CYBERS

PROTECTING YOUR BUSINESS

Unlocking SOAR

Journey from Concept to Conquering Phishing Investigation

Reno Špitsmeister

Security Analyst, Cybers

Fredrik Ødegårdstuen

Platform Lead, Shuffle

Modern security team problems

- Security teams are suffering under a lack of **manpower, skills**, and **efficient solutions**.

(SOAR) Security Orchestration, Automation, Response

- **SOAR workflows** to streamline SecOps
- **Unifies** security tools
- **Centralized** platform/engine
- **Usecases**

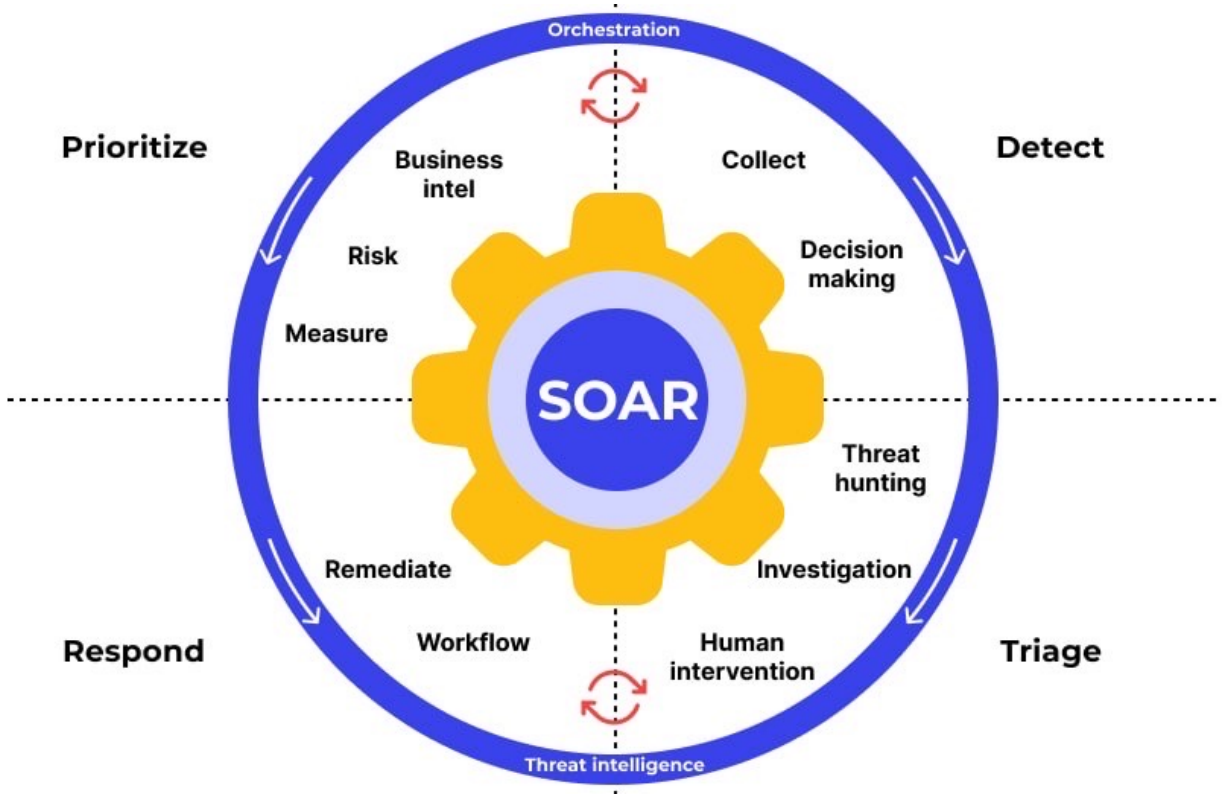


Image source: „SOAR"

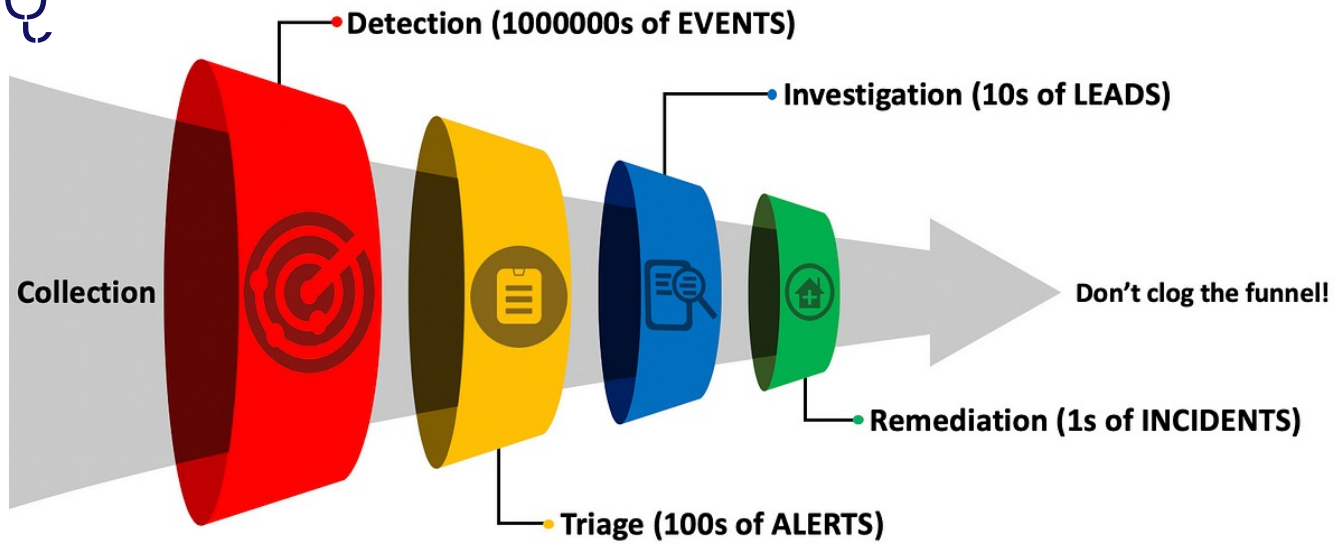
SOAR - Who and Why

Who?

- **Mature** security teams
- Large cybersecurity **budget**

Why?

- **Alert fatigue**
- Security **staffing** problems
- Improving SOC **metrics**
- **Integrating** tools and systems



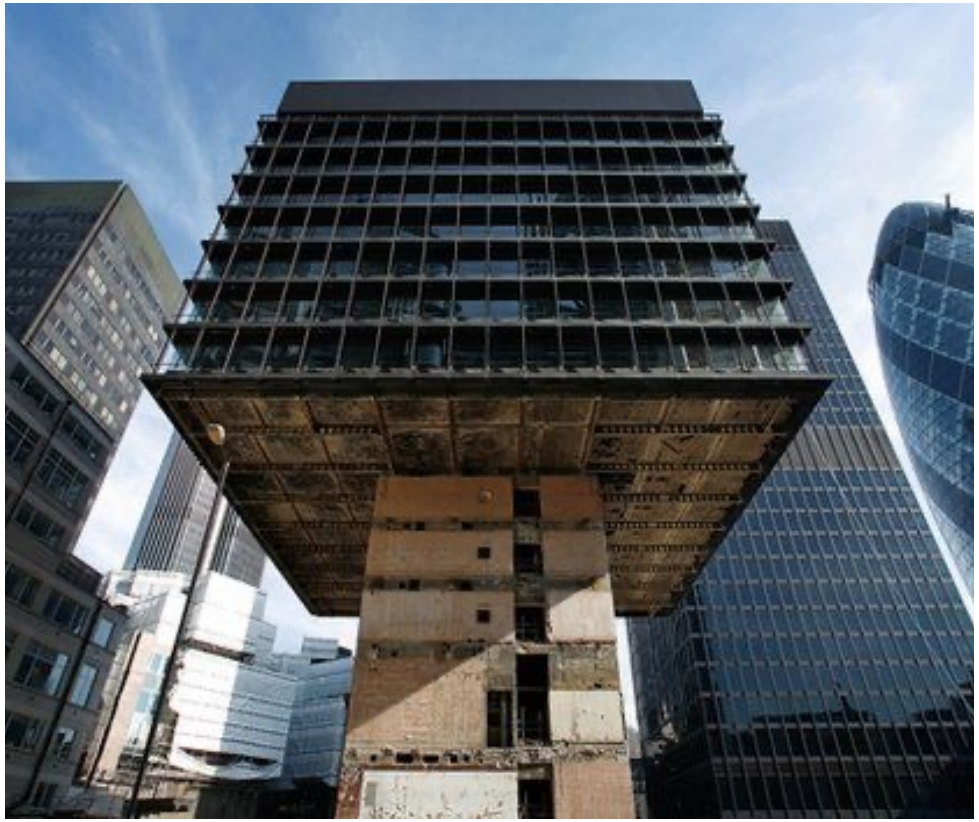
Determine if SOAR is the solution → Fulfill maturity criteria → Secure stakeholder support → Plan and find opportunities for SOAR → Choose optimal SOAR → Onboarding & Deploy in PROD

Image source: „Funnel of fidelity"

CYBERS

Are you ready for SOAR?

- **Goals** and operational **challenges**
- **Skills** and **resources**
- **Stakeholder** support
- **Integration**
- **Consistent** manual processes
- **Mature** SIEM/XDR



Determine if SOAR is the solution → Fulfill maturity criteria → Secure stakeholder support → Plan and find opportunities for SOAR → Choose optimal SOAR → Onboarding & Deploy in PROD

Stakeholders - ROI and Business Value

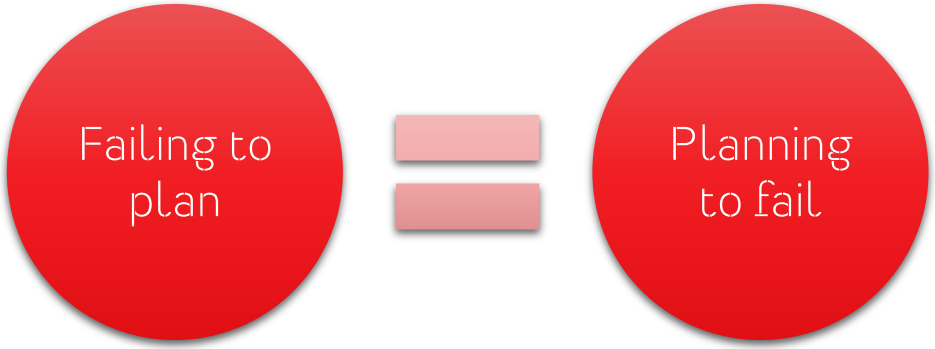
- Is SOAR **expensive**?

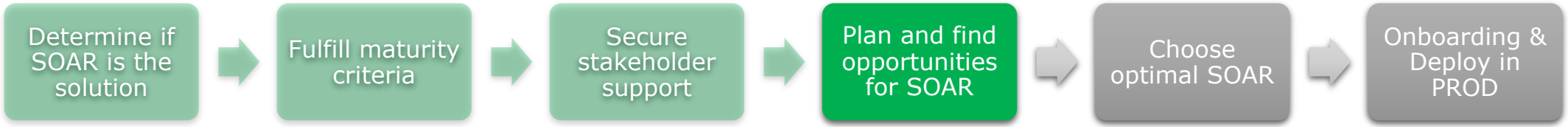
- **ROI** / value proposition of SOAR
  - Labor & Resource
  - Future-proofing
  - Risk reduction

Determine if SOAR is the solution → Fulfill maturity criteria → **Secure stakeholder support** → Plan and find opportunities for SOAR → Choose optimal SOAR → Onboarding & Deploy in PROD

Planning for success

- **Dedicated** team or person
- **Force multiplier/empowerment**
- **Clear objectives** during planning

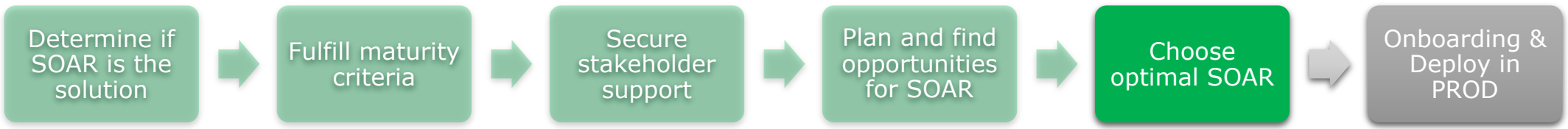




CYBERS

SOAR selection factors

- **Capabilities**
- **Expenditure**
- **Open-source SOARs**



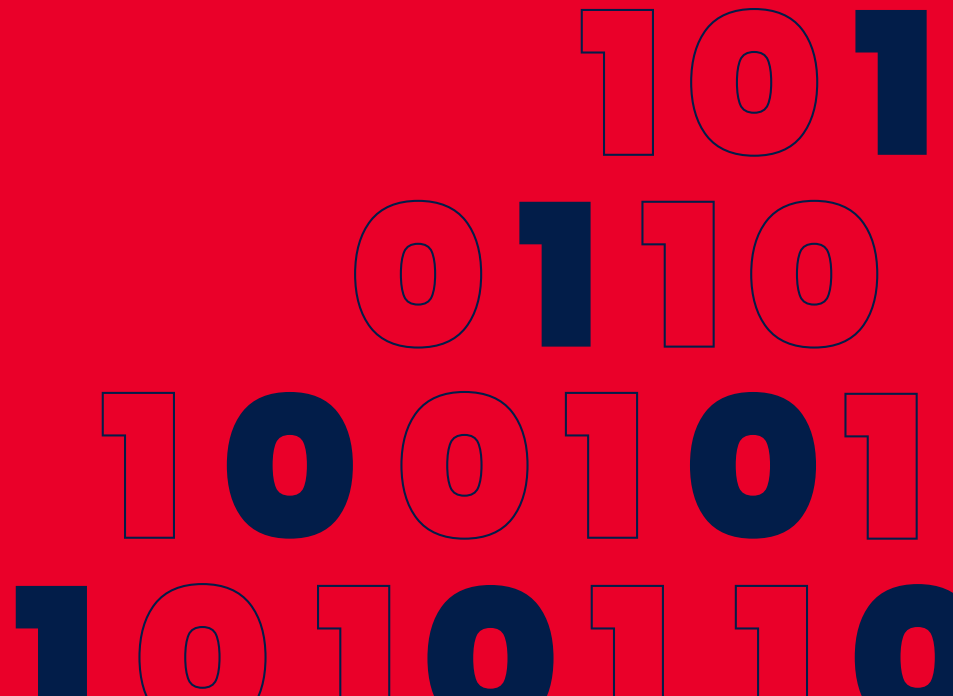
Onboarding & Execution

- **Dedicated** personnel
- **Configure** tool
- **Develop** workflows

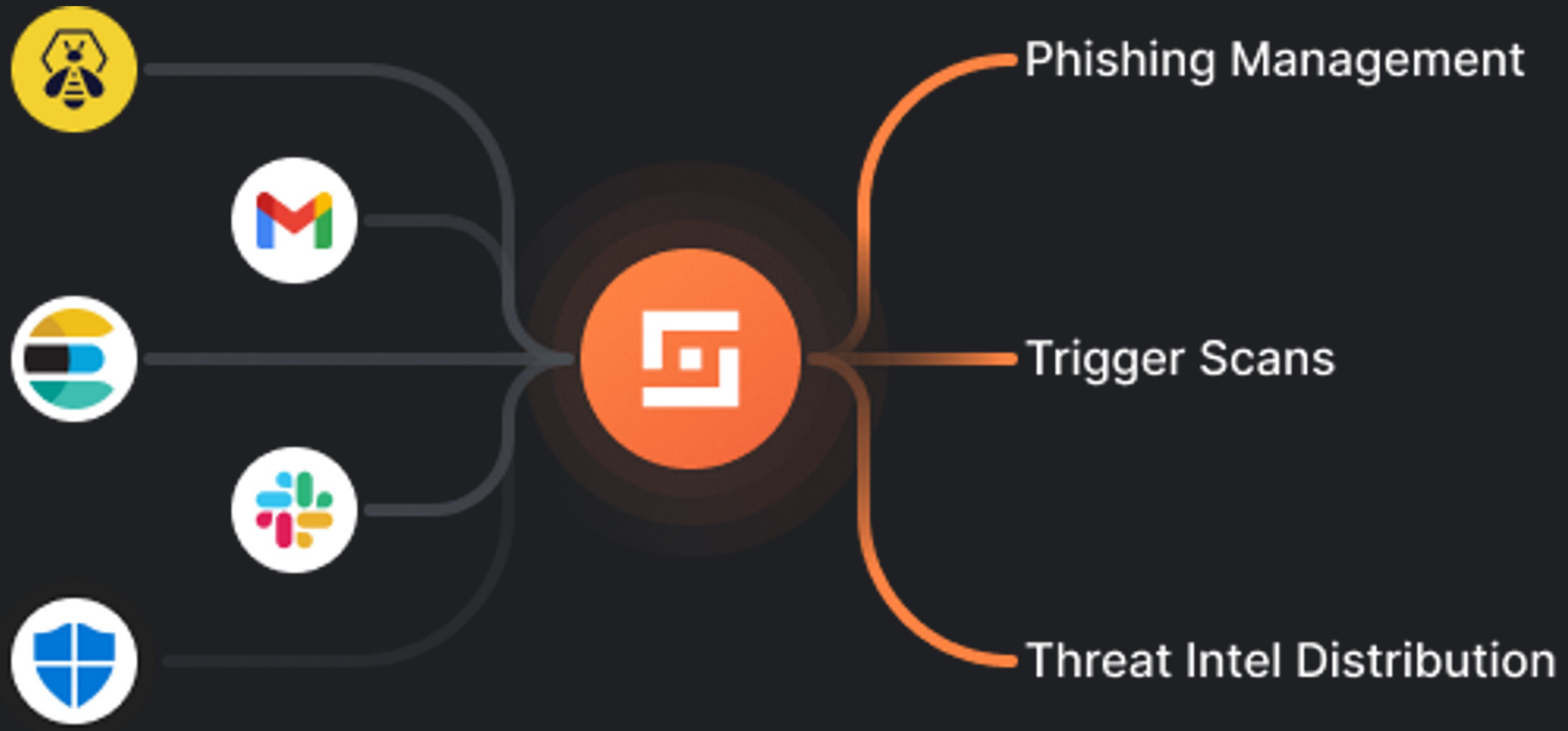
Determine if SOAR is the solution → Fulfill maturity criteria → Secure stakeholder support → Plan and find opportunities for SOAR → Choose optimal SOAR → Onboarding & Deploy in PROD

CYBERS

A Practical Implementation



CYBERS


Phishing Management
Trigger Scans
Threat Intel Distribution

CYBERS

Detection & Prevention

Finds and eradicates

SIEM

SIGMA

NETWORK

SNORT

yara

ERADICATE

CASES

COMMS

IAM

ASSETS

INTEL

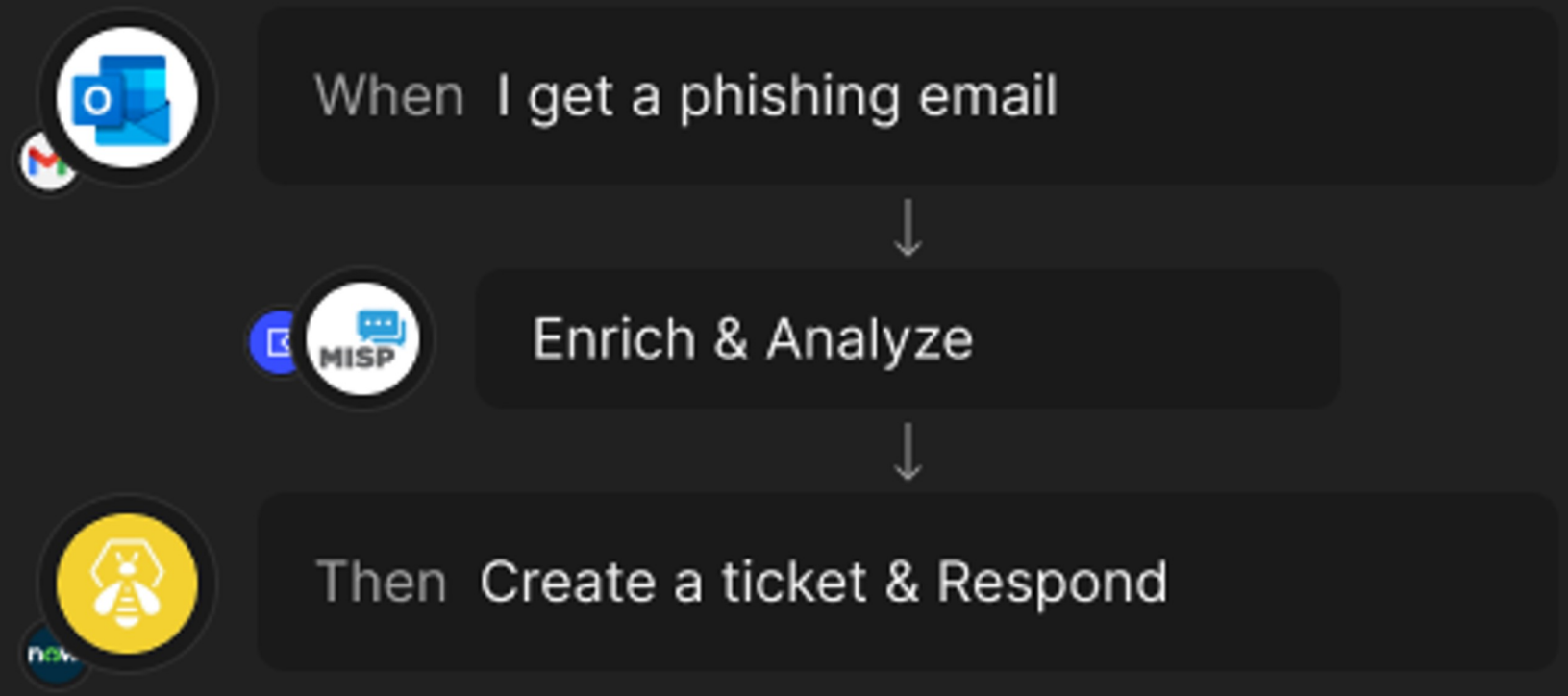
Context

Provided for detections

Vulnerabilities
Domains
Usernames
Hostnames
URLs
Hashes
Subjects
Email
Powershell
Scheduled task
...

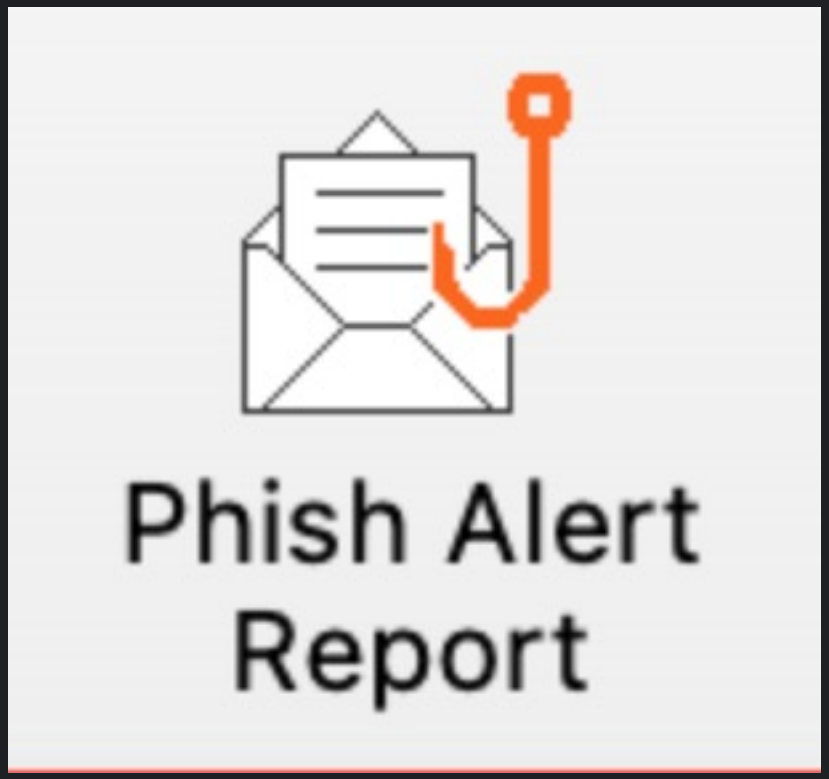
CYBERS

A Phishing Usecase

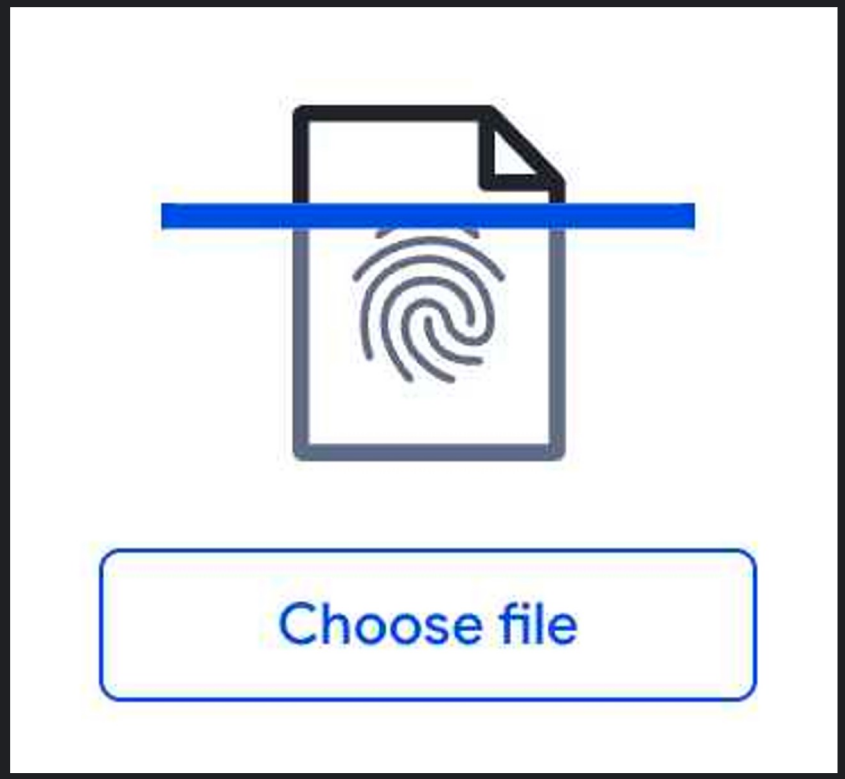


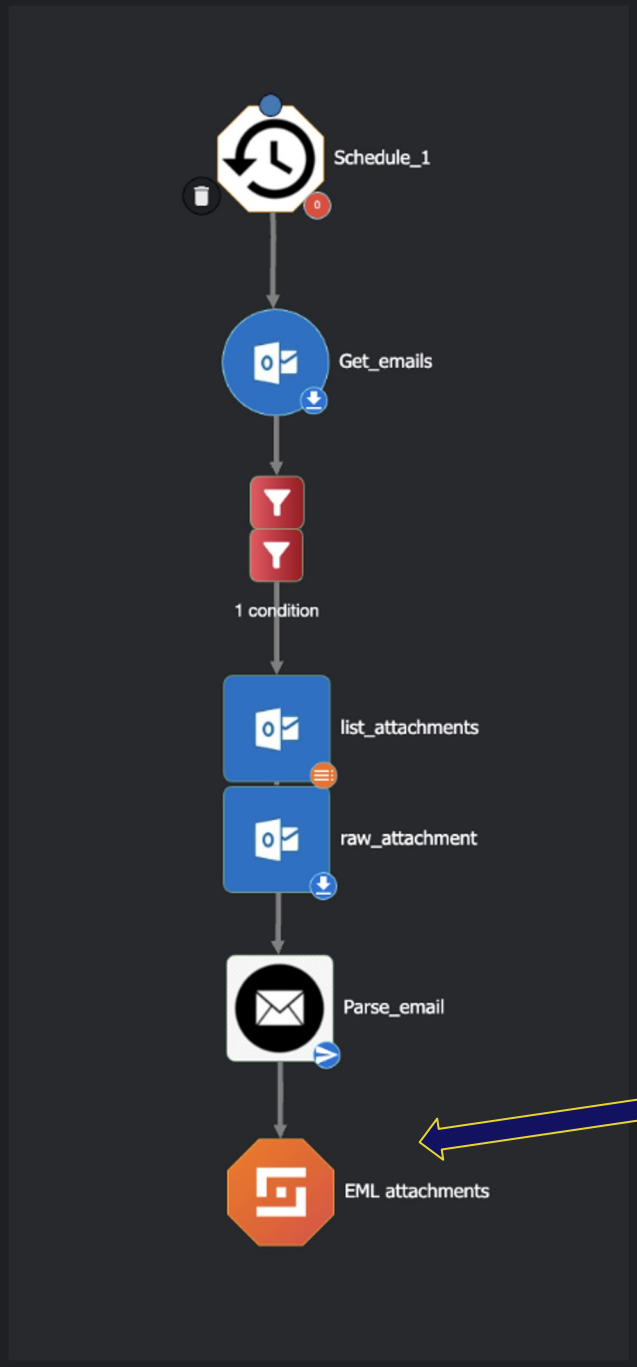
CYBERS

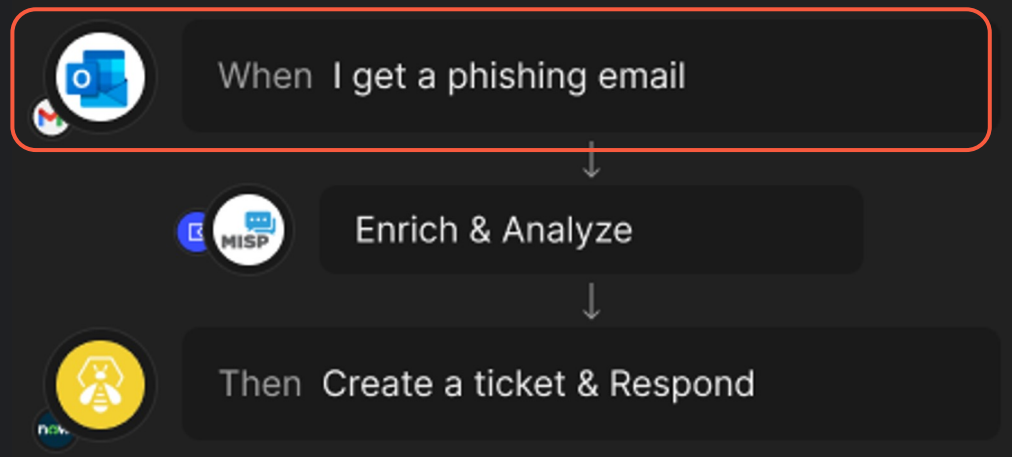
Mail button



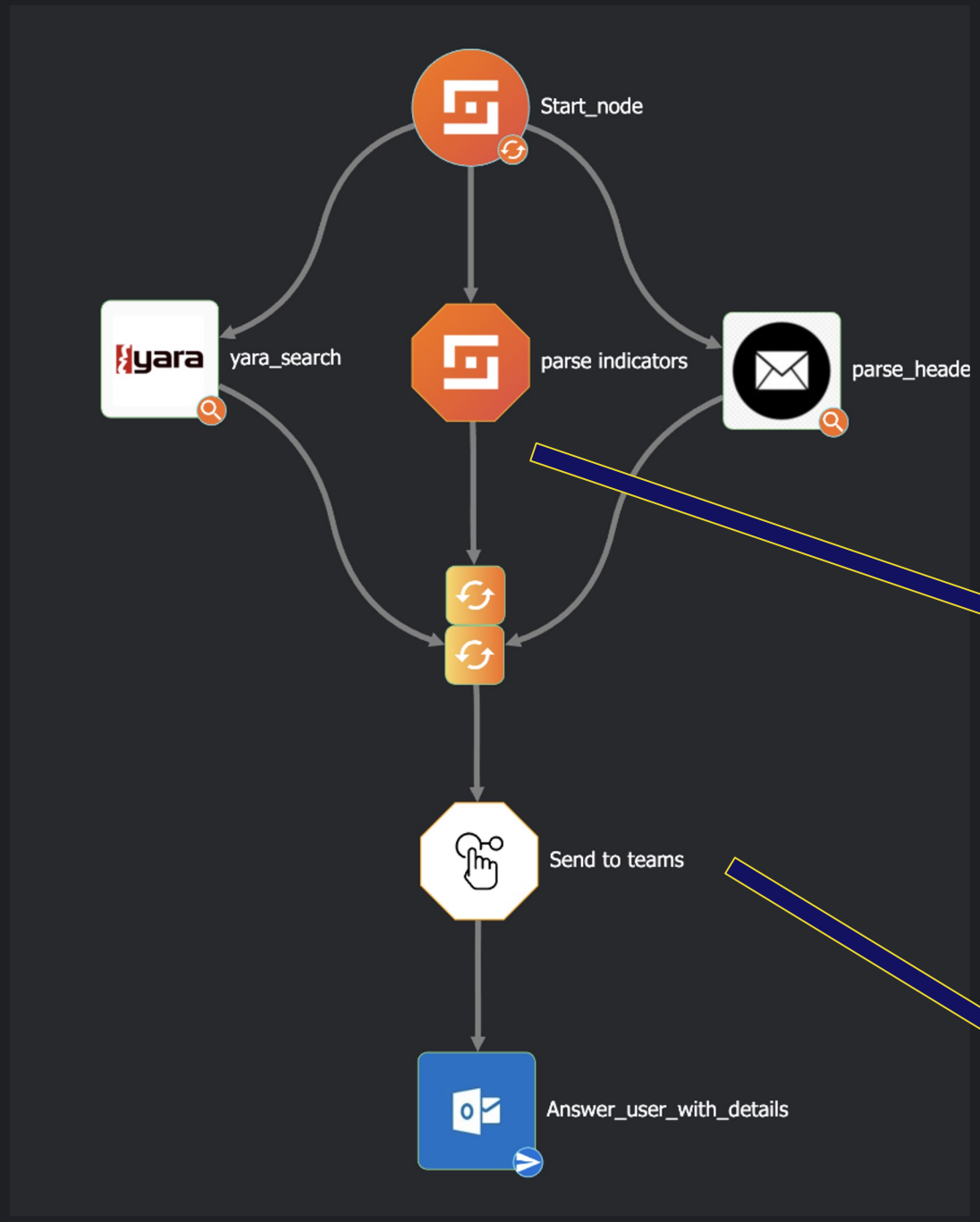
Sandbox

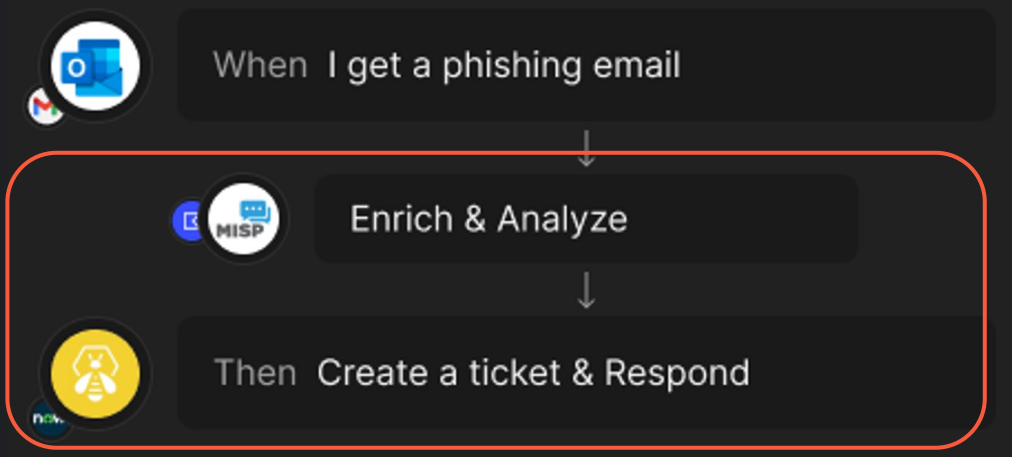


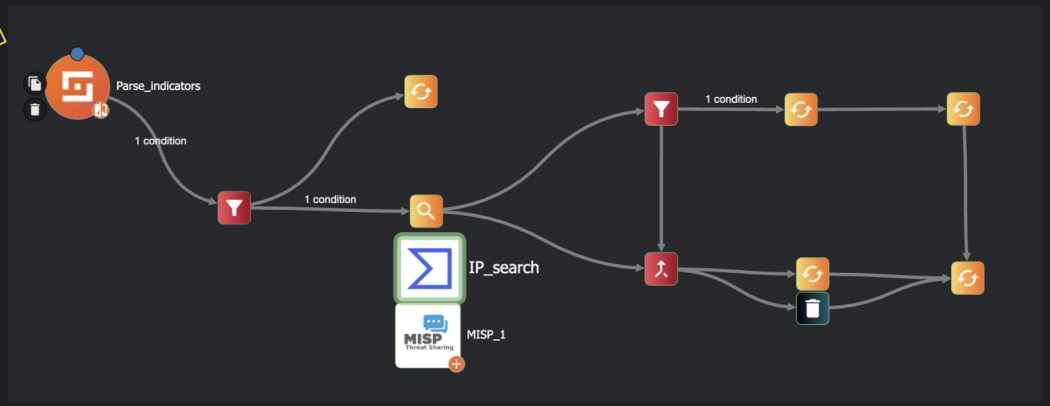




Forward to Enrich & Analyze

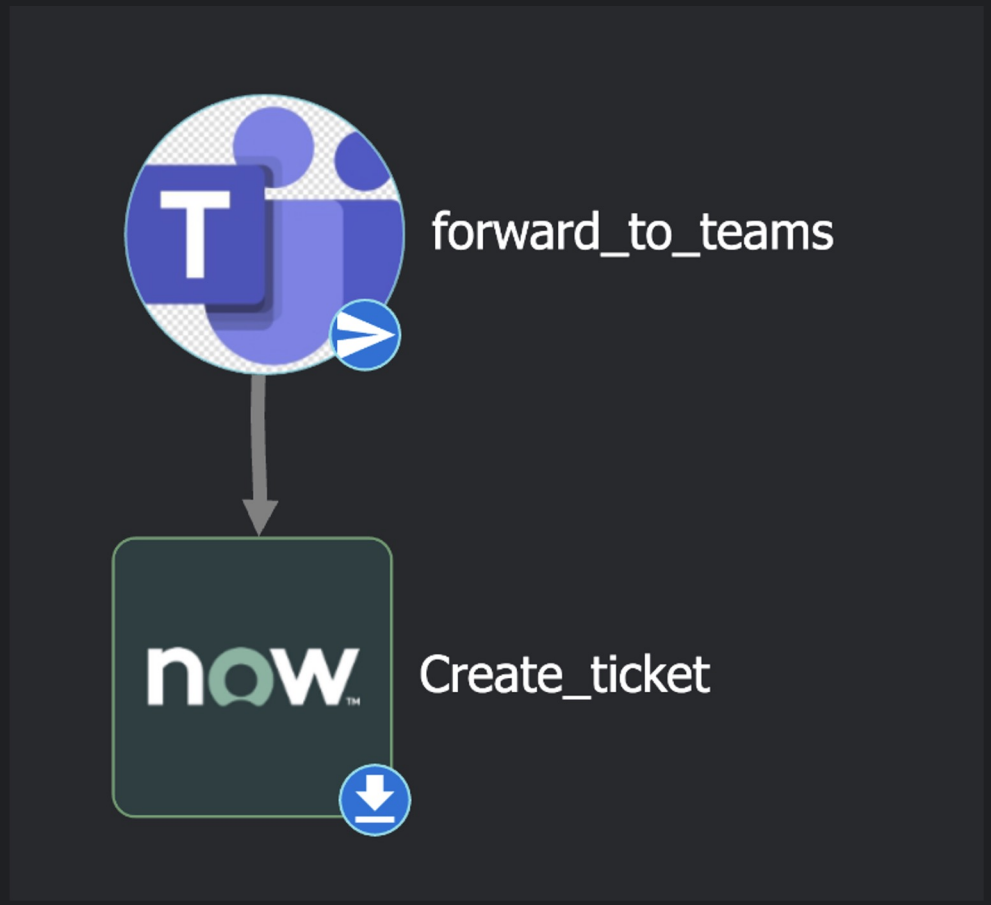






Send to teams

Actionable Outcome



Email analysis

Subject: [External] URGENT To: finance@cybers.eu From: officeonline474544@gmail.com:

Headers

spf: false () dkim: false () dmarc: false () spoofed: false ()

Indicators

(51/64) 9ce9c5a68201f8990489ebde68569cd20b5fc905ac09fa0fa7702ea0f382b313

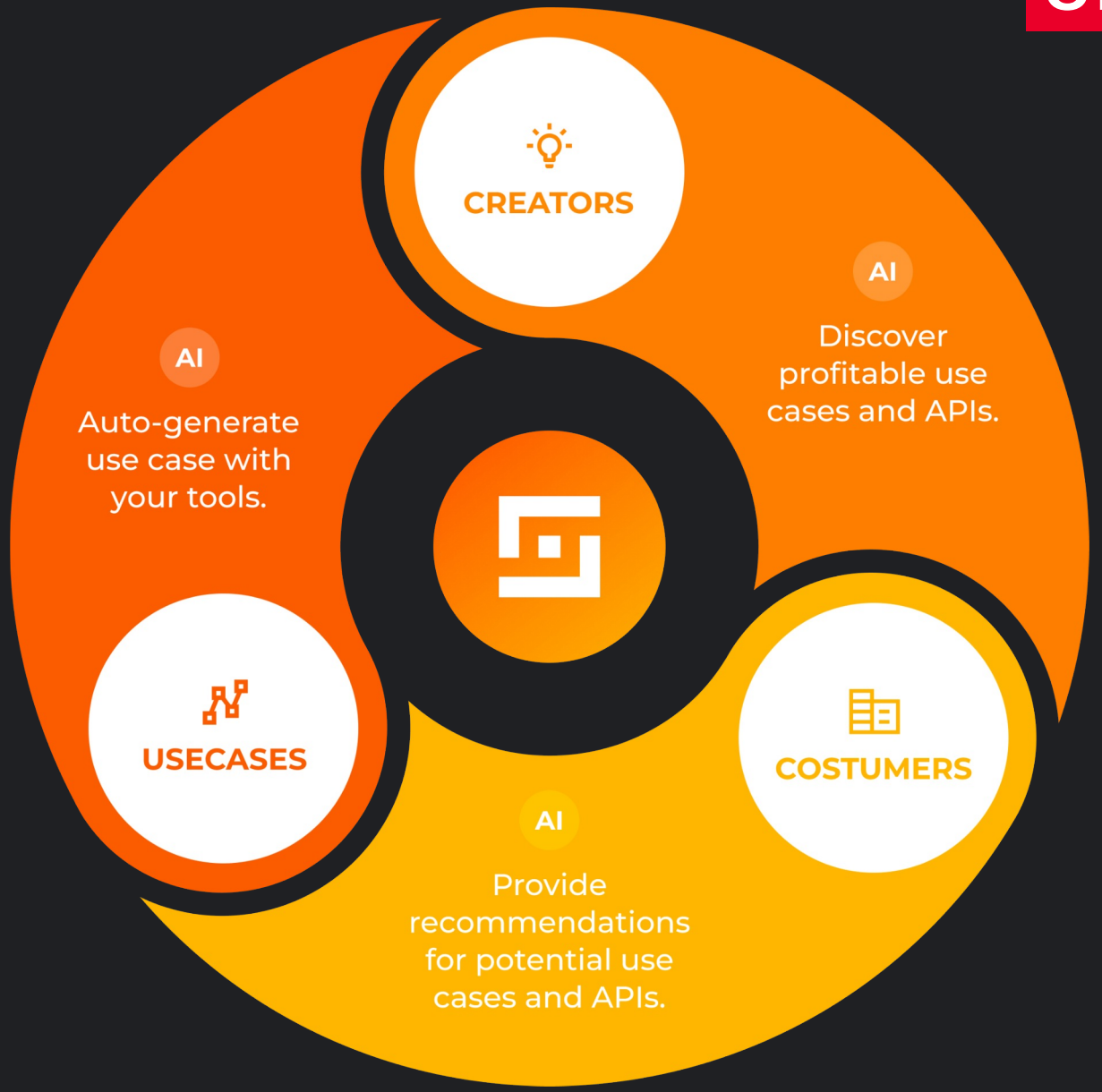
Outcome

This email is likely a phishing email due to the same email being found malicious previously."

Answer user

CYBERS

Creator Incentive Program



CYBERS

With SOAR, we turn the tide in our favour, automating the routine to focus on the extraordinary