nviso

www.nviso.eu

SHIELD

Microsoft XDR and Logic Apps

11/03/2025

ATHENS

BRUSSELS

FRANKFURT

MUNICH

VIENNA

Where to find us.

Website
nviso.eu

Blog
blog.nviso.eu

E-Mail
info@nviso.eu

Linkedin
nviso-cyber

X
@NVISOsecurity

Have you been hacked?

Emergency Response

Belgium
+32 (0)2 588 43 80
csirt@nviso.eu

Germany
+49 69 8088 3829
csirt@nviso.de

Austria
+43 720 228 337
csirt@nviso.at

About NVISO

Our Company

NVISO is a pure play **Cyber Security services firm** of 300+ specialized security experts and founded in 2013.

Initially founded in **Belgium**, we've been in **Germany** since 2019, and **Greece** & **Austria** since 2022.

Our mission is to **safeguard the foundations of European society from cyber attacks**.

Our DNA

We are proud: we are proud of who we are and what we do.

We care: we care about our customers and people.

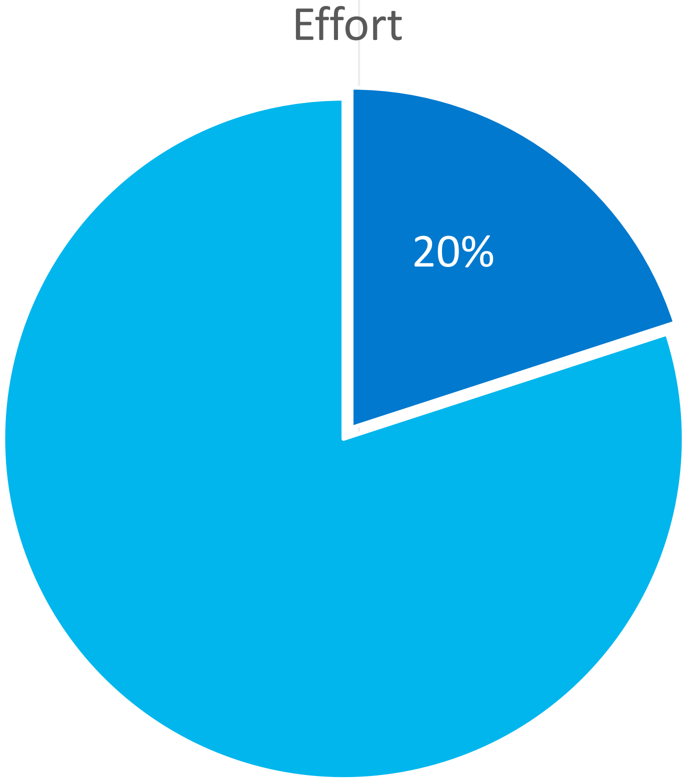
We break barriers: We challenge the status quo by continuous innovation.

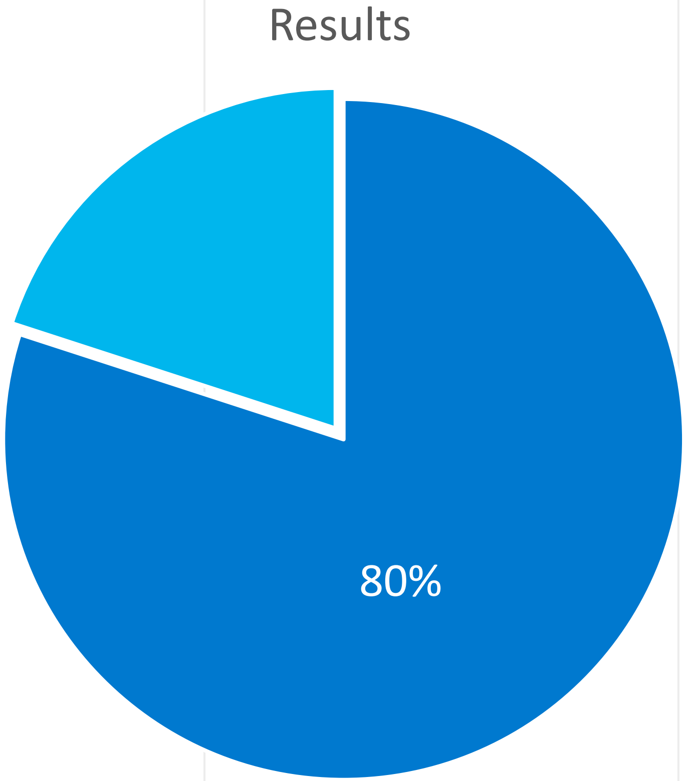
No BS: We keep our promises and don't fool around.

Our Research

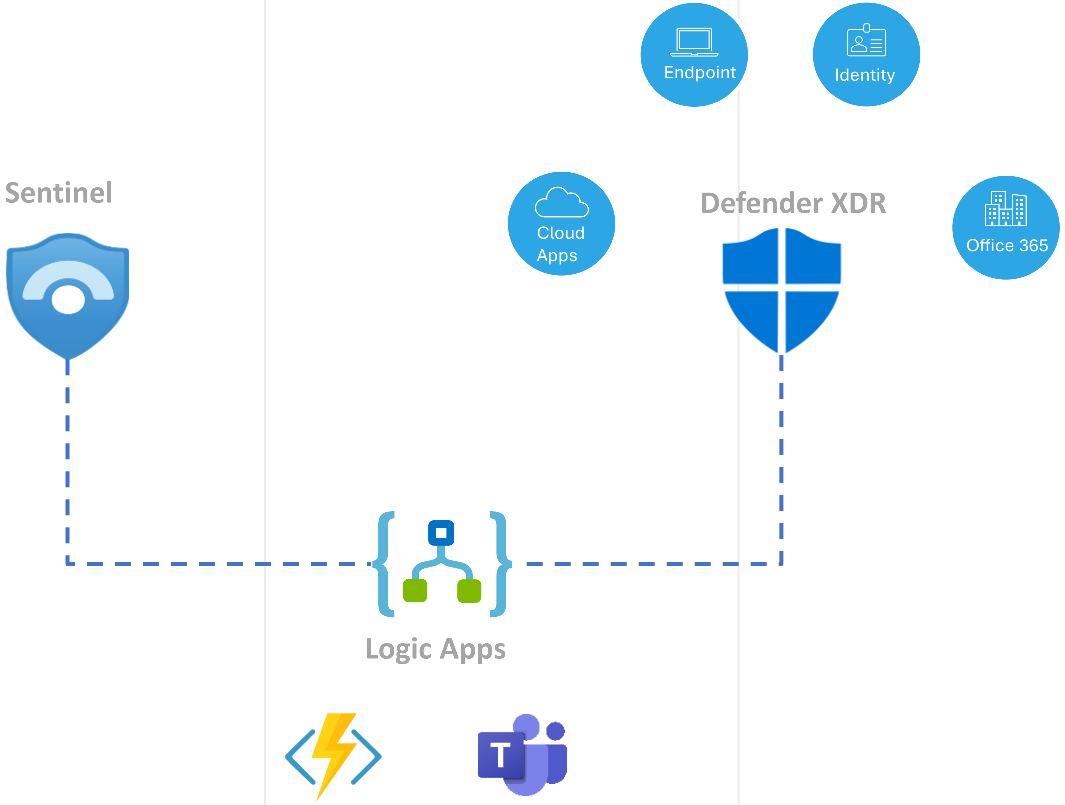
We **invest 10% of our annual revenue** in research of new security techniques and the development of new solutions.

Pareto Principle





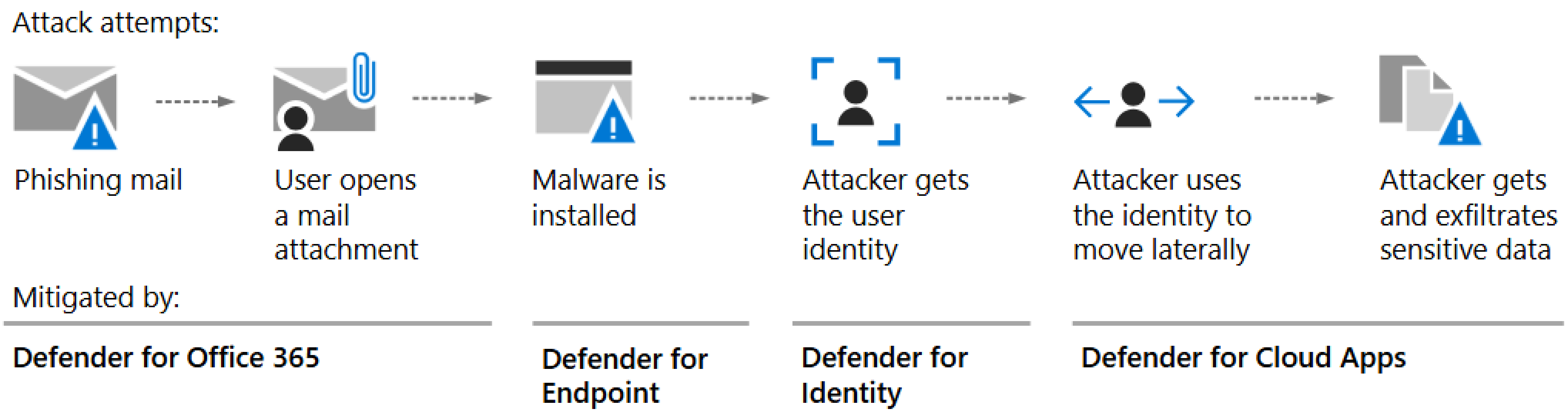
XDR and Logic Apps Concept



XDR Components

	Tool	Detect	Respond
Endpoint	Defender for Endpoint	• Process creation • Registry changes • File changes • Network events • Logon events • >100 other actions	• Isolate the Host • Quarantine files/processes • Collect forensic artifacts • Interactive Response Session • Restrict app execution • Block Hash
Identity	Defender for Identity	• AD Logons • Changes to directory objects (create/update/delete) • Users • Devices • Groups	• Disable a user • Force password change on logon
Office 365	Defender for Office365	• Email sent/received with attachment and URL info • Links clicked in emails/Office documents	• Quarantine emails
Cloud Apps	Defender for Cloud Apps	• App activity	• Disable users in apps • Prevent access to apps • Block apps

XDR Components: Mitigating a Phishing Attack



Attack attempts:

- Phishing mail
- User opens a mail attachment
- Malware is installed
- Attacker gets the user identity
- Attacker uses the identity to move laterally
- Attacker gets and exfiltrates sensitive data

Mitigated by:

- **Defender for Office 365**
- **Defender for Endpoint**
- **Defender for Identity**
- **Defender for Cloud Apps**

Logic Apps Features

Integrations & Connectors

Incident playbooks

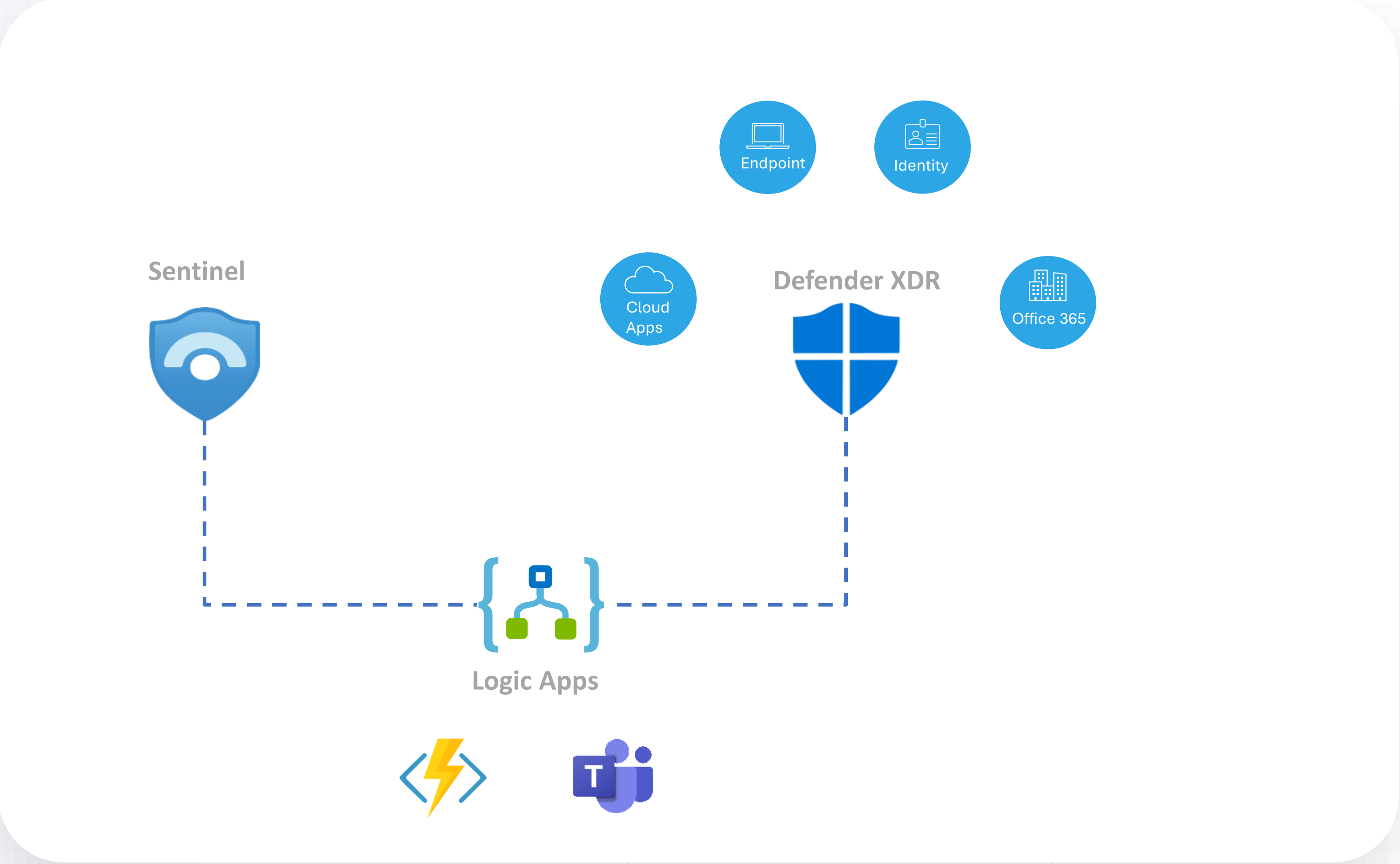
Response actions

Automation playbooks

Code Execution

Playbook categories

- Enrichment
- Alerting
- Response



Logic Apps Features

Integrations & Connectors

Incident playbooks

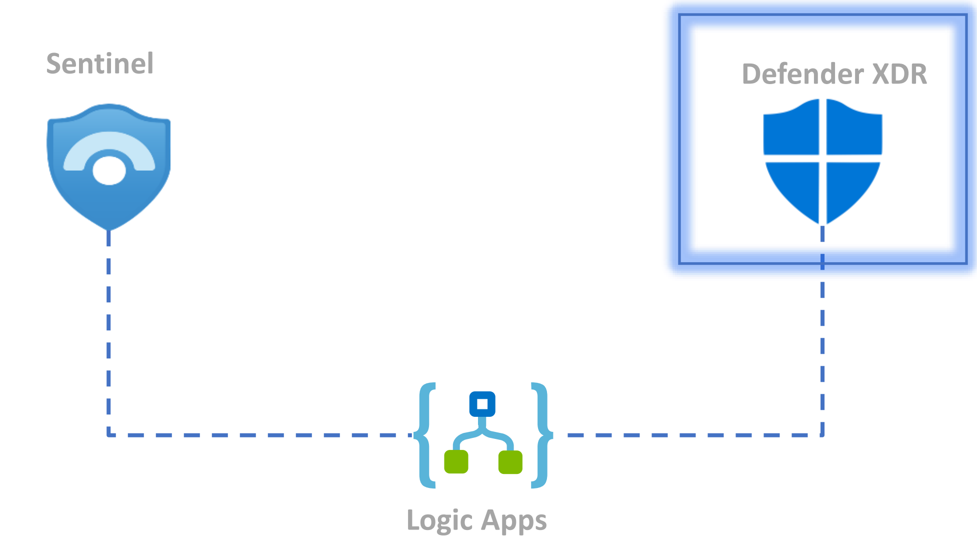
Response actions

Automation playbooks

Code Execution

Playbook categories

- Enrichment
- Alerting
- Response



Logic Apps Features

Integrations & Connectors

Incident playbooks

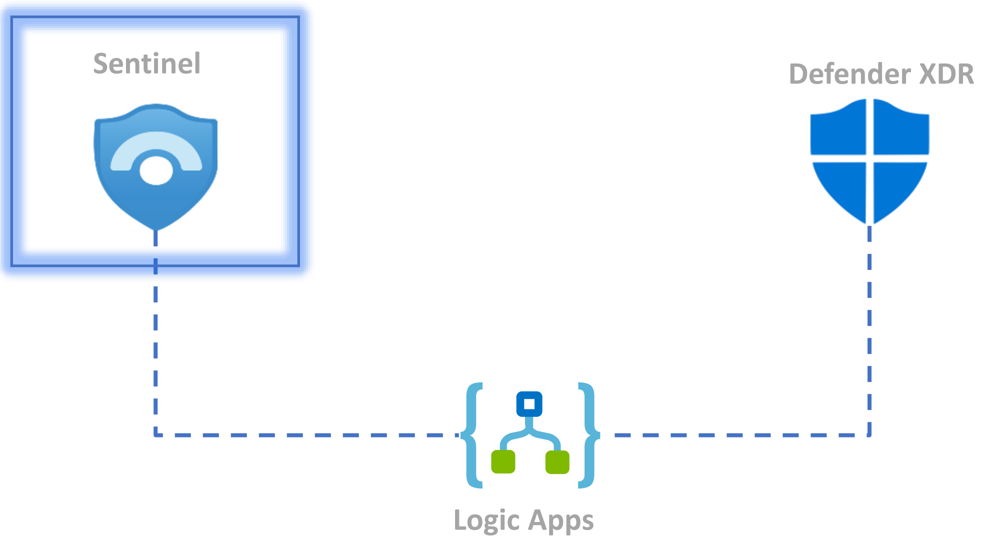
Response actions

Automation playbooks

Code Execution

Playbook categories

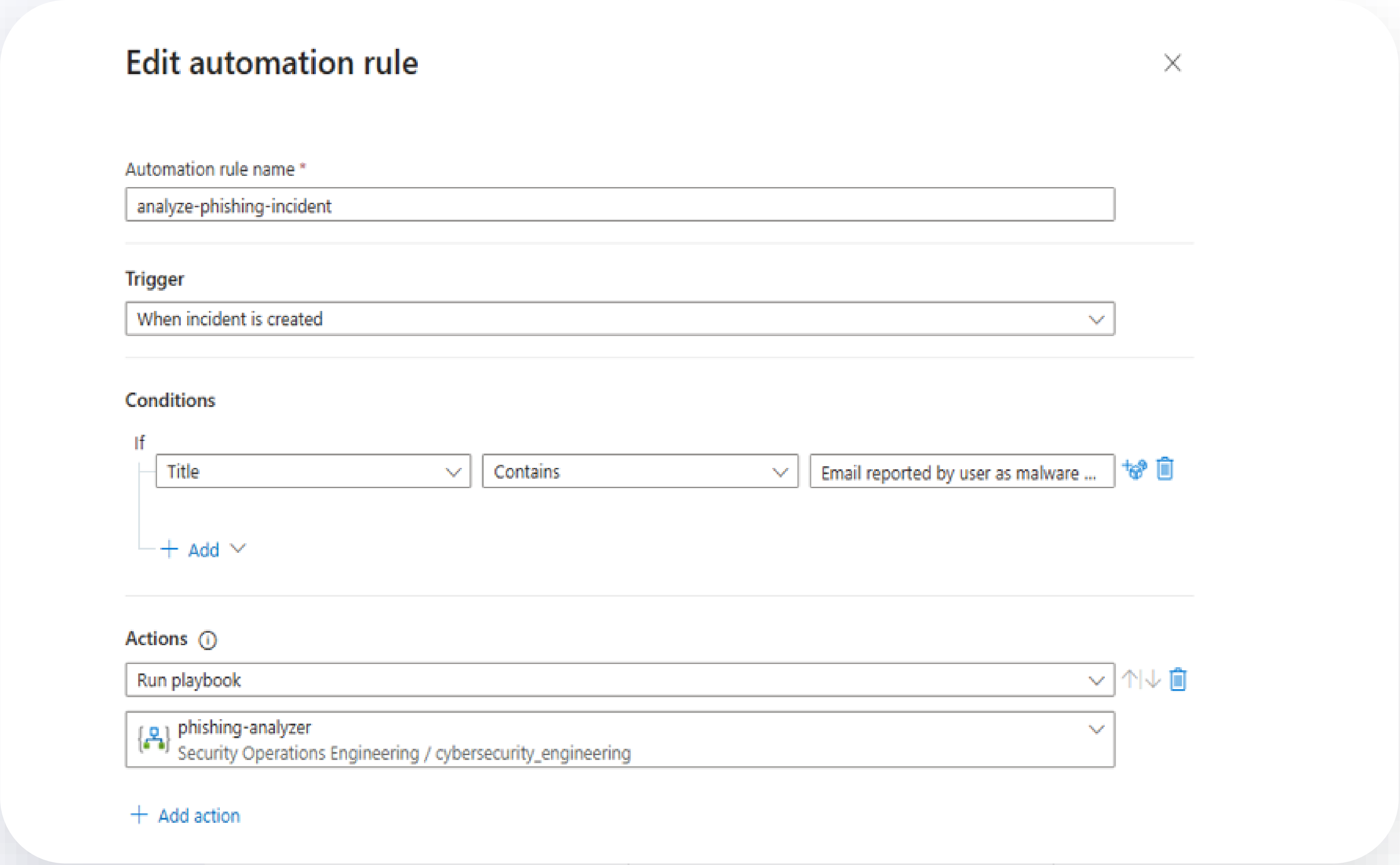
- Enrichment
- Alerting
- Response



Logic Apps Features

Integrations & Connectors
Incident playbooks
Response actions
Automation playbooks
Code Execution
Playbook categories

- Enrichment
- Alerting
- Response



Edit automation rule

Automation rule name *
analyze-phishing-incident

Trigger
When incident is created

Conditions
If
Title | Contains | Email reported by user as malware ...

Actions
Run playbook
phishing-analyzer
Security Operations Engineering / cybersecurity_engineering

Logic Apps Features

Integrations & Connectors

Incident playbooks

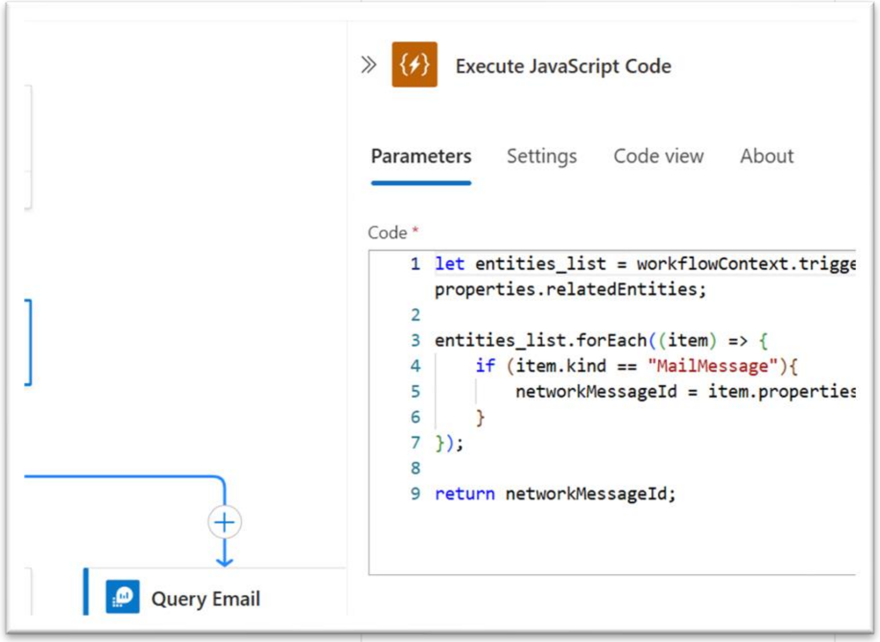
Response actions

Automation playbooks

Code Execution

Playbook categories

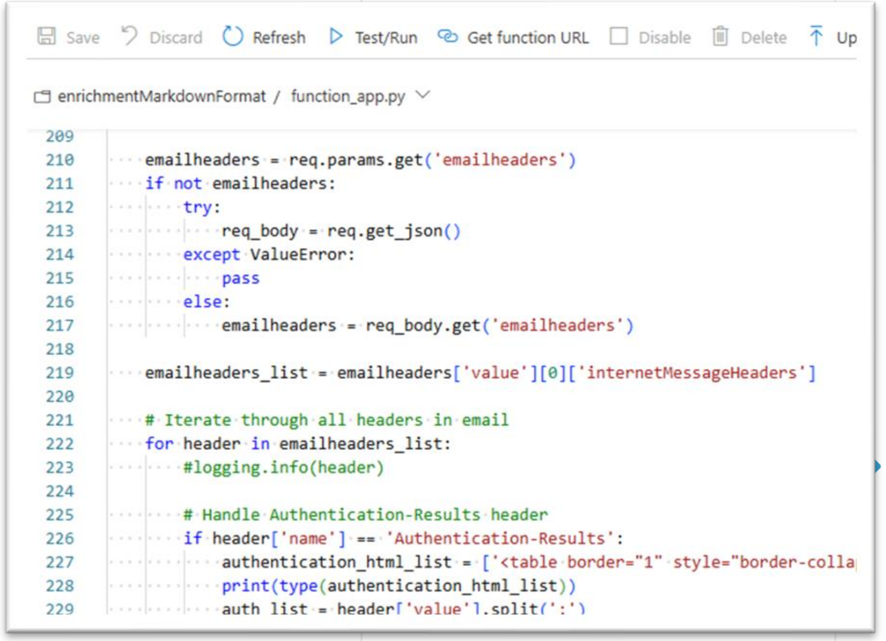
- Enrichment
- Alerting
- Response



```
let entities_list = workflowContext.trigge
properties.relatedEntities;

entities_list.forEach((item) => {
    if (item.kind == "MailMessage"){
        networkMessageId = item.properties
    }
});

return networkMessageId;
```



```

    emailheaders = req.params.get('emailheaders')
    if not emailheaders:
        try:
            req_body = req.get_json()
        except ValueError:
            pass
        else:
            emailheaders = req_body.get('emailheaders')

    emailheaders_list = emailheaders['value'][0]['internetMessageHeaders']

    # Iterate through all headers in email
    for header in emailheaders_list:
        #logging.info(header)

        # Handle Authentication-Results header
        if header['name'] == 'Authentication-Results':
            authentication_html_list = ['<table border="1" style="border-colla
            print(type(authentication_html_list))
            auth_list = header['value'].split(':')
```

Logic Apps Features

Integrations & Connectors

Incident playbooks

Response actions

Automation playbooks

Code Execution

Playbook categories

Enrichment

Alerting

Response

Enrichment

Collect data from integrated sources and present them to analysts in the comments section, that will guide the analyst during the alert triage.

Alerting

A message will be sent to SOC channel in MS Teams to make sure a critical incident will be acknowledged promptly.

Response

Take immediate actions on incident entities.

Logic Apps Features

- Integrations & Connectors
- Incident playbooks
- Response actions
- Automation playbooks
- Code Execution
- Playbook categories
  - Enrichment
  - Alerting
  - Response

Phishing Analysis

Collect data about suspicious email activity, analyze email headers, check for URLs and attachments ...

User account

Query Entra ID, check Entra ID Protection, look for suspicious activity ...

Host Enrichment

Query MDE to get all information about machine, get logged-on users ...

Suspicious Access

Check source IP address of access attempt, compare the IP's geolocation to the user's location in Entra ID, find other users with access attempts from the same IP address, check authentication details like MFA ...

Logic Apps Features

Integrations & Connectors

Incident playbooks

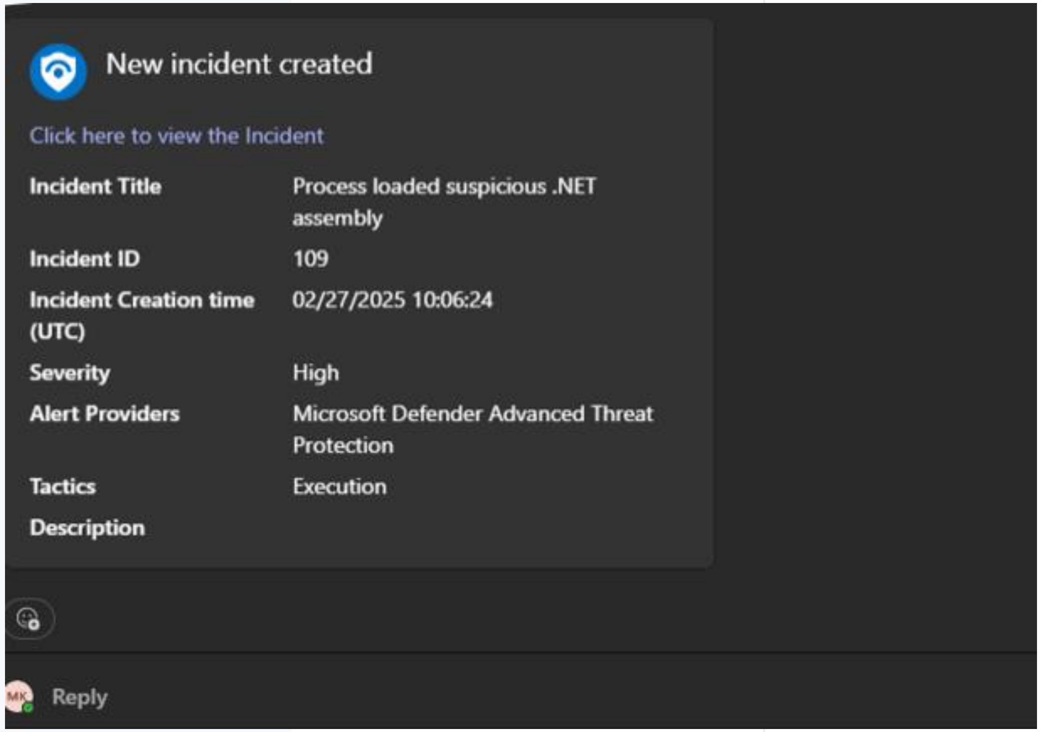
Response actions

Automation playbooks

Code Execution

Playbook categories

- Enrichment
- Alerting
- Response



New incident created

Click here to view the Incident

Incident Title	Process loaded suspicious .NET assembly
Incident ID	109
Incident Creation time (UTC)	02/27/2025 10:06:24
Severity	High
Alert Providers	Microsoft Defender Advanced Threat Protection
Tactics	Execution
Description	

MS Teams

- Run on ‘High’ severity alerts
- Notify a Teams channel
- Acknowledge an incident faster

Logic Apps Features

Integrations & Connectors
Incident playbooks
Response actions
Automation playbooks
Code Execution
Playbook categories
- Enrichment
- Alerting
- Response

Isolate Host

Revoke User Access

Get MDE Investigation Package

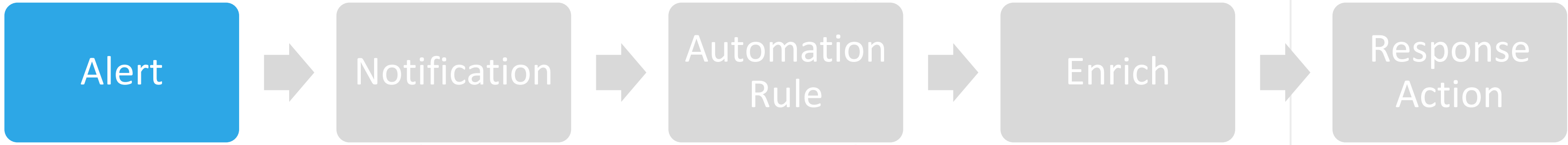
Start automatic investigation

Get File Activity

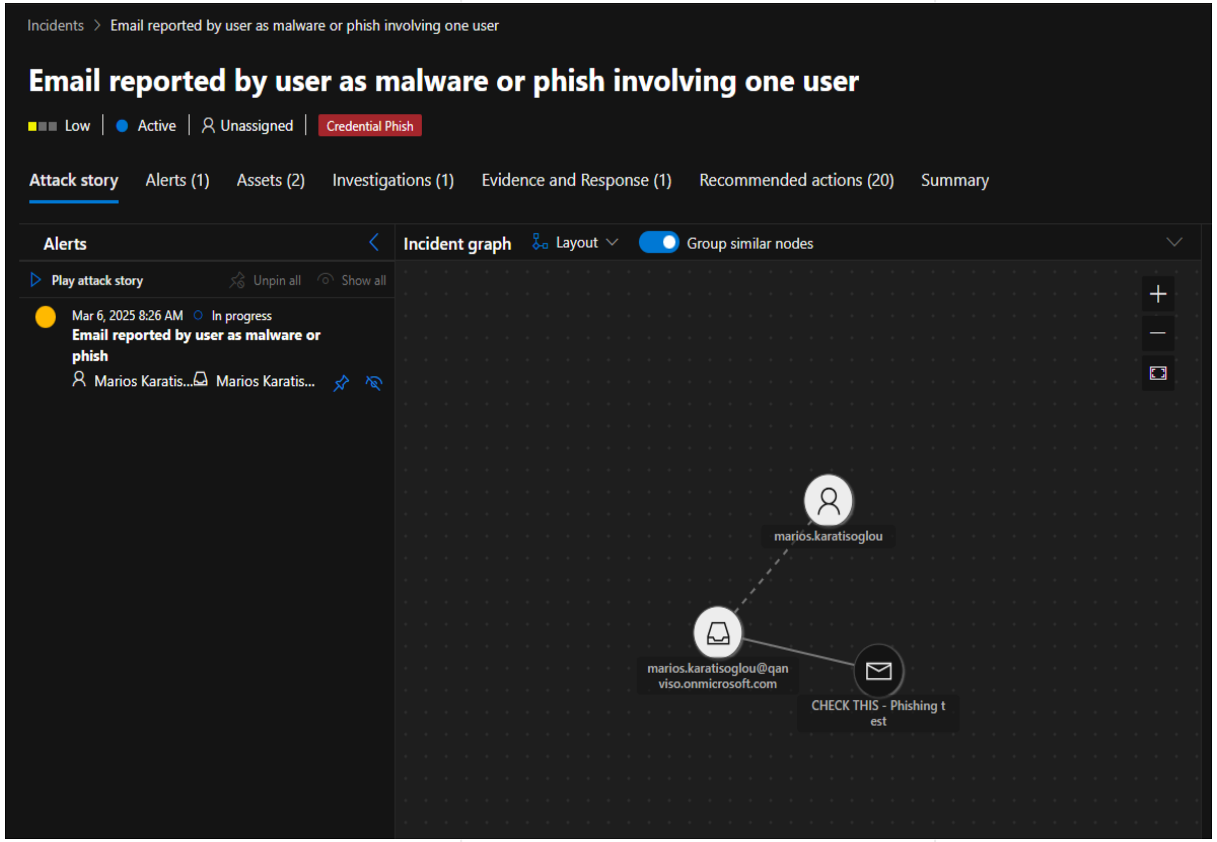
Block Hash in Defender

Logic Apps

Use Case: Phishing Incident



Alert → Notification → Automation Rule → Enrich → Response Action



Incidents > Email reported by user as malware or phish involving one user

Email reported by user as malware or phish involving one user

Low | Active | Unassigned | Credential Phish

Attack story | Alerts (1) | Assets (2) | Investigations (1) | Evidence and Response (1) | Recommended actions (20) | Summary

Alerts

Play attack story | Unpin all | Show all

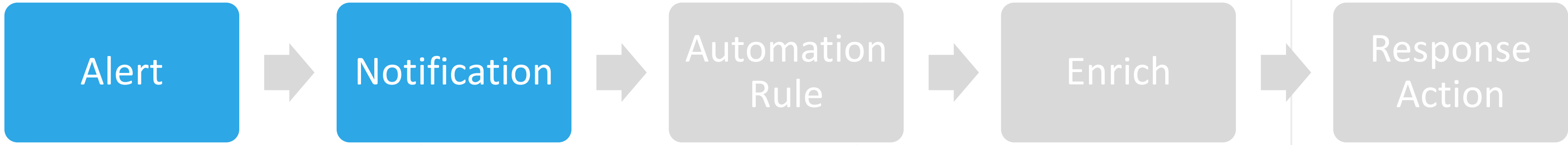
Mar 6, 2025 8:26 AM | In progress
Email reported by user as malware or phish
Marios Karatis... Marios Karatis...

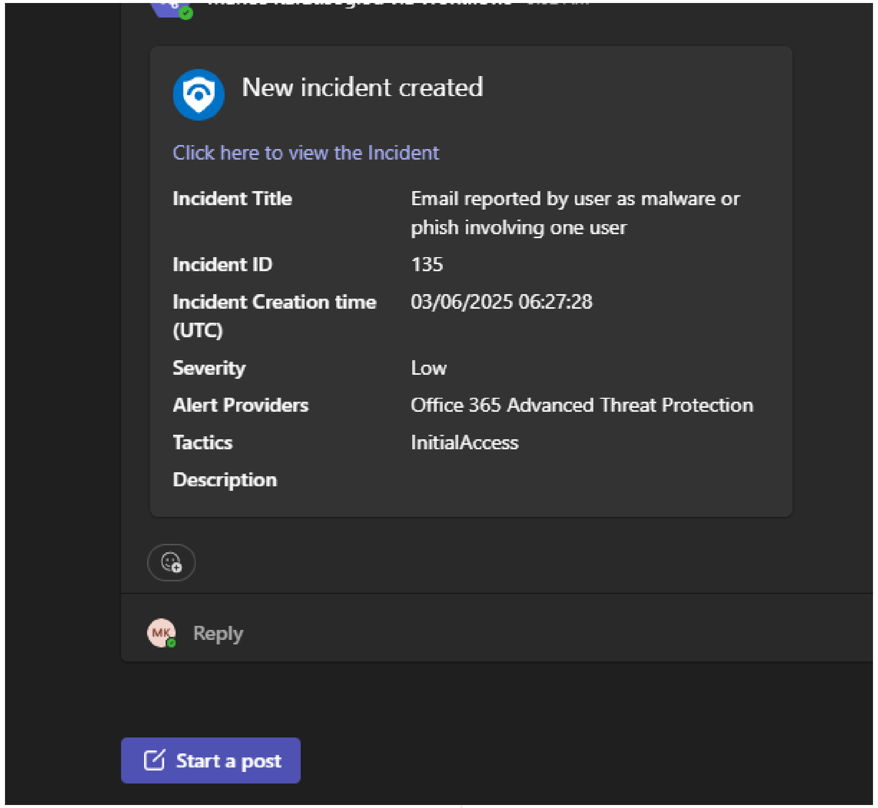
Incident graph | Layout | Group similar nodes

marios.karatisoglou
marios.karatisoglou@qanviso.onmicrosoft.com
CHECK THIS - Phishing test

Logic Apps

Use Case: Phishing Incident





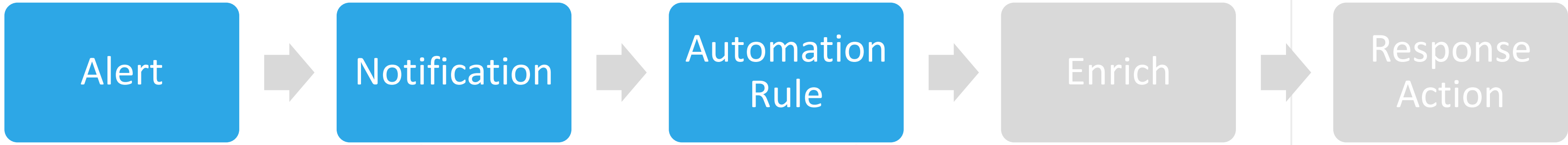
New incident created

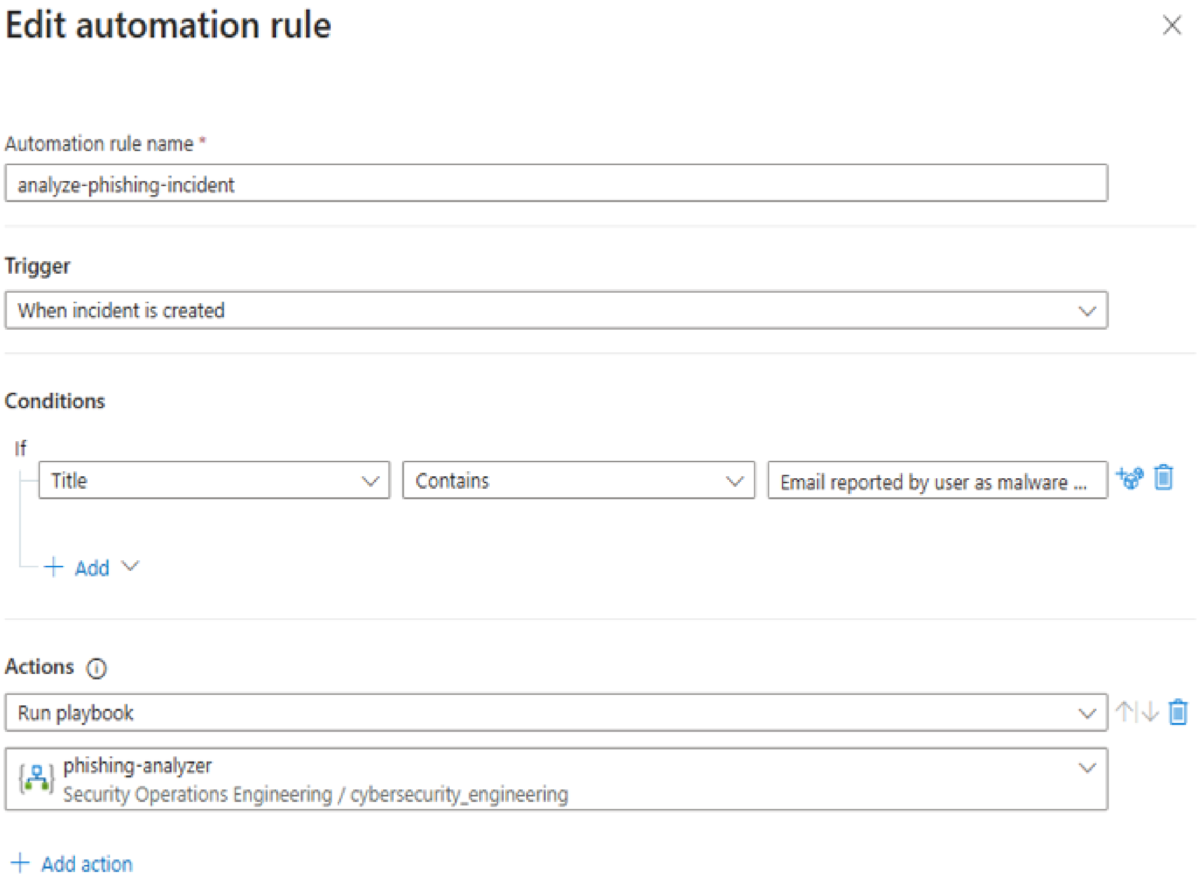
Click here to view the Incident

Incident Title	Email reported by user as malware or phish involving one user
Incident ID	135
Incident Creation time (UTC)	03/06/2025 06:27:28
Severity	Low
Alert Providers	Office 365 Advanced Threat Protection
Tactics	InitialAccess
Description	

Logic Apps

Use Case: Phishing Incident





Edit automation rule

Automation rule name *

analyze-phishing-incident

Trigger

When incident is created

Conditions

If

Title | Contains | Email reported by user as malware ...

+ Add

Actions

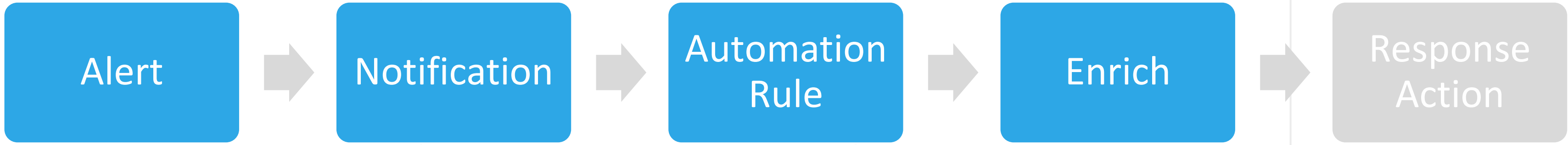
Run playbook

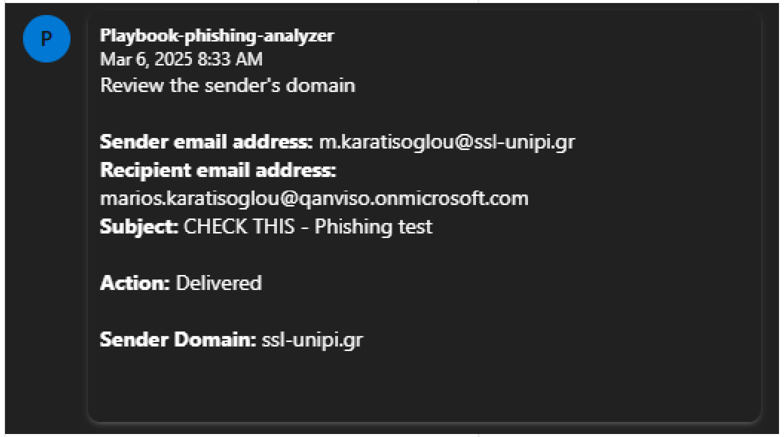
phishing-analyzer
Security Operations Engineering / cybersecurity_engineering

+ Add action

Logic Apps

Use Case: Phishing Incident



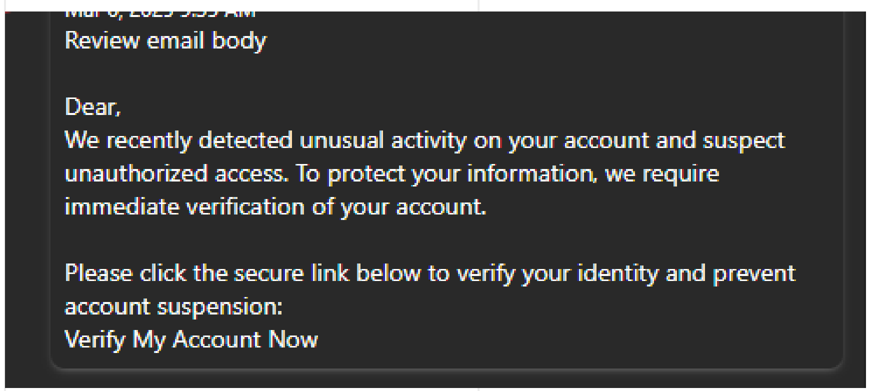


Playbook-phishing-analyzer
Mar 6, 2025 8:33 AM
Review the sender's domain

Sender email address: m.karatisoglou@ssl-unipi.gr
Recipient email address: marios.karatisoglou@qanviso.onmicrosoft.com
Subject: CHECK THIS - Phishing test

Action: Delivered

Sender Domain: ssl-unipi.gr



Mar 6, 2025 9:35 AM
Review email body

Dear,
We recently detected unusual activity on your account and suspect unauthorized access. To protect your information, we require immediate verification of your account.

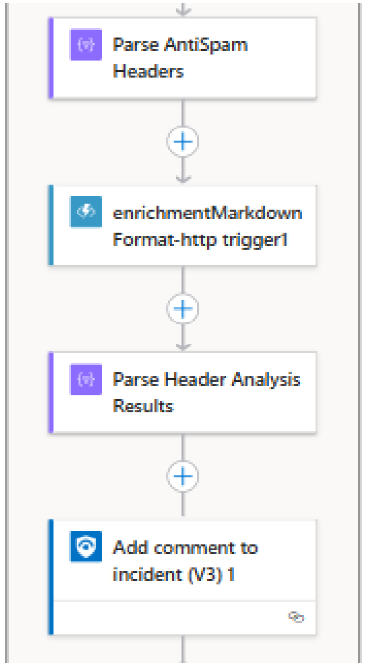
Please click the secure link below to verify your identity and prevent account suspension:
Verify My Account Now

- ☒ Email body
- Email headers
- User clicks
- Attachment

Logic Apps

Use Case: Phishing Incident

Alert → Notification → Automation Rule → Enrich → Response Action

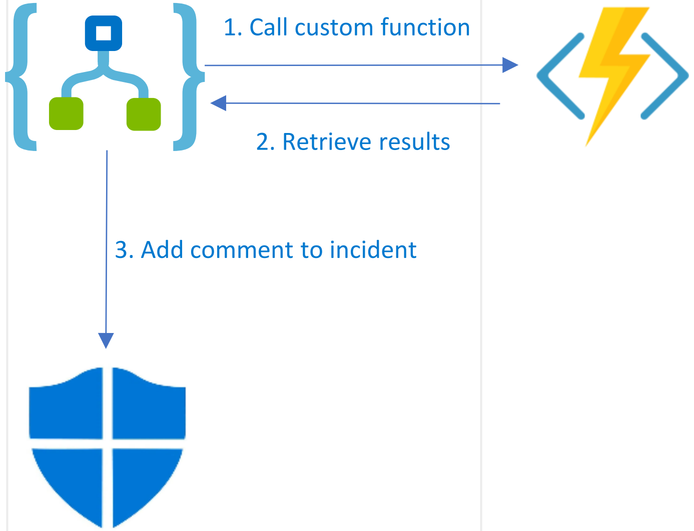


Parse AntiSpam Headers

enrichmentMarkdownFormat-http trigger1

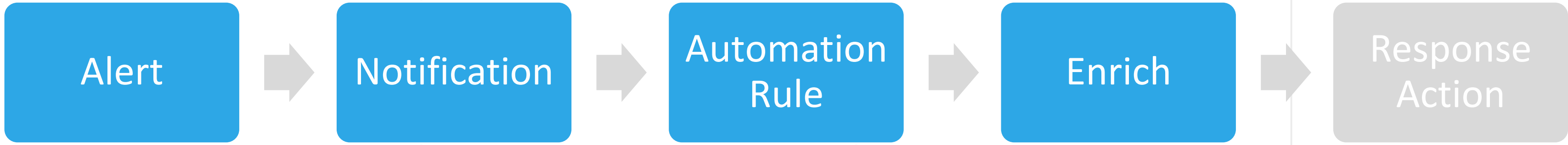
Parse Header Analysis Results

Add comment to incident (V3) 1

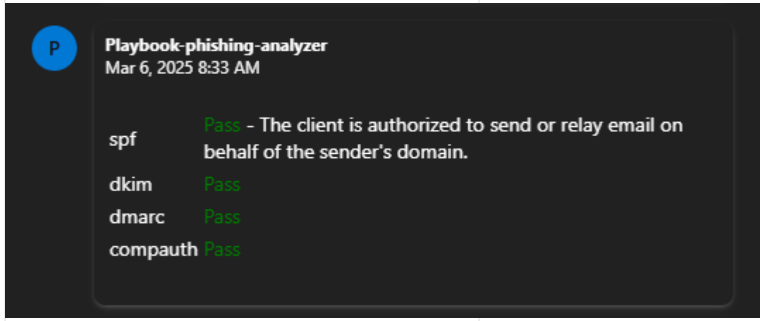


Logic Apps

Use Case: Phishing Incident

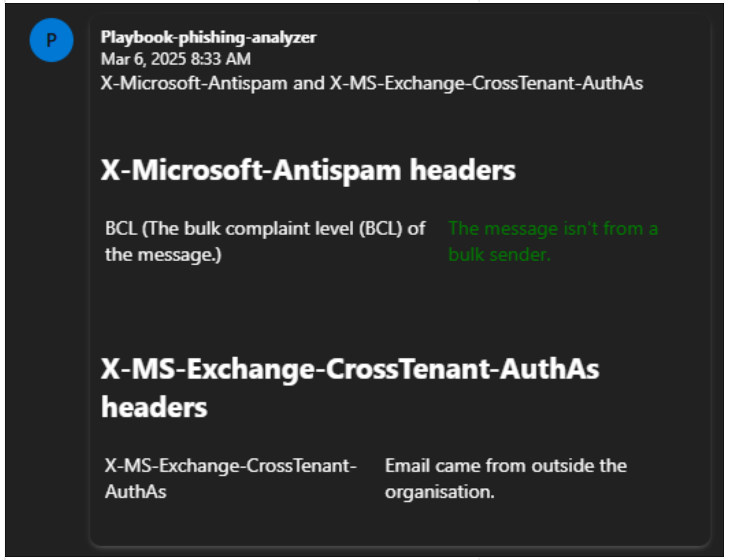


Alert → Notification → Automation Rule → Enrich → Response Action



Playbook-phishing-analyzer
Mar 6, 2025 8:33 AM

spf	Pass - The client is authorized to send or relay email on behalf of the sender's domain.
dkim	Pass
dmarc	Pass
compauth	Pass



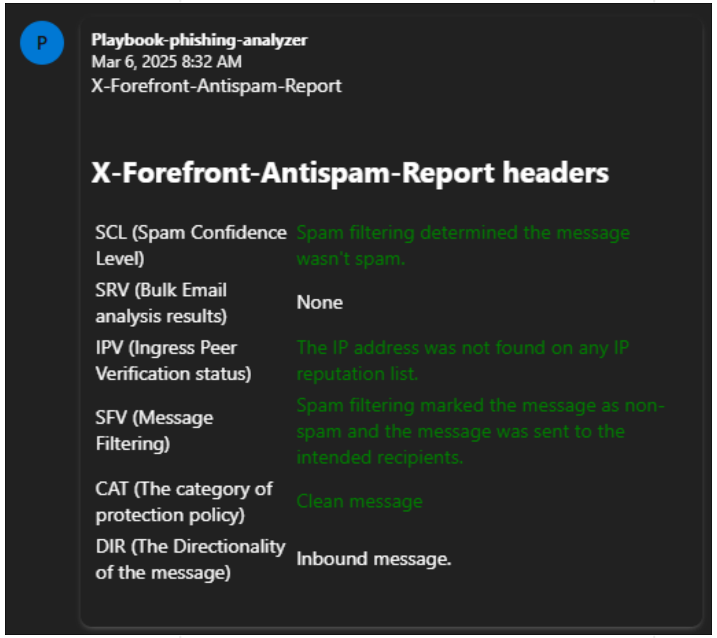
Playbook-phishing-analyzer
Mar 6, 2025 8:33 AM
X-Microsoft-Antispam and X-MS-Exchange-CrossTenant-AuthAs

X-Microsoft-Antispam headers

BCL (The bulk complaint level (BCL) of the message.)	The message isn't from a bulk sender.

X-MS-Exchange-CrossTenant-AuthAs headers

X-MS-Exchange-CrossTenant-AuthAs	Email came from outside the organisation.



Playbook-phishing-analyzer
Mar 6, 2025 8:32 AM
X-Forefront-Antispam-Report

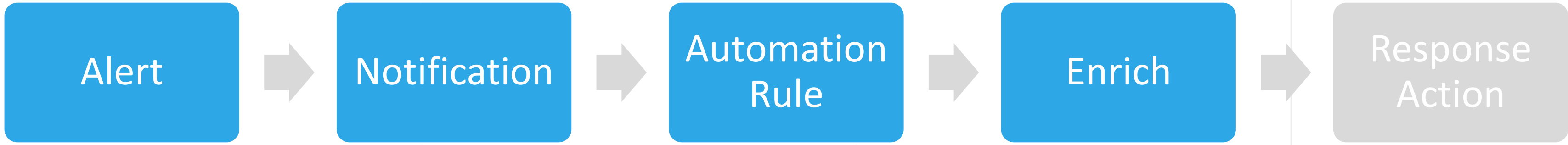
X-Forefront-Antispam-Report headers

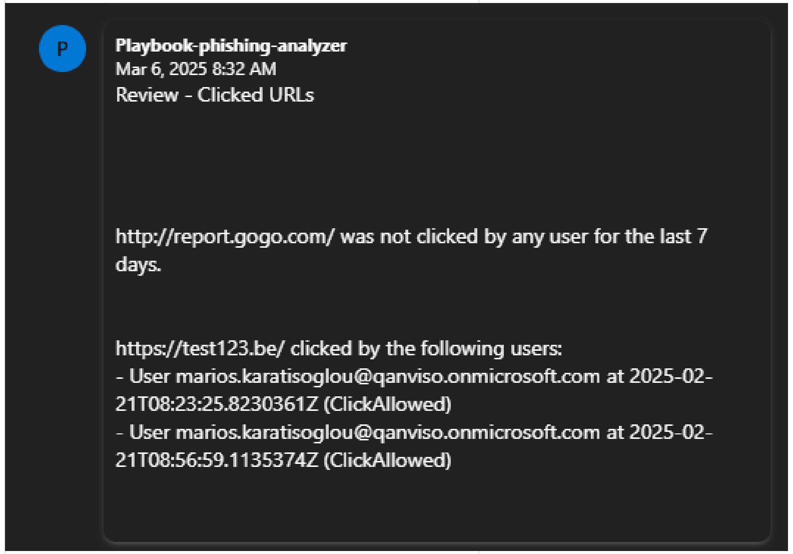
SCL (Spam Confidence Level)	Spam filtering determined the message wasn't spam.
SRV (Bulk Email analysis results)	None
IPV (Ingress Peer Verification status)	The IP address was not found on any IP reputation list.
SFV (Message Filtering)	Spam filtering marked the message as non-spam and the message was sent to the intended recipients.
CAT (The category of protection policy)	Clean message
DIR (The Directionality of the message)	Inbound message.

☒ Email body
☑ Email headers
User clicks
Attachment

Logic Apps

Use Case: Phishing Incident

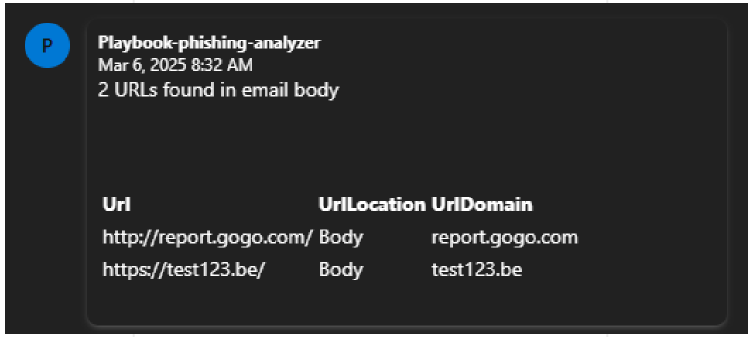




Playbook-phishing-analyzer
Mar 6, 2025 8:32 AM
Review - Clicked URLs

http://report.gogo.com/ was not clicked by any user for the last 7 days.

https://test123.be/ clicked by the following users:
- User marios.karatisoglou@qanviso.onmicrosoft.com at 2025-02-21T08:23:25.8230361Z (ClickAllowed)
- User marios.karatisoglou@qanviso.onmicrosoft.com at 2025-02-21T08:56:59.1135374Z (ClickAllowed)



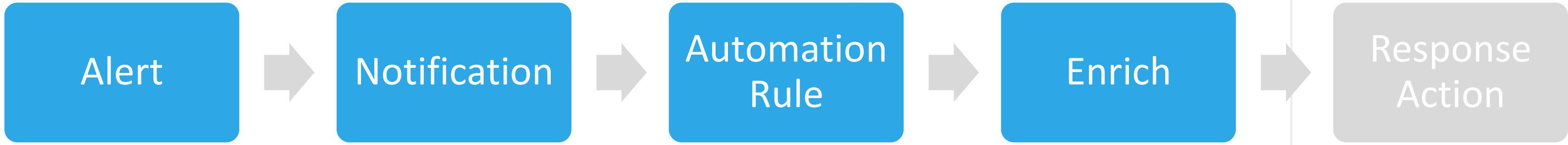
Playbook-phishing-analyzer
Mar 6, 2025 8:32 AM
2 URLs found in email body

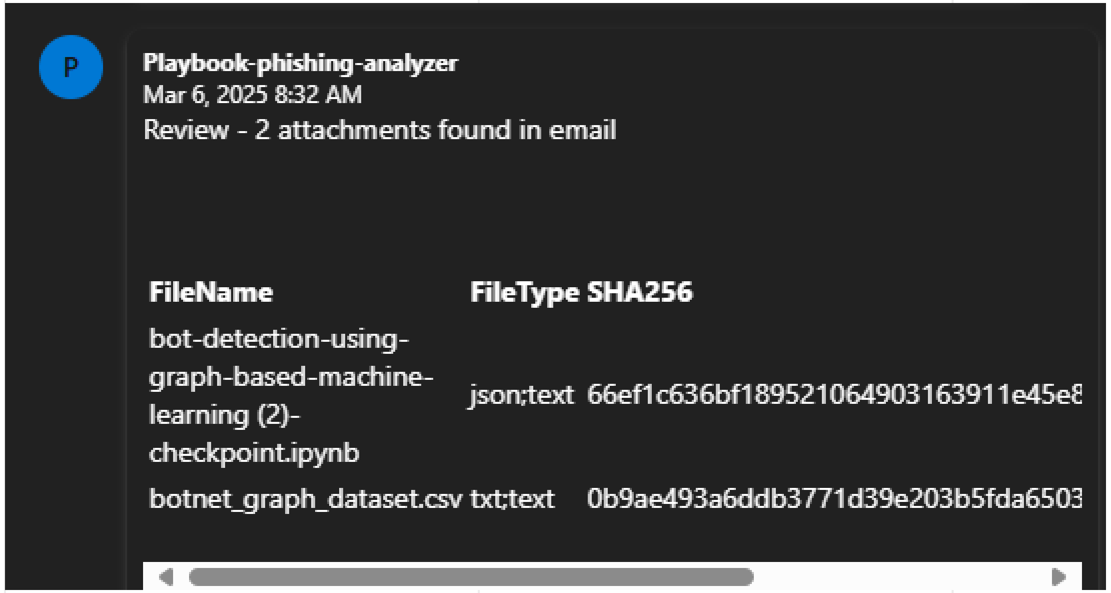
Url	UrlLocation	UrlDomain
http://report.gogo.com/	Body	report.gogo.com
https://test123.be/	Body	test123.be

☒ Email body
☑ Email headers
☒ User clicks
Attachment

Logic Apps

Use Case: Phishing Incident





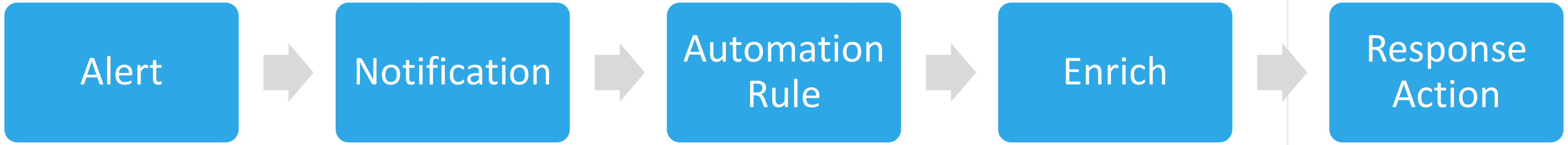
Playbook-phishing-analyzer
Mar 6, 2025 8:32 AM
Review - 2 attachments found in email

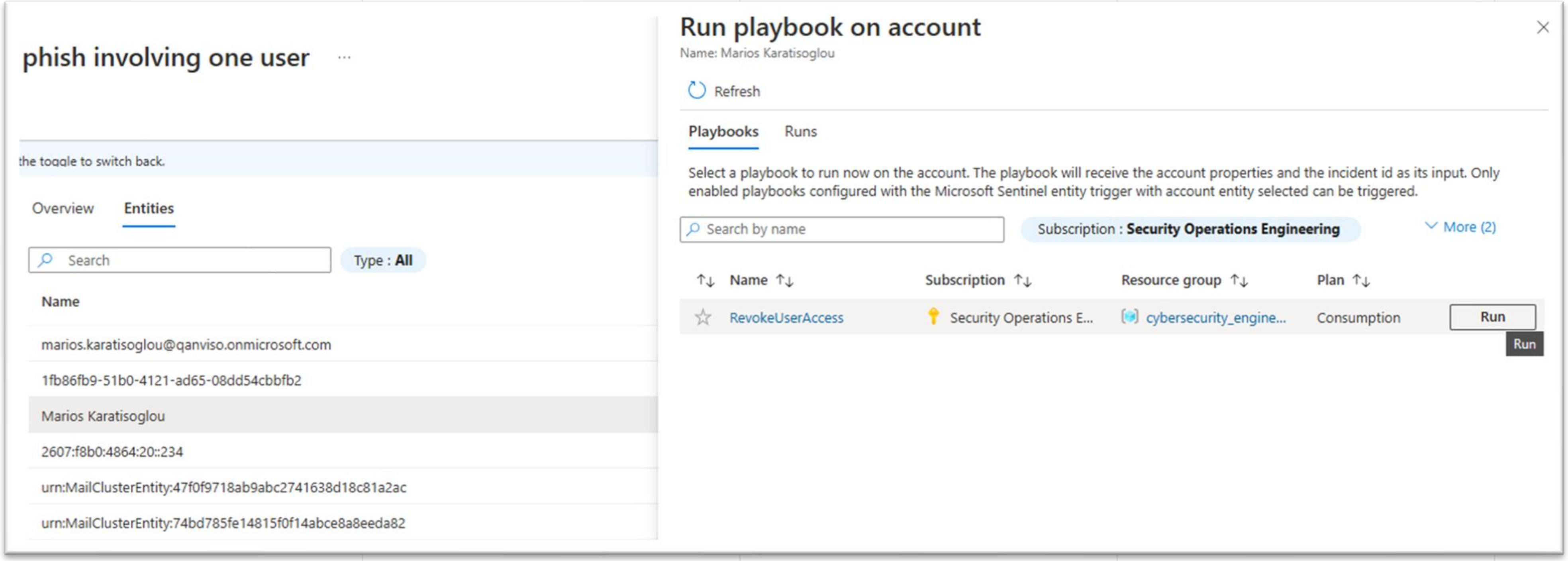
FileName	FileType	SHA256
bot-detection-using-graph-based-machine-learning (2)-checkpoint.ipynb	json;text	66ef1c636bf18952106490316391 1e45e8
botnet_graph_dataset.csv	txt;text	0b9ae493a6ddb3771d39e203b5fda6503

☒ Email body
☑ Email headers
☒ User clicks
☒ Attachment

Logic Apps

Use Case: Phishing Incident





phish involving one user ···

the toggle to switch back.

Overview | **Entities**

Search | Type : **All**

Name
marios.karatisoglou@qanviso.onmicrosoft.com
1fb86fb9-51b0-4121-ad65-08dd54cbbfb2
Marios Karatisoglou
2607:f8b0:4864:20::234
urn:MailClusterEntity:47f0f9718ab9abc2741638d18c81a2ac
urn:MailClusterEntity:74bd785fe14815f0f14abce8a8eeda82

Run playbook on account

Name: Marios Karatisoglou

Refresh

Playbooks | Runs

Select a playbook to run now on the account. The playbook will receive the account properties and the incident id as its input. Only enabled playbooks configured with the Microsoft Sentinel entity trigger with account entity selected can be triggered.

Search by name | Subscription : **Security Operations Engineering** | More (2)

	Name	Subscription	Resource group	Plan	
☆	RevokeUserAccess	Security Operations E...	cybersecurity_engine...	Consumption	Run

Thanks!
Questions?

koen.vanhees@nviso.eu