Contact - Howest

Research Manager
Shane Deconinck
shane.deconicnk@howest.be

Project lead
Aaron De Rybel
Aaron.de.rybel@howest.be

Researcher
Tijl Atoui
tijl.atoui@howest.be

howest

Security & Privacy research group
Experts in Cyber Security, Blockchain & AI

Contact - Ugent

UNIVERSITEIT GENT
CAMPUS KORTRIJK

XIAK research group
Experts in industrial automation

Research manager
Johannes Cottyn
johannes.cottyn@ugent.be

Project lead
Stijn Huysentruyt
stijn.huysentruyt@ugent.be

Researcher
Elias Cappon
elias.cappon@ugent.be

Researcher
Axl Van Alboom
axl.vanalboom@ugent.be

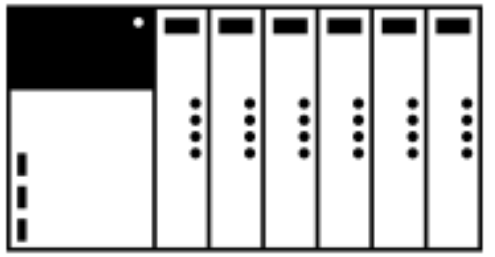
Agenda

1. Inleiding
2. Doelstellingen project
3. Aanval scenario I
4. ML-OT toolbox
5. Workshop en webinar topics
6. Verzamelen Feedback

1. Inleiding

Gedrag gebaseerde **A**rtificiële **I**ntelligentie voor **c**yber **i**ndustriële **a**anvallen

GAICIA



Voorgeschiedenis

AI voor intrusie detectie (2018-2020)

- Interne studie Howest
- Netwerk van typische ‘kantoor’
- Postgraduaat applied AI

IC4 (2019 - 2025)

- Samenwerking Howest - Ugent
- Industriële netwerk monitoring
- Expertise in Industriële netwerken en security

howest hogeschool

UNIVERSITEIT GENT

GAICIA

1. Inleiding

Preventieve maatregelen zijn beperkt

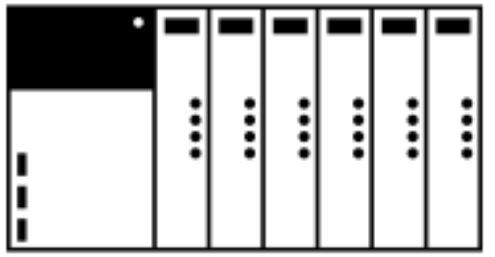
- Hardware in OT is robuust, 10 tot 30 jaar levensduur
- 24/7 werking
- Legacy systemen, zonder security updates
- Ongeëncrypteerde protocollen zonder inherente security

Netwerk monitoren is een oplossing

1. Inleiding

Gedrag gebaseerde **A**rtificiële **I**ntelligentie voor **c**yber **i**ndustriële **a**anvallen

GAICIA



"Live detecteren en melden van cyberaanvallen op industriële netwerken met behulp van AI in een monitoringoplossing"

Doelgroep

- Maakbedrijven
- Integratoren
- Security & AI technologiebedrijven

howest hogeschool

UNIVERSITEIT GENT

GAICIA

1. Inleiding

- Eerste toegang tot projectresultaten
  - OT aanvalsgedrag en indicatoren
  - Overzicht Algoritmes
  - Integratie tussen AI en monitoringoplossingen
  - 2 use case scenario’s
  - …
- Valideren intelligente monitoring.
- Deelname workshops en webinars + inspraak topics.
- Gevalideerde algoritmes ter beschikking gesteld.

2. Doelstellingen project

WP 2: Literatuurstudie

Leverbaarheid: *Een Lijst van machine learning algoritmes en neurale netwerken die we valideren in werkpakket 3*

Welke Algoritmes zijn veelbelovend?

Brede literatuurstudie over AI algoritmes/technieken voor netwerkdata, update van kennis.

Kortere experimenten op beperkte datasets

2. Doelstellingen project

Werkpakket 2: Literatuurstudie

Leverbaarheid: *Een Lijst van machine learning algoritmes en neurale netwerken die we valideren in werkpakket 3*

Overzicht wordt beschikbaar gesteld

Machine learning

- Set klassieke ML algoritmes
- Forest ensembles
- Isolation forests

→ **Weinig computatiekracht**

Deep learning

- Gradient boosted trees → **Goede accuratie en implementatie**
- Auto-encoder varianten → **Cutting-edge techniek**
- Graph Neural networks → **Alphafold**
  anti-biotica (halycin)
  Computer netwerken

2. Doelstellingen project

Werkpakket 2: Literatuurstudie
Leverbaarheid: *een catalogus van aanvalsgedrag en aanvalsdetectoren*

Gedrag - Hoe werken OT aanvallen en wat is hun doel?

Detectoren – Hoe kan door security expert en AI een aanval gedecteerd worden

=> Dit volgt deels uit de literatuurstudie en onze eigen experimenten.

2. Doelstellingen project

Werkpakket 3: Data Generatie en Algoritme Selectie

Opbouwen van nieuwe testomgeving om datasets te maken.

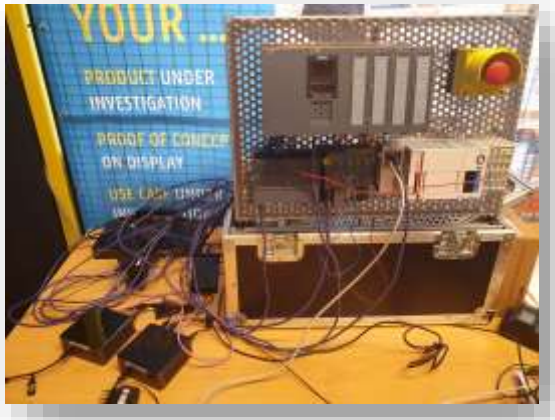
- Een echte Fysieke set-up
- Hedendaagse protocollen
- Realistische scenario's uitwerken.

2. Doelstellingen project

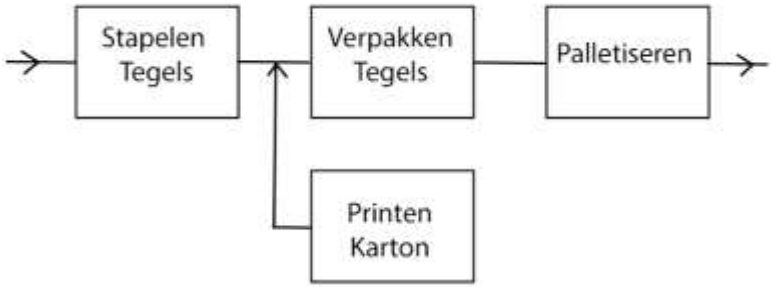
Werkpakket 3: Data Generatie en Algoritme Selectie

Uitbreiding van de bestaande IC4 FicTile opstelling (fictieve tegelfabriek) met nieuwe koffer

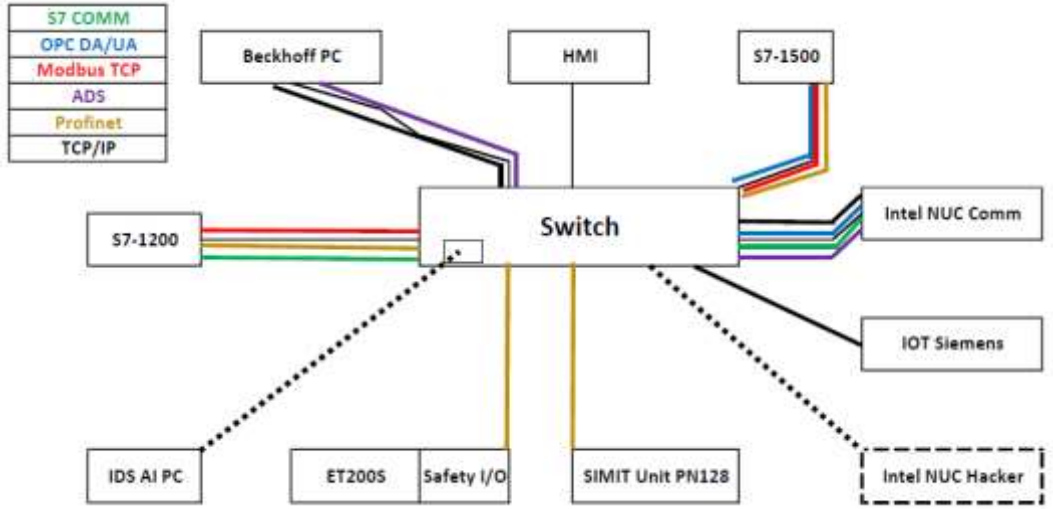
Opstelling



Applicatie



Communicatie stromen

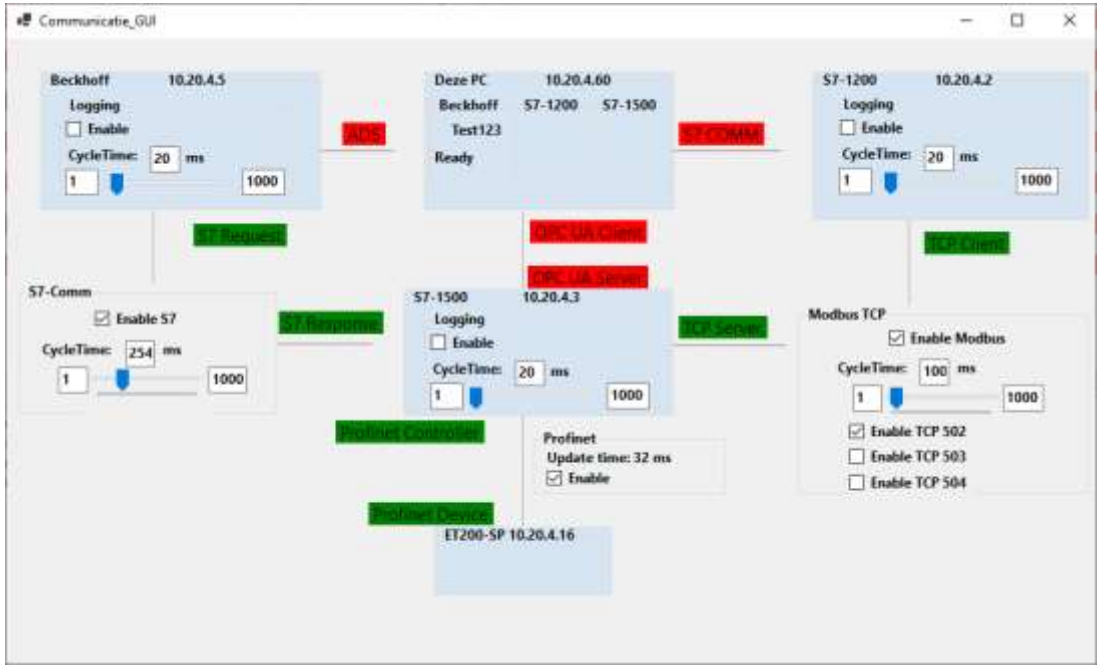


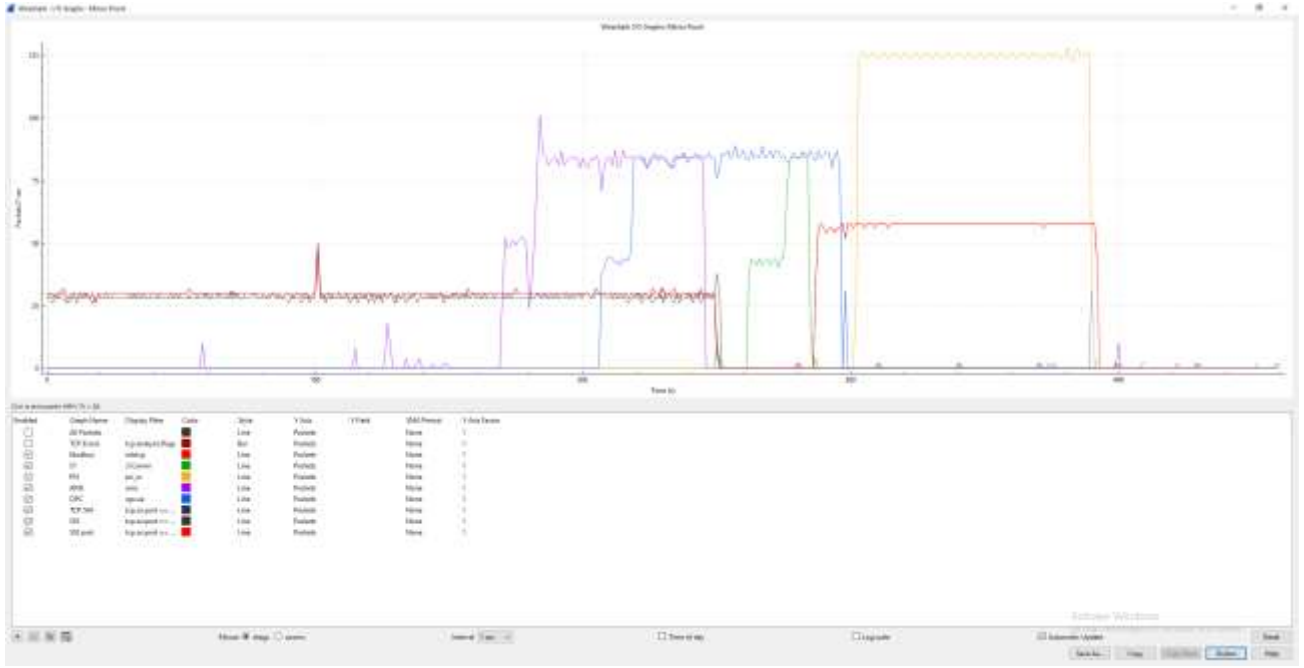
2. Doelstellingen project

Werkpakket 3: Data Generatie en Algoritme Selectie

Instelbare communicatiestroom (volume en mix) => nabootsen van productievloer scenario's

Validatie / Dimensionering van IDS





2. Doelstellingen project

Werkpakket 3: Data Generatie en Algoritme Selectie

2. Doelstellingen project

Werkpakket 3: Data Generatie en Algoritme Selectie

'ML-OT' algoritmes, Een selectie van gevalideerde algoritmes ter beschikking stellen.

⇒ code, datasets, aanvalscenario's en experimenten in publiek project aanbieden.

Wetenschappelijke rapportage van resultaten van de experimenten.

⇒ Overzicht van performantie van algoritmes
Accuratie, snelheid

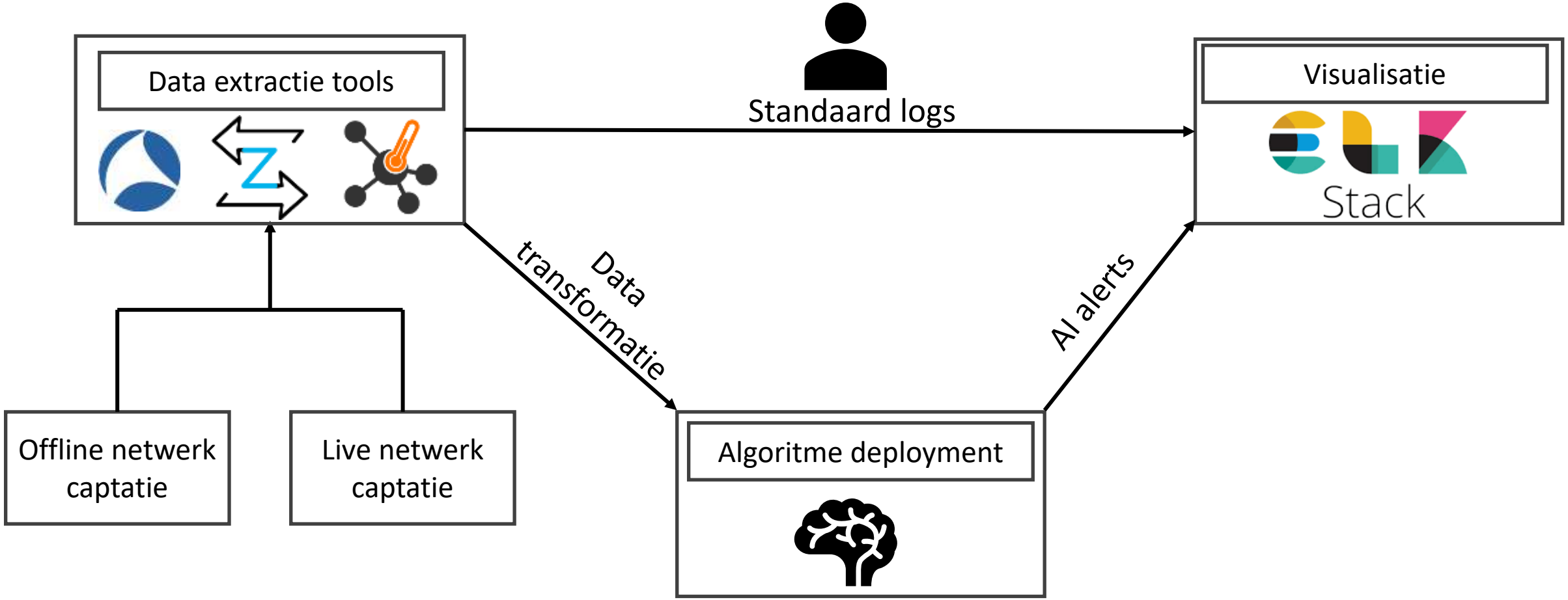
2. Doelstellingen project

Werkpakket 4: Realtime OT monitoring systeem

Leverbaarheid: *het integreren van de drie softwarecomponenten tot een intelligente OT monitorsysteem in een kennisdatabank aanbieden.*

2. Doelstellingen project

Werkpakket 4: Realtime OT monitoring systeem



2. Doelstellingen project

Werkpakket 5: Ontwikkelen van business cases

Leverbaarheid: *2 demo en instructievideo's voor het opstellen van een intelligente monitor oplossing.*

Wat krijgt een security specialist te zien bij een aanval?

- 2 scenario's met demovideo's.
- Instructievideo's voor technische instellingen monitoringsysteem

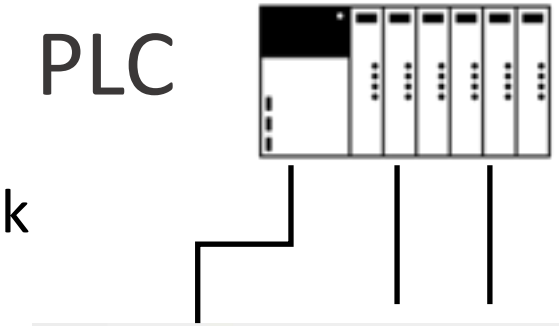
4. Aanval scenario I

PLC stuurt productiemachines aan

Verstoring of aanpassing in

Programmatie heeft directe inpak op productielijn

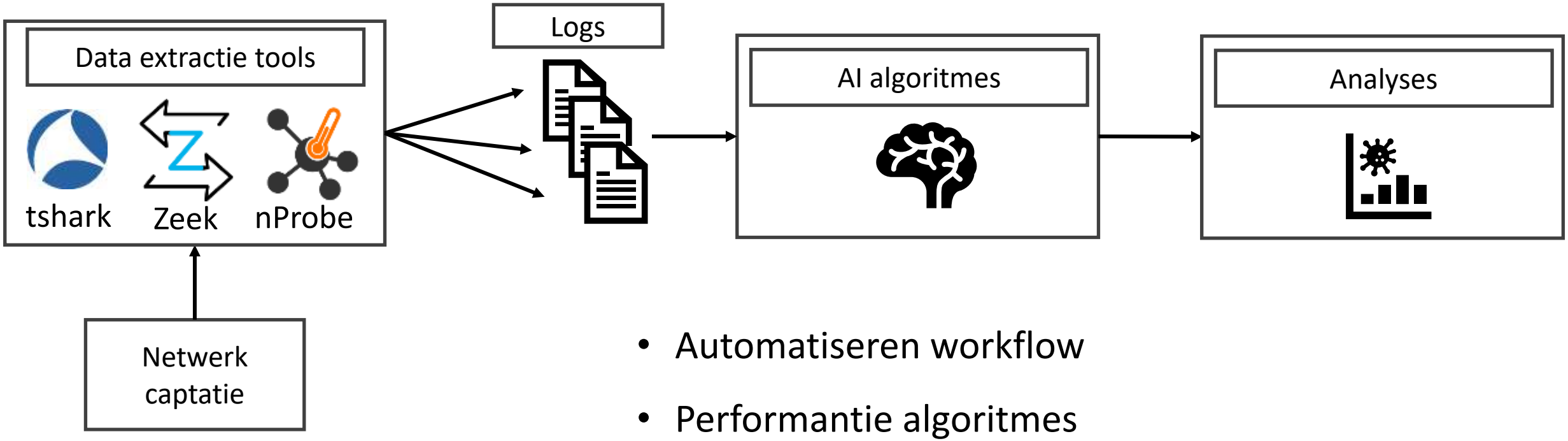
Temperatuur industriële bakkerij



4. Aanval scenario I

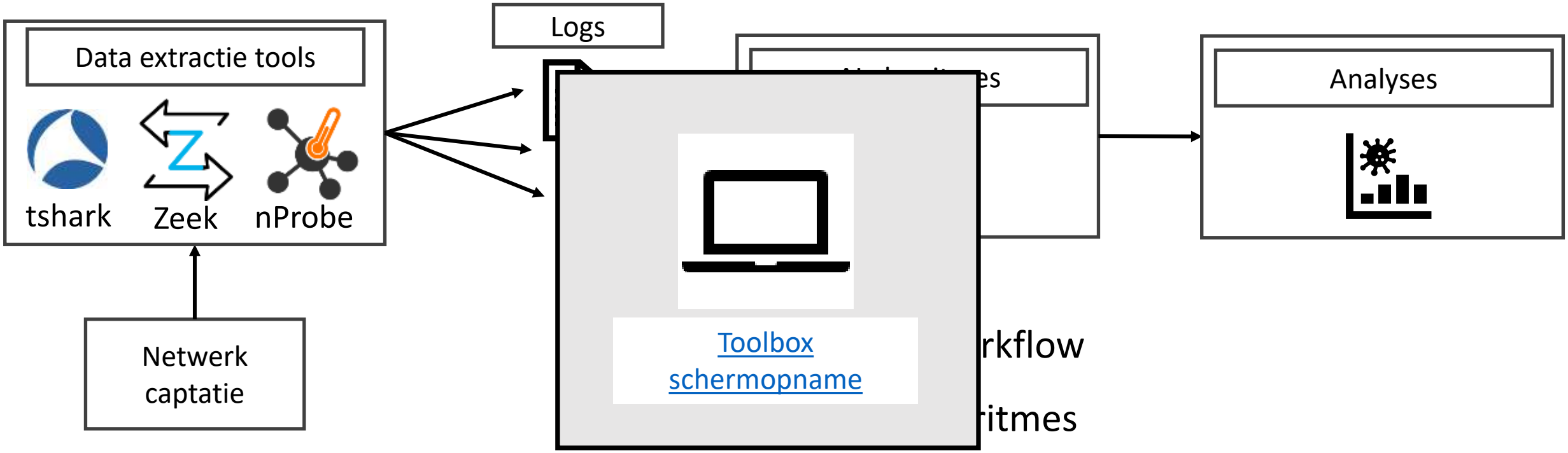
1. Scan het netwerk af naar Modbus toestellen
2. Lees de holding registers 5 keer uit (interval 30 seconden)
3. Schrijf 10 keer willekeurige data naar de holding registers (interval 10 seconden)
4. Lees de holding registers uit

5. ML-OT toolbox



- Automatiseren workflow
- Performantie algoritmes
- Explainable AI

5. ML-OT toolbox

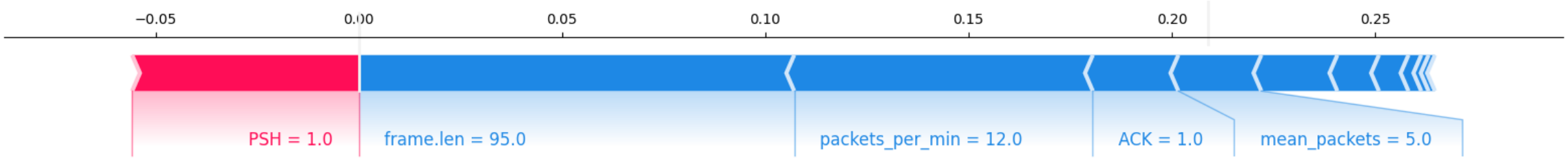


- Explainable AI

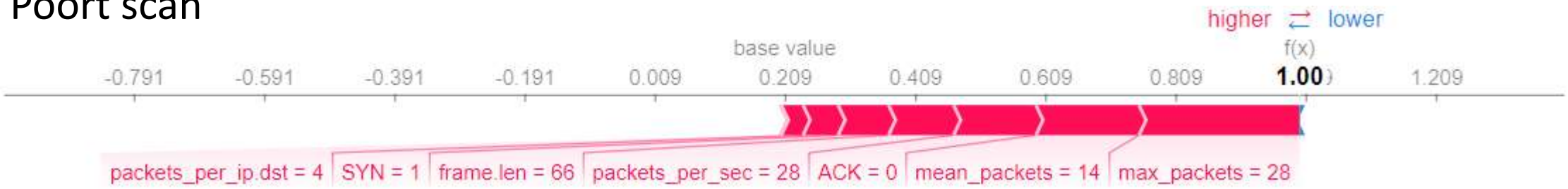
Scenario I

Explainable AI met feature importance

Normale netwerktraffiek



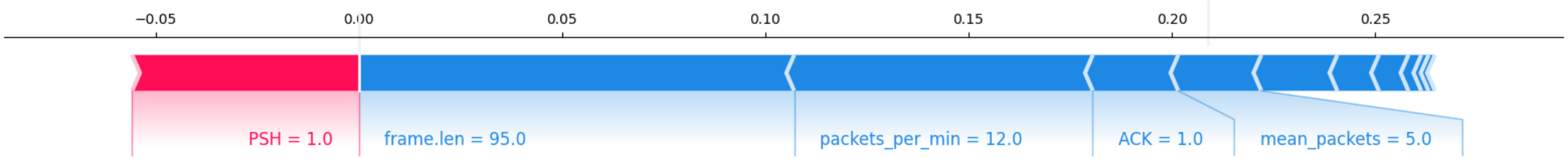
Poort scan



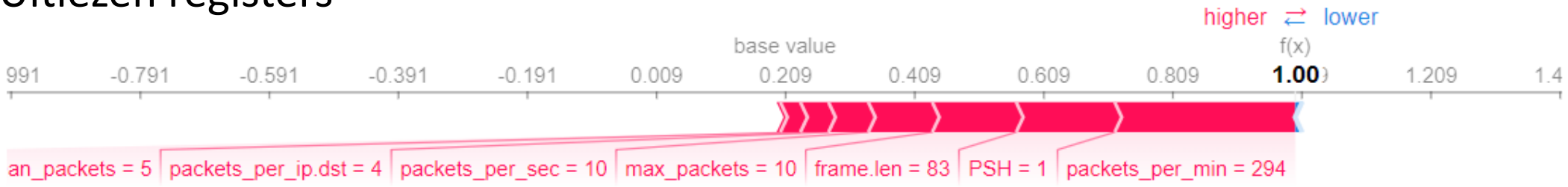
Scenario I

Explainable AI met feature importance

Normale netwerktraffiek



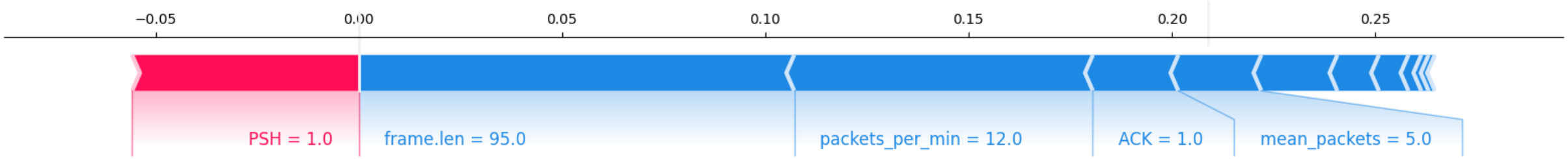
Uitlezen registers



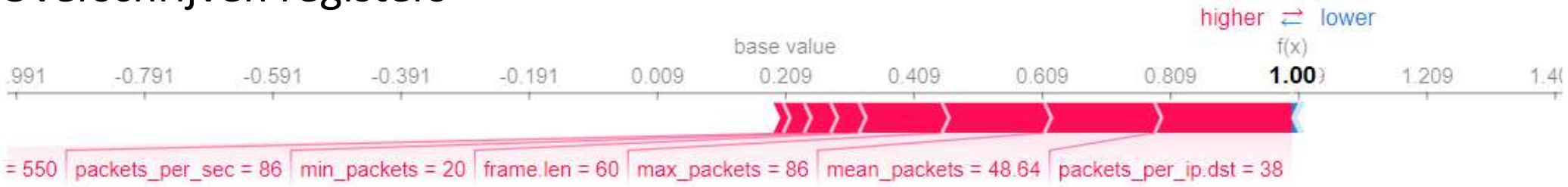
Scenario I

Explainable AI met feature importance

Normale netwerktraffiek



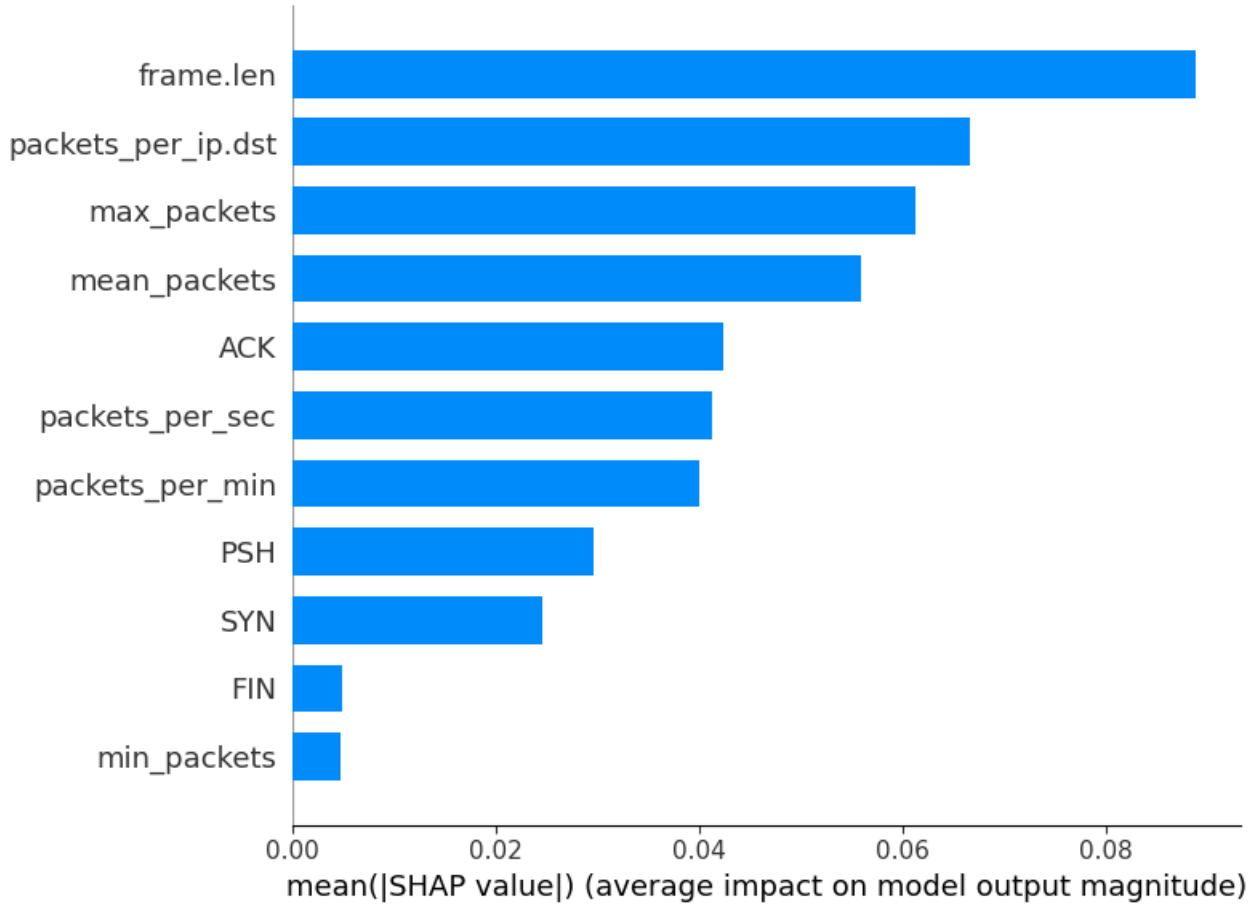
Overschrijven registers



Scenario I

Belang van input over geheel van scenario I

- Poort scan
- Registers uitlezen
- Registers aanpassen



5. Workshop en webinar topics

3 Workshops = live demonstratie of praktische uitwerking mee te volgen door de deelnemers
Bv. Instellen van logging software voor specifieke OT aanvallen/scenario's

2 Webinars = Een in-depth presentatie (online) met mogelijkheid tot discussie/brainstorming.
Bv. Voor en nadelen van de verschillende algoritmes of Integratie van AI met monitoringsystemen.

6. Verzamelen Feedback

Verbind met

www.wooclap.com/BLYHSJ

of scan de QR-code

om deel te nemen

Contacten & Info

Research Manager
Shane Deconinck
shane.deconicnk@howest.be

Research manager
Johannes Cottyn
johannes.cottyn@ugent.be

Project lead
Aaron De Rybel
Aaron.de.rybel@howest.be

Project lead
Stijn Huysentruyt
stijn.huysentruyt@ugent.be

https://gaicia.ic4.be/

- Registratierechten volgt voor leden
- Info meetings
- Resultaten project