

Presenting PCSI on PvlB innovation event
February 11th 2025
Reinder Wolthuis



Partnership for
Cyber Security
Innovation

Introductie Reinder



- Electrotechnisch Ingenieur **UNIVERSITEIT TWENTE**.
-  **kpn**,  **Atos**. Bij  **TNO** sinds 2006.
- 25+ jaar ervaring in **innovatie in informatie beveiliging & Cybersecurity**
- Initiator en programmamanager van

Partnership for Cyber Security Innovation is a collaboration of



- Belangrijkste SOC gerelateerd werk
 - Mede-ontwerper van het eerst KPN SOC (2012)
 - Coordinator van het EU H2020 project  **SOCCRATES** (2019-2022)
SOC & CSIRT Response to Attacks & Threats based on attack defense graphs Evaluation Systems
 - Lid van  **enisa** ad-hoc werkgroep voor SOC/CSIRT, TaskForce lead voor Cyber Threat Intelligence (2022-2024)
 - Jaarlijkse Europese  **Etis** THE COMMUNITY FOR TELECOM PROFESSIONALS **telecom security benchmark** (meer dan 25 deelnemers waaronder Deutsche Telekom, British Telecom, Orange, Telefonica, KPN, Proximus)
 - Partner lead in EU Horizon project  **eFORT** met als doel om Europese elektriciteitsnetwerken veiliger te maken



PCSI is a collaboration of



Our predecessor

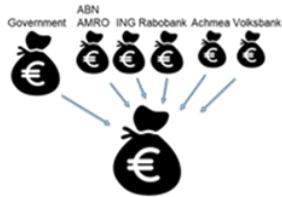
Shared Research Program (SRP)



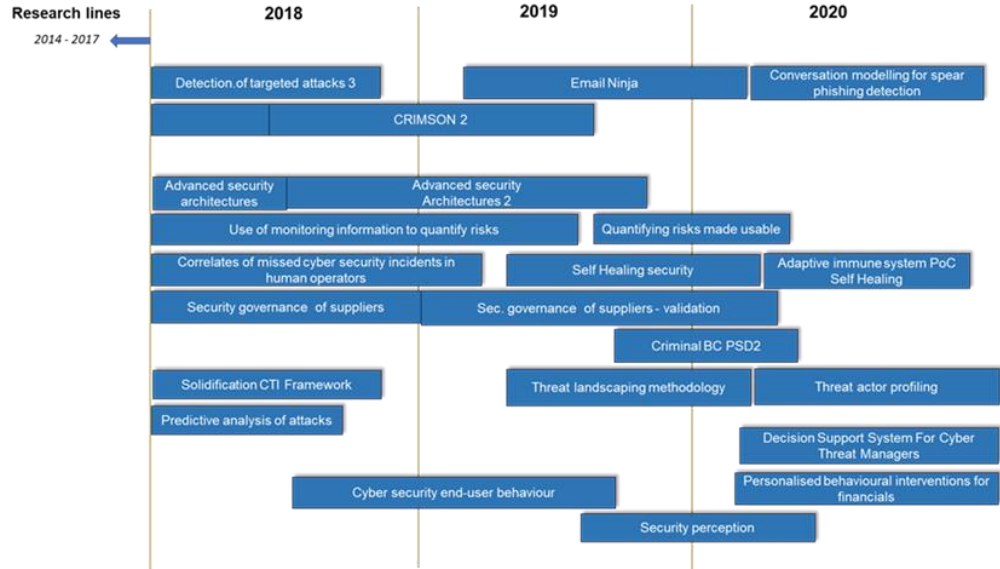
Shared working



Sharing data



Shared funding



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



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

Our value

PCSI is a unique opportunity to tackle your biggest threats: save money, talent and time, while upgrading your output, branding and network



Instant return on investment through shared budgets and match funding



Contribute to increased societal resilience by sharing findings and results



Collaborative workforce that speeds up craftsmanship development



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



Show thought leadership through premium innovation and cyber security



Join a network of experts, innovators, researchers, suppliers and startups



To pursue our empowering purpose, ING has to stay a step ahead of the cybersecurity challenges we're facing now and in the future. This requires collaboration, innovation and access to collective knowledge and data. That's why our cybersecurity team is keen to be a part of the PCSI ecosystem. Together we can develop cutting-edge solutions that contribute to a safer and more secure digital future for everyone

Beate Zwijnenberg
Global CISO ING



Proper information security has always been important, but this is true even more today. Cooperation [...] provides faster and smarter responses to new technologies but also to new threats. PCSI is the perfect platform to facilitate this cooperation and is the next step beyond an already proven very successful cooperation

Martijn Dekker
CISO ABN AMRO



PCSI is a collaboration of

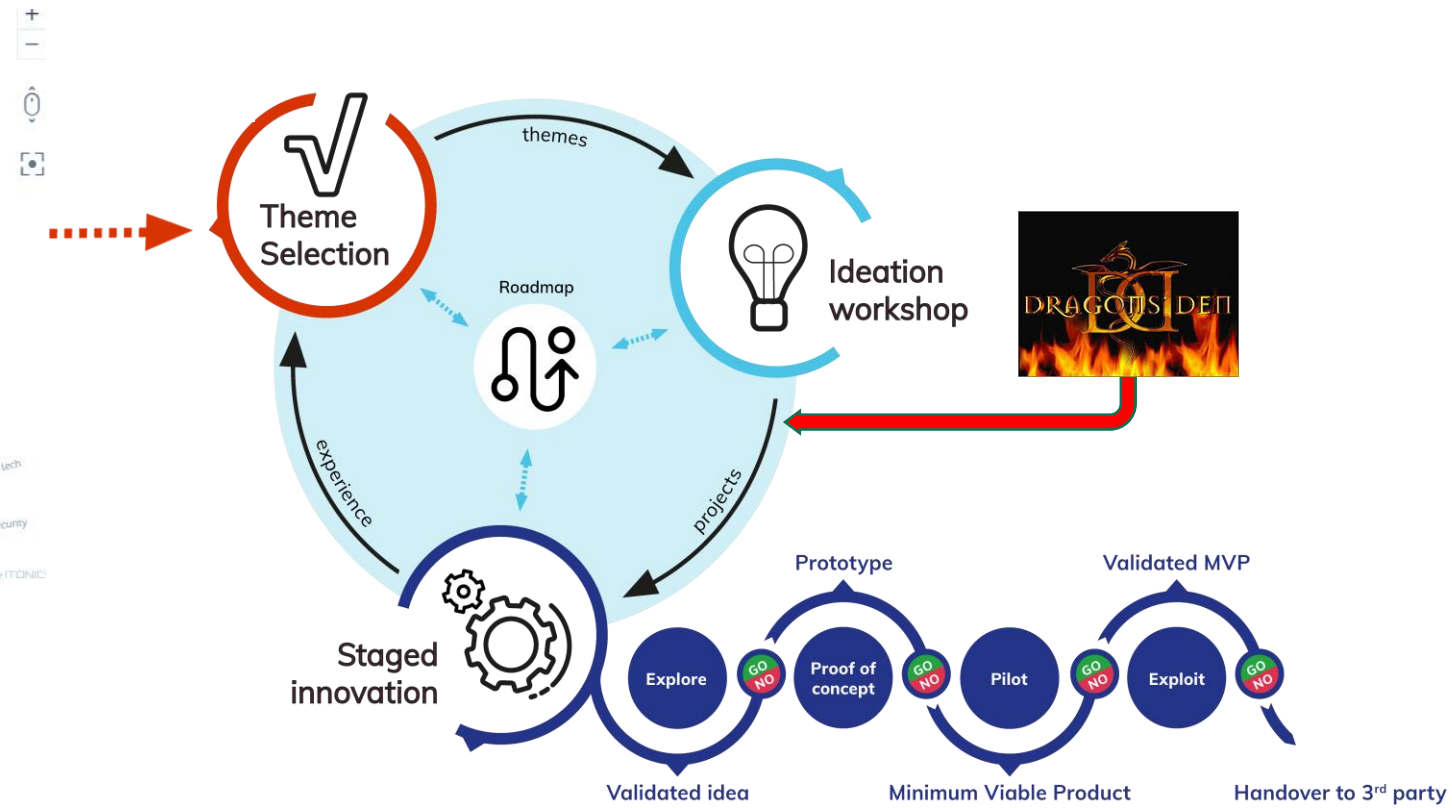


How we work

Our security radar identifies themes and trends that are relevant to our partners. Periodically the steering committee selects which themes are selected for ideation and staged innovation

Project ideas are born in Ideation workshops, and pitched in the Dragon's Den that selects which ideas will enter our staged innovation process

Collaborative 'orchestrating innovation' way of working



PCSI is a collaboration of

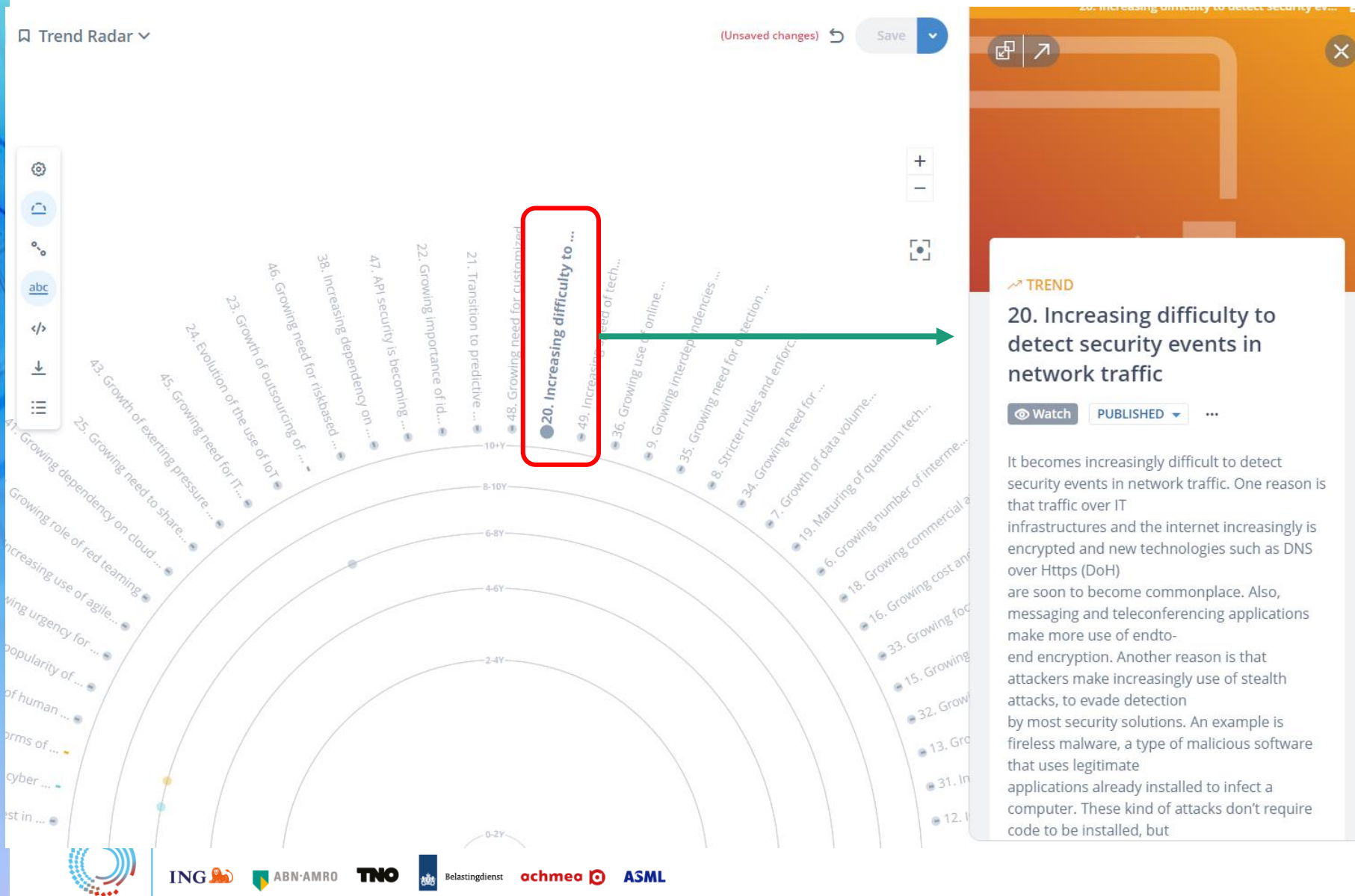


Belastingdienst



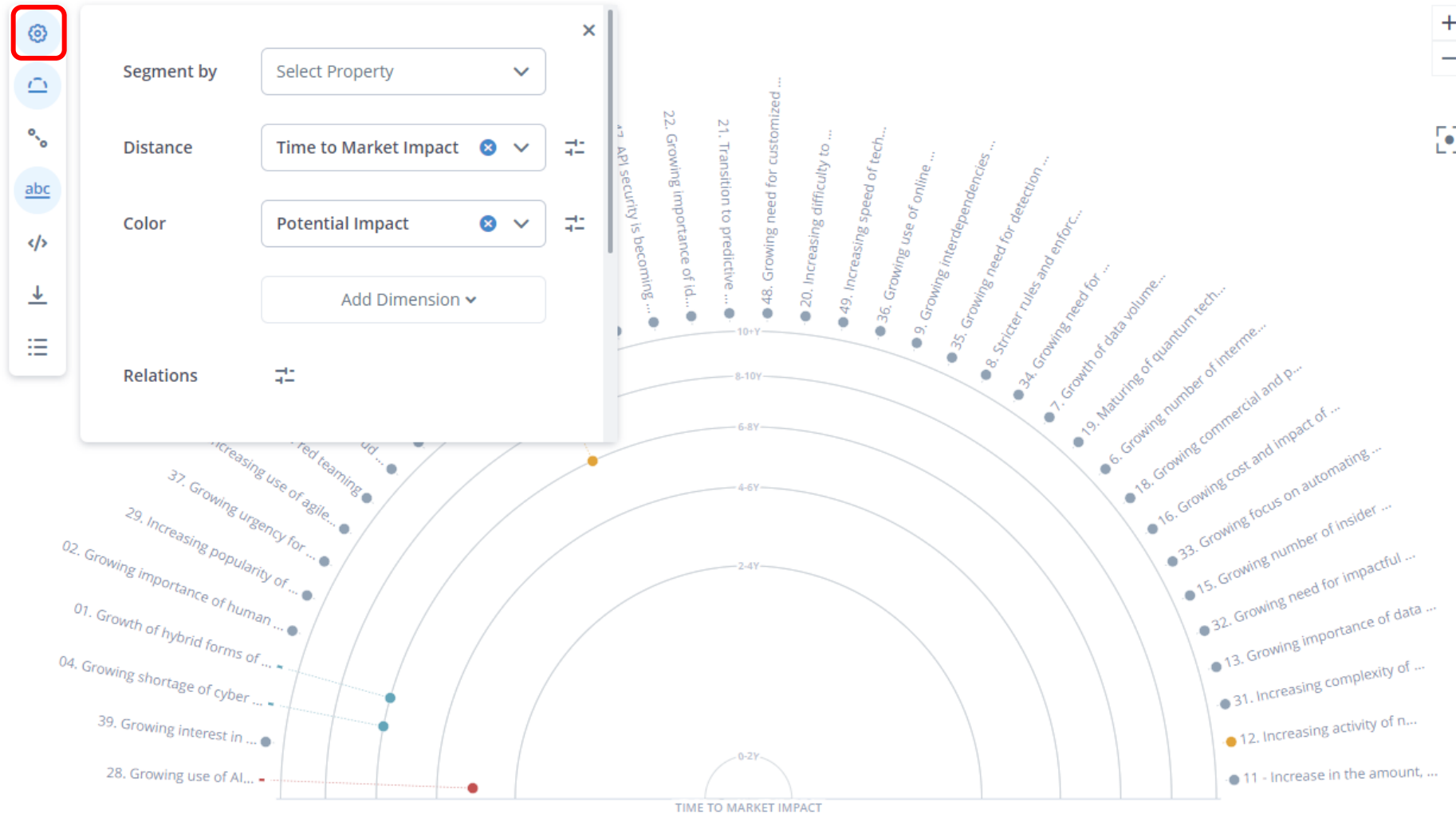
Published on PCSI website

<https://pcsi.nl/en/cyber-security-radar-en>



By clicking on an Element, it opens a sidebar with the information related to it.

Configurable for the viewer



+

-

⊞

Via the Configuration button, multiple views are possible.

Our ecosystem

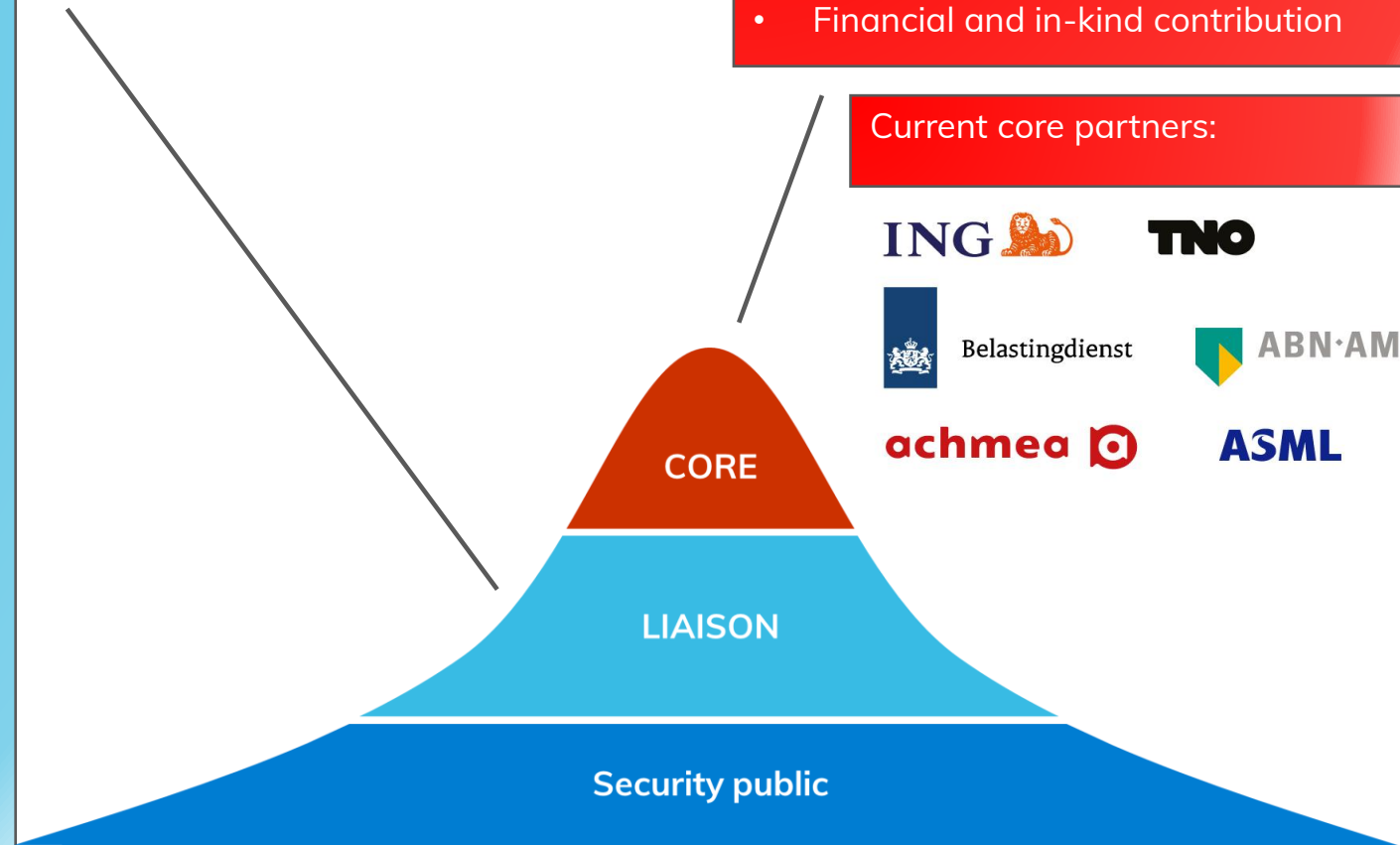
- Closely informed on progress and results
- Provide feedback and suggestions
- Occasional involvement in projects when mutual beneficial
- Some in-kind contribution

- Define the strategic direction
- Participate in projects
- Pilot experience
- Benefit from all results
- Full learning experience
- High visibility to outside world
- Financial and in-kind contribution

Current liaison partners:

- | | |
|---------------------------|---------------------------|
| • AFM | • Labyrinth |
| • Akamai | • Linksight |
| • Axiomatics | • Lupovis |
| • Beyond Products | • Mindgame |
| • Bizzdezin | • Niagara Networks |
| • Cisco | • NS |
| • Connect2Trust | • OneTrust |
| • Contrast Security | • ONVZ |
| • Countercraft | • Orange Cyberdefense |
| • Crowdstrike | • Proofpoint |
| • Cryptography in Context | • Rabobank |
| • Cybertrap | • Radically Open Security |
| • Cyemptive | • Scepter |
| • DNB | • Securify |
| • Dtact | • Security Academy |
| • Enclave Networks | • SURF |
| • Endor Labs | • Thales |
| • F8th | • Topicus |
| • Forelens | • TrendMicro |
| • Fortinet | • Verizon Business |
| • Goldilock | • Vidua |
| • IBM | • Z-Cert |
| • ID Control | • Zivver |

Current core partners:



Access to information via website, newsletters, webinars and social media

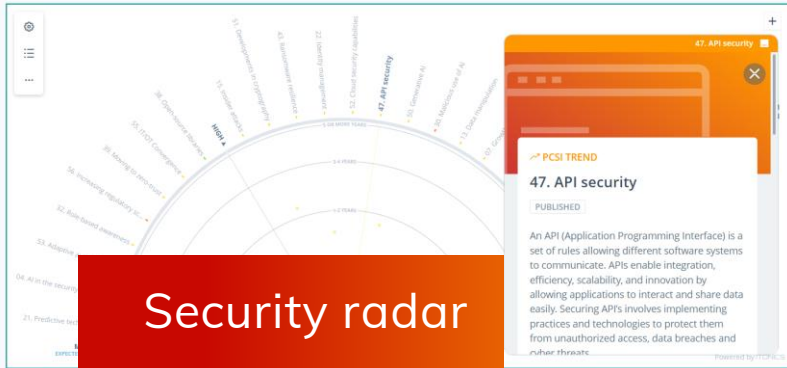
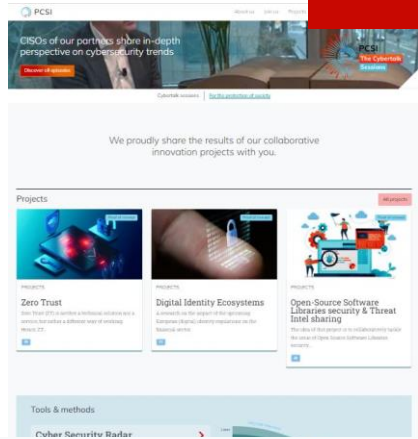


PCSI is a collaboration of

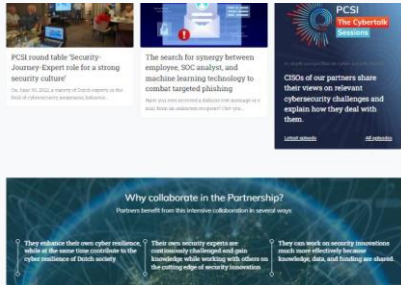


Our brand

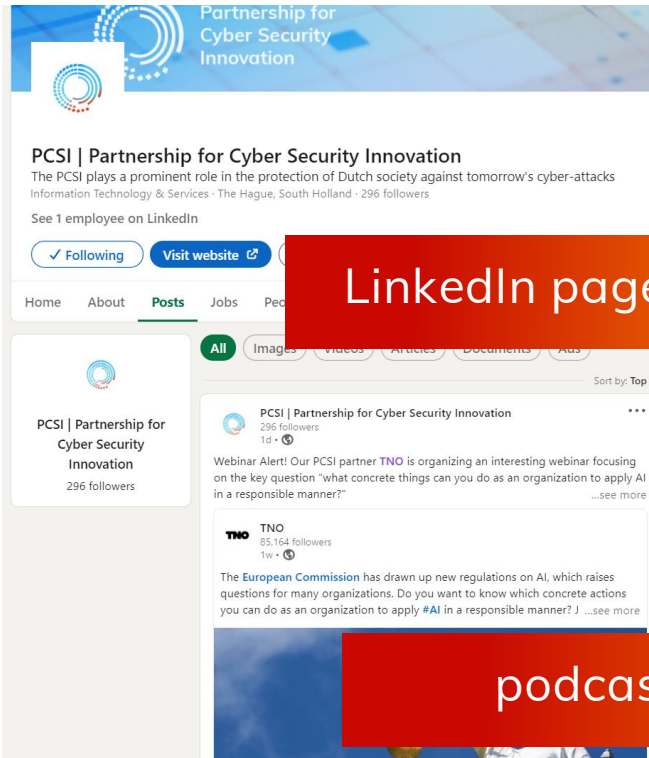
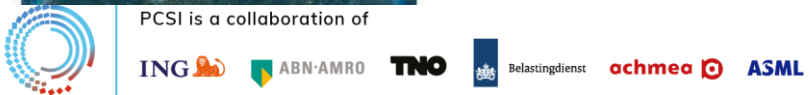
pcsi.nl website



Security radar



PCSI is a collaboration of



LinkedIn page

podcast



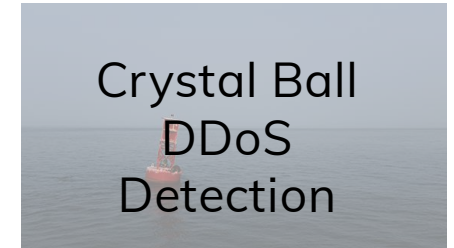
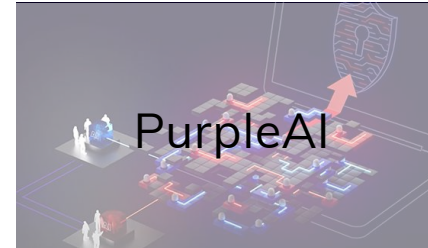
webinars



Media exposure



Finalized PCSI projects since the start in 2020





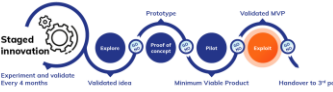
PCSI is a collaboration of



Running projects

Recently finalized projects:

- Generative AI
- Open Source Library Security

PCSI phase	Project
	Automated Cyber security
	Malicious use of AI
	Causal AI DDoS
	Post Quantum Crypto
	Digital DeltaWorks
	Finding API
	PurpleAI 2 (DNB, AFM, Securify)



PCSI is a collaboration of



Belastingdienst





50. Generative AI

50. Generative AI

PUBLISHED

Generative AI: Best companion or worst enemy

Generative AI, using tools such as LLMs, is more frequently used and has become available to both enterprises as well as the public.

On one side, it can be used to streamline and automate entire workflows, from data analysis to automated assistants.

On the other side, it can be misused to quickly generate malicious code, spread disinformation or set up large scale frauds. Even when put to good use, Generative AI is very scalable, fast, and efficient, but not always reliable.

The challenge for companies is to investigate

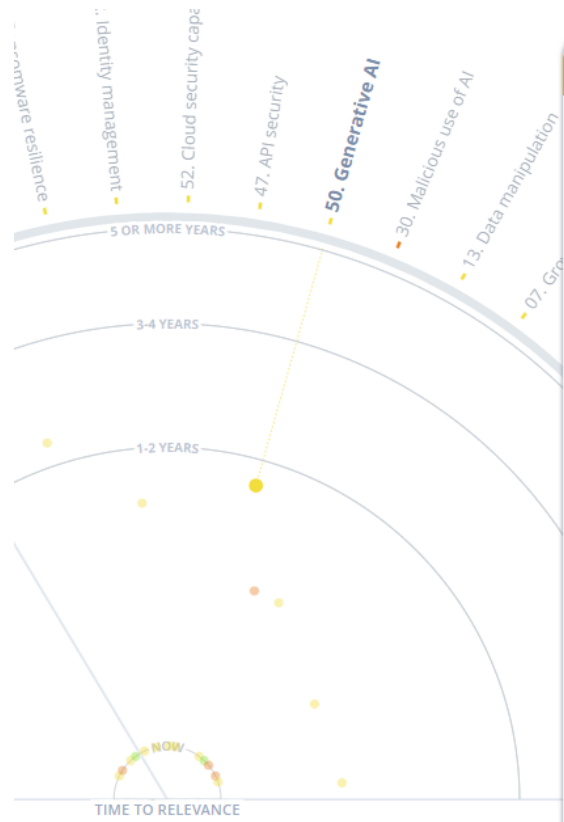


PCSI is a collaboration of



Belastingdienst





Rating

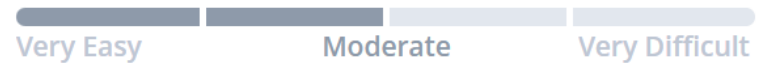
Opportunity or Threat ?



Expected Impact ?



Fit for PCSI ?



Time to Relevance ?



PCSI is a collaboration of





Initial copied ratings



Has an active project?

Yes

Related Projects

[Generative AI | Projects \(pcsi.nl\)](#)

Tags

ai

data

llm

Relations (0)

No Elements to Show



PCSI is a collaboration of



Belastingdienst

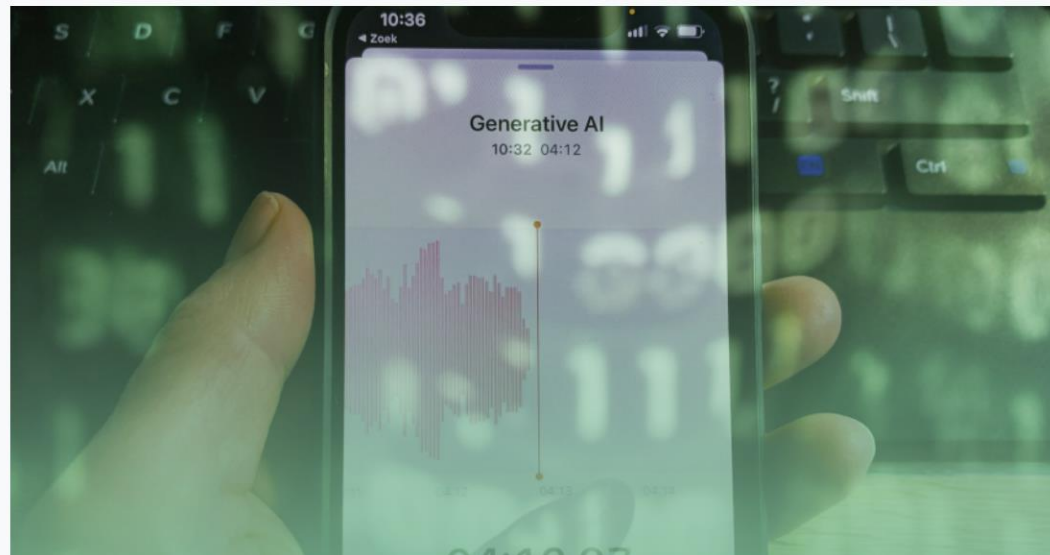
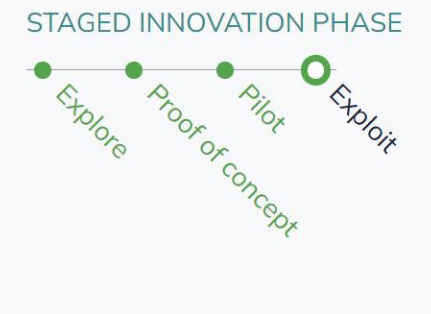


← All projects

Generative AI

Started in August 2023

AI voice cloning is already being used for spear phishing. Soon, companies may be targeted on a large scale by criminals. Therefore, it is of crucial importance that PCSI partners are adequately prepared for AI voice calls.



PCSI is a collaboration of



Belastingdienst



Partnership for Cyber Security Innovation is a collaboration of



ING 

TNO



Belastingdienst



ABN-AMRO

achmea 

ASML

www.pcsi.nl 

follow us 



PCSI is a collaboration of

ING 

 ABN-AMRO

TNO



Belastingdienst

achmea 

ASML