Microsoft

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

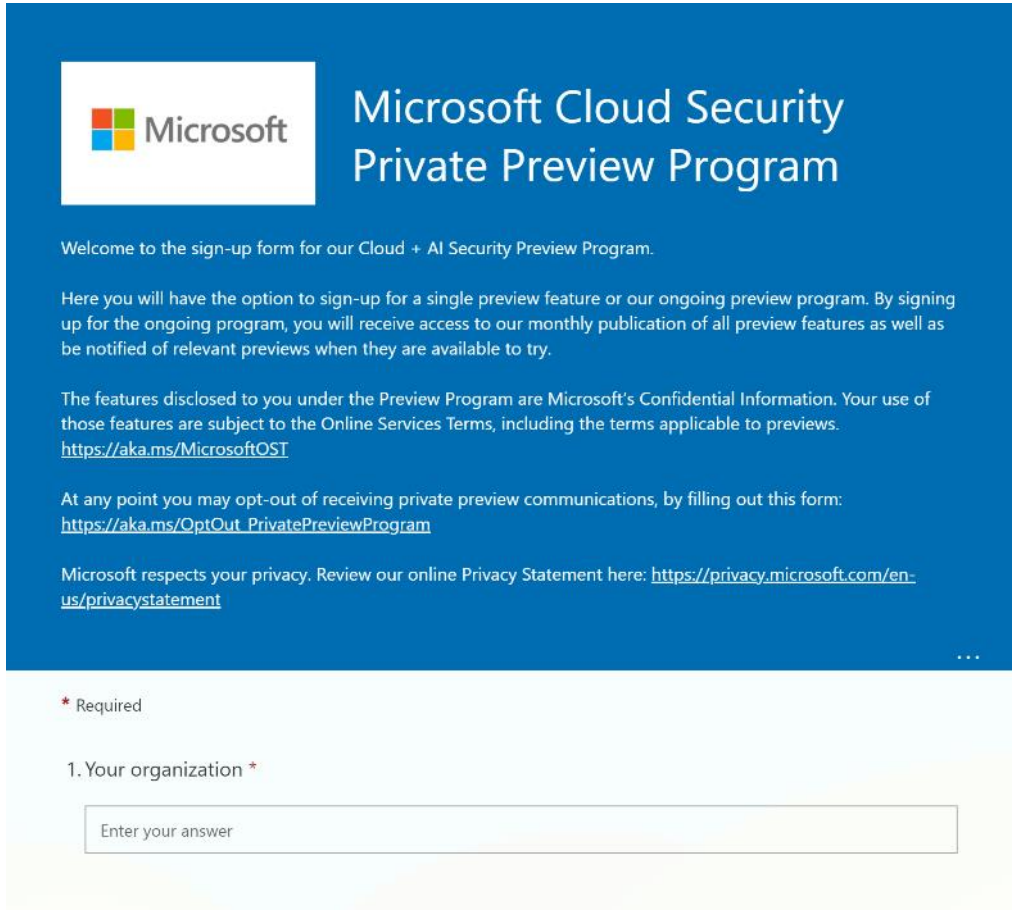
Azure Sentinel Technical Playbook for MSSPs

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

Microsoft Cloud Security Private Preview Program

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



Microsoft

Microsoft Cloud Security Private Preview Program

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

Microsoft

Cloud + AI Security

Private Feature-Preview Program

March 2021 Edition

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

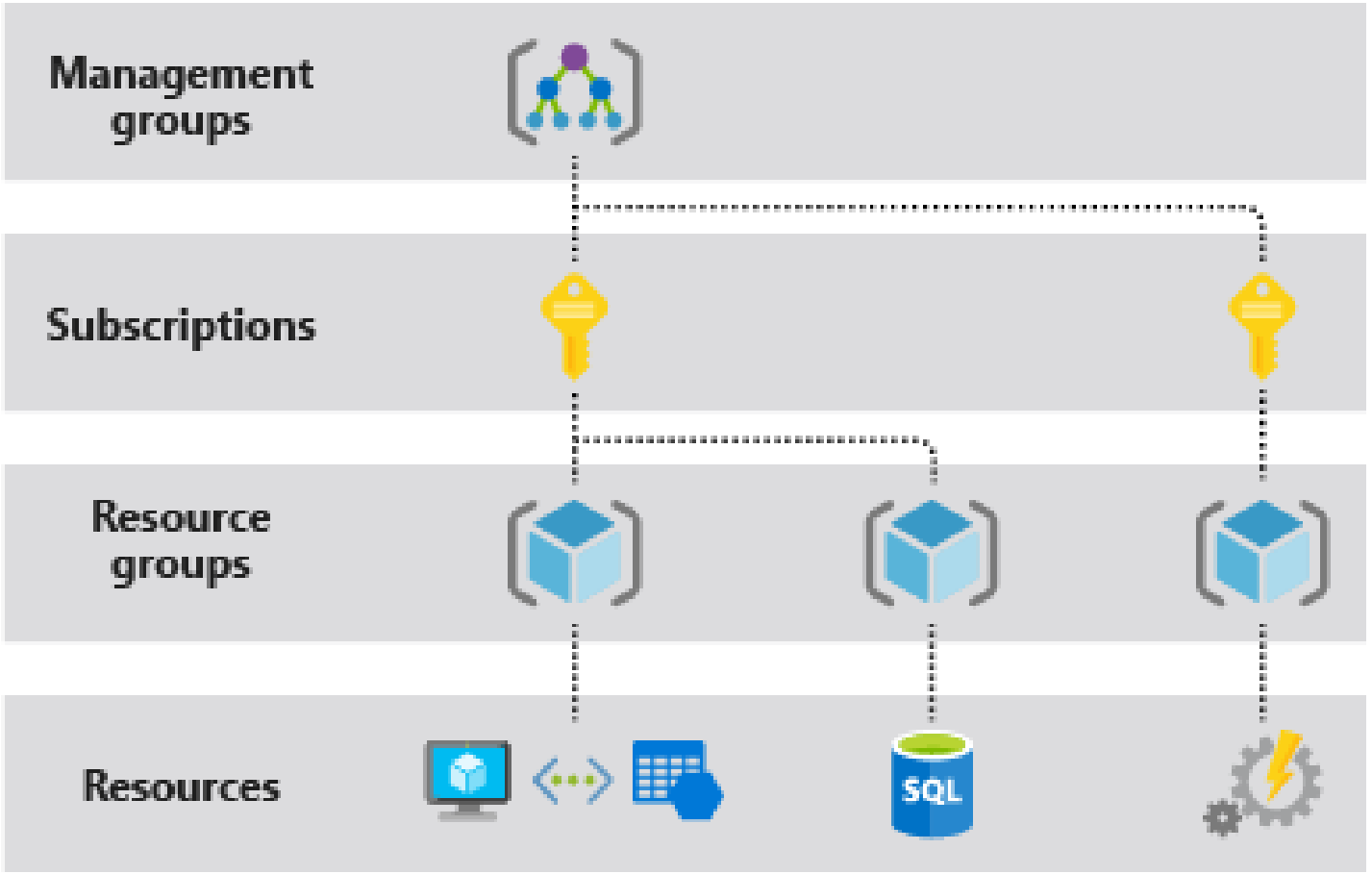
Azure Security Center

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.

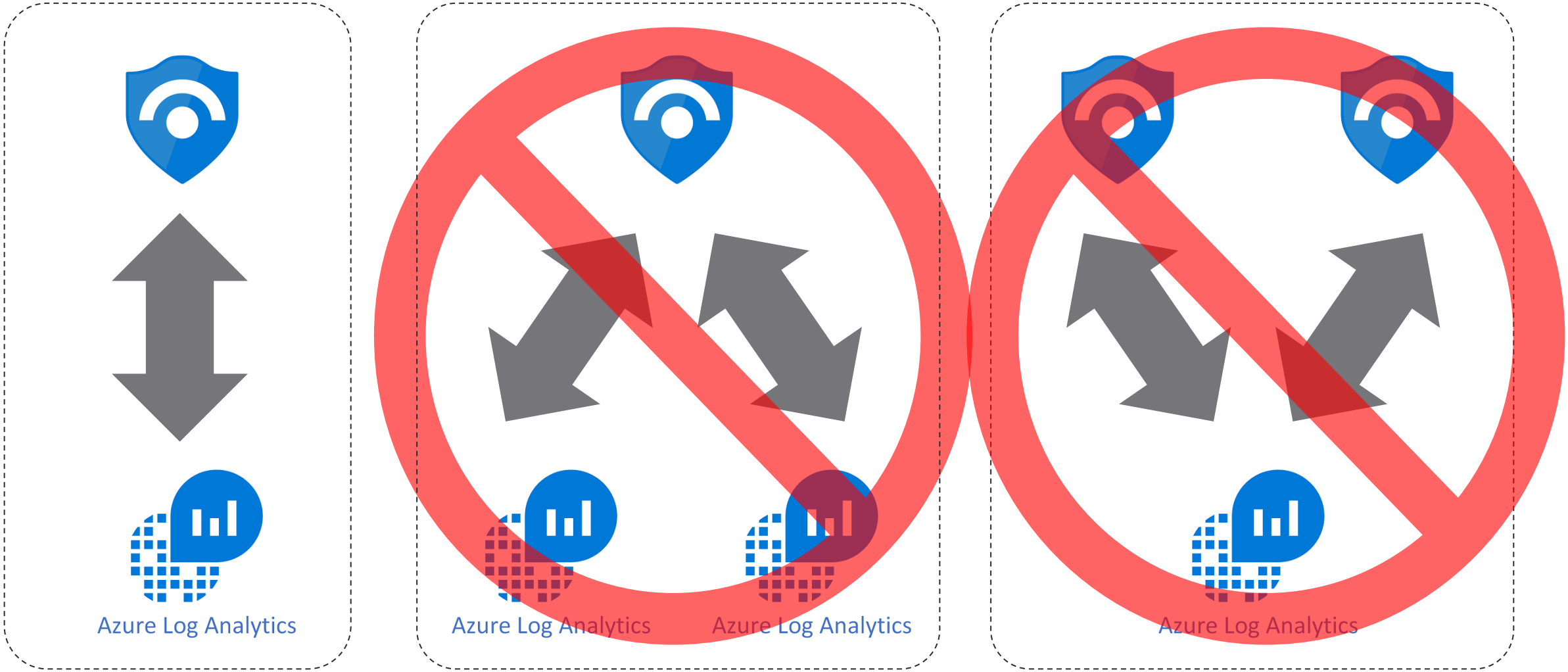
Microsoft Azure

Design and Setup

Azure subscriptions and resources

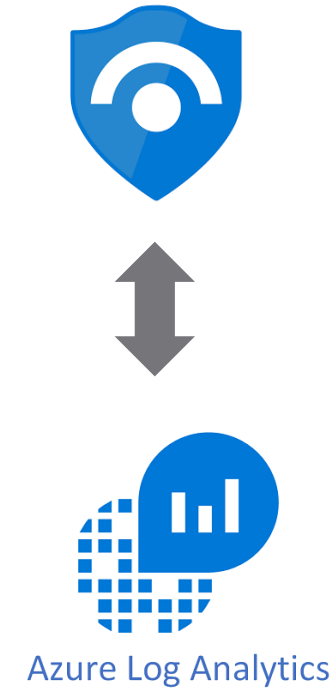


Log Analytics workspace to Azure Sentinel connection is 1-to-1

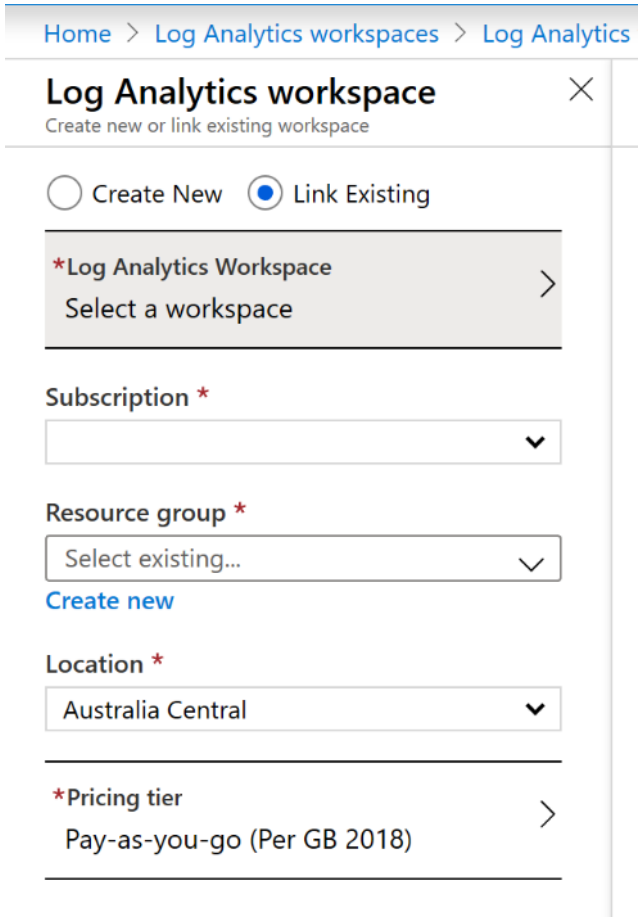


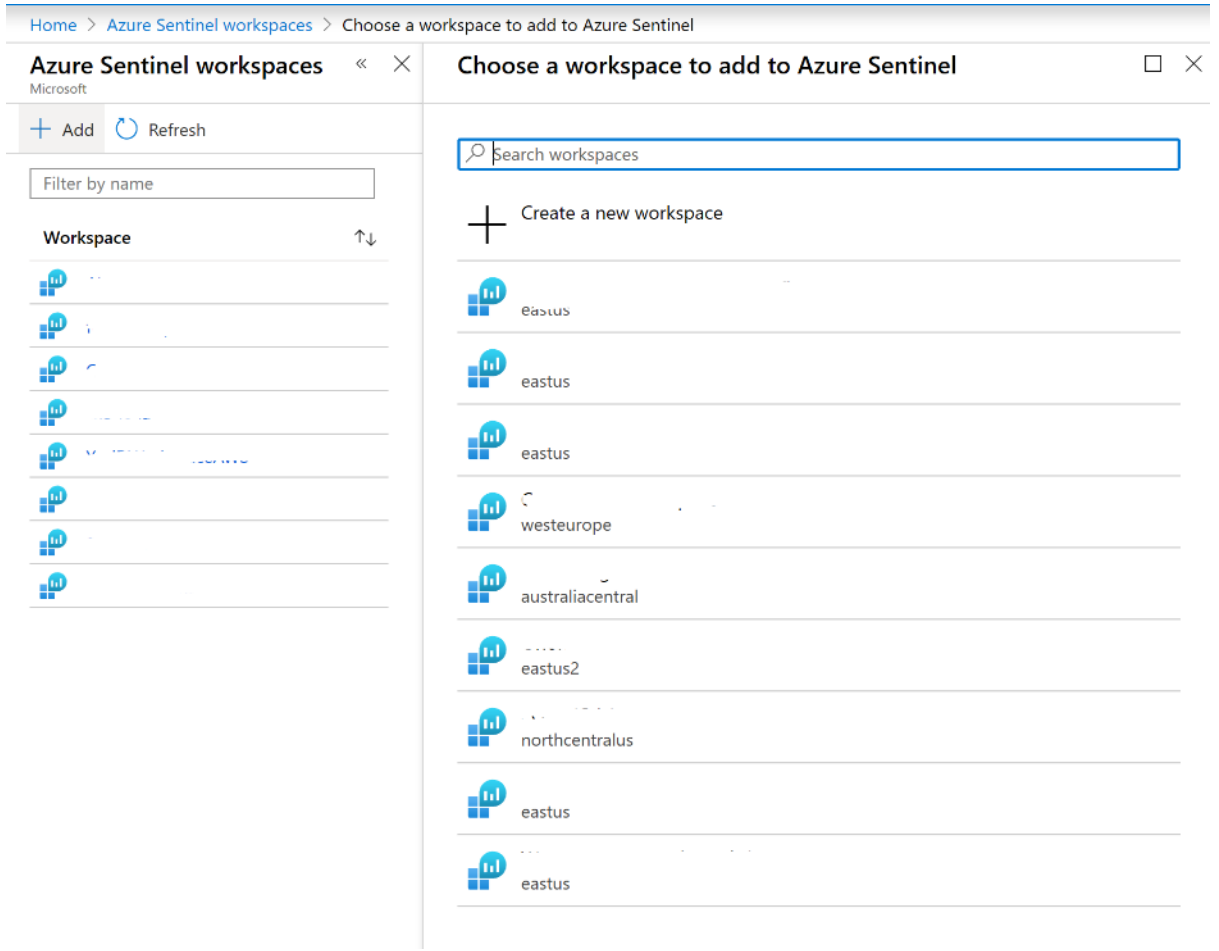
Data can be sent from multiple sources into 1 Log Analytics workspace

- On-premise data, data in the cloud
- Data from multiple workspaces, resource groups, subscriptions, tenants



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





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

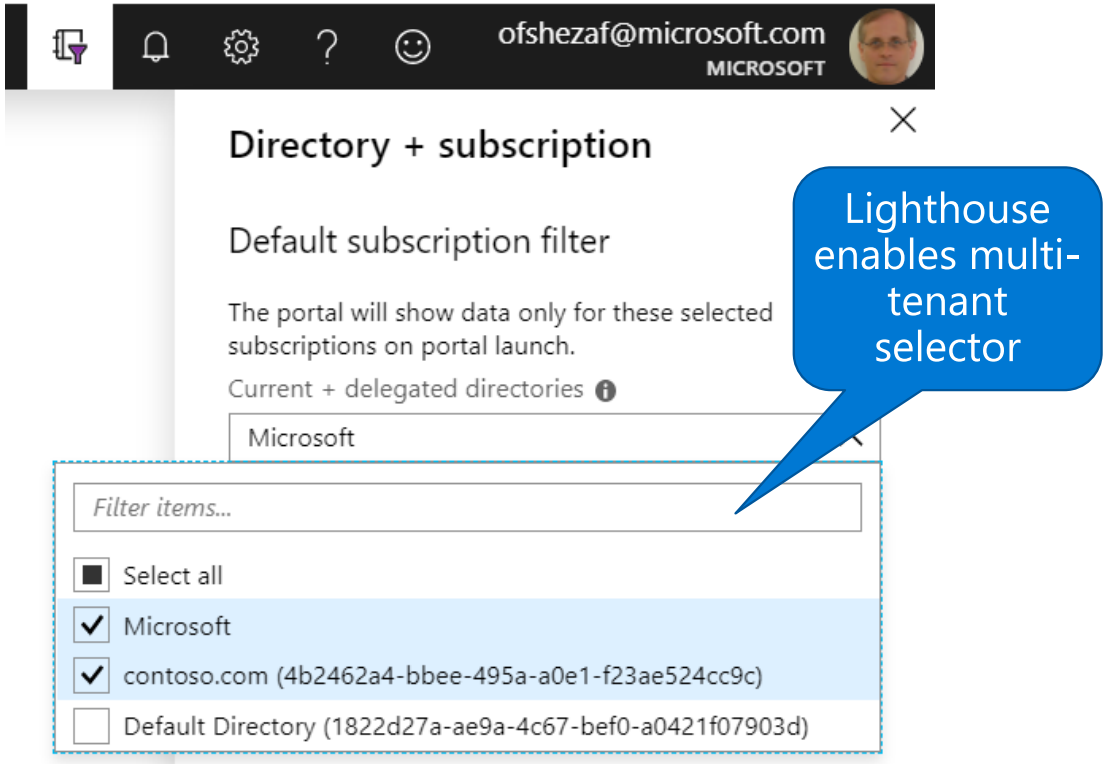
Works across workspaces:

- 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




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

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

Extend Azure Sentinel across workspaces and tenants:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Azure Sentinel RBAC

Actions

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

Users can define custom roles

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

Data

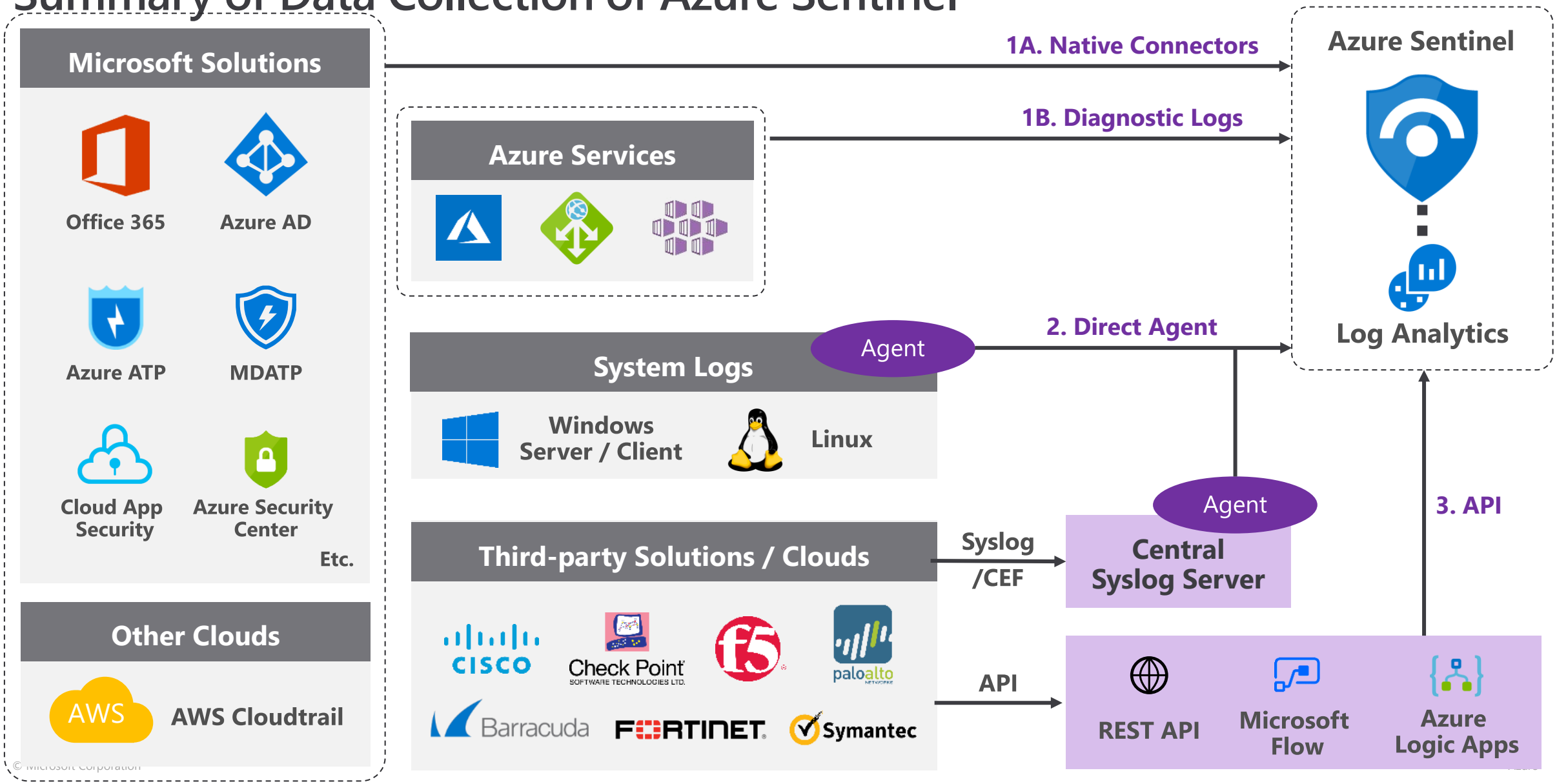
- Resource-context (workspace)
- Table-level RBAC (more info)

Permissions in Azure Sentinel:
https://docs.microsoft.com/en-us/azure/sentinel/roles

Microsoft Azure

Data Collection

Summary of Data Collection of Azure Sentinel

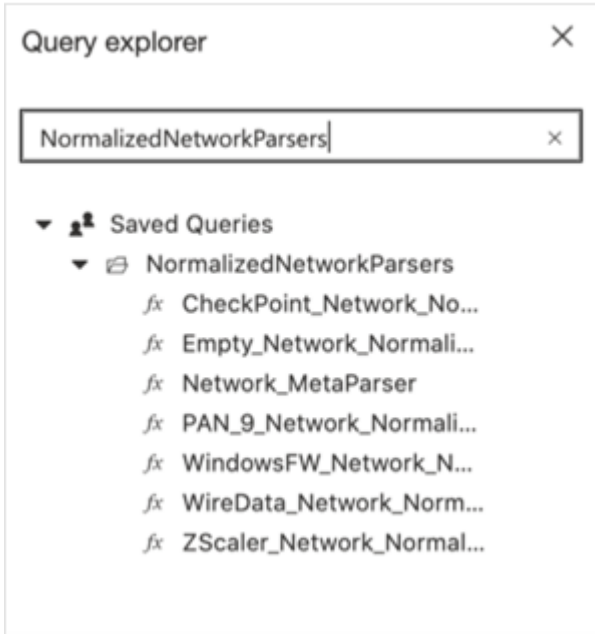


Data Dictionaries (DD)

Common Data Model (CDM)

Detection Model (DM)

https://ossemproject.com/intro.html



Network_MetaParser

Empty_Network_NormalizedParser

CheckPoint_Network_NormalizedParser

PAN_9_Network_NormalizedParser

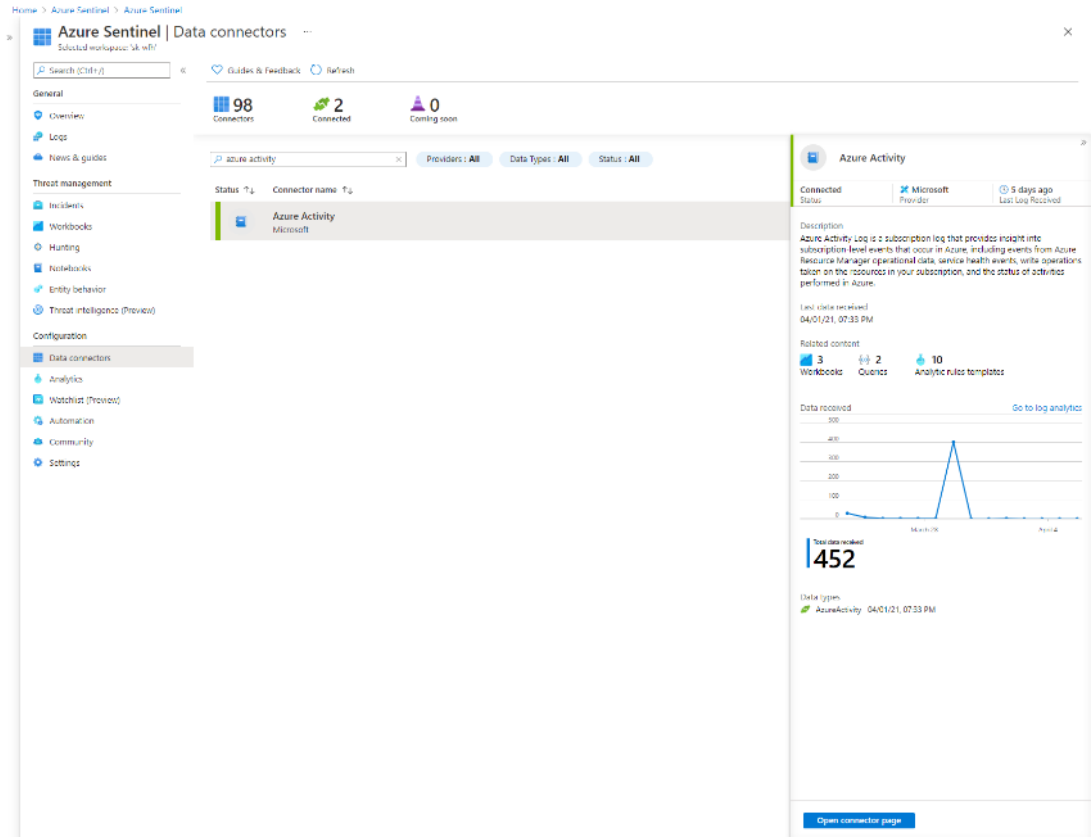
WireData_Network_NormalizedParser

...

Syslog / CEF

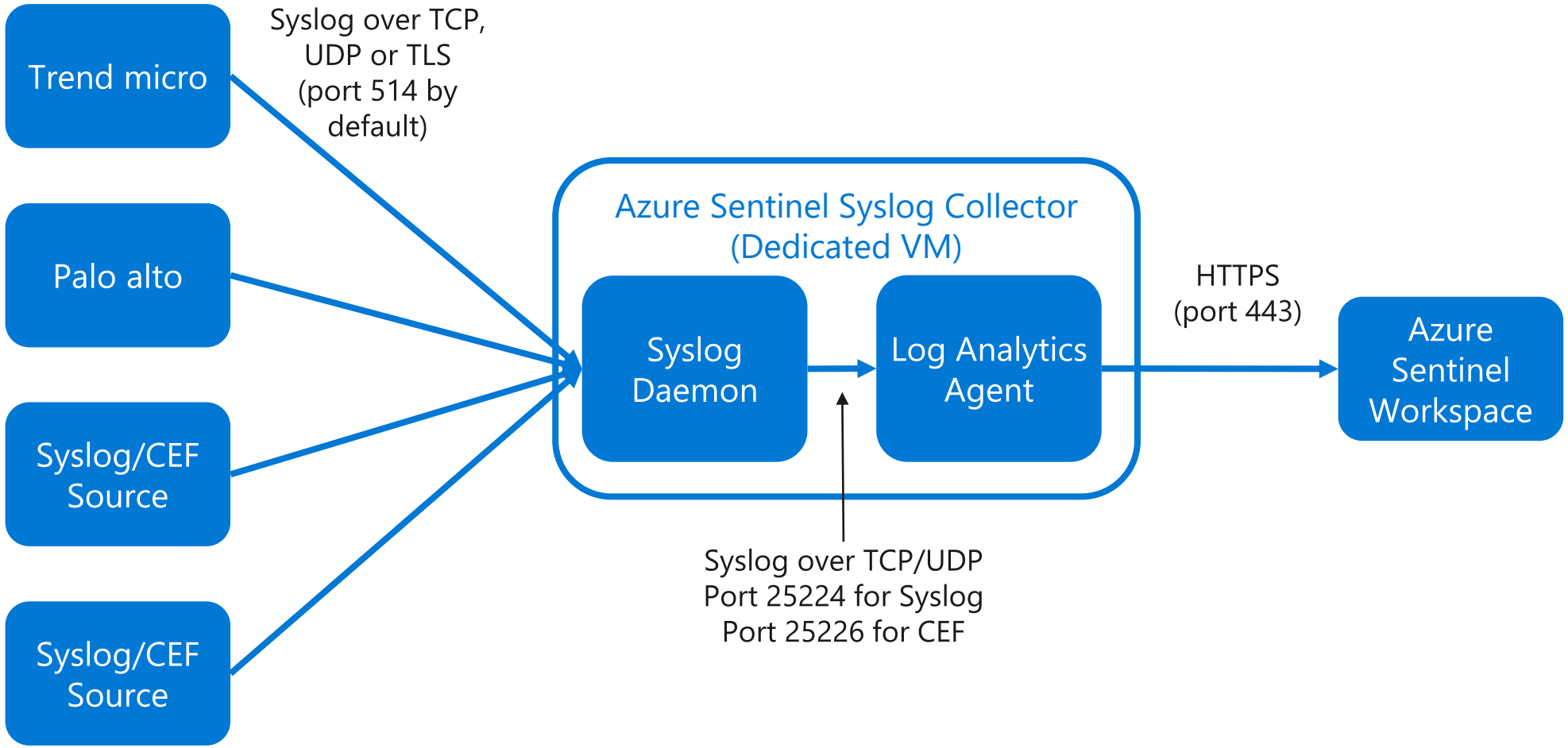
- https://docs.microsoft.com/en-us/azure/sentinel/normalization-schema
- https://docs.microsoft.com/en-us/azure/sentinel/normalization

Demo: Connect Azure Activity Data Connector

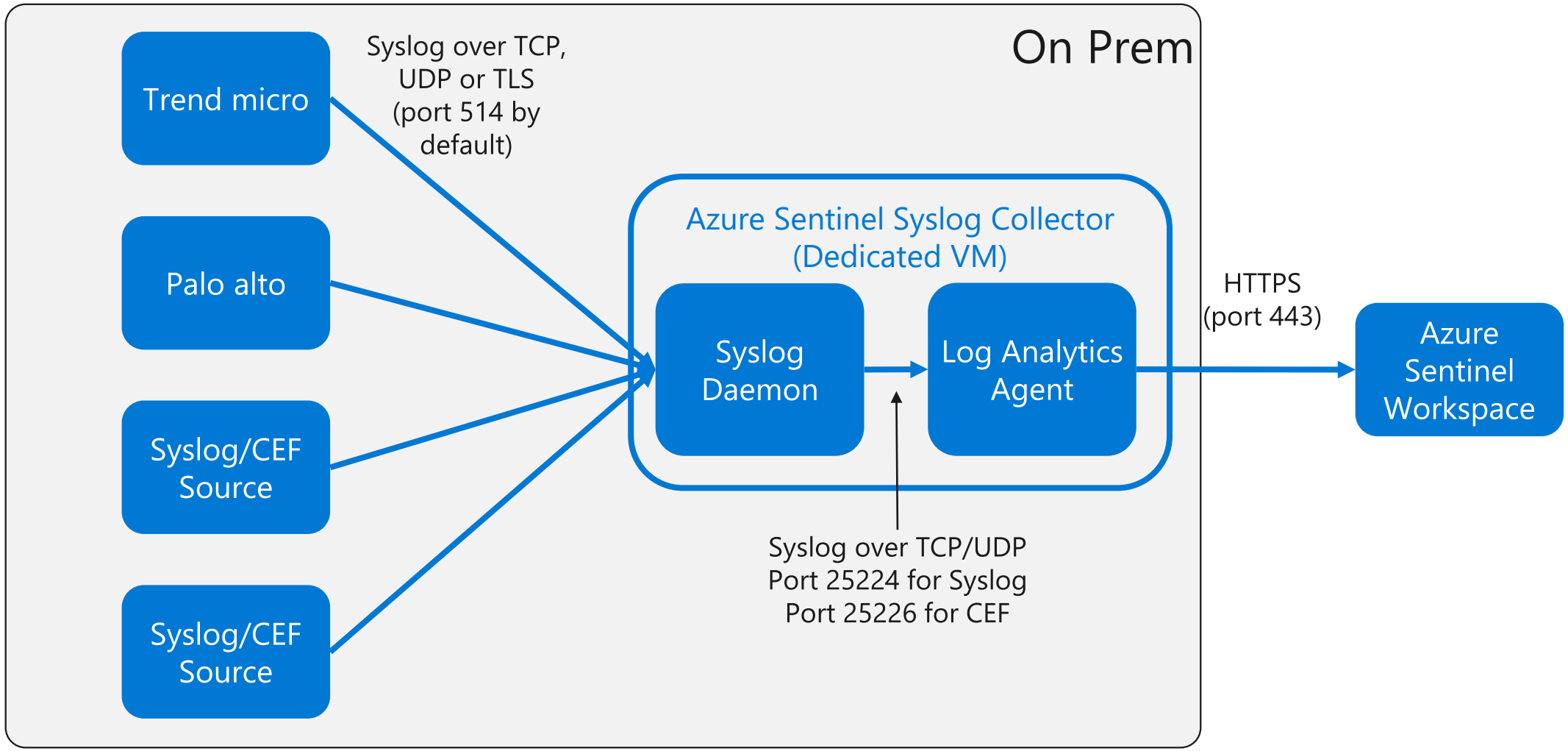


Minimum rights required for connection: varies per connector
(Azure Activity = workspace read, write permissions)

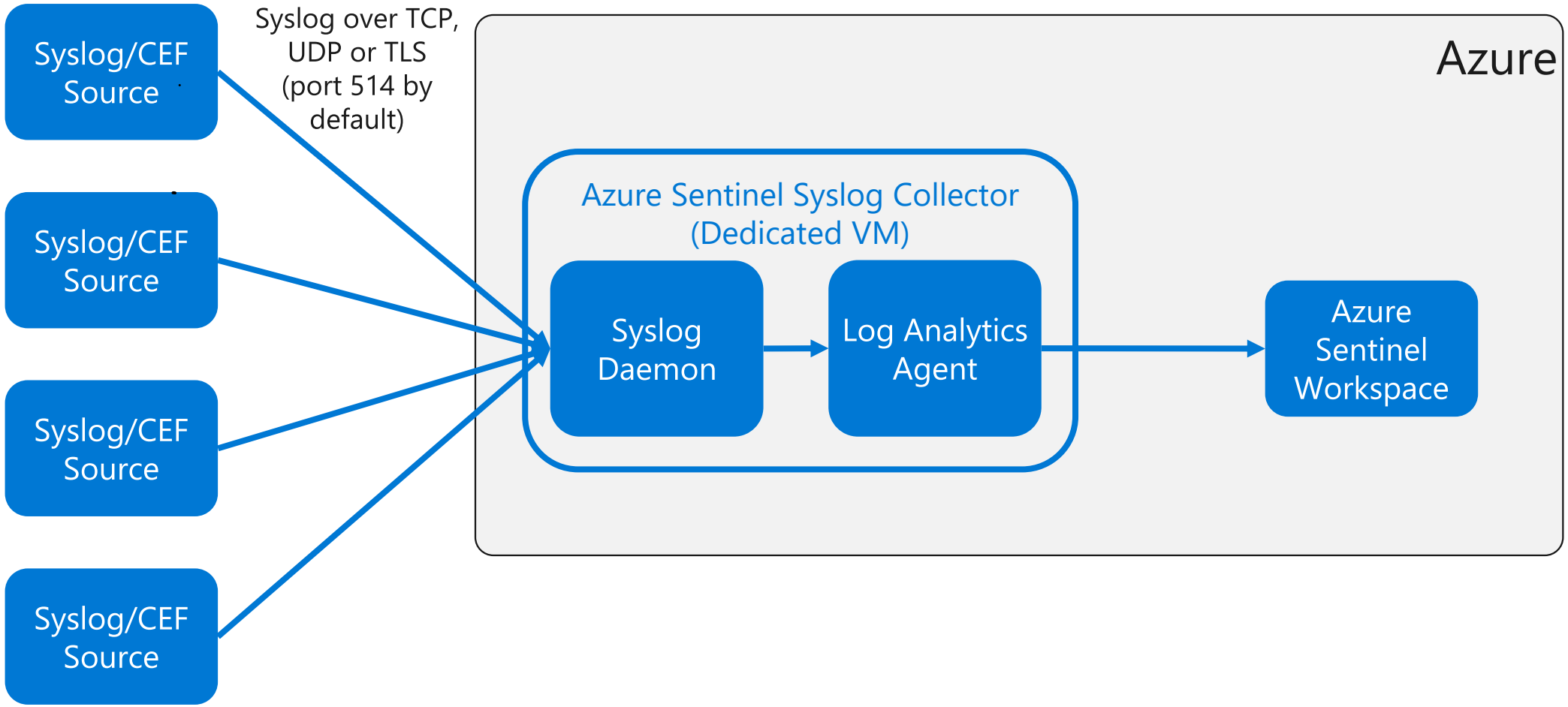
#2 Other Sources via Syslog / CEF



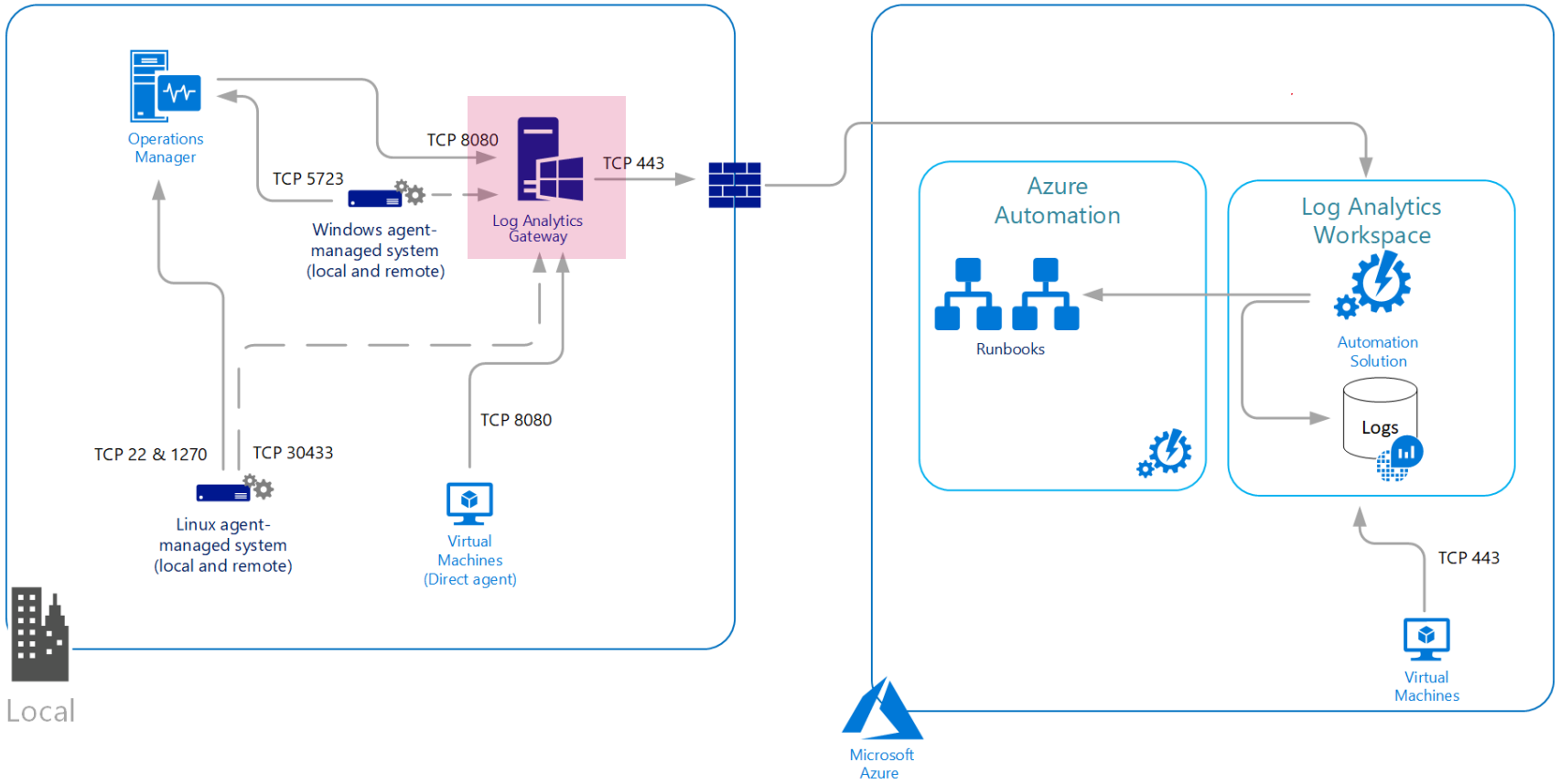
#2 On-Premise Data Collection – On-Premise Collector



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



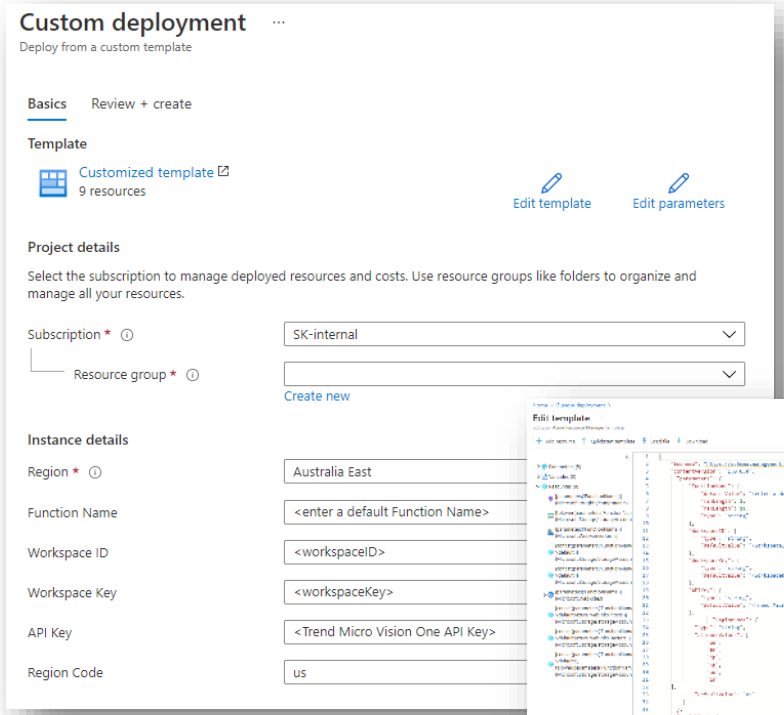
#2 Connect computers without internet access by using the Log Analytics gateway in Azure Monitor

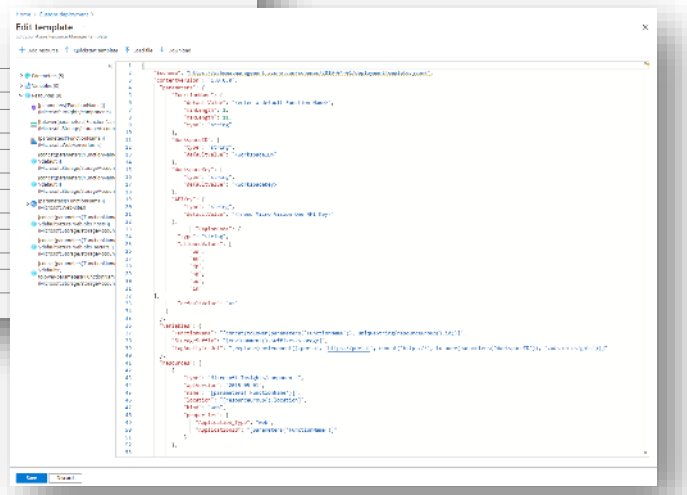


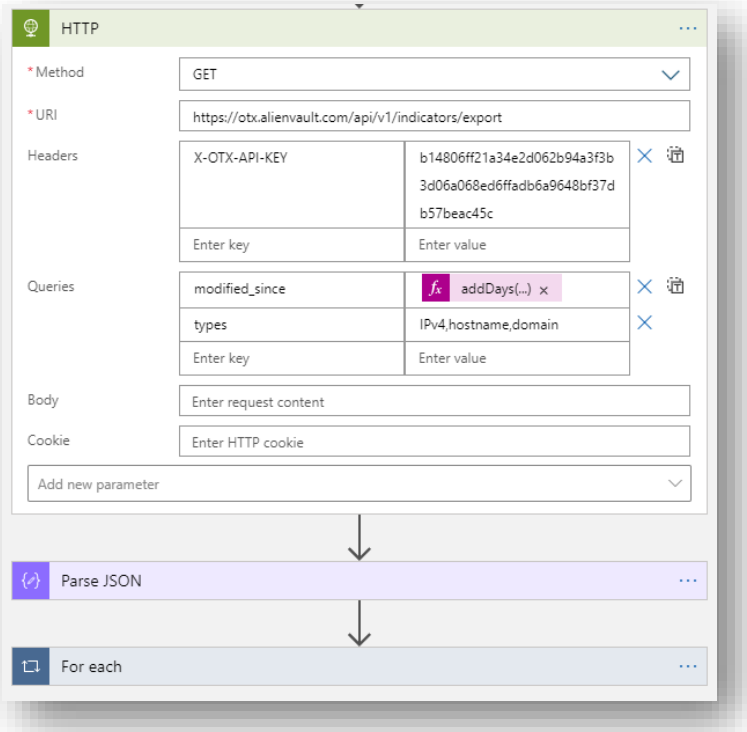
If your IT security policies do not allow computers on the network to connect to the Internet, you can set up a Log Analytics gateway and then configure the agent to connect through the gateway to Azure Monitor logs.

#3 API ingest – via Logic Apps / Azure Functions

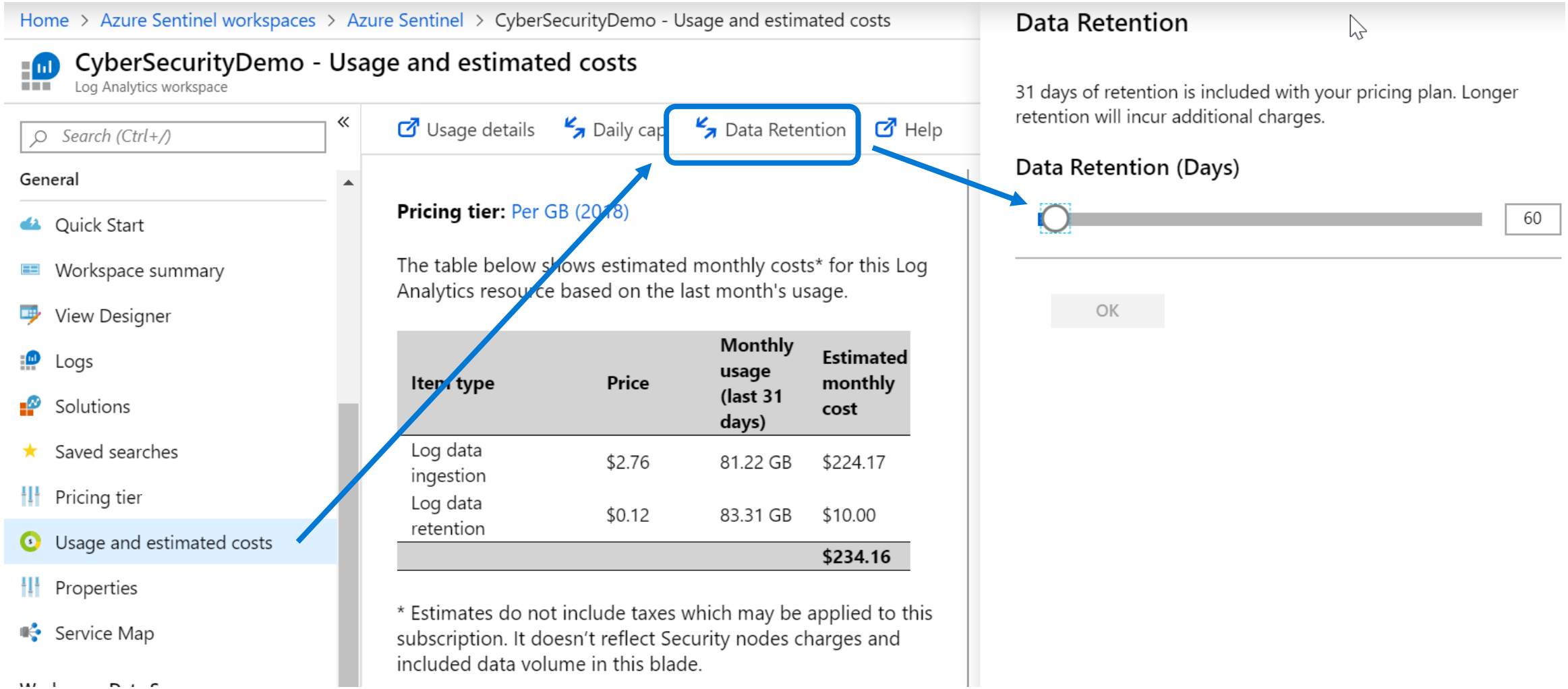
Functions	Logic Apps
Developer Productivity	Visual Designer
Triggers and Bindings	200+ Connectors
Flexible Deployment options	Functions Orchestration







Define data retention (workspace)



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:

Copy

```
/subscriptions/00000000-0000-0000-0000-00000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.OperationalInsi
```

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 Copy

```
GET /subscriptions/00000000-0000-0000-0000-00000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.Operati
```

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 Copy

```
GET /subscriptions/00000000-0000-0000-0000-00000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.Operati
```

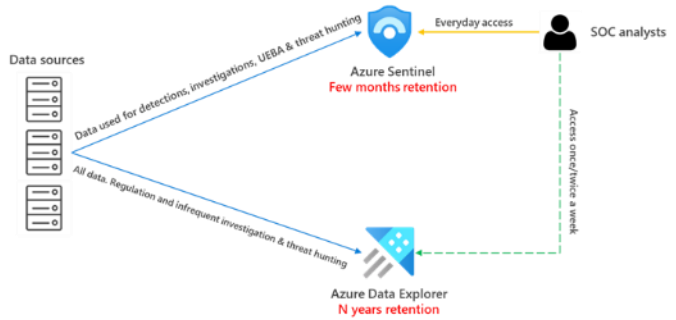
To set the retention of a particular data type (in this example SecurityEvent) to 730 days, do

JSON Copy

```
PUT /subscriptions/00000000-0000-0000-0000-00000000000/resourceGroups/MyResourceGroupName/providers/Microsoft.Operati
{
        "properties":
            {
                "retentionInDays": 730
    }
}
```

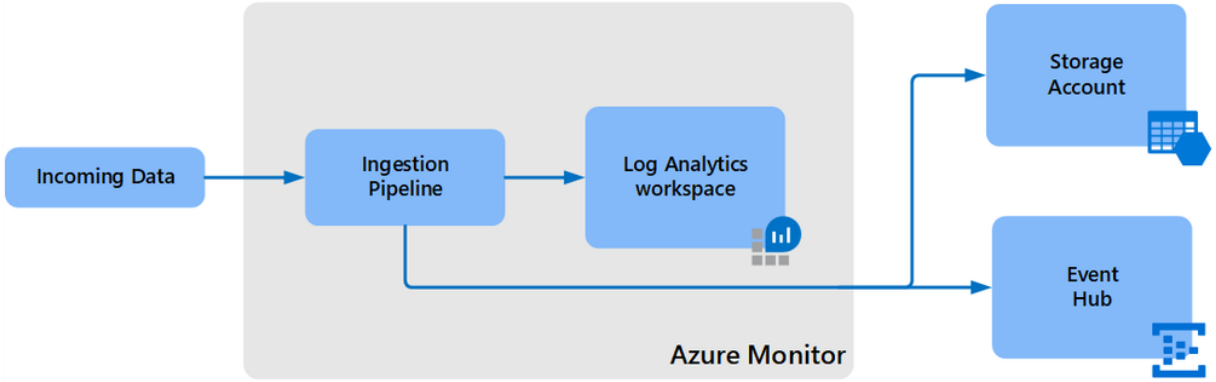
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-cost-storage#retention-by-data-type

Long Term Retention of Logs (Alternatives)

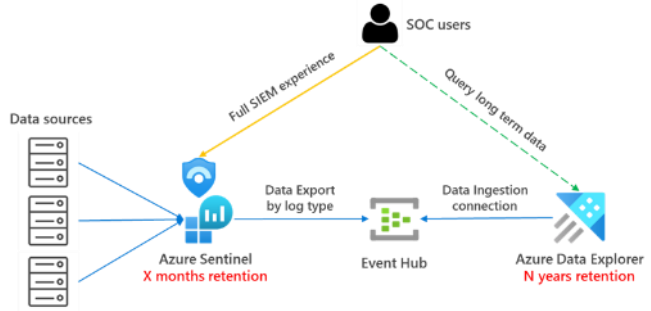


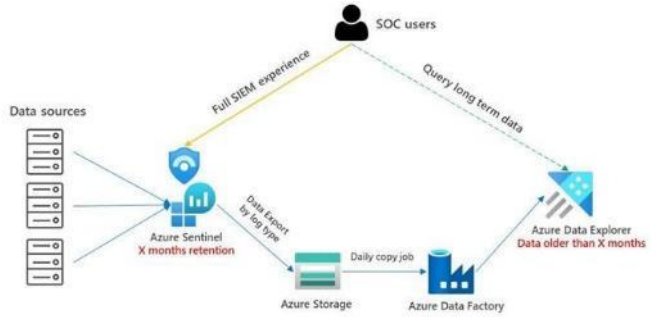
Log Analytics Data Export feature

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.





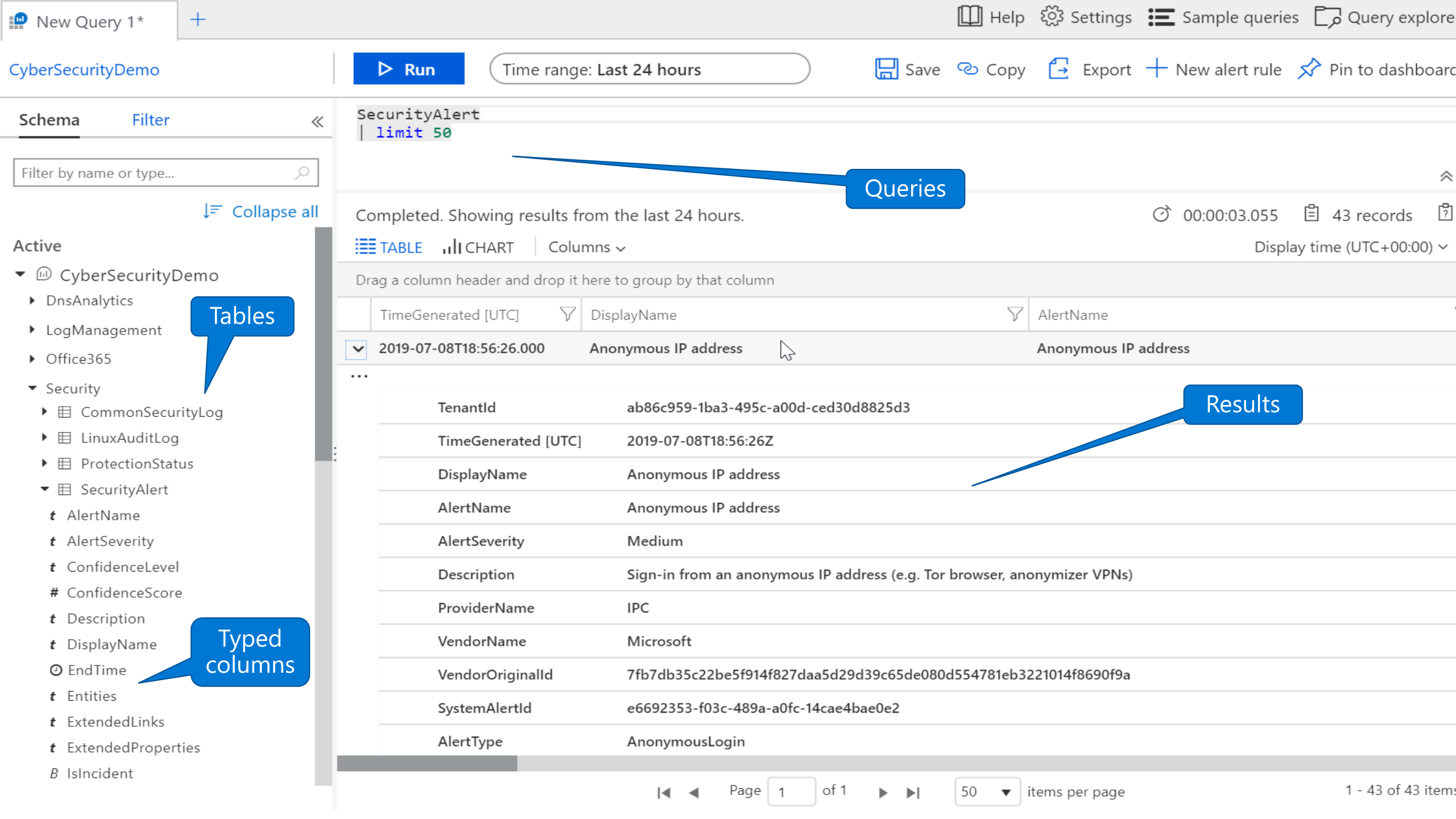
Using ADX for long term retention:
https://techcommunity.microsoft.com/t5/azure-sentinel/using-azure-data-explorer-for-long-term-retention-of-azure/ba-p/1883947

Microsoft Azure

Break – 5 minutes

Microsoft Azure

KQL Introduction


New Query 1*
Help
Settings
Sample queries
Query explore
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 columns
SecurityAlert
| limit 50
Queries
Completed. Showing results from the last 24 hours.
00:00:03.055
43 records
TABLE
CHART
Columns
Display time (UTC+00:00)
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
Results
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
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 | where Predicate*

Examples: *SecurityEvent | where TimeGenerated > ago(1d)*

*SecurityEvent | where * 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* | *limit* <*number*>
Example: *SecurityEvent* | *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* | *count*

Example: *SecurityEvent* | *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 | summarize Aggregation [by Group Expression]*
Examples: *SecurityEvent | summarize count() 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)

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 | extend ColumnName [= Expression] [, …]*
Example: *SecurityEvent | extend ComputerNameLength = strlen(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 | project ColumnName [= Expression] [, …]*
Example: *SecurityEvent | project 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* | *distinct Column1, Column2*

Example: *SecurityEvent* | *distinct 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)

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 “ContosoASCAlert\\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 “ContosoASCAlert\\LBecker”
SecurityEvent
| where EventID == 4624
| where Account == "ContosoASCAlert\\LBecker"
| summarize max(TimeGenerated)
```

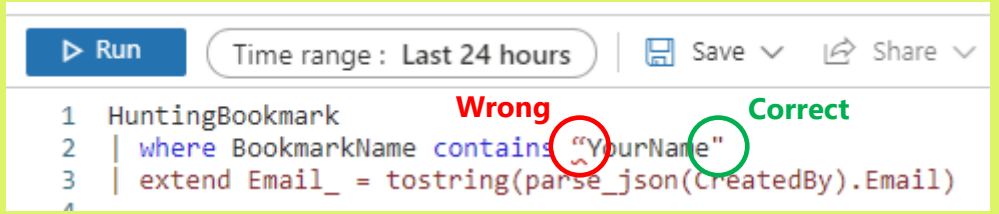
Microsoft Azure

Break – 10 minutes

Microsoft Azure

Externaldata Query / Watchlist

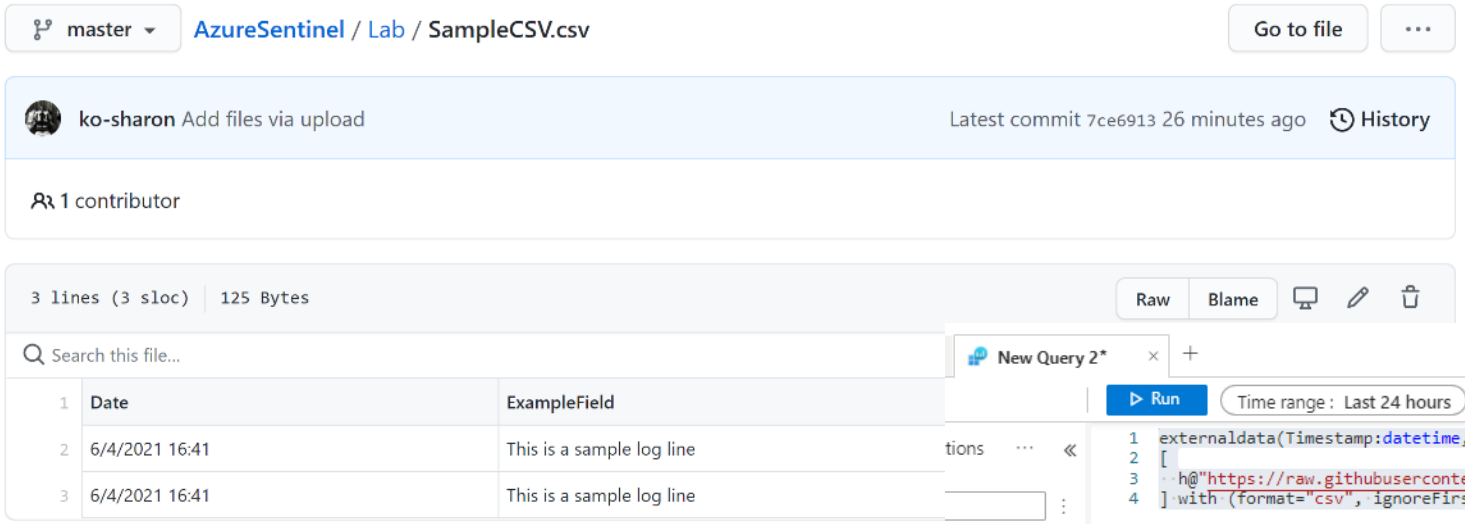
Note:
When copying and pasting please check that the "s are correct

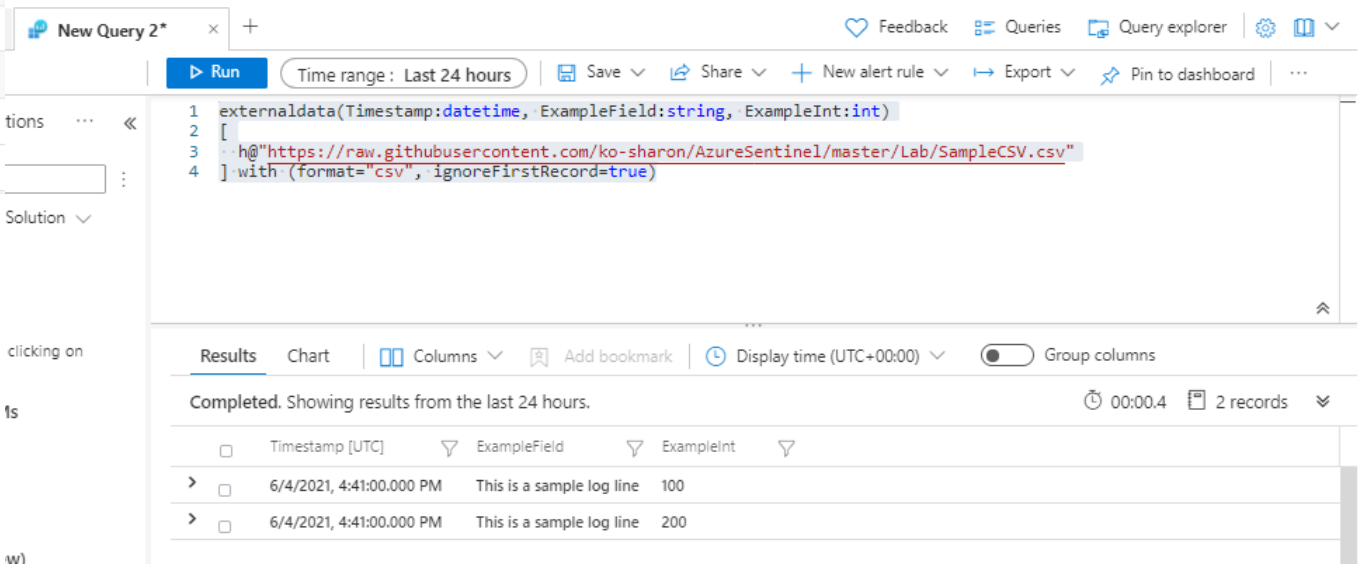


Lab: Externaldata() operator

Code:

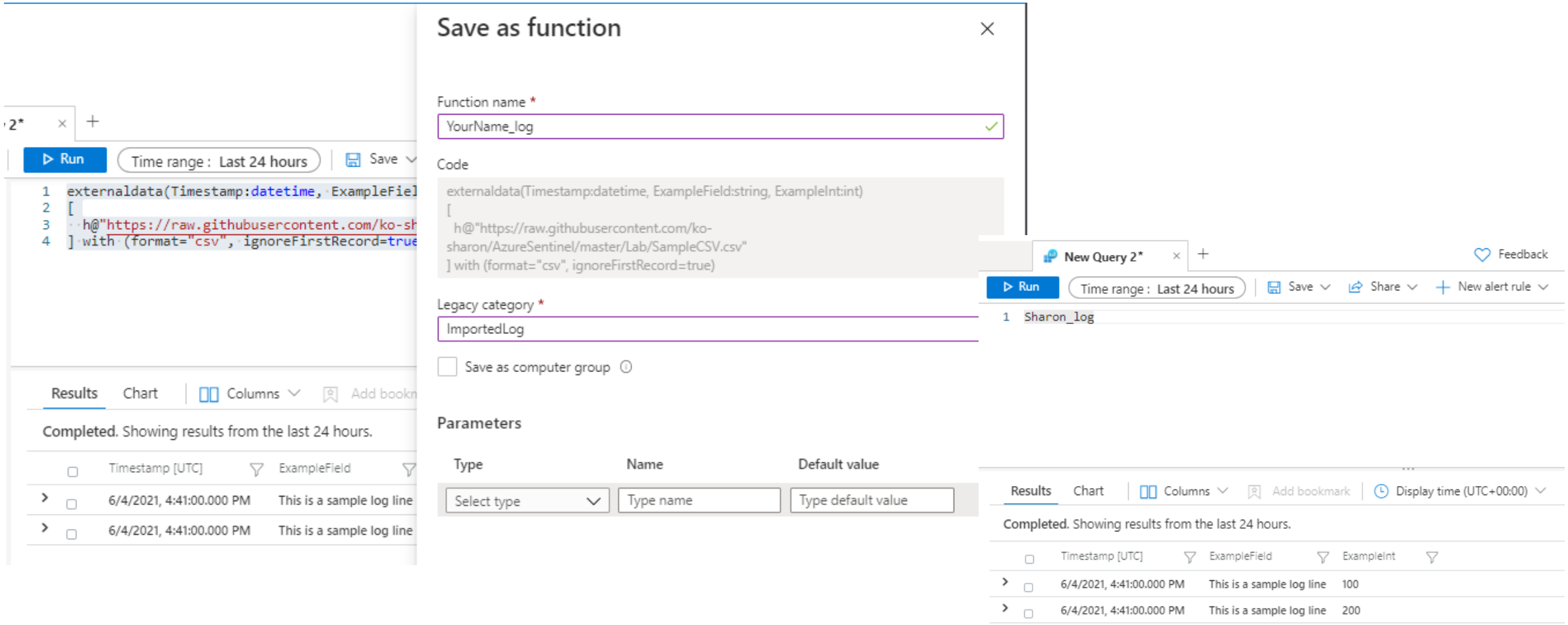
```
externaldata(Timestamp:datetime, ExampleField:string, ExampleInt:int) [h@"https://raw.githubusercontent.com/ko-sharon/AzureSentinel/master/Lab/SampleCSV.csv"] with (format="csv", ignoreFirstRecord=true)
```





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

Lab: Save as Function



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

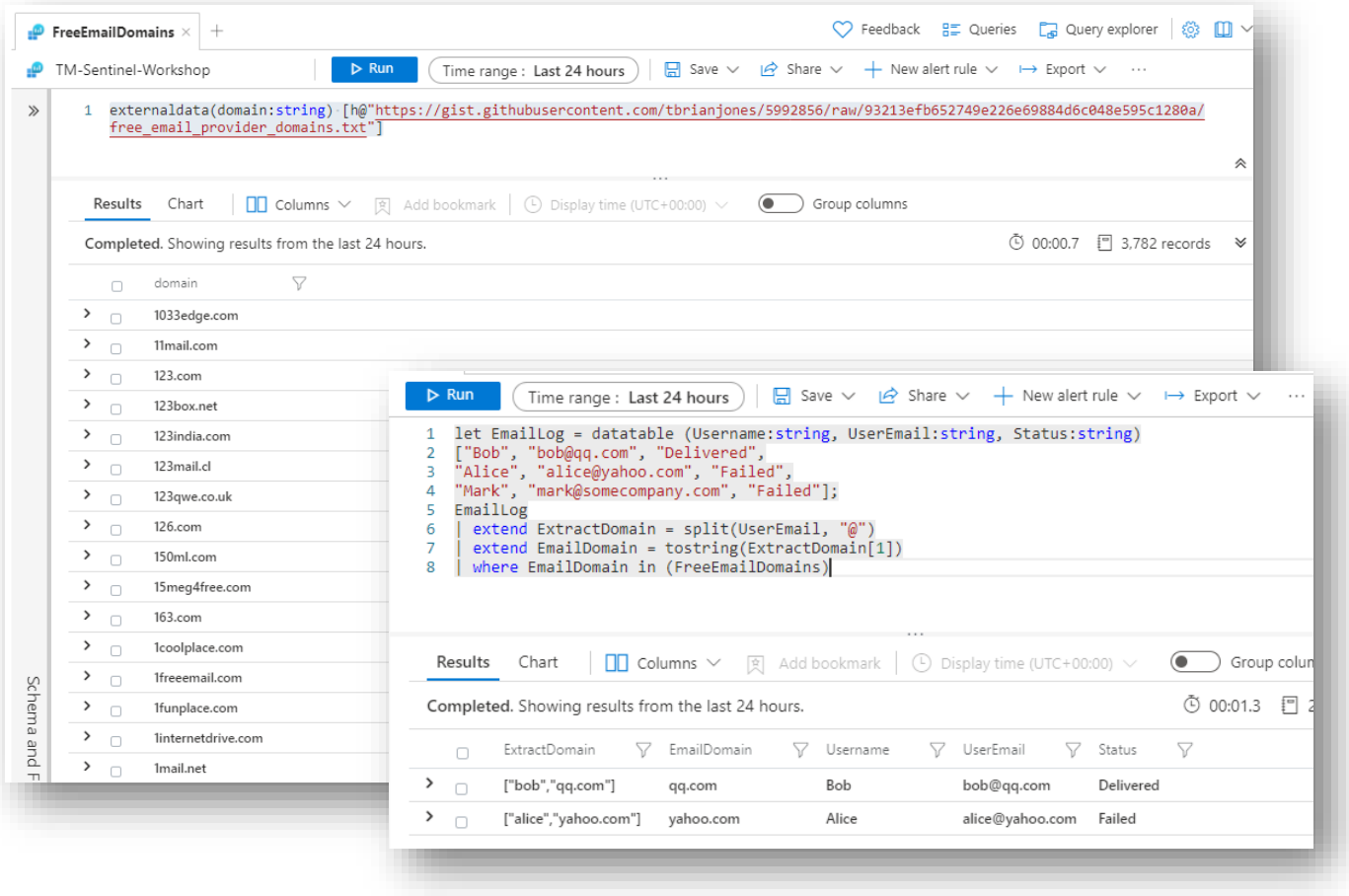
Demo: Externaldata() operator for Enrichment

Code:

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

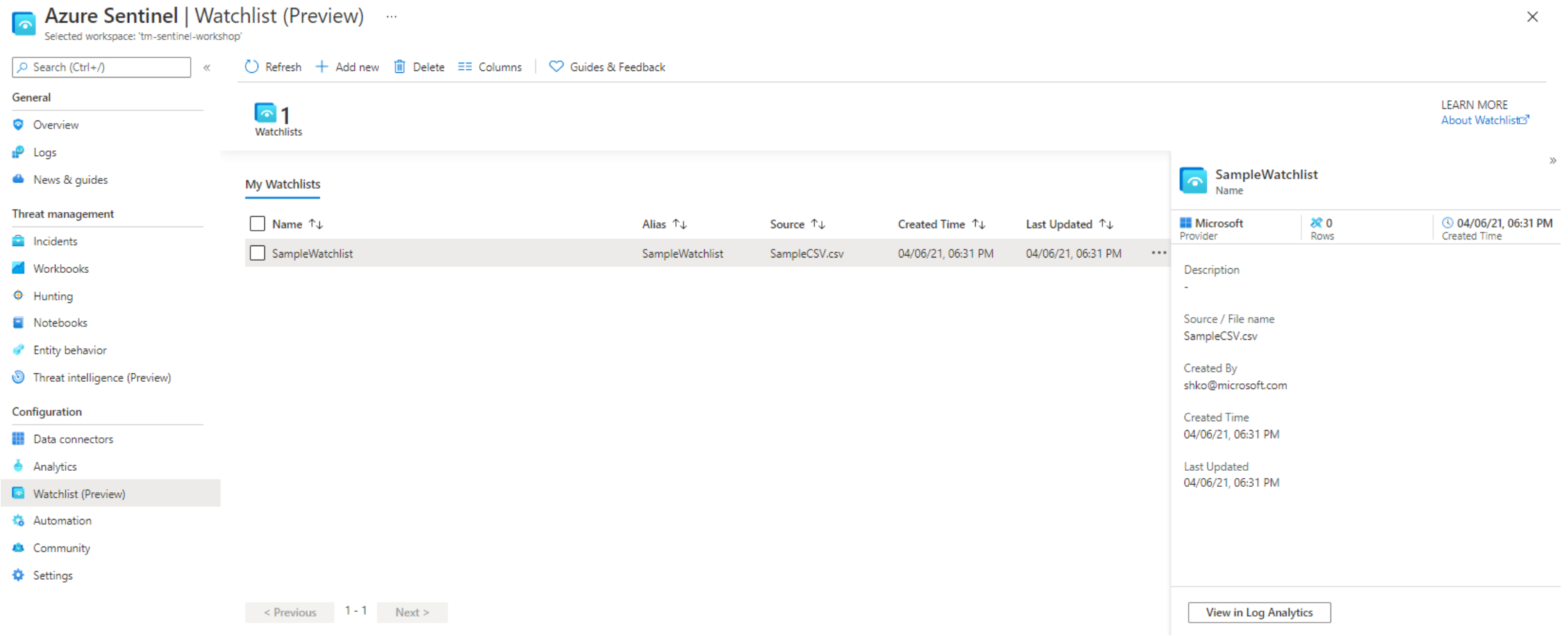
Code:

```
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)

Watchlist



_GetWatchlist('SampleWatchlist')

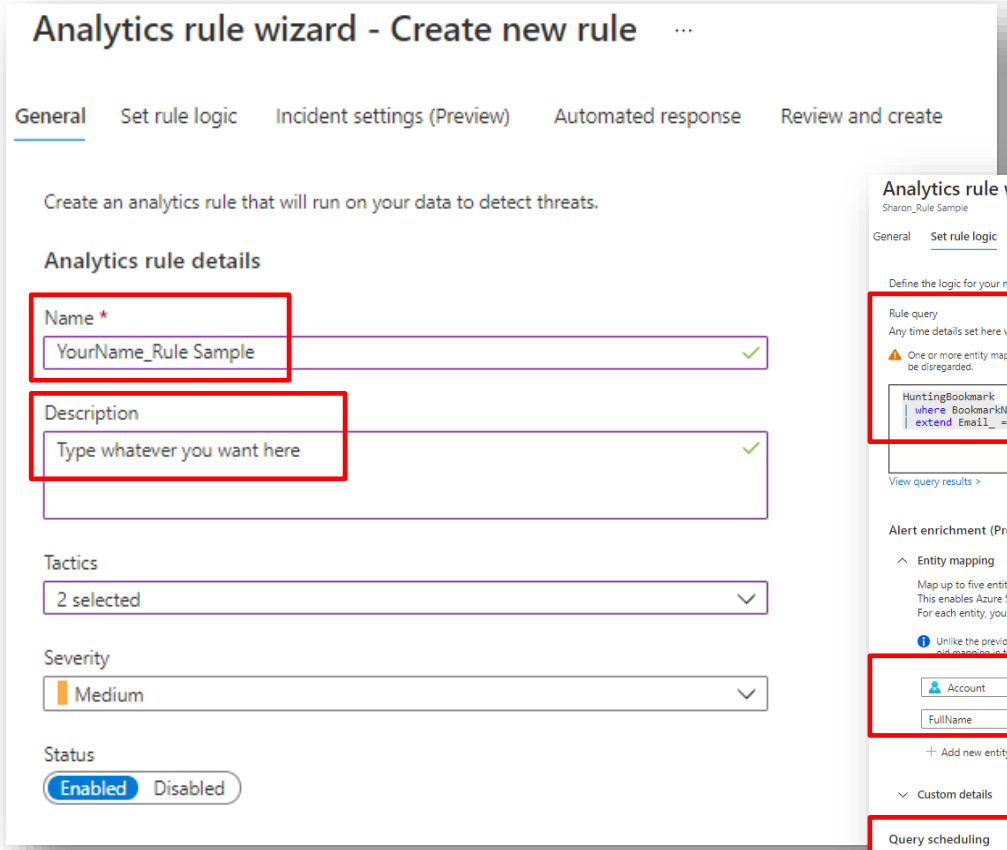
Microsoft Azure

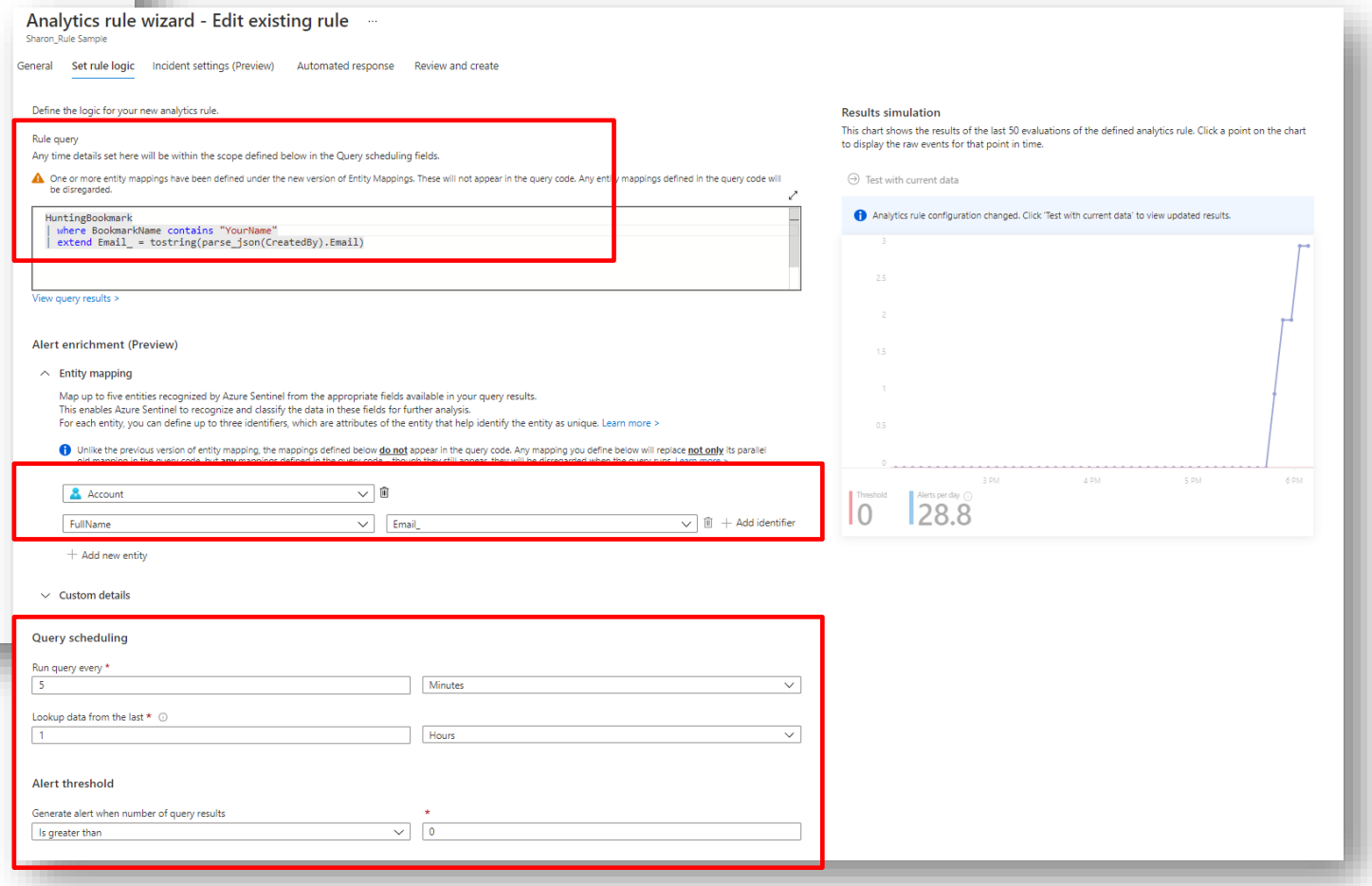
Analytics

Lab: Creating Scheduled Rule

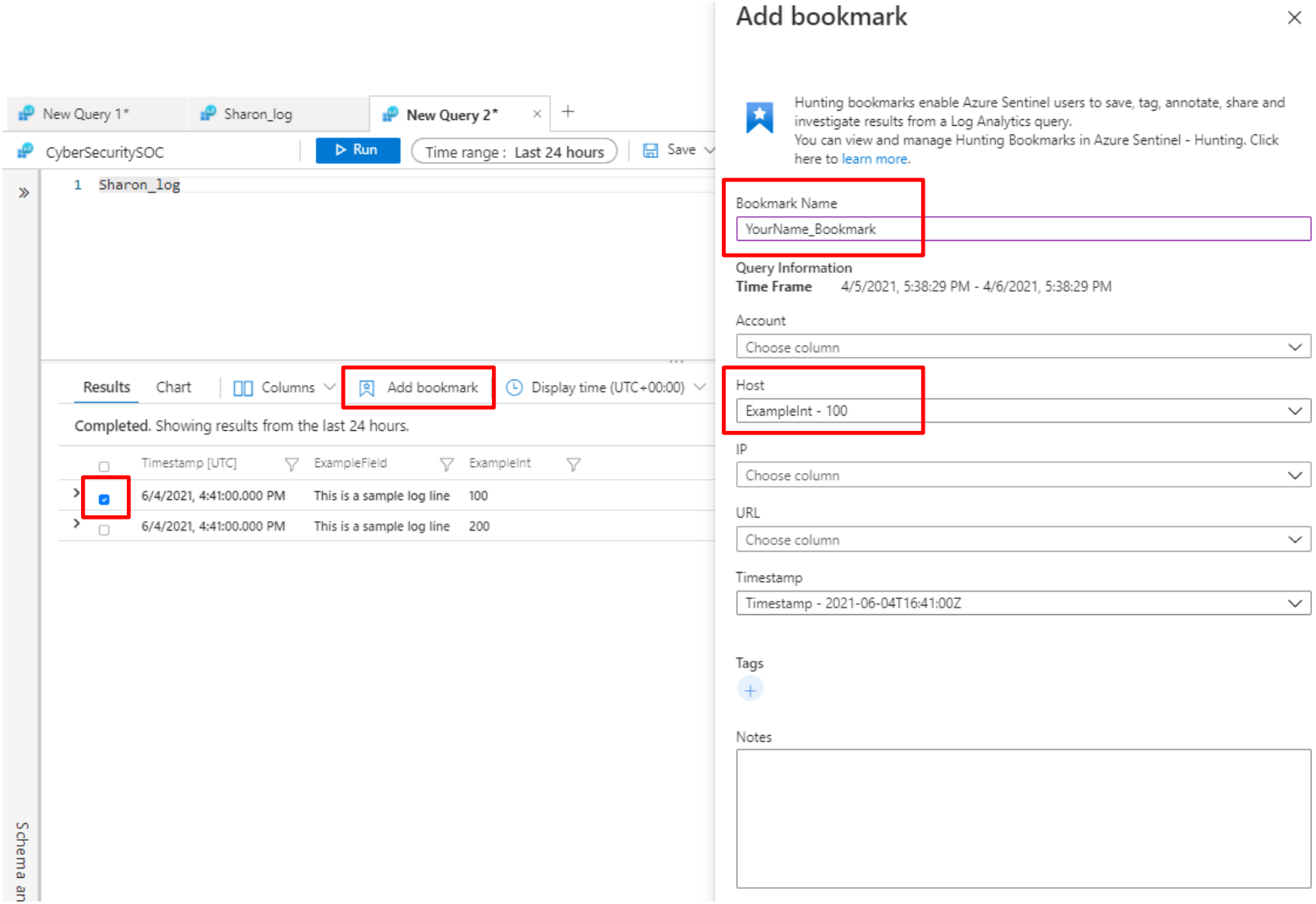
Code:

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





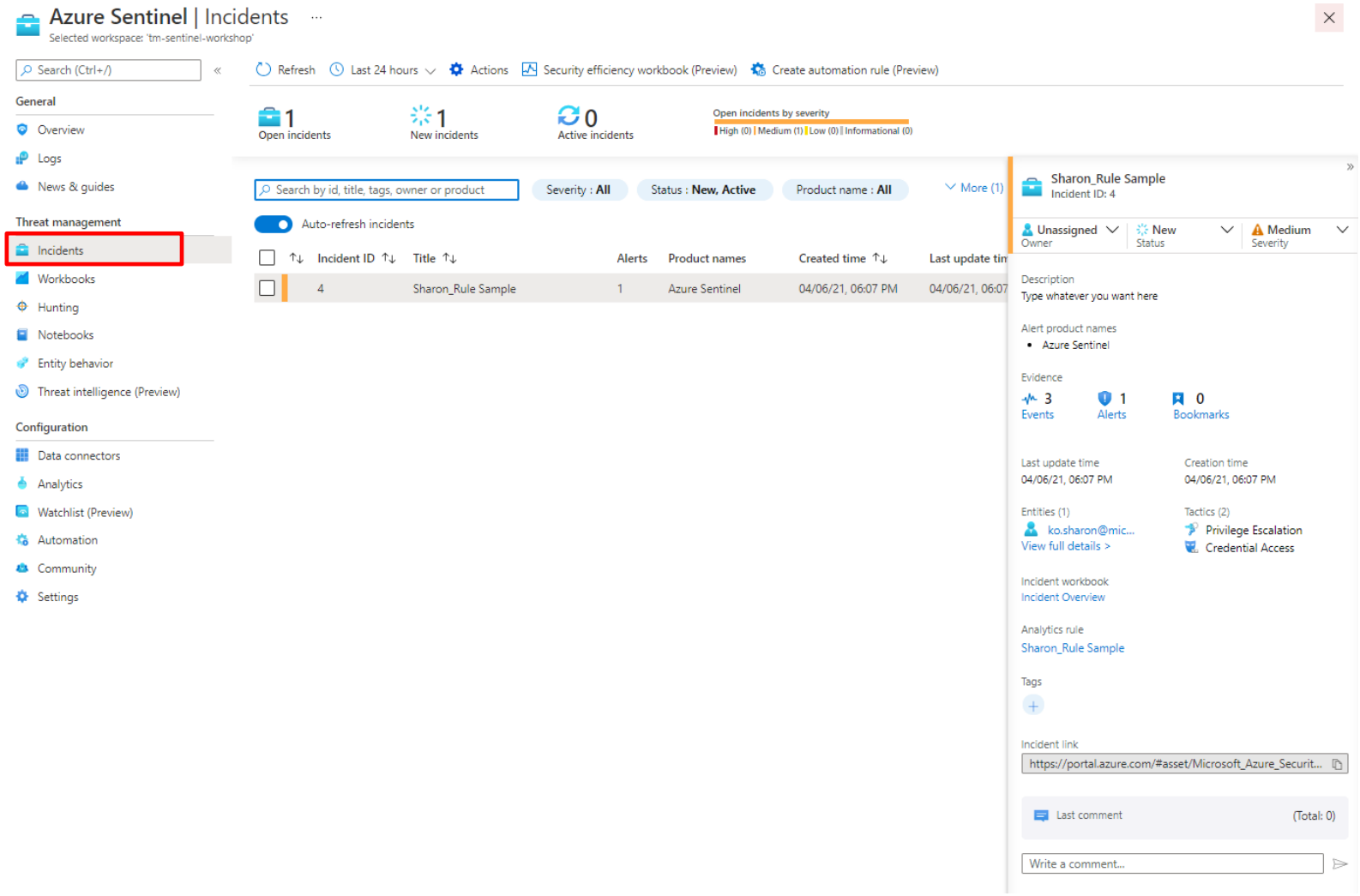
Lab: Triggering the Analytics Rule



Microsoft Azure

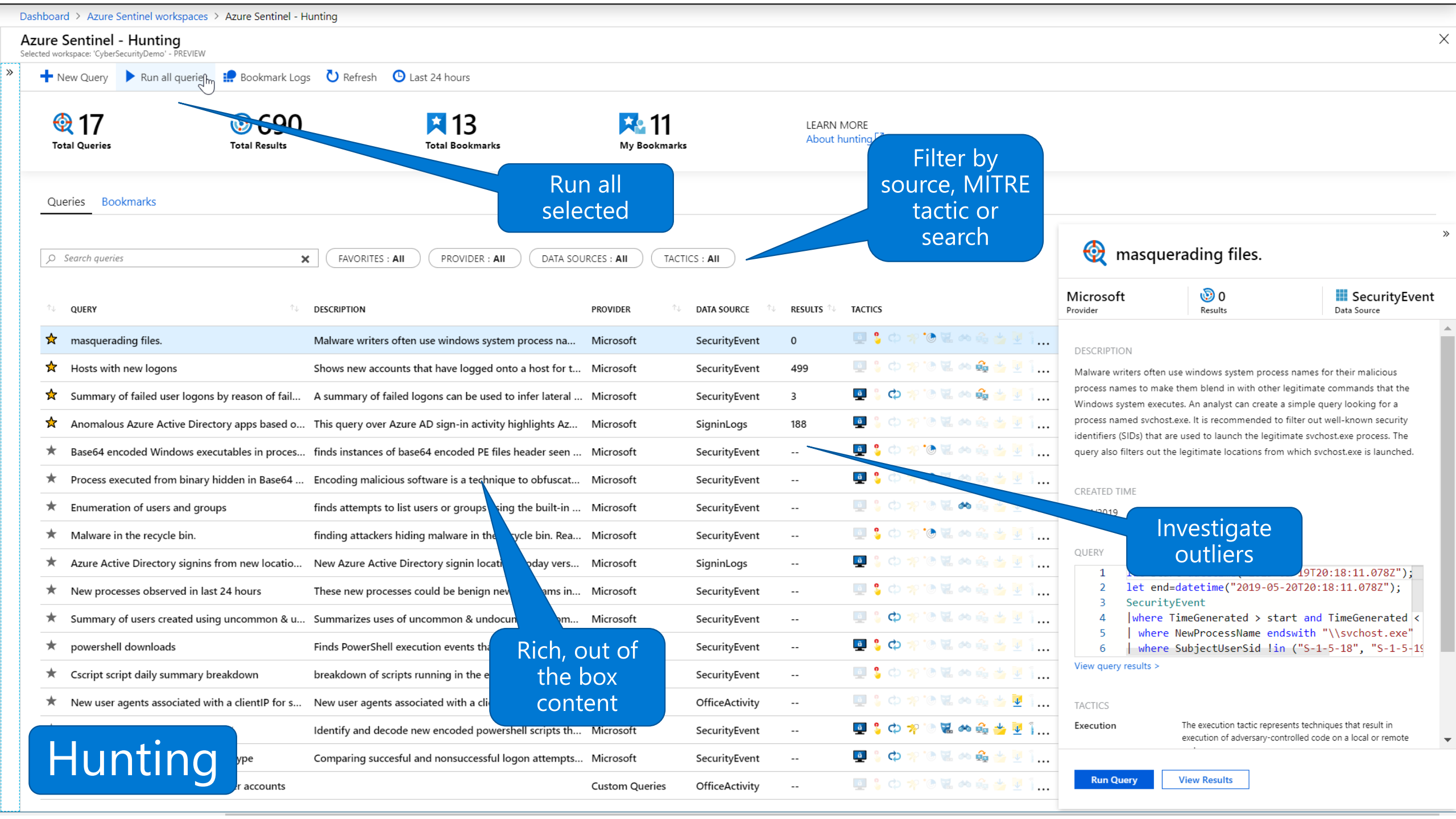
Break – 13 minutes

Lab: Investigating Incidents



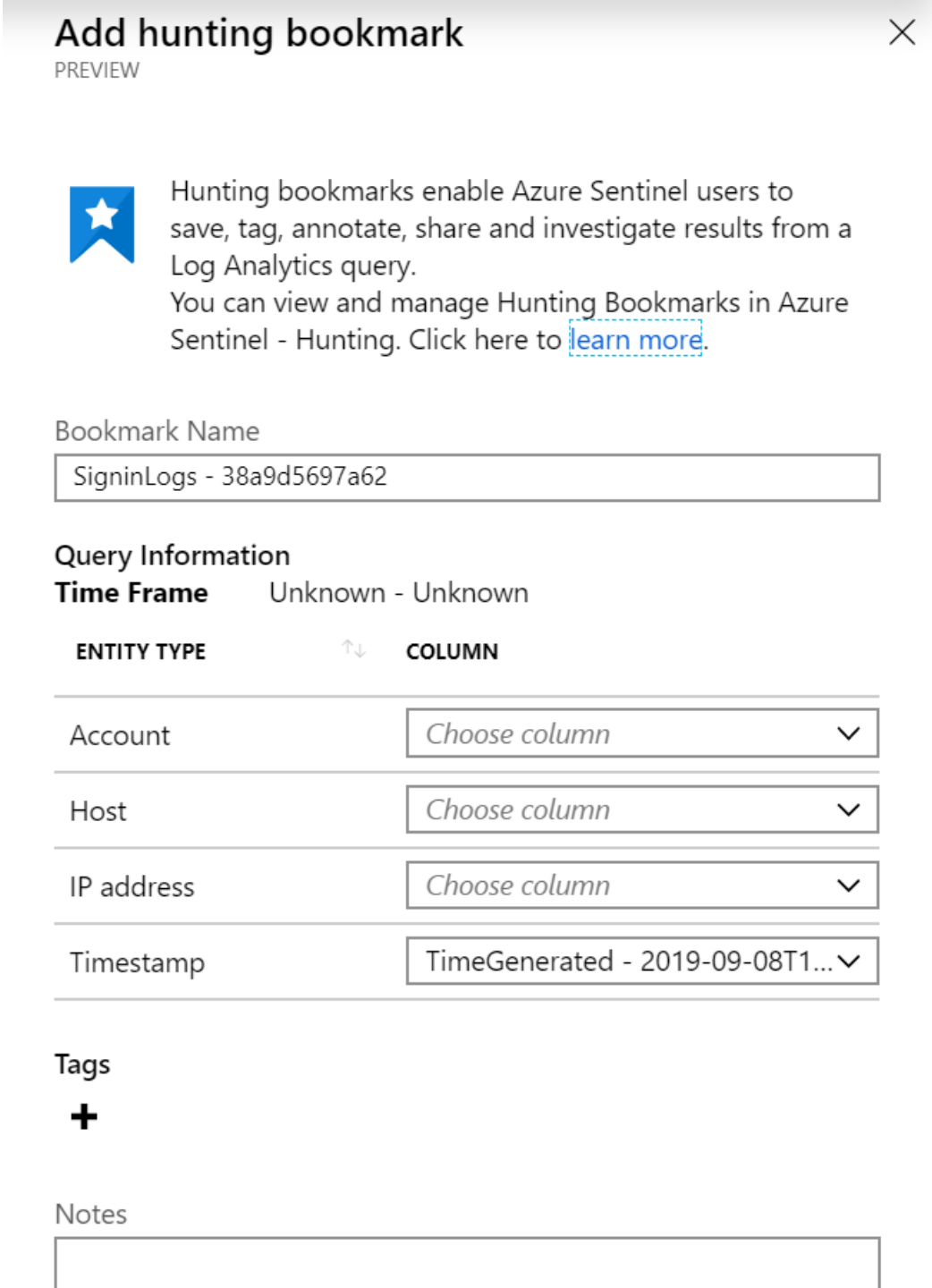
Microsoft Azure

Hunting

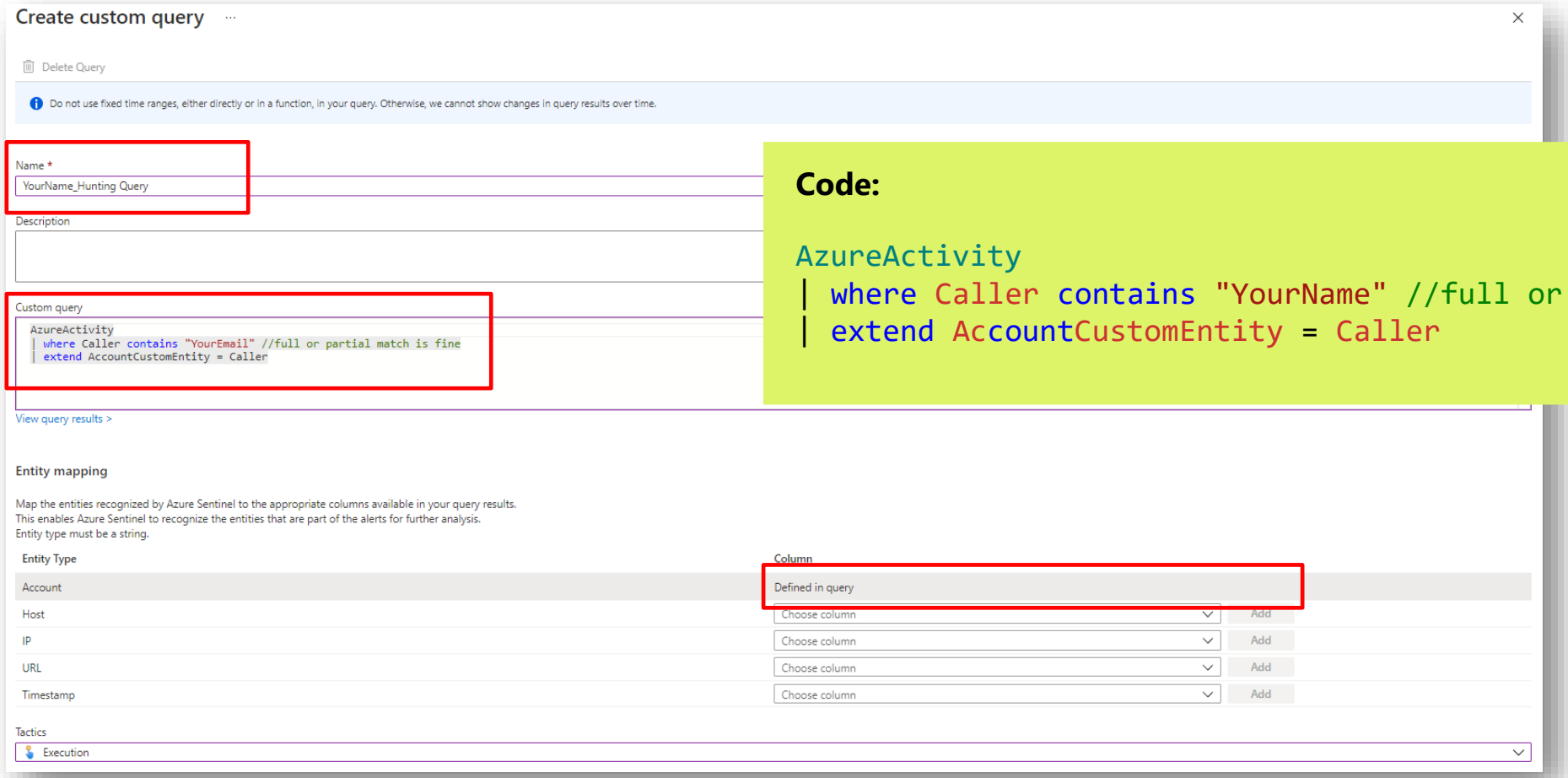

Dashboard > Azure Sentinel workspaces > Azure Sentinel - Hunting
Azure Sentinel - Hunting
Selected workspace: 'CyberSecurityDemo' - PREVIEW
New Query
Run all queries
Bookmark Logs
Refresh
Last 24 hours
17
Total Queries
690
Total Results
13
Total Bookmarks
11
My Bookmarks
LEARN MORE
About hunting
Run all selected
Filter by source, MITRE tactic or search
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 obfuscat...
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 locati
oday vers...
Microsoft
SigninLogs
--
New processes observed in last 24 hours
These new processes could be benign new
ams in...
Microsoft
SecurityEvent
--
Summary of users created using uncommon & u...
Summarizes uses of uncommon & undocum
m...
Microsoft
SecurityEvent
--
powershell downloads
Finds PowerShell execution events tha
SecurityEvent
--
Cscript script daily summary breakdown
breakdown of scripts running in the e
SecurityEvent
--
New user agents associated with a clientIP for s...
New user agents associated with a cli
OfficeActivity
--
Identify and decode new encoded powershell scripts th...
Microsoft
SecurityEvent
--
ype
Comparing succesful and nonsuccessful logon attempts...
Microsoft
SecurityEvent
--
r accounts
Custom Queries
OfficeActivity
--
Rich, out of the box content
Investigate outliers
Hunting
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
QUERY
let end=datetime("2019-05-20T20:18:11.078Z");
SecurityEvent
|where TimeGenerated > start and TimeGenerated <
| where NewProcessName endswith "\\svchost.exe"
| 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

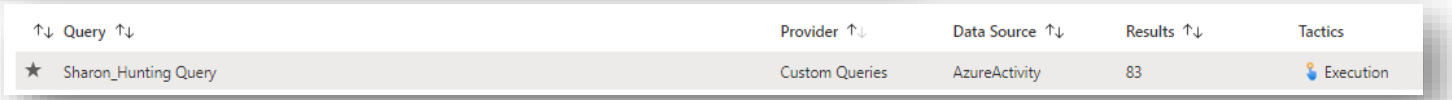


Lab: Create a Hunting Query

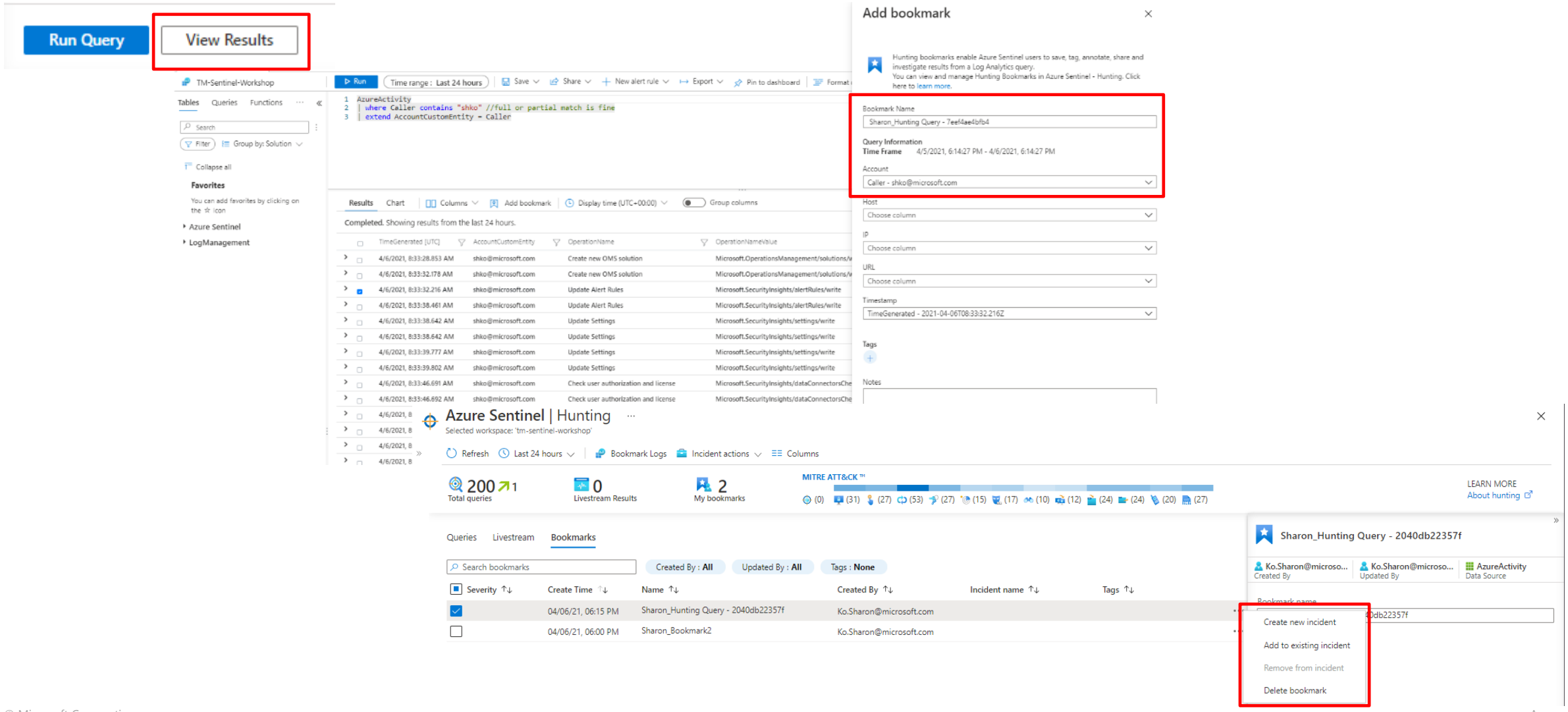


Code:

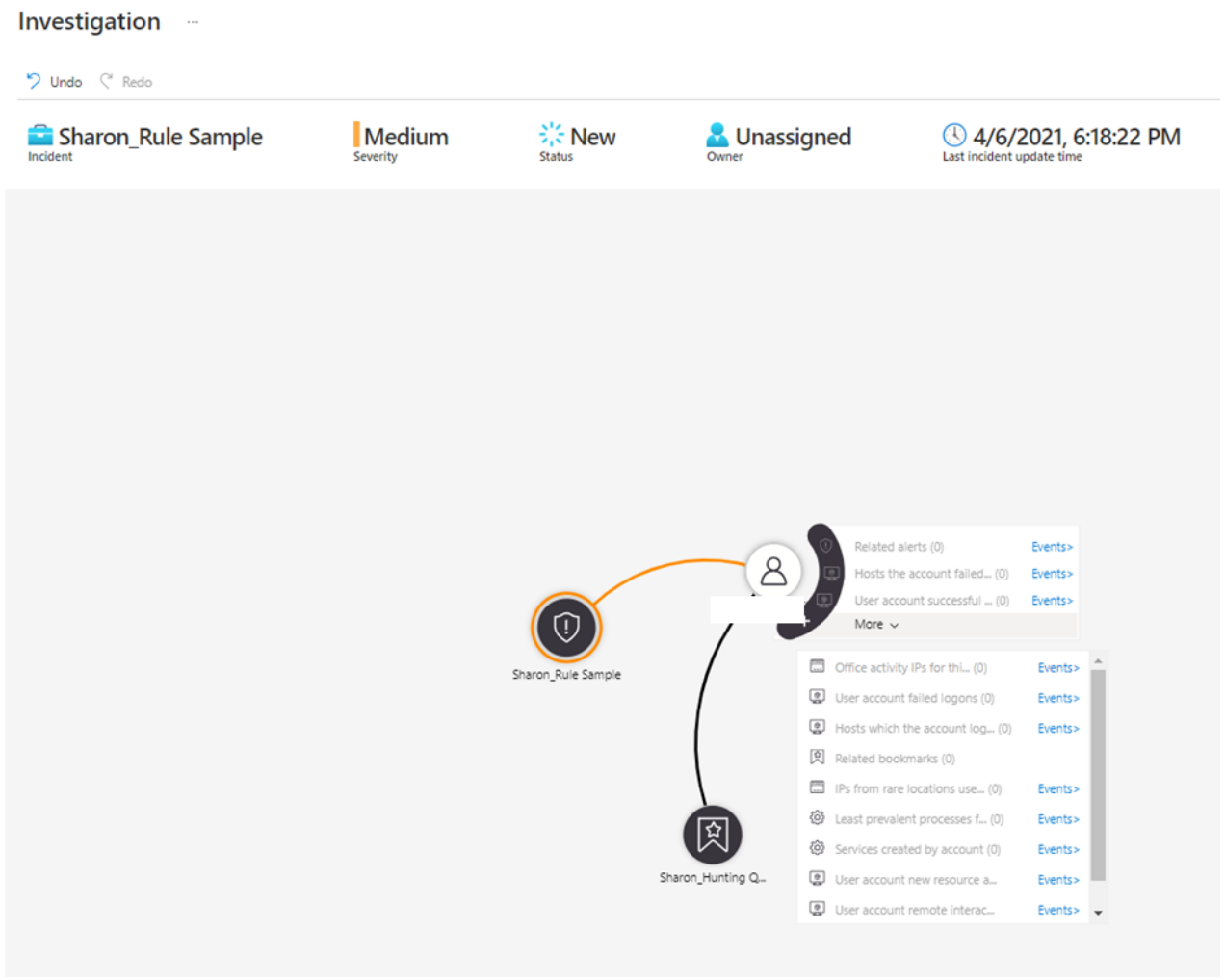
```
AzureActivity
| where Caller contains "YourName" //full or partial match is fine
| extend AccountCustomEntity = Caller
```



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



Lab: Investigating Incidents

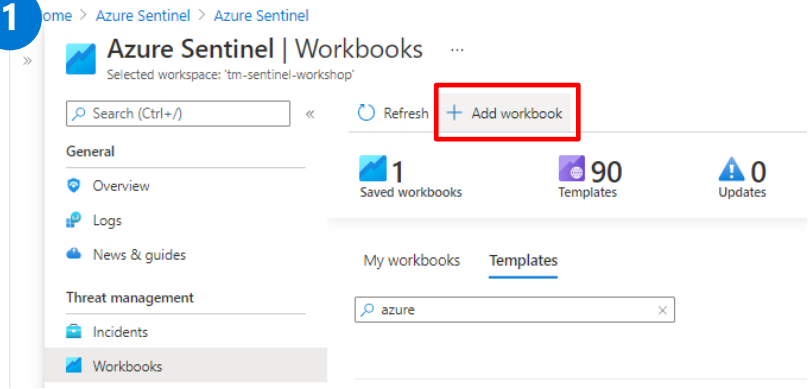


Microsoft Azure

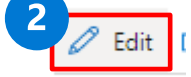
Workbooks

Lab: Add and Save a Workbook

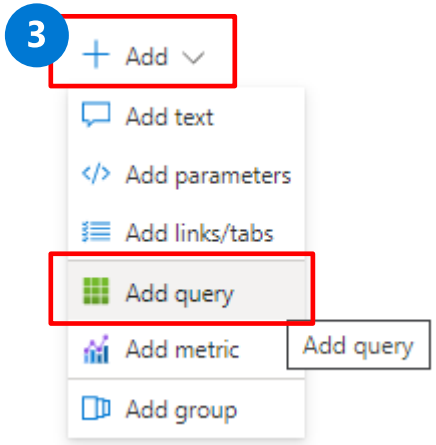
1



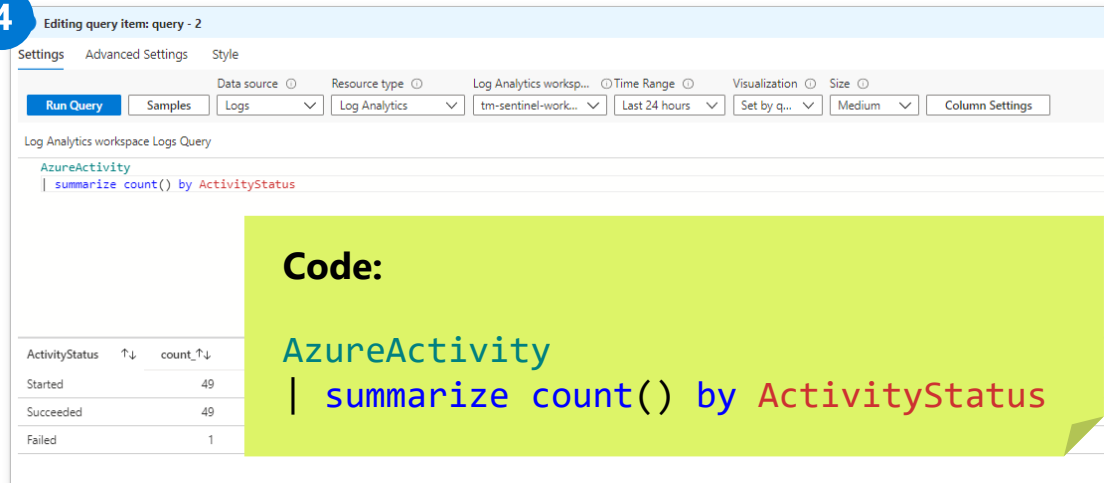
2



3



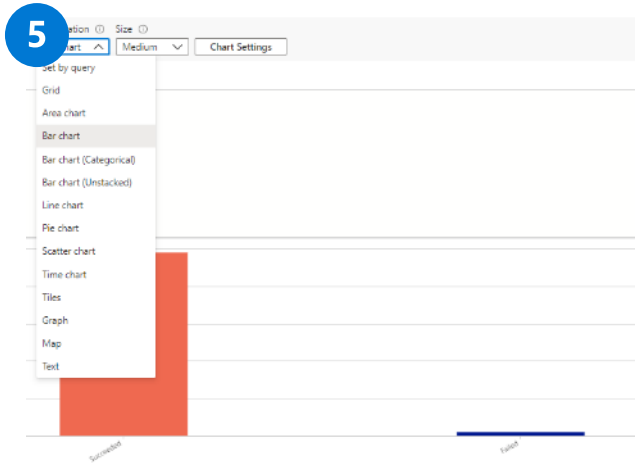
4



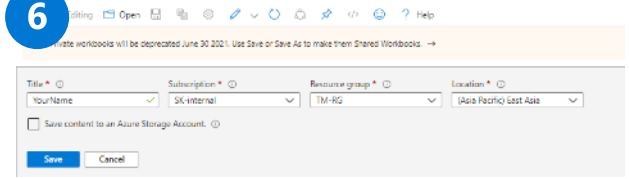
Code:

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

5



6

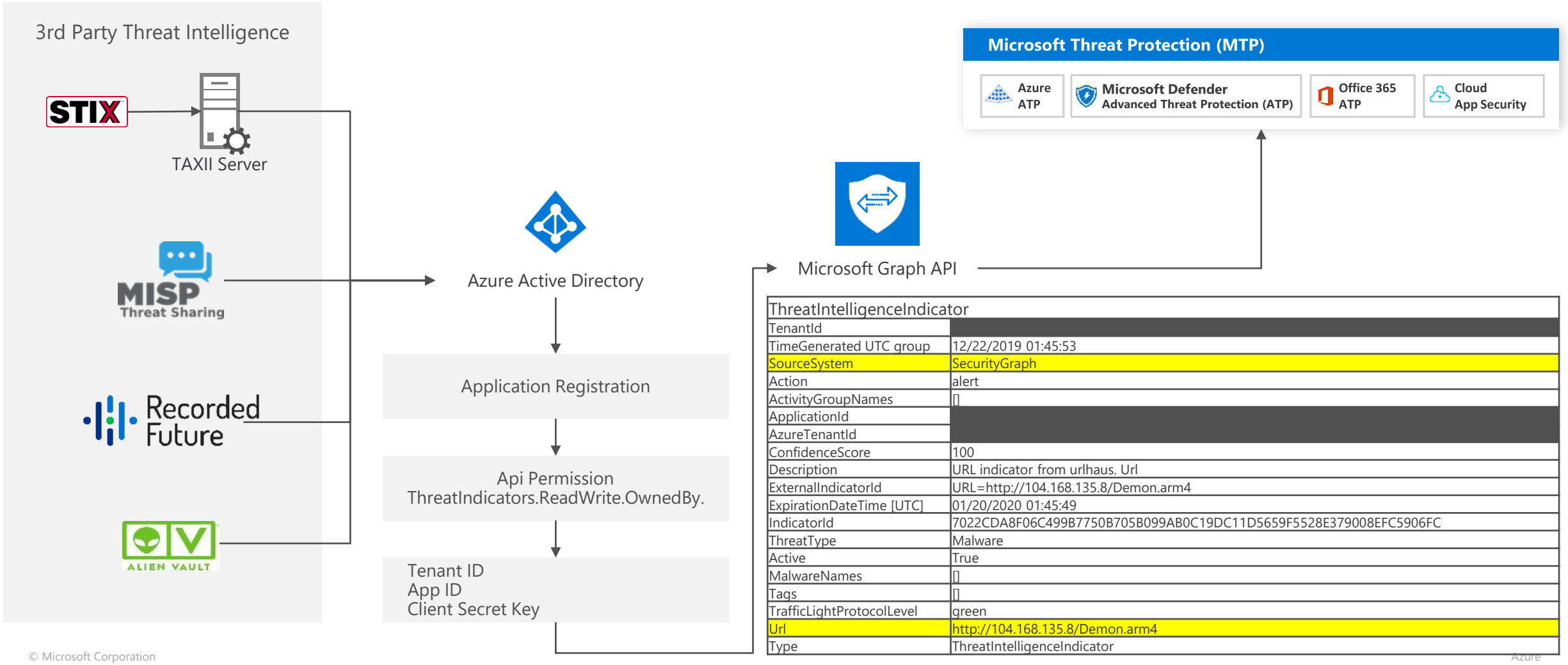


Microsoft Azure

Threat Intelligence

External Threat Intelligence Enrichment

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



ThreatIntelligenceIndicator	
TenantId	[redacted]
TimeGenerated UTC group	12/22/2019 01:45:53
SourceSystem	SecurityGraph
Action	alert
ActivityGroupNames	[]
ApplicationId	[redacted]
AzureTenantId	[redacted]
ConfidenceScore	100
Description	URL indicator from urlhaus. Url
ExternalIndicatorId	URL=http://104.168.135.8/Demon.arm4
ExpirationDateTime [UTC]	01/20/2020 01:45:49
IndicatorId	7022CDA8F06C499B7750B705B099AB0C19DC11D5659F5528E379008EFC5906FC
ThreatType	Malware
Active	True
MalwareNames	[]
Tags	[]
TrafficLightProtocolLevel	green
Url	http://104.168.135.8/Demon.arm4
Type	ThreatIntelligenceIndicator

Azure Sentinel | Threat intelligence (Preview)

Selected workspace: 'cybersecuritysoc'

ThreatIntelligence:SaveAndCloseBlade 11:42 AM
Indicator saved

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

Name	Values	Types	Source	Confidence	Alerts	Tags	Threat Type	Created
Malicious URL	http://www.badurl.com	url	Azure Sentinel	80	0		malicious-activity	Fri Aug 14 2
Custom Threat Intellig...	F688F50D695F8D00AE...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	2CFE8ADA24FE875B4F...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	05C9B086778BA1DC3...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	6441682094420E1677...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	5392AD13A9DA47D12...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	AFFFE16995DEEA180A...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	56611DF4A4F91A0596...	file	SecurityGraph	100	0		Malware	Thu Aug 13
Custom Threat Intellig...	956D28C0F7567973D...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	D10BFAC7CC64FE82FB...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	6A8B18C3FE5B742F77...	file	SecurityGraph	100	0		Malware	Thu Aug 13
Custom Threat Intellig...	688A17478DDE70A31...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	A66A3B2E9F83141937...	file	SecurityGraph	100	0		Phishing	Thu Aug 13
Custom Threat Intellig...	48E0AF0073249940C1...	file	SecurityGraph	100	0		Malware	Thu Aug 13
Custom Threat Intellig...	EE176315191D8EE831...	file	SecurityGraph	100	0		Malware	Thu Aug 13

< Previous | 1 - 100 | Next >

Malicious URL

80 Confidence | 0 Alerts | url Types

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

Azure Sentinel | Analytics

Selected workspace: 'sk-wfh'

Search (Ctrl+/)

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

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

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**

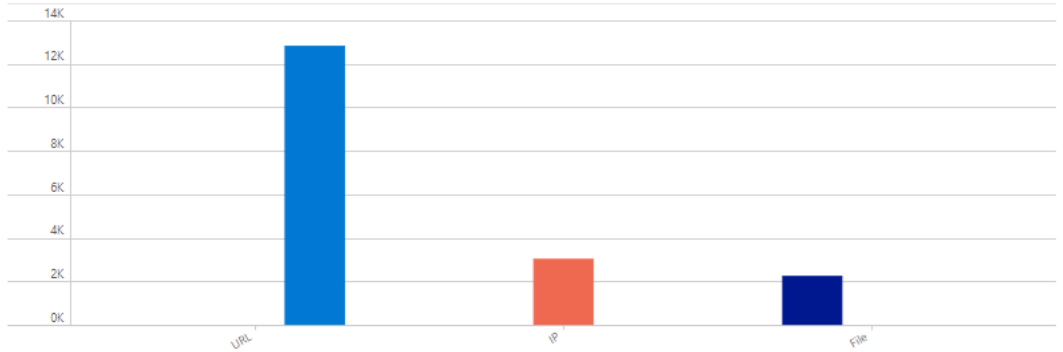
SEVERITY	NAME	RULE TYPE	DATA SOURCES	TACTICS
Medium	TI map IP entity to GitHub_CL	Scheduled	Threat Intelligence Platforms (Preview) +1	Impact
Medium	(Preview) TI map IP entity to DnsEvents	Scheduled	Threat Intelligence Platforms (Preview) +2	Impact
Medium	(Preview) TI map IP entity to OfficeActivity	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 W3CIISLog	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

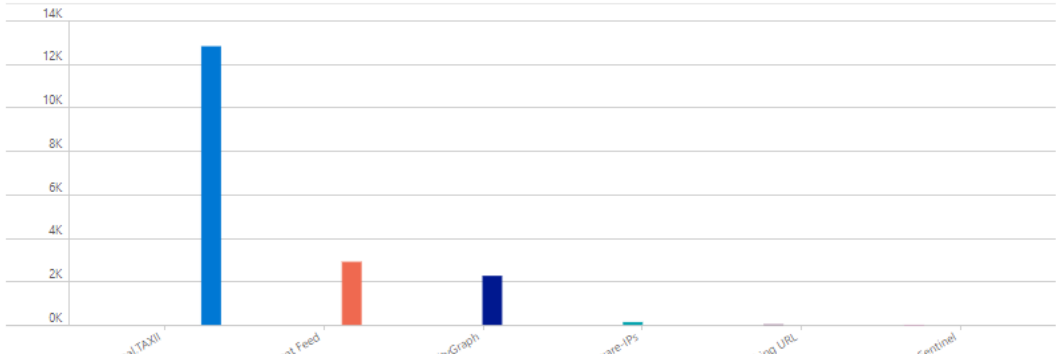
Edit | Open | Help | Auto refresh: Off

Active indicators by indicator type



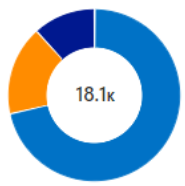
URL 12.8K | IP 3.04K | File 2.25K

Active indicators by indicator source



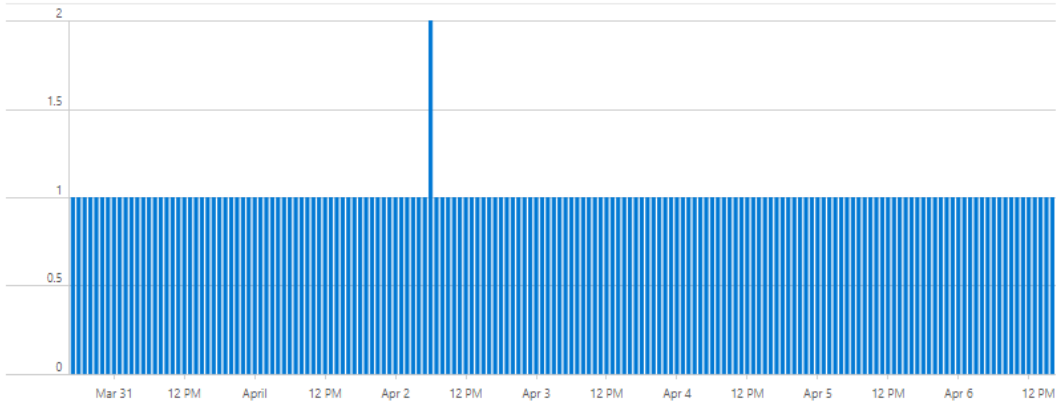
TAXII-External.TAXII 12.8K | Microsoft Emerging Threa... 2.91K | SecurityGraph 2.25K | TAXII-Anomali-Abuse-Ra... 134 | Bing Safety Phishing URL 18 | Azure Sentinel 7

Active indicators by confidence score



12.9K
100.0 3.04K
75.0 2.13K
Other 3
0.0 1
33.0 1

Alerts generated from threat intelligence by alert severity and date



Medium (Sum) 169

Alert counts by indicator

Value	ThreatType	Description	Source	Ale
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

Microsoft Azure

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

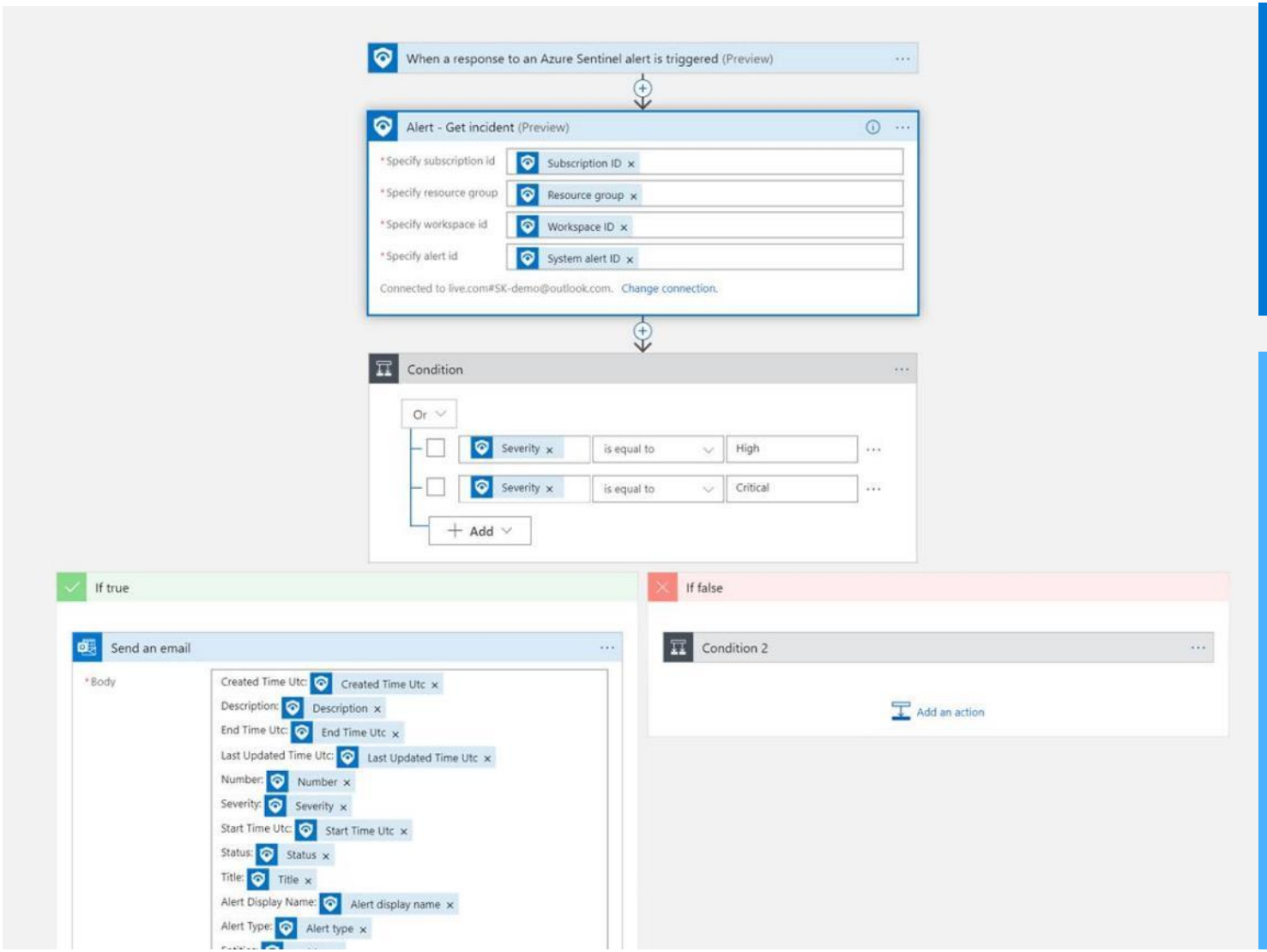
Enrichment

(trigger: scheduled)

Examples:

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

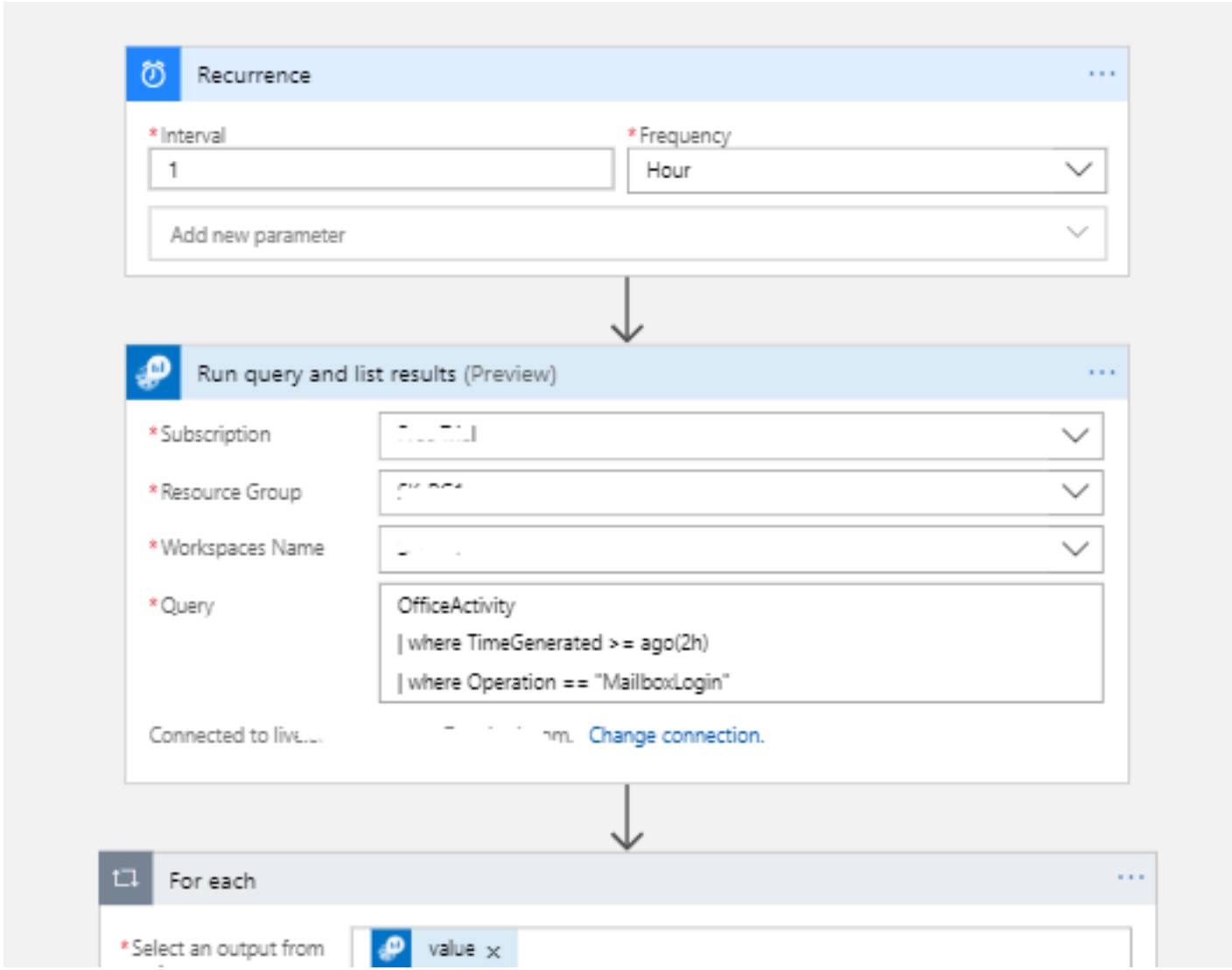
Example (Response)



Trigger

Logical Workflow

Example (Enrichment)

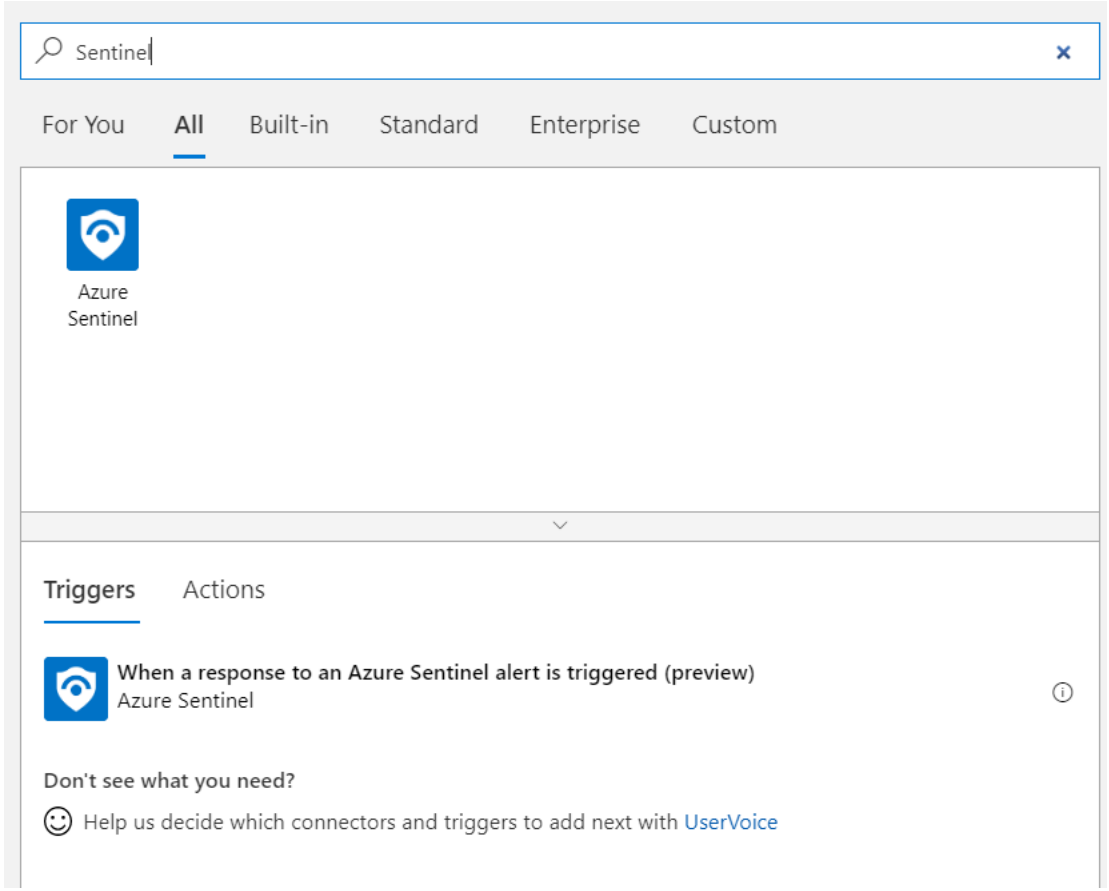


Trigger

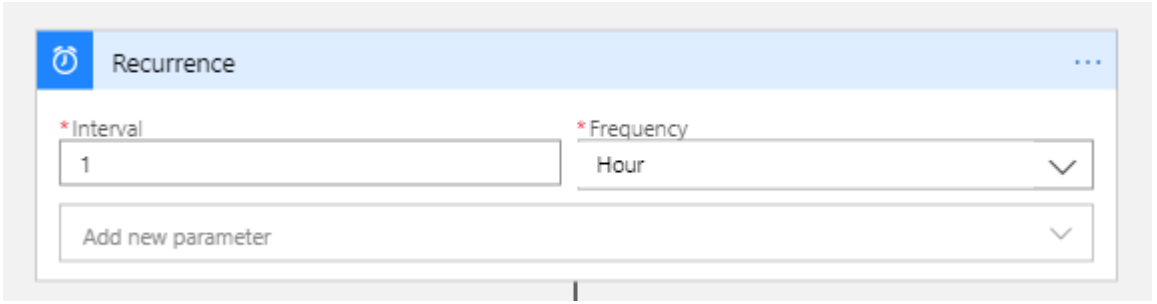
Logical Workflow

Trigger

Response



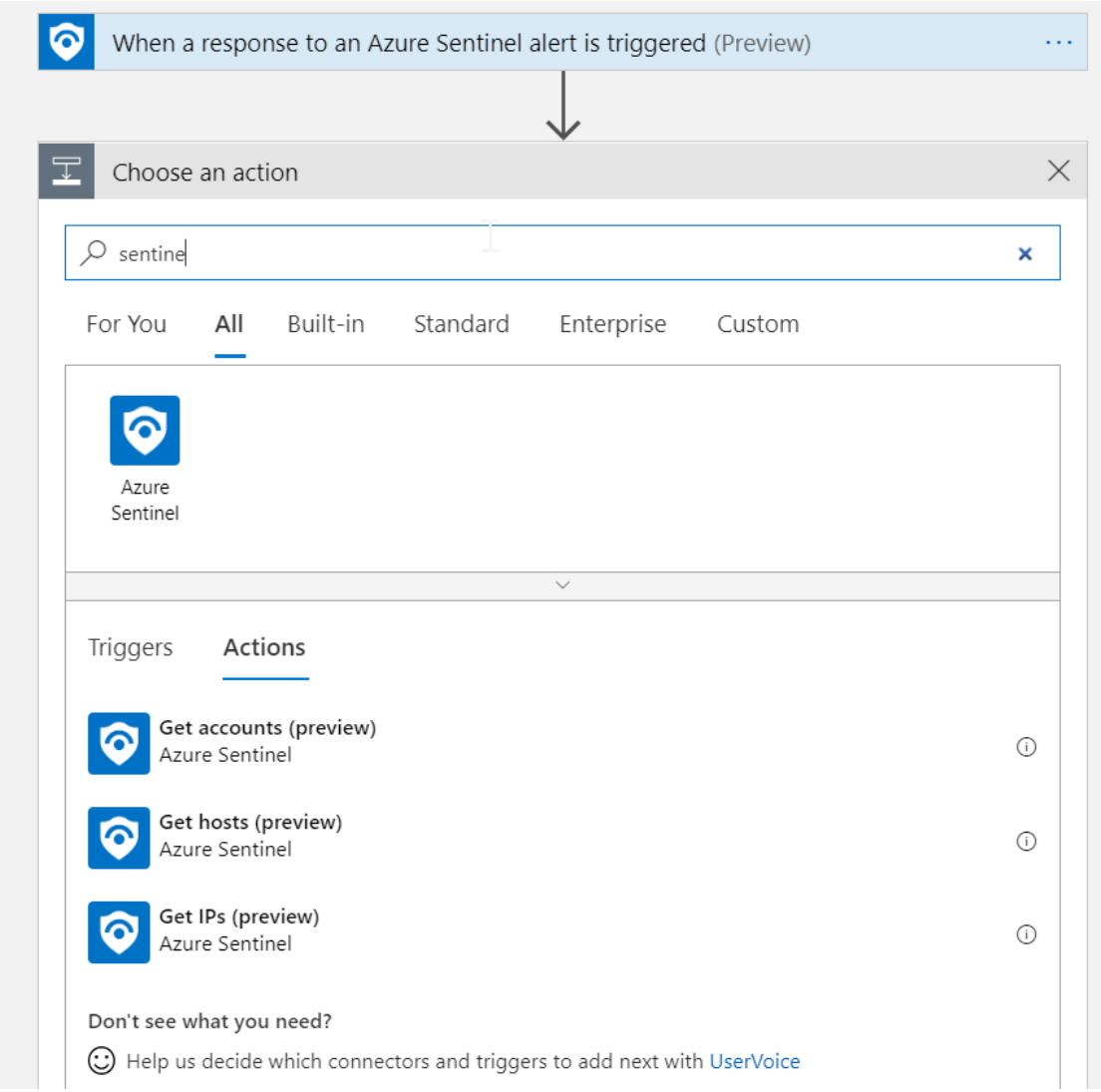
Recurrence



Common Workflow Modules

Sentinel

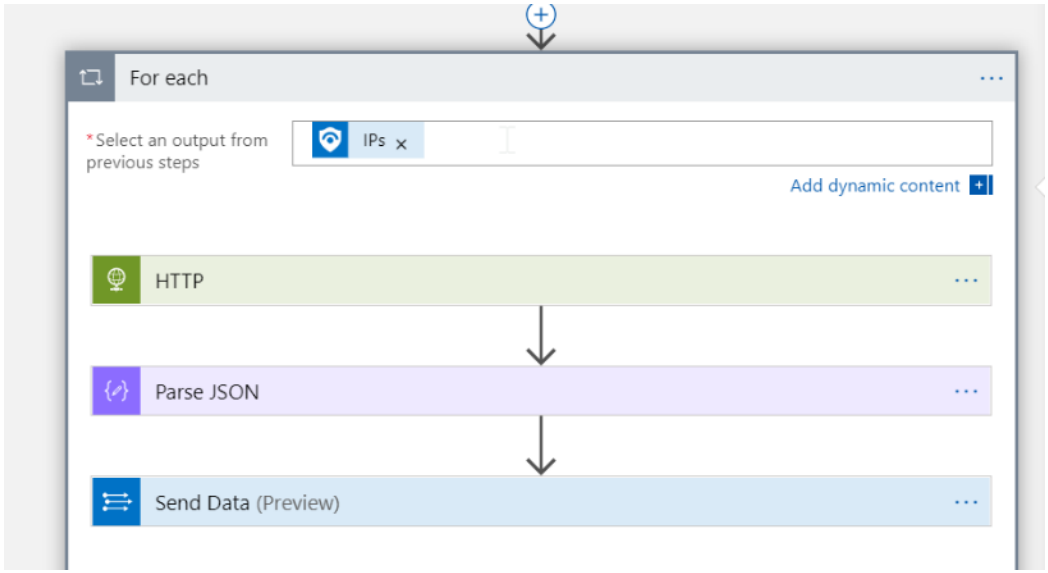
Extract specific values from the entities field

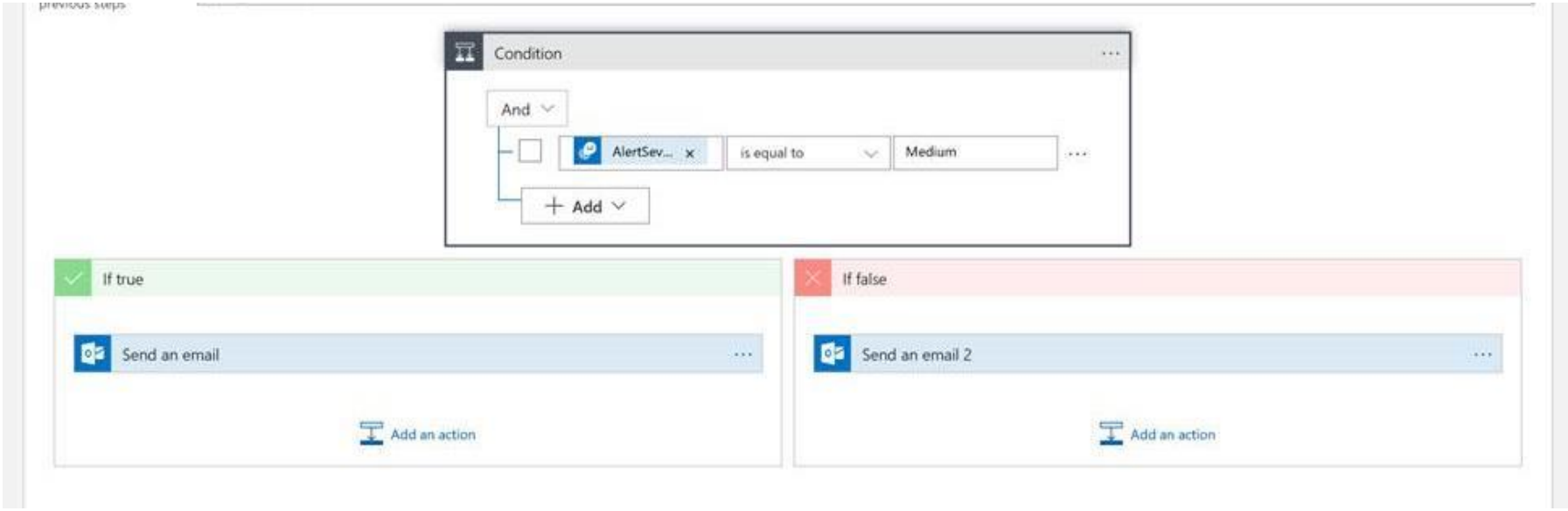


Common Workflow Modules

For Each / Condition (if/and)

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

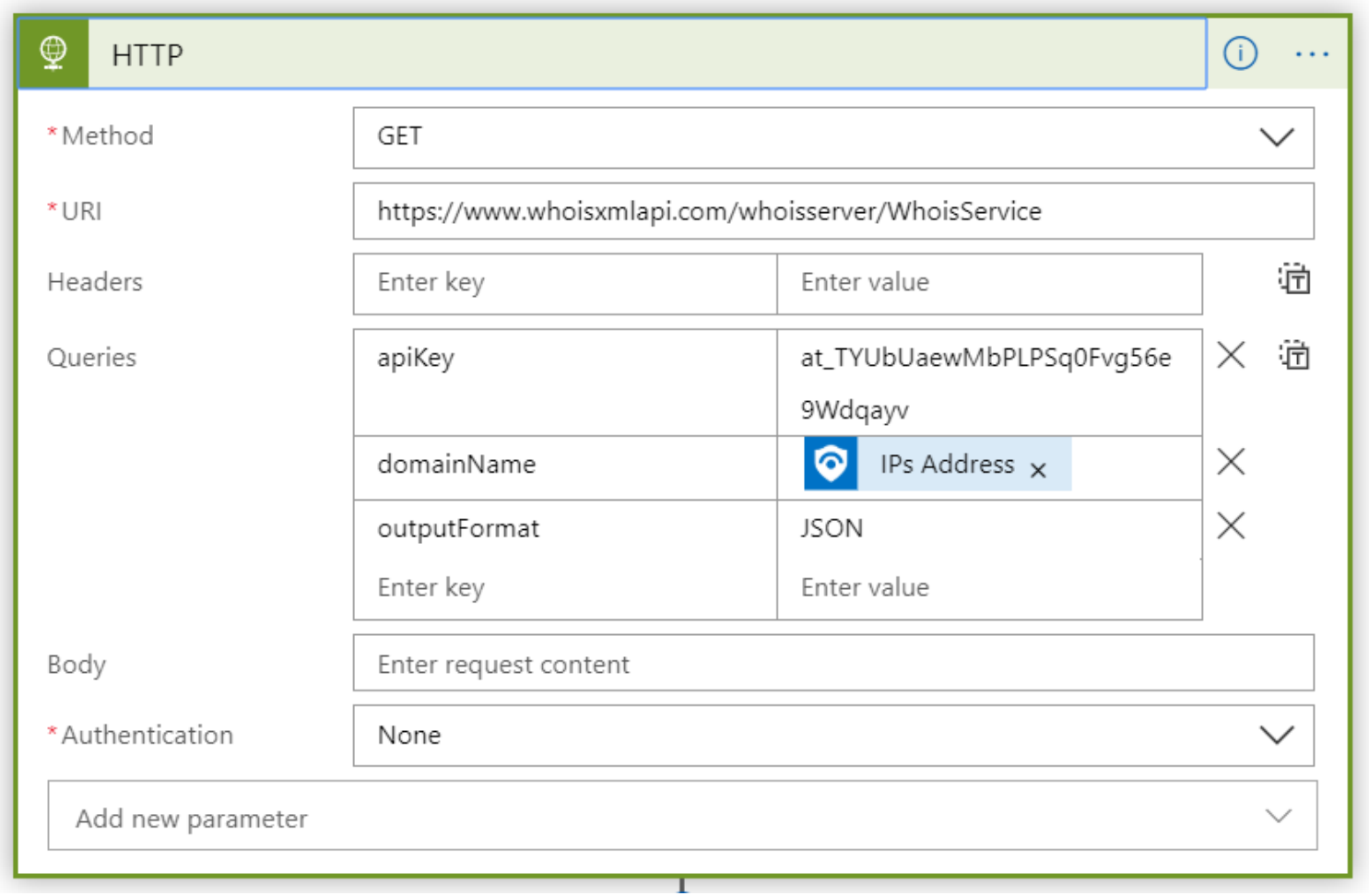




Common Workflow Modules

HTTP

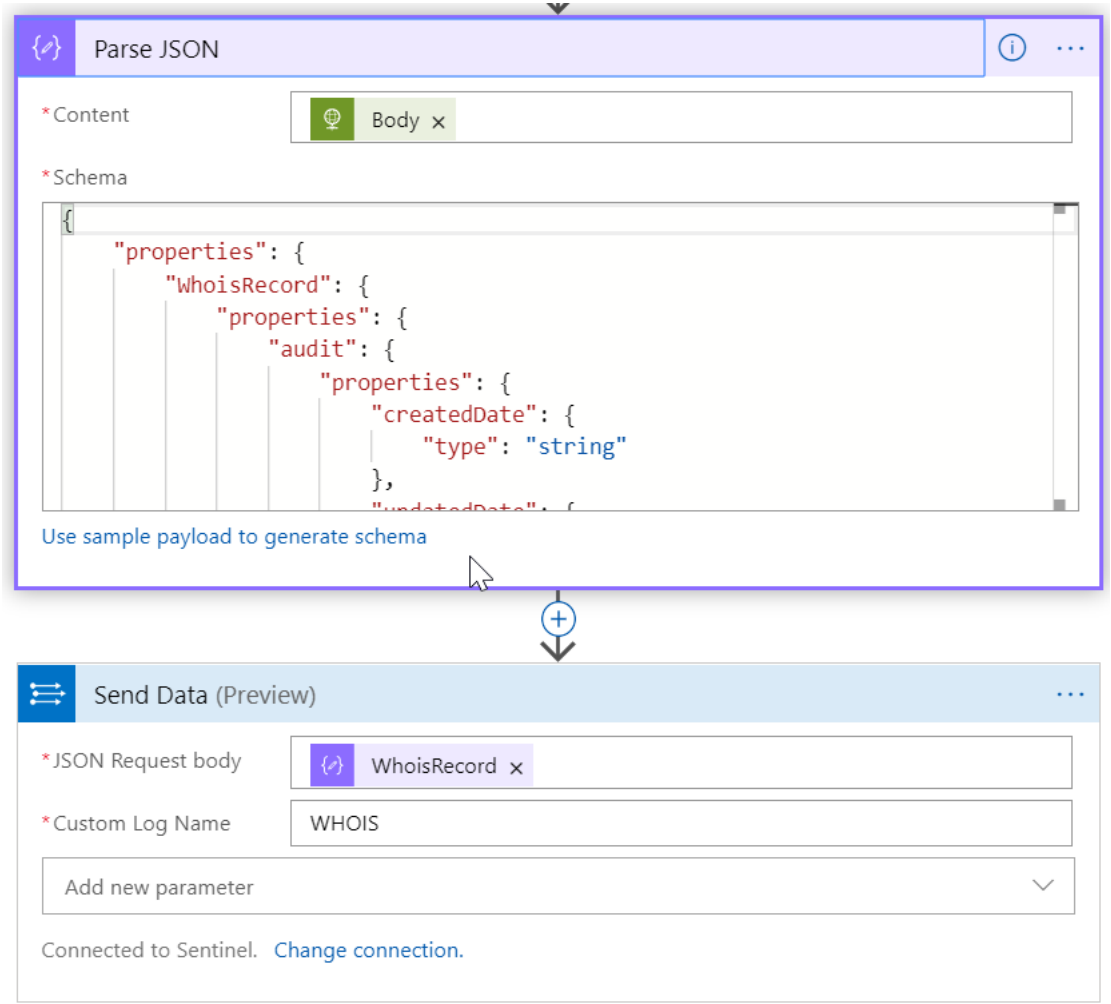
Call an external API



Common Workflow Modules

Parse

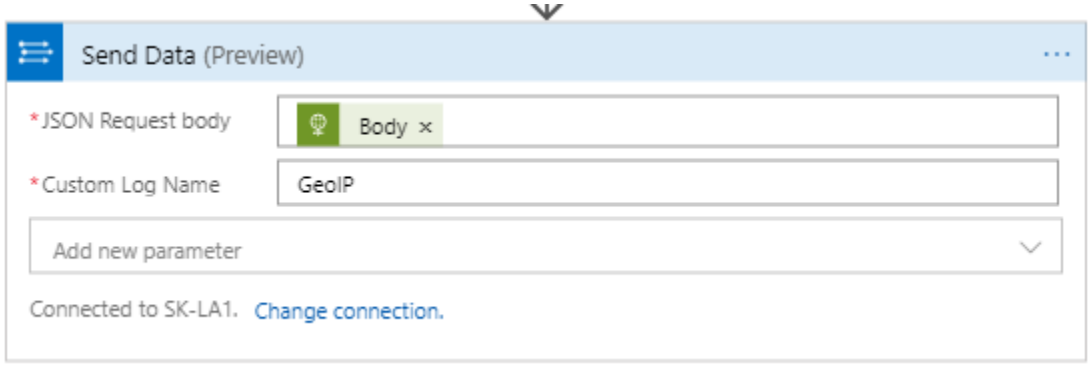
Parse JSON enables you to parse information received (e.g. from the Body of the API call earlier)



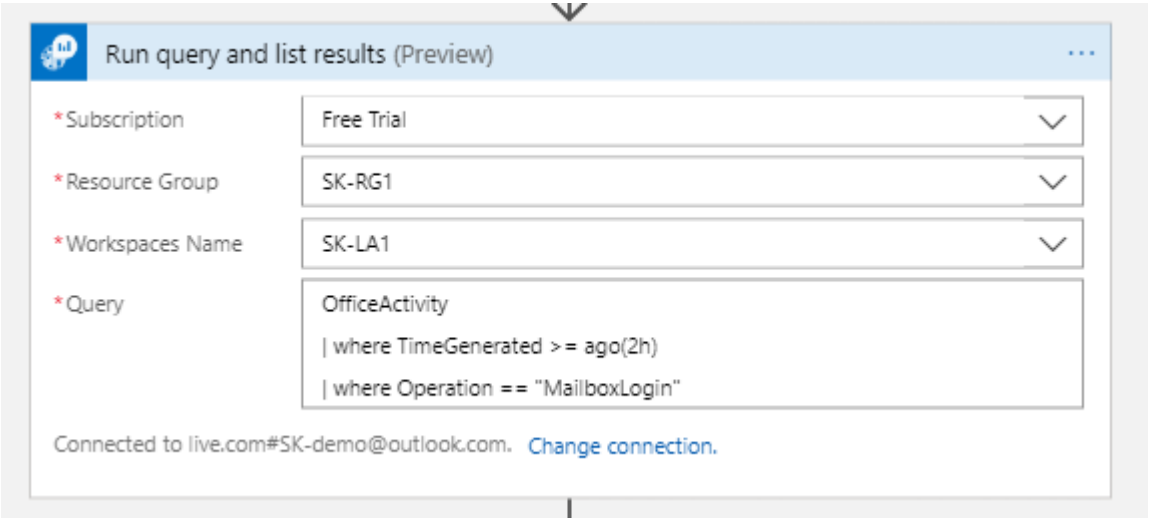
Common Workflow Modules

Log Analytics

Enables you to write data into Log Analytics



Enables you to query Log Analytics

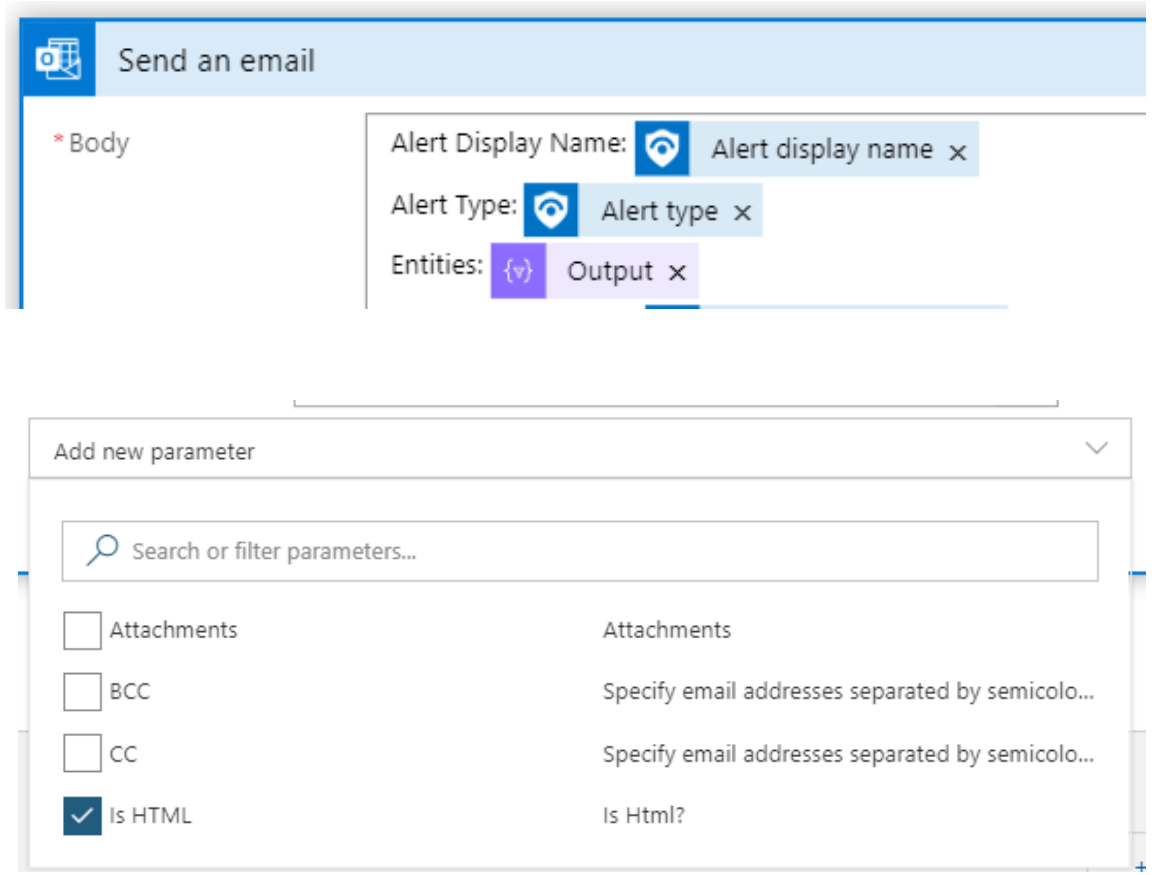


Common Workflow Modules

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

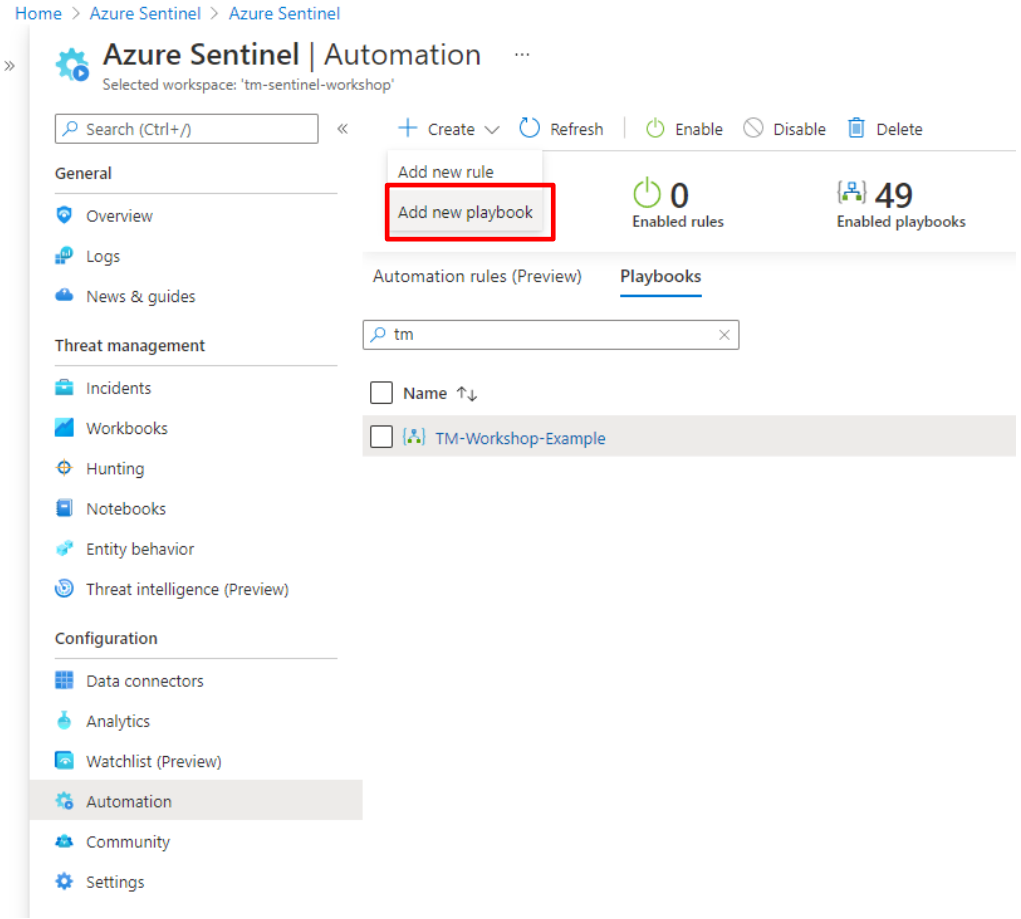


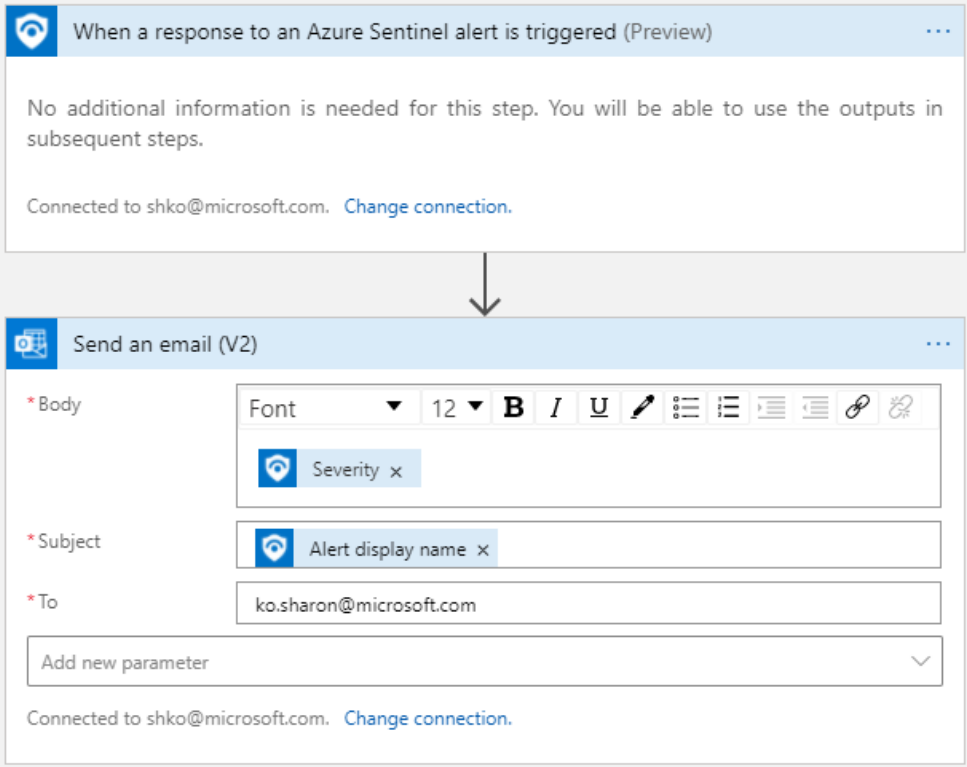
Common Workflow Modules

Servicenow / JIRA

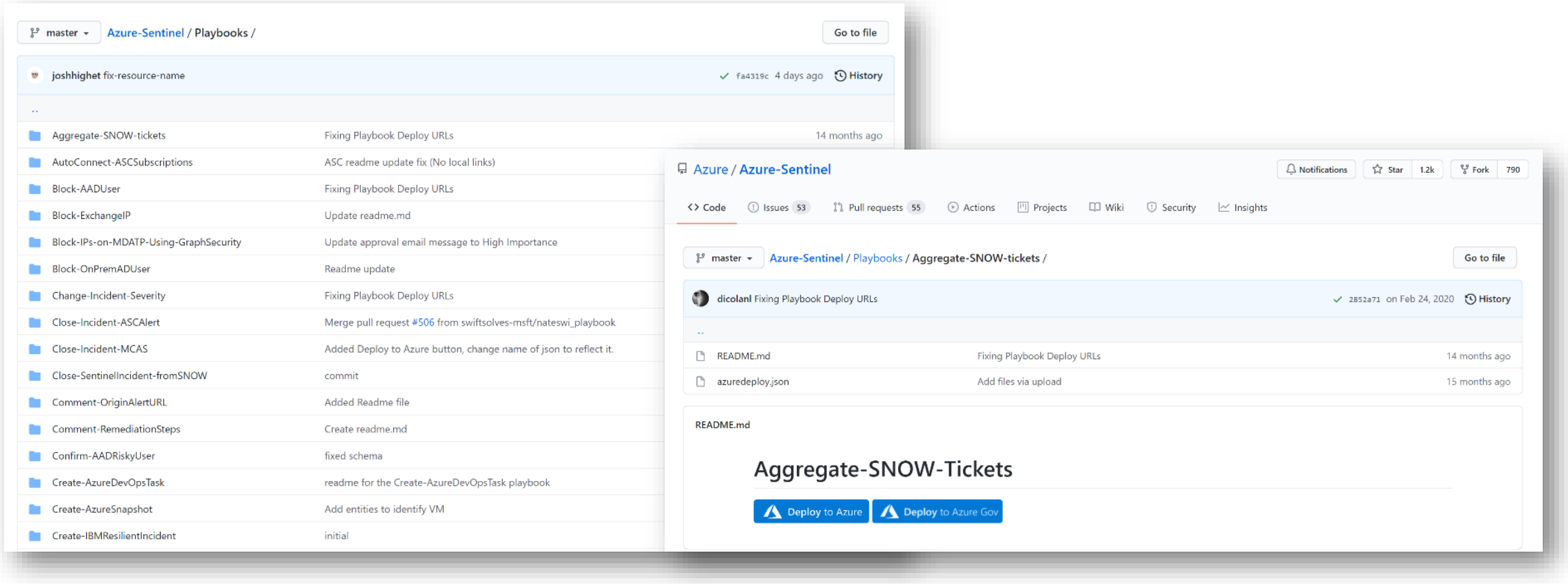
Enables you to open/modify/close/etc.
a case in Servicenow or JIRA

Lab: Creating a Playbook



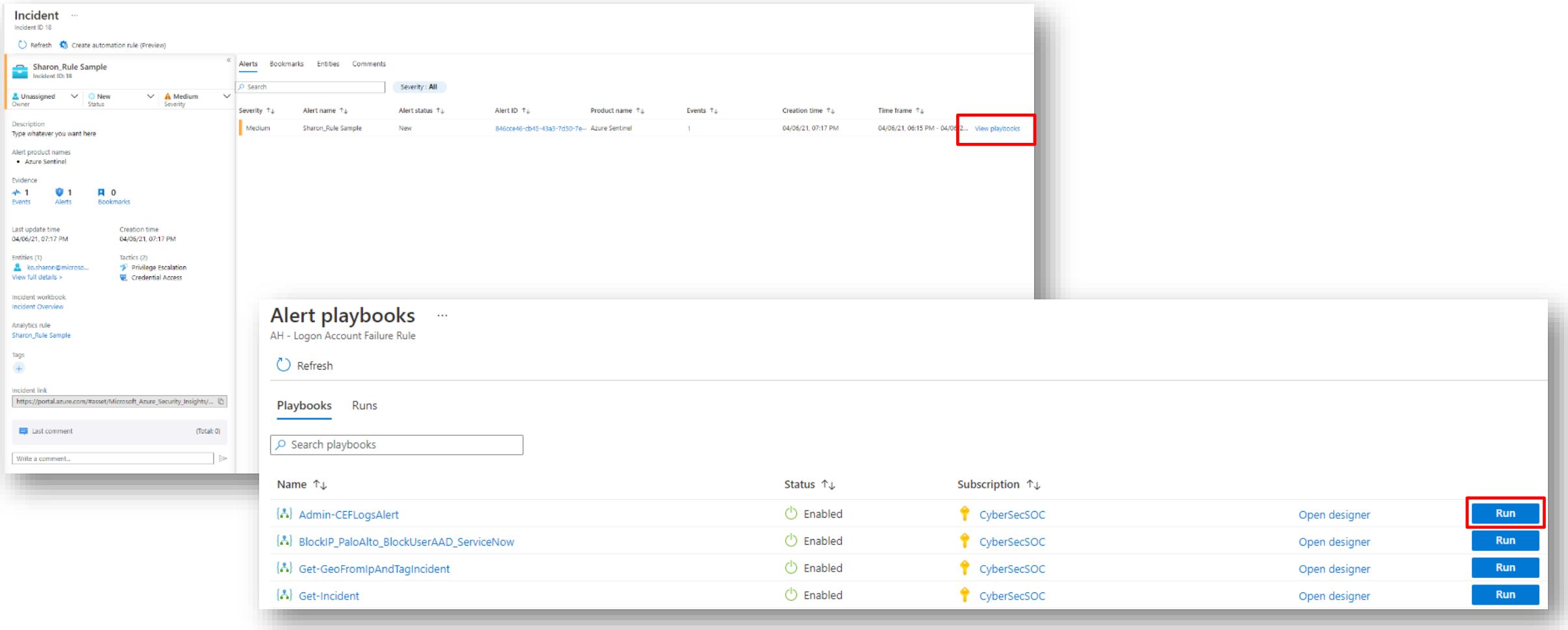


Deploy Playbook Templates from Github

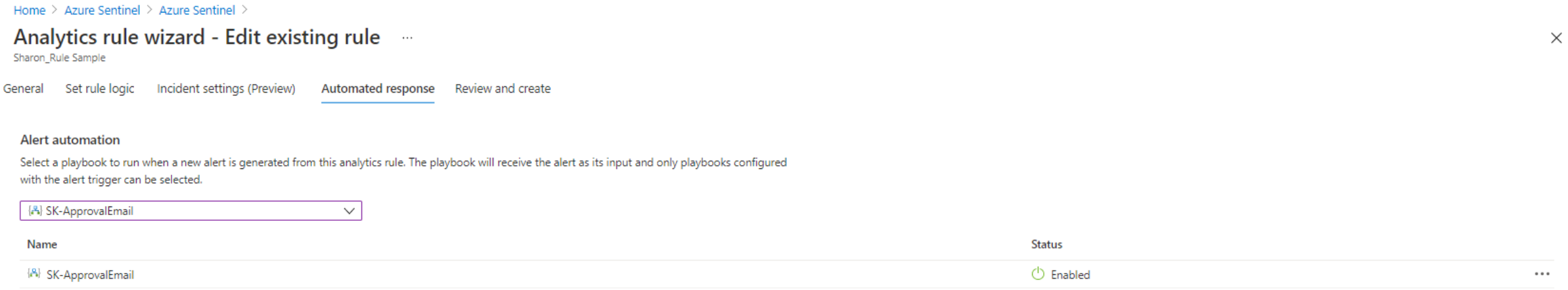


Azure Sentinel Github (Playbooks):
https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks

Lab: Manually Triggering a Playbook



Demo: Attaching a Playbook to a Rule



Microsoft Azure

Feedback Survey