Drag, Drop, Defend:

Making Security Scripts Accessible to Everyone

Intro

- 20+ year career in IT and Security
- Experience in a wide array of industry sectors
- Have run SOCs for Fortune 500s
- Focus on blue team (best team)
  - SOC
  - Detection Engineering
  - Threat Hunting
  - Tool Development
  - Incident Response

Agenda

WHY FOCUS ON SCRIPTING?

CHALLENGES

SOLUTION(S)

LET'S GO ON AN ADVENTURE

WRAP-UP

QUESTIONS?

Why Scripting?

State of Sec Ops – Perspectives

Security Operations

- Alert volumes
- Response times
- Talent shortages
- Disparate systems

Executives

- Reputation
- Profits

State of Sec Ops – So what do we do?

Goals?

- Reduce workload
- Work faster
  - Simplify workflows
  - Increase staff
  - Simplify tool knowledge

Options

- Better tuning
- Scripting
- Automated enrichment
- Increase capacity

Challenges

```
ls

ls  cd /home.user
ls   cd /home.user
ll

user@lochbast:~>
ls -1
user@lochbast:~>
                rm-rf /
```

Scripting challenges

Languages

OS

Storage

Dependencies

Context switching

Scripting Solution

AI

- Centralized investigation platform
- Integrates with automation platforms
- Lesson learning curve
- Standardize runtime platform

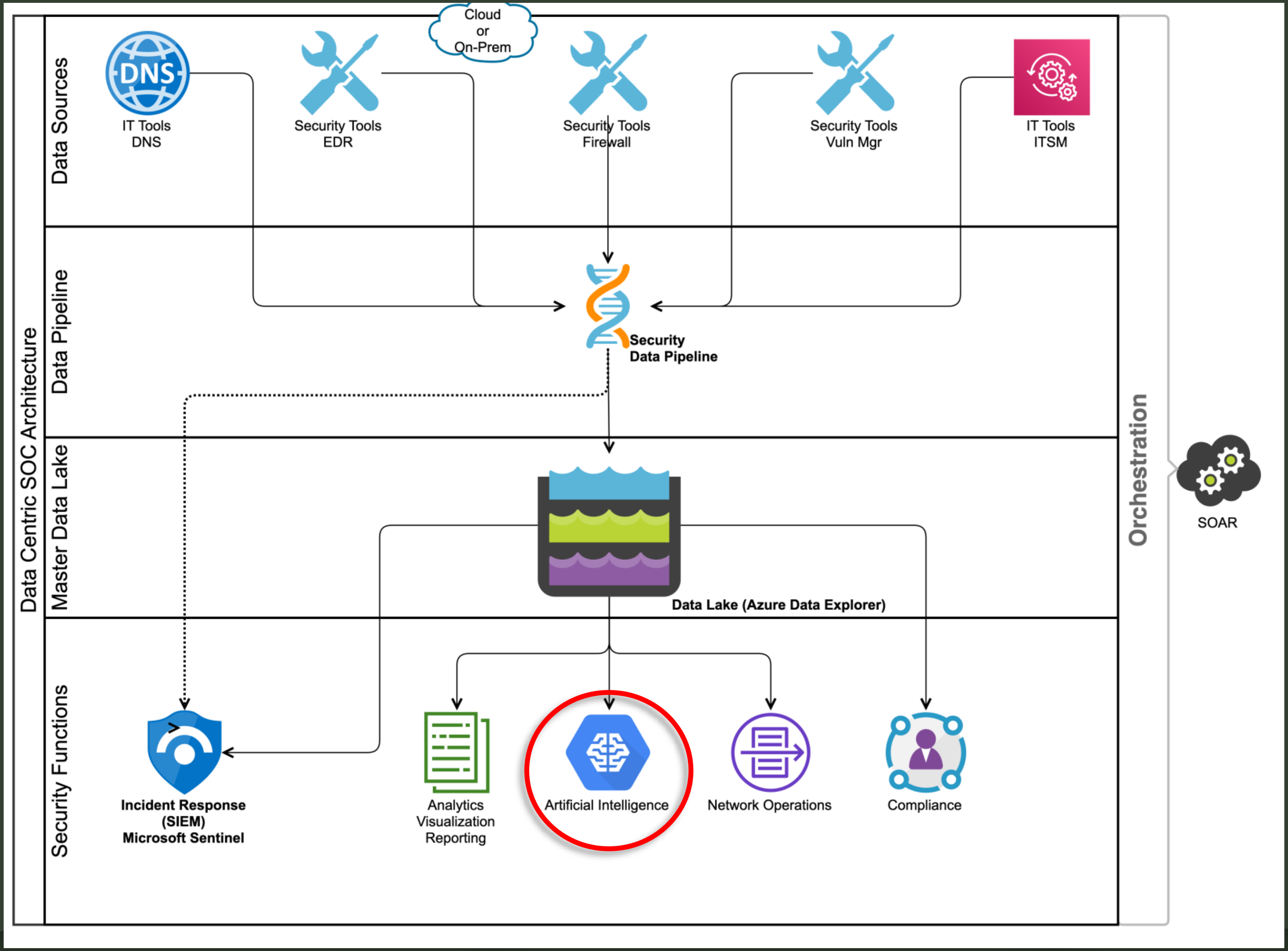
Where/How AI fits in your SOC (you need to know this)

- Natural Language Querying
- Accelerate Triage and Investigation
- Automation of repetitive tasks
- Faster Response
- Knowledge management
- Trainer, coach, first pass engineer

Myths

- Replace my Tier 1 SOC
- Find bleeding edge attacks

Let's talk AI for a quick minute



Let's go on an adventure

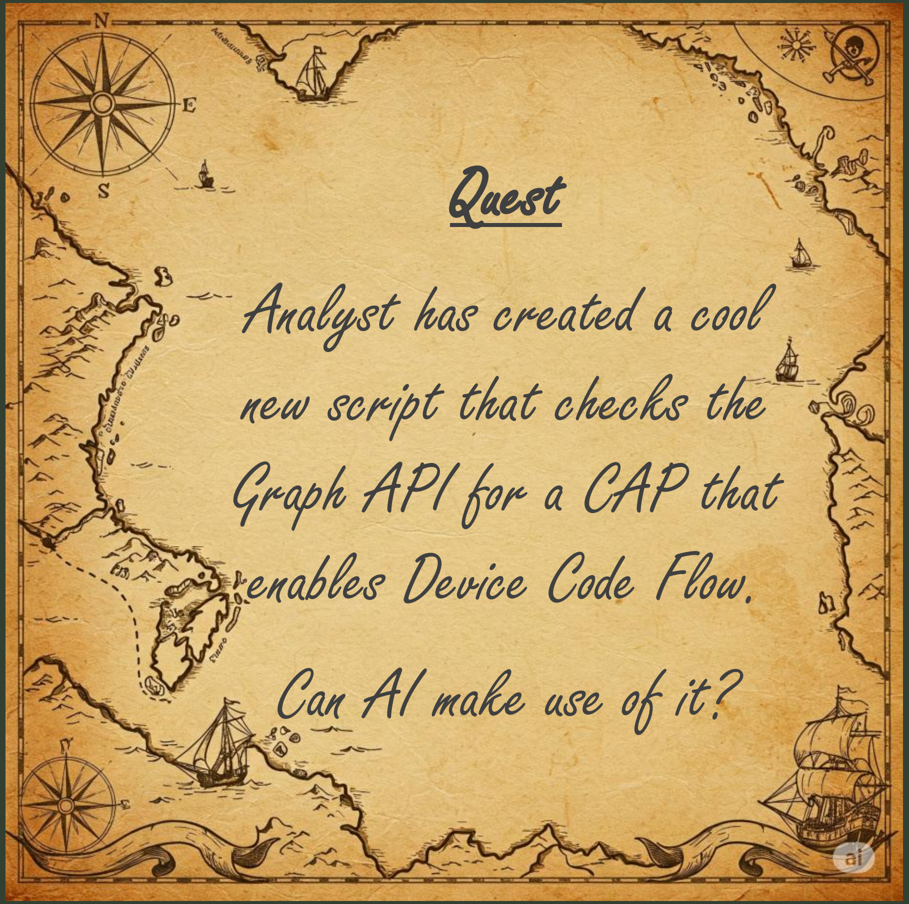
Choose your own adventure

Several options for implementing AI

Balance between:

- Cost
- Implementation Time
- Effectiveness

So many AI's which is the right one?

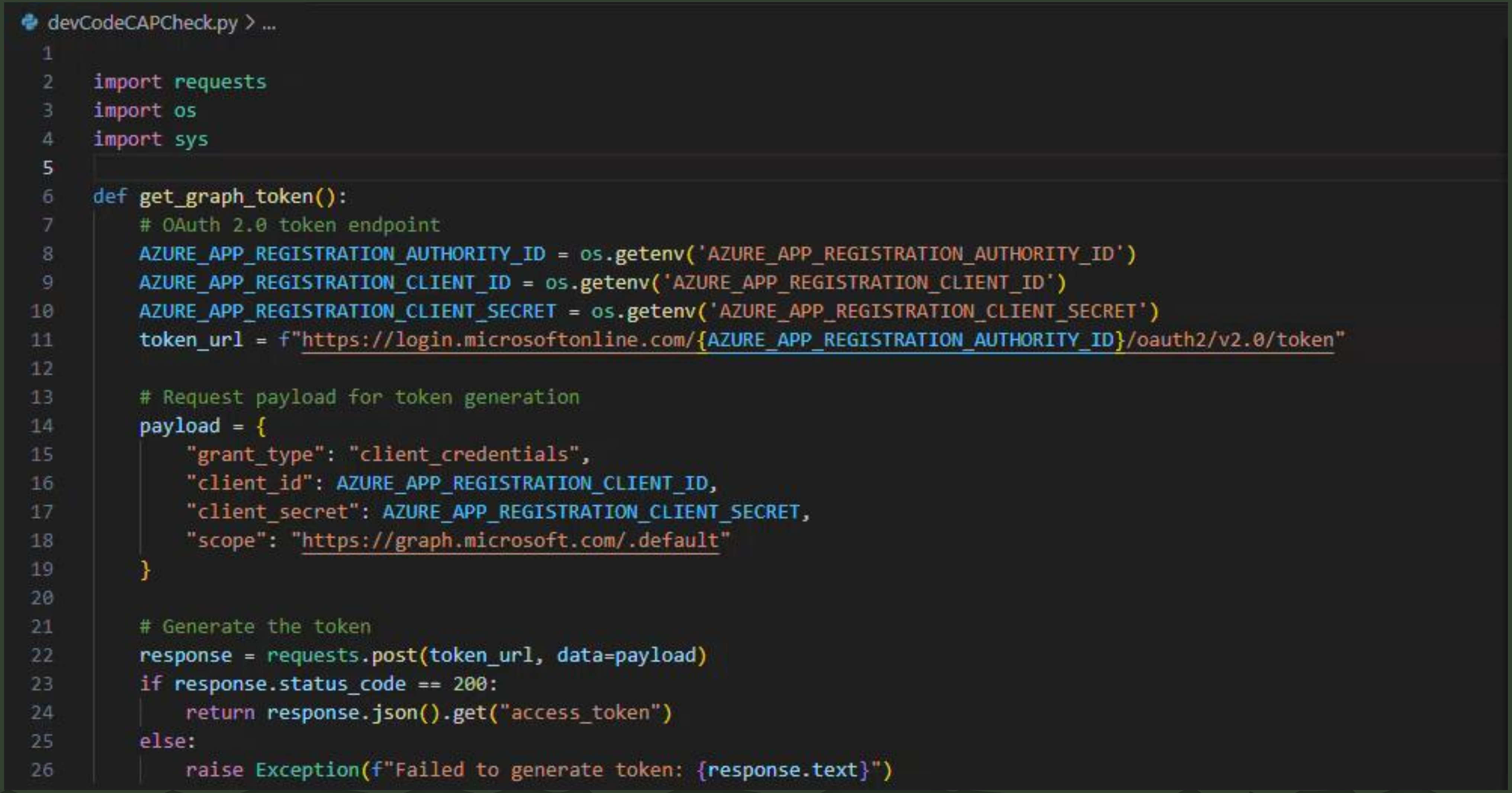


Quest

Analyst has created a cool new script that checks the Graph API for a CAP that enables Device Code Flow.

Can AI make use of it?

Script

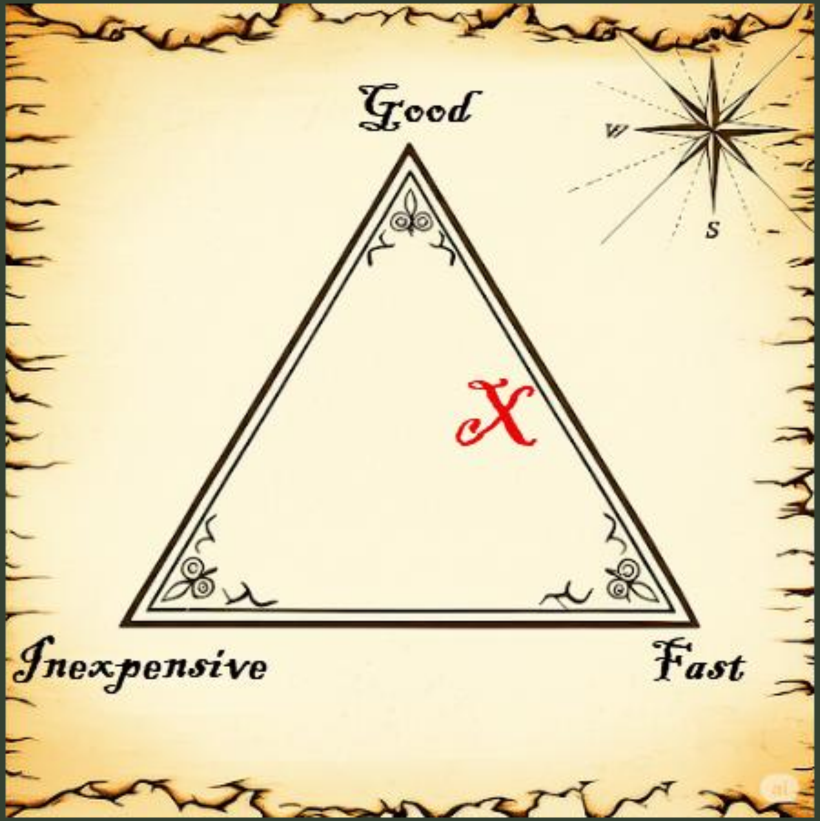


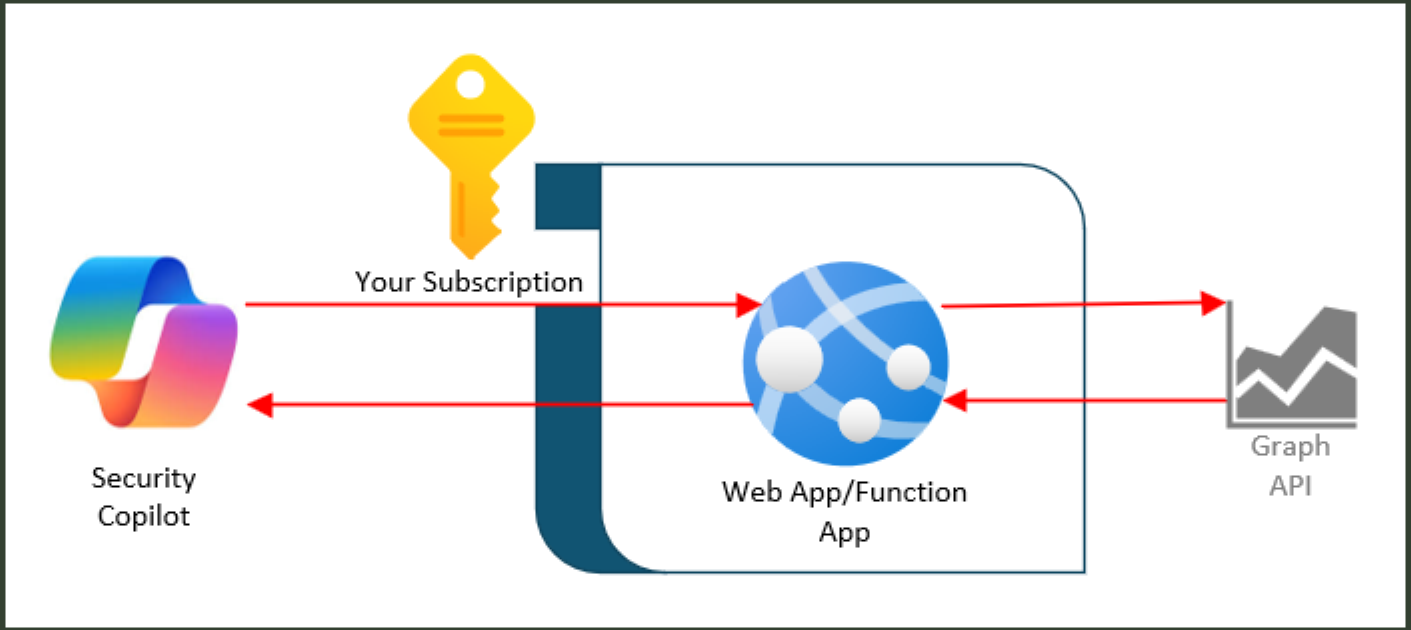
devCodeCAPCheck.py > ...

```python

import requests
import os
import sys

def get_graph_token():
    # OAuth 2.0 token endpoint
    AZURE_APP_REGISTRATION_AUTHORITY_ID = os.getenv('AZURE_APP_REGISTRATION_AUTHORITY_ID')
    AZURE_APP_REGISTRATION_CLIENT_ID = os.getenv('AZURE_APP_REGISTRATION_CLIENT_ID')
    AZURE_APP_REGISTRATION_CLIENT_SECRET = os.getenv('AZURE_APP_REGISTRATION_CLIENT_SECRET')
    token_url = f"https://login.microsoftonline.com/{AZURE_APP_REGISTRATION_AUTHORITY_ID}/oauth2/v2.0/token"

    # Request payload for token generation
    payload = {
        "grant_type": "client_credentials",
        "client_id": AZURE_APP_REGISTRATION_CLIENT_ID,
        "client_secret": AZURE_APP_REGISTRATION_CLIENT_SECRET,
        "scope": "https://graph.microsoft.com/.default"
    }

    # Generate the token
    response = requests.post(token_url, data=payload)
    if response.status_code == 200:
        return response.json().get("access_token")
    else:
        raise Exception(f"Failed to generate token: {response.text}")
```

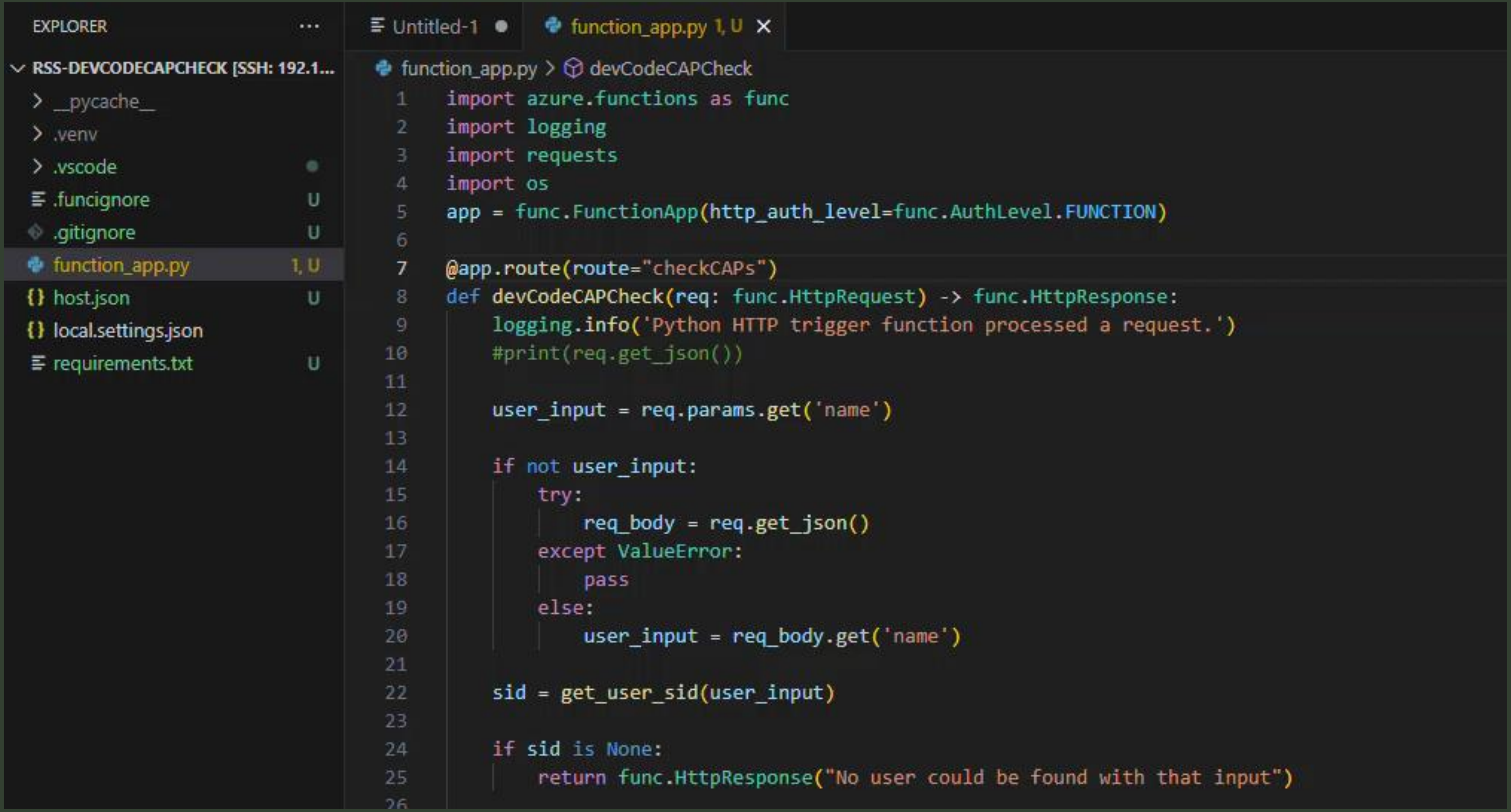
Option 1

Microsoft Security Copilot





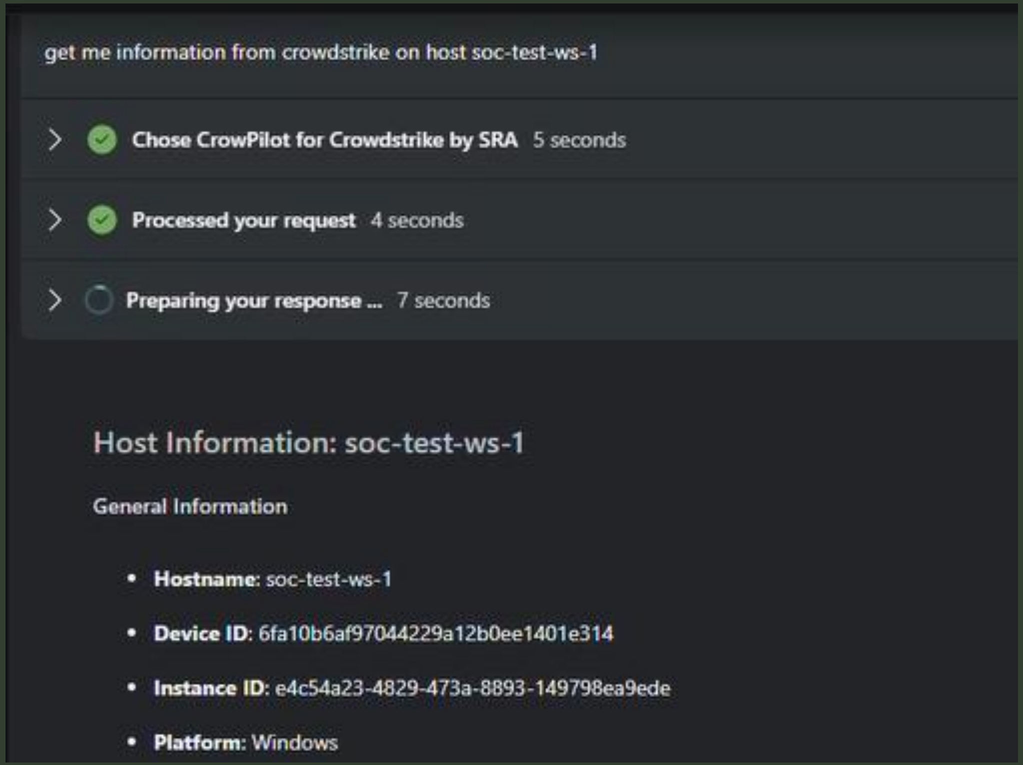
Modified Script



```python
import azure.functions as func
import logging
import requests
import os
app = func.FunctionApp(http_auth_level=func.AuthLevel.FUNCTION)

@app.route(route="checkCAPs")
def devCodeCAPCheck(req: func.HttpRequest) -> func.HttpResponse:
    logging.info('Python HTTP trigger function processed a request.')
    #print(req.get_json())

    user_input = req.params.get('name')

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

    sid = get_user_sid(user_input)

    if sid is None:
        return func.HttpResponse("No user could be found with that input")
```

Example

- Perform Health Check of CS Configuration
- List CrowdStrike incidents
- Unblock/block IOCs
- Add/Release Host Isolation
- Gather incident details
- Retrieve host information
- Hide/Unhide a host
- Move host between host groups
- Perform/Cancel/Report from On Demand Scans
- Suppress/Unsuppress detections
- Retrieve host Zero Trust Score



get me information from crowdstrike on host soc-test-ws-1

Chose CrowPilot for Crowdstrike by SRA 5 seconds

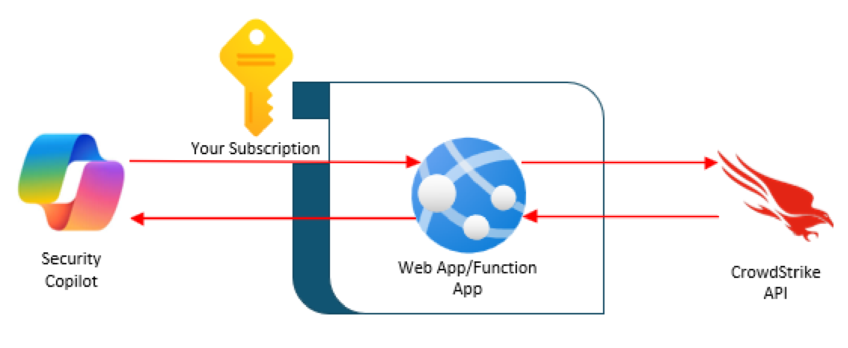
Processed your request 4 seconds

Preparing your response ... 7 seconds

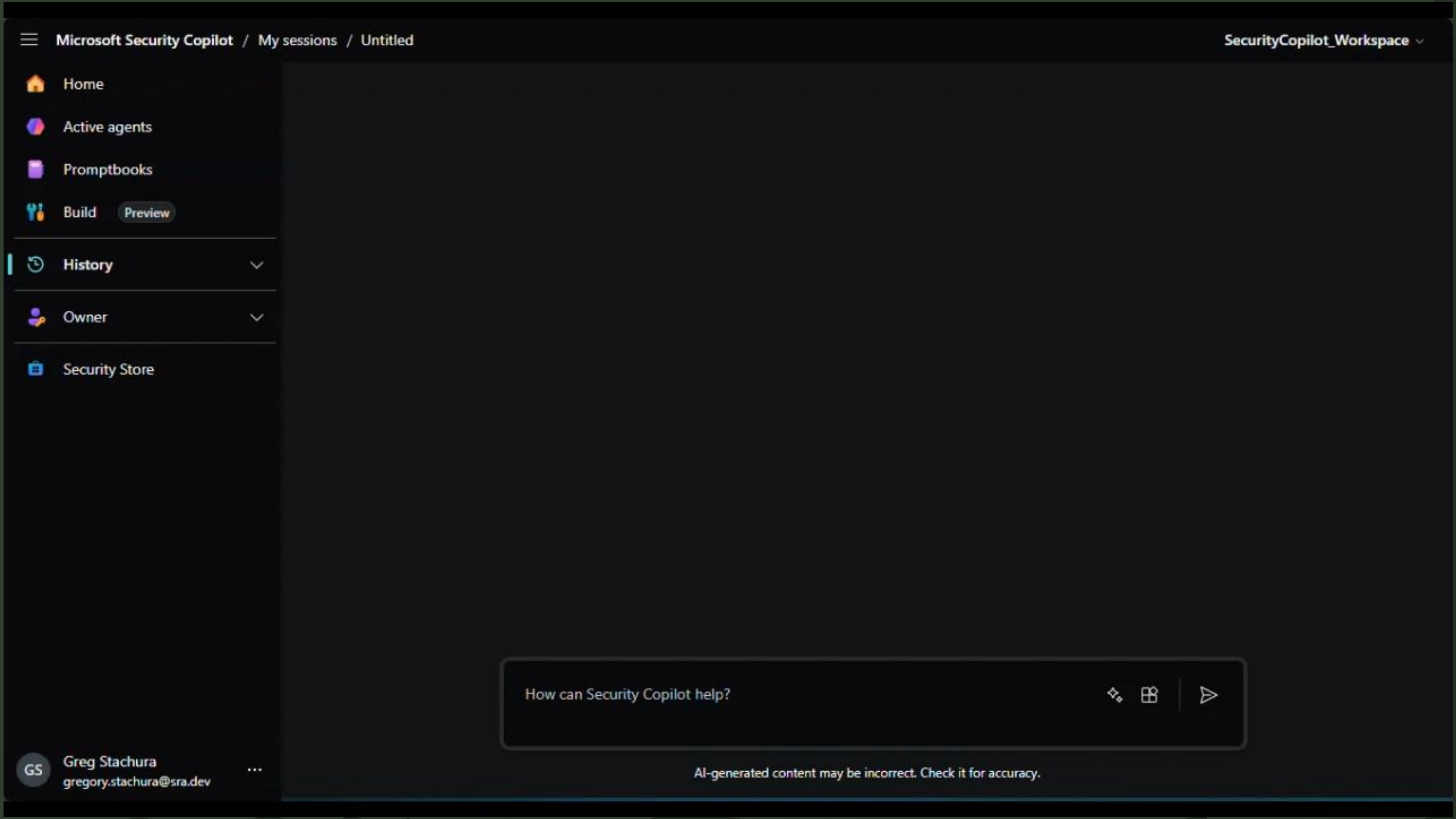
Host Information: soc-test-ws-1

General Information

- **Hostname:** soc-test-ws-1
- **Device ID:** 6fa10b6af97044229a12b0ee1401e314
- **Instance ID:** e4c54a23-4829-473a-8893-149798ea9ede
- **Platform:** Windows



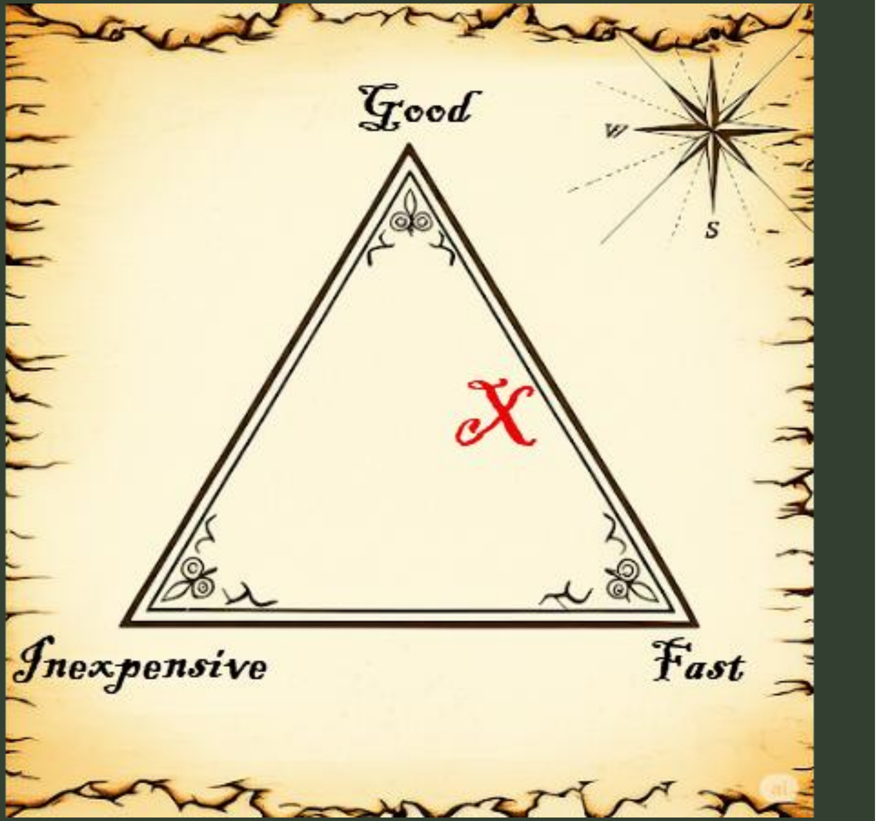
Demo

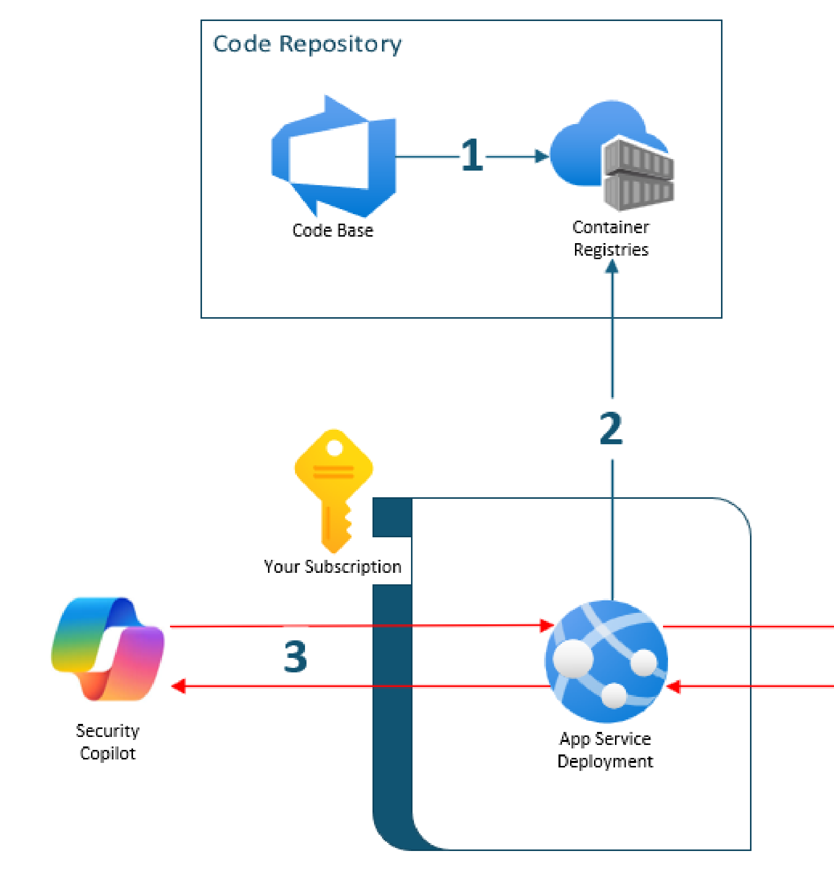


Microsoft Security Copilot / My sessions / Untitled
SecurityCopilot_Workspace
Home
Active agents
Promptbooks
Build
Preview
History
Owner
Security Store
GS
Greg Stachura
gregory.stachura@sra.dev
How can Security Copilot help?
AI-generated content may be incorrect. Check it for accuracy.

Option 2

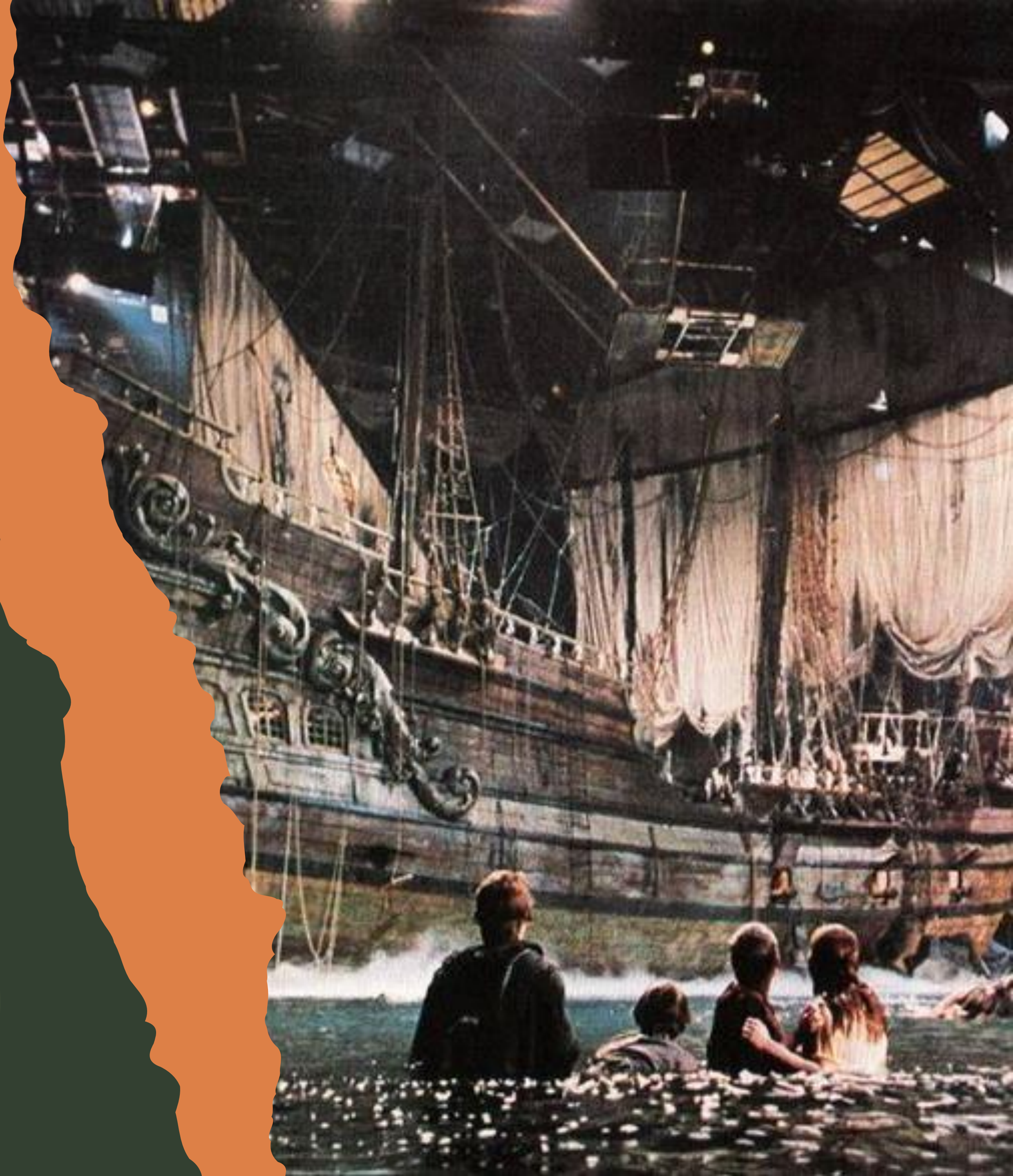
Microsoft Security Copilot ++



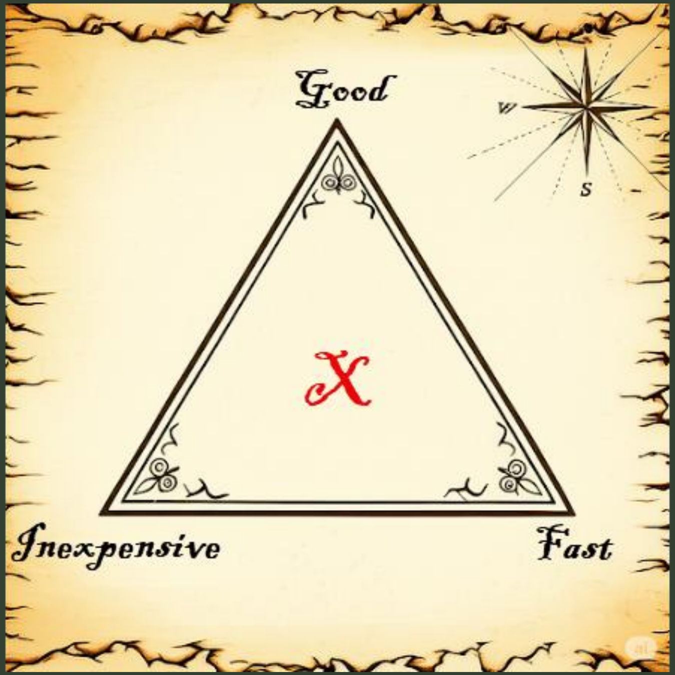


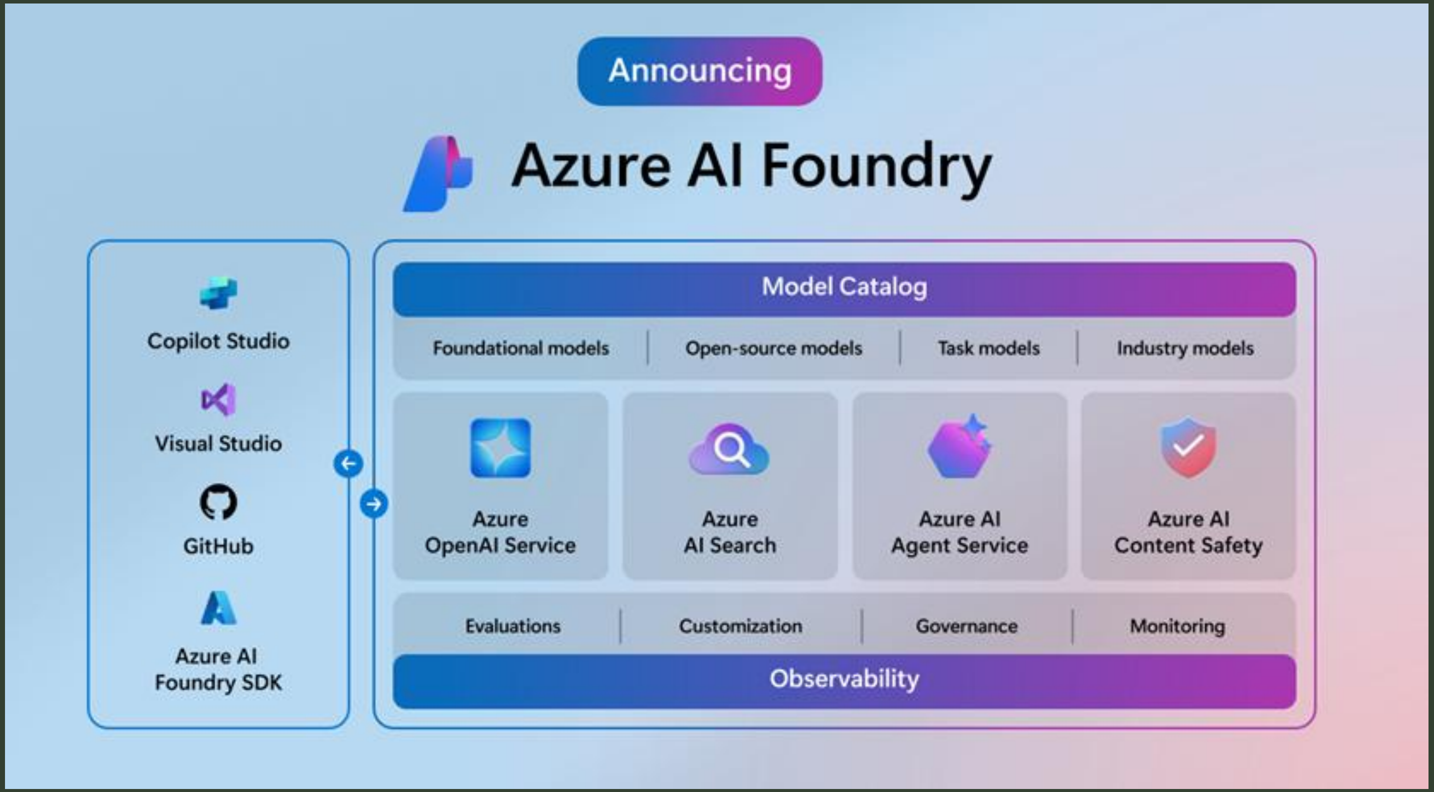
1. New Features Released
2. App sees the new release and updates it's container
3. Security Copilot calls App to interface with the Graph API
4. App takes care of the complicated calls to Graph API, returning what Copilot needs to respond to your commands

Option 3



Azure AI Foundry





Announcing

Azure AI Foundry

Copilot Studio

Visual Studio

GitHub

Azure AI Foundry SDK

Model Catalog

Foundational models | Open-source models | Task models | Industry models

Azure OpenAI Service

Azure AI Search

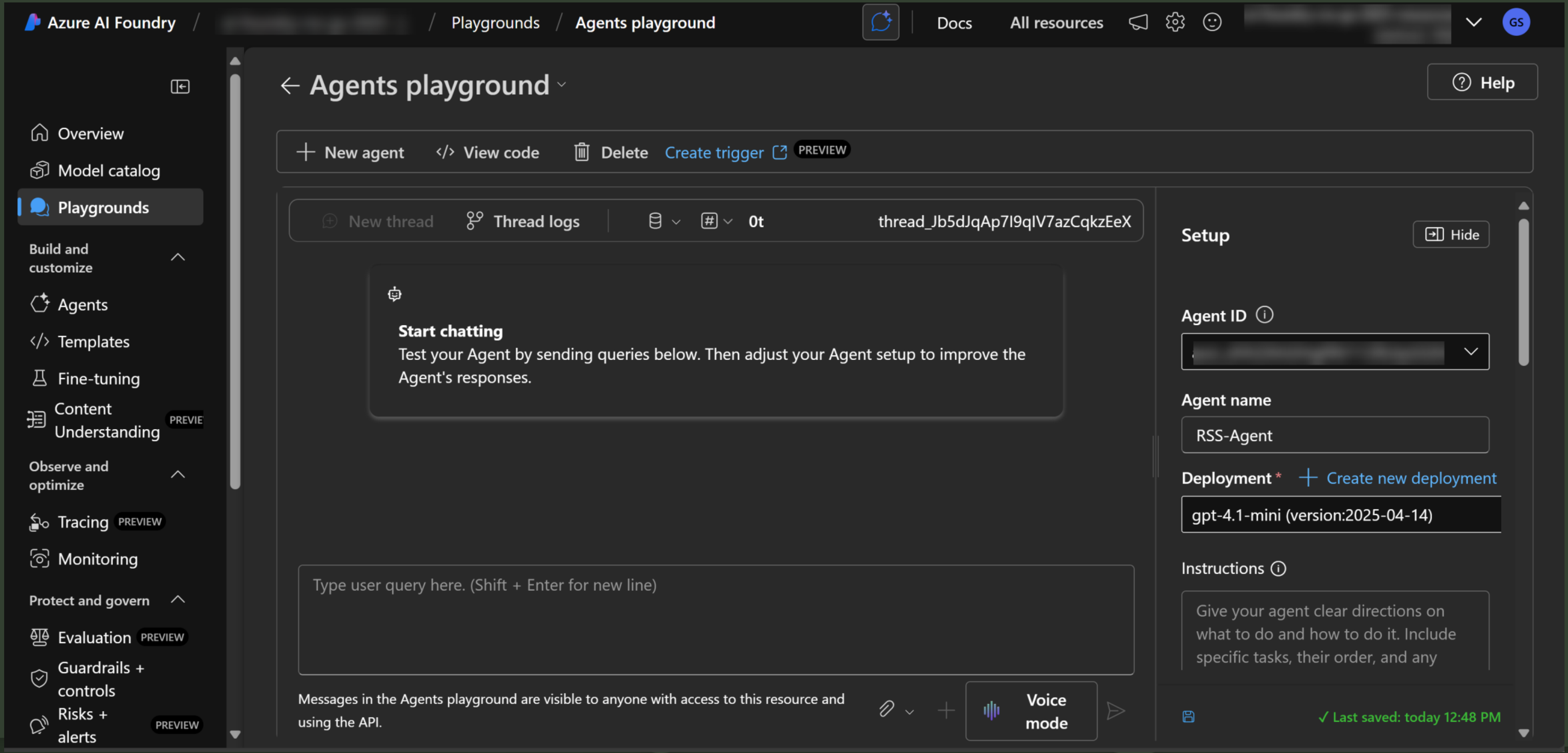
Azure AI Agent Service

Azure AI Content Safety

Evaluations | Customization | Governance | Monitoring

Observability

AI Foundry



thread_Jb5dJqAp7I9qIV7azCqkzEeX

Start chatting
Test your Agent by sending queries below. Then adjust your Agent setup to improve the Agent's responses.

Type user query here. (Shift + Enter for new line)

Messages in the Agents playground are visible to anyone with access to this resource and using the API.

Agent ID: [redacted]

Agent name: RSS-Agent

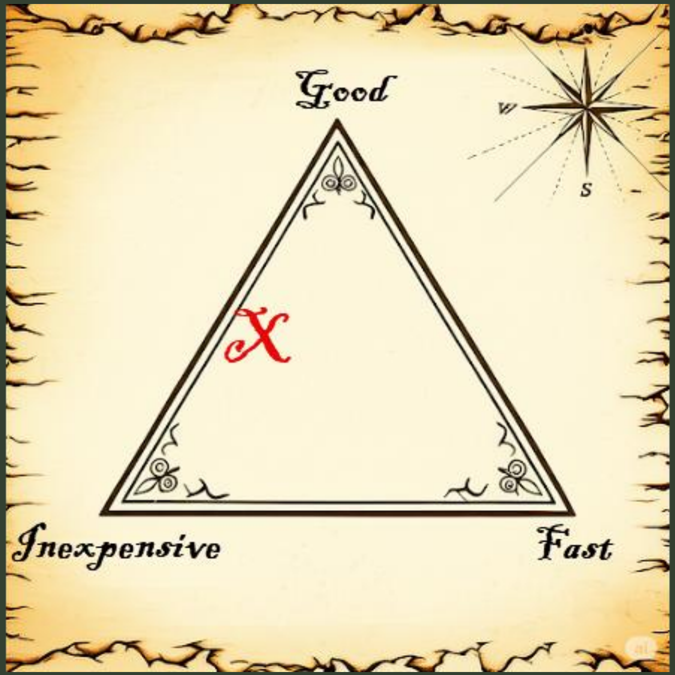
Deployment * + Create new deployment: gpt-4.1-mini (version:2025-04-14)

Instructions: Give your agent clear directions on what to do and how to do it. Include specific tasks, their order, and any

✓ Last saved: today 12:48 PM

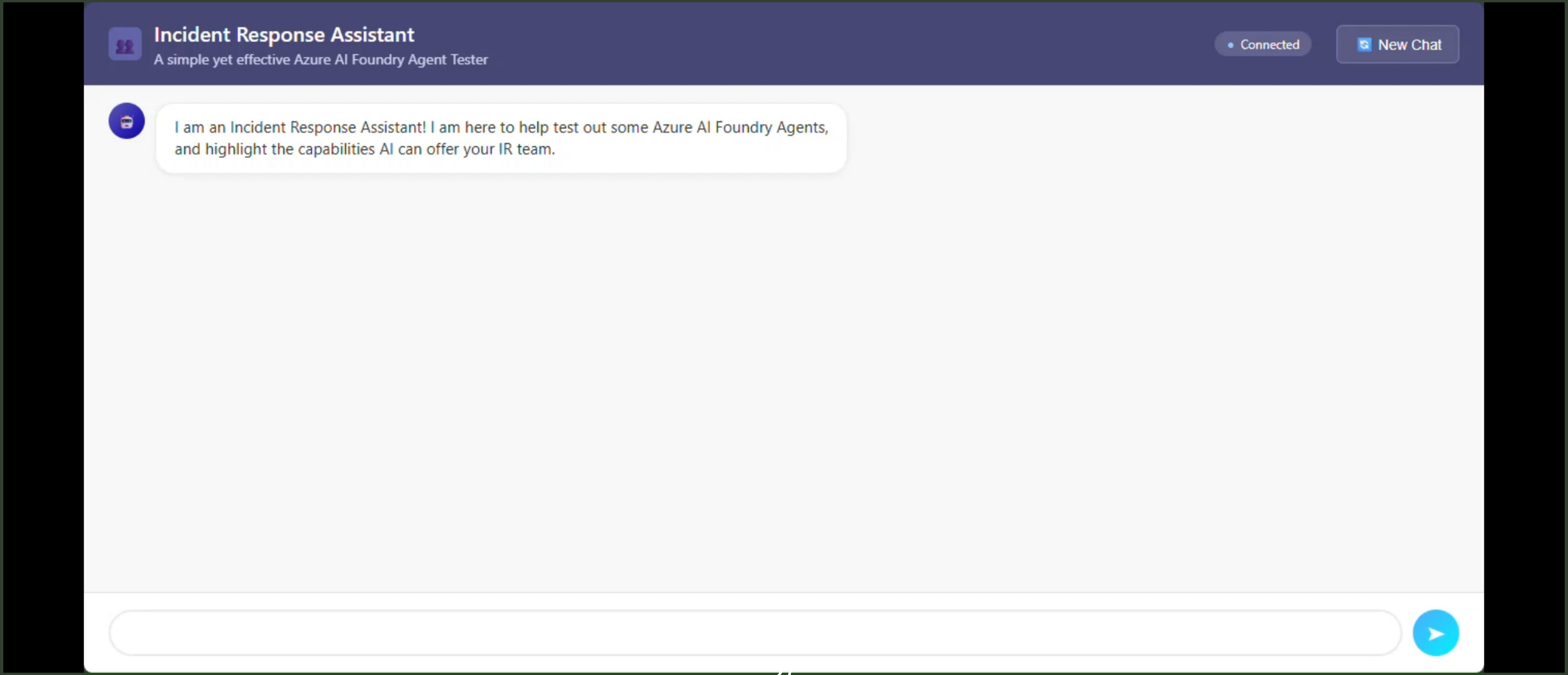
Option 4

Build Your Own!



- Custom Web App
- Integrated Agents using FastAPI
- Highly customizable
- Purpose built for your organization

Demo



Incident Response Assistant
A simple yet effective Azure AI Foundry Agent Tester
Connected
New Chat

I am an Incident Response Assistant! I am here to help test out some Azure AI Foundry Agents, and highlight the capabilities AI can offer your IR team.

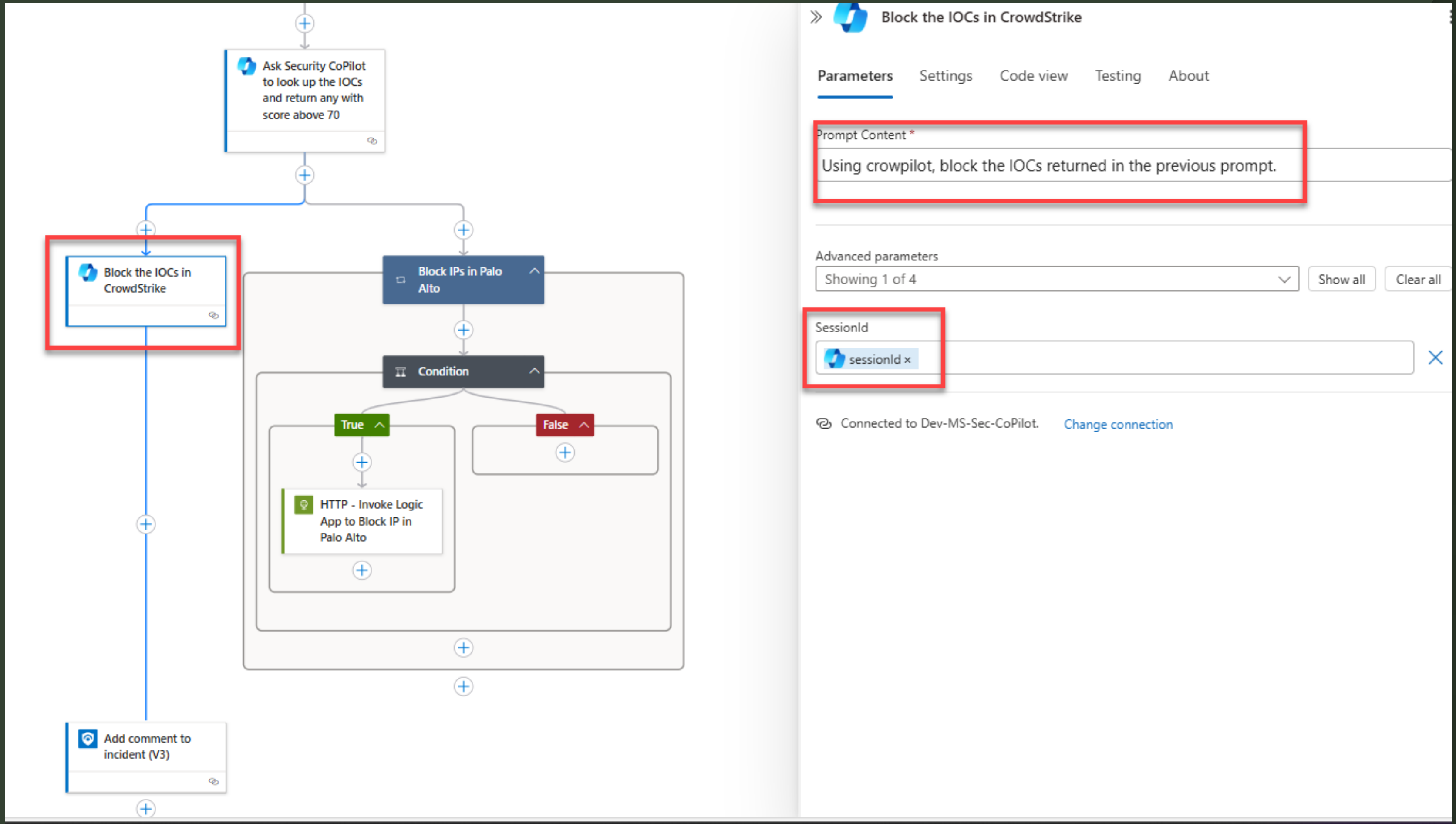
Interface based off of: GitHub - Shailender-Youtube

Why are we doing this?

- Unify your investigation platform, without going single vendor
- Simplify your workflows
- Let your analysts focus on analysis
- Enable your AI for future expansion
- Time to value of your tools increases

Enable Your Analysts

- Allow your team to quickly deploy integrations using your AI
- Take the backend programming headaches out of the equation and let your analyst/engineers think more about the solution then how to develop it



Ask Security CoPilot to look up the IOCs and return any with score above 70
Block the IOCs in CrowdStrike
Block IPs in Palo Alto
Condition
True
False
HTTP - Invoke Logic App to Block IP in Palo Alto
Add comment to incident (V3)
Block the IOCs in CrowdStrike
Parameters
Settings
Code view
Testing
About
Show all
Clear all
Change connection

Prompt Content *

Using crowpilot, block the IOCs returned in the previous prompt.

Advanced parameters

Showing 1 of 4

SessionId

sessionId ×

Connected to Dev-MS-Sec-CoPilot.

What you tell your boss...

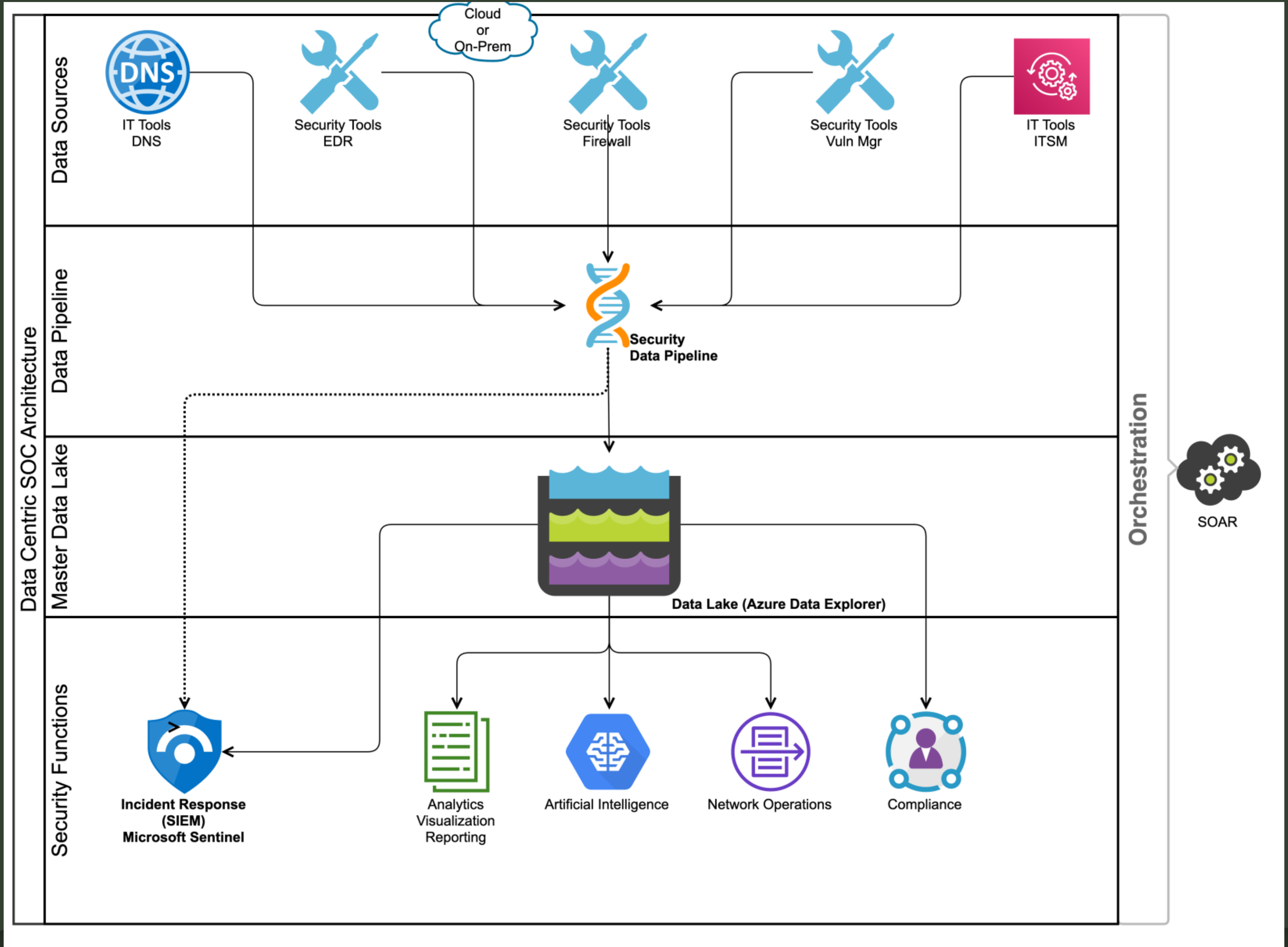
- Maintain or increase quality of investigations
  (fewer business impacts, greater profitability)
- Reduce incident resolution time
  (reduce business impacts, greater profitability)
- More work same people
  (maintain op costs, greater profitability)
- Analyst spin up time reduced
- …….

Wrap Up

Wrap Up

- AI is going to play an important role in SecOps future
- SIEM/Data Lake needs to be part of a data centric SOC architecture with AI as a component
- Need to balance cost, maintenance and easy of use
- Go beyond prompts…

Moving to a Data Centric SOC Architecture



Questions?

Thank you

GREG STACHURA

GREGORY.STACHURA@SRA.IO

HTTPS://GITHUB.COM/THEOWLERY/RSS2025