IT Track

Detect & Response: AI en automatisering in uw SOC

Anthony De Smet

Business Development

Anthony.desmet@inetum-realdolmen.world

+32 02 801 50 47

Stopping breaches demands faster incident response

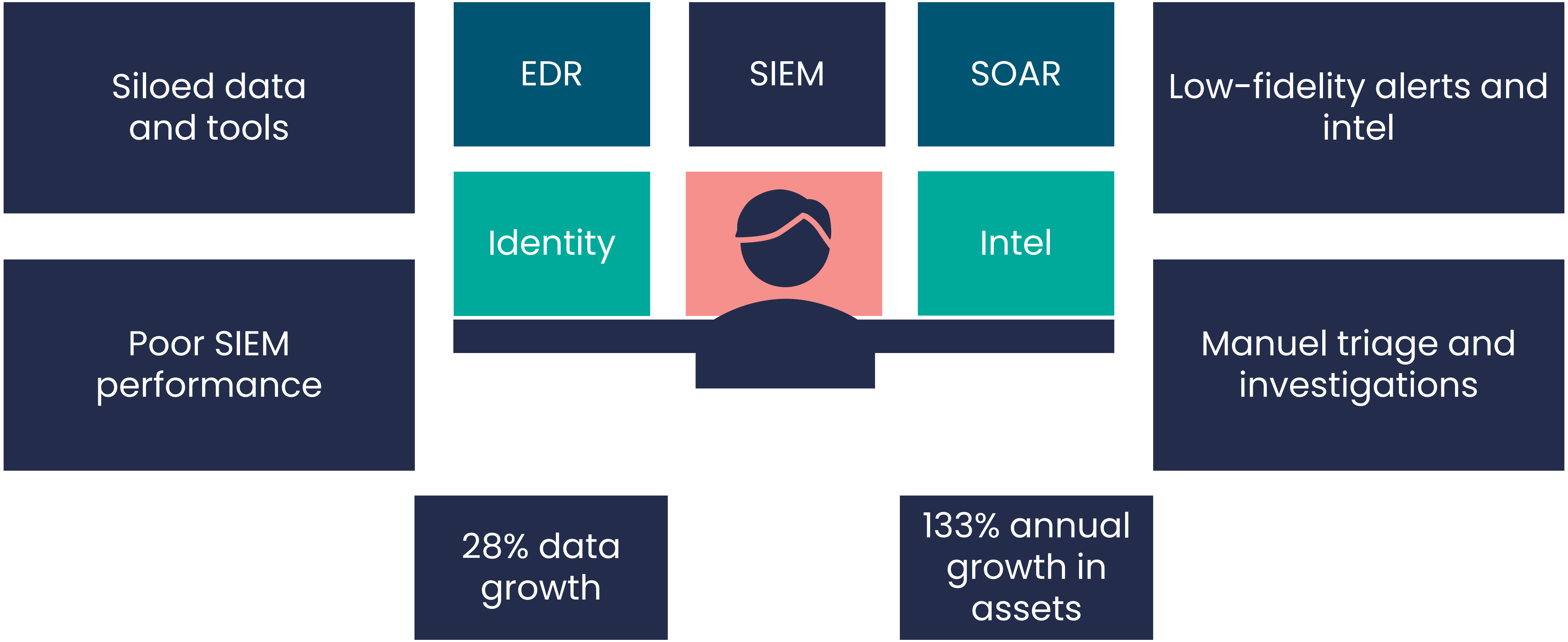
2m7s

Fastest Recorded eCrime Breakout Time

Average Breakout Time – 62min

SOC

Today’s SOCs struggle to keep up with adversaries



Siloed data and tools

EDR

SIEM

SOAR

Low-fidelity alerts and intel

Identity

Intel

Poor SIEM performance

Manuel triage and investigations

28% data growth

133% annual growth in assets

Rising attack sophistication amid a skills shortage

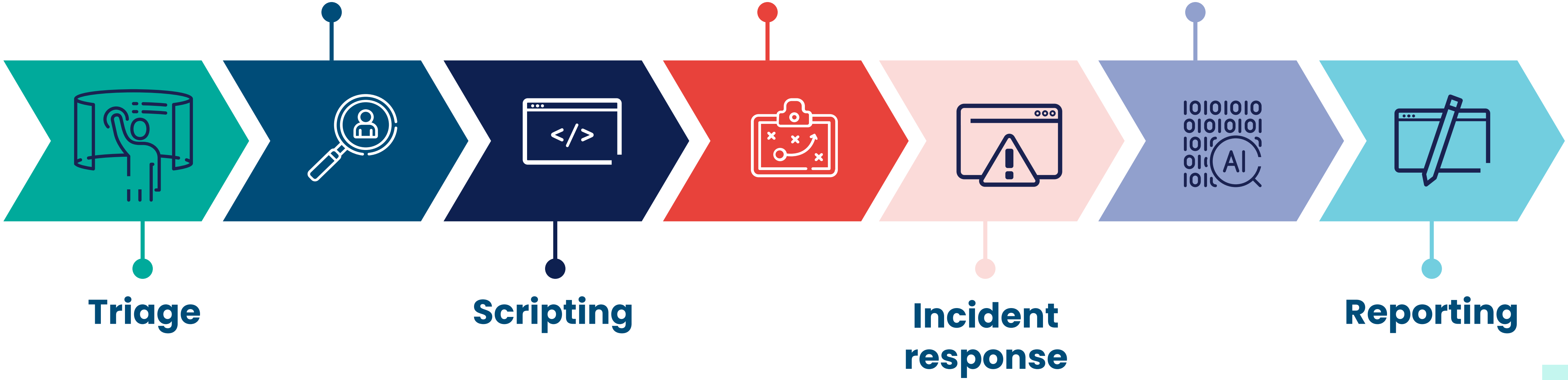
Attack surface sprawl & siloed data

Cybersecurity skills gap

Slow MTTD & MTTR

Adversary speed & sophistication

AI and automation is everywhere



Triage

Analyse

Scripting

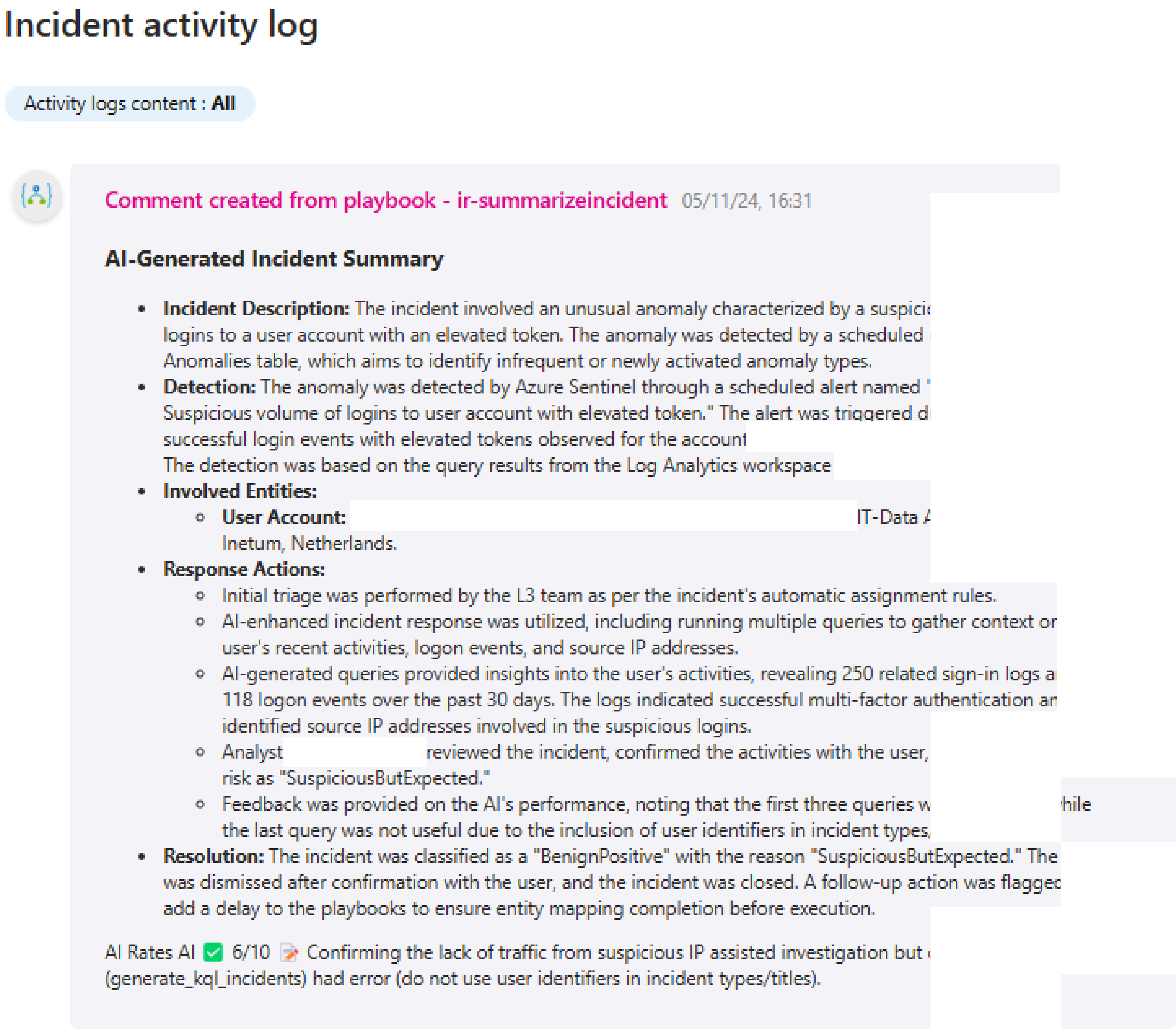
Correlation

Incident response

Suggestions

Reporting

Examples



Incident activity log

Activity logs content : **All**

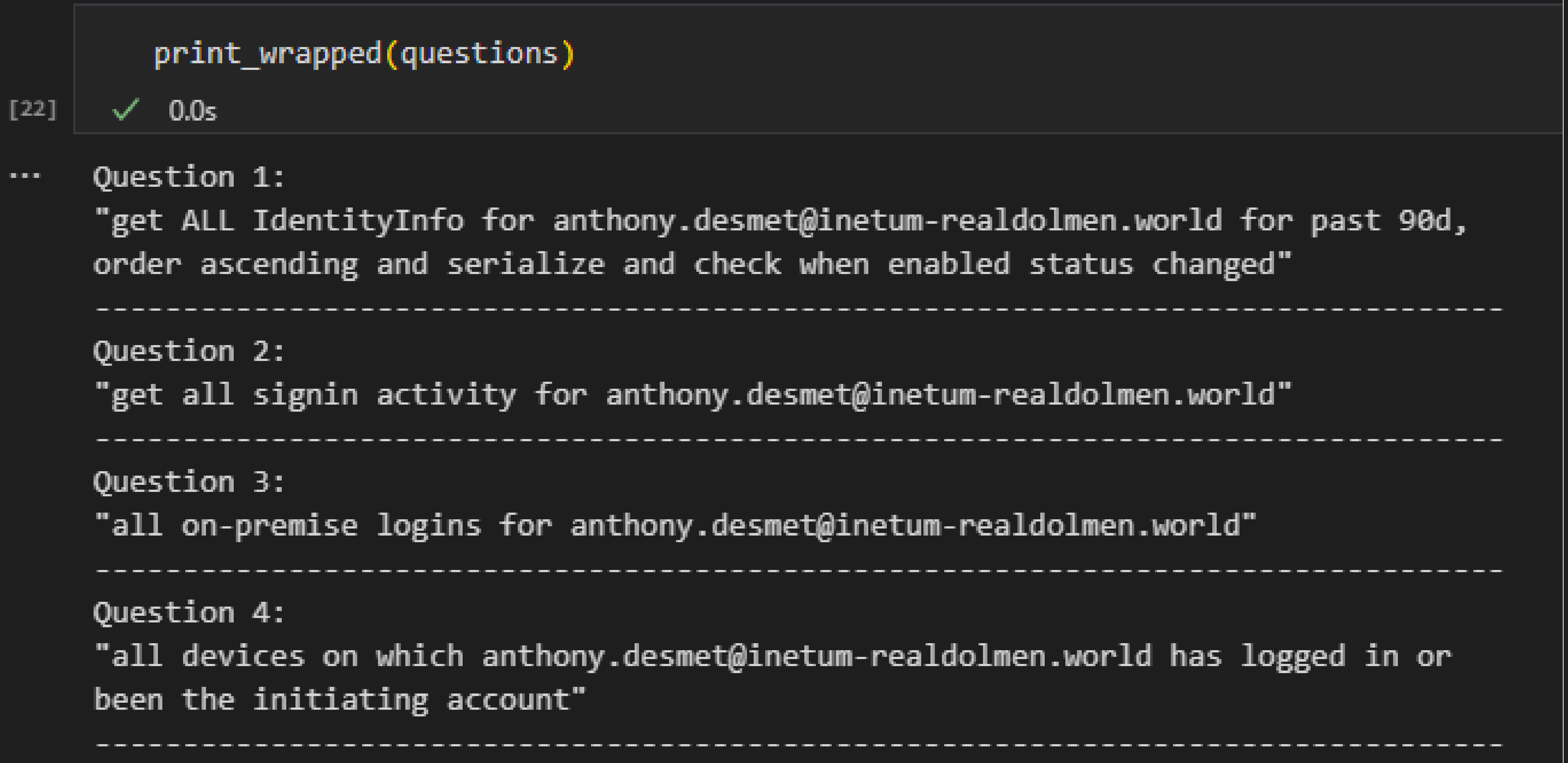
Comment created from playbook - ir-summarizeincident 05/11/24, 16:31

AI-Generated Incident Summary

- **Incident Description:** The incident involved an unusual anomaly characterized by a suspici
logins to a user account with an elevated token. The anomaly was detected by a scheduled
Anomalies table, which aims to identify infrequent or newly activated anomaly types.
- **Detection:** The anomaly was detected by Azure Sentinel through a scheduled alert named "
Suspicious volume of logins to user account with elevated token." The alert was triggered d
successful login events with elevated tokens observed for the account [redacted]
The detection was based on the query results from the Log Analytics workspace [redacted]
- **Involved Entities:**
  - **User Account:** [redacted] IT-Data A
Inetum, Netherlands.
- **Response Actions:**
  - Initial triage was performed by the L3 team as per the incident's automatic assignment rules.
  - AI-enhanced incident response was utilized, including running multiple queries to gather context or
user's recent activities, logon events, and source IP addresses.
  - AI-generated queries provided insights into the user's activities, revealing 250 related sign-in logs a
118 logon events over the past 30 days. The logs indicated successful multi-factor authentication ar
identified source IP addresses involved in the suspicious logins.
  - Analyst [redacted] reviewed the incident, confirmed the activities with the user,
risk as "SuspiciousButExpected."
  - Feedback was provided on the AI's performance, noting that the first three queries w hile
the last query was not useful due to the inclusion of user identifiers in incident types,
- **Resolution:** The incident was classified as a "BenignPositive" with the reason "SuspiciousButExpected." The
was dismissed after confirmation with the user, and the incident was closed. A follow-up action was flagged
add a delay to the playbooks to ensure entity mapping completion before execution.

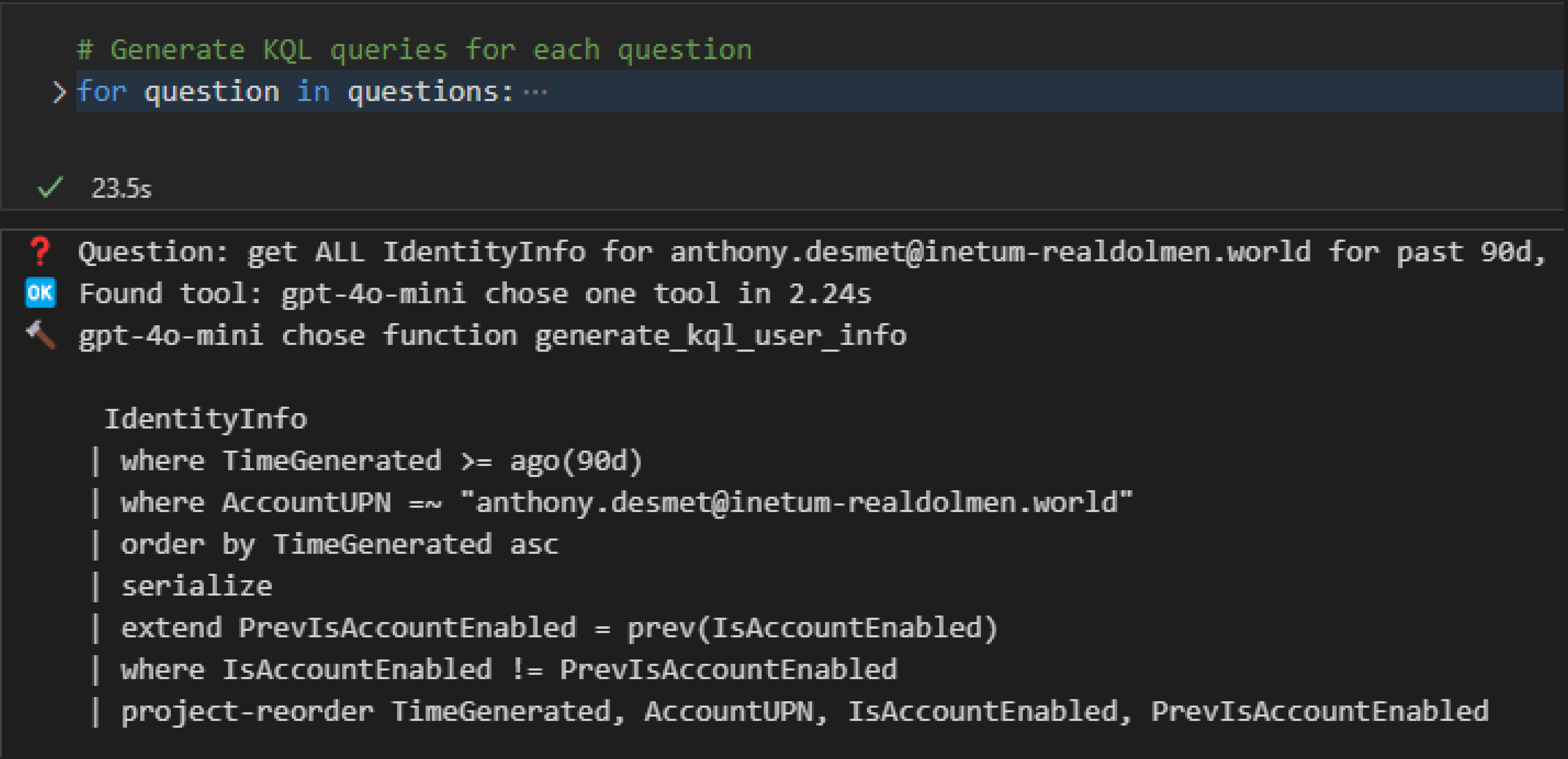
AI Rates AI ✅ 6/10 📝 Confirming the lack of traffic from suspicious IP assisted investigation but
(generate_kql_incidents) had error (do not use user identifiers in incident types/titles).

Questions to convert to KQL



```
print_wrapped(questions)
```

```
Question 1:
"get ALL IdentityInfo for anthony.desmet@inetum-realdolmen.world for past 90d,
order ascending and serialize and check when enabled status changed"
----------------------------------------------------------------------------------
Question 2:
"get all signin activity for anthony.desmet@inetum-realdolmen.world"
----------------------------------------------------------------------------------
Question 3:
"all on-premise logins for anthony.desmet@inetum-realdolmen.world"
----------------------------------------------------------------------------------
Question 4:
"all devices on which anthony.desmet@inetum-realdolmen.world has logged in or
been the initiating account"
----------------------------------------------------------------------------------
```



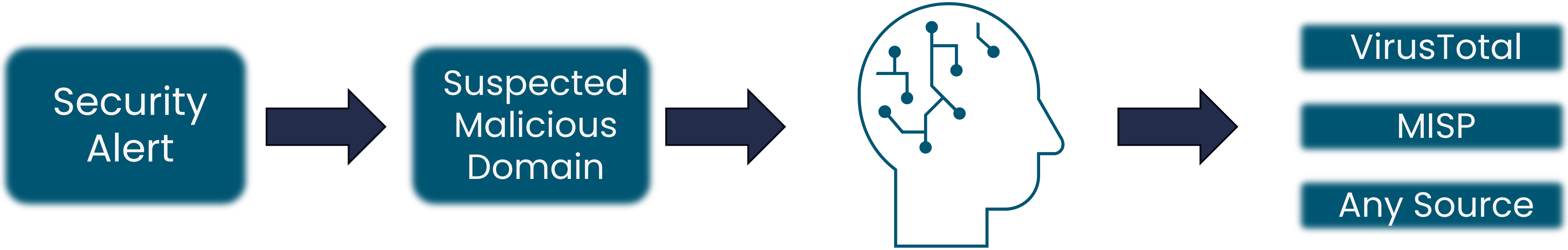
```
# Generate KQL queries for each question
for question in questions:···
```

✓ 23.5s

```
❓ Question: get ALL IdentityInfo for anthony.desmet@inetum-realdolmen.world for past 90d,
🆗 Found tool: gpt-4o-mini chose one tool in 2.24s
🔨 gpt-4o-mini chose function generate_kql_user_info

   IdentityInfo
  | where TimeGenerated >= ago(90d)
  | where AccountUPN =~ "anthony.desmet@inetum-realdolmen.world"
  | order by TimeGenerated asc
  | serialize
  | extend PrevIsAccountEnabled = prev(IsAccountEnabled)
  | where IsAccountEnabled != PrevIsAccountEnabled
  | project-reorder TimeGenerated, AccountUPN, IsAccountEnabled, PrevIsAccountEnabled
```

The SOC Journey: From Basic Automation to AI in Cybersecurity



Security Alert

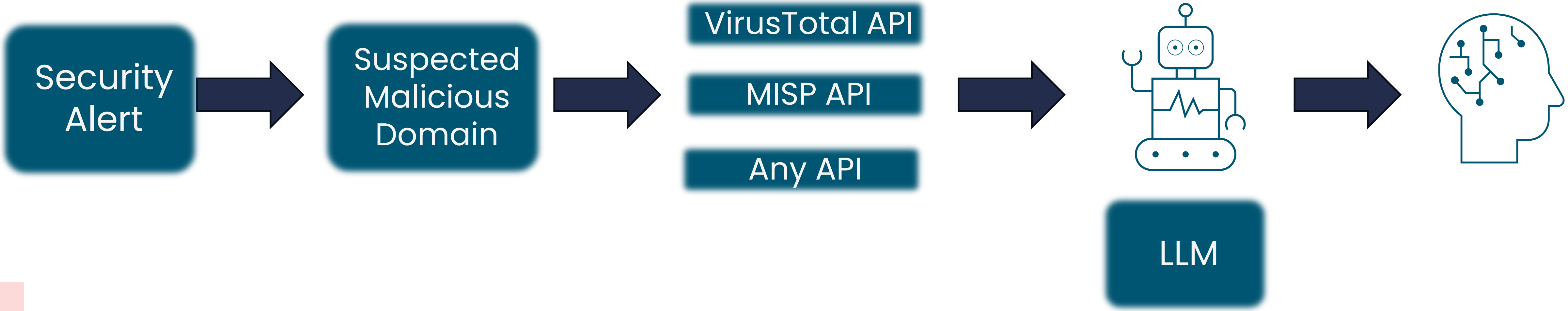
Suspected Malicious Domain

VirusTotal

MISP

Any Source

The SOC Journey: From Basic Automation to AI in Cybersecurity



Security Alert

Suspected Malicious Domain

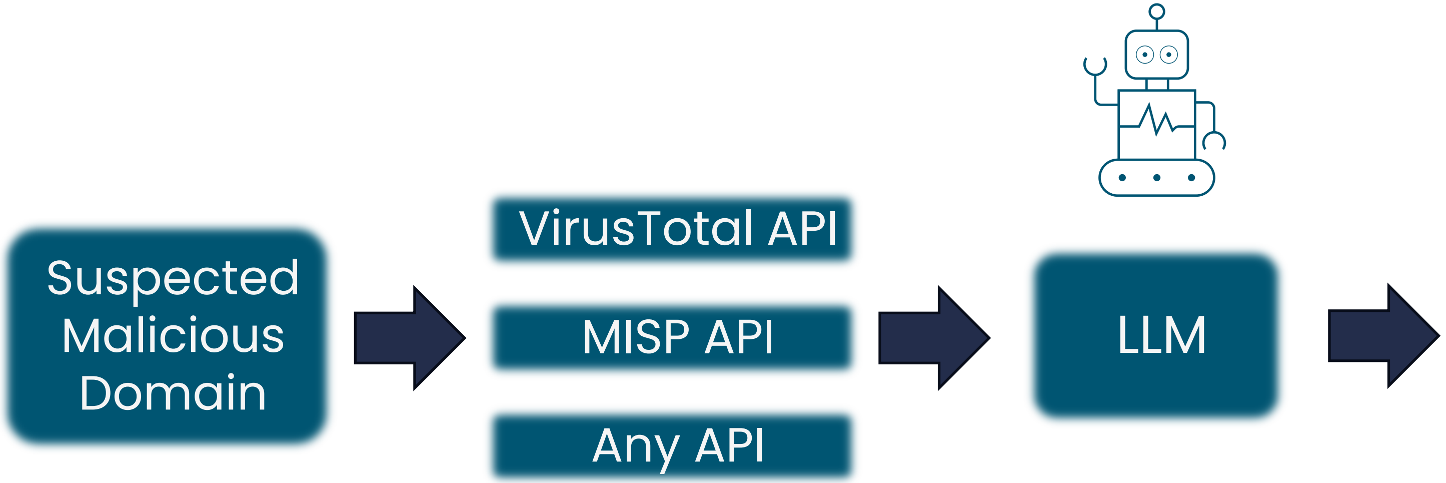
VirusTotal API

MISP API

Any API

LLM

The SOC Journey: From Basic Automation to AI in Cybersecurity

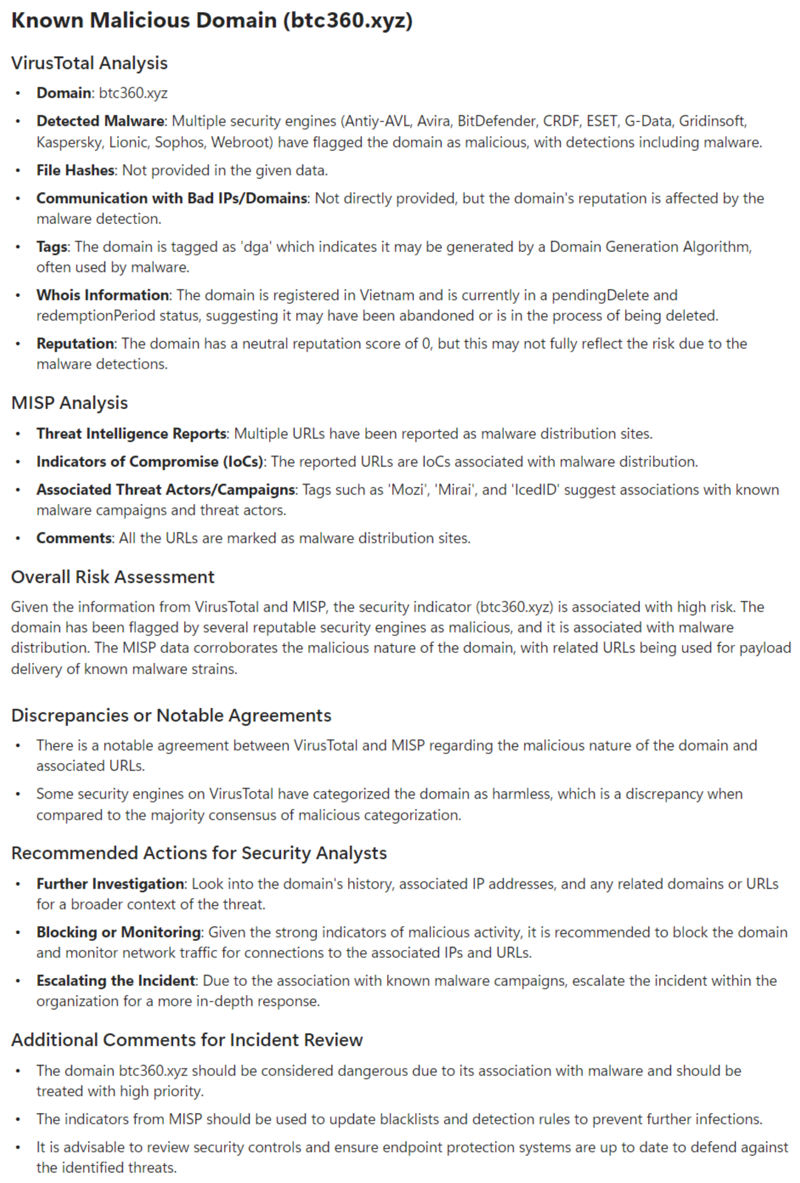

Suspected Malicious Domain

VirusTotal API

MISP API

Any API

LLM


Known Malicious Domain (btc360.xyz)

VirusTotal Analysis

- **Domain**: btc360.xyz
- **Detected Malware**: Multiple security engines (Antiy-AVL, Avira, BitDefender, CRDF, ESET, G-Data, Gridinsoft, Kaspersky, Lionic, Sophos, Webroot) have flagged the domain as malicious, with detections including malware.
- **File Hashes**: Not provided in the given data.
- **Communication with Bad IPs/Domains**: Not directly provided, but the domain's reputation is affected by the malware detection.
- **Tags**: The domain is tagged as 'dga' which indicates it may be generated by a Domain Generation Algorithm, often used by malware.
- **Whois Information**: The domain is registered in Vietnam and is currently in a pendingDelete and redemptionPeriod status, suggesting it may have been abandoned or is in the process of being deleted.
- **Reputation**: The domain has a neutral reputation score of 0, but this may not fully reflect the risk due to the malware detections.

MISP Analysis

- **Threat Intelligence Reports**: Multiple URLs have been reported as malware distribution sites.
- **Indicators of Compromise (IoCs)**: The reported URLs are IoCs associated with malware distribution.
- **Associated Threat Actors/Campaigns**: Tags such as 'Mozi', 'Mirai', and 'IcedID' suggest associations with known malware campaigns and threat actors.
- **Comments**: All the URLs are marked as malware distribution sites.

Overall Risk Assessment

Given the information from VirusTotal and MISP, the security indicator (btc360.xyz) is associated with high risk. The domain has been flagged by several reputable security engines as malicious, and it is associated with malware distribution. The MISP data corroborates the malicious nature of the domain, with related URLs being used for payload delivery of known malware strains.

Discrepancies or Notable Agreements

- There is a notable agreement between VirusTotal and MISP regarding the malicious nature of the domain and associated URLs.
- Some security engines on VirusTotal have categorized the domain as harmless, which is a discrepancy when compared to the majority consensus of malicious categorization.

Recommended Actions for Security Analysts

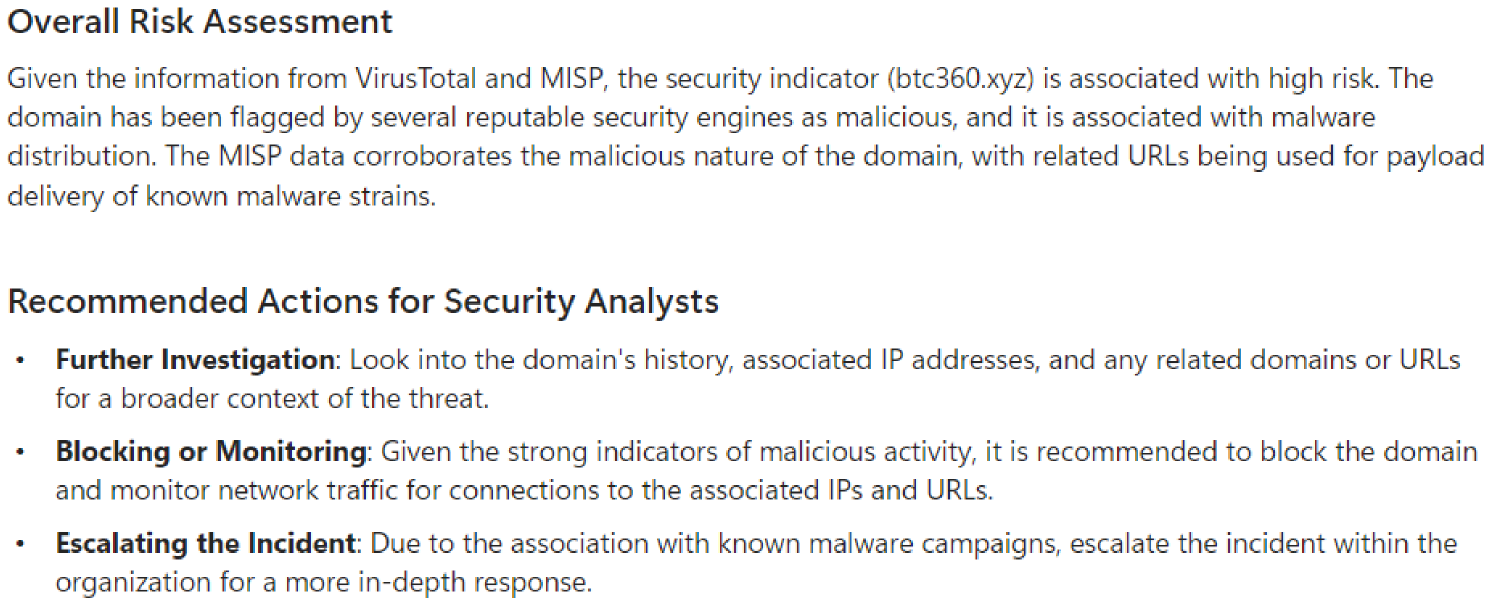
- **Further Investigation**: Look into the domain's history, associated IP addresses, and any related domains or URLs for a broader context of the threat.
- **Blocking or Monitoring**: Given the strong indicators of malicious activity, it is recommended to block the domain and monitor network traffic for connections to the associated IPs and URLs.
- **Escalating the Incident**: Due to the association with known malware campaigns, escalate the incident within the organization for a more in-depth response.

Additional Comments for Incident Review

- The domain btc360.xyz should be considered dangerous due to its association with malware and should be treated with high priority.
- The indicators from MISP should be used to update blacklists and detection rules to prevent further infections.
- It is advisable to review security controls and ensure endpoint protection systems are up to date to defend against the identified threats.

The SOC Journey: From Basic Automation to AI in Cybersecurity

LLM



Overall Risk Assessment

Given the information from VirusTotal and MISP, the security indicator (btc360.xyz) is associated with high risk. The domain has been flagged by several reputable security engines as malicious, and it is associated with malware distribution. The MISP data corroborates the malicious nature of the domain, with related URLs being used for payload delivery of known malware strains.

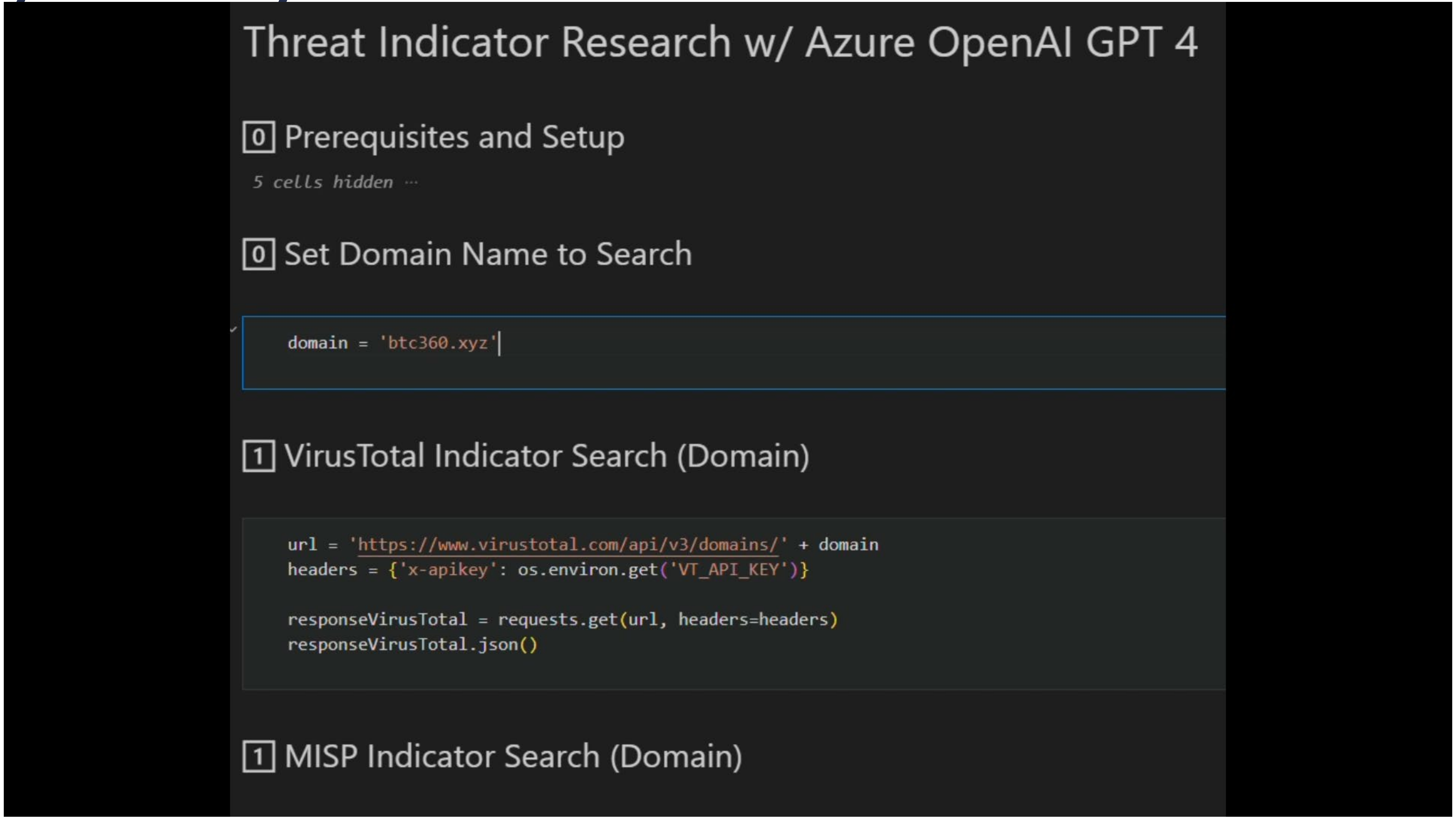
Recommended Actions for Security Analysts

- **Further Investigation**: Look into the domain's history, associated IP addresses, and any related domains or URLs for a broader context of the threat.
- **Blocking or Monitoring**: Given the strong indicators of malicious activity, it is recommended to block the domain and monitor network traffic for connections to the associated IPs and URLs.
- **Escalating the Incident**: Due to the association with known malware campaigns, escalate the incident within the organization for a more in-depth response.

Add to Incident Comments

Start Investigation

The SOC Journey: From Basic Automation to AI in Cybersecurity



Threat Indicator Research w/ Azure OpenAI GPT 4

0 Prerequisites and Setup

5 cells hidden ...

0 Set Domain Name to Search

```
domain = 'btc360.xyz'
```

1 VirusTotal Indicator Search (Domain)

```
url = 'https://www.virustotal.com/api/v3/domains/' + domain
headers = {'x-apikey': os.environ.get('VT_API_KEY')}

responseVirusTotal = requests.get(url, headers=headers)
responseVirusTotal.json()
```

1 MISP Indicator Search (Domain)

inetum

Thank you