



Automate(d) Security with Microsoft Defender for Cloud

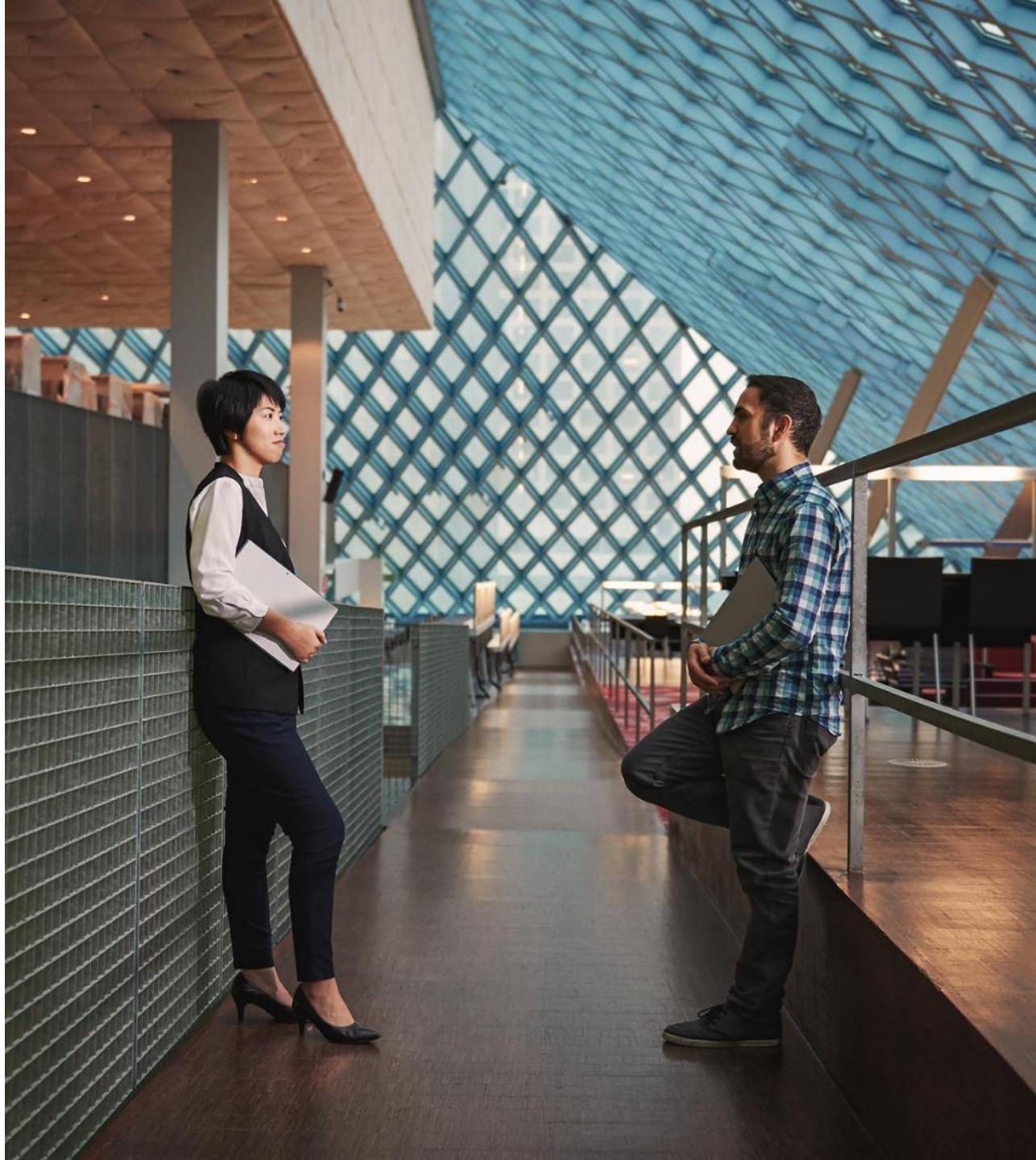
Tom Janetscheck

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

Microsoft Defender for Cloud | Recommendations Showing 4 subscriptions X

Search (Cmd+/) Refresh Download CSV report Open query Guides & Feedback

General

- Overview
- Getting started
- Recommendations **Secure score recommendations**
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Secure score 51% Secure score recommendations All recommendations Azure AWS GCP

Active items Controls 14/15 Recommendations 30/94

Resource health Unhealthy (434) Healthy (222) Not applicable (94)

Search recommendations Recommendation status == None Severity == None Resource type == None Recommendation maturity == None Add filter

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	5.00	+ 9%	Unhealthy	2 of 4 resources	
Secure management ports	8	6.59	+ 2%	Unhealthy	9 of 103 resources	
Remediate vulnerabilities	6	0.93	+ 9%	Unhealthy	120 of 160 resources	
Machines should have vulnerability finding...				Unhealthy	27 of 130 resources	
Machines should have a vulnerability asses...				Unhealthy	73 of 125 resources	
Container registry images should have vuln...				Unhealthy	4 of 4 container registries	
Container images should be deployed fro...				Unhealthy	14 of 24 resources	
Azure Kubernetes Service clusters should h...				Unhealthy	3 of 10 Kubernetes servi...	

Security Alerts

Microsoft Defender for Cloud | Security alerts Showing 4 subscriptions X

Search (Cmd+/) Refresh Change status Open query Suppression rules Security alerts map Sample alerts Alerts workbook Download CSV report Guides & Feedback

General

- ! Overview
- ! Getting started
- ! Recommendations
- ! **Security alerts** (selected)
- ! Inventory
- ! Workbooks
- ! Community
- ! Diagnose and solve problems

Cloud Security

- ! Security posture
- ! Regulatory compliance
- ! Workload protections
- ! Firewall Manager

Management

- ! Environment settings
- ! Security solutions
- ! Workflow automation

12.3K Active alerts **59** Affected resources

Active alerts by severity

High (7.2K) Medium (1.4K) Low (3.7K)

<input type="checkbox"/>	Severity ↑↓	Alert title ↑↓	Affected resource ↑↓	Activity start time (UTC+2) ↑↓	MITRE ATT&CK® tactics	Status ↑↓
<input type="checkbox"/>	High	DDoS Attack detected for Public IP	CyberSecSOC	05/03/22, 05:31 PM	Pre-attack	Active
<input type="checkbox"/>	High	Access from a Tor exit node to a storage...	paysub2022	04/26/22, 01:14 AM	Pre-attack	Active
<input type="checkbox"/>	High	Suspicious process executed	Workstation20	04/26/22, 12:30 AM	Credential Access	Active
<input type="checkbox"/>	High	Security incident detected	Workstation20	04/26/22, 12:27 AM		Active
<input type="checkbox"/>	High	Possible attempt to steal credentials	attackworkstation	04/22/22, 11:52 AM	Credential Access	Active
<input type="checkbox"/>	High	Possible attempt to steal credentials	attackworkstation	04/22/22, 11:52 AM	Credential Access	Active
<input type="checkbox"/>	High	Possible attempt to steal credentials	attackworkstation	04/22/22, 11:52 AM	Credential Access	Active
<input type="checkbox"/>	High	Possible attempt to steal credentials	attackworkstation	04/22/22, 11:52 AM	Credential Access	Active
<input type="checkbox"/>	High	Possible attempt to steal credentials	attackworkstation	04/22/22, 11:52 AM	Credential Access	Active

Search by ID, title, or affected resource Subscription == ASC DEMO, ASC Multi-Cloud Demo, ... Status == Active Severity == Low, Medium, High Add filter No grouping

Security Alerts

Security alert ⚡ ...

Access from a Tor exit node to a storage blob container

High Severity Active Status 04/26/22, ... Activity time

Alert description [Copy alert JSON](#)

An IP that is a known Tor exit node accessed Storage container 'files' in storage account . The actor's access was authenticated using Shared access signature (SAS). Threat actors use Tor to make it difficult to trace the activity back to them. Authenticated access from a Tor exit node is a likely indication that a threat actor is trying to hide their identity. Actions performed include: 'GetBlob'.

Affected resource

 Storage account

 CyberSecSOC Subscription

MITRE ATT&CK® tactics ⓘ

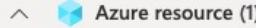
- Pre-attack



Alert details [Take action](#)

Azure AD user N/A (Azure AD user authentication was not used)	Authentication type Shared access signature (SAS)	Container files
User agent Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0 See more	Investigation steps • Check if this actor is legitimate. Examine the authen... See more	Potential causes This alert indicates that this account has been access... See more
Api type Blob	Operations types GetBlob	Size of extracted data 11.93 KB
Client location  Germany	Service type Azure Blobs	Detected by  Microsoft

Related entities

 Azure resource (1)

Resource ID	Subscription ID
/subscriptions/  /providers/Mi...	

 Blob container (1)

Name	Storage resource	URL
files		/subscriptions/  /storag...

Security Alerts

Security alert

Access from a Tor exit node to a storage blob container

High Severity **Active Status** **04/26/22, ... Activity time**

Alert description [Copy alert JSON](#)

An IP that is a known Tor exit node accessed Storage container 'files' in storage account . The actor's access was authenticated using Shared access signature (SAS). Threat actors use Tor to make it difficult to trace the activity back to them. Authenticated access from a Tor exit node is a likely indication that a threat actor is trying to hide their identity. Actions performed include: 'GetBlob'.

Affected resource

Storage account CyberSecSOC Subscription

MITRE ATT&CK® tactics

- Pre-attack

Was this useful? Yes No

Alert details **Take action**

Inspect resource context
Start with examining the resource logs around the time of the alert. [Open logs](#)

Mitigate the threat

- Revoke all credentials that may be compromised and ensure that they're only shared with authorized users.
- Ensure that storage access tokens are stored in a secured location such as Azure Key Vault. Avoid storing or sharing storage access tokens in source code, documentation, and email.

You have 0 more alerts on the affected resource. [View all >>](#)

Prevent future attacks
Your top 3 active security recommendations on :

Medium Storage account should use a private link connection
Medium Storage accounts should restrict network access using virtual network rules
Medium Storage account public access should be disallowed

Solving security recommendations can prevent future attacks by reducing attack surface. [View all 8 recommendations >>](#)

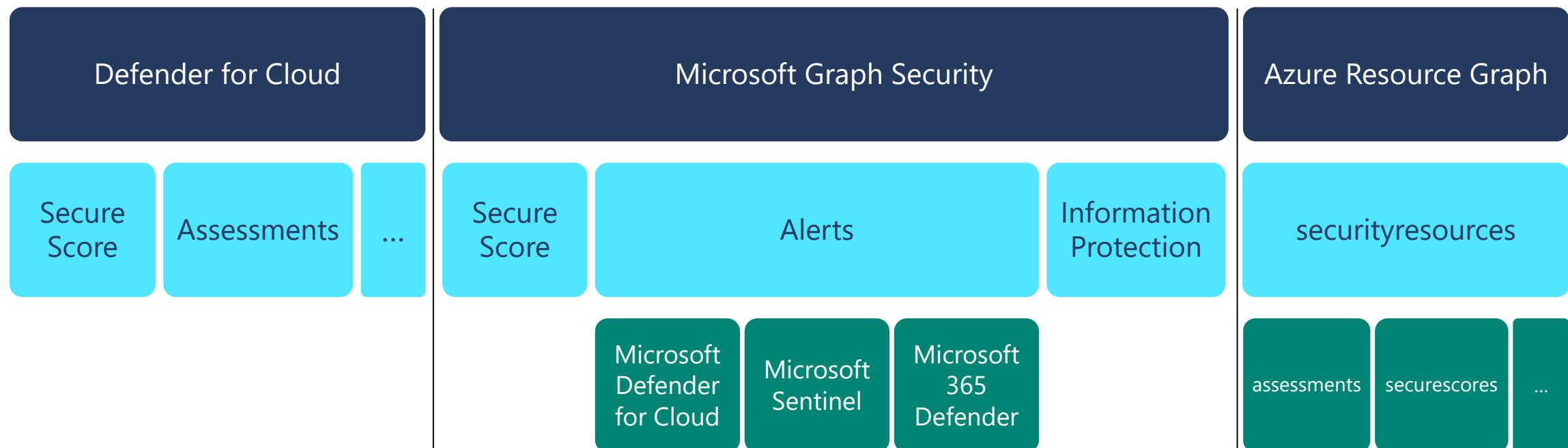
Trigger automated response
Trigger logic app as an automated response to this security alert. You can get suggested responses in [the ASC Community GitHub Repo](#). [Trigger logic app](#)

Suppress similar alerts

Configure email notification settings

API options

RESTful APIs



REST APIs

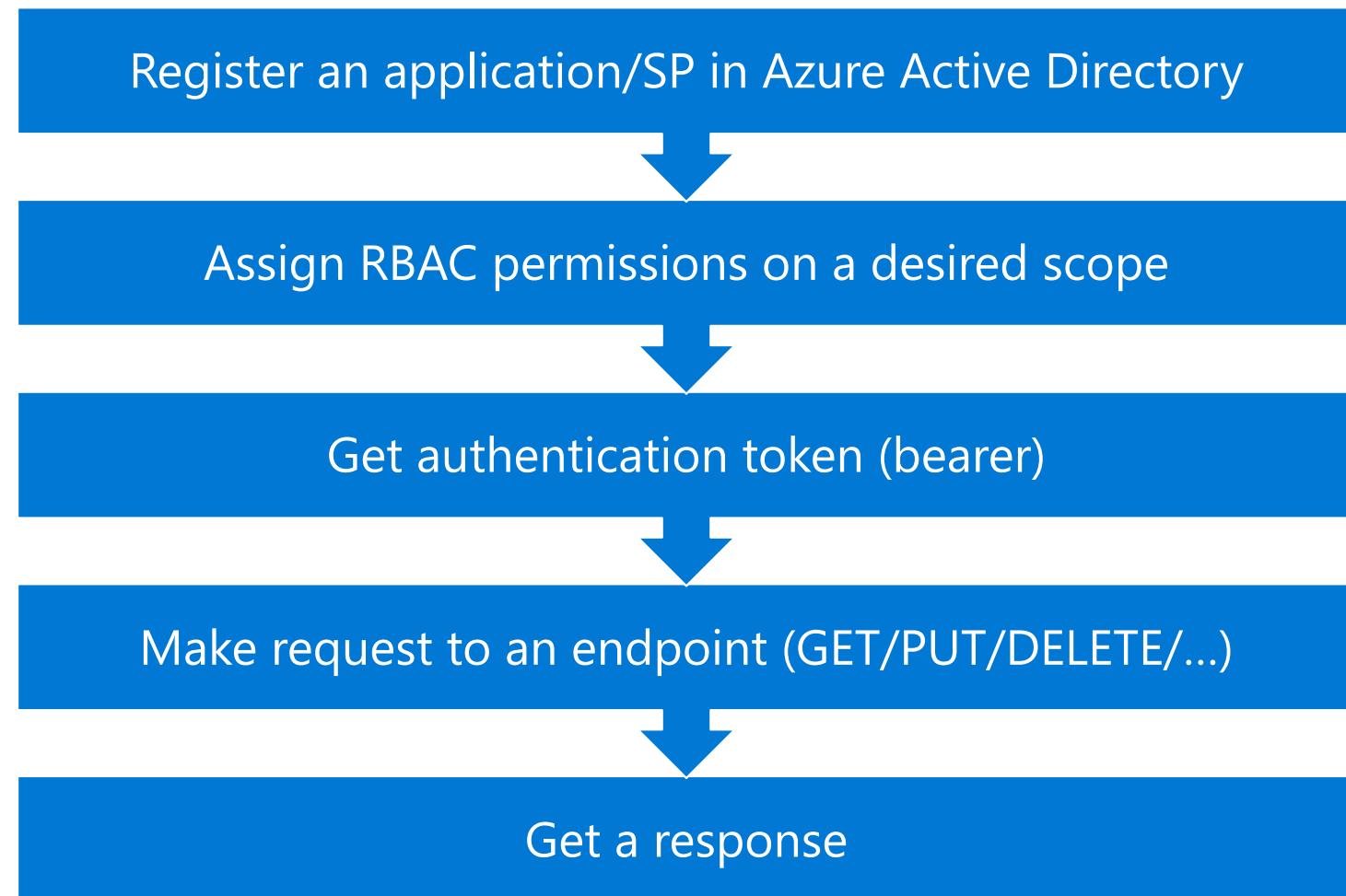
- Defender for Cloud
 - Provides a variety of [operation groups](#)
- Microsoft Security Graph
 - [Consolidated API](#) for security products
- Azure Resource Graph
 - Ability to query and access data [from the graph](#)

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





Demo

Continuous export

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

Settings | Continuous export 

ASC_Demo

Search (Ctrl+ /) Save

Settings

- Azure Defender plans
- Auto provisioning
- Email notifications
- Threat detection
- Workflow automation
- Continuous export**
- Cloud connectors

Continuous export

Configure streaming export setting of Security Center data to multiple export targets. Exporting Security Center's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer. [Learn More >](#)

Event hub Log Analytics workspace

Export enabled **On** Off

Exported data types

Security recommendations Vulnerability assessment findings ...
 Secure score (Preview) Overall score,Control score
 Security alerts High
 Regulatory compliance (Preview) ISO-27001

Include security findings Yes

Controls All controls selected

Export frequency

Streaming updates
 Snapshots (Preview)

Export configuration

Resource group * Select resource group

Export target

Subscription * ASC DEMO
Event Hub namespace * Select Event Hub namespace
Event Hub name * Select Event Hub
Event hub policy name * Select Event Hub policy name

Workflow automation

Automatically react on

- Security alerts
- Recommendations
- Regulatory compliance status changes

Security Center | Workflow automation

Showing 41 subscriptions

Search (Ctrl+ /)

Add workflow automation Refresh Enable Disable Delete Learn more

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Community

Cloud Security

- Secure Score
- Regulatory compliance
- Azure Defender

Management

- Pricing & settings
- Security policy
- Security solutions
- Workflow automation
- Coverage
- Multi cloud connectors

Name Status Scope Trigger Type Logic App

Name	Status	Scope	Trigger Type	Logic App
TestAlertsTe	Enabled	ASC DEMO	Security Center alert	Temp
NewTemplate	Enabled	ASC DEMO	Security Center alert	k(L)
NewD	Enabled	ASC DEMO	Security Center recom...	NewDesign
Auto	Enabled	ASC DEMO	Security Center alert	LA(Logic)
TestRecs	Enabled	ASC DEMO	Security Center alert	Recs
Testrts	Enabled	ASC DEMO	Security Center alert	TestA
TestWAS	Enabled	ASC DEMO	Security Center recom...	ForP
Test6	Enabled	ASC DEMO	Security Center recom...	triggerable
UITETS	Enabled	ASC DEMO	Security Center recom...	ManualT
PolicyAS	Enabled	ASC DEMO	Security Center alert	PolicyLogicA
Test	Enabled	ASC DEMO	Security Center alert	mTest
est1	Enabled	ASC DEMO	Security Center alert	Test2(Ld)
Remove-M	Enabled	DS-Threat	Security Center alert	Mal
Delete-Blob	Enabled	DS-Threat	Security Center alert	Ask:
Rec	Disabled	ASC DEMO	Security Center recom...	yo



Logic Apps

Let's bring it all together

Logic Apps

Builtin Defender for Cloud triggers



When an Azure Security Center Alert is created or triggered
Security Center Alert



When an Azure Security Center Recommendation is created or triggered
Security Center Recommendation



When a Security Center Regulatory Compliance Assessment is created or triggered (preview)
Security Center Regulatory Compliance

Logic Apps

Native connectors to Microsoft and 3rd party services

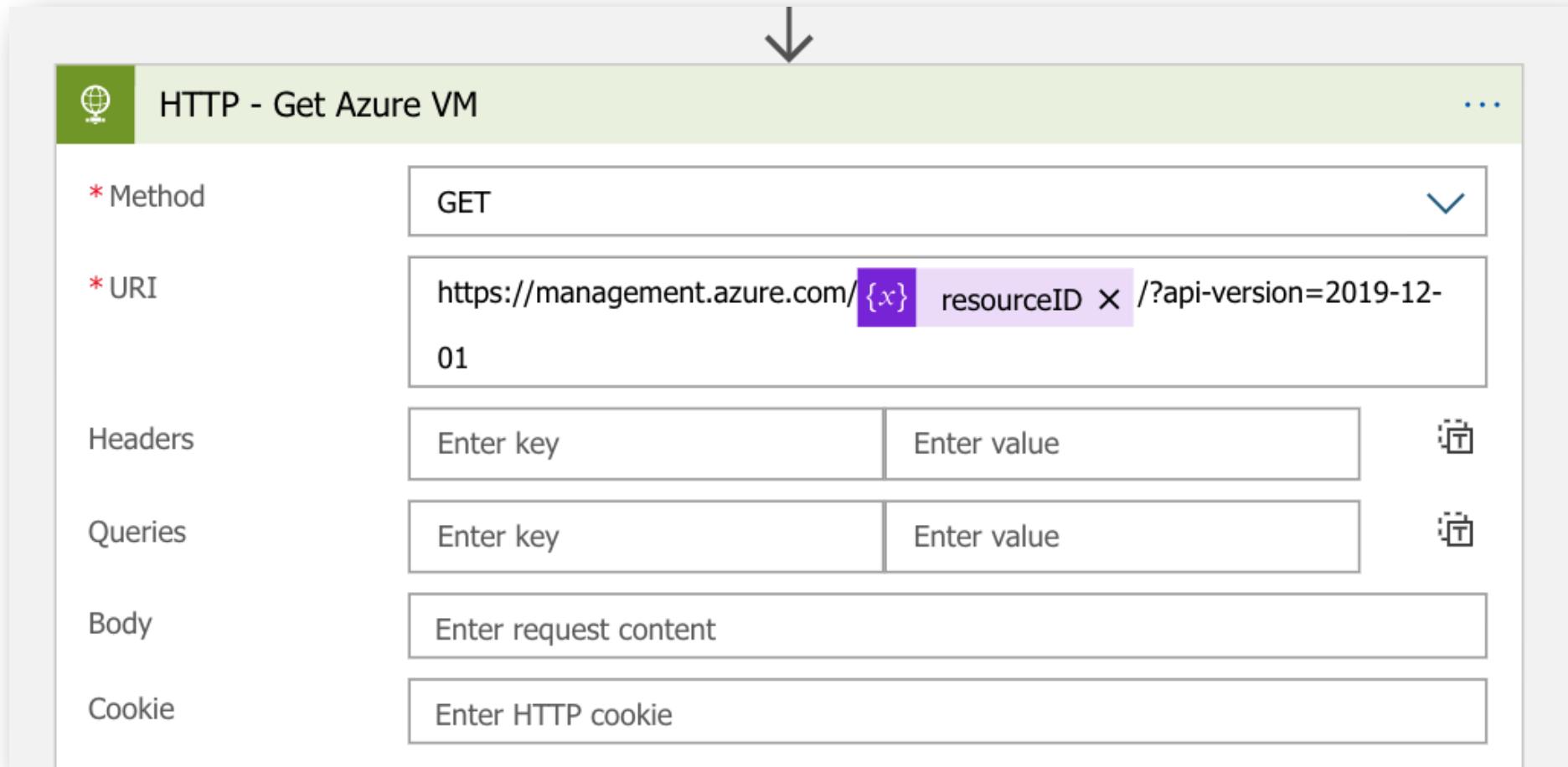
For You All Built-in Standard Enterprise Custom

Recent Clear

 Variables	 HTTP	 Security Center Alert	 ServiceNow	 JIRA	 Control	 Data Operations
--	---	---	---	---	--	--

Logic Apps

Invoke REST APIs



The screenshot shows the Logic Apps designer interface with a single action step selected. The action is titled "HTTP - Get Azure VM". The configuration fields are as follows:

- * Method: GET
- * URI: `https://management.azure.com/{x}/resourceID/?api-version=2019-12-01`
- Headers: Enter key | Enter value
- Queries: Enter key | Enter value
- Body: Enter request content
- Cookie: Enter HTTP cookie

A large downward arrow is positioned above the action step, indicating the flow of the logic app.

Managed Identity & Role Assignments

The screenshot shows two overlapping Azure interface windows. The top window is titled 'LA-TEST-123 | Identity' and displays the 'System assigned' managed identity configuration. It includes fields for 'Status' (set to 'On'), 'Object (principal) ID' (showing 'aafb4ce3-f317-4d25-bcc7-d9f8d3ca355b'), and a 'Permissions' section with a 'Azure role assignments' button. A large blue arrow points downwards from this window towards the second window. The bottom window is titled 'Azure role assignments' and lists role assignments for the 'BuildEnv' subscription. It shows two entries: one for 'Reader' role assigned to 'BuildEnv' with 'None' condition, and another for 'Security Admin' role assigned to 'BuildEnv' with 'None' condition.

Home > LA-TEST-123 | Identity

LA-TEST-123 | Identity

System assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code. [Learn more about Managed identities](#).

Status: On

Object (principal) ID: aafb4ce3-f317-4d25-bcc7-d9f8d3ca355b

Permissions: Azure role assignments

This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. [Learn more](#)

Home > LA-TEST-123

Azure role assignments

+ Add role assignment (Preview) Refresh

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *	Role	Resource Name	Resource Type	Assigned To	Condition
BuildEnv	Reader	BuildEnv	Subscription	LA-TEST-123	None
BuildEnv	Security Admin	BuildEnv	Subscription	LA-TEST-123	None

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 <[REDACTED]>

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	[REDACTED]
Resource type	[REDACTED]
Resource location	[REDACTED]

Alert information

Alert name	Successful SSH brute force attack
Description	Analysis of host data has detected a successful brute force attack. The IP [REDACTED] 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](#).



Demo

Automation capabilities - when to use which?

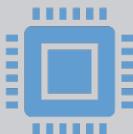


PowerShell and **Azure CLI** are good for one-time tasks

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



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



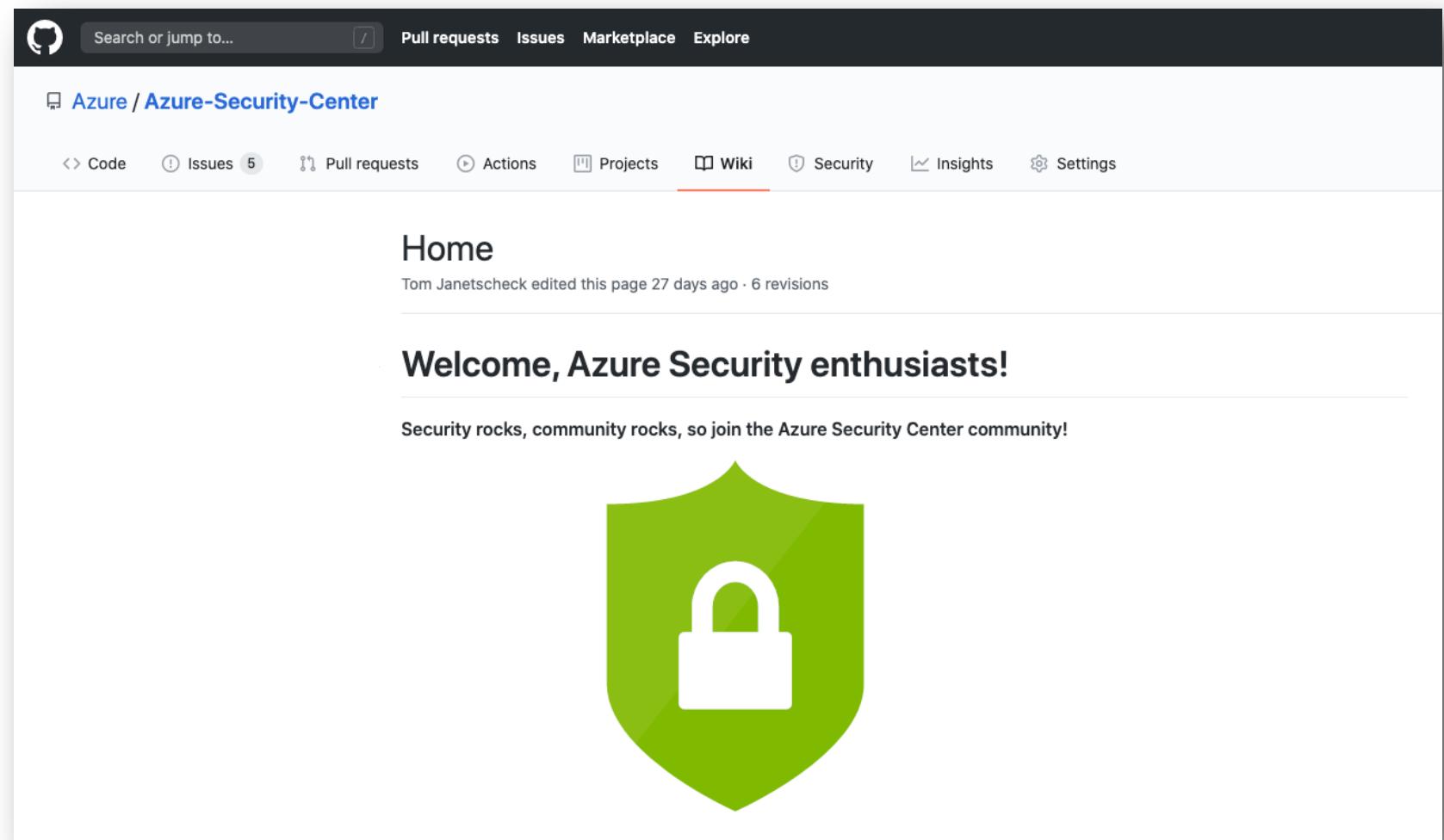
Logic Apps - low-code automations for recurring tasks, to be fired regularly, or whenever needed

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.



The screenshot shows the GitHub interface for the 'Azure / Azure-Security-Center' repository. The top navigation bar includes links for Search or jump to..., Pull requests, Issues, Marketplace, and Explore. Below the bar, the repository name 'Azure / Azure-Security-Center' is displayed. The main navigation menu includes Code, Issues (5), Pull requests, Actions, Projects, Wiki, Security, Insights, and Settings. The 'Home' section features a message from Tom Janetscheck edited 27 days ago with 6 revisions. It welcomes 'Welcome, Azure Security enthusiasts!' and encourages joining the Azure Security Center community. A large green shield icon with a white padlock is prominently displayed.

Q&A





© Copyright Microsoft Corporation. All rights reserved.