

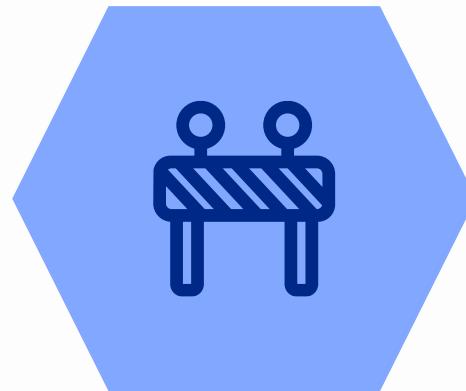


SOARCA

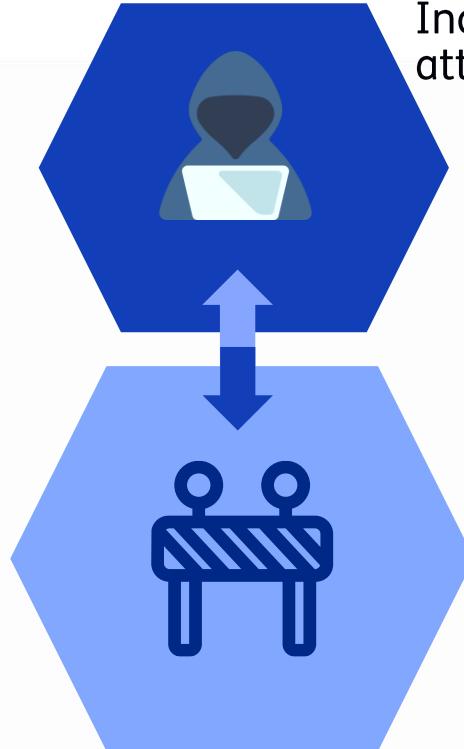
open-source SOAR for CACAO
playbook automation

Jan-Paul Konijn, Maarten de Kruijf | ONE Conference

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

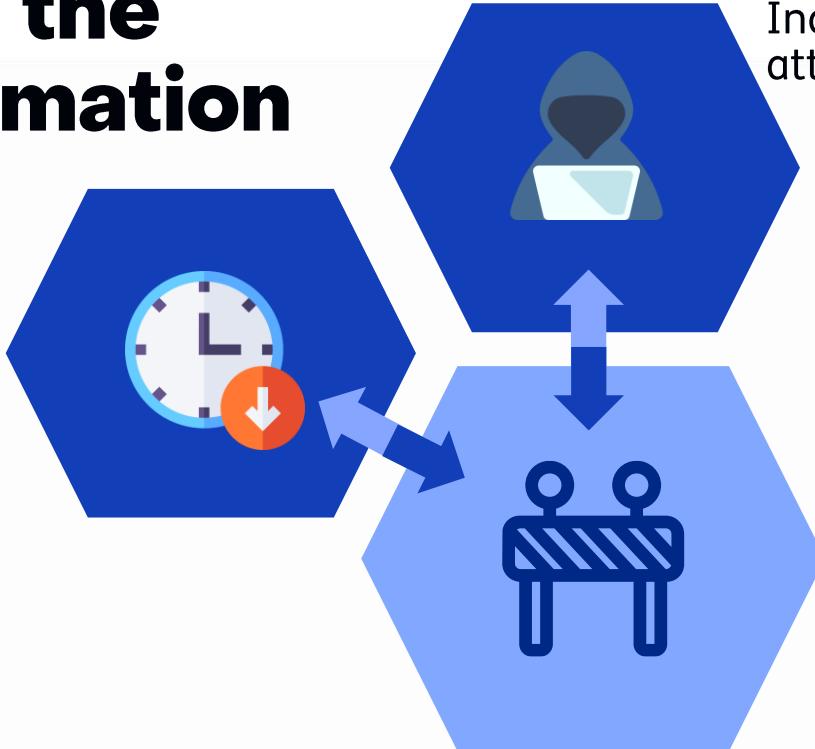
Listen with [Speechify](#)
0:00 ● 3:10

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)

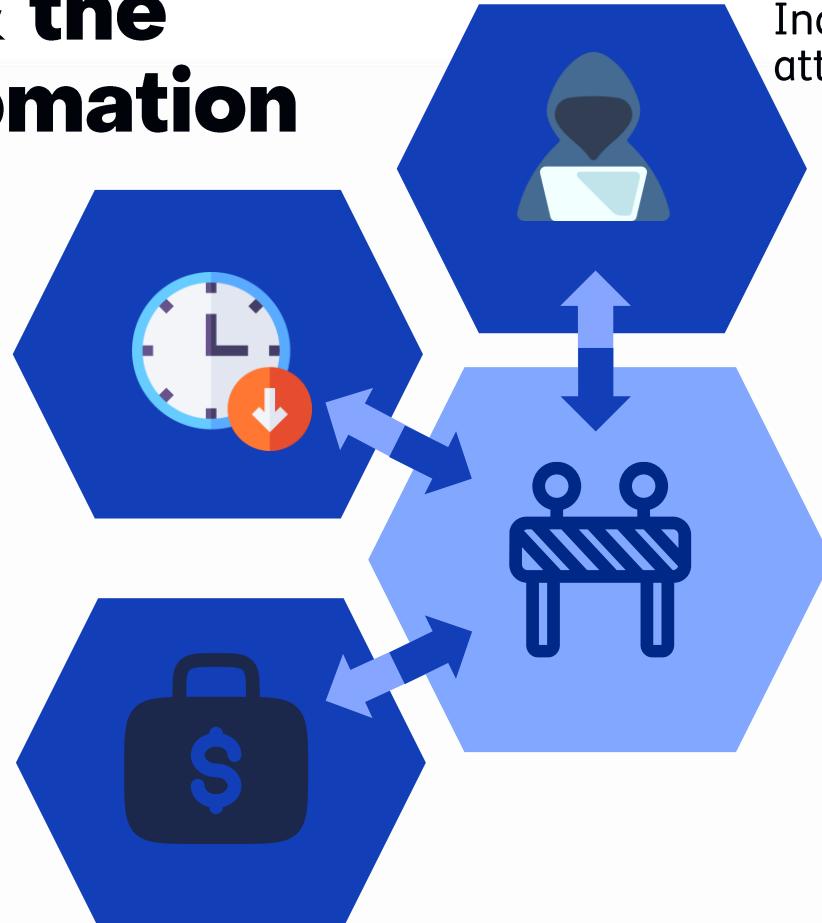
In the ever-evolving landscape of cybersecurity, security operations centers (SOCs) play a vital role in detecting and responding to unfolding attacks, proactively hunting for threats, and reinforcing the enterprise's overall security posture.

Challenges & the need for automation

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

Increasing in number of attacks and complexity



Challenges & the need for automation

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



Increasing in number of attacks and complexity

The screenshot shows a blog post from Sangfor Technologies. The title is "Defining AI Hacking: The Rise of AI Cyber Attacks". The post discusses the rise of AI-based cyber-attacks, mentioning how AI is used for cybercrime and the creation of AI-based threats. It also covers topics like Deepfake AI Hacking, Generating Malware AI Hacking, AI Social Engineering, AI Brute Force Attacks, and AI Hack Phishing. The sidebar includes social sharing buttons and a table of contents.

Challenges & the need for automation

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

Increasing in number of attacks and complexity

Attacks are being automated



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

Challenges & the need for automation

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

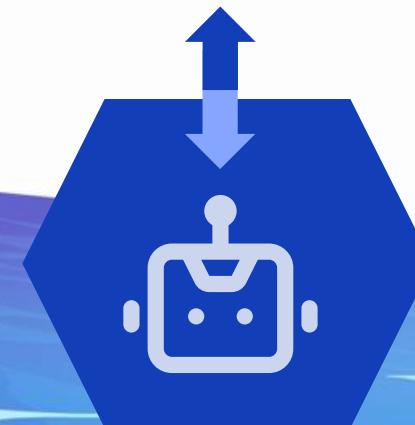
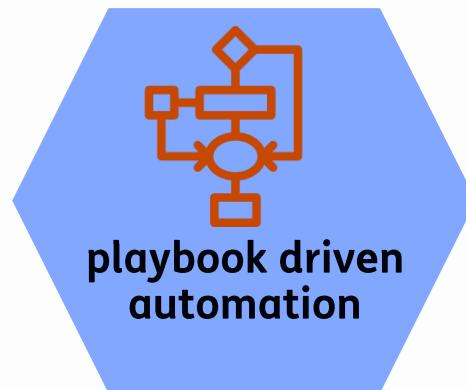
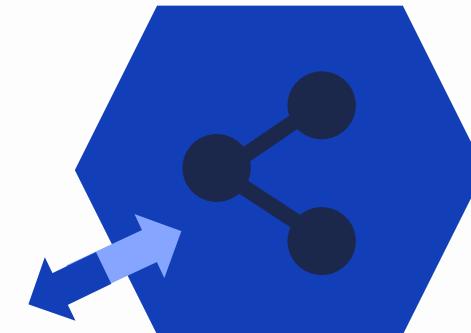
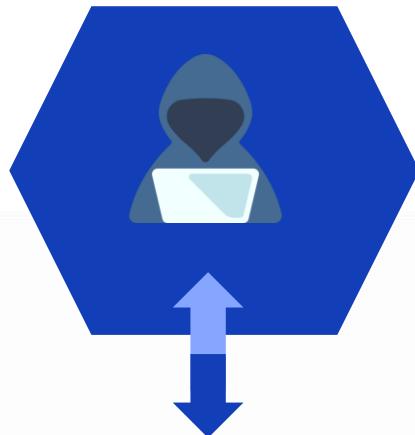
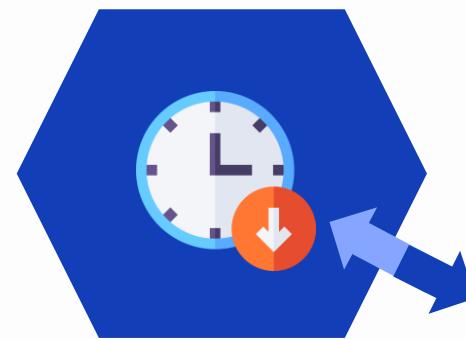
Increasing in number of attacks and complexity

Automation playbooks are often proprietary and are hard to share

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

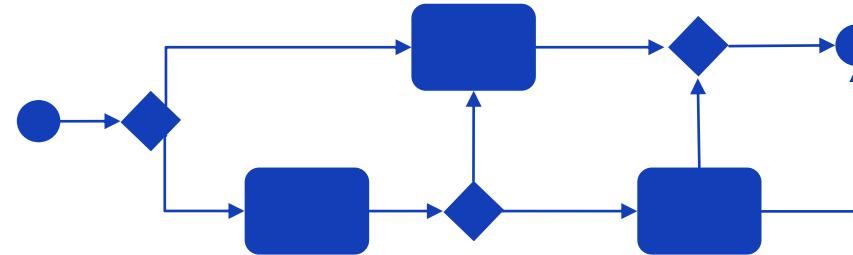
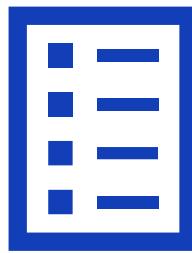
Attacks are being automated

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

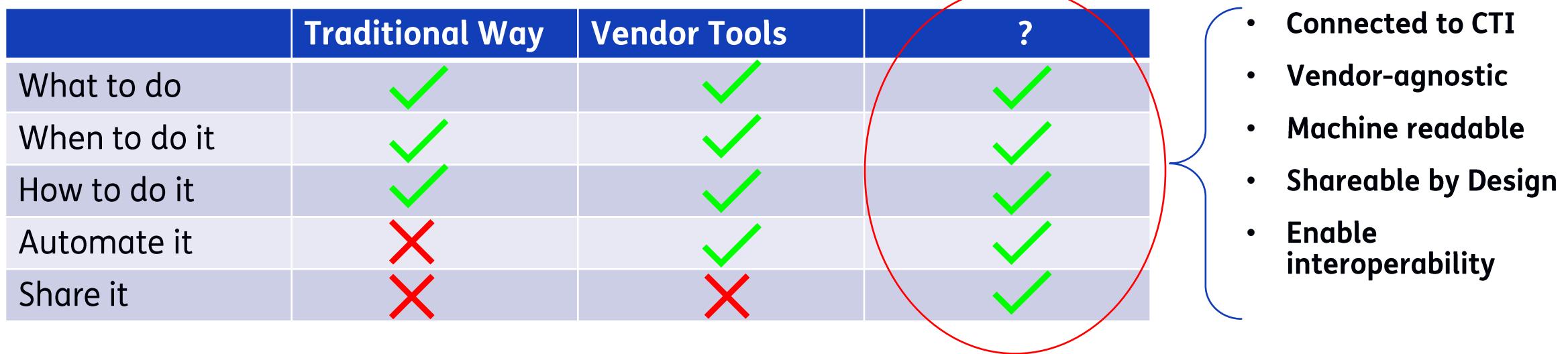
	Traditional Way	Vendor Tools	?
What to do	✓	✓	✓
When to do it	✓	✓	✓
How to do it	✓	✓	✓
Automate it	✗	✓	✓
Share it	✗	✗	✓

✓ = 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

The screenshot shows the front page of the CACAO Security Playbooks Version 2.0 Committee Specification 01. The page features the OASIS OPEN logo at the top left. Below it, the title "CACAO Security Playbooks Version 2.0" is displayed in bold blue text. Underneath the title, the text "Committee Specification 01" and the date "27 November 2023" are shown. The page contains several sections with links to different versions of the specification, such as "This version", "Previous version", and "Latest version". It also lists the "Technical Committee", "Chairs", "Editors", and "Related Work". At the bottom, there is copyright information and a page number.

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.doc>(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.doc>(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:

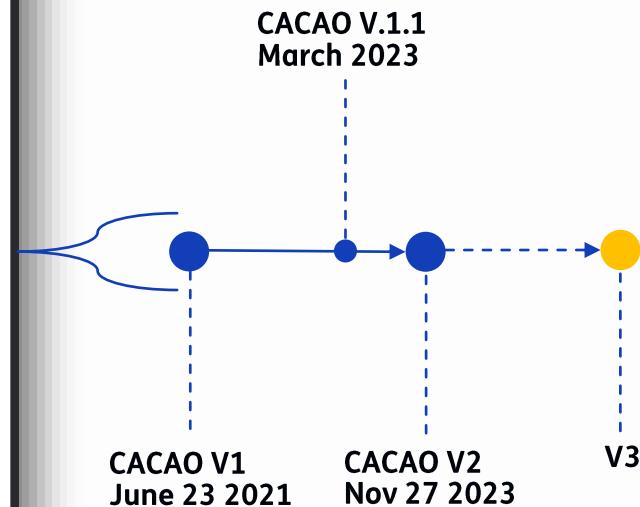
security-playbooks-v2.0-cs01
Standards Track Work Product

Copyright © OASIS Open 2023. All Rights Reserved.

27 November 2023
Page 1 of 135

An Open and Common Schema for Security Playbooks

The screenshot shows the front page of the CACAO Security Playbooks Version 2.0 Committee Specification 01. It features the OASIS OPEN logo at the top left. Below it, the title "CACAO Security Playbooks Version 2.0" is displayed in bold blue text. Underneath the title, the subtitle "Committee Specification 01" and the date "27 November 2023" are shown. The page contains several sections of text with hyperlinks to various documents. At the bottom, there is a copyright notice: "security-playbooks-v2.0-cs01 Standards Track Work Product Copyright © OASIS Open 2023. All Rights Reserved. 27 November 2023 Page 1 of 135".



Why CACAO as open standard for automating Security Operations?



OASIS OPEN
interoperable

connected to
CTI

machine-
readable

shareable and
reusable

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?



OASIS OPEN
interoperable

connected to
CTI

Playbook
pluggable in STIX
COA object



machine-
readable

shareable and
reusable

CACAO Playbook

Metadata

Workflow

Steps (control logic)

Commands

Agents via reference

Targets via reference

Other CACAO Playbooks via reference

Authentication Information

Agents

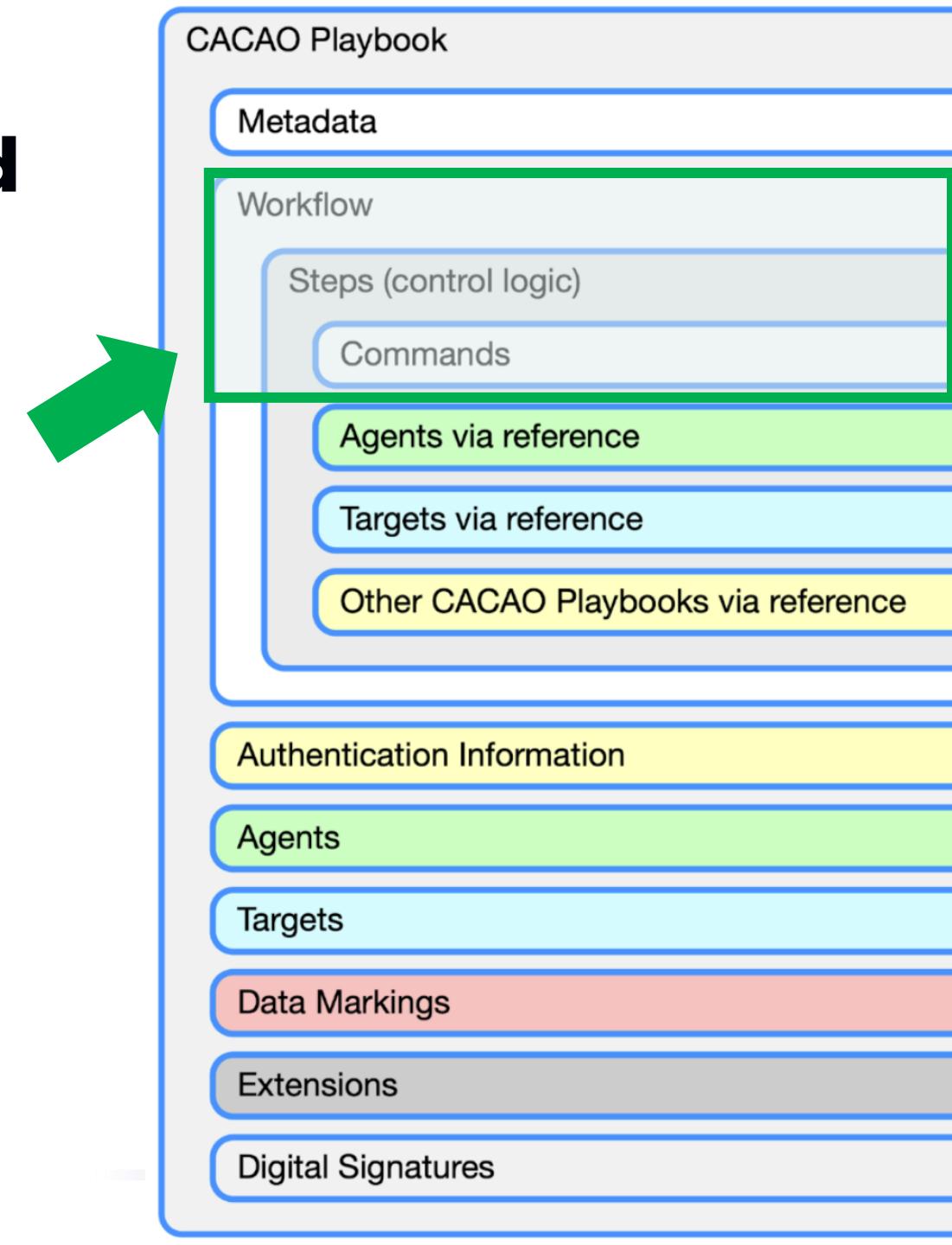
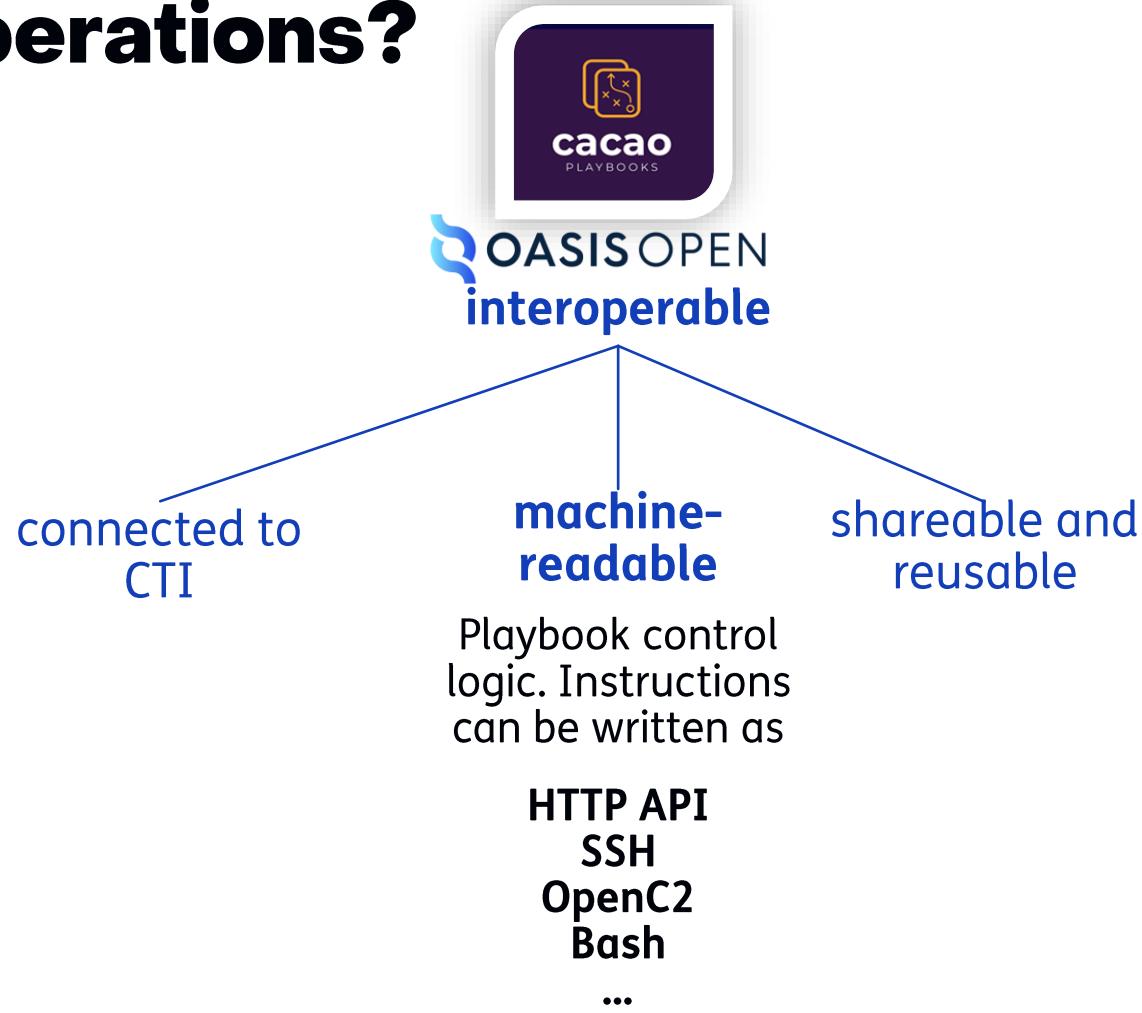
Targets

Data Markings

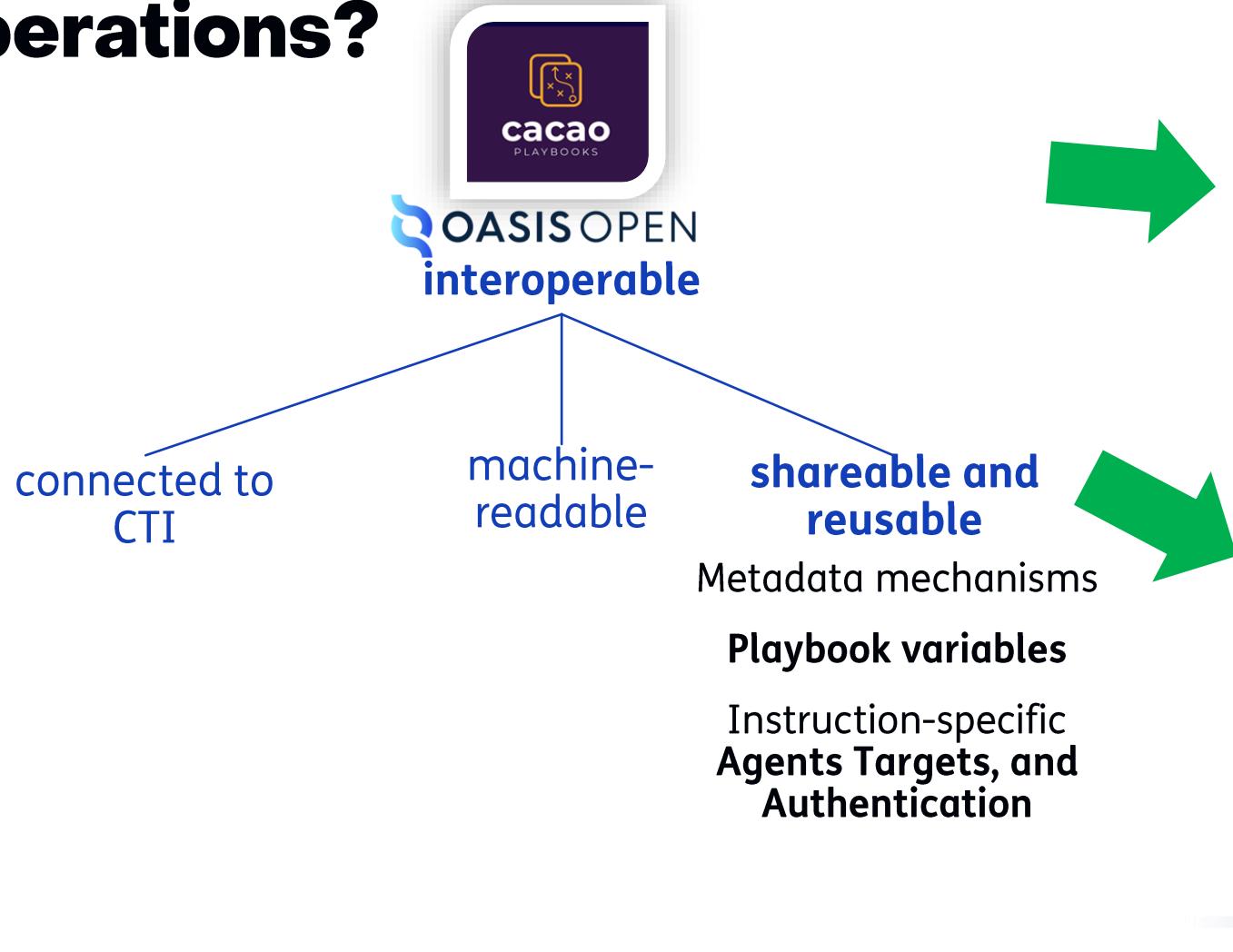
Extensions

Digital Signatures

Why CACAO as open standard for automating Security Operations?



Why CACAO as open standard for automating Security Operations?



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

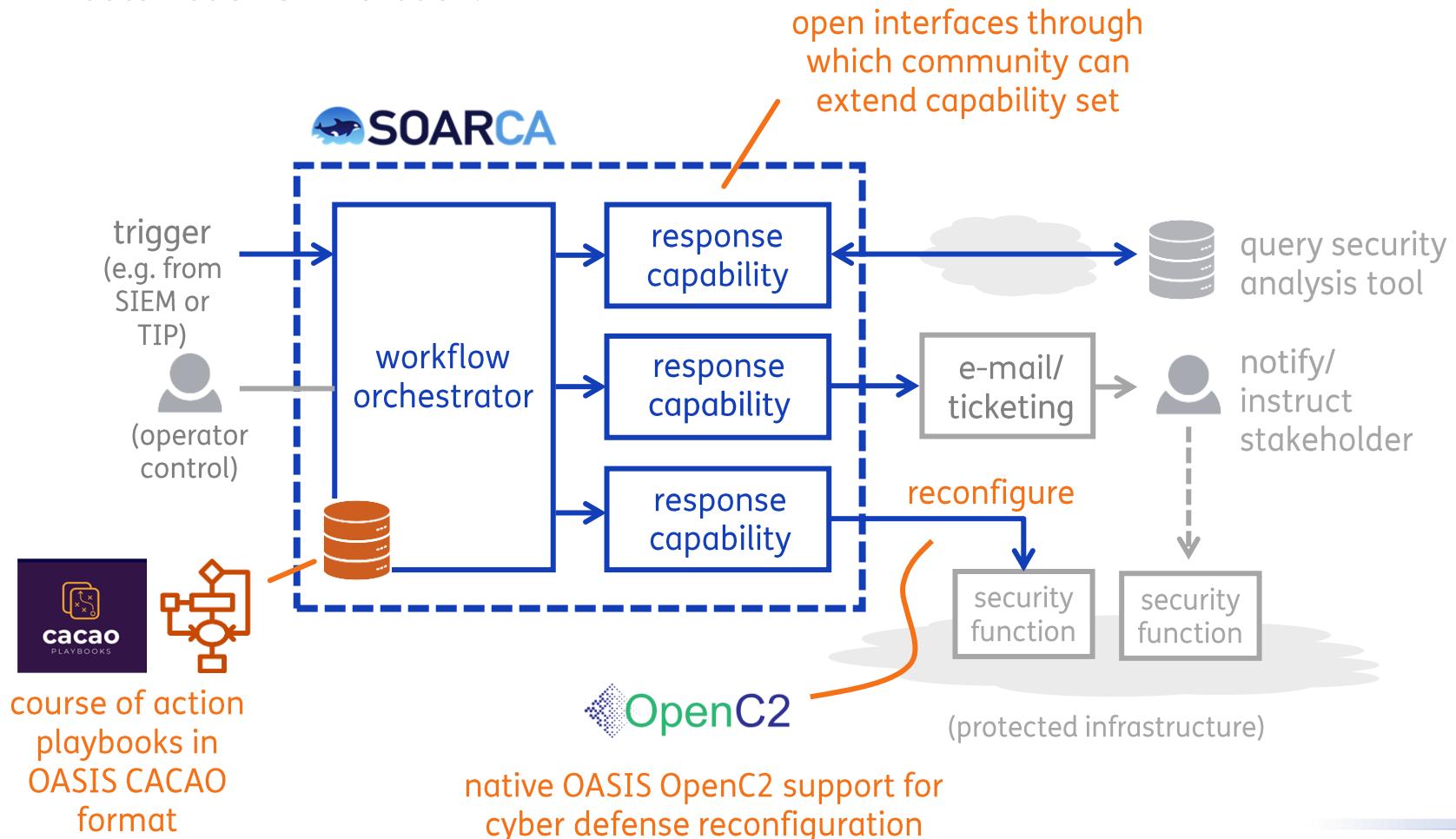
A Growing Ecosystem



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.



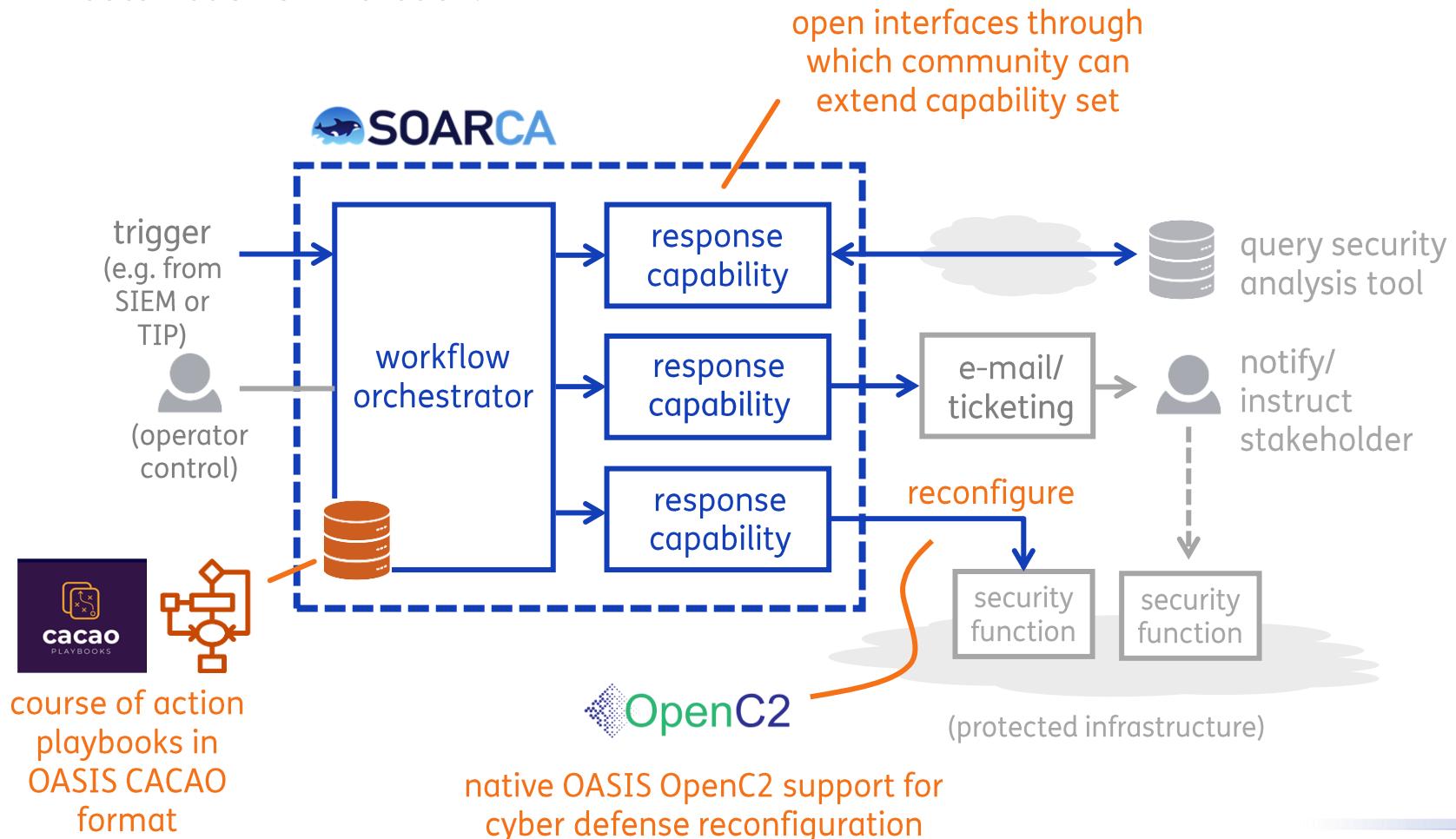
No tool that:

- 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.



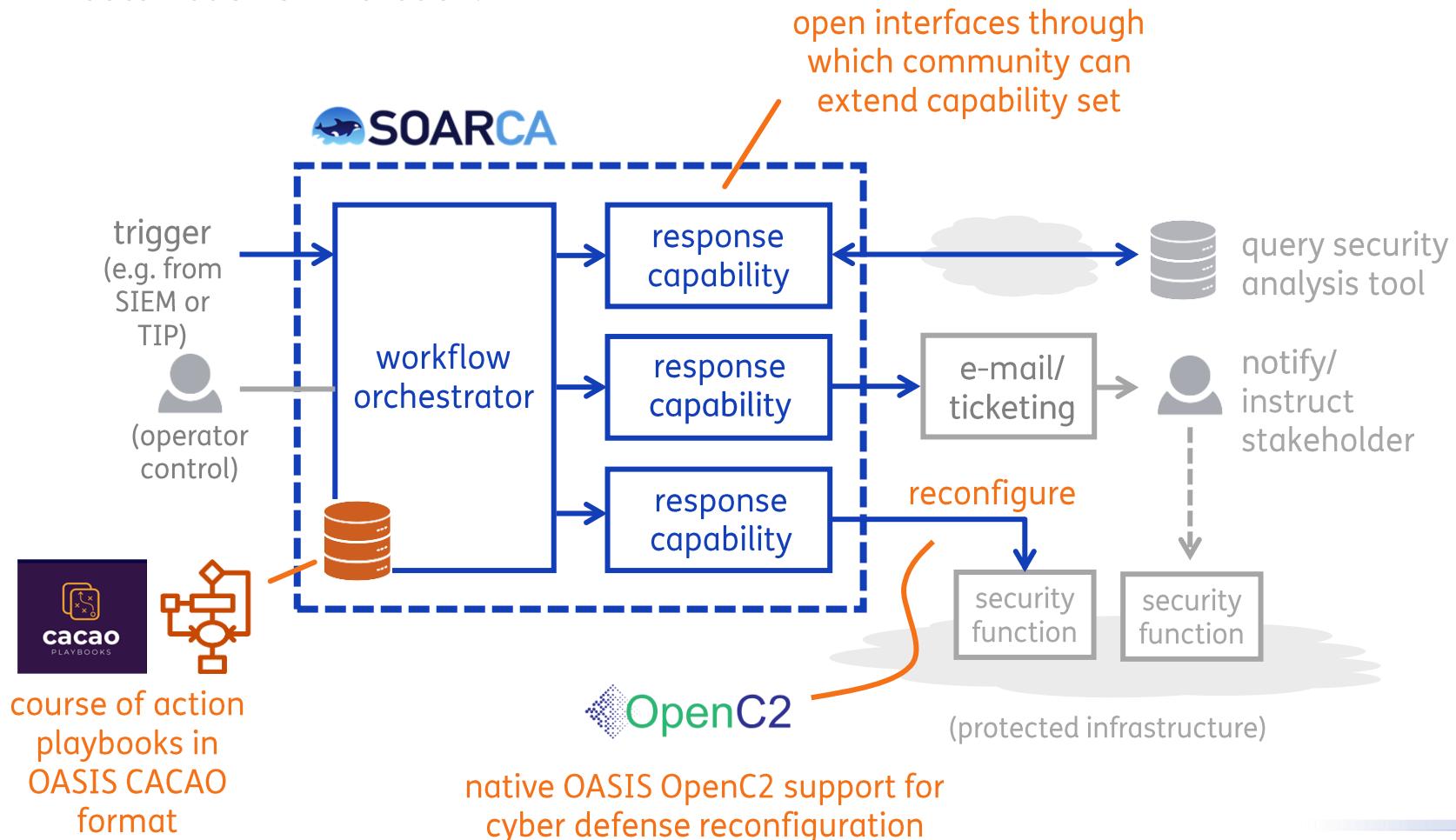
No tool that

- **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.



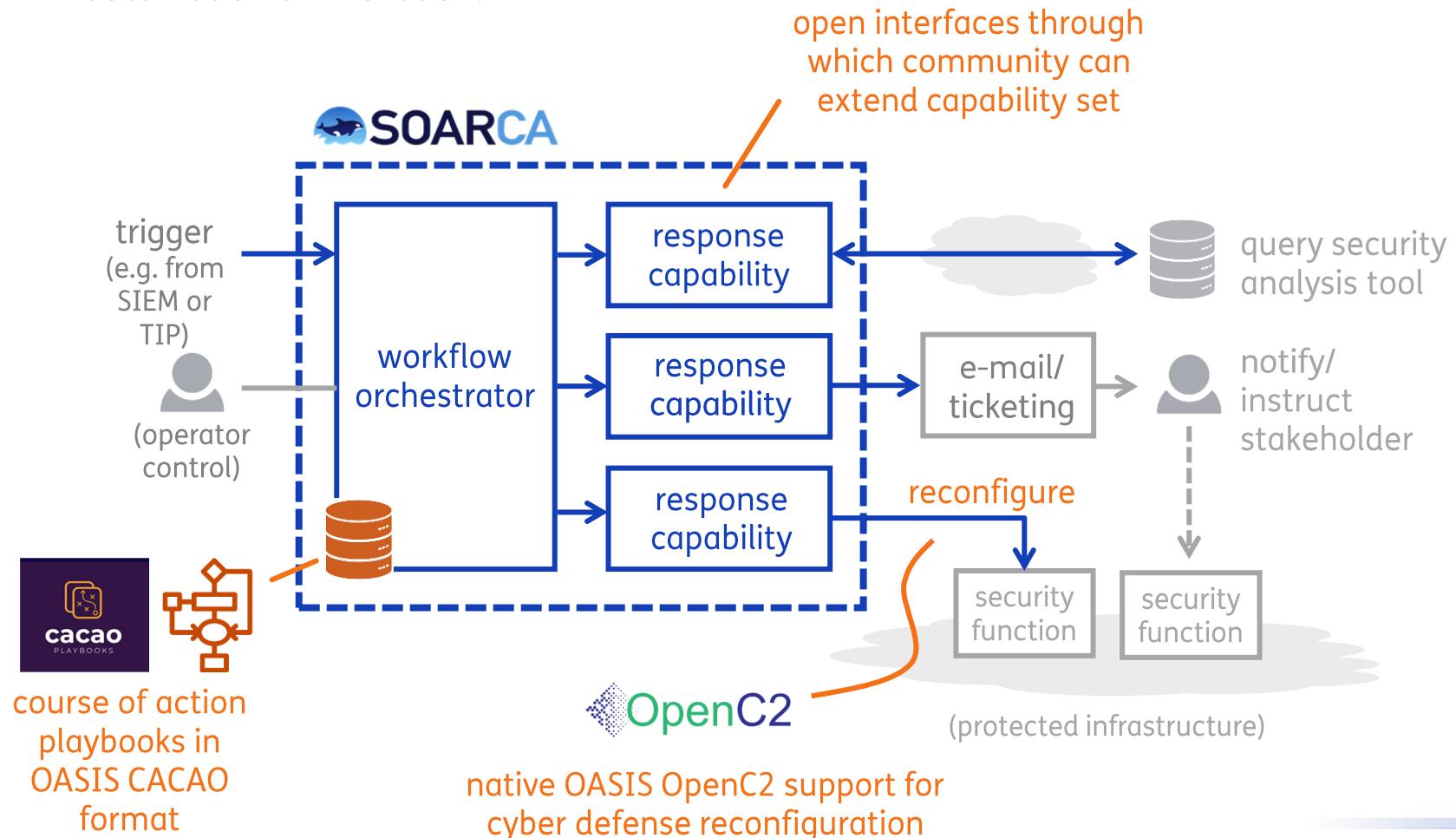
No tool that

- 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.



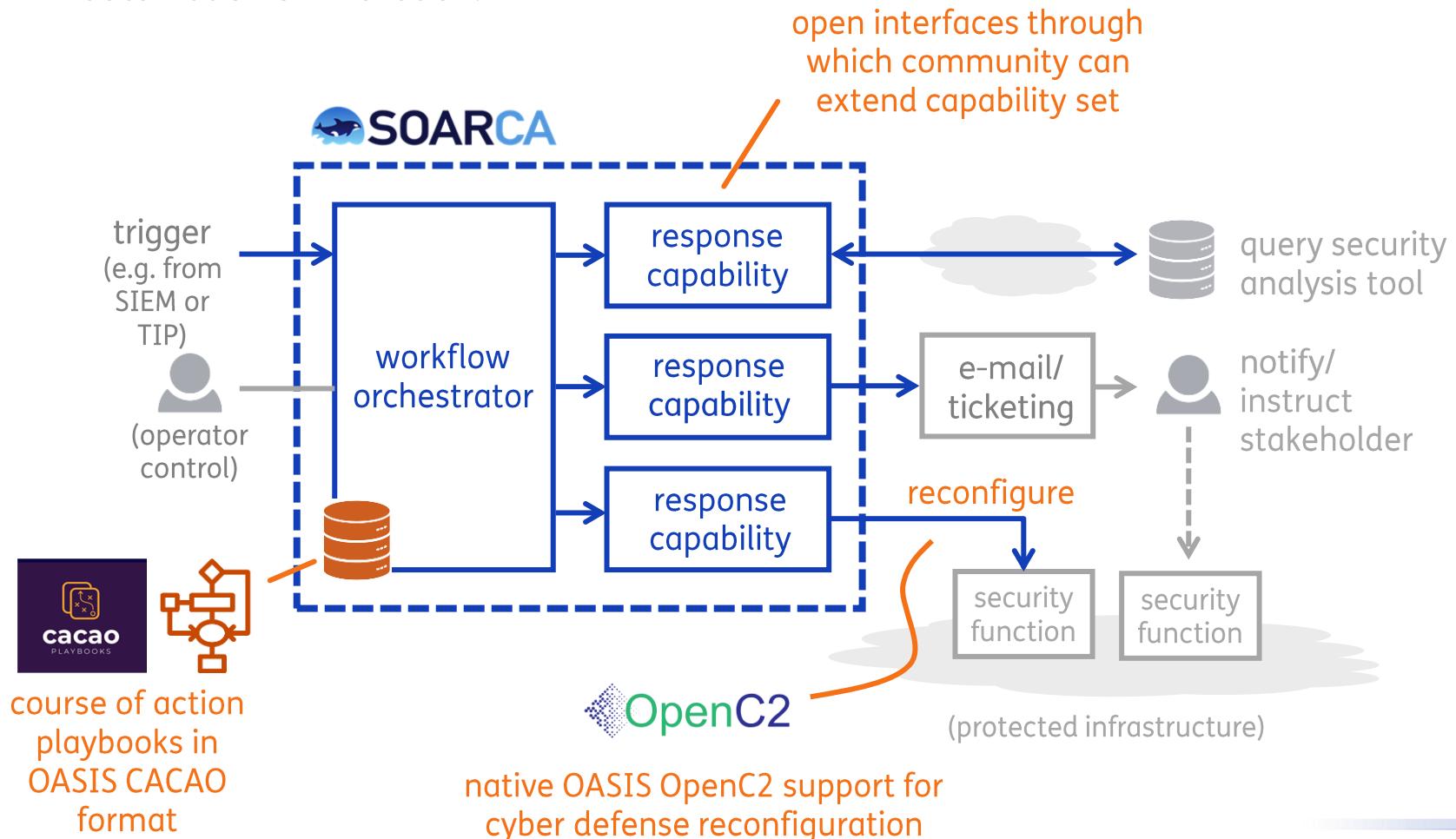
No tool that

- 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.



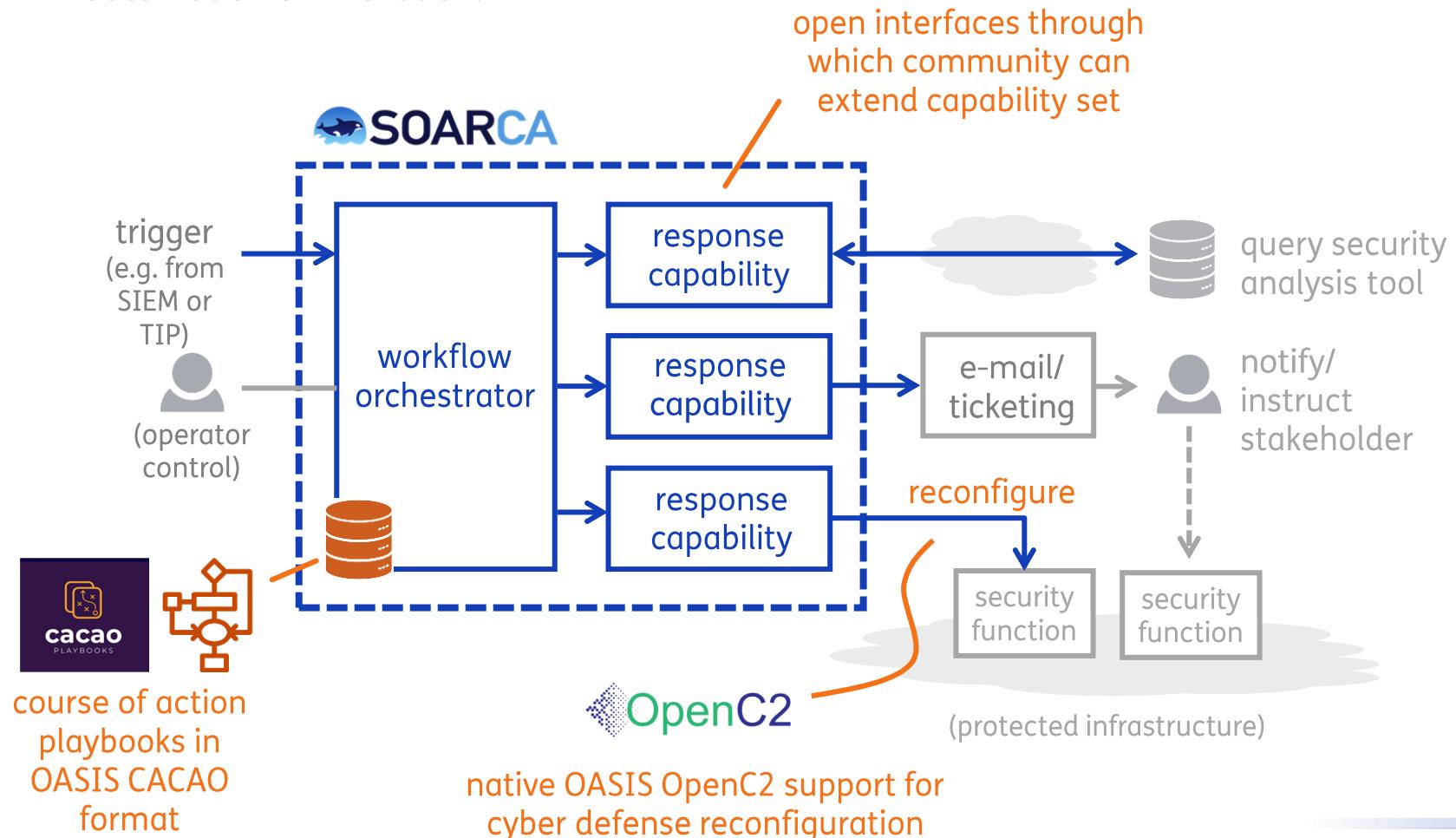
No tool that

- 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>

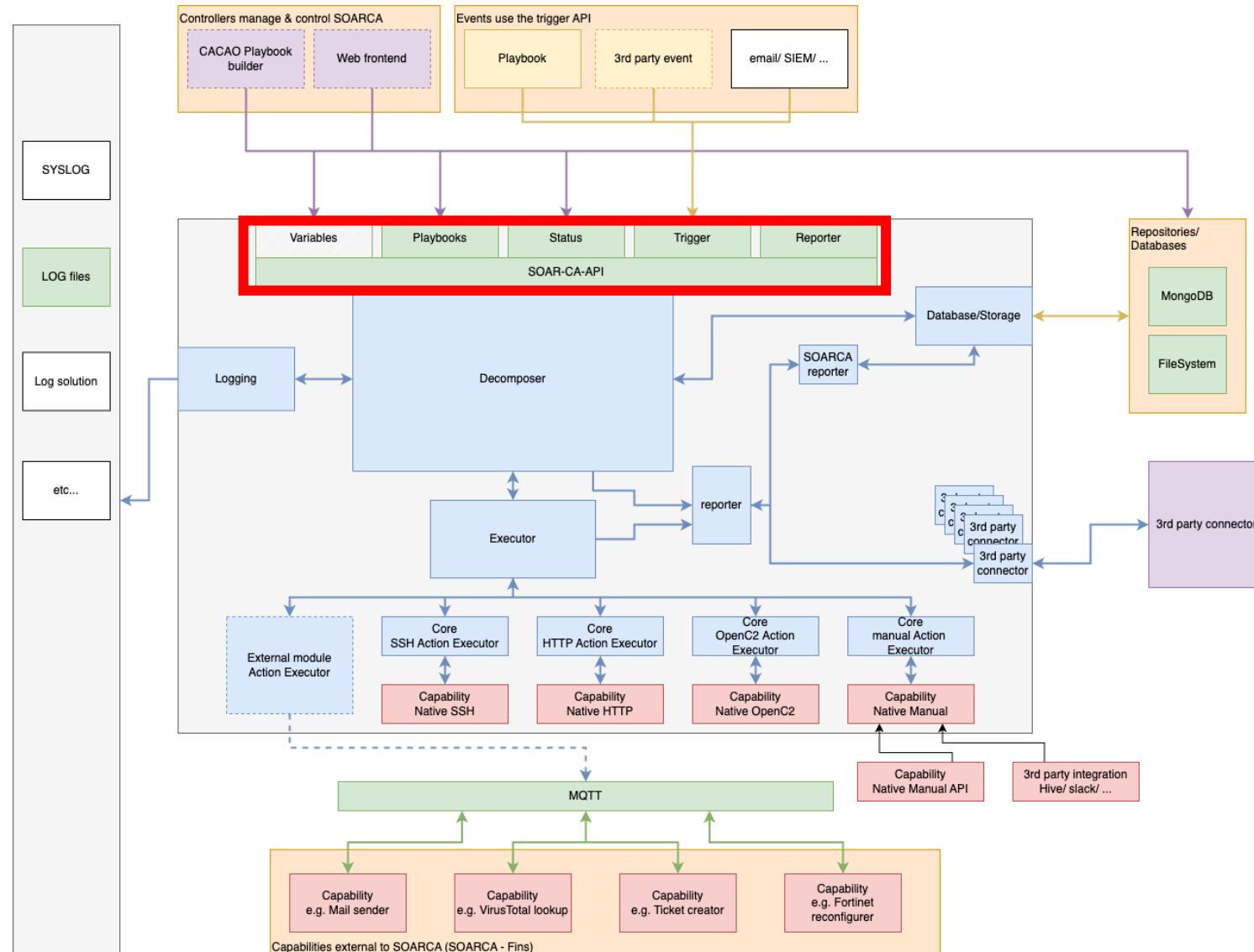
The screenshot shows the GitHub repository page for SOARCA. The repository is public and has 14 branches and 2 tags. The 'About' section describes SOARCA as 'The Open Source CACAO-based Security Orchestrator!' and includes links to cossas.github.io/SOARCA and several tags: automation, cybersecurity, soar, cacao, and cacao-playbooks. The 'Releases' section shows one release, '1.0.0 Latest' (on Mar 18). The 'Packages' section indicates 'No packages published' and provides a link to 'Publish your first package'. The 'Contributors' section lists 11 contributors with their profile icons. The main area of the page displays a list of commits from user MaartendeKruijf, each with a commit message, a link to the pull request, and the date it was made.

Commit Message	Pull Request	Date
Use docker compose (#203)	#203	3 days ago
Feature/48 switch to markdown from asciidoc	#198	7 months ago
Feature/176 trigger api trigger playbook by UUID (#201)	#201	3 days ago
Add docker registry URL to image name (#177)	#177	last month
Fixed missing name field in documentation fin-protocol (#19...)	#19...	3 days ago
Feature/docs/80 add example playbooks to example folder (...)	#80	5 months ago
Update docs (#79)	#79	5 months ago
Feature/176 trigger api trigger playbook by UUID (#201)	#201	3 days ago
Update logging throughout SOARCA		7 months ago
Feature/1 basic workflow api cacao validation		last year
Feature/157 improve playbook execution speed by embeddi...	#157	3 days ago
Feature/176 trigger api trigger playbook by UUID (#201)	#201	3 days ago
Feature/176 trigger api trigger playbook by UUID (#201)	#201	3 days ago
replaced username with user_id (#163)	#163	3 months ago
Added HTTP_SKIP_CERT_VALIDATION and http implementati...		3 months ago
Feature/docs/18 docs update (#20)	#20	5 months ago
typos + fixed spelling error in the documentation. (#9)	#9	5 months ago

SOARCA Technical architecture

Main Takeaways

- 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

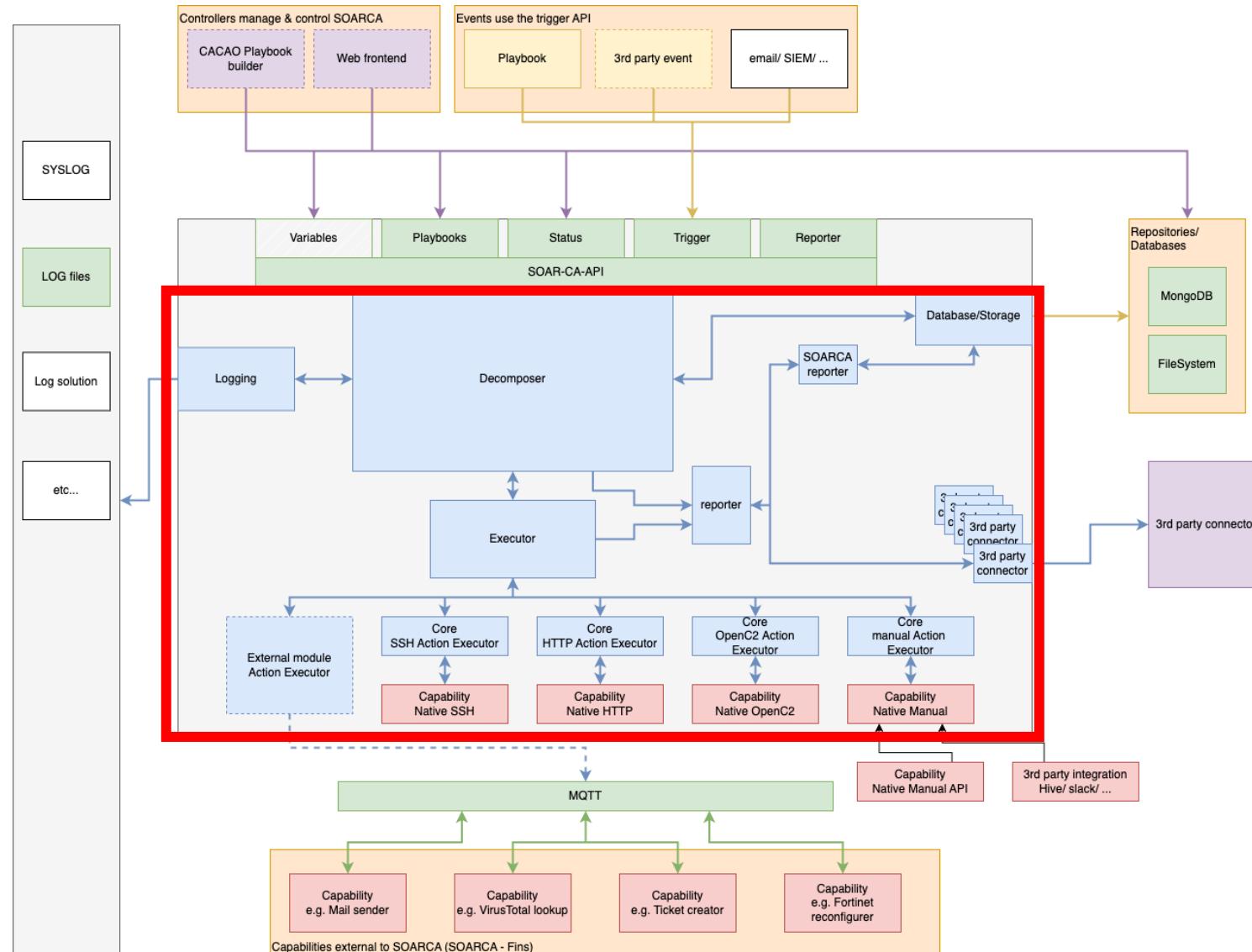


SOARCA fins enable SOARCA to leverage 3rd party services. This enables a response in a more abstract way than is possible when only using the core capabilities.

SOARCA Technical architecture

Main Takeaways

- 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

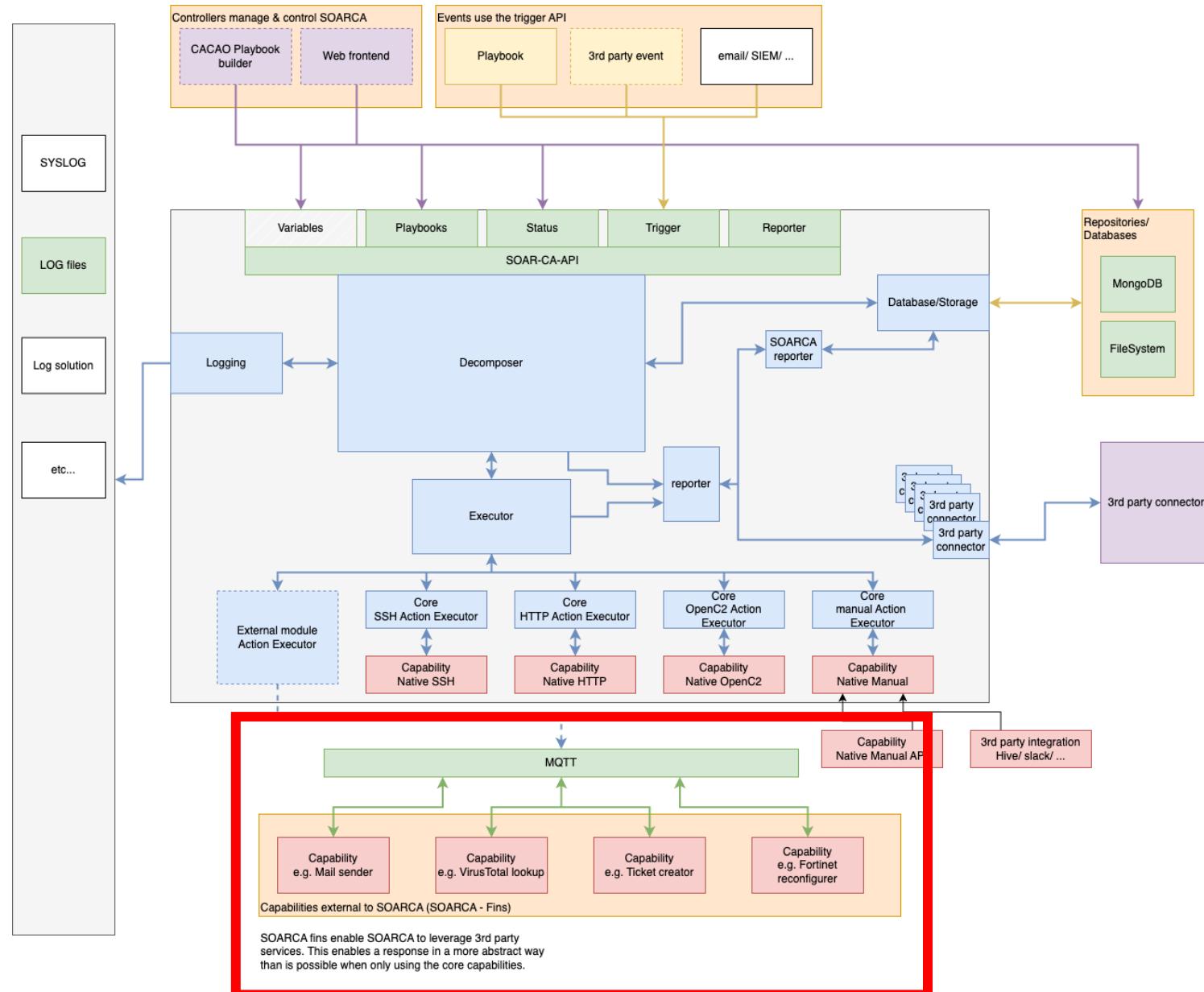


SOARCA fins enable SOARCA to leverage 3rd party services. This enables a response in a more abstract way than is possible when only using the core capabilities.

SOARCA Technical architecture

Main Takeaways

- 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**

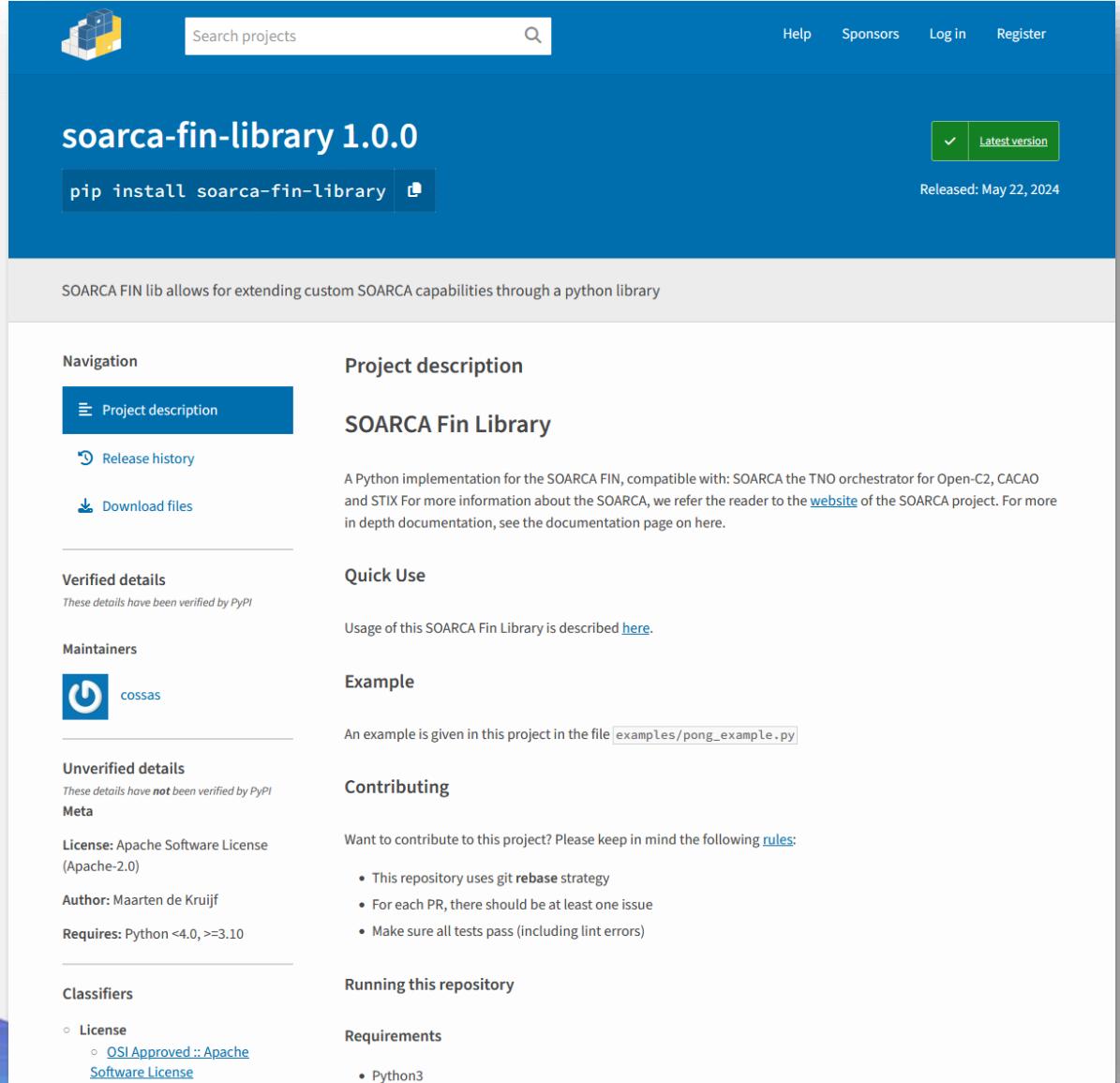


Extending SOARCA with Custom Fins (extensions)

SOARCA compatible library for extending to custom needs

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

Install through pip: `pip install soarca-fin-library`



The screenshot shows the PyPI project page for `soarca-fin-library` version 1.0.0. The page has a blue header with the SOARCA logo, a search bar, and navigation links for Help, Sponsors, Log in, and Register. A green button labeled "Latest version" is visible. The main content area features a title "soarca-fin-library 1.0.0" with a "pip install soarca-fin-library" button. Below the title is a description: "SOARCA FIN lib allows for extending custom SOARCA capabilities through a python library". The page is divided into sections: "Navigation" (Project description, Release history, Download files), "Verified details" (Maintainers, cossas), "Unverified details" (Meta, License: Apache Software License (Apache-2.0), Author: Maarten de Kruifj, Requires: Python <4.0, >=3.10), "Classifiers" (License: OSI Approved :: Apache Software License), "Project description" (SOARCA Fin Library), "Quick Use" (Usage described [here](#)), "Example" (An example in file `examples/pong_example.py`), "Contributing" (Rules for contribution), "Running this repository" (Requirements: Python3), and "Requirements" (Python3).

From CACAO to SOARCA



<https://cossas-project.org/portfolio/SOARCA/>



<https://github.com/COSSAS/SOARCA>

SOARCA

Search this site... Docs / Vision & Concepts

Vision & Concepts

The what and why of SOARCA

Context and Background

Security Orchestrator for Advanced Response to Cyber Attacks - SOARCA

Organisations are increasingly automating threat and incident response through playbook driven security workflow orchestration. The essence of this concept is that specific security events trigger a predefined series of response actions that are executed with no or only limited human intervention. These automated workflows are captured in machine-readable security playbooks, which are typically executed by a so called Security Orchestration, Automation and Response (SOAR) tool. The market for SOAR solutions has matured significantly over the past years and present day products support sophisticated automation workflows and a wide array of integrations with external security tools and data resources. Typically, however, the technology employed is proprietary and not easily adaptable for research and experimentation purposes. SOARCA aims to offer an open-source alternative for such solutions that is free of vendor dependencies and supports standardized formats and technologies where applicable.

SOARCA, TNO's open-source SOAR, was developed for research and innovation purposes and allows SOC, CERT and CTI professionals to experiment with the concept of playbook driven security automation. It is open and extensible and its interfaces are well-defined and elaborately documented. It also offers native support for two emerging technology standards, both developed and maintained by OASIS Open:

- [CACAOv2](#). The Collaborative Automated Course of Action Operations (CACAO) standard provides a common framework and machine-processable schema for security playbooks that are natively interoperable and can be shared and executed across technological and organizational boundaries.
- [OpenC2](#). A standardized language for the command and control of cyber defense technologies. In essence it provides a vendor agnostic language and interface through which so called security actuators (e.g. firewalls or IAM solutions) can be reconfigured automatically.

SOARCA is available through [TNO's](#) community platform [COSSAS](#) (Community for Open Source Security Automation Software) under the [Apache 2.0 license](#). With its release, TNO aims to drive both the adoption and further development of novel technologies for cyber security automation forward. Here we note that open and accessible SOAR functionality is not only relevant for automation in threat and incident response but also for attack & defense simulations, cyber ranges, digital twinning and other emerging innovations that require orchestration of complex (security oriented) workflows.

View page source | Edit this page | Create child page | Create documentation issue | Create project issue | Print entire section

Context and Background | Current state of SOARCA | Core Concepts | Course of Action | CACAO Playbooks: Streamlining Cybersecurity Operations | SOARCA Fin(s): Extending the core capabilities | Join the SOARCA Community | Key Details

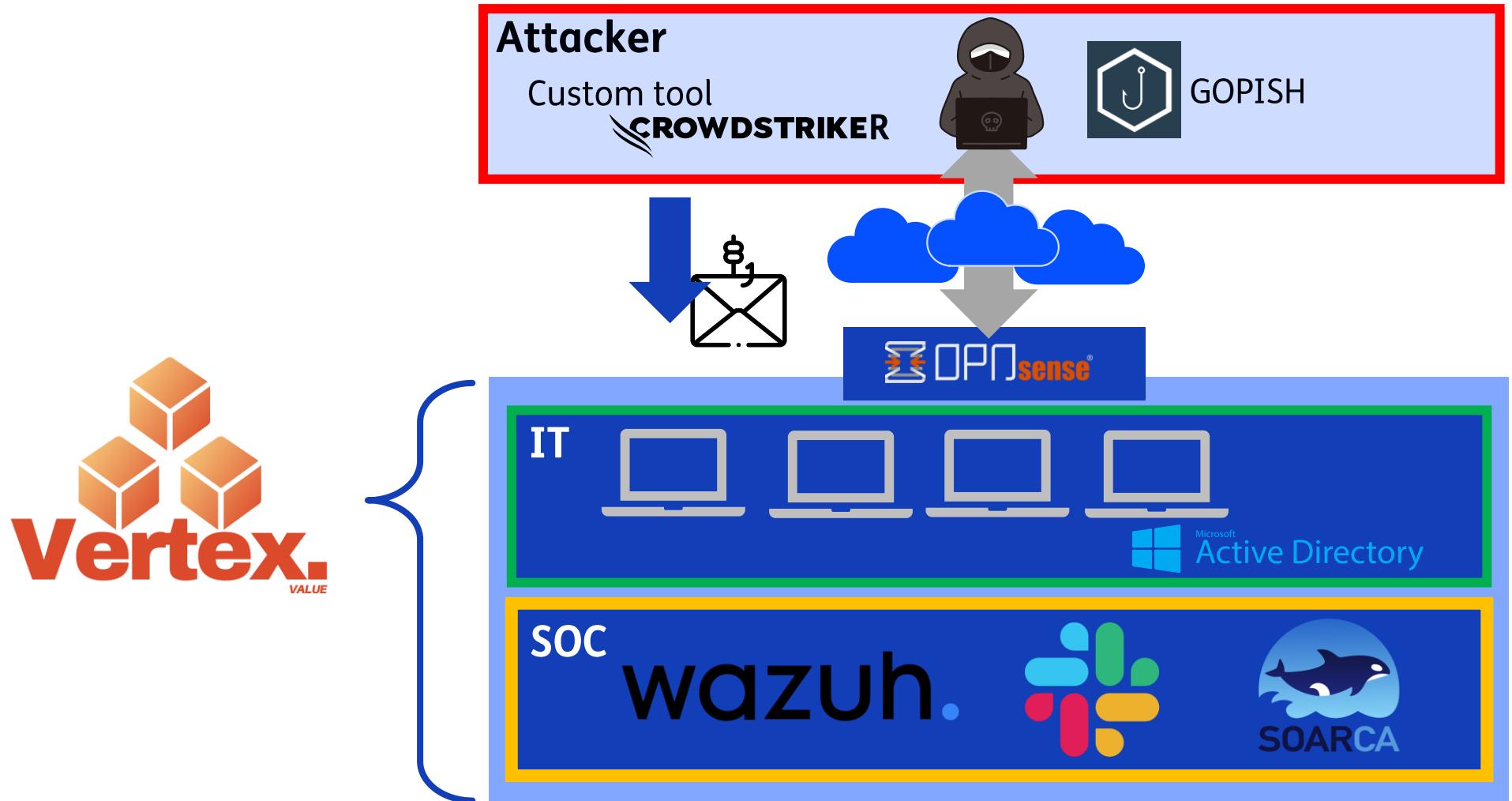
Tags

- Api 4 | Bash 1 | Components 2 | Database 1 | Docker 1 | Fin 3 | Http 3 | Logging 1 | Native 1 | Protocol 3 | Python 1 | Rest 3 | Swagger 1

Categories

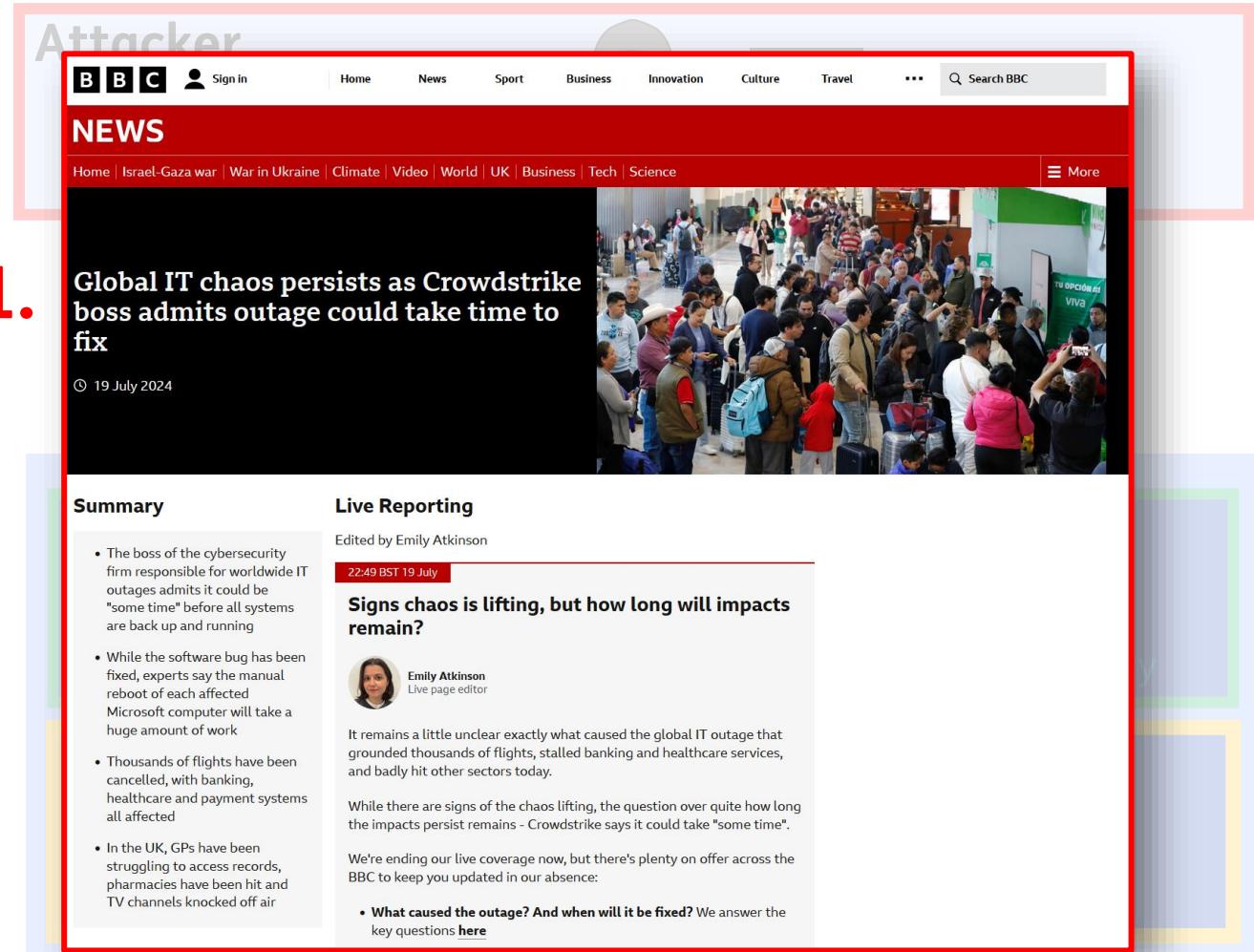
- API 3 | Architecture 10 | Capabilities 2 | Documentation 1 | Extensions 3 | Getting-Started 1

Phishing on VertexValue: a SOARCA demo scenario



Phishing on VertexValue: a SOARCA demo scenario

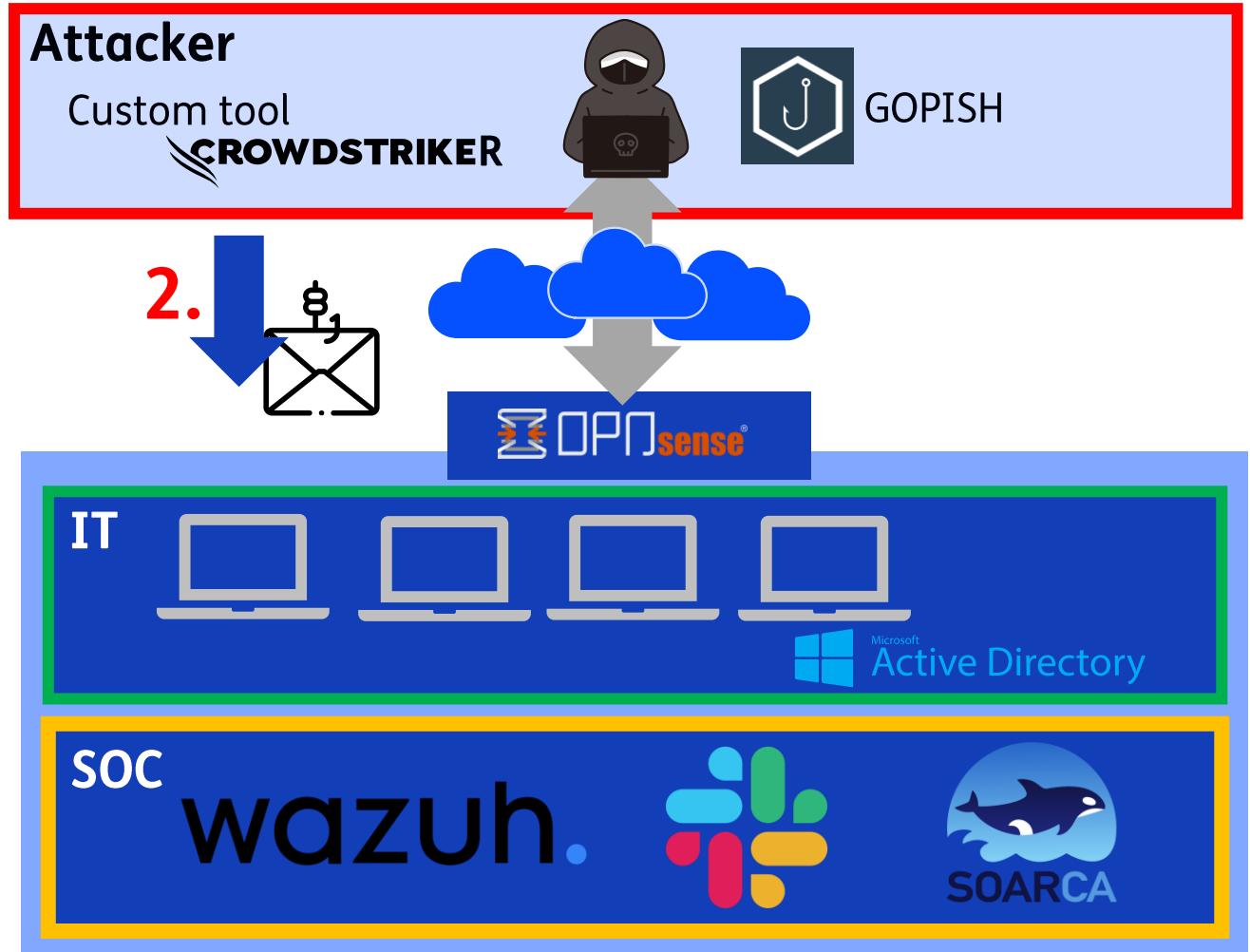
1. Crowdstrike outage situation
2. Attacker launches phishing campaign with fake Crowdstrike update tool
3. User received email and is redirected to legitimate looking website
4. User downloads fake update tool (ransomware)
5. Download gets detected by Wazuh
6. Wazuh triggers SOARCA by sending a CACAO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



The screenshot shows a BBC News article titled "Global IT chaos persists as Crowdstrike boss admits outage could take time to fix". The article was published on 19 July 2024. The BBC navigation bar includes Home, News, Sport, Business, Innovation, Culture, Travel, and a search bar. The main content area features a large image of a crowded airport terminal. Below the image, there are two columns: "Summary" and "Live Reporting". The "Summary" column contains a bulleted list of facts about the outage. The "Live Reporting" column is edited by Emily Atkinson and includes a timestamp of 22:49 BST 19 July, a photo of Emily Atkinson, and a section titled "Signs chaos is lifting, but how long will impacts remain?". A sidebar on the right lists questions related to the outage.

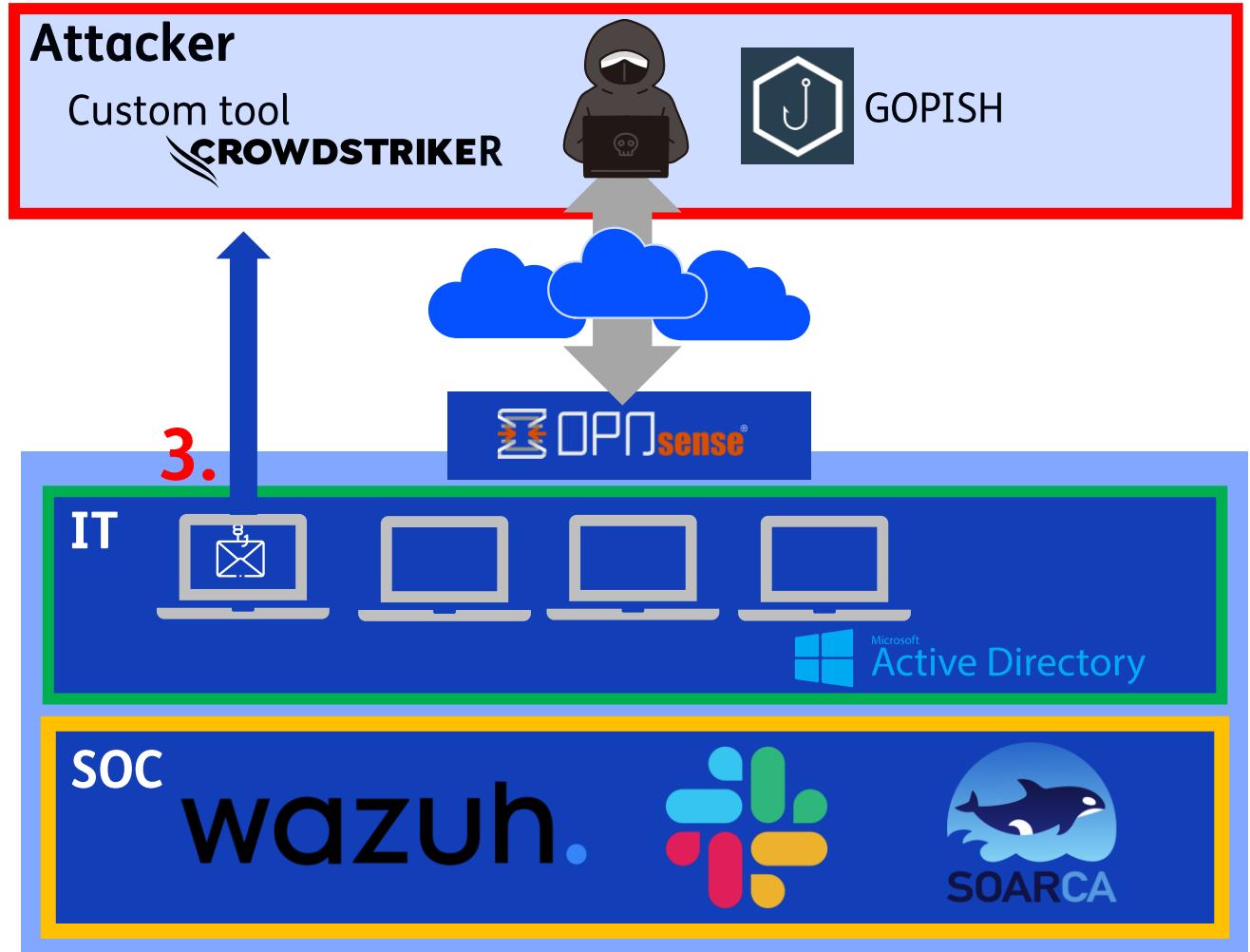
Phishing on VertexValue: a SOARCA demo scenario

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



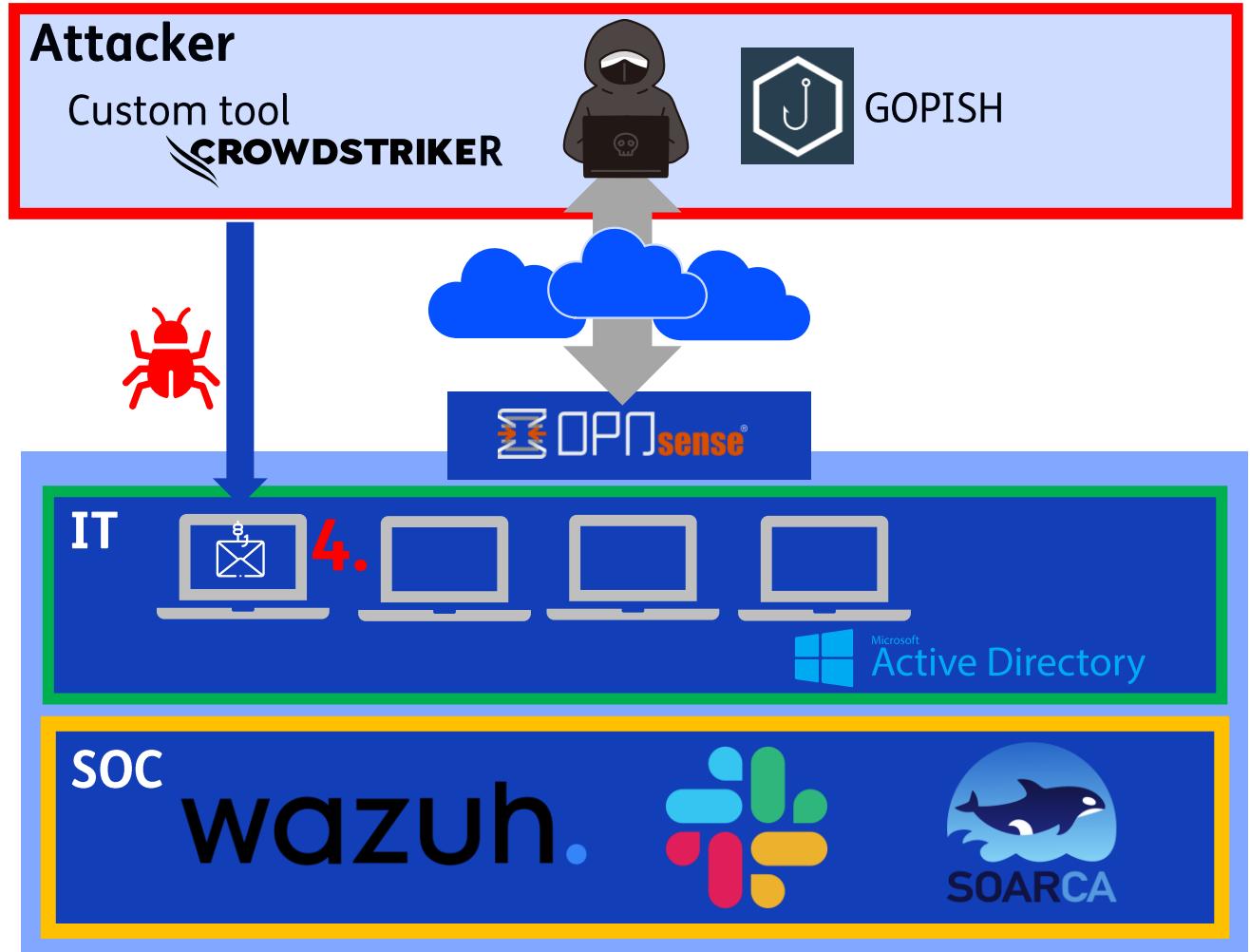
Phishing on VertexValue: a SOARCA demo scenario

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



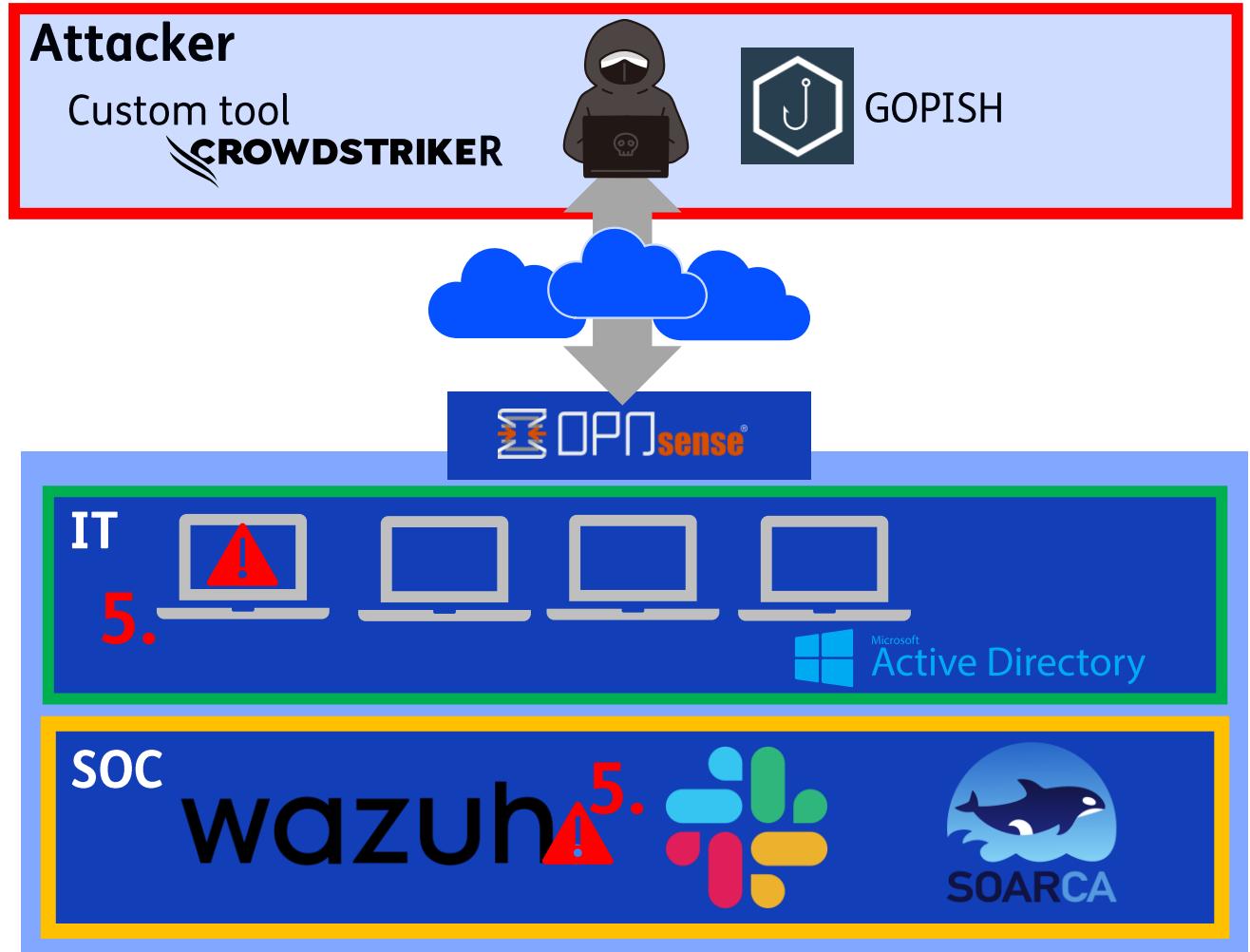
Phishing on VertexValue: a SOARCA demo scenario

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



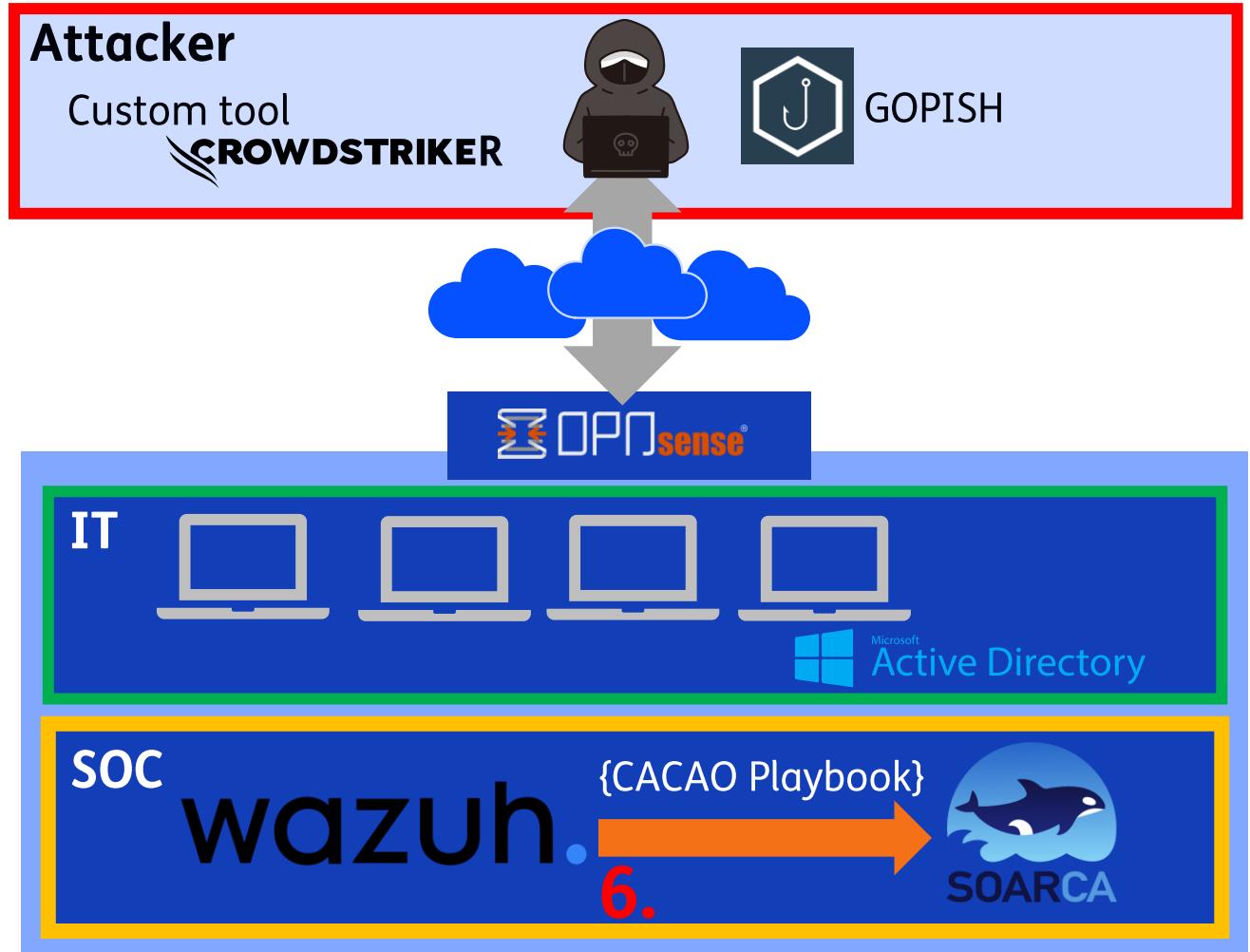
Phishing on VertexValue: a SOARCA demo scenario

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



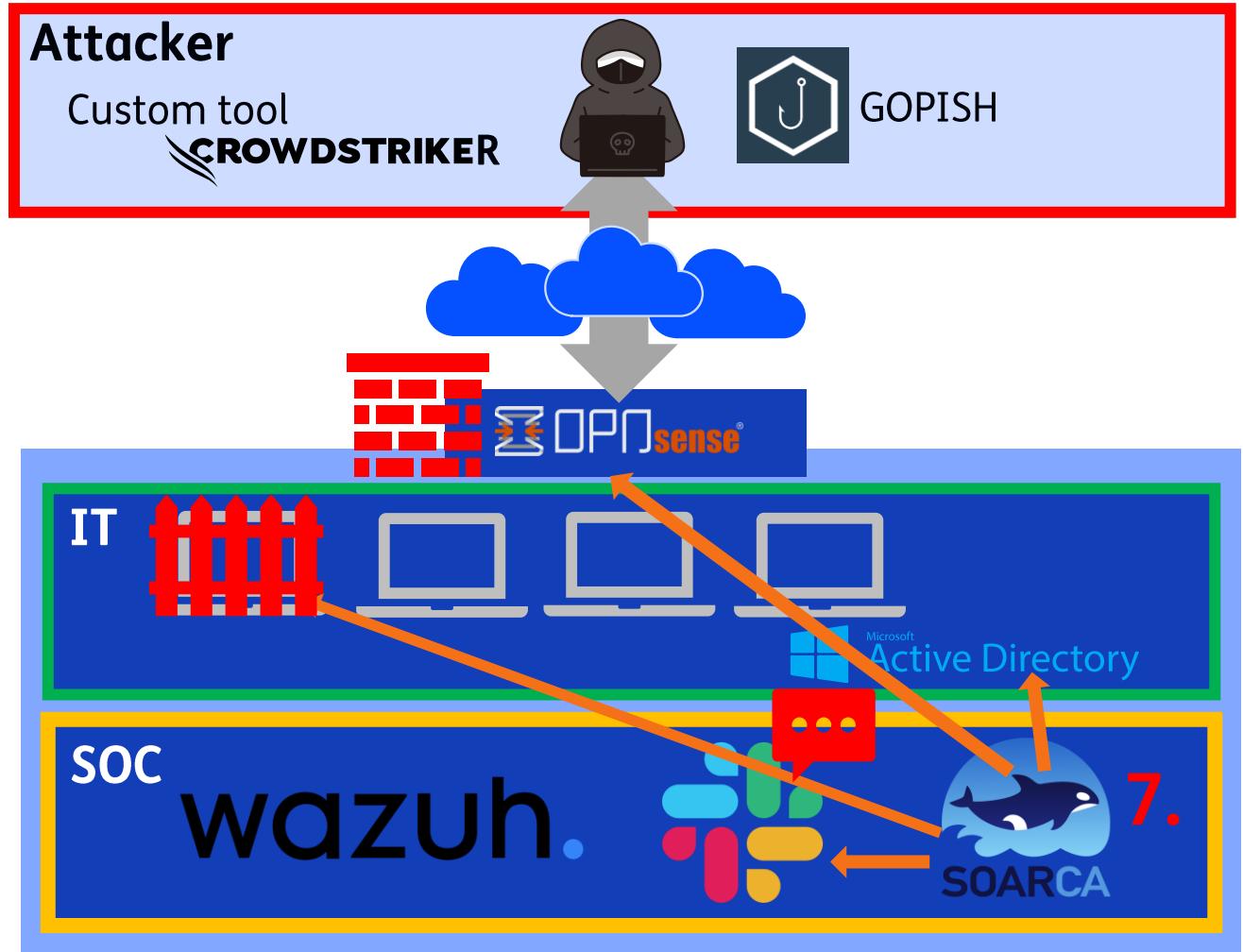
Phishing on VertexValue: a SOARCA demo scenario

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

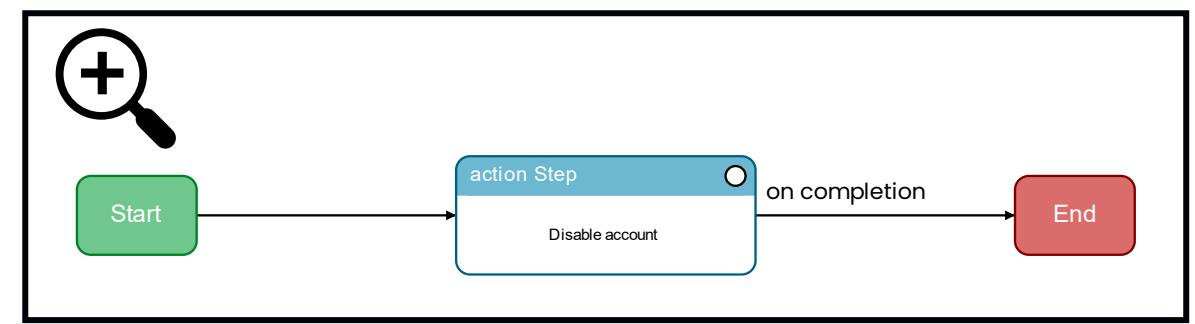
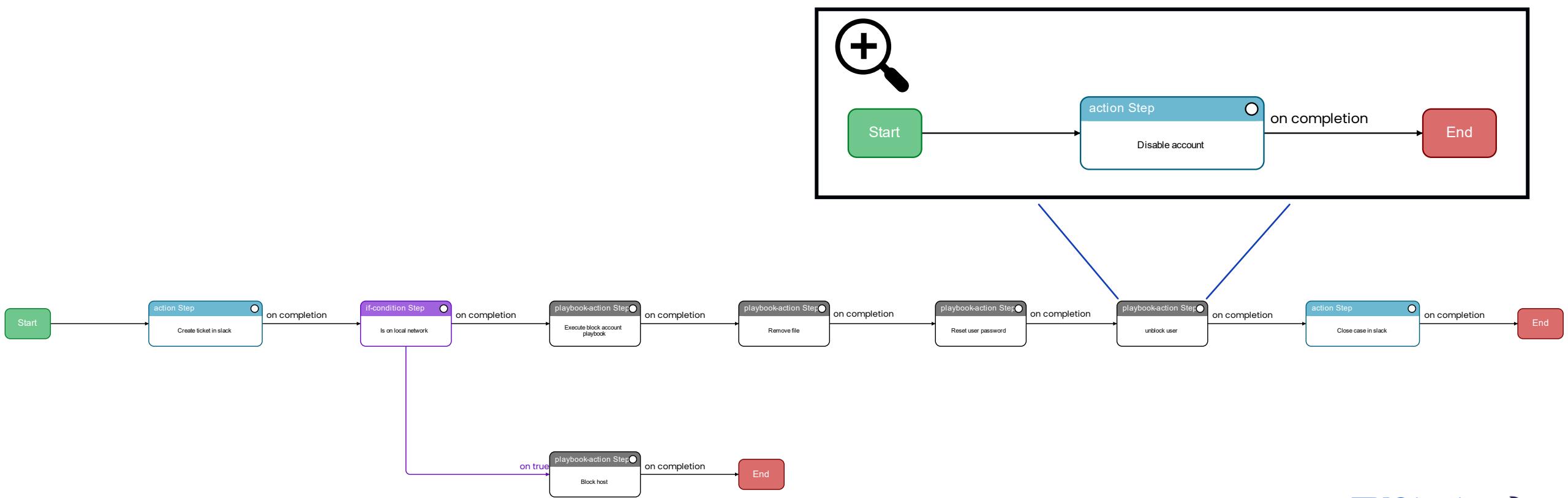


Phishing on VertexValue: a SOARCA demo scenario

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



Playbook-based remediation: Example CACAO Playbooks

Powershell

properties json

- Type: powershell
- Description: Block user given to the playbook

Command: `Disable-ADAccount -Identity __user__.value`

Command B64 (displayed in plaintext)

Version

Playbook Activity

External References

Confirm Cancel

```

graph LR
    Start((Start)) --> ActionStep["action Step  
Disable account"]
    ActionStep -- "on completion" --> End((End))
  
```

Agents Display

Type	Name	Description
soarca	soarca-powershell	

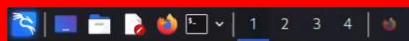
Confirm Cancel

Targets Display

Type	Name	Description
net-address	Windows AD DS server	

Confirm Cancel





Attacker View – Environment Overview



Kali Linux a...



Trash



File System



Home

21:33

User View - Environment Overview

The screenshot shows a Microsoft Word document window. At the top, the ribbon menu is visible with tabs like File, Home, Insert, Layout, References, Review, View, and Help. The Home tab is selected. Below the ribbon is the toolbar with various editing tools. The main content area contains the following text:

SOARCA

"*Neque porro quisquam est qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit...*"

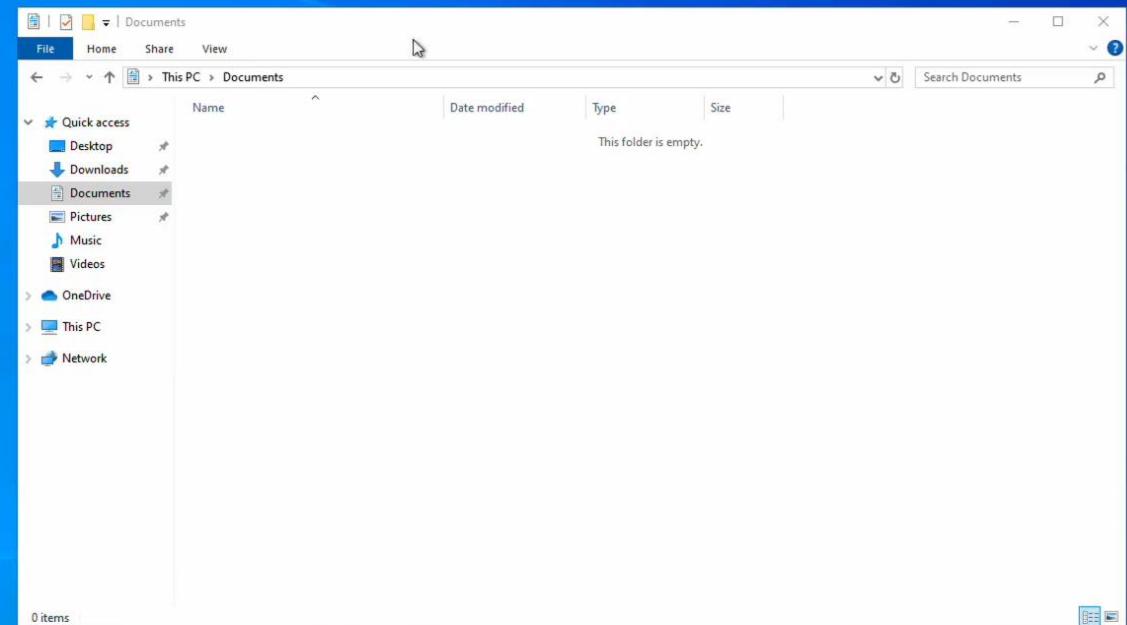
"There is no one who loves pain itself, who seeks after it and wants to have it, simply because it is pain..."

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi dui nisl, ultrices ut nibh vitae. tristique consequat ipsum. Curabitur nec nulla ut ligula tincidunt blandit fringilla vitae quam. Nulla facilisi. Quisque nec est eleifend, posuere nibh vel, egestas nunc. Quisque lobortis aliquam convallis. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Morbi at urna ut turpis mattis euismod vel ac dolor. Fusce sit amet semper turpis. Curabitur et metus sit amet nulla eleifend varius quis et turpis. Cras ut sapien ut mi vehicula euismod. Integer sit amet risus volutpat, accumsan tortor in, imperdiet est. Pellentesque imperdiet mauris ut mi dapibus elementum. Morbi lacinia augue eu ipsum ultrices mollis. Nunc eget nulla sagittis, porttitor orci sed, tempus tellus.

Duis mollis nisi eget tortor maximus auctor id dictum mi. Nunc at dapibus nibh. Nulla congue leo quis tincidunt gravida. Vivamus pellentesque, mauris at dignissim tempus, est nibh aliquam erat, id ornare nibh velit et quam. Aenean sit amet arcu nibh. Donec felis nunc, porttitor ut dignissim at, ultrices et quam. Donec accumsan nibh massa. In elementum arcu vitae lacinia viverra. Duis porttitor ipsum id elit eleifend porttitor.

Sed rutrum nisi pharetra, elementum odio sed, consectetur quam. Sed tortor purus, faucibus vitae lacinia in, lobortis nec metus. Aenean id eros ut orci pretium gravida ac nec tortor. Cras aliquam nulla eget elementum gravida. Praesent convallis mi a eros rhoncus, eu efficitur nisi iaculis. Quisque at dolor scelerisque, laoreet sem sit amet, interdum mi. Integer neque ligula, bibendum scelerisque condimentum eu, auctor eget tortor. Aenean ligula turpis, condimentum ac ultrices nec, lacinia ac dolor. Ut id vulputate turpis, vehicula pellentesque

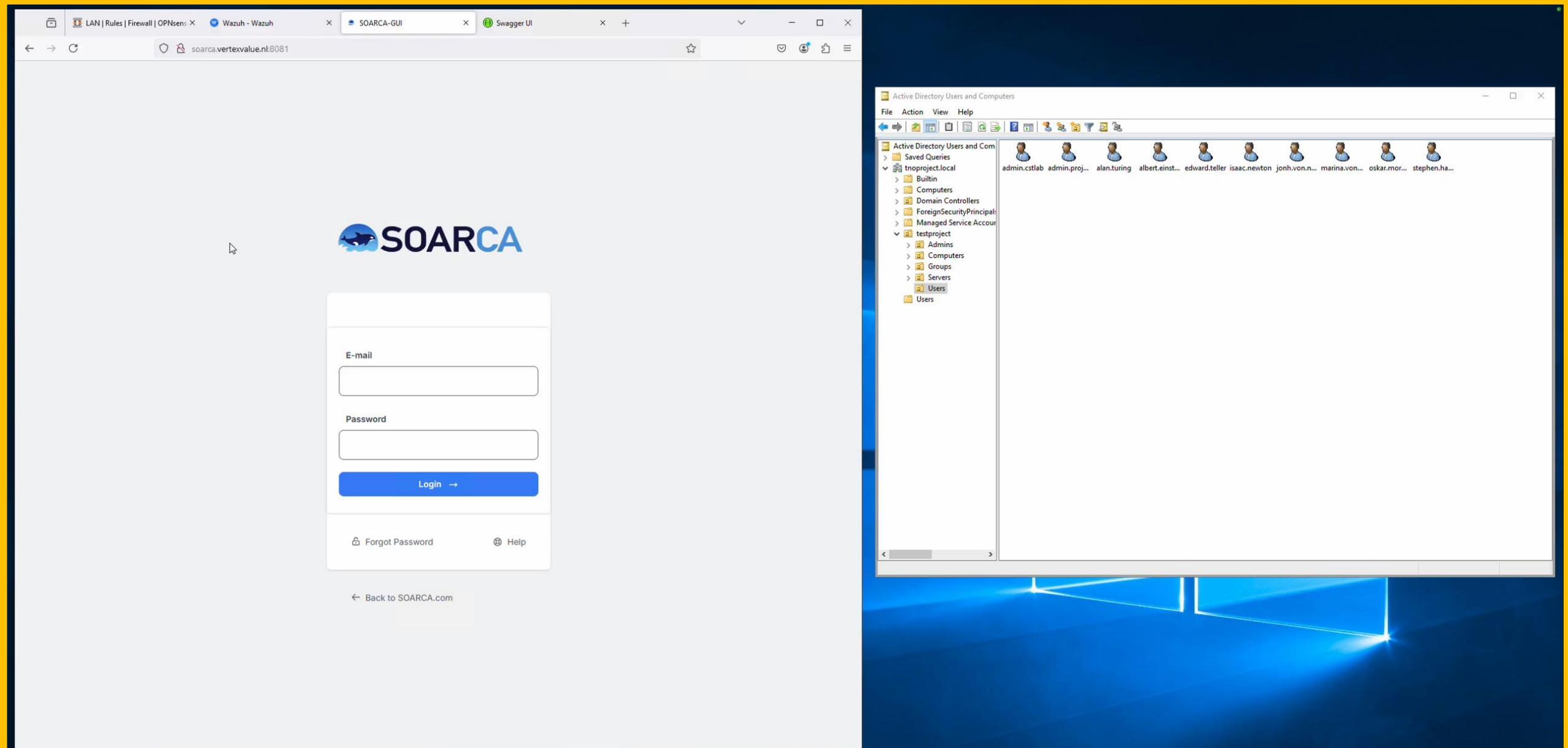
Page 1 of 2, 531 words, Editor Suggestions: Showing



The screenshot shows a Windows desktop environment with two browser windows open:

- OPNsense Dashboard**: The main window displays system information, interface statistics, and firewall rules. Key details include:
 - System Information**: Name: OPNsense.localdomain, Versions: OPNsense 24.7.3_1-amd64, FreeBSD 14.1-RELEASE-p3, OpenSSL 3.0.14.
 - Interface Statistics**: A donut chart showing traffic distribution between WAN and LAN.
 - CPU**: QEMU Virtual CPU version 2.5+ (2 cores, 2 threads).
 - Gateways**: WAN_GW (IP 10.100.5.1) and WAN_DHCP6.
- Active Directory Users and Computers**: A Windows application showing a list of users in the domain. A user named "alan.turing" is selected.

SOC View - Environment Overview



SOC View - Environment Overview

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Campaigns - Gophish" and has the URL <https://gophish:3333/campaigns>. The browser's address bar also displays this URL. The page content is the "Campaigns" section of the Gophish application. On the left, there is a sidebar with various navigation links: Dashboard, Campaigns (which is selected and highlighted in dark blue), Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (with an "Admin" badge), Webhooks (with an "Admin" badge), User Guide, and API Documentation. The main content area has a large title "Campaigns". Below it is a teal button labeled "+ New Campaign". Underneath the button are two tabs: "Active Campaigns" (which is currently selected) and "Archived Campaigns". A light blue banner at the bottom of the main content area says "No campaigns created yet. Let's create one!". In the top right corner of the browser window, there is a user profile icon labeled "admin" and a green "Logout" button. The top of the browser window shows the Kali Linux desktop environment with various icons and a system status bar.

Attacker View – Launching the attack

Mail - alan turing - Outlook

https://outlook.live.com/mail/0/inbox/id/AQQkADAwATM3ZmYBLTg0YWUtODlkNy0wMAitMDA...

Outlook

Home View Help

New mail Delete Archive Report Move to Reply all Read / Unread Flag / Unflag ...

Avoid losing access to Outlook by adding a recovery phone number. Add now.

Favorites

- Inbox 2
- Drafts
- Archive
- Add favorite

Folders

- Inbox 2
- Junk Email
- Drafts
- Sent Items
- Deleted Items 1
- Archive
- Notes
- Conversation History
- Create new folder

Groups

New group

Manual update required BSOD - IT services

hackyoneconf@gmail.com Manual update required... 10:04 PM Dear alan.turing.vertexvalue@outlook.com

Microsoft Get to know your OneDrive... 9:57 PM Go to your OneDrive ...

Dear alan.turing.vertexvalue@outlook.com,

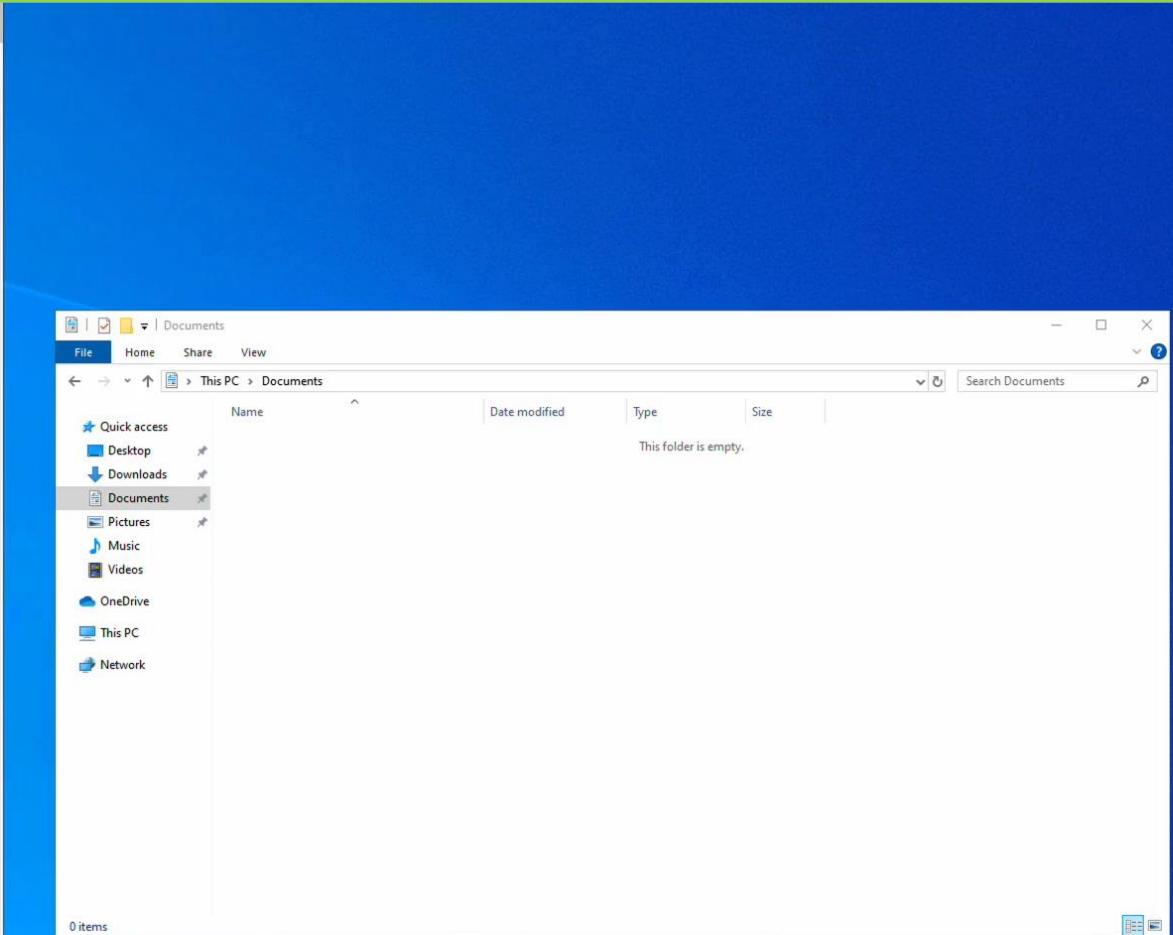
The Information Technology Department at VertexValue has detected that your computer is missing a critical security update. To ensure the continued safety and performance of our corporate network, please download and install the necessary update within the next 24 hours. Failure to comply may result in disconnection from the network.

Due to the risk of a blue screen of death (BSOD) occurring, the IT department cannot roll out this update via Intune. Therefore, this action must be performed manually once.

To update your system, please follow these steps:

1. **SAVE and CLOSE** any documents or files you're currently working on.
2. **DOWNLOAD** the update file from this link: [Download CrowdStrike Update](#).
3. Once the download is complete, **OPEN** the file to start the installation process.
4. **FOLLOW** the on-screen instructions to complete the installation.
5. **REBOOT YOUR COMPUTER** if prompted. Some updates may require a restart to take full effect.

If you encounter any issues or have questions, please notify the IT Department immediately. Should you need an extension, you can request to extend your deadline to 72 hours by clicking ?rid=LLTYWdB and logging in with your corporate credentials, then selecting "Extend Deadline."



User View – Under Attack

Windows 10 Enterprise Evaluation
Windows License valid for 43 days
Build 19041.vb_release.191206-1406
9/23/2024

10:06 PM NLD

The screenshot shows a Windows desktop environment with several open windows:

- SOARCA-GUI**: A web-based interface for managing playbooks. It displays 6 Executed Playbooks, 0 Ongoing Playbooks, and 0 Failed Playbooks. A table lists recent playbook executions with columns: Playbook Name, Start Time, Execution Duration, and Status (all marked as 'succes').
- Active Directory Users and Computers**: A Windows management console showing the structure of Active Directory. It includes a tree view of containers like 'tnopproject.local' and 'testproject', and a list of users on the right.
- Taskbar Icons**: Icons for LAN | Rules | Firewall | OPNsense, Wazuh - Wazuh, SOARCA-GUI, and Swagger UI.

SOC View – Events & Remediation of the attack

SOC View – Slack tickets

The screenshot shows a Slack interface with the following details:

- Left Sidebar:** Shows the "SOARCA-DEMO-SLACK" workspace with sections for Home, DMS, Activity, Automata..., More, Channels, Direct messages, Apps, and a list of users (Luca Morgese Zangrandi, Maarten you, soarca-bot).
- Top Bar:** Includes a search bar ("Search SOARCA-DEMO-SLACK"), a refresh icon, and user status indicators.
- Channel Header:** "# slack-integration" with tabs for Messages, Add canvas, Files, and a plus sign.
- Message Timeline:** A timestamp bar at the top indicates messages from 10:15 to Today. It shows two messages from "Maarten" at 11:01 AM and 1:20 PM, and one message from "soarca-bot" at 10:07 PM.
- Message Content:** The "soarca-bot" message at 10:07 PM states:
 - 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.
- Bottom Bar:** Includes a rich text editor toolbar and a message input field.

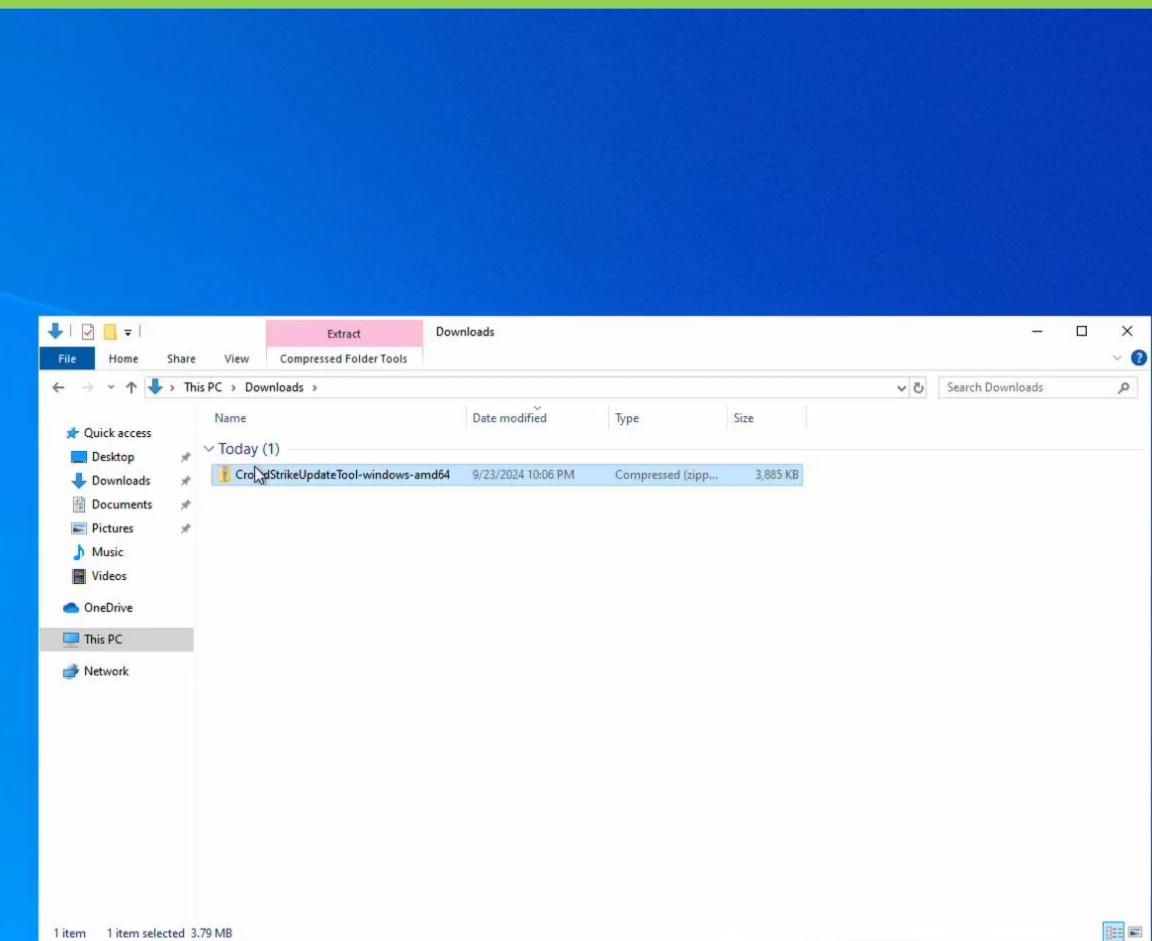
Crowdstriker Recovery Tool®

Restore from a potential BSOD
Download here

[Get Updater Tool](#)

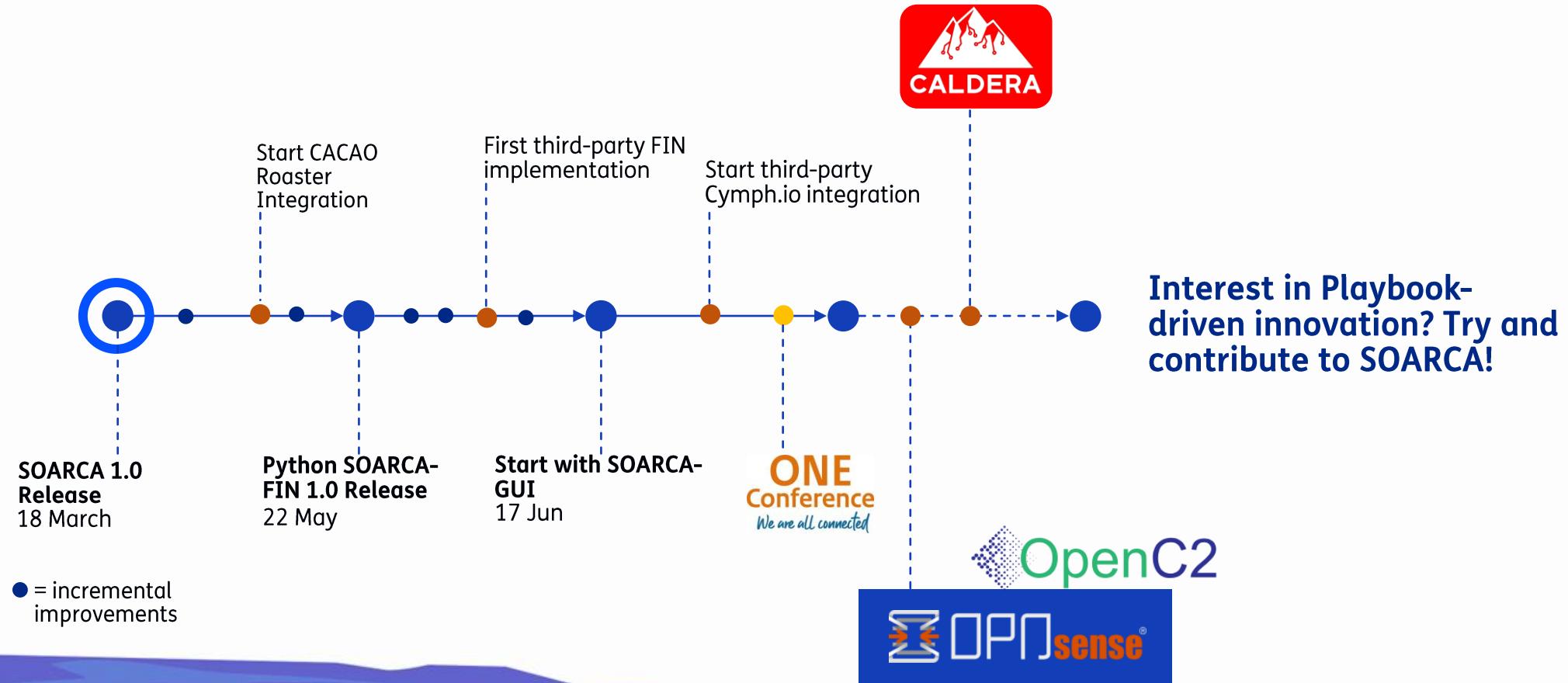
Why Crowdstriker

-  **affordable protection**
bundles built with small businesses in mind
-  **simple setup**
One-time easy installation of the Falcon sensor
-  **Responsive support**
Global support team available 24/7



User View – No Mitigation

Roadmap: What is next for SOARCA?



All demo files and references can be found here:

 <https://github.com/the cyber project/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



Questions?

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

