Microsoft Security

# Automate(d) Security with Microsoft Defender for Cloud

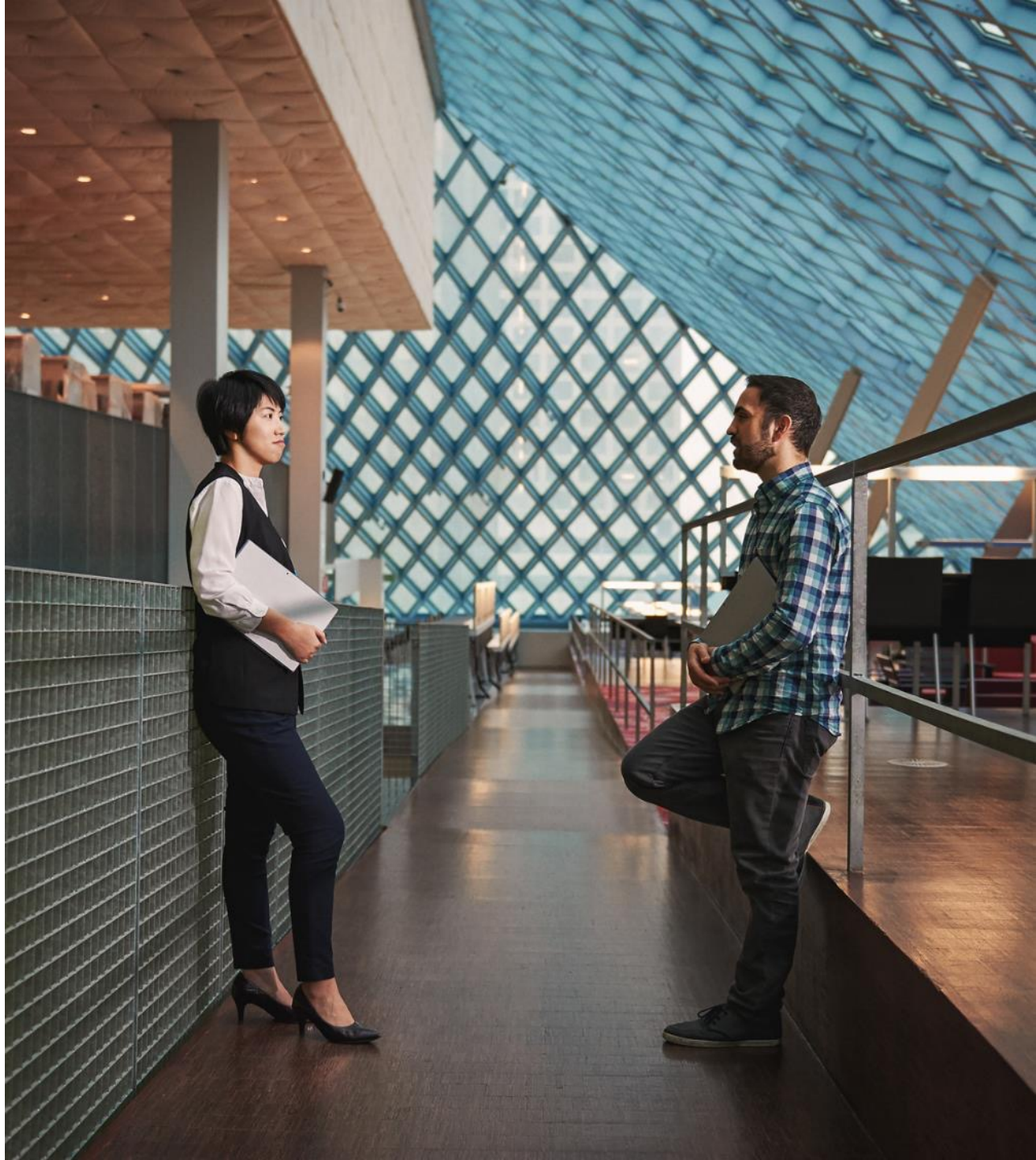
**Tom Janetscheck**

Senior Program Manager

Defender for Cloud Engineering

# Agenda

- Microsoft Defender for Cloud Data Overview
- REST APIs
- Continuous Export
- Workflow Automation
- Logic Apps



# Microsoft Defender for Cloud

## Strengthen multi cloud security posture

Secure Score | Policies and compliance | Improved automation

Leveraging Azure Arc

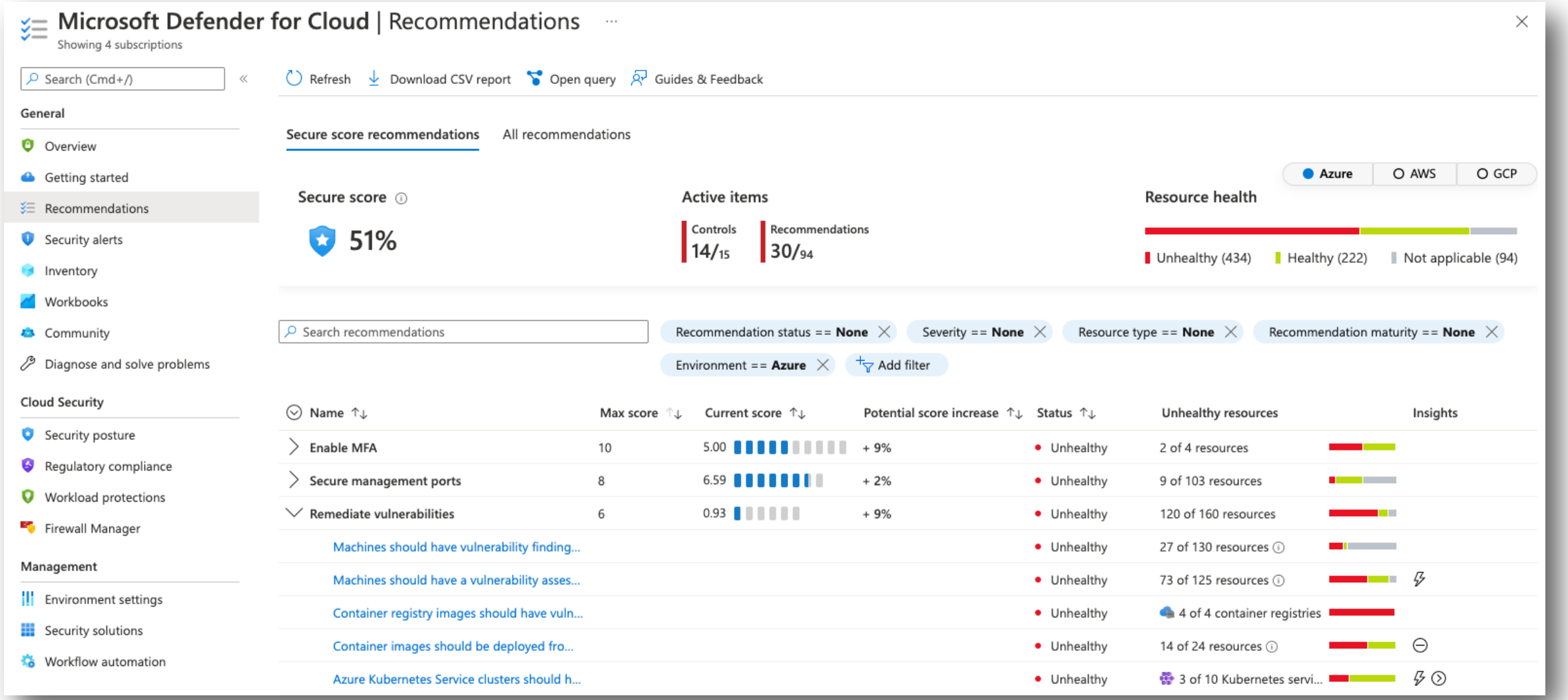
## Protect your hybrid cloud with Microsoft Defender

For servers | For cloud native workloads | For databases and storage

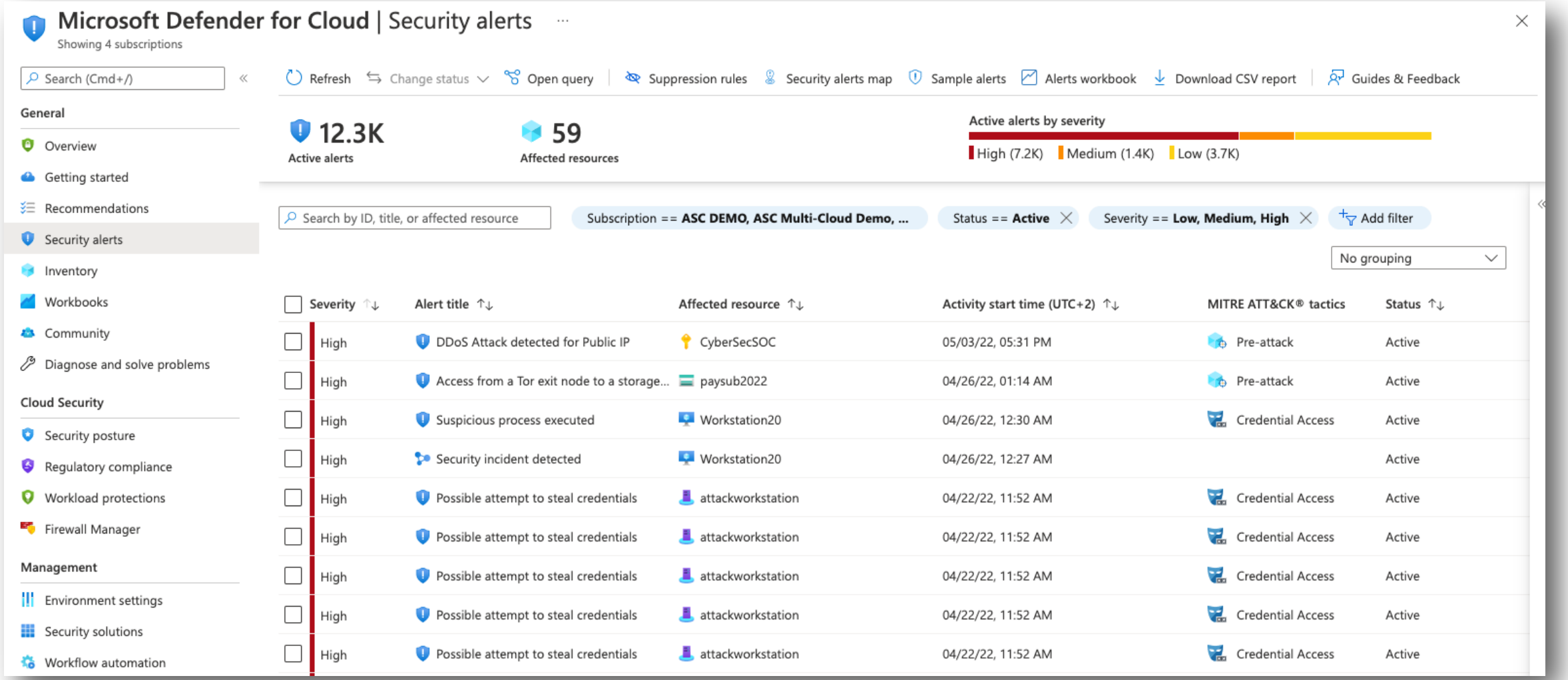
For Azure service layers | For IoT devices

Streamline security management

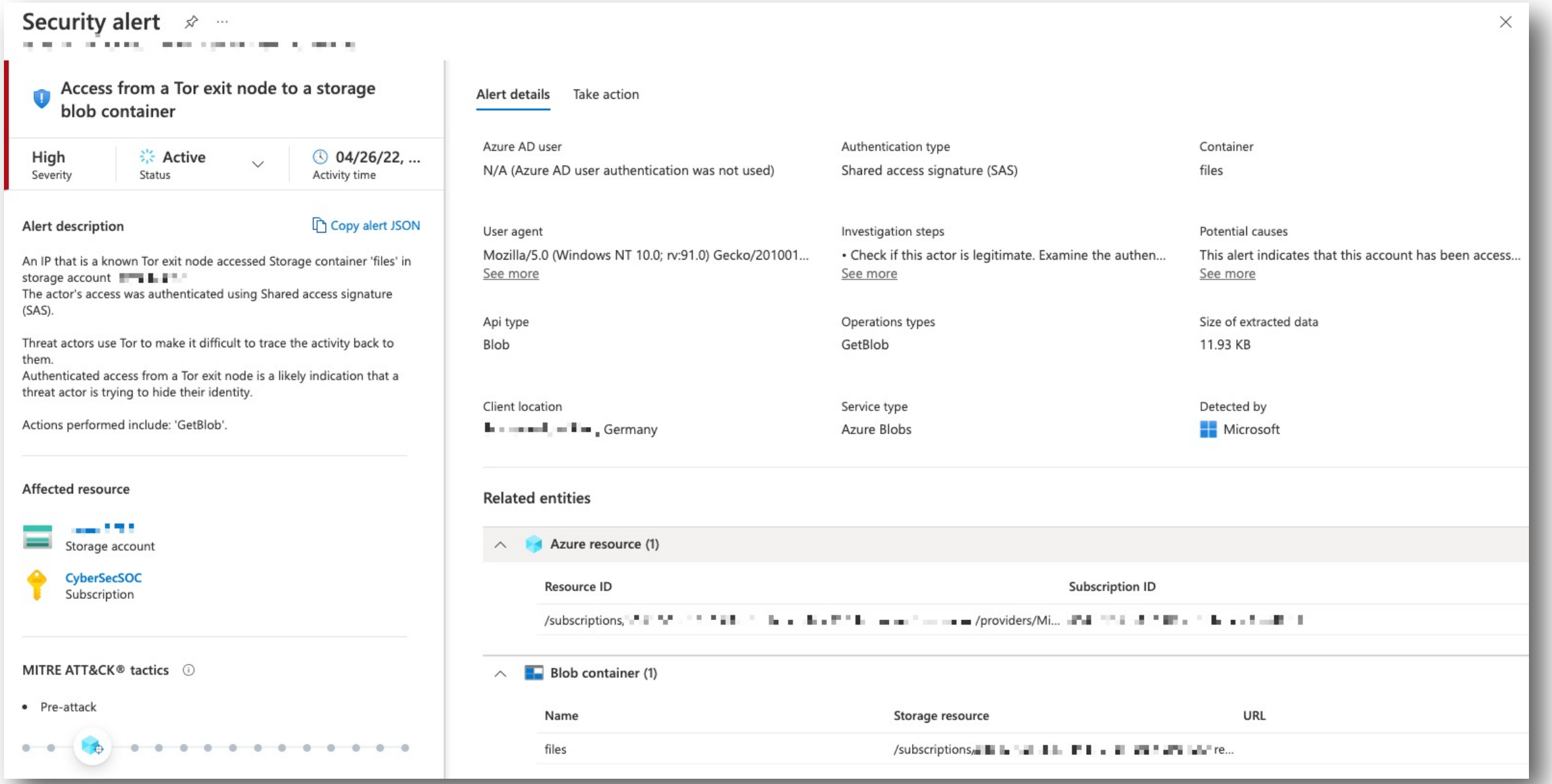
# Secure Score and recommendations



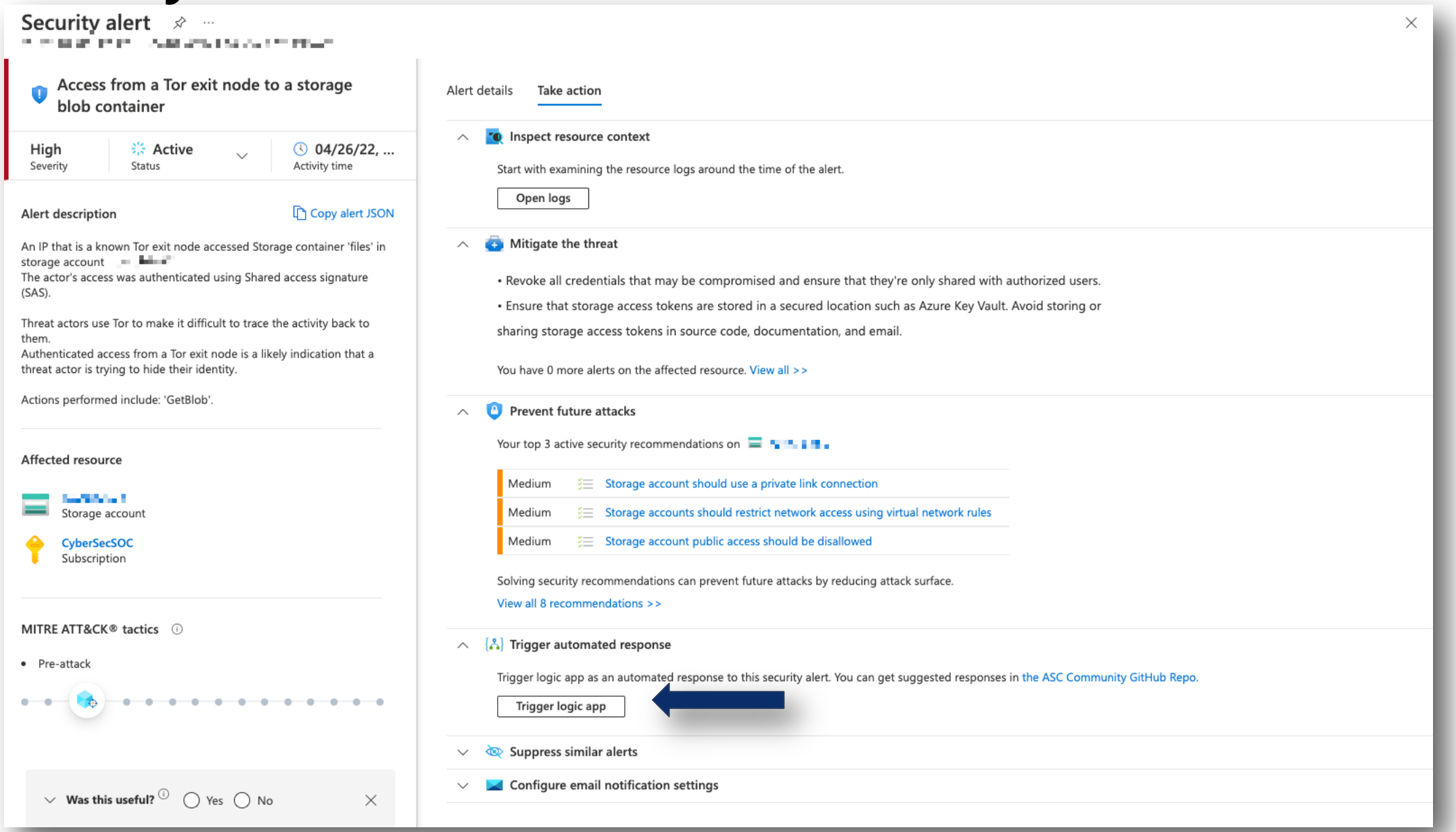
# Security Alerts



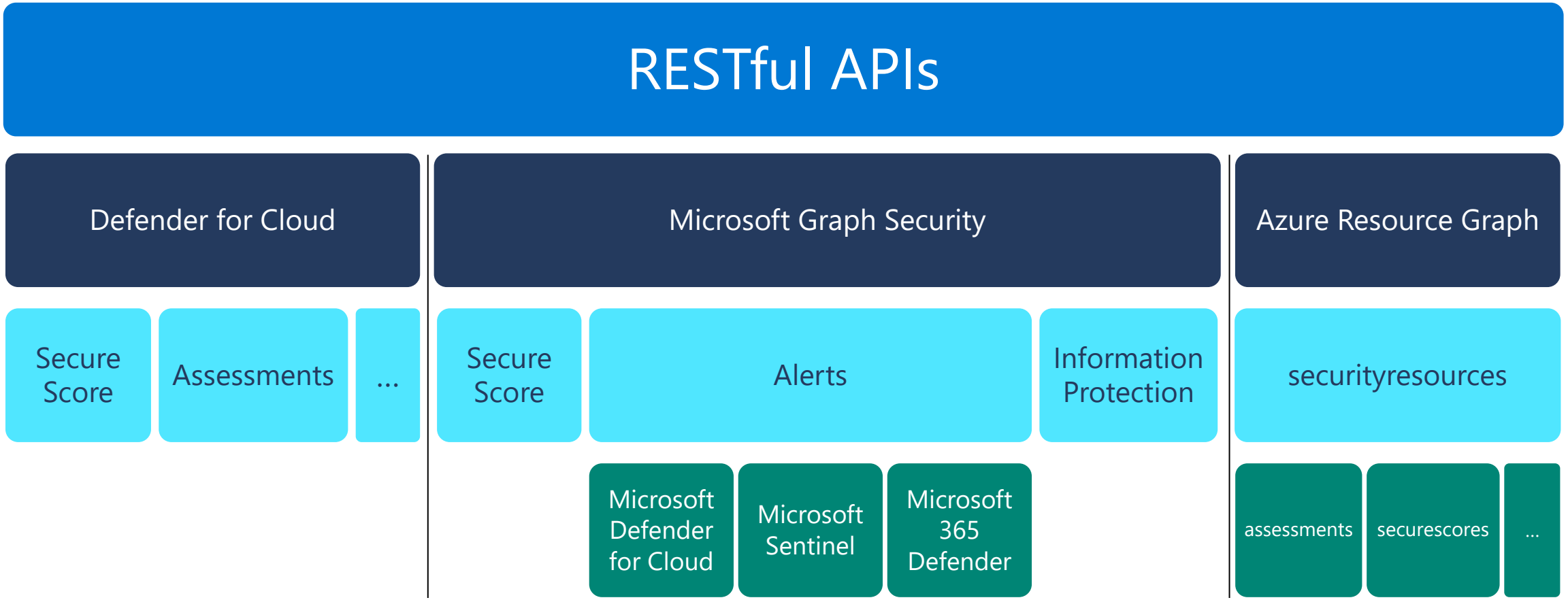
# Security Alerts



# Security Alerts



# API options


RESTful APIs
Defender for Cloud
Microsoft Graph Security
Azure Resource Graph
Secure Score
Assessments
...
Secure Score
Alerts
Information Protection
securityresources
Microsoft Defender for Cloud
Microsoft Sentinel
Microsoft 365 Defender
assessments
securescores
...

# REST APIs

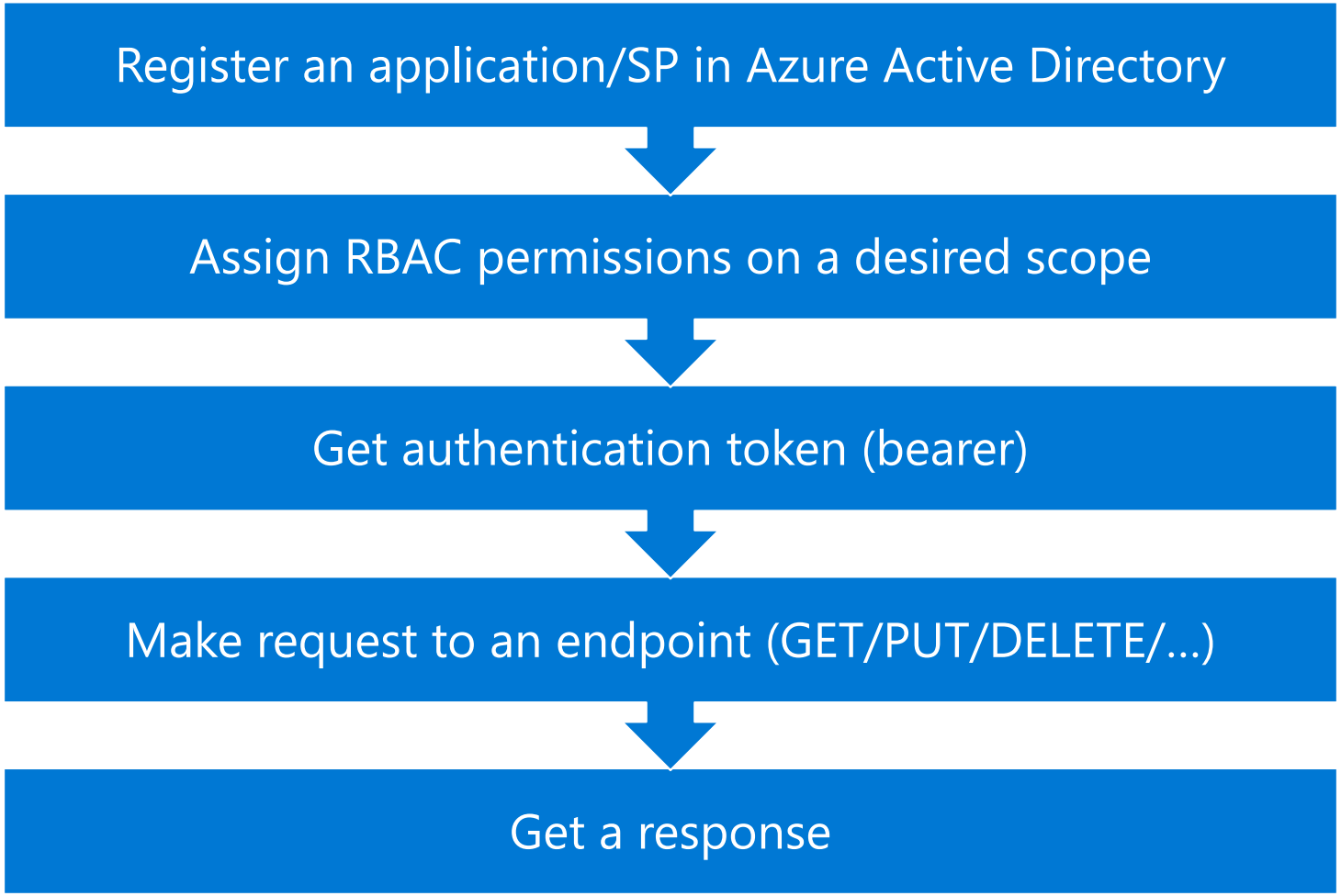
- Defender for Cloud
  - Provides a variety of operation groups
- Microsoft Security Graph
  - Consolidated API for security products
- Azure Resource Graph
  - Ability to query and access data from the graph

docs.microsoft.com/rest/api/azure/

## REST Operation Groups

| Operation Group | Description |
|---|---|
| Adaptive Application Controls | Configuration of application control rules on groups of VMs/servers. |
| Adaptive Network Hardenings | Controls for Adaptive Network Hardening resources and rules. |
| Advanced Threat Protection | Advanced Threat Protection settings on a specified resource. |
| Alerts | Alerts on security events that happened on the subscription. |
| Alerts Suppression Rules | View and edit alert suppression rules. |
| Allowed Connections | Lists the permissible traffic routes between resources. |
| Assessments | Manage security assessments. |
| Assessments Metadata | Manage metadata for the security assessments. |
| Auto Provisioning Settings | Auto provisioning settings of the subscriptions. |
| Automations | Manage security automations. |
| Compliances | Details of specific Compliances. |
| Device Security Groups | Manage the device security group for a specified IoT Hub resource. |
| Discovered Security Solutions | Details of specific discovered Security Solution. |
| External Security Solutions | External Security Solutions for the subscription and location. |
| Information Protection Policies | Details of the information protection policies. |
| Iot Alert Types | Details of an IoT alert type. |
| Iot Alerts | Get the IoT alerts. |
| Iot Recommendation Types | Get IoT recommendation types. |

# Prerequisites to work with APIs

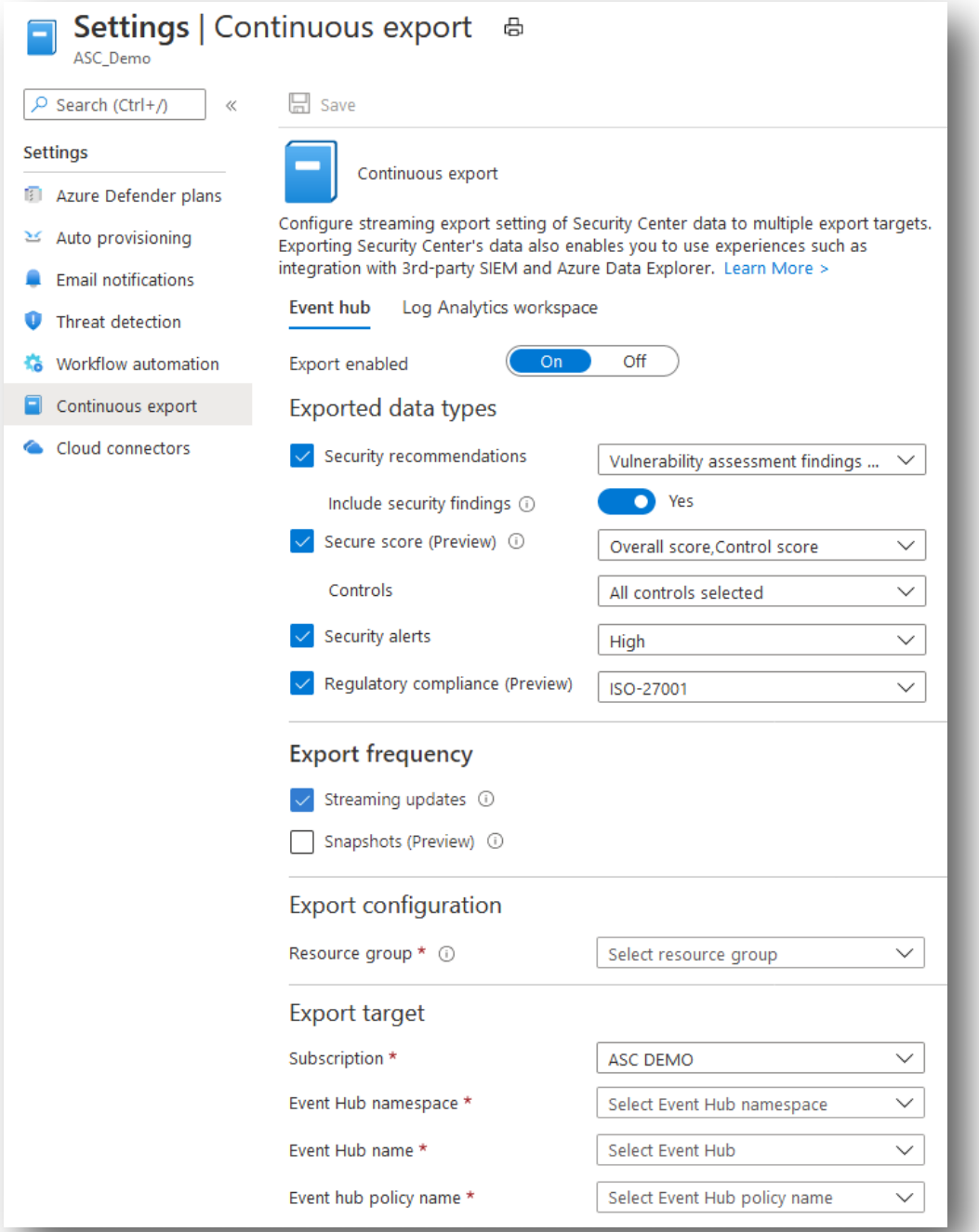


Microsoft

# Demo

# Continuous export

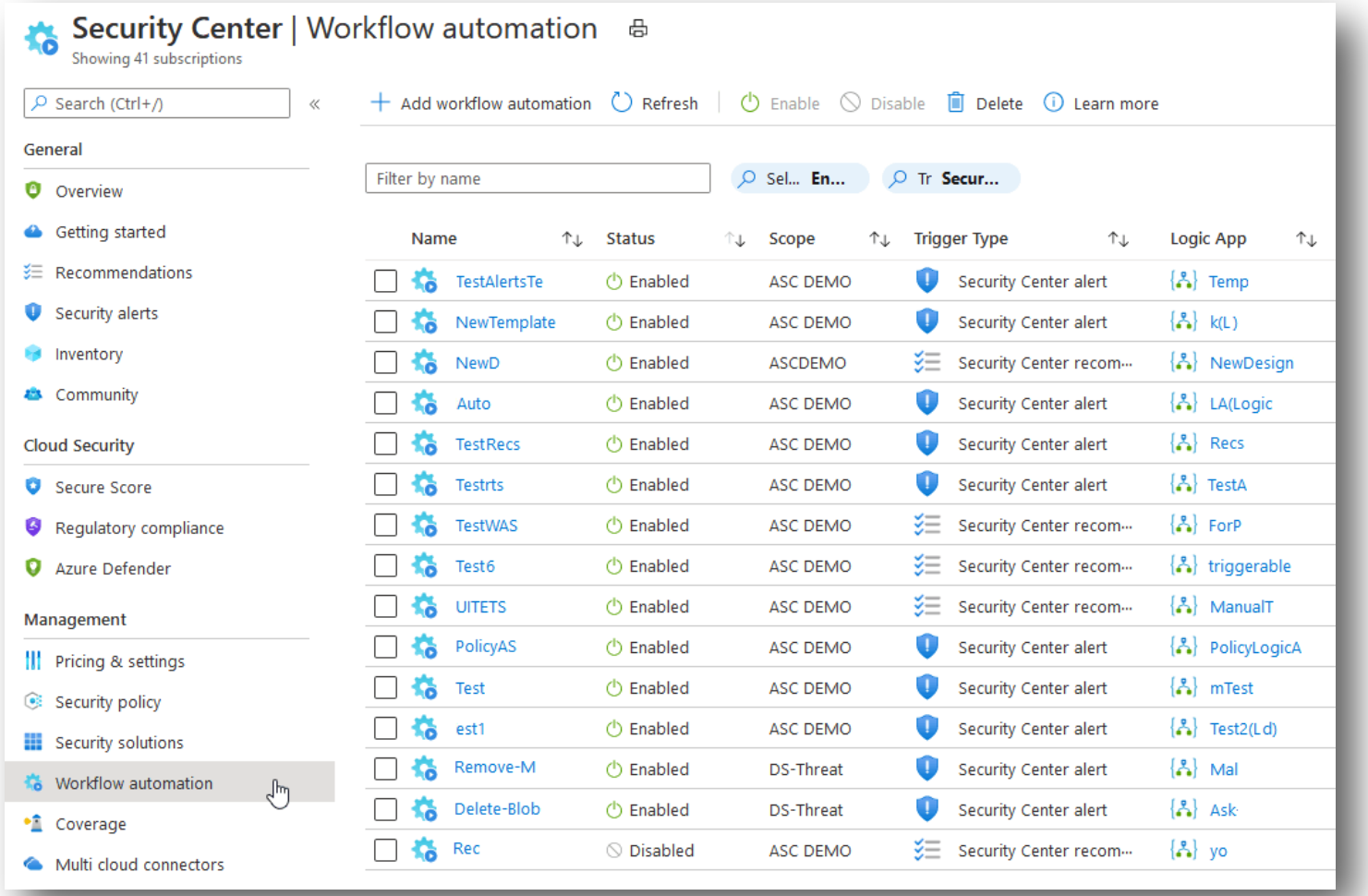
Automatically and regularly export ASC data to Azure Event Hub or Log Analytics workspace

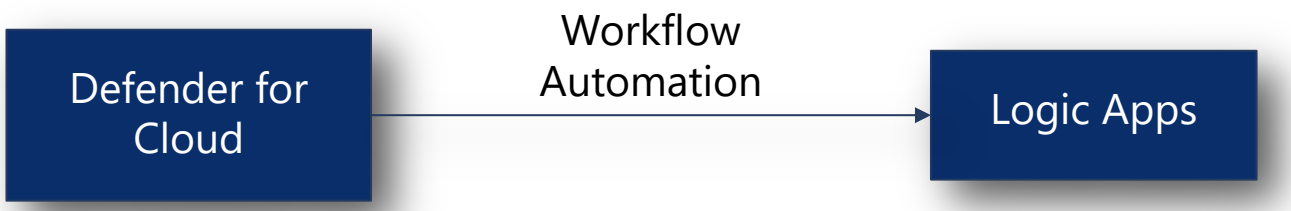


# Workflow automation

Automatically react on

- Security alerts
- Recommendations
- Regulatory compliance status changes



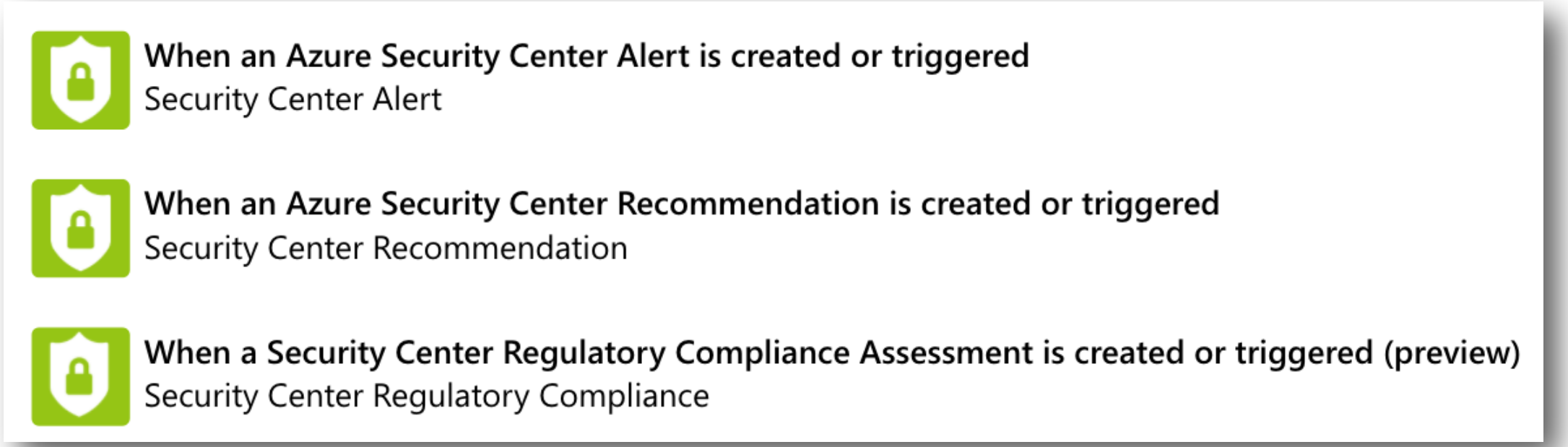



# Logic Apps

Let’s bring it all together

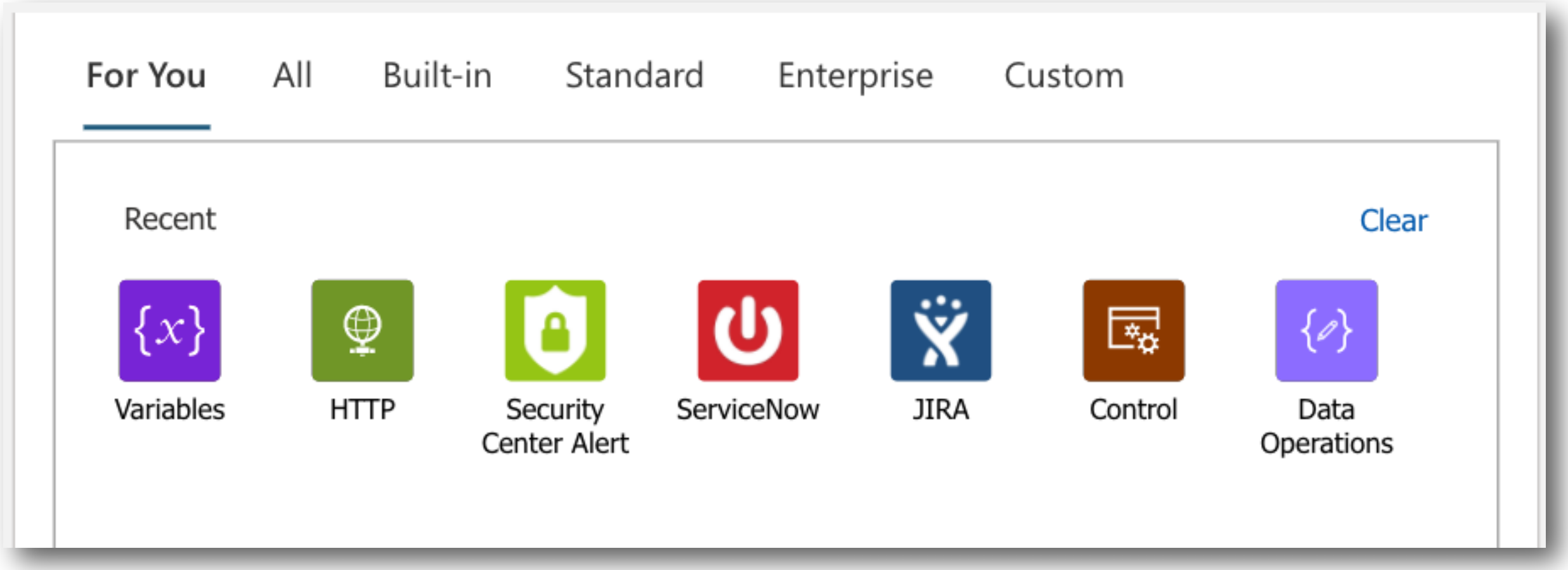
# Logic Apps

## Builtin Defender for Cloud triggers



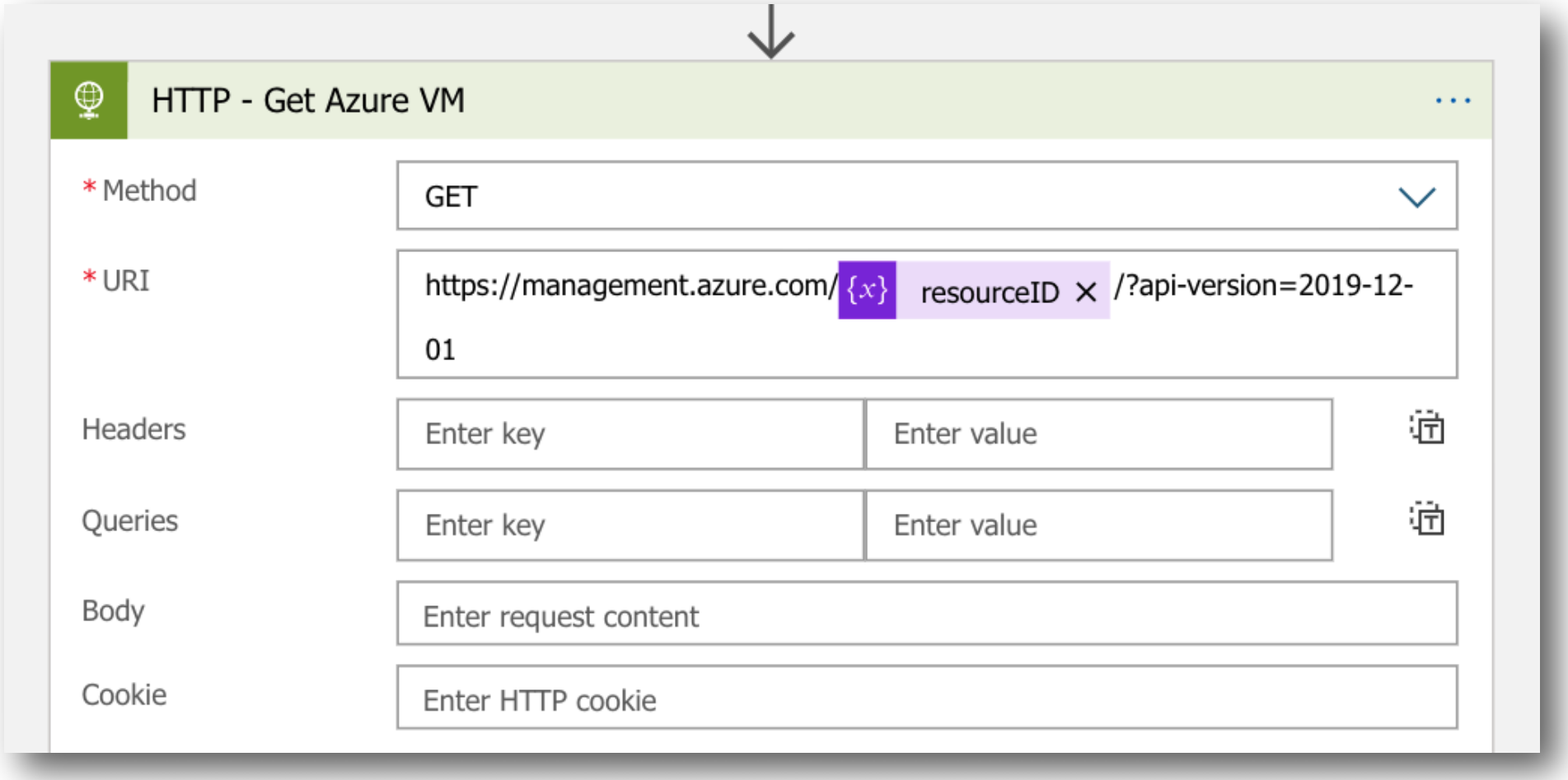
# Logic Apps

Native connectors to Microsoft and 3rd party services

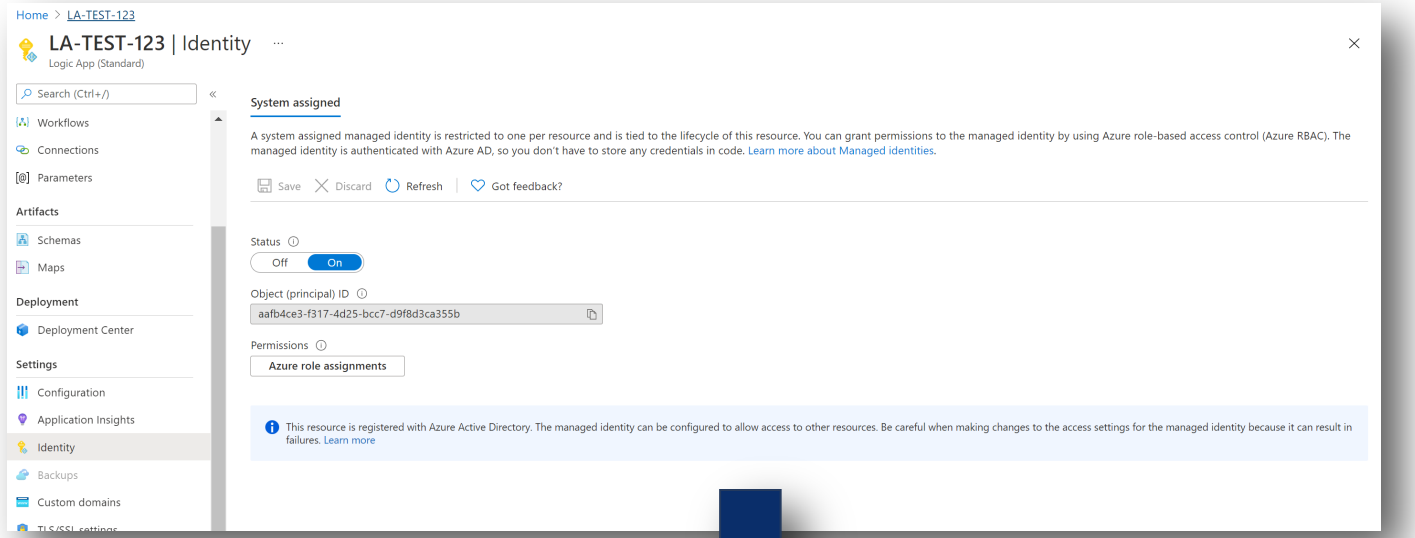


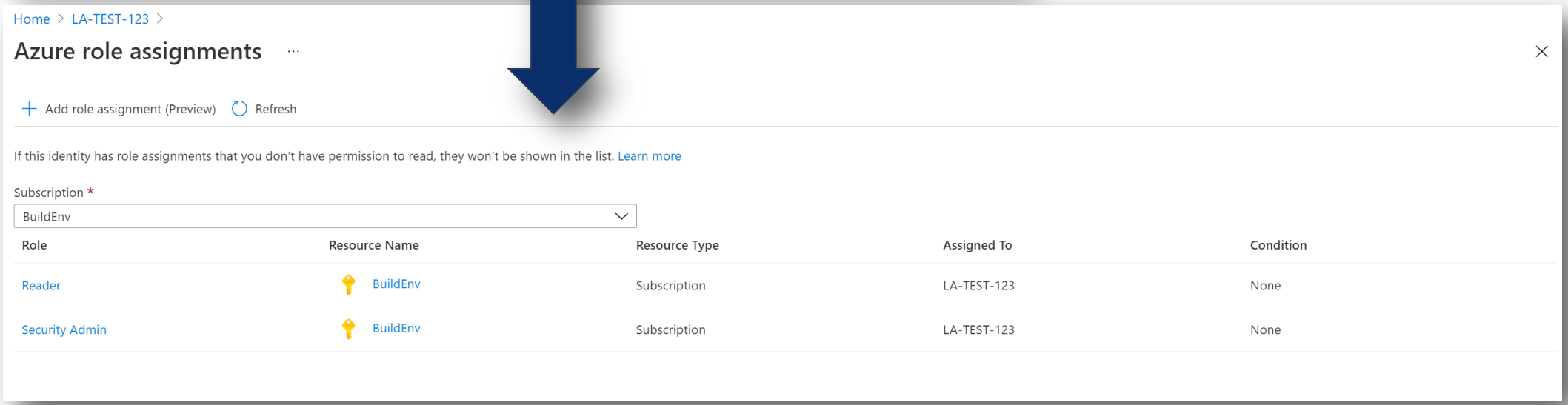
# Logic Apps

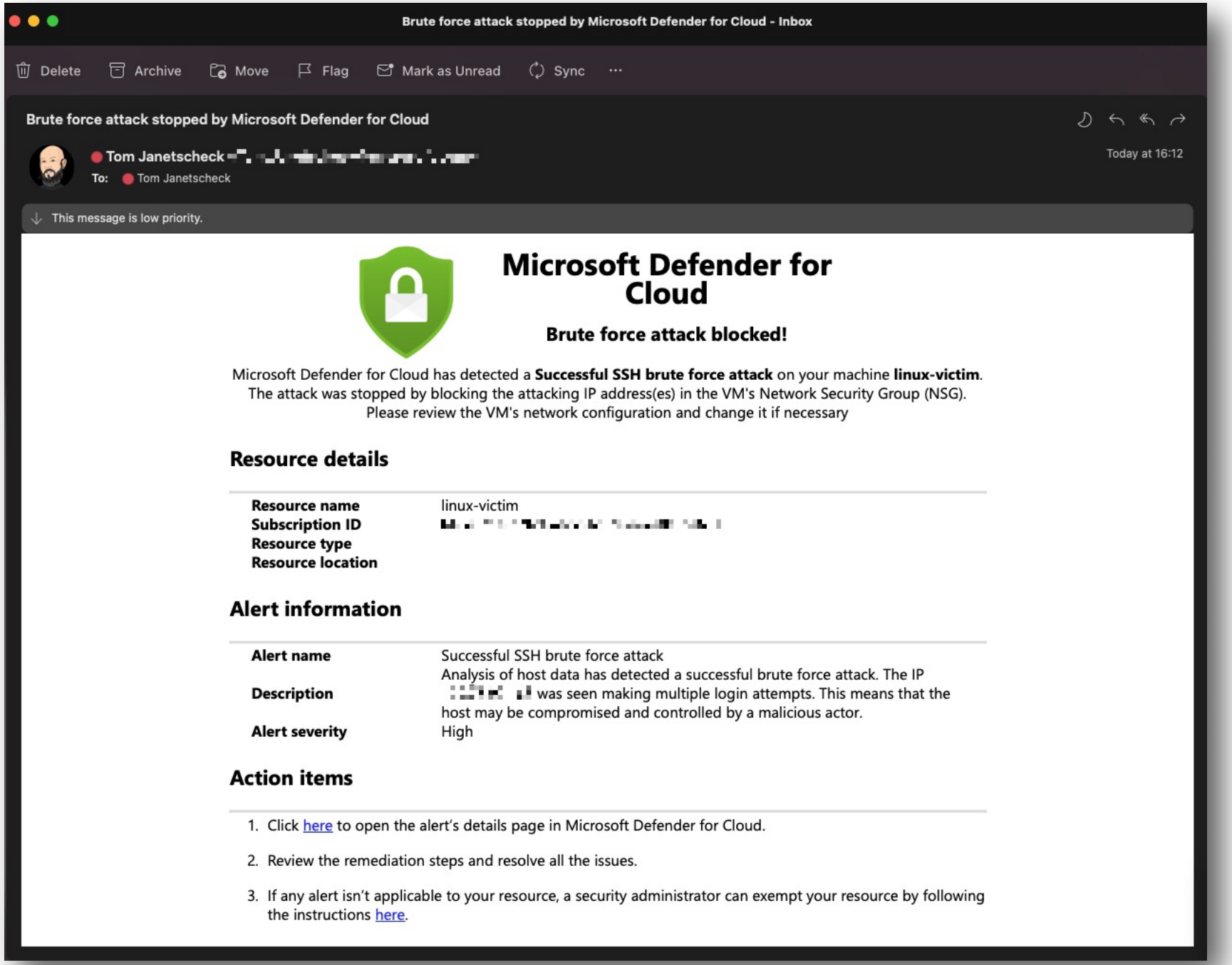
## Invoke REST APIs



# Managed Identity & Role Assignments



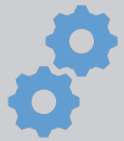




Brute force attack stopped by Microsoft Defender for Cloud - Inbox
Delete
Archive
Move
Flag
Mark as Unread
Sync
Brute force attack stopped by Microsoft Defender for Cloud
Tom Janetscheck
To: Tom Janetscheck
Today at 16:12
This message is low priority.
Microsoft Defender for Cloud
Brute force attack blocked!
Microsoft Defender for Cloud has detected a Successful SSH brute force attack on your machine linux-victim.
The attack was stopped by blocking the attacking IP address(es) in the VM's Network Security Group (NSG).
Please review the VM's network configuration and change it if necessary
Resource details
Resource name linux-victim
Subscription ID
Resource type
Resource location
Alert information
Alert name Successful SSH brute force attack
Description Analysis of host data has detected a successful brute force attack. The IP was seen making multiple login attempts. This means that the host may be compromised and controlled by a malicious actor.
Alert severity High
Action items
1. Click here to open the alert's details page in Microsoft Defender for Cloud.
2. Review the remediation steps and resolve all the issues.
3. If any alert isn't applicable to your resource, a security administrator can exempt your resource by following the instructions here.

Microsoft

# Demo

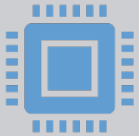
# Automation capabilities - when to use which?



**PowerShell** and **Azure CLI** are good for one-time tasks

pull data, export data, set a configuration,...

**APIs** – high code interfaces, to be used in apps and services



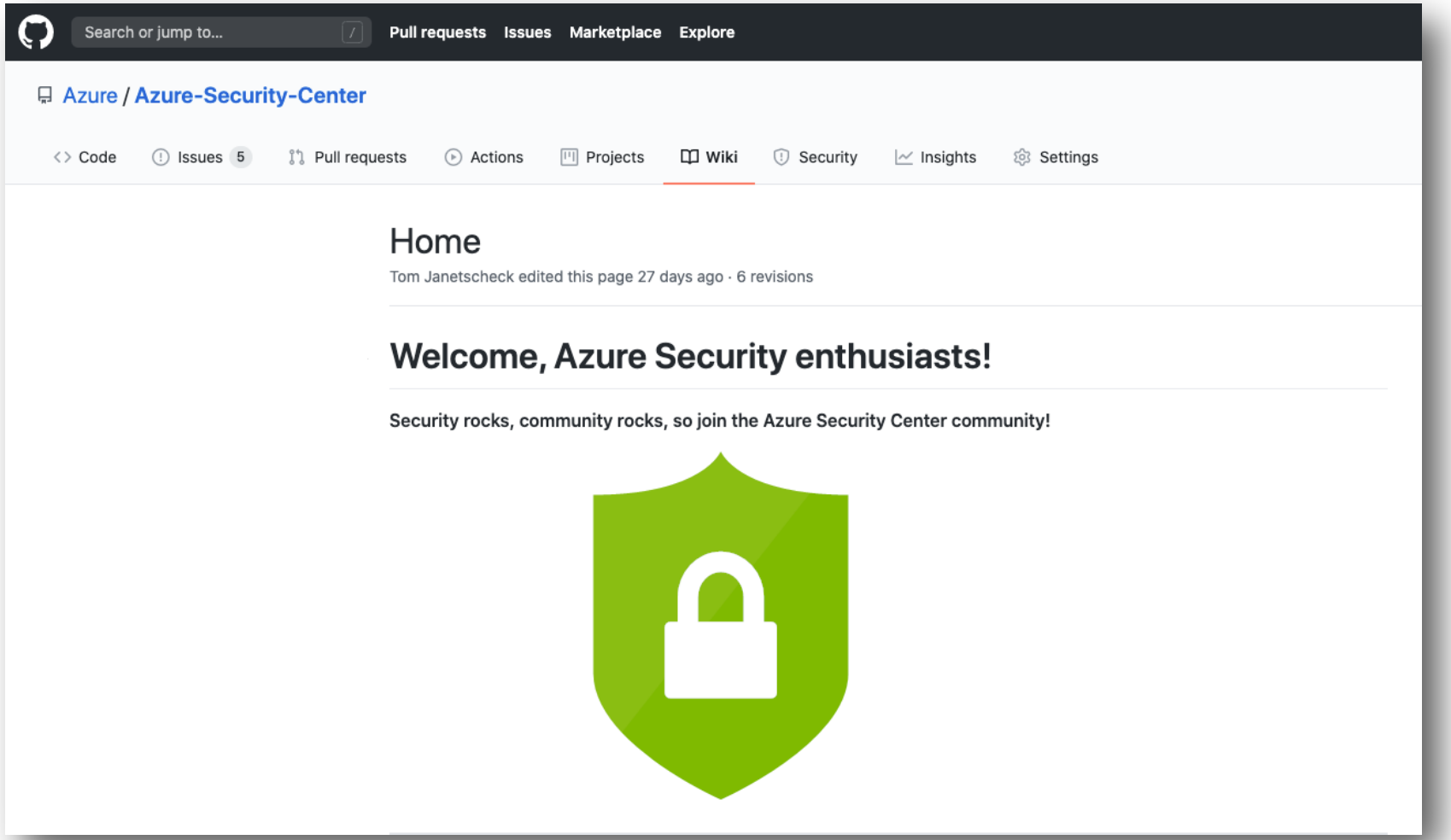
**Logic Apps** - low-code automations for recurring tasks, to be fired regularly, or whenever needed

# Join the Defender for Cloud community

Our [Defender for Cloud GitHub repo] is deeply integrated with the product portal.

Place for publishing tools and automation artifacts, such as Policy Templates, LogicApps, PowerShell scripts, that enable automated response, governance, and remediation at scale.

Visit [https://aka.ms/mdfcgithub] for more details.



# Q&A

Microsoft