

Azure Defender in Action!

Maxime Coquerel - MVP Azure



Speaker

Maxime Coquerel

Director Cloud Security Architecture

Email : max.coquerel@live.fr

Blog : zigmax.net (since 2012)

Github : <https://github.com/zigmax>

Twitter : [@zig_max](https://twitter.com/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.”

Thanks!

meetup



THE AZURE GROUP
Azure User Community – Toronto

Réseau **Azure Tech Groups** – 243 groupes ?

The Azure Group (Azure User Community)

📍 Toronto, ON

👤 1798 membres · Groupe public ?

👤 Organisé par The Azure Group et 4 autres personnes

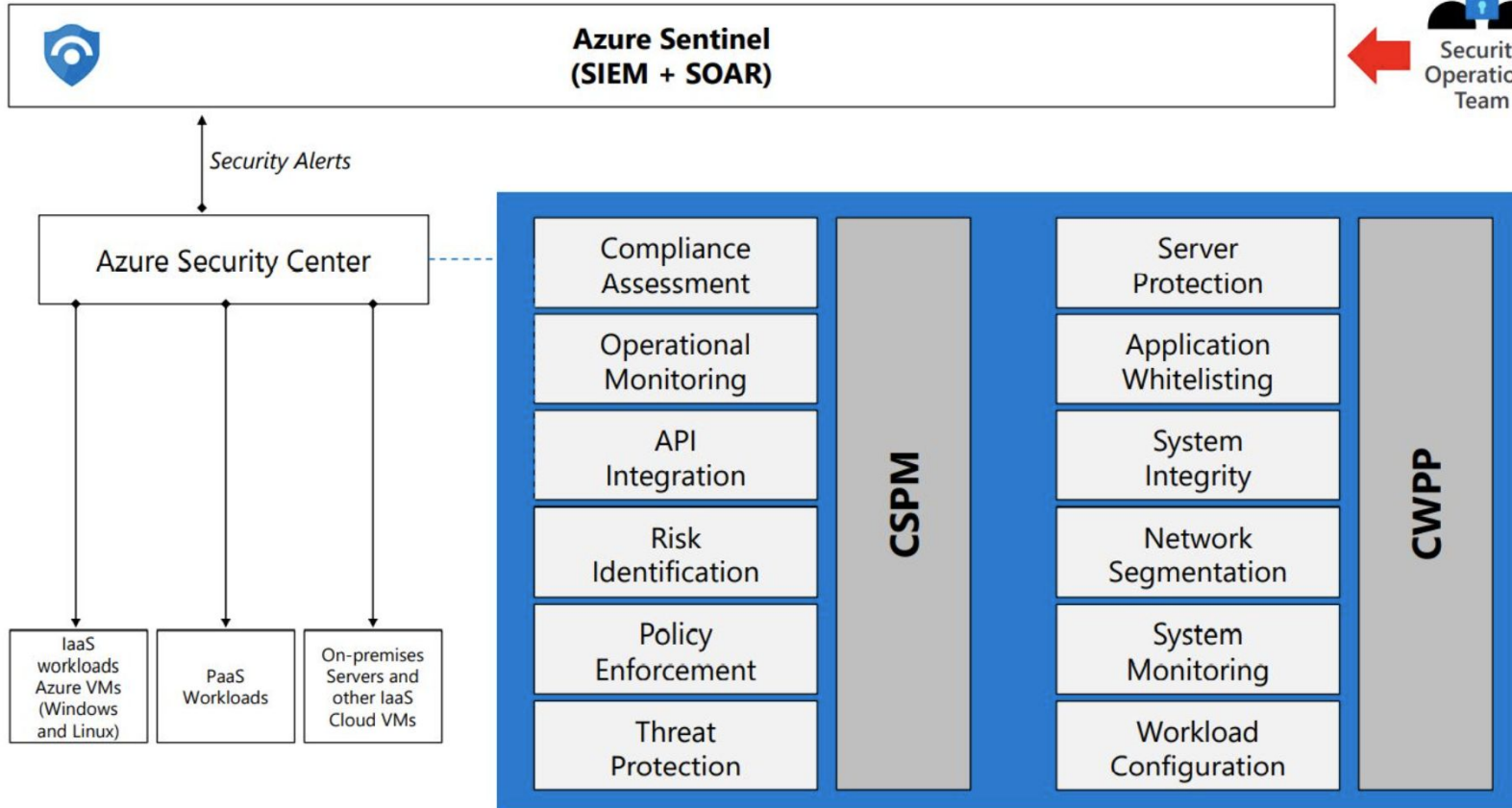
Partager : [!\[\]\(aa53ad6fea213b8b2226d3077e30533a_img.jpg\)](#) [!\[\]\(a1c2189b125458bd8fa8822d0c2da6bc_img.jpg\)](#) [!\[\]\(2fd953c3ecfc88f2692d4bd02c4e8bdc_img.jpg\)](#)

Session Agenda / Goal

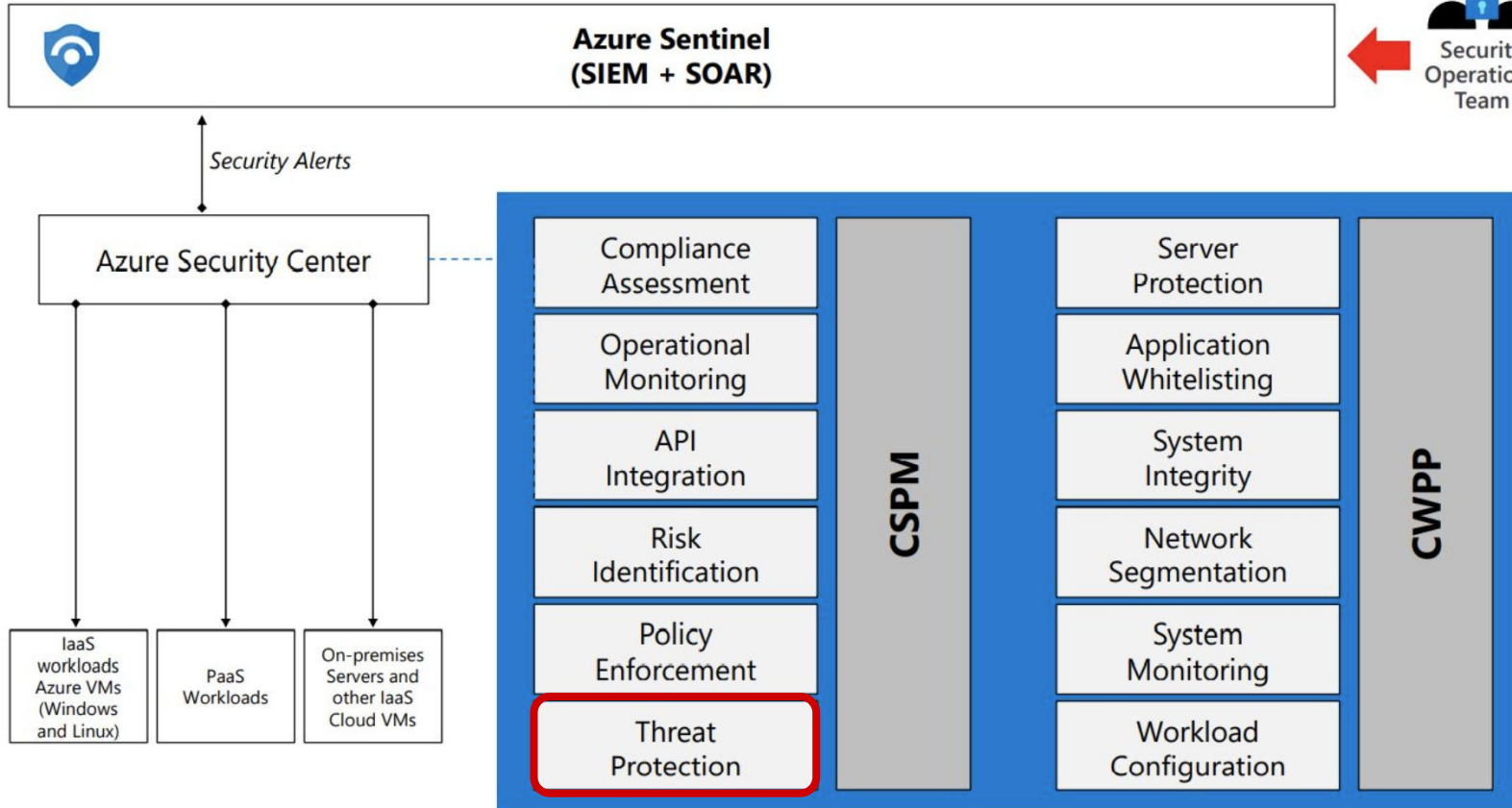
- Azure Security Overview
- Azure Defender
- Examples of Azure Defender Alerts
- Suspicious incoming RDP network activity
- Export - Alerts to SIEM
- Alert - Notification
- Alert Simulation
- Azure Graph
- Alert Automation
- Azure Defender for IoT
- Azure Security Center - Multi Cloud



Azure Security Overview



Azure Security Overview



 **41**
Azure subscriptions

 **1**
AWS accounts

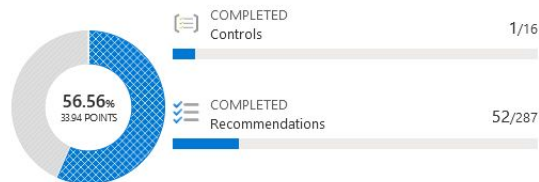
 **3**
GCP projects

 **235**
Active recommendations

 **112**
Security alerts

Secure score

Current secure score



[Improve your secure score >](#)

Compliance

Current compliance by passed controls



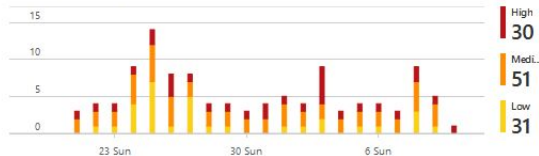
[Improve your compliance >](#)

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






[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 >](#)

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



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

Security alerts



Advanced protection

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

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

Most attacked resources

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

High severity VM vulnerabilities

No information to show

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			

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



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



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	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
App services	4 instances	\$ x/Instance/Month	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Azure SQL database servers	7 servers	\$ x/Server/Month	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
SQL servers on machines (Pre...	0 servers	FREE during preview	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Storage	54 storage accounts	\$ x/10k transactions	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Kubernetes	20 kubernetes cores	\$ x/VM core/Month	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Container registries	2 container registries	\$ x/Image	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Key vault	4 key vaults	\$ x/10k transactions	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off

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

Security alerts

[Refresh](#) [Change status](#) [Open query](#) | [Suppression rules](#) [Security alerts map](#) [Sample alerts](#) [Download CSV report](#) | [Guides & Feedback](#)

[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




[Subscription == All](#) [Status == Active](#) [Severity == Low, Medium, High](#) [Add filter](#)

No grouping

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

Security alerts

« Refresh Change status ▾ Open query | Suppression rules Security alerts map Sample alerts Download CSV report

 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 X

Severity == Low, Medium, High X

<input type="checkbox"/> Severity ↑↓	Alert title ↑↓	Affected resource ↑↓	Activity start time (UTC+2) ↑↓
<input type="checkbox"/> Low	 Suspicious incoming RDP network activity	 DC1	02/14/21, 11:00 PM

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

Add filter

No grouping

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

View full details

Take action

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


Security alert

251788964399999999_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

Alert details

Take action

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**

Analytics rule wizard - Edit existing rule

Create incidents based on Azure Security Center alerts

General Review and create

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

**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](#)

[Investigate](#)

Alerts | [Bookmarks](#) | [Entities](#) | [Comments](#)

Severity : **All**

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/>

```

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

```

Results | Chart | Columns ▾ | Add bookmark | Display time (UTC+00:00) ▾ | Group columns

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	<p>Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to 104.40.207.109, associated with your resource DC1.</p> <p>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 res</p> <p>Specifically, sampled network data shows 125 incoming connections to your resource, which is considered abnormal for this environment.</p> <p>This activity may indicate an attempt to brute force your RDP end point</p>			
	ProviderName	Azure Security Center			

Azure Sentinel Threat Hunting

Brute Force RDP Attack

General Set rule logic Incident settings (Preview) Automated response Review and create

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
```

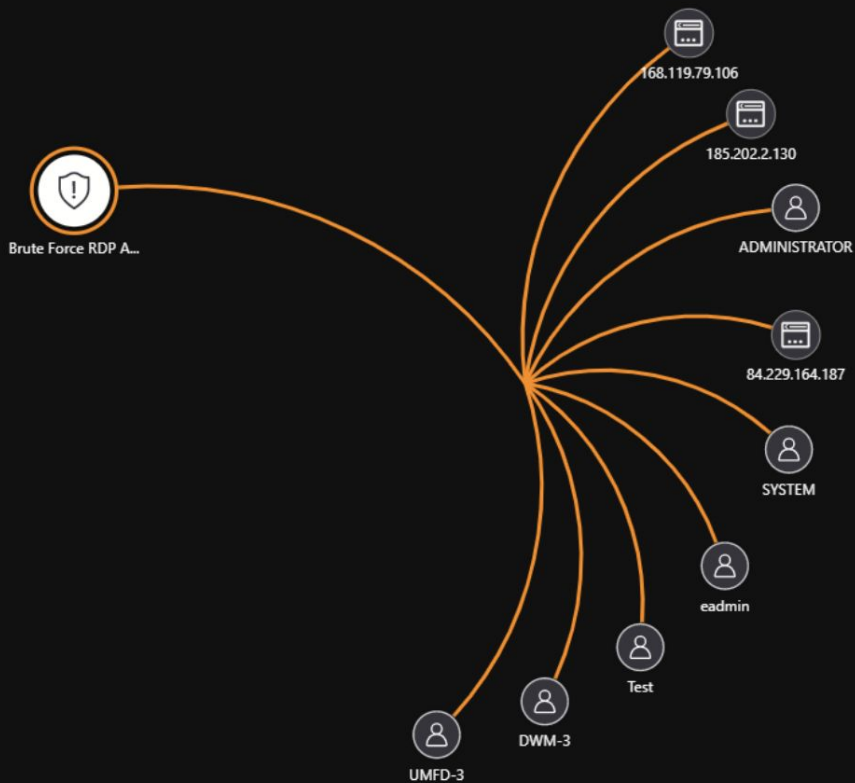
☐ Please wait while we evaluate your query...

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)

▶ Run

Time range : Last 24 hours

Save

Copy link

New alert rule

Export

Pin to dashboard

...

```
1 SecurityEvent
2 | where EventID == "4625"
3 | extend _Account = trim(@"^[^\\]+", Account)
4 | where SubStatus =~ "0xc000006a"
5 | project TimeGenerated,
6 |         Computer,
7 |         _Account,
8 |         LogonType,
9 |         LogonProcessName,
10 |        SubStatus,
11 |        Activity
12
```

Results

Chart

Columns

Add bookmark

Display time (UTC+00:00)

Group columns

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

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

i Saving data to event hub incurs ingestion charges, as detailed [here](#)>

Alert - Notification

[Home](#) > [Security Center](#) > [Settings](#)



Settings | Email notifications

Microsoft Azure Sponsorship



Save

Settings

Azure Defender plans

Auto provisioning

Email notifications

Threat detection

Workflow automation

Continuous export

Cloud connectors

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



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

[View the full alert >](#)

Azure Security Center has detected suspicious activity in your environment



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



[View the full alert >](#)

Slack

[Home](#) > [Microsoft.EmptyWorkflow | Overview](#) > [asc-notify](#) > Logic Apps Designer

Logic Apps Designer



 Save  Discard  Run  Designer  Code view  Parameters  Templates  Connectors  Help

 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](#)



Security Center | Workflow automation

Showing subscription 'Visual Studio Enterprise'

Search (Cmd+/)

+ Add workflow automation Refresh Enable Disable Delete Learn more

Overview

Getting started

Pricing & settings

Community

Workflow automation

Filter by name

Search Select... Enable...

Search T.: Security...

Name	↑↓	Status	↑↓	Scope	↑↓	Trigger Type	↑↓	Description	↑↓	Logic App	↑↓
<input type="checkbox"/> Workflow_ASC_Notify_Alerts		Enabled		Visual Studio Enterprise		Security Center alert		Owner: Maxime Alert: When an A...		asc-notify	

Nouveaux messages



Microsoft Azure Logic-Apps APPLI 18:09

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

Alert - Simulation

[Home](#) > [Security Center](#)



Security Center | Security alerts

Showing subscription 'Microsoft Azure Sponsorship'



Refresh

↔ Change status

🔗 Open query

🚫 Suppression rules

🗺 Security alerts map (Preview)

🛡 Create sample alerts

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 (Preview)



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



Subscription == All

Status == Active

Severity == Low, Medium, High

Time == Last month

Add filter

No grouping

<input type="checkbox"/>	Severity	Alert title	Affected resource	Activity start time (...)	MITRE ATT&...	Status
<input type="checkbox"/>	High	U... Sample alert	Sample-Storage	12/16/20, 02:55 PM	Exfiltration	Active
<input type="checkbox"/>	High	P... Sample alert	Sample-DB	12/16/20, 02:55 PM		Active
<input type="checkbox"/>	High	D... Sample alert	Sample-VM	12/16/20, 02:55 PM	Execution	Active
<input type="checkbox"/>	High	U... Sample alert	Sample-DB	12/16/20, 02:55 PM	Exfiltration	Active

< Previous

Page

1

of 1

Next >

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

[Home](#) > [Resource Graph queries](#) >

Azure Resource Graph Explorer

Search

- 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 ...

+ New query Open a query Run query Save Save as Feedback

Query 1 x Query 2 x

```
1 securityresources
2 | where type == "microsoft.security/locations/alerts"
3 | project
4   ['TimeGeneratedUtc'] = properties.TimeGeneratedUtc,
5   ['AlertName'] = properties.AlertDisplayName,
6   ['Severity'] = properties.Severity,
7   ['Intent'] = properties.Intent,
8   ['ResourceId'] = (toString(properties['ResourceIdentifiers'][0]['AzureResourceId']))
```

Get started Results Charts Messages

Download as CSV Pin to dashboard

Formatted results

Off

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

< Previous Page 1 of 1 Next >

Alert Automation

[Home](#) > [defender-automation](#) > [Ask-Remove-MalwareBlob](#)



Ask-Remove-MalwareBlob | Logic app designer

Logic app



Save



Discard



Run



Designer



Code view



Parameters



Templates

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Development Tools

Logic app designer

Logic app code view

Versions

API connections



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'

 Search (Cmd+/)

«

 Add workflow automation

 Refresh

|

 Enable

 Disable

 Delete

 Learn more

 Guides & Feedback

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

Filter by name

 Sel... En...

 T Securi...

Name	↑↓	Status	↑↓	Scope	↑↓	Trigger Type	↑↓	Description	↑↓	Logic App	↑↓
<input type="checkbox"/>  Ask-Remove-MalwareB...		 Enabled		Microsoft Azure Sponsorship		 Security Center alert		Remove Malware Blob		 Ask-Remove-MalwareBI...	

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)

[Refresh](#) [View logic app](#)

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

Delete

Ignore

Message sent via [Microsoft Logic Apps](#), enabling you to create automated workflows between your favorite apps and services.

© Microsoft Corporation 2021

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](#)



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

[Run Trigger](#) [Refresh](#) [Edit](#) [Delete](#) [Disable](#) [Update Schema](#) [Clone](#) [Export](#) [Feedback](#)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Development Tools

Logic app designer

Logic app code view

Versions

API connections

Quick start guides

Settings

Workflow settings

Authorization

Access keys

Identity

Properties

Locks

Monitoring

Alerts

Metrics

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](#)

Location : Canada Central

Subscription ([change](#)) : [Visual Studio Enterprise](#)

Subscription ID : 80049629-87b3-4a06-89ec-bbde42e6465e

Definition : 1 trigger, 5 actions

Status : Enabled

Runs last 24 hours : 2 successful, 1 failed

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



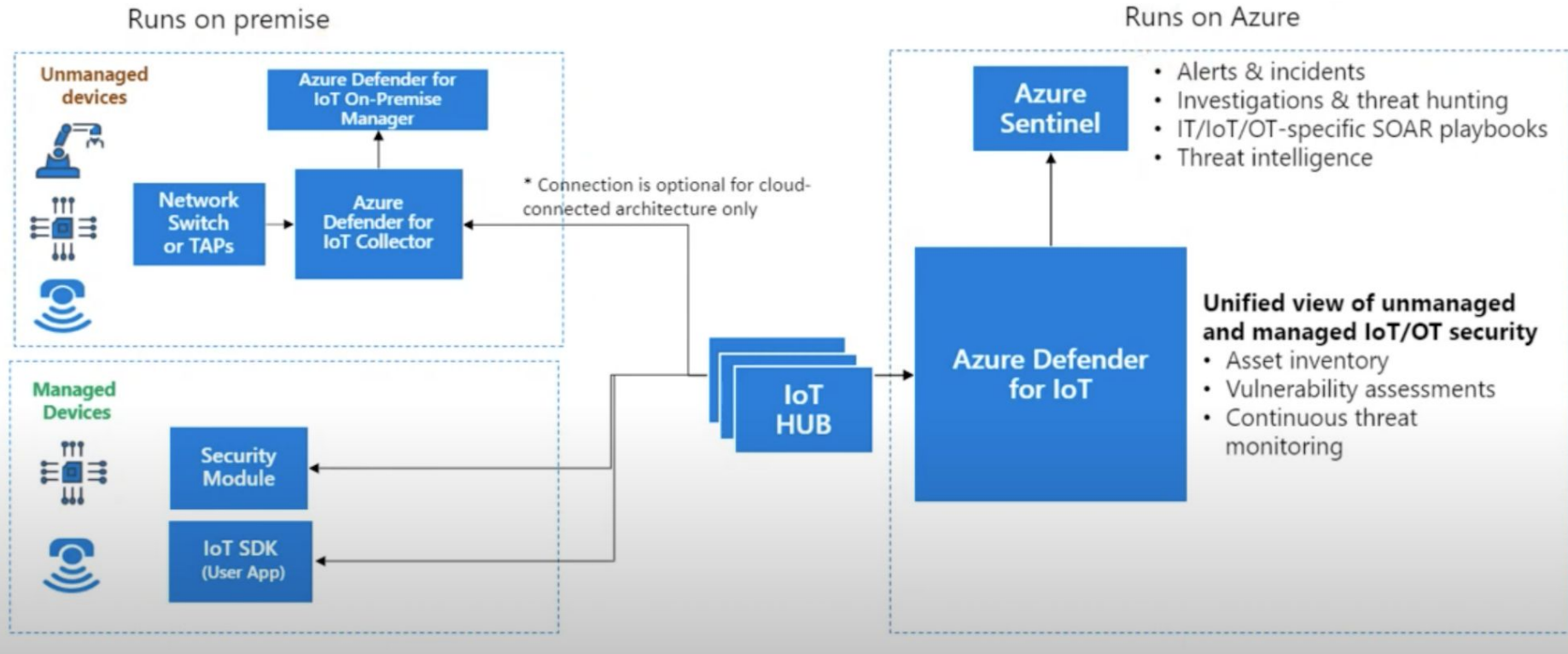
Pick a time

Specify the run identifier to open monitor view directly

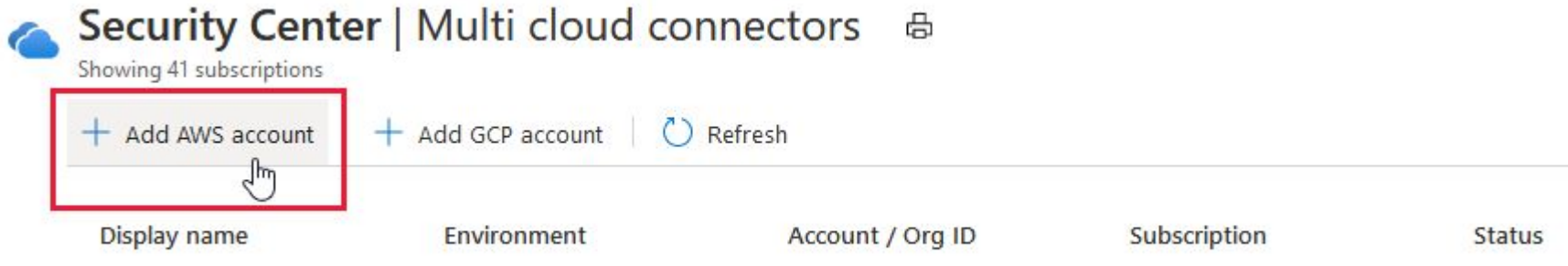
Status	Start time	Identifier	Duration	Static Results
✓ Succeeded	2/20/2021, 8:23 PM	08585877362637247315528293021CU12	30.56 Seconds	
✓ Succeeded	2/20/2021, 8:21 PM	08585877363747108477880708683CU09	13 Seconds	




Azure Defender for IoT



Azure Security Center - Multi Cloud













Security Center | Multi cloud connectors 

Showing 41 subscriptions

[+ Add AWS account](#) [+ Add GCP account](#) [Refresh](#)

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

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

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



Alert details

Take action



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 >>](#)



Trigger automated response



Suppress similar alerts (preview)

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



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



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



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

Vous regardez : Découvrir Azure Policy

Dans le cours : Microsoft Azure : La sécurité

31 150

Microsoft Azure

Contrôle et gouvernance actifs et à l'échelle pour vos ressources Azure

- Gérez vos ressources Azure avec simplicité
- Appliquez la gestion et la sécurité à l'échelle
- Appliquez des stratégies et auditez la conformité
- Effectuez le monitoring de la conformité en continu
- Créez des stratégies personnalisées avec flexibilité
- Appliquez des stratégies intégrées fournies par Microsoft et la communauté

Essayez-le dès maintenant

Ajoutez des stratégies à vos ressources

Vue d'ensemble Contenu Transcriptions Notes

3. Assurer la conformité

Découvrir Azure Policy

1 min 1 sec

Assigner une stratégie

2 min 31 sec

Valider le bon fonctionnement de la stratégie

1 min 36 sec

Connaître le résultat de la non-conformité

1 min 16 sec

4. Aborder la sécurité de l'infrastructure

Découvrir Network Security Groups

1 min 9 sec

Mettre en œuvre Network Security Groups

5 min 15 sec

Créer une passerelle applicative

3 min 39 sec

Configurer Application Gateway

4 min 52 sec

Mettre en place le pare-feu

3 min 3 sec

5. Administrer les identités

Gérer les identités avec Azure Active Directory

5 min 16 sec

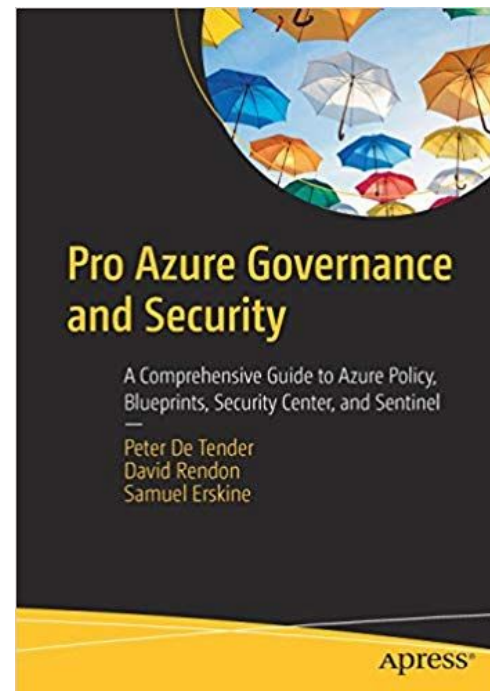
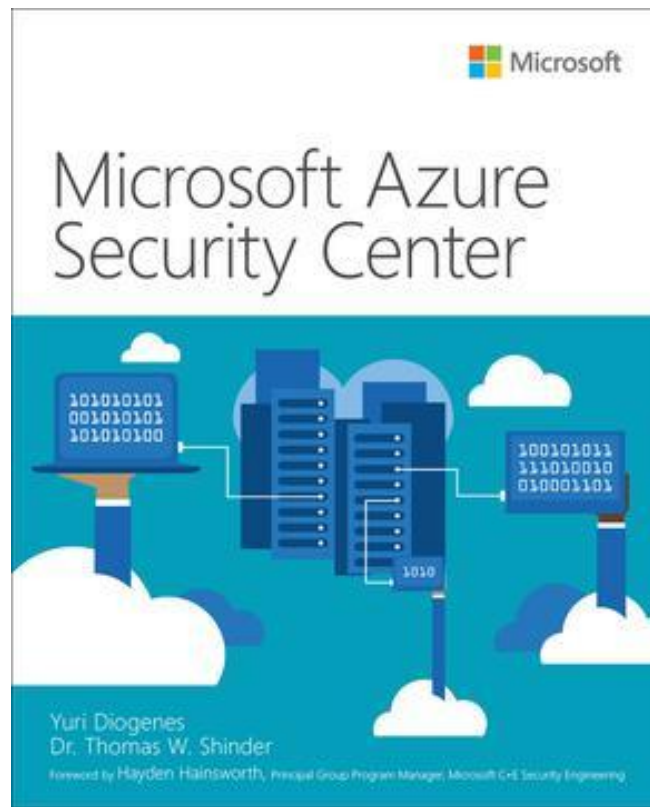
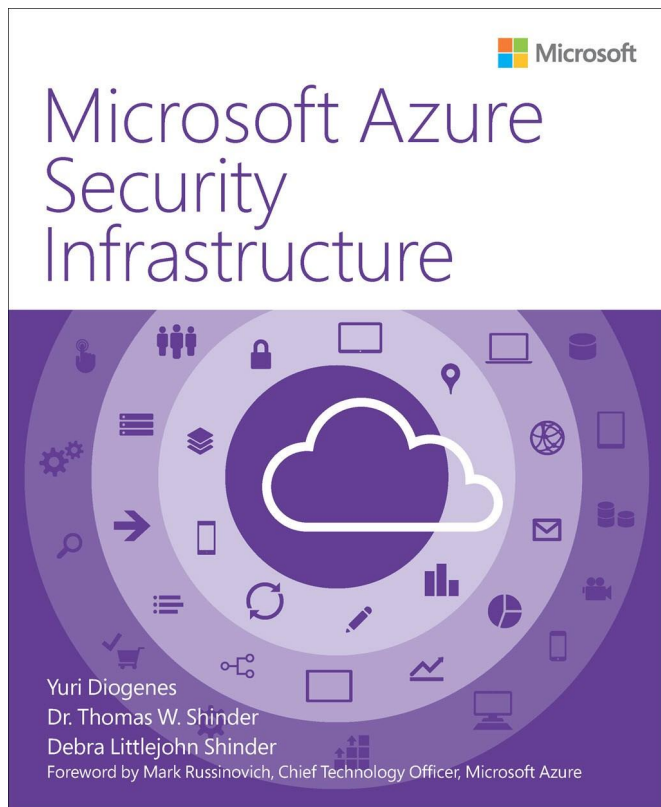
Créer un groupe

Aide/Commentaires

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 - <http://zigmax.net>

Books



Questions / Talks