

Even voorstellen



René Meijer

Security Test Lead / Ethical Hacker

HALL OF FAME

The University of Twente would like to thank the people who have contributed to making its network, applications, and users safer. Anyone who has made a report in accordance with the guidelines in the [responsible disclosure](#) policy can be included in the Hall of Fame.

It is possible to have a link added to your entry in the Hall of Fame. Maintenance of that link is not the university's responsibility, though. As a reporter, you have to make sure the link stays operational.

2023	# reports in 2023	Reports in previous years
René Meijer	1	

Hall of Fame

Recognitions through 7 July 2023

nr. 15 June 2023

[vulnerability on un.org](#)

René Meijer (Dutch Railways)

Reported SDE vulnerability on [un.org](#)

13 June 2023



Agenda



- 01** IT/OT bij NS
- 02** Het probleem
- 03** De aanpak
- 04** Voorbeelden



Nederland duurzaam bereikbaar. Voor iedereen



Verstedelijking
Razendsnelle ontwikkeling Technologie
Nieuwe & Andere Aanbieders

Externe Trends

Beter
Leuker
Goedkoper
Sneller

NS IT
NS Business

Nieuwe Treinen op het spoor

Goedkoper treinkaartje

Nieuwe Medewerkers

Medewerker

Kennis & kunde versterken

Continu leren & groeien

Automatisering

Robotisering

Process Mining

Innovatie

Visueel Management

Data

Tijdweg diagram

Betaalbaarheid en Behoudzaamheid

Standaardisering

Proces denken

Leiderschap

Applicatie Strategie

Manner van Werken

Kortcyclisch

Slim onderhoud

Waarde denken

Experimenteren

Sourcing Strategie

NS IT Clusters



ComIT

- Kaartverkoop
- Abonnementen
- MijnNS
- Etc.



IT Stations

- Kiosken etc.
- OV-Fiets
- Bagagekluizen
- Etc.



IT Operatie

- Treindienst
- Treinonderhoud
- Sociale veiligheid
- Reizigers begeleiding

QES

CPO

HR

Staven

Data





Agenda



- 01** IT/OT bij NS
- 02** Het probleem
- 03** De aanpak
- 04** Voorbeelden





Redacted

Takeaway:

- NS IT/OT landschap is GROOT en divers
- alleen al op internet 500+ domeinnamen



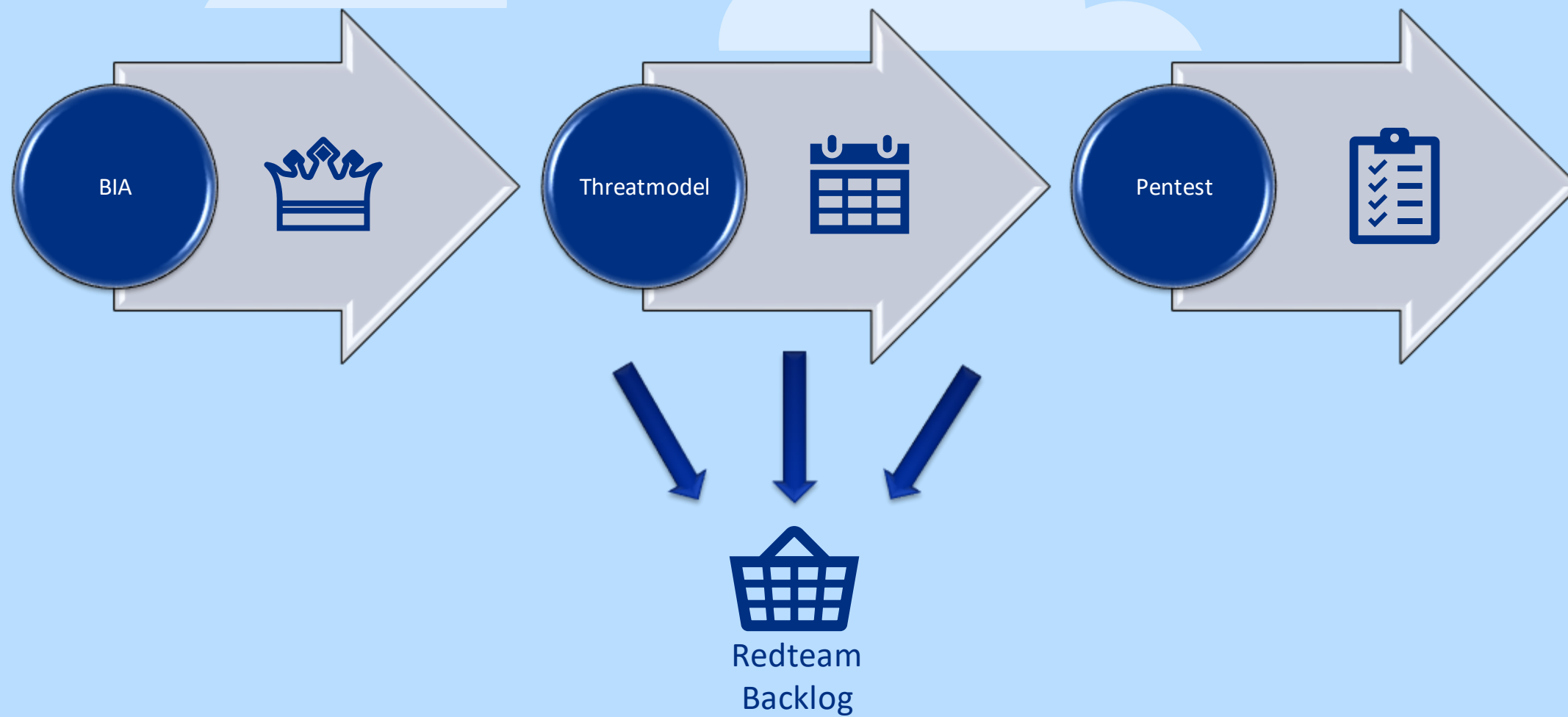
Agenda



- 01** IT/OT bij NS
- 02** Het probleem
- 03** De aanpak
- 04** Voorbeelden



De aanpak



De aanpak

Pentesten:

- Zoeken naar kwetsbaarheden
- Beperkte scope (systeem of team)
- Kortere tijdsduur (dagen)
- Vooraf aangekondigd bij het team
- Conform testplan vormgegeven door dreigingsmodel

Red Teaming:

- Zoeken naar zwakke punten in de infrastructuur en processen
- Brede scope (informatieketens)
- Langere tijdsduur (weken/maanden)
- Moment niet aangekondigd bij het team wegens testen detectie en response
- Emulatie echte aanvallers via *technieken*, *tactieken* en *procedures* vanuit Mitre Att&ck framework
- Ook sociale en fysieke aspecten worden meegenomen



De aanpak



ComIT

- Kaartverkoop
- Abonnementen
- Etc.



IT Stations

- Kiosken etc.
- OV-Fiets
- Bagagekluizen
- Etc.



IT Operatie

- Treindienst
- Treinonderhoud
- Sociale veiligheid
- Reizigers begeleiding

CPO

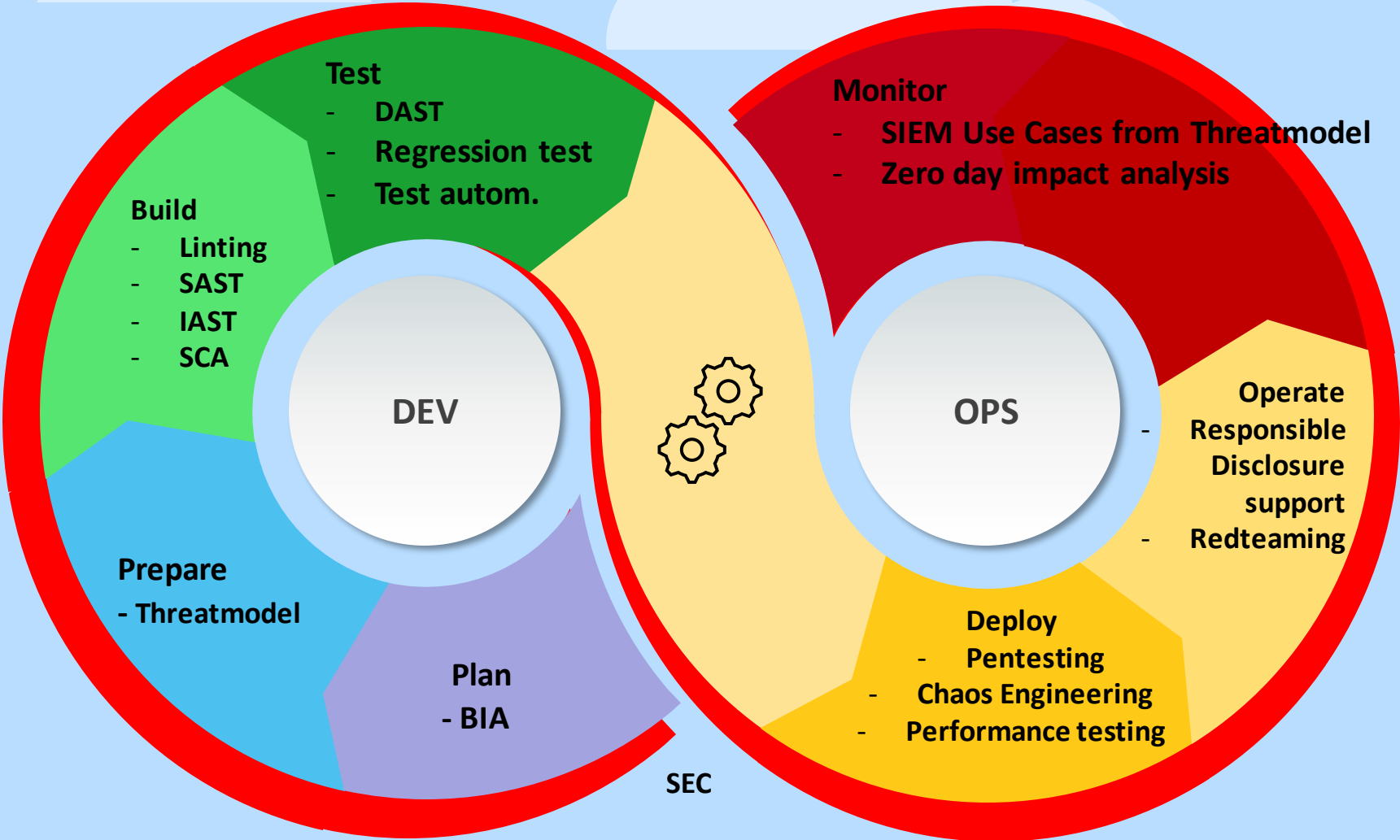
HR

Staven

Data



De aanpak



Agenda



01

IT/OT bij NS

02

Het probleem

03

De aanpak

04

Voorbeelden



Wat testen we dan?

NS blokkeert 2100 accounts na 'credential stuffing'-aanval

Nieuws • 21-05-2021



Credential stuffing

Miljoenen wachtwoorden en privégegevens op straat door hack webshop Allekabels.nl

15 april 2021 15:10
Aangepast: 17 april 2021 10:54

Welkom bij Nederlandse Spoorwegen

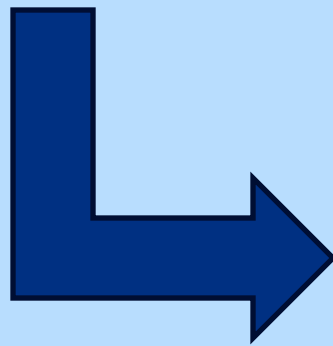
Inloggen

E-mailadres

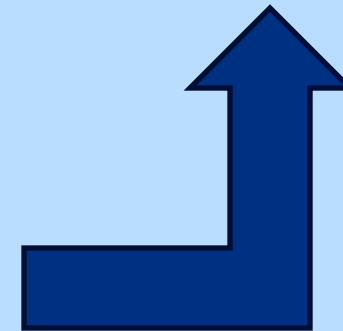
Wachtwoord

Onthoud mijn e-mailadres

NS-
✓
✓
✓
✓



```
pankang@live.nl ~~~~~ R@ndyorton1  
dome@kpnplanet.nl ~~~~~ Jannet01!  
[redacted]@live.nl ~~~~~ Blackberry123!  
[redacted]@kpnplanet.nl ~~~~~ Hondkyra1!  
joep@live.nl ~~~~~ Joep1992!  
[redacted]@dabok.nl ~~~~~ Bokworst1!  
noah@quicknet.nl ~~~~~ Noah2001!  
[redacted]@live.nl ~~~~~ Guitar12!
```



Zodat we dit kunnen voorkomen

<https://www.youtube.com/watch?v=CxwPEQLGh9M>

MacBook





**Bedankt voor je aandacht!
Vragen?**

René Meijer

Security Test Lead



06-16473333



rene.meijer@ns.nl



<https://www.linkedin.com/in/meijerrene/>



Laan van Puntenburg 100,
3511 ER Utrecht

