SIKKERHETS
FESTIVALEN

28-30/08/2023

TLP:CLEAR

From Threat Intelligence to Defense Intelligence with a Cup of CACAO

Vasileios Mavroeidis, PhD
University of Oslo

TLP:CLEAR

Disclaimer: The views and opinions expressed in this presentation are those of the speakers and do not necessarily reflect the views or positions of any entities they represent.

Disclaimer: This presentation incorporates **Traffic Light Protocol (TLP)** Version 2 labels (possibly applicable per slide) to indicate the sharing boundaries to be applied by the recipients of this presentation and **MUST** be strictly followed. Details about FIRST's TLP are available at: https://www.first.org/tlp/.

whoami

Domain: Cybersecurity with a focus on ***Cyber Threat Intelligence*** and ***Security Automation***

Associate Professor @ **University of Oslo**

Lecturer of MC102 Cyber Threat Intelligence @ **Kristiania**

Standards Architect @ **Sekoia.io**

Chairman of **OASIS** Threat Actor Context Standardization Committee

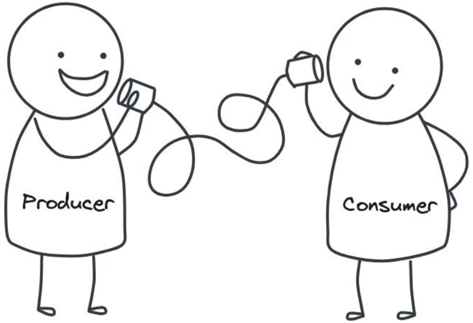
Board of Directors @ **OASIS** SDO

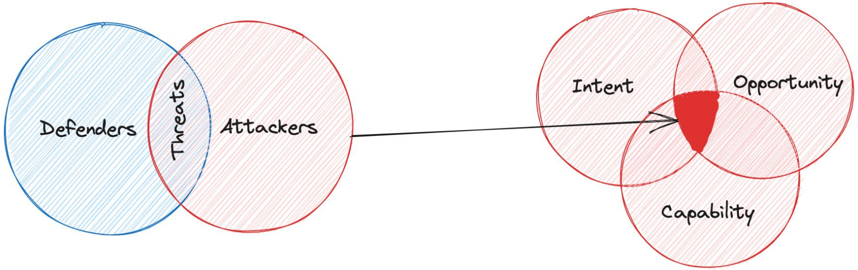
ENISA AHWG on Cyber Threat Landscapes and Security Operations Centres

Cyber Threat Intelligence (CTI) - 101

- Intelligence is the collection, processing, and analysis of information about a competitive entity and its agents, needed by an organization or group for its security and well-being. [FOR578 – Robert M. Lee, 2021]

- Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. [Gartner, 2013]





TLP:CLEAR

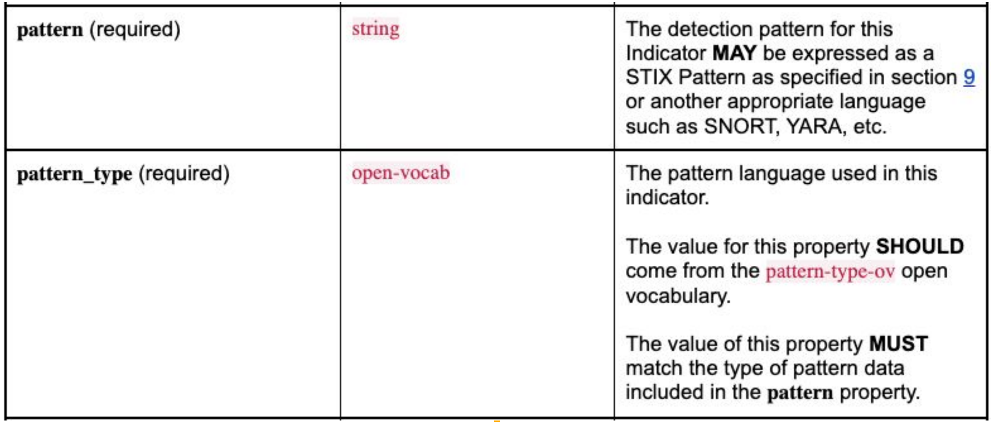
Incident Response & Why We Created CACAO

- **Manual** incident response is cumbersome and slow
- Teams and systems are **siloed** and **isolated**
  - Many different groups inside an organization are part of the response
  - Incident response is not a single action but a series of tasks that require execution by multiple stakeholders and systems
- Searching blog posts for mitigation and remediation steps cannot scale to the present threat landscape. The process is time-consuming, and teams still need to extrapolate this information to bring together a response plan.
- Threat actors, intrusions sets and campaigns are advancing quickly
  - Defenders need to respond in **cyber-relevant time**
  - Defenders need to do for **playbooks** what STIX / TAXII and MISP did for CTI
- There is **no easy way to share** threat response / cybersecurity operations playbooks
  - **Standardization** is key for **Interoperability**

Machine Processable Detection & Response

✓

Detection
(structured content)



pattern (required)	string	The detection pattern for this Indicator **MAY** be expressed as a STIX Pattern as specified in section 9 or another appropriate language such as SNORT, YARA, etc.
pattern_type (required)	open-vocab	The pattern language used in this indicator. The value for this property **SHOULD** come from the pattern-type-ov open vocabulary. The value of this property **MUST** match the type of pattern data included in the **pattern** property.

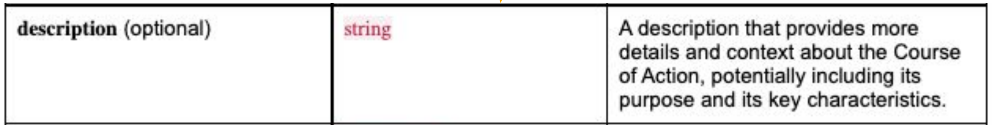
```
"pattern":
"[file:hashes.'md5' =
'd8c00fed6625e5f8d0b8188a5caa
c115']"
```

```
"pattern_type": "stix"
```

Now What?

✗

What steps to take
(unstructured content)



description (optional)	string	A description that provides more details and context about the Course of Action, potentially including its purpose and its key characteristics.

```
"description": "add a packet
filter rule to block outbound
connections to IP 660.10.1.120
and block/clean systems from
d8c00fed6625e5f8d0b8188a5caac115
. . ."
```

TLP:CLEAR

What is a Cybersecurity Playbook?

Cybersecurity playbook is an all-encompassing term referring to structured and principled processes and procedures in the context of cybersecurity that have been **documented** and are aimed to be **reusable**, **repeatable**, and **optimized**.

"All-encompassing" refers to the **agnostic** nature of the term, meaning the playbook's underlying representation format and encoding, operational roles and activities involved and supported, and the level and type of automation applied in its execution.

[Vasileios Mavroeidis 2022]

Benefits from Cybersecurity Playbooks

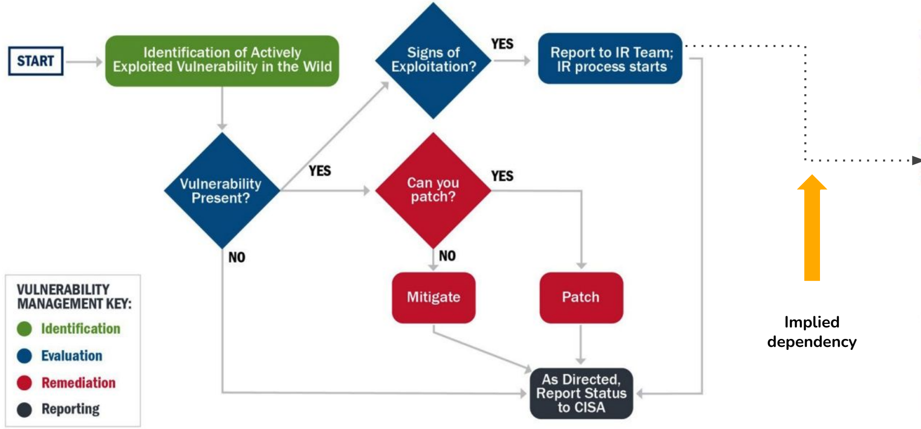
- Increase security operations efficiency
- Increase security operations effectiveness
- Reduce human errors and increase response confidence
- Engage less experienced analysts and support operational role development
- Assist with policy and regulatory compliance
- **Demonstrate a path to automate the process over time**

Example Playbooks

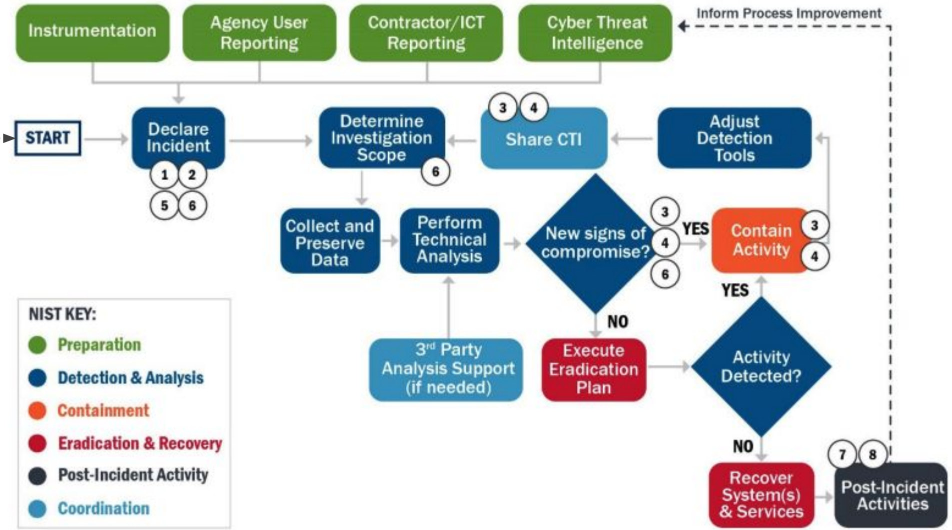
- Static document
- List of tasks with defined sequential order and decision logic (if statements)
- Task assignment
- May provide detailed guidance and best practices through comprehensive documentation

Vulnerability Response Process

Standard vulnerability management programs include phases for identifying, analyzing, remediating, and reporting vulnerabilities. Figure 4 describes the vulnerability response process in terms of standard vulnerability management program phases.


START
Identification of Actively Exploited Vulnerability in the Wild
Vulnerability Present?
YES
NO
Signs of Exploitation?
YES
Report to IR Team; IR process starts
Can you patch?
YES
NO
Mitigate
Patch
As Directed, Report Status to CISA
VULNERABILITY MANAGEMENT KEY:
● Identification
● Evaluation
● Remediation
● Reporting
Implied dependency

Incident Response Process



Source: Cybersecurity Incident & Vulnerability Response Playbooks
Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems
Publication: November 2021
Cybersecurity and Infrastructure Security Agency

TLP:CLEAR

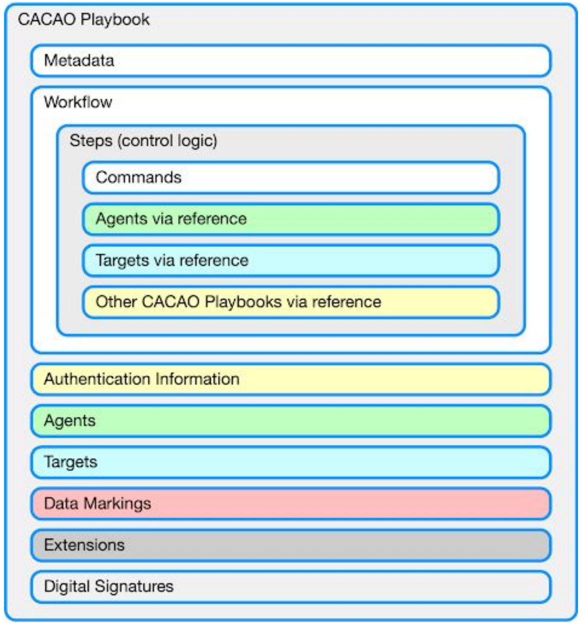
CACAO

Collaborative Automated Course of Action Operations

TLP:CLEAR

CACAO - 101

- A common framework to **create** and **share** cybersecurity playbooks
- CACAO puts the glue between different tasks, tools, people, languages and standards for cyber security operations
- Machine-readable; playbooks are encoded in JSON
- Template and <<tailored-to-your-specific-environment>> playbooks
- Automatable (automate as you go)
- Hybrid playbooks
  - Tasks that are performed automatically and/or manually
- Modular design
  - Object centric
  - Easy to extend
  - Allows to connect playbooks



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

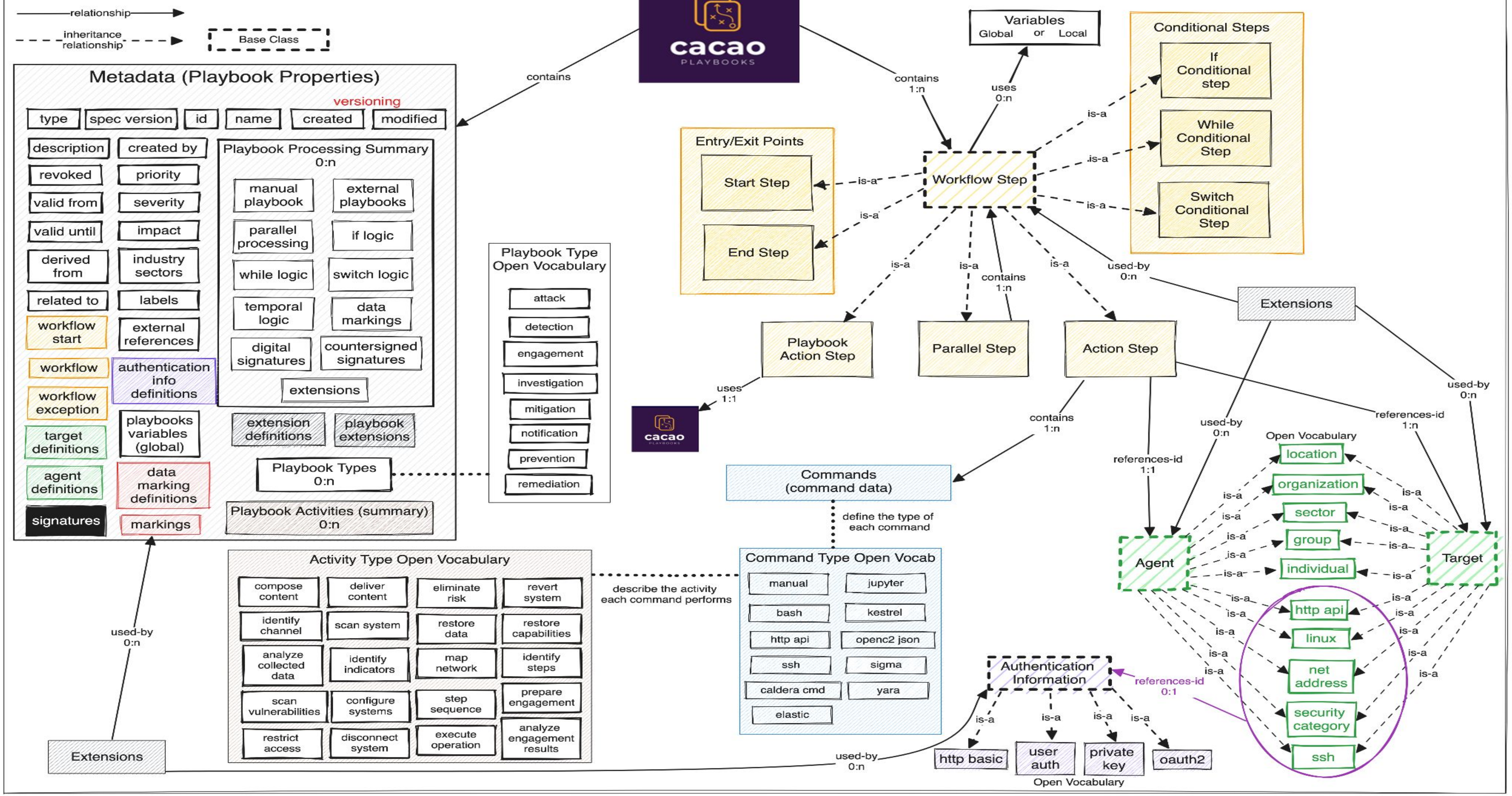
Extensions

Digital Signatures

OASIS OPEN

CACAO (High-Level) Model

TLP:CLEAR



relationship

inheritance relationship

Base Class

cacao PLAYBOOKS

contains

Metadata (Playbook Properties)

versioning

type | spec version | id | name | created | modified

description | created by | revoked | priority | valid from | severity | valid until | impact | derived from | industry sectors | related to | labels | workflow start | external references | workflow | authentication info definitions | workflow exception | playbooks variables (global) | target definitions | agent definitions | data marking definitions | signatures | markings

Playbook Processing Summary 0:n

manual playbook | external playbooks | parallel processing | if logic | while logic | switch logic | temporal logic | data markings | digital signatures | countersigned signatures | extensions

extension definitions | playbook extensions

Playbook Types 0:n

Playbook Activities (summary) 0:n

Playbook Type Open Vocabulary

attack | detection | engagement | investigation | mitigation | notification | prevention | remediation

Activity Type Open Vocabulary

compose content | deliver content | eliminate risk | revert system | identify channel | scan system | restore data | restore capabilities | analyze collected data | identify indicators | map network | identify steps | scan vulnerabilities | configure systems | step sequence | prepare engagement | restrict access | disconnect system | execute operation | analyze engagement results

describe the activity each command performs

Extensions

used-by 0:n

contains 1:n

Variables
Global or Local

uses 0:n

Conditional Steps

If Conditional step | While Conditional Step | Switch Conditional Step

is-a

Entry/Exit Points

Start Step | End Step

Workflow Step

is-a

Playbook Action Step | Parallel Step | Action Step

contains 1:n

uses 1:1

cacao PLAYBOOKS

used-by 0:n

Extensions

contains 1:n

Commands (command data)

define the type of each command

Command Type Open Vocab

manual | jupyter | bash | kestrel | http api | openc2 json | ssh | sigma | caldera cmd | yara | elastic

references-id 1:1

used-by 0:n

references-id 1:n

used-by 0:n

Open Vocabulary

location | organization | sector | group | individual | http api | linux | net address | security category | ssh

Agent | Target

is-a

references-id 0:1

Authentication Information

is-a

http basic | user auth | private key | oauth2

Open Vocabulary

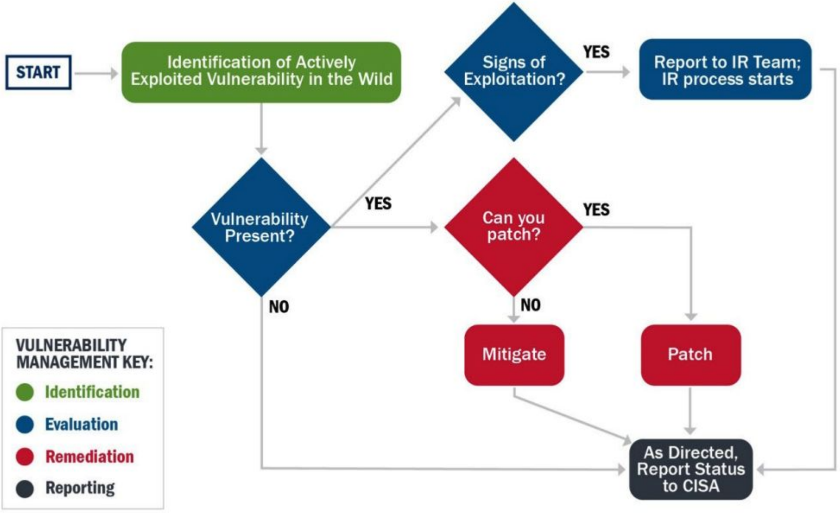
used-by 0:n

TLP:CLEAR

CACAO Playbook

Vulnerability Response Process

Standard vulnerability management programs include phases for identifying, analyzing, remediating, and reporting vulnerabilities. Figure 4 describes the vulnerability response process in terms of standard vulnerability management program phases.



START

Identification of Actively Exploited Vulnerability in the Wild

Vulnerability Present?

YES

NO

Signs of Exploitation?

YES

Report to IR Team; IR process starts

Can you patch?

YES

NO

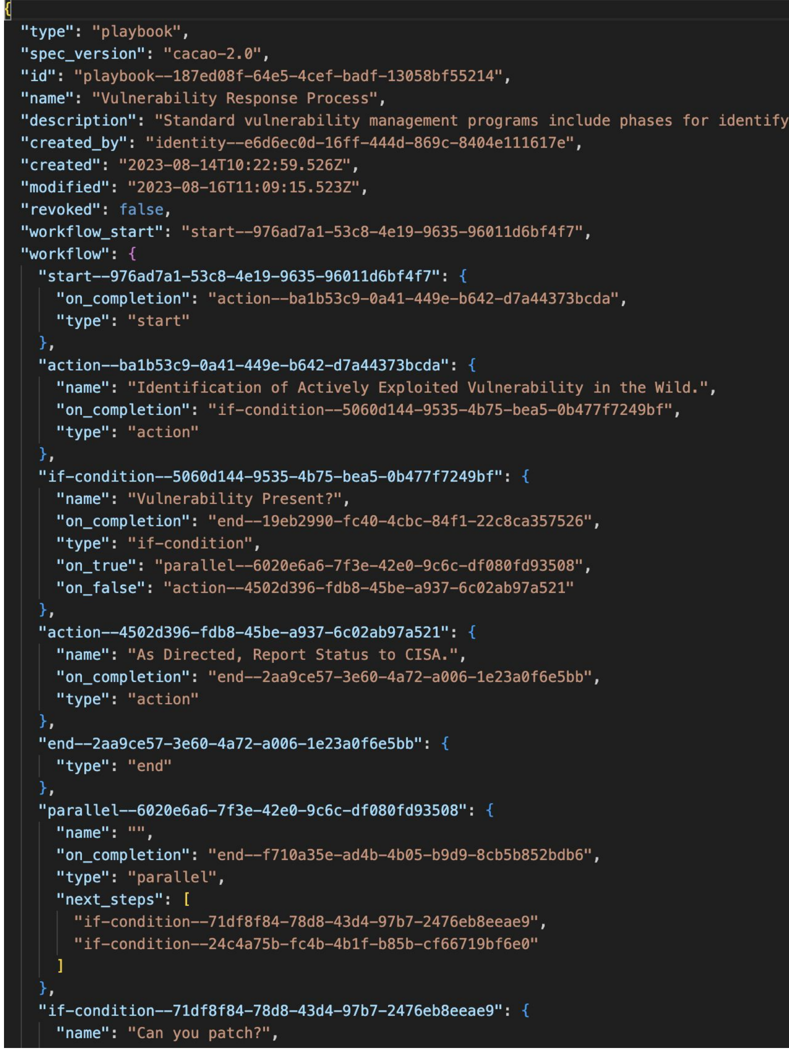
Mitigate

Patch

As Directed, Report Status to CISA

VULNERABILITY MANAGEMENT KEY:

- ● Identification
- ● Evaluation
- ● Remediation
- ● Reporting



```
{
  "type": "playbook",
  "spec_version": "cacao-2.0",
  "id": "playbook--187ed08f-64e5-4cef-badf-13058bf55214",
  "name": "Vulnerability Response Process",
  "description": "Standard vulnerability management programs include phases for identify
  "created_by": "identity--e6d6ec0d-16ff-444d-869c-8404e111617e",
  "created": "2023-08-14T10:22:59.526Z",
  "modified": "2023-08-16T11:09:15.523Z",
  "revoked": false,
  "workflow_start": "start--976ad7a1-53c8-4e19-9635-96011d6bf4f7",
  "workflow": {
    "start--976ad7a1-53c8-4e19-9635-96011d6bf4f7": {
      "on_completion": "action--ba1b53c9-0a41-449e-b642-d7a44373bcda",
      "type": "start"
    },
    "action--ba1b53c9-0a41-449e-b642-d7a44373bcda": {
      "name": "Identification of Actively Exploited Vulnerability in the Wild.",
      "on_completion": "if-condition--5060d144-9535-4b75-bea5-0b477f7249bf",
      "type": "action"
    },
    "if-condition--5060d144-9535-4b75-bea5-0b477f7249bf": {
      "name": "Vulnerability Present?",
      "on_completion": "end--19eb2990-fc40-4cbc-84f1-22c8ca357526",
      "type": "if-condition",
      "on_true": "parallel--6020e6a6-7f3e-42e0-9c6c-df080fd93508",
      "on_false": "action--4502d396-fdb8-45be-a937-6c02ab97a521"
    },
    "action--4502d396-fdb8-45be-a937-6c02ab97a521": {
      "name": "As Directed, Report Status to CISA.",
      "on_completion": "end--2aa9ce57-3e60-4a72-a006-1e23a0f6e5bb",
      "type": "action"
    },
    "end--2aa9ce57-3e60-4a72-a006-1e23a0f6e5bb": {
      "type": "end"
    },
    "parallel--6020e6a6-7f3e-42e0-9c6c-df080fd93508": {
      "name": "",
      "on_completion": "end--f710a35e-ad4b-4b05-b9d9-8cb5b852bdb6",
      "type": "parallel",
      "next_steps": [
        "if-condition--71df8f84-78d8-43d4-97b7-2476eb8eeae9",
        "if-condition--24c4a75b-fc4b-4b1f-b85b-cf66719bf6e0"
      ]
    },
    "if-condition--71df8f84-78d8-43d4-97b7-2476eb8eeae9": {
      "name": "Can you patch?",
```

TLP:CLEAR

End of Presentation

Q&A

in vasileiosmavroeidis