



Hands-On Cybersecurity Training Series

Immersive and Gamified Cybersecurity Practices for SMEs

19 January 2026

10:00–11:30 CET

REGISTER NOW!



Funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Training Webinar Series

1 - Building Cybersecurity Awareness and Defense Foundations for SMEs

 2025-11-26  10:00 – 11:30 a.m. CET

2 - Advanced Threat Detection and Privacy Protection for SMEs

 2025-12-03  10:00 – 11:30 a.m. CET

3 - Immersive and Gamified Cybersecurity Practices for SMEs

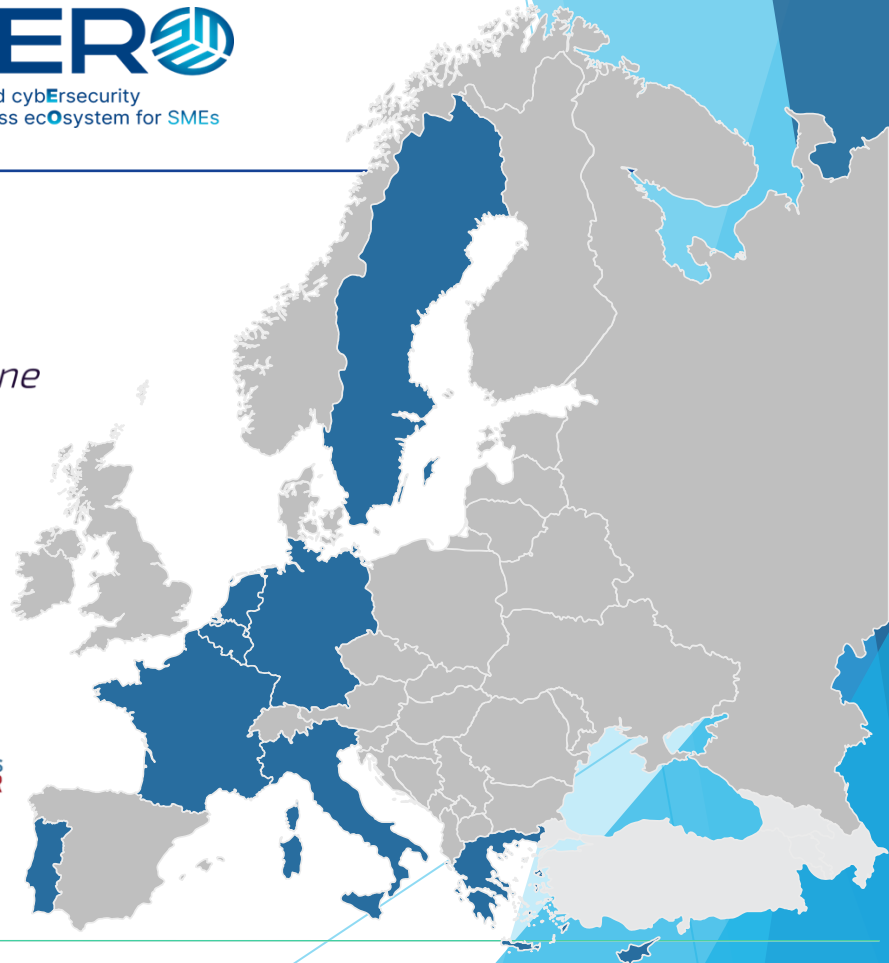
 2026-01-19  10:00 – 11:30 a.m. CET

Mastering the Tools of the NERO Marketplace

 2026-01-26  10:00 – 11:30 a.m. CET

 nerocybersecurity.eu/events

Consortium



Vision and Objectives



Vision: Improve knowledge & auditing of *cybersecurity*

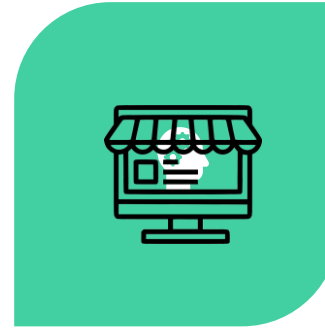
Objectives:

1. Design the NERO advanced cybersecurity **awareness ecosystem** focused on SMEs; provide its modules through a user-friendly **marketplace**.
2. Demonstrate the benefits of NERO through **3 use cases** in healthcare, finance, transportation/logistics sectors.
3. Support SMEs by sharing knowledge and advanced **training materials utilizing EU tools** that follow security-by-design and privacy-by-design approaches.

NERO main outcomes



**CYBERSECURITY AWARENESS
ECOSYSTEM**



**USER FRIENDLY
MARKETPLACE – TRAININGS
PLATFORM**

Speakers



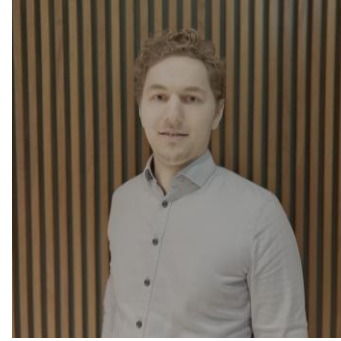
advan**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs



Wissam Mallouli
Project Manager & CTO



Kostas Poullos



Ole Höfener
Project Manager



A few tips for today

- ▶ Please use the **Q&A box** at the bottom of your screen to submit your questions.
- ▶ The speakers will reply during the **panel discussion or in written form**.
- ▶ The session is being **recorded** and will be shared on the NERO website and YouTube channel.
- ▶ **Presentation slides** will be available after the session on the NERO website.
- ▶ **Pre and Post training questionnaire** to be filled during the webinar



Pre-Training Questionnaire



Agenda

Webinar 3 – Hands-On Cybersecurity Training Series on Immersive and Gamified Cybersecurity Practices for SMEs

- ▶ Cyber Ranges Training and Exercises
 - ▶ Wissam Mallouli (Montimage)
- ▶ Gamification-Based Cybersecurity
 - ▶ Ole Höfener (Massive Dynamic Sweden)
- ▶ Incident response using CACAO playbooks
 - ▶ Kostas Poullos (Sphinx)



Questionnaire



advan**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs



► Post your questions into the chat



Training Webinar Series

1 - Building Cybersecurity Awareness and Defense Foundations for SMEs

 2025-11-26  10:00 – 11:30 a.m. CET

2 - Advanced Threat Detection and Privacy Protection for SMEs

 2025-12-03  10:00 – 11:30 a.m. CET

3 - Immersive and Gamified Cybersecurity Practices for SMEs

 2026-01-19  10:00 – 11:30 a.m. CET

Mastering the Tools of the NERO Marketplace

 2026-01-26  10:00 – 11:30 a.m. CET

 nerocybersecurity.eu/events

Follow us & Stay tuned for the next webinars!



company/nero-cybersecurity



@NEROcybersec



@NEROcybersec



communities/NEROcybersec



nerocybersecurity.eu



advan**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs



adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

Thank you for joining today!

Questionnaire



adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs





advaNced cybErsecurity
awaReness ecOsysteem for SMEs

Cyber Ranges Training and Exercises : Anti-Phishing Focus

Wissam Mallouli
Montimage, France



montimage

Training Objectives

By the end of this session, SMEs will be able to:

- ▶ **Recognize phishing** and social engineering attempts in everyday email communications
- ▶ Identify concrete **warning signs** across email elements (sender, content, timing, attachments, links)
- ▶ Understand common **phishing techniques** and attack types used to target SMEs
- ▶ Make informed **decisions and react** appropriately when facing suspicious emails

Reduce the risk of successful phishing attacks by strengthening human cyber-resilience within SMEs.

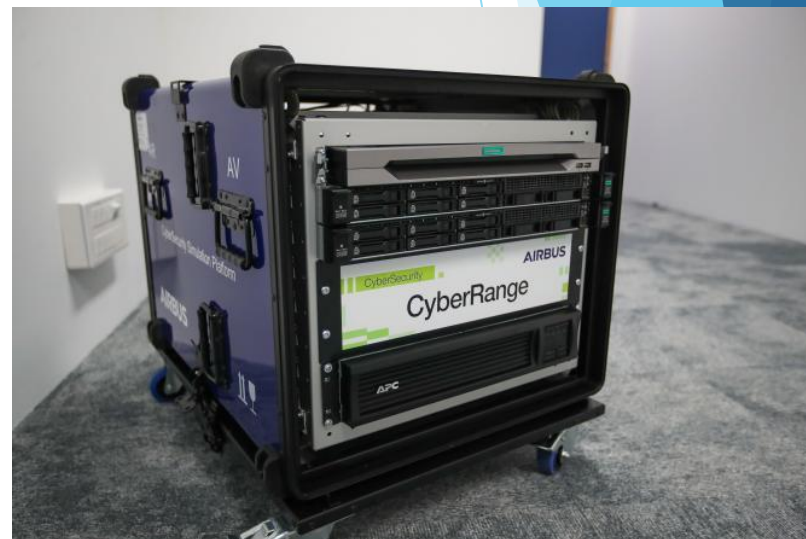


adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

Cyber Ranges Training

What is a Cyber Range?

- ▶ Cyber ranges are **closed** physical/virtual environments used for training about Cybersecurity.
 - ▶ It can emulate a **controlled, realistic, and safe environment** and provide tools that help strengthen the stability, security and performance of cyber infrastructures and IT systems.
- ▶ Cyber ranges play a crucial role in developing **cyber-resilience**. They allow organizations to simulate real-world attacks, assess their defense mechanisms and identify weaknesses.
 - ▶ This proactive approach helps in preparing teams for actual cyber incidents.

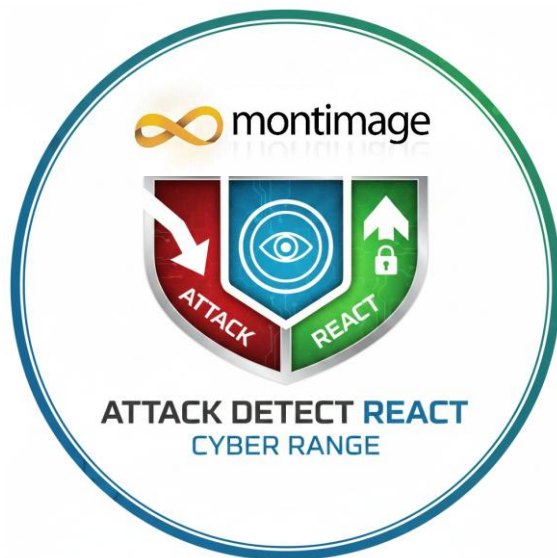


Cyber ranges allow people to *learn by doing* without real-world risk.

Montimage Cyber ranges



advanNced cybErsecurity
awaReness ecOsysteem for SMEs



Learn about attack generation,
detection and countermeasures



Learn about Email Phishing
Identification



adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

Email Phishing Training

What is phishing ?

- ▶ **Definition :** A form of **social engineering** used to trick people into revealing sensitive information or clicking malicious links and download malware.

- ▶ **Types of Phishing Attacks**



Email Phishing

Deceptive emails with malicious links



Smishing

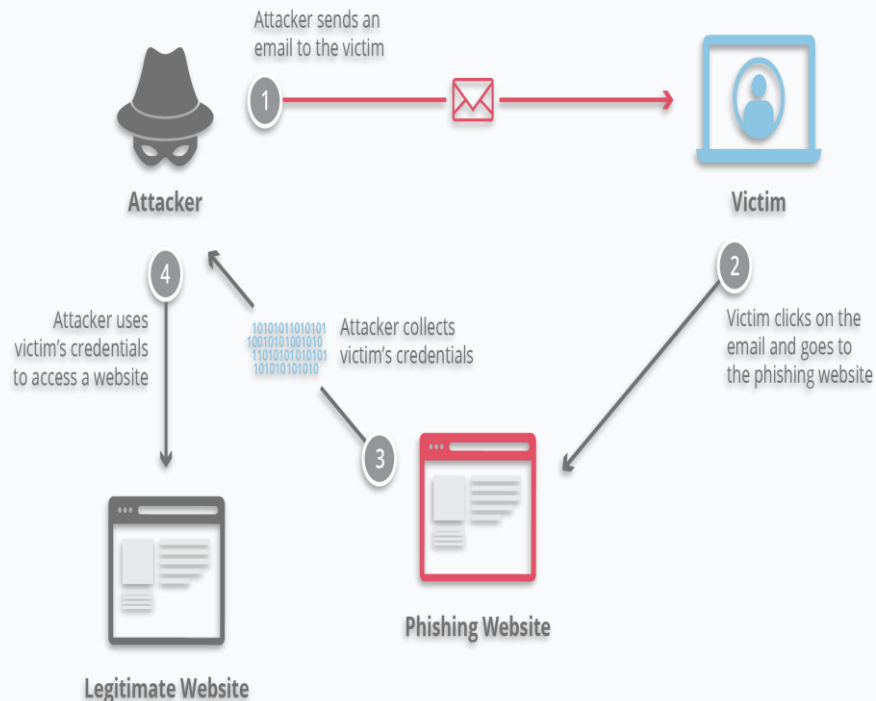
Phishing via text messages



Vishing

Voice phishing over phone calls

Example of Phishing Email



Impact on European SMEs

Based on ENISA's comprehensive study of European SMEs:

60%
of intrusions

Phishing attacks are the #1 entry point for cybercriminals

85%
of SMEs

Agree cybersecurity issues would have a serious
detrimental impact on their business

57%
of SMEs

Would go out of business as a direct result of a
successful cyberattack

SME Cyber Breach Reality

Percentage of data breaches
involving small business victims

Small business victims

43%



Why Phishing is Successful



Urgency



Fear



Distraction

80+ % **AI-supported phishing** now represents the majority of social engineering activity

Phishing-as-a-Service (PhaaS)



Industrialized platforms enable attackers of all skill levels to launch complex campaigns

How Security Awareness Training Protects Organizations from Phishing Attacks



Understanding Phishing Tactics:

Teaches employees to identify phishing techniques and red flags.



Real-World Simulations:

Provides hands-on practice with phishing scenarios.



Regular Updates:

Keeps training current with the latest phishing trends.



Interactive Learning:

Engages employees with quizzes and activities.



Management Involvement:

Ensures leadership supports security initiatives.



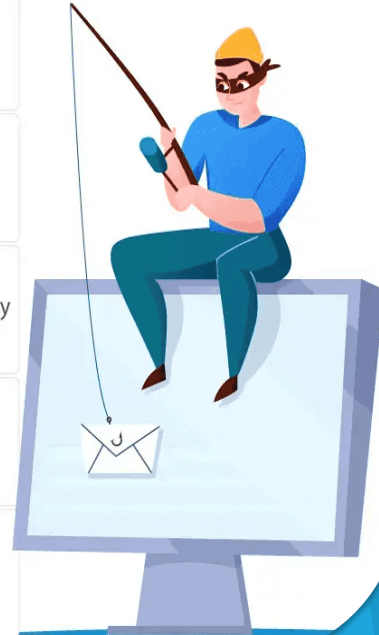
Continuous Assessment:

Improves training through feedback and metrics.



Reporting Procedures:

Trains employees to report suspected phishing quickly.



Consequences of Phishing Attacks



advanced cybersecurity
awareness ecosystem for SMEs

When someone clicks a malicious link or opens an infected file:



Credential Theft

Attackers gain access to company accounts and sensitive data



Ransomware Attacks

Malware encrypts systems, demanding payment for restoration



Business Email Compromise

Attackers hijack inboxes to scam clients and partners



Financial Loss

Direct costs and lost revenue



Reputation Damage

Loss of customer trust

WHAT ARE THE RISKS OF A PHISHING ATTACK?



Business Disruption



Financial Losses



Data Breaches



Government Fines



Degraded Reputation



Loss of Intellectual Property

Raising Awareness - People

Building human resilience through strategic awareness initiatives:



Security Awareness Training

Ongoing education, not once-a-year exercise



Phishing Simulations

Controlled campaigns to test and educate staff



Security Culture

Make security part of everyday conversation



Encourage Reporting

Create safe environment for incident reporting

How Can Phishing Scams Be
Prevented with Effective
Security Awareness Training?



Raising Awareness - Processes

Implementing technical safeguards to prevent and respond to attacks



Email Protection

SPF, DKIM, DMARC - verify senders and block spoofing



Multi-Factor Authentication

Add verification layers - critical for protecting accounts



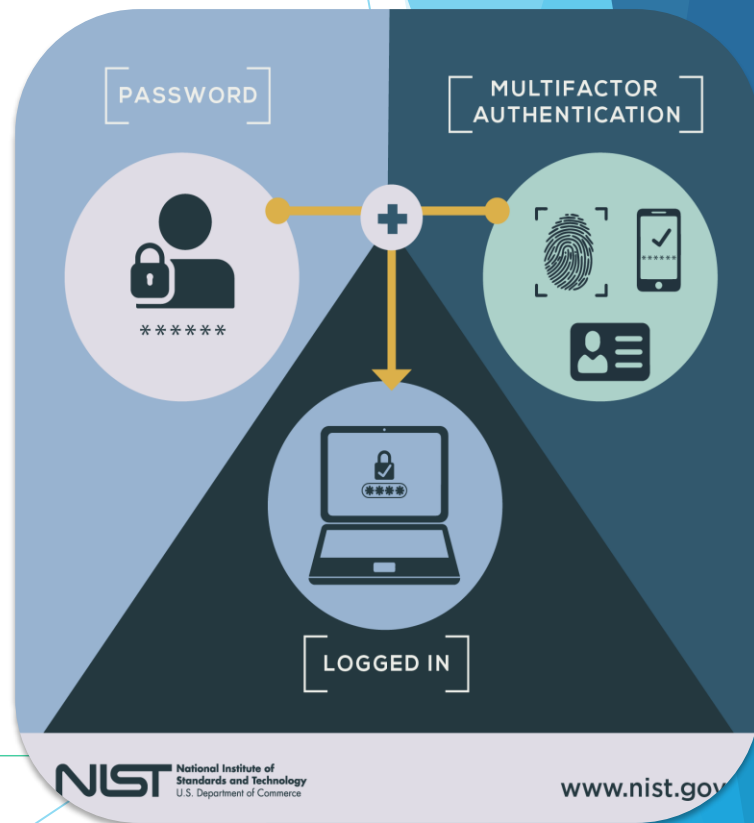
Web Filtering

Block known malicious websites and phishing domains



Incident Response Planning

Define and practice response procedures for quick containment



ENISA Recommendations for SMEs



advan**N**ced cybe**R**security
awa**R**eness eco**S**ystem for SMEs

ENISA's three-pillar approach to comprehensive cybersecurity



People

Training • Employee buy-in • Policies • Third-party management



Processes

Audits • Incident planning • Passwords • Software patches
• Data protection



Technical

Network security • Anti-virus • Encryption • Security monitoring
• Backups

Defense in Depth

Phishing attacks: Defending your organisation

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.



LAYER 1

Make it difficult for attackers to reach users.



Implement anti-spoofing controls to stop your email addresses being a resource for attackers.



Consider what information is available to attackers on your website and social media and help your users do the same



Filter or block incoming phishing emails.

LAYER 2

Help users identify and report suspected phishing emails.



Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.



Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.



Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3

Protect your organisation from the effects of undetected phishing emails.



Protect your accounts: make authentication more resistant to phishing (such as setting up MFA) and ensure authorisation only gives privileges to people who need them.



Protect users from malicious websites by using a proxy services and an up-to-date browser.



Protect your devices from malware.

LAYER 4

Respond to incidents quickly.



Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.



Detect incidents quickly by encouraging users to report any suspicious activity.







adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

The Montimage Email Phishing Platform : Training

The Montimage Email Phishing Training

- ▶ Free Training : <https://pdtp.montimage.eu/>
- ▶ 📊 4-Level Training System - Beginner to expert (0-600+ points)
- ▶ 🏁 Marathon Challenges - 10-min timed competitions
- ▶ 🤖 AI-Powered Feedback - Instant scoring & explanations
- ▶ 🎮 Gamification - 18 badges, 6 certificates, leaderboards



Level	Points	Task
 Level 0: Beginner	0-100	Classify: Phishing or Legitimate
 Level 1: Intermediate	100-300	Identify suspicious elements
 Level 2: Advanced	300-600	Explain why elements are suspicious
 Level 3: Expert	600+	Classify attack type + risk level (1-5)



[← Back to Challenges](#)

CyberSuite Hackathon 10/2025

Draft

Montimage Public EN

About This Challenge

CyberSuite Hackathon 10/2025

Challenge Details

Duration

10 minutes

Language

English

Visibility

Public

Created By

super.admin@montimage.eu

Emails

20 emails

Gameplay Mode

Level 0

Participants

1

Participation

✓ You're registered!

Waiting for challenge to start...

Your Progress

Status

Registered ✓

Score

0 / 20 pts

Phishing Detection Training

AI-Enhanced Phishing Awareness Training Platform helping you identify and prevent phishing attacks.

Developed by [Montimage](#)

Quick Links

[Dashboard](#)

[Start Training](#)

[Challenges](#)

[Leaderboard](#)

[Certificates](#)

Resources

[Help Center](#)

[GEIGER Project](#)

[CyberSuite Project](#)

[NERO Project](#)

Legal

[Privacy Policy](#)

[Data Usage](#)

[About Montimage](#)

Key Takeaways



Phishing is the #1 threat to European SMEs



People are your best defense line



Implement MFA on all accounts



Have an incident response plan

Start Building Your Defense Today!

Take Action Now

1

Train Your Team

Start awareness training this month

2

Enable MFA

Protect email and financial systems

3

Secure Email

Implement SPF, DKIM, DMARC

4

Run Simulations

Test and improve employee readiness



adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

Thank you!



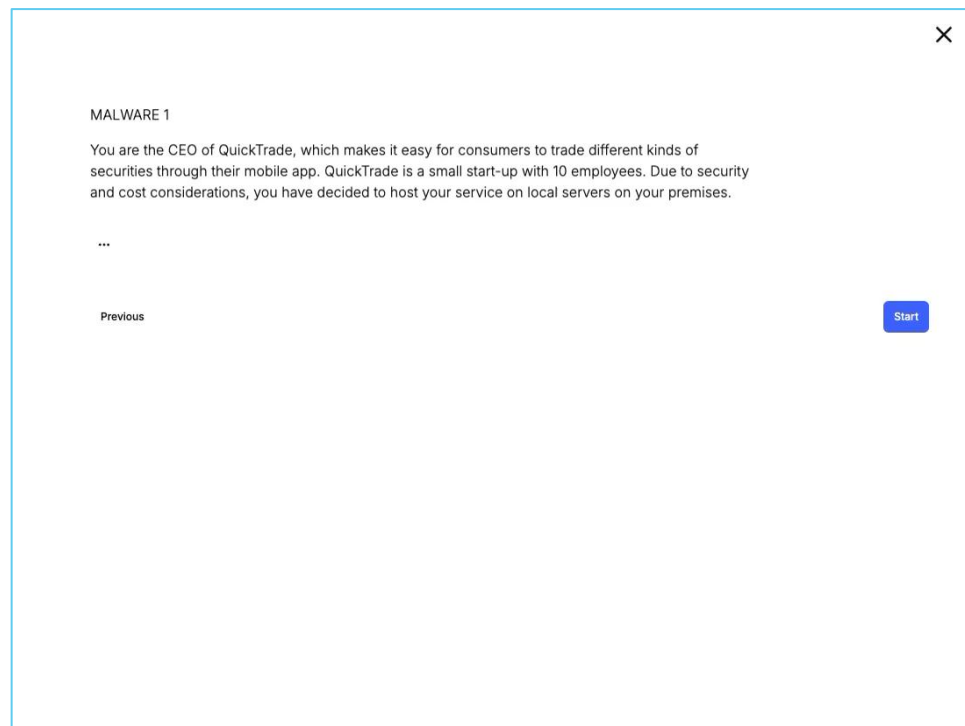
adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

Scenario-based Cybersecurity Training

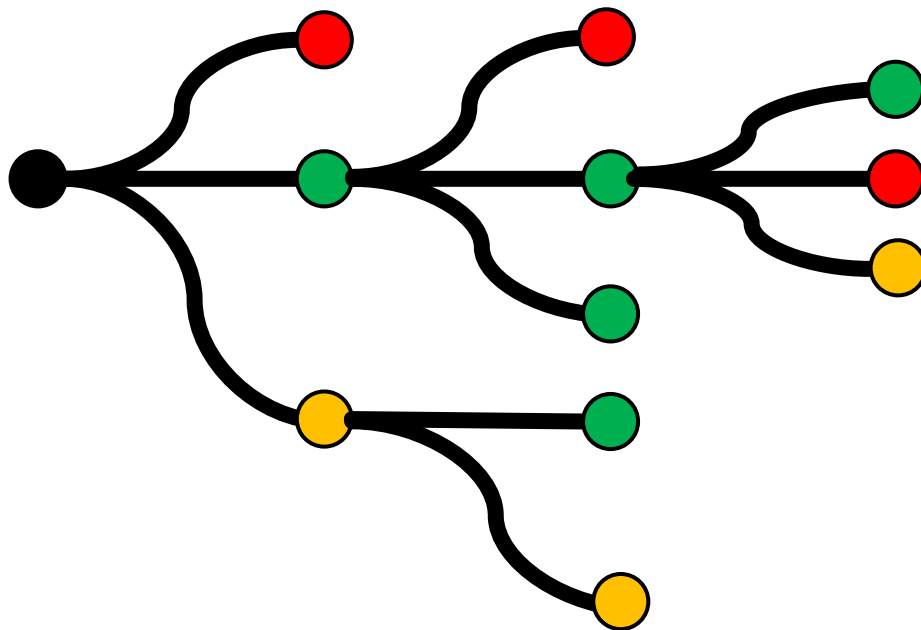
via KIOKU

Ole Höfener

Play Scenarios – Demo



Play Scenarios – Tree



Register



Healthcare



Finance



Logistics

Register



Healthcare



Finance



Logistics

Sign up

It's quick and easy

 Pilot: NERO Training Webinar Series — Healthcare

Name

Last Name

Email

Password



Cybersecurity



The module is the area that you want to learn

Healthcare




The specific field where you work.

IT



The role you have in your company

By registering to KIOKU, you agree to our [Terms](#) and [Privacy Policy](#)

Next 

Pilot page



Healthcare



Finance



Logistics



NERO TRAINING WEBINAR SERIES — HEALTHCARE

Welcome to the scenario-based training as part of the NERO training webinar series (webinar 3). Below, you will find a selection of training scenarios across various topics specifically tailored toward the healthcare sector.

January 14, 2026 - January 20, 2026

ASSIGNED SCENARIOS

DATA BREACH LEVEL 1



GDPR LEVEL 1



MALWARE LEVEL 1



PHISHING LEVEL 1



MALWARE LEVEL 2



PILOT PROGRESS



Scenarios completed 4

Total scenarios 6

Thank you for participating!

kioku.se

→ Join our waitlist



advaNced cybErsecurity
awaReness ecOsysteem for SMEs

Incident response using CACAO playbooks

Kostas Poullos
Sphynx, Greece

Training Objectives

By the end of this session, SMEs will be able to:

- ▶ Understand the **value of CACAO playbooks** in Incident Response
- ▶ Recognise the **structure of a CACAO playbook**
- ▶ **Create a CACAO playbook** using the Sphinx IR Editor
- ▶ View the **execution of a CACAO playbook** in real-time

CACAO turns incident response from documentation into automation.

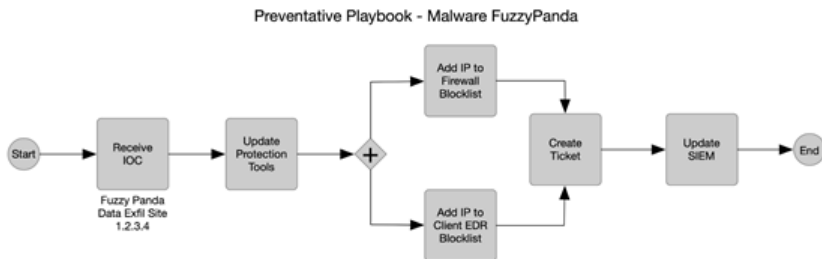


adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

Incident response using CACAO playbooks

Incident Response & Playbooks

- ▶ An organized approach to addressing and managing the aftermath of a security breach
- ▶ The mitigation process is documented with files, called “playbooks”, usually using **free text**
- ▶ Playbooks might provide logic graphs containing nodes that roughly map to executable actions
- ▶ IR playbooks provided by security agencies and organizations are **not executable workflows**
- ▶ Industry solutions provide executable playbooks that **are not free or interoperable** between tools

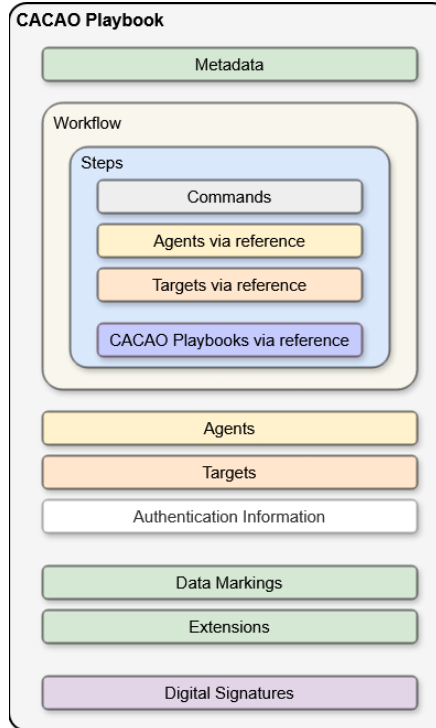


Collaborative Automated Course of Action Operations (CACAO) Playbooks

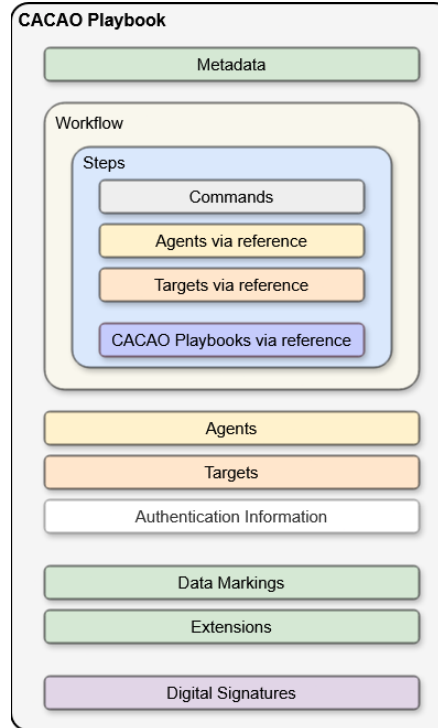
- ▶ A modern standard that strictly defines the elements needed to implement incident response playbooks, first drafted in 2021
- ▶ CACAO playbooks are **structured** JSON objects that allow the **definition** of **executable workflows**
- ▶ Offer a variety of **logic elements** such as loops, conditions, parallel execution, etc.
- ▶ Each playbook can also provide **metadata and information** related to the incident to be handled
- ▶ Each CACAO engine is responsible for parsing the playbooks and provide workflow execution
- ▶ CACAO playbooks address the **sharing and interoperability problem**

CACAO Playbook Structure

- ▶ A CACAO playbook is:
Metadata + Workflow + Execution Context.



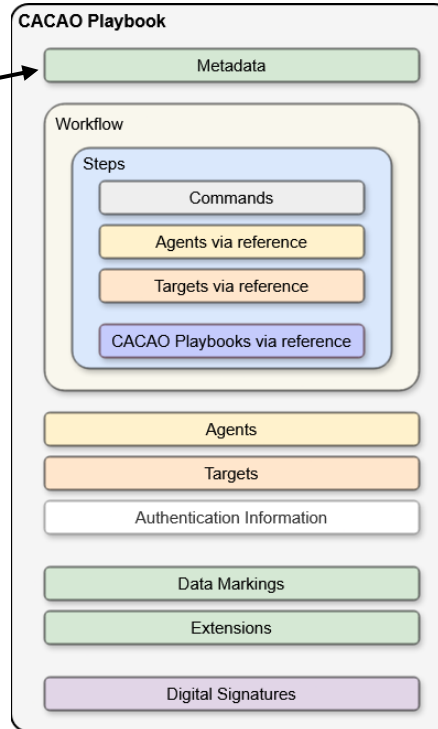
CACAO Playbook Structure



- ▶ CACAO playbooks are encoded as JSON objects
- ▶ The specification provides strict rules on playbook structure
- ▶ Schema validators ensure correct structure

CACAO Playbook Structure

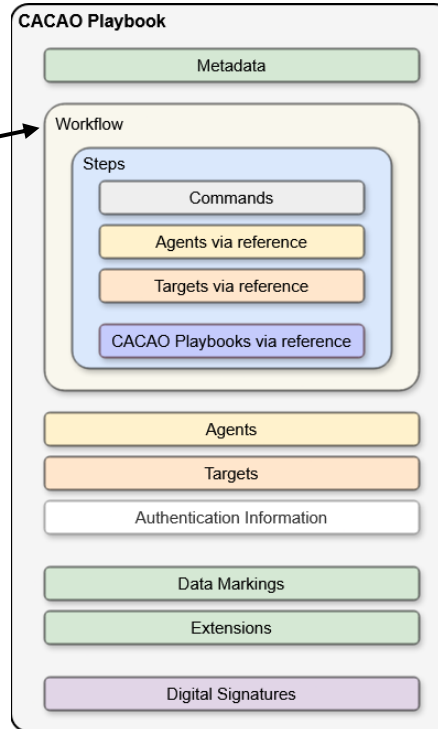
1. Metadata



- ▶ Playbook name and UUID
- ▶ Description
- ▶ Timestamps
- ▶ Priority, severity, impact
- ▶ Labels
- ▶ Signatures
- ▶ etc.

CACAO Playbook Structure

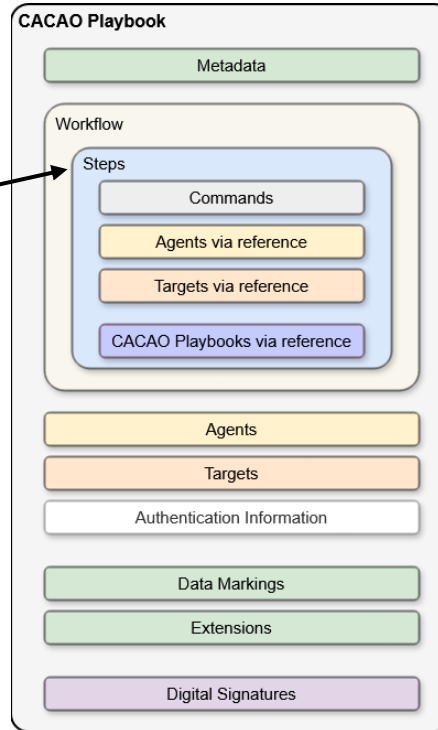
1. Metadata
2. Workflow



- ▶ List of all executable playbook steps
- ▶ Each workflow provides a single entry-point
- ▶ Steps are linked to each other to create the playbook's logic

CACAO Playbook Structure

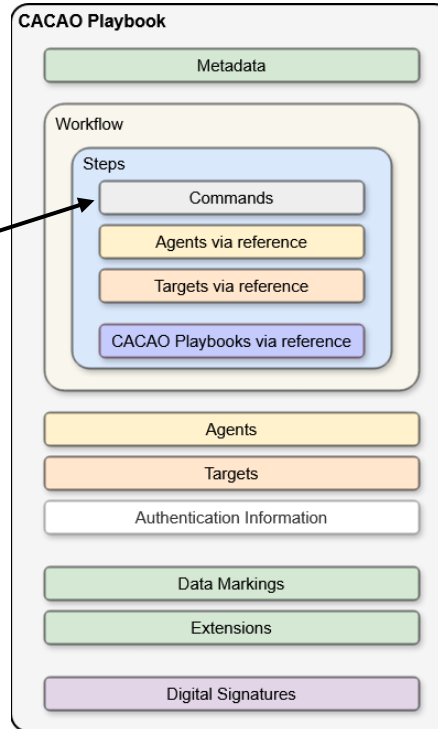
1. Metadata
2. Workflow
3. Steps



- ▶ Each workflow *step* is encoded as a JSON object
- ▶ Provide various fields such as name, delay, timeout, commands, etc.
- ▶ Steps that execute *commands* reference *agents* and *targets*

CACAO Playbook Structure

1. Metadata
2. Workflow
3. Steps
4. Commands



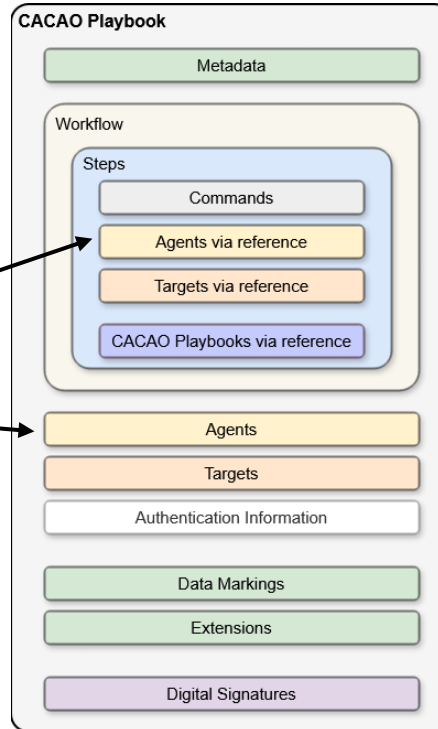
▶ A list of one or more *commands* to be executed by each step

▶ Command Types:

- ▶ Bash
- ▶ SSH
- ▶ HTTP-API
- ▶ Manual
- ▶ etc.

CACAO Playbook Structure

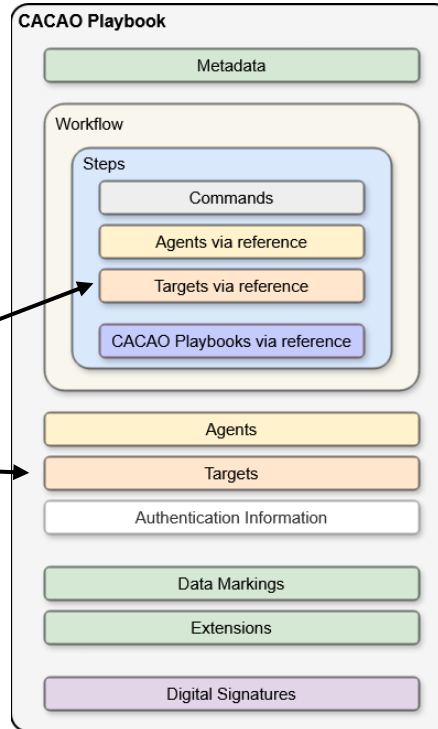
1. Metadata
2. Workflow
3. Steps
4. Commands
5. Agents



- ▶ Agents are the entities that execute *commands*
- ▶ One or more agents may be available for executing the same command (e.g., software system and human operator)
- ▶ Agents can involve either manual or automated processing

CACAO Playbook Structure

1. Metadata
2. Workflow
3. Steps
4. Commands
5. Agents
6. Targets



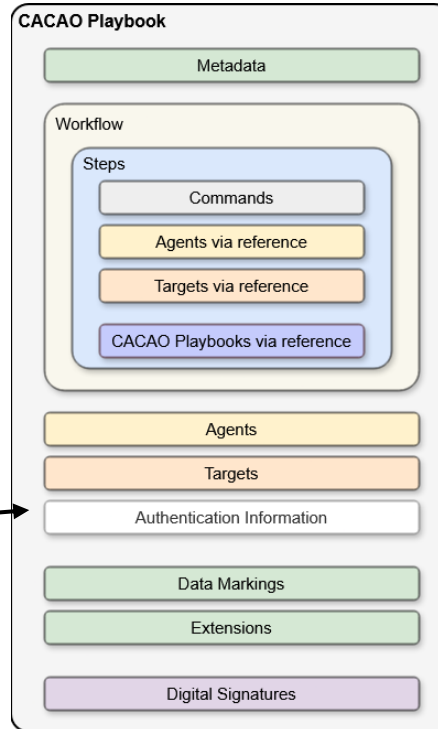
▶ Each *command* can be executed by *agents* on or against one or more *targets*

▶ Types of targets:

- ▶ Linux or windows hosts
- ▶ Tools and software
- ▶ REST endpoints
- ▶ Etc.

CACAO Playbook Structure

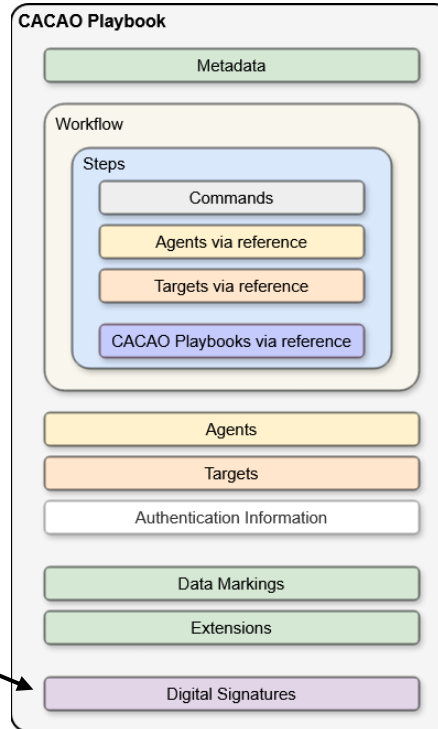
1. Metadata
2. Workflow
3. Steps
4. Commands
5. Agents
6. Targets
7. Authentication Info



- ▶ The authentication info required by an agent A to execute command C on target T
- ▶ May contain user credentials, tokens, API keys, etc.

CACAO Playbook Structure

1. Metadata
2. Workflow
3. Steps
4. Commands
5. Agents
6. Targets
7. Authentication Info
8. Digital Signatures



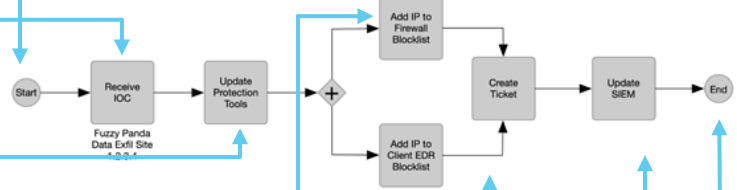
► Playbooks can be digitally signed to protect their validity and designate the creator

CACAO Playbook workflow Example

- Workflow
- Steps

```
{
  "workflow": {
    "start--7269bda2-e651-44d3-9fe5-aa7e6848b93": {
      "type": "start",
      "on_completion": "action--a13c8450-2bd1-4a2b-9241-cf4f7e9f48cb"
    },
    "action--a13c8450-2bd1-4a2b-9241-cf4f7e9f48cb": {
      "type": "action",
      "name": "Receive IOC",
      "description": "Get FuzzyPanda Data Exfil Site IP Address of 1.2.3.4",
      "on_completion": "parallel--054c7e3a-20e7-4df4-a95f-6c6e401c65c3",
      "commands": [
        {
          "type": "manual",
          "command": "Get IOC from threat feed"
        }
      ]
    },
    "parallel--054c7e3a-20e7-4df4-a95f-6c6e401c65c3": {
      "type": "parallel",
      "name": "Update Protection Tools",
      "description": "Update the firewall and client EDR in parallel",
      "next_steps": [
        "action--8c46cab0-46a3-48f4-b4bb-9643dcfaf642",
        "action--3d39f808-e22c-4dd4-996f-61f2d022112c"
      ]
    },
    "action--8c46cab0-46a3-48f4-b4bb-9643dcfaf642": {
      "type": "action",
      "name": "Add IP to Firewall Blocklist",
      "description": "Add the IP address of the ata exfil site to the firewall",
      "on_completion": "action--d5780323-5107-4cd0-bac4-6553c9d90c8e",
      "commands": [
        {
          "type": "manual",
          "command": "Add 1.2.3.4 to the firewall blocking policy"
        }
      ]
    },
    "action--3d39f808-e22c-4dd4-996f-61f2d022112c": {
      "type": "action",
      "name": "Add IP to Client EDR Blocklist",
      "description": "Add the IP address of the data exfil site to the client EDR",
      "on_completion": "action--d5780323-5107-4cd0-bac4-6553c9d90c8e",
      "commands": [
        {
          "type": "manual",
          "command": "Open EDR console and add 1.2.3.4 to the blocking policy"
        }
      ]
    },
    "action--d5780323-5107-4cd0-bac4-6553c9d90c8e": {
      "type": "action",
      "name": "Create Ticket",
      "description": "This step will create a ticket for this issue",
      "on_completion": "action--33dc512c-263d-4f8a-a07d-cfe9f66ed26c",
      "commands": [
        {
          "type": "manual",
          "command": "Create a ticket with the details of what was done"
        }
      ]
    },
    "action--33dc512c-263d-4f8a-a07d-cfe9f66ed26c": {
      "type": "action",
      "name": "Update SIEM",
      "description": "Update SIEM to look for traffic attempts to data exfil site",
      "on_completion": "end--6d43fbf3-54b3-432a-978b-e2b96647b786",
      "commands": [
        {
          "type": "manual",
          "command": "Open SIEM solution and add rule to look for 1.2.3.4"
        }
      ]
    },
    "end--6d43fbf3-54b3-432a-978b-e2b96647b786": {
      "type": "end"
    }
  }
}
```

Preventative Playbook - Malware FuzzyPanda

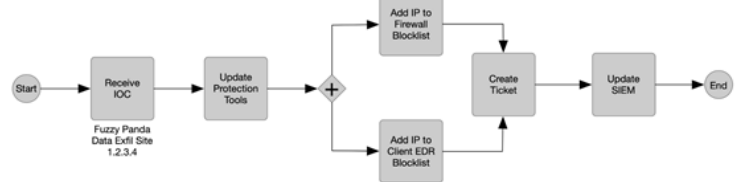


CACAO Playbook workflow Example

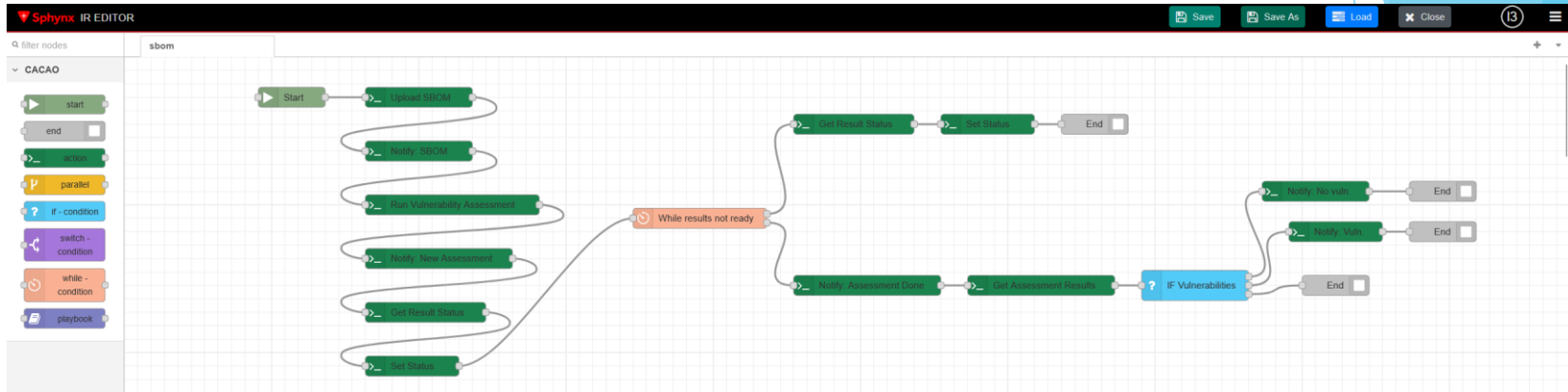
- Workflow
- Steps
- Commands

```
{
  "workflow": {
    "start": "7269bda2-e651-44d3-9fe5-aa7e6848b93": {
      "type": "start",
      "on_completion": "action--a13c8450-2bd1-4a2b-9241-cf4f7e9f48cb"
    },
    "action--a13c8450-2bd1-4a2b-9241-cf4f7e9f48cb": {
      "type": "action",
      "name": "Receive IOC",
      "description": "Get FuzzyPanda Data Exfil Site IP Address of 1.2.3.4",
      "on_completion": "parallel--054c7e3a-20e7-4df4-a95f-6c6e401c65c3",
      "commands": [
        {
          "type": "manual",
          "command": "Get IOC from threat feed"
        }
      ]
    },
    "parallel--054c7e3a-20e7-4df4-a95f-6c6e401c65c3": {
      "type": "parallel",
      "name": "Update Protection Tools",
      "description": "Update the firewall and client EDR in parallel",
      "next_steps": [
        {
          "action": "8c46cab0-46a3-48f4-b4bb-9643dcfaf642": "",
          "action": "3d39f808-e22c-4d44-996f-61f2d022112c": ""
        }
      ]
    },
    "action--8c46cab0-46a3-48f4-b4bb-9643dcfaf642": {
      "type": "action",
      "name": "Add IP to Firewall Blocklist",
      "description": "Add the IP address of the ata exfil site to the firewall",
      "on_completion": "action--d5780323-5107-4cd0-bac4-6553c9d90c8e",
      "commands": [
        {
          "type": "manual",
          "command": "Add 1.2.3.4 to the firewall blocking policy"
        }
      ]
    },
    "action--3d39f808-e22c-4d44-996f-61f2d022112c": {
      "type": "action",
      "name": "Add IP to Client EDR Blocklist",
      "description": "Add the IP address of the data exfil site to the client EDR",
      "on_completion": "action--d5780323-5107-4cd0-bac4-6553c9d90c8e",
      "commands": [
        {
          "type": "manual",
          "command": "Open EDR console and add 1.2.3.4 to the blocking policy"
        }
      ]
    },
    "action--d5780323-5107-4cd0-bac4-6553c9d90c8e": {
      "type": "action",
      "name": "Create Ticket",
      "description": "This step will create a ticket for this issue",
      "on_completion": "action--33dc512c-263d-4f8a-a07d-cfe9f66ed26c",
      "commands": [
        {
          "type": "manual",
          "command": "Create a ticket with the details of what was done"
        }
      ]
    },
    "action--33dc512c-263d-4f8a-a07d-cfe9f66ed26c": {
      "type": "action",
      "name": "Update SIEM",
      "description": "Update SIEM to look for traffic attempts to data exfil site",
      "on_completion": "end--6d43fbf3-54b3-432a-978b-e2b96647b786",
      "commands": [
        {
          "type": "manual",
          "command": "Open SIEM solution and add rule to look for 1.2.3.4"
        }
      ]
    },
    "end--6d43fbf3-54b3-432a-978b-e2b96647b786": {
      "type": "end"
    }
  }
}
```

Preventative Playbook - Malware FuzzyPanda



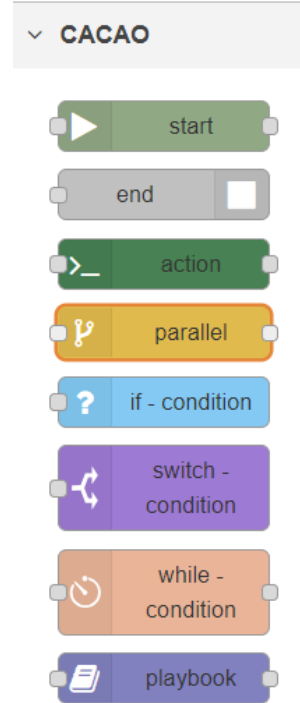
CACAO Playbook Editor



- Provides CACAO workflow steps as graph nodes
- Enables graphical, drag-and-drop based playbook design
- Each step provides dedicated configuration editor
- Playbooks are exported in CACAO v2 format
- Imported playbooks are automatically visualized as editable graphs

CACAO Playbook Editor: Nodes

- ▶ 8 different types of workflow nodes
- ▶ “**start**” and “**end**” nodes are mandatory for each playbook
- ▶ **action**: Executes playbook actions
- ▶ **parallel**: Executes node branches in parallel
- ▶ **if**: Performs comparisons like an “if” statement
- ▶ **switch**: Performs switch operations on a CACAO variable
- ▶ **while**: Performs loops while its condition is “true”
- ▶ **playbook**: Triggers the execution of other playbooks



CACAO Playbook Editor: Variables

- ▶ The variables are defined and managed within the playbook's "start" step.
- ▶ All variable names must be wrapped in underscores (e.g. __url__ or __port__)
- ▶ How to Manage:
 - ▶ **Edit:** Select the variable from the "Variable list", change the "Variable Value", and click "Edit Variable".
 - ▶ **Add:** Type a new name and value into the form fields and click "Add Variable".
- ▶ Accessing Values: To use a variable inside a command or message, use the syntax: __variable_name__:value
- ▶ Data types: multiple types are supported including String, Integer and IPv4 Addresses.

The screenshot shows the 'Edit start node' dialog box in the CACAO Playbook Editor. The 'Variables' section is active, displaying a form for editing a variable. The 'Variable Name' field contains '__demoVar__', the 'Variable Value' field contains '1', and the 'Variable Type' dropdown is set to 'INTEGER'. Below the form are three buttons: 'Add Variable', 'Edit Variable', and 'Delete Variable'. At the bottom, the 'Variables list' shows two variables: '__demoVar__ (integer): 1' (which is selected) and '__demoVar2__ (string): text'.

Edit start node

Delete Cancel Done

Properties

Variables

Variable form

Variable Name: __demoVar__

Variable Value: 1

Variable Type: INTEGER

Add Variable Edit Variable Delete Variable

Variables list

- __demoVar__ (integer): 1
- __demoVar2__ (string): text

CACAO Playbook Editor: Action Step

- ▶ Action steps contain a list of commands executed in sequence
- ▶ Command types:
 - ▶ **Bash:** Arbitrary shell commands executed locally on the engine
 - ▶ **Manual:** Sends notifications to human operators via Email or Slack
 - ▶ **SSH:** Shell commands that are executed remotely on a specified target
 - ▶ **HTTP-API:** POST/GET/PATCH/DELETE requests for interacting with RESTful APIs

The screenshot shows the 'Edit action node' dialog box in the CACAO Playbook Editor. The dialog has a title bar with 'Delete', 'Cancel', and 'Done' buttons. Below the title bar is a 'Properties' section with an ID field containing '74794168a35d0c39'. The 'Step Metadata' section includes a 'Name' field with 'Upload SBOM', a 'Delay' field with '1000' milliseconds, and a 'Timeout' field with '5000' milliseconds. The 'Outputs' section has a 'Completion' dropdown set to 'on_completion'. The 'Targets' section shows '1 selected' target with a dropdown arrow. Below this, the 'Selected Targets' section displays a JSON object:

```
{ "id": "http-api-24b19dfd-19b9-414e-88ec-d83479b97841", "targetData": { "type": "http-api", "name": "CORE", "address": { "url": { "http://core-platform"}, "port": "8080" } } }
```

. The 'Commands' section is a form with 'Command Type' set to 'http-api', 'HTTP Method' set to 'POST', 'Path' set to '/core-platform/assets/import-via-sbom/organisations/1/projects/', 'REST headers' set to

```
{ "Content-Type": "multipart/form-data", "x-classification-le ... }
```

, and 'REST body' set to

```
{ "file": "file[0]-" }
```

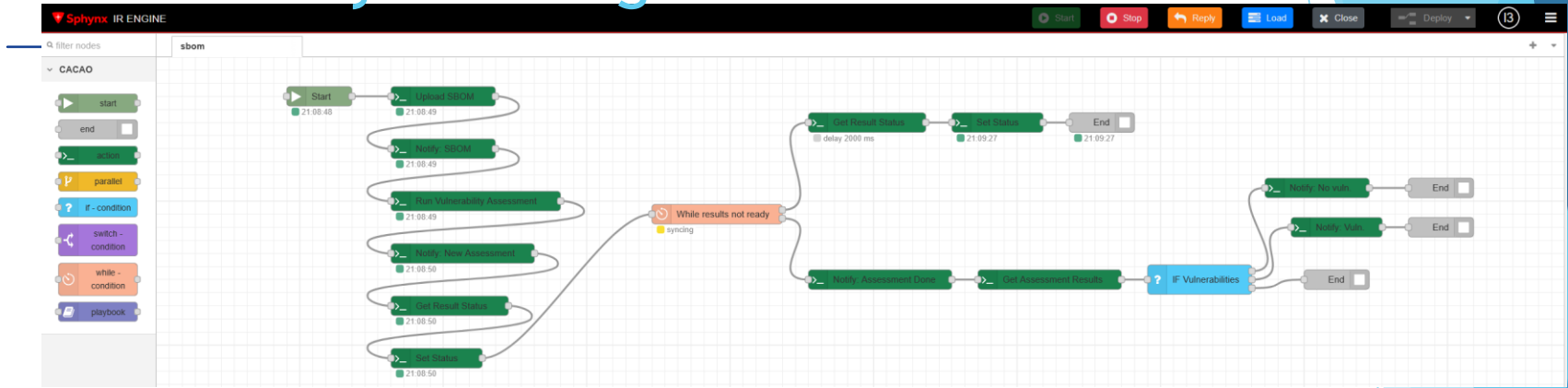
. At the bottom, there is a checkbox labeled 'Enabled' which is currently checked.

CACAO Playbook Editor: Switch Step

- ▶ The Switch step evaluates a CACAO variable and routes the flow to the first matching branch
- ▶ Configuration:
 - ▶ **Switch Variable:** The data to be evaluated
 - ▶ **Cases:** The specific values to look for
- ▶ Managing Cases:
 - ▶ **Adding:** Cases can be created by clicking the “+ add” button at the bottom of the list
 - ▶ **Reordering:** Cases can be dragged and dropped to change their priority
 - ▶ **Visual Impact:** Reordering cases in the list will automatically reorder their connection links on the graph
- ▶ **Default path:** If no match is found, the flow follows the “**default**” branch

The screenshot shows the 'Edit switch-condition node' dialog box. It has a title bar with 'Delete', 'Cancel', and 'Done' buttons. The 'Properties' section shows the ID '9e268e3df4a030ed'. The 'Step Metadata' section includes a 'Name' field with 'Switch Step' and a 'Delay' field with '2000' milliseconds. The 'Outputs' section has a 'Completion' dropdown set to 'on_completion'. The 'Switch' field contains '___inData___value'. The 'Cases' section shows 'Hidden outputs' as '["0":0,"1":1,"2":2,"3":3,"4":4)'. Below this is a list of cases: 'default' (with a '→ default' link), 'INFO' (with a '→ INFO' link and a close button), 'WARN' (with a '→ WARN' link and a close button), and 'ERR' (with a '→ ERR' link and a close button). At the bottom, there is a '+ add' button and a checkbox labeled 'Enabled'.

CACAO Playbook Engine



- Real-time view of playbook execution
- Playbook execution management
- Graphical playbook representation
- Users can provide replies/input to executing playbooks

Takeaways

CACAO enables standardised, executable incident response

Playbooks are shareable and interoperable

Suitable for manual, semi-automated, and fully automated IR

SPHYNX provides end-to-end CACAO support: design → execute → monitor



adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

Thank you!