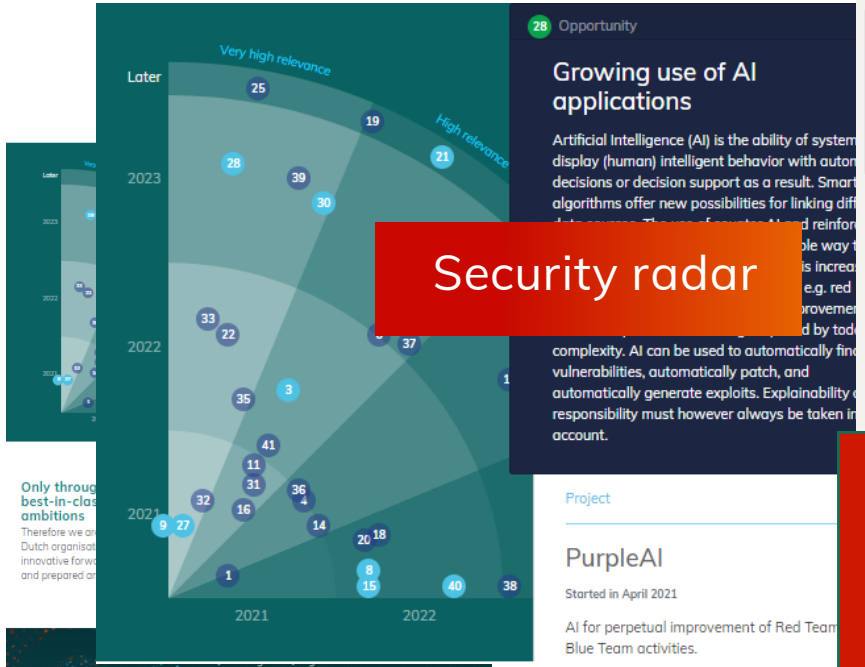
Current:
- ABN AMRO
- Achmea
- ASML
- ING
- TNO
- De Volksbank

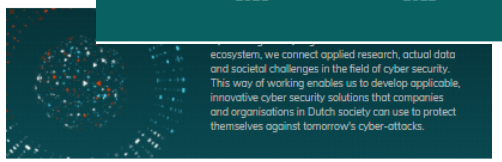
Potential:
- Dutch tax services
- Ahold
- Shell
- ..

# Our brand

## pcsi.nl website



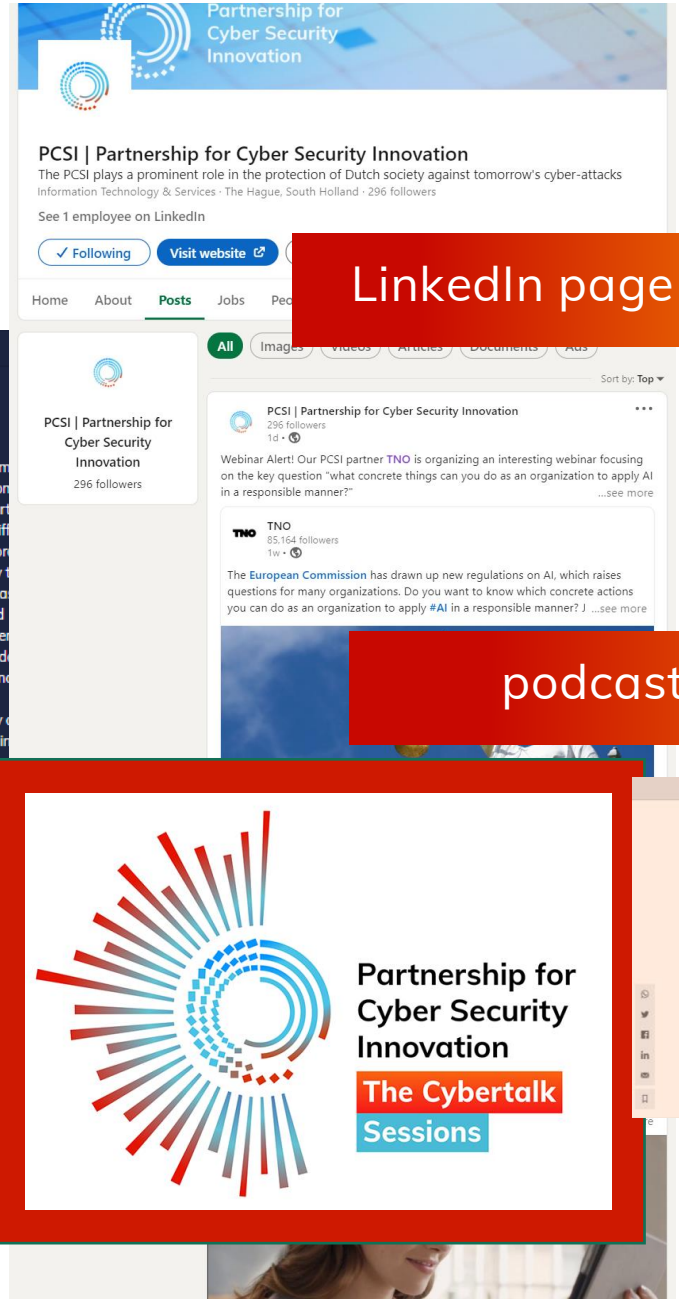








## Security radar

## LinkedIn page




## webinars



## podcast





## Media exposure





PCSI is a collaboration of

ABN·AMRO achmea ASML ING TNO de volksbank

How we work

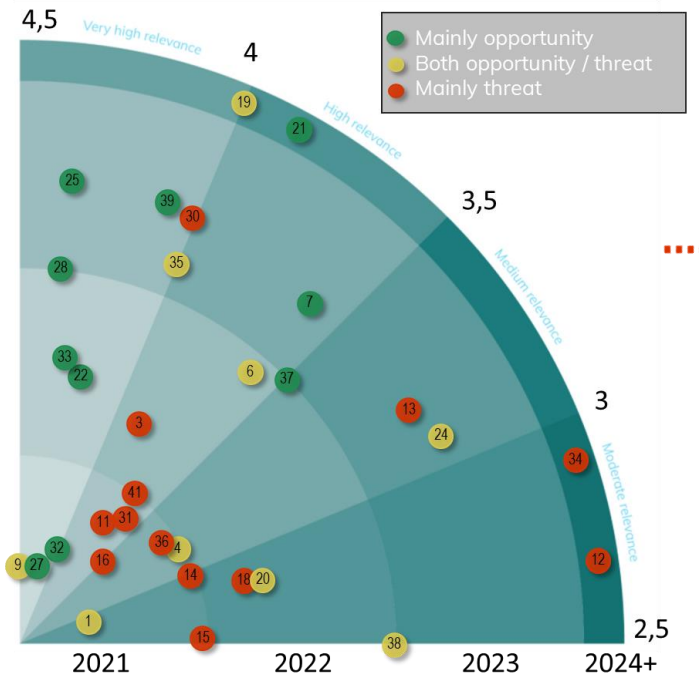
# Our security radar identifies themes and trends that are relevant to our partners, after which we cooperatively decide which themes are selected for ideation & staged innovation

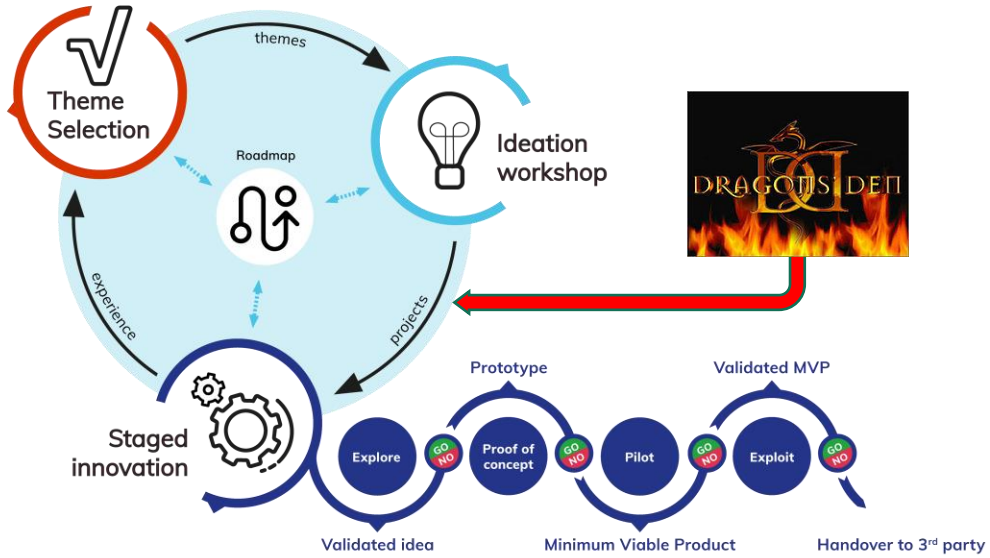
Collaborative ‘orchestrating innovation’ way of working

## Top 10 most relevant trends

(Highest average score for impact and fit with PCSI)

| # | Trend |
|---|---|
| 9 | Growing dependency on third parties |
| 33 | Growing need for security automation in cyber defense |
| 25 | Growing willingness to join forces (inter)nationally |
| 28 | Growing use of AI applications |
| 22 | Growing importance of identity and access management |
| 27 | Increasing use of agile software development |
| 39 | Growing interest in zero-trust initiatives |
| 19 | Maturing of quantum technology |
| 30 | Increase of malicious uses and abuses of AI |
| 32 | Growing need for impactful awareness campaigns and behavioral change programs |



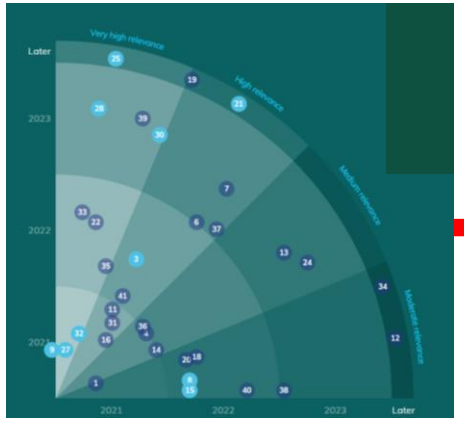



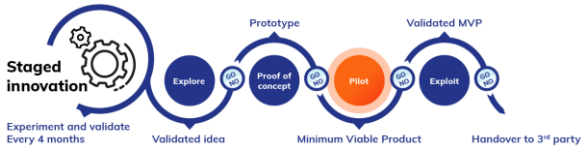

PCSI Cyber Security Radar identifies threats and opportunities in terms of urgency and impact
Specifically developed for the PCSI with expert input from all partners.

PCSI is a collaboration of

ABN·AMRO achmea ASML ING TNO de volksbank

# Example of projects & results



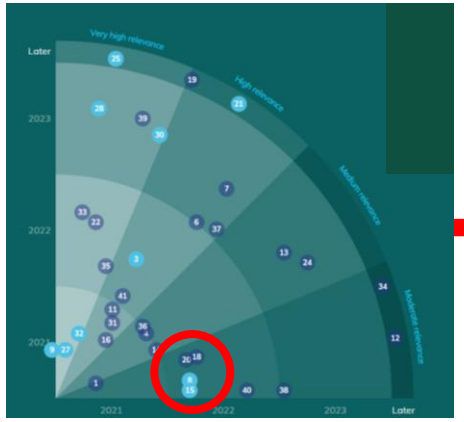



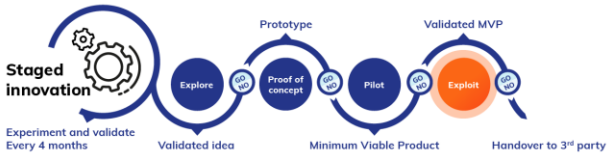

## Early warning system insider attacks

### Trend 15: Growing number of insider attacks

Employees are increasingly getting involved in data leaks intentionally or unintentionally due to social as well as technical reasons. A growing market has emerged for confidential data on the Dark Web. As a result, on the social side, data is increasingly being stolen and sold by malicious employees or used in other kinds of ways. There are different forms of intentional insider attack threats; e.g. an employee radicalizes, is extorted or has been premeditated to work in an organization. Also due to technical reasons (access without official permission) attacks (can) take place.

See the previous presentation & table outside (Ellen van Bergen & Krista van Kan)

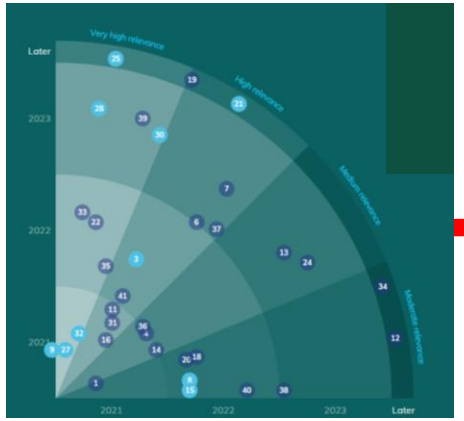


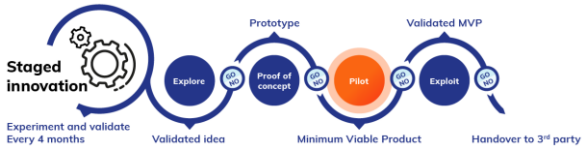




## Automated data labeling for unstructured data

### Trend 8: Stricter rules and enforcement on information sharing

The DNB ('toezichthouder') is paying more attention to privacy, as expressed in the GDPR, and other regulations. For example it becomes more important to demonstrate compliance with privacy regulation at every step taken in capturing or modifying data.




## PurpleAI

### Trend 28: Growing use of AI applications

Artificial Intelligence (AI) is the ability of systems to display (human) intelligent behavior with automatic decisions or decision support as a result. Smart algorithms offer new possibilities for linking different data sources. The use of counter AI and reinforced learning for detection could be a possible way to make cyber security more effective. AI is increasingly used by defenders and attackers both, AI can be used to automatically find vulnerabilities, automatically patch, and automatically generate exploits. Explainability and responsibility must however always be taken into account.

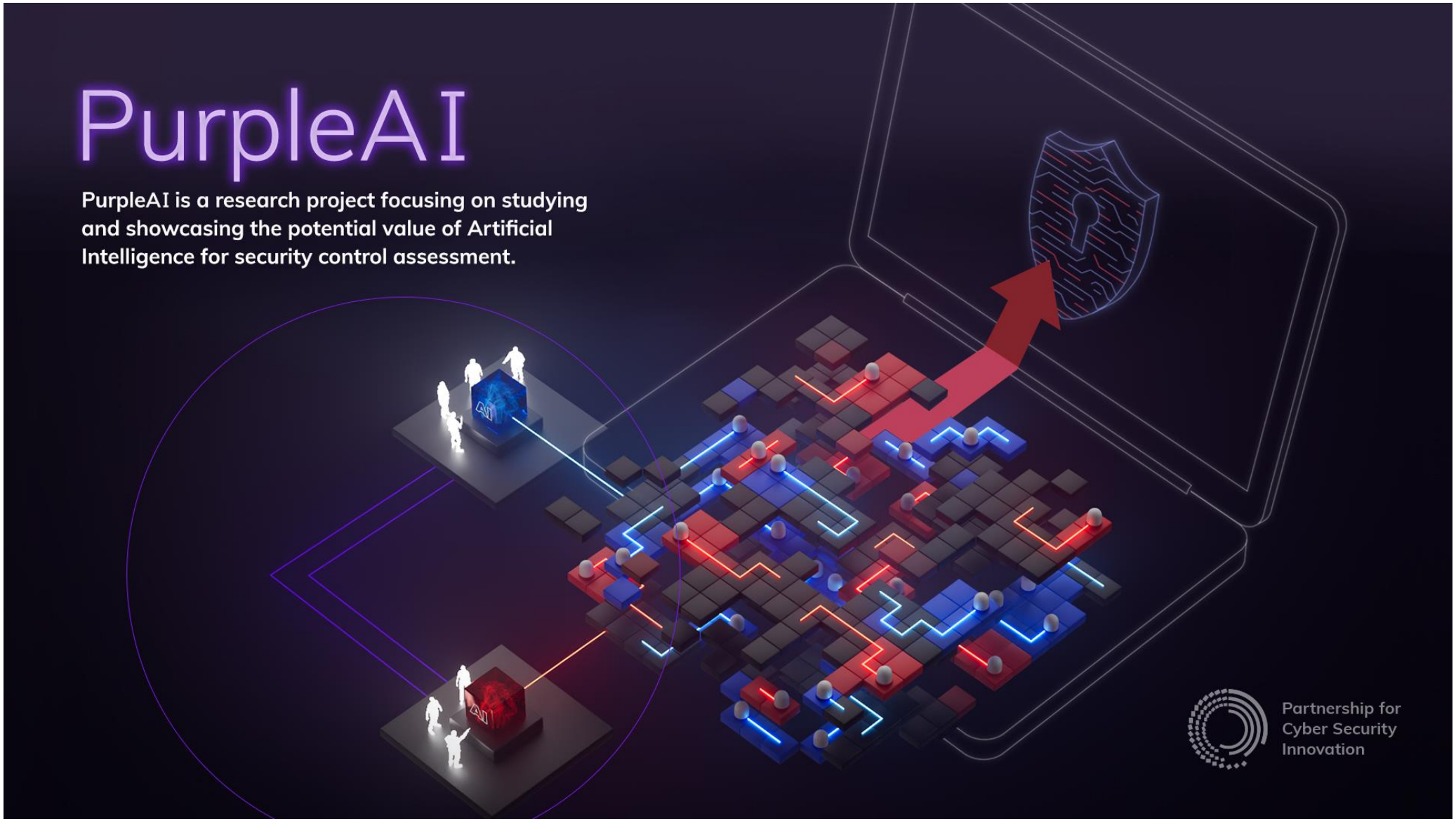
&

### Trend 30: Increase of malicious uses and abuses of AI

Artificial Intelligence (AI) is the ability of systems to display (human) intelligent behavior with automatic decisions or decision support as a result. Smart algorithms offer new possibilities for linking different data sources. The use of counter AI and reinforced learning for detection could be a possible way to make cyber security more effective. AI is increasingly used by defenders and attackers both, e.g. red teaming can experience significant improvements as traditional penetration testing outpaced by today's complexity. AI can be used to automatically find vulnerabilities, automatically patch, and automatically generate exploits. Explainability and responsibility must however always be taken into account.

# PurpleAI

PurpleAI is a research project focusing on studying and showcasing the potential value of Artificial Intelligence for security control assessment.




Partnership for Cyber Security Innovation

PCSI is a collaboration of

ABN·AMRO achmea ASML ING TNO de volksbank

# PurpleAI use-cases

## Red team use-case

**Goal:**

Learn a machine learning model to perform red team actions such as reconnaissance, privilege escalation and lateral movement starting from an employee laptop while blending in with normal user behavior

**Business value:**

- Improving infrastructural resilience
- Knowledge about optimal attack paths for the blue

## Blue team use-case:

**Goal:**

Optimize tripwire placement using a reinforcement learning algorithm, both before and during ongoing incidents

**Business value:**

- Improve infrastructural resilience
- Optimize tripwire placement

PCSI is a collaboration of

ABN·AMRO achmea ASML

ING TNO de volksbank

For more info:

- Mark Buningh, PCSI business development – mark.buningh@tno.nl
- Reinder Wolthuis, PCSI program manager – reinder.wolthuis@tno.nl

www.pcsi.nl follow us

This project is co-funded by Holland High Tech with a PPP Grant for Research and Innovation in Top Sector HTSM