Modern SecOps

11/03/2025 – SHIELD VZW Event

Maxim Deweerdt

NVISO

Modern SecOps

Key Issues and Critical Success Factors

Key issues

Of a highly functioning SOC

Expensive

Alert Fatigue

Skill Shortage

Ever-Expanding Landscape

Critical Success Factors

Of a highly functioning SOC

SOAR-Centric

Automation-First

AI Powered

Human Brainpower

Modern SecOps

The first step was automation

SOAR

Security Orchestration, Automation and Response (SOAR) tools refer to a collection of tools that help organizations coordinate, execute and automate tasks between security tools and people. They are composed of **4 main blocks**:

Integration with security tools with plugins to build **security playbooks** to automate tasks and respond to alerts automatically.

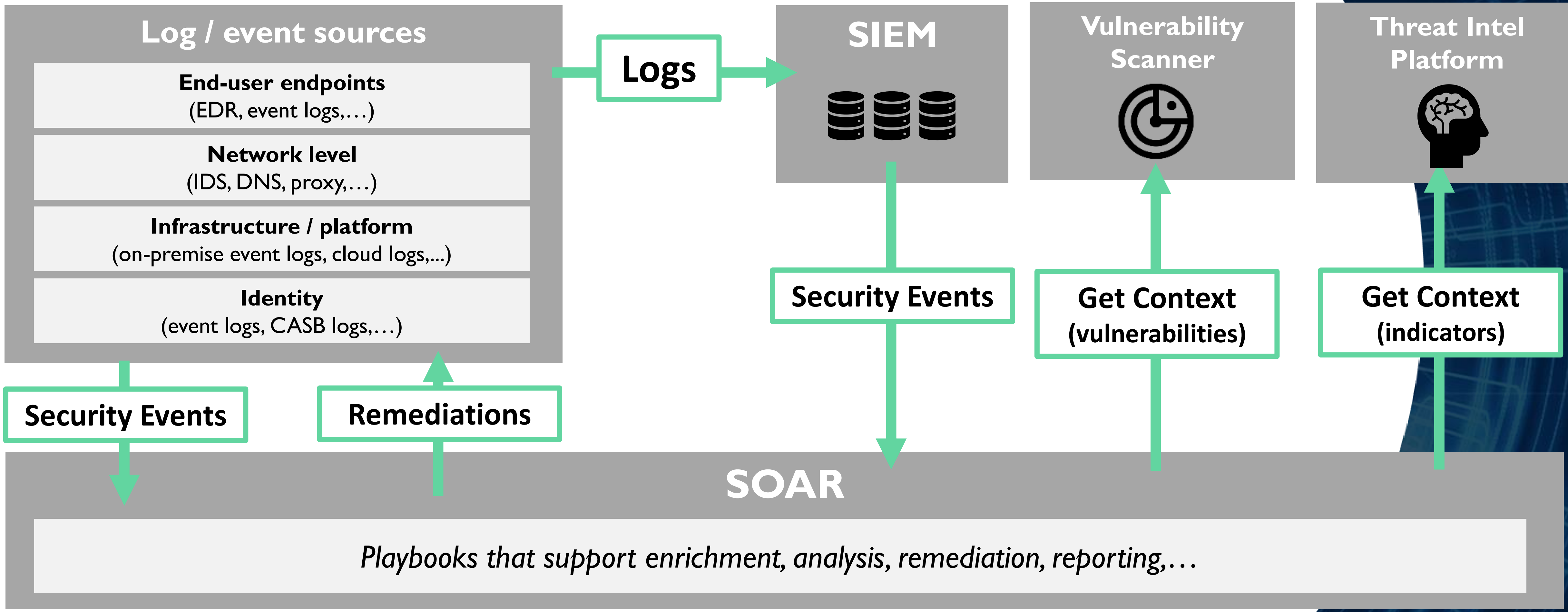
Present **contextualized** information and **enriched** alerts to allow analysts to **take decisions and actions quickly**.

Provide **reports and insights** about manual and automatic actions and about possible improvements.

Provide one **single centralized platform** for analysts with all the **dashboards** and **alerts** from the different sources.

Modern SecOps

SOAR-Centric Architecture



Log / event sources

End-user endpoints
(EDR, event logs,…)

Network level
(IDS, DNS, proxy,…)

Infrastructure / platform
(on-premise event logs, cloud logs,...)

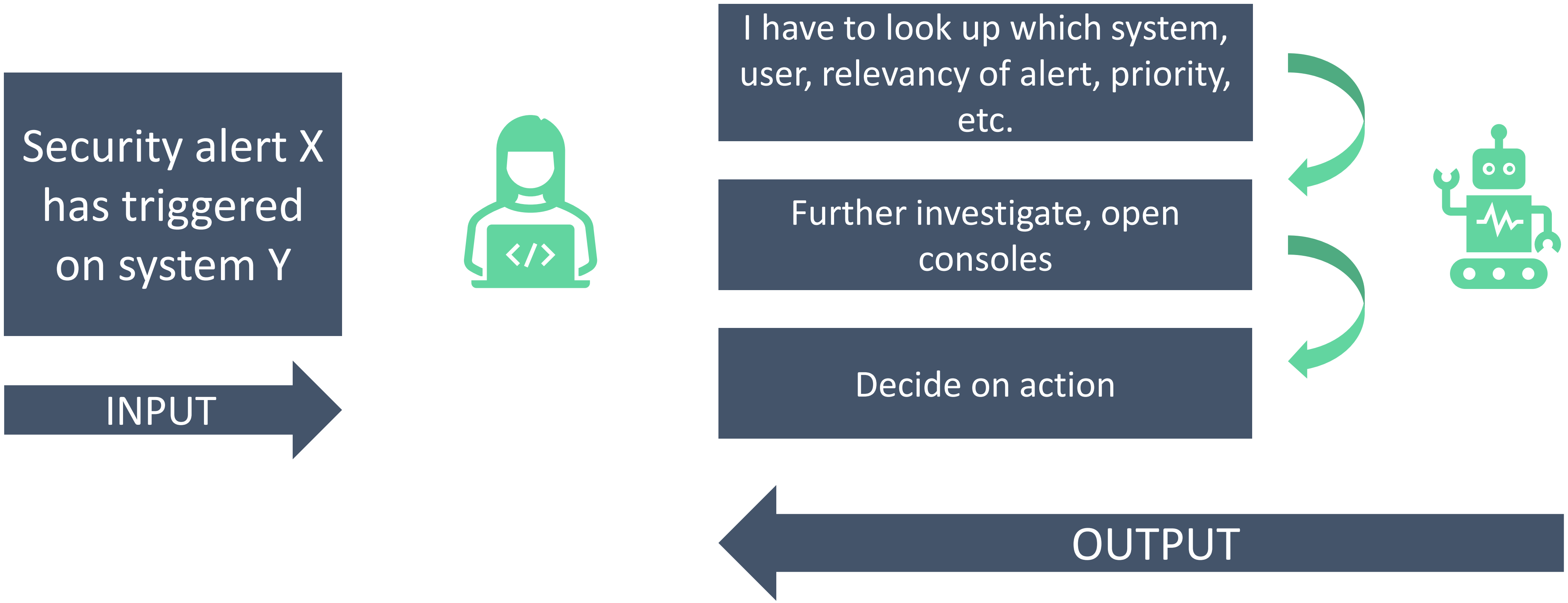
Identity
(event logs, CASB logs,…)

Playbooks that support enrichment, analysis, remediation, reporting,…

The **SOAR platform becomes the "central brain"** of the Fusion Center (instead of the SIEM).
All security technologies should be connected to the SOAR (both for detection, contextualisation, handling, reporting and remediation)

Modern SecOps

The human process



Security alert X has triggered on system Y

INPUT

I have to look up which system, user, relevancy of alert, priority, etc.

Further investigate, open consoles

Decide on action

OUTPUT

SOAR helps to automate **menial tasks** and **simple actions**

Modern SecOps

The first step was automation

Given the **ever-expanding technology landscape** and the **global talent shortage**, automation is no longer a nice-to-have in Security Operations. Some examples where automation plays a pivotal role to prevent, detect and respond to incidents:

PREVENT

Desired State Configuration
Automated Patch Roll-Out
Infrastructure-as-code scanning
Privilege Management
Posture Management (e.g. CSPM)

DETECT

Analytical Playbooks
Automated testing of detection analytics

RESPOND

Automated Response / Remediation Playbooks

Do you see any other big use cases for automation?

Modern SecOps

Why is automation so important?

L1 Security Analyst Industry Stats:

20 Minutes Per Security Event

25 security events per day

Industry reports indicate that we are lacking two million personnel worldwide… So how does a Security Operations team deal with this? **Automation** is a key component:

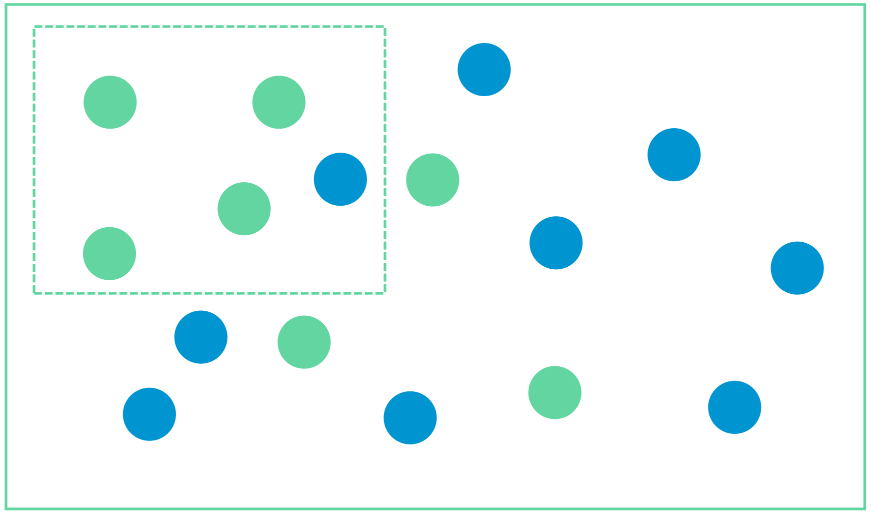
647 Security Events = 26 Analysts
24x7 = 12 Analysts Minimum

For specific incident types (e.g. access anomalies), **automation** has decreased the analytical workload by **97.42%.**

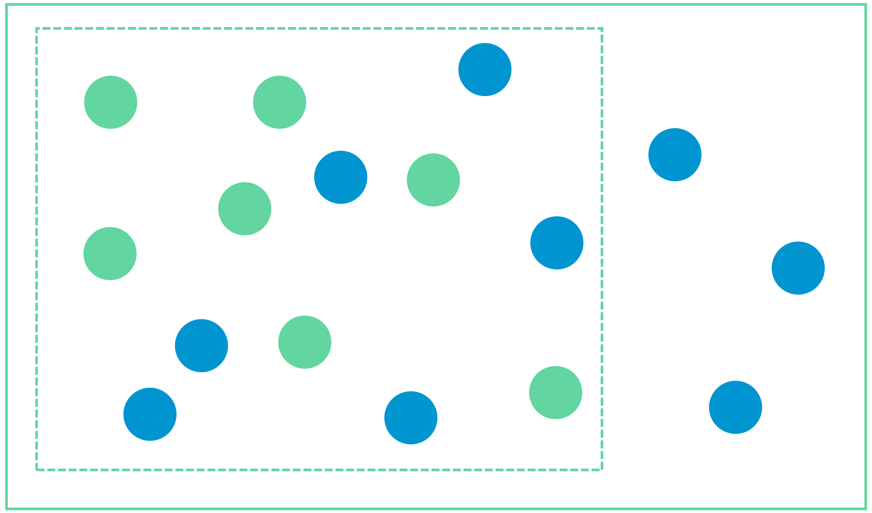
Modern SecOps

Automation allows us to tune for recall

After designing an Anomaly Detection Use Case, the bulk of the work is tuning the parameters to improve precision and recall



Tuned for precision:
High TP rate, but high FN rate
→ **Not acceptable**



Tuned for recall:
High TP rate, but high FP rate
→ **Higher Workload**

🟢 = Relevant

🔵 = Irrelevant

Modern SecOps

A perfect marriage between humans and robots

1. A user reports a suspected phishing email (e.g. using Outlook button) 🤖
2. Automatic check for URLs and Indicators of Compromise (IoCs) 🤖
3. Based on available data / context, make decision on benign / malicious 👤
4. If confirmed malicious, scan the user endpoint for malware 🤖
5. Block incoming e-mails with similar properties (URLs, sender, subject,…) 🤖
6. Automatically remove already delivered e-mails from mailboxes 🤖
7. Provide feedback to reporter + warn others about the phishing attack 🤖

Modern SecOps

Dealing with access anomalies

“Geographically improbable log-on for user Maxim Deweerdt”

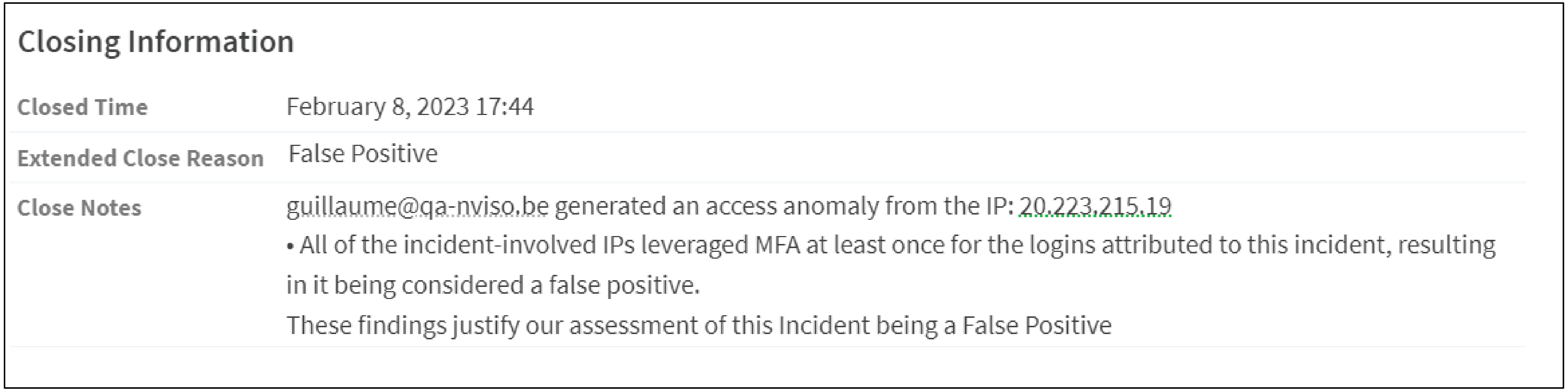
Enrich: Add privileges of user Maxim Deweerdt to security event
Enrich: Add insights & reputation of source IP address to security event
Enrich: Add whether or not MFA was used in authentication to security event
Enrich: Add historic locations used by Maxim Deweerdt to security event
Enrich: Add security risk score for user Maxim Deweerdt to security event
Enrich: Add info on workstation security alerts for Maxim Deweerdt ’s workstation to security event
Enrich:…

Decide: Confirm whether, based on the above enrichments, a false positive can be confirmed

Remediate: When confirmed true positive (and allow-listed for remediation), execute remediation action
Present: When unsure, present enriched security event to analyst for further follow-up & analysis

Modern SecOps

Dealing with access anomalies

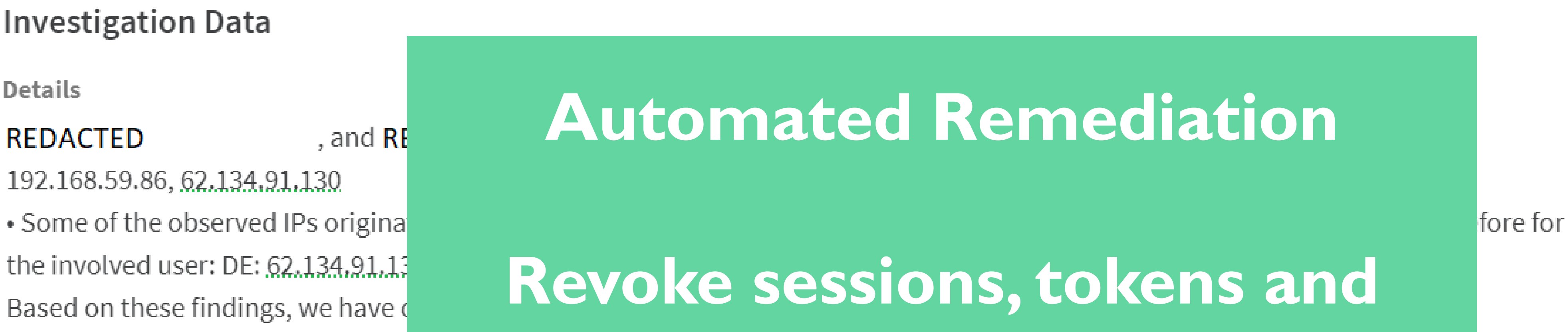


Closing Information

Closed Time	February 8, 2023 17:44
Extended Close Reason	False Positive
Close Notes	guillaume@qa-nviso.be generated an access anomaly from the IP: 20.223.215.19 • All of the incident-involved IPs leveraged MFA at least once for the logins attributed to this incident, resulting in it being considered a false positive. These findings justify our assessment of this Incident being a False Positive

Modern SecOps

Dealing with access anomalies



Investigation Data

Details

REDACTED , and RE

192.168.59.86, 62.134.91.130

• Some of the observed IPs origina fore for

the involved user: DE: 62.134.91.13

Based on these findings, we have c

Automated Remediation

Revoke sessions, tokens and reset credentials

Modern SecOps

NVISO’s offering to SHIELD members

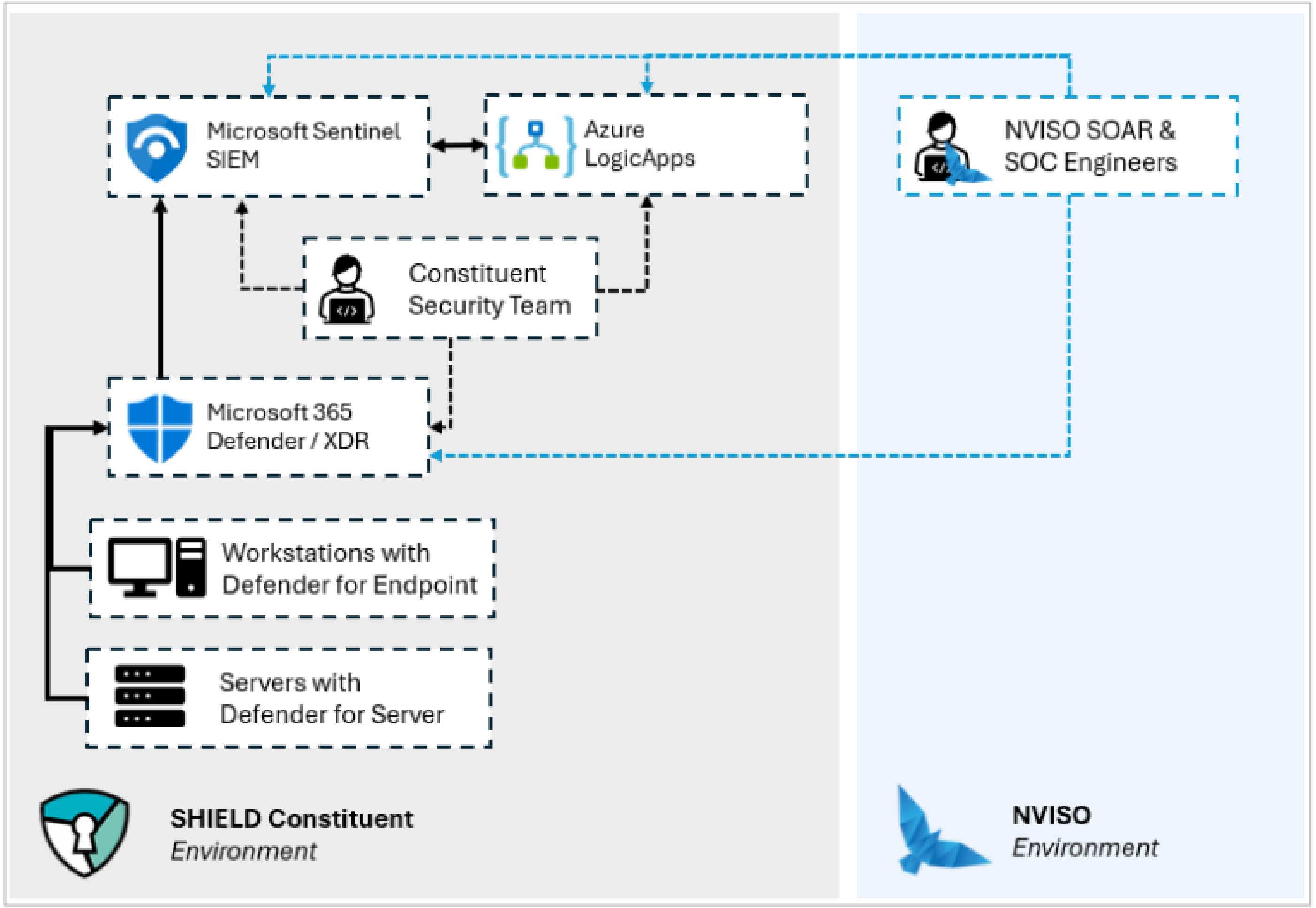
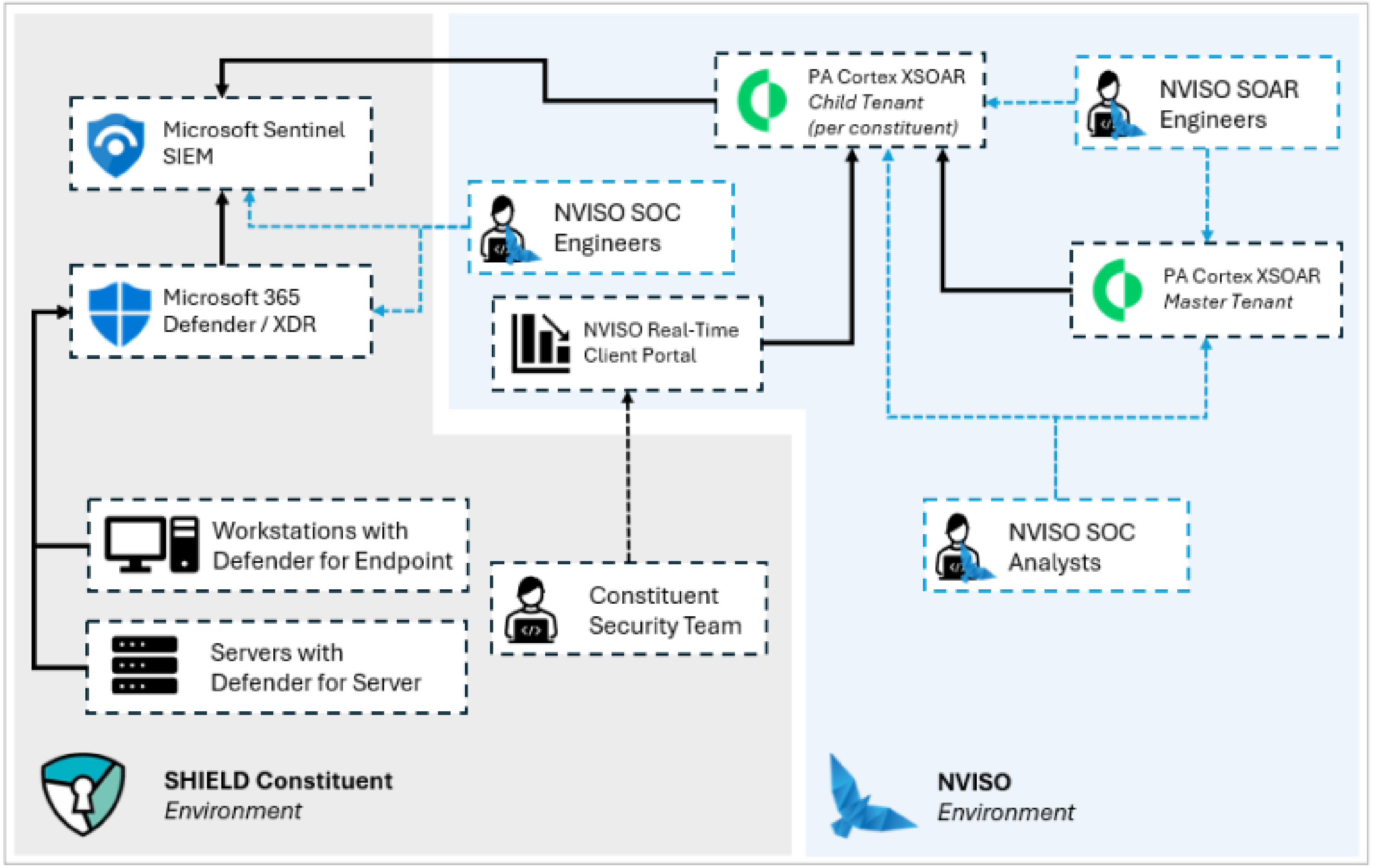


Figure: Architecture without MDR services

Modern SecOps

NVISO's offering to SHIELD members



Microsoft Sentinel SIEM
PA Cortex XSOAR *Child Tenant* *(per constituent)*
NVISO SOAR Engineers
NVISO SOC Engineers
Microsoft 365 Defender / XDR
NVISO Real-Time Client Portal
PA Cortex XSOAR *Master Tenant*
Workstations with Defender for Endpoint
Constituent Security Team
NVISO SOC Analysts
Servers with Defender for Server
SHIELD Constituent *Environment*
NVISO *Environment*

Figure: Proposed architecture with MDR services

Modern SecOps

The human process

I have to create a new detection rule

I have to process the output from SOAR

I have to figure out how to do X

GenAI **assists** humans in **solving complex problems using our language**

AI as a force multiplier

The first step was automation

Given the **ever-expanding technology landscape** and the **global talent shortage**, automation is no longer a nice-to-have in Security Operations. Some examples where automation plays a pivotal role to prevent, detect and respond to incidents:

PREVENT

- Desired State Configuration
- Automated Patch Roll-Out
- Infrastructure-as-code scanning
- Privilege Management
- Posture Management (e.g. CSPM)

DETECT

- Analytical Playbooks
- Automated testing of detection analytics

RESPOND

- Automated Response / Remediation Playbooks

Do you see any other big use cases for automation?

AI as a force multiplier

The first step was automation

SOAR

Security Orchestration, Automation and Response (SOAR) tools refer to a collection of tools that help organizations coordinate, execute and automate tasks between security tools and people. They are composed of **4 main blocks**:

Integration with security tools with plugins to build **security playbooks** to automate tasks and respond to alerts automatically.

Present **contextualized** information and **enriched** alerts to allow analysts to **take decisions and actions quickly**.

Provide **reports and insights** about manual and automatic actions and about possible improvements.

Provide one **single centralized platform** for analysts with all the **dashboards** and **alerts** from the different sources.

AI as a force multiplier

The human process

I have to create a new detection rule

I have to process the output from SOAR

I have to figure out how to do X

GenAI **assists** humans in **solving complex problems using our language**

AI as a force multiplier

How AI can help us out for defense

We have shown a number of examples of how AI can be used to facilitate adversarial behaviour (e.g. write phishing mails, propose sample code to bypass EDRs,…). Fortunately, it can also be applied to defensive security scenarios:

PREVENT

- Intelligent Code Review
- Attack Surface Identification
- Intelligent Privilege Management

DETECT

- Anomaly Detection
- User Behavior Analytics
- Phishing Detection
- Intelligent Threat Hunting
- Intelligent Use Case Development

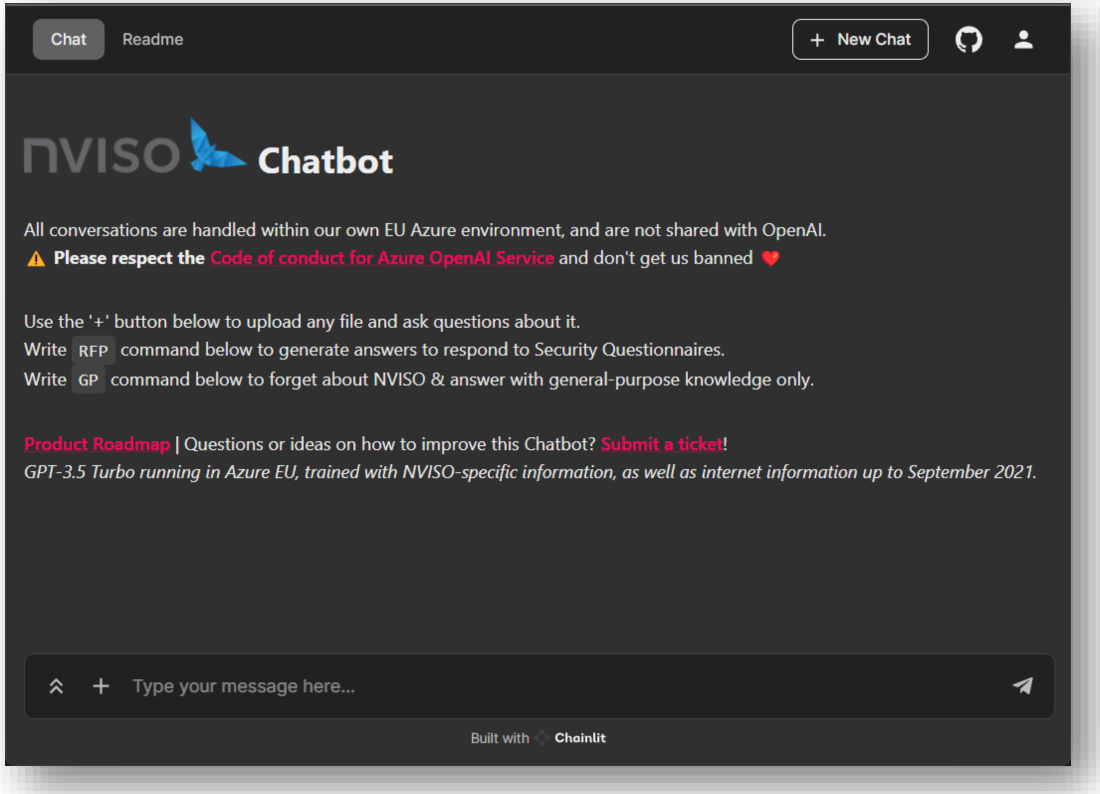
RESPOND

- Incident Triage & Prioritisation
- Incident Correlation

Do you see any other big use cases for AI?

AI as a force multiplier

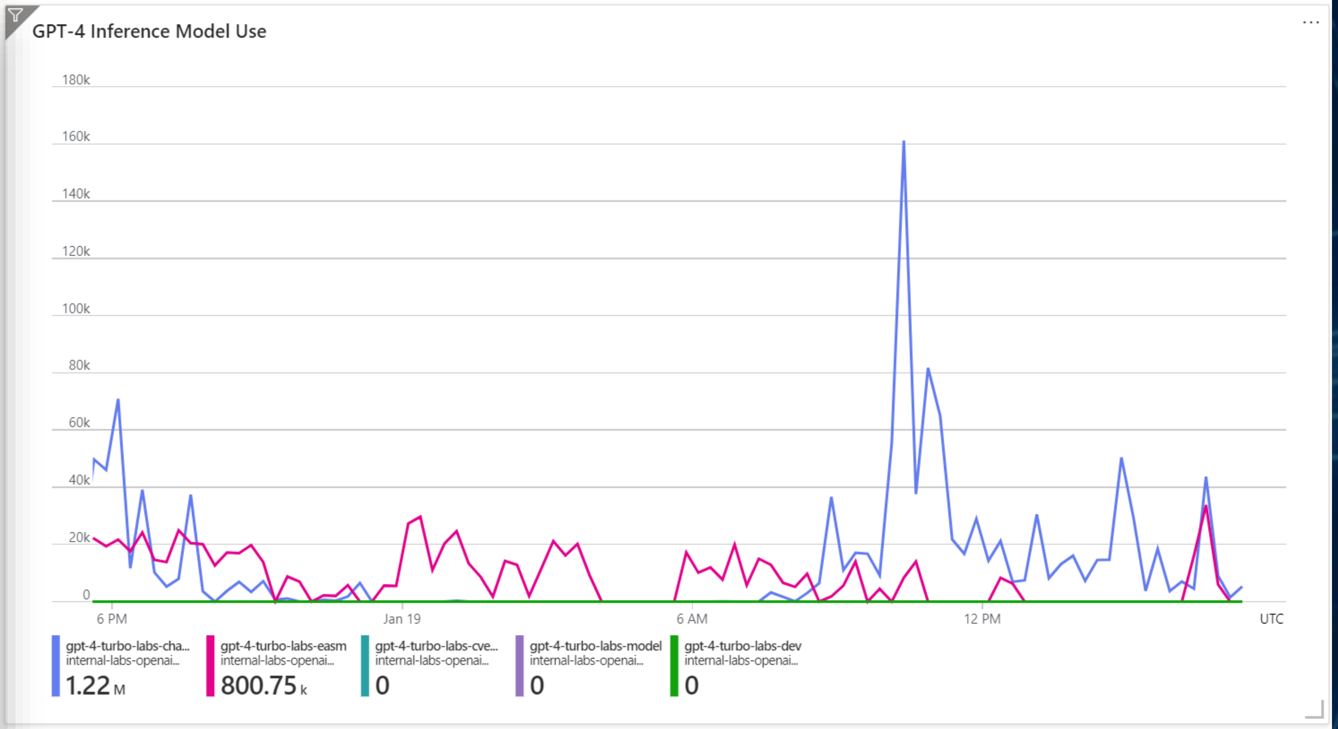
Leveraging AI as an internal knowledge base



All conversations are handled within our own EU Azure environment, and are not shared with OpenAI.
⚠ **Please respect the Code of conduct for Azure OpenAI Service** and don't get us banned ❤

Use the '+' button below to upload any file and ask questions about it.
Write `RFP` command below to generate answers to respond to Security Questionnaires.
Write `GP` command below to forget about NVISO & answer with general-purpose knowledge only.

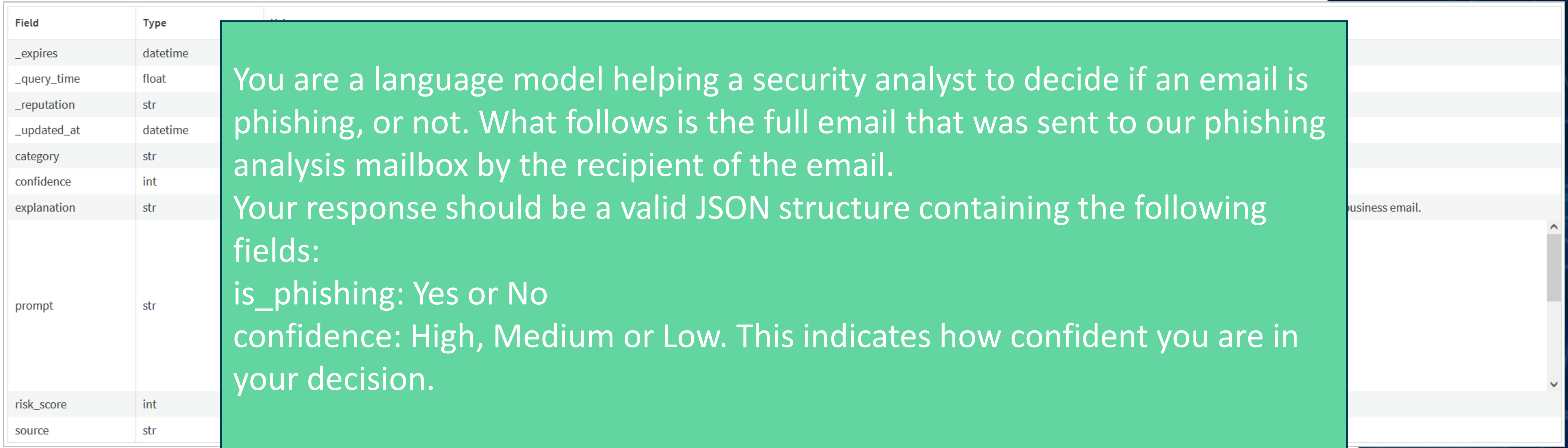
Product Roadmap | Questions or ideas on how to improve this Chatbot? Submit a ticket!
GPT-3.5 Turbo running in Azure EU, trained with NVISO-specific information, as well as internet information up to September 2021.



How to let your organization use GPT without the privacy/security/ethics risk? **Deploy your own GPT!**

AI as a force multiplier

Leveraging AI to analyze phishing emails



Field	Type	
_expires	datetime	
_query_time	float	
_reputation	str	
_updated_at	datetime	
category	str	
confidence	int	
explanation	str	business email.
prompt	str	
risk_score	int	
source	str	

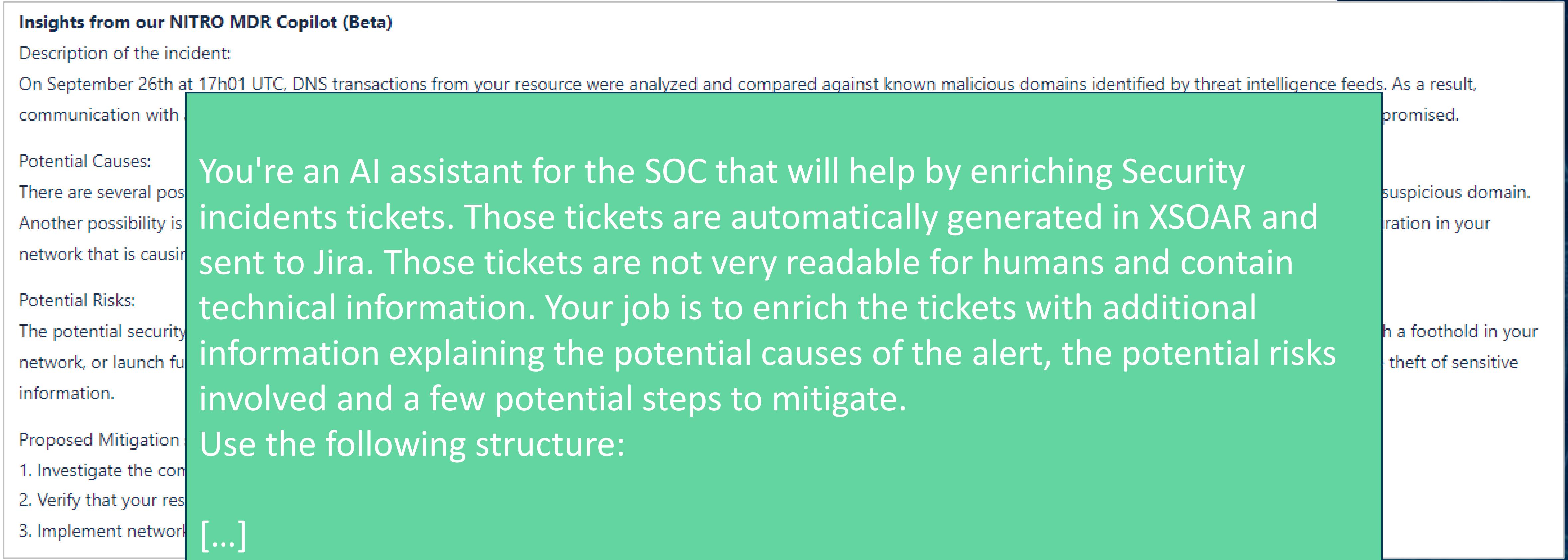
You are a language model helping a security analyst to decide if an email is phishing, or not. What follows is the full email that was sent to our phishing analysis mailbox by the recipient of the email.
Your response should be a valid JSON structure containing the following fields:
is_phishing: Yes or No
confidence: High, Medium or Low. This indicates how confident you are in your decision.

[…]

One of the key examples of how we use OpenAI in the SOC is the **analysis of phishing e-mails.**
How you "prompt" the AI is however of the utmost importance!

AI as a force multiplier

Leveraging AI to enhance incidents/tickets



Insights from our NITRO MDR Copilot (Beta)

Description of the incident:

On September 26th at 17h01 UTC, DNS transactions from your resource were analyzed and compared against known malicious domains identified by threat intelligence feeds. As a result,
communication with
promised.

Potential Causes:

There are several pos
suspicious domain.
Another possibility is
ration in your
network that is causi

Potential Risks:

The potential security
h a foothold in your
network, or launch fu
theft of sensitive
information.

Proposed Mitigation
1. Investigate the con
2. Verify that your res
3. Implement networ

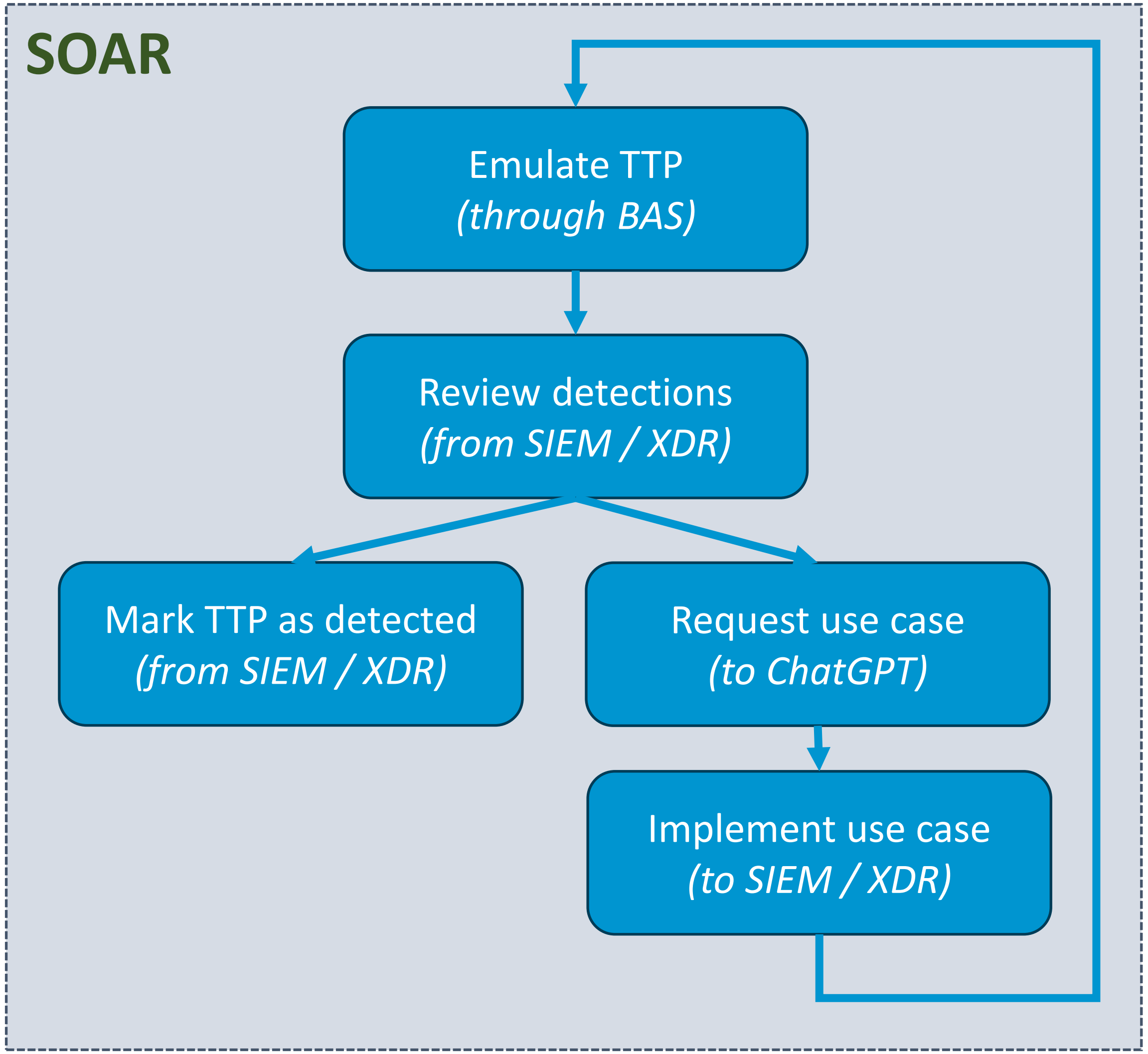
You're an AI assistant for the SOC that will help by enriching Security incidents tickets. Those tickets are automatically generated in XSOAR and sent to Jira. Those tickets are not very readable for humans and contain technical information. Your job is to enrich the tickets with additional information explaining the potential causes of the alert, the potential risks involved and a few potential steps to mitigate.
Use the following structure:

[…]

Add ChatGPT-generated insights to tickets when communicated to your constituents.

AI as a force multiplier

Leveraging AI in the detection engineering pipeline

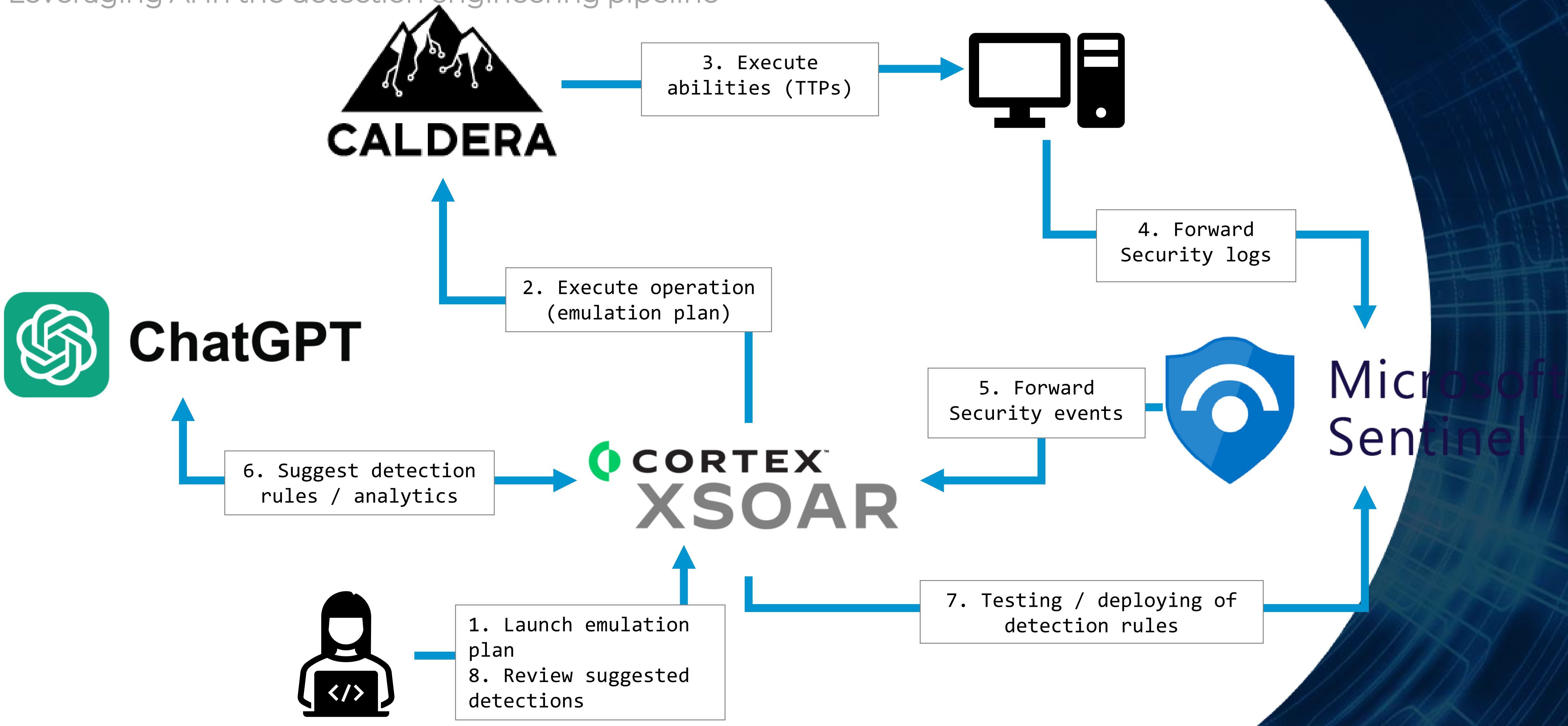

SOAR
Emulate TTP *(through BAS)*
Review detections *(from SIEM / XDR)*
Mark TTP as detected *(from SIEM / XDR)*
Request use case *(to ChatGPT)*
Implement use case *(to SIEM / XDR)*

An active topic of research at NVISO is how we can further automate **detection engineering.** High-level action plan is below:

1. Trigger emulation of a TTP by calling the BAS (Breach Attack Simulation) tool
2. Review detections from SIEM / XDR (which are already being ingested in the SOAR platform) and determine whether the TTP was successfully detected
3. If the TTP was successfully detected, mark it as such and move to the next TTP.
4. If the TTP was not successfully detected, generate a detection analytic specific to our technology through ChatGPT
5. Push the suggested detection analytic to the SIEM / XDR for testing
6. Rinse and repeat

AI as a force multiplier

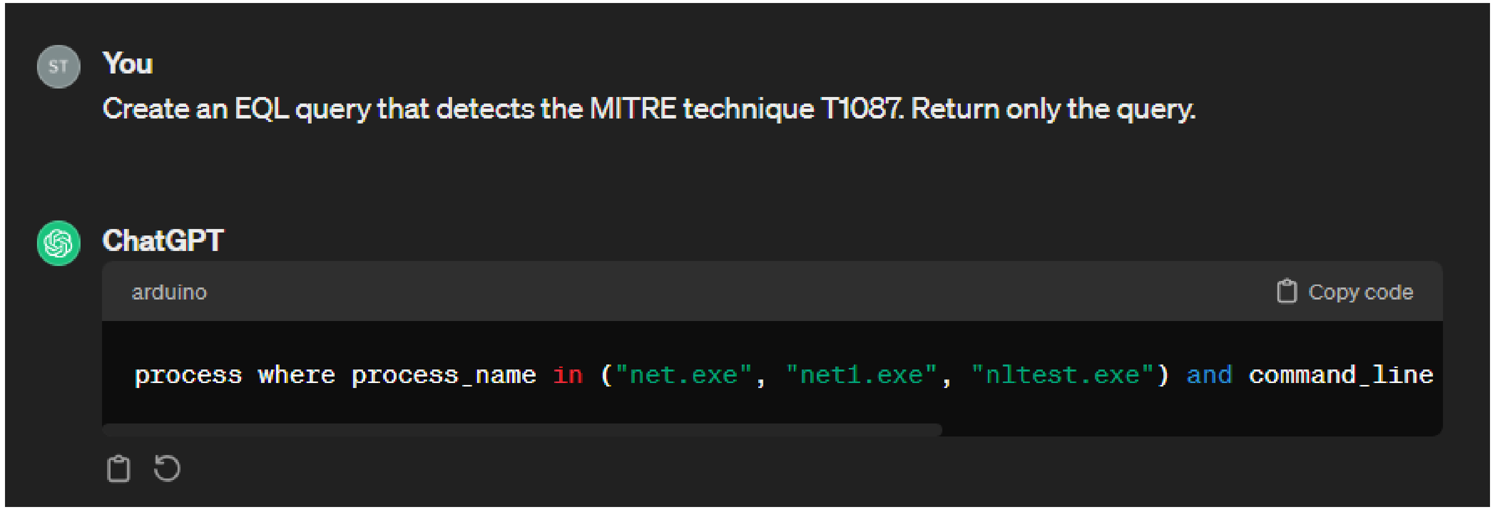
Leveraging AI in the detection engineering pipeline



1. Launch emulation plan
2. Execute operation (emulation plan)
3. Execute abilities (TTPs)
4. Forward Security logs
5. Forward Security events
6. Suggest detection rules / analytics
7. Testing / deploying of detection rules
8. Review suggested detections

AI as a force multiplier

Leveraging AI in the detection engineering pipeline

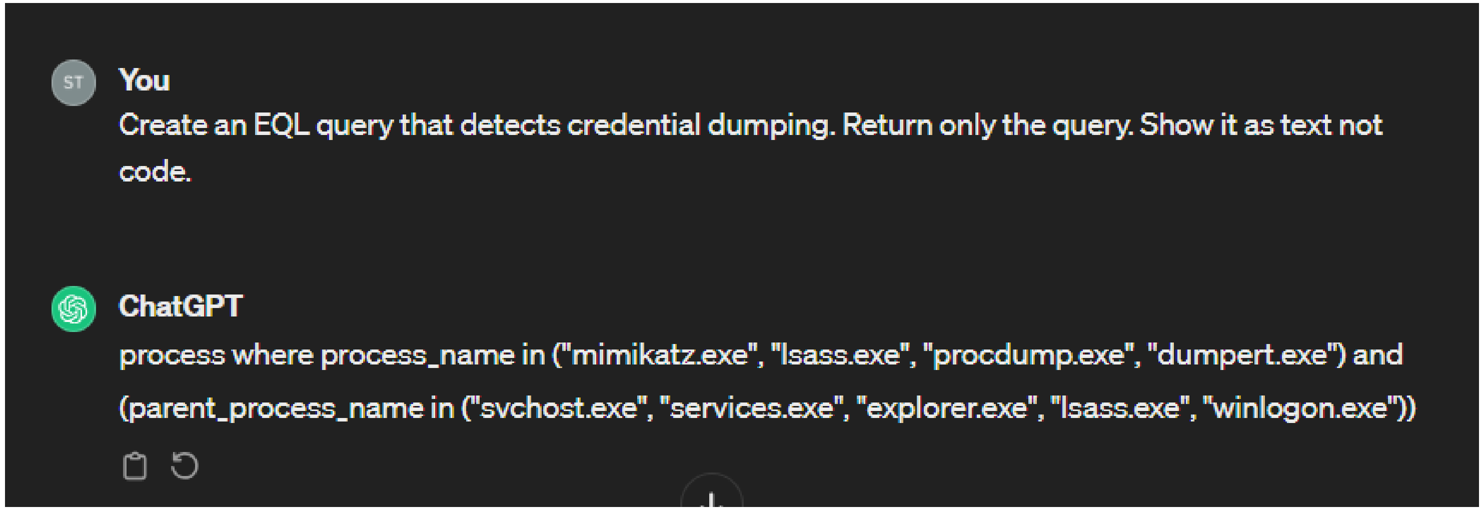


You

Create an EQL query that detects the MITRE technique T1087. Return only the query.

ChatGPT

```
process where process_name in ("net.exe", "net1.exe", "nltest.exe") and command_line
```



You

Create an EQL query that detects credential dumping. Return only the query. Show it as text not code.

ChatGPT

process where process_name in ("mimikatz.exe", "lsass.exe", "procdump.exe", "dumpert.exe") and (parent_process_name in ("svchost.exe", "services.exe", "explorer.exe", "lsass.exe", "winlogon.exe"))

You’re are an assistant supporting our security analysts in doing an initial triage of observations. We want to know if we should notify a security analyst about important External Attack Surface vulnerabilities, based on scan results we retrieve automatically from the Shodan API.

Your conclusion will be used to alert our security analysts about security vulnerabilities that require attention.

Response format: JSON with fields:

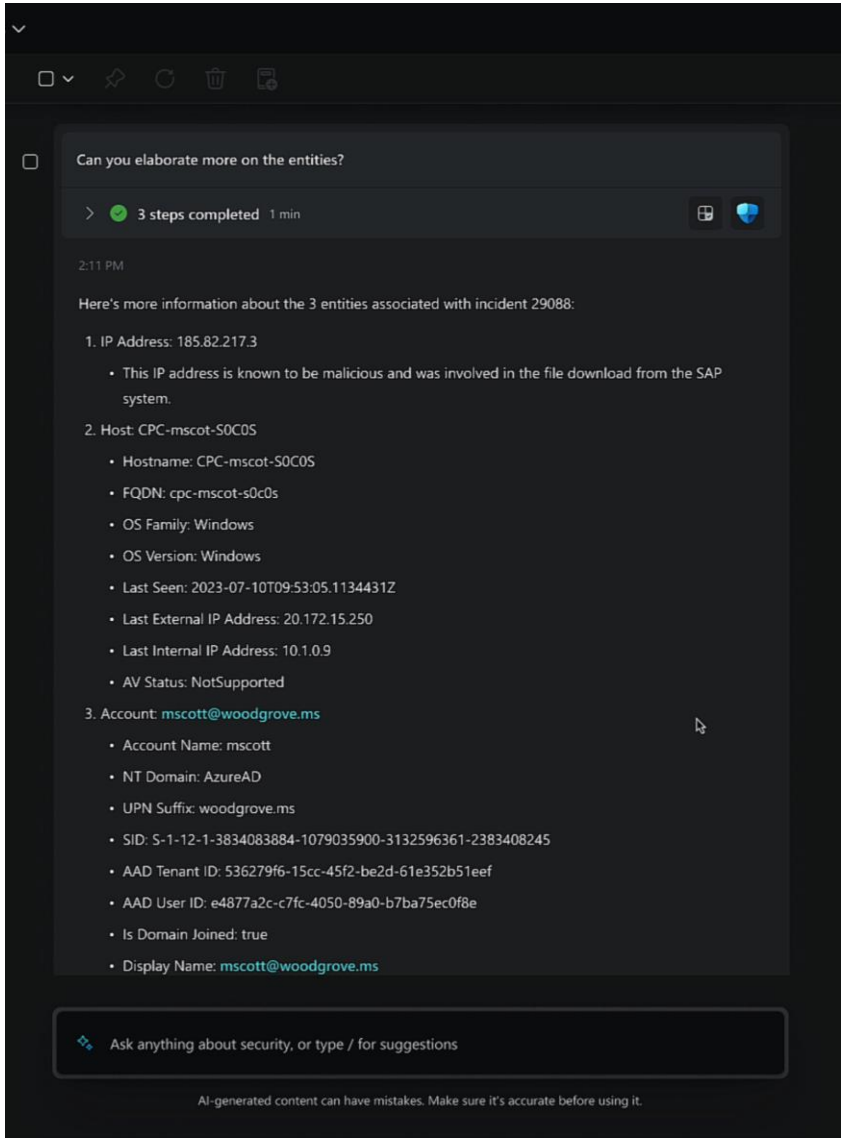
Always mention a priority in the title and summary, choosing one of the following exact values: CRITICAL, HIGH, MEDIUM, LOW, INFO.

The following are examples of observations you should always rate as INFORMATIONAL:
[…]

The following are examples of observations you should always rate as HIGH or CRITICAL (use your own judgement):
[…]

AI as a force multiplier

Microsoft Co-Pilot



Can you elaborate more on the entities?

3 steps completed 1 min

2:11 PM

Here's more information about the 3 entities associated with incident 29088:

1. IP Address: 185.82.217.3
   - This IP address is known to be malicious and was involved in the file download from the SAP system.
2. Host: CPC-mscot-S0C0S
   - Hostname: CPC-mscot-S0C0S
   - FQDN: cpc-mscot-s0c0s
   - OS Family: Windows
   - OS Version: Windows
   - Last Seen: 2023-07-10T09:53:05.1134431Z
   - Last External IP Address: 20.172.15.250
   - Last Internal IP Address: 10.1.0.9
   - AV Status: NotSupported
3. Account: mscott@woodgrove.ms
   - Account Name: mscott
   - NT Domain: AzureAD
   - UPN Suffix: woodgrove.ms
   - SID: S-1-12-1-3834083884-1079035900-3132596361-2383408245
   - AAD Tenant ID: 536279f6-15cc-45f2-be2d-61e352b51eef
   - AAD User ID: e4877a2c-c7fc-4050-89a0-b7ba75ec0f8e
   - Is Domain Joined: true
   - Display Name: mscott@woodgrove.ms

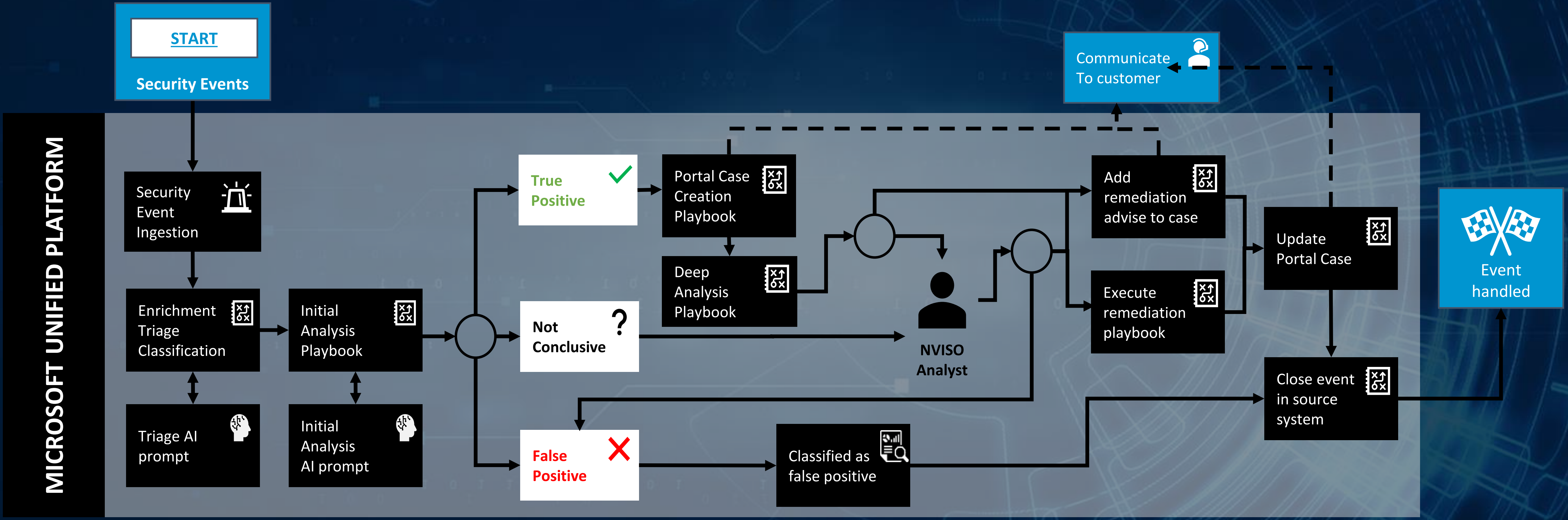
AI-generated content can have mistakes. Make sure it's accurate before using it.

Security Co-Pilot was recently introduced by Microsoft and aims to leverage AI to help support the following tasks:

- **Security Posture Management:** Ask questions to the Co-Pilot on weaknesses and exposure (identified through their EASM and Defender for Endpoint products)
- **Incident Response:** Assist with handling security events by providing additional context and respond to analyst questions while analyzing events at hand
- **Security Reporting:** Highly capable of transforming information to a desired output format (e.g. create PowerBI dashboards)

Modern SecOps

Tying everything together


START
Security Events
MICROSOFT UNIFIED PLATFORM
Security Event Ingestion
Enrichment Triage Classification
Triage AI prompt
Initial Analysis Playbook
Initial Analysis AI prompt
True Positive ✓
Not Conclusive ?
False Positive ✗
Portal Case Creation Playbook
Deep Analysis Playbook
Classified as false positive
NVISO Analyst
Communicate To customer
Add remediation advise to case
Execute remediation playbook
Update Portal Case
Close event in source system
Event handled

AI as a force multiplier

How will this evolve?

GenAI is currently very **input/output** focused

Native Integration into tools

New Key Analyst Skillset: **AI proficiency**

Conclusions

AI is our ally

The rapidly evolving threat landscape is making it **easier for adversaries to mount effective attacks** in a short timespan and without advanced knowledge.

Given the above, **automation is not a nice-to-have** in Security Operations but is essential in today's security landscape. A key example of this is leveraging playbooks.

AI will have a **significant impact** on the further evolution of Security Operations and cyber security in general. There is however **a lot of "noise"** in these early stages, time will tell what the most valuable use cases are.

Q&A

SCAN ME

Maxim Deweerdt
maxim.deweerdt@nviso.eu