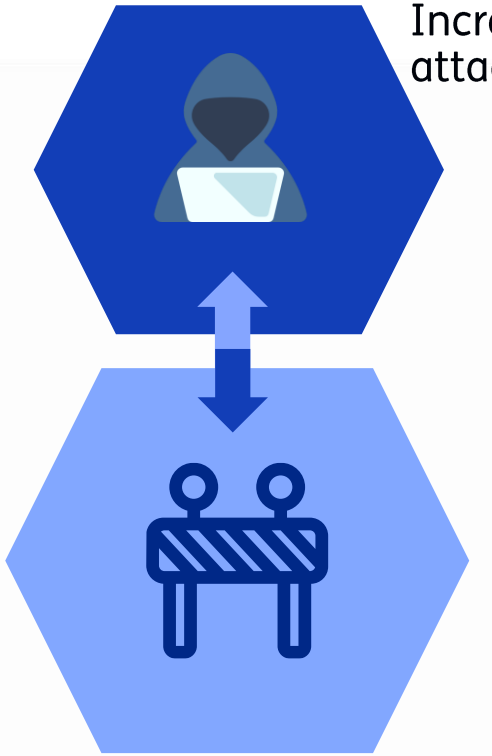

SOARCA
open-source SOAR for CACAO
playbook automation
Jan-Paul Konijn, Maarten de Kruijf | ONE Conference
TNO innovation for life

Challenges & the need for automation

Challenges & the need for automation



Increasing in number of attacks and complexity

Financial sector stability

Rising Cyber Threats Pose Serious Concerns for Financial Stability

Greater digitalization and heightened geopolitical tensions imply that the risk of a cyberattack with systemic consequences has risen

Fabio Natalucci, Mahvash S. Qureshi, Felix Suntheim

April 9, 2024

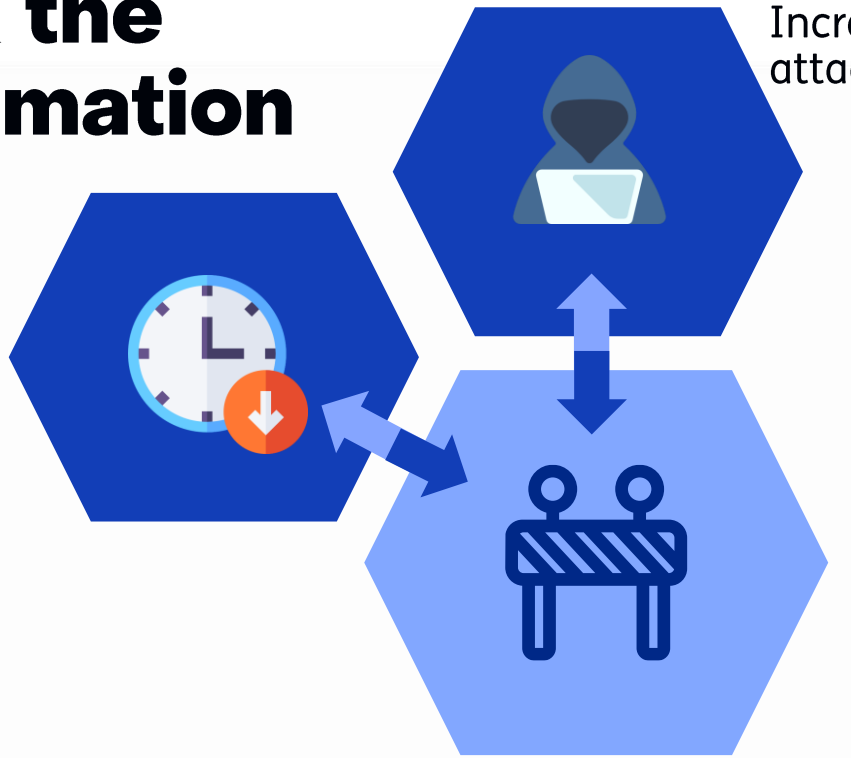
Listen with Speechify 0:00 3:16

Cyberattacks have more than doubled since the pandemic. While companies have historically suffered relatively modest direct losses from cyberattacks, some have experienced a much heavier toll. US credit reporting agency Equifax, for example, paid more than $1 billion in penalties after a major data breach in 2017 that affected about 150 million consumers.

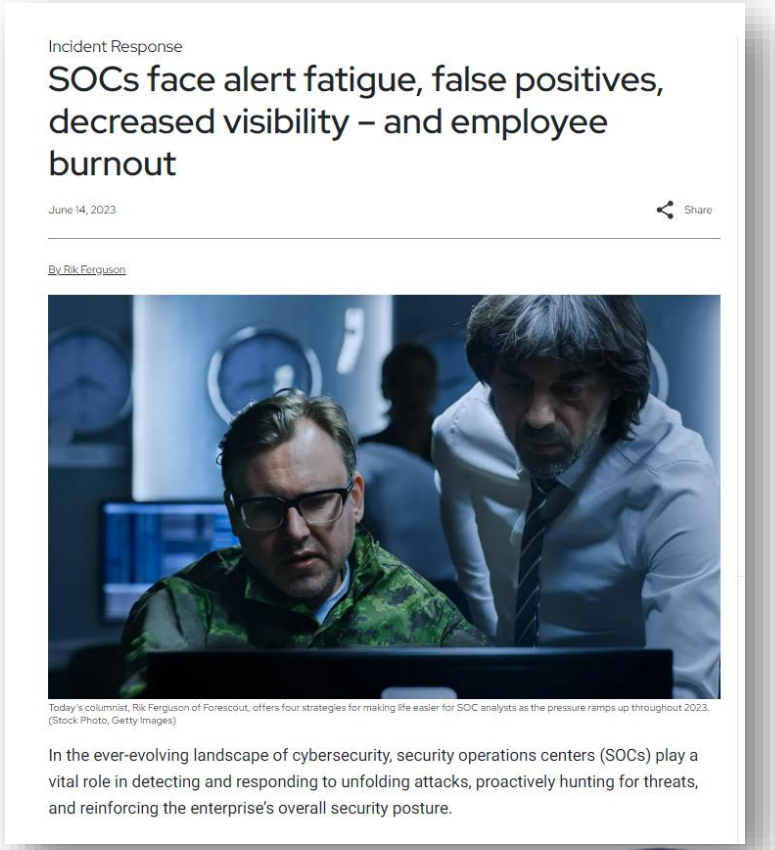
As we show in a chapter of the April 2024 Global Financial Stability Report, the risk of extreme losses from cyber incidents is increasing. Such losses could potentially cause funding problems for companies and even jeopardize their solvency. The size of these extreme losses has more than quadrupled since 2017 to $2.5 billion. And indirect losses like reputational damage or security upgrades are substantially higher.

Challenges & the need for automation

SOC operators have to deal with repetitive tasks that can be automated, handle alert fatigue



Increasing in number of attacks and complexity



Incident Response

SOCs face alert fatigue, false positives, decreased visibility – and employee burnout

June 14, 2023 Share

By Rik Ferguson

Today's columnist, Rik Ferguson of Forescout, offers four strategies for making life easier for SOC analysts as the pressure ramps up throughout 2023. (Stock Photo, Getty Images)

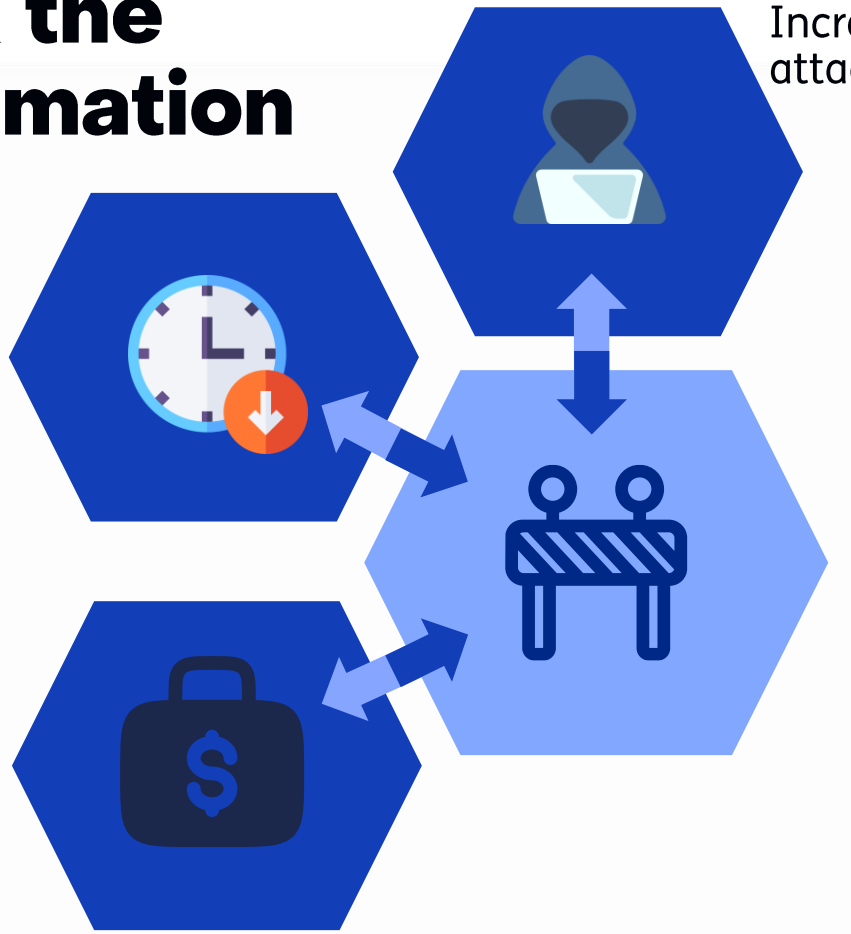
In the ever-evolving landscape of cybersecurity, security operations centers (SOCs) play a vital role in detecting and responding to unfolding attacks, proactively hunting for threats, and reinforcing the enterprise's overall security posture.

Challenges & the need for automation

Increasing in number of attacks and complexity

SOC operators have to deal with repetitive tasks that can be automated, handle alert fatigue

Closed-source automation tooling are proprietary, can lead to vendor lock-in



Challenges & the need for automation

Increasing in number of attacks and complexity

SOC operators have to deal with repetitive tasks that can be automated, handle alert fatigue

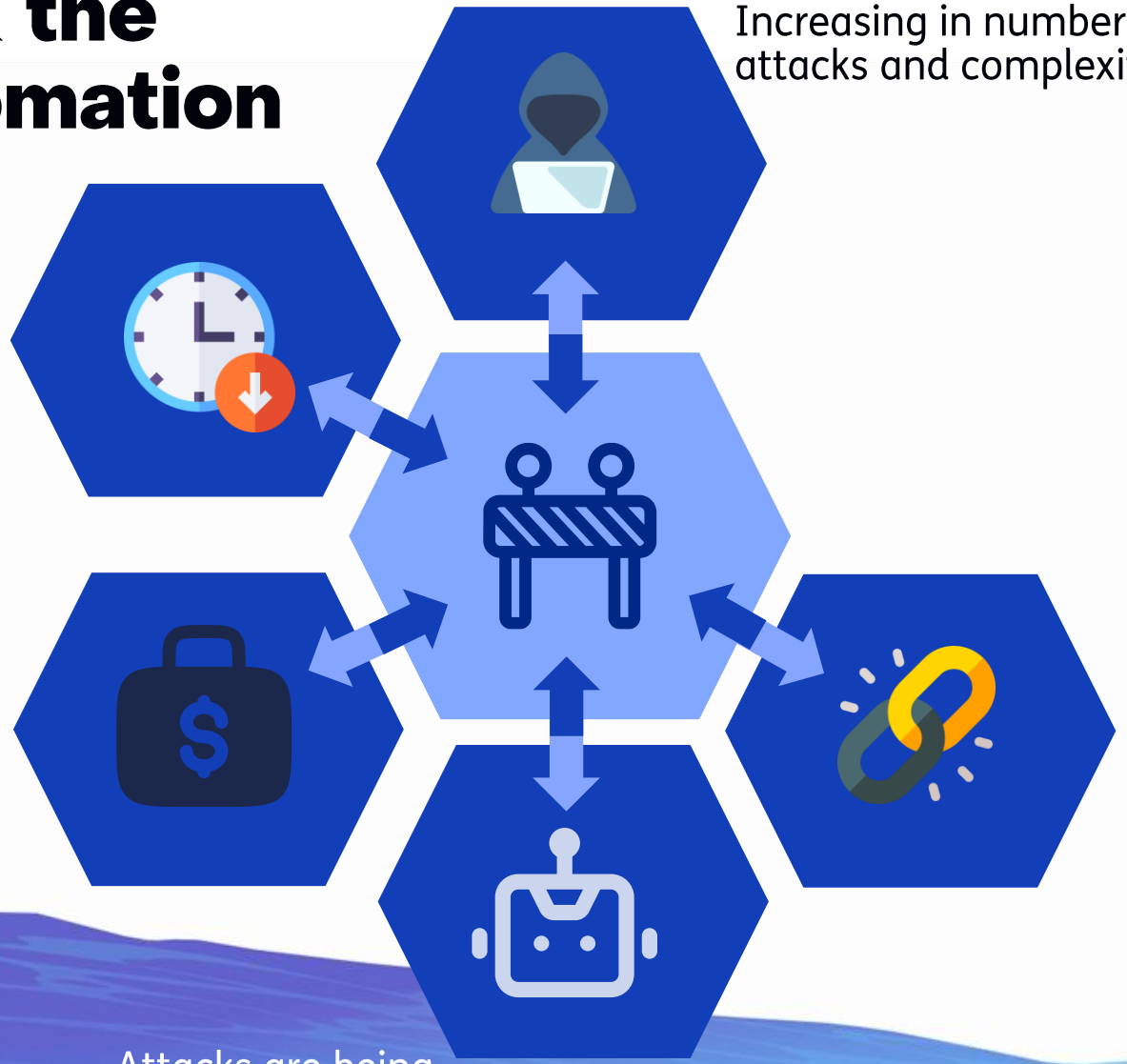
Closed-source automation tooling are proprietary, can lead to vendor lock-in

Attacks are being automated

Challenges & the need for automation

Increasing in number of attacks and complexity

SOC operators have to deal with repetitive tasks that can be automated, handle alert fatigue



Closed-source automation tooling are proprietary, can lead to vendor lock-in

IT landscape is complex and can consist of many different vendor solutions that need to work in an integrated manner

Attacks are being automated

Challenges & the need for automation

Increasing in number of attacks and complexity

SOC operators have to deal with repetitive tasks that can be automated, handle alert fatigue

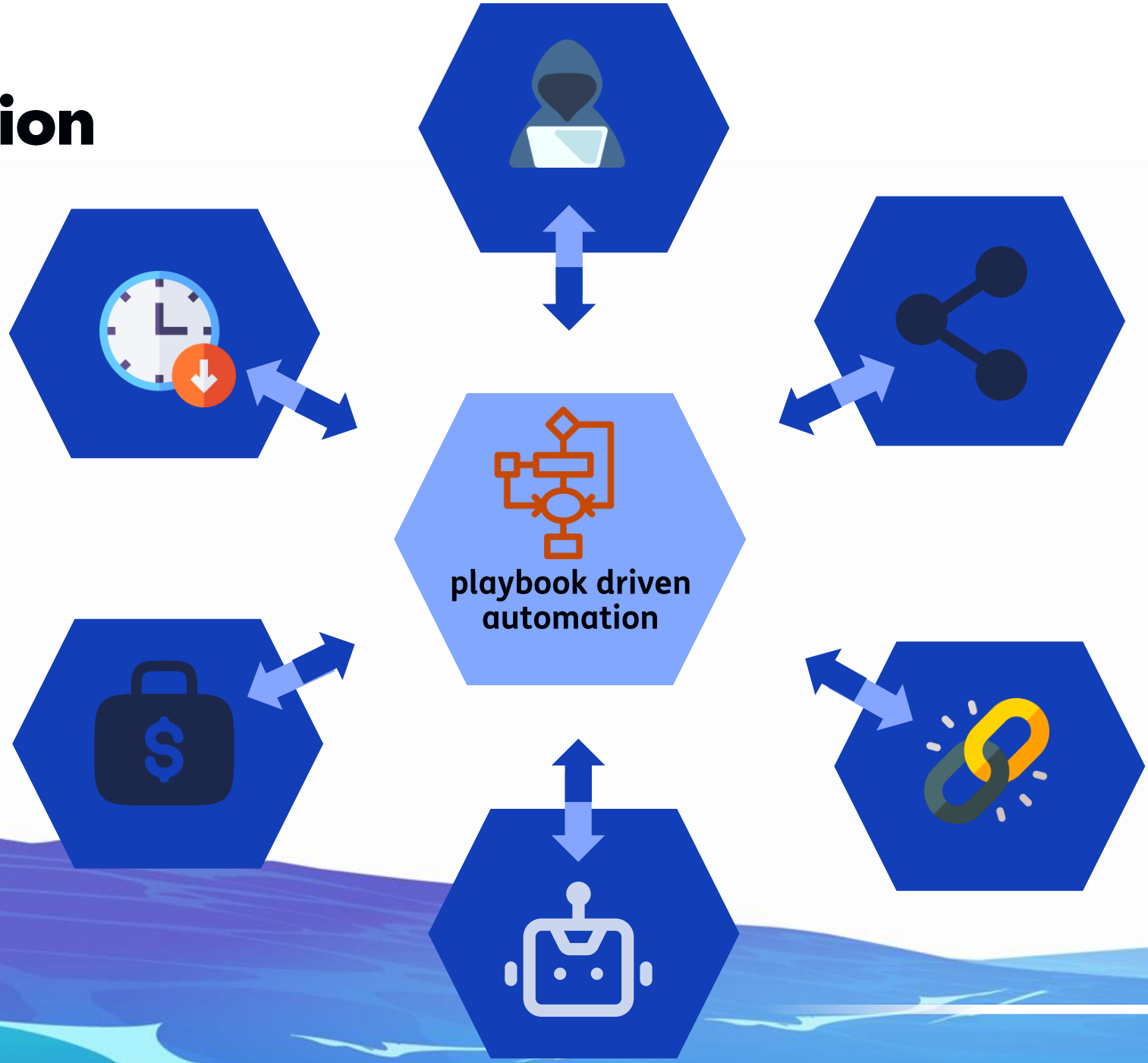
Automation playbooks are often proprietary and are hard to share

Closed-source automation tooling are proprietary, can lead to vendor lock-in

IT landscape is complex and can consist of many different vendor solutions that need to work in an integrated manner

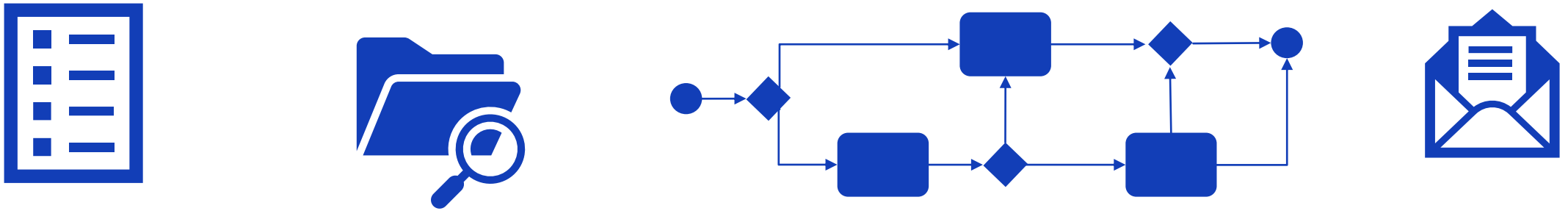
Attacks are being automated

The Solution



Playbooks for Security Response: What to do, When to do it

"A series of instructions that are structured and principled processes and procedures, which are documented, reusable, repeatable and optimised"



- Generally paper, text, wiki, BPMN, flow diagrams, emails, …
- Normalization intentions such as NIST and IACD
  - Machine-readable, but still flow diagrams and BPMN

Playbook-Driven Security Operations

	Traditional Way	Vendor Tools	?
What to do	✓	✓	✓
When to do it	✓	✓	✓
How to do it	✓	✓	✓
Automate it	✗	✓	✓
Share it	✗	✗	✓

✓ = Yes

✗ = It depends

Playbook-Driven Security Operations

	Traditional Way	Vendor Tools	?
What to do	✓	✓	✓
When to do it	✓	✓	✓
How to do it	✓	✓	✓
Automate it	✗	✓	✓
Share it	✗	✗	✓

✓ = Yes

✗ = It depends

Playbook-Driven Security Operations

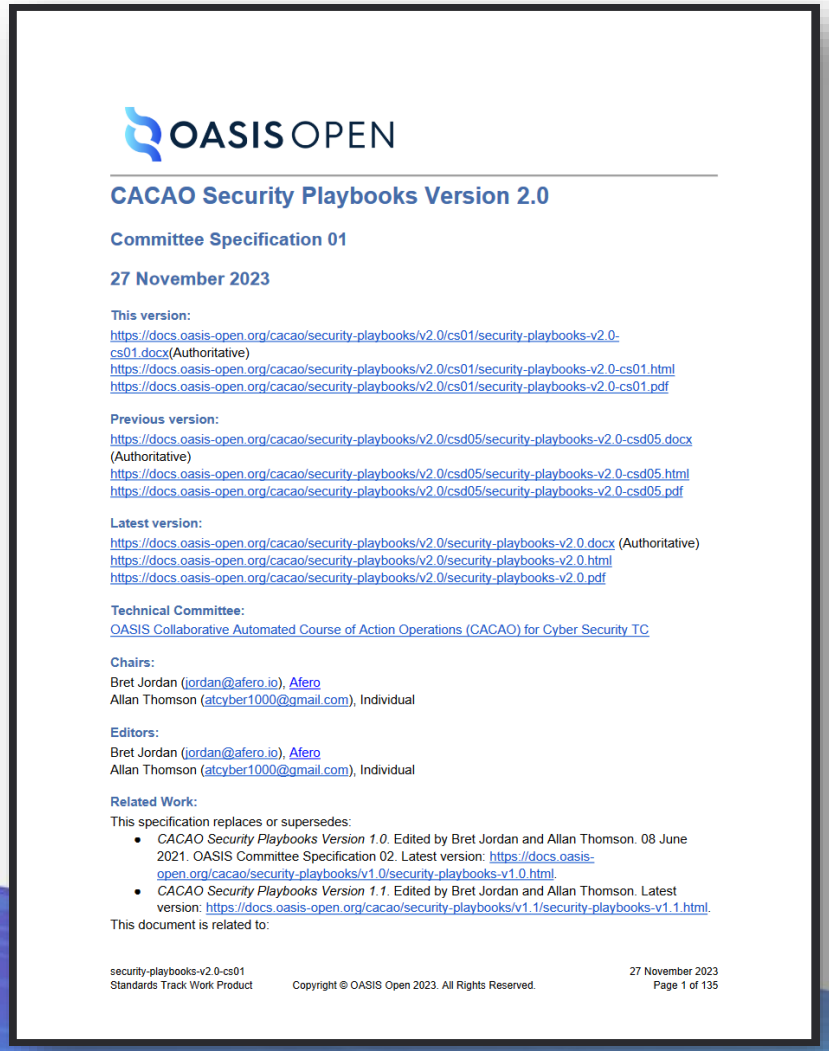
	Traditional Way	Vendor Tools	?
What to do	✓	✓	✓
When to do it	✓	✓	✓
How to do it	✓	✓	✓
Automate it	✗	✓	✓
Share it	✗	✗	✓

- **Connected to CTI**
- **Vendor-agnostic**
- **Machine readable**
- **Shareable by Design**
- **Enable interoperability**

✓ = Yes

✗ = It depends

An Open and Common Schema for Security Playbooks



OASIS OPEN

CACAO Security Playbooks Version 2.0

Committee Specification 01

27 November 2023

This version:
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.docx(Authoritative)
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.html
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.pdf

Previous version:
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd05/security-playbooks-v2.0-csd05.docx (Authoritative)
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd05/security-playbooks-v2.0-csd05.html
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd05/security-playbooks-v2.0-csd05.pdf

Latest version:
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.docx (Authoritative)
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.pdf

Technical Committee:
OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC

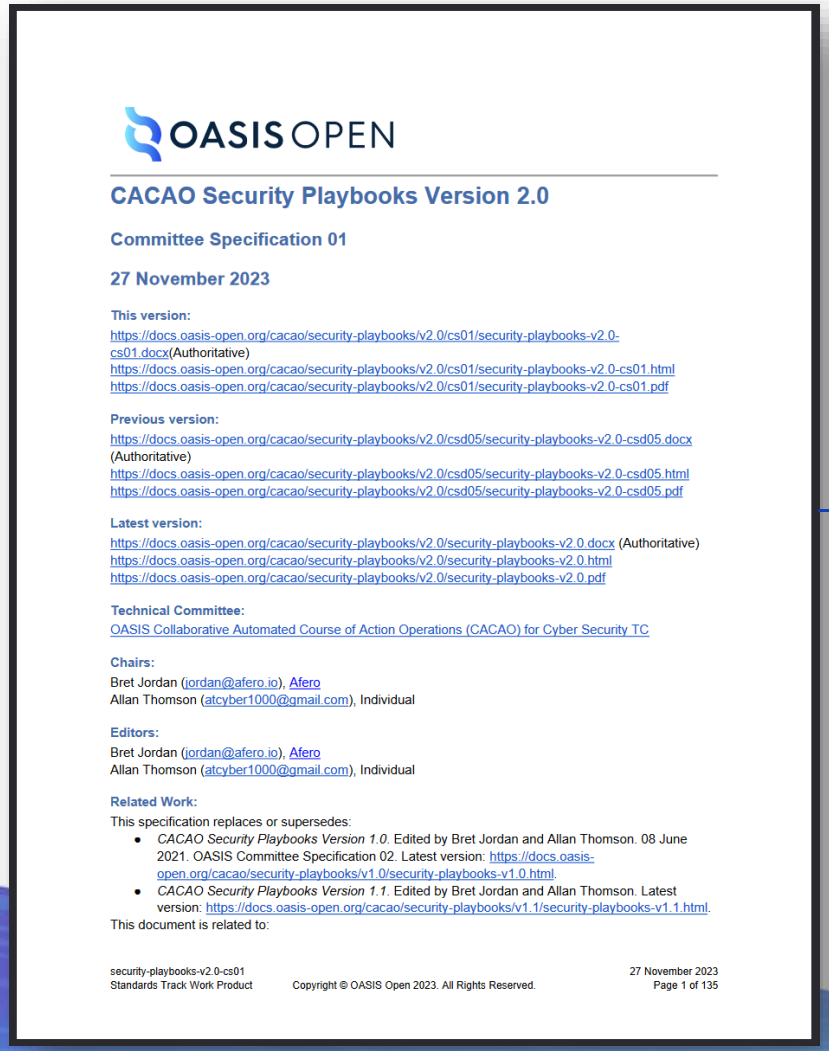
Chairs:
Bret Jordan (jordan@afero.io), Afero
Allan Thomson (atcyber1000@gmail.com), Individual

Editors:
Bret Jordan (jordan@afero.io), Afero
Allan Thomson (atcyber1000@gmail.com), Individual

Related Work:
This specification replaces or supersedes:
- *CACAO Security Playbooks Version 1.0*. Edited by Bret Jordan and Allan Thomson. 08 June 2021. OASIS Committee Specification 02. Latest version: https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html.
- *CACAO Security Playbooks Version 1.1*. Edited by Bret Jordan and Allan Thomson. Latest version: https://docs.oasis-open.org/cacao/security-playbooks/v1.1/security-playbooks-v1.1.html.

This document is related to:

An Open and Common Schema for Security Playbooks



OASIS OPEN

CACAO Security Playbooks Version 2.0

Committee Specification 01

27 November 2023

This version:
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.docx(Authoritative)
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.html
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.pdf

Previous version:
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd05/security-playbooks-v2.0-csd05.docx (Authoritative)
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd05/security-playbooks-v2.0-csd05.html
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd05/security-playbooks-v2.0-csd05.pdf

Latest version:
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.docx (Authoritative)
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html
https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.pdf

Technical Committee:
OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC

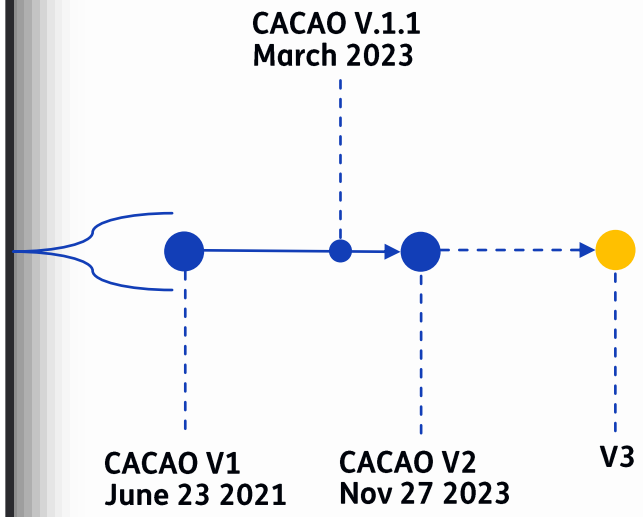
Chairs:
Bret Jordan (jordan@afero.io), Afero
Allan Thomson (atcyber1000@gmail.com), Individual

Editors:
Bret Jordan (jordan@afero.io), Afero
Allan Thomson (atcyber1000@gmail.com), Individual

Related Work:
This specification replaces or supersedes:
- *CACAO Security Playbooks Version 1.0*. Edited by Bret Jordan and Allan Thomson. 08 June 2021. OASIS Committee Specification 02. Latest version: https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html.
- *CACAO Security Playbooks Version 1.1*. Edited by Bret Jordan and Allan Thomson. Latest version: https://docs.oasis-open.org/cacao/security-playbooks/v1.1/security-playbooks-v1.1.html.

This document is related to:

security-playbooks-v2.0-cs01 27 November 2023
Standards Track Work Product Copyright © OASIS Open 2023. All Rights Reserved. Page 1 of 135



Why CACAO as open standard for automating Security Operations?

cacao PLAYBOOKS

OASIS OPEN

interoperable

- connected to CTI
- machine-readable
- shareable and reusable

Why CACAO as open standard for automating Security Operations?

cacao PLAYBOOKS

OASIS OPEN

interoperable

connected to CTI

Playbook pluggable in STIX COA object

machine-readable

shareable and reusable

STIX™

TAXII™

CACAO Playbook

- Metadata
- Workflow
  - Steps (control logic)
    - Commands
    - Agents via reference
    - Targets via reference
    - Other CACAO Playbooks via reference
- Authentication Information
- Agents
- Targets
- Data Markings
- Extensions
- Digital Signatures

Why CACAO as open standard for automating Security Operations?

cacao PLAYBOOKS

OASIS OPEN

interoperable

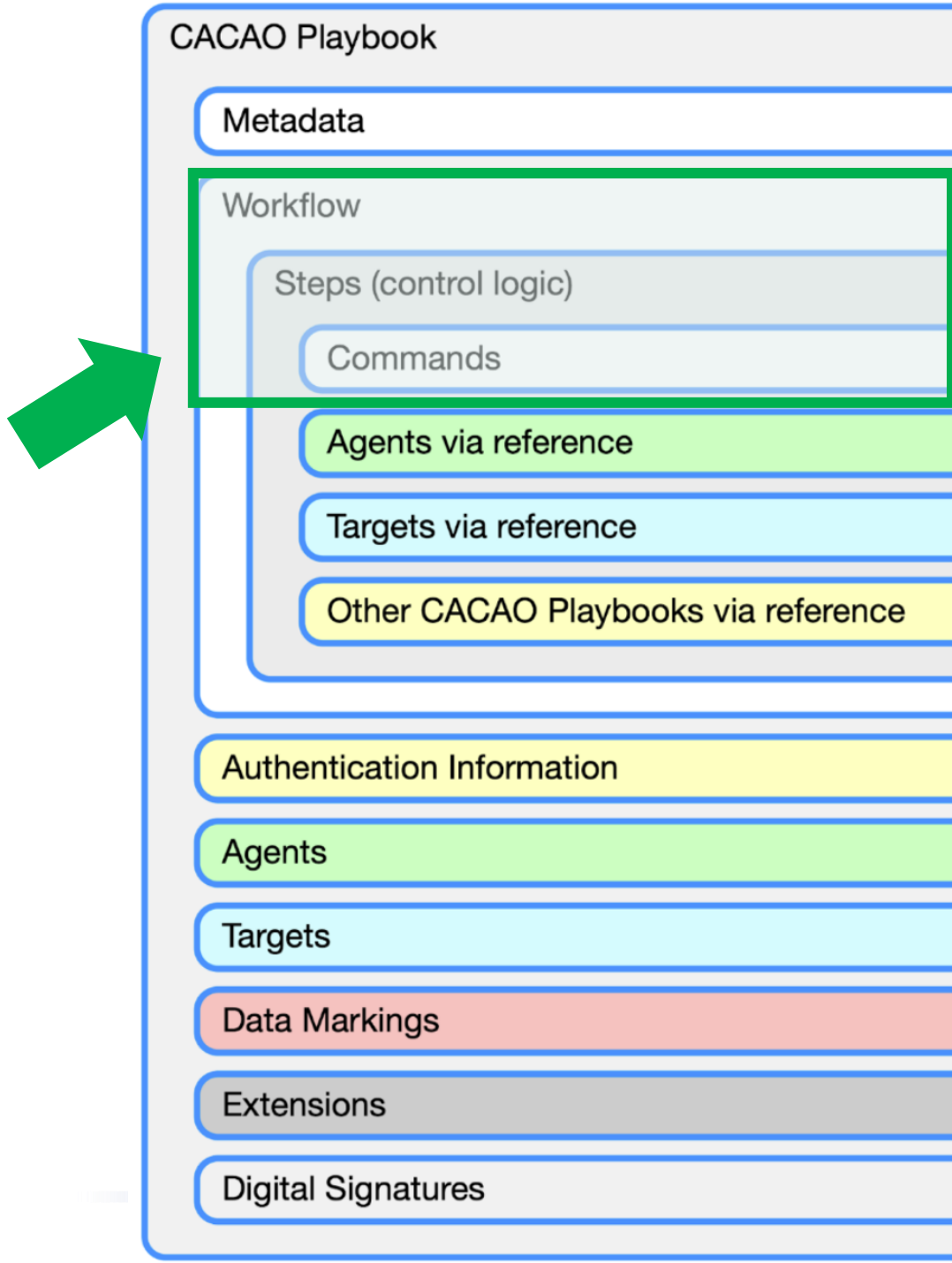
connected to CTI

machine-readable

Playbook control logic. Instructions can be written as

HTTP API
SSH
OpenC2
Bash
...

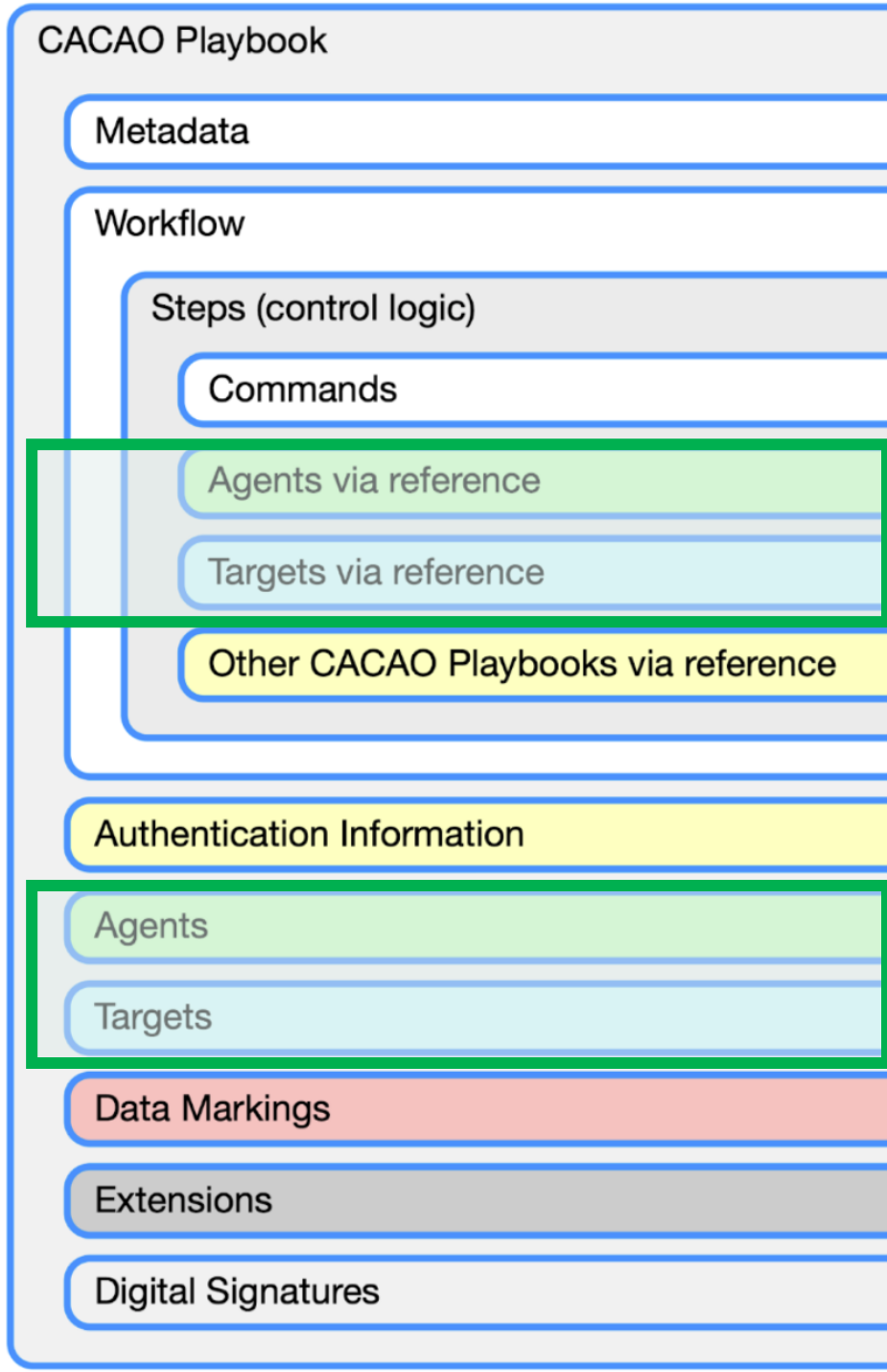
shareable and reusable



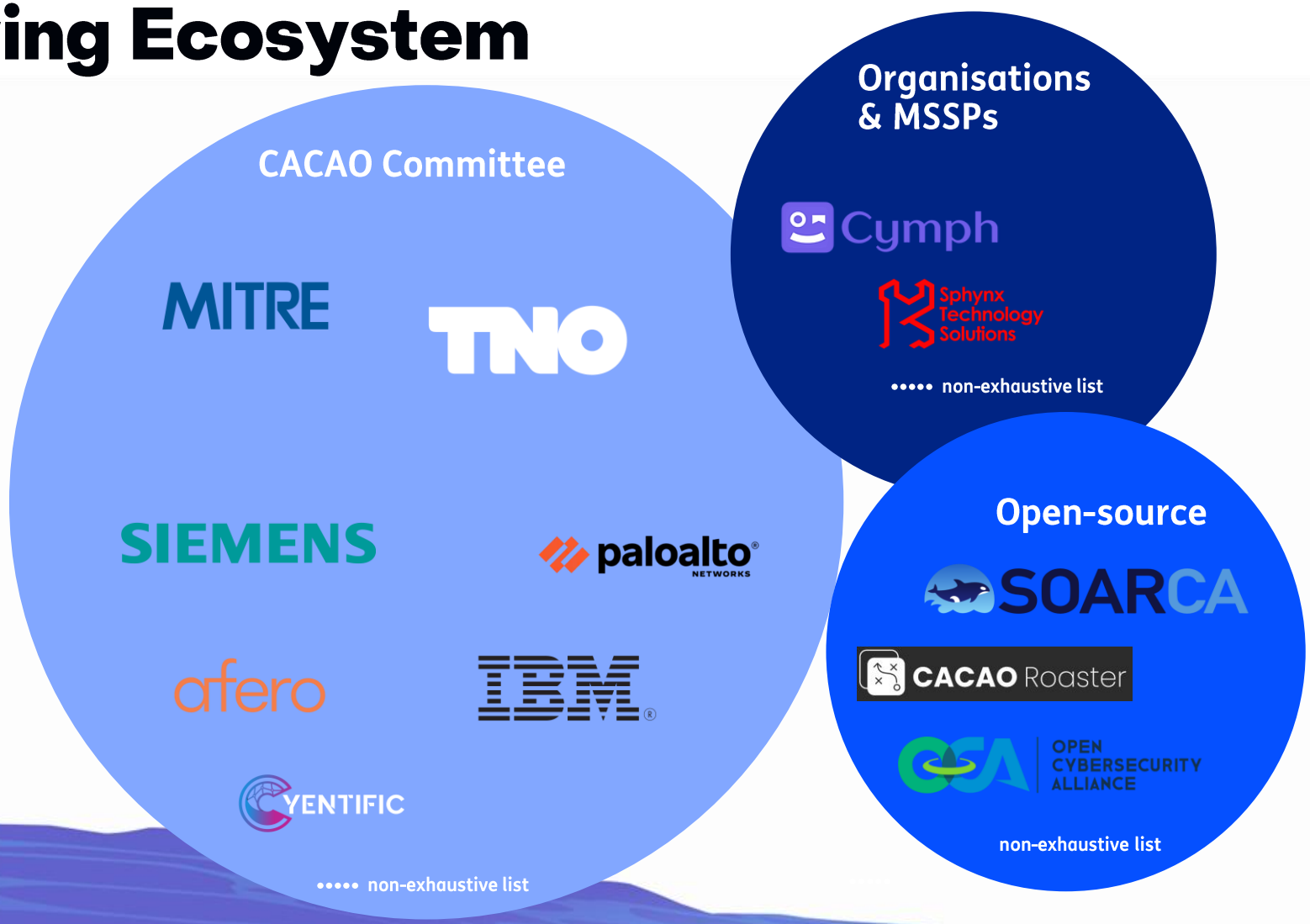
Why CACAO as open standard for automating Security Operations?

OASIS OPEN **interoperable**

- connected to CTI
- machine-readable
- **shareable and reusable**
  - Metadata mechanisms
  - **Playbook variables**
  - Instruction-specific **Agents Targets, and Authentication**



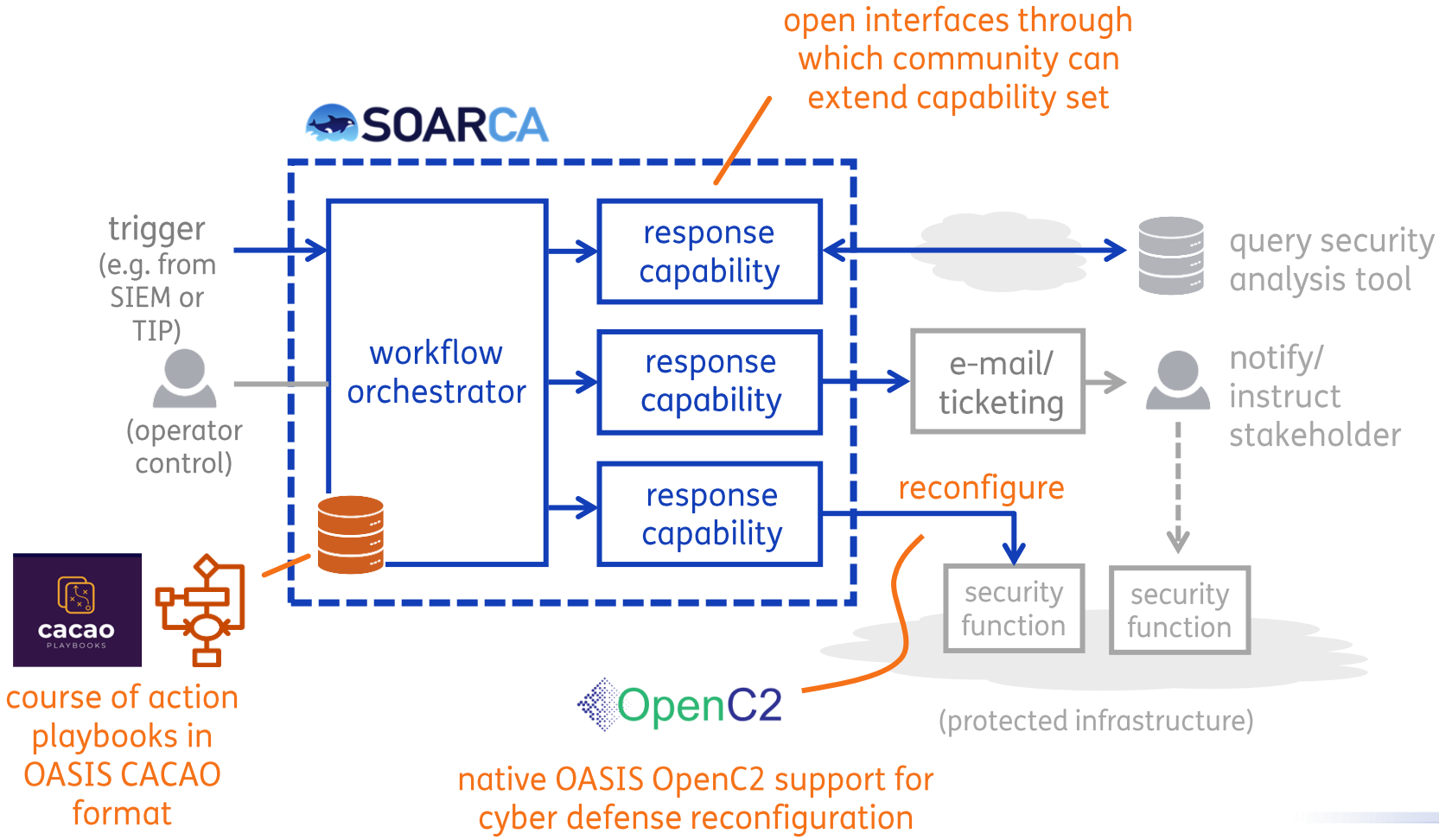
A Growing Ecosystem



The need: from CACAO to SOARCA

The need for an OS playbook execution engine

Both inside and outside of TNO need for interoperable workflow orchestration tooling that aids (cybersecurity) automation & innovation.



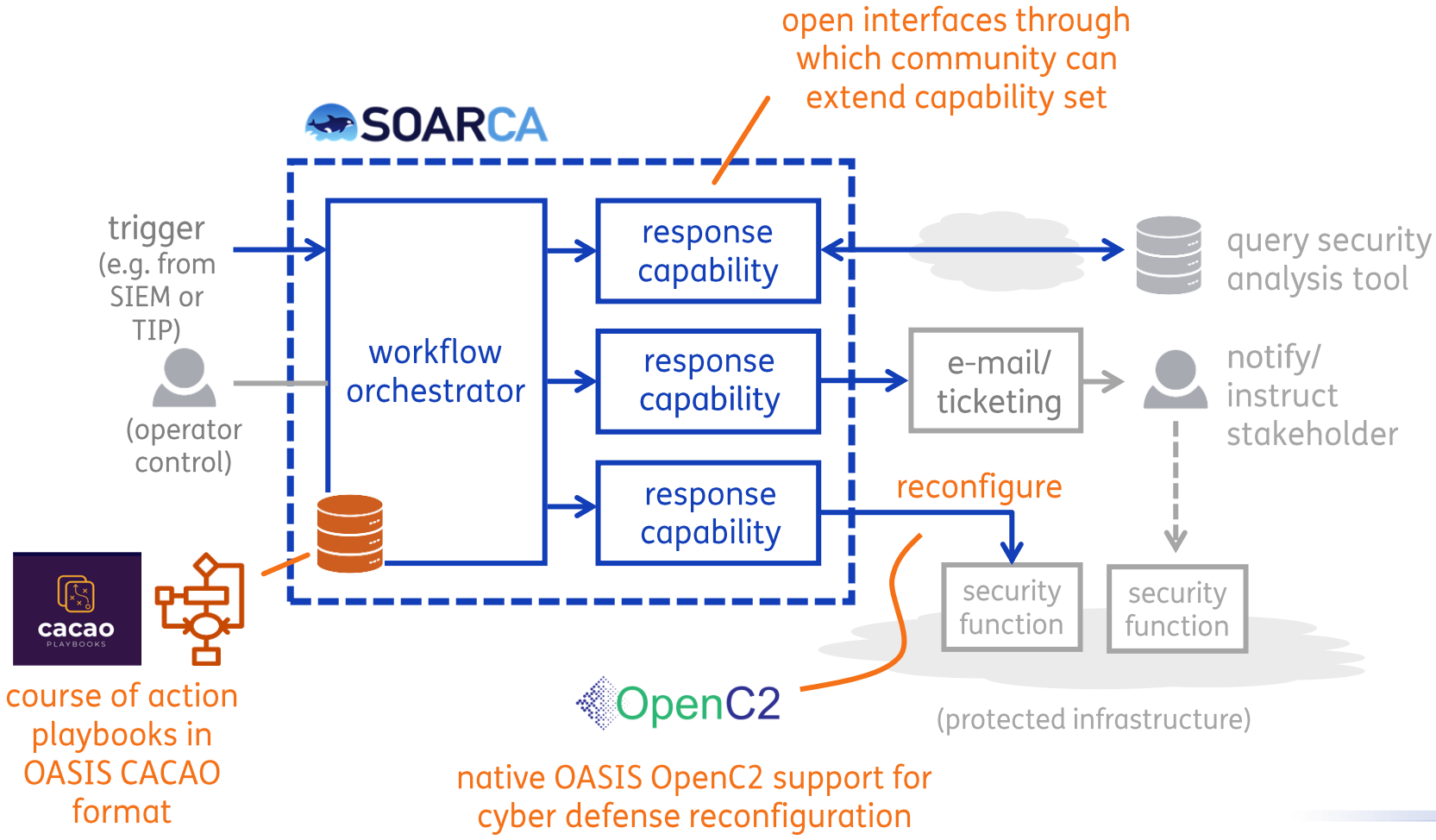
No tool that:

- is vendor-agnostic
- is Open-Source
- complies with the newest standards CACAOv2.0 and OpenC2
- is extensible and has open and well-defined interfaces
- can be used and adapted freely for research, demonstrations and PoC purposes.

The need: from CACAO to SOARCA

The need for an OS playbook execution engine

Both inside and outside of TNO need for interoperable workflow orchestration tooling that aids (cybersecurity) automation & innovation.



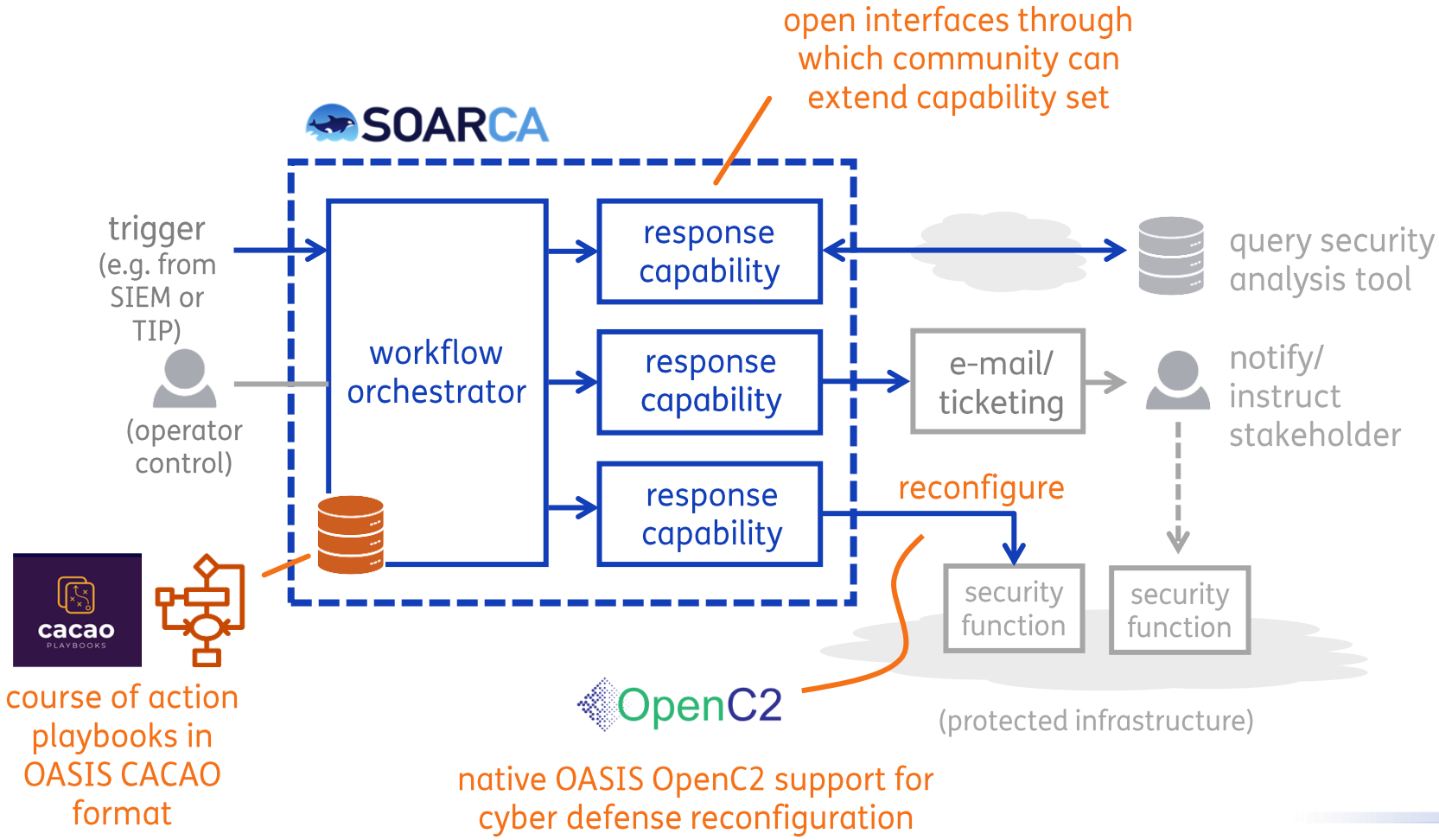
No tool that

- **is vendor-agnostic**
- is Open-Source
- complies with the newest standards CACAOv2.0 and OpenC2
- is extensible and has open and well-defined interfaces
- can be used and adapted freely for research, demonstrations and PoC purposes.

The need: from CACAO to SOARCA

The need for an OS playbook execution engine

Both inside and outside of TNO need for interoperable workflow orchestration tooling that aids (cybersecurity) automation & innovation.



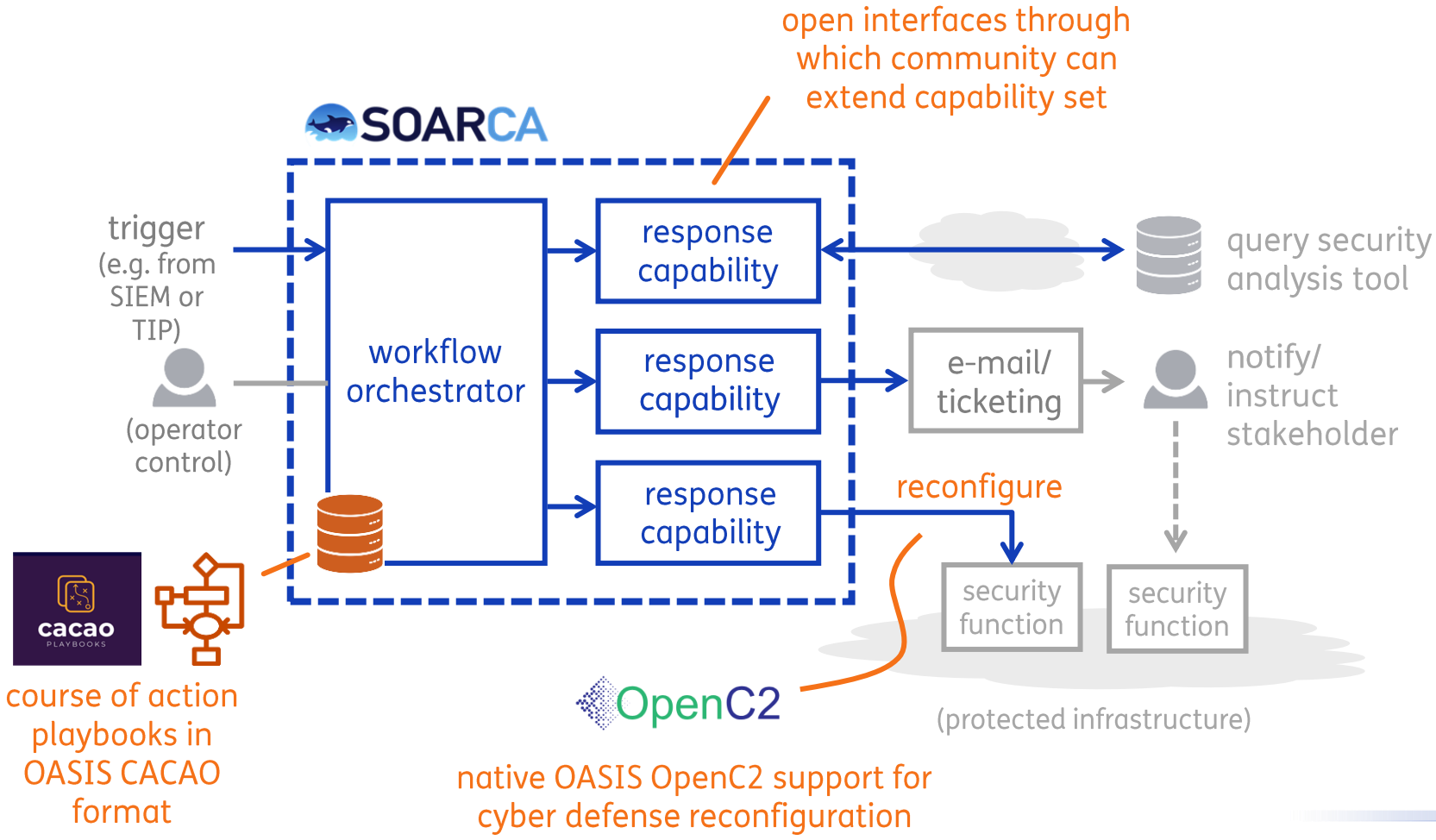
No tool that

- is vendor-agnostic
- **is Open-Source**
- complies with the newest standards CACAOv2.0 and OpenC2
- is extensible and has open and well-defined interfaces
- can be used and adapted freely for research, demonstrations and PoC purposes.

The need: from CACAO to SOARCA

The need for an OS playbook execution engine

Both inside and outside of TNO need for interoperable workflow orchestration tooling that aids (cybersecurity) automation & innovation.



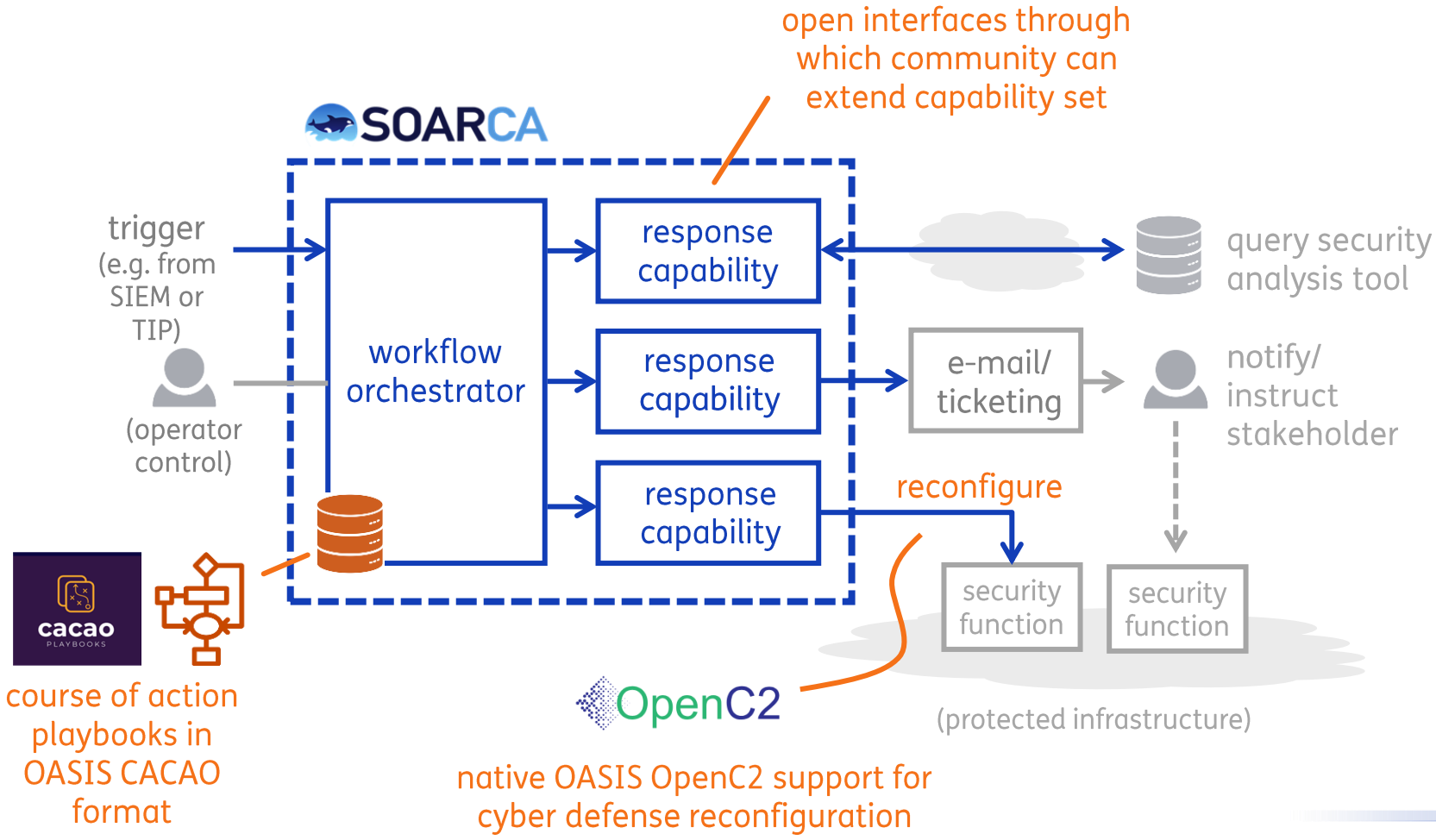
No tool that

- is vendor-agnostic
- is Open-Source
- **complies with the newest standards CACAOv2.0 and OpenC2**
- is extensible and has open and well-defined interfaces
- can be used and adapted freely for research, demonstrations and PoC purposes.

The need: from CACAO to SOARCA

The need for an OS playbook execution engine

Both inside and outside of TNO need for interoperable workflow orchestration tooling that aids (cybersecurity) automation & innovation.



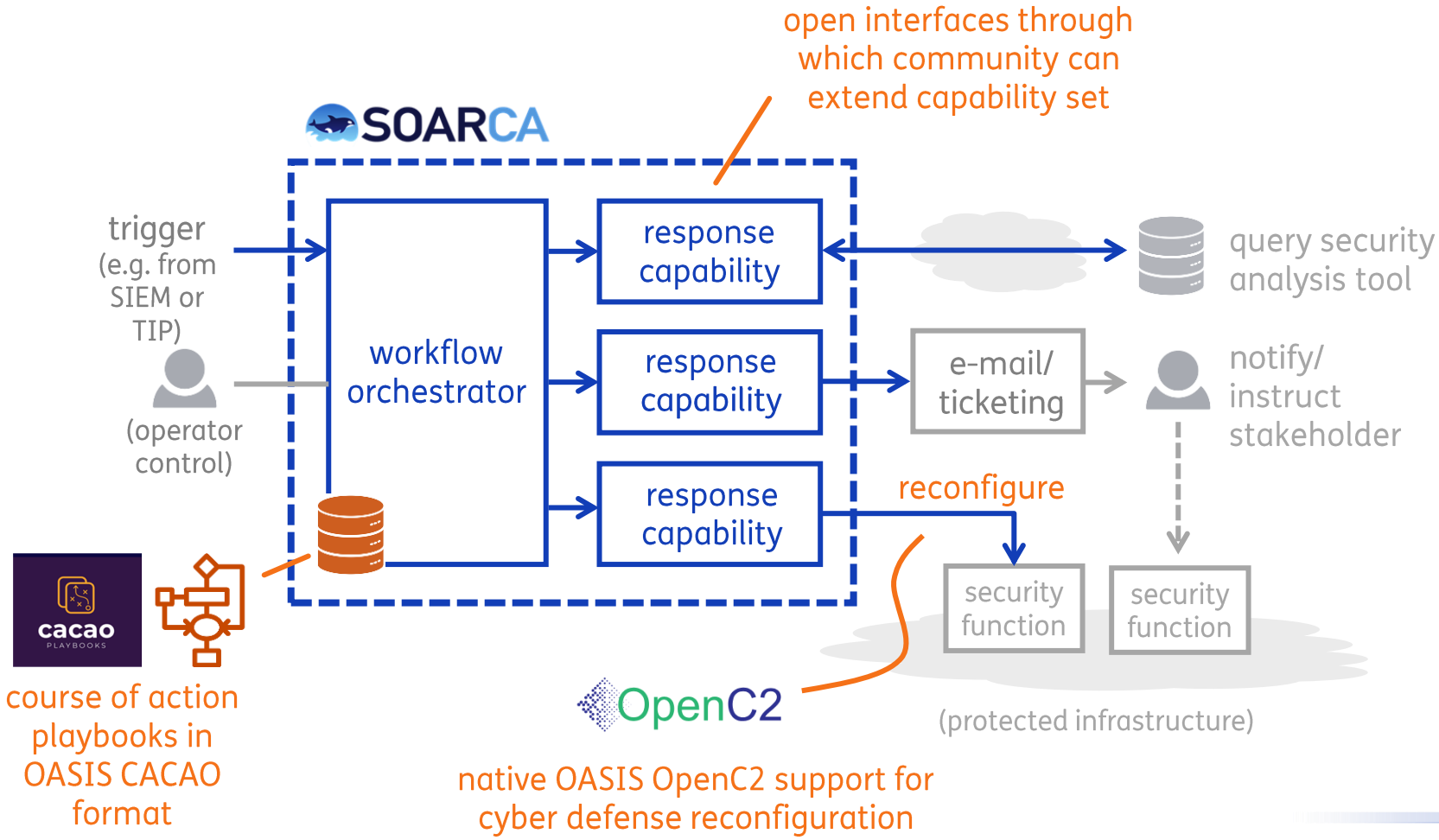
No tool that

- is vendor-agnostic
- is Open-Source
- complies with the newest standards CACAOv2.0 and OpenC2
- **is extensible and has open and well-defined interfaces**
- can be used and adapted freely for research, demonstrations and PoC purposes.

The need: from CACAO to SOARCA

The need for an OS playbook execution engine

Both inside and outside of TNO need for interoperable workflow orchestration tooling that aids (cybersecurity) automation & innovation.

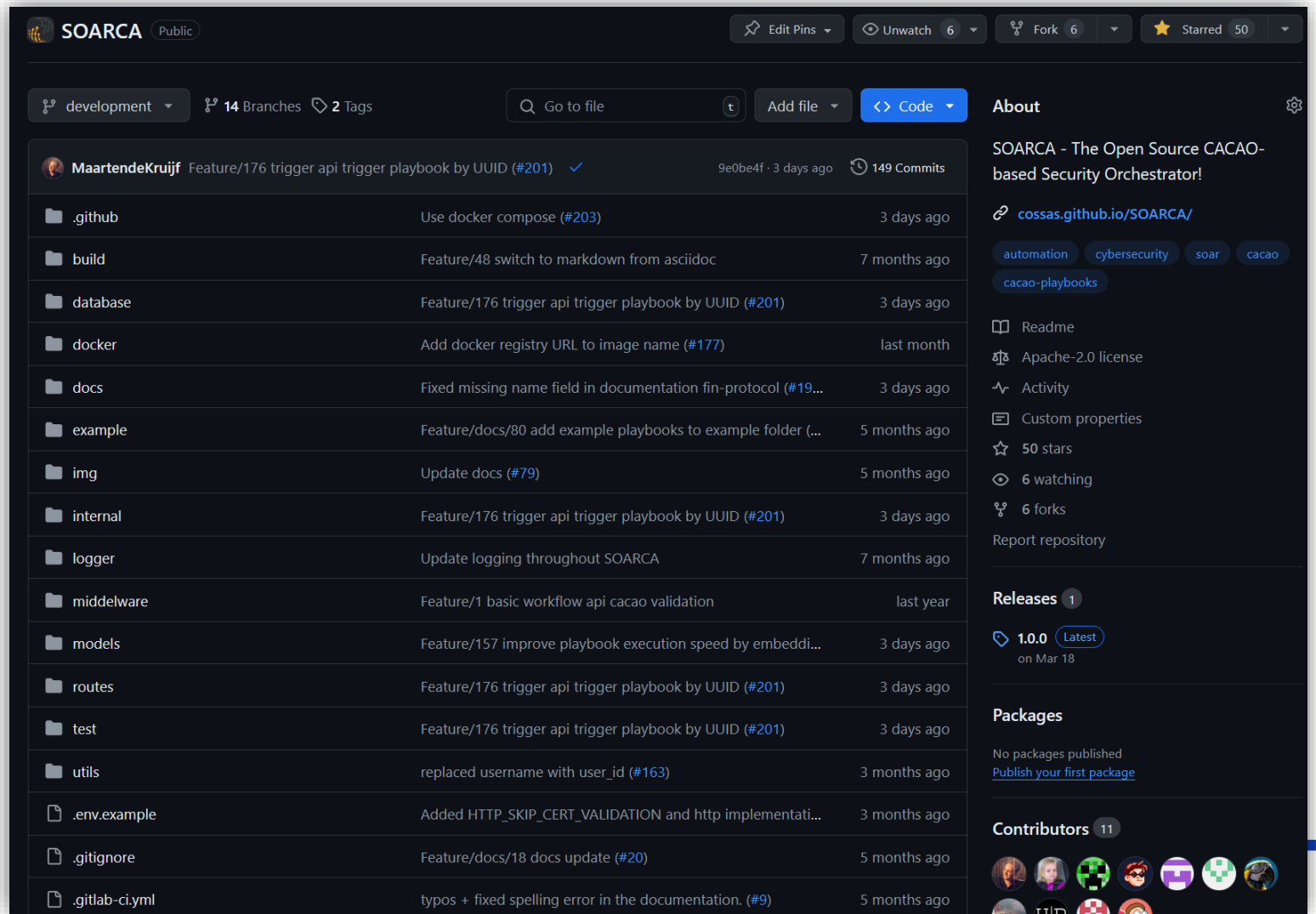


No tool that

- is vendor-agnostic
- is Open-Source
- complies with the newest standards CACAOv2.0 and OpenC2
- is extensible and has open and well-defined interfaces
- **can be used and adapted freely for research, demonstrations and PoC purposes.**

From CACAO to SOARCA

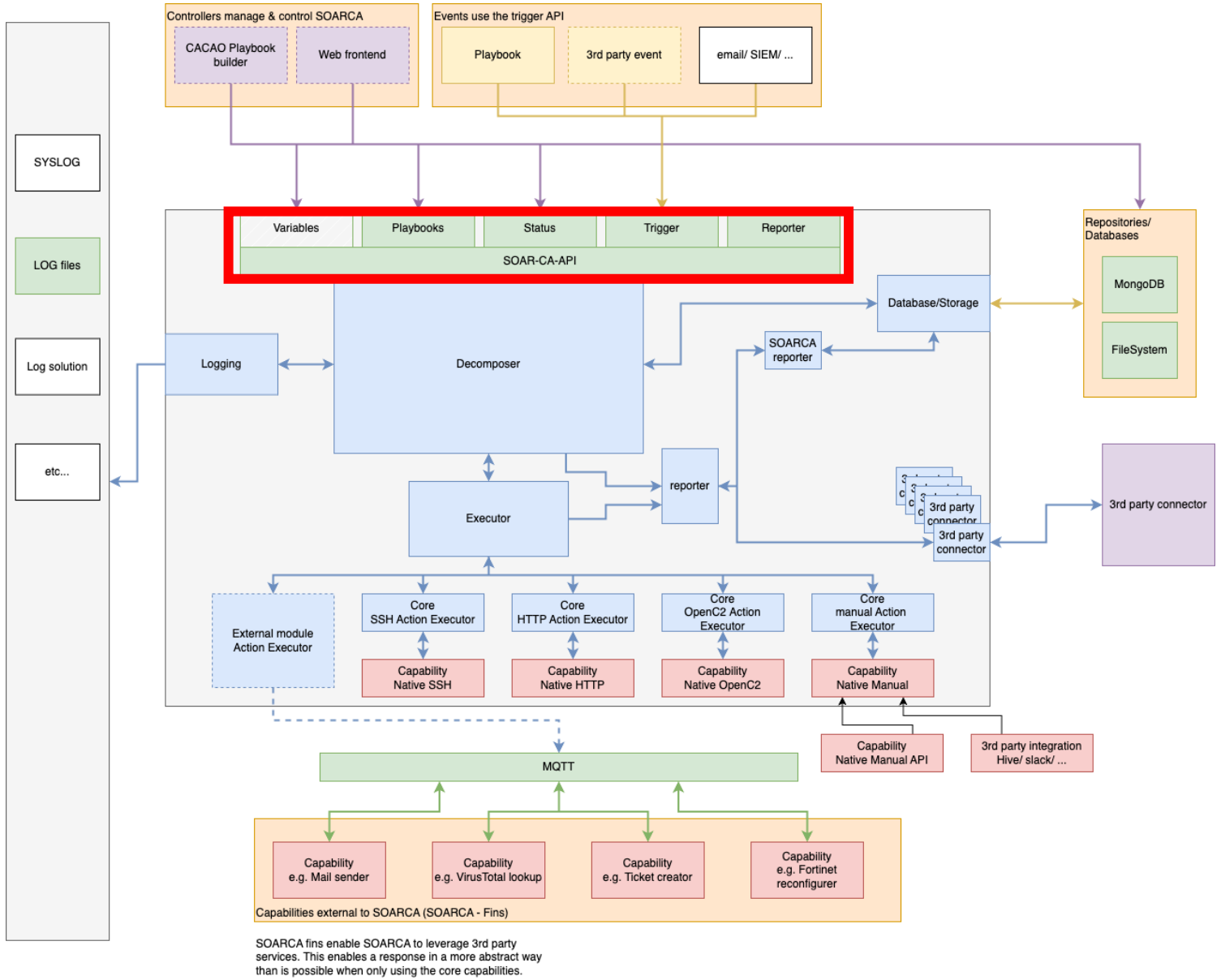
https://cossas-project.org/portfolio/SOARCA/
https://github.com/COSSAS/SOARCA



SOARCA Technical architecture

Main Takeways

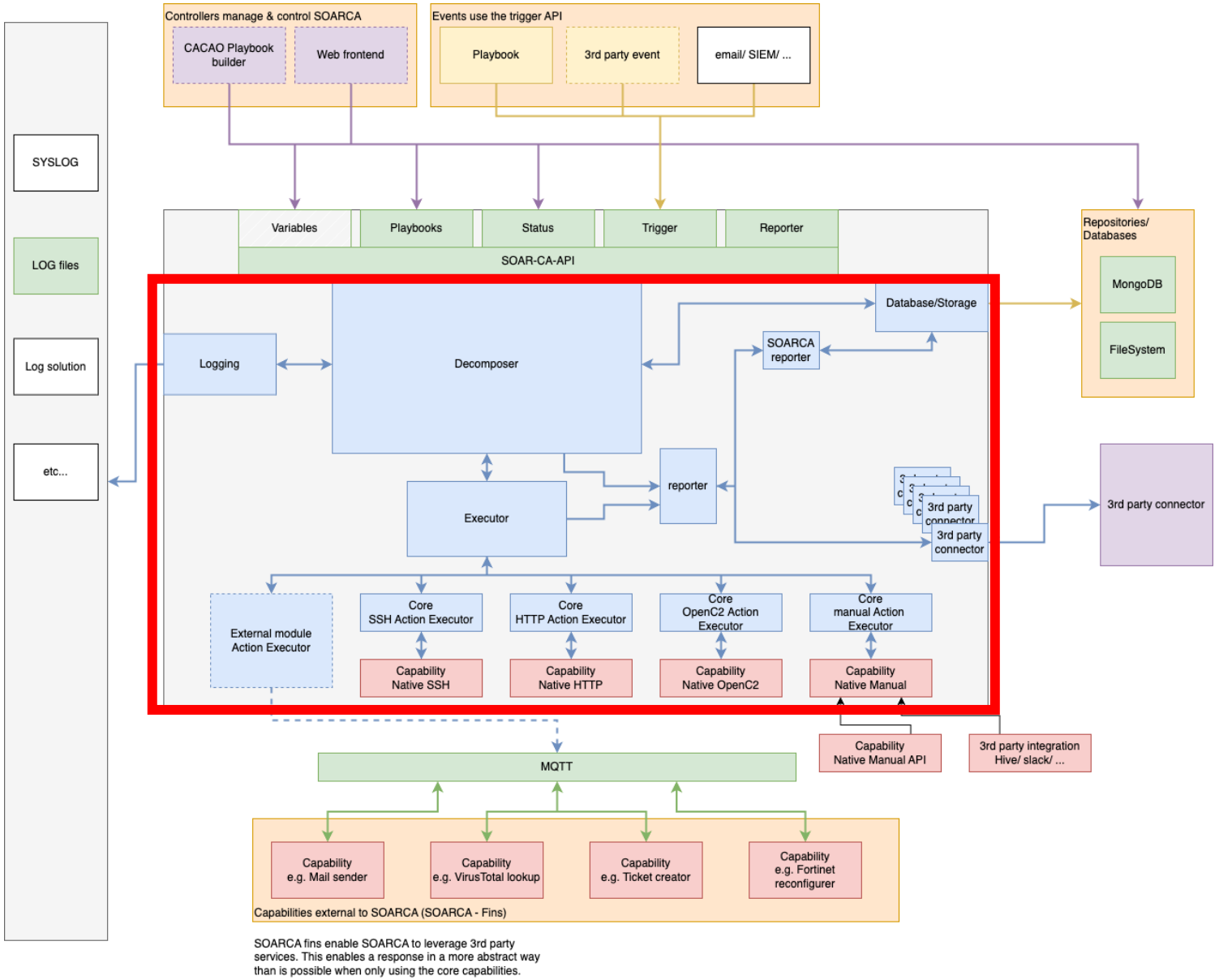
- **SOARCA offers a well designed and documented API allowing for easy integration**
- Modular design to allow easy changes and extension
- SOARCA allows for extending upon CACAO step types by utilising our MQTT based extensions, called SOARCA-fins



SOARCA Technical architecture

Main Takeways

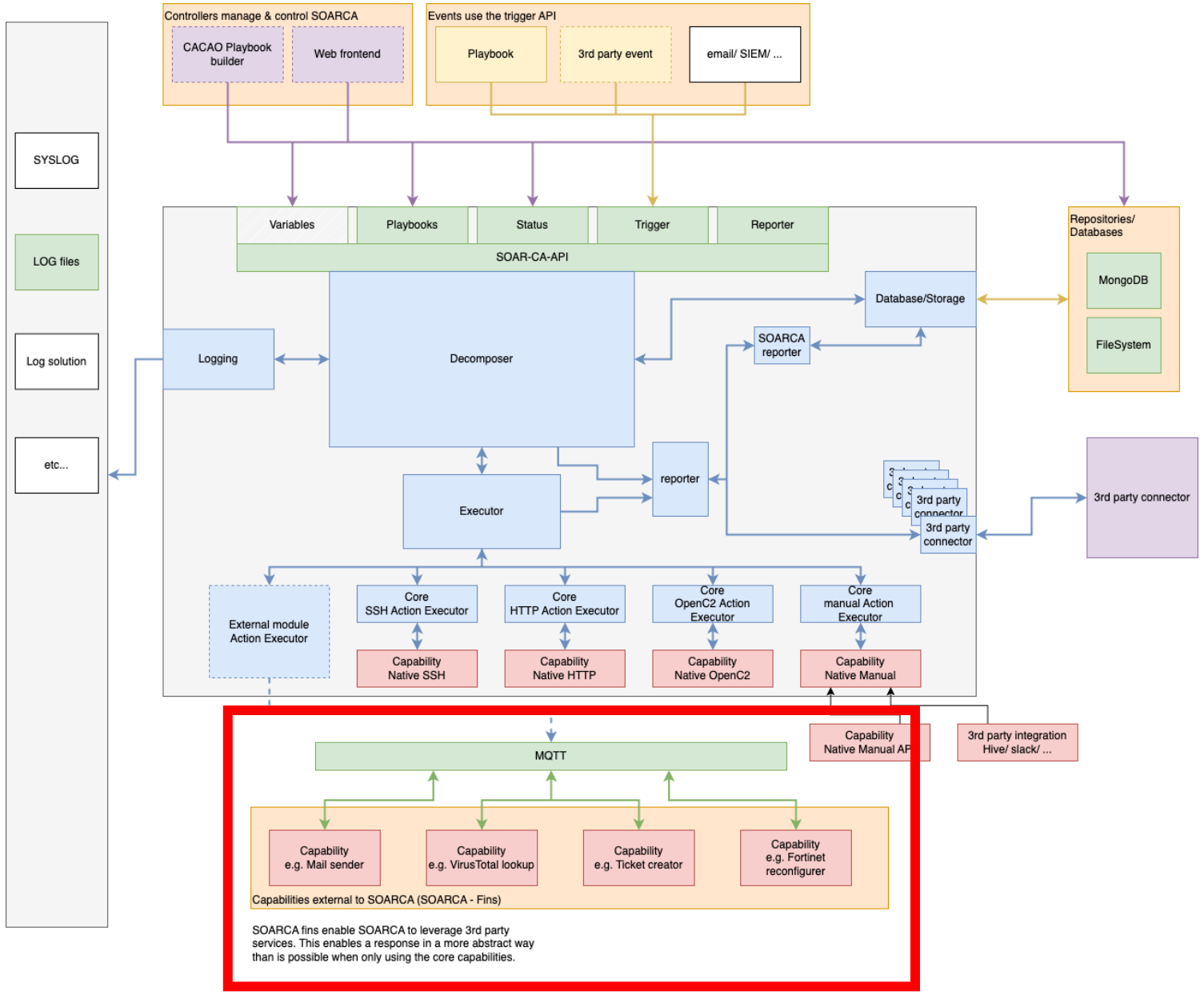
- SOARCA offers a well designed and documented API allowing for easy integration
- **Modular design to allow easy changes and extension**
- SOARCA allows for extending upon CACAO step types by utilising our MQTT based extensions, called SOARCA-fins



SOARCA Technical architecture

Main Takeways

- SOARCA offers a well designed and documented API allowing for easy integration
- Modular design to allow easy changes and extension
- **SOARCA allows for extending upon CACAO step types by utilising our MQTT based extensions, called SOARCA-fins**

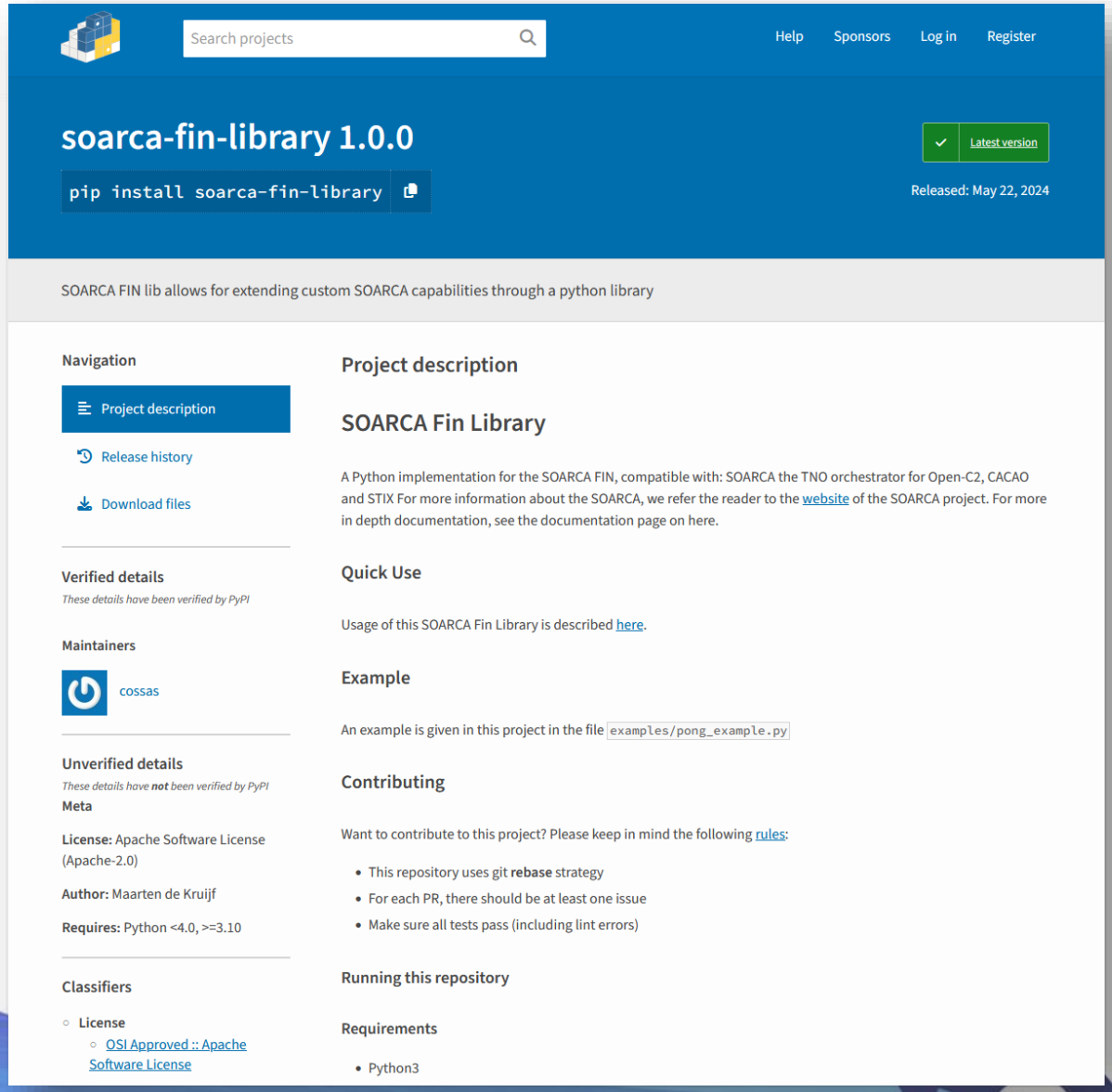


Extending SOARCA with Custom Fins (extensions)

SOARCA compatible library for extending to custom needs

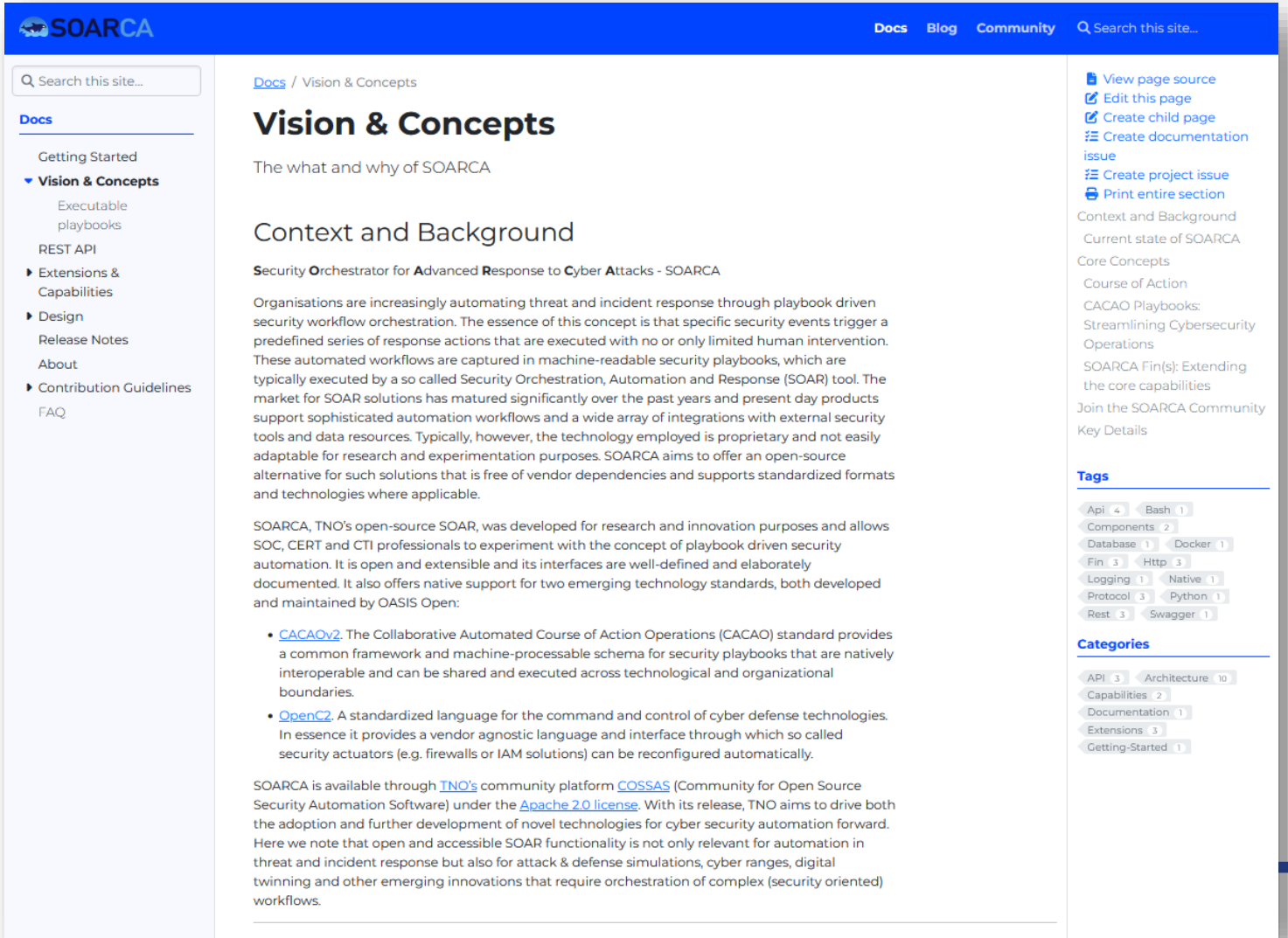
In some cases you might require additional capabilities.....

Install through pip: pip install soarca-fin-library

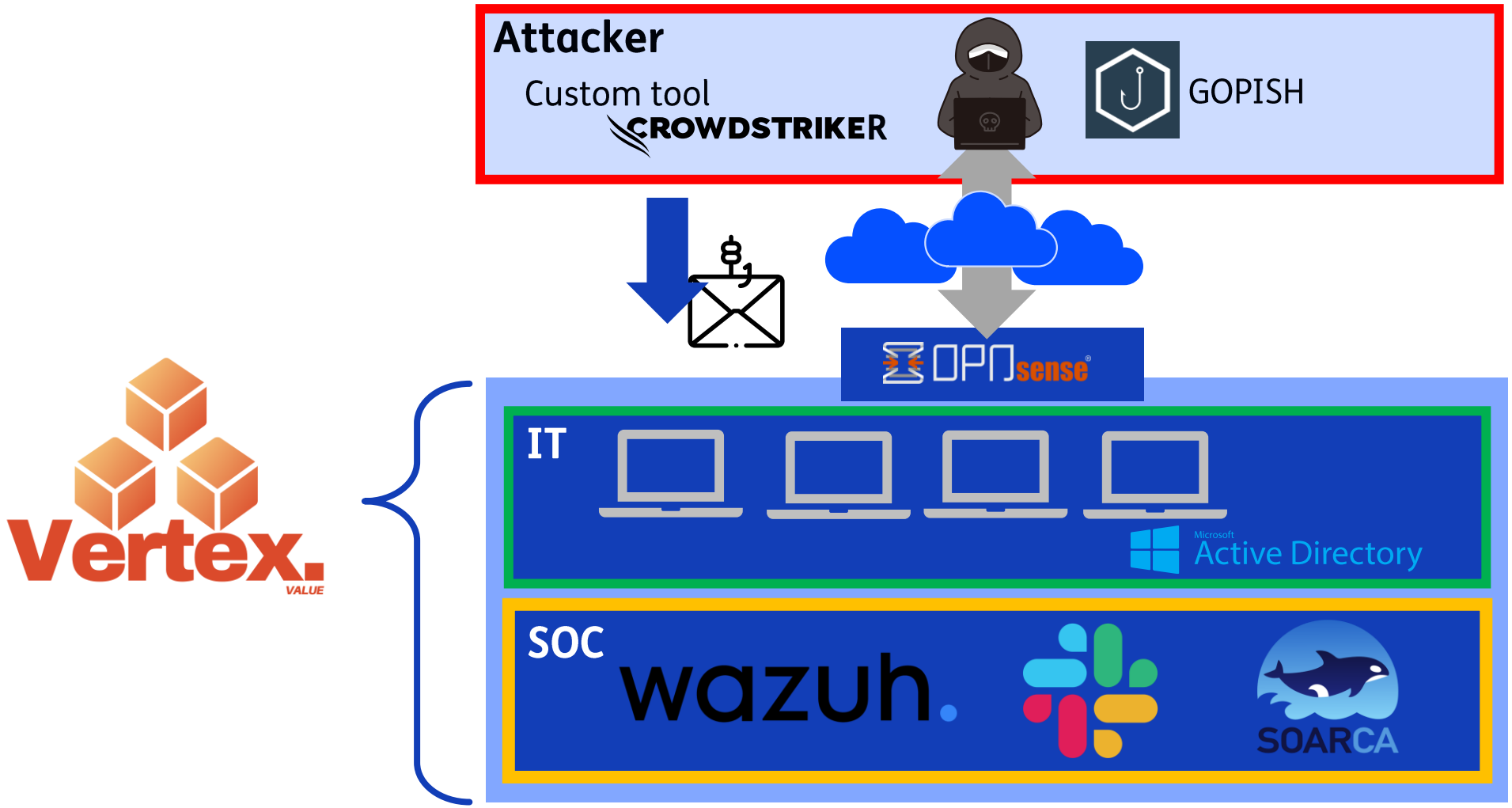


From CACAO to SOARCA

https://cossas-project.org/portfolio/SOARCA/
https://github.com/COSSAS/SOARCA



Phishing on VertexValue: a SOARCA demo scenario

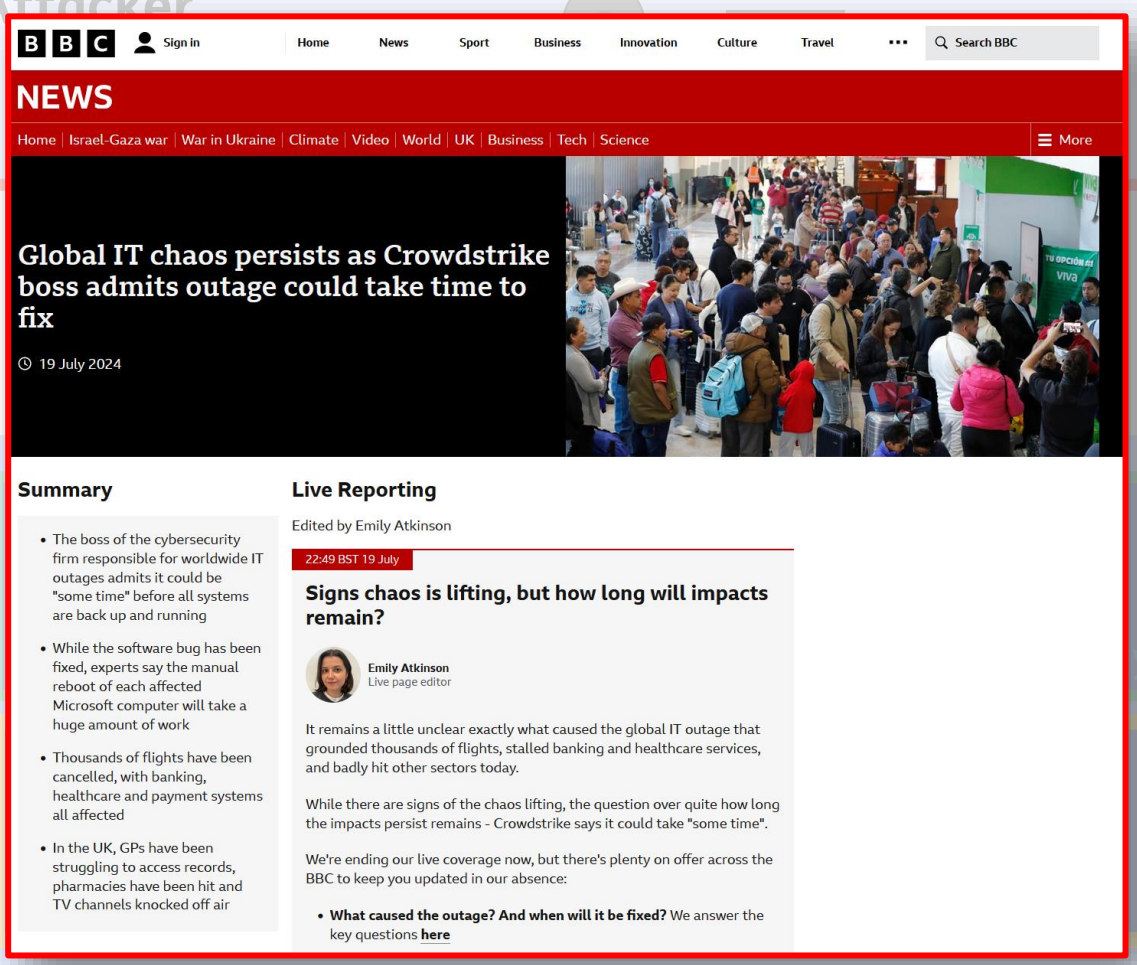


Phishing on VertexValue: a SOARCA demo scenario

1. **Crowdstrike outage situation**
2. Attacker launches phishing campaign with fake Crowdstrike update tool
3. User received email and is redirected to legitimate looking website
4. User downloads fake update tool (ransomware)
5. Download gets detected by Wazuh
6. Wazuh triggers SOARCA by sending a CACAO Playbook
7. SOARCA & CACAO playbook based remediation

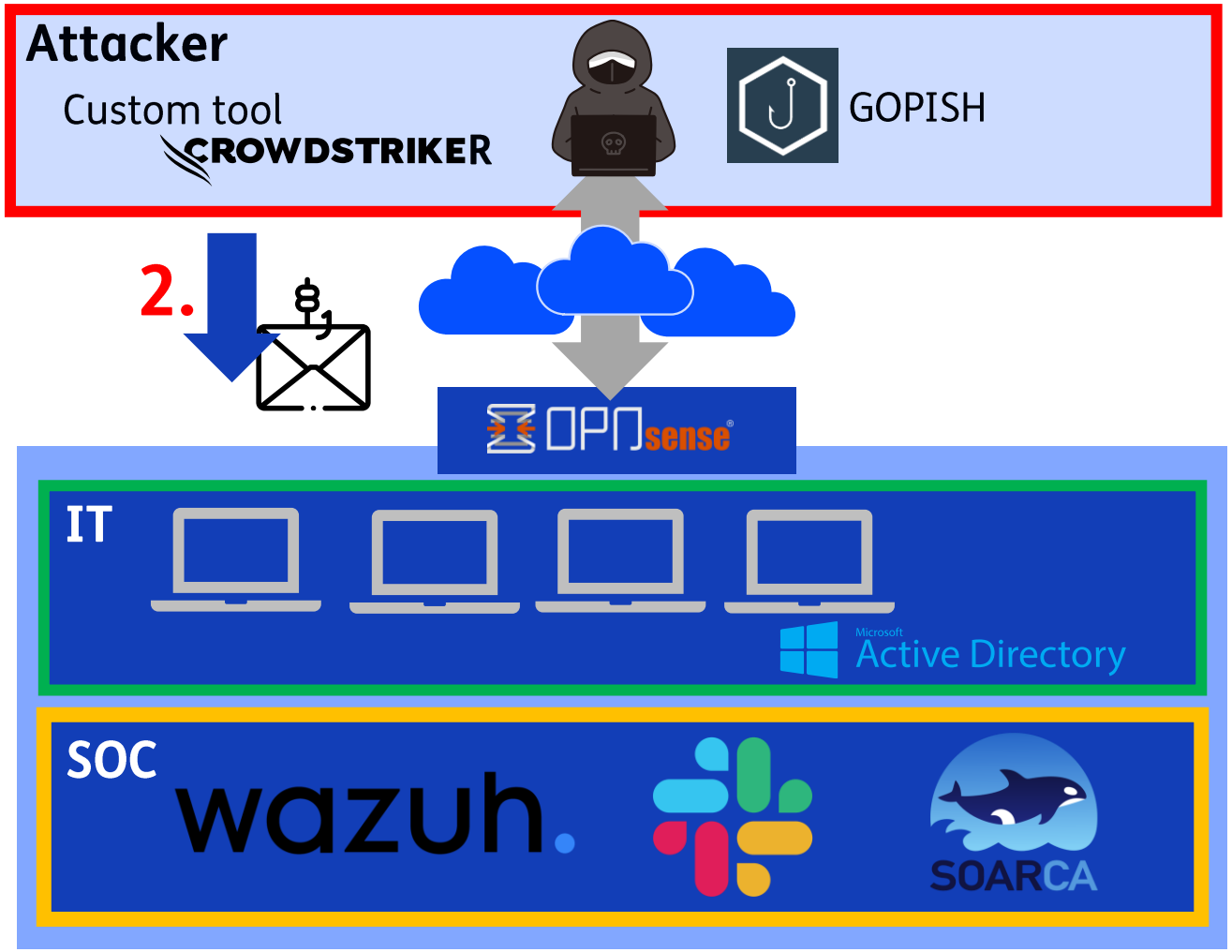
Attacker

1.



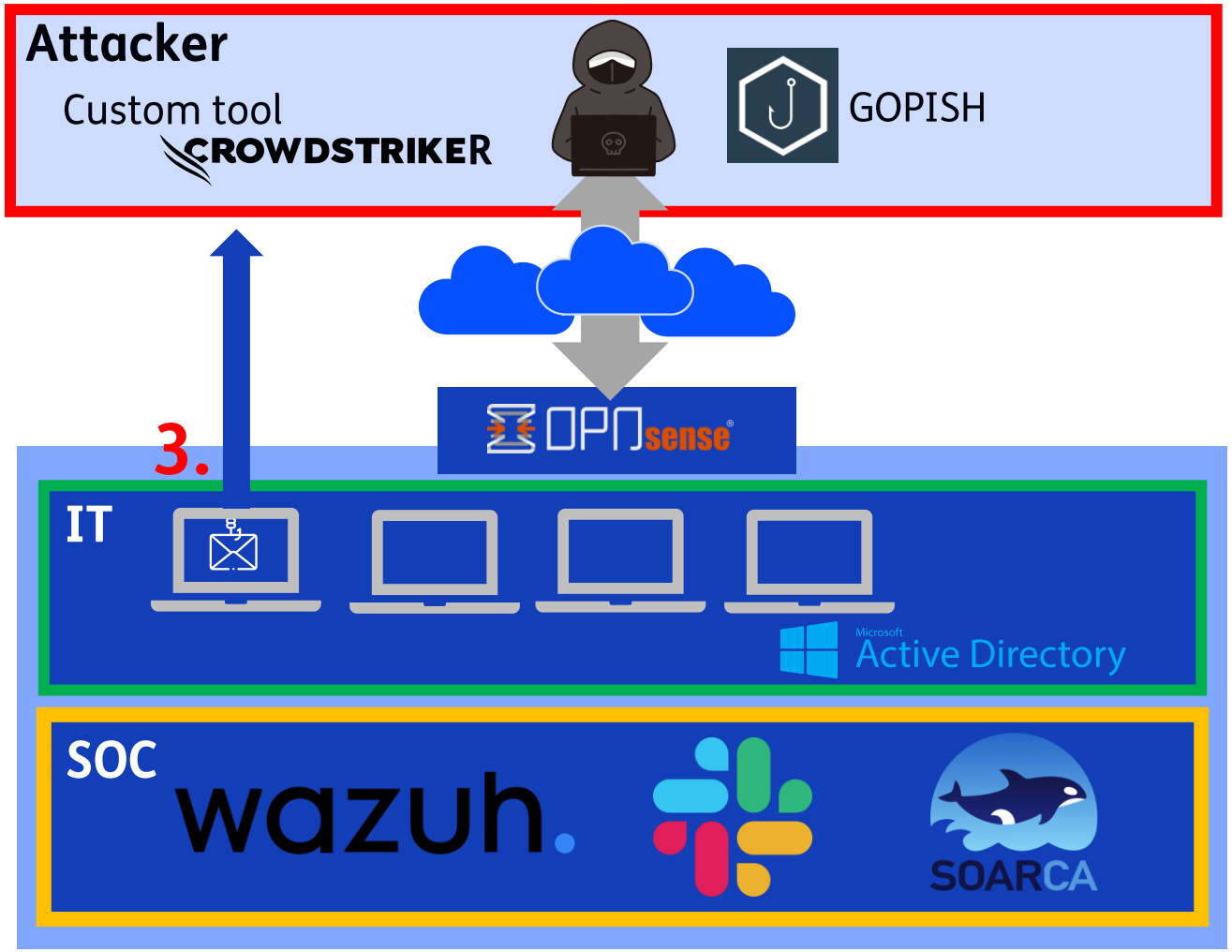
Phishing on VertexValue: a SOARCA demo scenario

1. Crowdstrike outage situation
2. **Attacker launches phishing campaign with fake Crowdstrike update tool**
3. User received email and is redirected to legitimate looking website
4. User downloads fake update tool (ransomware)
5. Download gets detected by Wazuh
6. Wazuh triggers SOARCA by sending a CACAO Playbook
7. SOARCA & CACAO playbook based remediation



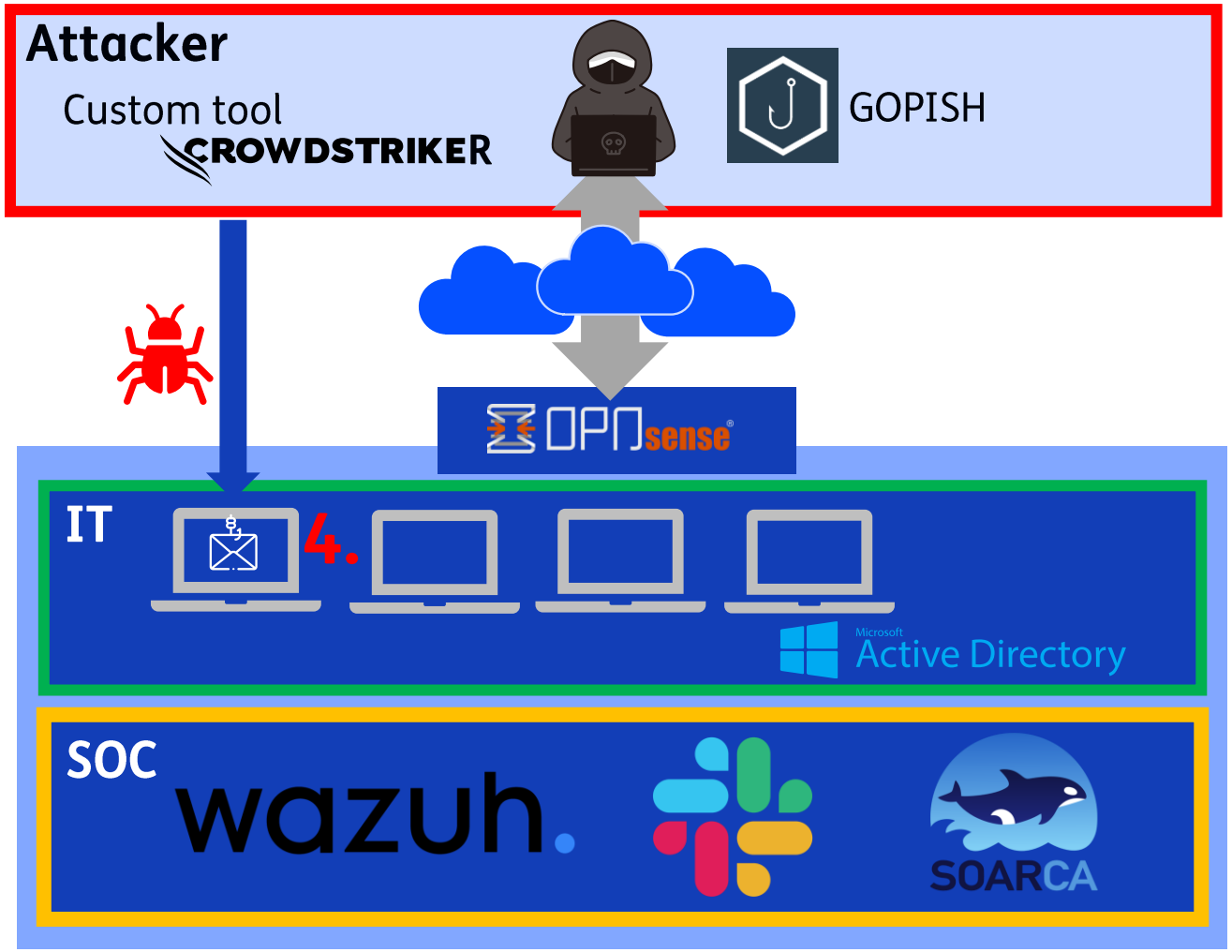
Phishing on VertexValue: a SOARCA demo scenario

1. Crowdstrike outage situation
2. Attacker launches phishing campaign with fake Crowdstrike update tool
3. **User received email and is redirected to legitimate looking website**
4. User downloads fake update tool (ransomware)
5. Download gets detected by Wazuh
6. Wazuh triggers SOARCA by sending a CACAO Playbook
7. SOARCA & CACAO playbook based remediation



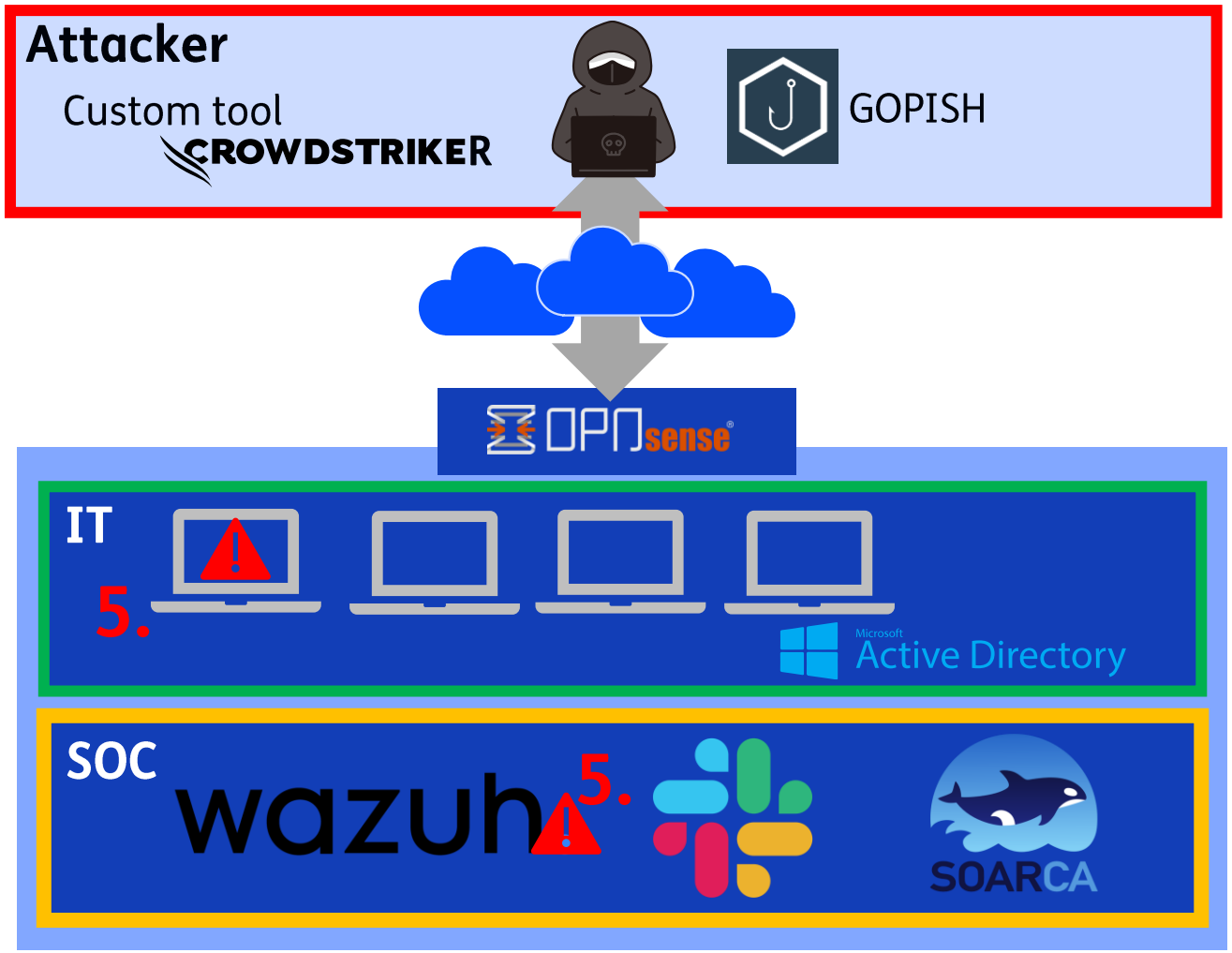
Phishing on VertexValue: a SOARCA demo scenario

1. Crowdstrike outage situation
2. Attacker launches phishing campaign with fake Crowdstrike update tool
3. User received email and is redirected to legitimate looking website
4. **User downloads fake update tool (ransomware)**
5. Download gets detected by Wazuh
6. Wazuh triggers SOARCA by sending a CACAO Playbook
7. SOARCA & CACAO playbook based remediation



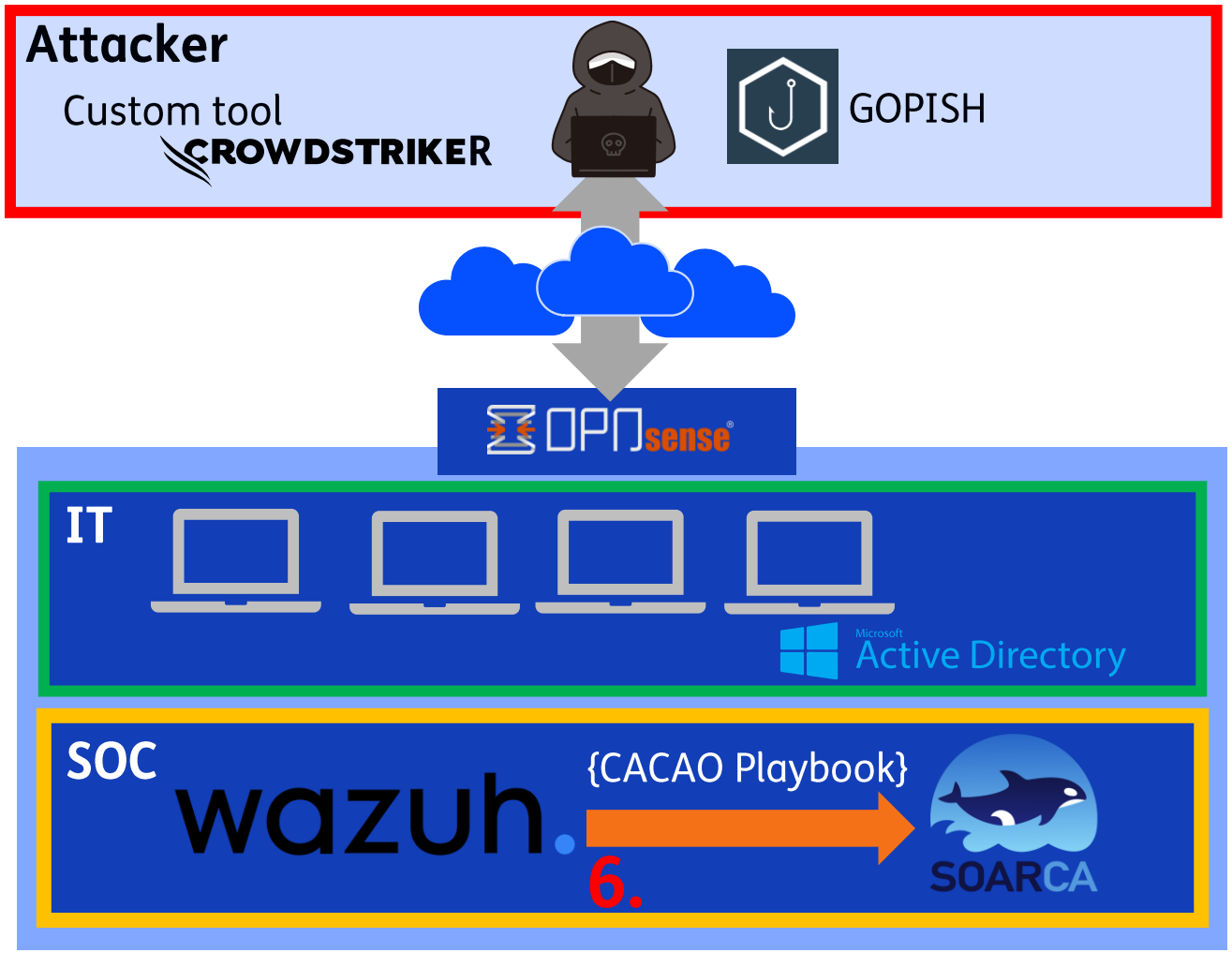
Phishing on VertexValue: a SOARCA demo scenario

1. Crowdstrike outage situation
2. Attacker launches phishing campaign with fake Crowdstrike update tool
3. User received email and is redirected to legitimate looking website
4. User downloads fake update tool (ransomware)
5. **Download gets detected by Wazuh**
6. Wazuh triggers SOARCA by sending a CACAO Playbook
7. SOARCA & CACAO playbook based remediation



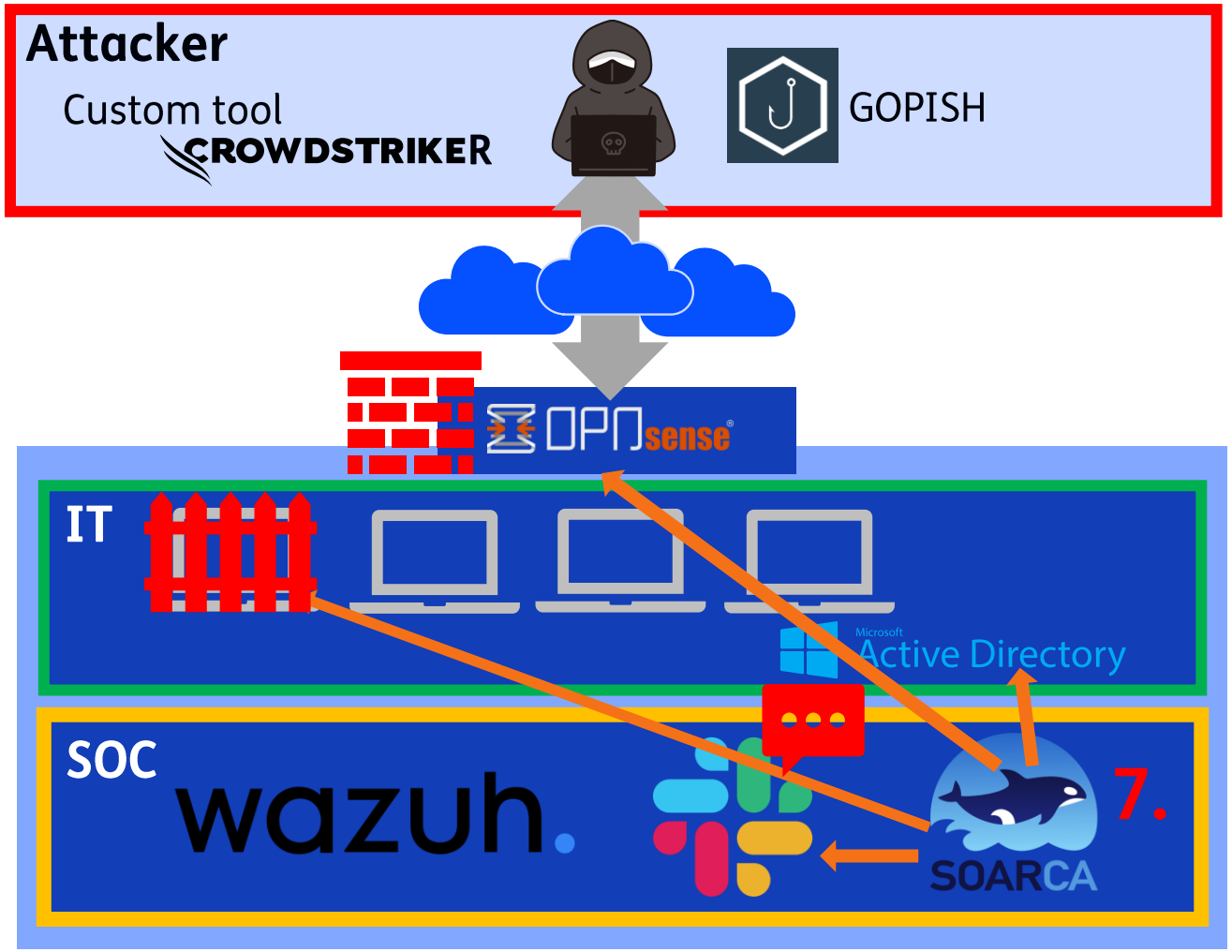
Phishing on VertexValue: a SOARCA demo scenario

1. Crowdstrike outage situation
2. Attacker launches phishing campaign with fake Crowdstrike update tool
3. User received email and is redirected to legitimate looking website
4. User downloads fake update tool (ransomware)
5. Download gets detected by Wazuh
6. **Wazuh triggers SOARCA by sending a CACAO Playbook**
7. SOARCA & CACAO playbook based remediation

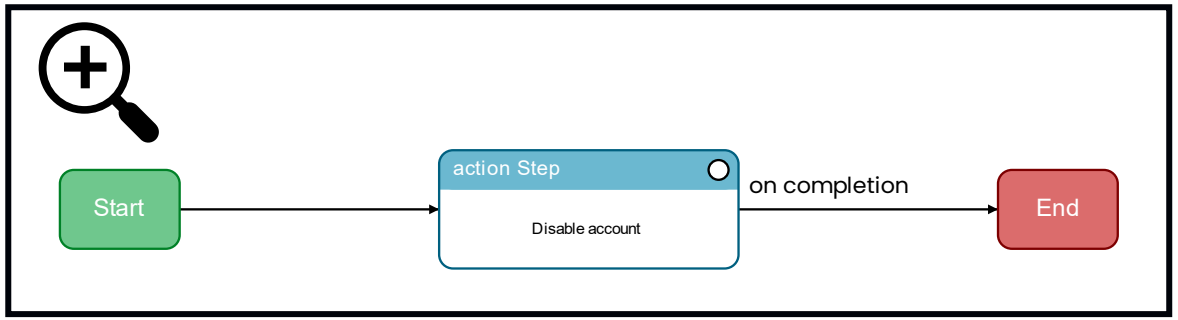


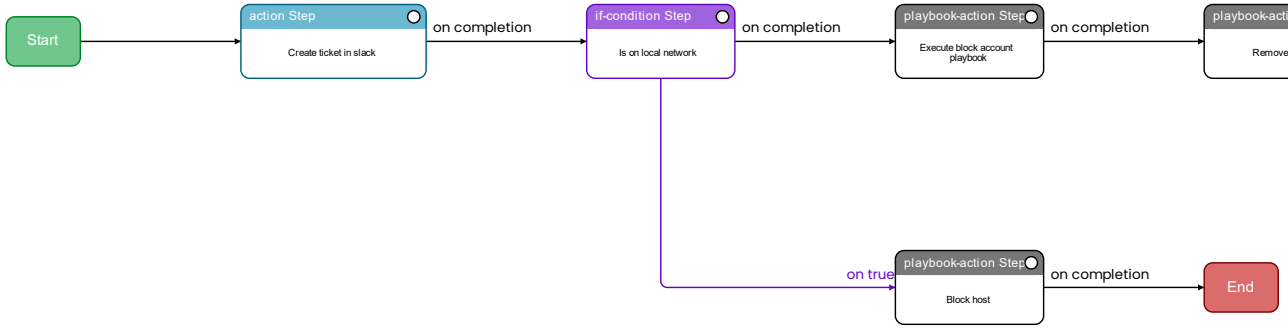
Phishing on VertexValue: a SOARCA demo scenario

1. Crowdstrike outage situation
2. Attacker launches phishing campaign with fake Crowdstrike update tool
3. User received email and is redirected to legitimate looking website
4. User downloads fake update tool (ransomware)
5. Download gets detected by Wazuh
6. Wazuh triggers SOARCA by sending a CACAO Playbook
7. **SOARCA & CACAO playbook based remediation**



Playbook-based remediation: Example CACAO Playbooks

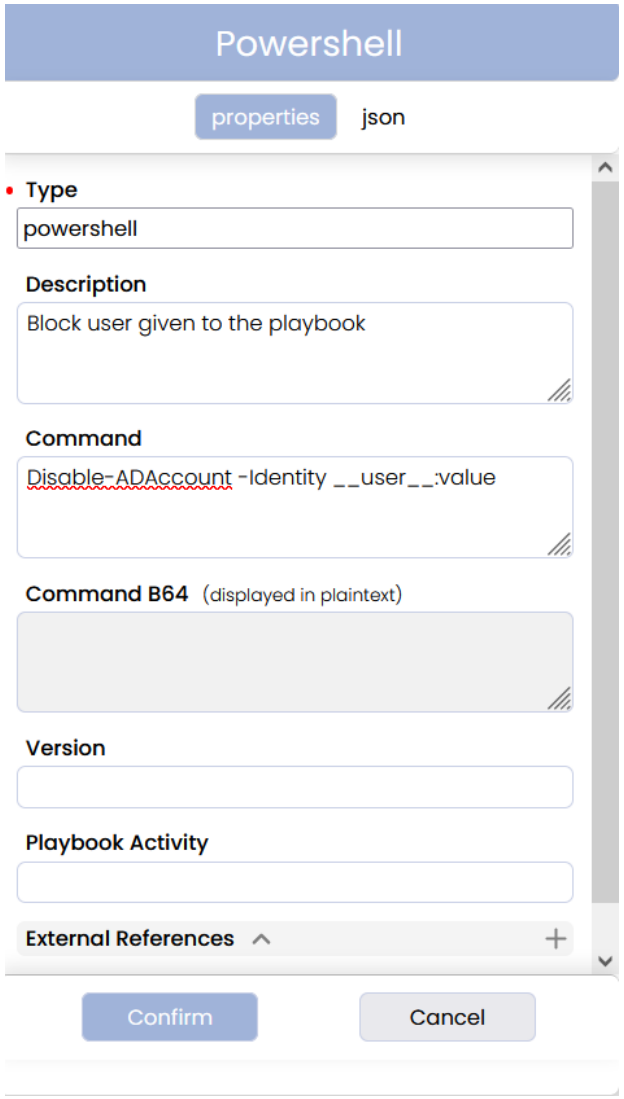


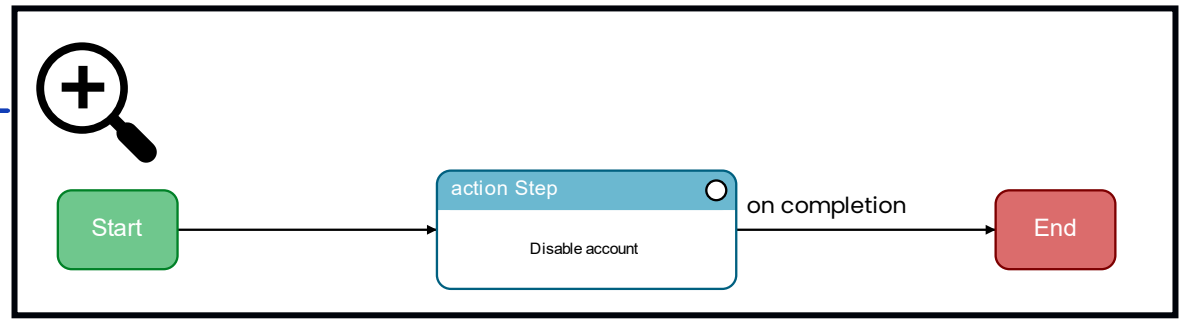


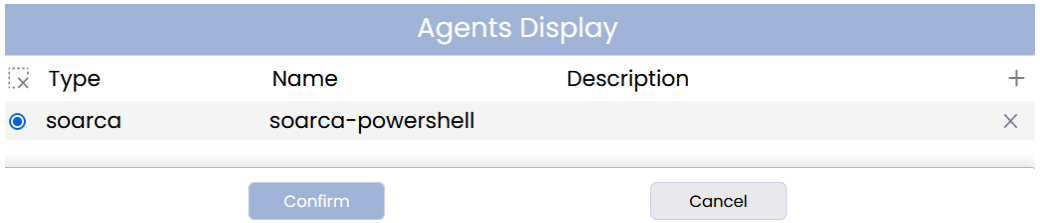
Built & visualised using CACAO Roaster

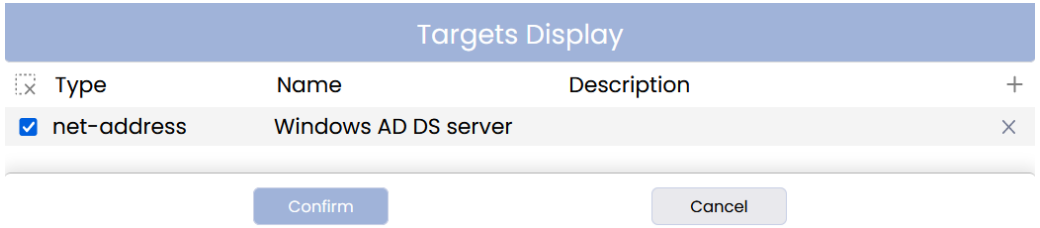
TNO innovation for life

Playbook-based remediation: Example CACAO Playbooks



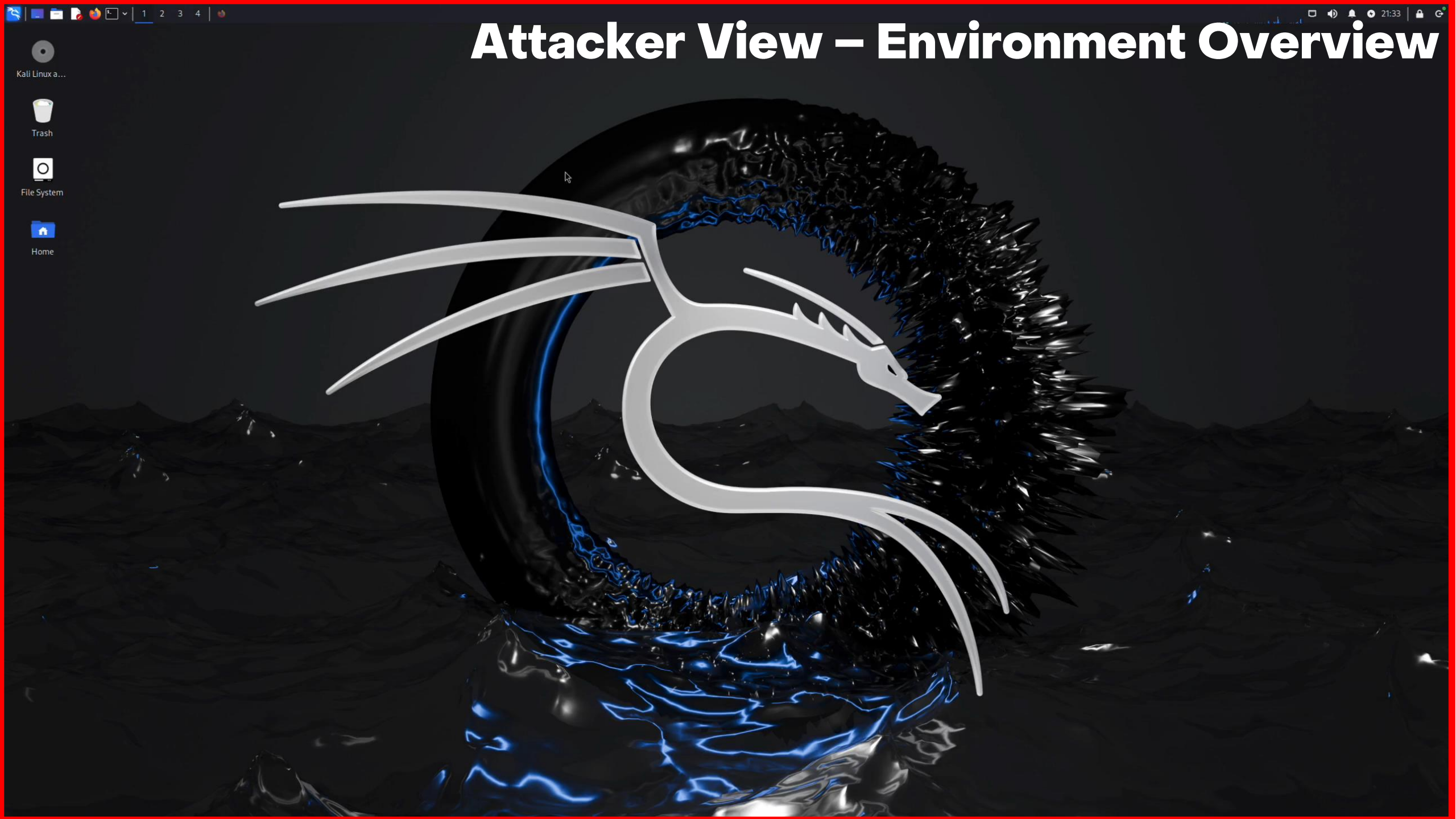




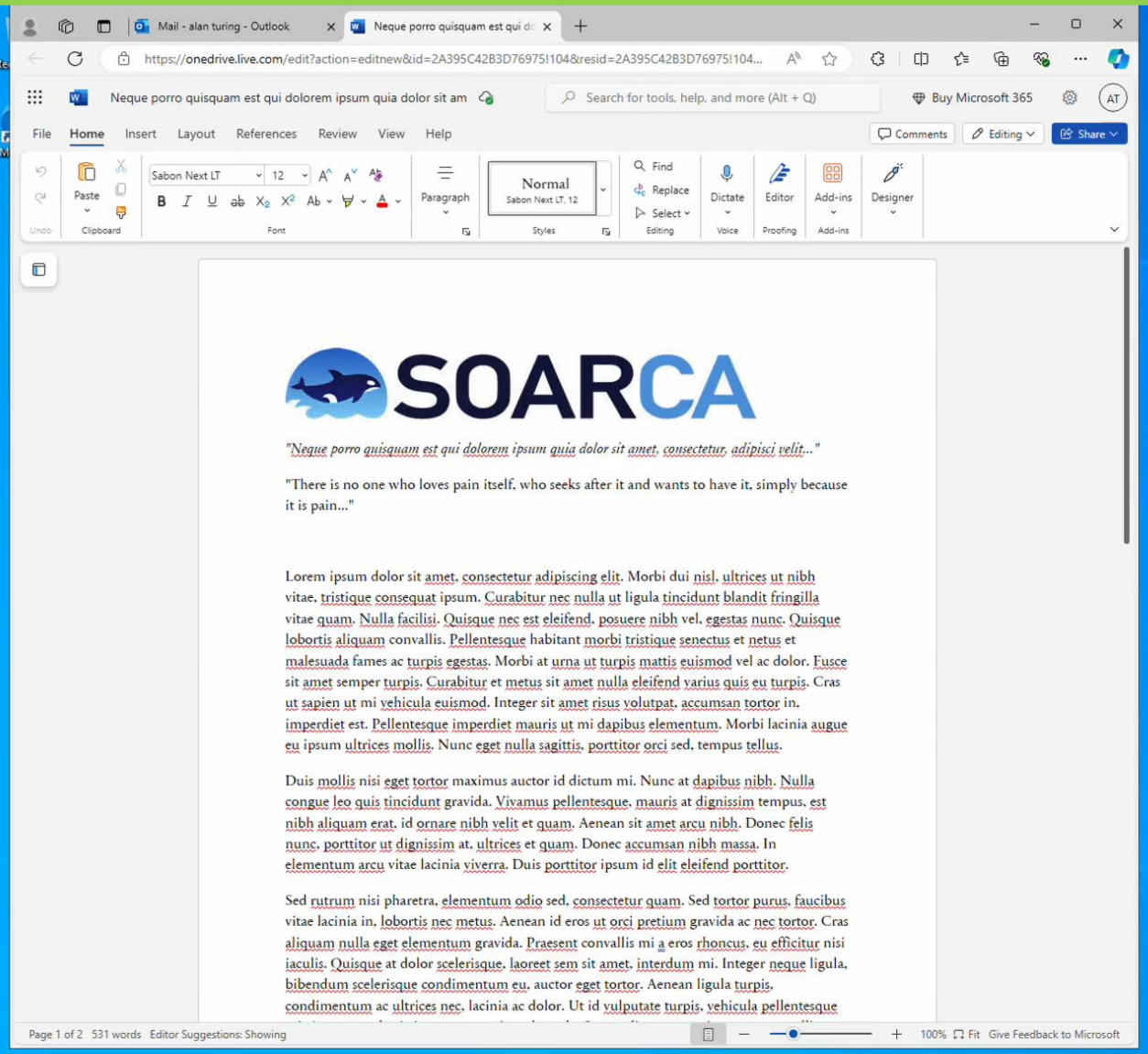


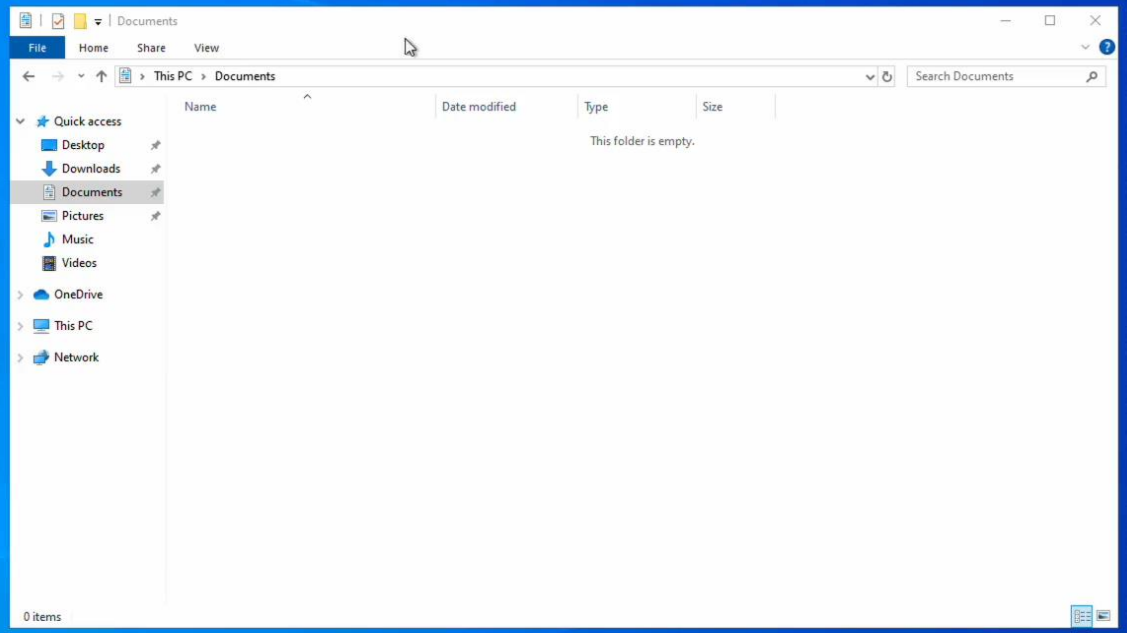
Built & visualised using CACAO Roaster

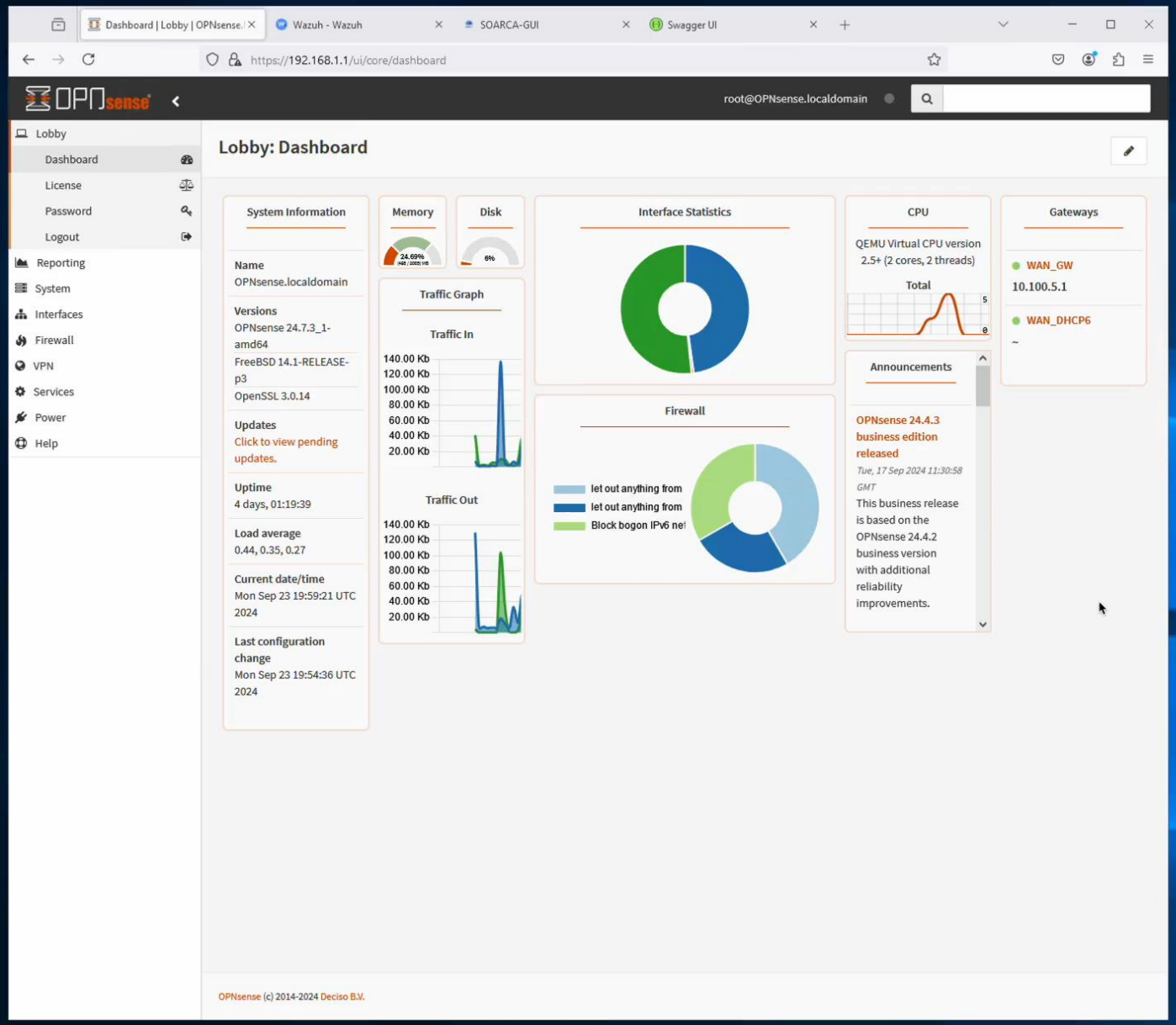
Attacker View – Environment Overview

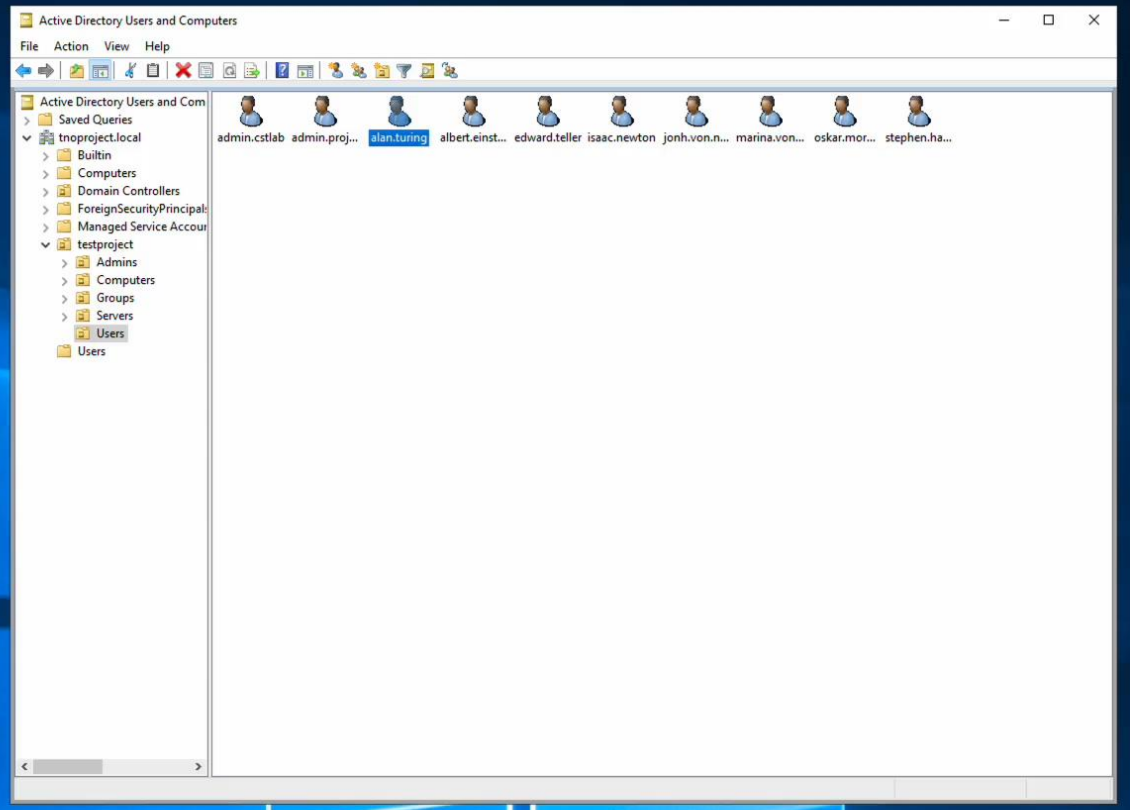


User View - Environment Overview

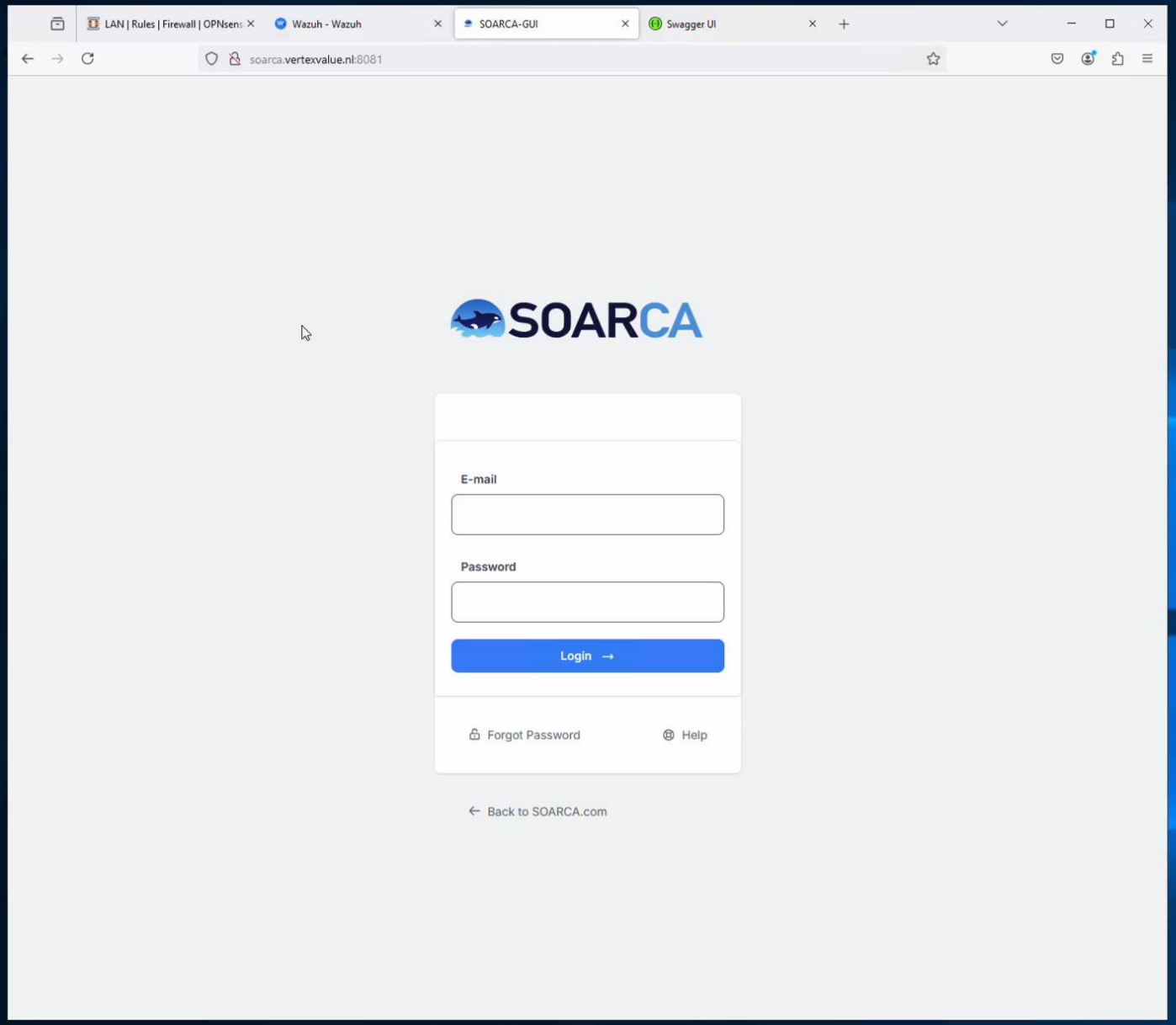


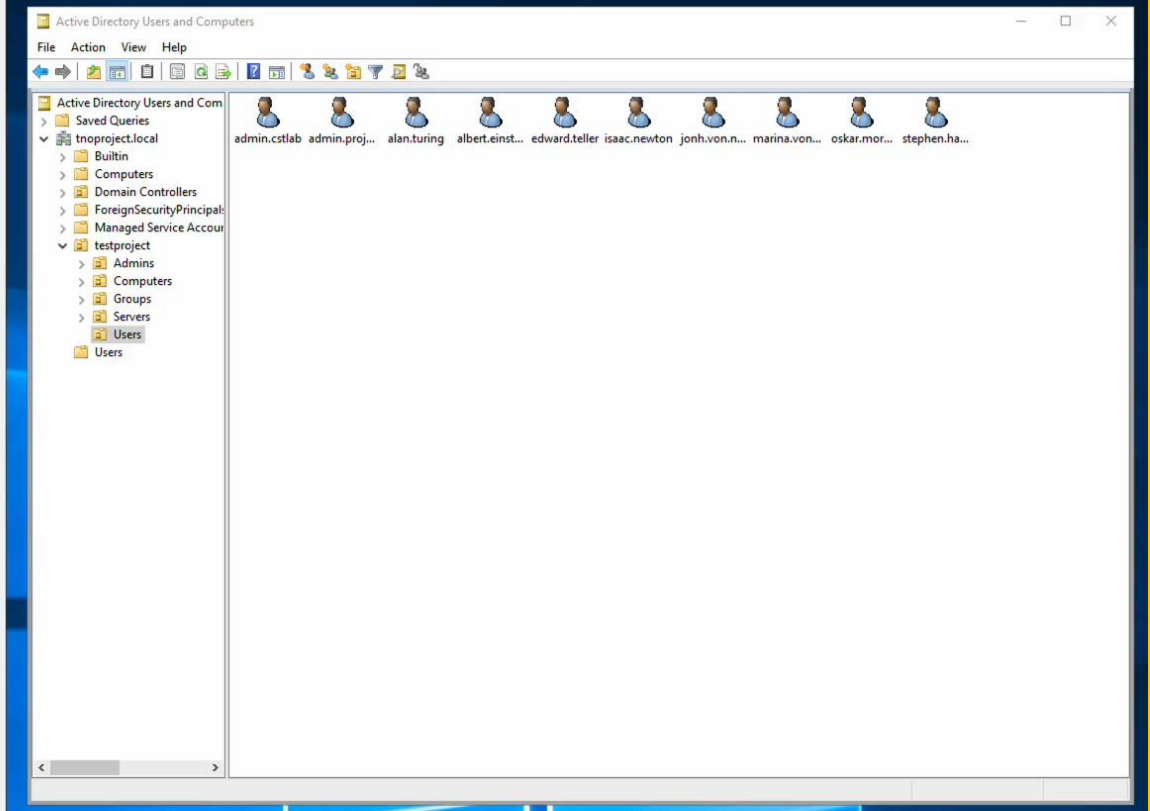




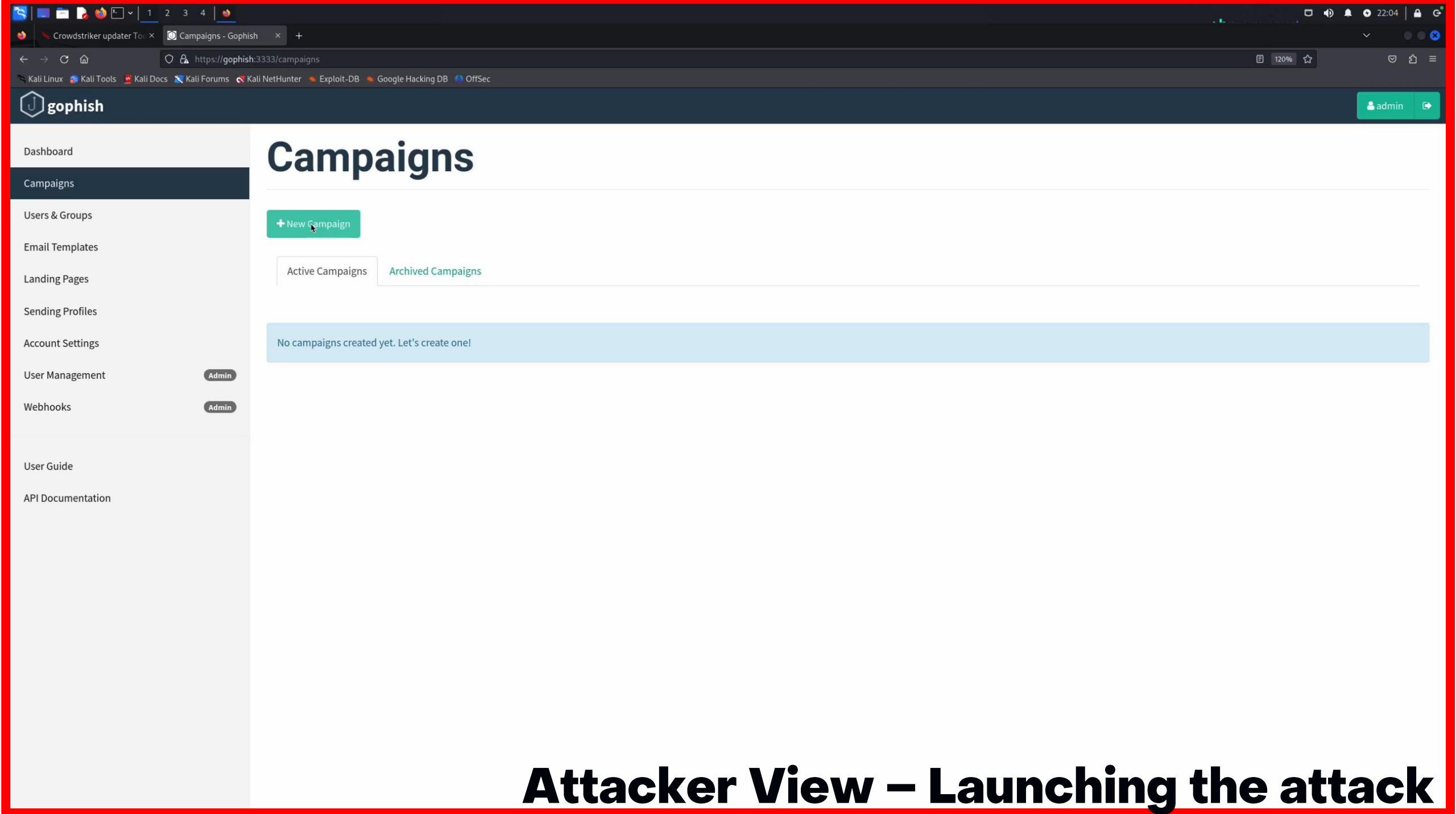


SOC View - Environment Overview

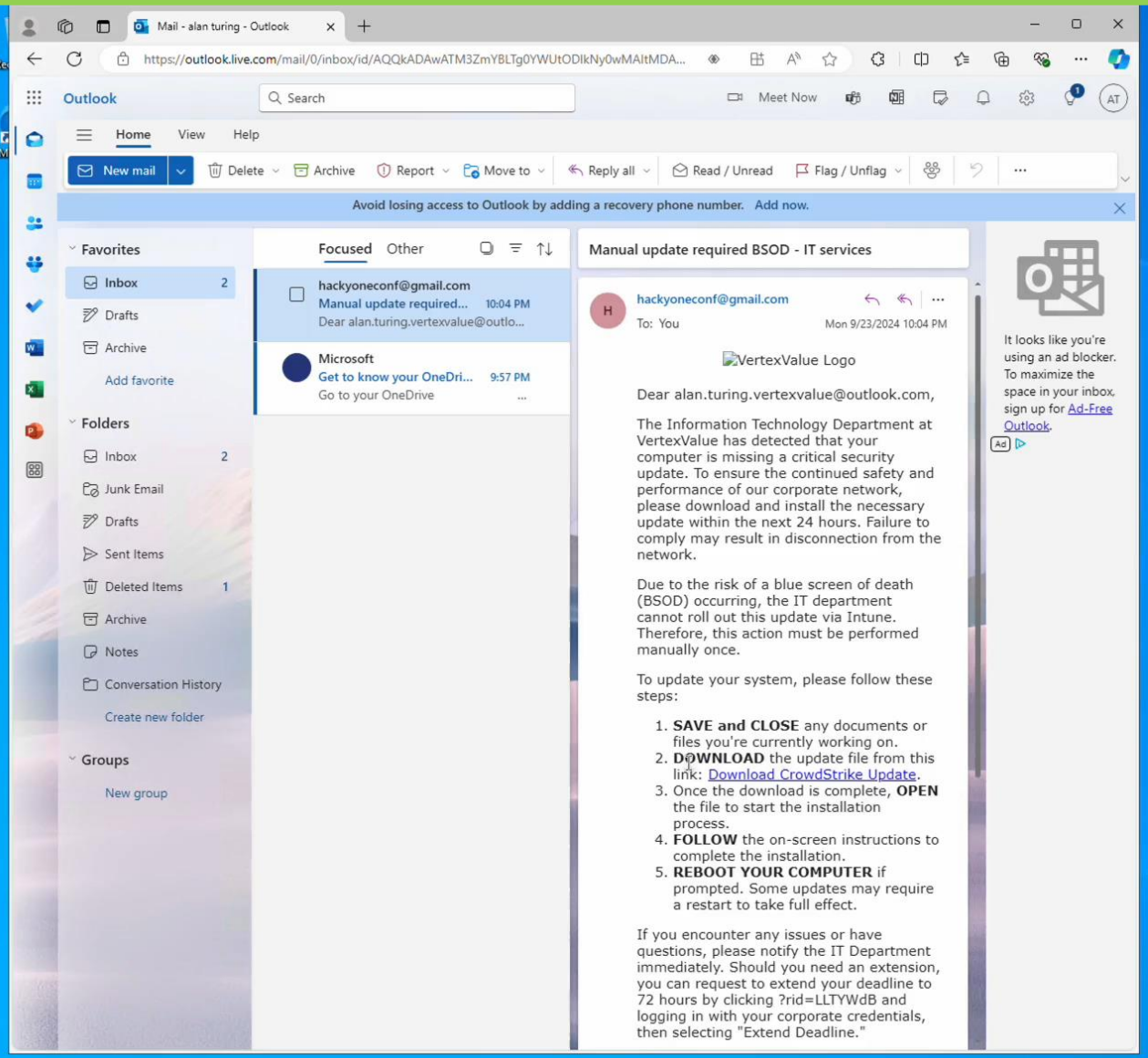


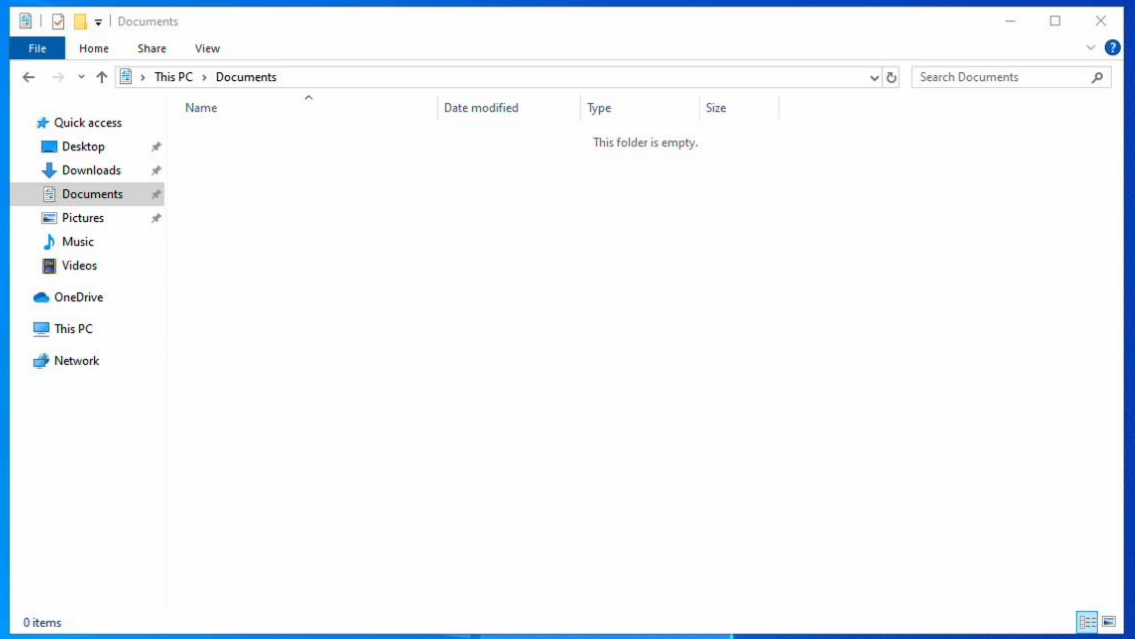


SOC View - Environment Overview

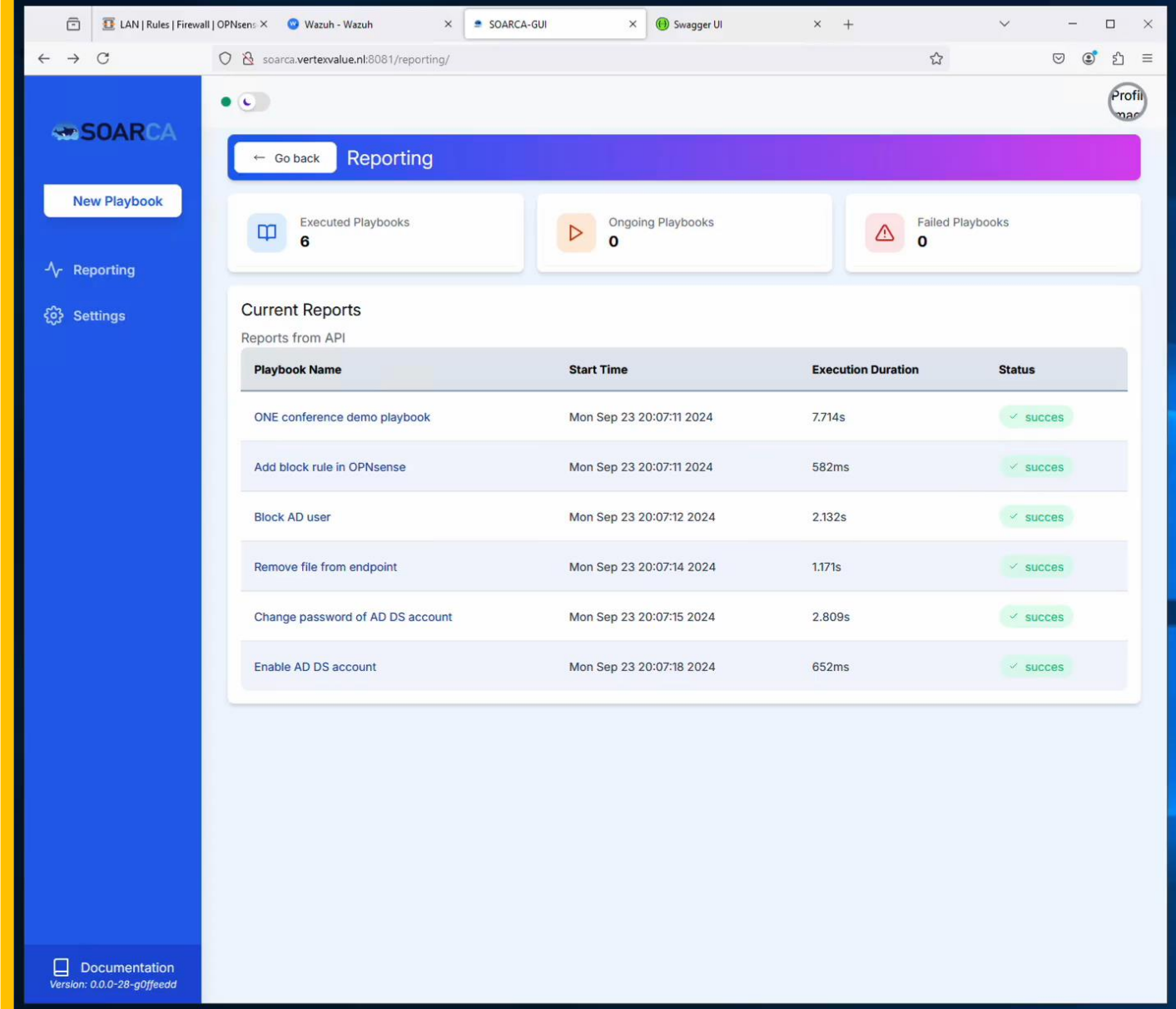


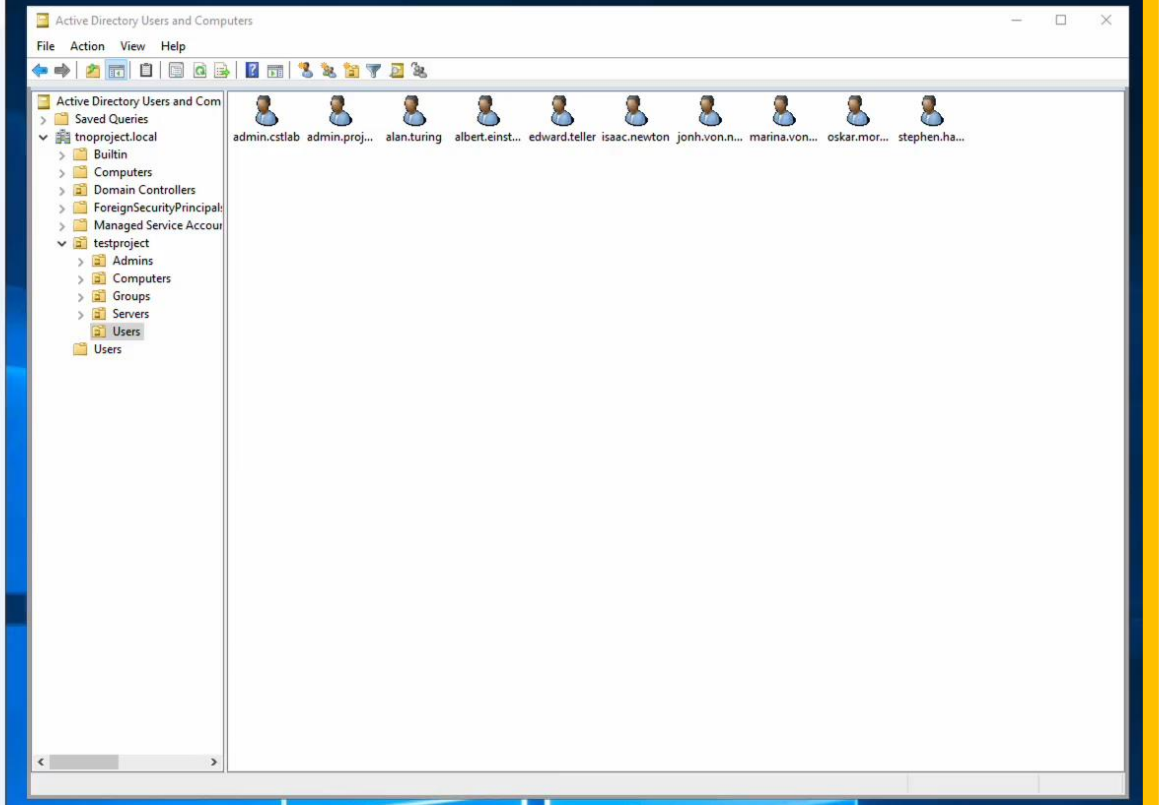
Attacker View – Launching the attack





User View – Under Attack





SOC View – Events & Remediation of the attack

SOC View – Slack tickets

Search SOARCA-DEMO-SLACK

SOARCA-DEMO-SLACK

Drafts & sent

Channels
- general
- random
- slack-integration
- wazuh-bot

Add channels

Direct messages
- Luca Morgese Zangrandi
- Maarten you

Add coworkers

Apps
- soarca-bot

Add apps

Home
DMs
Activity
Automa...
More

slack-integration

Messages | Add canvas | Files

Friday, September 20th

React | Reply

10:15

Maarten 11:01 AM

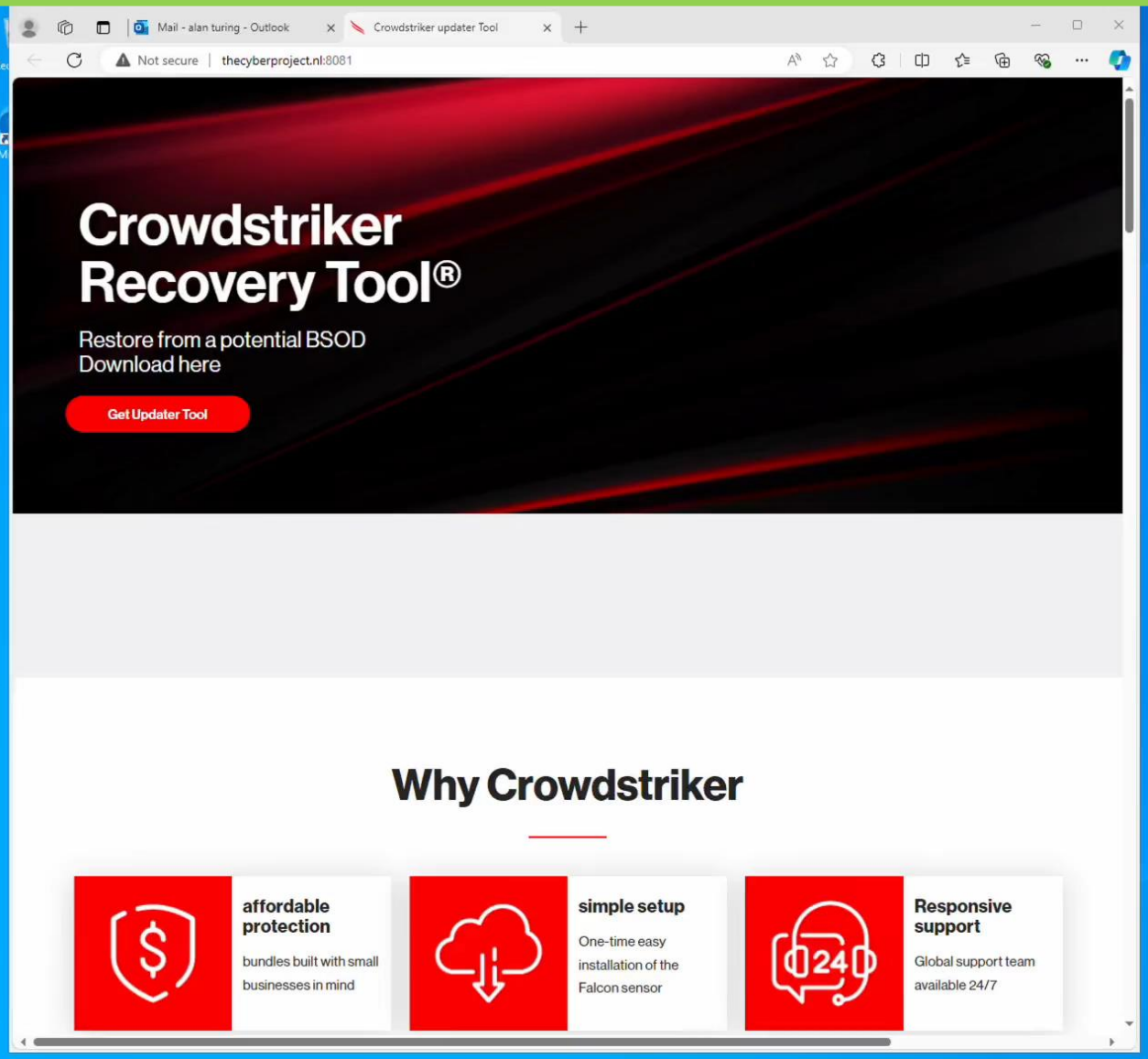
Maarten 1:20 PM

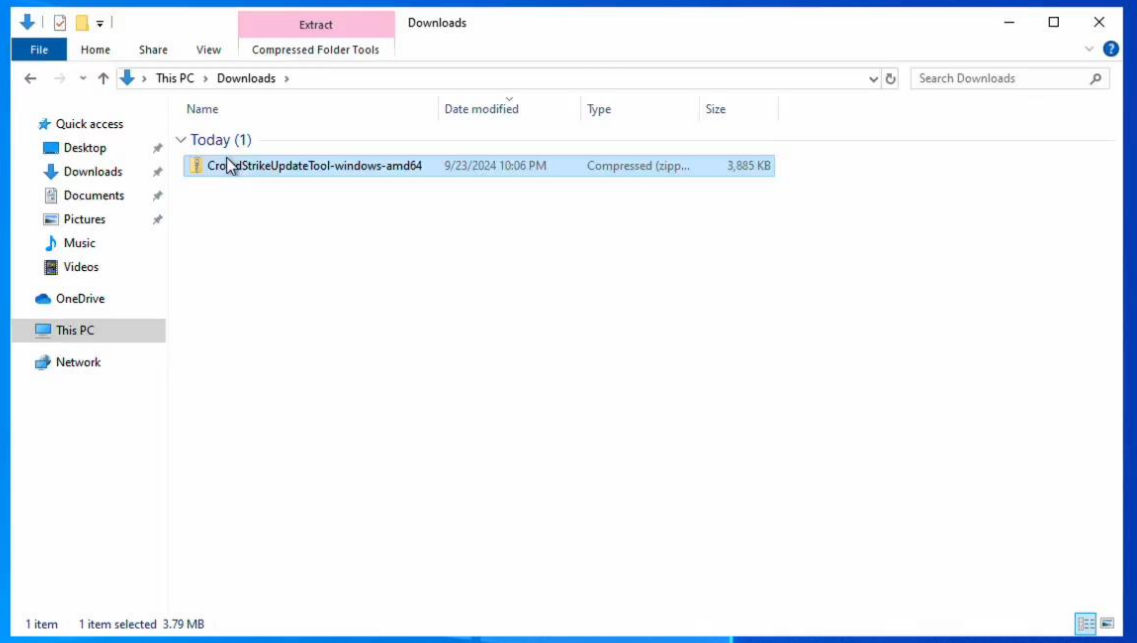
Today

soarca-bot APP 10:07 PM

User: alan.turing is affected by phishing and downloaded ransomware, automatic remediation is started for endpoint: WINTNO-E6PTITI3

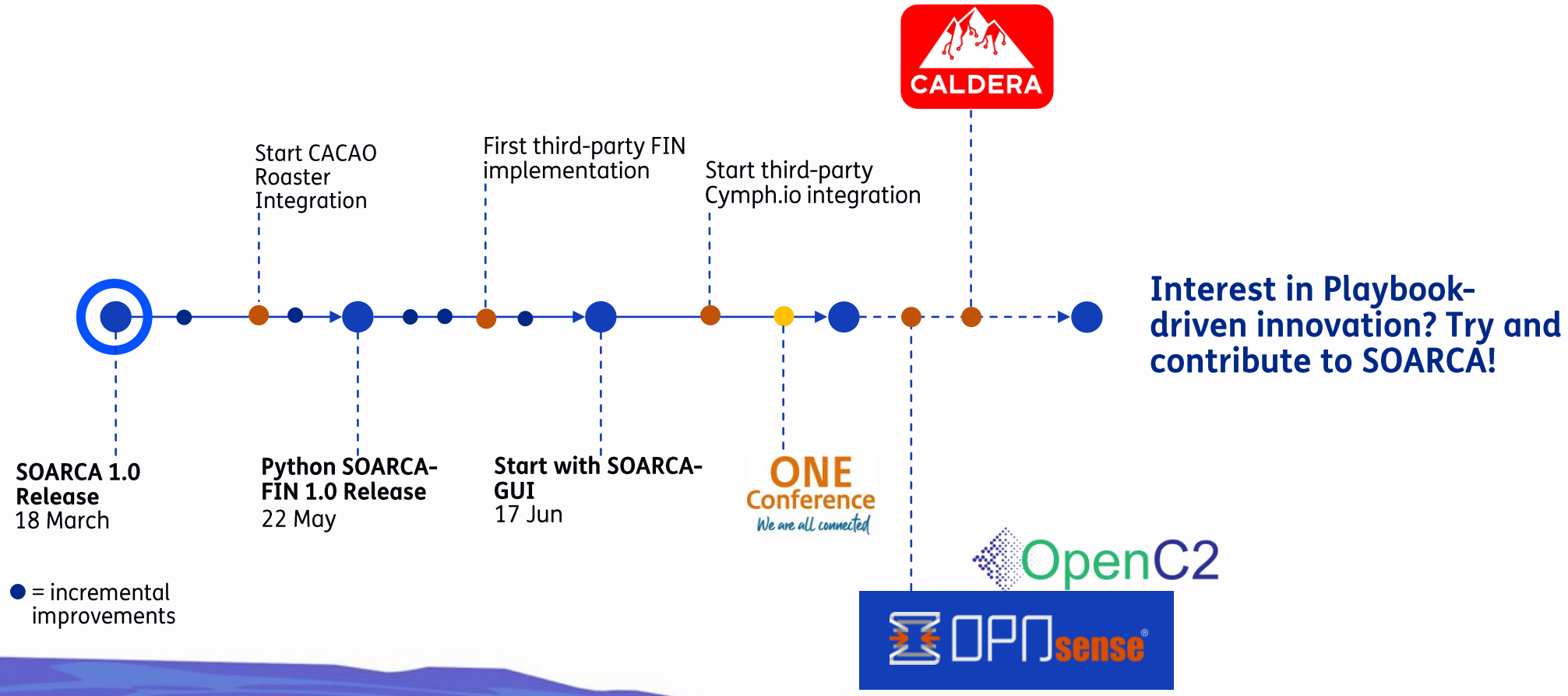
User: alan.turing password is reset, endpoint: WINTNO-E6PTITI3 is isolated and malware removed.





User View – No Mitigation

Roadmap: What is next for SOARCA?



All demo files and references can be found here:

https://github.com/thecyberproject/soarca-one-conference-2024

Ir. Jan-Paul Konijn

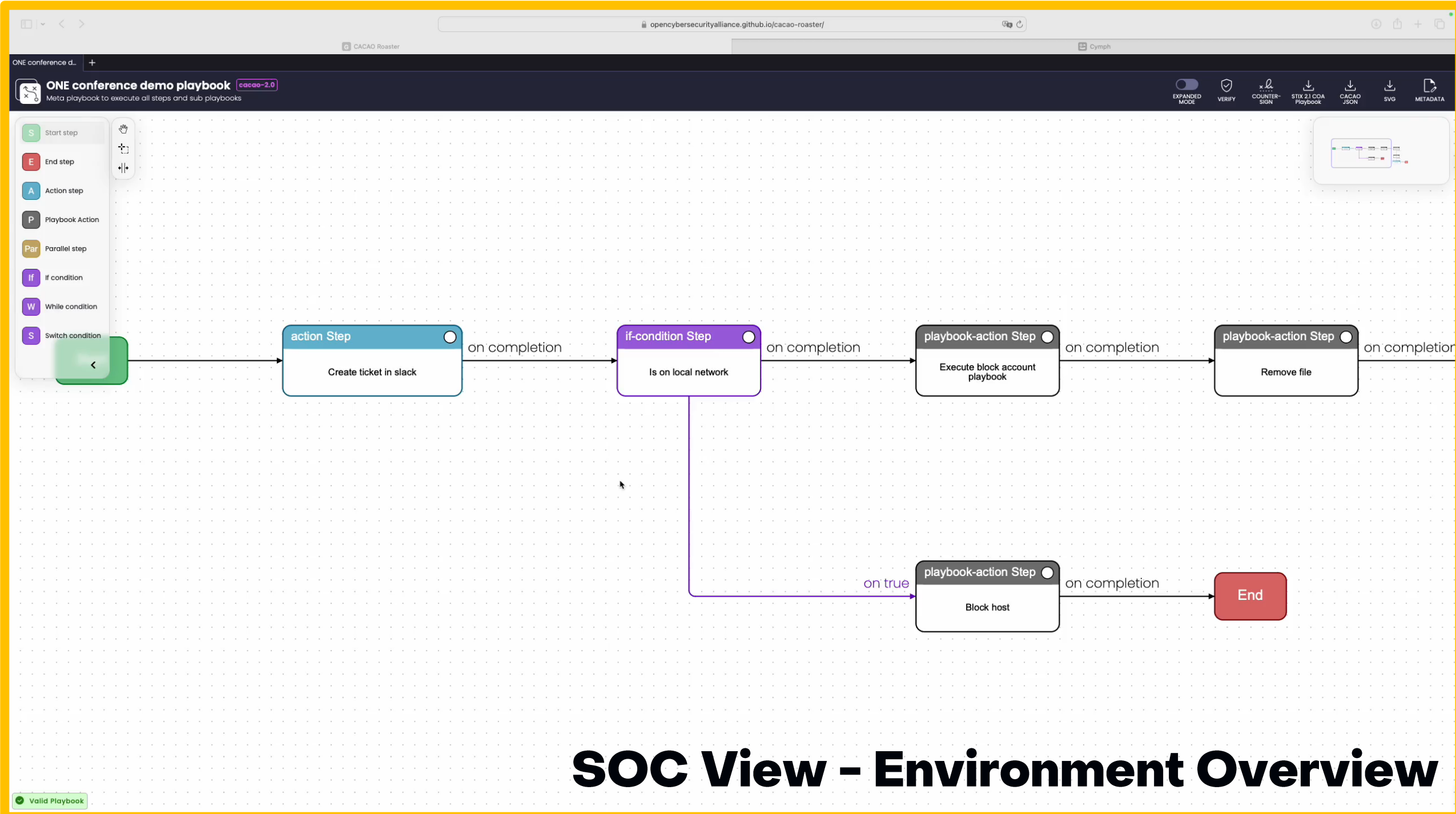
- Security Monitoring & detection research
- Automated Security research
- OT security research

Ing. Maarten de Kruijf

- Automated Security research
- OT security research
- Vulnerability research
- Security Monitoring & detection research

Team: Maarten de Kruijf, Jan-Paul Konijn, Luca Morgese, Shari Finner, Richard Kerkdijk, Hidde-Jan Jongsma, Ivo Kroskinski, and Frank Fransen

TNO innovation for life



SOC View - Environment Overview