



Technical Workshop

Azure Sentinel

Sharon KO

Advanced Security Analytics – Global Black Belt

 [ko-sharon](#)
 [ko-sharon](#)

Agenda

1. Design and setup
2. Data collection
3. KQL introduction
4. Externaldata Query / Watchlist
5. Analytics, Hunting and Workbooks
6. Threat Intelligence
7. Playbooks and automation

Azure Sentinel Ninja L400 Training

Part 1: Overview

- Module 0: Other learning and support options
- Module 1: Get started with Azure Sentinel
- Module 2: How is Azure Sentinel used?

Part 2: Architecting & Deploying

- Module 3: Workspace and tenant architecture
- Module 4: Data collection
- Module 5: Log Management
- Module 6: Enrichment: TI, Watchlists, and more

Part 3: Creating Content

- Module 7: The Kusto Query Language (KQL)
- Module 8: Analytics
- Module 9: SOAR
- Module 10: Workbooks, reporting, and visualization
- Module 11: Use cases and solutions

Part 4: Operating

- Module 12: A day in a SOC analyst's life, incident management, and investigation
- Module 13: Hunting
- Module 14: User and Entity Behavior Analytics (UEBA)
- Module 15: Monitoring Azure Sentinel's health

Part 5: Advanced Topics

- Module 16: Extending and Integrating using Azure Sentinel APIs
- Module 17: Bring your own ML



<https://techcommunity.microsoft.com/t5/azure-sentinel/become-an-azure-sentinel-ninja-the-complete-level-400-training/ba-p/1246310>

Azure Sentinel Technical Playbook for MSSPs

Access the document here –

<http://aka.ms/azsentinelmssp>

- Azure Sentinel's capabilities
- Technical dependencies
- Data collection models
- Multi-tenant management
- Threat detection & analytics
- Investigation processes
- Strategies for automated response
- Activity summaries and reports
- Cost models and data storage



Azure Sentinel Technical Playbook for MSSPs

How to deploy Azure Sentinel as a managed security services provider

Published: March-2021, Revision: V0.9

Microsoft Cloud Security Private Preview Program

Sign up via this link – <https://aka.ms/SecurityPrP>

The screenshot shows a sign-up form for the Microsoft Cloud + AI Security Preview Program. It features a Microsoft logo at the top left and a large title "Microsoft Cloud Security Private Preview Program" in the center. Below the title, there's a welcome message and a paragraph about the preview program. It includes links for the Online Services Terms and a privacy statement. At the bottom, there's a section for entering organization information, with a note about required fields.

Welcome to the sign-up form for our Cloud + AI Security Preview Program.

Here you will have the option to sign-up for a single preview feature or our ongoing preview program. By signing up for the ongoing program, you will receive access to our monthly publication of all preview features as well as be notified of relevant previews when they are available to try.

The features disclosed to you under the Preview Program are Microsoft's Confidential Information. Your use of those features are subject to the Online Services Terms, including the terms applicable to previews.
<https://aka.ms/MicrosoftOST>

At any point you may opt-out of receiving private preview communications, by filling out this form:
https://aka.ms/OptOut_PrivatePreviewProgram

Microsoft respects your privacy. Review our online Privacy Statement here: <https://privacy.microsoft.com/en-us/privacystatement>

...
* Required
1. Your organization *
Enter your answer

The screenshot shows a document titled "Cloud + AI Security" and "Private Feature-Preview Program". It includes a "March 2021 Edition" header and a "Important Note" about confidential information and preview terms. It features an "Overview" section with a goal of gaining quality insight on products and capabilities before release. It also includes a call to action for joining previews at <https://aka.ms/SecurityPrP>. Below this is an "Azure Security Center" section with a table of feature previews and their details.

Important Note: The content disclosed within this document is Microsoft's Confidential Information. All private previews are subject to the [Online Services Terms](#), including the terms applicable to previews.

At any point you may opt-out of receiving private preview communications, by filling out [this form](#).

Overview

The goal of our private feature-preview program is to gain quality insight on our products and capabilities before we release them to the general public. Because of this, we are continually seeking NDA-participants that are willing to try-out our features and give direct input/suggestions.

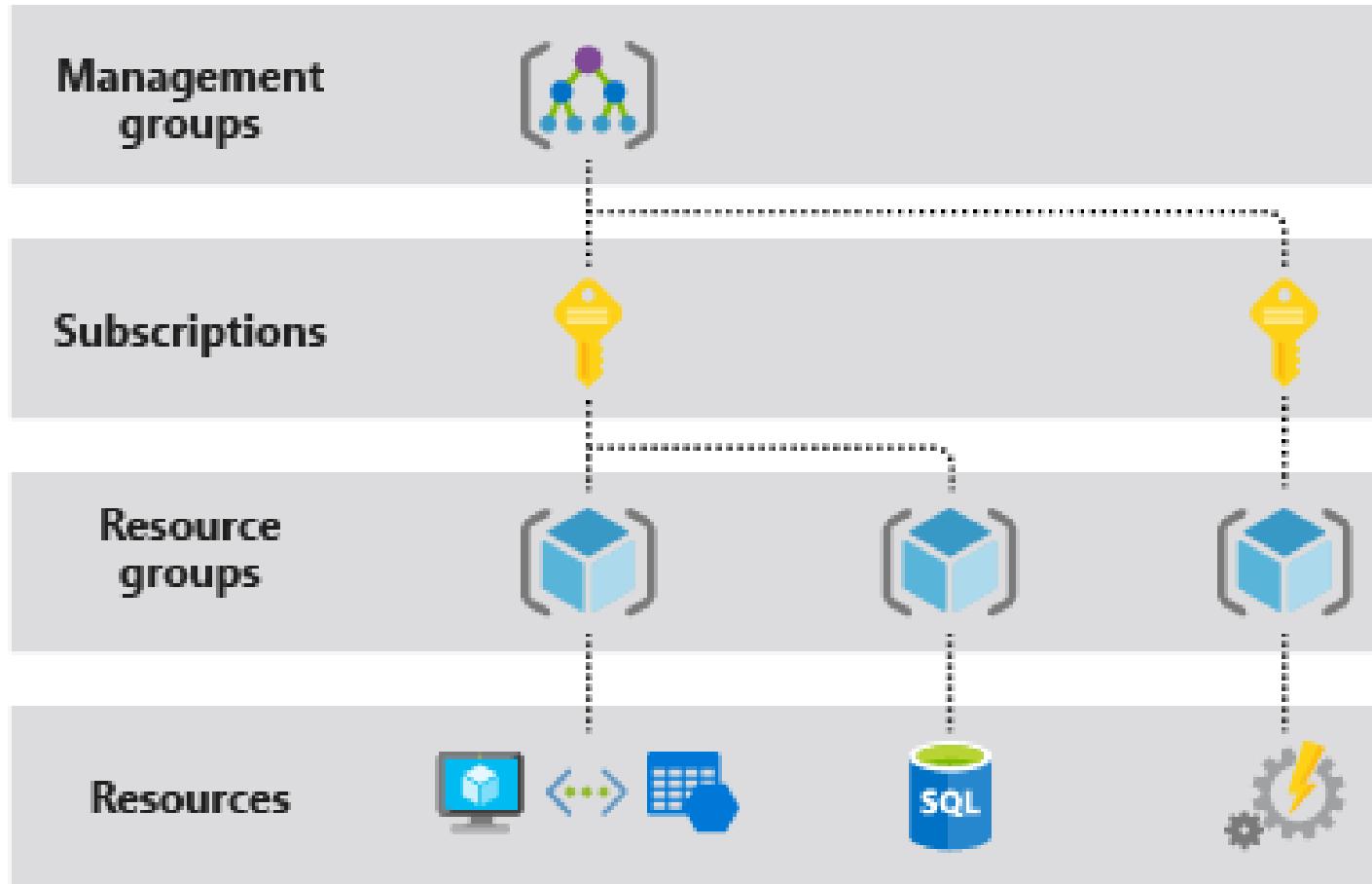
At any time, join one of our previews (or our ongoing preview program) at: <https://aka.ms/SecurityPrP>

Azure Security Center

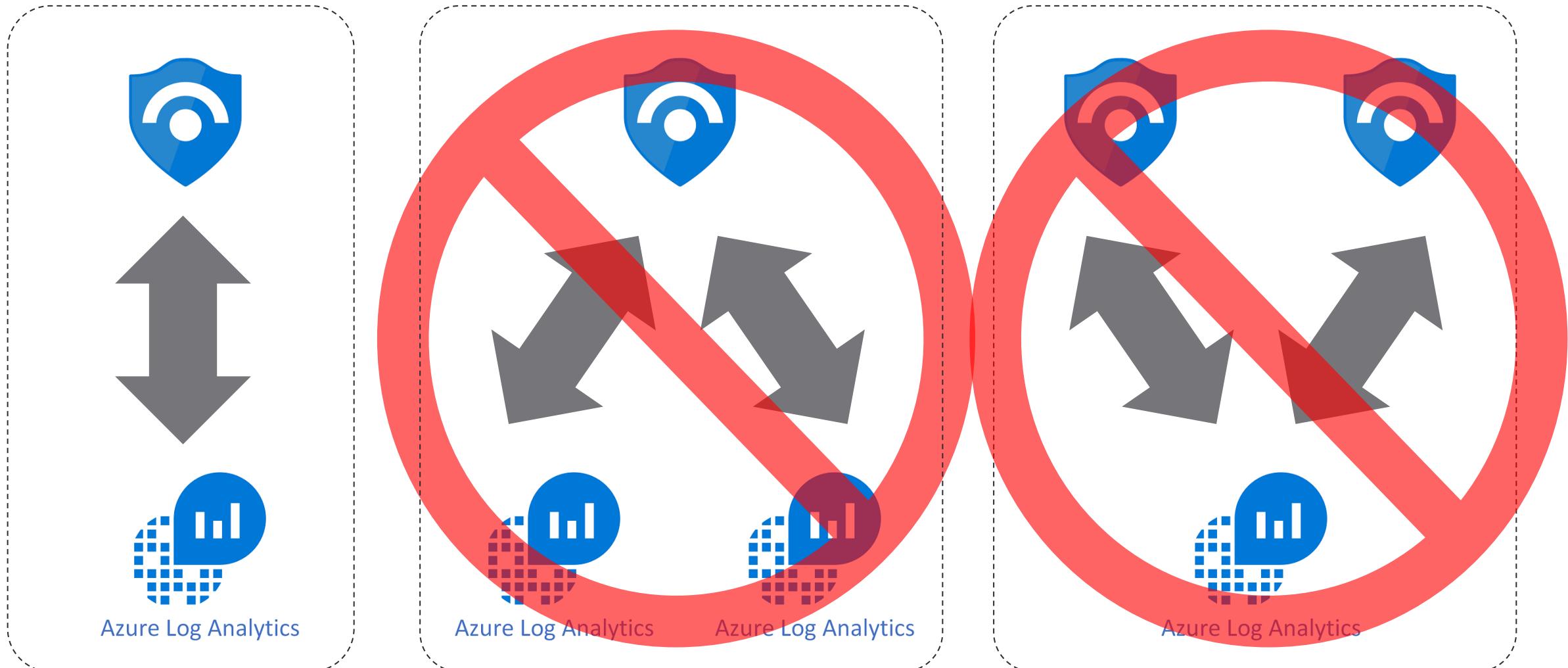
Feature Preview	Start	Time Needed	Prerequisites/Comments
ASC enrichment with Azure Purview data	MAR. 9, 2021	1-2 Hours	Use Azure Purview to classify resources with auto-classification rules. Azure Defender enabled. Sign-up
Guest Configuration Based Recommendation in ASC	MAR. 4, 2021	Less than 1 hour	Subscription registered to Security Center & a running Az. virtual machine is required.
Azure Audit Reports	FEB. 10, 2021	1-2 Hours	Azure Security Center Environment
Systems Updates v2	FEB. 9, 2021	Less than 1 hour	Azure Compute virtual machine or online/active Azure Arc machine. Sign-up
CI/CD Build-Stage Vulnerability Assess.	FEB. 4, 2021	Less than 1 hour	Azure Security Center Environment
ASC transition to Azure Monitor Agent	FEB 3, 2021	2+ Hours	AMA supported OS versions for Windows and Linux
Azure Defender for Kubernetes Anywhere	JAN 26, 2021	1-2 Hours	1+ Kubernetes cluster (Vanilla, AKS Engine, OpenShift version 4+). Azure Security Center enabled on your designated subscription.

Design and Setup

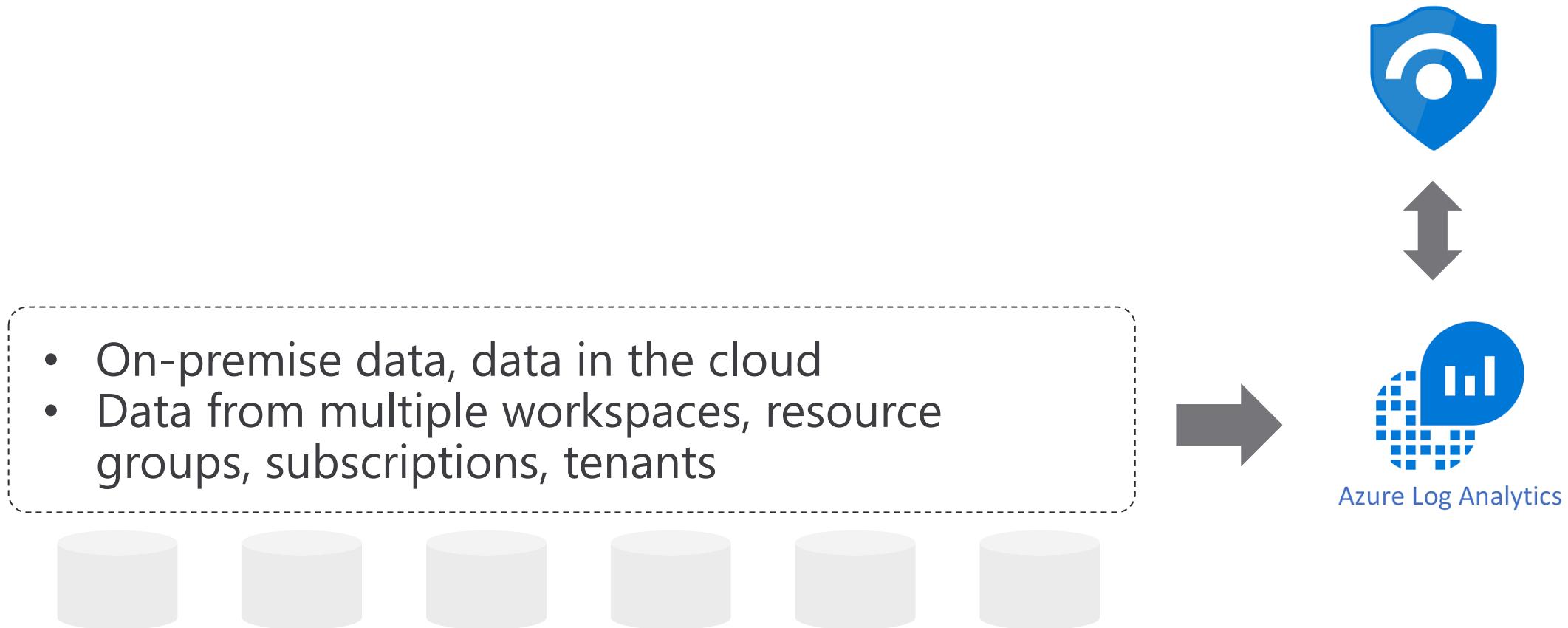
Azure subscriptions and resources



Log Analytics workspace to Azure Sentinel connection is 1-to-1



Data can be sent from multiple sources into 1 Log Analytics workspace



Lab: Create a Log Analytics workspace, then an Azure Sentinel instance

Home > Log Analytics workspaces > Log Analytics

Log Analytics workspace

Create new or link existing workspace

Create New Link Existing

*Log Analytics Workspace
Select a workspace

Subscription *

Resource group *

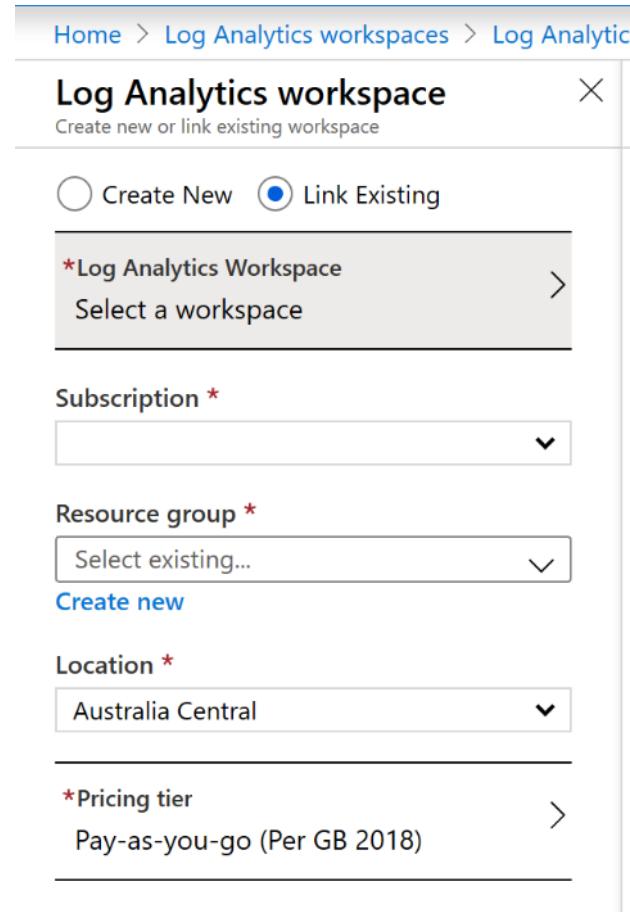
Select existing...

Create new

Location *

Australia Central

*Pricing tier
Pay-as-you-go (Per GB 2018)



Home > Azure Sentinel workspaces > Choose a workspace to add to Azure Sentinel

Azure Sentinel workspaces

Microsoft

+ Add Refresh

Filter by name

Workspace
eastus
westeurope
australiacentral
eastus2
northcentralus
eastus
eastus

Choose a workspace to add to Azure Sentinel

Search workspaces

+ Create a new workspace

eastus

eastus

eastus

westeurope

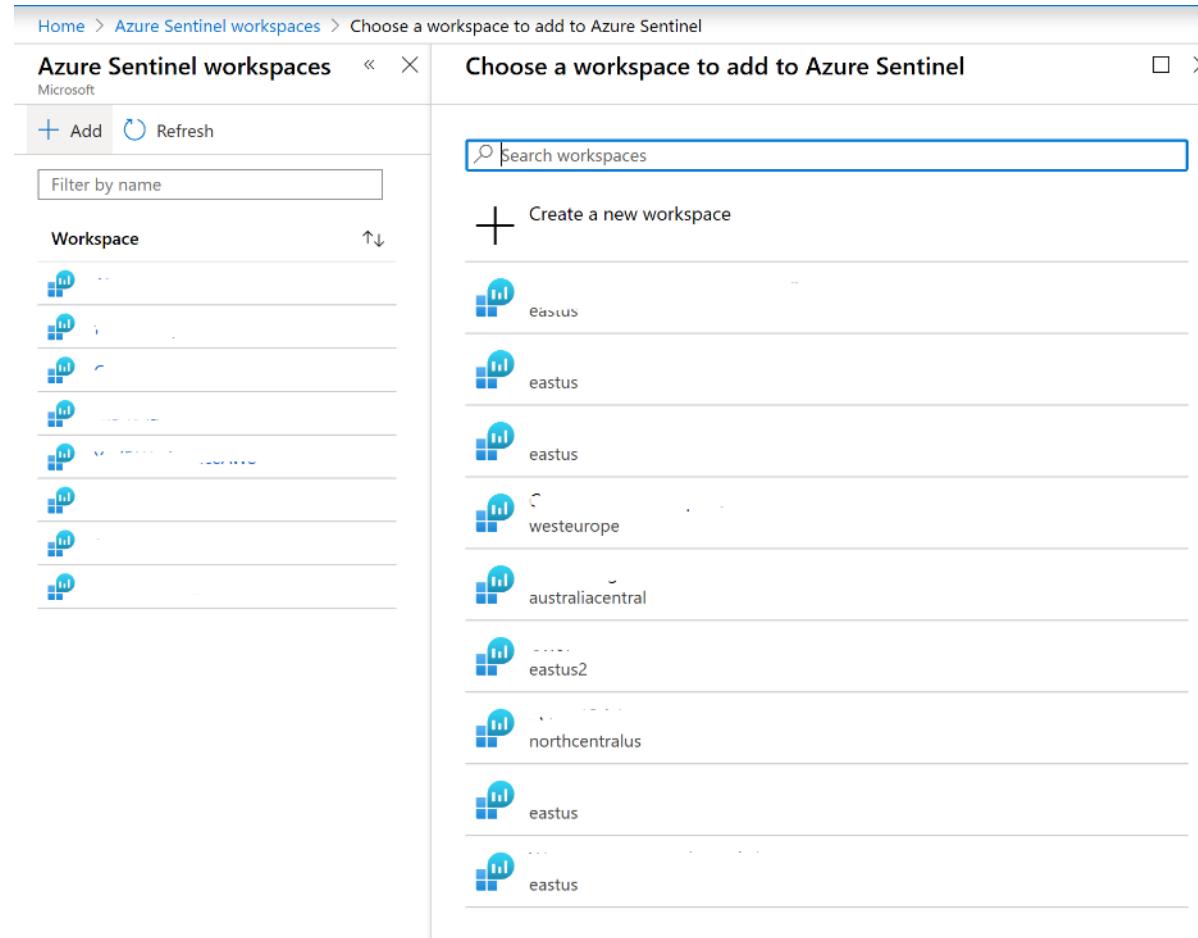
australiacentral

eastus2

northcentralus

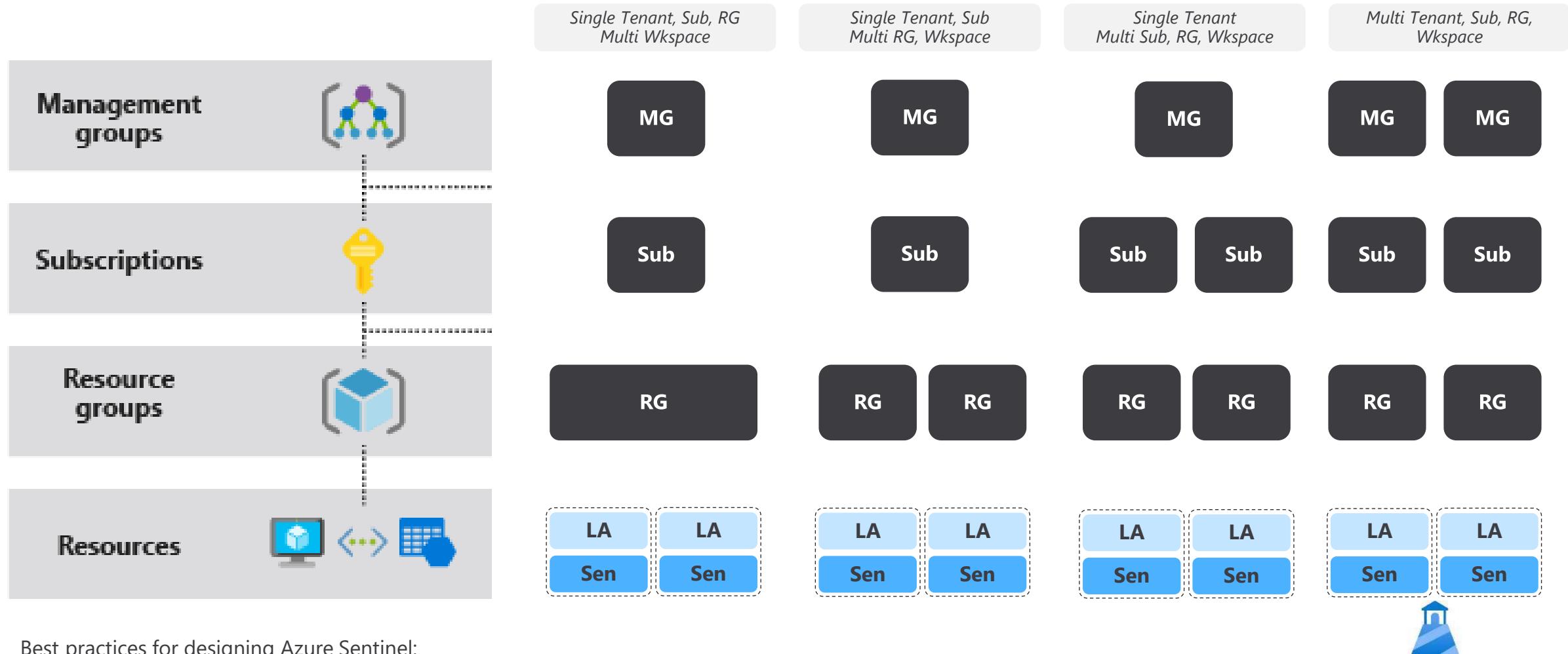
eastus

eastus



Minimum rights required for creation: Subscription contributor

Possible Azure Sentinel Deployments



Best practices for designing Azure Sentinel:

<https://techcommunity.microsoft.com/t5/azure-sentinel/best-practices-for-designing-an-azure-sentinel-or-azure-security/ba-p/832574>

Demo: Multi-Workspace Support

Works across workspaces:

- Queries
- Dashboards
- Hunting
- Alert rules (up to 20 workspaces per single query)

Also across tenant using Azure Lighthouse



Doesn't work across workspaces:

- Cases
- Investigation

Extend Azure Sentinel across workspaces and tenants:

<https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>

The screenshot shows the Azure portal's 'Directory + subscription' configuration screen. It includes sections for 'Default subscription filter' and 'Current + delegated directories'. A blue callout bubble points to the 'Microsoft' checkbox in a list of selected subscriptions, with the text 'Lighthouse enables multi-tenant selector'.

Subscription
<input type="checkbox"/> Select all
<input checked="" type="checkbox"/> Microsoft
<input checked="" type="checkbox"/> contoso.com (4b2462a4-bbee-495a-a0e1-f23ae524cc9c)
<input type="checkbox"/> Default Directory (1822d27a-ae9a-4c67-bef0-a0421f07903d)

```
workspace("contosoretail-IT"). AzureActivity  
| limit 10
```

```
workspace("CyberSecurityDemo"). AzureActivity  
| limit 10
```

Azure Sentinel RBAC

Actions

- Reader
- Responder
- Contributor (Sentinel)
- Contributor (Sentinel & LogicApp)

Role	Create and run playbooks	Create and edit dashboards, analytic rules, and other Azure Sentinel resources	Manage incidents (dismiss, assign, etc.)	View data, incidents, dashboards and other Azure Sentinel resources
Azure Sentinel reader	--	--	--	X
Azure Sentinel responder	--	--	X	X
Azure Sentinel contributor	--	X	X	X
Azure Sentinel contributor + Logic App contributor	X	X	X	X

Users can define custom roles

Data

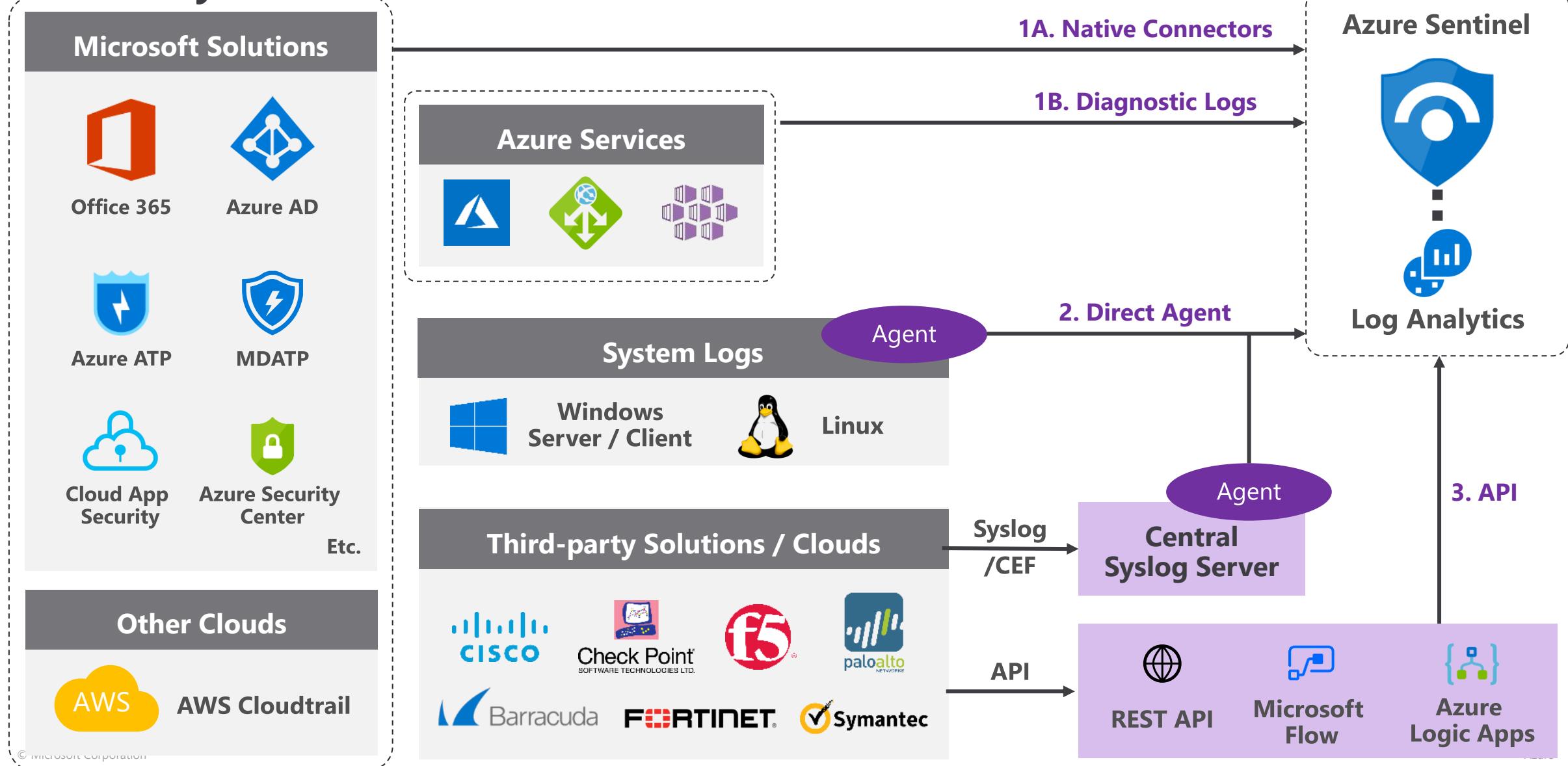
- Resource-context (workspace)
- Table-level RBAC ([more info](#))

Permissions in Azure Sentinel:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

Data Collection

Summary of Data Collection of Azure Sentinel





Data Dictionaries (DD)

Common Data Model
(CDM)

Detection Model (DM)

<https://ossemproject.com/intro.html>

Query explorer X

NormalizedNetworkParsers X

▼ Saved Queries

 ▼ NormalizedNetworkParsers

- fx CheckPoint_Network_No...
 fx Empty_Network_Normali...
 fx Network_MetaParser
 fx PAN_9_Network_Normali...
 fx WindowsFW_Network_N...
 fx WireData_Network_Norm...
 fx ZScaler_Network_Normal...

Network_MetaParser

Empty_Network_NormalizedParser

CheckPoint_Network_No
rmalizedParser

PAN_9_Network_Norma
lizedParser

WireData_Network_Nor
malizedParser

...

Syslog / CEF

- <https://docs.microsoft.com/en-us/azure/sentinel/normalization-schema>
- <https://docs.microsoft.com/en-us/azure/sentinel/normalization>

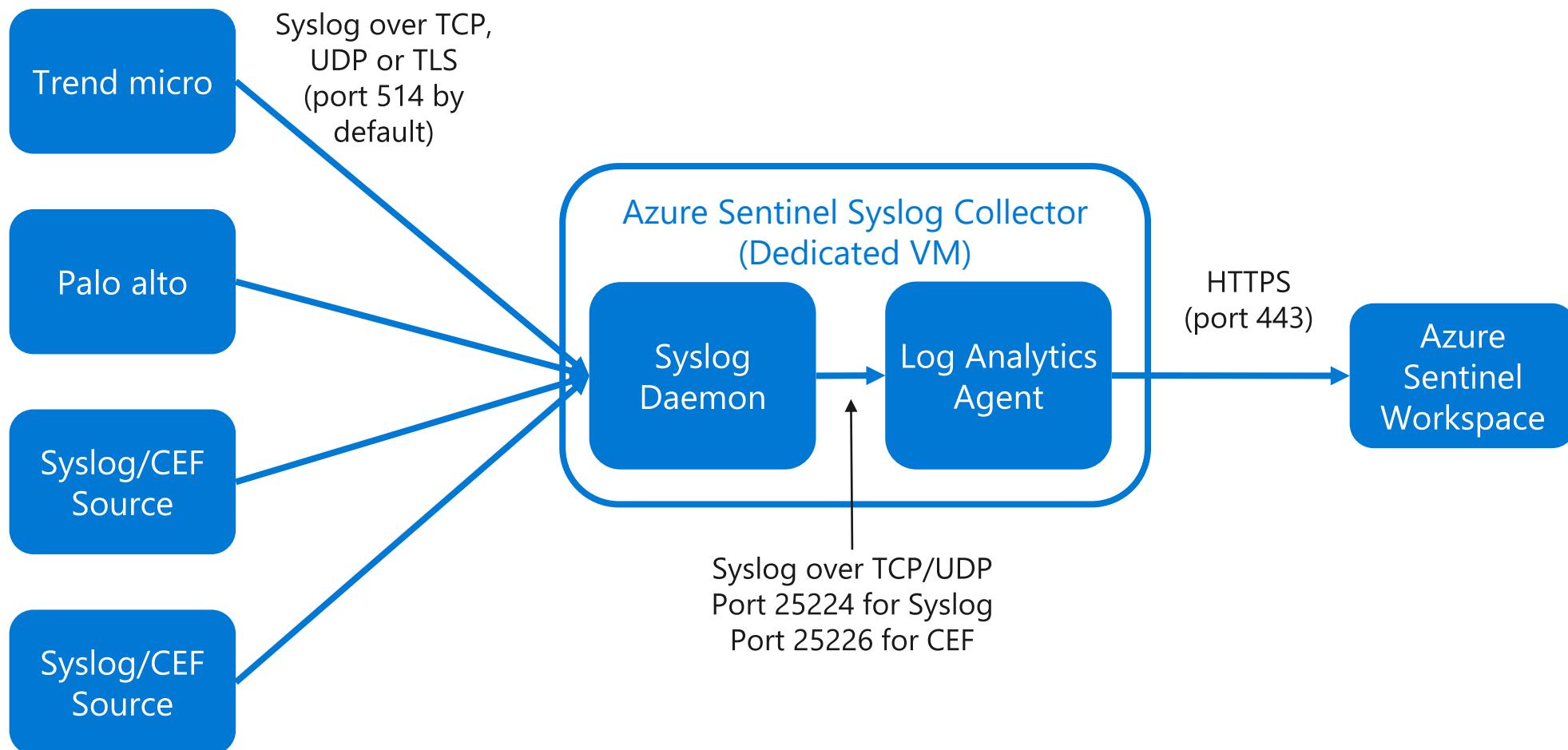
Demo: Connect Azure Activity Data Connector

The screenshot shows the Azure Sentinel Data connectors page. On the left, there's a navigation sidebar with links like Home, Overview, Logs, News & guides, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence), Configuration (Data connectors, Analytics, Watchlist [Review], Automation, Community, Settings), and a search bar. The main area displays a summary: 98 Connectors, 2 Connected, and 0 Coming soon. A search bar at the top right allows filtering by connector name (e.g., "azure activity"), provider (All), data type (All), and status (All). Below this, a list of connectors is shown, with "Azure Activity" highlighted. To the right of the list is a detailed view of the Azure Activity connector. It shows the connector is connected to Microsoft and was last updated 5 days ago. A description notes that Azure Activity Log is a subscription log providing insight into subscription-level events in Azure, including Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure. It also mentions the last date received (04/01/21, 07:33 PM) and related content (3 Workbooks, 2 Quicks, 10 Analytic rules/templates). A chart titled "Data received" shows a sharp peak of 452 on March 28, with a total count of 452. Below the chart, it says "Last data received 04/01/21, 07:33 PM". At the bottom right of the connector view is a blue button labeled "Open connector page".

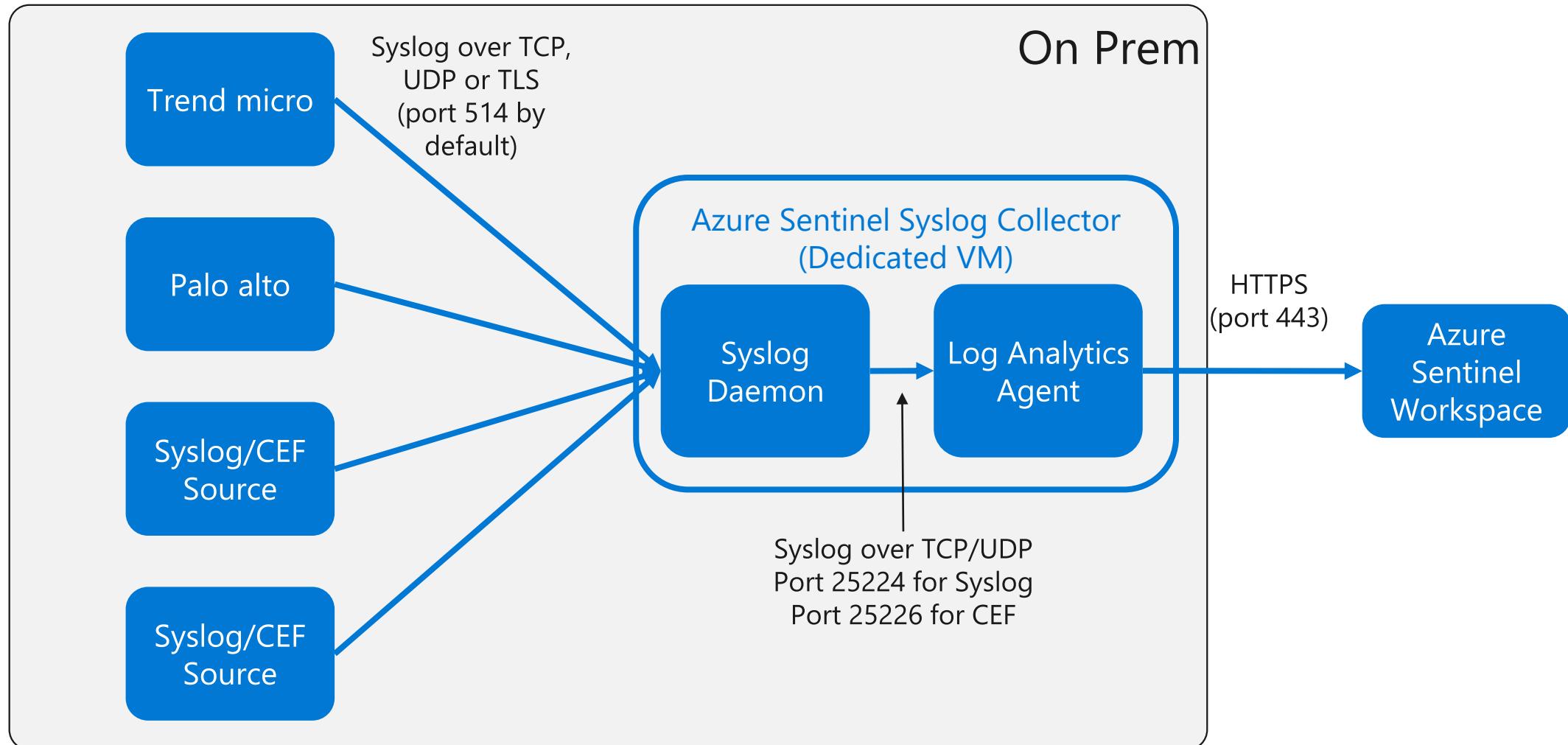
Minimum rights required for connection: varies per connector
(Azure Activity = workspace read, write permissions)

#2

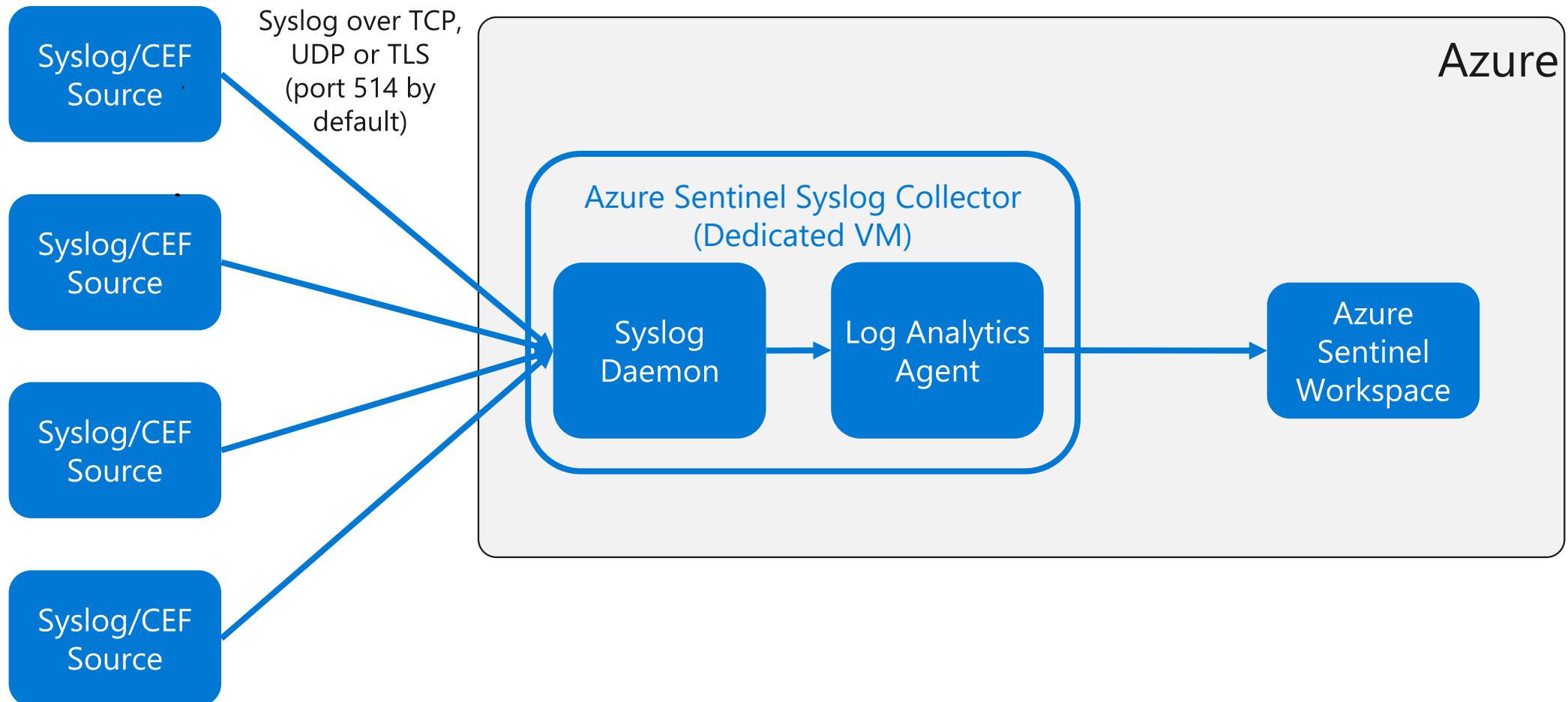
Other Sources via Syslog / CEF



#2 On-Premise Data Collection – On-Premise Collector

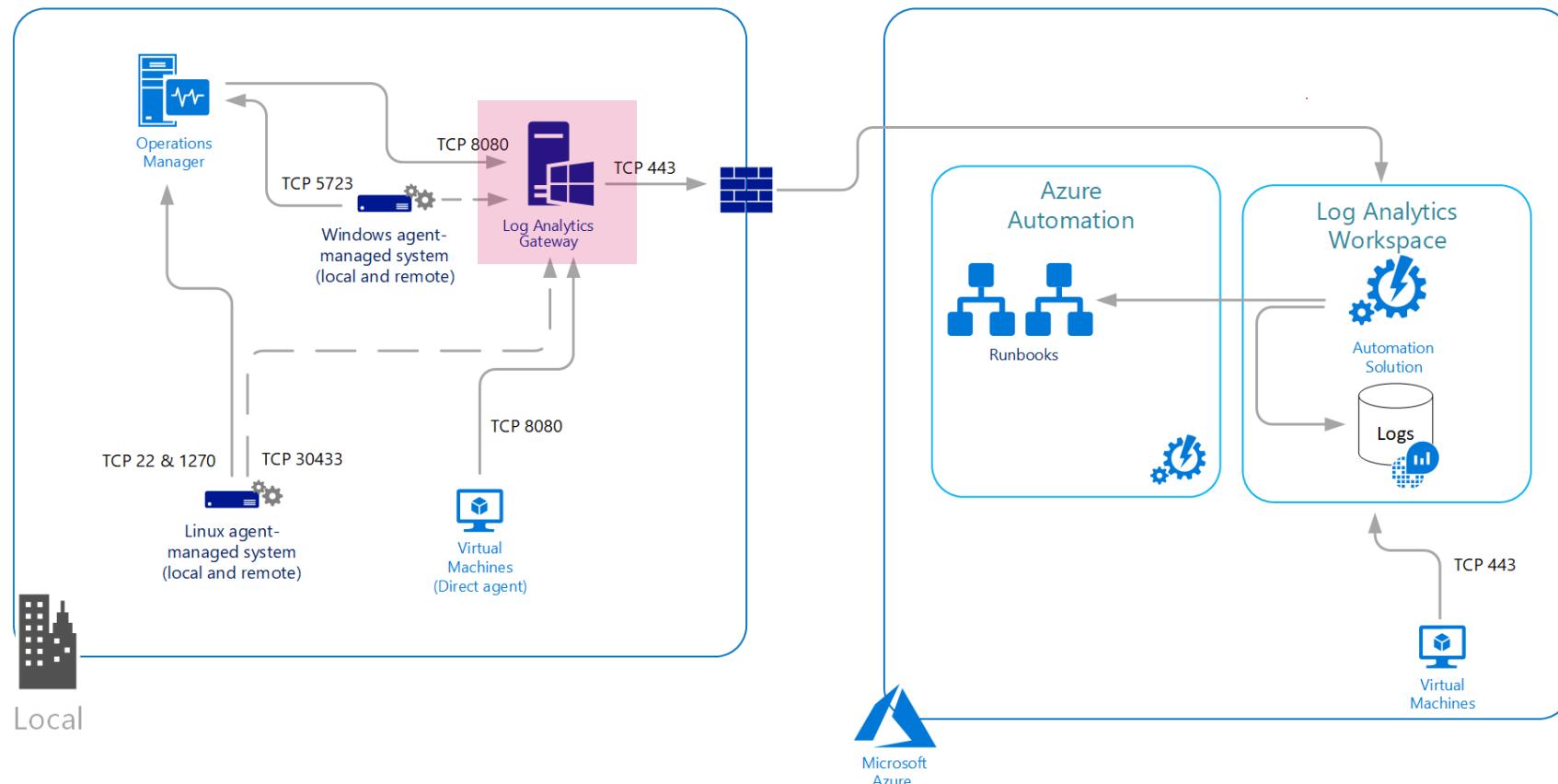


#2 On-Premise Data Collection – Cloud-based Collector



#2

Connect computers without internet access by using the Log Analytics gateway in Azure Monitor



If your IT security policies do not allow computers on the network to connect to the Internet, you can set up a [Log Analytics gateway](#) and then configure the agent to connect through the gateway to Azure Monitor logs.

#3 API ingest – via Logic Apps / Azure Functions

Custom deployment ...

Deploy from a custom template

Basics Review + create

Template

Customized template 9 resources

Project details

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

Subscription * SK-internal

Resource group * Create new

Instance details

Region * Australia East

Function Name <enter a default Function Name>

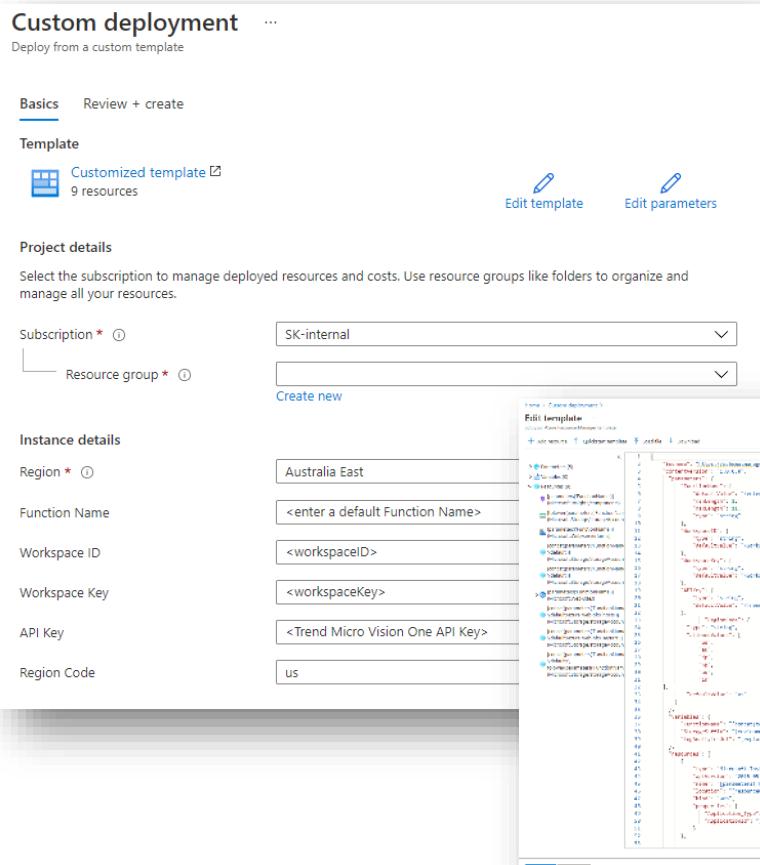
Workspace ID <workspaceID>

Workspace Key <workspaceKey>

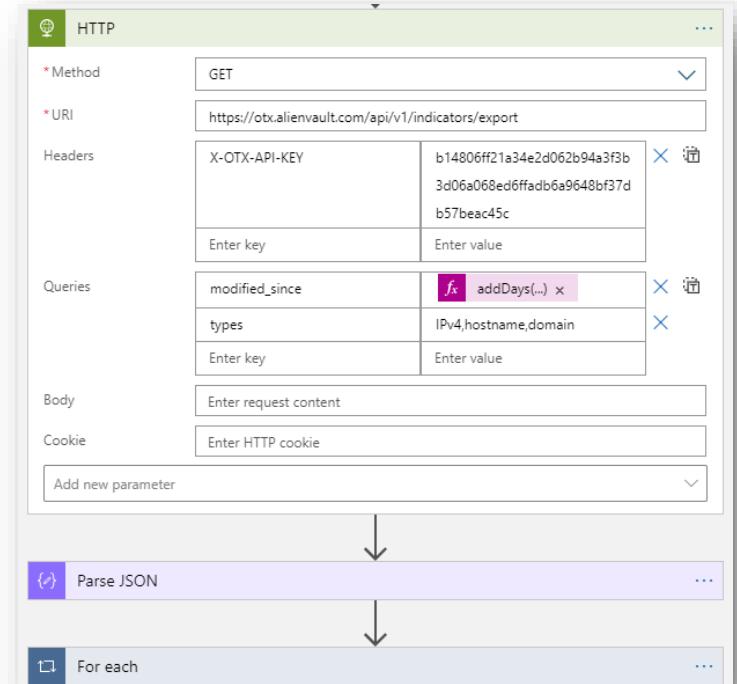
API Key <Trend Micro Vision One API Key>

Region Code us

Custom deployment



Functions	Logic Apps
Developer Productivity	Visual Designer
Triggers and Bindings	200+ Connectors
Flexible Deployment options	Functions Orchestration



Define data retention (workspace)

Home > Azure Sentinel workspaces > Azure Sentinel > CyberSecurityDemo - Usage and estimated costs

CyberSecurityDemo - Usage and estimated costs

Log Analytics workspace

Search (Ctrl+ /)

General

- Quick Start
- Workspace summary
- View Designer
- Logs
- Solutions
- Saved searches
- Pricing tier
- Usage and estimated costs**
- Properties
- Service Map

Usage details Daily cap Data Retention Help

Pricing tier: Per GB (2018)

The table below shows estimated monthly costs* for this Log Analytics resource based on the last month's usage.

Item type	Price	Monthly usage (last 31 days)	Estimated monthly cost
Log data ingestion	\$2.76	81.22 GB	\$224.17
Log data retention	\$0.12	83.31 GB	\$10.00
\$234.16			

* Estimates do not include taxes which may be applied to this subscription. It doesn't reflect Security nodes charges and included data volume in this blade.

Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges.

Data Retention (Days)

60

OK

Retention by table

Retention by data type

It is also possible to specify different retention settings for individual data types. Each data type is a sub-resource of the workspace. For instance the SecurityEvent table can be addressed in [Azure Resource Manager](#) as:

```
/subscriptions/00000000-0000-0000-0000-0000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.OperationalInsights/datasets/SecurityEvent
```

Note that the data type (table) is case sensitive. To get the current per data type retention settings of a particular data type (in this example SecurityEvent), use:

```
JSON  
GET /subscriptions/00000000-0000-0000-0000-0000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.OperationalInsights/datasets/SecurityEvent?api-version=2016-09-01
```

To get the current per data type retention settings for all data types in your workspace, just omit the specific data type, for example:

```
JSON  
GET /subscriptions/00000000-0000-0000-0000-0000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.OperationalInsights/datasets?api-version=2016-09-01
```

To set the retention of a particular data type (in this example SecurityEvent) to 730 days, do

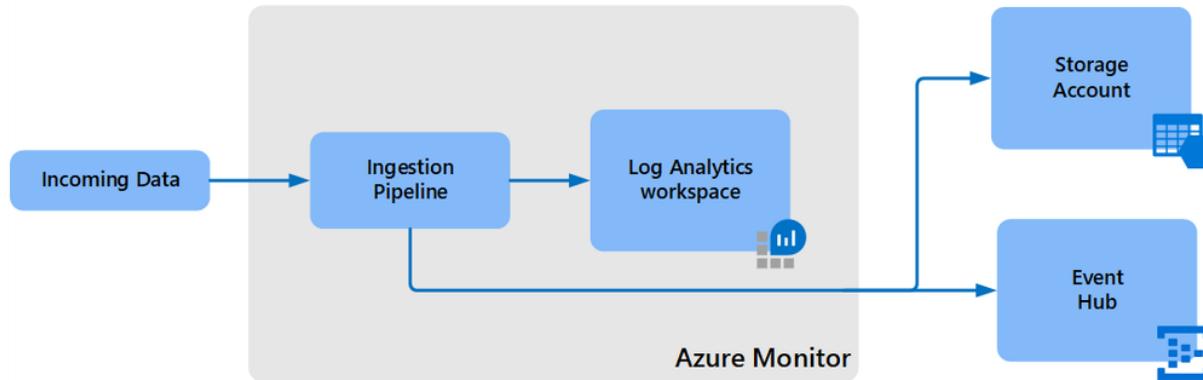
```
JSON  
PUT /subscriptions/00000000-0000-0000-0000-0000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.OperationalInsights/datasets/SecurityEvent?api-version=2016-09-01  
{  
  "properties": {  
    "retentionInDays": 730  
  }  
}
```

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-cost-storage#retention-by-data-type>

Long Term Retention of Logs (Alternatives)

Log Analytics Data Export feature

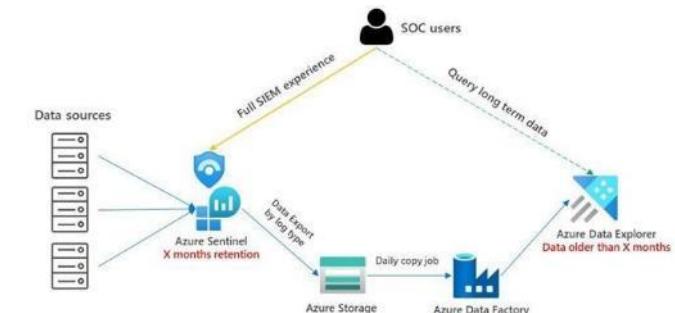
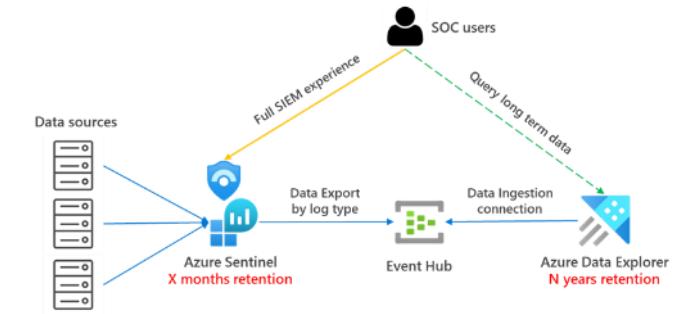
Let's take a look at the new Data Export feature in Log Analytics that we will use in some of the architectures below (full documentation on this feature [here](#)).



This feature lets you export data of selected tables (see supported tables [here](#)) in your Log Analytics workspace as it reaches ingestion, and continuously send it to Azure Storage Account and/or Event Hub.

Using ADX for long term retention:

<https://techcommunity.microsoft.com/t5/azure-sentinel/using-azure-data-explorer-for-long-term-retention-of-azure/ba-p/1883947>



Break – 5 minutes

KQL Introduction

CyberSecurityDemo

Run

Time range: Last 24 hours

Save

Copy

Export

New alert rule

Pin to dashboard

Schema

Filter

Filter by name or type...  Collapse all

Active

CyberSecurityDemo

DnsAnalytics

LogManagement

Office365

Security

CommonSecurityLog

LinuxAuditLog

ProtectionStatus

SecurityAlert

AlertName

AlertSeverity

ConfidenceLevel

ConfidenceScore

Description

DisplayName

EndTime

Entities

ExtendedLinks

ExtendedProperties

IsIncident

 Tables Typed columnsSecurityAlert
| limit 50

Completed. Showing results from the last 24 hours.

00:00:03.055

43 records

Display time (UTC+00:00) ▾

 TABLE CHART

Columns ▾

Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	DisplayName	AlertName
2019-07-08T18:56:26.000	Anonymous IP address	Anonymous IP address
...		
TenantId	ab86c959-1ba3-495c-a00d-ced30d8825d3	
TimeGenerated [UTC]	2019-07-08T18:56:26Z	
DisplayName	Anonymous IP address	
AlertName	Anonymous IP address	
AlertSeverity	Medium	
Description	Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)	
ProviderName	IPC	
VendorName	Microsoft	
VendorOriginalId	7fb7db35c22be5f914f827daa5d29d39c65de080d554781eb3221014f8690f9a	
SystemAlertId	e6692353-f03c-489a-a0fc-14cae4bae0e2	
AlertType	AnonymousLogin	

 Queries Results

Page

1

of 1

> >

50

▼

items per page

1 - 43 of 43 items

aka.ms/LAdemo

[Getting started with Kusto | Microsoft Docs](#)

Common commands

- Where
- Limit
- Count
- Summarize
- Distinct
- Extend
- Project
- Project-away
- Order by
- *Additional: extract, let, union, join, iff, parse*

[KQL documentation](#)

[Free Pluralsight KQL course](#)

[Open to use KQL playground](#)

'where' command

Filters a table to the subset of rows that satisfy a predicate.

Syntax: $T \mid \text{where } \textit{Predicate}$

Examples: $\text{SecurityEvent} \mid \text{where } \text{TimeGenerated} > \text{ago}(1d)$

$\text{SecurityEvent} \mid \text{where } * \text{ contains "Kusto"}$

- String predicates: ==, has, contains, startswith, endswith, matches regex, etc
- Numeric/Date predicates: ==, !=, <, >, <=, >=
- Empty predicates: isempty(), notempty(), isnull(), notnull()

'where' exercise

```
SecurityEvent
```

```
| where TimeGenerated > ago(1d)
```

```
SecurityEvent
```

```
| where TimeGenerated > ago(1h) and EventID == 4624 // Successful logon
```

```
SecurityEvent
```

```
| where TimeGenerated > ago(1h)  
| where EventID == 4624  
| where AccountType =~ "user" // case insensitive
```

```
Perf
```

```
| where InstanceName matches regex "^[A-Z]:"
```

'limit' / 'take' command

Return up to the specified number of rows.

Syntax: $T \mid \text{limit} <\text{number}>$

Example: $\text{SecurityEvent} \mid \text{limit } 5$

- Sort is not guaranteed to be preserved.
- Consistent result is not guaranteed (when running the same query twice)
- Very useful when trying out new queries.
- Default limit is 10,000.

'limit' exercise

```
SecurityEvent
```

```
| limit 10
```

```
SecurityEvent
```

```
| where TimeGenerated > ago(1h)
| where EventID == 4624
| where AccountType =~ "user"
| take 10
```

'count' command

Returns the number of records in the input record set.

Syntax: $T \mid count$

Example: $SecurityEvent \mid count$

'count' exercise

Perf

```
| count
```

SecurityEvent

```
| where TimeGenerated > ago(1h)
| where EventID == 4624
| count
```

'summarize' command

Produces a table that aggregates the content of the input table.

Syntax: $T \mid \text{summarize} \text{ Aggregation [by Group Expression]}$

Examples: $\text{SecurityEvent} \mid \text{summarize} \text{ count()} \text{ by Computer}$

- Simple aggregation functions: count(), sum(), avg(), min(), max(),
- Advanced functions (next slide): arg_min(), arg_max(), percentiles(), makelist(), countif()
- No Group Expression implies 'distinct'.

'summarize' exercise

Perf

```
| where CounterName == "Free Megabytes"
| where InstanceName matches regex "^[A-Z]:$"
| summarize min(CounterValue)
```

SecurityEvent

```
| where TimeGenerated > ago(1h)
| where EventID == 4624
| summarize count() by AccountType, Computer
```

SecurityEvent

```
| where TimeGenerated >= ago(1d)
| summarize count() by bin(TimeGenerated,1h)
| render timechart
```

KQL Lab #1

Use the [open to use KQL playground](https://aka.ms/LAdemo) (<https://aka.ms/LAdemo>)

1. Render a time chart of free MB over last 7 days for disk C: (hint: InstanceName should be 'C:', CounterName should be 'Free Megabytes')

Log table used: Perf

KQL Lab #1 solution

Perf

```
| where InstanceName == "C:"  
| where CounterName == "Free Megabytes"  
| summarize FreeMB = avg(CounterValue) by bin(TimeGenerated, 1h) | render  
timechart
```

'extend' command

Create calculated columns and append them to the result set.

Syntax: $T \mid \text{extend } \textit{ColumnName} [= \textit{Expression}] [, ...]$

Example: $\textit{SecurityEvent} \mid \text{extend } \textit{ComputerNameLength} = \textit{strlen}(\textit{Computer})$

- The new added column is not indexed.
- To only change a column name, use 'project-rename'.
- Useful function for in 'extend': iff, extract

'project' command

Select the columns to include, rename or drop, and insert new computed columns.

Syntax: $T \mid \text{project} \text{ ColumnName} [= \text{Expression}] [, ...]$

Example: $\text{SecurityEvent} \mid \text{project} \text{ TimeGenerated, Computer}$

'| project-away' – Removed specified column/s.

'| project-rename' – Rename specified column/s.

'extend' & 'project' exercise

Perf

```
| where CounterName == "Free Megabytes"
| where InstanceName == "C:"
| extend FreeKB = CounterValue * 1000
| extend FreeGB = CounterValue / 1000
```

Perf

```
| where CounterName == "Free Megabytes"
| project Computer , CounterName , CounterValue
```

Perf

```
| where CounterName == "Free Megabytes"
| extend FreeKB = CounterValue * 1000
| extend FreeGB = CounterValue / 1000
| extend FreeMB = CounterValue
| project Computer , CounterName , FreeGB , FreeMB , FreeKB
```

'distinct' command

Produces a table with the distinct combination of the provided columns of the input table.

Syntax: $T \mid \text{distinct } \textit{Column1}, \textit{Column2}$

Example: $\textit{SecurityEvent} \mid \text{distinct } \textit{Computer}$

'order by' / 'sort by' & 'top' operator

Order by: Sort the rows of the input table into order by one or more columns.

Top: returns the top values after sort. Faster and can sort by expression

Syntax:

T | *sort by column [asc | desc] [nulls first | nulls last]*

T | *top NumberOfRows by Expression [asc | desc] [nulls first | nulls last]*

Example:

Table | *order by country asc, price desc*

Don't assume order by default

'order by' / 'top' exercise

```
SecurityEvent
```

```
| where TimeGenerated > ago(7d)  
| order by TimeGenerated desc  
| limit 100 // try also top
```

```
SecurityEvent
```

```
| top 100 by TimeGenerated desc
```

```
SecurityEvent
```

```
| where EventID == 4624  
| summarize cnt=count() by Account  
| top 10 by cnt
```

KQL Lab #2

Use the [open to use KQL playground](https://aka.ms/LAdemo) (<https://aka.ms/LAdemo>)

The table “SecurityEvent” contains security events collected from Windows machines. The events are identified by their IDs. Find the column that represents this ID, and complete the following tasks:

- a. Render graph of logon events over time, starting from two weeks ago until one week ago.
- b. Render graph of successful (4624) vs failed (4625) logons over the last 7 days, use alias for the legend (“Success”, “Failed”)
- c. Find the last logon time for a user named “ContosoASCAAlert\\LBecker”

Lab #2 solution

//Question #A: Render graph of logon events over time, starting from two weeks ago until one week ago.

SecurityEvent

```
| where EventID == 4624  
| summarize count() by bin(TimeGenerated, 1h)  
| render timechart
```

//Question #B: Render graph of successful (4624) vs failed (4625) logons over the last 7 days, use alias for the legend ("Success", "Failed")

SecurityEvent

```
| summarize Success=countif(EventID == 4624), Failed=countif(EventID==4625) by  
bin(TimeGenerated, 1h)  
| render timechart
```

//Question #C: Find the last logon time for a user named "ContosoASCAAlert\\LBecker"

SecurityEvent

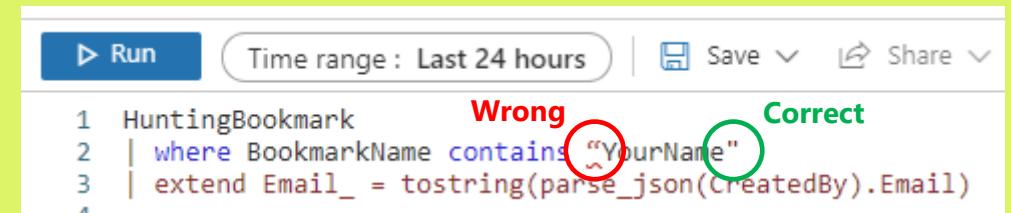
```
| where EventID == 4624  
| where Account == "ContosoASCAAlert\\LBecker"  
| summarize max(TimeGenerated)
```

Break – 10 minutes

Externaldata Query / Watchlist

Note:

When copying and pasting please check that the `"`'s are correct



The screenshot shows a Microsoft Power BI query editor interface. At the top, there is a toolbar with a 'Run' button, a 'Time range : Last 24 hours' dropdown, a 'Save' button, and a 'Share' button. Below the toolbar, the query editor displays the following code:

```
▶ Run Time range : Last 24 hours Save Share
1 HuntingBookmark
2 | where BookmarkName contains "YourName"
3 | extend Email_ = tostring(parse_json(CreatedBy).Email)
4
```

Annotations are present in the code:

- A red circle highlights the opening double quote in `"YourName"`, with the word **Wrong** written above it.
- A green circle highlights the closing double quote in `"YourName"`, with the word **Correct** written above it.

Lab: Externaldata() operator

The screenshot shows the Azure Data Explorer interface with a sample CSV file loaded. The file contains three log entries:

Date	ExampleField
6/4/2021 16:41	This is a sample log line
6/4/2021 16:41	This is a sample log line

In the query editor, the following Kusto query is run:

```
externaldata(Timestamp:datetime, ExampleField:string, ExampleInt:int) [h @"https://raw.githubusercontent.com/ko-sharon/AzureSentinel/master/Lab/SampleCSV.csv"] with (format="csv", ignoreFirstRecord=true)
```

The results pane shows the two log entries from the CSV file.

Externaldata operator:

<https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/externaldata-operator?pivots=azuredataexplorer>

Lab: Save as Function

Save as function

Function name *

 ✓

Code

```
externaldata(Timestamp:datetime, ExampleField:string, ExampleInt:int)
[
    h@:"https://raw.githubusercontent.com/ko-sharon/AzureSentinel/master/Lab/SampleCSV.csv"
] with (format="csv", ignoreFirstRecord=true)
```

Legacy category *

Save as computer group

Parameters

Type	Name	Default value
Select type	Type name	Type default value

Completed. Showing results from the last 24 hours.

Timestamp [UTC]	ExampleField
6/4/2021, 4:41:00.000 PM	This is a sample log line
6/4/2021, 4:41:00.000 PM	This is a sample log line

New Query 2*

Run Time range : Last 24 hours Save Share New alert rule

Sharon_log

Timestamp [UTC]	ExampleField	ExampleInt
6/4/2021, 4:41:00.000 PM	This is a sample log line	100
6/4/2021, 4:41:00.000 PM	This is a sample log line	200

Externaldata operator:

<https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/externaldata-operator?pivots=azuredataexplorer>

Demo: Externaldata() operator for Enrichment

Code:

```
externaldata(domain:string) [h@"https://gist.githubusercontent.com/tbrianjones/5992856/raw/93213efb652749e226e69884d6c048e595c1280a/free_email_provider_domains.txt"]
```

Code:

```
let EmailLog = datatable (Username:string, UserEmail:string, Status:string)
["Bob", "bob@qq.com", "Delivered",
"Alice", "alice@yahoo.com", "Failed",
"Mark", "mark@somecompany.com", "Failed"];
EmailLog
| extend ExtractDomain = split(UserEmail, "@")
| extend EmailDomain = tostring(ExtractDomain[1])
| where EmailDomain in (FreeEmailDomains)
```

A list of free email provider domains. Some of these are probably not around anymore. I've combined a dozen lists from around the web. Current "major providers" should all be in here as of the date this is created. (github.com)

The screenshot shows the Microsoft Sentinel Query Editor interface with two separate query panes.

Top Query (FreeEmailDomains):

```
1 externaldata(domain:string) [h@"https://gist.githubusercontent.com/tbrianjones/5992856/raw/93213efb652749e226e69884d6c048e595c1280a/free_email_provider_domains.txt"]
```

This query retrieves a list of free email provider domains from a GitHub Gist. The results are displayed in a table:

domain
1033edge.com
11mail.com
123.com
123box.net
123india.com
123mail.cl
123qwe.co.uk
126.com
150ml.com
15meg4free.com
163.com
1coolplace.com
1freemail.com
1funplace.com
1internetdrive.com
1mail.net

Bottom Query (EmailLog):

```
1 let EmailLog = datatable (Username:string, UserEmail:string, Status:string)
2 ["Bob", "bob@qq.com", "Delivered",
3 "Alice", "alice@yahoo.com", "Failed",
4 "Mark", "mark@somecompany.com", "Failed"];
5 EmailLog
6 | extend ExtractDomain = split(UserEmail, "@")
7 | extend EmailDomain = tostring(ExtractDomain[1])
8 | where EmailDomain in (FreeEmailDomains)
```

This query processes a table of email logs and enriches it with the domain extracted from the UserEmail field. The results are displayed in a table:

ExtractDomain	EmailDomain	Username	UserEmail	Status
["bob", "qq.com"]	qq.com	Bob	bob@qq.com	Delivered
["alice", "yahoo.com"]	yahoo.com	Alice	alice@yahoo.com	Failed

Watchlist

Azure Sentinel | Watchlist (Preview) ... X

Selected workspace: 'tm-sentinel-workshop'

Search (Ctrl+ /) Refresh Add new Delete Columns Guides & Feedback

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview) (Selected)
- Automation
- Community
- Settings

Watchlists 1

My Watchlists

Name ↑↓	Alias ↑↓	Source ↑↓	Created Time ↑↓	Last Updated ↑↓	...
SampleWatchlist	SampleWatchlist	SampleCSV.csv	04/06/21, 06:31 PM	04/06/21, 06:31 PM	...

SampleWatchlist

Name

Microsoft Provider

0 Rows

04/06/21, 06:31 PM Created Time

Description

-

Source / File name

SampleCSV.csv

Created By

shko@microsoft.com

Created Time

04/06/21, 06:31 PM

Last Updated

04/06/21, 06:31 PM

< Previous 1 - 1 Next >

View in Log Analytics

The screenshot shows the Azure Sentinel Watchlist (Preview) interface. On the left, there's a navigation sidebar with sections like General, Threat management, and Configuration. Under Configuration, 'Watchlist (Preview)' is selected and highlighted with a grey background. The main area displays a table titled 'My Watchlists' with one entry: 'SampleWatchlist'. To the right of the table, detailed information about the 'SampleWatchlist' is shown, including its provider (Microsoft), rows (0), and creation time (04/06/21, 06:31 PM). Below this, there are fields for Description, Source / File name (SampleCSV.csv), Created By (shko@microsoft.com), Created Time (04/06/21, 06:31 PM), and Last Updated (04/06/21, 06:31 PM). At the bottom, there are navigation buttons for 'Previous', 'Next', and a 'View in Log Analytics' button.

_GetWatchlist('SampleWatchlist')

Analytics

Lab: Creating Scheduled Rule

Analytics rule wizard - Create new rule

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

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name * ✓

Description ✓

Tactics

2 selected

Severity

Medium

Status

Enabled Disabled

Code:

```
HuntingBookmark  
| where BookmarkName contains "YourName"  
| extend Email_ = tostring(parse_json(CreatedBy).Email)
```

Analytics rule wizard - Edit existing rule

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.
⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
HuntingBookmark  
| where BookmarkName contains "YourName"  
| extend Email_ = tostring(parse_json(CreatedBy).Email)
```

[View query results >](#)

Alert enrichment (Preview)

Entity mapping

Map up to five entities recognized by Azure Sentinel from the appropriate fields available in your query results. This enables Azure Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

Unlike the previous version of entity mapping, the mappings defined below do not appear in the query code. Any mapping you define below will replace not only its parallel

[+ Add new entity](#)

Custom details

Query scheduling

Run query every * Minutes
Lookup data from the last * Hours

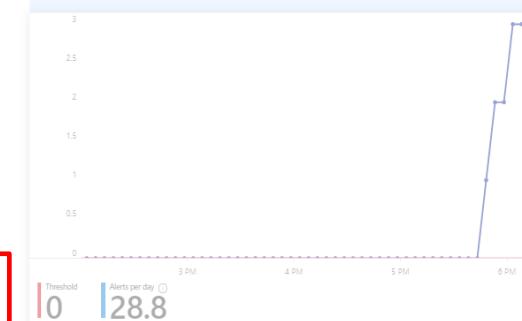
Alert threshold

Generate alert when number of query results
Is greater than

Results simulation

This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Analytics rule configuration changed. Click 'Test with current data' to view updated results.



Lab: Triggering the Analytics Rule

New Query 1* New Query 2* +

CyberSecuritySOC Run Time range : Last 24 hours Save

1 Sharon_log

Results Chart Columns Add bookmark Display time (UTC+00:00)

Completed. Showing results from the last 24 hours.

	Timestamp [UTC]	ExampleField	ExampleInt
> <input checked="" type="checkbox"/>	6/4/2021, 4:41:00.000 PM	This is a sample log line	100
> <input type="checkbox"/>	6/4/2021, 4:41:00.000 PM	This is a sample log line	200

Add bookmark

Hunting bookmarks enable Azure Sentinel users to save, tag, annotate, share and investigate results from a Log Analytics query. You can view and manage Hunting Bookmarks in Azure Sentinel - Hunting. Click here to learn more.

Bookmark Name: YourName_Bookmark

Query Information
Time Frame: 4/5/2021, 5:38:29 PM - 4/6/2021, 5:38:29 PM

Account: Choose column

Host: ExampleInt - 100

IP: Choose column

URL: Choose column

Timestamp: Timestamp - 2021-06-04T16:41:00Z

Tags: +

Notes:

Break – 13 minutes

Lab: Investigating Incidents

Azure Sentinel | Incidents ...

Selected workspace: 'tm-sentinel-workshop'

Search (Ctrl+ /) Refresh Last 24 hours Actions Security efficiency workbook (Preview) Create automation rule (Preview)

General

- Overview
- Logs
- News & guides

Threat management

- Incidents** (highlighted with a red box)
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Automation
- Community
- Settings

1 Open incidents, 1 New incidents, 0 Active incidents

Open incidents by severity: High (0), Medium (1), Low (0), Informational (0)

Search by id, title, tags, owner or product Severity: All Status: New, Active Product name: All More (1)

Auto-refresh incidents

Incident ID	Title	Alerts	Product names	Created time	Last update time
4	Sharon_Rule Sample	1	Azure Sentinel	04/06/21, 06:07 PM	04/06/21, 06:07

Sharon_Rule Sample Incident ID: 4

Owner: Unassigned Status: New Severity: Medium

Description: Type whatever you want here.

Alert product names:

- Azure Sentinel

Evidence:

- 3 Events
- 1 Alerts
- 0 Bookmarks

Last update time: 04/06/21, 06:07 PM Creation time: 04/06/21, 06:07 PM

Entities (1): ko.sharon@mic... View full details >

Tactics (2): Privilege Escalation, Credential Access

Incident workbook: Incident Overview

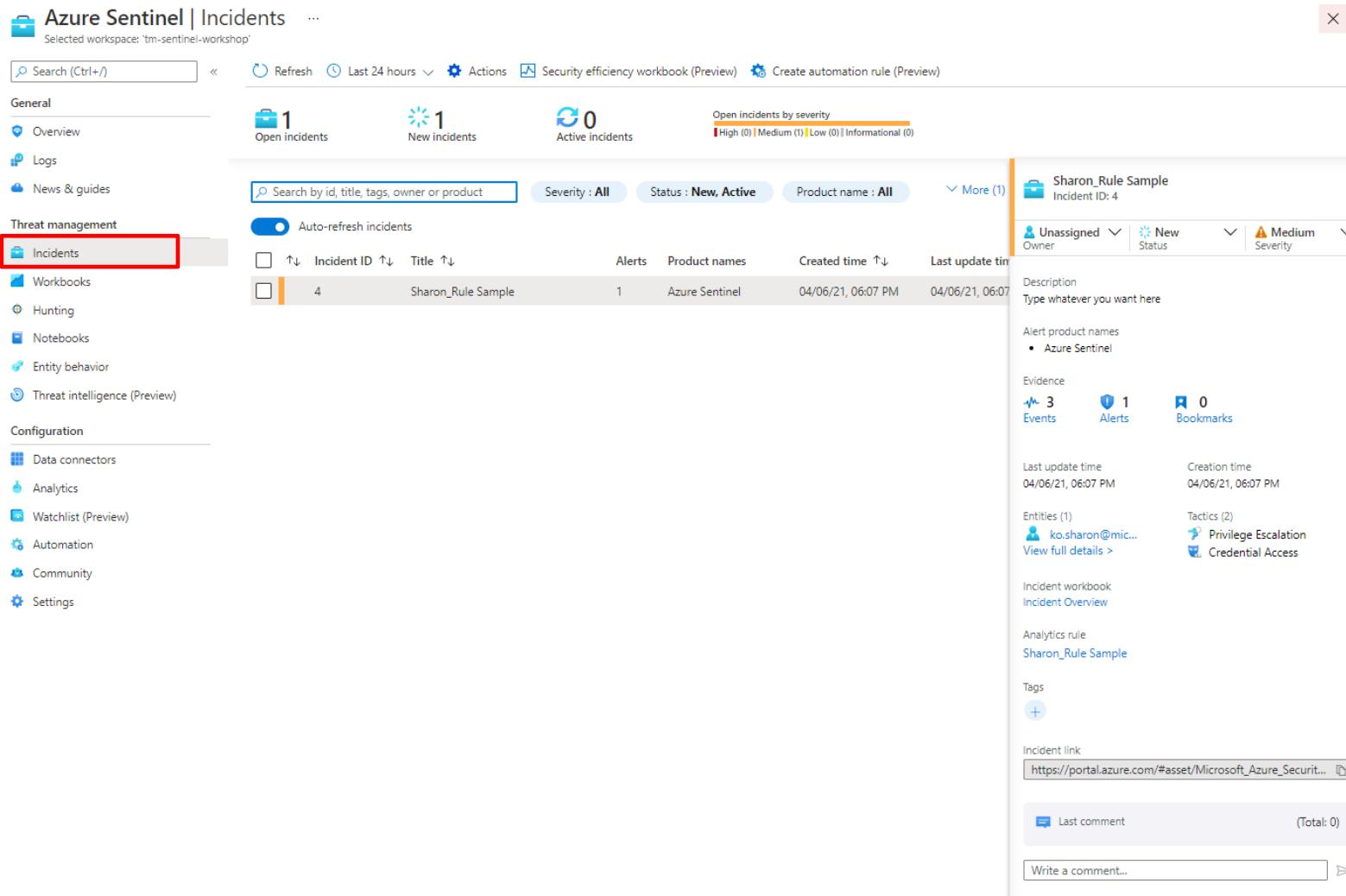
Analytics rule: Sharon_Rule Sample

Tags: +

Incident link: https://portal.azure.com/#asset/Microsoft_Azure_Security/...

Last comment (Total: 0)

Write a comment... ➤



Hunting

Azure Sentinel - Hunting
Selected workspace: 'CyberSecurityDemo' - PREVIEW

Hunting

New Query Run all queries Bookmark Logs Refresh Last 24 hours

17 Total Queries 690 Total Results 13 Total Bookmarks 11 My Bookmarks LEARN MORE About hunting

Queries Bookmarks

Search queries FAVORITES : All PROVIDER : All DATA SOURCES : All TACTICS : All

QUERY	DESCRIPTION	PROVIDER	DATA SOURCE	RESULTS	TACTICS
masquerading files.	Malware writers often use windows system process na...	Microsoft	SecurityEvent	0	
Hosts with new logons	Shows new accounts that have logged onto a host for t...	Microsoft	SecurityEvent	499	
Summary of failed user logons by reason of fail...	A summary of failed logons can be used to infer lateral ...	Microsoft	SecurityEvent	3	
Anomalous Azure Active Directory apps based o...	This query over Azure AD sign-in activity highlights Az...	Microsoft	SigninLogs	188	
Base64 encoded Windows executables in proces...	finds instances of base64 encoded PE files header seen ...	Microsoft	SecurityEvent	--	
Process executed from binary hidden in Base64 ...	Encoding malicious software is a technique to obfuscate...	Microsoft	SecurityEvent	--	
Enumeration of users and groups	finds attempts to list users or groups using the built-in ...	Microsoft	SecurityEvent	--	
Malware in the recycle bin.	finding attackers hiding malware in the recycle bin. Rea...	Microsoft	SecurityEvent	--	
Azure Active Directory signins from new locatio...	New Azure Active Directory signin locations today vers...	Microsoft	SigninLogs	--	
New processes observed in last 24 hours	These new processes could be benign new programs in...	Microsoft	SecurityEvent	--	
Summary of users created using uncommon & u...	Summarizes uses of uncommon & undocumented command-line ...	Microsoft	SecurityEvent	--	
powershell downloads	Finds PowerShell execution events that...	Microsoft	SecurityEvent	--	
Cscript script daily summary breakdown	breakdown of scripts running in the e...	Microsoft	SecurityEvent	--	
New user agents associated with a clientIP for s...	New user agents associated with a clientIP for s...	Microsoft	OfficeActivity	--	
Identify and decode new encoded powershell scripts th...	Identify and decode new encoded powershell scripts th...	Microsoft	SecurityEvent	--	
Comparing succesful and nonsuccessful logon attempts...	Comparing succesful and nonsuccessful logon attempts...	Microsoft	SecurityEvent	--	
User accounts	Custom Queries	OfficeActivity	--		

Run all selected Filter by source, MITRE tactic or search

Rich, out of the box content

masquerading files.

Microsoft Provider 0 Results SecurityEvent Data Source

DESCRIPTION

Malware writers often use windows system process names for their malicious process names to make them blend in with other legitimate commands that the Windows system executes. An analyst can create a simple query looking for a process named svchost.exe. It is recommended to filter out well-known security identifiers (SIDs) that are used to launch the legitimate svchost.exe process. The query also filters out the legitimate locations from which svchost.exe is launched.

CREATED TIME

2019-05-20T20:18:11.078Z

Investigate outliers

QUERY

```
1 let start=datetime("2019-05-20T20:18:11.078Z");
2 let end=datetime("2019-05-20T20:18:11.078Z");
3 SecurityEvent
4 |where TimeGenerated > start and TimeGenerated <
5 | where NewProcessName endswith "\svchost.exe"
6 | where SubjectUserSid !in ("S-1-5-18", "S-1-5-19")
```

View query results >

TACTICS

Execution The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote

Run Query View Results

Bookmarks

- Bookmark any event in search results
- Use as incident artifacts
- Map to entities to enable bookmark (and event) investigation

Add hunting bookmark

PREVIEW



Hunting bookmarks enable Azure Sentinel users to save, tag, annotate, share and investigate results from a Log Analytics query.

You can view and manage Hunting Bookmarks in Azure Sentinel - Hunting. Click here to [learn more](#).

Bookmark Name

SigninLogs - 38a9d5697a62

Query Information

Time Frame Unknown - Unknown

ENTITY TYPE



COLUMN

Account

Choose column



Host

Choose column



IP address

Choose column



Timestamp

TimeGenerated - 2019-09-08T1...



Tags



Notes

Lab: Create a Hunting Query

Create custom query ...



Do not use fixed time ranges, either directly or in a function, in your query. Otherwise, we cannot show changes in query results over time.

Name *

YourName_Hunting Query

Description

Custom query

```
AzureActivity  
| where Caller contains "YourEmail" //full or partial match is fine  
| extend AccountCustomEntity = Caller
```

[View query results >](#)

Entity mapping

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results.
This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis.
Entity type must be a string.

Entity Type

Account

Host

IP

URL

Timestamp

Tactics

Execution

Code:

AzureActivity

```
| where Caller contains "YourName" //full or partial match is fine  
| extend AccountCustomEntity = Caller
```

Column

Defined in query

Choose column

Add

Choose column

Add

Choose column

Add

Choose column

Add

↑↓ Query ↑↓

★ Sharon_Hunting Query

Provider ↑↓

Data Source ↑↓

Results ↑↓

Tactics

Custom Queries

AzureActivity

83

Execution

Lab: Create a Bookmark, and Create / Add to Incident

The screenshot illustrates the Azure Sentinel interface for creating a bookmark and managing hunting results.

Top Left: The main workspace shows a query run titled "TM-Sentinel-Workshop". A red box highlights the "View Results" button. The results table displays log entries from the last 24 hours, with the first few rows shown below:

```
1 AzureActivity
2   where Caller contains "shko" //full or partial match is fine
3   extend AccountCustomEntity = caller
```

Top Right: A modal window titled "Add bookmark" is open, also with a red box highlighting it. It contains fields for "Bookmark Name" (set to "Sharon_Hunting Query - 7eeff4ae4dbfb4"), "Query Information" (Time Frame: 4/5/2021, 6:14:27 PM - 4/6/2021, 6:14:27 PM), and "Account" (Caller - shko@microsoft.com). Other fields include Host, IP, URL, Timestamp, Tags, and Notes.

Bottom Left: The "Azure Sentinel | Hunting" section shows metrics: 200 Total queries, 0 Livestream Results, and 2 My bookmarks. It also displays the MITRE ATT&CK matrix with counts for various tactics and techniques.

Bottom Right: A detailed view of a bookmark named "Sharon_Hunting Query - 2040db22357f". A red box highlights the "Actions" menu on the right, which includes options: "Create new incident", "Add to existing incident", "Remove from incident", and "Delete bookmark".

Lab: Investigating Incidents

Investigation ...

Undo Redo

Sharon_Rule Sample
Incident

Medium
Severity

New
Status

Unassigned
Owner

4/6/2021, 6:18:22 PM
Last incident update time

The diagram illustrates the relationships between three entities:

- Sharon_Rule Sample** (Incident): Represented by a shield icon.
- User Account**: Represented by a person icon. It has a connection to the incident and another connection to the狩猎队 (Hunting Queue).
- Sharon_Hunting Q...** (狩猎队): Represented by a star icon. It has a connection from the User Account.

A context menu is open over the User Account icon, listing related items:

- Related alerts (0) [Events >](#)
- Hosts the account failed... (0) [Events >](#)
- User account successful ... (0) [Events >](#)
- More [▼](#)
- Office activity IPs for thl... (0) [Events >](#)
- User account failed logons (0) [Events >](#)
- Hosts which the account log... (0) [Events >](#)
- Related bookmarks (0) [Events >](#)
- IPs from rare locations use... (0) [Events >](#)
- Least prevalent processes f... (0) [Events >](#)
- Services created by account (0) [Events >](#)
- User account new resource a... [Events >](#)
- User account remote interact... [Events >](#)

Workbooks

Lab: Add and Save a Workbook

1 Home > Azure Sentinel > Azure Sentinel

Azure Sentinel | Workbooks

Selected workspace: 'tm-sentinel-workshop'

Search (Ctrl+ /) Refresh + Add workbook

General

- Overview
- Logs
- News & guides

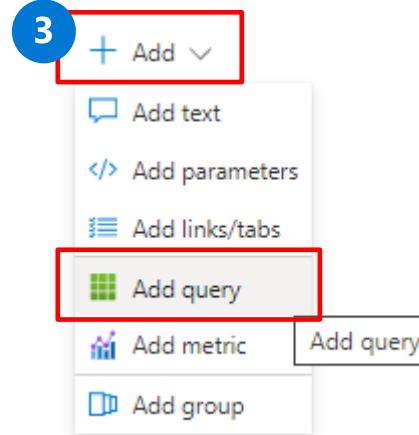
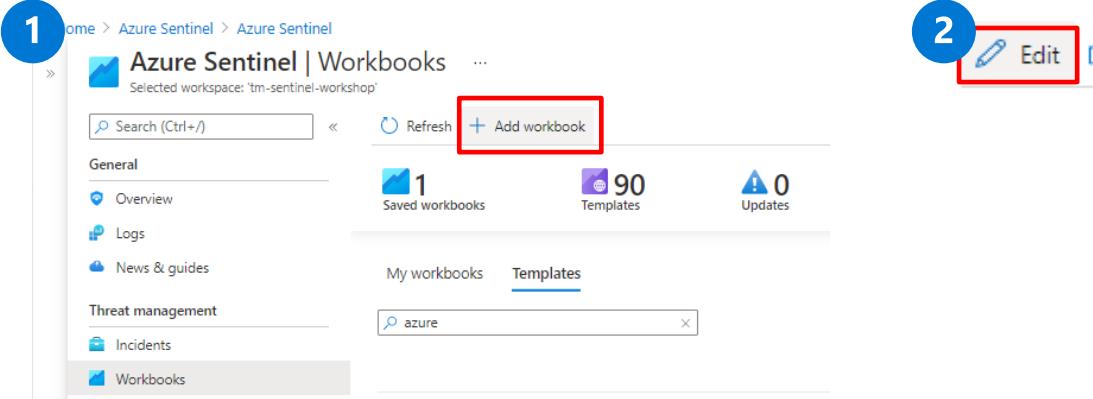
Threat management

- Incidents
- Workbooks

1 Saved workbooks 90 Templates 0 Updates

My workbooks Templates

azur



4 Editing query item: query - 2

Settings Advanced Settings Style

Run Query Samples Data source Logs Resource type Log Analytics workspace tm-sentinel-workshop Time Range Last 24 hours Visualization Size Medium Column Settings

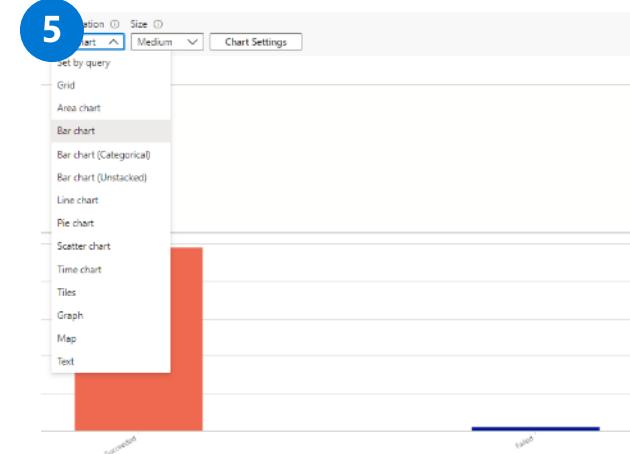
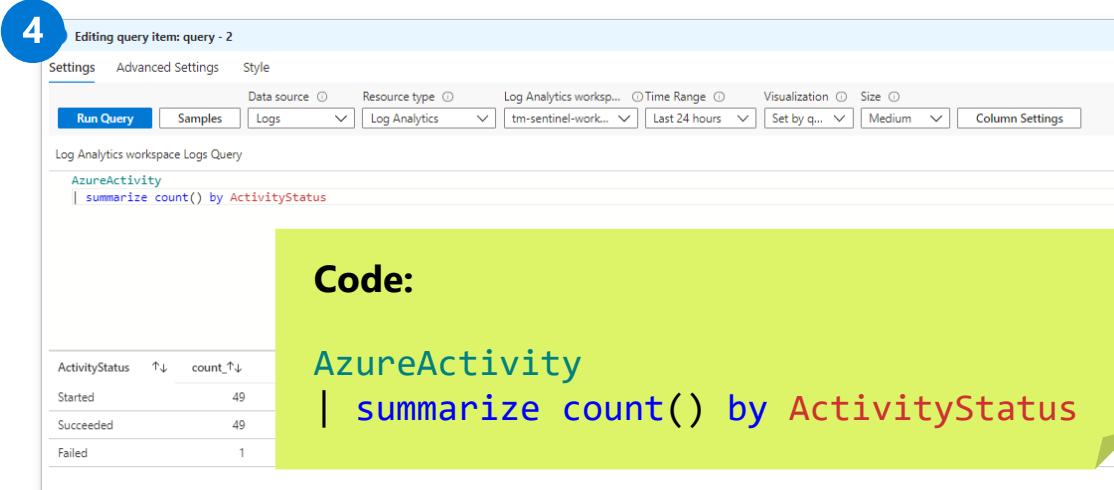
Log Analytics workspace Logs Query

```
AzureActivity  
| summarize count() by ActivityStatus
```

Code:

```
AzureActivity  
| summarize count() by ActivityStatus
```

ActivityStatus	count
Started	49
Succeeded	49
Failed	1



6

Editing Open

Deprecated workbooks will be deprecated June 30 2021. Use Save or Save As to make them Shared Workbooks. →

Title * YourName Subscription * SK-Internal Resource group * TM-HQ Location * (Asia Pacific) East Asia

Save content to an Azure Storage Account.

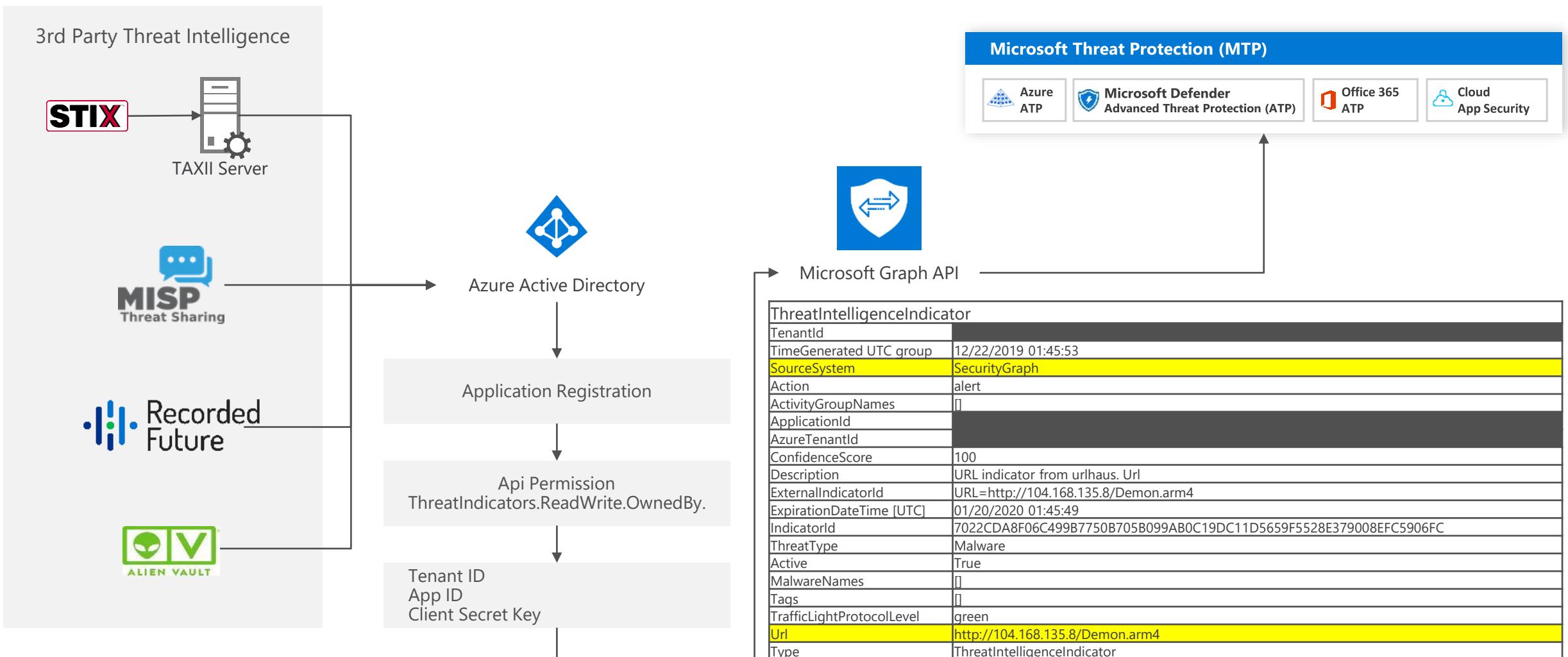
Save Cancel



Threat Intelligence

External Threat Intelligence Enrichment

Leverage Microsoft Graph Security API to store your Threat Indicators into Microsoft security solutions.



Azure Sentinel | Threat intelligence (Preview)

Selected workspace: 'cybersecuritysoc'

Indicator saved

11:42 AM

Search (Ctrl+ /)

Refresh Add new Add Tags Delete Columns Guides & Feedback

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks (Preview)

Entity behavior analytics (Preview)

Threat intelligence (Preview)

Configuration

Data connectors

Analytics

Playbooks

Community

Settings

37
TI alerts

28.6K
TI indicators

3
TI sources

Indicators

Search by Name, Values, Description or Tags

TYPE : All

SOURCE : All

THREAT TYPE : All

<input type="checkbox"/> Name ↑↓	Values	Types	Source ↑↓	Confidence ↑↓	Alerts	Tags	Threat Type	Created
<input type="checkbox"/> Malicious URL	http://www.badurl.com	url	Azure Sentinel	80	0		malicious-activity	Fri Aug 14 2
<input type="checkbox"/> Custom Threat Intellig...	F688F50D695F8D00AE...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	2CFE8ADA24FE875B4F...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	05C9B086778BA1DC3...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	6441682094420E1677...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	5392AD13A9DA47D12...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	AFFE16995DEEA180A...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	56611DF4A4F91A0596...	file	SecurityGraph	100	0		Malware	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	956D28C0F7567973D...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	D10BFAC7CC64FE82FB...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	6A8B18C3FE5B742F77...	file	SecurityGraph	100	0		Malware	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	688A17478DDE70A31...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	A66A3B2E9F83141937...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	48E0AF0073249940C1...	file	SecurityGraph	100	0		Malware	Thu Aug 13
<input type="checkbox"/> Custom Threat Intellig...	EE176315191D8EE831...	file	SecurityGraph	100	0		Malware	Thu Aug 13

 Malicious URL

80	Confidence	0	Alerts	url
Name Malicious URL				
Values Type : url url : http://www.badurl.com				
Tags + Add				
Threat Types malicious-activity				
Description Malicious URL				
Revoked false				
Confidence 80				
Source Azure Sentinel				

< Previous

1 - 100

Next >

 Azure Sentinel | Analytics ...


Selected workspace: 'sk-wfh'

Search (Ctrl+ /)

+ Create Refresh Analytics efficiency workbook (Preview) Enable Disable Delete

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence (Preview)

Configuration

Data connectors

Analytics

Watchlist (Preview)

Automation

Community

Settings

12 Active rules

Rules by severity

High (3) Medium (4) Low (1) Informational (4)
[LEARN MORE](#)
[About analytics rules](#)
Active rules Rule templates

Search

Severity : All

Rule Type : All

Tactics : All

Data Sources : 2 selected

SEVERITY ↑↓	NAME ↑↓	RULE TYPE ↑↓	DATA SOURCES	TACTICS
Medium	TI map IP entity to GitHub_CL	Scheduled	Threat Intelligence Platforms (Preview) +1 ⓘ	Impact
Medium	(Preview) TI map IP entity to DnsEvents	Scheduled	Threat Intelligence Platforms (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map IP entity to OfficeActivity	Scheduled	Threat Intelligence Platforms (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map Email entity to CommonSecurityLog	Scheduled	Palo Alto Networks +2 ⓘ	Impact
Medium	(Preview) TI map Domain entity to PaloAlto	Scheduled	Palo Alto Networks +2 ⓘ	Impact
Medium	(Preview) TI map Domain entity to Syslog	Scheduled	Syslog +2 ⓘ	Impact
Medium	(Preview) TI map IP entity to WireData	Scheduled	Threat Intelligence Platforms (Preview) +1 ⓘ	Impact
Medium	(Preview) TI map Email entity to SigninLogs	Scheduled	Threat Intelligence Platforms (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map IP entity to W3CISLog	Scheduled	Threat Intelligence Platforms (Preview) +1 ⓘ	Impact
Medium	(Preview) TI map Email entity to OfficeActivity	Scheduled	Office 365 +2 ⓘ	Impact
Medium	(Preview) TI map Domain entity to DnsEvent	Scheduled	DNS (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map URL entity to Syslog data	Scheduled	Syslog +2 ⓘ	Impact
Medium	(Preview) TI map IP entity to AzureNetworkAnalytics_CL (NSG Flow Logs)	Scheduled	Threat Intelligence Platforms (Preview) +1 ⓘ	Impact
Medium	(Preview) TI map Domain entity to CommonSecurityLog	Scheduled	Threat Intelligence Platforms (Preview) +1 ⓘ	Impact
Medium	(Preview) TI map File Hash to Security Event	Scheduled	Security Events +2 ⓘ	Impact
Medium	(Preview) TI map Email entity to SecurityAlert	Scheduled	Azure Defender +2 ⓘ	Impact
Medium	(Preview) TI map File Hash to CommonSecurityLog Event	Scheduled	Palo Alto Networks +2 ⓘ	Impact
Medium	(Preview) TI map URL entity to PaloAlto data	Scheduled	Palo Alto Networks +2 ⓘ	Impact
Medium	(Preview) TI map Email entity to SecurityEvent	Scheduled	Threat Intelligence Platforms (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map URL entity to AuditLogs	Scheduled	Azure Active Directory +2 ⓘ	Impact
Medium	(Preview) TI map Email entity to AzureActivity	Scheduled	Azure Activity +2 ⓘ	Impact
Medium	(Preview) TI map URL entity to SecurityAlert data	Scheduled	Microsoft Cloud App Security +3 ⓘ	Impact
Medium	(Preview) TI map Domain entity to SecurityAlert	Scheduled	Threat Intelligence Platforms (Preview) +3 ⓘ	Impact
Medium	(Preview) TI map IP entity to AWSCloudTrail	Scheduled	Threat Intelligence Platforms (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map IP entity to SigninLogs	Scheduled	Threat Intelligence Platforms (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map IP entity to VMConnection	Scheduled	Threat Intelligence Platforms (Preview) +1 ⓘ	Impact
Medium	(Preview) TI map IP entity to AzureActivity	Scheduled	Threat Intelligence Platforms (Preview) +2 ⓘ	Impact
Medium	(Preview) TI map URL entity to OfficeActivity data	Scheduled	Office 365 +1 ⓘ	Impact

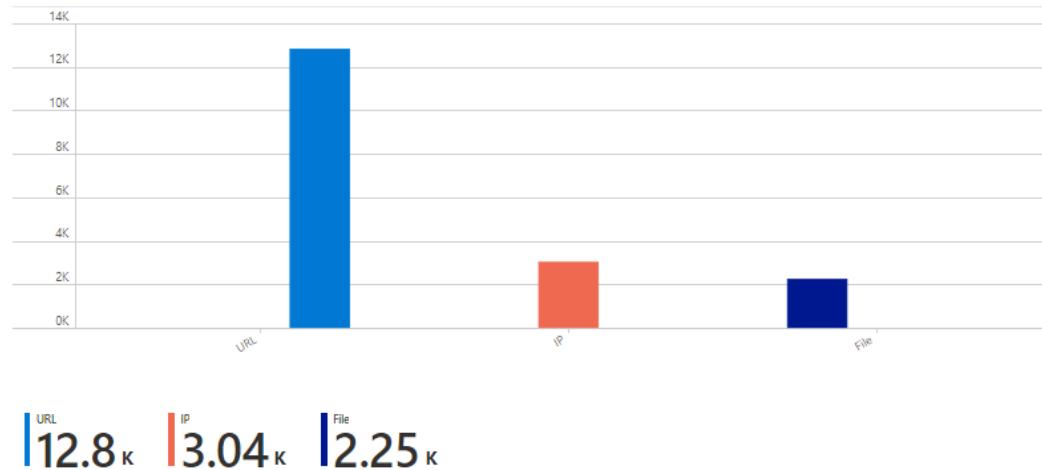
Threat Intelligence - cybersecuritysoc

cybersecuritysoc

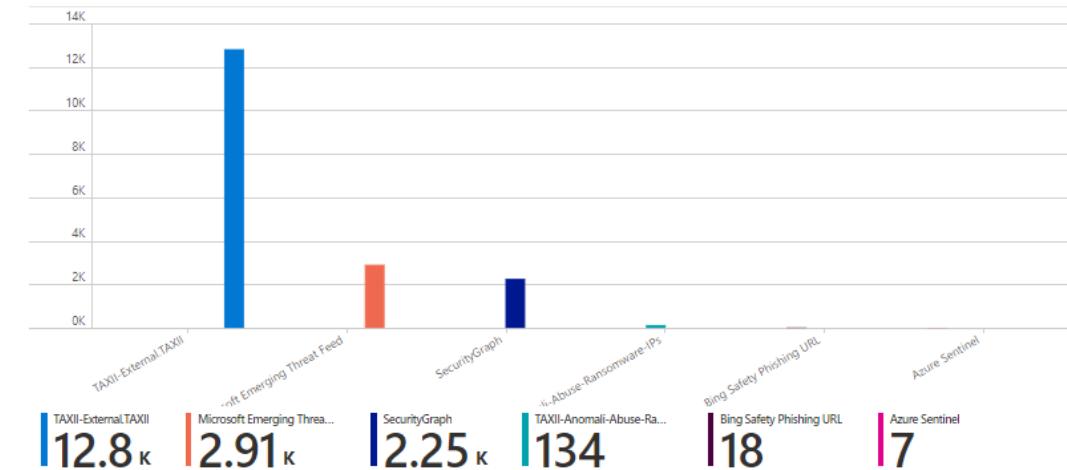
X

 Edit
 Open
 Auto refresh: Off

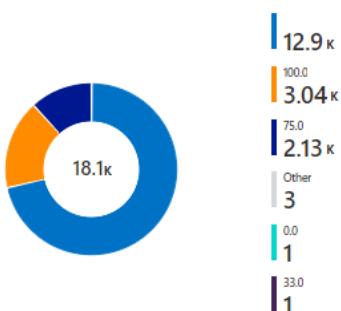
Active indicators by indicator type



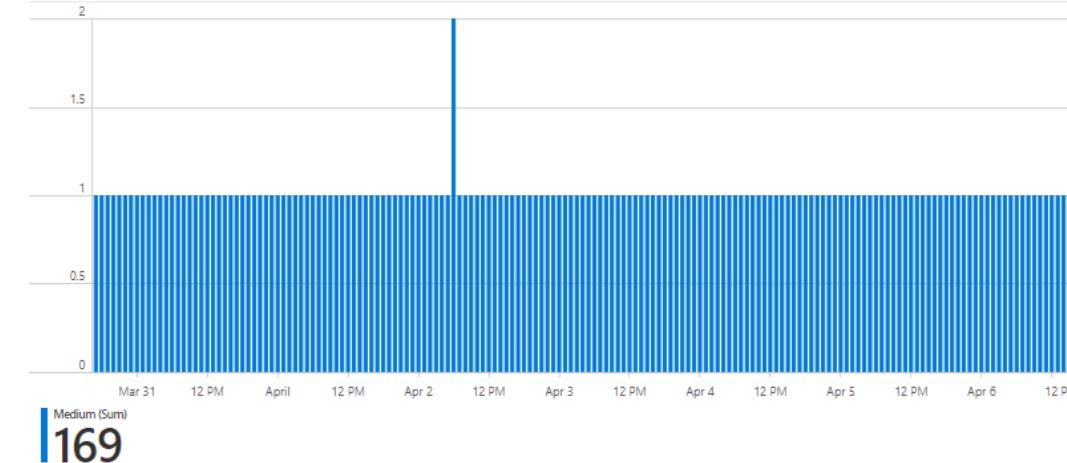
Active indicators by indicator source



Active indicators by confidence score



Alerts generated from threat intelligence by alert severity and date



Alert counts by indicator

Value	ThreatType	Description	Source	Alerts
144.91.119.160	malicious-activity	Malicious IP Address	Azure Sentinel	16
80.87.202.49	malicious-activity	TS ID: 51186673796; iType: mal_ip; State: active; Org: JSC ...	TAXII-Anomali-Abuse-Ransomware-IPs	7

Average detection time by source

Source	DetectionTime	Alerts
Azure Sentinel	18 hrs DELAYED	168
TAXII-Anomali-Abuse-Ransomware-IPs	06 hrs AHEAD	7

Playbooks and Automation

When to use Playbooks

Response

(trigger: incident)

Examples:

- Alerting / external case management
- Provide / gather data from other systems
- Containment and configuration changes

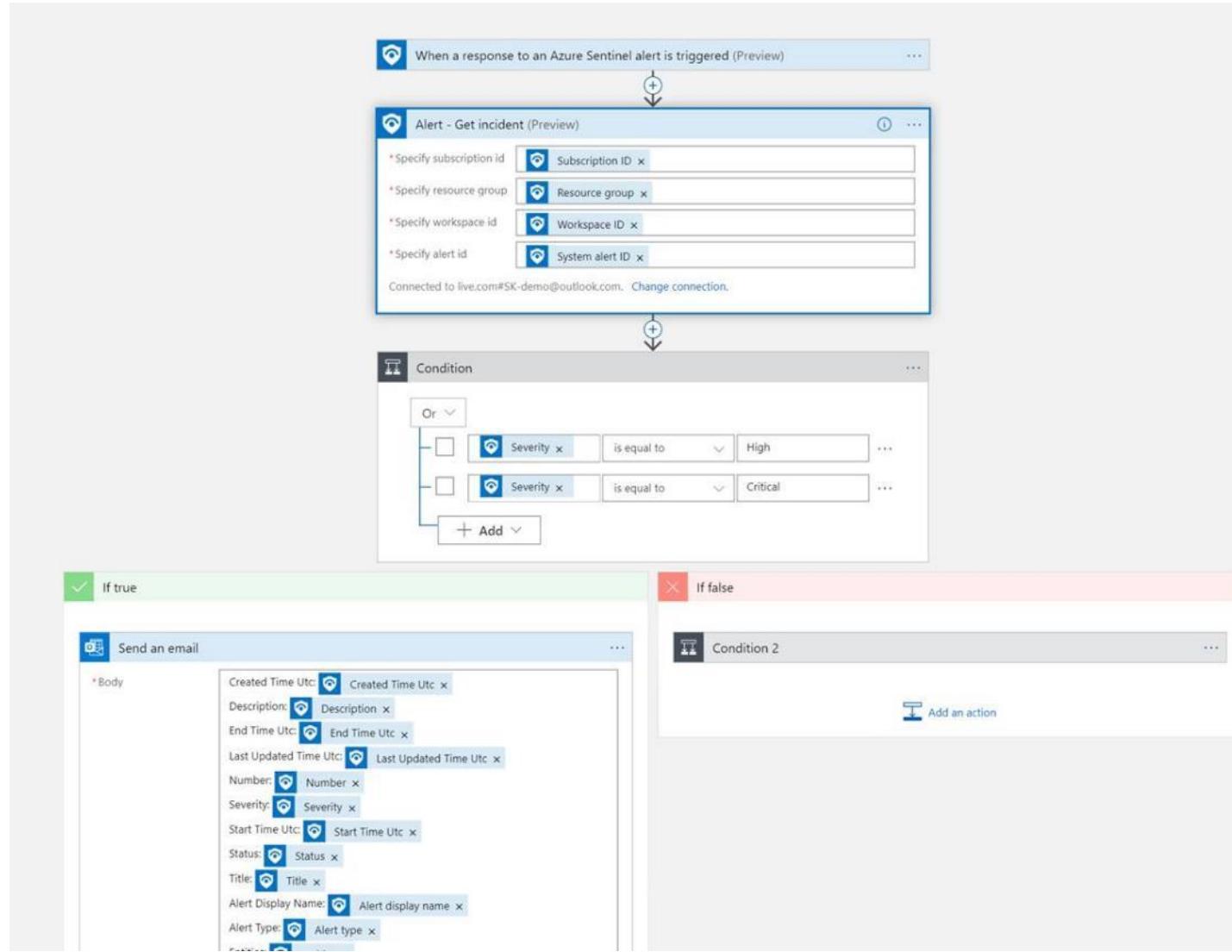
Enrichment

(trigger: scheduled)

Examples:

- Retrieving external data (IP lookup, VA, etc)
- Scheduled reporting / activity summary
- Recurring activity

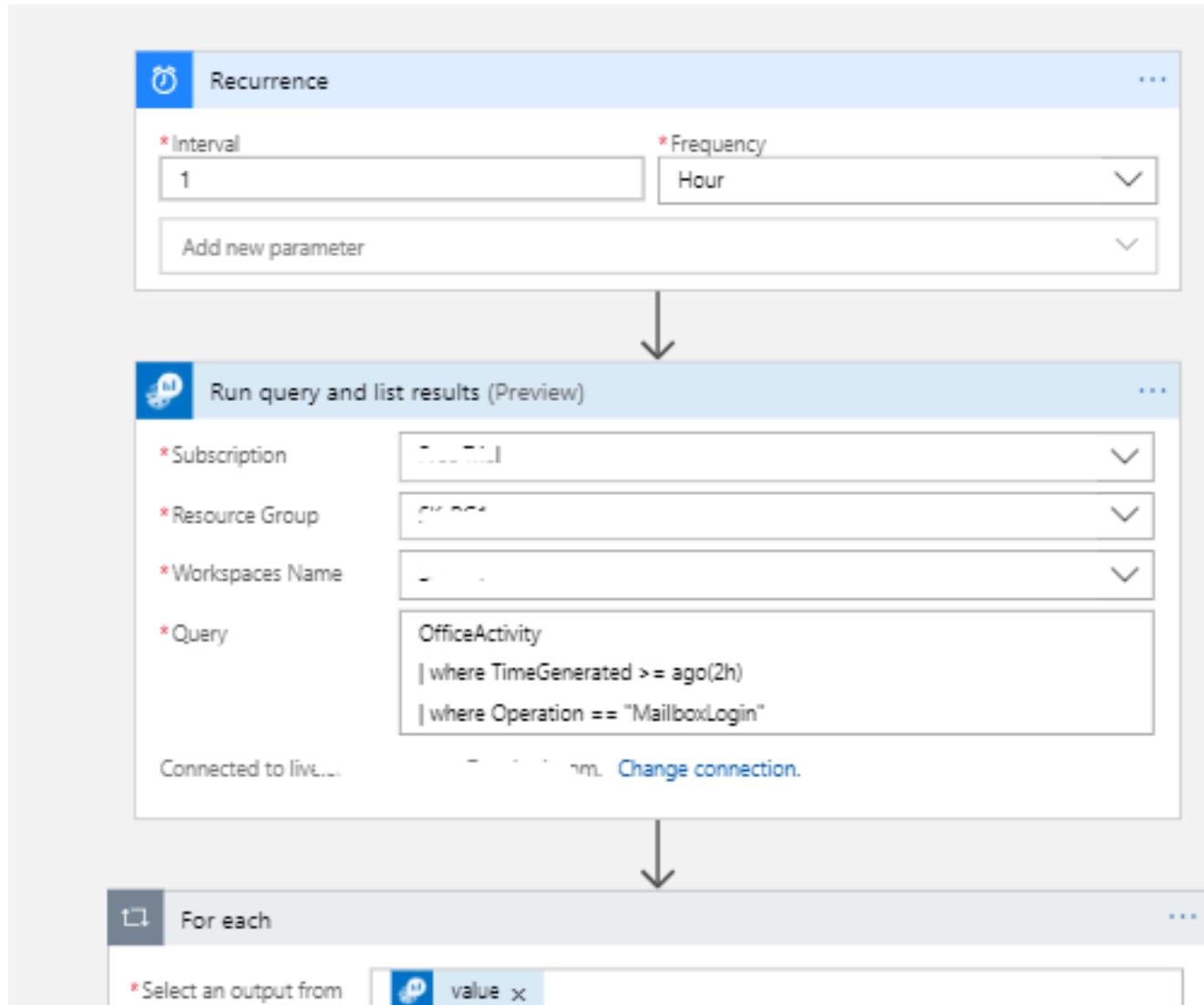
Example (Response)



Trigger

Logical Workflow

Example (Enrichment)



Trigger

Logical Workflow

Trigger

Response

The screenshot shows the Azure Sentinel Response interface. At the top, there's a search bar with the text "Sentinel". Below it, a navigation bar includes "For You", "All" (which is selected), "Built-in", "Standard", "Enterprise", and "Custom". A large blue button with a white icon and the text "Azure Sentinel" is prominently displayed. At the bottom, there are tabs for "Triggers" (selected) and "Actions". Under the "Triggers" tab, there's a single item: "When a response to an Azure Sentinel alert is triggered (preview)" with the "Azure Sentinel" connector. There are also links for "Don't see what you need?" and "Help us decide which connectors and triggers to add next with UserVoice".

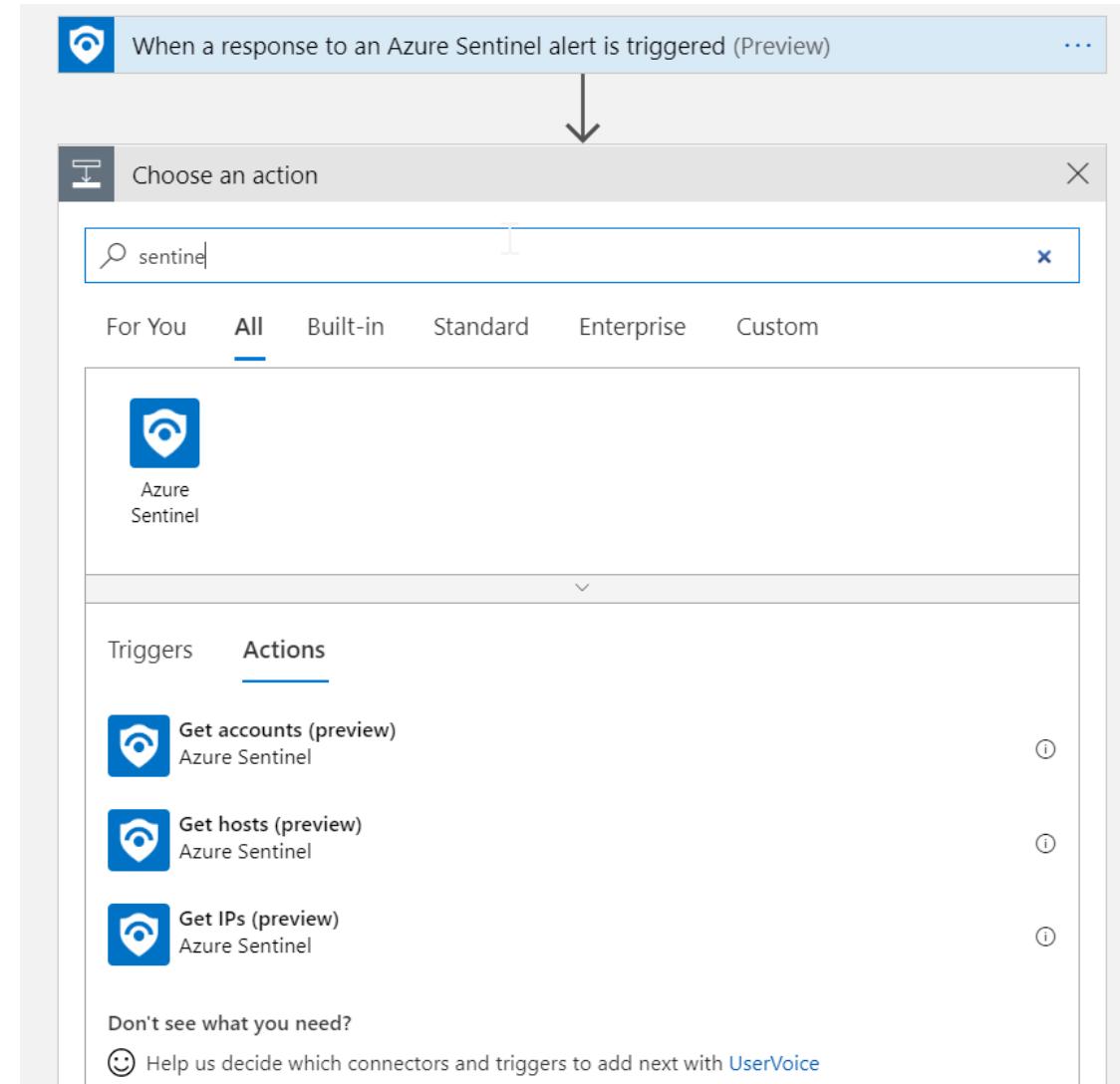
Recurrence

The screenshot shows the "Recurrence" configuration dialog. It has fields for "Interval" (set to 1) and "Frequency" (set to "Hour"). There's also a "Add new parameter" button. The dialog has a header with a timer icon and the word "Recurrence", and a close button in the top right corner.

Common Workflow Modules

Sentinel

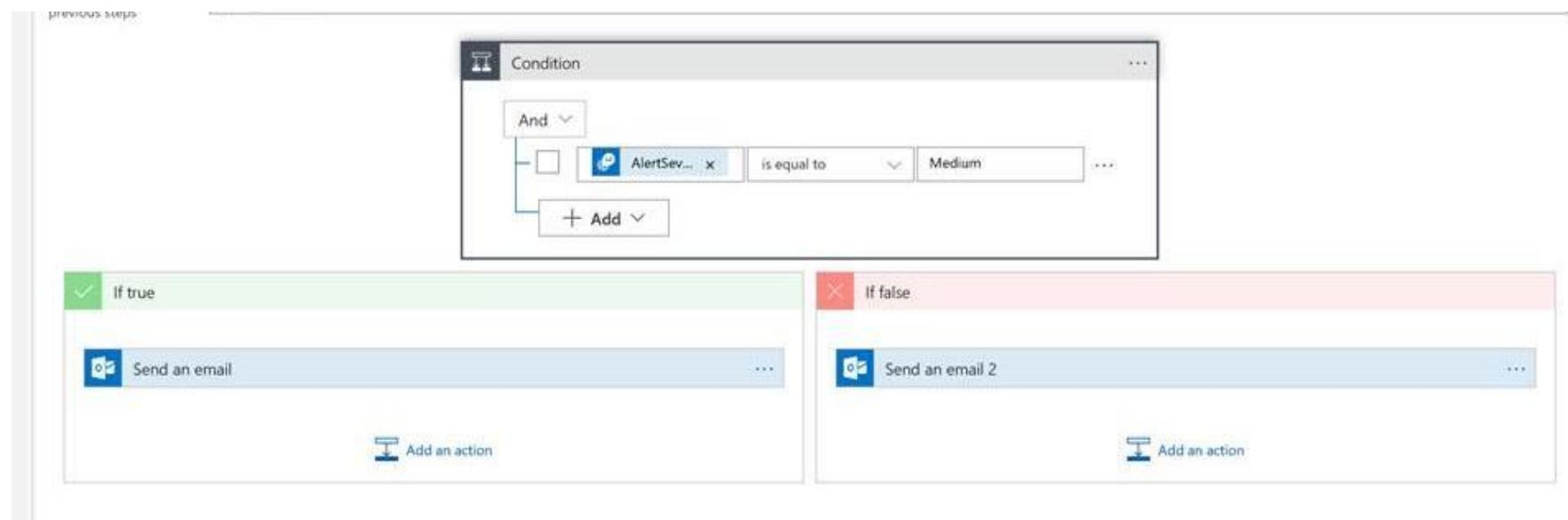
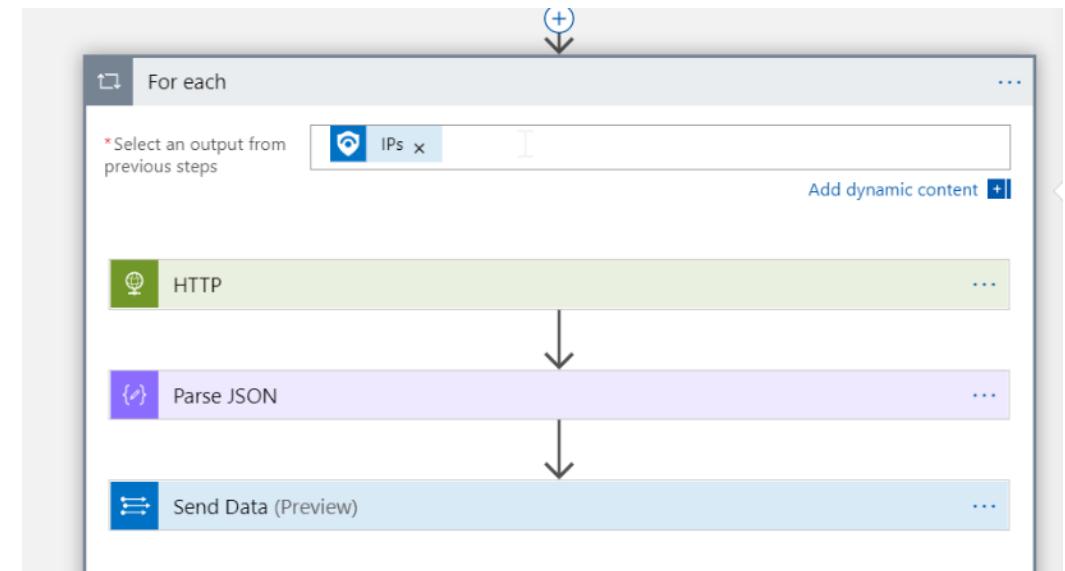
Extract specific values from the entities field



Common Workflow Modules

For Each / Condition (if/and)

Iterate (through a specified field – e.g.
for each IP / for each Entity / ...)



Common Workflow Modules

HTTP

Call an external API

HTTP

* Method: GET

* URI: https://www.whoisxmlapi.com/whoisserver/WhoisService

Headers: Enter key | Enter value

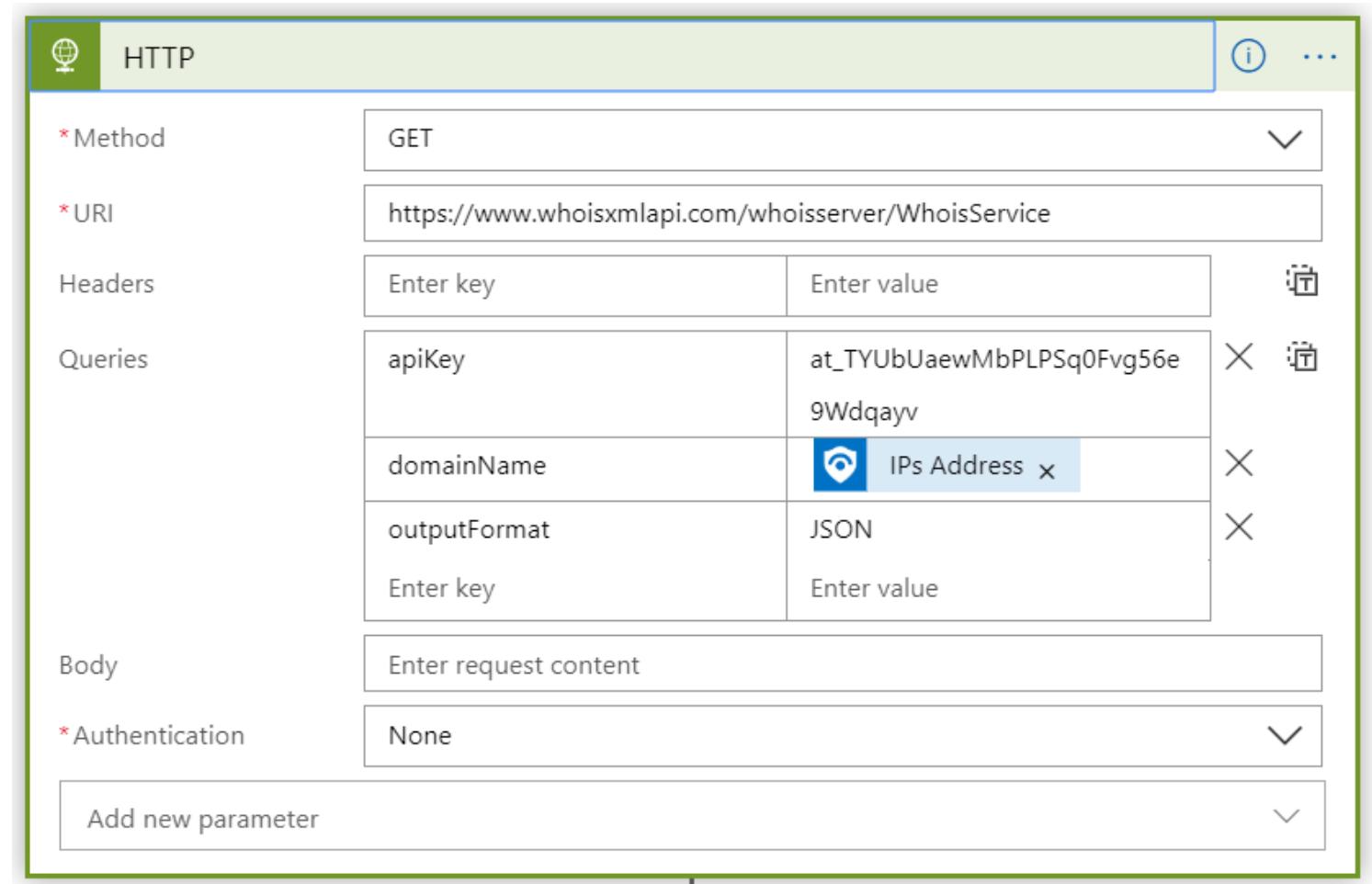
Queries:

apiKey	at_TYUbUaewMbPLPSq0Fvg56e 9Wdqayv
domainName	IPs Address <input type="button" value="X"/>
outputFormat	JSON
Enter key	Enter value

Body: Enter request content

* Authentication: None

Add new parameter



Common Workflow Modules

Parse

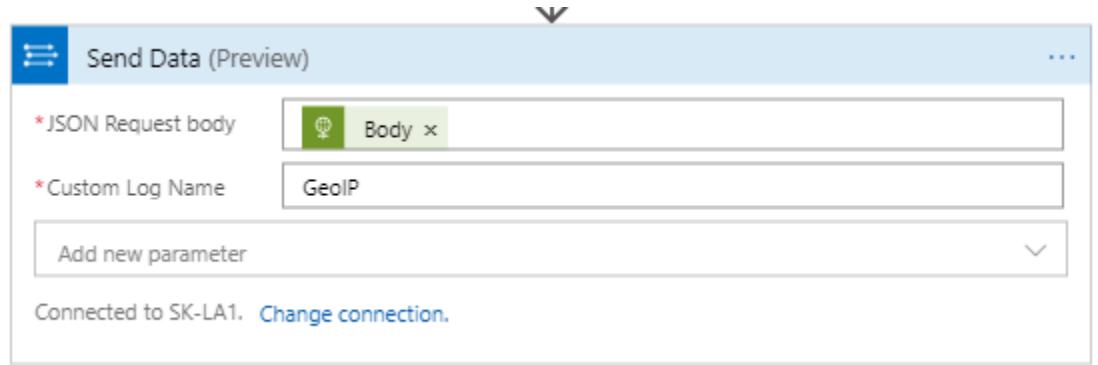
Parse JSON enables you to parse information received (e.g. from the Body of the API call earlier)

The screenshot shows the configuration of a 'Parse JSON' module in a Microsoft Flow. The 'Content' field is set to 'Body'. The 'Schema' field displays a complex JSON schema with nested properties for 'WhoisRecord' and 'audit'. A button at the bottom left says 'Use sample payload to generate schema'. Below this module is a 'Send Data (Preview)' module. Its 'JSON Request body' field contains a placeholder 'WhoisRecord' with a delete icon. The 'Custom Log Name' field is set to 'WHOIS'. At the bottom, it says 'Connected to Sentinel. Change connection.'

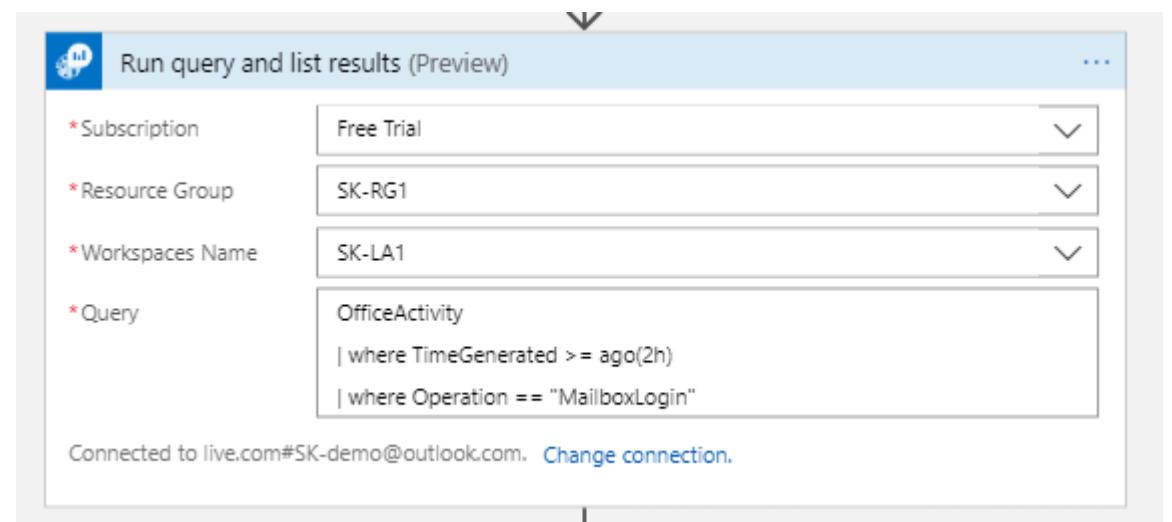
Common Workflow Modules

Log Analytics

Enables you to write data into Log Analytics



Enables you to query Log Analytics

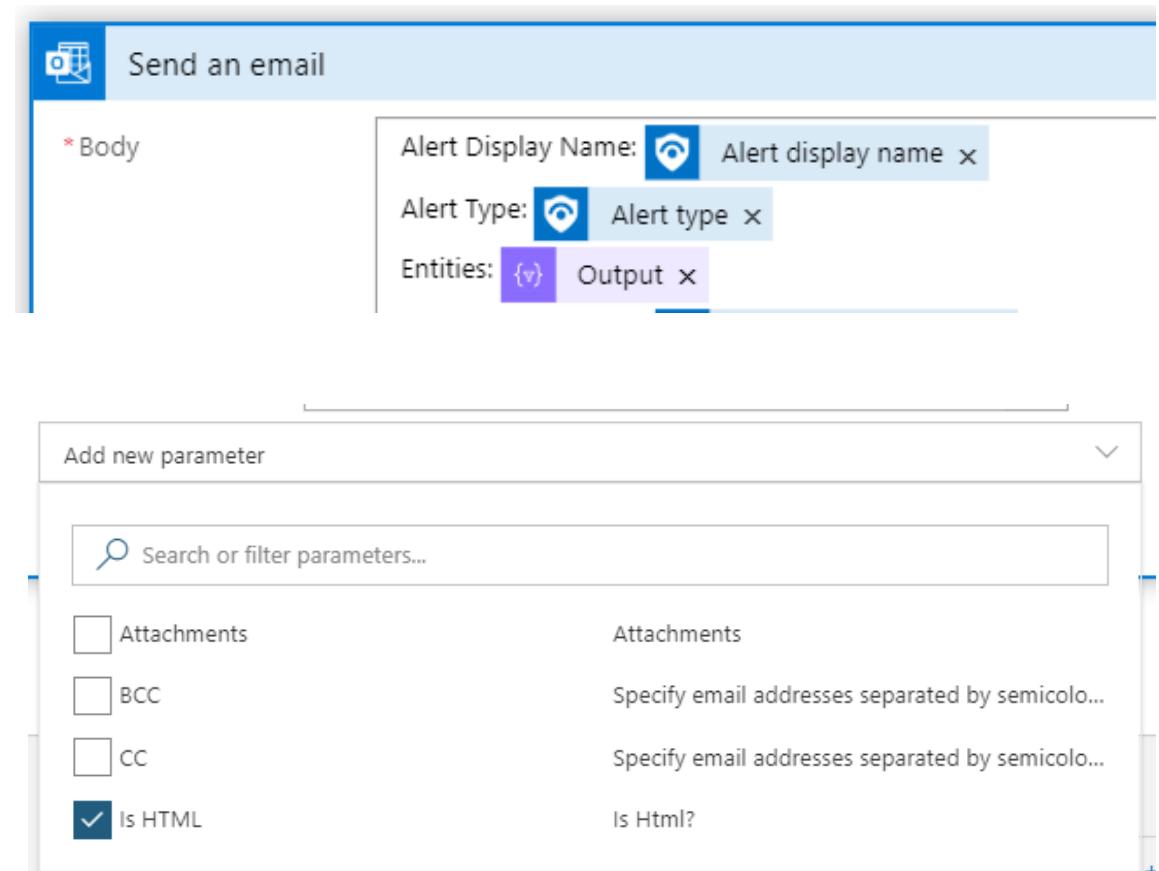


Common Workflow Modules

Send Email / Teams

Enables you to send an email and embed dynamic information (through fields)

Note: there are several options / email providers you can use



Common Workflow Modules

Servicenow / JIRA

Enables you to open/modify/close/etc.
a case in Servicenow or JIRA

Lab: Creating a Playbook

Home > Azure Sentinel > Azure Sentinel

Azure Sentinel | Automation

Selected workspace: 'tm-sentinel-workshop'

Search (Ctrl+ /) Create Refresh Enable Disable Delete

Add new rule Add new playbook

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

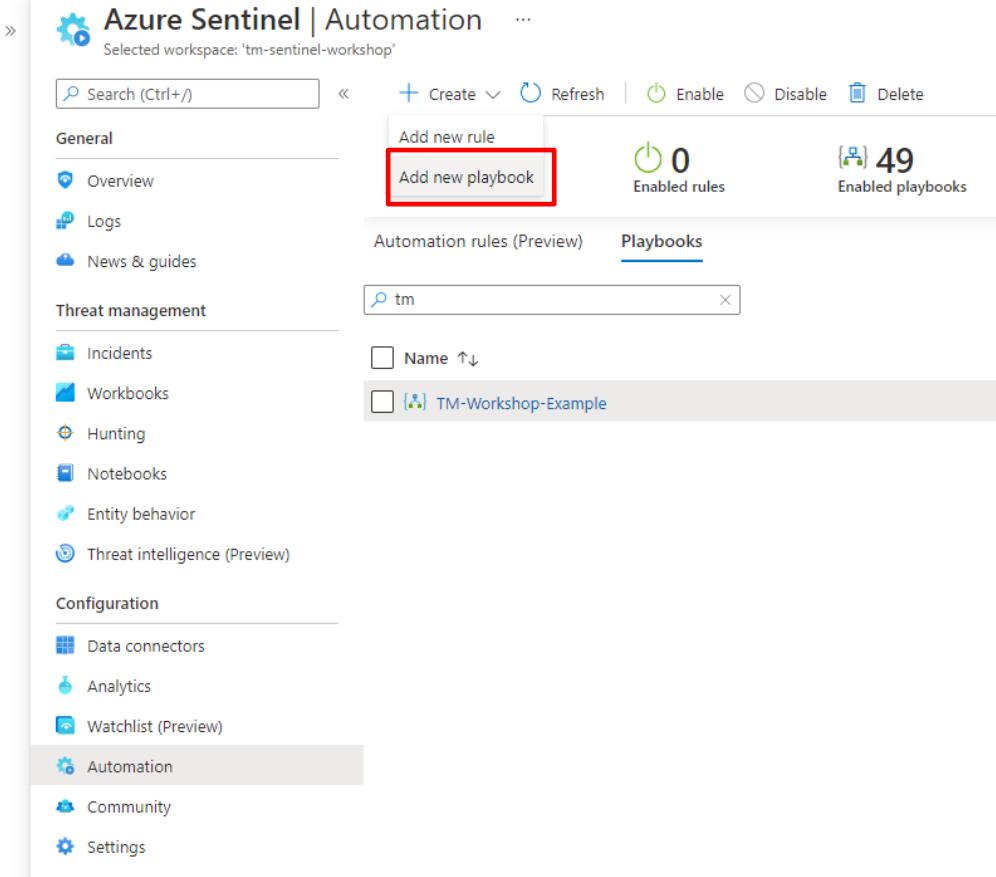
- Data connectors
- Analytics
- Watchlist (Preview)
- Automation
- Community
- Settings

Automation rules (Preview) Playbooks

tm

Name ↑↓

[+] TM-Workshop-Example



When a response to an Azure Sentinel alert is triggered (Preview)

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

Connected to shko@microsoft.com. Change connection.

Send an email (V2)

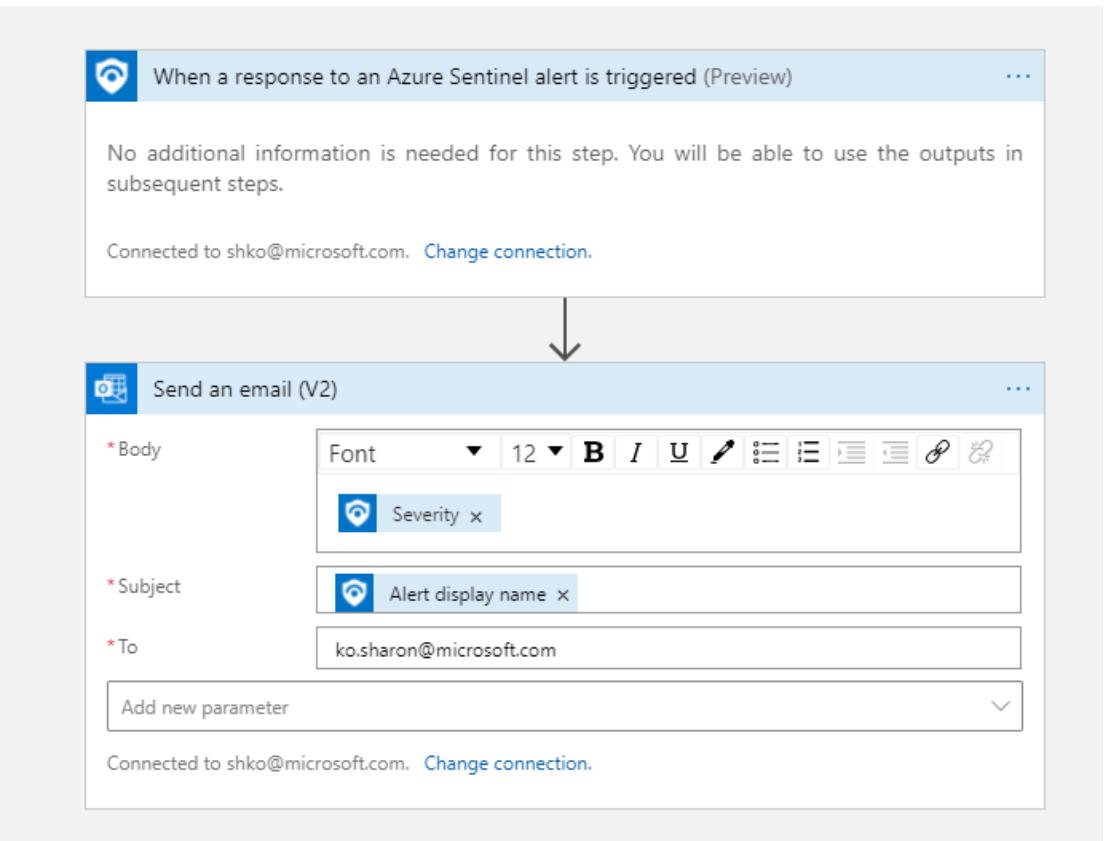
* Body Severity

* Subject Alert display name

* To ko.sharon@microsoft.com

Add new parameter

Connected to shko@microsoft.com. Change connection.



Deploy Playbook Templates from Github

The screenshot shows two views of a GitHub repository. On the left, the main repository page for 'Azure-Sentinel / Playbooks' is displayed, showing a list of commits. On the right, a detailed view of the 'Aggregate-SNOW-tickets' playbook is shown, including its README.md file and deployment options.

Azure-Sentinel / Playbooks

- joshhighet fix-resource-name (4 days ago)
- Aggregate-SNOW-tickets Fixing Playbook Deploy URLs (14 months ago)
- AutoConnect-ASCSubscriptions ASC readme update fix (No local links)
- Block-AADUser Fixing Playbook Deploy URLs
- Block-ExchangeIP Update readme.md
- Block-IPs-on-MDATP-Using-GraphSecurity Update approval email message to High Importance
- Block-OnPremADUser Readme update
- Change-Incident-Severity Fixing Playbook Deploy URLs
- Close-Incident-ASCArt Merge pull request #506 from swiftsolves-msft/nateswi_playbook
- Close-Incident-MCAS Added Deploy to Azure button, change name of json to reflect it.
- Close-SentinelIncident-fromSNOW commit
- Comment-OriginAlertURL Added Readme file
- Comment-RemediationSteps Create readme.md
- Confirm-AADRiskyUser fixed schema
- Create-AzureDevOpsTask readme for the Create-AzureDevOpsTask playbook
- Create-AzureSnapshot Add entities to identify VM
- Create-IBMResilientIncident initial

Azure / Azure-Sentinel

Azure-Sentinel / Playbooks / Aggregate-SNOW-tickets

- dicolanl Fixing Playbook Deploy URLs (2852a71 on Feb 24, 2020)
- ... (Ellipsis)
- README.md Fixing Playbook Deploy URLs (14 months ago)
- azuredeploy.json Add files via upload (15 months ago)

README.md

Aggregate-SNOW-Tickets

[Deploy to Azure](#) [Deploy to Azure Gov](#)

Azure Sentinel Github (Playbooks):

<https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks>

Lab: Manually Triggering a Playbook

The screenshot shows two windows side-by-side. The left window is the 'Incident' view for 'Sharon_Rule Sample' (Incident ID: 18). It displays basic incident details like owner, status, severity, and alert product names. The right window is the 'Alert playbooks' page for the 'AH - Logon Account Failure Rule'. It lists four available playbooks: 'Admin-CEFLogsAlert', 'BlockIP_PaloAlto_BlockUserAAD_ServiceNow', 'Get-GeoFromIpAndTagIncident', and 'Get-Incident'. Each playbook has a 'Run' button, which is highlighted with a red box in the bottom right corner of the screenshot.

Incident

- Incident ID: 18
- Sharon_Rule Sample (Alert name: New, Severity: Medium)
- Owner: Unassigned
- Status: New
- Severity: Medium
- Description: Type whatever you want here
- Alert product names: Azure Sentinel
- Evidence: 1 Events, 1 Alerts, 0 Bookmarks
- Last update time: 04/06/21, 07:17 PM
- Creation time: 04/06/21, 07:17 PM
- Entities (1): ko.sharon@microsoft.com
- Tactics (2): Privilege Escalation, Credential Access
- View full details >
- Incident workbook: Incident Overview
- Analytics rule: Sharon_Rule Sample
- Tags: +
- Incident link: https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/
- Last comment: (Total: 0)
- Write a comment...

Alert playbooks

AH - Logon Account Failure Rule

Playbooks Runs

Search playbooks

Name ↑↓	Status ↑↓	Subscription ↑↓	Action
[+] Admin-CEFLogsAlert	Enabled	CyberSecSOC	Open designer
[+] BlockIP_PaloAlto_BlockUserAAD_ServiceNow	Enabled	CyberSecSOC	Run
[+] Get-GeoFromIpAndTagIncident	Enabled	CyberSecSOC	Open designer
[+] Get-Incident	Enabled	CyberSecSOC	Run

Demo: Attaching a Playbook to a Rule

Home > Azure Sentinel > Azure Sentinel >

Analytics rule wizard - Edit existing rule ...

Sharon_Rule Sample

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

Alert automation

Select a playbook to run when a new alert is generated from this analytics rule. The playbook will receive the alert as its input and only playbooks configured with the alert trigger can be selected.

[SK-ApprovalEmail ▾

Name

[SK-ApprovalEmail

Status

[Enabled

...

Feedback Survey

