Microsoft Sentinel SIEM Lab: Cloud-Native SOC Deployment & Telemetry Integration

Executive Summary

This documentation outlines the end-to-end configuration and deployment of Microsoft Sentinel within an Azure-based cloud security lab environment. The primary objective was to simulate a realistic SOC monitoring setup leveraging native Microsoft security solutions, custom telemetry ingestion, and external threat intelligence feeds.

Key components implemented include:

- **Role-based access control (RBAC)** to enforce least-privilege access using the `Microsoft Sentinel Contributor` role
- **Log Analytics workspace tuning**, including extended retention configurations for SecurityEvent data
- **Comprehensive Content Hub integrations** covering the Microsoft Defender XDR suite, Sysmon, Azure Activity, and CEF-based connectors
- **Custom log ingestion pipeline** using Azure Monitor Agent (AMA), data collection rules, and custom table definitions
- **Threat intelligence enrichment** via TAXII-based integration with PulseDive to stream STIX 2.x objects
- **Validation of alerting and data flow** using simulated security events from Microsoft Defender for Cloud

Throughout the configuration process, a cloud-native mindset was applied, emphasizing scalable telemetry ingestion, cost awareness, and integration readiness with a future SIEM/SOAR stack. Identified constraints—such as VM selection limitations and endpoint configuration mismatches—have been documented with root cause analysis and remediation plans.

This deployment serves as a baseline template for future enterprise Sentinel rollouts and Tier 1 SOC onboarding.

1. Role Assignment: Microsoft Sentinel Contributor

Objective: Grant Sentinel permissions to a specific user
Path:
`Azure Portal → Resource Groups → Secops_Projects → Access Control (IAM)`
Steps:

1. Selected **"Add role assignment"**
2. Role: `Microsoft Sentinel Contributor`
3. Assign access to: `User, group, or service principal`
4. Selected user account (self) under **Members**
5. Confirmed role assignment

Outcome:
User now appears under "Microsoft Sentinel Contributor" role assignments with permissions to manage Sentinel resources.

portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d640-40d1-b278-11b1bedcf8fe/resourceGr...

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | ohhno961@gmail.com DEFAULT DIRECTORY

Dashboard >

Sentinel-Defender-Lab

Log Analytics workspace

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs
- Resource visualizer
- Settings
- Classic
- Monitoring
- Automation
- Help

Delete

The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to Azure Monitor Agent

Essentials JSON View

Resource group (move)	: secops_projects
Status	: Active
Location	: East US 2
Subscription (move)	: Azure subscription 1
Subscription ID	: 632d7a25-d640-40d1-b278-11b1bed...
Workspace Name	: Sentinel-Defender-Lab
Workspace ID	: eab7b64f-a74e-4a35-b833-cc95298c9...
Pricing tier	: Pay-as-you-go
Access control mode	: Use resource or workspace permissions
Operational issues	: OK
Tags (edit)	: Add tags

Get Started | Recommendations

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to

Add or remove favorites by pressing Cmd+Shift+F

Notifications

More events in the activity log → Dismiss all

$161.65 credit remaining

Subscription 'Azure subscription 1' has a remaining credit of $161.65.

Upgrade to a Pay-As-You-Go subscription.

4 minutes ago

portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d640-40d1-b278-11b1bedcf8fe/resourceGr...

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | ohhno961@gmail.com DEFAULT DIRECTORY

Dashboard > Sentinel-Defender-Lab

Sentinel-Defender-Lab | Access control (IAM)

Log Analytics workspace

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs
- Resource visualizer
- Settings
- Classic
- Monitoring
- Automation
- Help

Add | Download role assignments | Edit columns | Refresh

Check access | Role assignments | Roles | Deny assignments

Number of role assignments for this subscription

4 4000

Search by name or email

Type : **All** Role : **All** Scope : **All scopes** Group by : **Role**

All (3) Job function roles (2) Privileged administrator roles (1)

Name	Type	Role	Scope
Owner (1)			
ON ohh no c7649d8a-d928...	User	Owner	Subscriptio
Microsoft Sentinel Contributor (2)			
Microsoft Thre... 8ee8fdad-f234...	Service principal	Microsoft Sentinel Co···	Subscriptio
WindowsDefe... fc780465-201...	Service principal	Microsoft Sentinel Co···	Subscriptio

Showing 1 - 3 of 3 results.

Add or remove favorites by pressing Cmd+Shift+F

Notifications

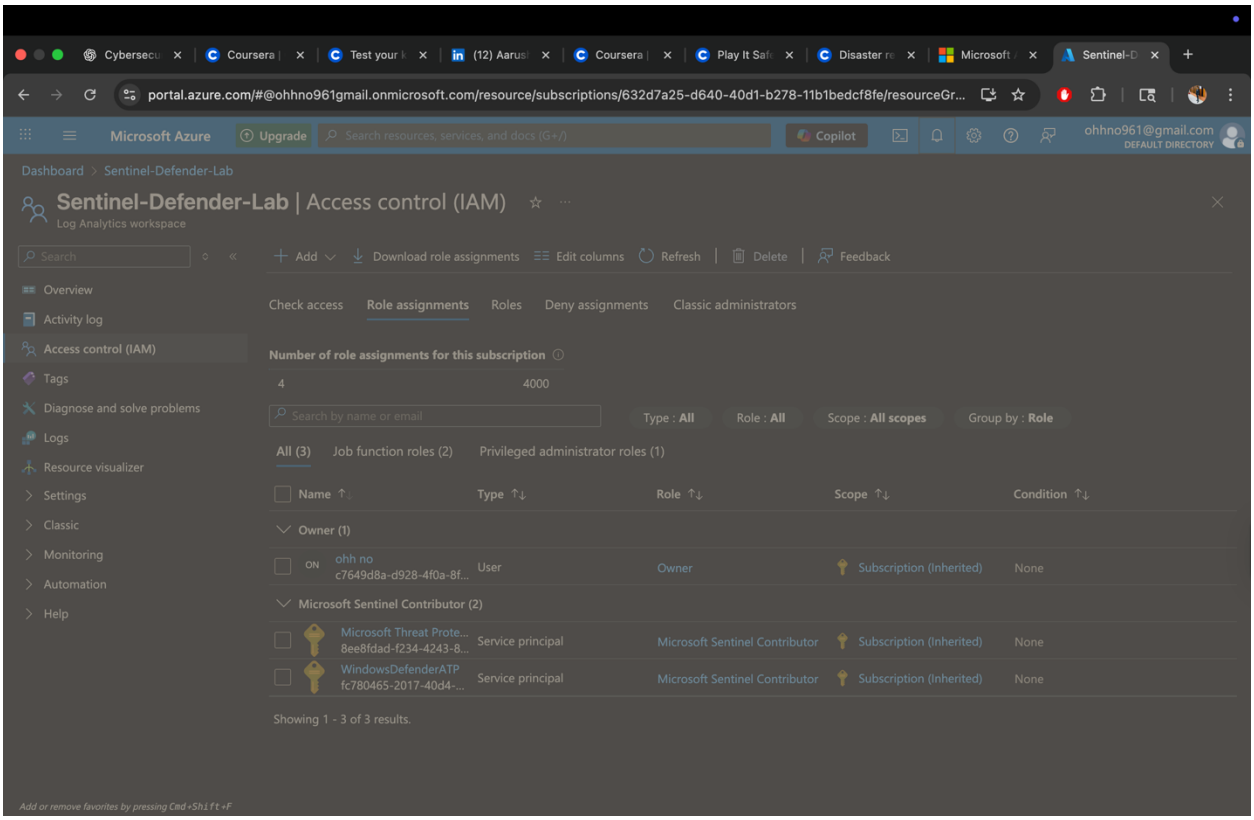
More events in the activity log → Dismiss all

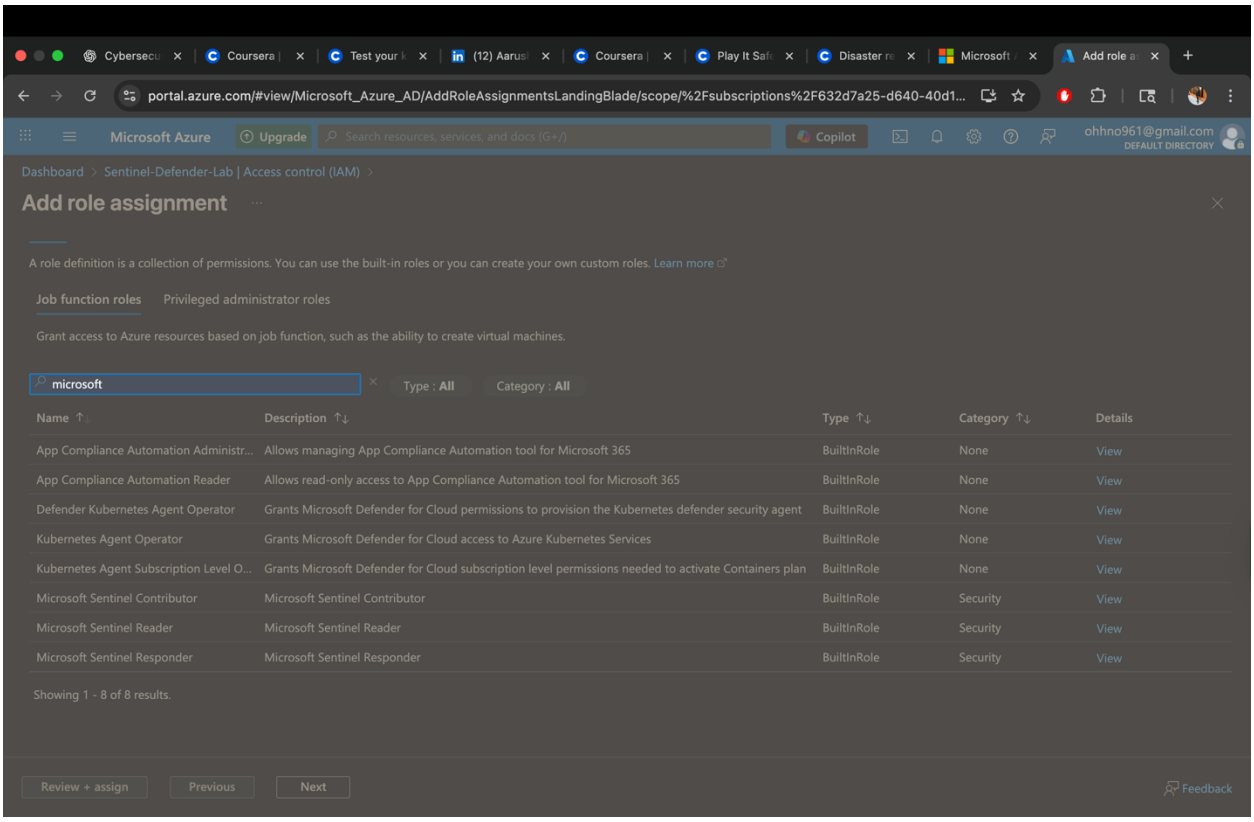
$161.65 credit remaining

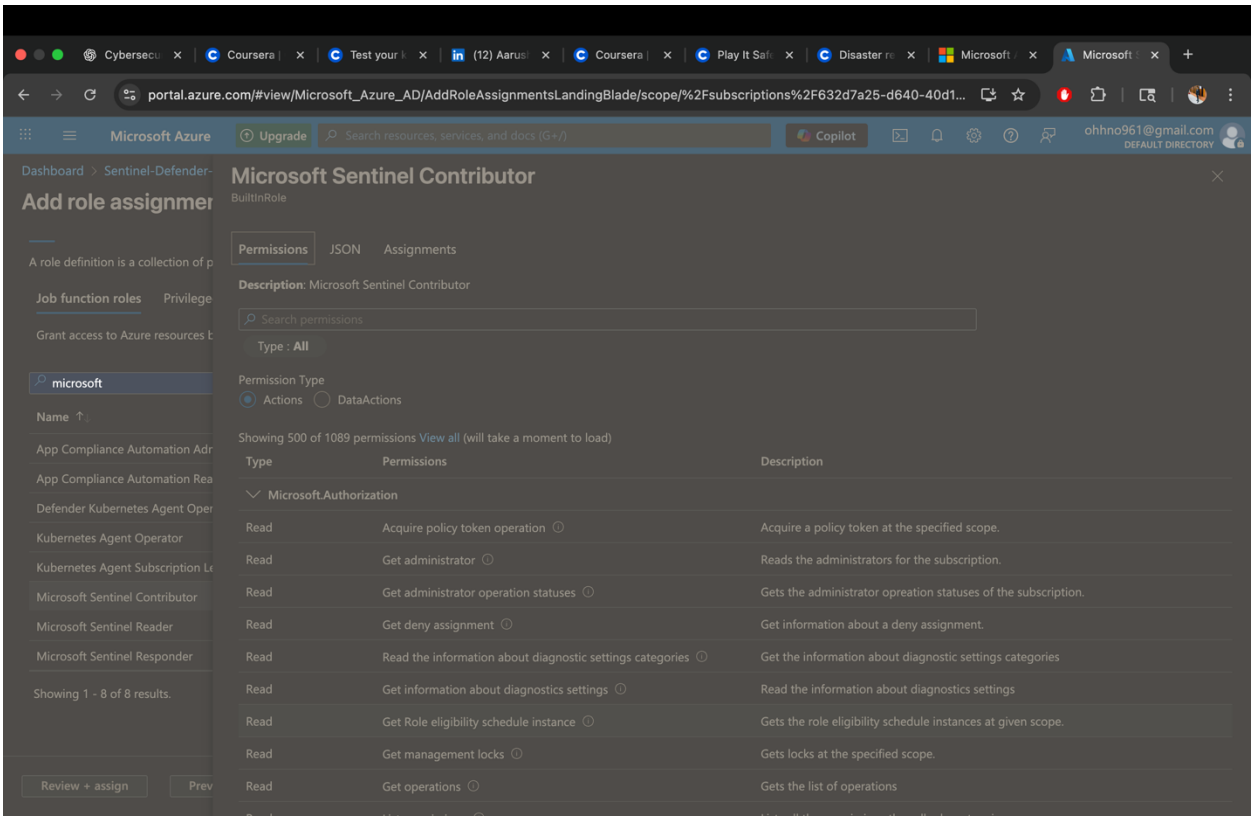
Subscription 'Azure subscription 1' has a remaining credit of $161.65.

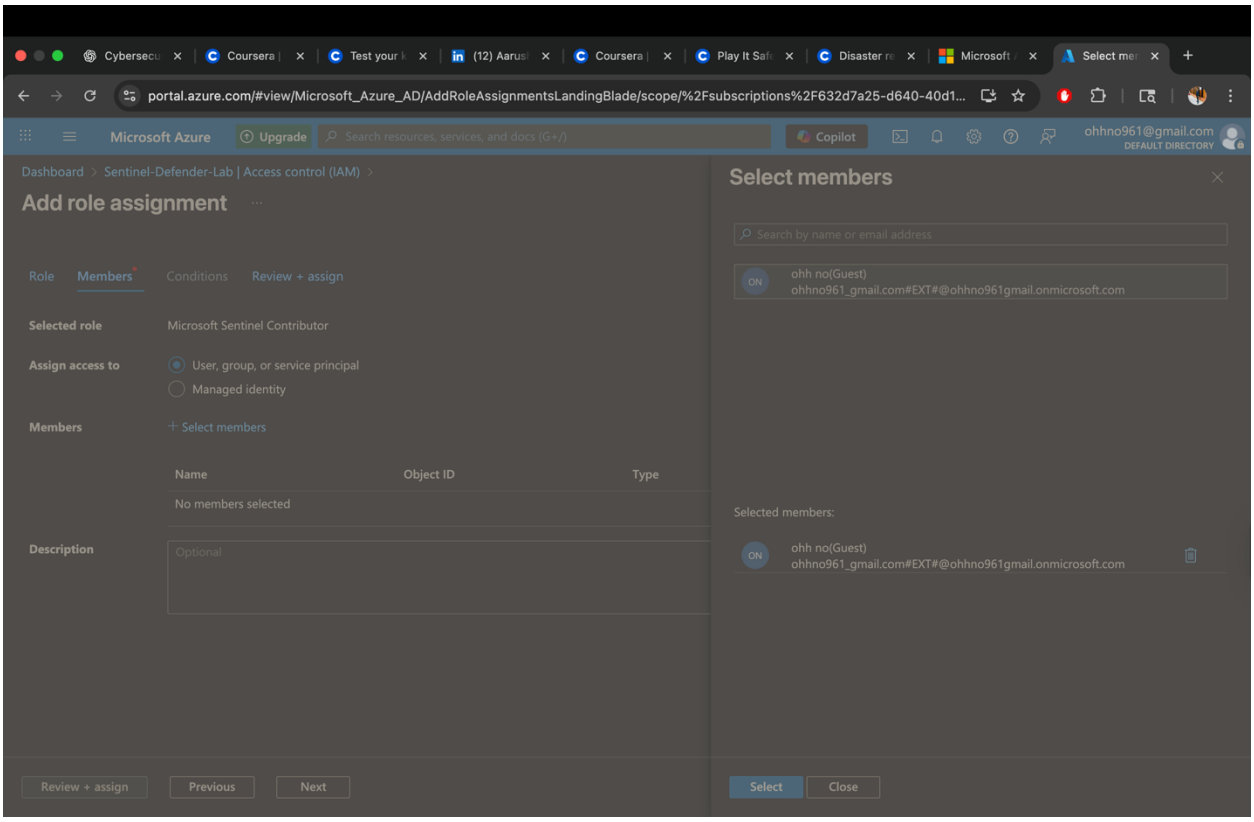
Upgrade to a Pay-As-You-Go subscription.

4 minutes ago


portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d640-40d1-b278-11b1bedcf8fe/resourceGr...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Dashboard > Sentinel-Defender-Lab
Sentinel-Defender-Lab | Access control (IAM)
Log Analytics workspace
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Add
Download role assignments
Edit columns
Refresh
Delete
Feedback
Check access
Role assignments
Roles
Deny assignments
Classic administrators
Number of role assignments for this subscription
4
4000
Type : All
Role : All
Scope : All scopes
Group by : Role
All (3)
Job function roles (2)
Privileged administrator roles (1)
Name
Type
Role
Scope
Condition
Owner (1)
ohh no
c7649d8a-d928-4f0a-8f...
User
Owner
Subscription (Inherited)
None
Microsoft Sentinel Contributor (2)
Microsoft Threat Prote...
8ee8fdad-f234-4243-8...
Service principal
Microsoft Sentinel Contributor
Subscription (Inherited)
None
WindowsDefenderATP
fc780465-2017-40d4-...
Service principal
Microsoft Sentinel Contributor
Subscription (Inherited)
None
Showing 1 - 3 of 3 results.


portal.azure.com/#view/Microsoft_Azure_AD/AddRoleAssignmentsLandingBlade/scope/%2Fsubscriptions%2F632d7a25-d640-40d1...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Dashboard > Sentinel-Defender-Lab | Access control (IAM) >
Add role assignment
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more
Job function roles
Privileged administrator roles
Grant access to Azure resources based on job function, such as the ability to create virtual machines.
microsoft
Type : All
Category : All
Name
Description
Type
Category
Details
App Compliance Automation Administr...
Allows managing App Compliance Automation tool for Microsoft 365
BuiltInRole
None
View
App Compliance Automation Reader
Allows read-only access to App Compliance Automation tool for Microsoft 365
BuiltInRole
None
View
Defender Kubernetes Agent Operator
Grants Microsoft Defender for Cloud permissions to provision the Kubernetes defender security agent
BuiltInRole
None
View
Kubernetes Agent Operator
Grants Microsoft Defender for Cloud access to Azure Kubernetes Services
BuiltInRole
None
View
Kubernetes Agent Subscription Level O...
Grants Microsoft Defender for Cloud subscription level permissions needed to activate Containers plan
BuiltInRole
None
View
Microsoft Sentinel Contributor
Microsoft Sentinel Contributor
BuiltInRole
Security
View
Microsoft Sentinel Reader
Microsoft Sentinel Reader
BuiltInRole
Security
View
Microsoft Sentinel Responder
Microsoft Sentinel Responder
BuiltInRole
Security
View
Showing 1 - 8 of 8 results.
Review + assign
Previous
Next
Feedback


portal.azure.com/#view/Microsoft_Azure_AD/AddRoleAssignmentsLandingBlade/scope/%2Fsubscriptions%2F632d7a25-d640-40d1...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Dashboard > Sentinel-Defender-
Add role assignmer
A role definition is a collection of p
Job function roles
Privilege
Grant access to Azure resources b
microsoft
Name
App Compliance Automation Adr
App Compliance Automation Rea
Defender Kubernetes Agent Oper
Kubernetes Agent Operator
Kubernetes Agent Subscription Le
Microsoft Sentinel Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder
Showing 1 - 8 of 8 results.
Review + assign
Prev
Microsoft Sentinel Contributor
BuiltInRole
Permissions
JSON
Assignments
Description: Microsoft Sentinel Contributor
Search permissions
Type : All
Permission Type
Actions
DataActions
Showing 500 of 1089 permissions View all (will take a moment to load)
Type
Permissions
Description
Microsoft.Authorization
Read
Acquire policy token operation
Acquire a policy token at the specified scope.
Read
Get administrator
Reads the administrators for the subscription.
Read
Get administrator operation statuses
Gets the administrator opreation statuses of the subscription.
Read
Get deny assignment
Get information about a deny assignment.
Read
Read the information about diagnostic settings categories
Get the information about diagnostic settings categories
Read
Get information about diagnostics settings
Read the information about diagnostics settings
Read
Get Role eligibility schedule instance
Gets the role eligibility schedule instances at given scope.
Read
Get management locks
Gets locks at the specified scope.
Read
Get operations
Gets the list of operations


portal.azure.com/#view/Microsoft_Azure_AD/AddRoleAssignmentsLandingBlade/scope/%2Fsubscriptions%2F632d7a25-d640-40d1...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
Dashboard > Sentinel-Defender-Lab | Access control (IAM) >
Add role assignment
Role
Members
Conditions
Review + assign
Selected role
Microsoft Sentinel Contributor
Assign access to
User, group, or service principal
Managed identity
Members
+ Select members
Name
Object ID
Type
No members selected
Description
Optional
Review + assign
Previous
Next
Select members
Search by name or email address
ON
ohh no(Guest)
ohhno961_gmail.com#EXT#@ohhno961gmail.onmicrosoft.com
Selected members:
ON
ohh no(Guest)
ohhno961_gmail.com#EXT#@ohhno961gmail.onmicrosoft.com
Select
Close

Cybersecu | Coursera | Test your k | (12) Aarus | Coursera | Play It Safe | Disaster re | Microsoft | Sentinel-D

portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d640-40d1-b278-11b1bedcf8fe/resourceGr...

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | ohhno961@gmail.com DEFAULT DIRECTORY

Dashboard > Sentinel-Defender-Lab

Sentinel-Defender-Lab | Access control (IAM)

Log Analytics workspace

Added Role assignment
ohh no(Guest) was added as Microsoft Sentinel Contributor for Sentinel-Defender-Lab.

Search | Add | Download role assignments | Edit columns | Refresh | Delete | Feedback

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs
- Resource visualizer
- Settings
- Classic
- Monitoring
- Automation
- Help

Check access | Role assignments | Roles | Deny assignments | Classic administrators

Number of role assignments for this subscription

Search by name or email | Type : All | Role : All | Scope : All scopes | Group by : Role

All (3) | Job function roles (2) | Privileged administrator roles (1)

Name	Type	Role	Scope	Condition
Owner (1)				
ON ohh no c7649d8a-d928-4f0a-8f...	User	Owner	Subscription (Inherited)	None
Microsoft Sentinel Contributor (2)				
Microsoft Threat Prote... 8ee8fdad-f234-4243-8...	Service principal	Microsoft Sentinel Contributor	Subscription (Inherited)	None
WindowsDefenderATP fc780465-2017-40d4-...	Service principal	Microsoft Sentinel Contributor	Subscription (Inherited)	None

Showing 1 - 3 of 3 results.

Add or remove favorites by pressing Cmd+Shift+F

Cybersecu | Coursera | Test your k | (12) Aarus | Coursera | Play It Safe | Disaster re | Microsoft | Sentinel-D

portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d640-40d1-b278-11b1bedcf8fe/resourceGr...

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | ohhno961@gmail.com DEFAULT DIRECTORY

Dashboard > Sentinel-Defender-Lab

Sentinel-Defender-Lab | Access control (IAM)

Log Analytics workspace

Search | Add | Download role assignments | Edit columns | Refresh | Delete | Feedback

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs
- Resource visualizer
- Settings
- Classic
- Monitoring
- Automation
- Help

Check access | Role assignments | Roles | Deny assignments | Classic administrators

Number of role assignments for this subscription

5 4000

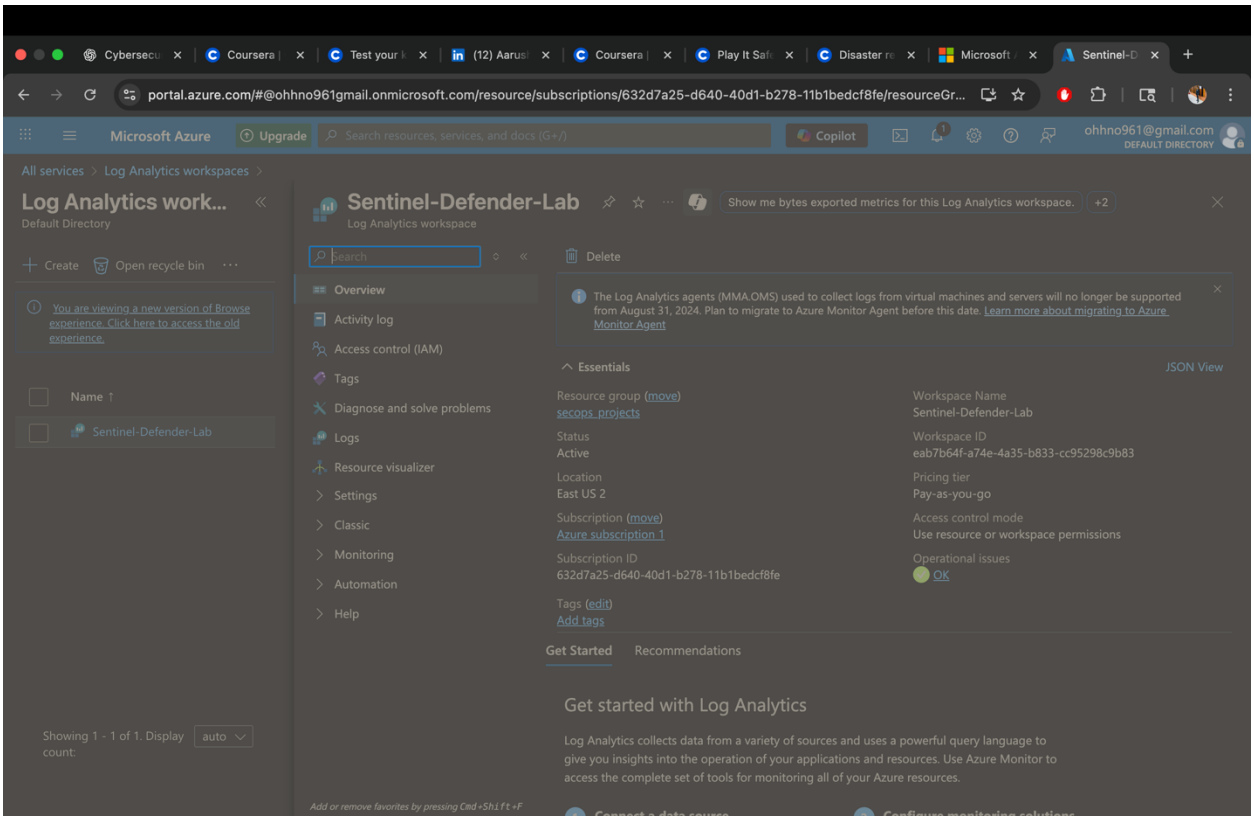
Search by name or email | Type : All | Role : All | Scope : All scopes | Group by : Role

All (4) | Job function roles (3) | Privileged administrator roles (1)

Name	Type	Role	Scope	Condition
Owner (1)				
ON ohh no c7649d8a-d928-4f0a-8f...	User	Owner	Subscription (Inherited)	None
Microsoft Sentinel Contributor (3)				
Microsoft Threat Prote... 8ee8fdad-f234-4243-8...	Service principal	Microsoft Sentinel Contributor	Subscription (Inherited)	None
ON ohh no c7649d8a-d928-4f0a-8f...	User	Microsoft Sentinel Contributor	This resource	None
WindowsDefenderATP fc780465-2017-40d4-...	Service principal	Microsoft Sentinel Contributor	Subscription (Inherited)	None

Showing 1 - 4 of 4 results.

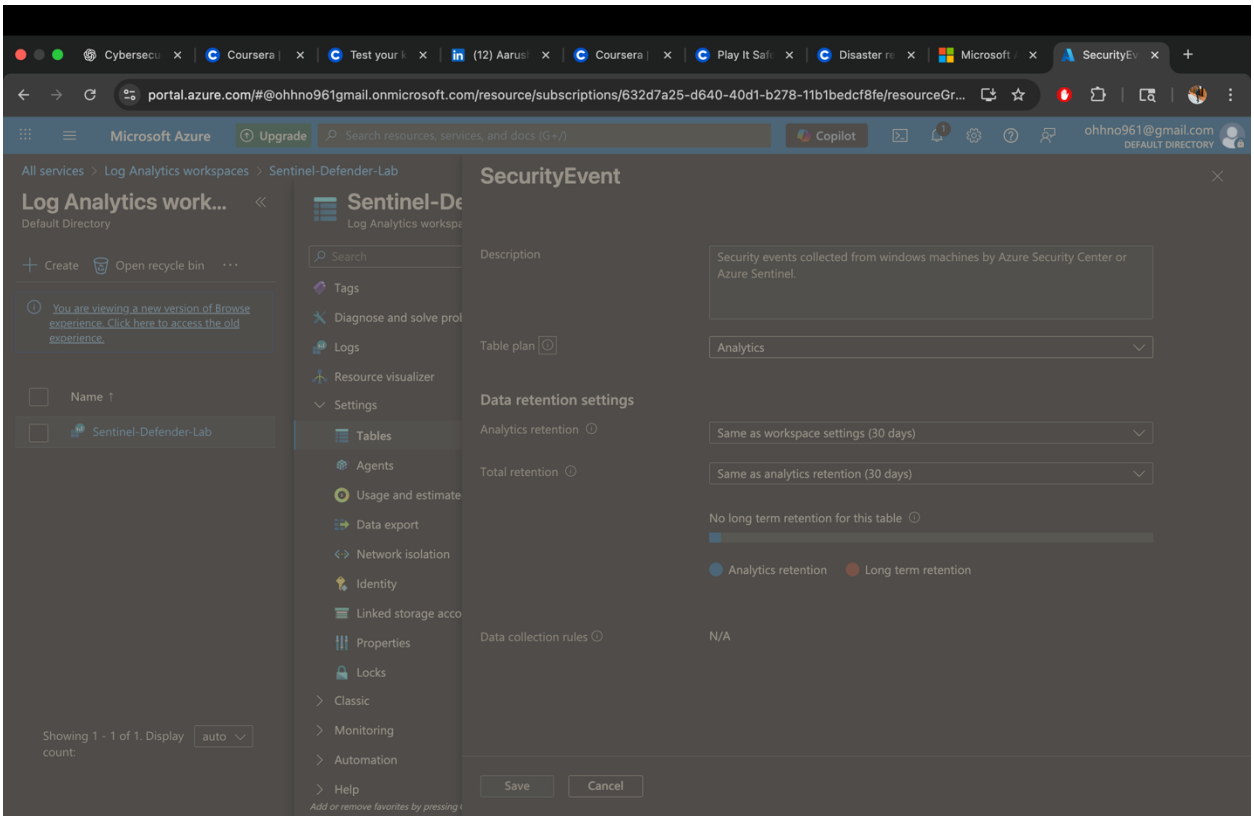
Add or remove favorites by pressing Cmd+Shift+F

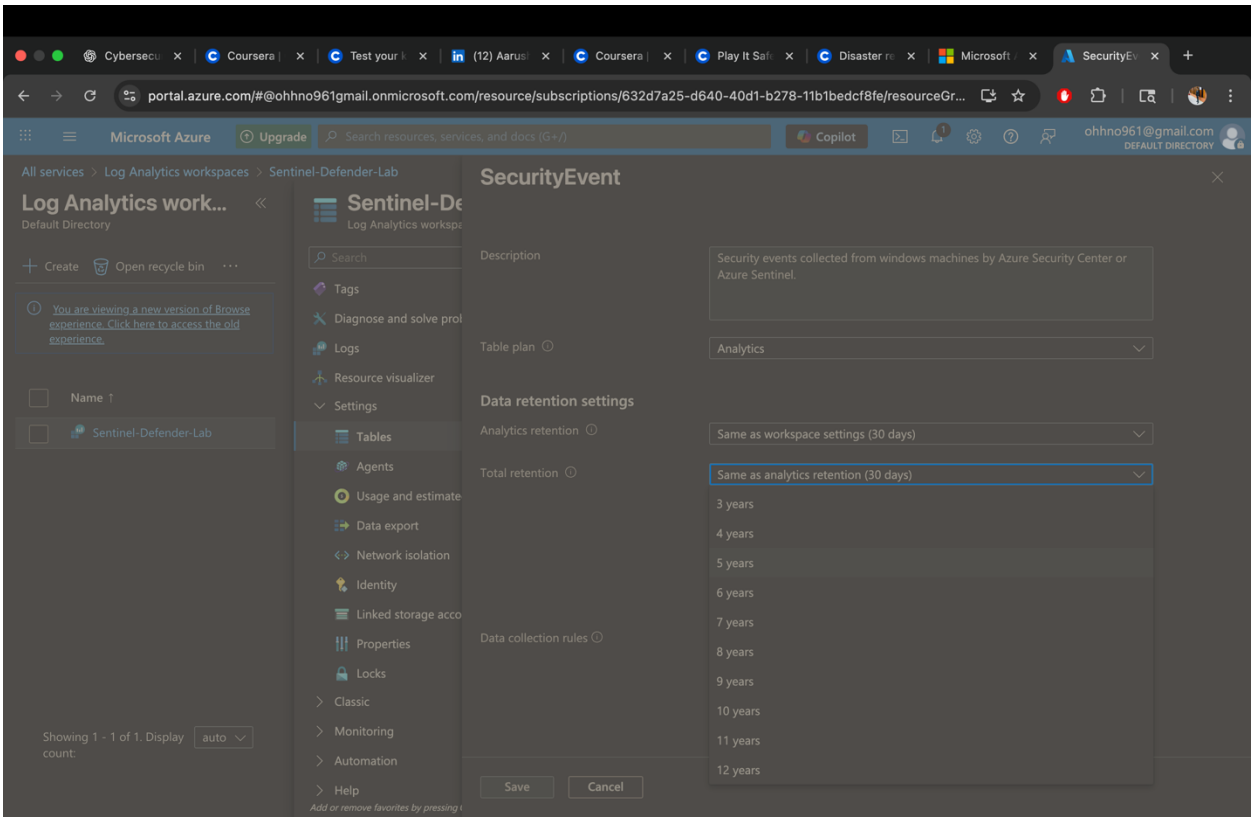


2. Log Analytics Workspace Retention Configuration

Objective: Adjust log retention period
Path:
`All Services → Log Analytics Workspaces → sentinel-defender-lab → Tables → SecurityEvent`
Configuration:

- Default retention: **30 days**
- Modified to: **Custom duration** (months/years as needed)
  Note: Retention changes apply to all ingested security event logs.


portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d640-40d1-b278-11b1bedcf8fe/resourceGr...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
All services > Log Analytics workspaces > Sentinel-Defender-Lab
Log Analytics work...
Default Directory
Create
Open recycle bin
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Sentinel-Defender-Lab
Showing 1 - 1 of 1. Display count:
auto
Sentinel-De
Log Analytics worksp
Search
Tags
Diagnose and solve prol
Logs
Resource visualizer
Settings
Tables
Agents
Usage and estimate
Data export
Network isolation
Identity
Linked storage acco
Properties
Locks
Classic
Monitoring
Automation
Help
SecurityEvent
Description
Security events collected from windows machines by Azure Security Center or Azure Sentinel.
Table plan
Analytics
Data retention settings
Analytics retention
Same as workspace settings (30 days)
Total retention
Same as analytics retention (30 days)
No long term retention for this table
Analytics retention
Long term retention
Data collection rules
N/A
Save
Cancel


portal.azure.com/#@ohhno961gmail.onmicrosoft.com/resource/subscriptions/632d7a25-d640-40d1-b278-11b1bedcf8fe/resourceGr...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
All services > Log Analytics workspaces > Sentinel-Defender-Lab
Log Analytics work...
Default Directory
Create
Open recycle bin
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Sentinel-Defender-Lab
Showing 1 - 1 of 1. Display count:
auto
Sentinel-De
Log Analytics worksp
Search
Tags
Diagnose and solve prol
Logs
Resource visualizer
Settings
Tables
Agents
Usage and estimate
Data export
Network isolation
Identity
Linked storage acco
Properties
Locks
Classic
Monitoring
Automation
Help
SecurityEvent
Description
Security events collected from windows machines by Azure Security Center or Azure Sentinel.
Table plan
Analytics
Data retention settings
Analytics retention
Same as workspace settings (30 days)
Total retention
Same as analytics retention (30 days)
3 years
4 years
5 years
6 years
7 years
8 years
9 years
10 years
11 years
12 years
Data collection rules
Save
Cancel

3. Content Hub & Data Connector Deployment

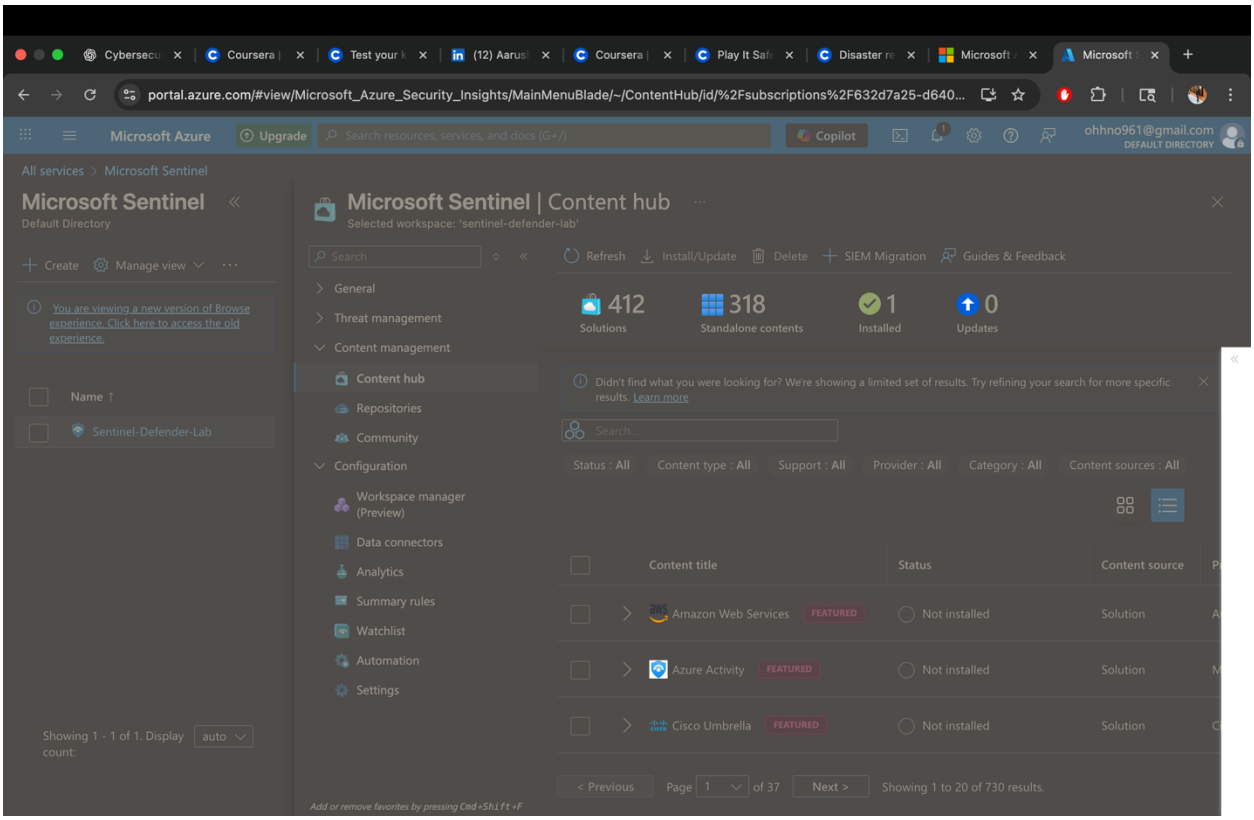
Objective: Enable threat data ingestion
Path:
`Microsoft Sentinel → Content Hub`

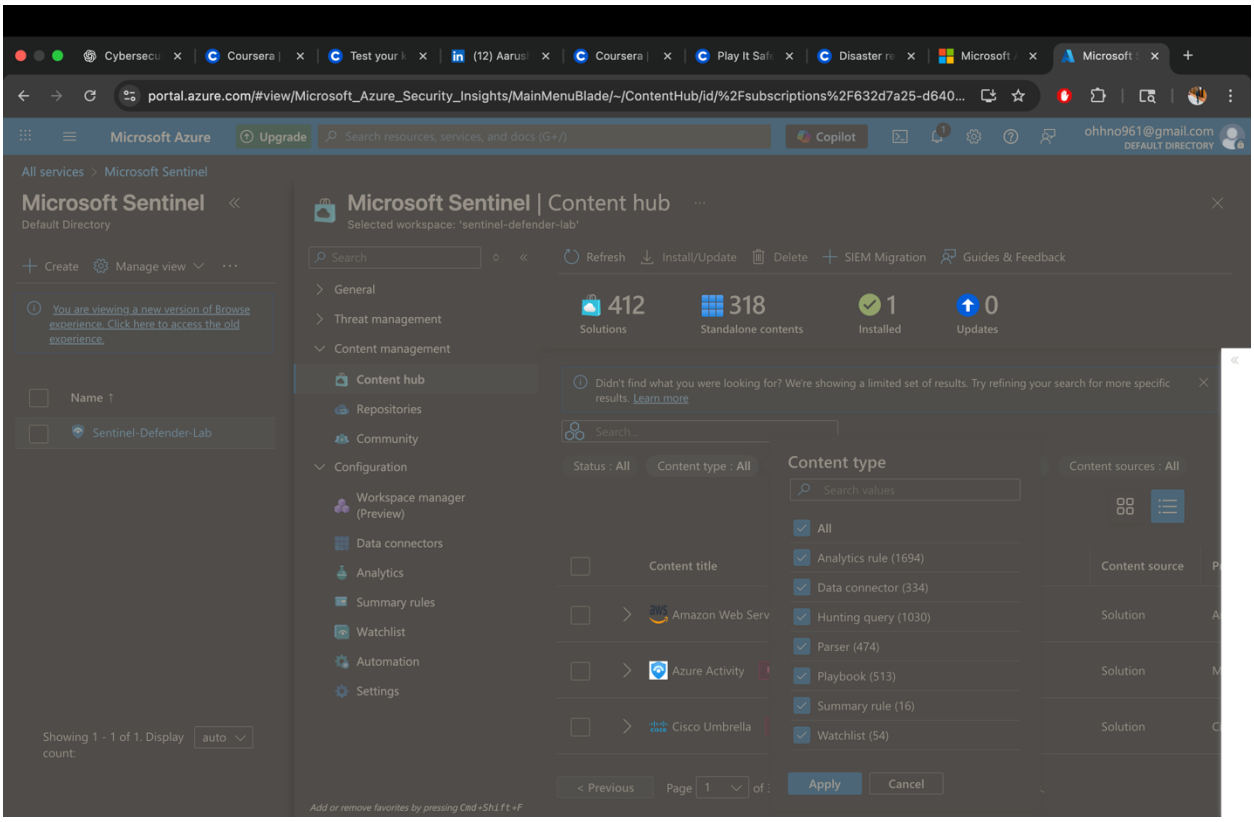
Actions Performed:

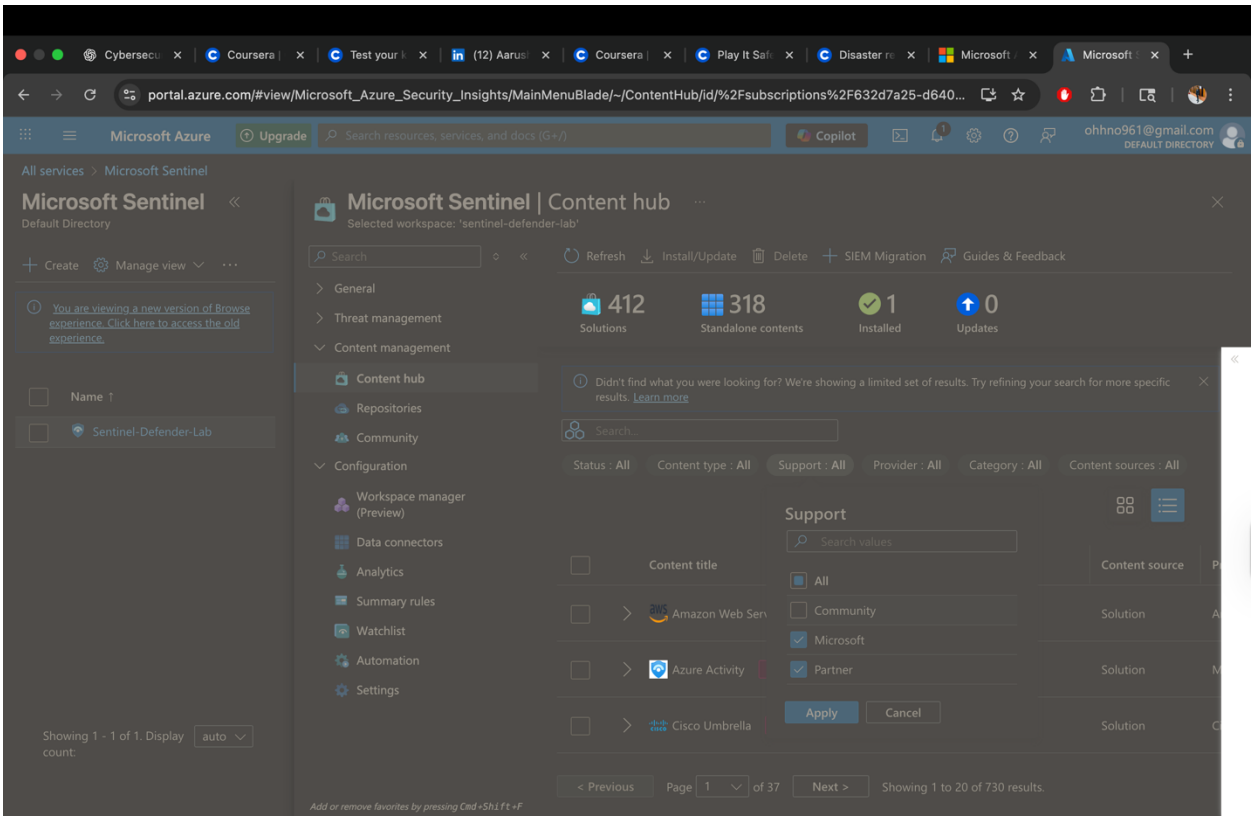
Connector Name	Type/Category	Status
Microsoft 365 Insider Risk Mgmt	Compliance	Installed
Microsoft Defender for Cloud Apps	Cloud Security	Installed
Microsoft Defender for Endpoint	Endpoint Protection	Installed
Microsoft Defender for Identity	Identity	Installed
Microsoft Defender for Cloud	Cloud Security	Installed
Microsoft Defender for Office 365	Email Security	Installed
Microsoft Sysmon for Linux	Endpoint Monitoring	Installed
Azure Activity	Platform Logs	Installed
Common Event Format (CEF)	Security	Installed

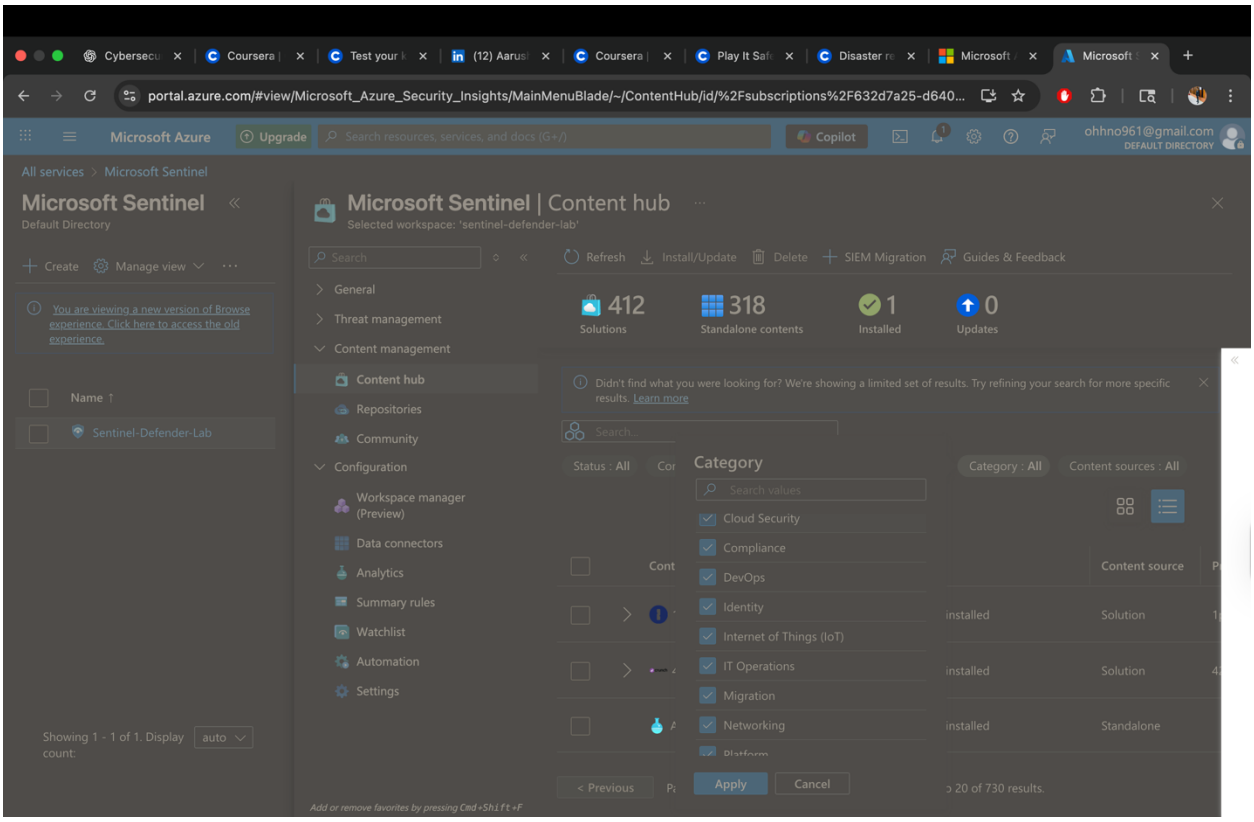
Filtering Applied:

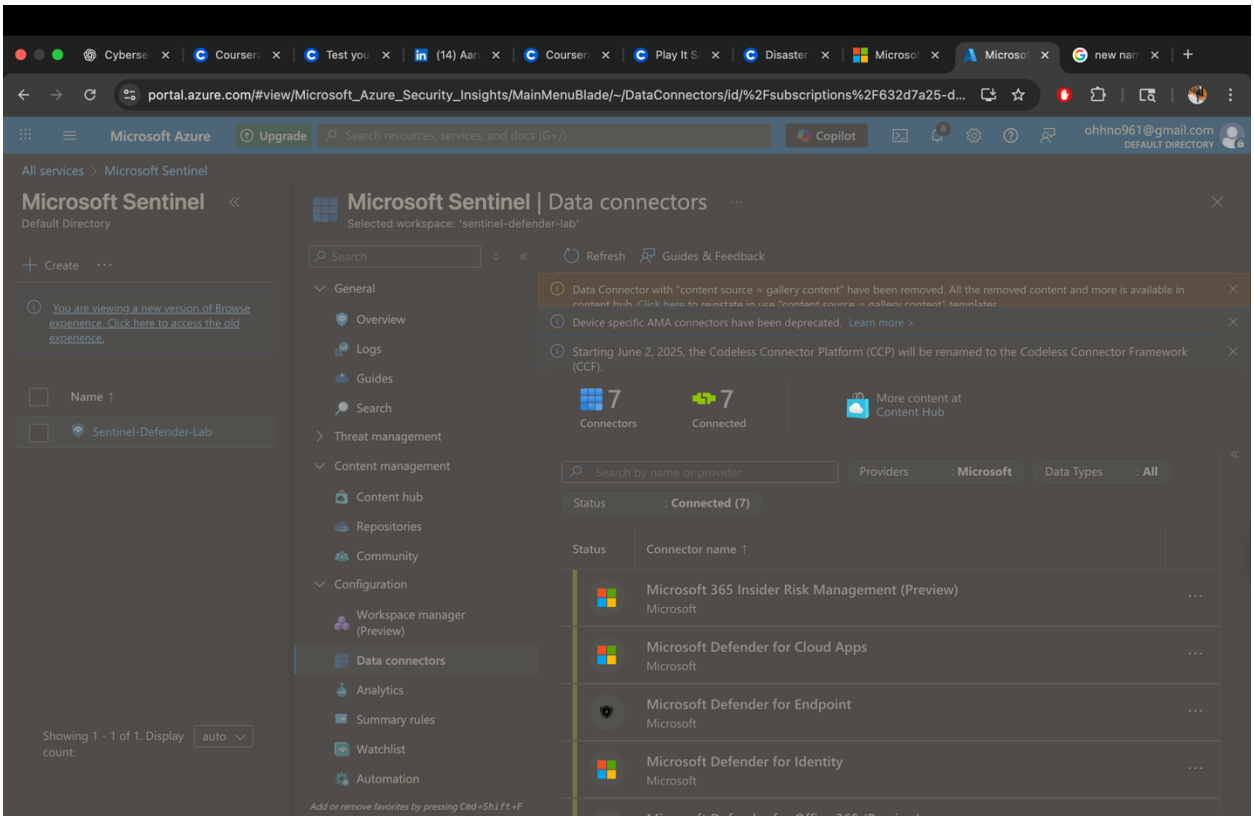
- **Support**: Microsoft-only selected
- **Category**: Cloud Security, Identity, Networking


portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/ContentHub/id/%2Fsubscriptions%2F632d7a25-d640...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
All services > Microsoft Sentinel
Microsoft Sentinel
Default Directory
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Sentinel-Defender-Lab
Showing 1 - 1 of 1. Display count:
auto
Microsoft Sentinel | Content hub
Selected workspace: 'sentinel-defender-lab'
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
General
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
Automation
Settings
412
Solutions
318
Standalone contents
1
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
Status : All
Content type : All
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Content source
Amazon Web Services
FEATURED
Not installed
Solution
Azure Activity
FEATURED
Not installed
Solution
Cisco Umbrella
FEATURED
Not installed
Solution
< Previous
Page 1 of 37
Next >
Showing 1 to 20 of 730 results.
Add or remove favorites by pressing Cmd+Shift+F


portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/ContentHub/id/%2Fsubscriptions%2F632d7a25-d640...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
All services > Microsoft Sentinel
Microsoft Sentinel
Default Directory
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Sentinel-Defender-Lab
Showing 1 - 1 of 1. Display count:
auto
Microsoft Sentinel | Content hub
Selected workspace: 'sentinel-defender-lab'
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
General
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
Automation
Settings
412
Solutions
318
Standalone contents
1
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
Status : All
Content type : All
Content sources : All
Content type
Search values
All
Analytics rule (1694)
Data connector (334)
Hunting query (1030)
Parser (474)
Playbook (513)
Summary rule (16)
Watchlist (54)
Content title
Content source
Amazon Web Serv
Azure Activity
Cisco Umbrella
Solution
Solution
Solution
< Previous
Page 1 of
Apply
Cancel
Add or remove favorites by pressing Cmd+Shift+F


portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/ContentHub/id/%2Fsubscriptions%2F632d7a25-d640...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
All services > Microsoft Sentinel
Microsoft Sentinel
Default Directory
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Sentinel-Defender-Lab
Showing 1 - 1 of 1. Display count:
auto
Microsoft Sentinel | Content hub
Selected workspace: 'sentinel-defender-lab'
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
General
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
Automation
Settings
412
Solutions
318
Standalone contents
1
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
Status : All
Content type : All
Support : All
Provider : All
Category : All
Content sources : All
Support
Search values
All
Community
Microsoft
Partner
Apply
Cancel
Content title
Content source
Amazon Web Serv
Azure Activity
Cisco Umbrella
Solution
< Previous
Page 1 of 37
Next >
Showing 1 to 20 of 730 results.
Add or remove favorites by pressing Cmd+Shift+F


portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/ContentHub/id/%2Fsubscriptions%2F632d7a25-d640...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
All services > Microsoft Sentinel
Microsoft Sentinel
Default Directory
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Sentinel-Defender-Lab
Showing 1 - 1 of 1. Display count:
auto
Microsoft Sentinel | Content hub
Selected workspace: 'sentinel-defender-lab'
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
General
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
Automation
Settings
412
Solutions
318
Standalone contents
1
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
Status : All
Category : All
Content sources : All
Category
Search values
Cloud Security
Compliance
DevOps
Identity
Internet of Things (IoT)
IT Operations
Migration
Networking
Content source
Solution
Standalone
Apply
Cancel
< Previous
Add or remove favorites by pressing Cmd+Shift+F

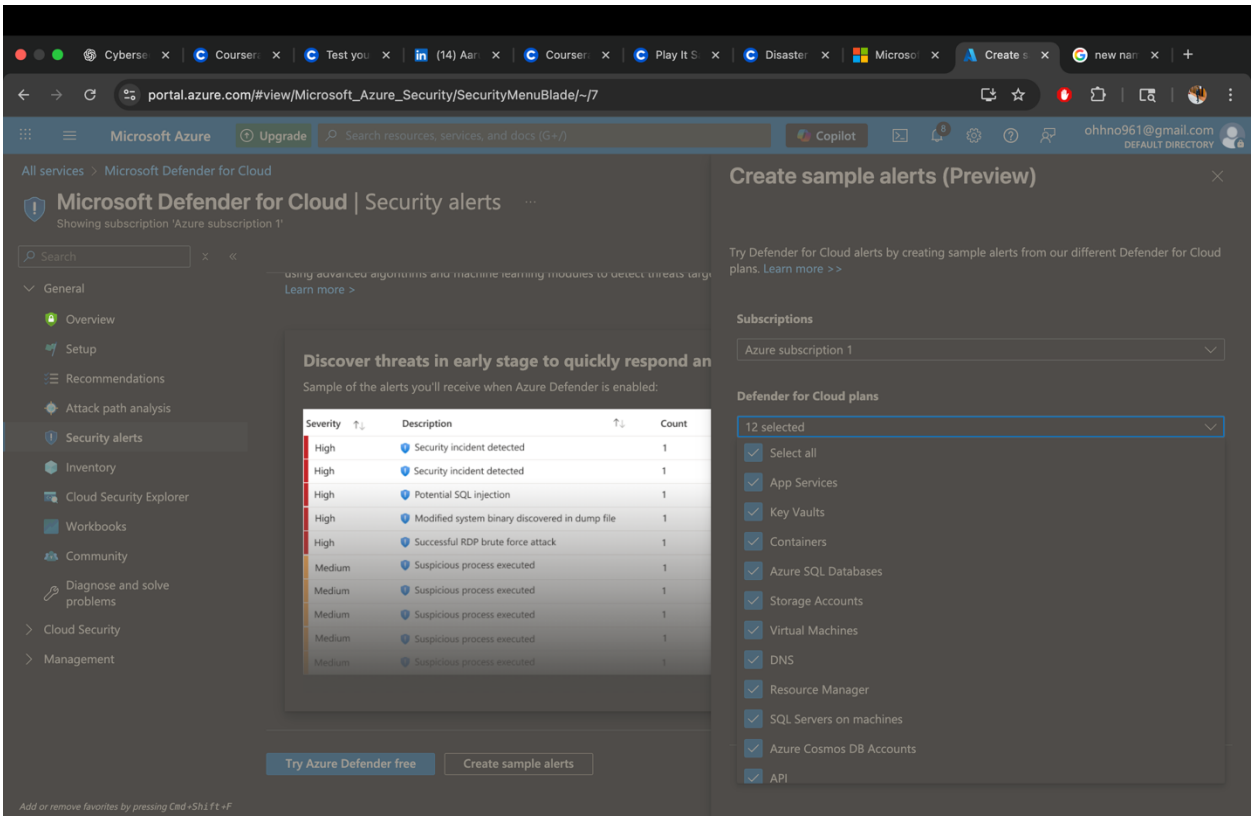


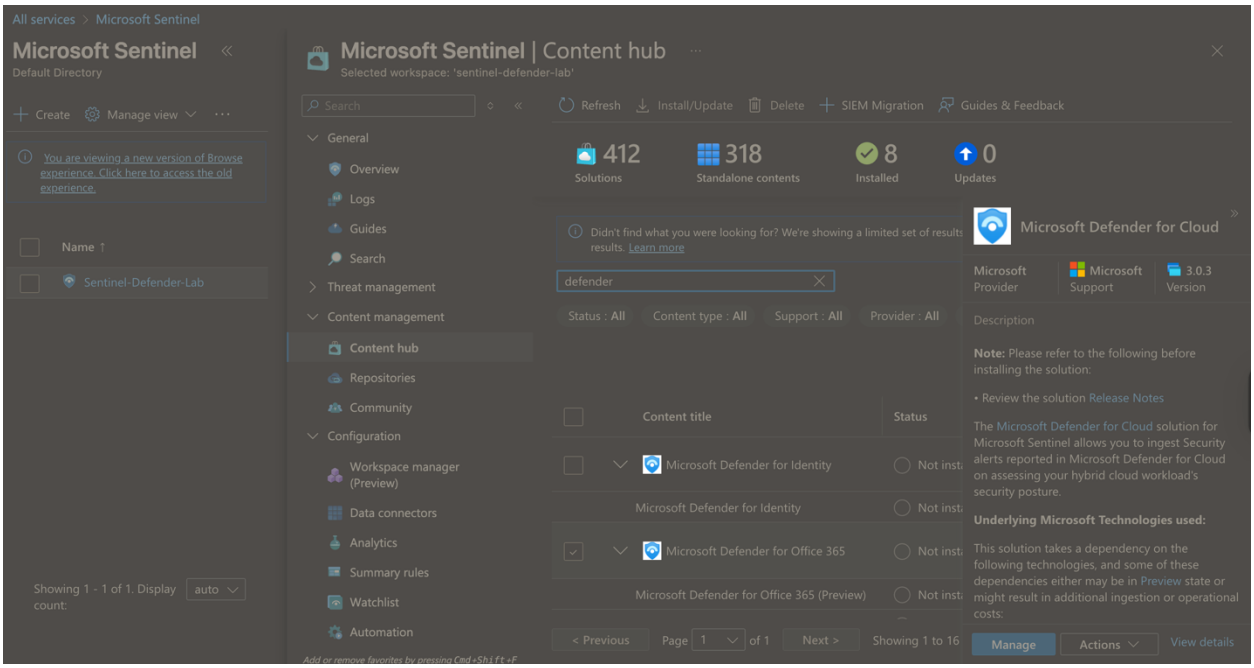
4. Defender for Cloud Sample Alerts

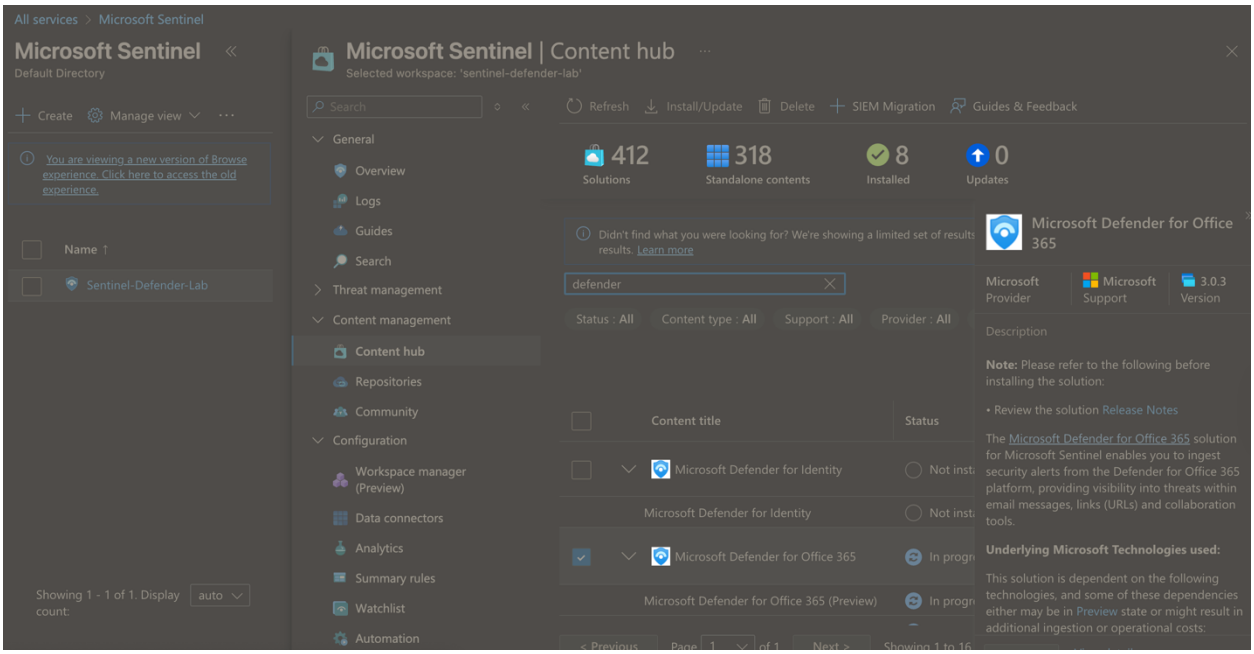
Objective: Generate test alerts
Path:
`Microsoft Defender for Cloud → Security Alerts → Create Sample Alerts`
Scope:
12 Defender plans enabled, including:

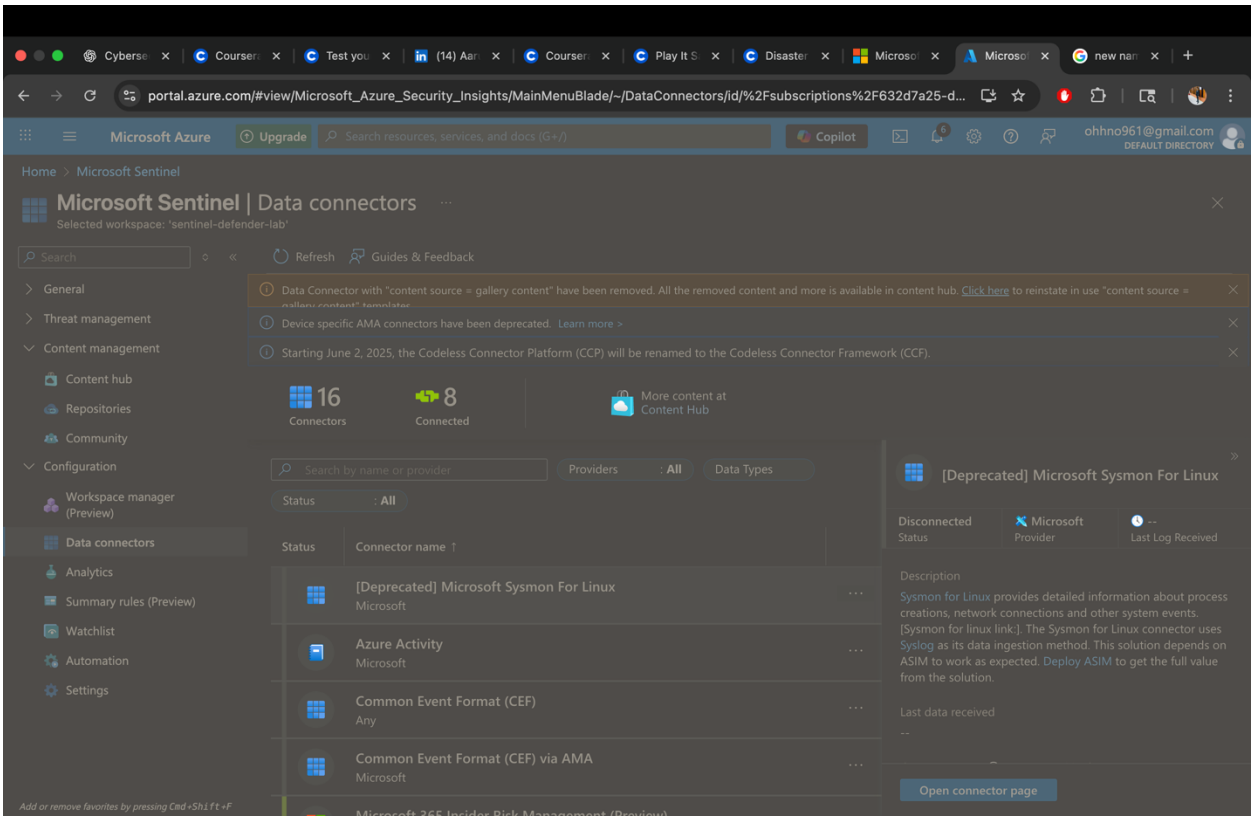
- App Services
- Azure SQL Databases
- Virtual Machines
- Key Vaults
- Storage Accounts

Purpose: Validate alert pipeline and Sentinel integration.


portal.azure.com/#view/Microsoft_Azure_Security/SecurityMenuBlade/~/7
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY
All services > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Security alerts
Showing subscription 'Azure subscription 1'
General
Overview
Setup
Recommendations
Attack path analysis
Security alerts
Inventory
Cloud Security Explorer
Workbooks
Community
Diagnose and solve problems
Cloud Security
Management
Learn more >
Discover threats in early stage to quickly respond an
Sample of the alerts you'll receive when Azure Defender is enabled:
Severity
Description
Count
High
Security incident detected
High
Security incident detected
High
Potential SQL injection
High
Modified system binary discovered in dump file
High
Successful RDP brute force attack
Medium
Suspicious process executed
Medium
Suspicious process executed
Medium
Suspicious process executed
Medium
Suspicious process executed
Try Azure Defender free
Create sample alerts
Create sample alerts (Preview)
Try Defender for Cloud alerts by creating sample alerts from our different Defender for Cloud plans. Learn more >>
Subscriptions
Azure subscription 1
Defender for Cloud plans
12 selected
Select all
App Services
Key Vaults
Containers
Azure SQL Databases
Storage Accounts
Virtual Machines
DNS
Resource Manager
SQL Servers on machines
Azure Cosmos DB Accounts
API


All services > Microsoft Sentinel
Microsoft Sentinel
Default Directory
Create
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Sentinel-Defender-Lab
Showing 1 - 1 of 1. Display count:
auto
Microsoft Sentinel | Content hub
Selected workspace: 'sentinel-defender-lab'
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
General
Overview
Logs
Guides
Search
Threat management
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
Watchlist
Automation
412
Solutions
318
Standalone contents
8
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Learn more
defender
Status : All
Content type : All
Support : All
Provider : All
Content title
Status
Microsoft Defender for Identity
Microsoft Defender for Identity
Microsoft Defender for Office 365
Microsoft Defender for Office 365 (Preview)
< Previous
Page 1 of 1
Next >
Showing 1 to 16
Microsoft Defender for Cloud
Microsoft Provider
Microsoft Support
3.0.3 Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
The Microsoft Defender for Cloud solution for Microsoft Sentinel allows you to ingest Security alerts reported in Microsoft Defender for Cloud on assessing your hybrid cloud workload's security posture.
Underlying Microsoft Technologies used:
This solution takes a dependency on the following technologies, and some of these dependencies either may be in Preview state or might result in additional ingestion or operational costs:
Manage
Actions
View details

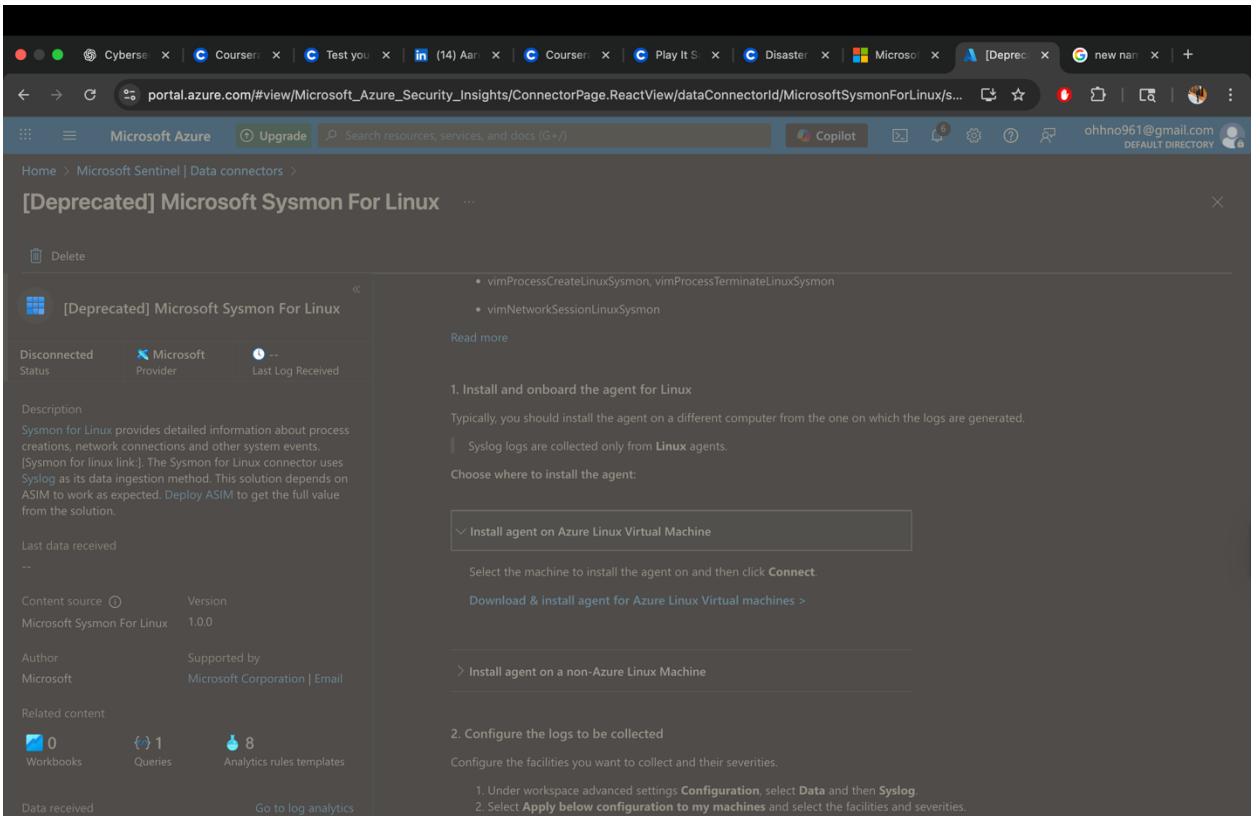


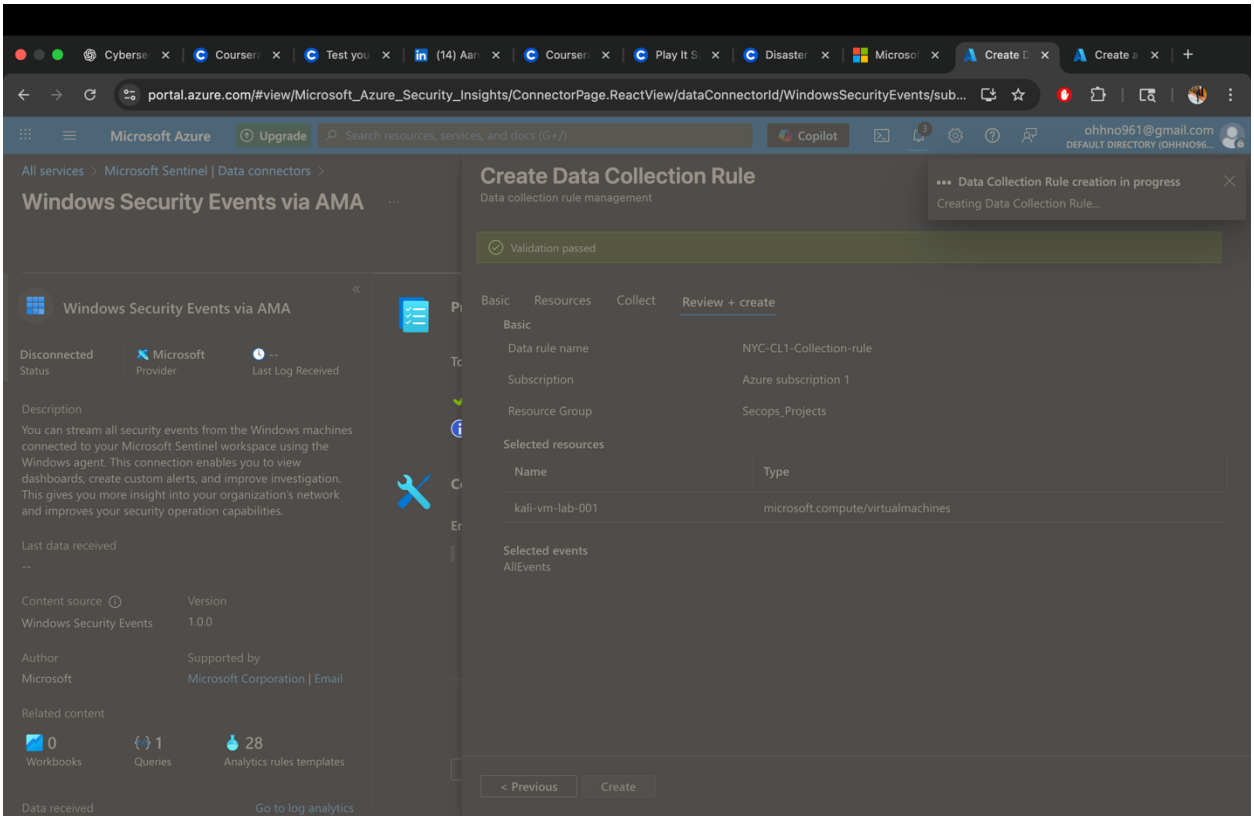


5. Sysmon for Linux Agent Configuration

Objective: Deploy monitoring agent
Path:
`Sysmon for Linux connector → Connect Page`
Options Selected:

- Installation target: **Non-Azure Linux machine**
  Status: Configuration initiated, but agent connectivity unverified due to resource constraints.





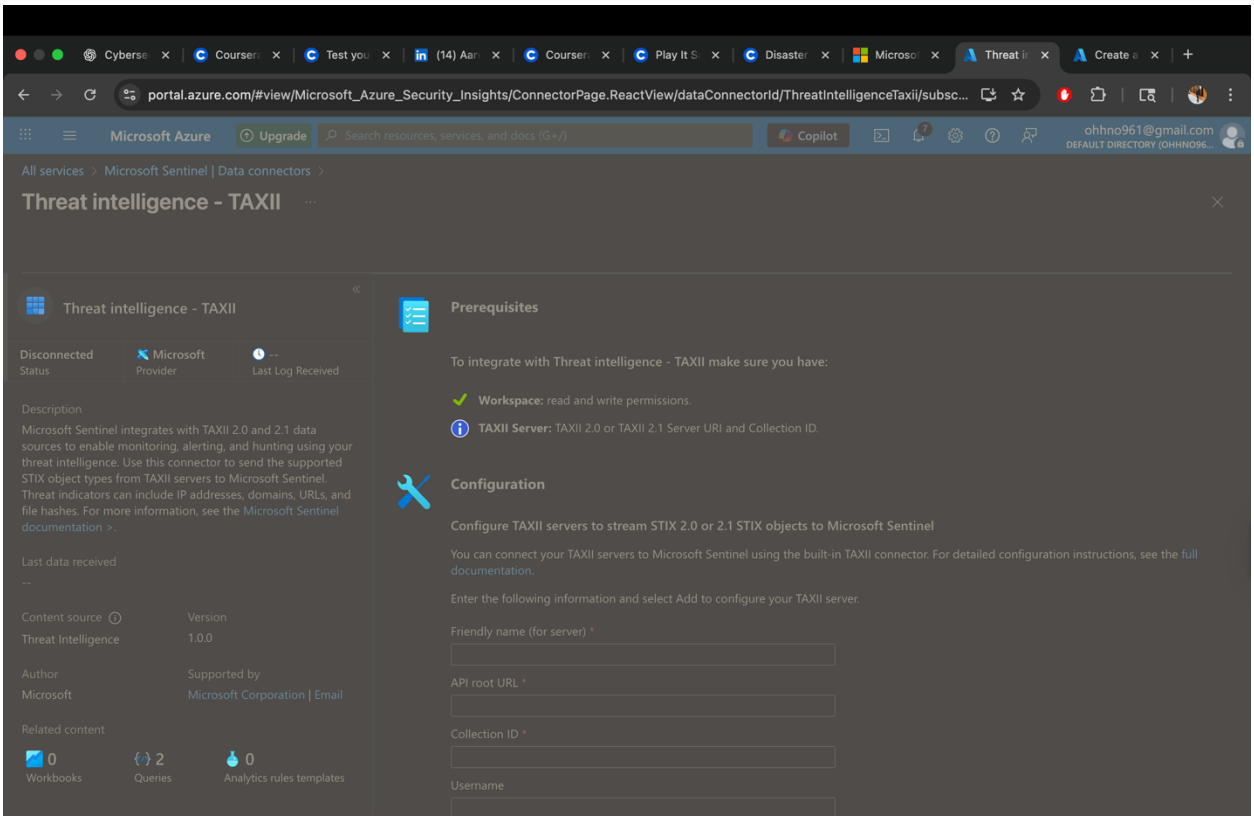
6. Threat Intelligence (TAXII) Integration

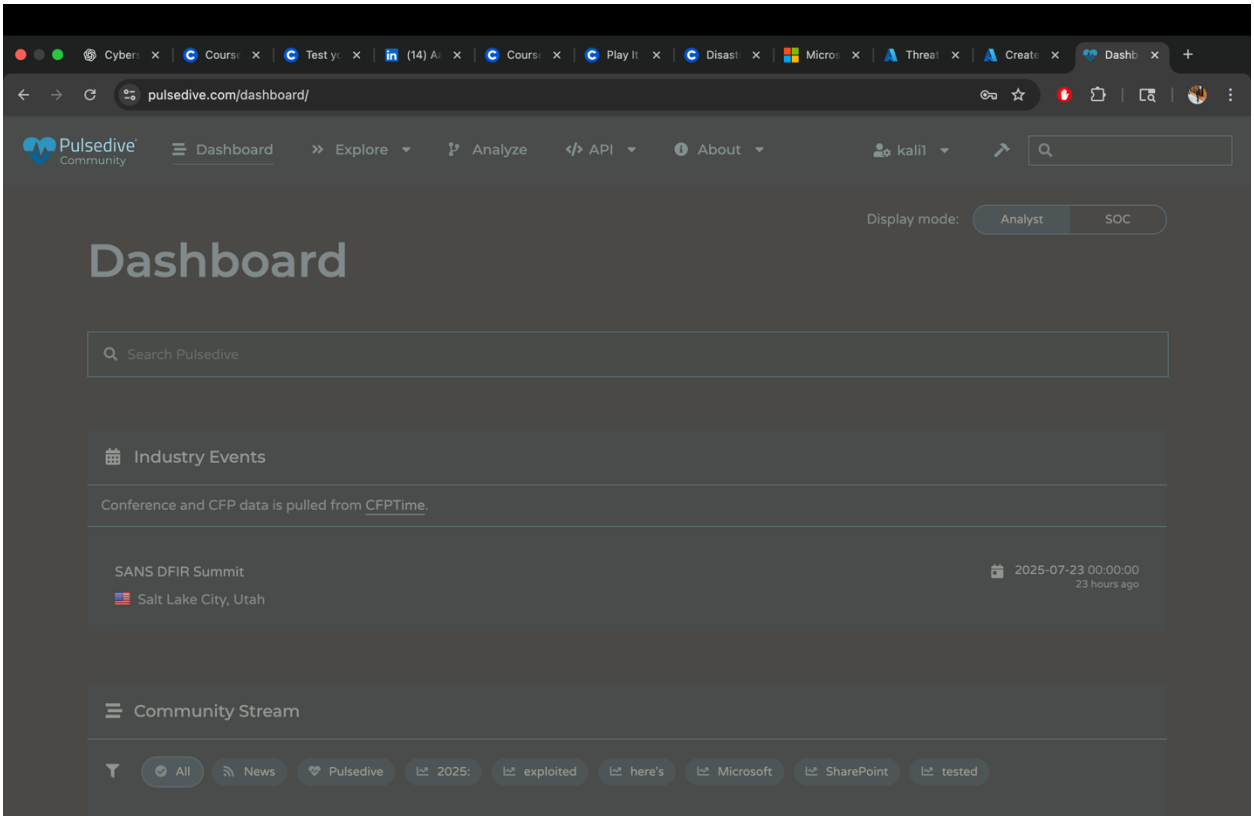
Objective: Stream STIX 2.x threat feeds
Source: PulseDive (pulsedive.com)
Configuration:

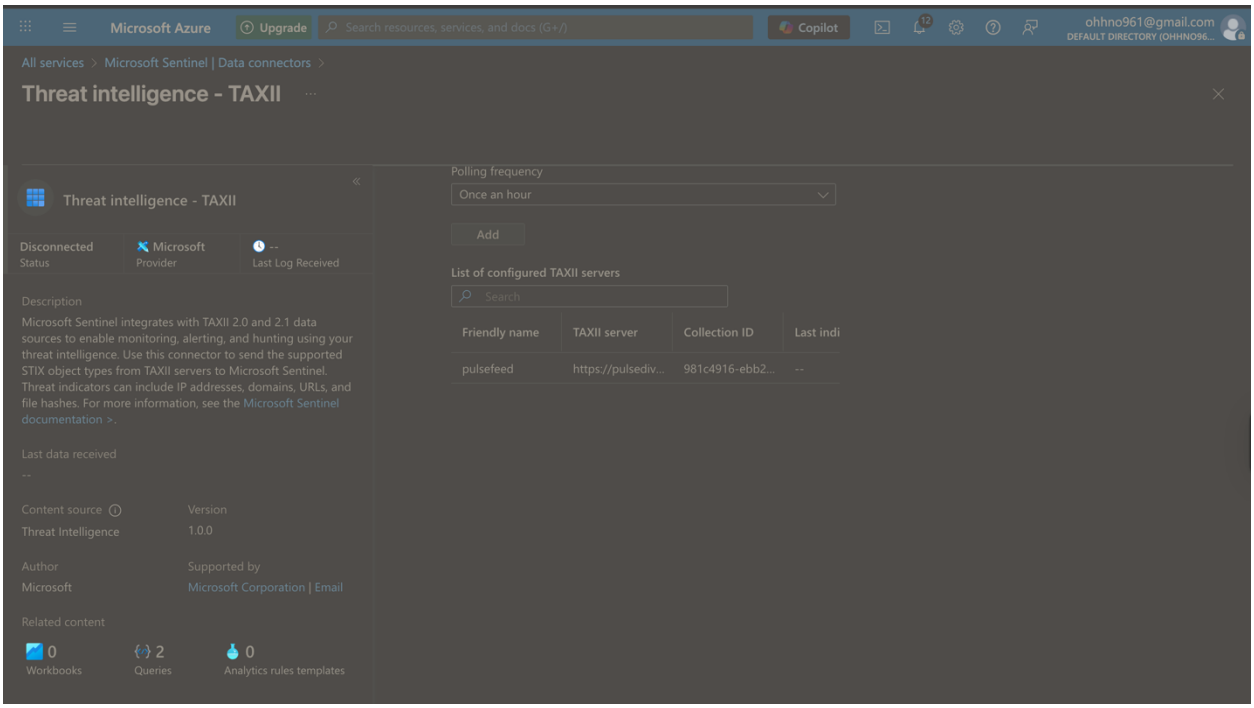
- **API Root URL**: Obtained from PulseDive
- **Collection ID**: Provided by PulseDive
- **Authentication**: API key

Path:
`Sentinel → Data Connectors → Threat Intelligence - TAXII`

Outcome:
TAXII server configured to stream STIX 2.0/2.1 objects into Sentinel's threat intelligence platform.


portal.azure.com/#view/Microsoft_Azure_Security_Insights/ConnectorPage.ReactView/dataConnectorId/ThreatIntelligenceTaxii/subsc...
Microsoft Azure
Upgrade
Copilot
ohhno961@gmail.com
DEFAULT DIRECTORY (OHHNO96...
All services > Microsoft Sentinel | Data connectors >
Threat intelligence - TAXII
Threat intelligence - TAXII
Disconnected
Status
Microsoft
Provider
--
Last Log Received
Description
Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send the supported STIX object types from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes. For more information, see the Microsoft Sentinel documentation >.
Last data received
--
Content source
Threat Intelligence
Version
1.0.0
Author
Microsoft
Supported by
Microsoft Corporation | Email
Related content
0
Workbooks
2
Queries
0
Analytics rules templates
Prerequisites
To integrate with Threat intelligence - TAXII make sure you have:
Workspace: read and write permissions.
TAXII Server: TAXII 2.0 or TAXII 2.1 Server URI and Collection ID.
Configuration
Configure TAXII servers to stream STIX 2.0 or 2.1 STIX objects to Microsoft Sentinel
You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector. For detailed configuration instructions, see the full documentation.
Enter the following information and select Add to configure your TAXII server.
Friendly name (for server) *
API root URL *
Collection ID *
Username


pulsedive.com/dashboard/
Pulsedive
Community
Dashboard
Explore
Analyze
API
About
kali1
Display mode:
Analyst
SOC
Dashboard
Search Pulsedive
Industry Events
Conference and CFP data is pulled from CFPTime.
SANS DFIR Summit
Salt Lake City, Utah
2025-07-23 00:00:00
23 hours ago
Community Stream
All
News
Pulsedive
2025:
exploited
here's
Microsoft
SharePoint
tested



7. Custom Log Collection Setup

Objective: Ingest custom logs via AMA
Path:
`Log Analytics Workspaces → sentinel-defender-lab → Tables → Create custom log`

Attempted Workflow:

1. **Basics Tab**:
   - Table name: Specified
   - Created new Data Collection Rule (DCR): `nyc-cl-collection-rule`
   - Resource Group: `secops_projects`
2. **Data Collection Endpoint**:
   - Created endpoint `costume-log-site`
   - Status: **Provisioning Succeeded**
3. **Failure Point**:
   - Endpoint not visible in DCR configuration interface
   - Target selection (Kali VM) failed due to subscription limitations

Issue Diagnosis:
Possible causes for endpoint visibility failure:

- Regional mismatch between endpoint and workspace
- RBAC permission gaps
- Azure Resource Manager propagation delay

Summary of Outstanding Issues

Component	Issue Description	Next Steps
Sysmon for Linux	Agent deployment status unknown	Verify agent heartbeat in Logs
Custom Log Collection	Endpoint-DCR association failure	Validate regional alignment
	Kali VM not selectable	Check subscription quotas
Data Collection Rules	Schema mapping incomplete	Retry with Windows VM test

Recommended Actions for Future Implementation

1. **Permission Validation**
    - Confirm `Microsoft Sentinel Contributor` role propagates to workspace level
2. **Data Collection Troubleshooting**
    - Recreate DCR and endpoint in the same region as the workspace
    - Use an Azure Windows VM for initial testing
3. **Cost Management**
    - Enable Azure Cost Alerts to monitor spending
4. **Agent Deployment**
    - Run Sysmon installation script manually on the Linux VM
5. **TAXII Feed Verification**
    - Query `ThreatIntelligenceIndicator` table in Logs

---

portal.azure.com/#view/Microsoft_OperationsManagementSuite_Workspace/CreateCustomLogV2TableBlade/workspaceResourceId/...

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | ohhno961@gmail.com DEFAULT DIRECTORY (OHHNO96...

All services > Log Analytics workspaces > Sentinel-Defender-Lab | Tables >

Create a custom log

Basics | Schema and transformation | Review

Table details

Start by adding a name and description for the table you're creating. On the next step, upload a sample of your custom log and adjust the table details to your needs.

Table name * — Up to 45 alphaunumeric characters _CL

Description — Description

Data collection rule

Data collection rules (DCR) define the data coming into Azure Monitor and specify where that data should be sent or stored. Learn more

Data collection rule * — Create a new data collection rule

Data collection endpoint * — No data collection endpoints were found in this region

« Previous | Next

---

portal.azure.com/#view/Microsoft_Azure_Monitoring/AzureMonitoringBrowseBlade/~/dataCollectionEndpoints

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | ohhno961@gmail.com DEFAULT DIRECTORY (OHHNO96...

All services > Monitor

Monitor | Data Collection Endpoints

Microsoft

Create data collection endpoint — Data collection endpoint customlogsite successfully created.

Search

- Alerts
- Metrics
- Logs
- Change Analysis
- Service health
- Workbooks
- Dashboards with Grafana (preview)
- Insights
- Managed Services
- Settings
  - Diagnostic settings
  - Data Collection Rules
  - Data Collection Endpoints
  - Azure Monitor pipelines (preview)
  - Autoscale
  - Private Link Scopes
- Support + Troubleshooting

Add or remove favorites by pressing Cmd+Shift+F

Create | Manage view | Refresh | Export to CSV | Open query | Assign tags | Delete

Filter for any field... | Subscription equals all | Resource group equals all | Location equals all | Add filter

Showing 0 to 0 of 0 records. | No grouping | List view

Name	Subscription	Resource group	Location

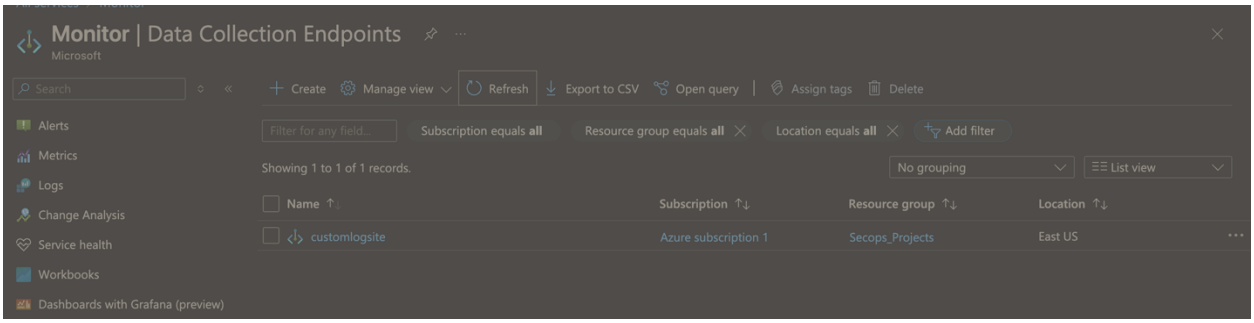
No data collection endpoints to display

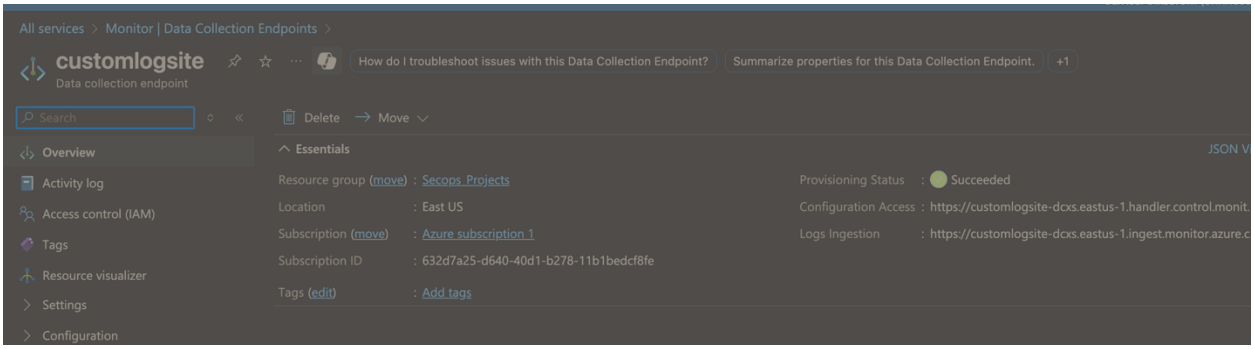
Simplify data ingestion from diverse sources into Azure with a scalable endpoint that ensures efficient and reliable data collection for analytics and insights.

Create data collection endpoint

Learn more

Give feedback


Monitor | Data Collection Endpoints
Microsoft
Search
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Delete
Alerts
Metrics
Logs
Change Analysis
Service health
Workbooks
Dashboards with Grafana (preview)
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 1 to 1 of 1 records.
No grouping
List view
Name
Subscription
Resource group
Location
customlogsite
Azure subscription 1
Secops_Projects
East US


All services > Monitor | Data Collection Endpoints >
customlogsite
Data collection endpoint
How do I troubleshoot issues with this Data Collection Endpoint?
Summarize properties for this Data Collection Endpoint.
+1
Search
Delete
Move
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Settings
Configuration
Essentials
JSON V
Resource group (move) : Secops_Projects
Location : East US
Subscription (move) : Azure subscription 1
Subscription ID : 632d7a25-d640-40d1-b278-11b1bedcf8fe
Tags (edit) : Add tags
Provisioning Status : Succeeded
Configuration Access : https://customlogsite-dcxs.eastus-1.handler.control.monit.
Logs Ingestion : https://customlogsite-dcxs.eastus-1.ingest.monitor.azure.c

Home > Monitor | Data Collection Rules >

Create Data Collection Rule

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

Basics | Resources | Collect and deliver | Tags | Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. Learn more

Rule details

Rule Name *	DCR-CustomLogs-SecOps-EastUS2
Subscription *	Azure subscription 1
Resource Group *	Secops_Projects Create new
Region *	East US
Platform Type *	Windows Linux All
Data Collection Endpoint	dce-secops-eastus2

Review + create | < Previous | Next : Resources >

Home > Monitor | Data Collection Rules >

Create Data Collection Rule

Data collection rule management

Form validation failed in Collect and deliver tab.

To create a Data Collection Rule that collects platform metrics, click here.

Basics | Resources | Collect and deliver | Tags | Review + create

Basics

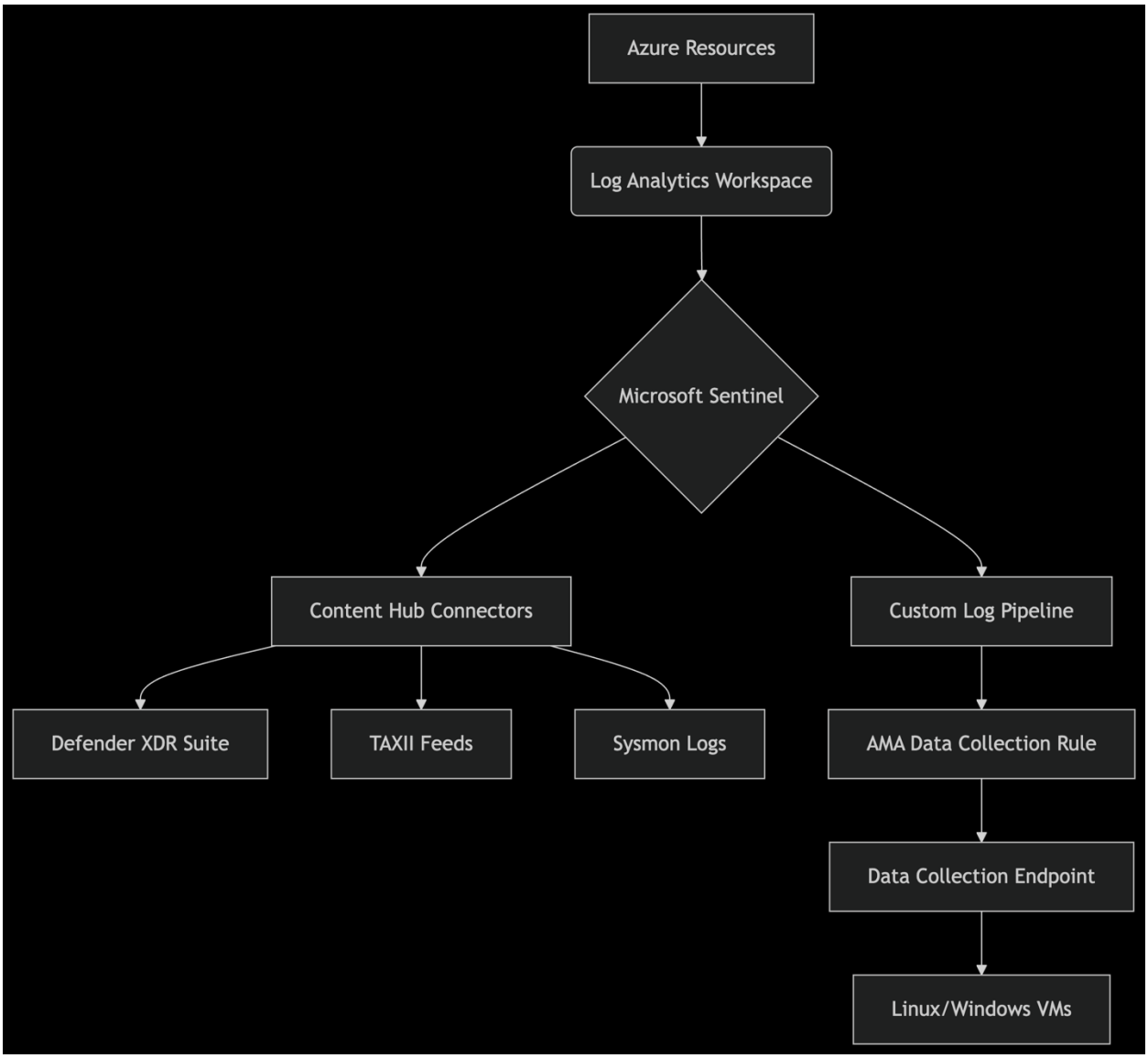
Data rule name	DCR-CustomLogs-SecOps-EastUS2
Subscription	Azure subscription 1
Resource Group	Secops_Projects

Selected resources

Resources	Type
kali-vm-lab-001	microsoft.compute/virtualmachines

Showing 1 - 1 of 1 results.

Create | < Previous | Next: >



Conclusion

The Sentinel lab deployment demonstrates foundational competency in designing and implementing a cloud-native SIEM solution using Microsoft Azure. By integrating critical telemetry sources, configuring role-based permissions, and enabling threat intelligence ingestion, this project lays the groundwork for advanced detection engineering, incident response, and threat hunting workflows.

While some limitations (e.g., Linux agent visibility and DCR binding) remain due to subscription constraints, the architecture is modular, scalable, and aligned with Microsoft's best practices for security operations. Future iterations will focus on endpoint telemetry validation, log enrichment, KQL detection rules, and integration with automated response mechanisms (Logic Apps or Azure Automation).

This hands-on configuration effort not only reinforces Sentinel platform expertise but also demonstrates real-world readiness for SOC analyst tasks—ranging from connector deployment to troubleshooting log pipelines.