Microsoft

Microsoft Automation
4 xOps

Elli Shlomo

in/elishlomo/

In a nutshell

□ Microsoft Sentinel Specialist
□ Cloud IR
□ AppSec Analyst

Contributions

□ Microsoft Sentinel 4 SecOps projects
□ MS Defender xOPS
□ Technical writer
□ Contributes to GitHub Projects
□ Mentorship

Skills & interests

□ Microsoft Sentinel
□ DevSecOps / AppSec
□ Threat Hunting
□ KQL
□ Cloud-Native Security
□ SOC Builder
□ DFIR
□ Azure Security
□ Microsoft 365 Security

Experience

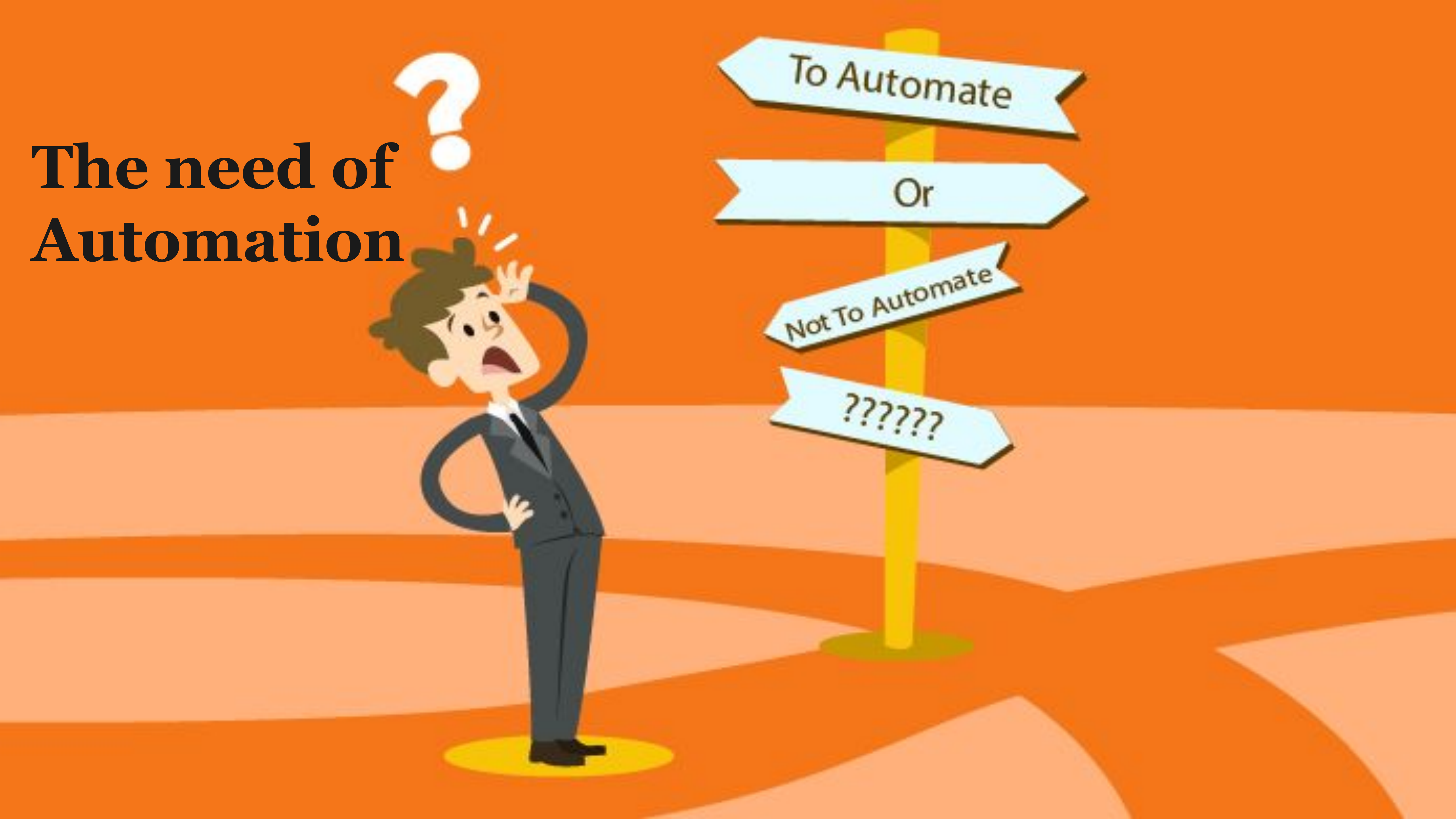
□ 20+ years working with IT, cloud and security
□ Working on Cloud since 2010

Recognitions

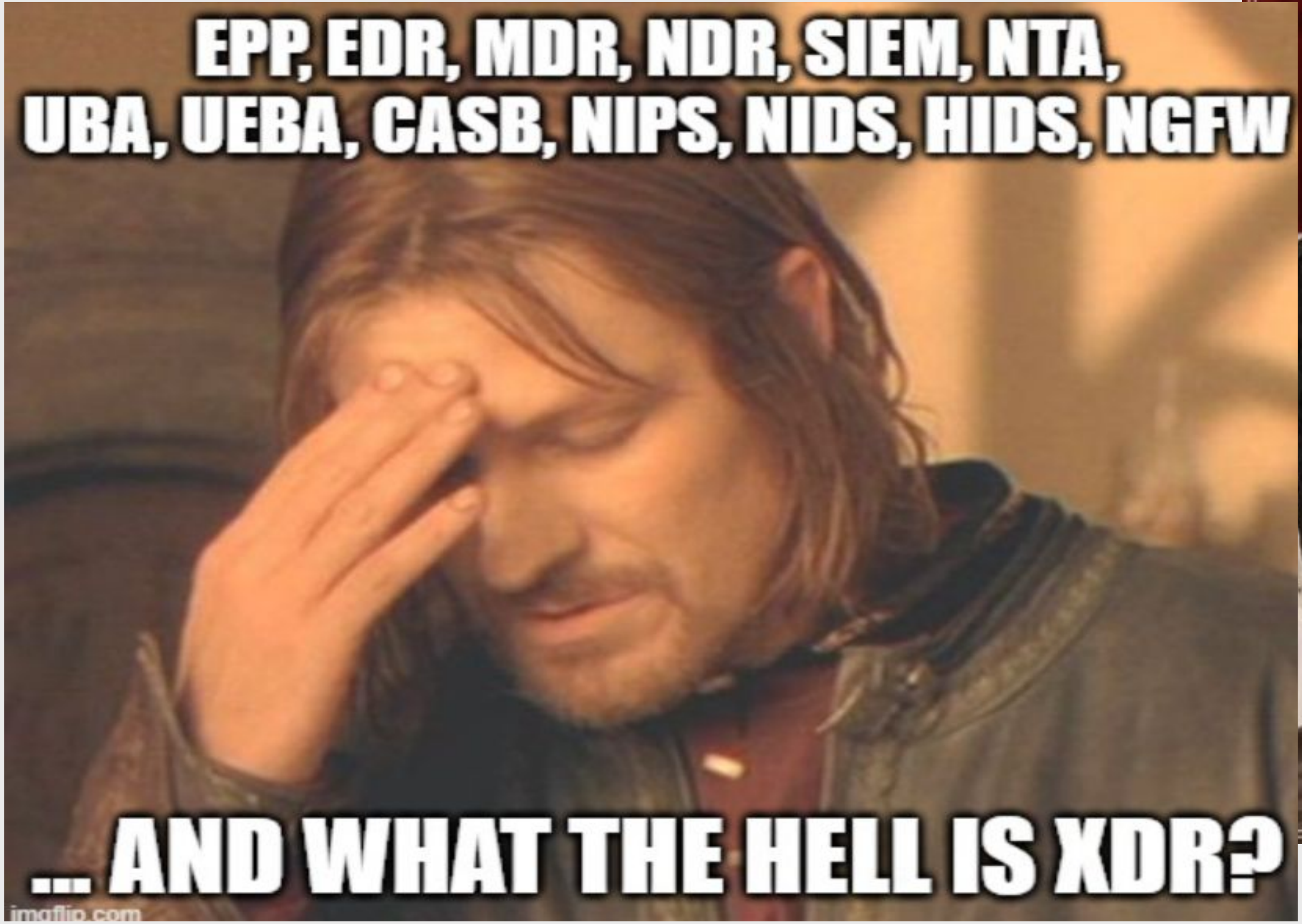
□ Microsoft MVP award since 2013
□ Community Leader since 2009
□ Azure Certified
□ Microsoft Certified
□ AWS Security Certified

The Reality

The need of Automation



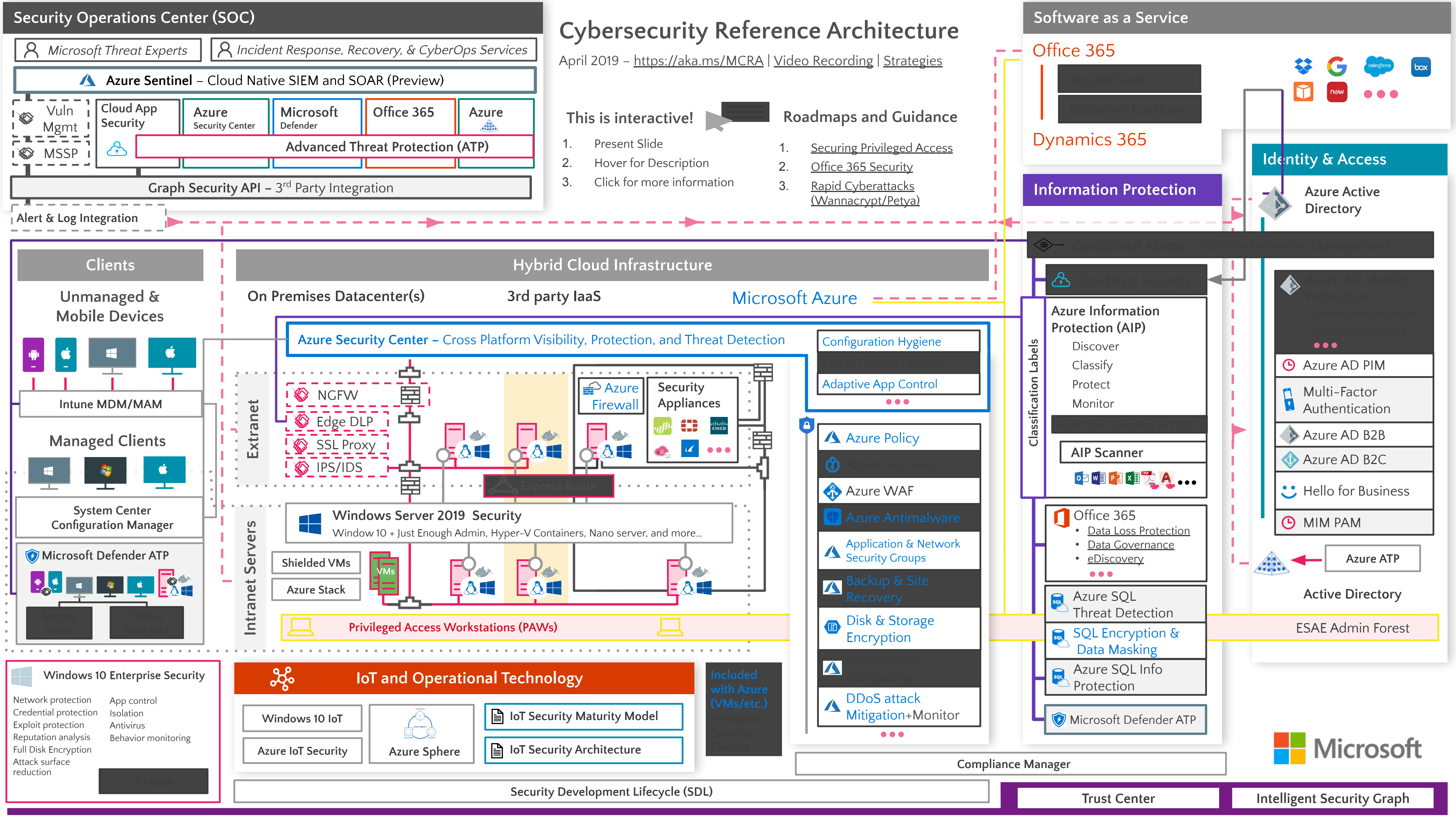
let's buzz it


EPP, EDR, MDR, NDR, SIEM, NTA,
UBA, UEBA, CASB, NIPS, NIDS, HIDS, NGFW
... AND WHAT THE HELL IS XDR?
imgflip.com

I DON'T ALWAYS AUTOMATE
BUT WHEN I DO, IT'S MANUAL
makeameme.org

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies



This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

Microsoft Threat Experts | Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Microsoft Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score

Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

●●●

Extranet

NGFW

Edge DLP

SSL Proxy

IPS/IDS

Azure Firewall

Security Appliances

●●●

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

●●●

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

salesforce

box

now

●●●

Information Protection

Conditional Access – Identity Perimeter Management

Cloud App Security

Classification Labels

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

●●●

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

●●●

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Identity & Access

Azure Active Directory

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

●●●

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Windows 10 Enterprise Security

Network protection
Credential protection
Exploit protection
Reputation analysis
Full Disk Encryption
Attack surface reduction

App control
Isolation
Antivirus
Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Included with Azure (VMs/etc.)

Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

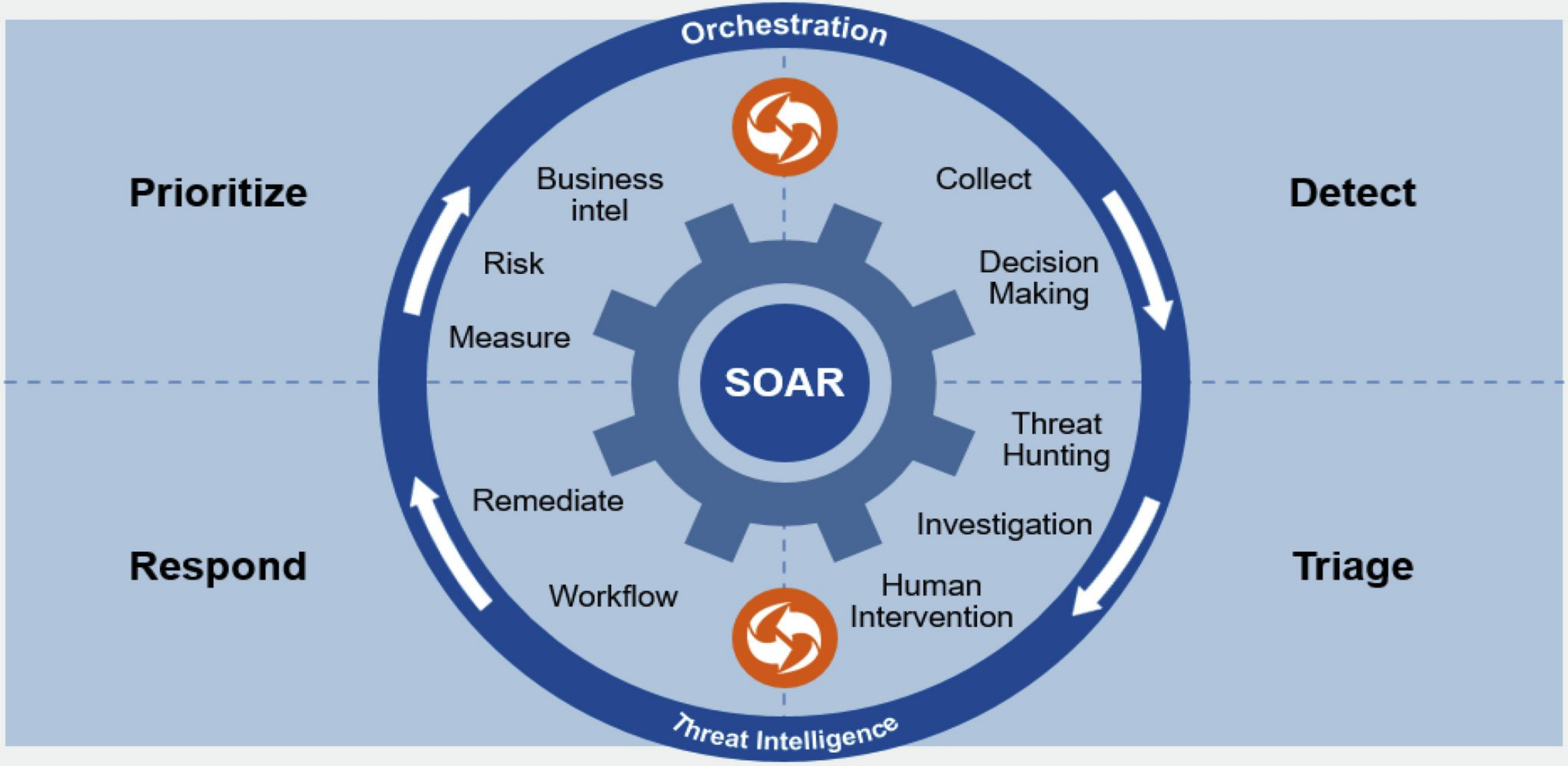
Intelligent Security Graph

Microsoft

Microsoft

Starting Point

Security Orchestration, Automation and Response: An Overview



ID: 338719

What SOAR is not

- Governance, risk and compliance (GRC)
- SIEM
- User and entity behavior analytics (UEBA)
- Threat and vulnerability management (TVM)

Drivers for SOAR

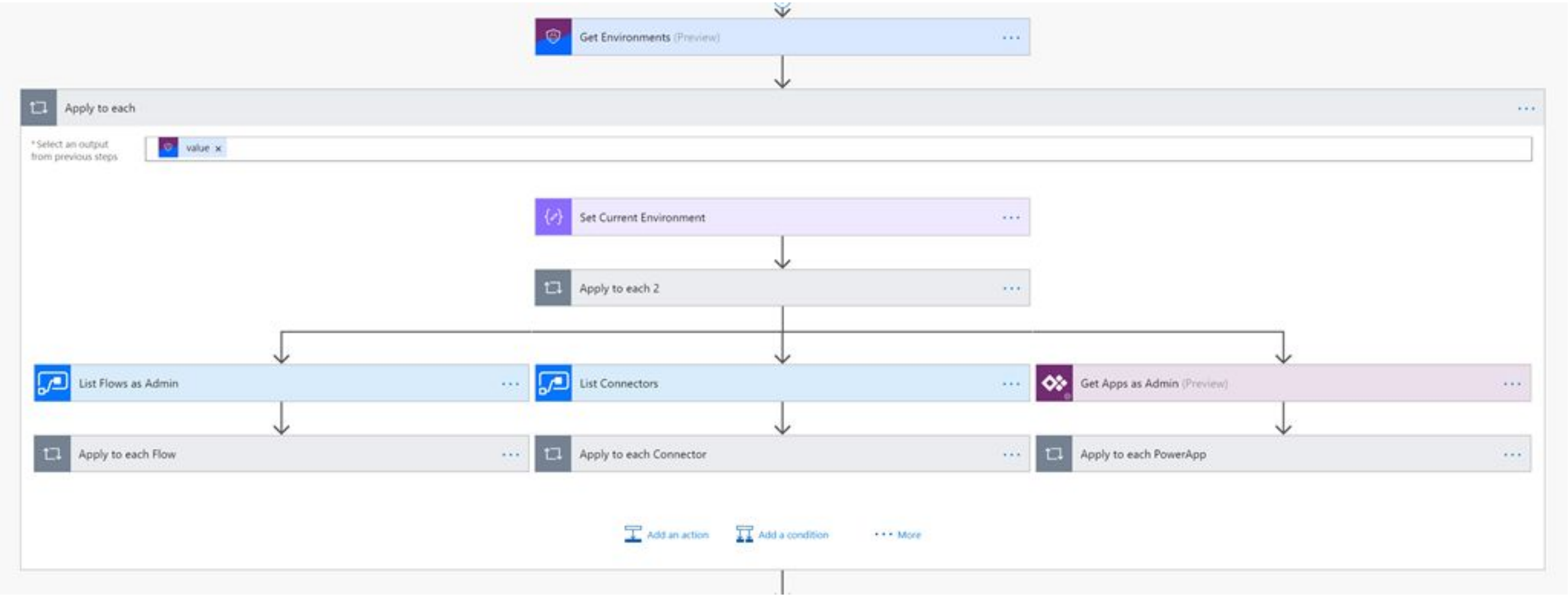
- Staff shortage
- The explosion of unattended alerts
- Threats becoming more destructive
- Awareness of the intersection of your environment with the prevailing threat landscape

Microsoft

The Good, Bad and the Security Gaps

The Good ~ Built-in Automation

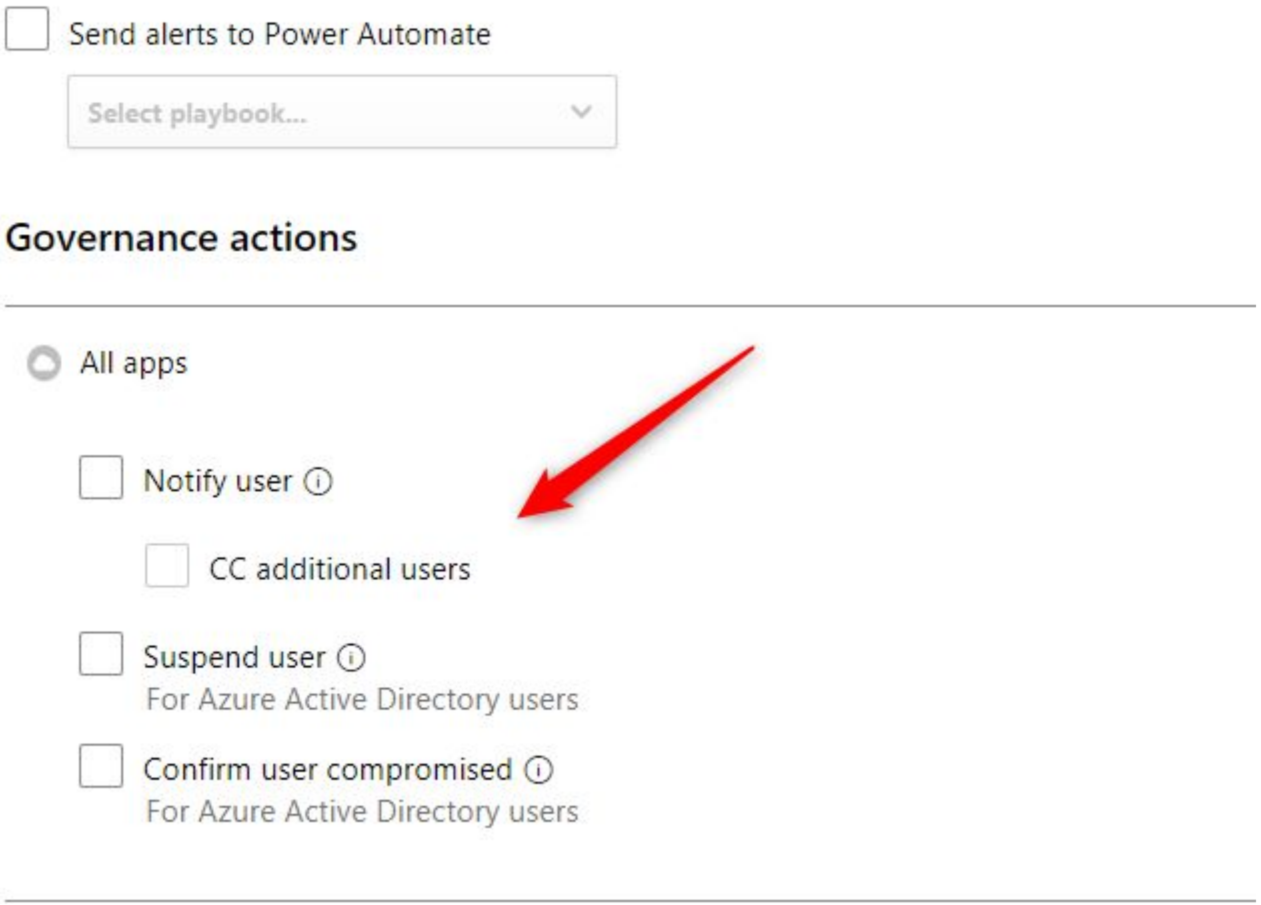
- Threat Protection tools
- Azure DevOps process
- Azure Security



*Select an output from previous steps: value

The Bad ~ General Automation

- Specific Action & Scenarios
- Not granularity
- It’s all or nothing



□ Send alerts to Power Automate

Select playbook...

Governance actions

○ All apps

□ Notify user ⓘ

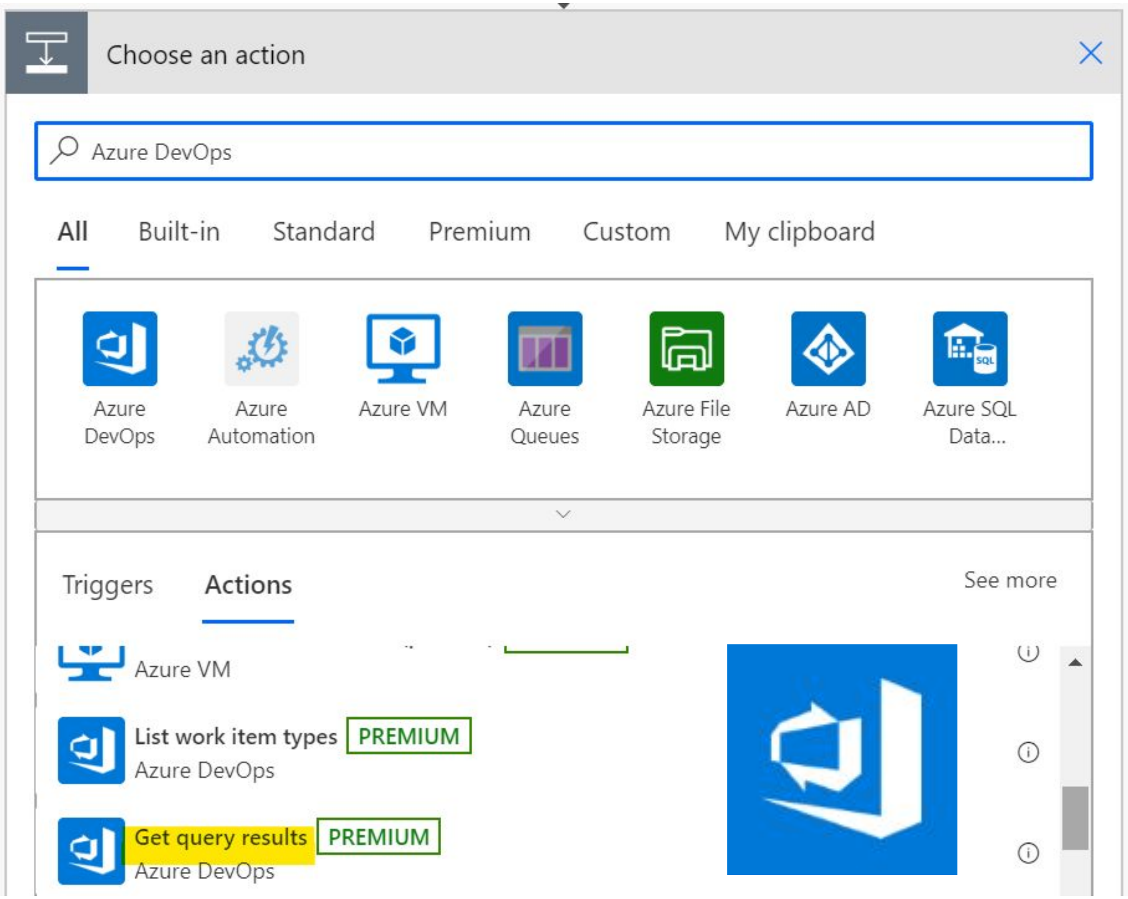
□ CC additional users

□ Suspend user ⓘ
For Azure Active Directory users

□ Confirm user compromised ⓘ
For Azure Active Directory users

The Gaps ~ Power-Automate

- M365 Security integration
- Azure DevOps integration
- Azure integration

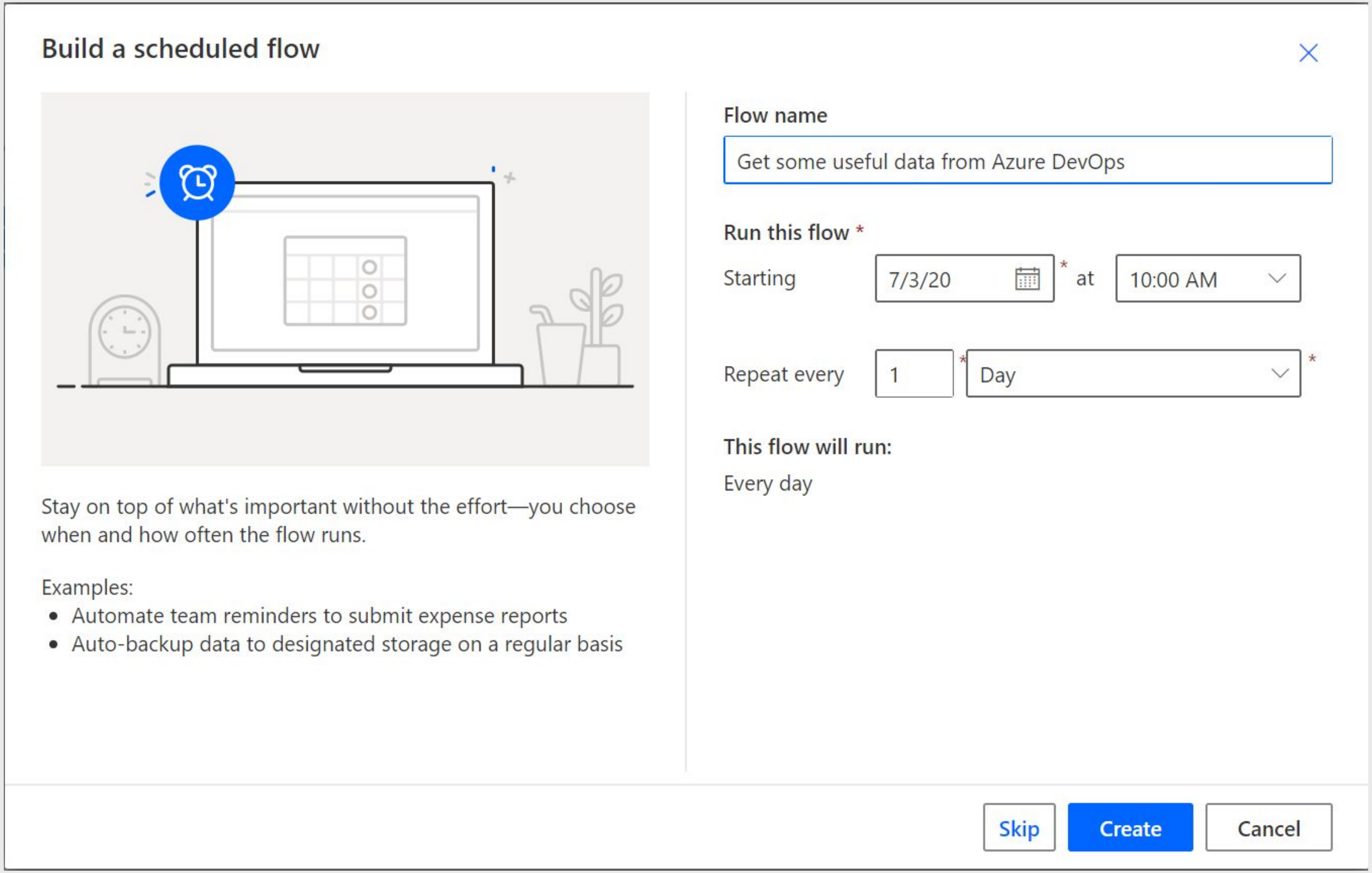


Power-Automate Scenario’s

Azure DevOps Reports - Scenario

- Features are going to be released
- Developers working on in a particular Sprint
- To list out the sprints/iterations

Azure DevOps Reports – Cont’d



Build a scheduled flow

Stay on top of what's important without the effort—you choose when and how often the flow runs.

Examples:

- Automate team reminders to submit expense reports
- Auto-backup data to designated storage on a regular basis

Flow name

Get some useful data from Azure DevOps

Run this flow *

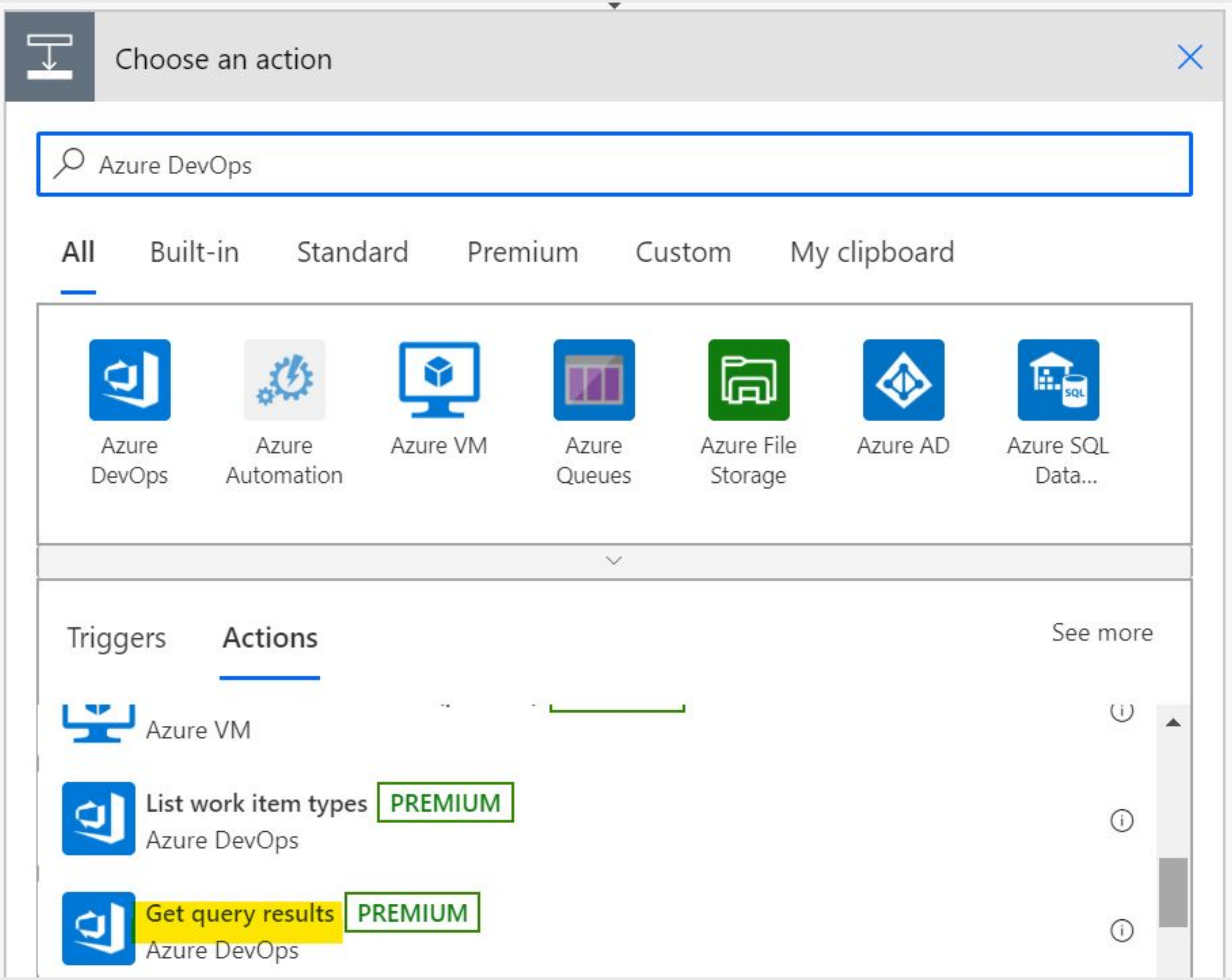
Starting 7/3/20 * at 10:00 AM

Repeat every 1 * Day *

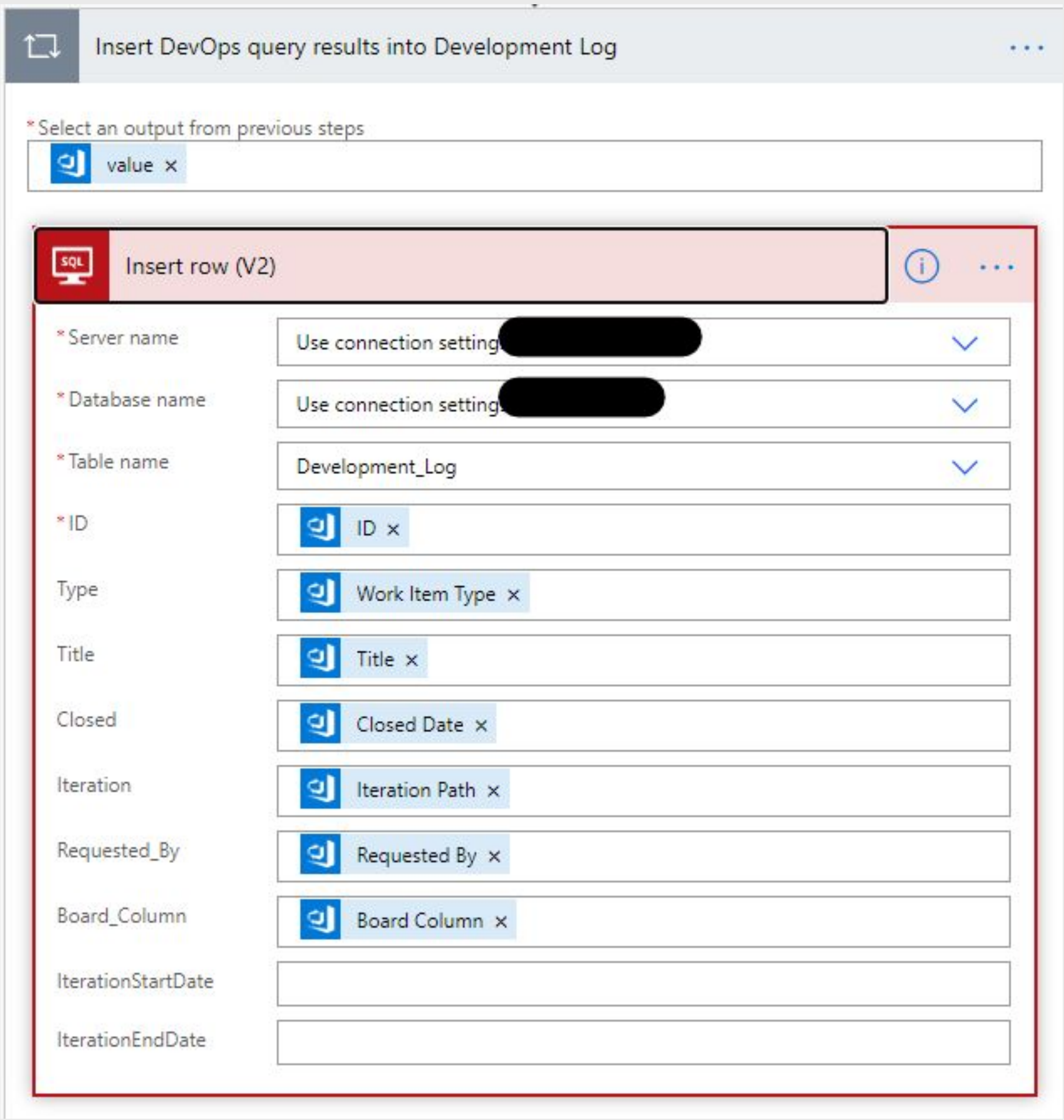
This flow will run:

Every day

Azure DevOps Reports – Cont’d



Azure DevOps Reports – Cont’d



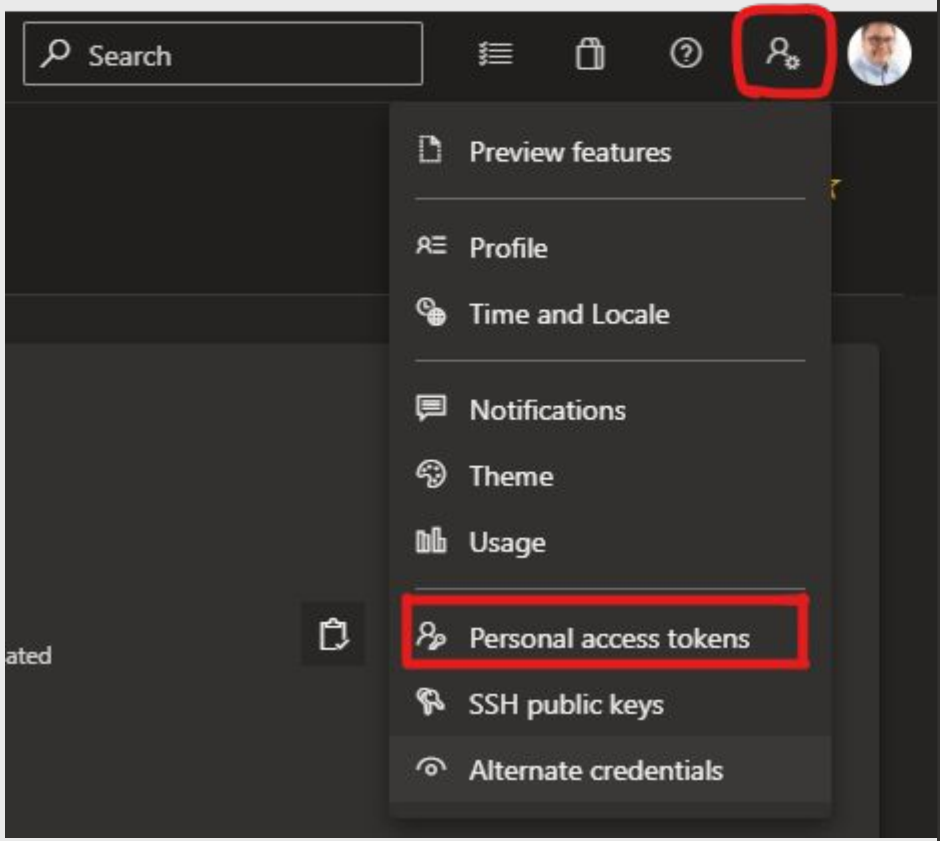
Insert DevOps query results into Development Log

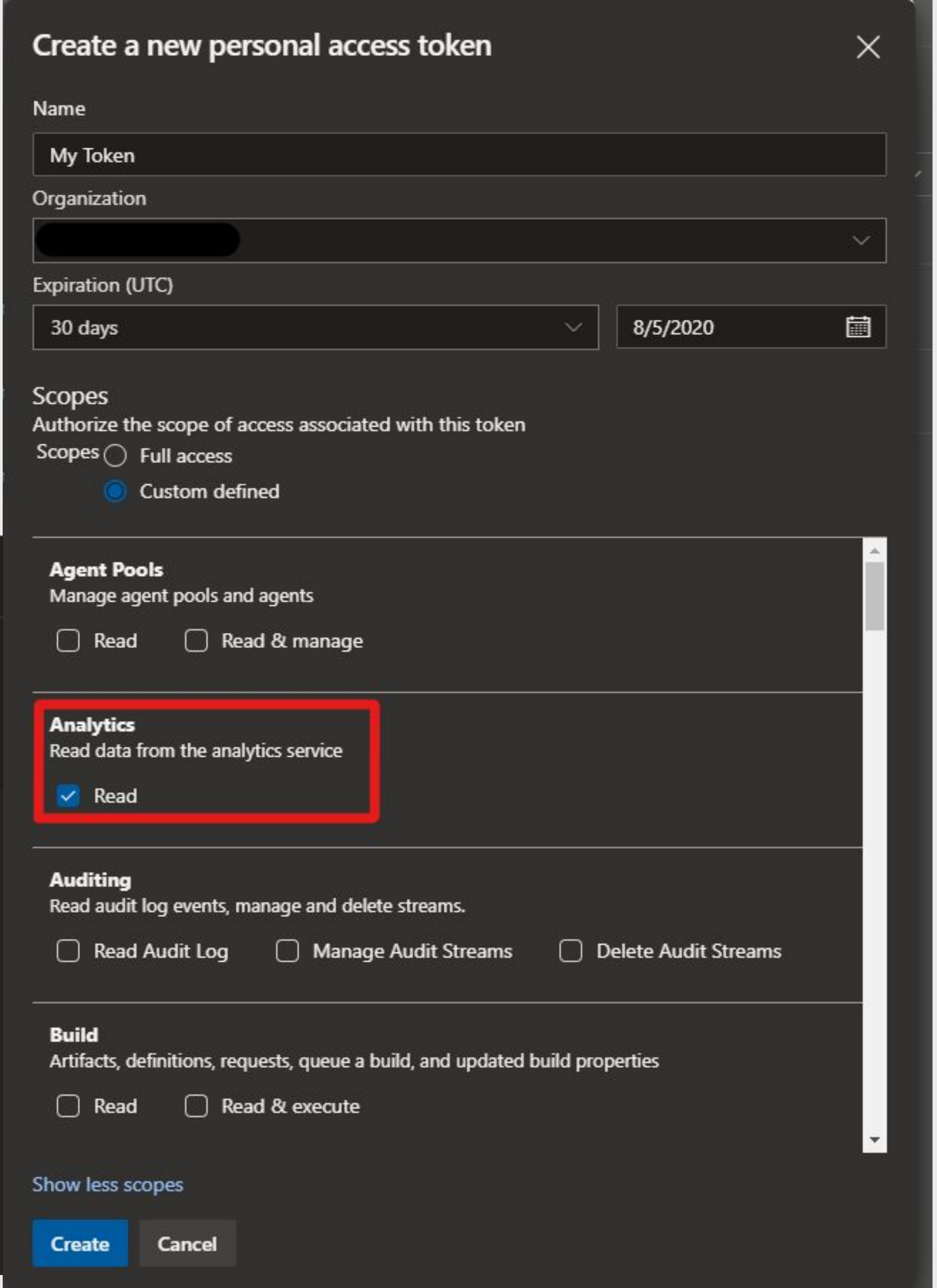
*Select an output from previous steps: value ×

Insert row (V2)

*Server name	Use connection setting [redacted]
*Database name	Use connection setting [redacted]
*Table name	Development_Log
*ID	ID ×
Type	Work Item Type ×
Title	Title ×
Closed	Closed Date ×
Iteration	Iteration Path ×
Requested_By	Requested By ×
Board_Column	Board Column ×
IterationStartDate	
IterationEndDate	

Azure DevOps Reports – Cont'd





Create a new personal access token

Name: My Token

Organization: [redacted]

Expiration (UTC): 30 days 8/5/2020

Scopes

Authorize the scope of access associated with this token

Scopes ○ Full access ● Custom defined

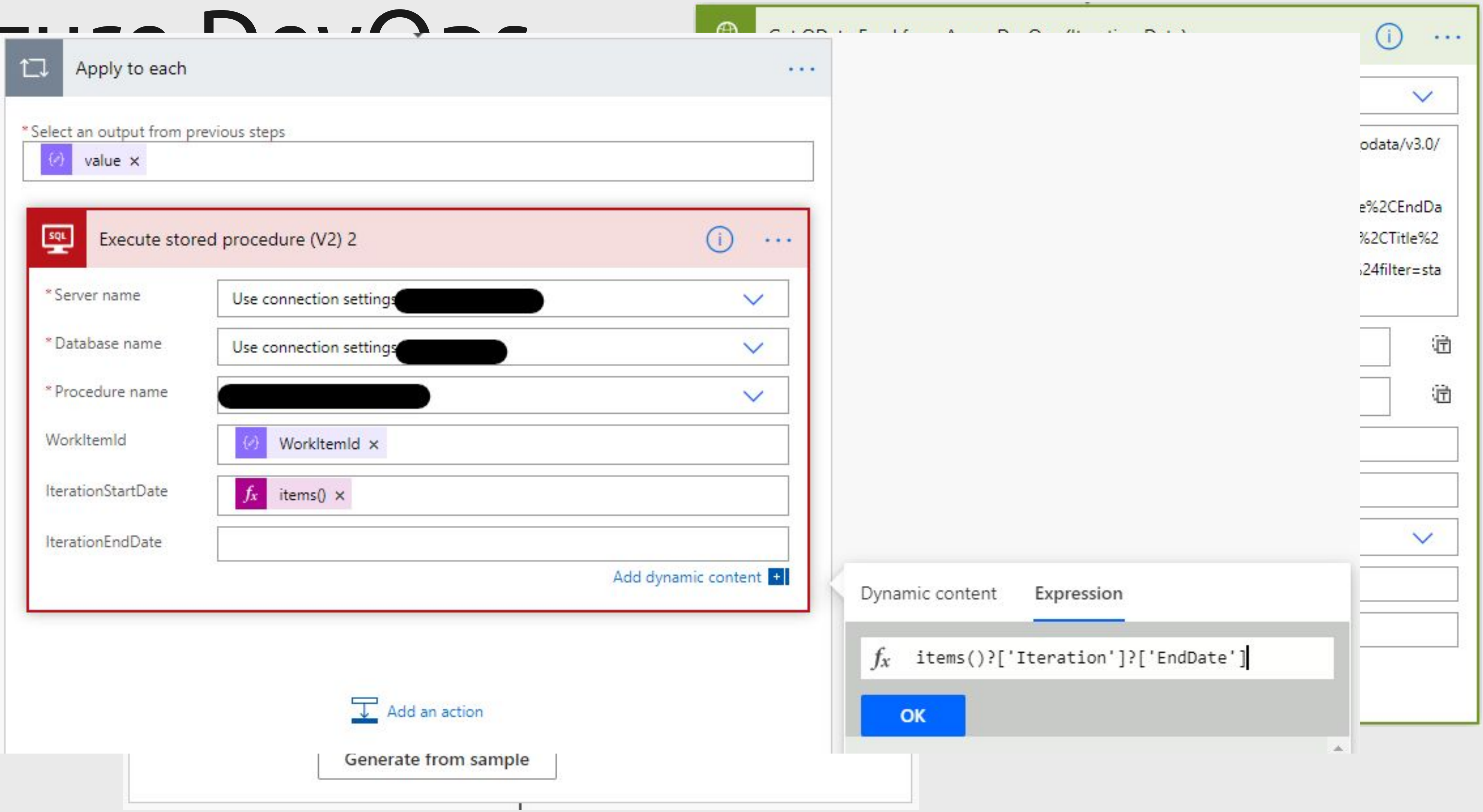
Agent Pools
Manage agent pools and agents
☐ Read ☐ Read & manage

Analytics
Read data from the analytics service
☑ Read

Auditing
Read audit log events, manage and delete streams.
☐ Read Audit Log ☐ Manage Audit Streams ☐ Delete Audit Streams

Build
Artifacts, definitions, requests, queue a build, and updated build properties
☐ Read ☐ Read & execute

Azure DevOps
Re
Co



odata/v3.0/

e%2CEndDa

%2CTitle%2

24filter=sta

Apply to each

* Select an output from previous steps: value ×

Execute stored procedure (V2) 2

* Server name: Use connection settings [redacted]

* Database name: Use connection settings [redacted]

* Procedure name: [redacted]

WorkItemId: WorkItemId ×

IterationStartDate: items() ×

IterationEndDate:

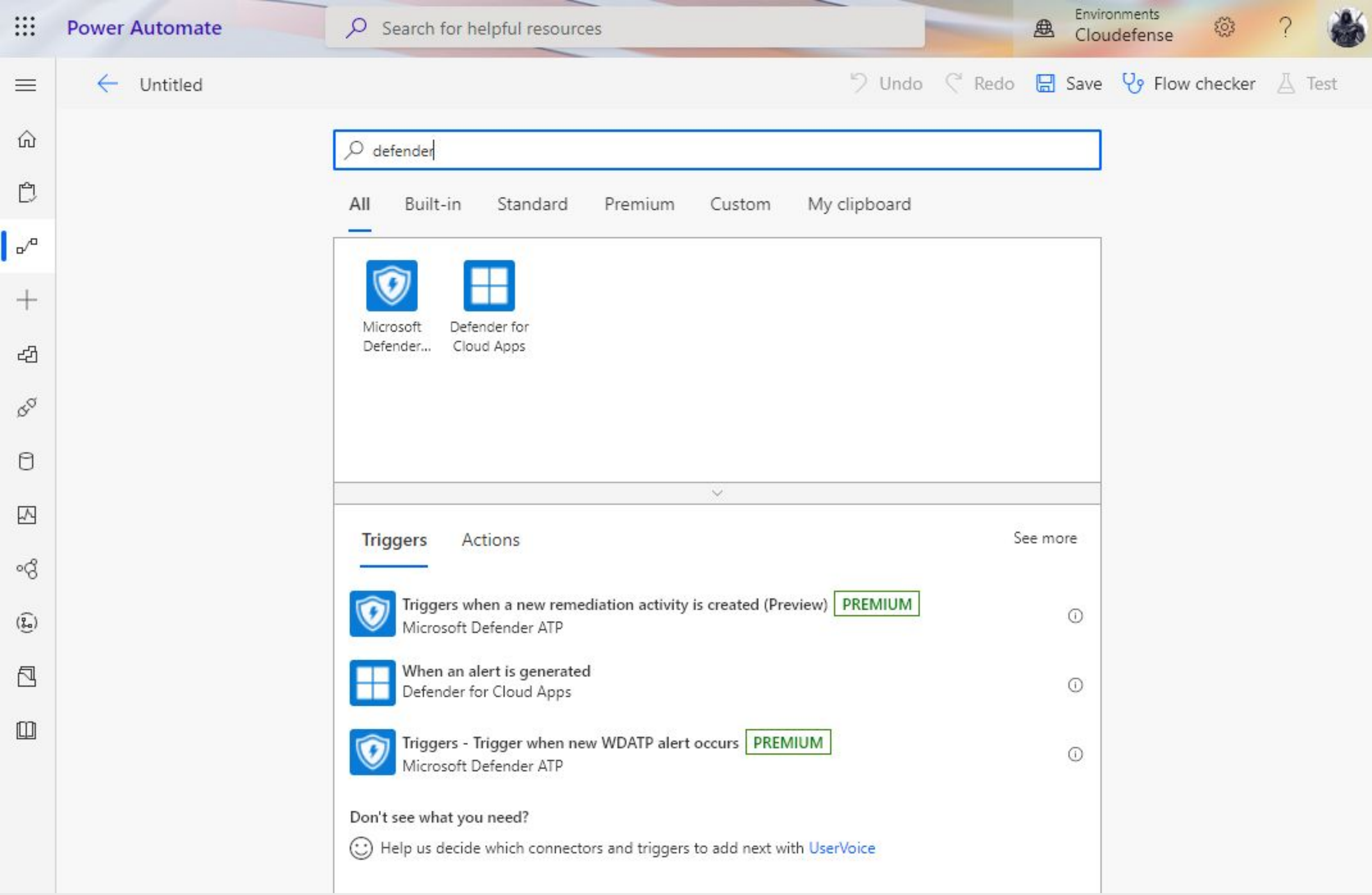
Add dynamic content

Dynamic content | Expression

```
items()?['Iteration']?['EndDate']
```

Security Automation - Demo

- Auto-Triage Defender for Cloud in 5 min’



defender

Triggers when a new remediation activity is created (Preview) PREMIUM
Microsoft Defender ATP

When an alert is generated
Defender for Cloud Apps

Triggers - Trigger when new WDATP alert occurs PREMIUM
Microsoft Defender ATP

Don't see what you need?

Help us decide which connectors and triggers to add next with UserVoice

Security Automation - Demo

Power Automate packages for Microsoft Defender for Cloud Apps (PA 4 MDA)

https://github.com/eshlomo1/MS-Defender-4-xOPS/tree/main/Security-Automation/MDA

Microsoft

THANK YOU!