#GlobalAzureTO

Azure Defender in Action!

Maxime Coquerel - MVP Azure

MVP Microsoft® Most Valuable Professional

#GlobalAzure

#GlobalAzureTO

Thanks to our Global and Local Sponsors

Microsoft

ObjectSharp
a CentriLogic company

Speaker

Microsoft® MVP Most Valuable Professional

Maxime Coquerel

Director Cloud Security Architecture

Email : max.coquerel@live.fr

Blog : zigmax.net (since 2012)

Github : https://github.com/zigmax

Twitter : @zig_max

Open Source Contributor (Kubernetes / VSCode)

Disclaimer

“Any views or opinions expressed in this presentation are those of the presenter and not necessarily represent the view and opinions of my employer, its ownership, management or its employees.“

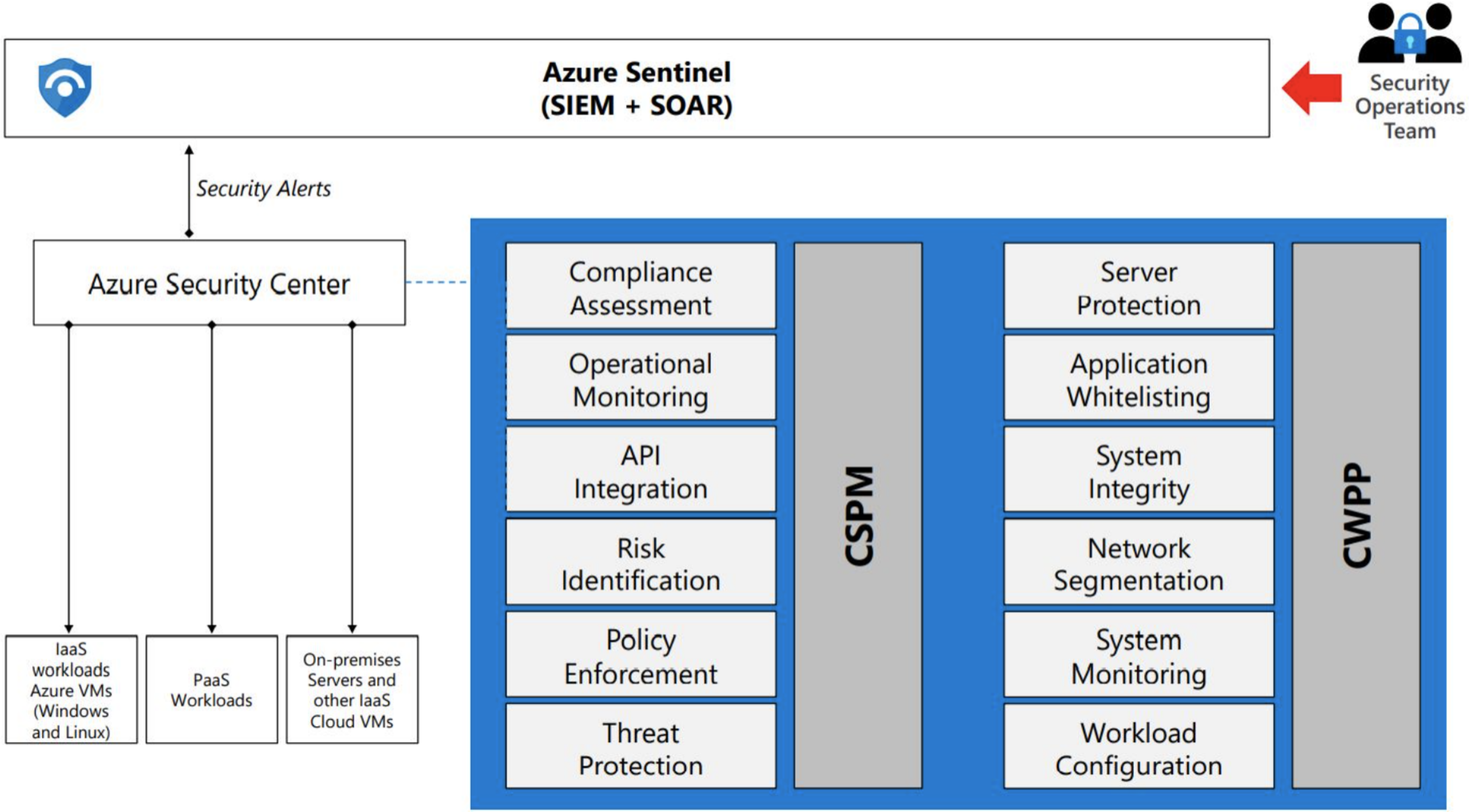
Session Agenda / Goal

- Azure Security Overview
- Azure Defender
- Examples of Azure Defender Alerts
- Suspicious incoming RDP network activity
- Export - Alerts to SIEM
- Alert - Notification
- Alert - Simulation
- Azure Graph
- Alert Automation
- Azure Security Center - Multi Cloud

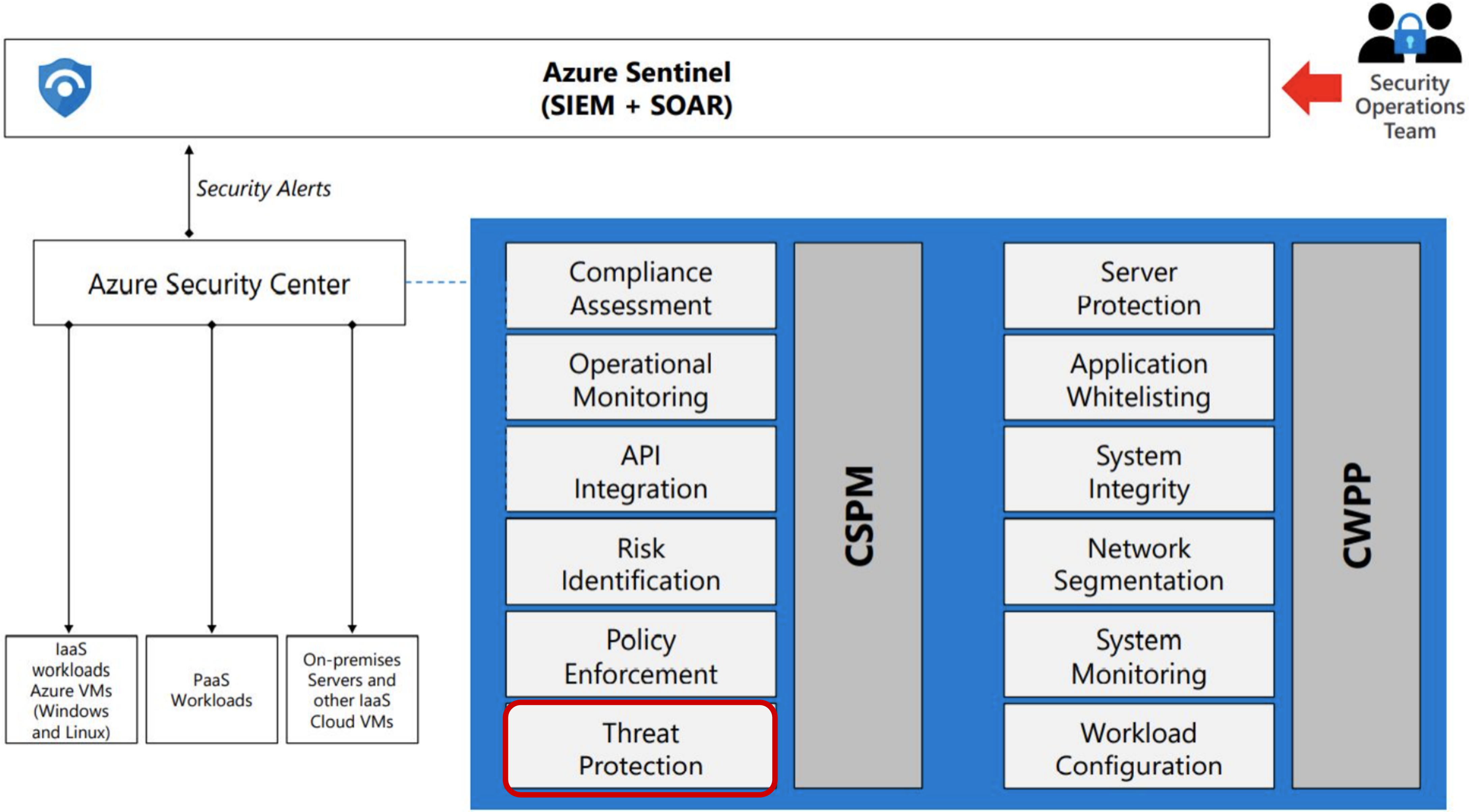
#GlobalAzureTO

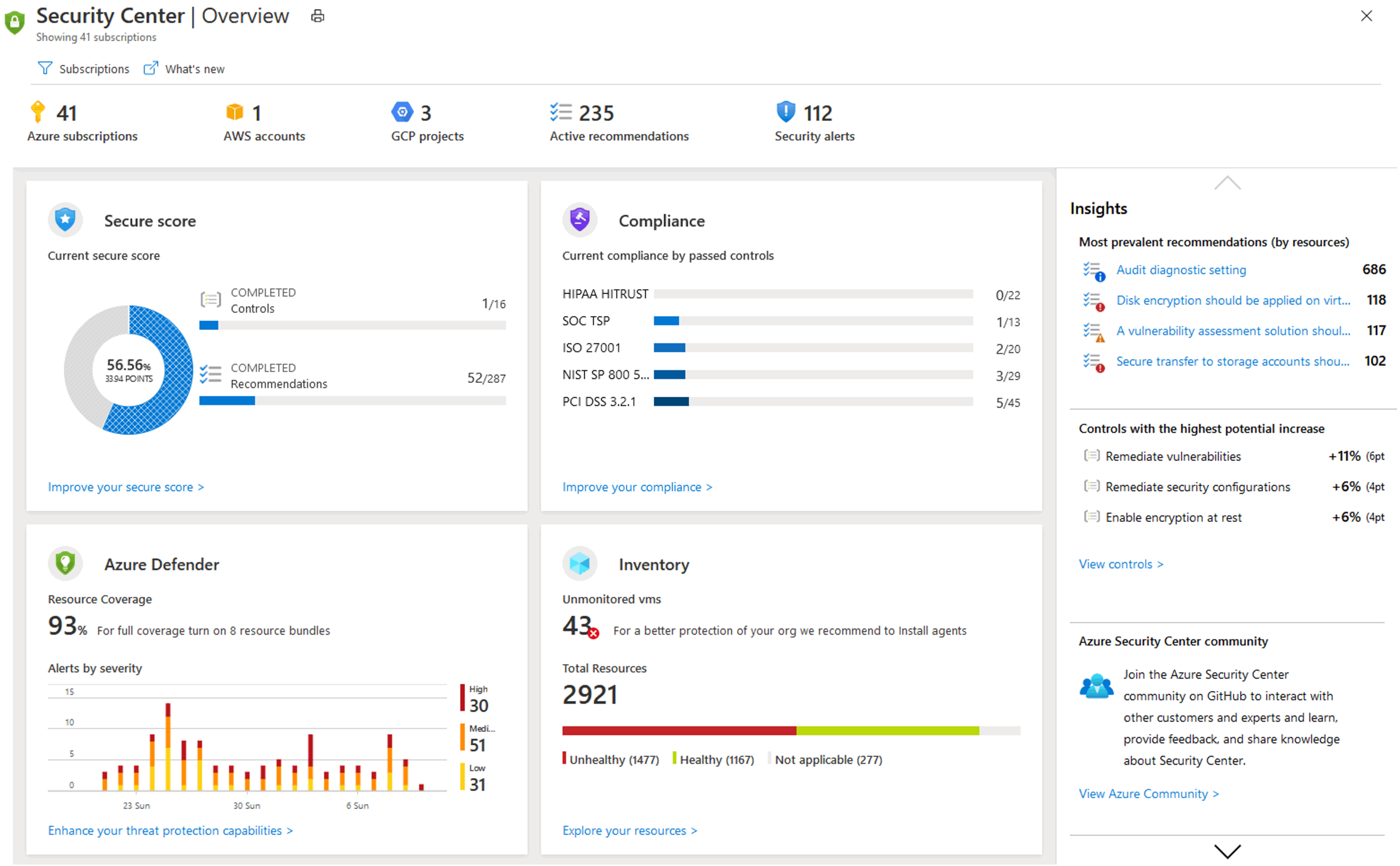
Azure Security Overview

Azure Security Overview



Azure Security Overview





Security Center | Overview

Showing 41 subscriptions

Subscriptions What's new

41 Azure subscriptions

1 AWS accounts

3 GCP projects

235 Active recommendations

112 Security alerts

Secure score

Current secure score

56.56% 33.94 POINTS

COMPLETED Controls 1/16

COMPLETED Recommendations 52/287

Improve your secure score >

Compliance

Current compliance by passed controls

HIPAA HITRUST	0/22
SOC TSP	1/13
ISO 27001	2/20
NIST SP 800 5...	3/29
PCI DSS 3.2.1	5/45

Improve your compliance >

Azure Defender

Resource Coverage

93% For full coverage turn on 8 resource bundles

Alerts by severity

Enhance your threat protection capabilities >

Inventory

Unmonitored vms

43 For a better protection of your org we recommend to Install agents

Total Resources

2921

Unhealthy (1477) Healthy (1167) Not applicable (277)

Explore your resources >

Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	686
Disk encryption should be applied on virt...	118
A vulnerability assessment solution shoul...	117
Secure transfer to storage accounts shou...	102

Controls with the highest potential increase

Remediate vulnerabilities	+11% (6pt
Remediate security configurations	+6% (4pt
Enable encryption at rest	+6% (4pt

View controls >

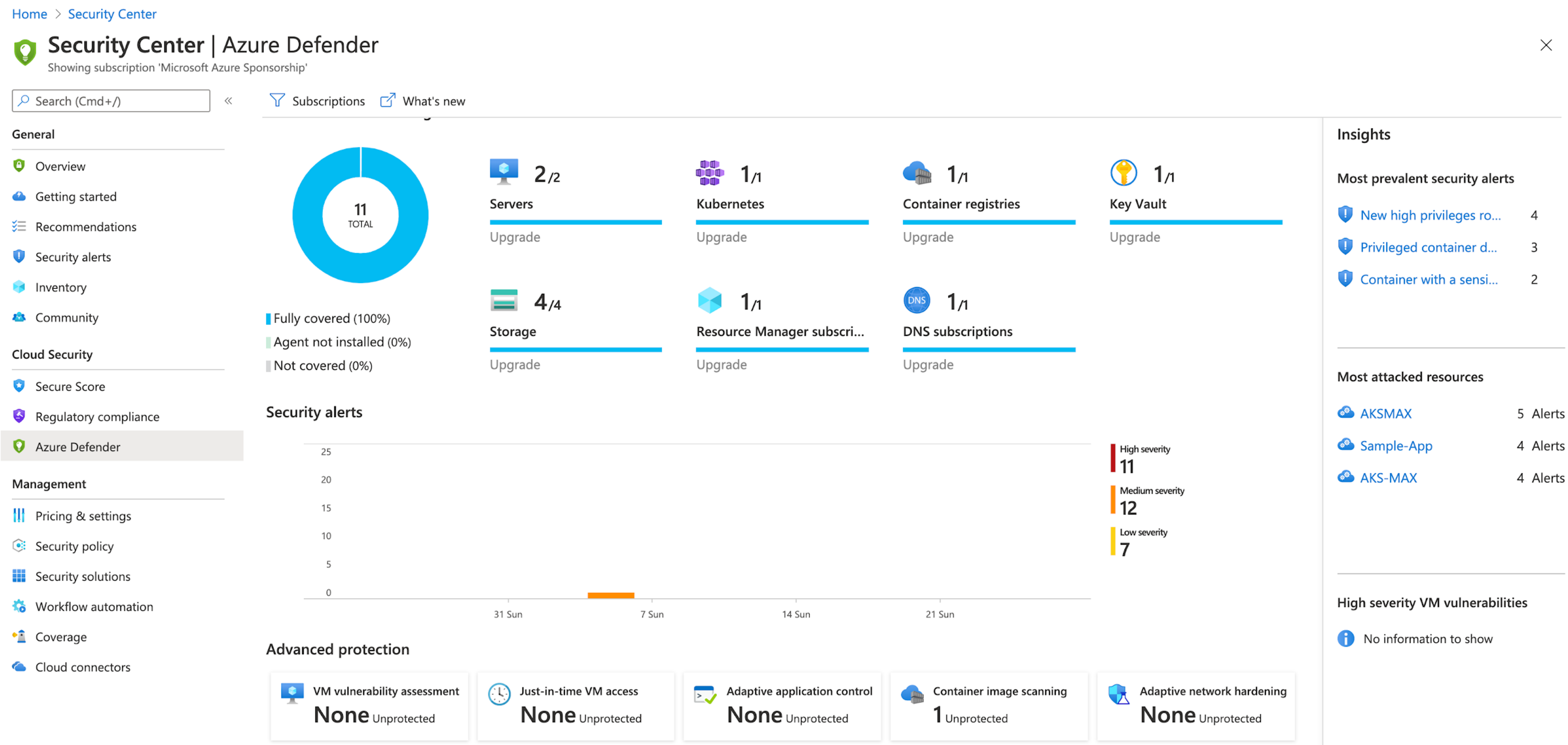
Azure Security Center community

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center.

View Azure Community >

#GlobalAzureTO

Azure Defender



Home > Security Center

Security Center | Azure Defender

Showing subscription 'Microsoft Azure Sponsorship'

Search (Cmd+/)

Subscriptions | What's new

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
- Cloud connectors

11 TOTAL

- Fully covered (100%)
- Agent not installed (0%)
- Not covered (0%)

Resource	Covered	Action
Servers	2/2	Upgrade
Kubernetes	1/1	Upgrade
Container registries	1/1	Upgrade
Key Vault	1/1	Upgrade
Storage	4/4	Upgrade
Resource Manager subscri...	1/1	Upgrade
DNS subscriptions	1/1	Upgrade

Security alerts

Severity	Count
High severity	11
Medium severity	12
Low severity	7

Advanced protection

Feature	Status
VM vulnerability assessment	None Unprotected
Just-in-time VM access	None Unprotected
Adaptive application control	None Unprotected
Container image scanning	1 Unprotected
Adaptive network hardening	None Unprotected

Insights

Most prevalent security alerts

Alert	Count
New high privileges ro...	4
Privileged container d...	3
Container with a sensi...	2

Most attacked resources

Resource	Alerts
AKSMAX	5 Alerts
Sample-App	4 Alerts
AKS-MAX	4 Alerts

High severity VM vulnerabilities

No information to show

#GlobalAzureTO

Examples of Azure Defender Alerts

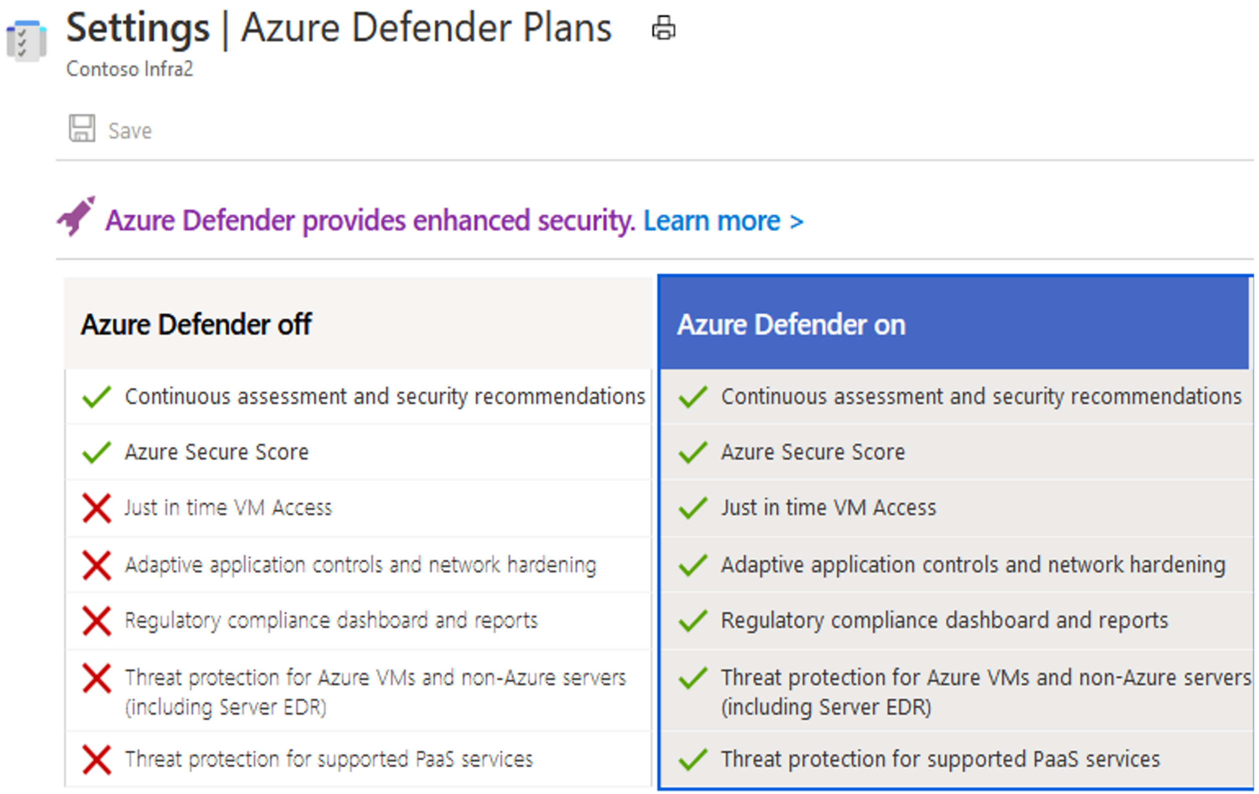
Examples of Azure Defender Alerts

Alert (alert type)	Description	MITRE tactics	Severity
Alert for containers - Azure Kubernetes Service clusters			
Alert for Azure Storage			
Alert for Azure Key Vault			

https://docs.microsoft.com/en-us/azure/security-center/alerts-reference

Alert (alert type)	Description	MITRE tactics	Severity
Alert for containers - Azure Kubernetes Service clusters			
Digital currency mining container detected	Kubernetes audit log analysis detected a container that has an image associated with a digital currency mining tool	Execution	High
Alert for Azure Storage			
Anonymous access to a storage account (Storage.Blob_AnonymousAccessAnomaly)	Indicates that there's a change in the access pattern to a storage account. For instance, the account has been accessed anonymously (without any authentication), which is unexpected compared to the recent access pattern on this account. A potential cause is that an attacker has exploited public read access to a container that holds blob storage. Applies to: Azure Blob Storage	Exploitation	High
Alert for Azure Key Vault			
Access from a TOR exit node to a key vault KV_TORAccess	A key vault has been accessed from a known TOR exit node. This could be an indication that a threat actor has accessed the key vault and is using the TOR network to hide their source location. We recommend further investigations.	Credential Access	Medium

https://docs.microsoft.com/en-us/azure/security-center/alerts-reference



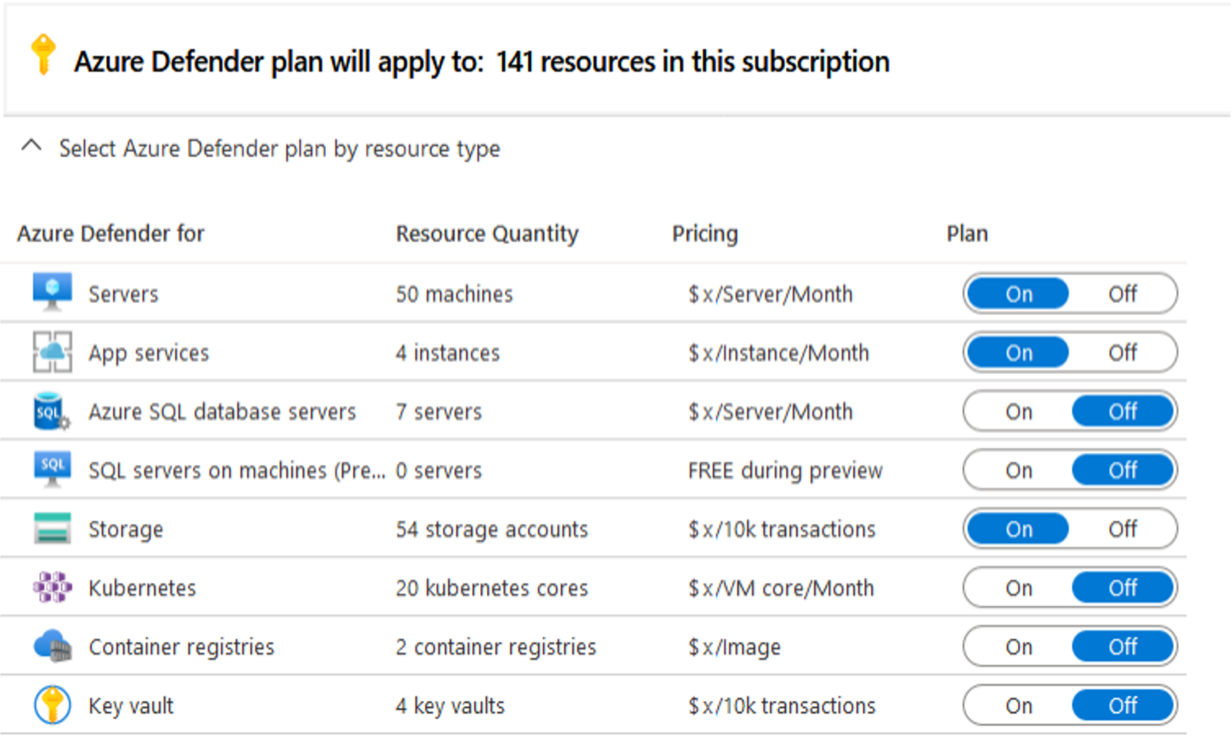
Settings | Azure Defender Plans

Contoso Infra2

Save

Azure Defender provides enhanced security. Learn more >

Azure Defender off	Azure Defender on
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Azure Secure Score	✓ Azure Secure Score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services



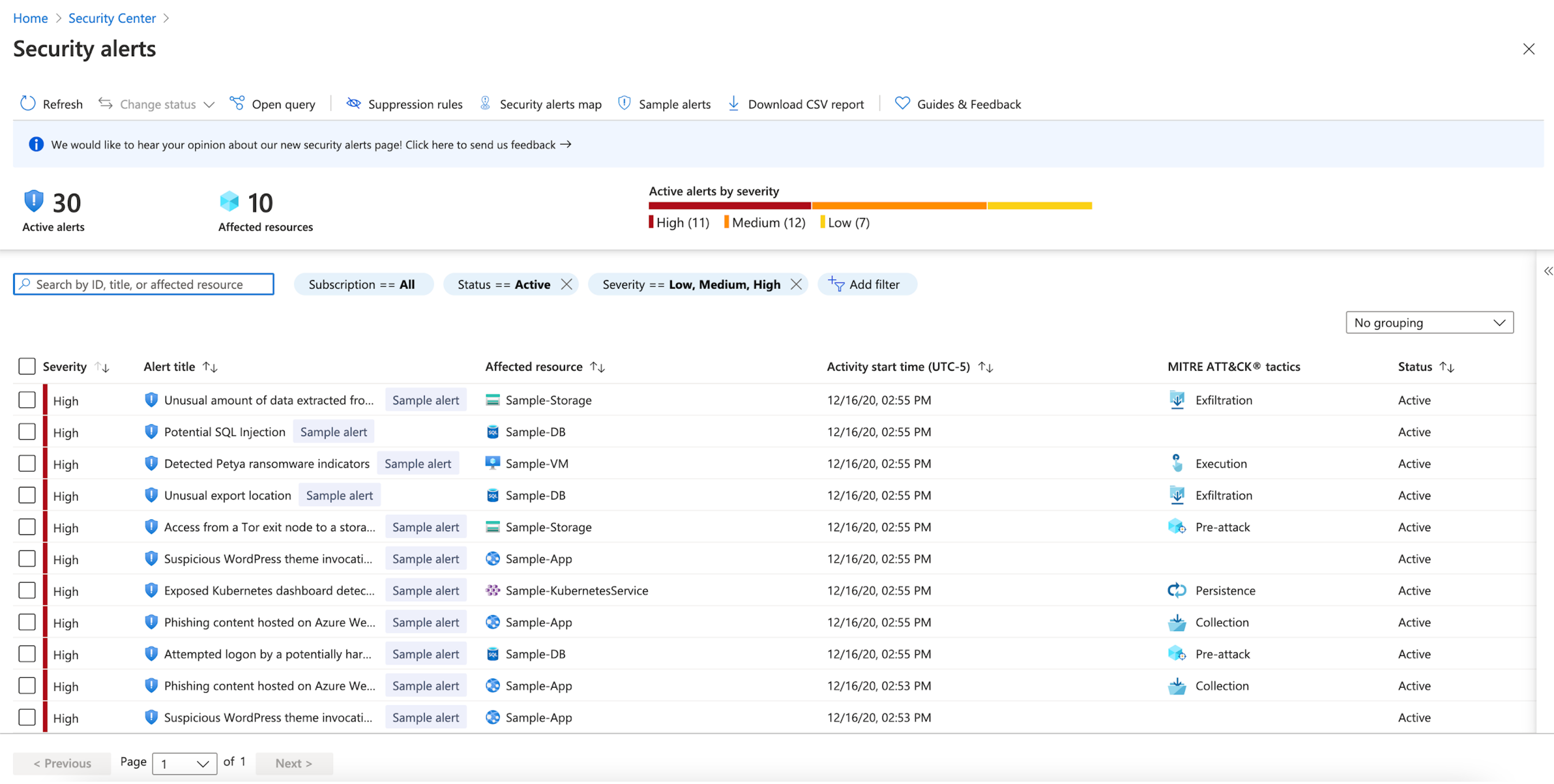
Azure Defender plan will apply to: 141 resources in this subscription

Select Azure Defender plan by resource type

Azure Defender for	Resource Quantity	Pricing	Plan
Servers	50 machines	$x/Server/Month	[✓ On] Off
App services	4 instances	$x/Instance/Month	[✓ On] Off
Azure SQL database servers	7 servers	$x/Server/Month	On [✓ Off]
SQL servers on machines (Pre...	0 servers	FREE during preview	On [✓ Off]
Storage	54 storage accounts	$x/10k transactions	[✓ On] Off
Kubernetes	20 kubernetes cores	$x/VM core/Month	On [✓ Off]
Container registries	2 container registries	$x/Image	On [✓ Off]
Key vault	4 key vaults	$x/10k transactions	On [✓ Off]

- Azure Defender for servers
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL
- Azure Defender for Kubernetes

- Azure Defender for container registries
- Azure Defender for Key Vault
- Azure Defender for Resource Manager
- Azure Defender for DNS



Security alerts

We would like to hear your opinion about our new security alerts page! Click here to send us feedback →

30 Active alerts

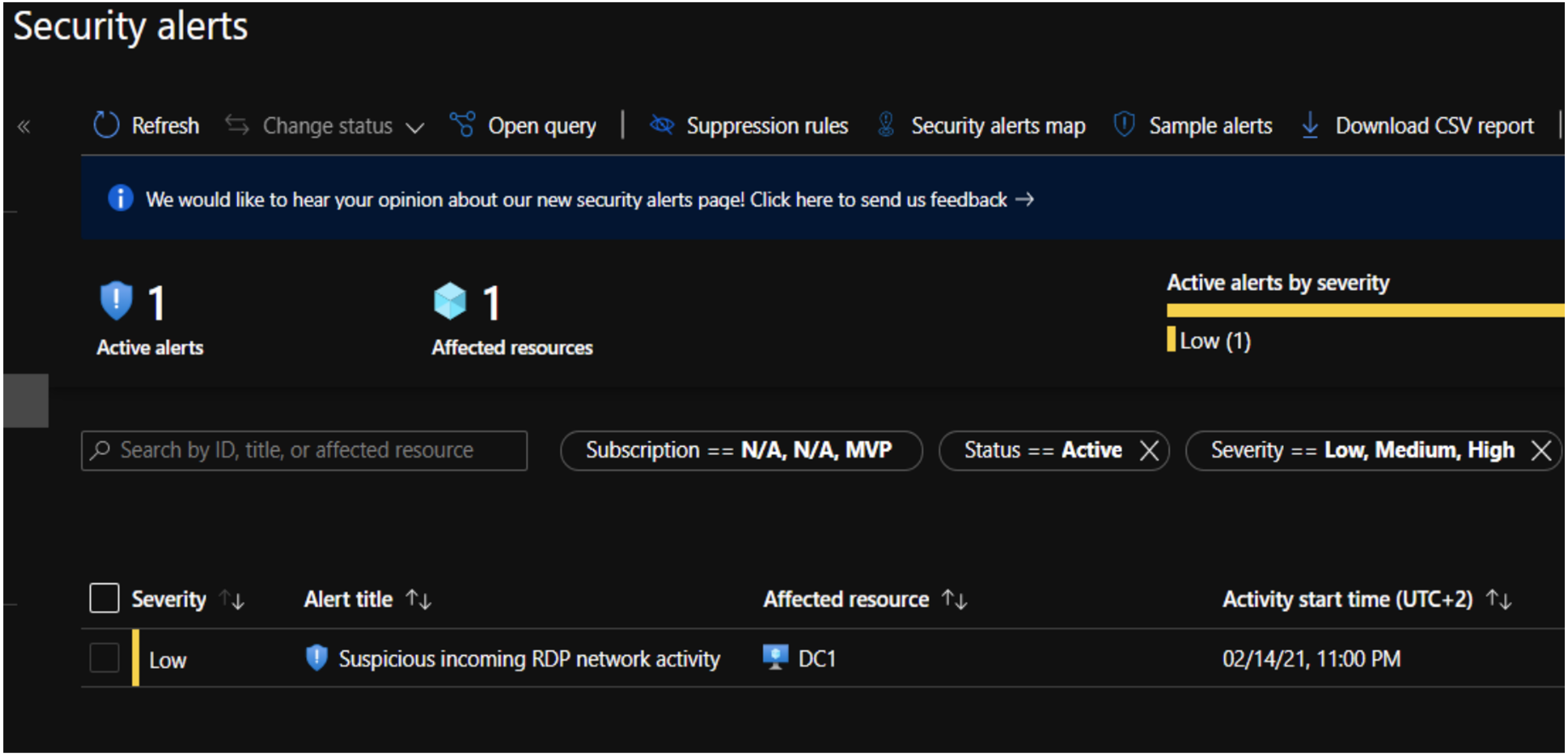
10 Affected resources

Active alerts by severity

High (11) Medium (12) Low (7)

□	Severity	Alert title	Affected resource	Activity start time (UTC-5)	MITRE ATT&CK® tactics	Status
□	High	Unusual amount of data extracted fro... Sample alert	Sample-Storage	12/16/20, 02:55 PM	Exfiltration	Active
□	High	Potential SQL Injection Sample alert	Sample-DB	12/16/20, 02:55 PM		Active
□	High	Detected Petya ransomware indicators Sample alert	Sample-VM	12/16/20, 02:55 PM	Execution	Active
□	High	Unusual export location Sample alert	Sample-DB	12/16/20, 02:55 PM	Exfiltration	Active
□	High	Access from a Tor exit node to a stora... Sample alert	Sample-Storage	12/16/20, 02:55 PM	Pre-attack	Active
□	High	Suspicious WordPress theme invocati... Sample alert	Sample-App	12/16/20, 02:55 PM		Active
□	High	Exposed Kubernetes dashboard detec... Sample alert	Sample-KubernetesService	12/16/20, 02:55 PM	Persistence	Active
□	High	Phishing content hosted on Azure We... Sample alert	Sample-App	12/16/20, 02:55 PM	Collection	Active
□	High	Attempted logon by a potentially har... Sample alert	Sample-DB	12/16/20, 02:55 PM	Pre-attack	Active
□	High	Phishing content hosted on Azure We... Sample alert	Sample-App	12/16/20, 02:53 PM	Collection	Active
□	High	Suspicious WordPress theme invocati... Sample alert	Sample-App	12/16/20, 02:53 PM		Active

Suspicious incoming RDP network activity



Security alerts

We would like to hear your opinion about our new security alerts page! Click here to send us feedback →

1 Active alerts

1 Affected resources

Active alerts by severity

Low (1)

Search by ID, title, or affected resource

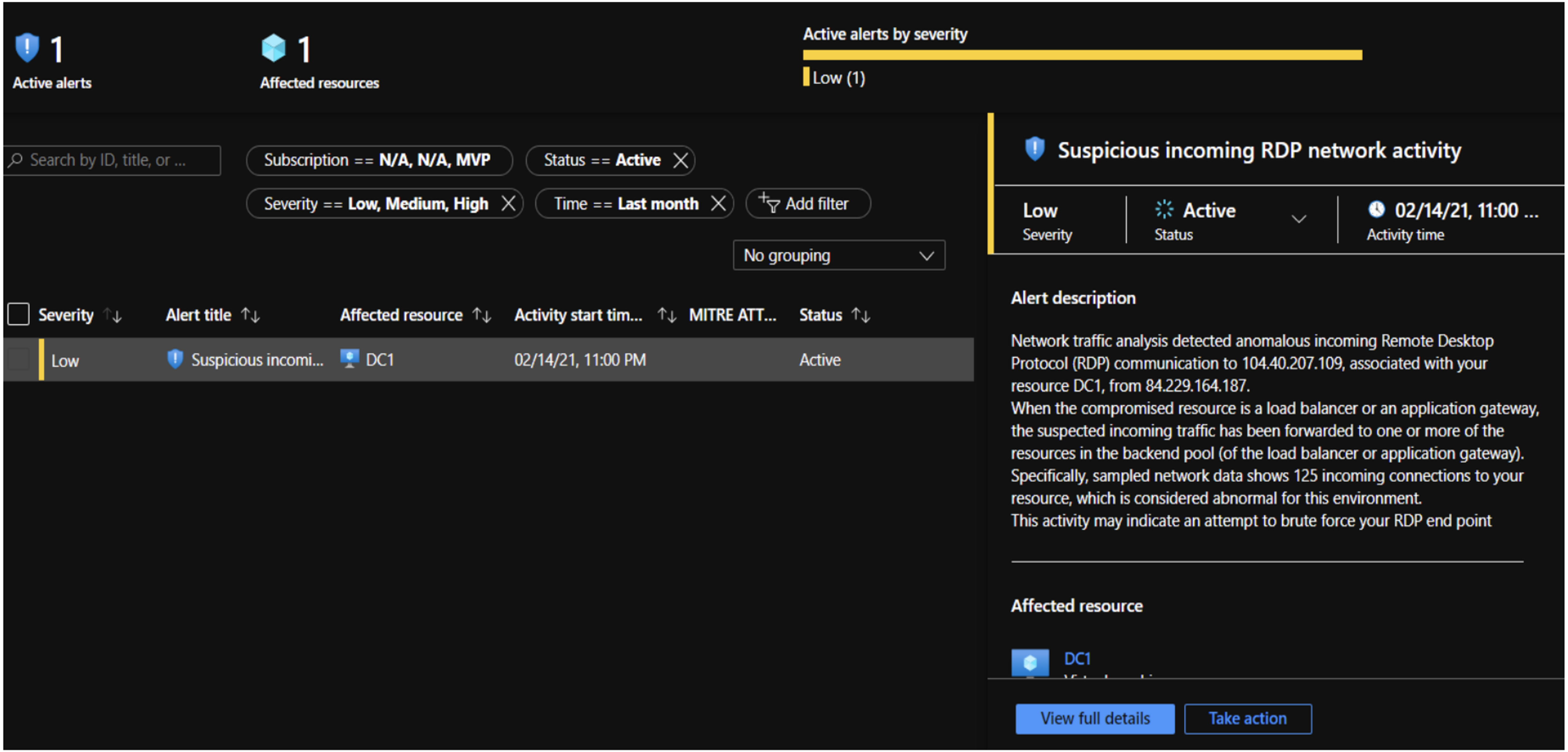
Subscription == **N/A, N/A, MVP**

Status == **Active**

Severity == **Low, Medium, High**

□ Severity	Alert title	Affected resource	Activity start time (UTC+2)
□ Low	Suspicious incoming RDP network activity	DC1	02/14/21, 11:00 PM

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/



1 Active alerts

1 Affected resources

Active alerts by severity

Low (1)

Search by ID, title, or ...

Subscription == **N/A, N/A, MVP**

Status == **Active**

Severity == **Low, Medium, High**

Time == **Last month**

Severity	Alert title	Affected resource	Activity start tim...	MITRE ATT...	Status
Low	Suspicious incomi...	DC1	02/14/21, 11:00 PM		Active

Suspicious incoming RDP network activity

Low
Severity

Active
Status

02/14/21, 11:00 ...
Activity time

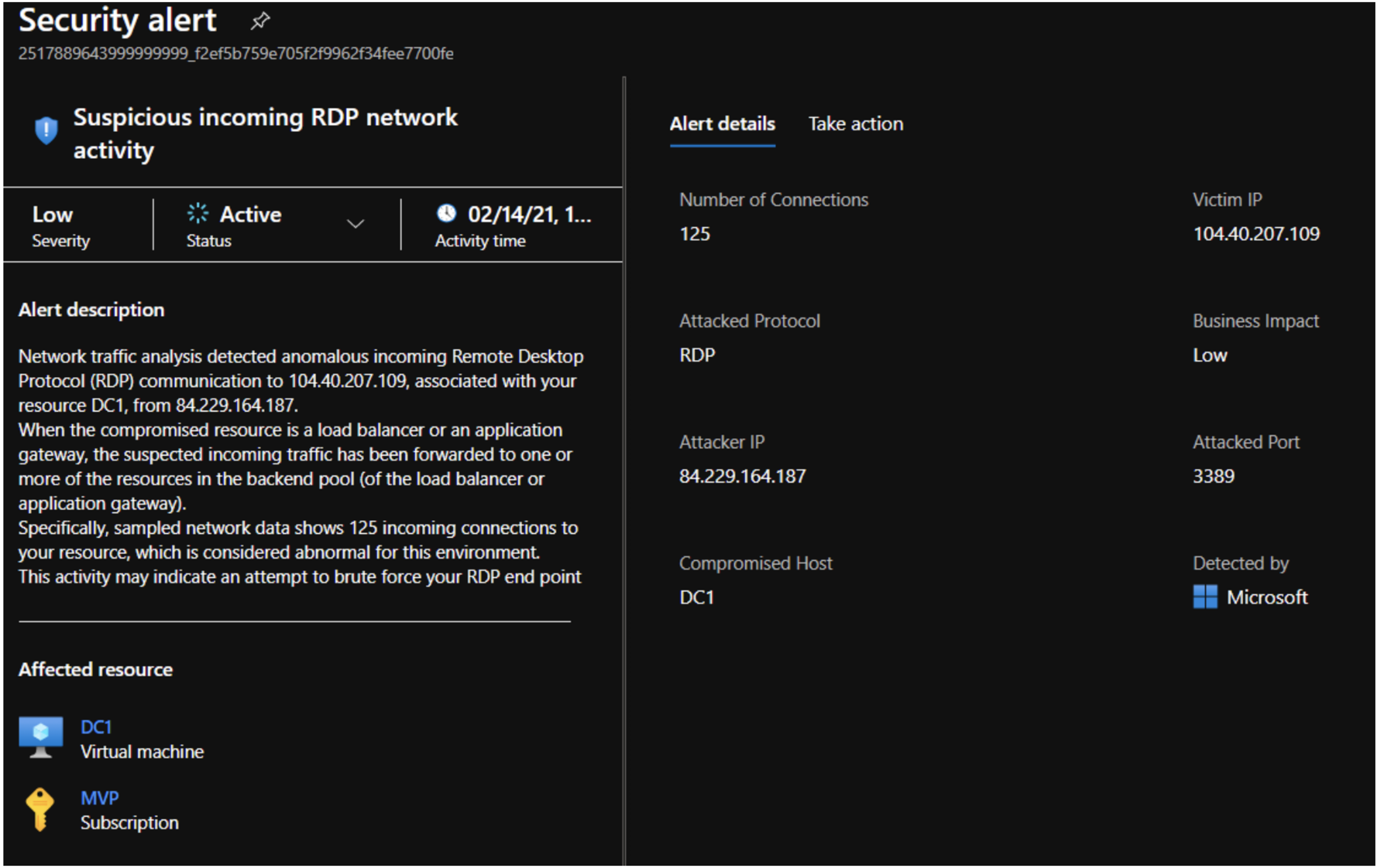
Alert description

Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to 104.40.207.109, associated with your resource DC1, from 84.229.164.187.
When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway).
Specifically, sampled network data shows 125 incoming connections to your resource, which is considered abnormal for this environment.
This activity may indicate an attempt to brute force your RDP end point

Affected resource

DC1

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/



Security alert

2517889643999999999_f2ef5b759e705f2f9962f34fee7700fe

Suspicious incoming RDP network activity

Low
Severity

Active
Status

02/14/21, 1...
Activity time

Alert description

Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to 104.40.207.109, associated with your resource DC1, from 84.229.164.187.
When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway).
Specifically, sampled network data shows 125 incoming connections to your resource, which is considered abnormal for this environment.
This activity may indicate an attempt to brute force your RDP end point

Affected resource

DC1
Virtual machine

MVP
Subscription

Number of Connections
125

Victim IP
104.40.207.109

Attacked Protocol
RDP

Business Impact
Low

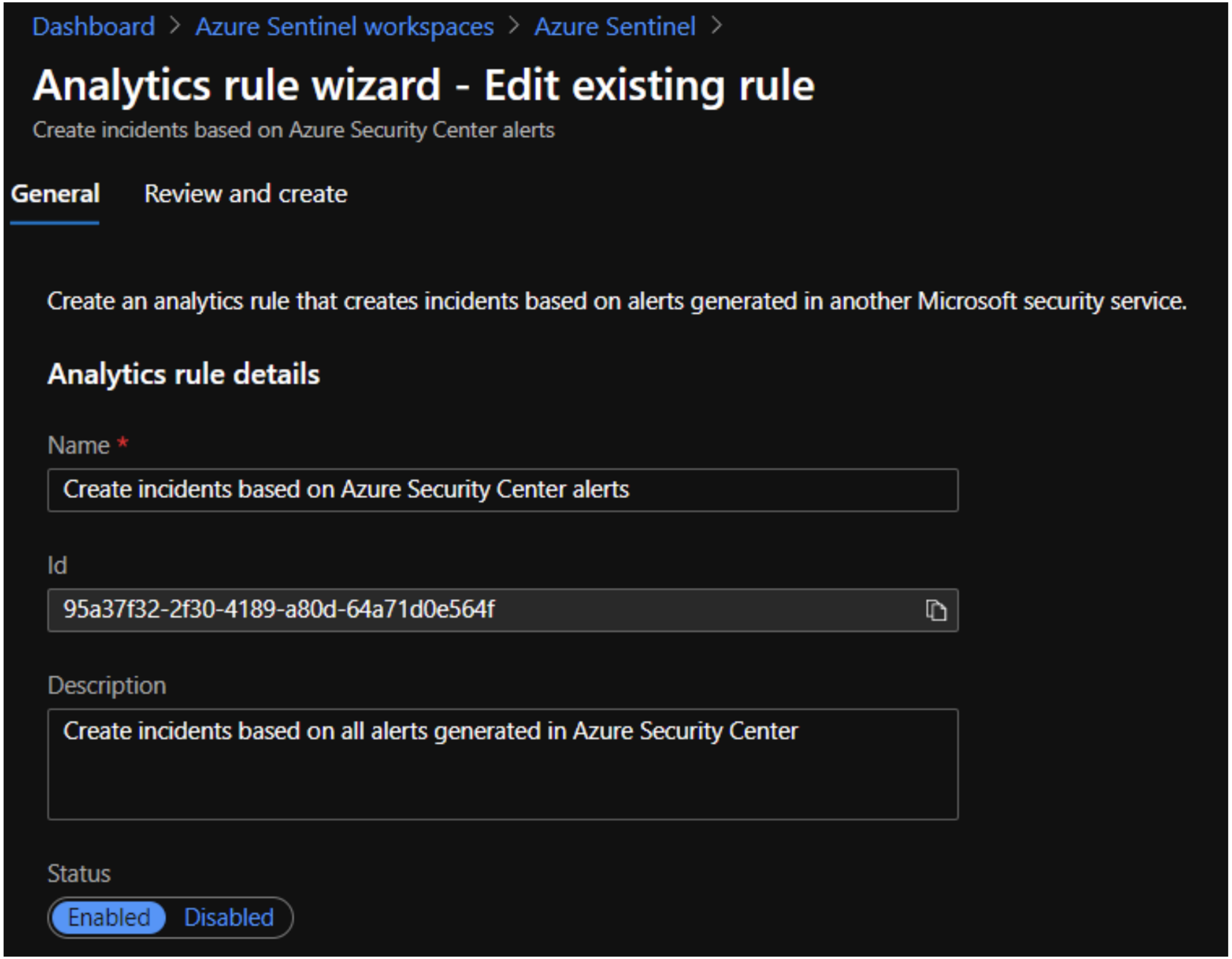
Attacker IP
84.229.164.187

Attacked Port
3389

Compromised Host
DC1

Detected by
Microsoft

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/



Analytics rule wizard - Edit existing rule

Create incidents based on Azure Security Center alerts

Create an analytics rule that creates incidents based on alerts generated in another Microsoft security service.

Analytics rule details

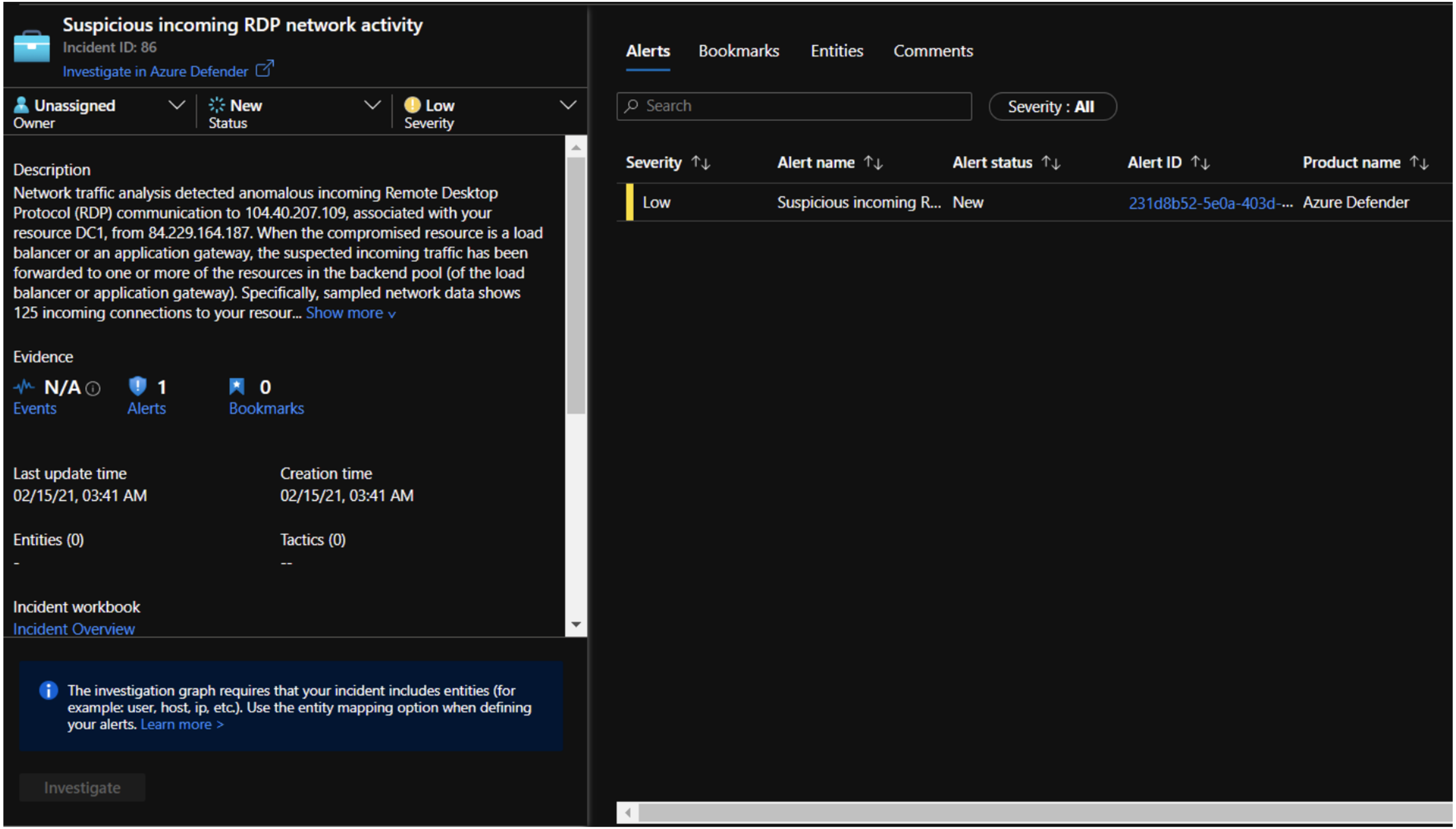
Name *
Create incidents based on Azure Security Center alerts

Id
95a37f32-2f30-4189-a80d-64a71d0e564f

Description
Create incidents based on all alerts generated in Azure Security Center

Status
Enabled Disabled

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/



Suspicious incoming RDP network activity

Incident ID: 86

Investigate in Azure Defender

Unassigned
Owner

New
Status

Low
Severity

Description

Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to 104.40.207.109, associated with your resource DC1, from 84.229.164.187. When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows 125 incoming connections to your resour... Show more

Evidence

N/A Events

1 Alerts

0 Bookmarks

Last update time
02/15/21, 03:41 AM

Creation time
02/15/21, 03:41 AM

Entities (0)
-

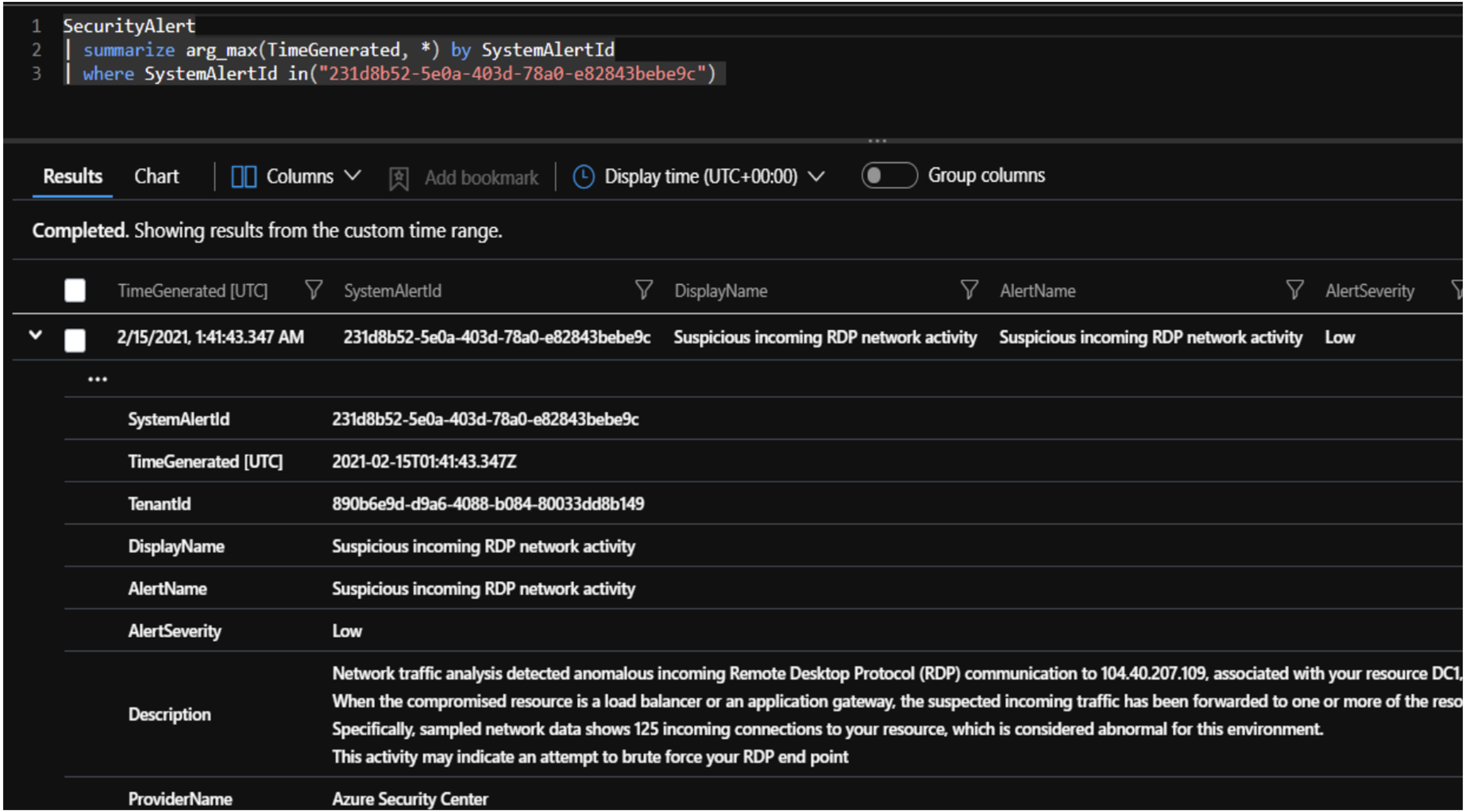
Tactics (0)
--

Incident workbook
Incident Overview

The investigation graph requires that your incident includes entities (for example: user, host, ip, etc.). Use the entity mapping option when defining your alerts. Learn more >

Severity	Alert name	Alert status	Alert ID	Product name
Low	Suspicious incoming R...	New	231d8b52-5e0a-403d-...	Azure Defender

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/



```
SecurityAlert
| summarize arg_max(TimeGenerated, *) by SystemAlertId
| where SystemAlertId in("231d8b52-5e0a-403d-78a0-e82843bebe9c")
```

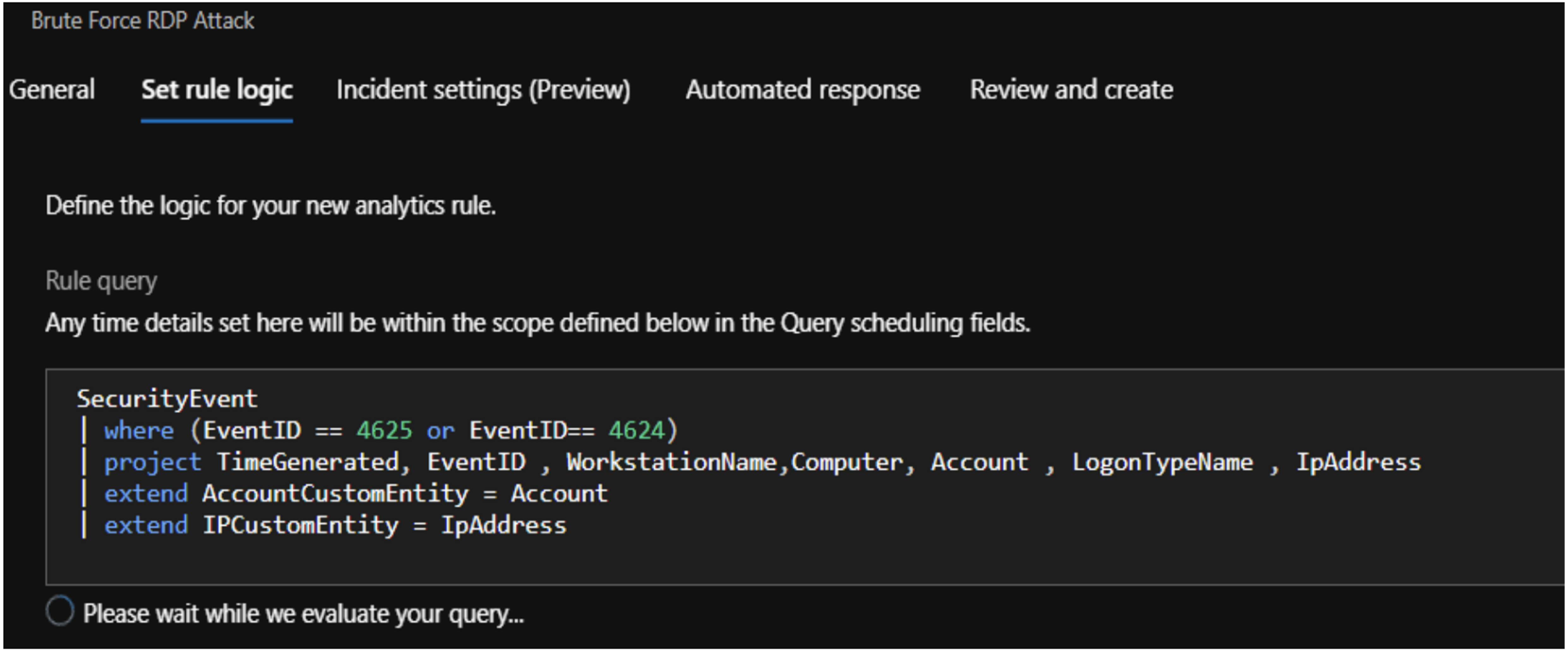
Completed. Showing results from the custom time range.

TimeGenerated [UTC]	SystemAlertId	DisplayName	AlertName	AlertSeverity
2/15/2021, 1:41:43.347 AM	231d8b52-5e0a-403d-78a0-e82843bebe9c	Suspicious incoming RDP network activity	Suspicious incoming RDP network activity	Low

SystemAlertId	231d8b52-5e0a-403d-78a0-e82843bebe9c
TimeGenerated [UTC]	2021-02-15T01:41:43.347Z
TenantId	890b6e9d-d9a6-4088-b084-80033dd8b149
DisplayName	Suspicious incoming RDP network activity
AlertName	Suspicious incoming RDP network activity
AlertSeverity	Low
Description	Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to 104.40.207.109, associated with your resource DC1, When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the reso Specifically, sampled network data shows 125 incoming connections to your resource, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point
ProviderName	Azure Security Center

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/

Azure Sentinel Threat Hunting



Define the logic for your new analytics rule.

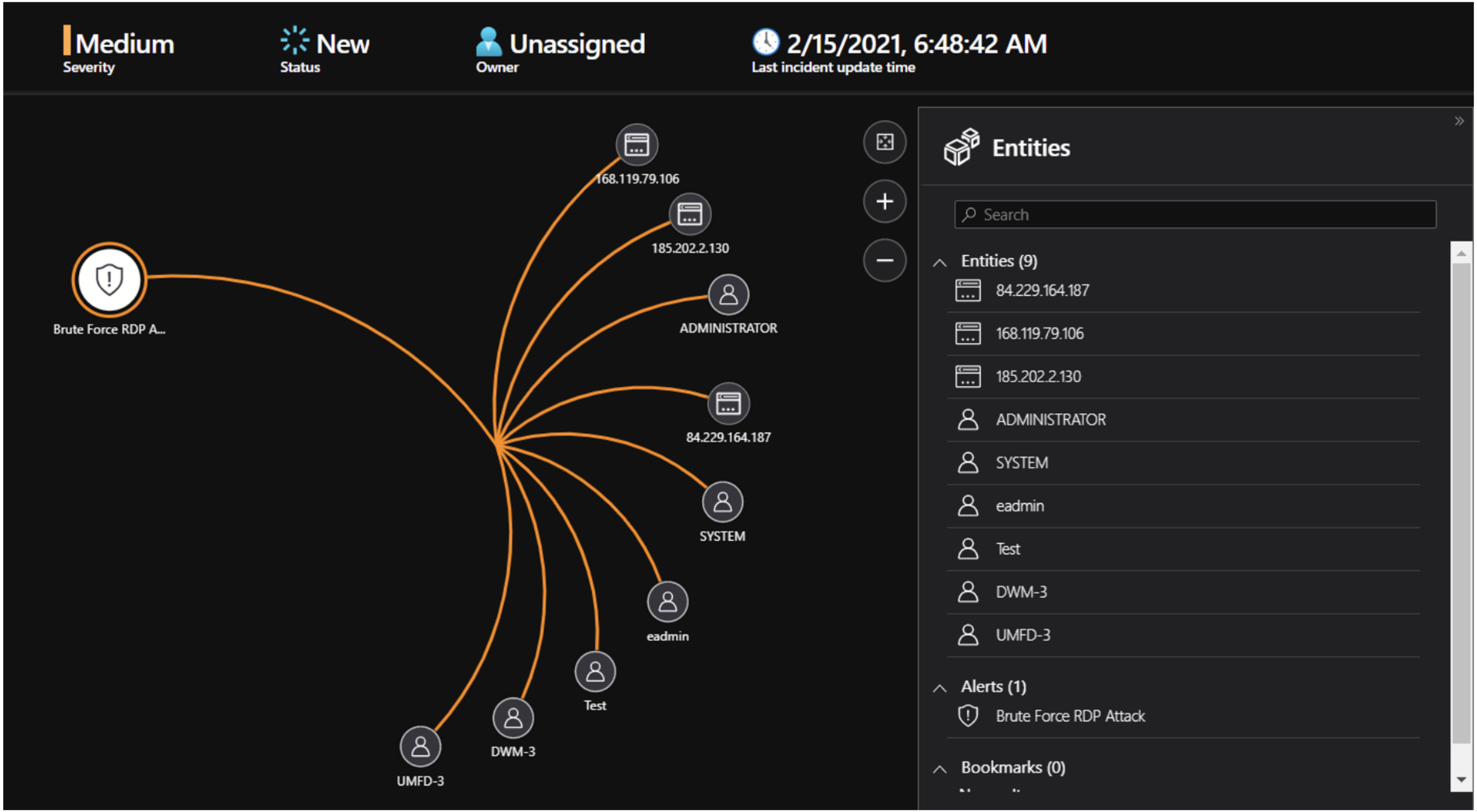
Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
SecurityEvent
| where (EventID == 4625 or EventID== 4624)
| project TimeGenerated, EventID , WorkstationName,Computer, Account , LogonTypeName , IpAddress
| extend AccountCustomEntity = Account
| extend IPCustomEntity = IpAddress
```

○ Please wait while we evaluate your query...

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/



Medium
Severity

New
Status

Unassigned
Owner

2/15/2021, 6:48:42 AM
Last incident update time

Entities

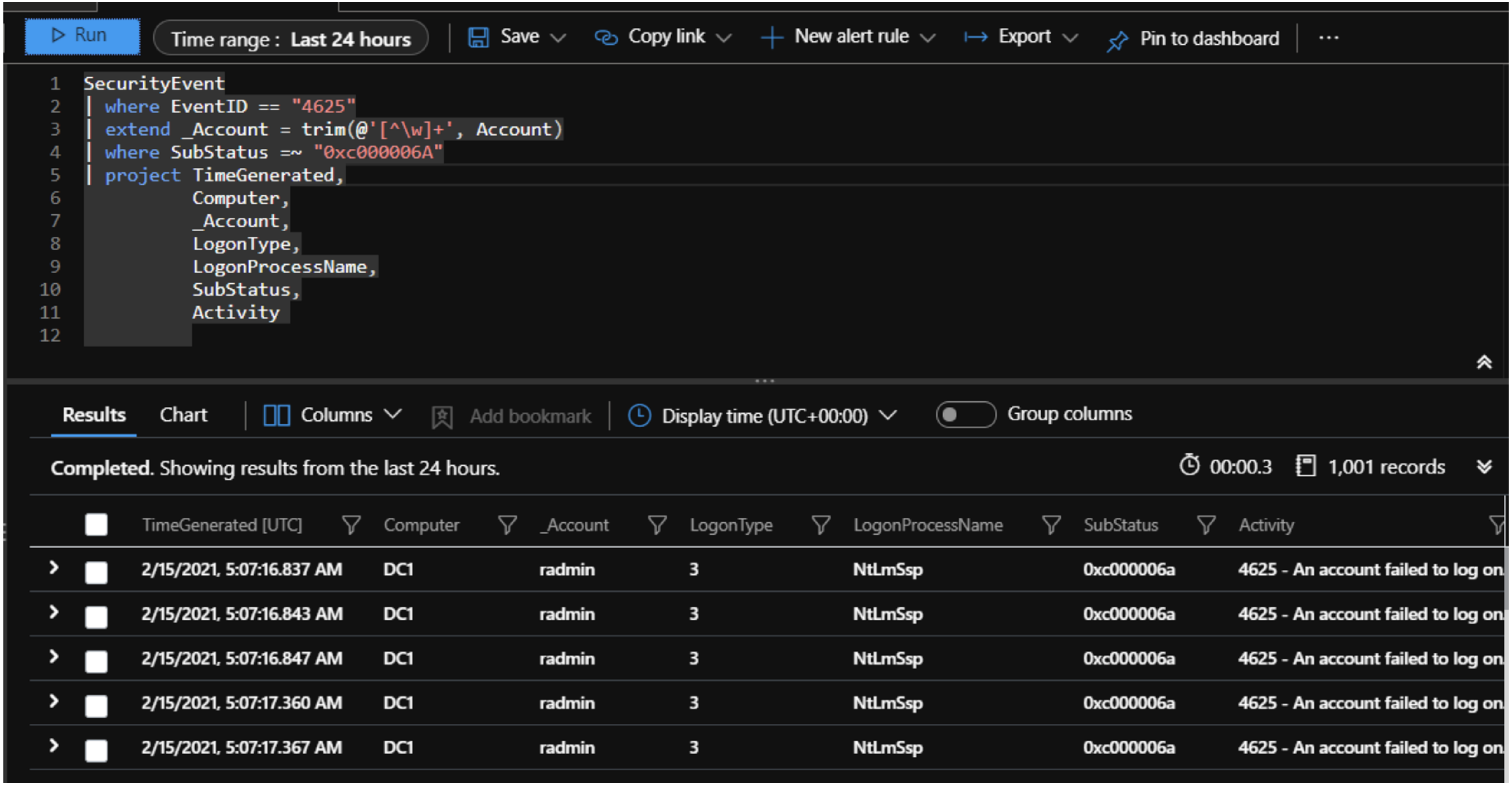
Search

Entities (9)
- 84.229.164.187
- 168.119.79.106
- 185.202.2.130
- ADMINISTRATOR
- SYSTEM
- eadmin
- Test
- DWM-3
- UMFD-3

Alerts (1)
- Brute Force RDP Attack

Bookmarks (0)

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/



```
SecurityEvent
| where EventID == "4625"
| extend _Account = trim(@'[^\w]+', Account)
| where SubStatus =~ "0xc000006A"
| project TimeGenerated,
          Computer,
          _Account,
          LogonType,
          LogonProcessName,
          SubStatus,
          Activity

```

Completed. Showing results from the last 24 hours.

00:00.3 1,001 records

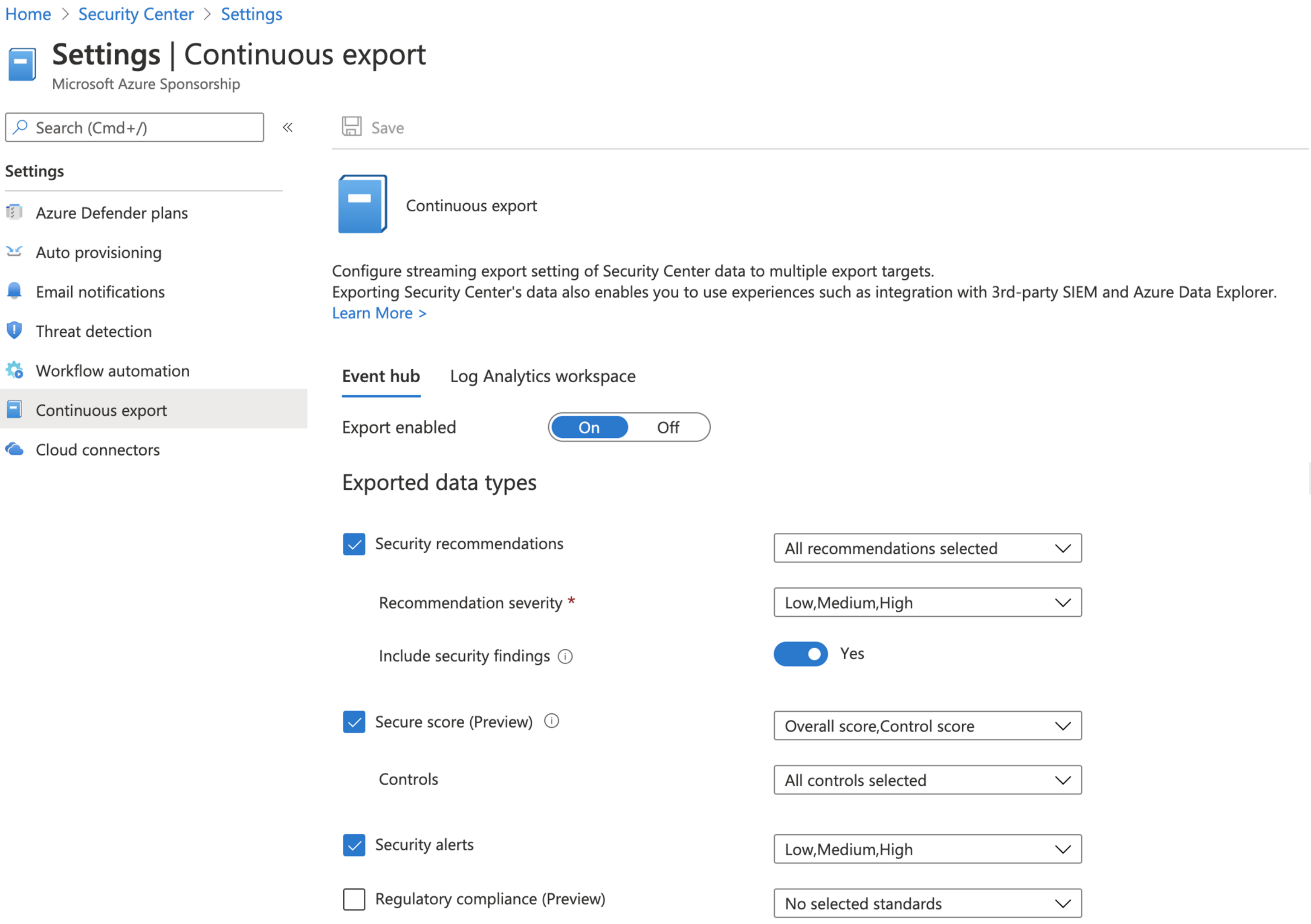
TimeGenerated [UTC]	Computer	_Account	LogonType	LogonProcessName	SubStatus	Activity
2/15/2021, 5:07:16.837 AM	DC1	radmin	3	NtLmSsp	0xc000006a	4625 - An account failed to log on
2/15/2021, 5:07:16.843 AM	DC1	radmin	3	NtLmSsp	0xc000006a	4625 - An account failed to log on
2/15/2021, 5:07:16.847 AM	DC1	radmin	3	NtLmSsp	0xc000006a	4625 - An account failed to log on
2/15/2021, 5:07:17.360 AM	DC1	radmin	3	NtLmSsp	0xc000006a	4625 - An account failed to log on
2/15/2021, 5:07:17.367 AM	DC1	radmin	3	NtLmSsp	0xc000006a	4625 - An account failed to log on

https://www.eshlomo.us/monitor-azure-security-center-with-azure-sentinel/

#GlobalAzureTO

Export - Alerts to SIEM

Export - Alerts to SIEM



Home > Security Center > Settings

Settings | Continuous export

Microsoft Azure Sponsorship

Search (Cmd+/) «

Save

Settings

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

Continuous export

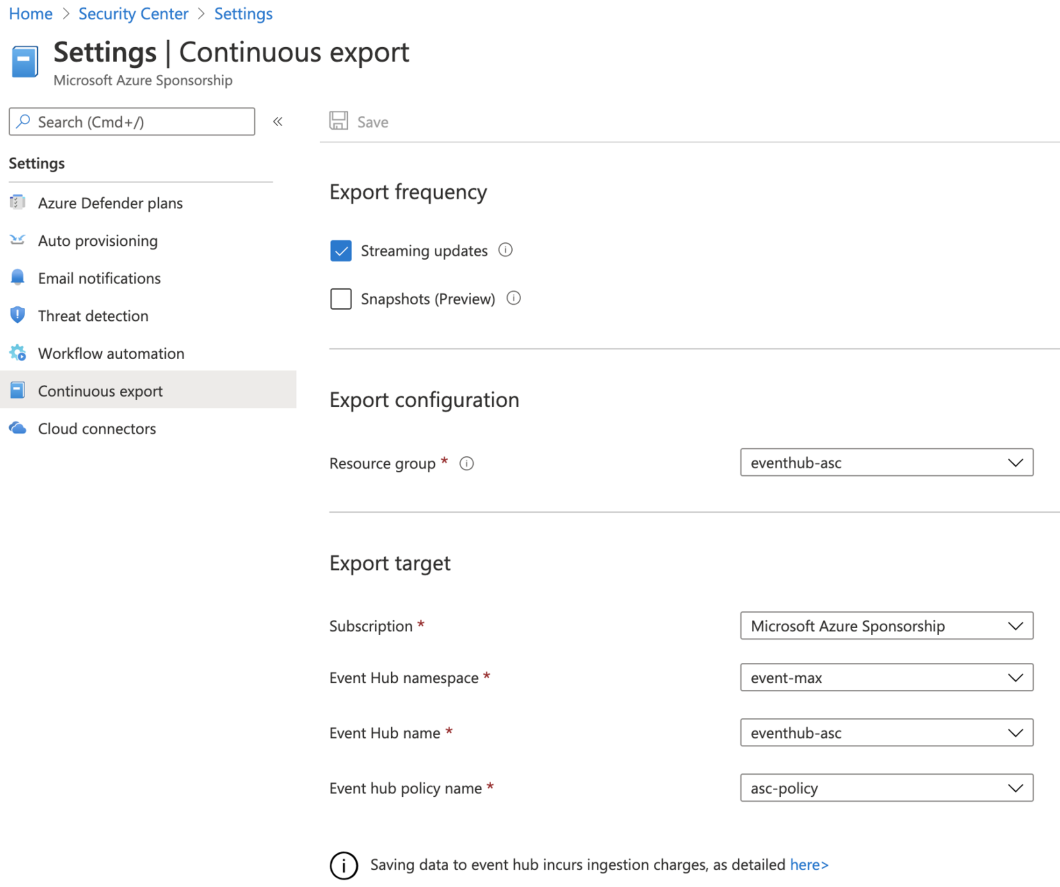
Configure streaming export setting of Security Center data to multiple export targets.
Exporting Security Center's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer.
Learn More >

Event hub | Log Analytics workspace

Export enabled: **On** | Off

Exported data types

☑ Security recommendations	All recommendations selected
Recommendation severity *	Low,Medium,High
Include security findings ⓘ	Yes
☑ Secure score (Preview) ⓘ	Overall score,Control score
Controls	All controls selected
☑ Security alerts	Low,Medium,High
☐ Regulatory compliance (Preview)	No selected standards



Home > Security Center > Settings

Settings | Continuous export

Microsoft Azure Sponsorship

Search (Cmd+/) «

Save

Settings

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

Export frequency

☑ Streaming updates ⓘ

☐ Snapshots (Preview) ⓘ

Export configuration

Resource group * ⓘ	eventhub-asc

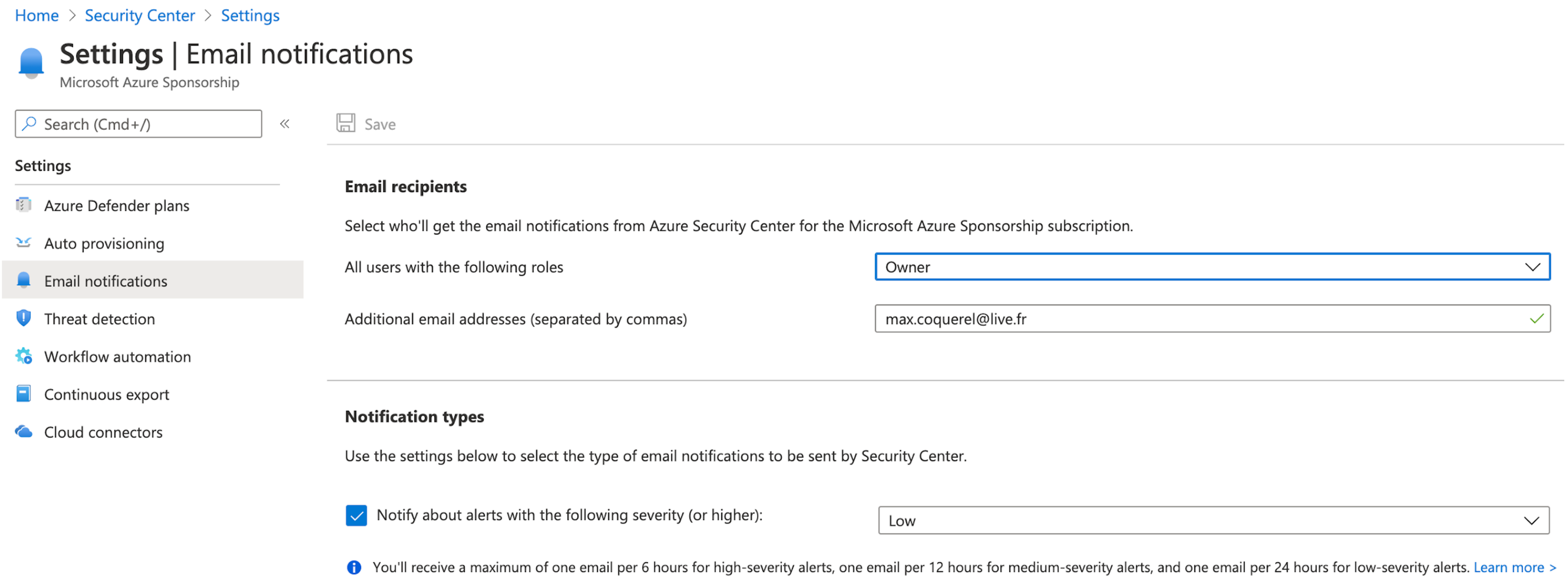
Export target

Subscription *	Microsoft Azure Sponsorship
Event Hub namespace *	event-max
Event Hub name *	eventhub-asc
Event hub policy name *	asc-policy

ⓘ Saving data to event hub incurs ingestion charges, as detailed here>

Alert - Notification

Alert - Notification



Home > Security Center > Settings

Settings | Email notifications

Microsoft Azure Sponsorship

Email recipients

Select who'll get the email notifications from Azure Security Center for the Microsoft Azure Sponsorship subscription.

All users with the following roles: Owner

Additional email addresses (separated by commas): max.coquerel@live.fr ✓

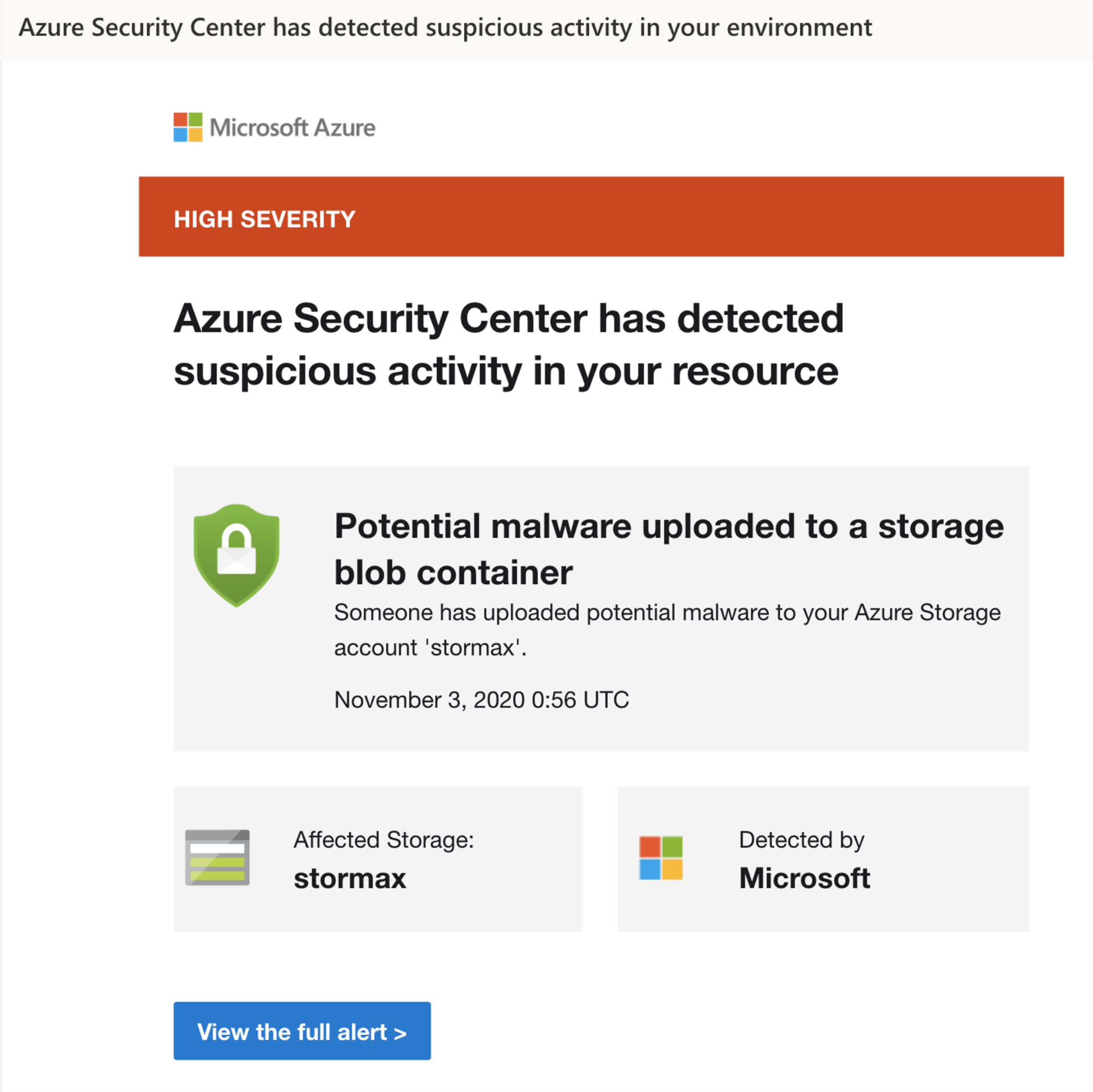
Notification types

Use the settings below to select the type of email notifications to be sent by Security Center.

☑ Notify about alerts with the following severity (or higher): Low

ⓘ You'll receive a maximum of one email per 6 hours for high-severity alerts, one email per 12 hours for medium-severity alerts, and one email per 24 hours for low-severity alerts. Learn more >

Alert - Notification



Azure Security Center has detected suspicious activity in your environment

Microsoft Azure

HIGH SEVERITY

Azure Security Center has detected suspicious activity in your resource

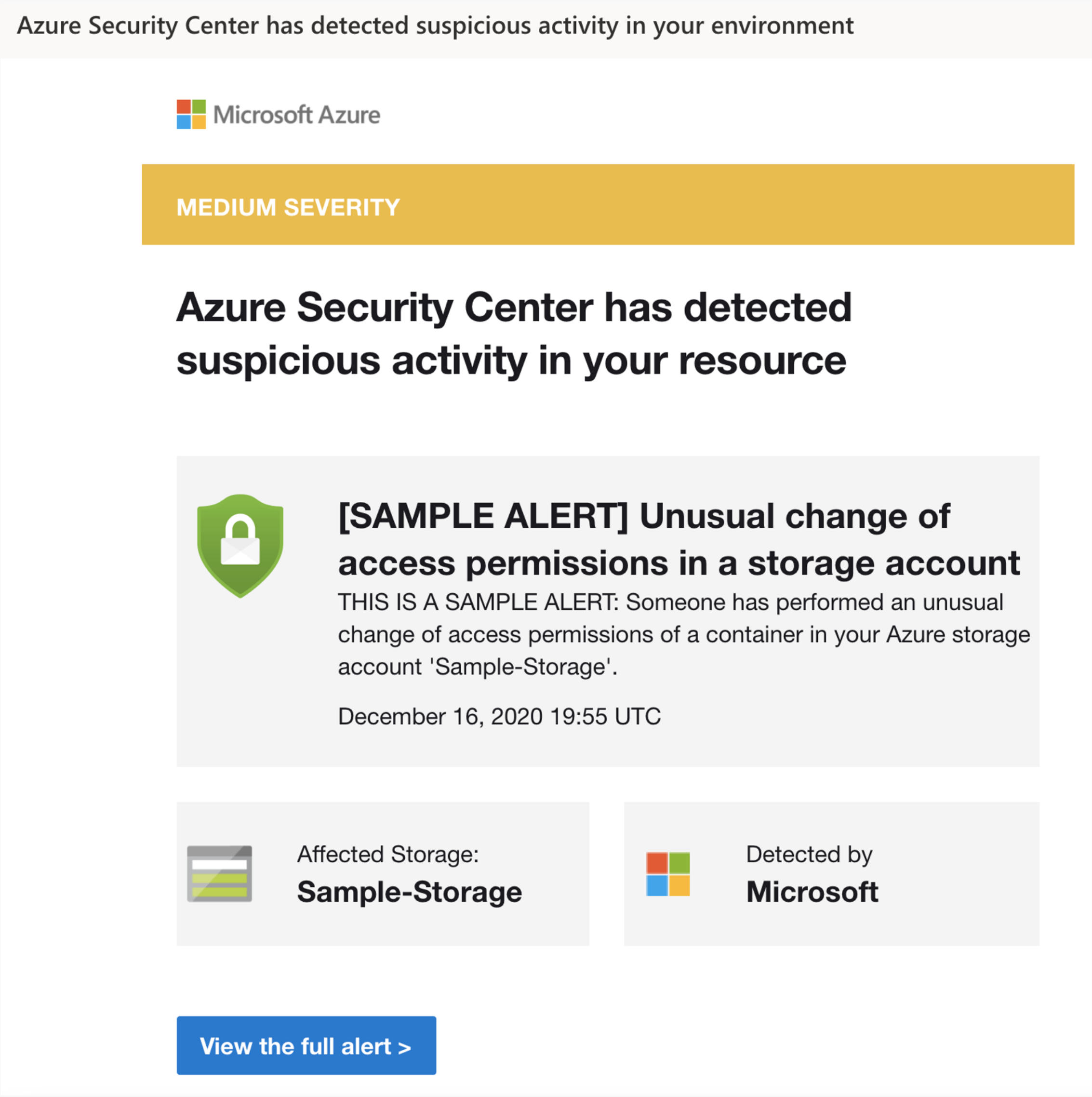
Potential malware uploaded to a storage blob container

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

November 3, 2020 0:56 UTC

Affected Storage:
stormax

Detected by
Microsoft



Azure Security Center has detected suspicious activity in your environment

Microsoft Azure

MEDIUM SEVERITY

Azure Security Center has detected suspicious activity in your resource

[SAMPLE ALERT] Unusual change of access permissions in a storage account

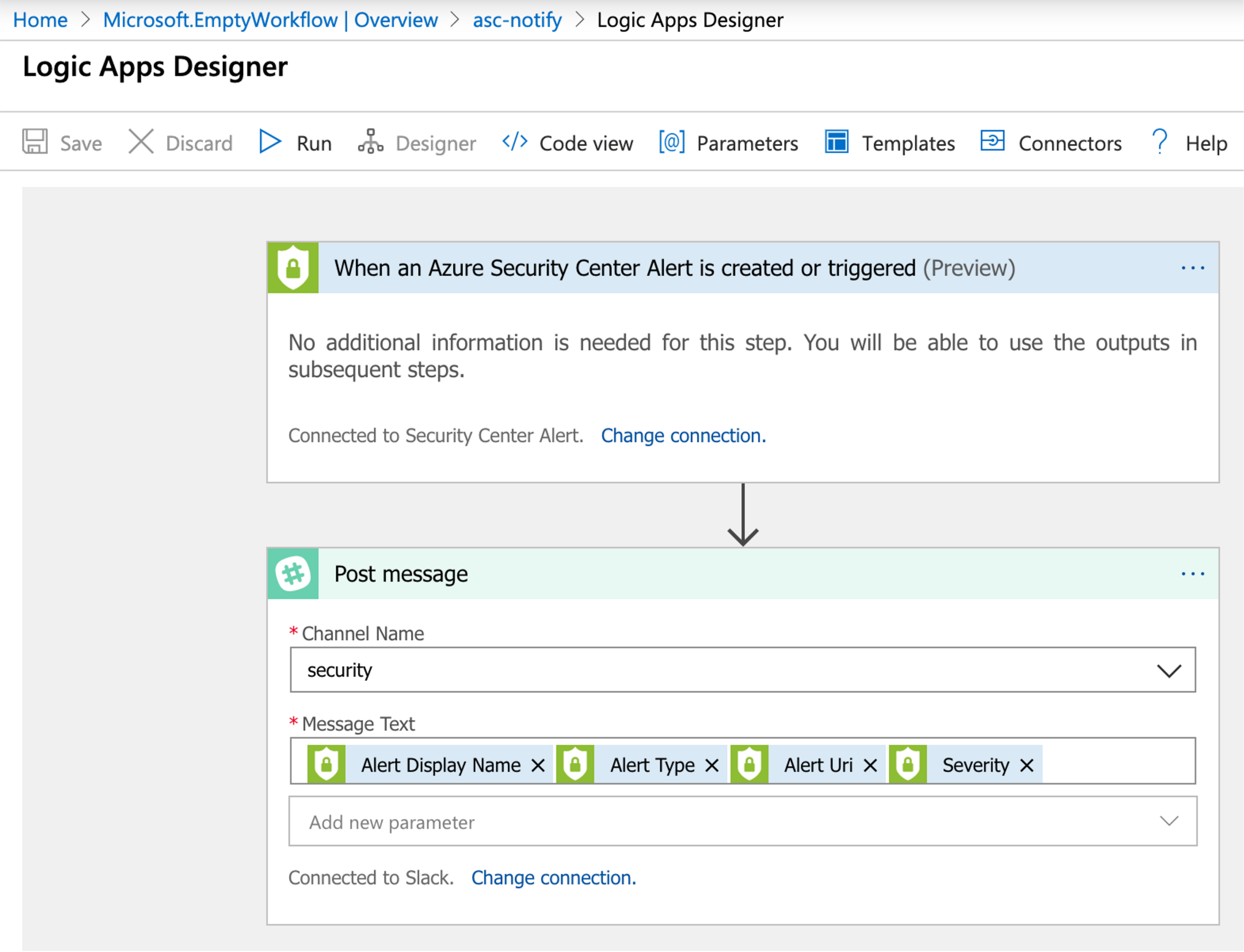
THIS IS A SAMPLE ALERT: Someone has performed an unusual change of access permissions of a container in your Azure storage account 'Sample-Storage'.

December 16, 2020 19:55 UTC

Affected Storage:
Sample-Storage

Detected by
Microsoft

Slack



Home > Microsoft.EmptyWorkflow | Overview > asc-notify > Logic Apps Designer

Logic Apps Designer

When an Azure Security Center Alert is created or triggered (Preview)

No additional information is needed for this step. You will be able to use the outputs in subsequent steps.

Connected to Security Center Alert. Change connection.

Post message

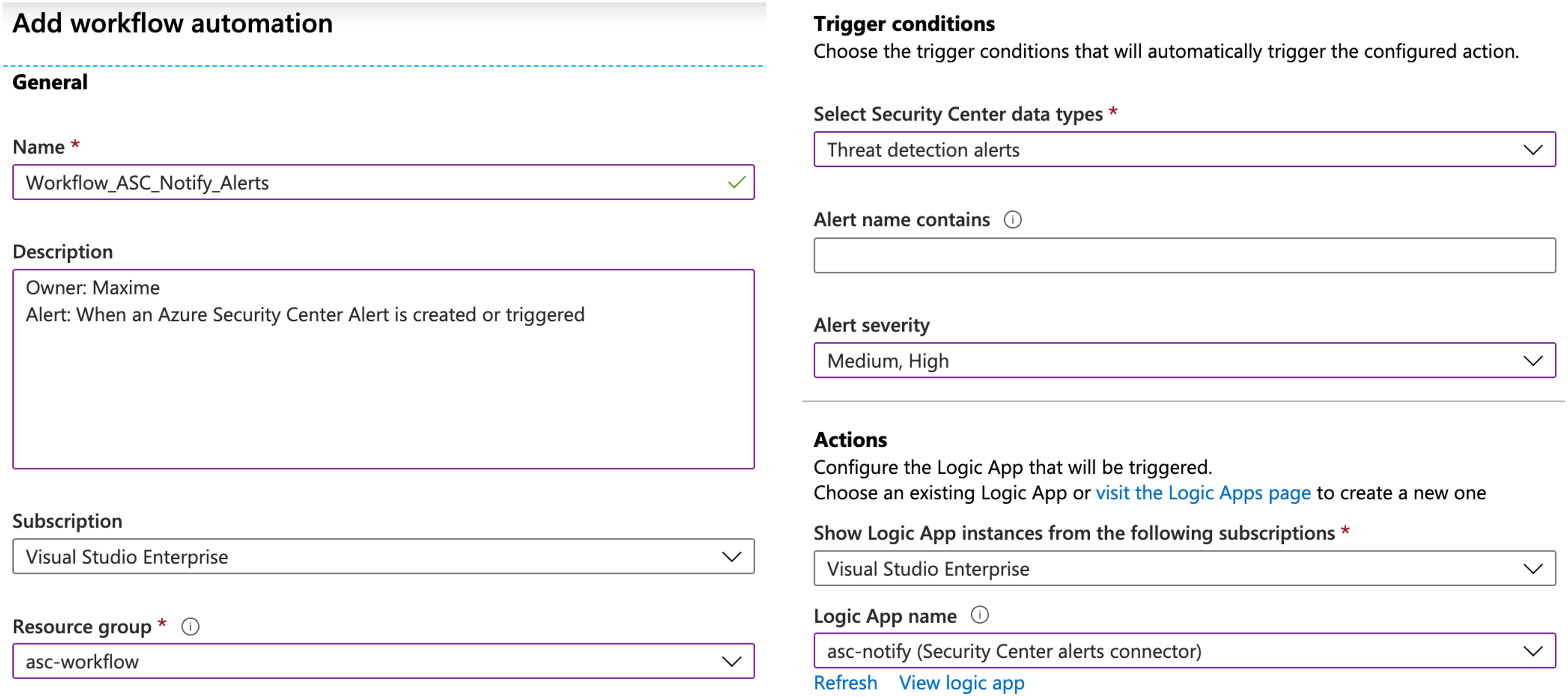
* Channel Name: security

* Message Text: Alert Display Name ✕ Alert Type ✕ Alert Uri ✕ Severity ✕

Add new parameter

Connected to Slack. Change connection.

Slack



Add workflow automation

General

Name *
Workflow_ASC_Notify_Alerts ✓

Description
Owner: Maxime
Alert: When an Azure Security Center Alert is created or triggered

Subscription
Visual Studio Enterprise

Resource group * ⓘ
asc-workflow

Trigger conditions

Choose the trigger conditions that will automatically trigger the configured action.

Select Security Center data types *
Threat detection alerts

Alert name contains ⓘ

Alert severity
Medium, High

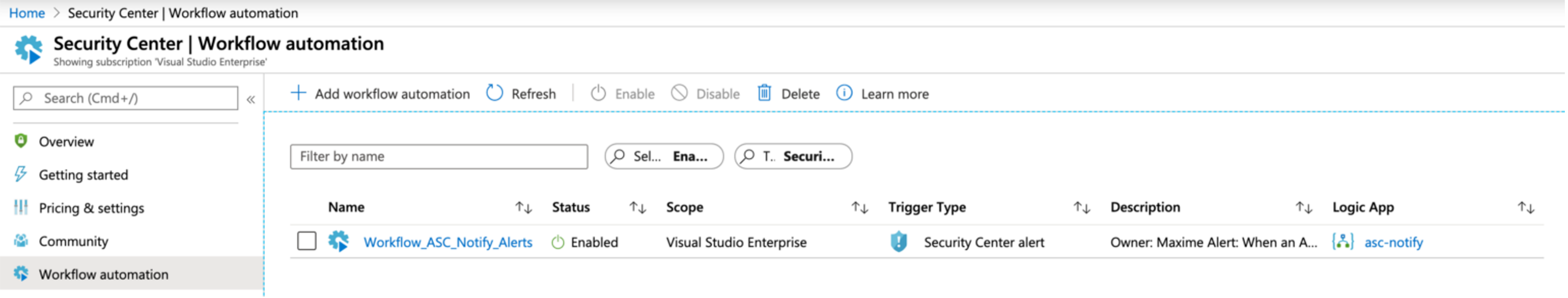
Actions

Configure the Logic App that will be triggered.
Choose an existing Logic App or visit the Logic Apps page to create a new one

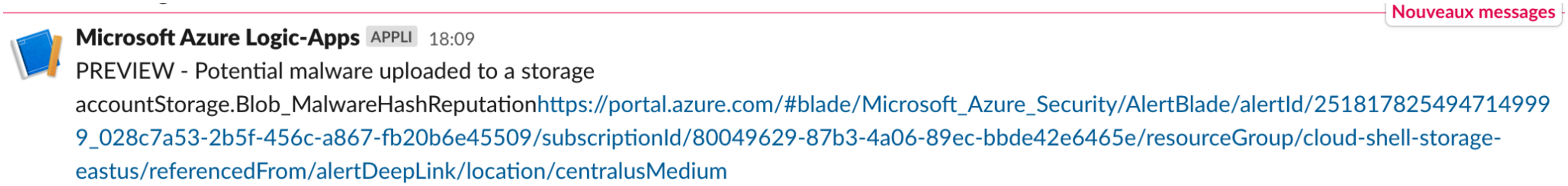
Show Logic App instances from the following subscriptions *
Visual Studio Enterprise

Logic App name ⓘ
asc-notify (Security Center alerts connector)

Refresh View logic app



Name	Status	Scope	Trigger Type	Description	Logic App
Workflow_ASC_Notify_Alerts	Enabled	Visual Studio Enterprise	Security Center alert	Owner: Maxime Alert: When an A...	asc-notify

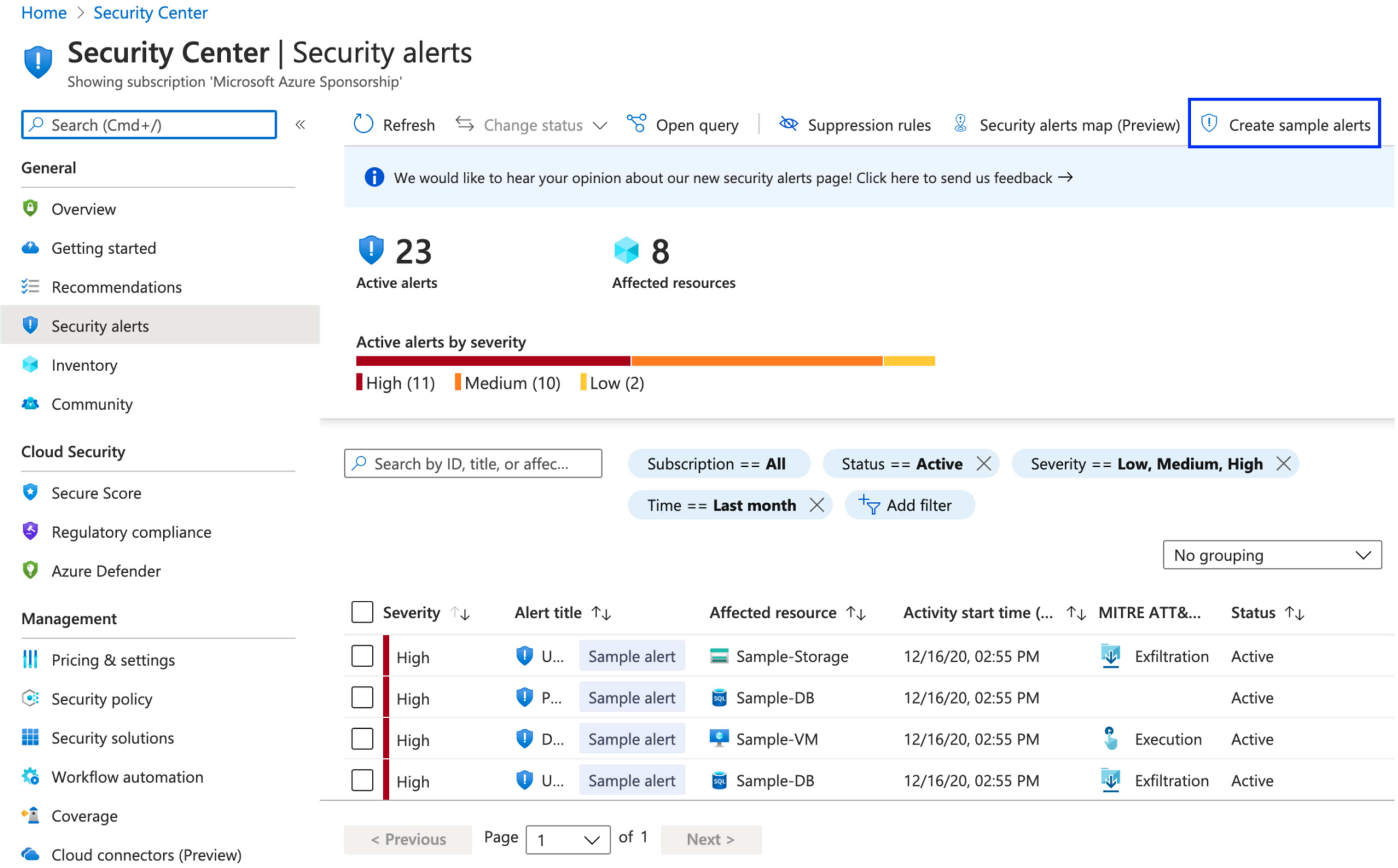


PREVIEW - Potential malware uploaded to a storage accountStorage.Blob_MalwareHashReputationhttps://portal.azure.com/#blade/Microsoft_Azure_Security/AlertBlade/alertId/2518178254947149999_028c7a53-2b5f-456c-a867-fb20b6e45509/subscriptionId/80049629-87b3-4a06-89ec-bbde42e6465e/resourceGroup/cloud-shell-storage-eastus/referencedFrom/alertDeepLink/location/centralusMedium

#GlobalAzureTO

Alert - Simulation

Alert - Simulation



Security Center | Security alerts

Showing subscription 'Microsoft Azure Sponsorship'

We would like to hear your opinion about our new security alerts page! Click here to send us feedback →

23 Active alerts

8 Affected resources

Active alerts by severity

High (11) Medium (10) Low (2)

Subscription == **All**

Status == **Active**

Severity == **Low, Medium, High**

Time == **Last month**

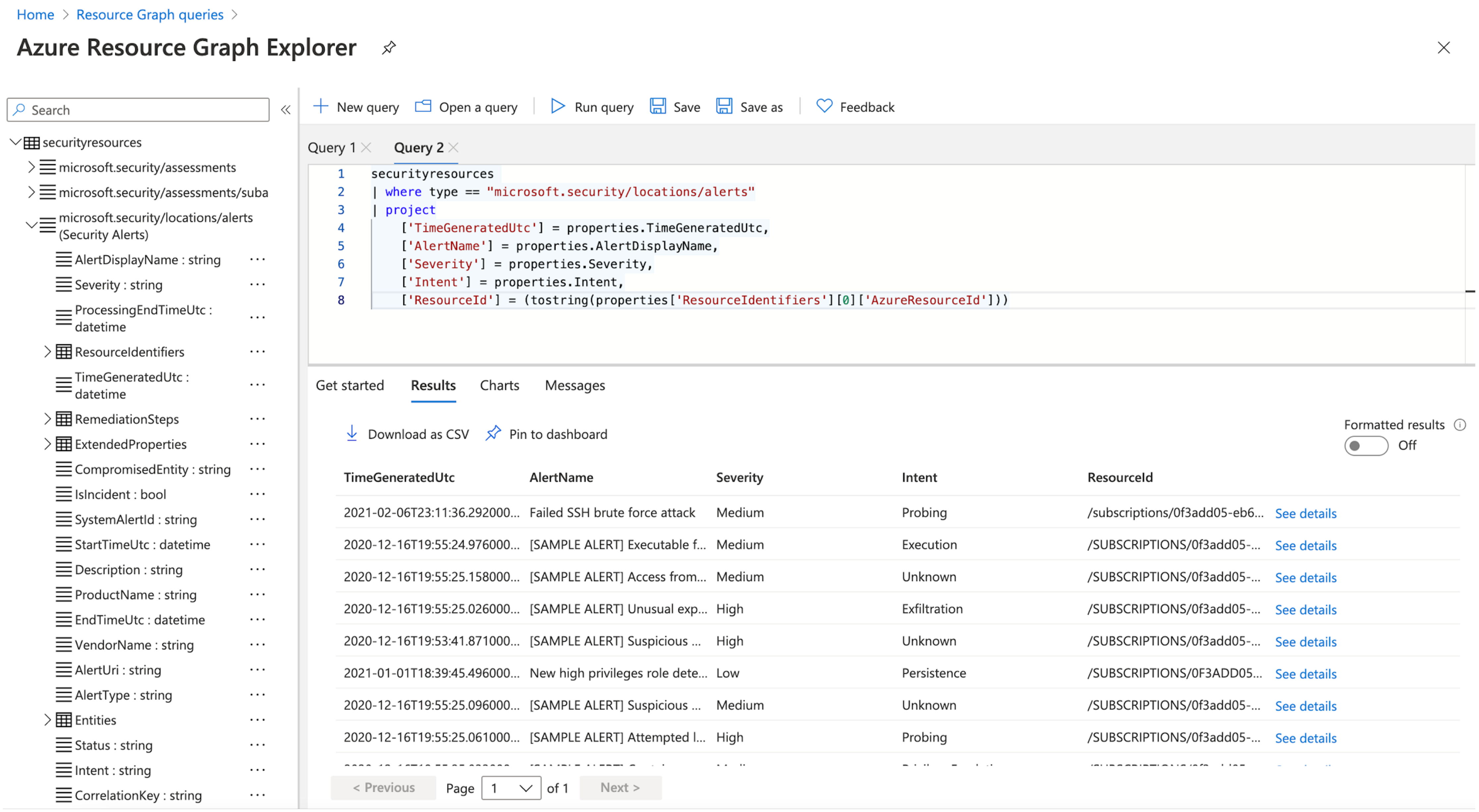
□	Severity ↑↓	Alert title ↑↓	Affected resource ↑↓	Activity start time (... ↑↓	MITRE ATT&...	Status ↑↓
□	High	U... Sample alert	Sample-Storage	12/16/20, 02:55 PM	Exfiltration	Active
□	High	P... Sample alert	Sample-DB	12/16/20, 02:55 PM		Active
□	High	D... Sample alert	Sample-VM	12/16/20, 02:55 PM	Execution	Active
□	High	U... Sample alert	Sample-DB	12/16/20, 02:55 PM	Exfiltration	Active

Azure Alert - Simulation

- App Service / Suspicious WordPress theme invocation detected
- App Service / Phishing content hosted on Azure Webapps
- App Service / Attempt to run high privilege command detected
- AKS / Exposed Kubernetes dashboard detected
- AKS / Container with a sensitive volume detected
- AKV / Access from a TOR exit node to a Key Vault
- AKV / High volume of operations in a Key Vault
- AKV / Suspicious secret listing and query in a Key Vault
- SQL / Unusual export location
- SQL / Attempted logon by a potentially harmful application
- SQL / Logon from an unusual location
- SQL / Potential SQL injection
- Storage / Unusual amount of data extracted from a storage account
- Storage / Unusual change of access permissions in a storage account
- Windows / Detected Petya ransomware indicators
- Windows / Executable found running from a suspicious location

Azure Graph

Azure Graph



- securityresources
  - microsoft.security/assessments
  - microsoft.security/assessments/suba
  - microsoft.security/locations/alerts (Security Alerts)
    - AlertDisplayName : string
    - Severity : string
    - ProcessingEndTimeUtc : datetime
    - ResourceIdentifiers
    - TimeGeneratedUtc : datetime
    - RemediationSteps
    - ExtendedProperties
    - CompromisedEntity : string
    - IsIncident : bool
    - SystemAlertId : string
    - StartTimeUtc : datetime
    - Description : string
    - ProductName : string
    - EndTimeUtc : datetime
    - VendorName : string
    - AlertUri : string
    - AlertType : string
    - Entities
    - Status : string
    - Intent : string
    - CorrelationKey : string

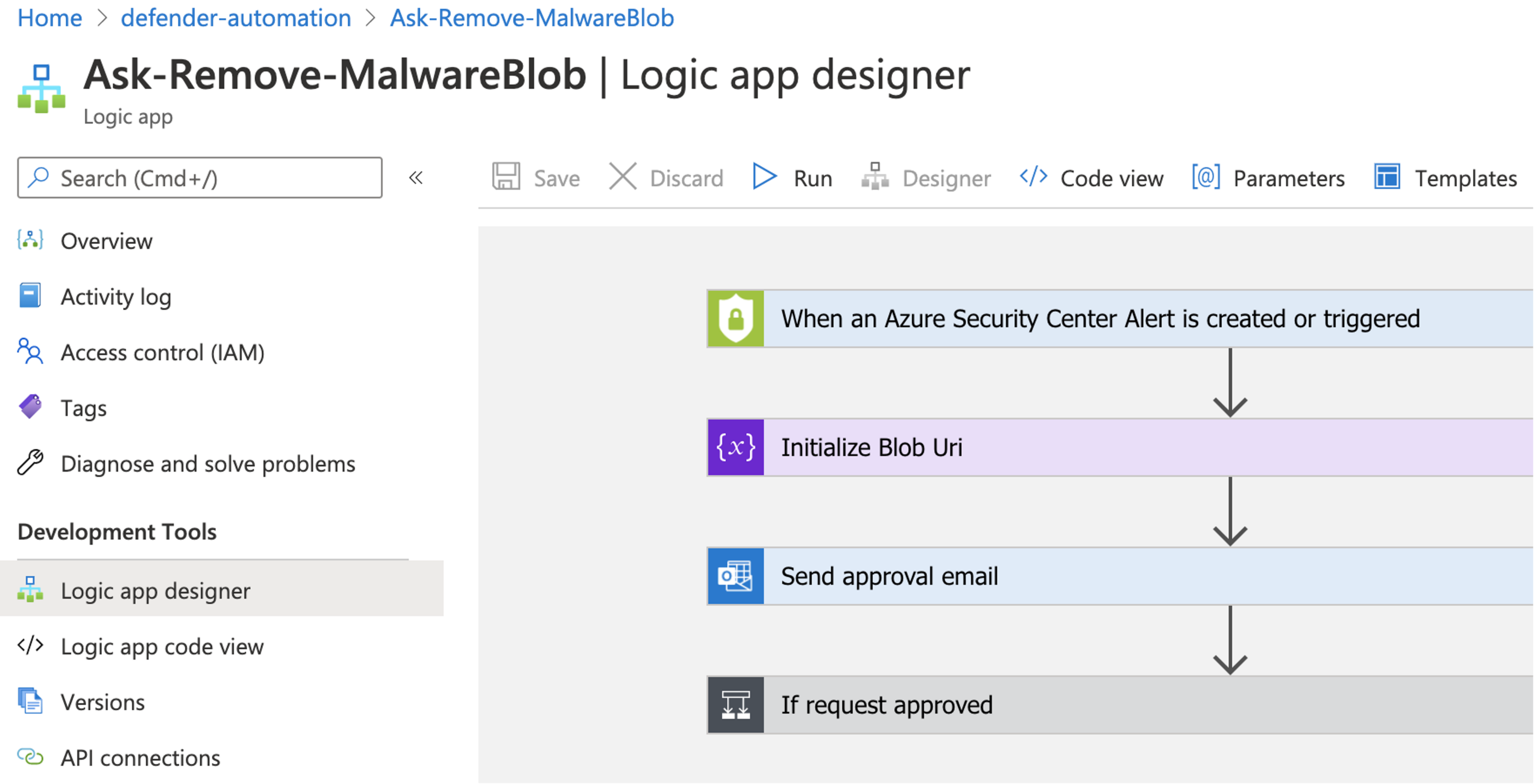
```
securityresources
| where type == "microsoft.security/locations/alerts"
| project
    ['TimeGeneratedUtc'] = properties.TimeGeneratedUtc,
    ['AlertName'] = properties.AlertDisplayName,
    ['Severity'] = properties.Severity,
    ['Intent'] = properties.Intent,
    ['ResourceId'] = (tostring(properties['ResourceIdentifiers'][0]['AzureResourceId']))
```

TimeGeneratedUtc	AlertName	Severity	Intent	ResourceId	
2021-02-06T23:11:36.292000...	Failed SSH brute force attack	Medium	Probing	/subscriptions/0f3add05-eb6...	See details
2020-12-16T19:55:24.976000...	[SAMPLE ALERT] Executable f...	Medium	Execution	/SUBSCRIPTIONS/0f3add05-...	See details
2020-12-16T19:55:25.158000...	[SAMPLE ALERT] Access from...	Medium	Unknown	/SUBSCRIPTIONS/0f3add05-...	See details
2020-12-16T19:55:25.026000...	[SAMPLE ALERT] Unusual exp...	High	Exfiltration	/SUBSCRIPTIONS/0f3add05-...	See details
2020-12-16T19:53:41.871000...	[SAMPLE ALERT] Suspicious ...	High	Unknown	/SUBSCRIPTIONS/0f3add05-...	See details
2021-01-01T18:39:45.496000...	New high privileges role dete...	Low	Persistence	/SUBSCRIPTIONS/0F3ADD05...	See details
2020-12-16T19:55:25.096000...	[SAMPLE ALERT] Suspicious ...	Medium	Unknown	/SUBSCRIPTIONS/0f3add05-...	See details
2020-12-16T19:55:25.061000...	[SAMPLE ALERT] Attempted l...	High	Probing	/SUBSCRIPTIONS/0f3add05-...	See details

#GlobalAzureTO

Alert Automation

Alert Automation



Home > defender-automation > Ask-Remove-MalwareBlob

Ask-Remove-MalwareBlob | Logic app designer

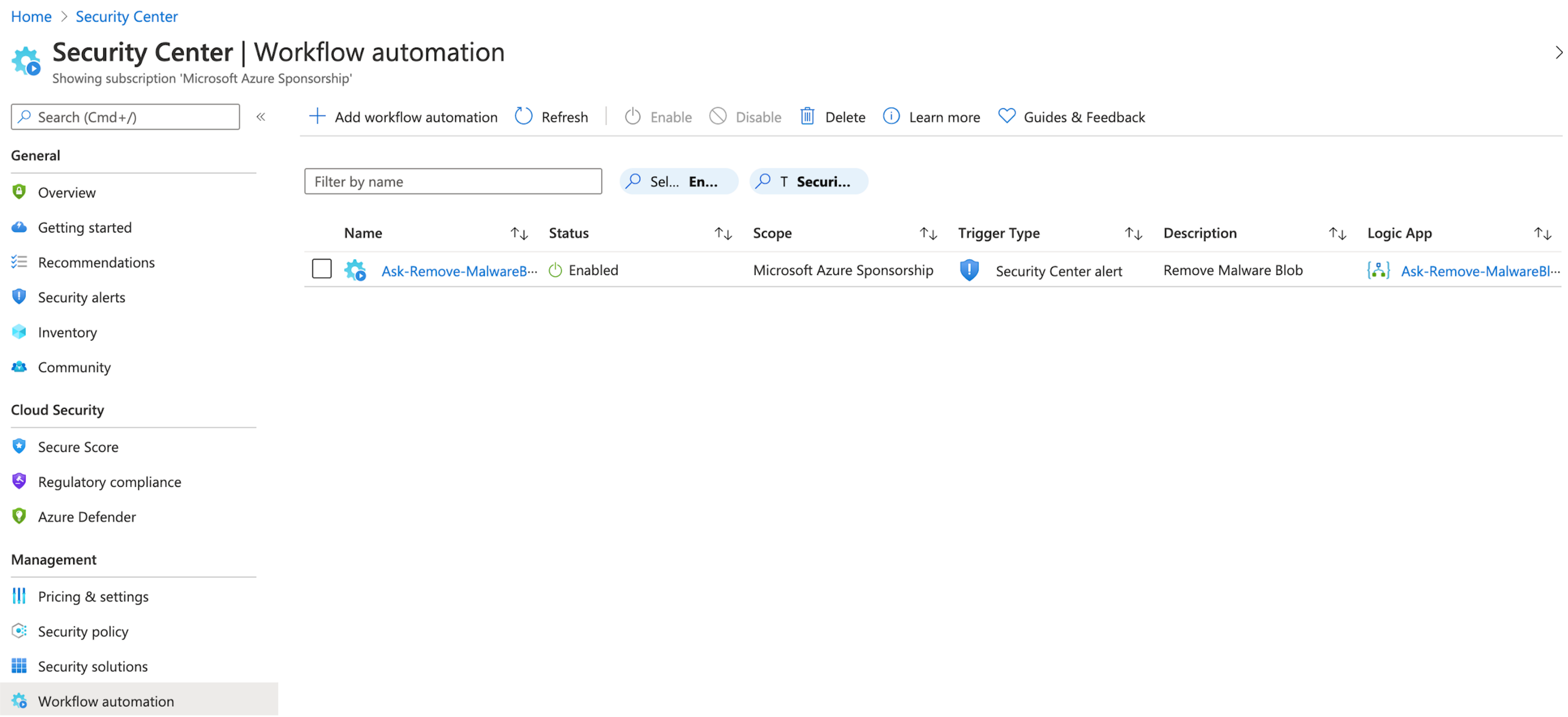
Logic app

When an Azure Security Center Alert is created or triggered

Initialize Blob Uri

Send approval email

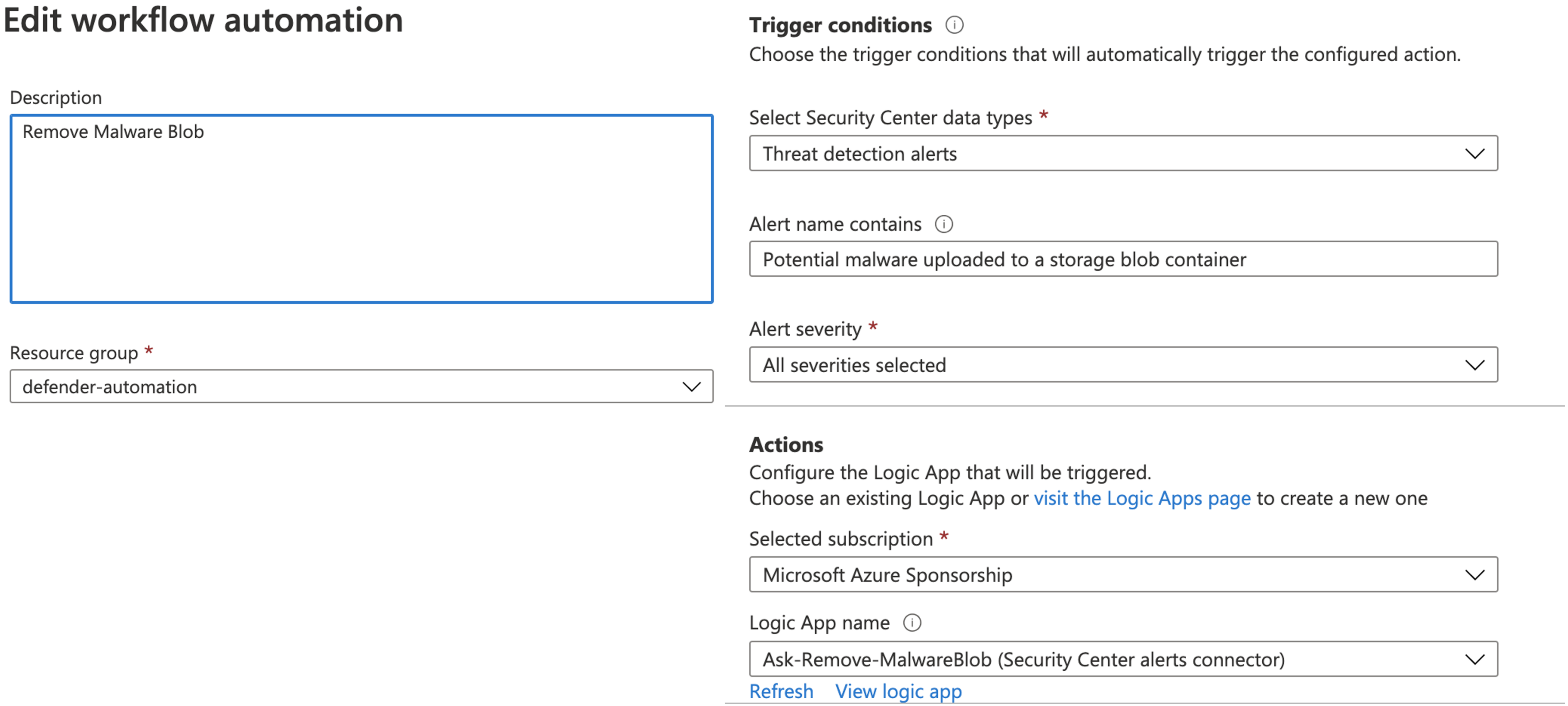
If request approved



Security Center | Workflow automation

Showing subscription 'Microsoft Azure Sponsorship'

	Name	Status	Scope	Trigger Type	Description	Logic App
□	Ask-Remove-MalwareB···	Enabled	Microsoft Azure Sponsorship	Security Center alert	Remove Malware Blob	Ask-Remove-MalwareBl···



Edit workflow automation

Description

Remove Malware Blob

Resource group *

defender-automation

Trigger conditions ⓘ

Choose the trigger conditions that will automatically trigger the configured action.

Select Security Center data types *

Threat detection alerts

Alert name contains ⓘ

Potential malware uploaded to a storage blob container

Alert severity *

All severities selected

Actions

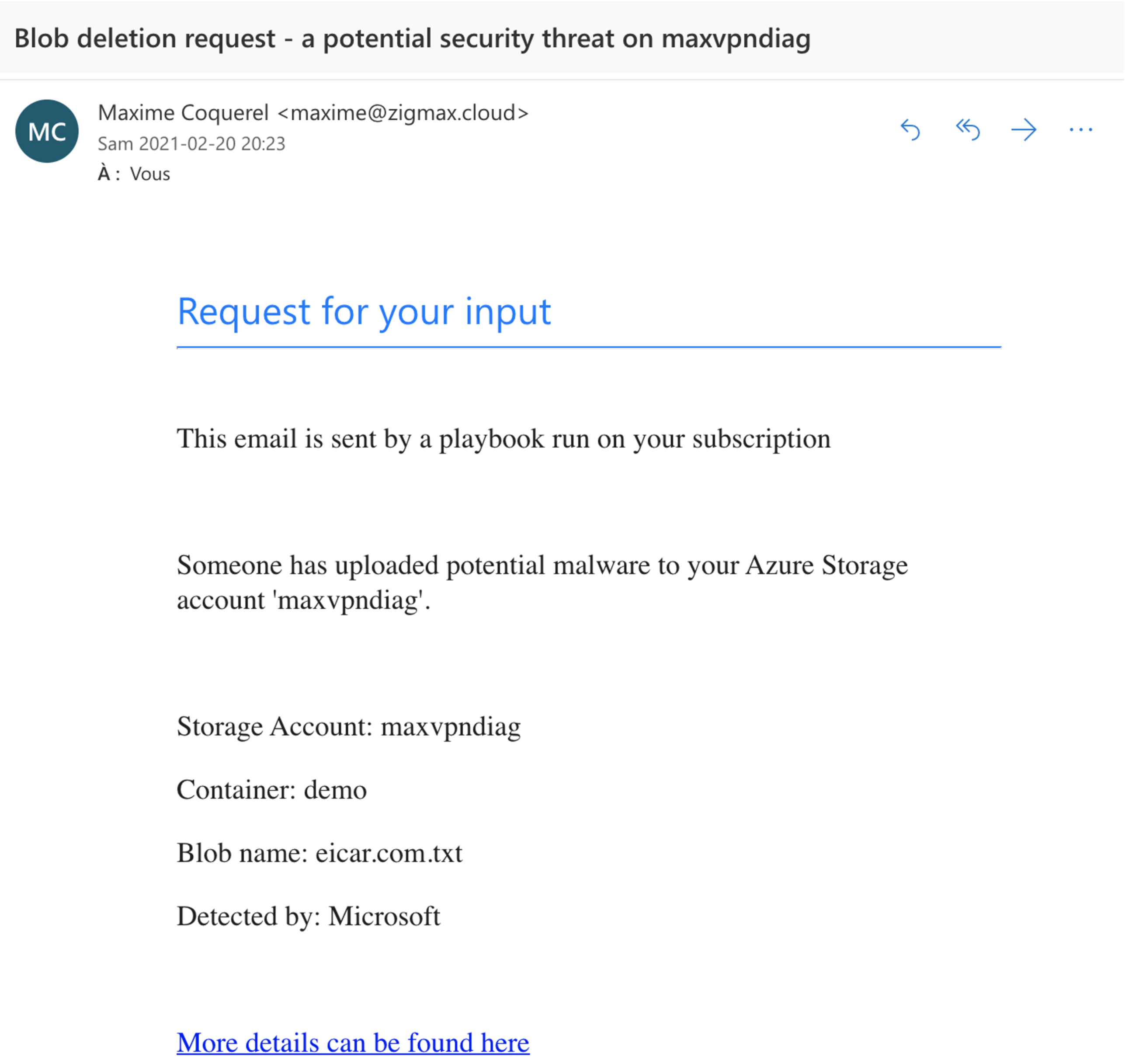
Configure the Logic App that will be triggered.
Choose an existing Logic App or visit the Logic Apps page to create a new one

Selected subscription *

Microsoft Azure Sponsorship

Logic App name ⓘ

Ask-Remove-MalwareBlob (Security Center alerts connector)



Blob deletion request - a potential security threat on maxvpndiag

Maxime Coquerel <maxime@zigmax.cloud>
Sam 2021-02-20 20:23
À : Vous

Request for your input

This email is sent by a playbook run on your subscription

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

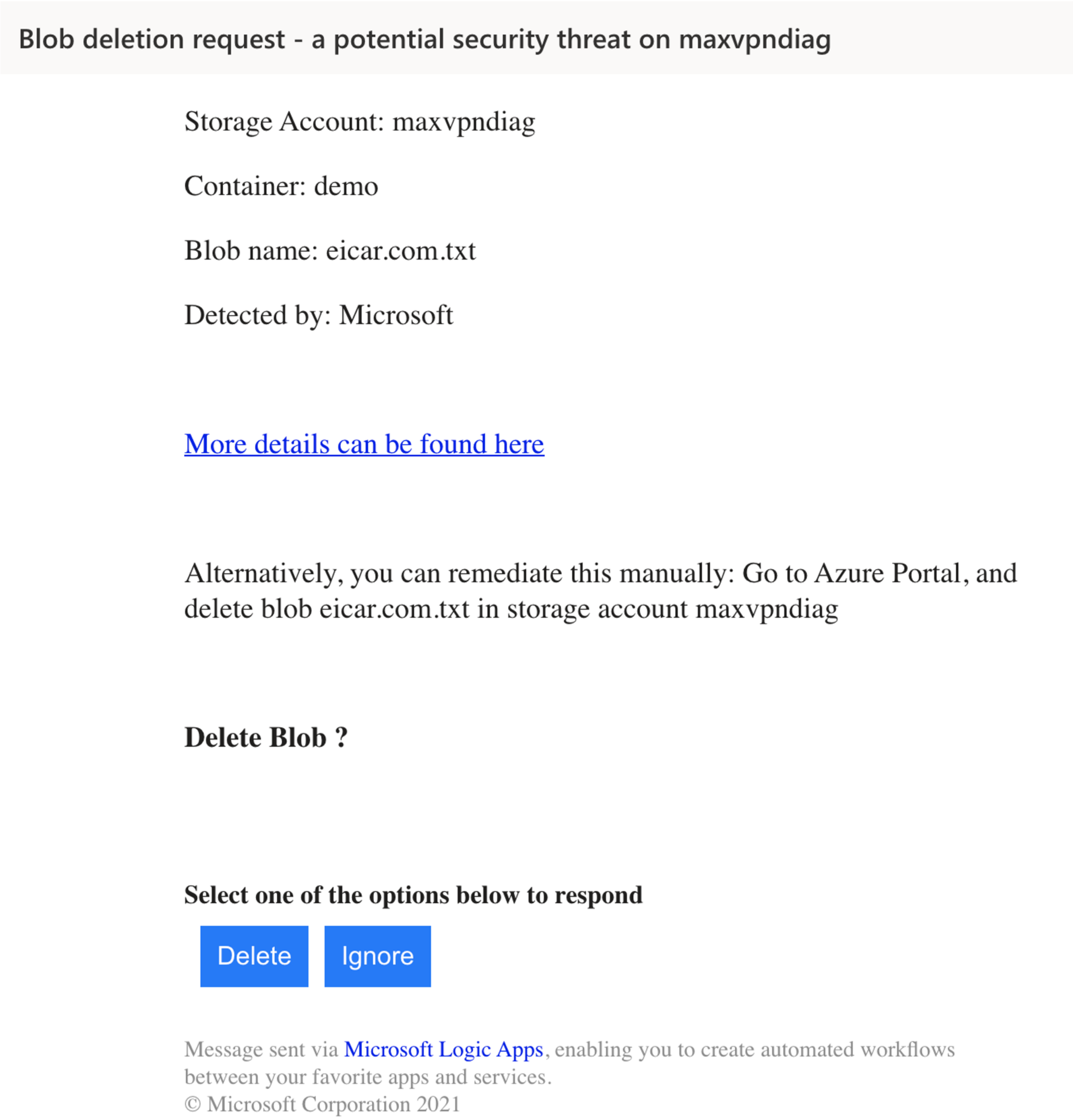
Storage Account: maxvpndiag

Container: demo

Blob name: eicar.com.txt

Detected by: Microsoft

More details can be found here



Blob deletion request - a potential security threat on maxvpndiag

Storage Account: maxvpndiag

Container: demo

Blob name: eicar.com.txt

Detected by: Microsoft

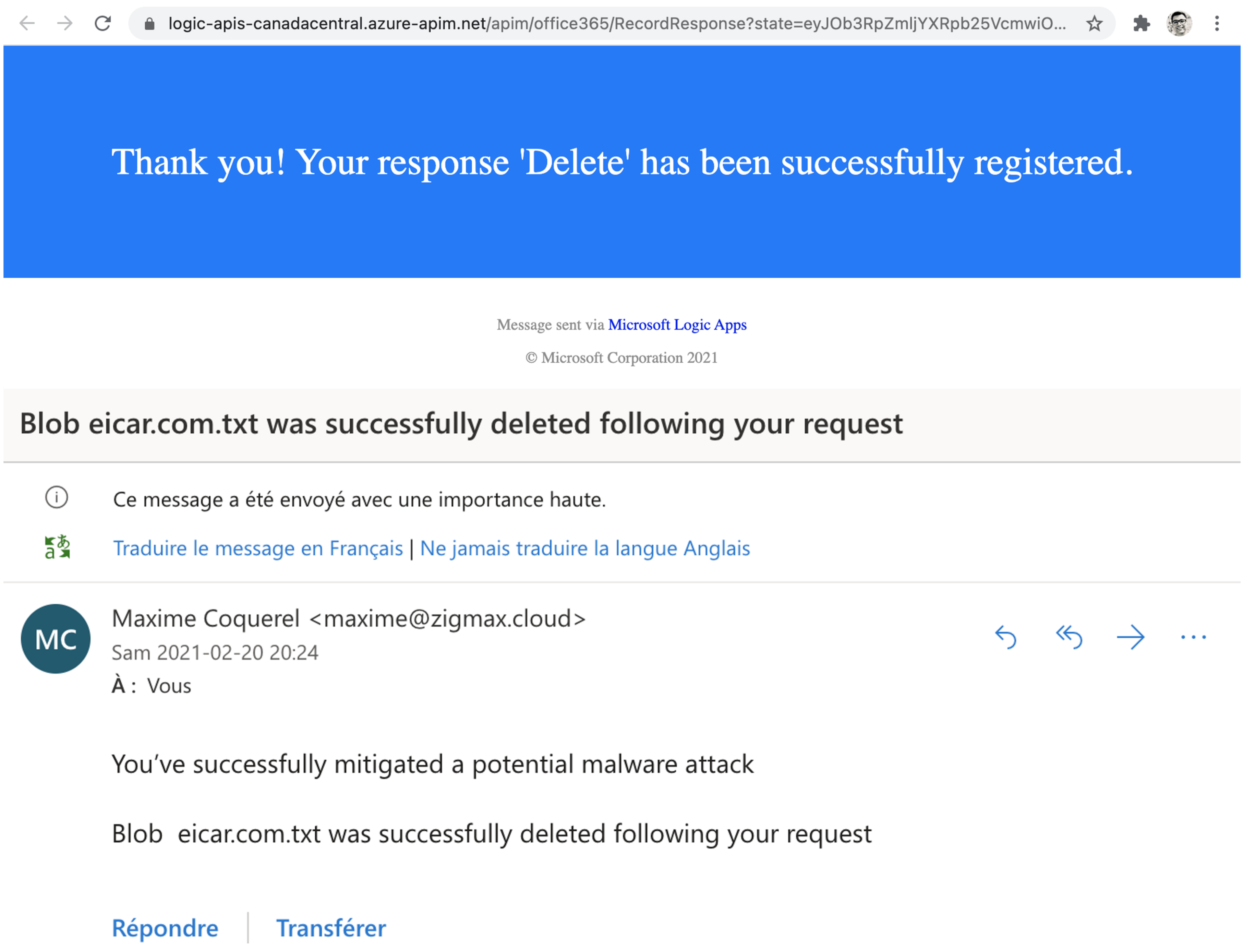
More details can be found here

Alternatively, you can remediate this manually: Go to Azure Portal, and delete blob eicar.com.txt in storage account maxvpndiag

Delete Blob ?

Select one of the options below to respond

Message sent via Microsoft Logic Apps, enabling you to create automated workflows between your favorite apps and services.
© Microsoft Corporation 2021



logic-apis-canadacentral.azure-apim.net/apim/office365/RecordResponse?state=eyJOb3RpZmljYXRpb25VcmwiO...

Thank you! Your response 'Delete' has been successfully registered.

Message sent via Microsoft Logic Apps

© Microsoft Corporation 2021

Blob eicar.com.txt was successfully deleted following your request

Ce message a été envoyé avec une importance haute.

Traduire le message en Français | Ne jamais traduire la langue Anglais

MC

Maxime Coquerel <maxime@zigmax.cloud>

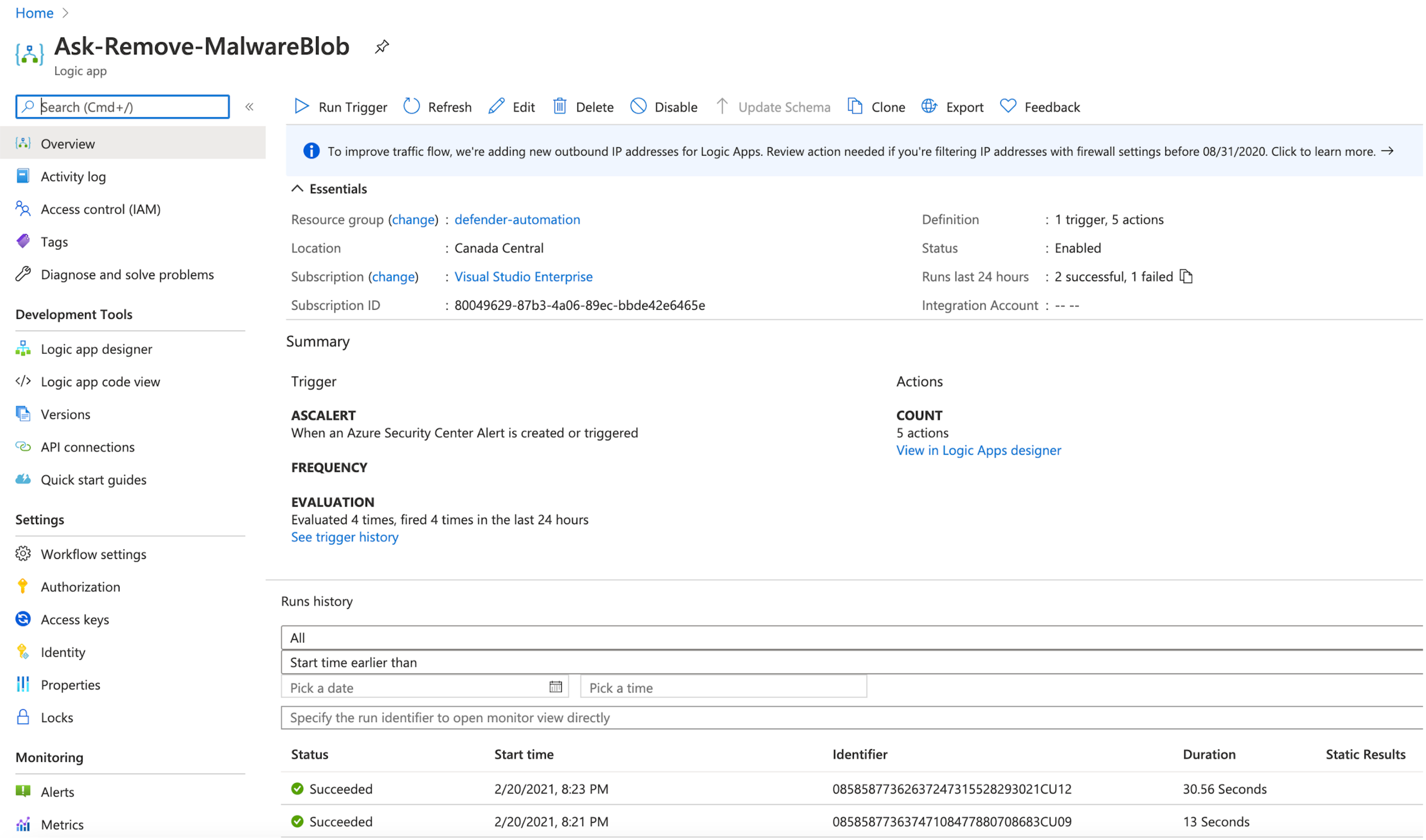
Sam 2021-02-20 20:24

À : Vous

You've successfully mitigated a potential malware attack

Blob eicar.com.txt was successfully deleted following your request

Répondre | Transférer



Ask-Remove-MalwareBlob

Logic app

To improve traffic flow, we're adding new outbound IP addresses for Logic Apps. Review action needed if you're filtering IP addresses with firewall settings before 08/31/2020. Click to learn more. →

Essentials

Resource group (change)	: defender-automation	Definition	: 1 trigger, 5 actions
Location	: Canada Central	Status	: Enabled
Subscription (change)	: Visual Studio Enterprise	Runs last 24 hours	: 2 successful, 1 failed
Subscription ID	: 80049629-87b3-4a06-89ec-bbde42e6465e	Integration Account	: -- --

Summary

Trigger

ASCALERT
When an Azure Security Center Alert is created or triggered

FREQUENCY

EVALUATION
Evaluated 4 times, fired 4 times in the last 24 hours
See trigger history

Actions

COUNT
5 actions
View in Logic Apps designer

Runs history

All

Start time earlier than

Pick a date

Pick a time

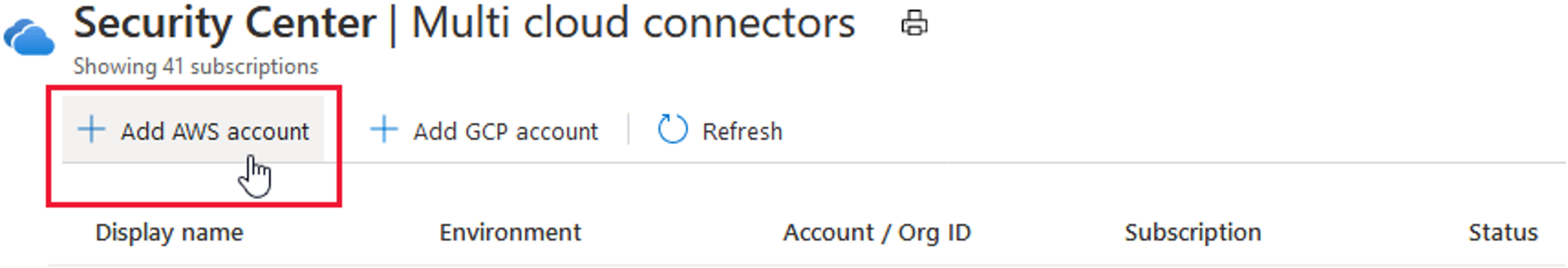
Specify the run identifier to open monitor view directly

Status	Start time	Identifier	Duration	Static Results
✓ Succeeded	2/20/2021, 8:23 PM	08585877362637247315528293021CU12	30.56 Seconds	
✓ Succeeded	2/20/2021, 8:21 PM	08585877363747108477880708683CU09	13 Seconds	

#GlobalAzureTO

Azure Security Center - Multi Cloud

Azure Security Center - Multi Cloud



Security Center | Multi cloud connectors

Showing 41 subscriptions

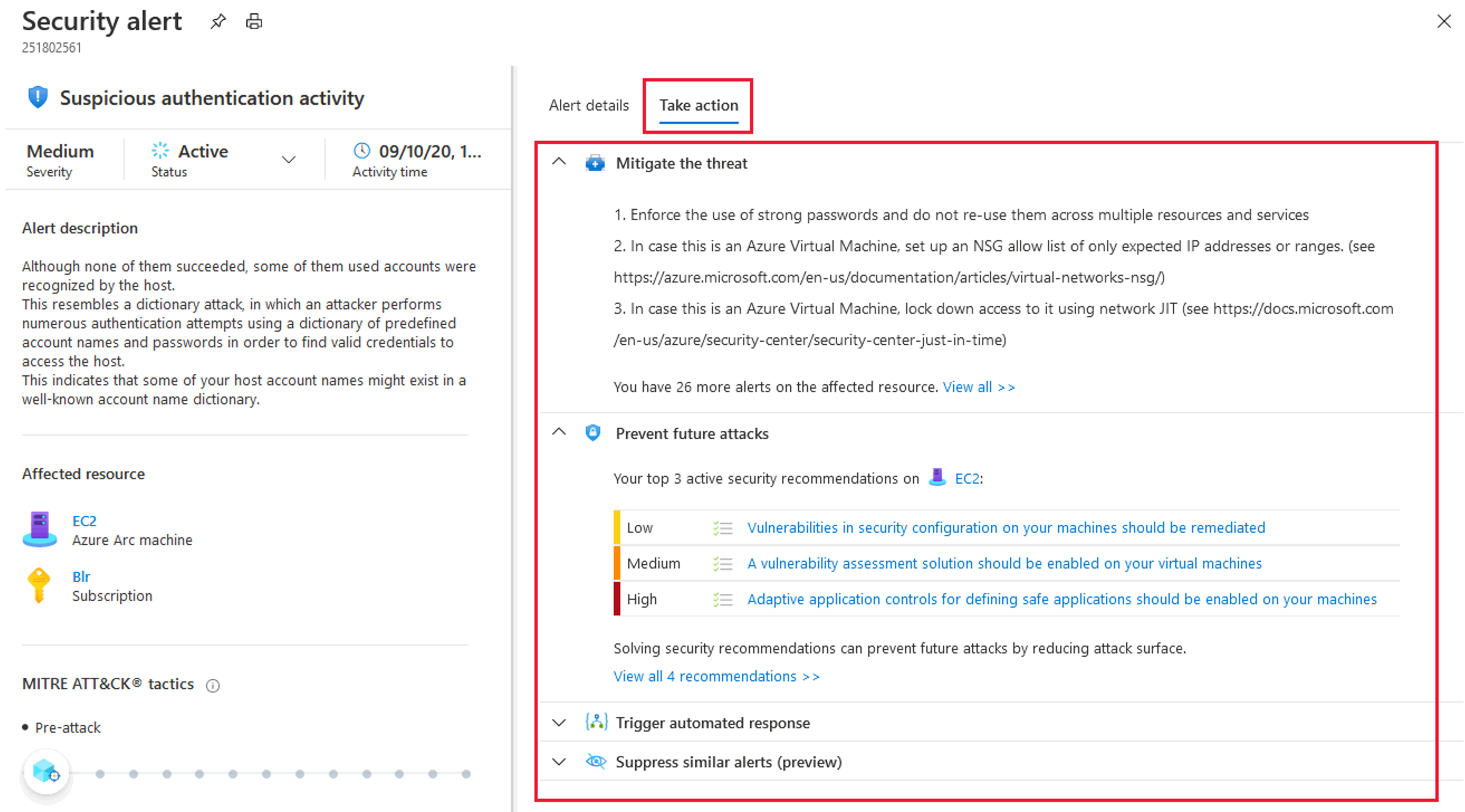
Display name	Environment	Account / Org ID	Subscription	Status

- Automatic agent provisioning (Security Center uses Azure Arc to deploy the Log Analytics agent to your AWS instances)
- Policy management
- Vulnerability management
- Embedded Endpoint Detection and Response (EDR)
- Detection of security misconfigurations
- A single view showing Security Center recommendations and AWS Security Hub findings
- Incorporation of your AWS resources into Security Center's secure score calculations
- Regulatory compliance assessments of your AWS resources

Search recommendations

Group by controls: On

Controls	Unhealthy resources	Resource Health
Remediate vulnerabilities	42 of 63 resources	🟥🟩⬜
Enable encryption at rest	31 of 39 resources	🟥🟩⬜
Remediate security configurations	29 of 38 resources	🟥🟩
Apply system updates	9 of 39 resources	🟥🟩
Apply adaptive application control	13 of 33 resources	🟥🟩
Enable auditing and logging	29 of 33 resources	🟥🟩
Auditing on SQL server should be enabled Quick Fix!	4 of 7 SQL servers	🟥🟩
Diagnostic logs in Data Lake Analytics should be enabled Quick Fix!	1 of 1 data lake analytics acco…	🟥
Diagnostic logs in IoT Hub should be enabled Quick Fix!	1 of 1 IoT Hubs	🟥
Ensure CloudTrail is enabled in all regions AWS Preview	3 of 3 AWS resources	🟥
Ensure CloudTrail trails are integrated with Amazon Cl... AWS Preview	1 of 3 AWS resources	🟥🟩
Ensure AWS Config is enabled in all regions AWS Preview	3 of 3 AWS resources	🟥
Ensure S3 bucket access logging is enable... ✓ Completed AWS Preview	None	🟩
Ensure VPC flow logging is enabled in all VPCs AWS Preview	5 of 5 AWS resources	🟥
Ensure a log metric filter and alarm exist for unauthor... AWS Preview	3 of 3 AWS resources	🟥



Security alert

251802561

Suspicious authentication activity

Medium Severity	Active Status
09/10/20, 1... Activity time	

Alert description

Although none of them succeeded, some of them used accounts were recognized by the host.
This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials to access the host.
This indicates that some of your host account names might exist in a well-known account name dictionary.

Affected resource

EC2
Azure Arc machine

Blr
Subscription

MITRE ATT&CK® tactics

- Pre-attack

Mitigate the threat

1. Enforce the use of strong passwords and do not re-use them across multiple resources and services

2. In case this is an Azure Virtual Machine, set up an NSG allow list of only expected IP addresses or ranges. (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/)

3. In case this is an Azure Virtual Machine, lock down access to it using network JIT (see https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time)

You have 26 more alerts on the affected resource. View all >>

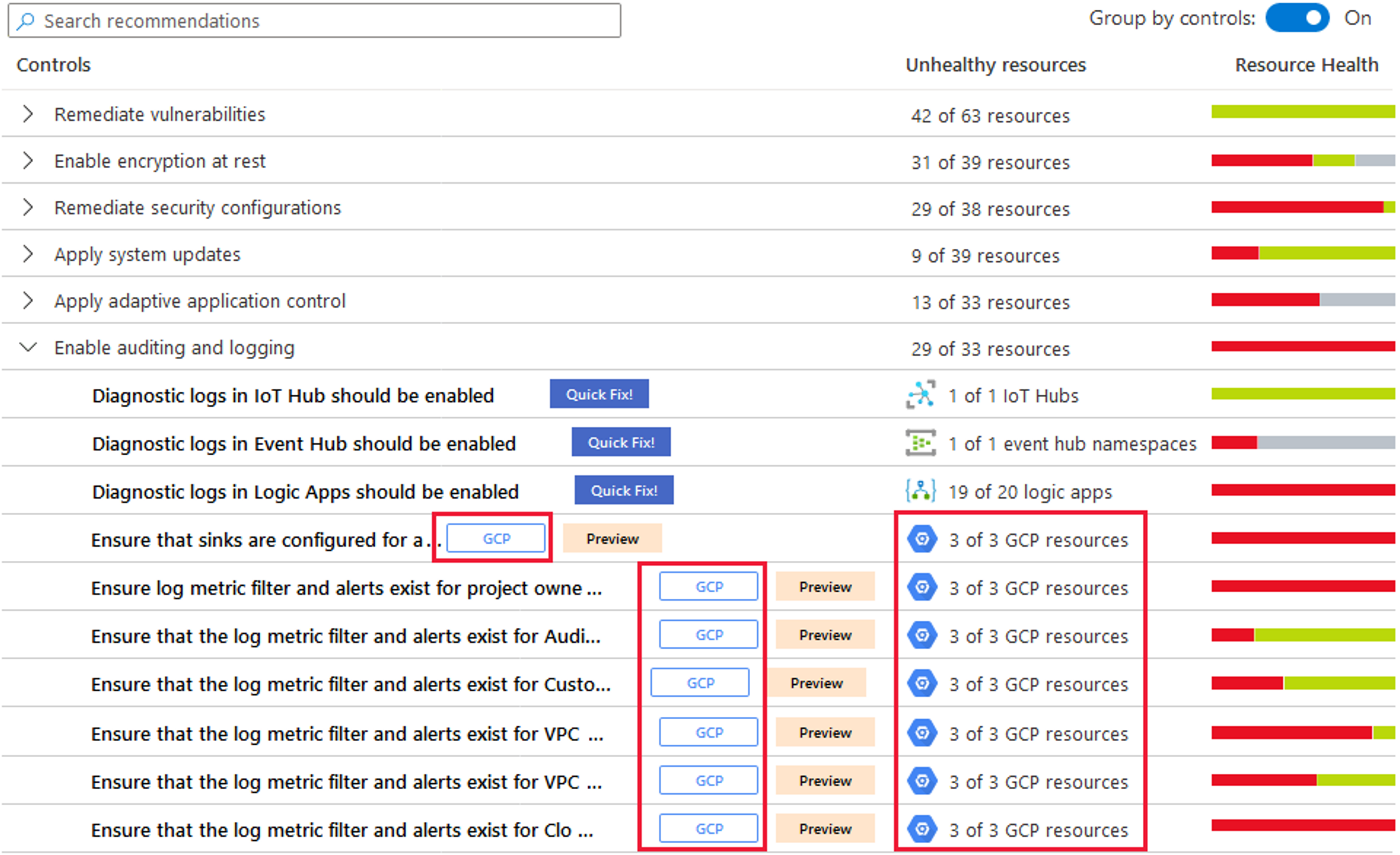
Prevent future attacks

Your top 3 active security recommendations on EC2:

Low	Vulnerabilities in security configuration on your machines should be remediated
Medium	A vulnerability assessment solution should be enabled on your virtual machines
High	Adaptive application controls for defining safe applications should be enabled on your machines

Solving security recommendations can prevent future attacks by reducing attack surface.

View all 4 recommendations >>



Search recommendations

Group by controls: On

Controls			Unhealthy resources	Resource Health
› Remediate vulnerabilities			42 of 63 resources	🟩
› Enable encryption at rest			31 of 39 resources	🟥🟩⬜
› Remediate security configurations			29 of 38 resources	🟥🟩
› Apply system updates			9 of 39 resources	🟥🟩
› Apply adaptive application control			13 of 33 resources	🟥⬜
⌄ Enable auditing and logging			29 of 33 resources	🟥
Diagnostic logs in IoT Hub should be enabled	Quick Fix!		1 of 1 IoT Hubs	🟩
Diagnostic logs in Event Hub should be enabled	Quick Fix!		1 of 1 event hub namespaces	🟥⬜
Diagnostic logs in Logic Apps should be enabled	Quick Fix!		19 of 20 logic apps	🟥
Ensure that sinks are configured for a ..	GCP	Preview	3 of 3 GCP resources	🟥
Ensure log metric filter and alerts exist for project owne ...	GCP	Preview	3 of 3 GCP resources	🟥
Ensure that the log metric filter and alerts exist for Audi...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for Custo...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for VPC ...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for VPC ...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for Clo ...	GCP	Preview	3 of 3 GCP resources	🟥

Microsoft CERTIFIED ASSOCIATE

Microsoft Certified: Security Operations Analyst Associate

SC-200

Mitigate threats using Microsoft 365 Defender (25-30%)

- Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365
- Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint
- Detect, investigate, respond, and remediate identity threats
- Manage cross-domain investigations in Microsoft 365 Defender Portal

Mitigate threats using Azure Defender (25-30%)

- Design and configure an Azure Defender implementation
- Plan and implement the use of data connectors for ingestion of data sources in Azure Defender
- Manage Azure Defender alert rules
- Configure automation and remediation
- Investigate Azure Defender alerts and incidents

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Myp3

Microsoft Certified: Security Operations Analyst Associate

SC-200

Mitigate threats using Azure Sentinel (40-45%)

- Design and configure an Azure Sentinel workspace
- Plan and Implement the use of Data Connectors for Ingestion of Data Sources in Azure Sentinel
- Manage Azure Sentinel analytics rules
- Configure Security Orchestration Automation and Remediation (SOAR) in Azure Sentinel
- Manage Azure Sentinel Incidents
- Use Azure Sentinel workbooks to analyze and interpret data
- Hunt for threats using the Azure Sentinel portal

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Myp3

Microsoft Certified: Azure Security Engineer Associate

AZ-500

Manage identity and access (30-35%)

- Manage Azure Active Directory identities
- Configure secure access by using Azure AD
- Manage application access
- Manage access control

Implement platform protection (15-20%)

- Implement advanced network security
- Configure advanced security for compute

Manage security operations (25-30%)

- Monitor security by using Azure Monitor
- Monitor security by using Azure Security Center
- Monitor security by using Azure Sentinel
- Configure security policies

Secure data and applications (20-25%)

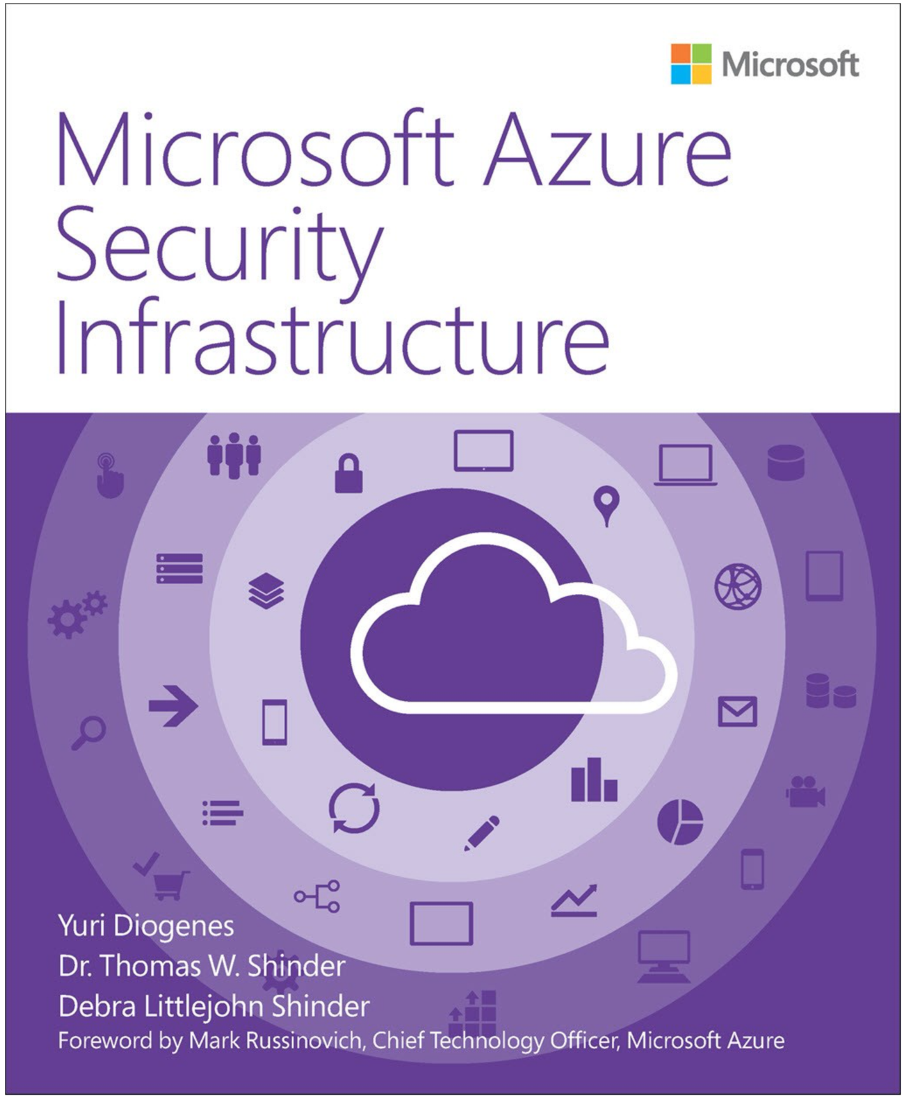
- Configure security for storage
- Configure security for databases
- Configure and manage Key Vault

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VC70

Technical Resources

- Microsoft Ignite 2020 - https://myignite.microsoft.com/home
- Microsoft Technical Community Content
  https://github.com/Microsoft/TechnicalCommunityContent
- Azure Security Blog - https://azure.microsoft.com/en-us/blog/topics/security/
- Maxime Blog - https://zigmax.net

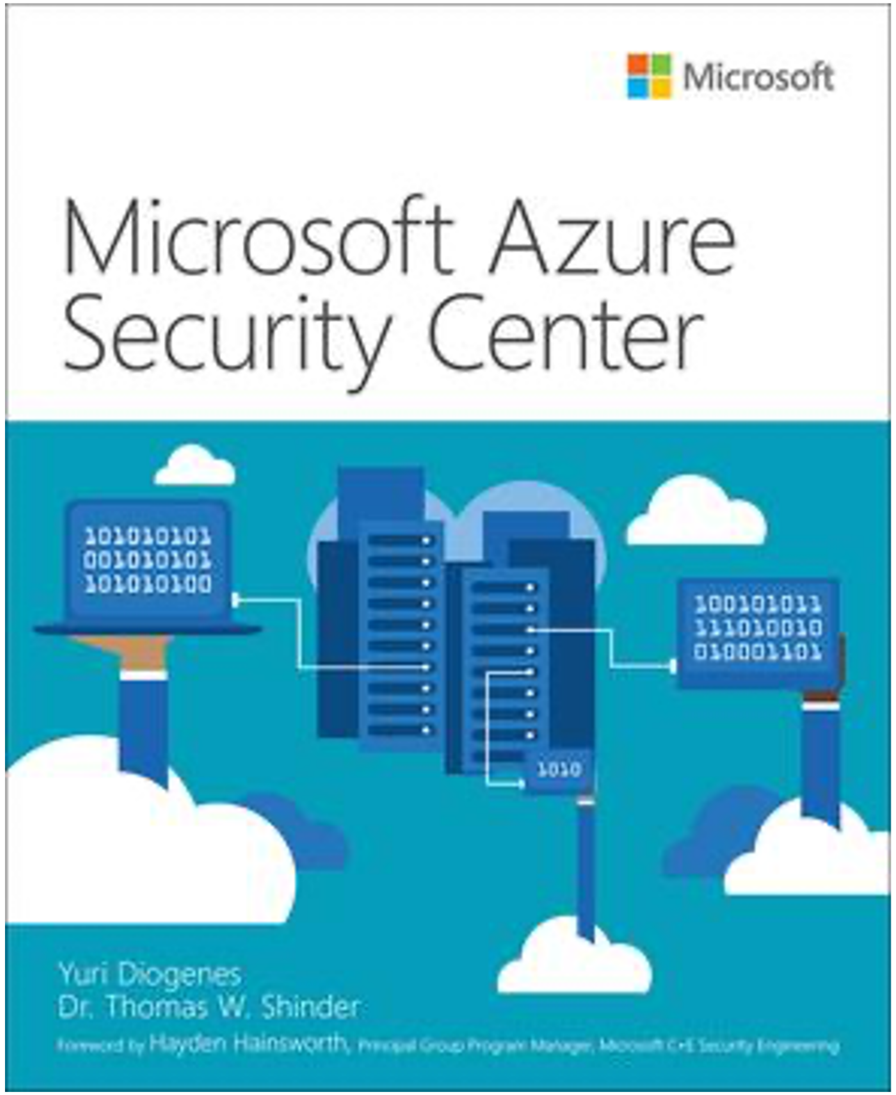
Books



Microsoft

Microsoft Azure Security Infrastructure

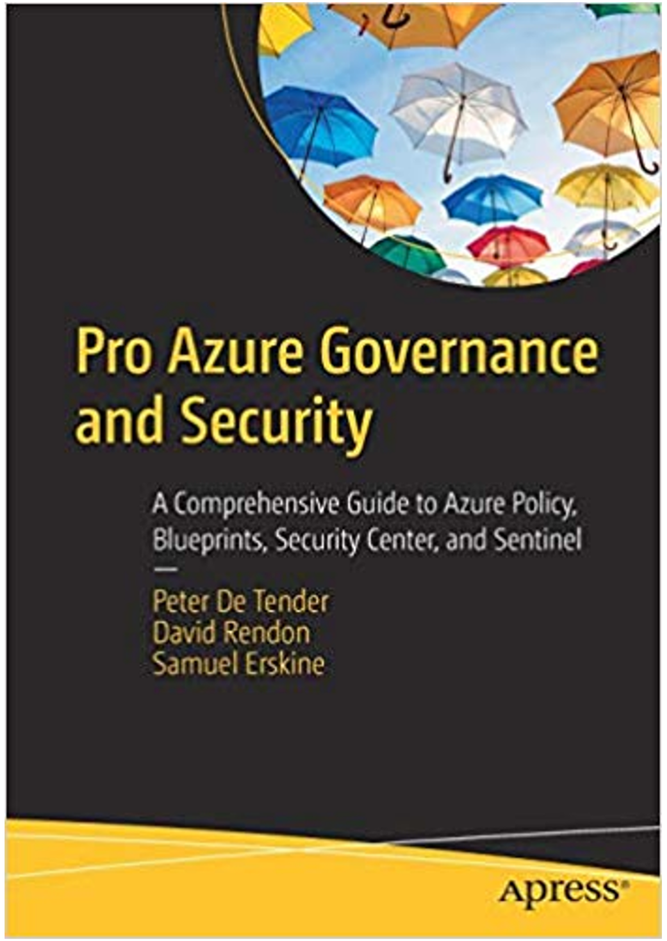
Yuri Diogenes
Dr. Thomas W. Shinder
Debra Littlejohn Shinder
Foreword by Mark Russinovich, Chief Technology Officer, Microsoft Azure



Microsoft

Microsoft Azure Security Center

Yuri Diogenes
Dr. Thomas W. Shinder
Foreword by Hayden Hainsworth, Principal Group Program Manager, Microsoft C+E Security Engineering



Pro Azure Governance and Security

A Comprehensive Guide to Azure Policy, Blueprints, Security Center, and Sentinel

Peter De Tender
David Rendon
Samuel Erskine

Apress®

Questions / Talks

• BY COMMUNITY • FOR COMMUNITY •

#GLOBALAZURE

2021