Chapter 1: The Current State of Cybersecurity and the Role of SOAR

No Images

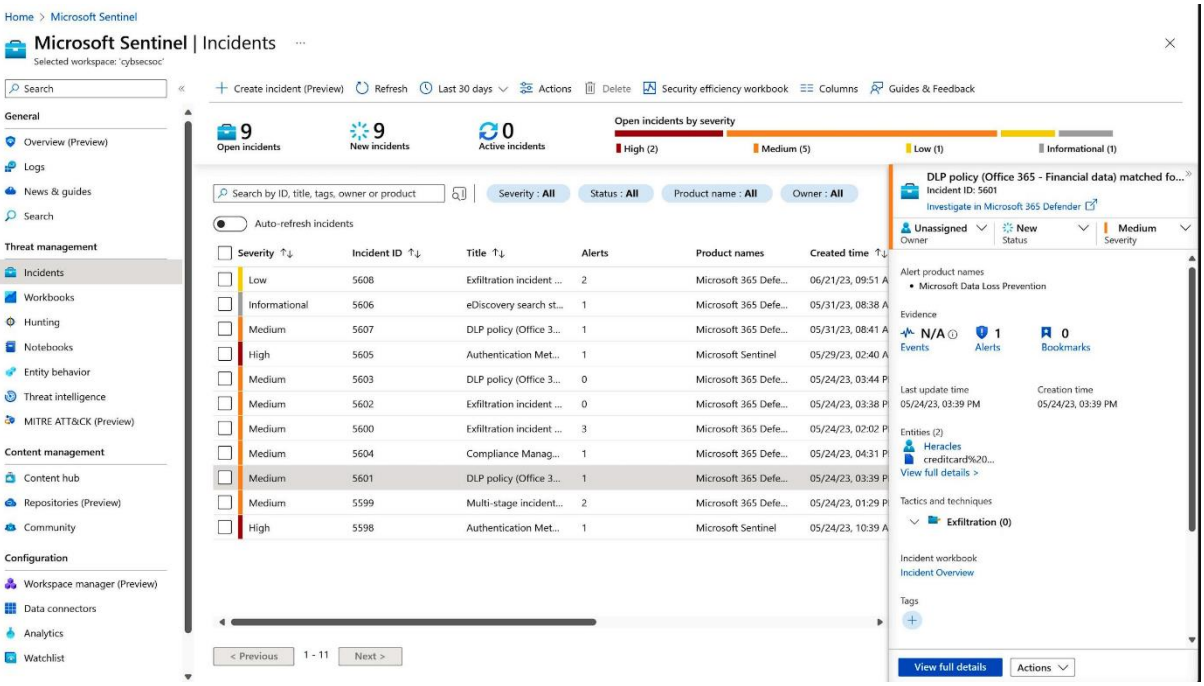
Chapter 2: A Deep Dive into Incident Management and Investigation

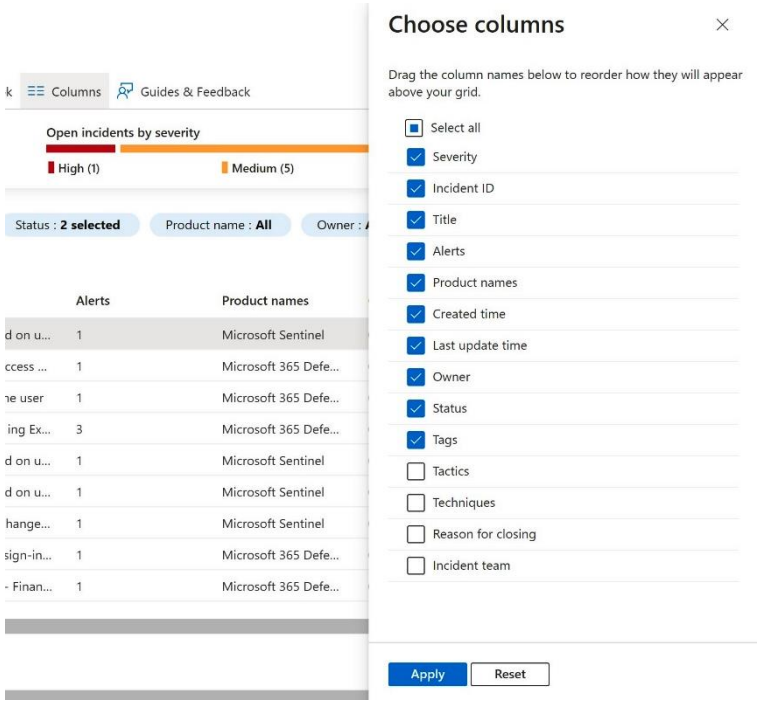
No Images

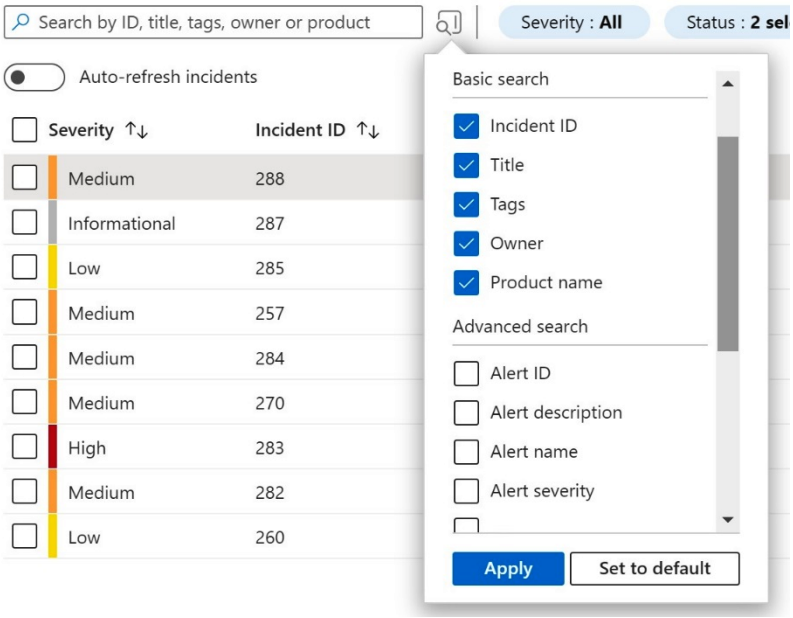
Chapter 3: A Deep Dive into Automation and Reporting

No Images

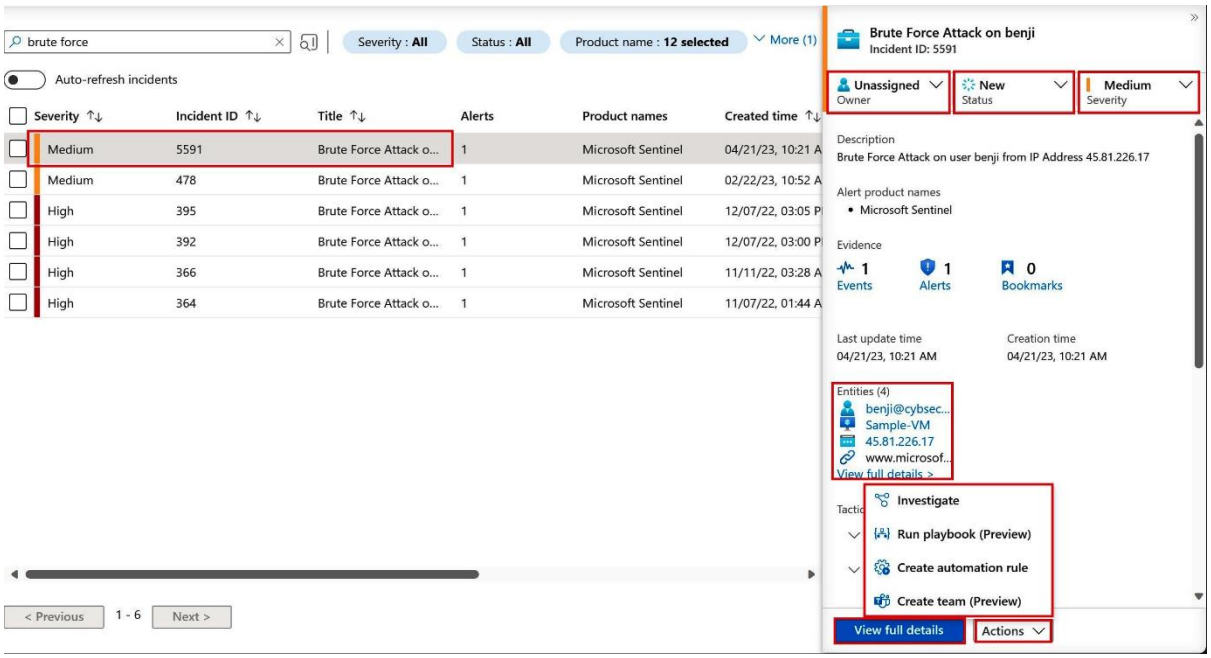
Chapter 4: Quick Dig into SOAR Tools

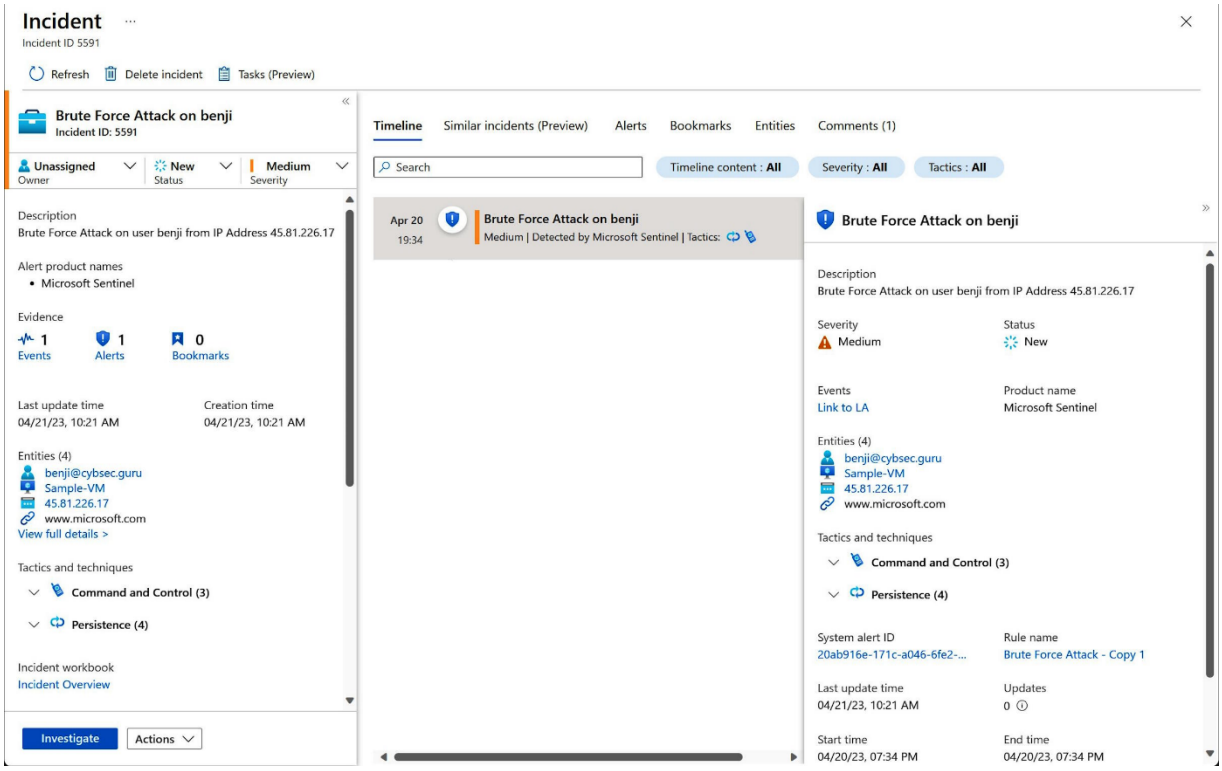


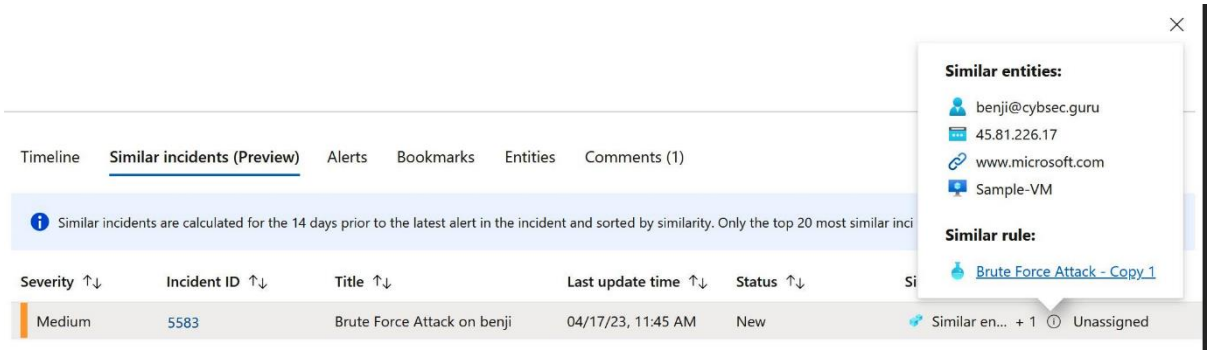


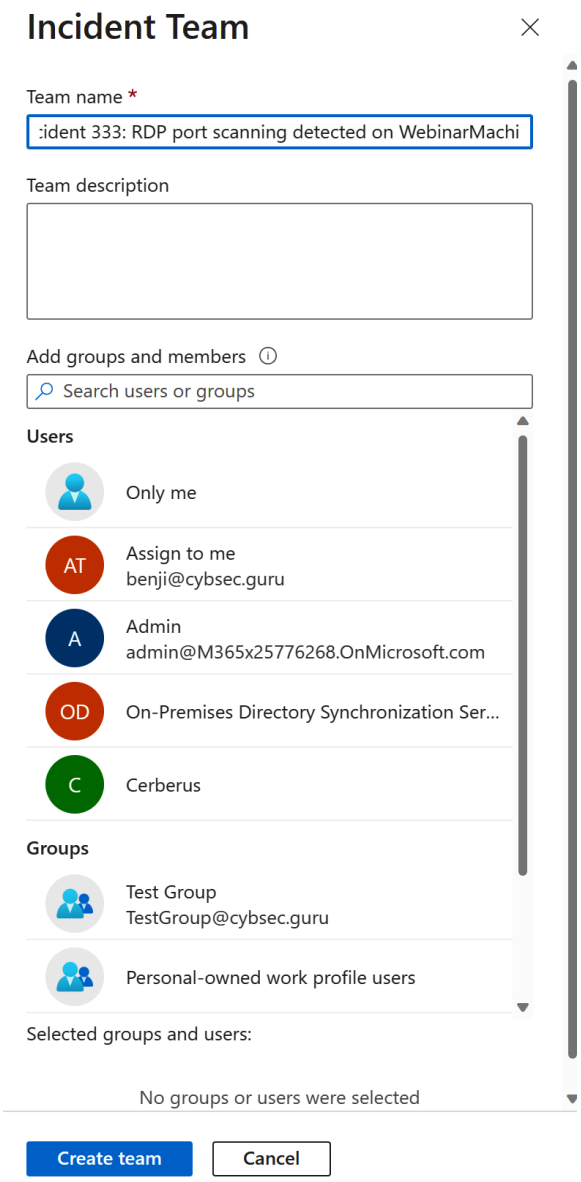

Search by ID, title, tags, owner or product
Severity : All
Status : 2 sel
Auto-refresh incidents
Severity
Incident ID
Medium 288
Informational 287
Low 285
Medium 257
Medium 284
Medium 270
High 283
Medium 282
Low 260
Basic search
Incident ID
Title
Tags
Owner
Product name
Advanced search
Alert ID
Alert description
Alert name
Alert severity
Apply
Set to default

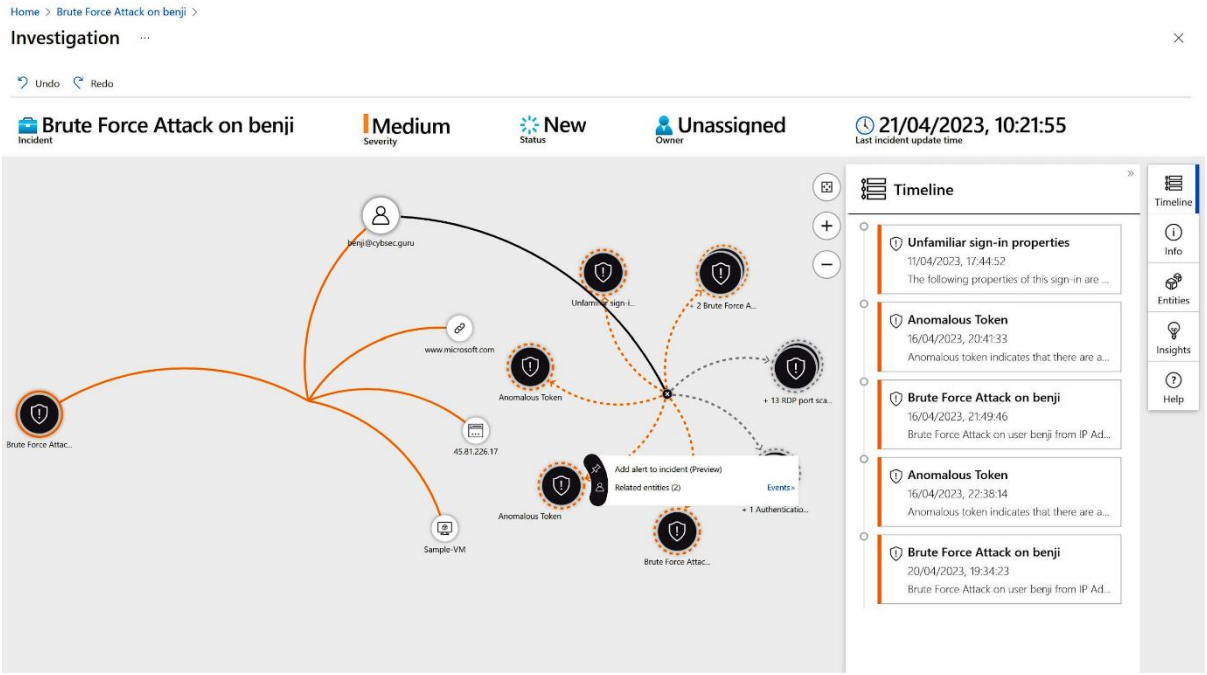

Severity : All
Status : 2 selected
Product name : All
Owner : All
Less

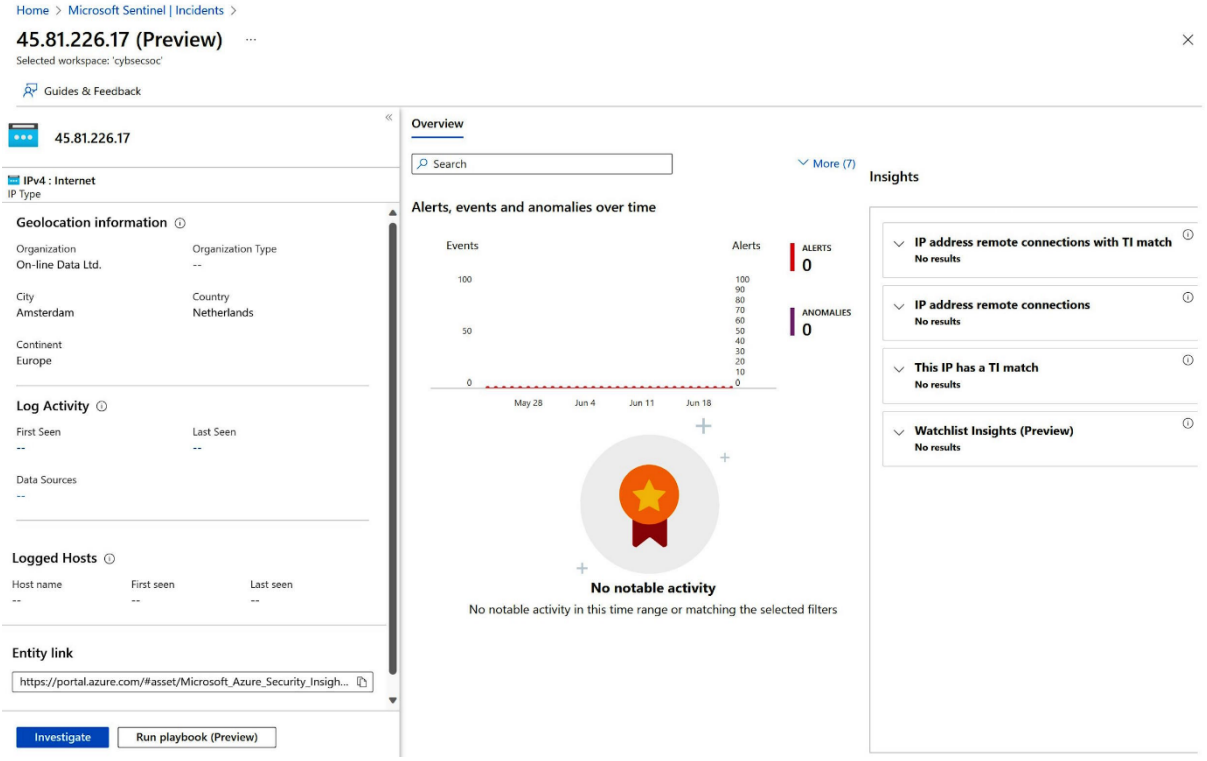

brute force
Severity : All
Status : All
Product name : 12 selected
More (1)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium 5591 Brute Force Attack o... 1 Microsoft Sentinel 04/21/23, 10:21 A
Medium 478 Brute Force Attack o... 1 Microsoft Sentinel 02/22/23, 10:52 A
High 395 Brute Force Attack o... 1 Microsoft Sentinel 12/07/22, 03:05 P
High 392 Brute Force Attack o... 1 Microsoft Sentinel 12/07/22, 03:00 P
High 366 Brute Force Attack o... 1 Microsoft Sentinel 11/11/22, 03:28 A
High 364 Brute Force Attack o... 1 Microsoft Sentinel 11/07/22, 01:44 A
< Previous
1 - 6
Next >
Brute Force Attack on benji
Incident ID: 5591
Unassigned
Owner
New
Status
Medium
Severity
Description
Brute Force Attack on user benji from IP Address 45.81.226.17
Alert product names
Microsoft Sentinel
Evidence
1 Events
1 Alerts
0 Bookmarks
Last update time
04/21/23, 10:21 AM
Creation time
04/21/23, 10:21 AM
Entities (4)
benji@cybsec...
Sample-VM
45.81.226.17
www.microsof...
View full details >
Investigate
Run playbook (Preview)
Create automation rule
Create team (Preview)
View full details
Actions

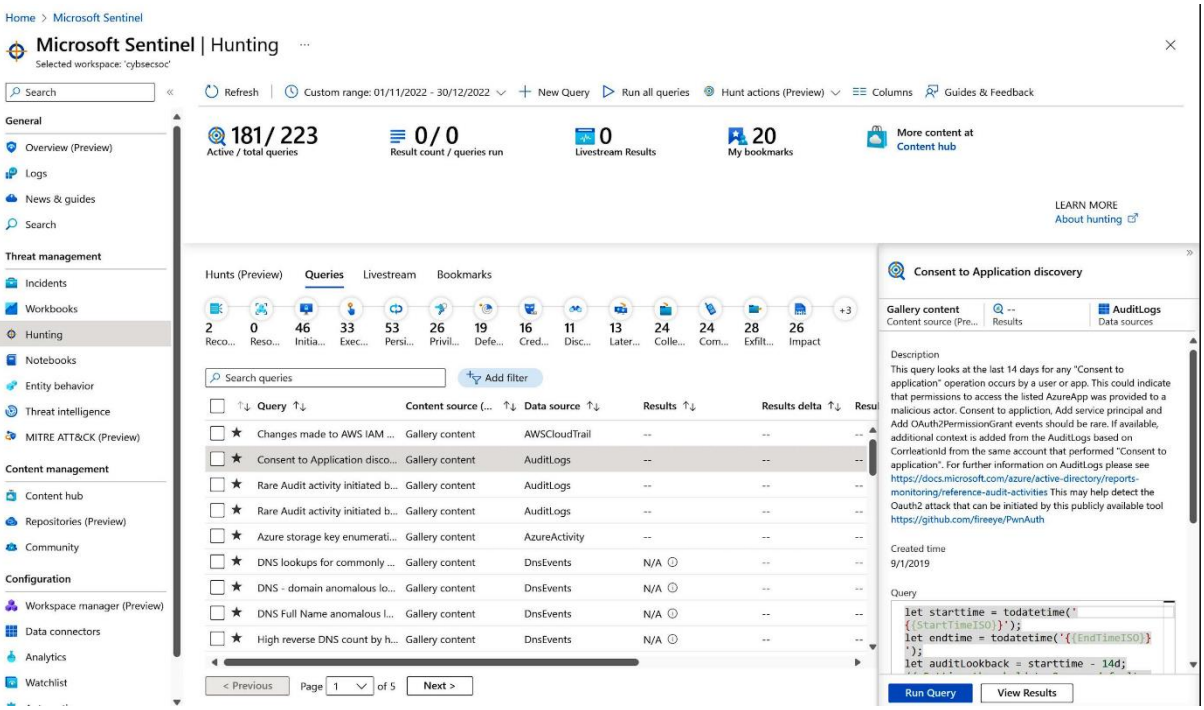

Incident
Incident ID 5591
Refresh
Delete incident
Tasks (Preview)
Brute Force Attack on benji
Incident ID: 5591
Unassigned
Owner
New
Status
Medium
Severity
Description
Brute Force Attack on user benji from IP Address 45.81.226.17
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
04/21/23, 10:21 AM
Creation time
04/21/23, 10:21 AM
Entities (4)
benji@cybsec.guru
Sample-VM
45.81.226.17
www.microsoft.com
View full details >
Tactics and techniques
Command and Control (3)
Persistence (4)
Incident workbook
Incident Overview
Investigate
Actions
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities
Comments (1)
Search
Timeline content : All
Severity : All
Tactics : All
Apr 20
19:34
Brute Force Attack on benji
Medium | Detected by Microsoft Sentinel | Tactics:
Brute Force Attack on benji
Description
Brute Force Attack on user benji from IP Address 45.81.226.17
Severity
Medium
Status
New
Events
Link to LA
Product name
Microsoft Sentinel
Entities (4)
benji@cybsec.guru
Sample-VM
45.81.226.17
www.microsoft.com
Tactics and techniques
Command and Control (3)
Persistence (4)
System alert ID
20ab916e-171c-a046-6fe2-...
Rule name
Brute Force Attack - Copy 1
Last update time
04/21/23, 10:21 AM
Updates
0
Start time
04/20/23, 07:34 PM
End time
04/20/23, 07:34 PM

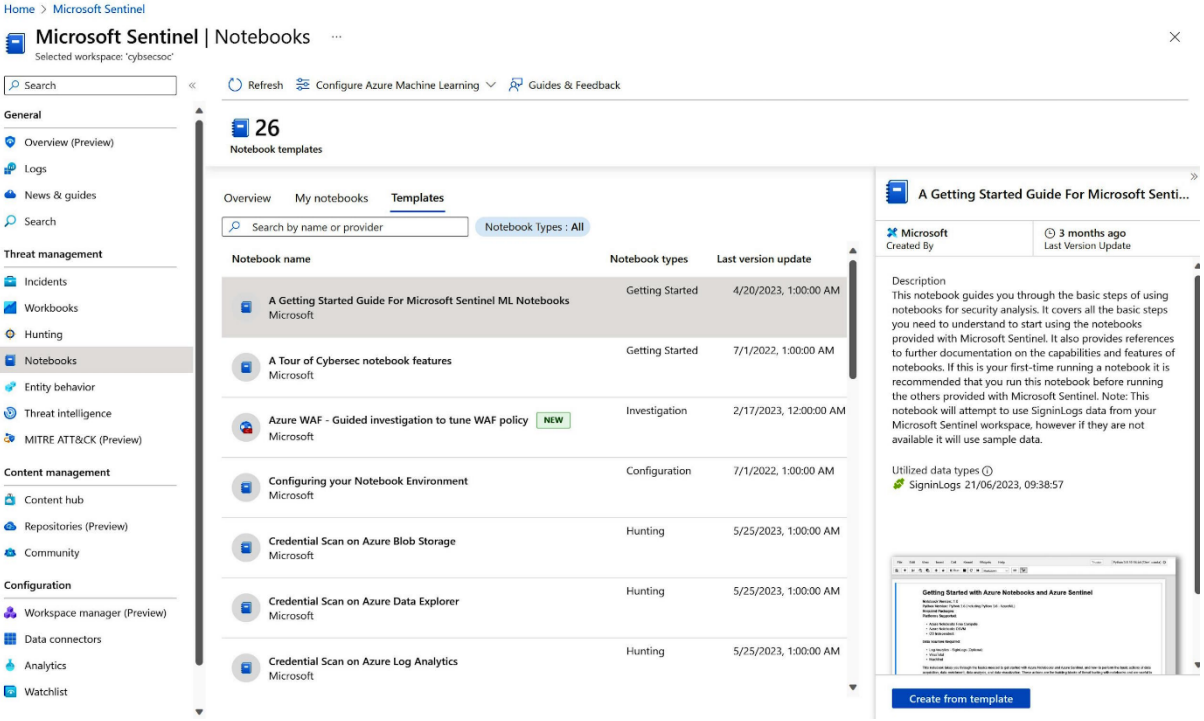

Similar entities:
benji@cybsec.guru
45.81.226.17
www.microsoft.com
Sample-VM
Similar rule:
Brute Force Attack - Copy 1
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities
Comments (1)
Similar incidents are calculated for the 14 days prior to the latest alert in the incident and sorted by similarity. Only the top 20 most similar inci
Severity
Incident ID
Title
Last update time
Status
Medium
5583
Brute Force Attack on benji
04/17/23, 11:45 AM
New
Similar en... + 1
Unassigned

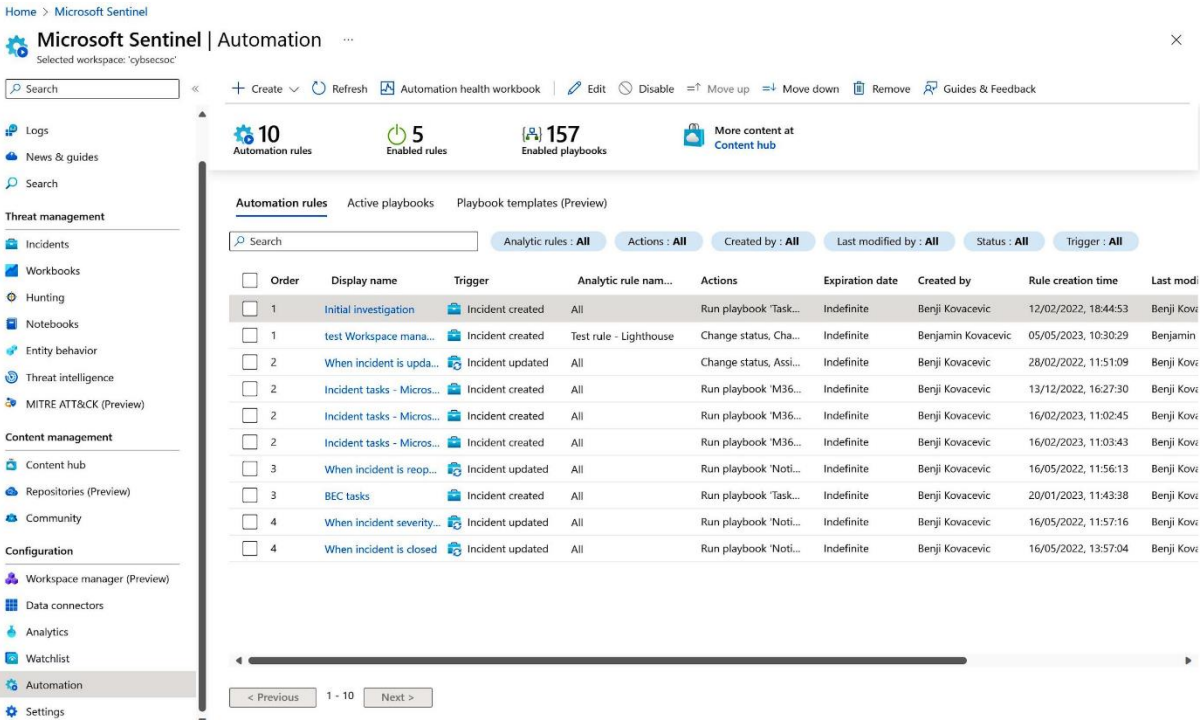

Incident Team
Team name *
:ident 333: RDP port scanning detected on WebinarMachi
Team description
Add groups and members
Search users or groups
Users
Only me
AT
Assign to me
benji@cybsec.guru
A
Admin
admin@M365x25776268.OnMicrosoft.com
OD
On-Premises Directory Synchronization Ser...
C
Cerberus
Groups
Test Group
TestGroup@cybsec.guru
Personal-owned work profile users
Selected groups and users:
No groups or users were selected
Create team
Cancel


Home > Brute Force Attack on benji >
Investigation
Undo
Redo
Brute Force Attack on benji
Incident
Medium
Severity
New
Status
Unassigned
Owner
21/04/2023, 10:21:55
Last incident update time
benji@cybsec.guru
www.microsoft.com
Anomalous Token
45.81.226.17
Sample-VM
Add alert to incident (Preview)
Related entities (2)
Events>
Timeline
Unfamiliar sign-in properties
11/04/2023, 17:44:52
The following properties of this sign-in are ...
Anomalous Token
16/04/2023, 20:41:33
Anomalous token indicates that there are a...
Brute Force Attack on benji
16/04/2023, 21:49:46
Brute Force Attack on user benji from IP Ad...
Anomalous Token
16/04/2023, 22:38:14
Anomalous token indicates that there are a...
Brute Force Attack on benji
20/04/2023, 19:34:23
Brute Force Attack on user benji from IP Ad...
Timeline
Info
Entities
Insights
Help


Home > Microsoft Sentinel | Incidents >
45.81.226.17 (Preview)
Selected workspace: 'cybsecsoc'
Guides & Feedback
45.81.226.17
IPv4 : Internet
IP Type
Geolocation information
Organization
On-line Data Ltd.
Organization Type
--
City
Amsterdam
Country
Netherlands
Continent
Europe
Log Activity
First Seen
--
Last Seen
--
Data Sources
--
Logged Hosts
Host name
First seen
Last seen
Entity link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insigh...
Investigate
Run playbook (Preview)
Overview
Search
More (7)
Alerts, events and anomalies over time
Events
Alerts
ALERTS
0
ANOMALIES
0
May 28
Jun 4
Jun 11
Jun 18
No notable activity
No notable activity in this time range or matching the selected filters
Insights
IP address remote connections with TI match
No results
IP address remote connections
No results
This IP has a TI match
No results
Watchlist Insights (Preview)
No results


Home > Microsoft Sentinel
Microsoft Sentinel | Hunting
Selected workspace: 'cybsecsoc'
Search
Refresh
Custom range: 01/11/2022 - 30/12/2022
New Query
Run all queries
Hunt actions (Preview)
Columns
Guides & Feedback
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Watchlist
181/ 223
Active / total queries
0/ 0
Result count / queries run
0
Livestream Results
20
My bookmarks
More content at
Content hub
LEARN MORE
About hunting
Hunts (Preview)
Queries
Livestream
Bookmarks
Search queries
Add filter
Query
Content source (...
Data source
Results
Results delta
Changes made to AWS IAM ...
Consent to Application disco...
Rare Audit activity initiated b...
Azure storage key enumerati...
DNS lookups for commonly ...
DNS - domain anomalous lo...
DNS Full Name anomalous l...
High reverse DNS count by h...
Gallery content
AuditLogs
AWSCloudTrail
AzureActivity
DnsEvents
N/A
< Previous
Page 1 of 5
Next >
Consent to Application discovery
Gallery content
Content source (Pre...
Results
AuditLogs
Data sources
Description
This query looks at the last 14 days for any "Consent to application" operation occurs by a user or app. This could indicate that permissions to access the listed AzureApp was provided to a malicious actor. Consent to appliction, Add service principal and Add OAuth2PermissionGrant events should be rare. If available, additional context is added from the AuditLogs based on CorrleationId from the same account that performed "Consent to application". For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities This may help detect the Oauth2 attack that can be initiated by this publicly available tool https://github.com/fireeye/PwnAuth
Created time
9/1/2019
Query
let starttime = todatetime('{StartTimeISO}');
let endtime = todatetime('{EndTimeISO}');
let auditLookback = starttime - 14d;
Run Query
View Results


Home > Microsoft Sentinel
Microsoft Sentinel | Notebooks
Selected workspace: 'cybsecsoc'
Search
Refresh
Configure Azure Machine Learning
Guides & Feedback
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Watchlist
26
Notebook templates
Overview
My notebooks
Templates
Search by name or provider
Notebook Types : All
Notebook name
Notebook types
Last version update
A Getting Started Guide For Microsoft Sentinel ML Notebooks
Microsoft
Getting Started
4/20/2023, 1:00:00 AM
A Tour of Cybersec notebook features
Microsoft
Getting Started
7/1/2022, 1:00:00 AM
Azure WAF - Guided investigation to tune WAF policy
NEW
Microsoft
Investigation
2/17/2023, 12:00:00 AM
Configuring your Notebook Environment
Microsoft
Configuration
7/1/2022, 1:00:00 AM
Credential Scan on Azure Blob Storage
Microsoft
Hunting
5/25/2023, 1:00:00 AM
Credential Scan on Azure Data Explorer
Microsoft
Hunting
5/25/2023, 1:00:00 AM
Credential Scan on Azure Log Analytics
Microsoft
Hunting
5/25/2023, 1:00:00 AM
A Getting Started Guide For Microsoft Senti...
Microsoft
Created By
3 months ago
Last Version Update
Description
This notebook guides you through the basic steps of using notebooks for security analysis. It covers all the basic steps you need to understand to start using the notebooks provided with Microsoft Sentinel. It also provides references to further documentation on the capabilities and features of notebooks. If this is your first-time running a notebook it is recommended that you run this notebook before running the others provided with Microsoft Sentinel. Note: This notebook will attempt to use SigninLogs data from your Microsoft Sentinel workspace, however if they are not available it will use sample data.
Utilized data types
SigninLogs 21/06/2023, 09:38:57
Getting Started with Azure Notebooks and Azure Sentinel
Create from template



Edit automation rule

Automation rule name

Initial investigation

Trigger

When incident is created

Conditions

If

Incident provider | Equals | All

AND

Analytic rule name | Contains | All

+ Add

Actions

Run playbook

Send-Teams-adaptive-card-on-incident-c...
VS FTE / CyberSecurity

And then

Run playbook

Send-email-with-formatted-incident-report
VS FTE / CyberSecurity

+ Add action

Rule expiration

Indefinite | Time

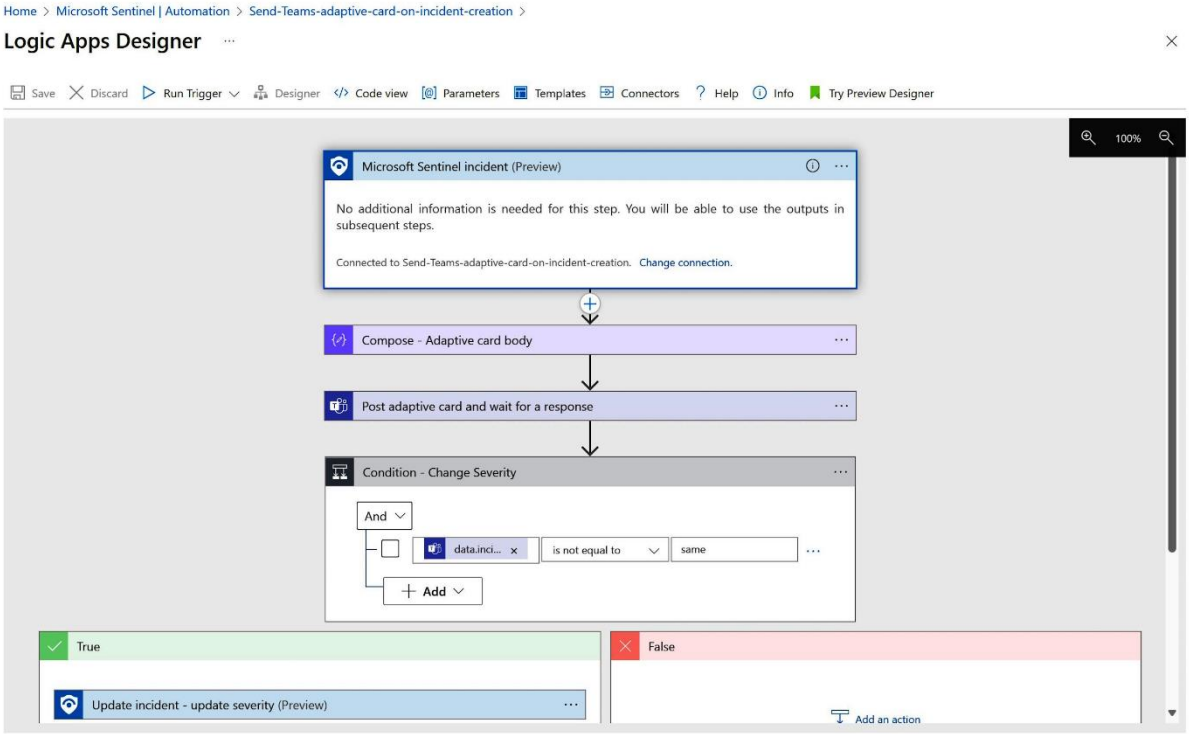
Order

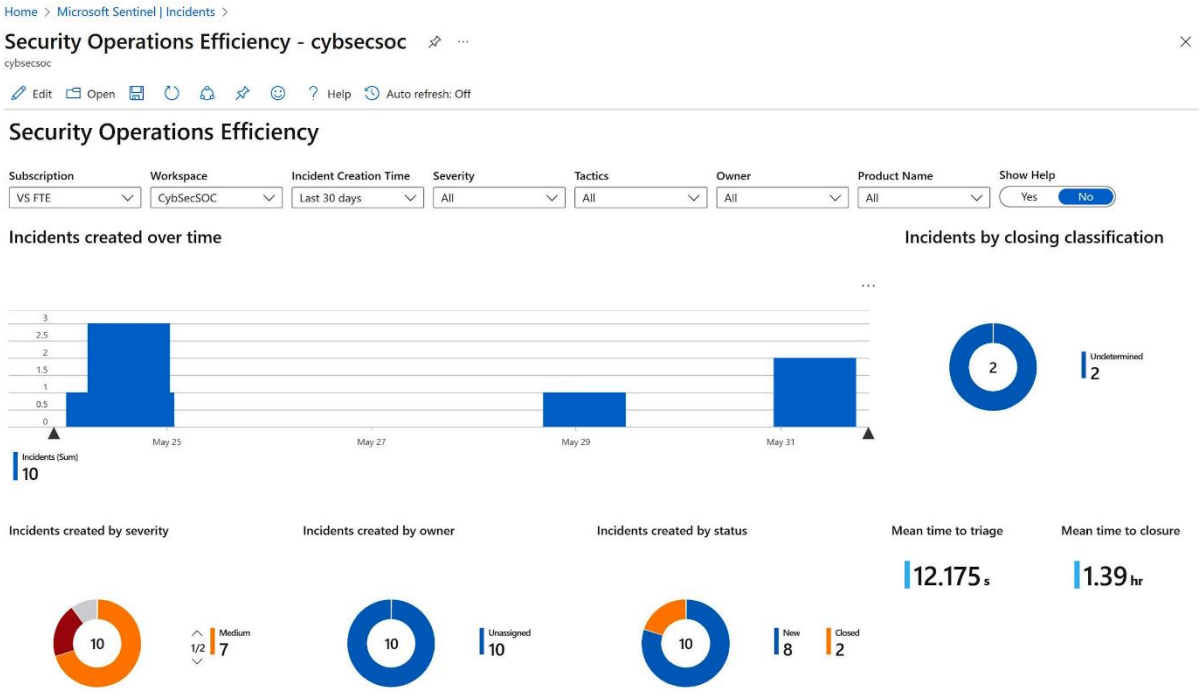
1

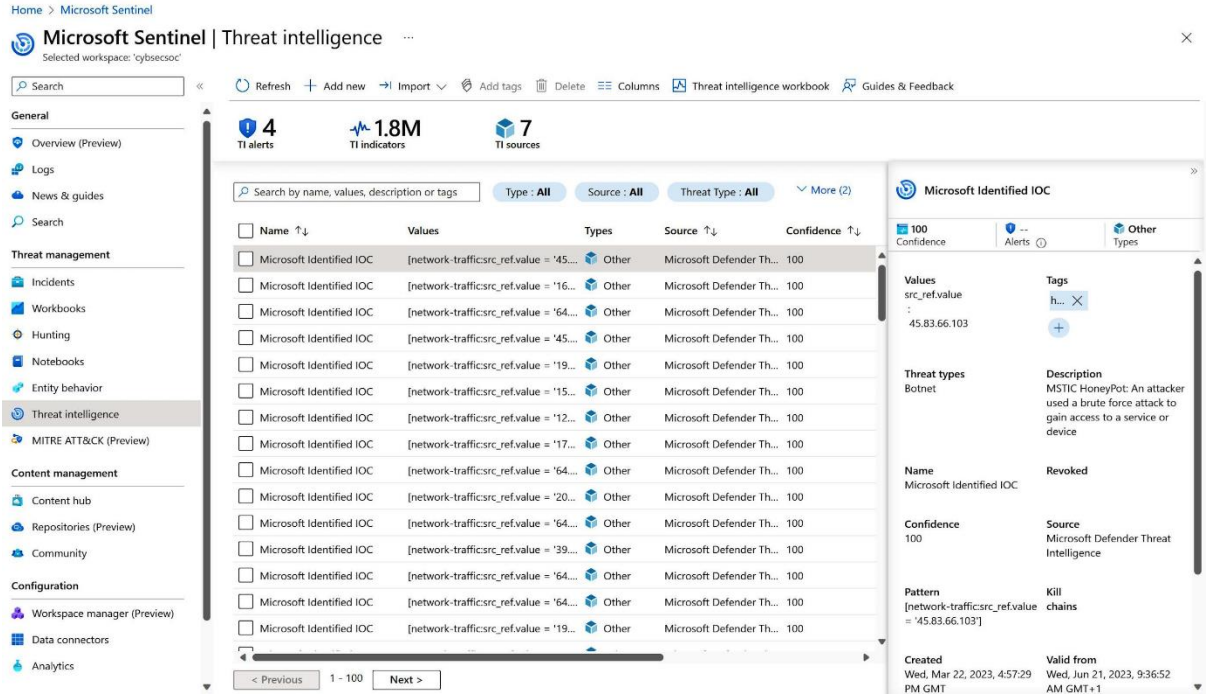
Status

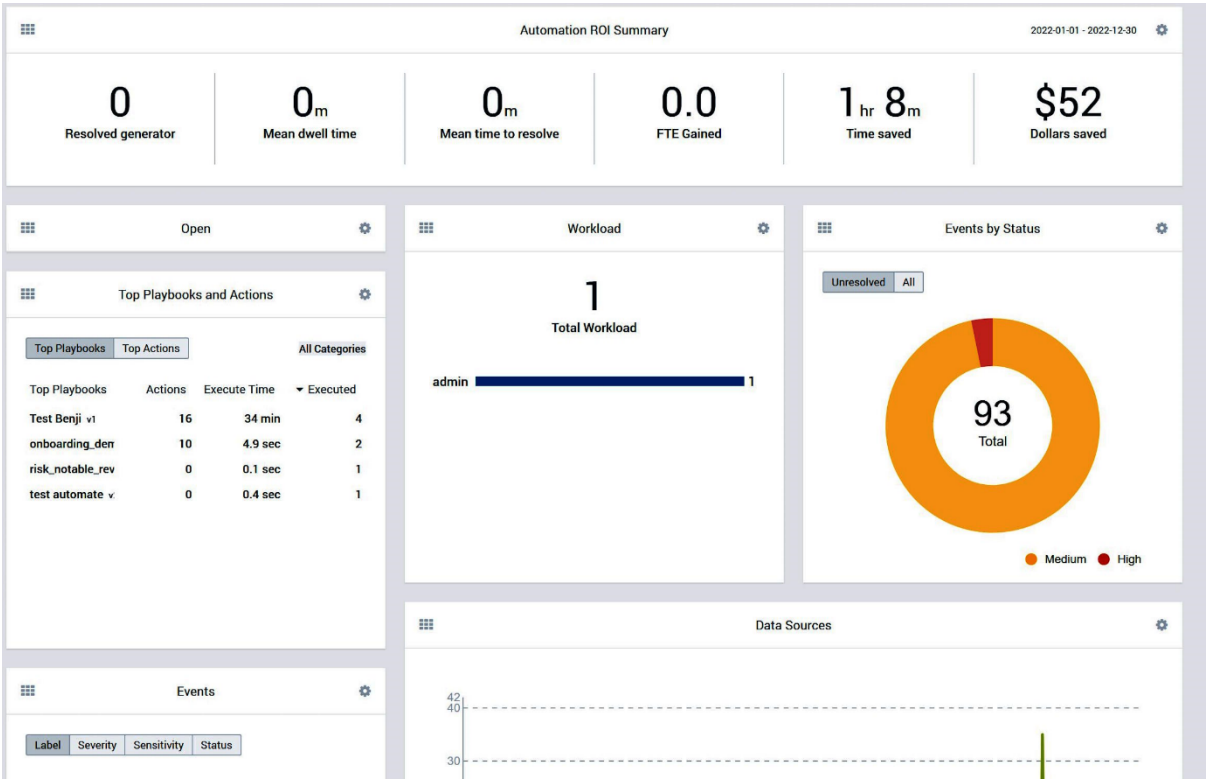
Enabled

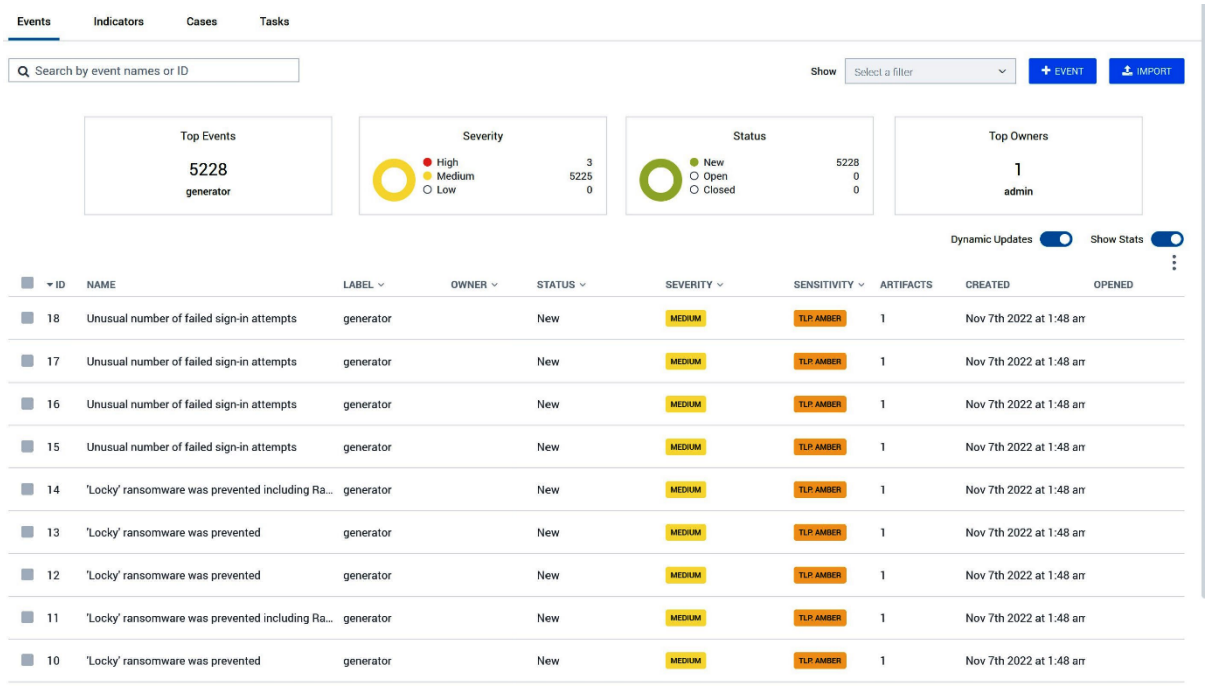
Apply | Cancel

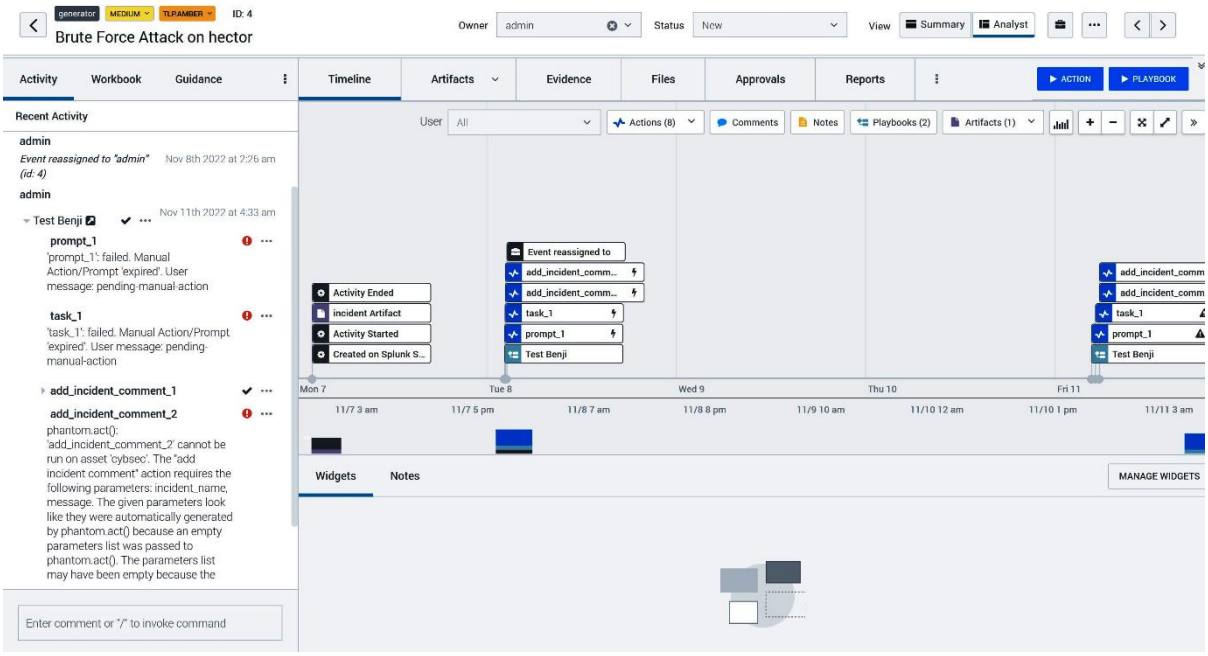

Home > Microsoft Sentinel | Automation > Send-Teams-adaptive-card-on-incident-creation >
Logic Apps Designer
Save
Discard
Run Trigger
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Try Preview Designer
100%
Microsoft Sentinel incident (Preview)
No additional information is needed for this step. You will be able to use the outputs in subsequent steps.
Connected to Send-Teams-adaptive-card-on-incident-creation. Change connection.
Compose - Adaptive card body
Post adaptive card and wait for a response
Condition - Change Severity
And
data.inci...
is not equal to
same
Add
True
False
Update incident - update severity (Preview)
Add an action

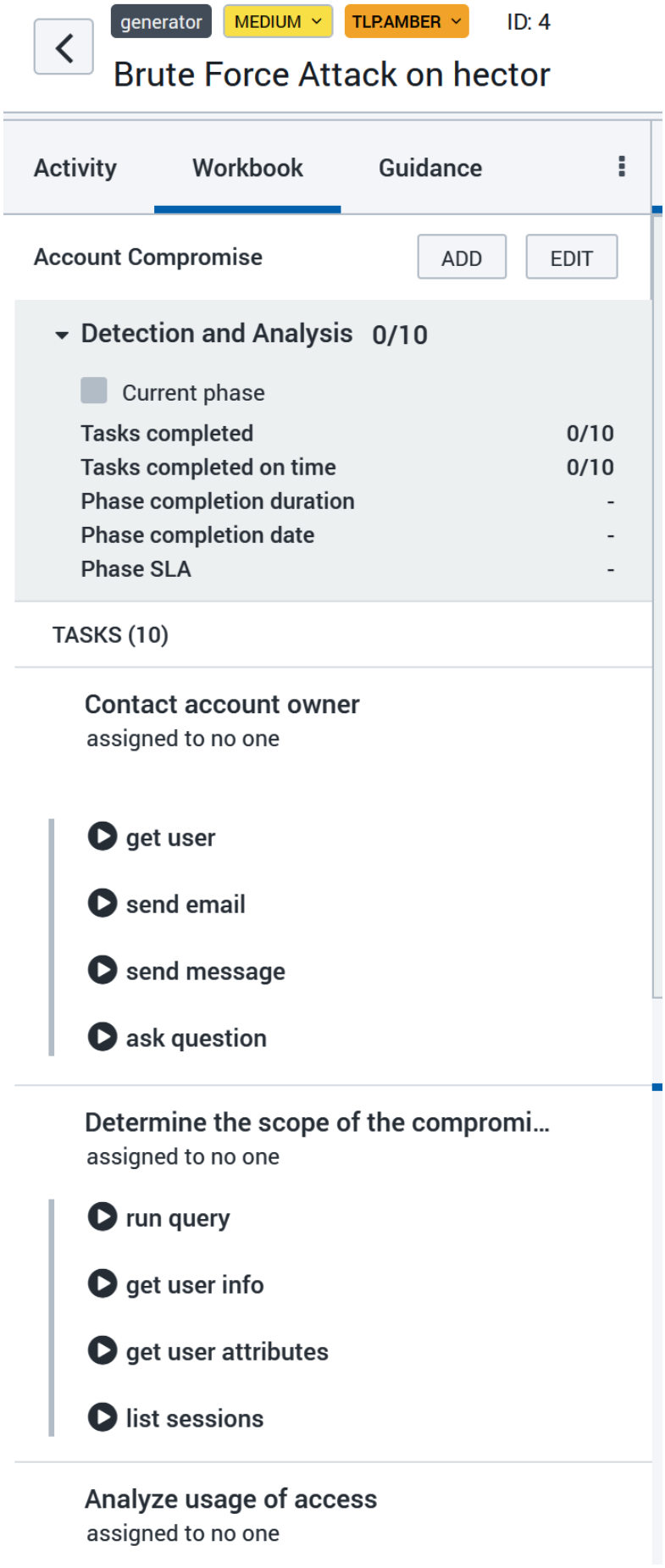

Home > Microsoft Sentinel | Incidents >
Security Operations Efficiency - cybsecsoc
cybsecsoc
Edit
Open
Help
Auto refresh: Off
Security Operations Efficiency
Subscription
VS FTE
Workspace
CybSecSOC
Incident Creation Time
Last 30 days
Severity
All
Tactics
All
Owner
All
Product Name
All
Show Help
Yes
No
Incidents created over time
3
2.5
2
1.5
1
0.5
0
May 25
May 27
May 29
May 31
Incidents (Sum)
10
Incidents by closing classification
2
Undetermined
2
Incidents created by severity
10
1/2
Medium
7
Incidents created by owner
10
Unassigned
10
Incidents created by status
10
New
8
Closed
2
Mean time to triage
12.175 s
Mean time to closure
1.39 hr

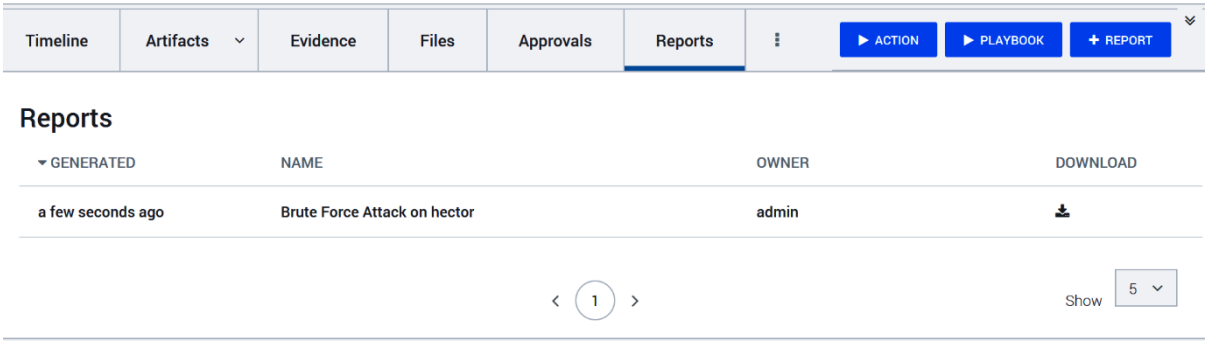

Home > Microsoft Sentinel
Microsoft Sentinel | Threat intelligence
Selected workspace: 'cybsecsoc'
Search
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Refresh
Add new
Import
Add tags
Delete
Columns
Threat intelligence workbook
Guides & Feedback
4
TI alerts
1.8M
TI indicators
7
TI sources
Search by name, values, description or tags
Type : All
Source : All
Threat Type : All
More (2)
Name
Values
Types
Source
Confidence
Microsoft Identified IOC
[network-traffic:src_ref.value = '45....
Other
Microsoft Defender Th...
100
< Previous
1 - 100
Next >
Microsoft Identified IOC
100
Confidence
Alerts
Other
Types
Values
src_ref.value
:
45.83.66.103
Tags
Threat types
Botnet
Description
MSTIC HoneyPot: An attacker used a brute force attack to gain access to a service or device
Name
Microsoft Identified IOC
Revoked
Confidence
100
Source
Microsoft Defender Threat Intelligence
Pattern
[network-traffic:src_ref.value = '45.83.66.103']
Kill chains
Created
Wed, Mar 22, 2023, 4:57:29 PM GMT
Valid from
Wed, Jun 21, 2023, 9:36:52 AM GMT+1

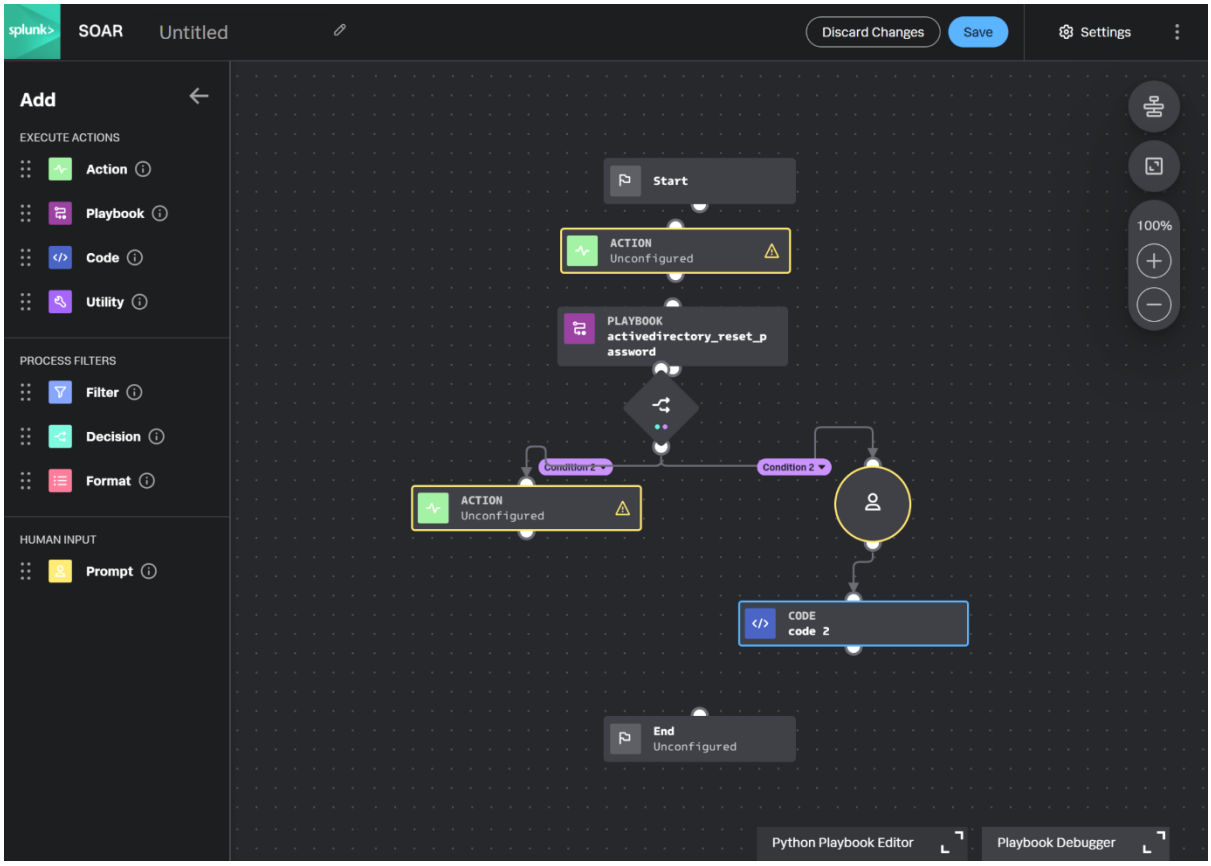

Automation ROI Summary
2022-01-01 - 2022-12-30
0
Resolved generator
0m
Mean dwell time
0m
Mean time to resolve
0.0
FTE Gained
1hr 8m
Time saved
$52
Dollars saved
Open
Workload
Events by Status
Top Playbooks and Actions
Top Playbooks
Top Actions
All Categories
Top Playbooks
Actions
Execute Time
Executed
Test Benji v1
16
34 min
4
onboarding_den
10
4.9 sec
2
risk_notable_rev
0
0.1 sec
1
test automate v
0
0.4 sec
1
1
Total Workload
admin
1
Unresolved
All
93
Total
Medium
High
Data Sources
Events
Label
Severity
Sensitivity
Status
42
40
30

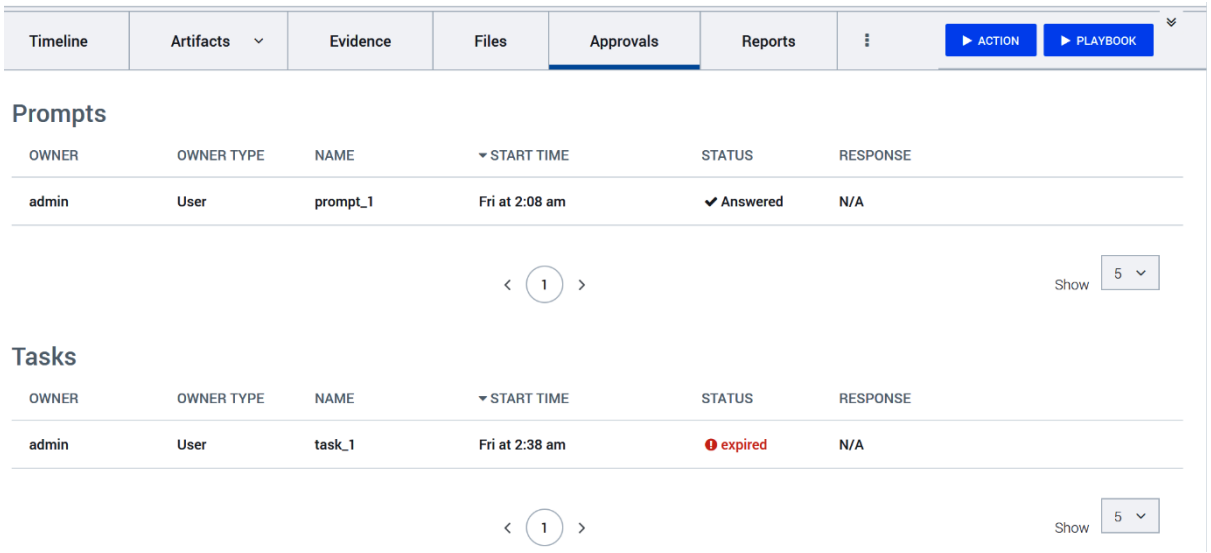

Events
Indicators
Cases
Tasks
Search by event names or ID
Show
Select a filter
+ EVENT
IMPORT
Top Events
5228
generator
Severity
High 3
Medium 5225
Low 0
Status
New 5228
Open 0
Closed 0
Top Owners
1
admin
Dynamic Updates
Show Stats
ID NAME LABEL OWNER STATUS SEVERITY SENSITIVITY ARTIFACTS CREATED OPENED
18 Unusual number of failed sign-in attempts generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
17 Unusual number of failed sign-in attempts generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
16 Unusual number of failed sign-in attempts generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
15 Unusual number of failed sign-in attempts generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
14 'Locky' ransomware was prevented including Ra... generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
13 'Locky' ransomware was prevented generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
12 'Locky' ransomware was prevented generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
11 'Locky' ransomware was prevented including Ra... generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am
10 'Locky' ransomware was prevented generator New MEDIUM TLP AMBER 1 Nov 7th 2022 at 1:48 am

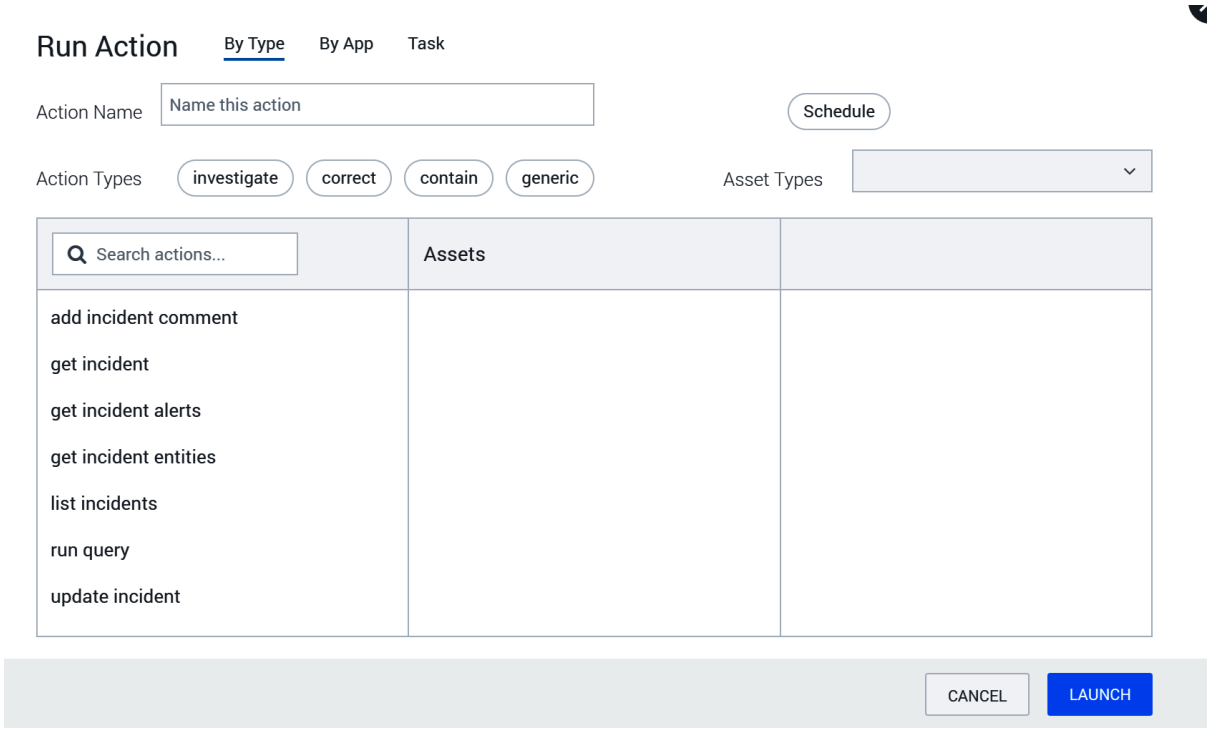

generator
MEDIUM
TLP:AMBER
ID: 4
Brute Force Attack on hector
Owner
admin
Status
New
View
Summary
Analyst
Activity
Workbook
Guidance
Timeline
Artifacts
Evidence
Files
Approvals
Reports
ACTION
PLAYBOOK
Recent Activity
admin
Event reassigned to "admin" (id: 4)
Nov 8th 2022 at 2:26 am
admin
Test Benji
Nov 11th 2022 at 4:33 am
prompt_1
'prompt_1': failed. Manual Action/Prompt 'expired'. User message: pending-manual-action
task_1
'task_1': failed. Manual Action/Prompt 'expired'. User message: pending-manual-action
add_incident_comment_1
add_incident_comment_2
phantom.act(): 'add_incident_comment_2' cannot be run on asset 'cybsec'. The "add incident comment" action requires the following parameters: incident_name, message. The given parameters look like they were automatically generated by phantom.act() because an empty parameters list was passed to phantom.act(). The parameters list may have been empty because the
Enter comment or "/" to invoke command
User
All
Actions (8)
Comments
Notes
Playbooks (2)
Artifacts (1)
Event reassigned to
add_incident_comm...
task_1
prompt_1
Test Benji
Activity Ended
incident Artifact
Activity Started
Created on Splunk S...
Mon 7
Tue 8
Wed 9
Thu 10
Fri 11
11/7 3 am
11/7 5 pm
11/8 7 am
11/8 8 pm
11/9 10 am
11/10 12 am
11/10 1 pm
11/11 3 am
Widgets
Notes
MANAGE WIDGETS

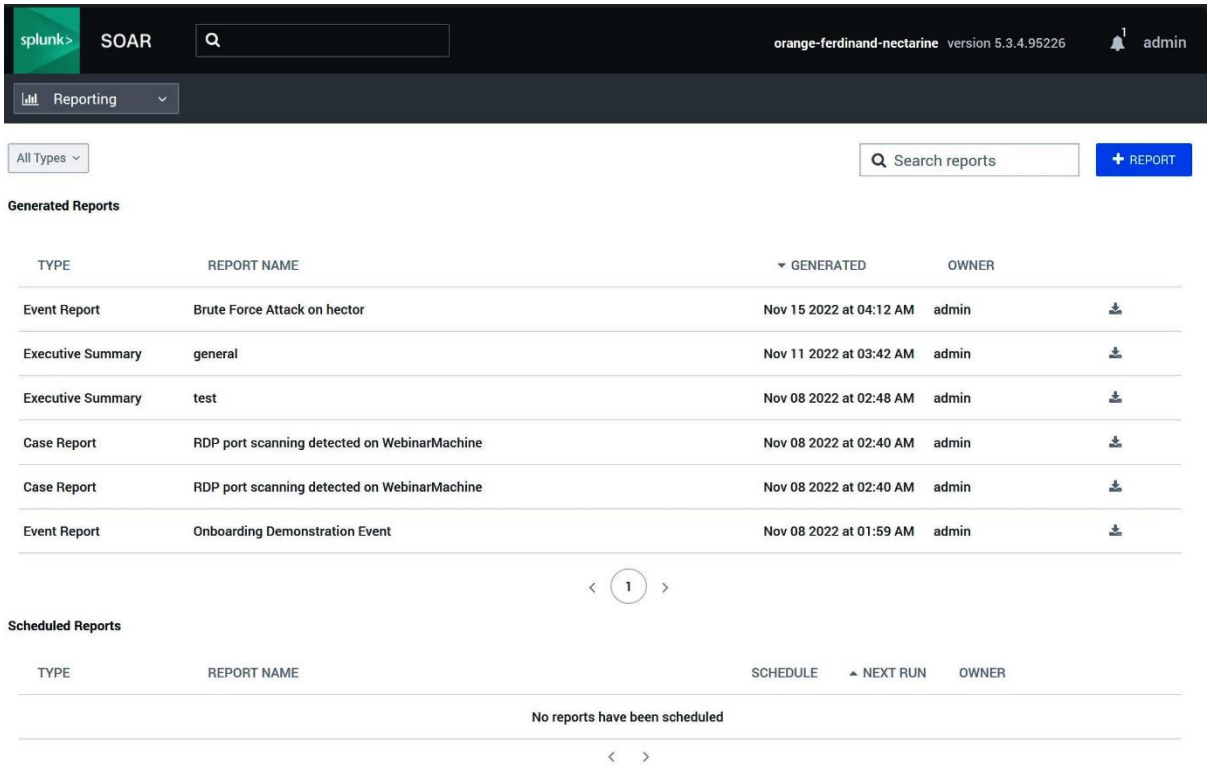

generator
MEDIUM
TLP:AMBER
ID: 4
Brute Force Attack on hector
Activity
Workbook
Guidance
Account Compromise
ADD
EDIT
Detection and Analysis 0/10
Current phase
Tasks completed 0/10
Tasks completed on time 0/10
Phase completion duration -
Phase completion date -
Phase SLA -
TASKS (10)
Contact account owner
assigned to no one
get user
send email
send message
ask question
Determine the scope of the compromi...
assigned to no one
run query
get user info
get user attributes
list sessions
Analyze usage of access
assigned to no one

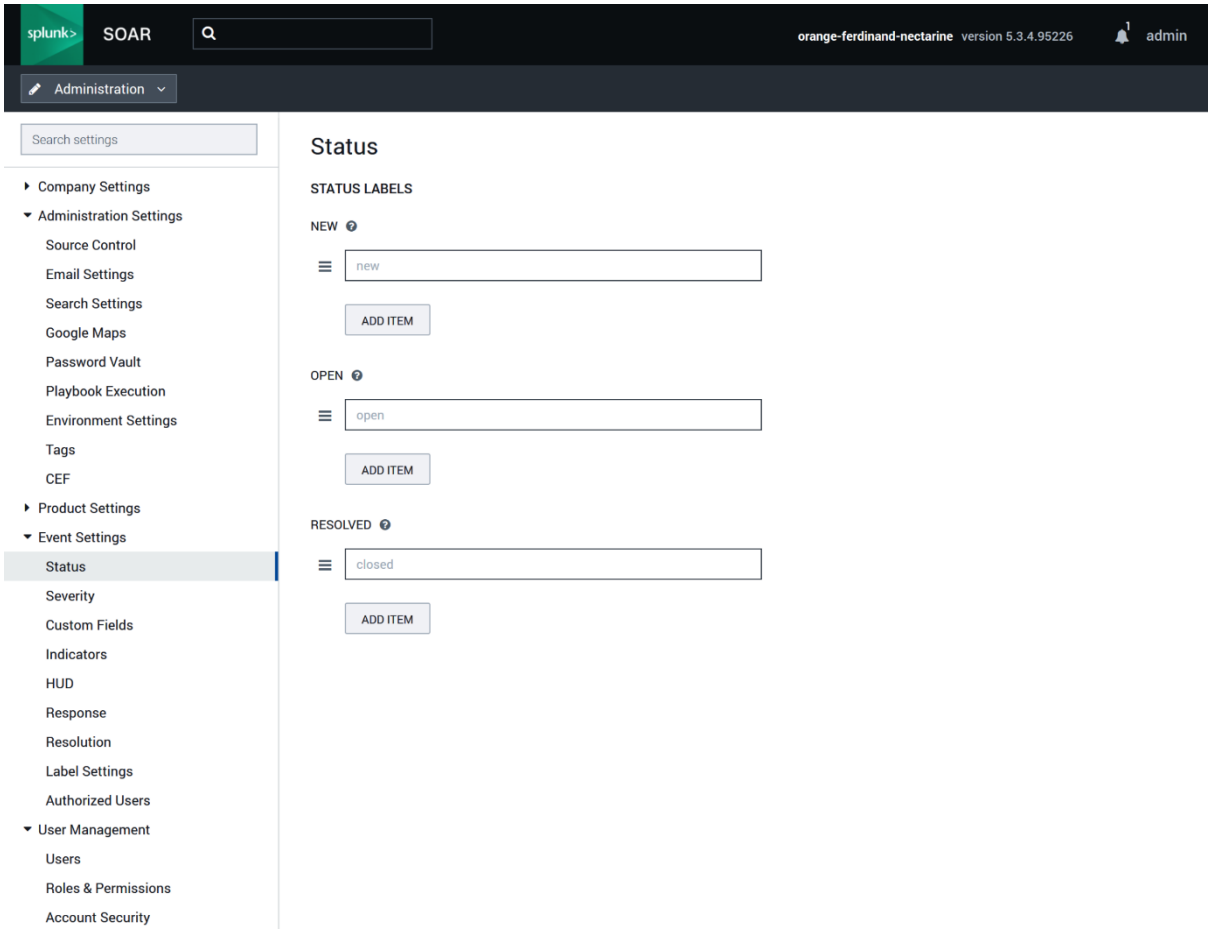

Timeline
Artifacts
Evidence
Files
Approvals
Reports
ACTION
PLAYBOOK
REPORT
Reports
GENERATED
NAME
OWNER
DOWNLOAD
a few seconds ago
Brute Force Attack on hector
admin
1
Show
5

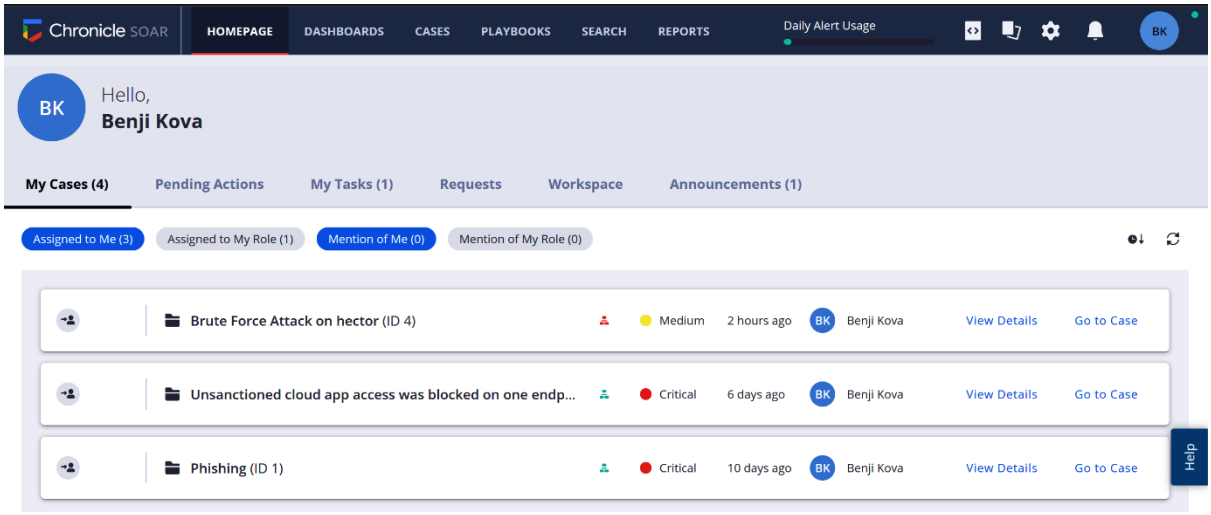

splunk>
SOAR
Untitled
Discard Changes
Save
Settings
Add
EXECUTE ACTIONS
Action
Playbook
Code
Utility
PROCESS FILTERS
Filter
Decision
Format
HUMAN INPUT
Prompt
Start
ACTION
Unconfigured
PLAYBOOK
activedirectory_reset_password
Condition 2
Condition 2
ACTION
Unconfigured
CODE
code_2
End
Unconfigured
100%
Python Playbook Editor
Playbook Debugger

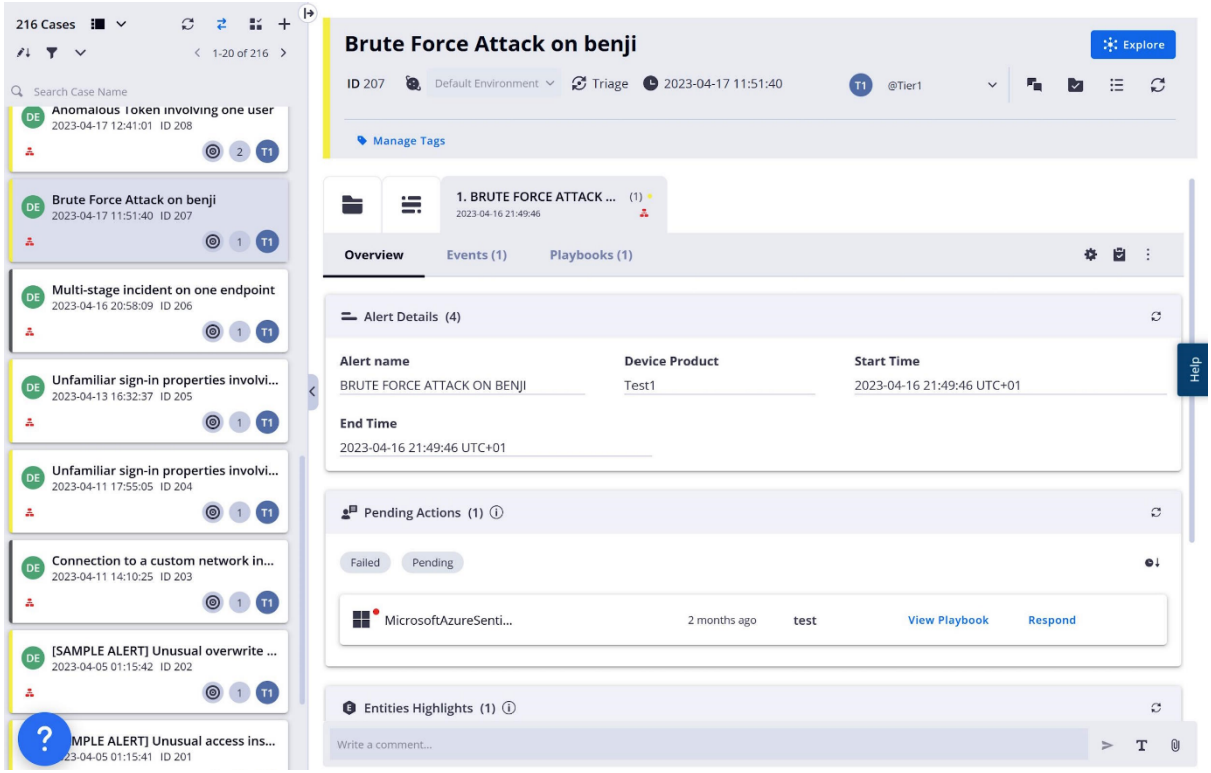

Timeline
Artifacts
Evidence
Files
Approvals
Reports
ACTION
PLAYBOOK
Prompts
OWNER
OWNER TYPE
NAME
START TIME
STATUS
RESPONSE
admin
User
prompt_1
Fri at 2:08 am
Answered
N/A
1
Show
5
Tasks
OWNER
OWNER TYPE
NAME
START TIME
STATUS
RESPONSE
admin
User
task_1
Fri at 2:38 am
expired
N/A
1
Show
5

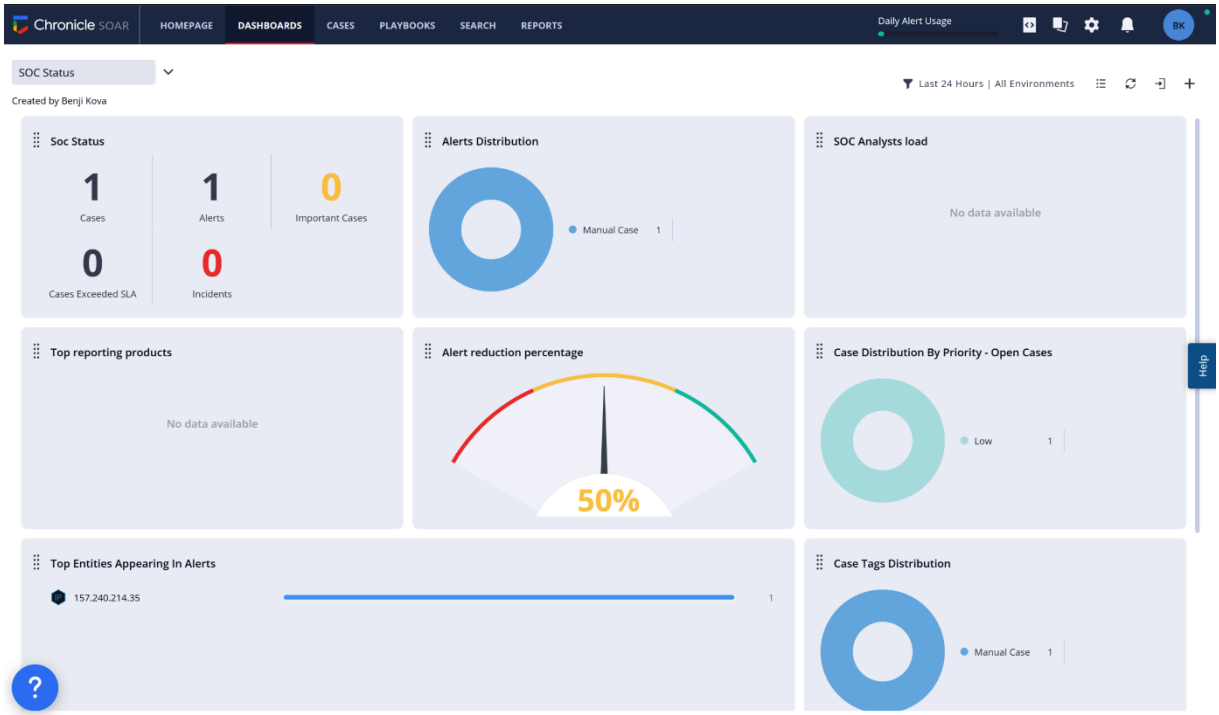

Run Action
By Type
By App
Task
Action Name
Name this action
Schedule
Action Types
investigate
correct
contain
generic
Asset Types
Search actions...
Assets
add incident comment
get incident
get incident alerts
get incident entities
list incidents
run query
update incident
CANCEL
LAUNCH

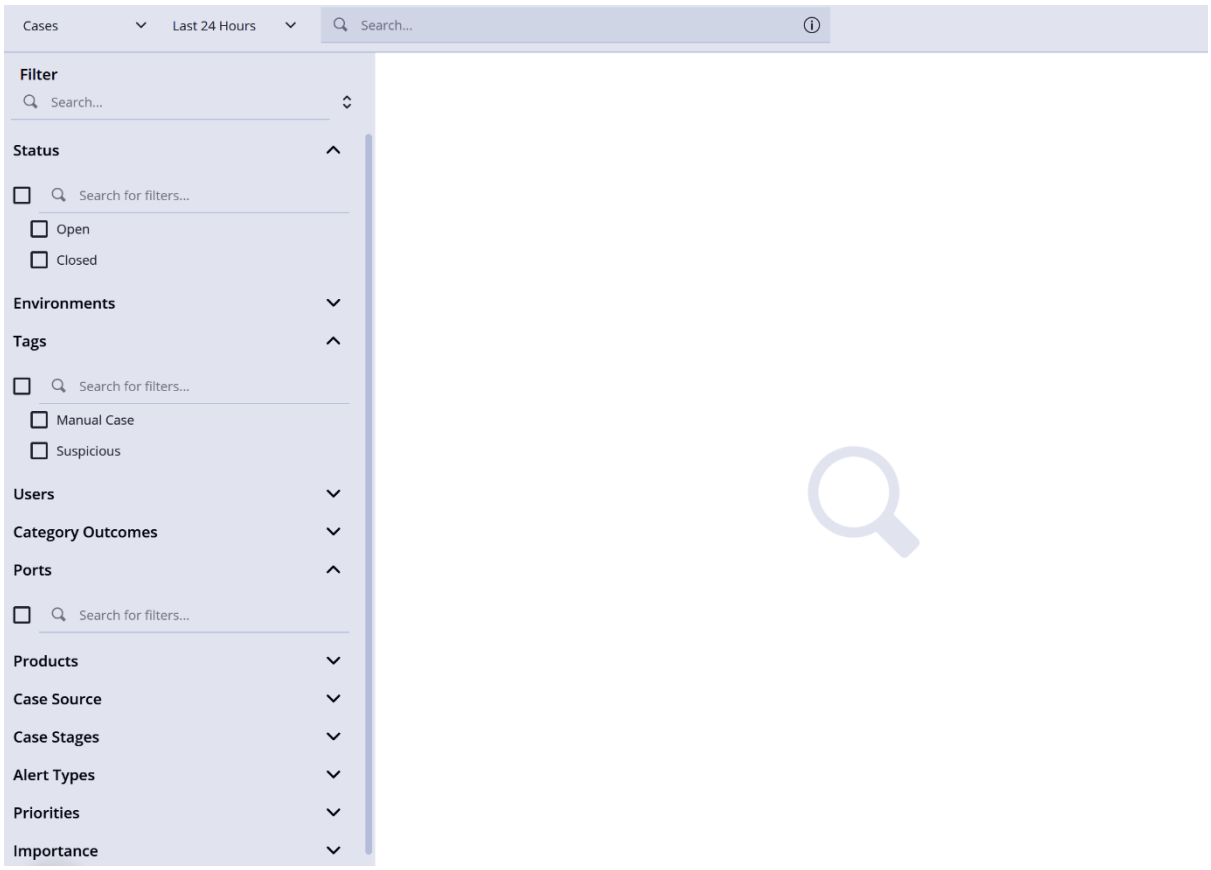

splunk> SOAR
orange-ferdinand-nectarine version 5.3.4.95226
admin
Reporting
All Types
Search reports
+ REPORT
Generated Reports
TYPE
REPORT NAME
GENERATED
OWNER
Event Report
Brute Force Attack on hector
Nov 15 2022 at 04:12 AM
admin
Executive Summary
general
Nov 11 2022 at 03:42 AM
admin
Executive Summary
test
Nov 08 2022 at 02:48 AM
admin
Case Report
RDP port scanning detected on WebinarMachine
Nov 08 2022 at 02:40 AM
admin
Case Report
RDP port scanning detected on WebinarMachine
Nov 08 2022 at 02:40 AM
admin
Event Report
Onboarding Demonstration Event
Nov 08 2022 at 01:59 AM
admin
1
Scheduled Reports
TYPE
REPORT NAME
SCHEDULE
NEXT RUN
OWNER
No reports have been scheduled

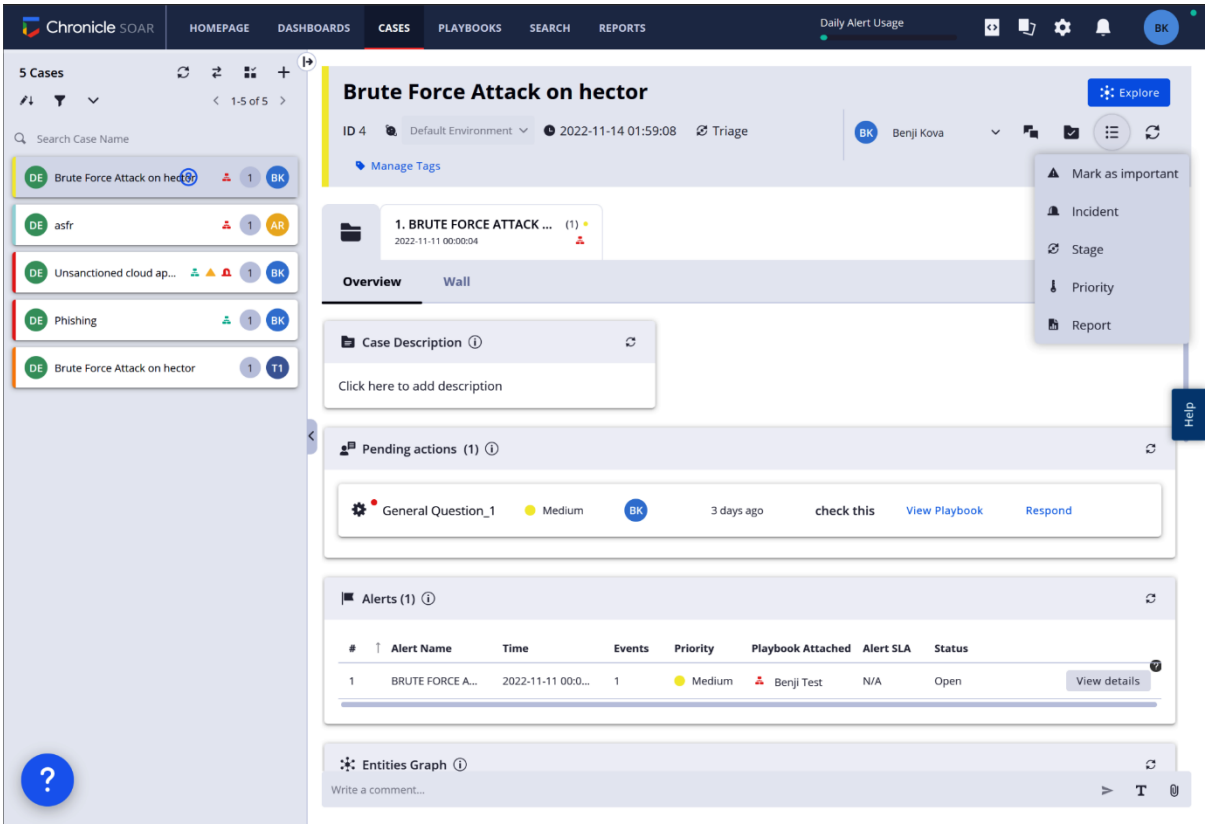

splunk> SOAR
orange-ferdinand-nectarine version 5.3.4.95226
admin
Administration
Search settings
Company Settings
Administration Settings
Source Control
Email Settings
Search Settings
Google Maps
Password Vault
Playbook Execution
Environment Settings
Tags
CEF
Product Settings
Event Settings
Status
Severity
Custom Fields
Indicators
HUD
Response
Resolution
Label Settings
Authorized Users
User Management
Users
Roles & Permissions
Account Security
Status
STATUS LABELS
NEW
new
ADD ITEM
OPEN
open
ADD ITEM
RESOLVED
closed
ADD ITEM

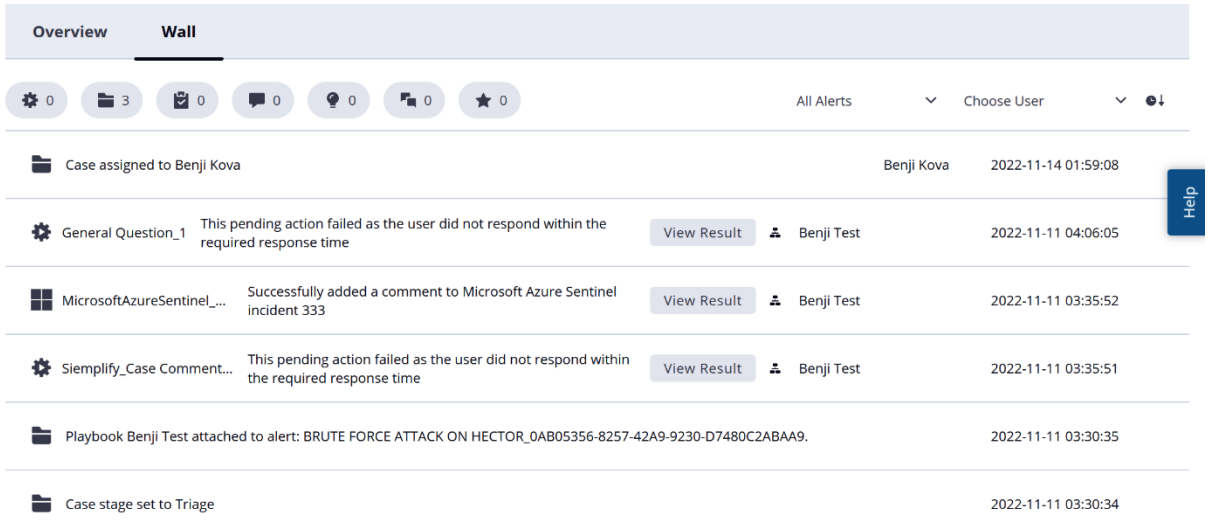

Chronicle SOAR
HOMEPAGE
DASHBOARDS
CASES
PLAYBOOKS
SEARCH
REPORTS
Daily Alert Usage
BK
Hello,
Benji Kova
My Cases (4)
Pending Actions
My Tasks (1)
Requests
Workspace
Announcements (1)
Assigned to Me (3)
Assigned to My Role (1)
Mention of Me (0)
Mention of My Role (0)
Brute Force Attack on hector (ID 4)
Medium
2 hours ago
Benji Kova
View Details
Go to Case
Unsanctioned cloud app access was blocked on one endp...
Critical
6 days ago
Benji Kova
View Details
Go to Case
Phishing (ID 1)
Critical
10 days ago
Benji Kova
View Details
Go to Case
Help

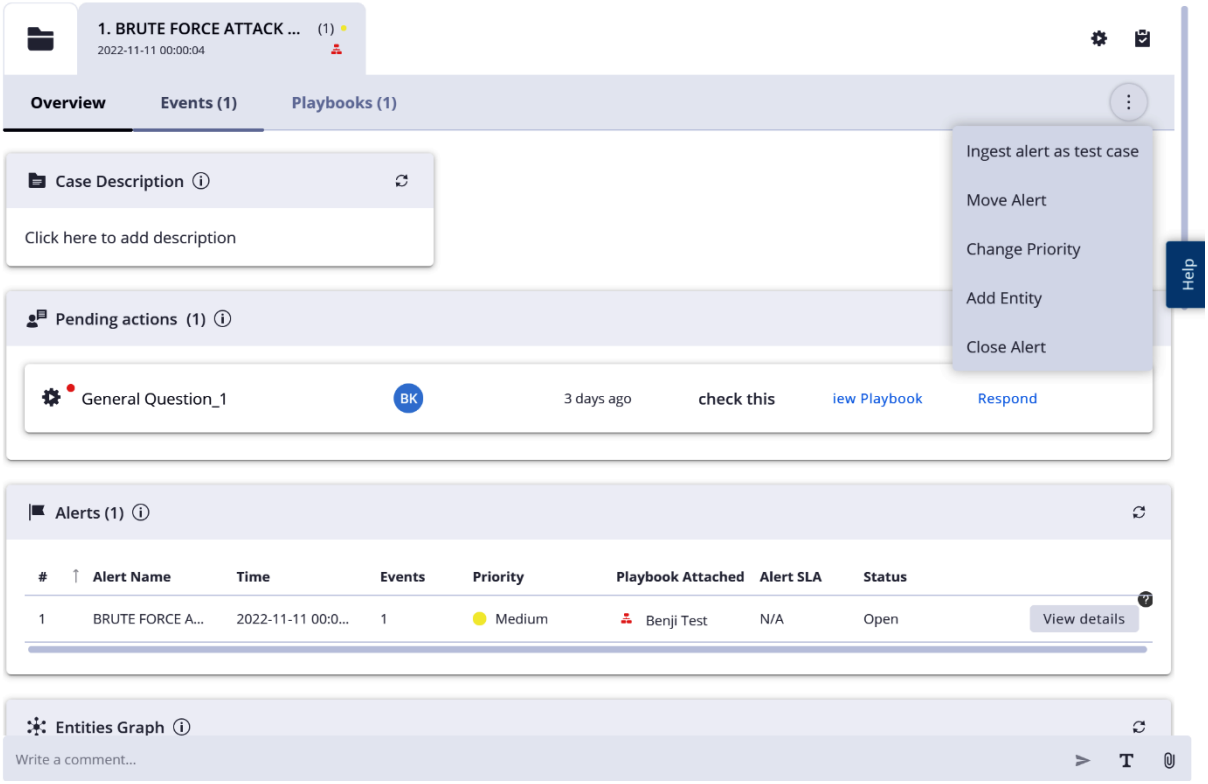

216 Cases
1-20 of 216
Search Case Name
Anomalous Token involving one user
2023-04-17 12:41:01 ID 208
Brute Force Attack on benji
2023-04-17 11:51:40 ID 207
Multi-stage incident on one endpoint
2023-04-16 20:58:09 ID 206
Unfamiliar sign-in properties involvi...
2023-04-13 16:32:37 ID 205
Unfamiliar sign-in properties involvi...
2023-04-11 17:55:05 ID 204
Connection to a custom network in...
2023-04-11 14:10:25 ID 203
[SAMPLE ALERT] Unusual overwrite ...
2023-04-05 01:15:42 ID 202
MPLE ALERT] Unusual access ins...
23-04-05 01:15:41 ID 201
Brute Force Attack on benji
Explore
ID 207
Default Environment
Triage
2023-04-17 11:51:40
@Tier1
Manage Tags
1. BRUTE FORCE ATTACK ... (1)
2023-04-16 21:49:46
Overview
Events (1)
Playbooks (1)
Alert Details (4)
Alert name
BRUTE FORCE ATTACK ON BENJI
Device Product
Test1
Start Time
2023-04-16 21:49:46 UTC+01
End Time
2023-04-16 21:49:46 UTC+01
Pending Actions (1)
Failed
Pending
MicrosoftAzureSenti...
2 months ago
test
View Playbook
Respond
Entities Highlights (1)
Write a comment...
Help

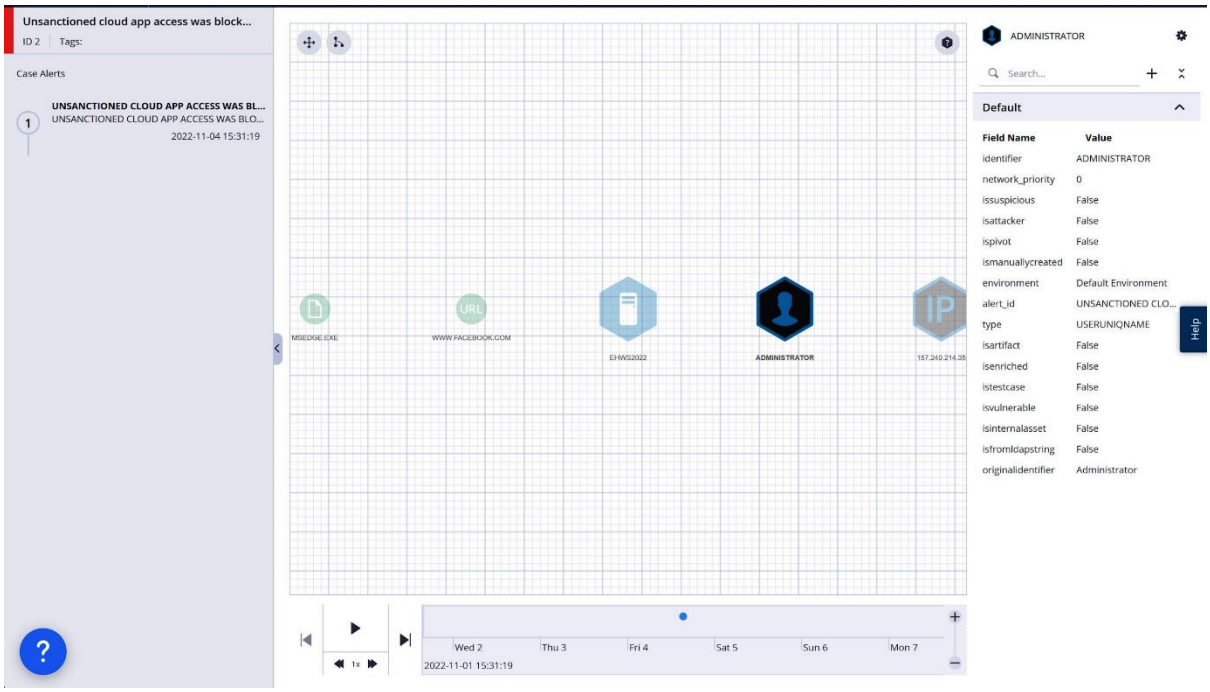

Chronicle SOAR
HOMEPAGE
DASHBOARDS
CASES
PLAYBOOKS
SEARCH
REPORTS
Daily Alert Usage
BK
SOC Status
Created by Benji Kova
Last 24 Hours | All Environments
Soc Status
1
Cases
1
Alerts
0
Important Cases
0
Cases Exceeded SLA
0
Incidents
Alerts Distribution
Manual Case 1
SOC Analysts load
No data available
Top reporting products
No data available
Alert reduction percentage
50%
Case Distribution By Priority - Open Cases
Low 1
Help
Top Entities Appearing In Alerts
157.240.214.35
1
Case Tags Distribution
Manual Case 1

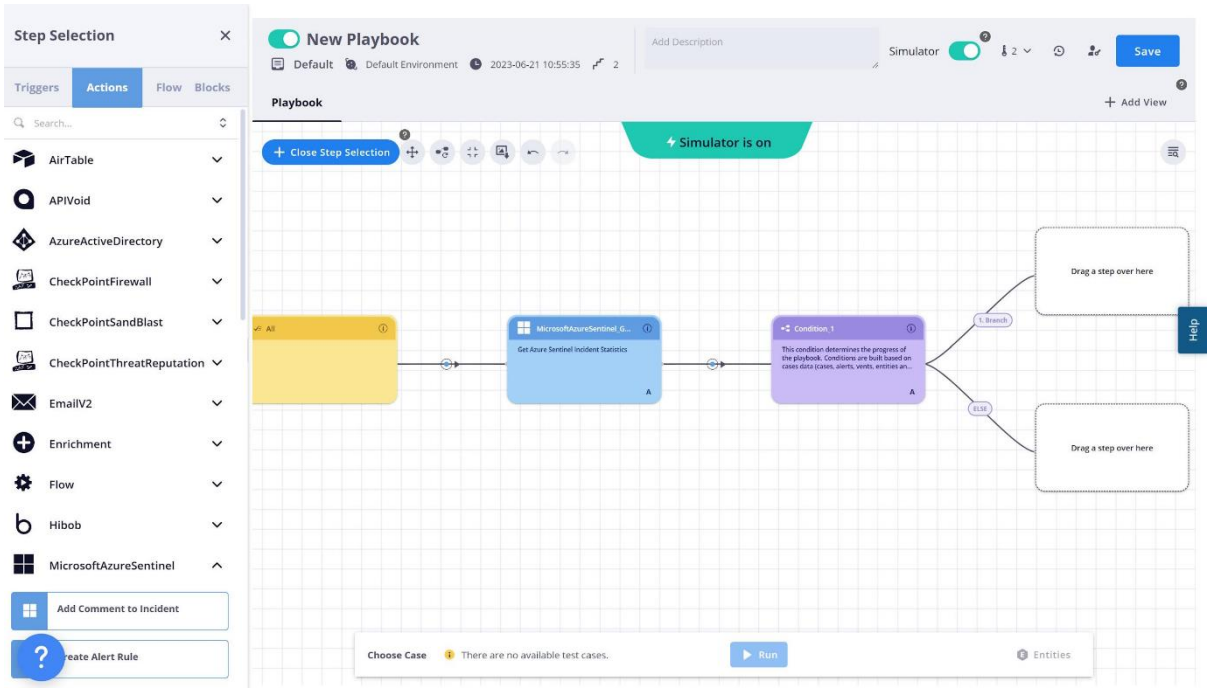

Cases
Last 24 Hours
Search...
Filter
Search...
Status
Search for filters...
Open
Closed
Environments
Tags
Search for filters...
Manual Case
Suspicious
Users
Category Outcomes
Ports
Search for filters...
Products
Case Source
Case Stages
Alert Types
Priorities
Importance

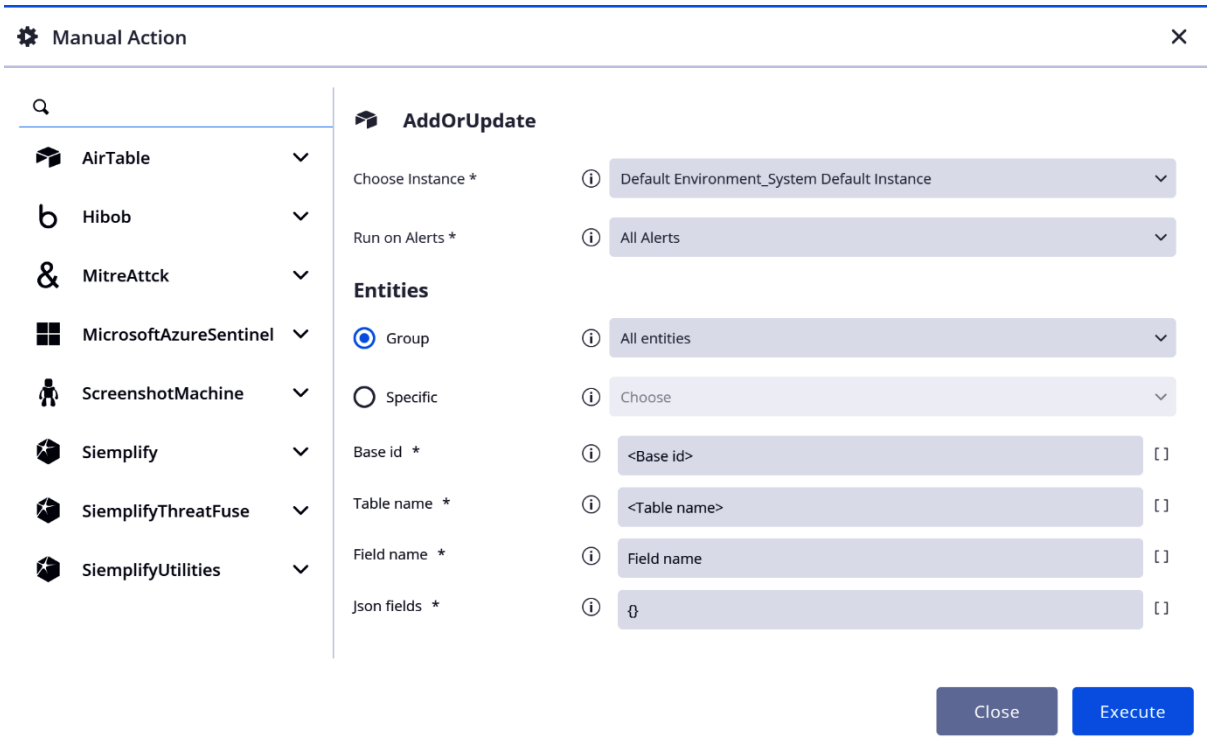

Chronicle SOAR
HOMEPAGE
DASHBOARDS
CASES
PLAYBOOKS
SEARCH
REPORTS
Daily Alert Usage
5 Cases
1-5 of 5
Search Case Name
Brute Force Attack on hector
asfr
Unsanctioned cloud ap...
Phishing
Brute Force Attack on hector
Brute Force Attack on hector
Explore
ID 4
Default Environment
2022-11-14 01:59:08
Triage
Benji Kova
Manage Tags
Mark as important
Incident
Stage
Priority
Report
1. BRUTE FORCE ATTACK ... (1)
2022-11-11 00:00:04
Overview
Wall
Case Description
Click here to add description
Pending actions (1)
General Question_1
Medium
3 days ago
check this
View Playbook
Respond
Alerts (1)
Alert Name Time Events Priority Playbook Attached Alert SLA Status
1 BRUTE FORCE A... 2022-11-11 00:0... 1 Medium Benji Test N/A Open
View details
Entities Graph
Write a comment...
Help

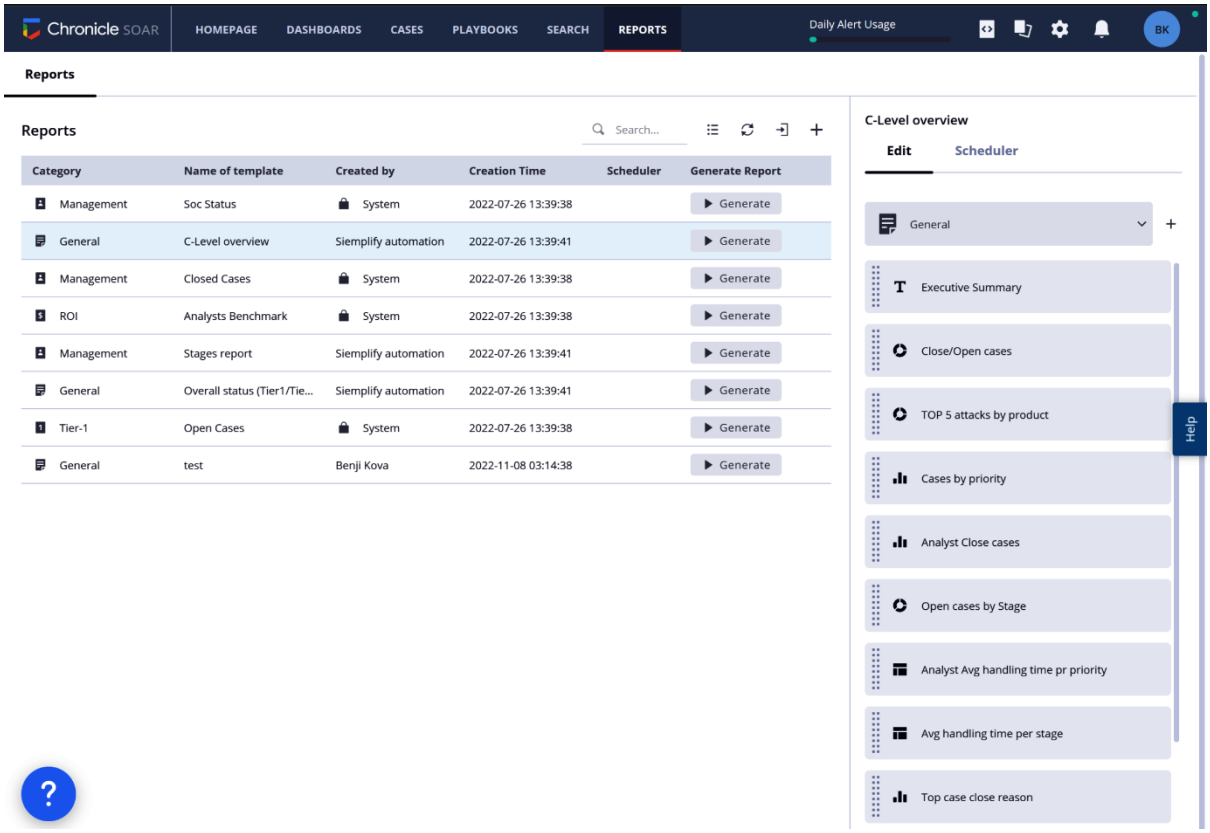

Overview
Wall
0
3
0
0
0
0
0
All Alerts
Choose User
Case assigned to Benji Kova
Benji Kova
2022-11-14 01:59:08
General Question_1
This pending action failed as the user did not respond within the required response time
View Result
Benji Test
2022-11-11 04:06:05
MicrosoftAzureSentinel_...
Successfully added a comment to Microsoft Azure Sentinel incident 333
View Result
Benji Test
2022-11-11 03:35:52
Siemplify_Case Comment...
This pending action failed as the user did not respond within the required response time
View Result
Benji Test
2022-11-11 03:35:51
Playbook Benji Test attached to alert: BRUTE FORCE ATTACK ON HECTOR_0AB05356-8257-42A9-9230-D7480C2ABAA9.
2022-11-11 03:30:35
Case stage set to Triage
2022-11-11 03:30:34
Help

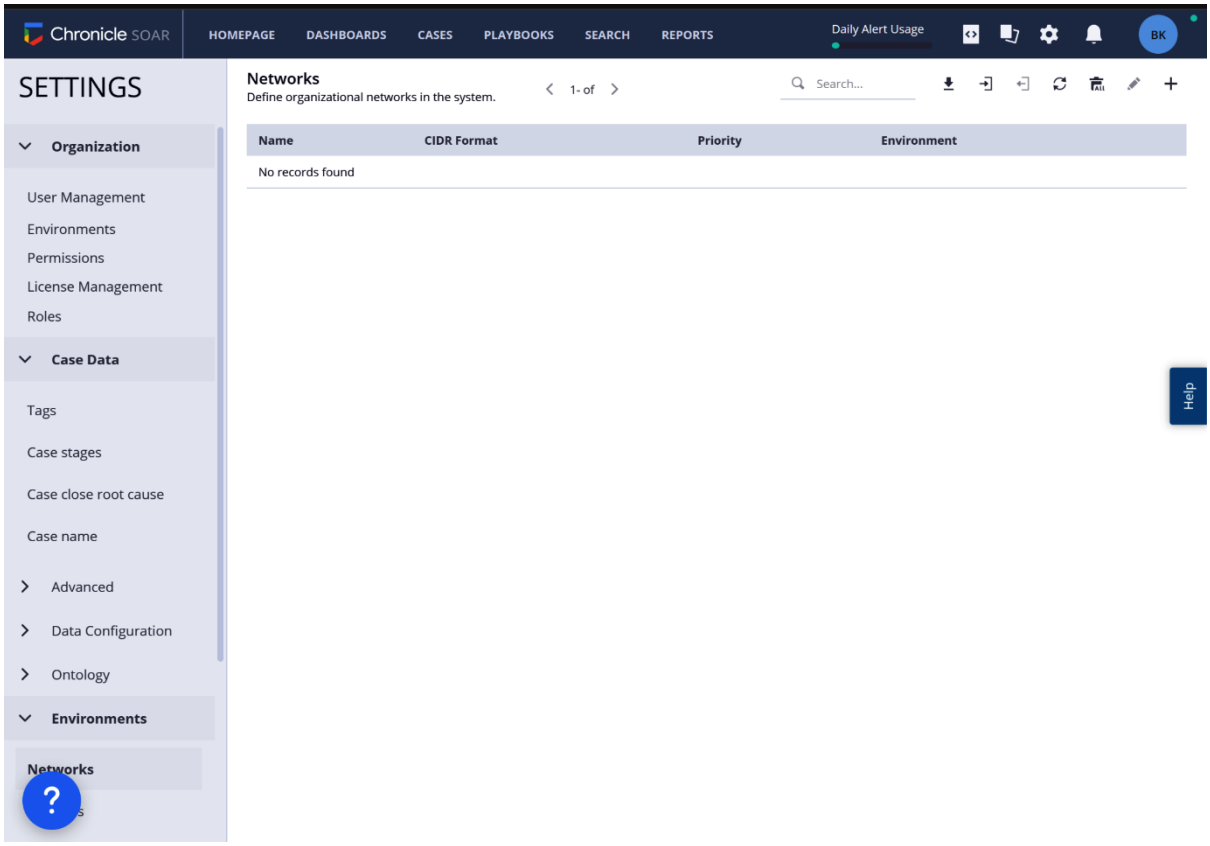

1. BRUTE FORCE ATTACK ... (1)
2022-11-11 00:00:04
Overview
Events (1)
Playbooks (1)
Ingest alert as test case
Move Alert
Change Priority
Add Entity
Close Alert
Case Description
Click here to add description
Pending actions (1)
General Question_1
BK
3 days ago
check this
iew Playbook
Respond
Alerts (1)
Alert Name Time Events Priority Playbook Attached Alert SLA Status
1 BRUTE FORCE A... 2022-11-11 00:0... 1 Medium Benji Test N/A Open View details
Entities Graph
Write a comment...
Help


Unsanctioned cloud app access was block...
ID 2 Tags:
Case Alerts
UNSANCTIONED CLOUD APP ACCESS WAS BL...
UNSANCTIONED CLOUD APP ACCESS WAS BLO...
2022-11-04 15:31:19
ADMINISTRATOR
Default
Field Name Value
identifier ADMINISTRATOR
network_priority 0
issuspicious False
isattacker False
ispivot False
ismanuallycreated False
environment Default Environment
alert_id UNSANCTIONED CLO...
type USERUNIQNAME
isartifact False
isenriched False
istestcase False
isvulnerable False
isinternalasset False
isfromldapstring False
originalidentifier Administrator
MSEDGE.EXE
WWW.FACEBOOK.COM
EHWS2022
ADMINISTRATOR
Wed 2
Thu 3
Fri 4
Sat 5
Sun 6
Mon 7
2022-11-01 15:31:19
Help

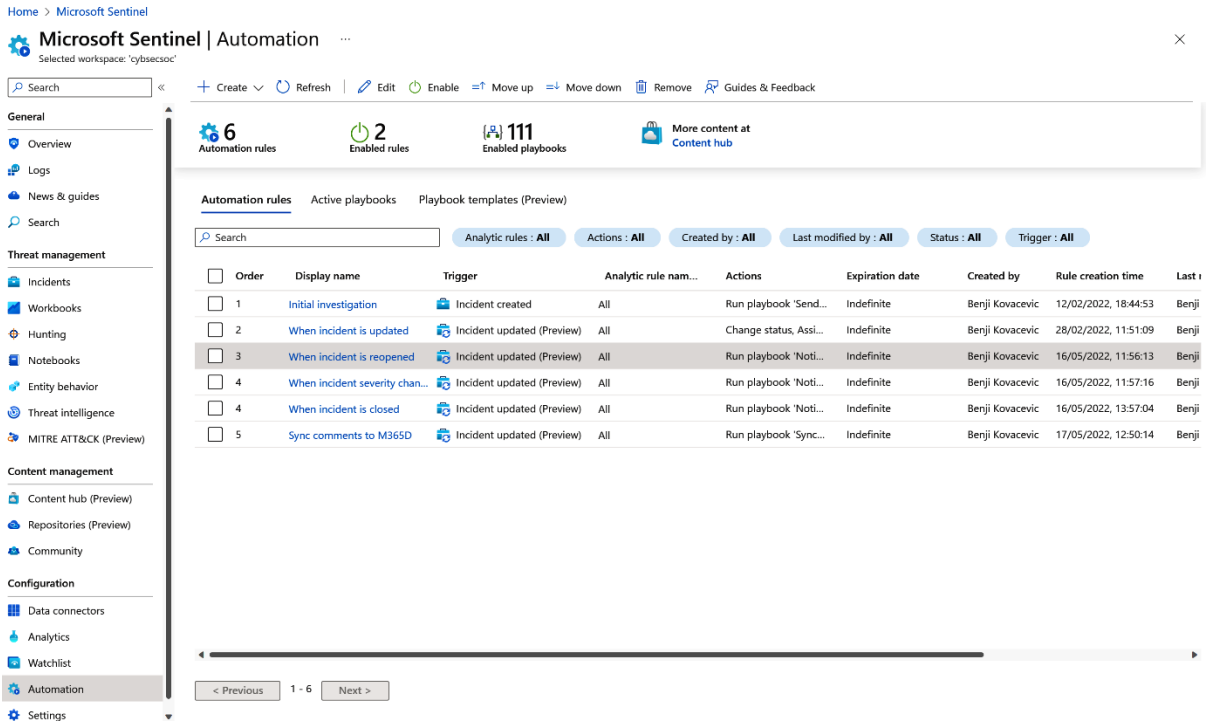

Step Selection
Triggers
Actions
Flow
Blocks
Search...
AirTable
APIVoid
AzureActiveDirectory
CheckPointFirewall
CheckPointSandBlast
CheckPointThreatReputation
EmailV2
Enrichment
Flow
Hibob
MicrosoftAzureSentinel
Add Comment to Incident
New Playbook
Default
Default Environment
2023-06-21 10:55:35
Add Description
Simulator
Save
Playbook
Add View
Close Step Selection
Simulator is on
All
MicrosoftAzureSentinel_G...
Get Azure Sentinel Incident Statistics
Condition_1
This condition determines the progress of the playbook. Conditions are built based on cases data (cases, alerts, vents, entities an...
1. Branch
ELSE
Drag a step over here
Drag a step over here
Help
Choose Case
There are no available test cases.
Run
Entities

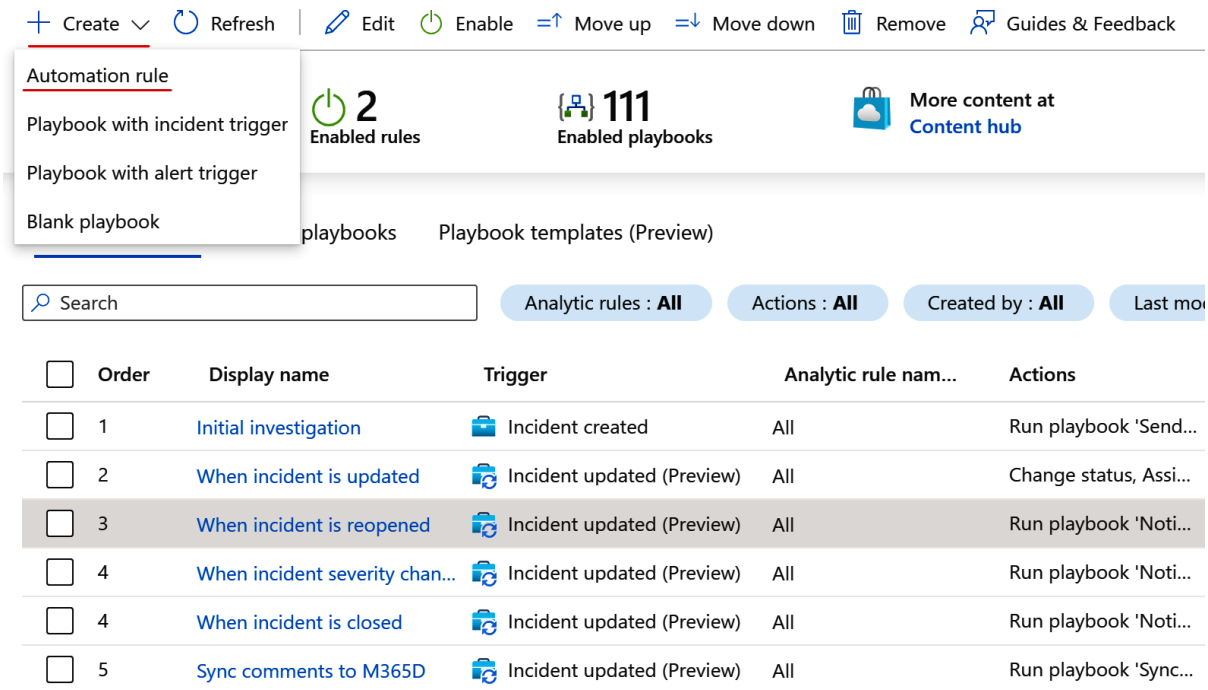

Manual Action
AirTable
Hibob
MitreAttck
MicrosoftAzureSentinel
ScreenshotMachine
Siemplify
SiemplifyThreatFuse
SiemplifyUtilities
AddOrUpdate
Choose Instance *
Default Environment_System Default Instance
Run on Alerts *
All Alerts
Entities
Group
All entities
Specific
Choose
Base id *
<Base id>
Table name *
<Table name>
Field name *
Field name
Json fields *
{}
Close
Execute


Chronicle SOAR
HOMEPAGE
DASHBOARDS
CASES
PLAYBOOKS
SEARCH
REPORTS
Daily Alert Usage
BK
Reports
Reports
Search...
Category
Name of template
Created by
Creation Time
Scheduler
Generate Report
Management
Soc Status
System
2022-07-26 13:39:38
Generate
General
C-Level overview
Siemplify automation
2022-07-26 13:39:41
Generate
Management
Closed Cases
System
2022-07-26 13:39:38
Generate
ROI
Analysts Benchmark
System
2022-07-26 13:39:38
Generate
Management
Stages report
Siemplify automation
2022-07-26 13:39:41
Generate
General
Overall status (Tier1/Tie...
Siemplify automation
2022-07-26 13:39:41
Generate
Tier-1
Open Cases
System
2022-07-26 13:39:38
Generate
General
test
Benji Kova
2022-11-08 03:14:38
Generate
C-Level overview
Edit
Scheduler
General
Executive Summary
Close/Open cases
TOP 5 attacks by product
Cases by priority
Analyst Close cases
Open cases by Stage
Analyst Avg handling time pr priority
Avg handling time per stage
Top case close reason
Help


Chronicle SOAR
HOMEPAGE
DASHBOARDS
CASES
PLAYBOOKS
SEARCH
REPORTS
Daily Alert Usage
BK
SETTINGS
Organization
User Management
Environments
Permissions
License Management
Roles
Case Data
Tags
Case stages
Case close root cause
Case name
Advanced
Data Configuration
Ontology
Environments
Networks
Networks
Define organizational networks in the system.
1- of
Search...
Name
CIDR Format
Priority
Environment
No records found
Help

Chapter 5: Introducing Microsoft Sentinel Automation





Create new automation rule

Automation rule name

Trigger

When incident is created

Conditions

If

Analytic rule name | Contains | All

+ Add

Actions

+ Add action

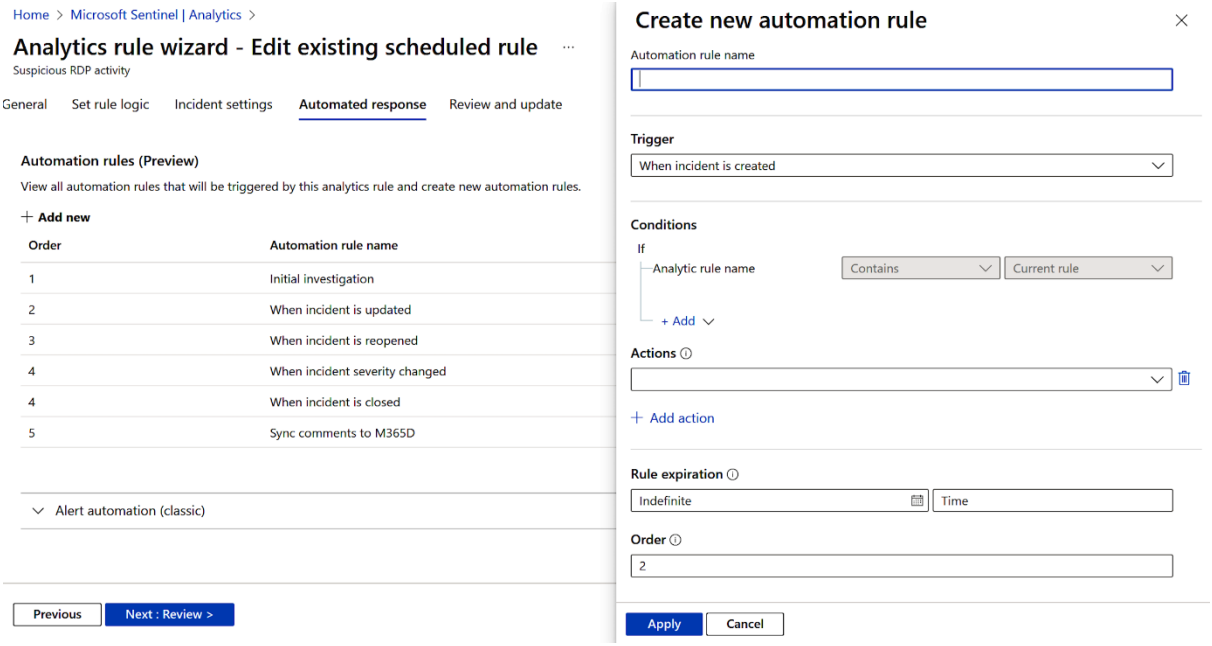
Rule expiration

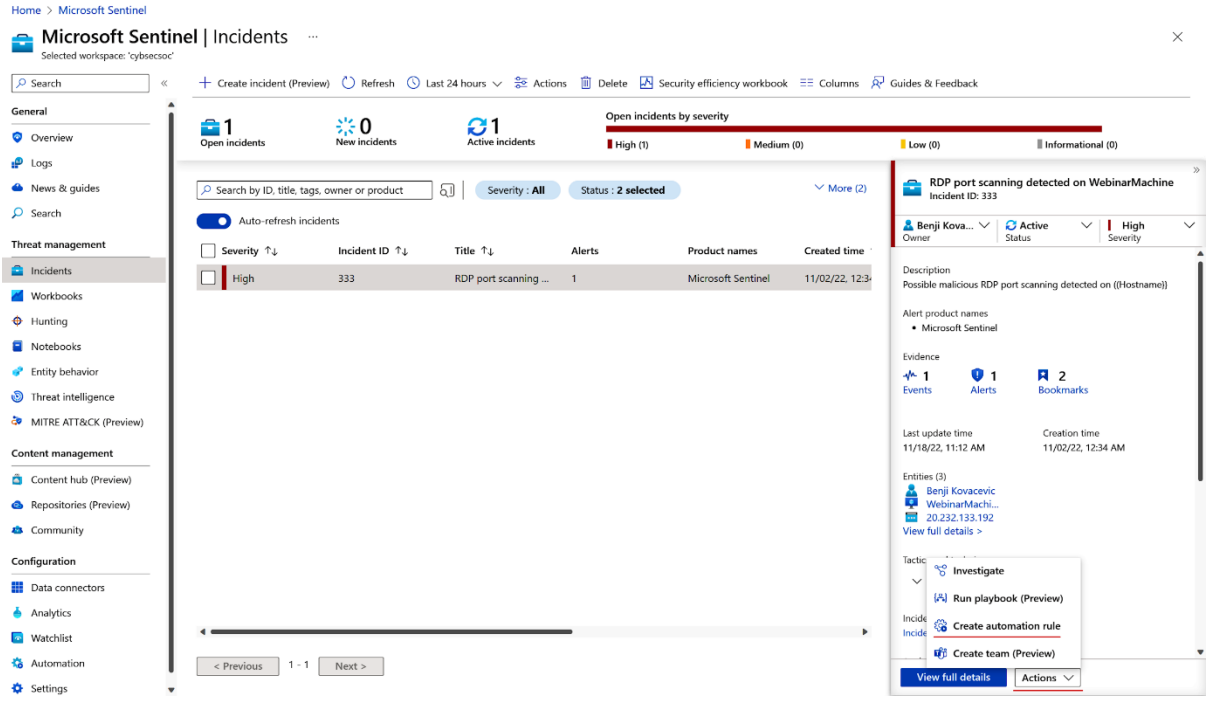
Indefinite | Time

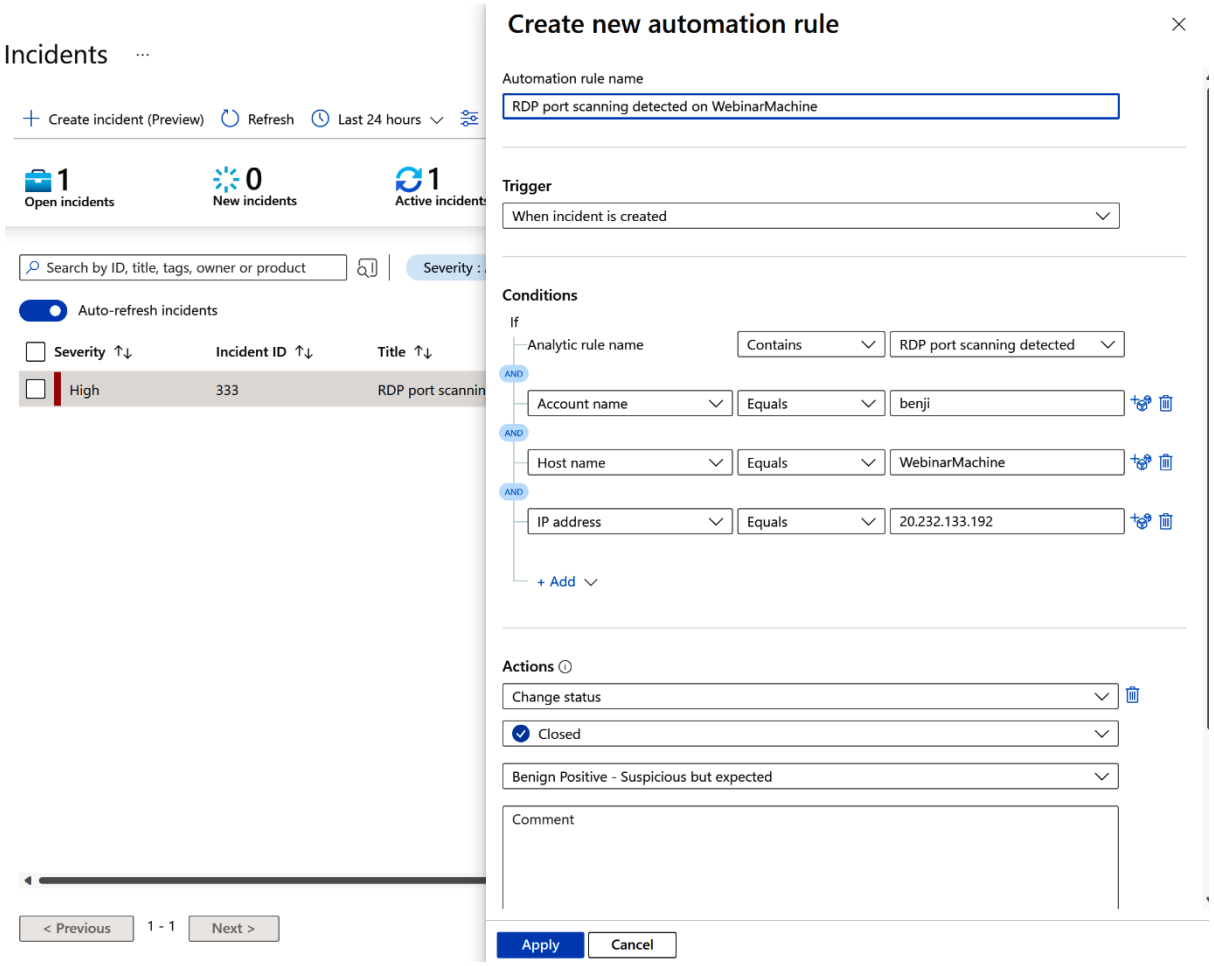
Order

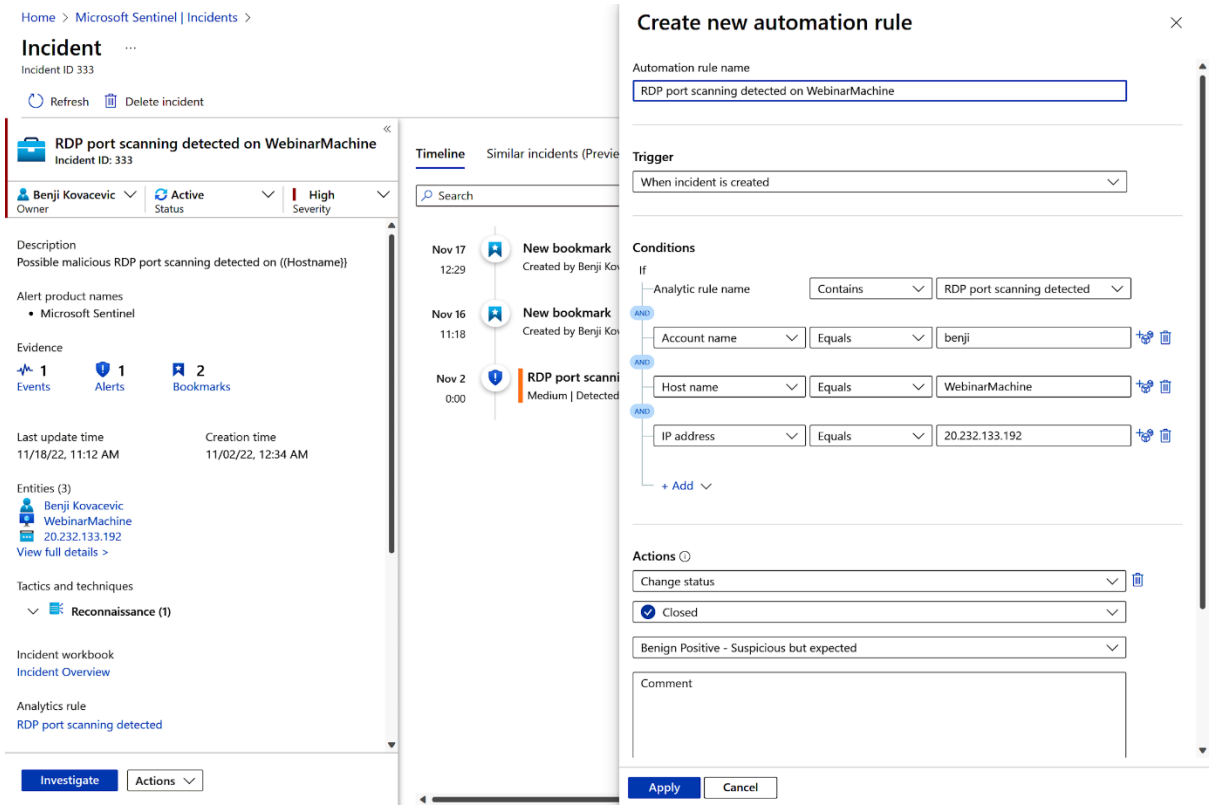
2

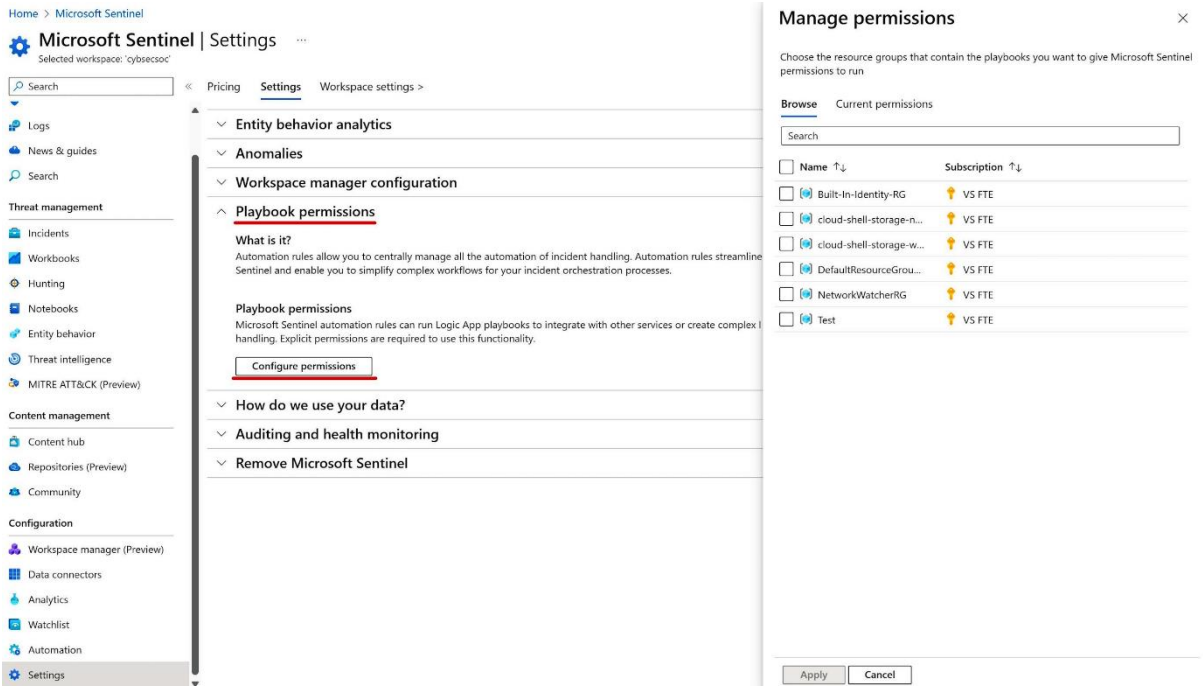
Apply | Cancel


Home > Microsoft Sentinel | Analytics >
Analytics rule wizard - Edit existing scheduled rule
Suspicious RDP activity
General
Set rule logic
Incident settings
Automated response
Review and update
Automation rules (Preview)
View all automation rules that will be triggered by this analytics rule and create new automation rules.
Add new
Order
Automation rule name
1
Initial investigation
2
When incident is updated
3
When incident is reopened
4
When incident severity changed
4
When incident is closed
5
Sync comments to M365D
Alert automation (classic)
Previous
Next : Review >
Create new automation rule
Automation rule name
Trigger
When incident is created
Conditions
If
Analytic rule name
Contains
Current rule
+ Add
Actions
Add action
Rule expiration
Indefinite
Time
Order
2
Apply
Cancel


Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'cybsecsoc'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
1
Open incidents
0
New incidents
1
Active incidents
Open incidents by severity
High (1)
Medium (0)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
More (2)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
High
333
RDP port scanning ...
1
Microsoft Sentinel
11/02/22, 12:3
< Previous
1 - 1
Next >
RDP port scanning detected on WebinarMachine
Incident ID: 333
Benji Kova...
Owner
Active
Status
High
Severity
Description
Possible malicious RDP port scanning detected on {{Hostname}}
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
2
Bookmarks
Last update time
11/18/22, 11:12 AM
Creation time
11/02/22, 12:34 AM
Entities (3)
Benji Kovacevic
WebinarMachi...
20.232.133.192
View full details >
Investigate
Run playbook (Preview)
Create automation rule
Create team (Preview)
View full details
Actions


Incidents
Create incident (Preview)
Refresh
Last 24 hours
1
Open incidents
0
New incidents
1
Active incidents
Search by ID, title, tags, owner or product
Severity :
Auto-refresh incidents
Severity
Incident ID
Title
High
333
RDP port scannin
< Previous
1 - 1
Next >
Create new automation rule
Automation rule name
RDP port scanning detected on WebinarMachine
Trigger
When incident is created
Conditions
If
Analytic rule name
Contains
RDP port scanning detected
AND
Account name
Equals
benji
AND
Host name
Equals
WebinarMachine
AND
IP address
Equals
20.232.133.192
+ Add
Actions
Change status
Closed
Benign Positive - Suspicious but expected
Comment
Apply
Cancel


Home > Microsoft Sentinel | Incidents >
Incident
Incident ID 333
Refresh
Delete incident
RDP port scanning detected on WebinarMachine
Incident ID: 333
Benji Kovacevic
Owner
Active
Status
High
Severity
Description
Possible malicious RDP port scanning detected on {{Hostname}}
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
2
Bookmarks
Last update time
11/18/22, 11:12 AM
Creation time
11/02/22, 12:34 AM
Entities (3)
Benji Kovacevic
WebinarMachine
20.232.133.192
View full details >
Tactics and techniques
Reconnaissance (1)
Incident workbook
Incident Overview
Analytics rule
RDP port scanning detected
Investigate
Actions
Timeline
Similar incidents (Previe
Search
Nov 17
12:29
New bookmark
Created by Benji Ko
Nov 16
11:18
New bookmark
Created by Benji Ko
Nov 2
0:00
RDP port scanni
Medium | Detected
Create new automation rule
Automation rule name
RDP port scanning detected on WebinarMachine
Trigger
When incident is created
Conditions
If
Analytic rule name
Contains
RDP port scanning detected
AND
Account name
Equals
benji
AND
Host name
Equals
WebinarMachine
AND
IP address
Equals
20.232.133.192
+ Add
Actions
Change status
Closed
Benign Positive - Suspicious but expected
Comment
Apply
Cancel



Trigger

When incident is created

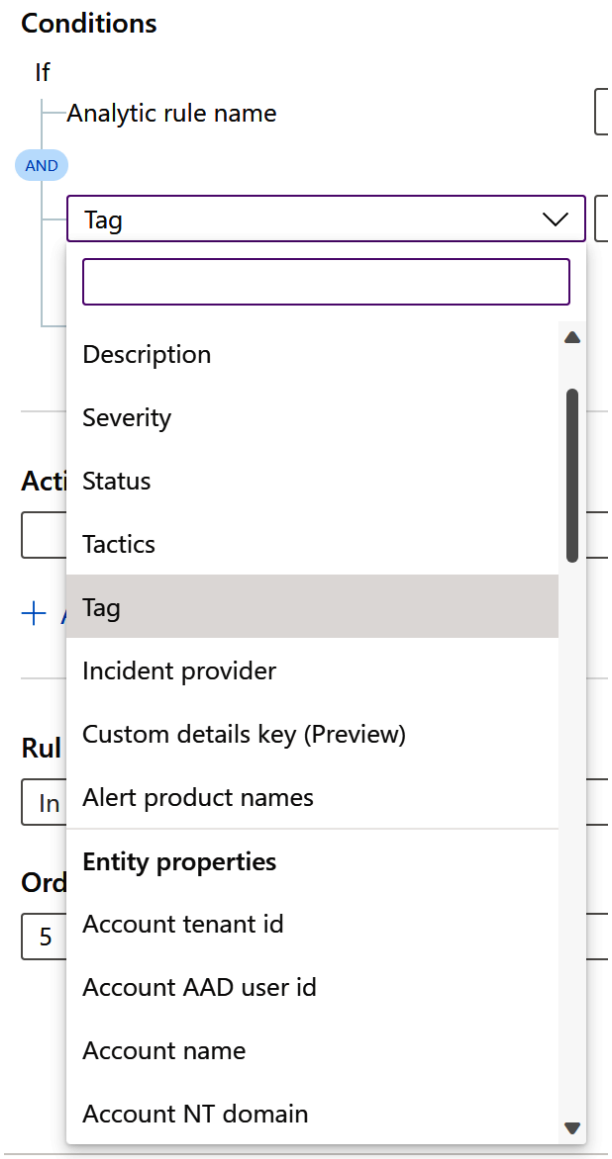
When incident is created

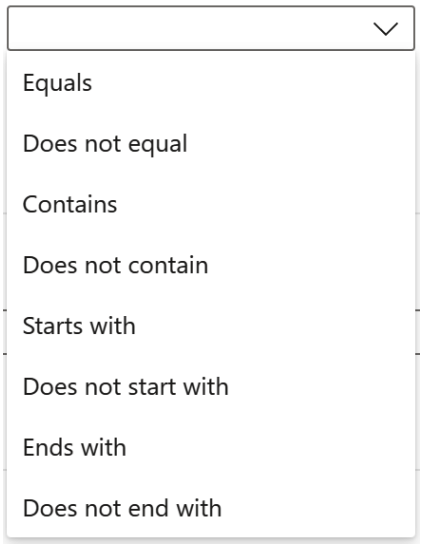
When incident is updated (Preview)

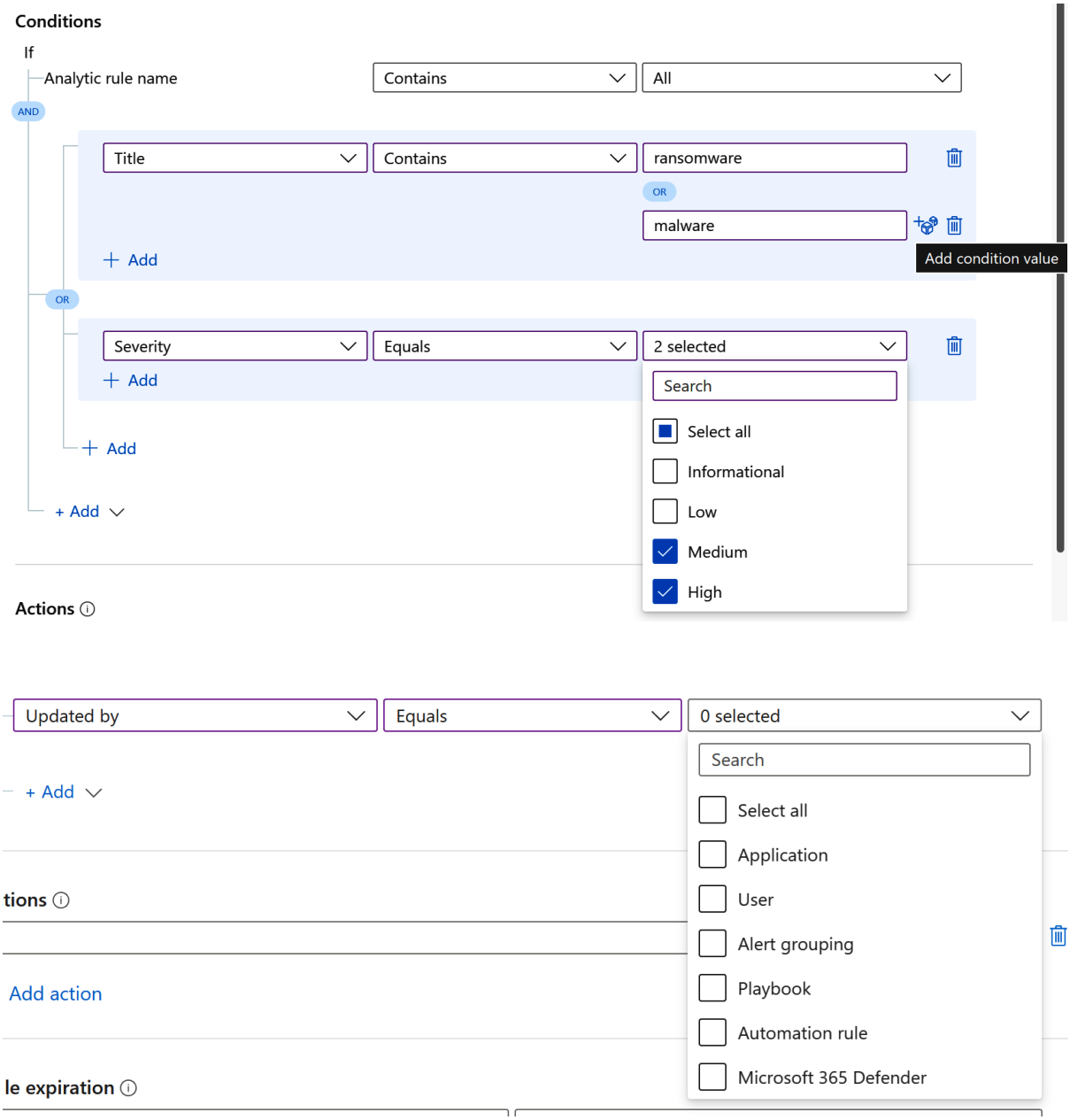
When alert is created (Preview)

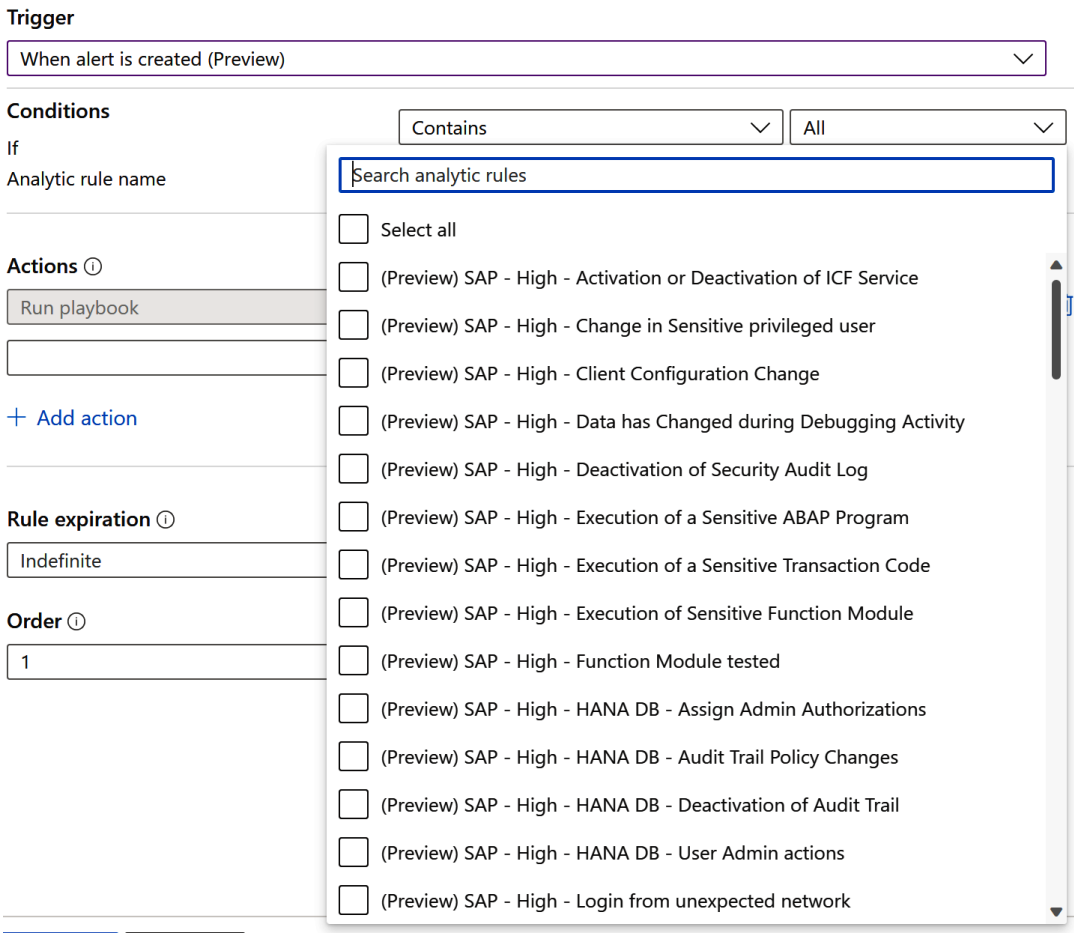
Conditions

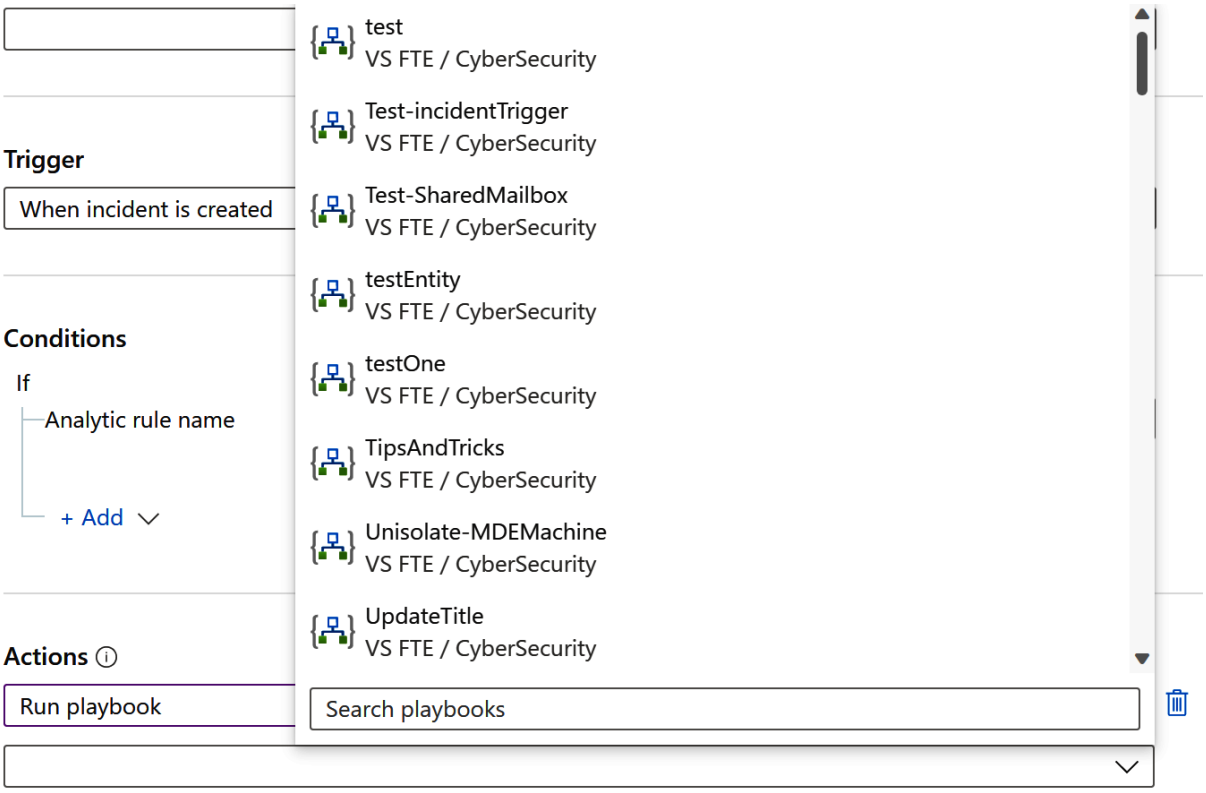
If

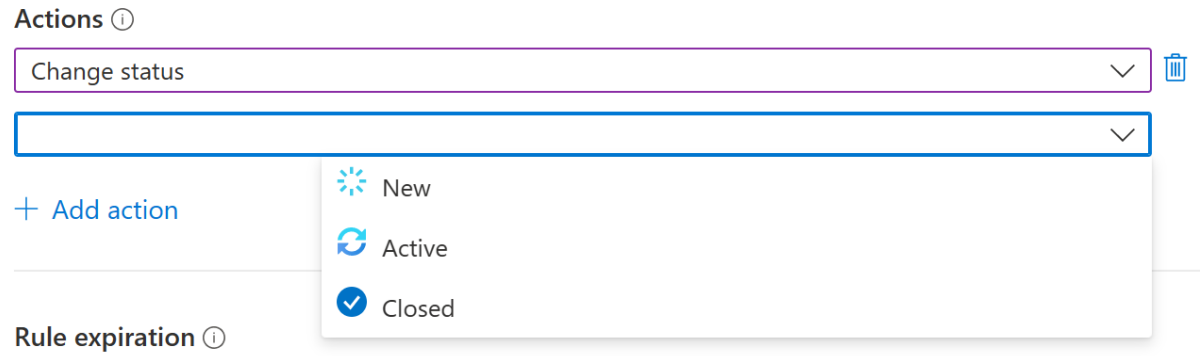

Conditions
If
Analytic rule name
AND
Tag
Description
Severity
Status
Tactics
Tag
Incident provider
Custom details key (Preview)
Alert product names
Entity properties
Account tenant id
Account AAD user id
Account name
Account NT domain

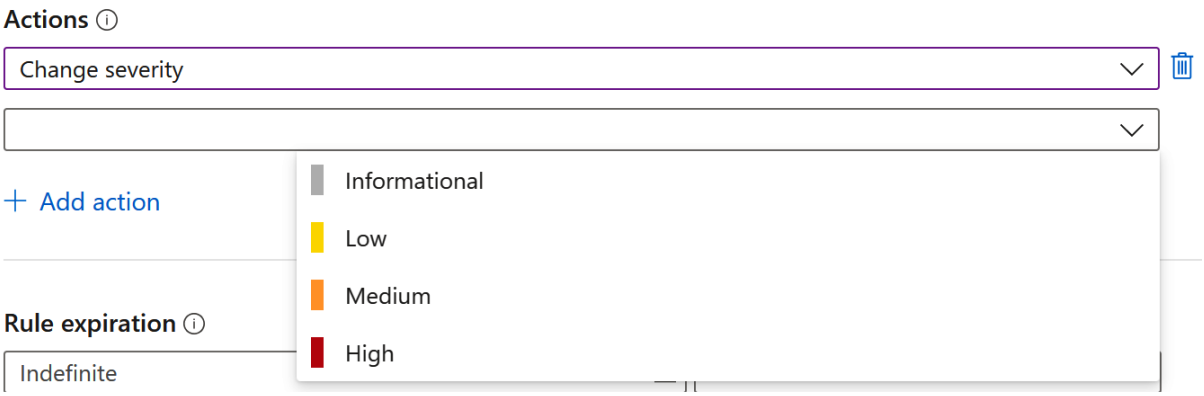

Equals
Does not equal
Contains
Does not contain
Starts with
Does not start with
Ends with
Does not end with

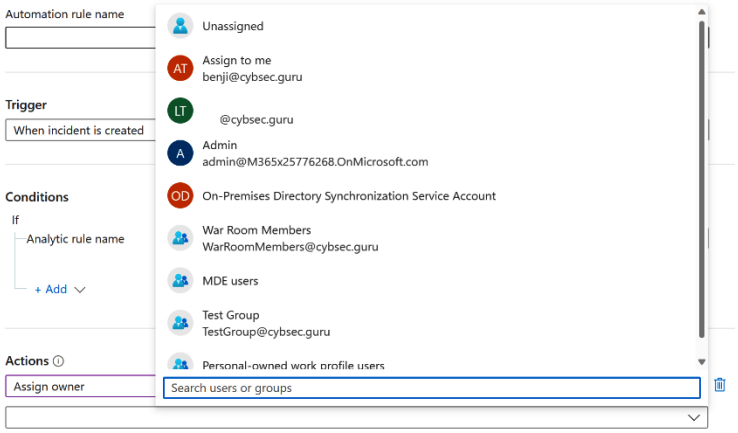

Conditions
If
Analytic rule name
Contains
All
AND
Title
Contains
ransomware
OR
malware
Add condition value
Add
OR
Severity
Equals
2 selected
Search
Select all
Informational
Low
Medium
High
Add
Add
+ Add
Actions
Updated by
Equals
0 selected
Search
Select all
Application
User
Alert grouping
Playbook
Automation rule
Microsoft 365 Defender
+ Add
tions
Add action
le expiration

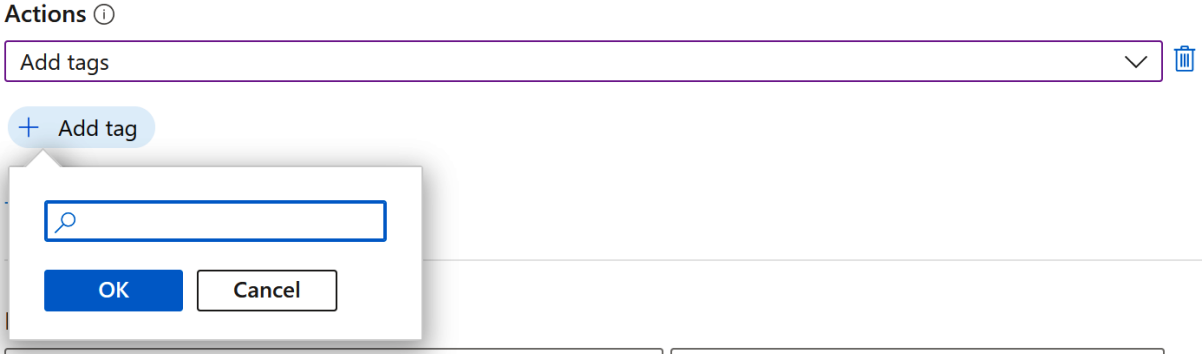

Trigger
When alert is created (Preview)
Conditions
If
Analytic rule name
Contains
All
Search analytic rules
Select all
(Preview) SAP - High - Activation or Deactivation of ICF Service
(Preview) SAP - High - Change in Sensitive privileged user
(Preview) SAP - High - Client Configuration Change
(Preview) SAP - High - Data has Changed during Debugging Activity
(Preview) SAP - High - Deactivation of Security Audit Log
(Preview) SAP - High - Execution of a Sensitive ABAP Program
(Preview) SAP - High - Execution of a Sensitive Transaction Code
(Preview) SAP - High - Execution of Sensitive Function Module
(Preview) SAP - High - Function Module tested
(Preview) SAP - High - HANA DB - Assign Admin Authorizations
(Preview) SAP - High - HANA DB - Audit Trail Policy Changes
(Preview) SAP - High - HANA DB - Deactivation of Audit Trail
(Preview) SAP - High - HANA DB - User Admin actions
(Preview) SAP - High - Login from unexpected network
Actions
Run playbook
+ Add action
Rule expiration
Indefinite
Order
1


test
VS FTE / CyberSecurity
Test-incidentTrigger
VS FTE / CyberSecurity
Test-SharedMailbox
VS FTE / CyberSecurity
testEntity
VS FTE / CyberSecurity
testOne
VS FTE / CyberSecurity
TipsAndTricks
VS FTE / CyberSecurity
Unisolate-MDEMachine
VS FTE / CyberSecurity
UpdateTitle
VS FTE / CyberSecurity
Trigger
When incident is created
Conditions
If
Analytic rule name
+ Add
Actions
Run playbook
Search playbooks


Actions
Change status
New
Active
Closed
Add action
Rule expiration


Actions
Change severity
Informational
Low
Medium
High
Add action
Rule expiration
Indefinite


Automation rule name
Trigger
When incident is created
Conditions
If
Analytic rule name
+ Add
Actions
Assign owner
Unassigned
Assign to me
benji@cybsec.guru
@cybsec.guru
Admin
admin@M365x25776268.OnMicrosoft.com
On-Premises Directory Synchronization Service Account
War Room Members
WarRoomMembers@cybsec.guru
MDE users
Test Group
TestGroup@cybsec.guru
Search users or groups

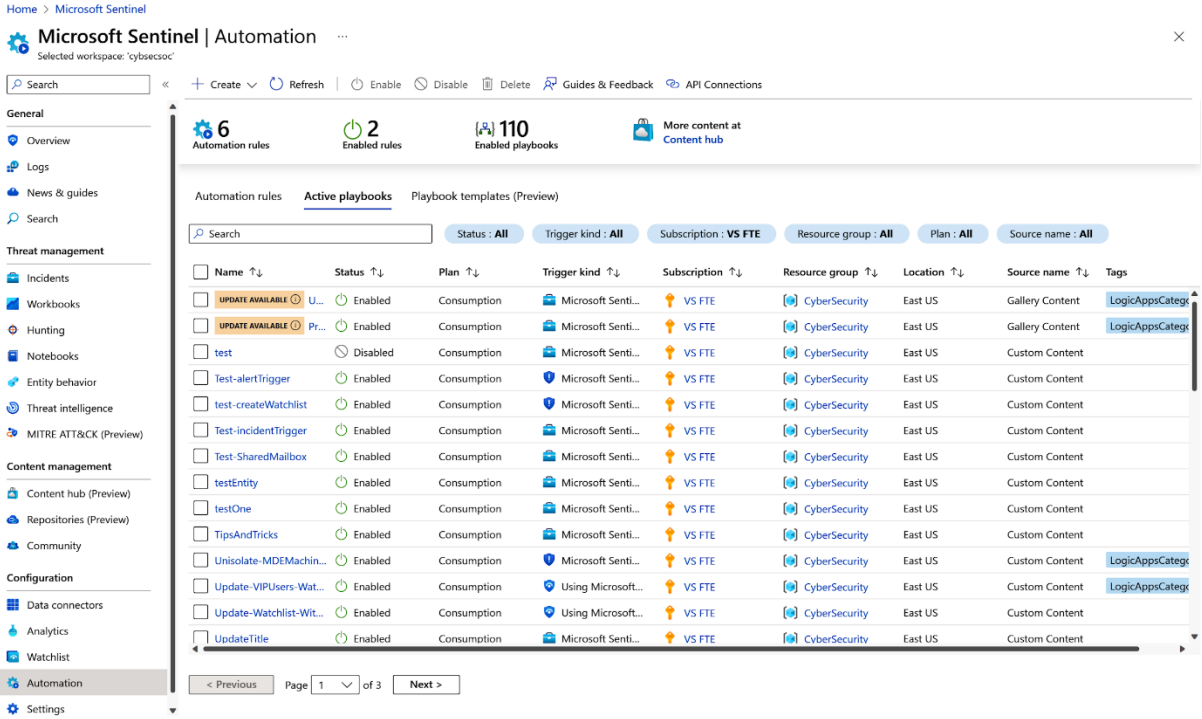

Actions
Add tags
Add tag
OK
Cancel

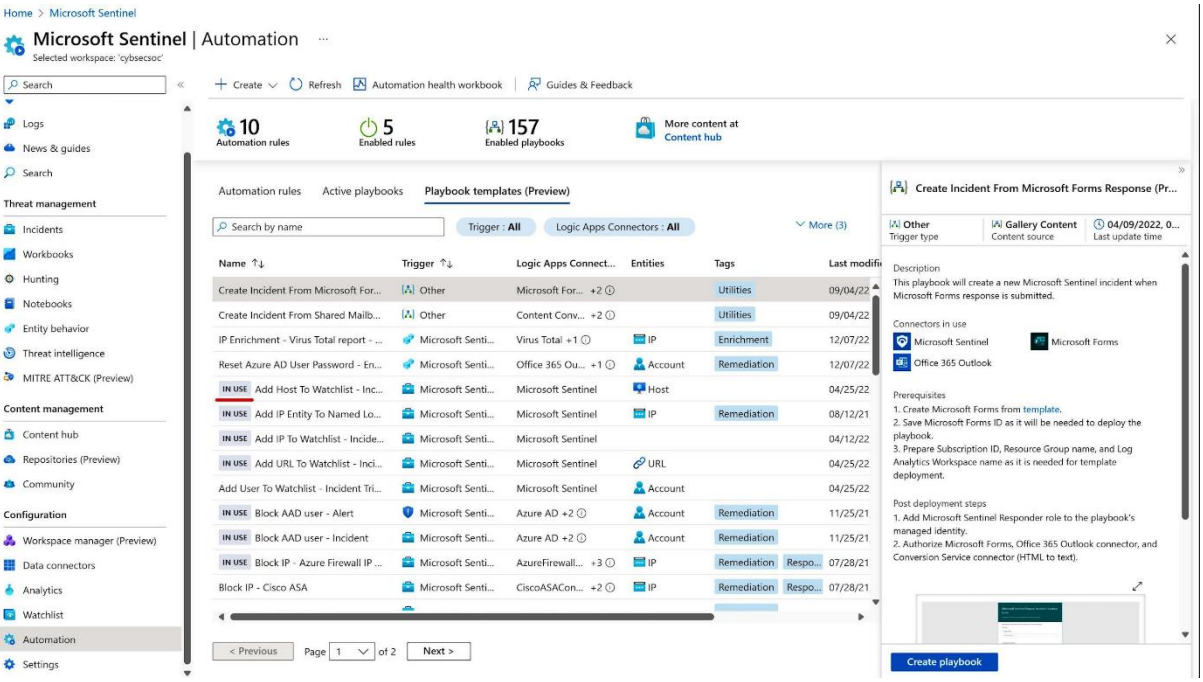
Rule expiration ⓘ

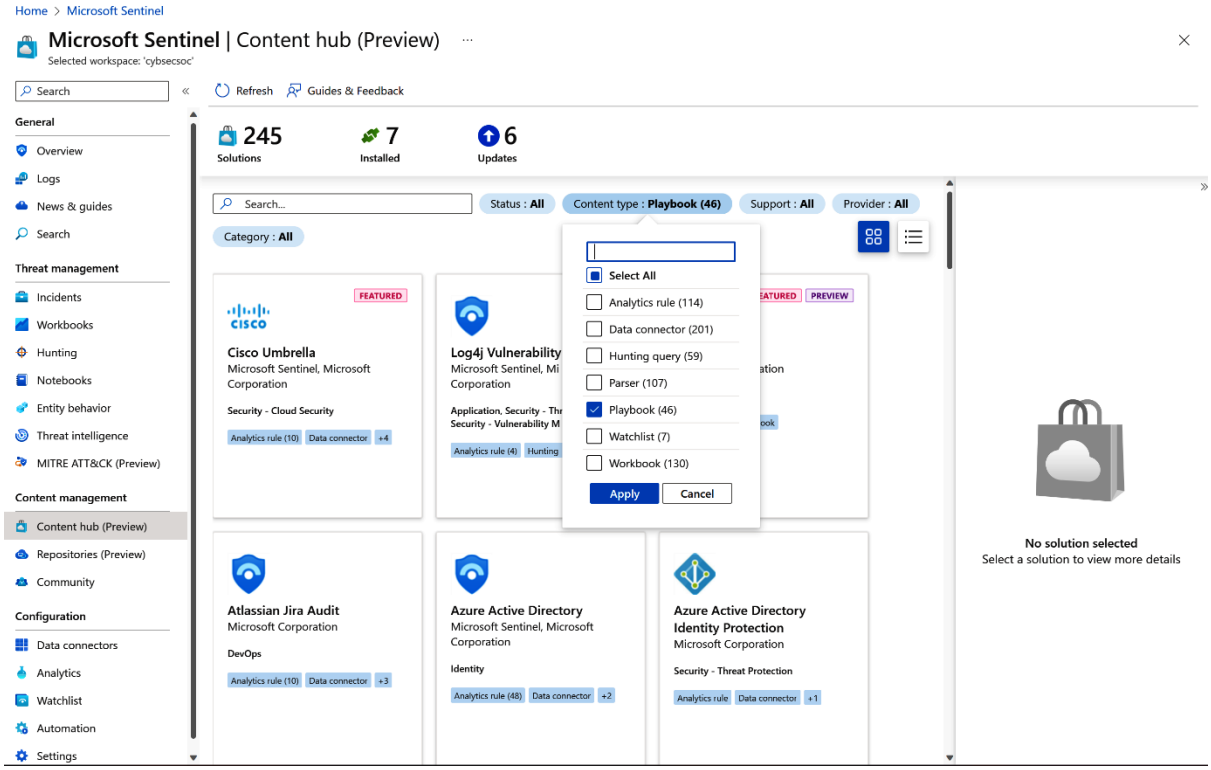
11/25/2022 | 12:00 AM

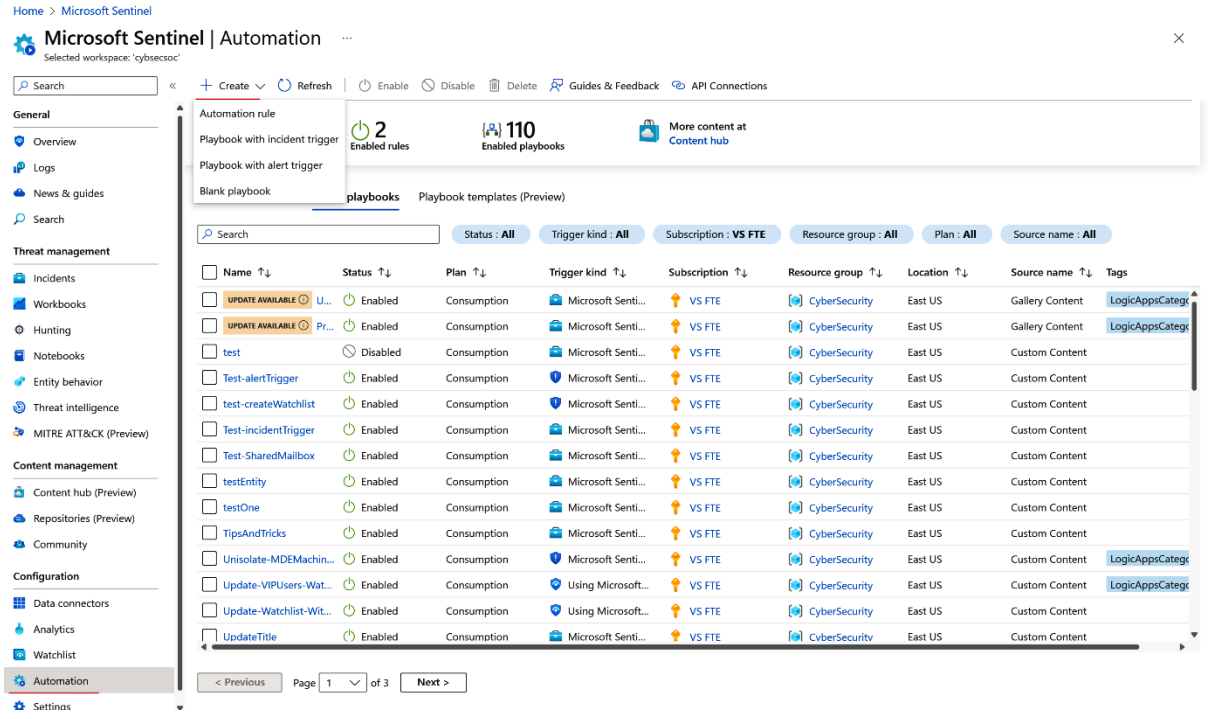
Order ⓘ

5






Home > Microsoft Sentinel
Microsoft Sentinel | Content hub (Preview)
Selected workspace: 'cybsecsoc'
Search
Refresh
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
245
Solutions
7
Installed
6
Updates
Search...
Status : All
Content type : Playbook (46)
Support : All
Provider : All
Category : All
Select All
Analytics rule (114)
Data connector (201)
Hunting query (59)
Parser (107)
Playbook (46)
Watchlist (7)
Workbook (130)
Apply
Cancel
FEATURED
Cisco Umbrella
Microsoft Sentinel, Microsoft Corporation
Security - Cloud Security
Analytics rule (10)
Data connector
+4
Log4j Vulnerability
Microsoft Sentinel, Mi
Corporation
Analytics rule (4)
Hunting
PREVIEW
Atlassian Jira Audit
Microsoft Corporation
DevOps
Analytics rule (10)
Data connector
+3
Azure Active Directory
Microsoft Sentinel, Microsoft Corporation
Identity
Analytics rule (48)
Data connector
+2
Azure Active Directory Identity Protection
Microsoft Corporation
Security - Threat Protection
Analytics rule
Data connector
+1
No solution selected
Select a solution to view more details


Home > Microsoft Sentinel
Microsoft Sentinel | Automation
Selected workspace: 'cybsecsoc'
Search
Create
Refresh
Enable
Disable
Delete
Guides & Feedback
API Connections
Automation rule
Playbook with incident trigger
Playbook with alert trigger
Blank playbook
2
Enabled rules
110
Enabled playbooks
More content at
Content hub
playbooks
Playbook templates (Preview)
Status : All
Trigger kind : All
Subscription : VS FTE
Resource group : All
Plan : All
Source name : All
Name
Status
Plan
Trigger kind
Subscription
Resource group
Location
Source name
Tags
Enabled
Consumption
Microsoft Senti...
VS FTE
CyberSecurity
East US
Gallery Content
Custom Content
Disabled
test
Test-alertTrigger
test-createWatchlist
Test-incidentTrigger
Test-SharedMailbox
testEntity
testOne
TipsAndTricks
Unisolate-MDEMachin...
Update-VIPUsers-Wat...
Update-Watchlist-Wit...
UpdateTitle
Using Microsoft...
< Previous
Page 1 of 3
Next >

Home > Microsoft Sentinel | Automation >

Create playbook ...

1 Basics 2 Connections 3 Review and create

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

Subscription *: VS FTE

Resource group *: CyberSecurity

Create new

Region *: East US

Playbook name *: SOAR

Enable diagnostics logs in Log Analytics

Log Analytics workspace: cybsecsoc

Associate with integration service environment

Integration service environment:

Next : Connections >

Home > Microsoft Sentinel | Automation >

Create playbook ...

Basics | 2 Connections | 3 Review and create

For each connector this playbook uses, you can choose to use an existing connection from another playbook. Otherwise, you must create a new connection and authenticate when you are brought to the Logic Apps designer after your playbook is deployed.

Microsoft Sentinel — Connect with managed identity

Connect with managed identity

FailedTrigger

benji@cybsec.guru

ttt

Previous | Next : Review and create >

Home > Microsoft Sentinel | Automation >

Create playbook ...

Basics | Connections | 3 Review and create

Basics

Subscription	VS FTE
Resource group	CyberSecurity
Region	East US
Playbook name	SOAR
Diagnostics logs workspace	Disabled
Integration service environment	Disabled

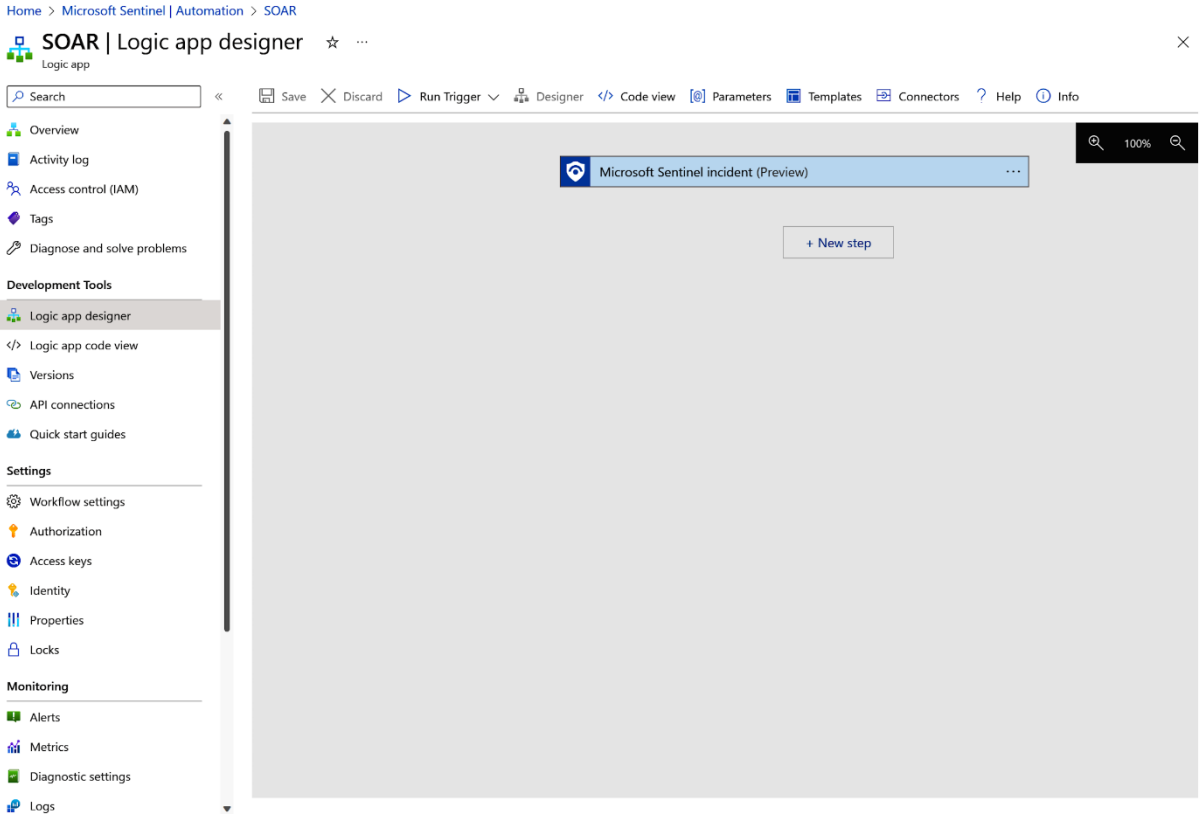
Connections

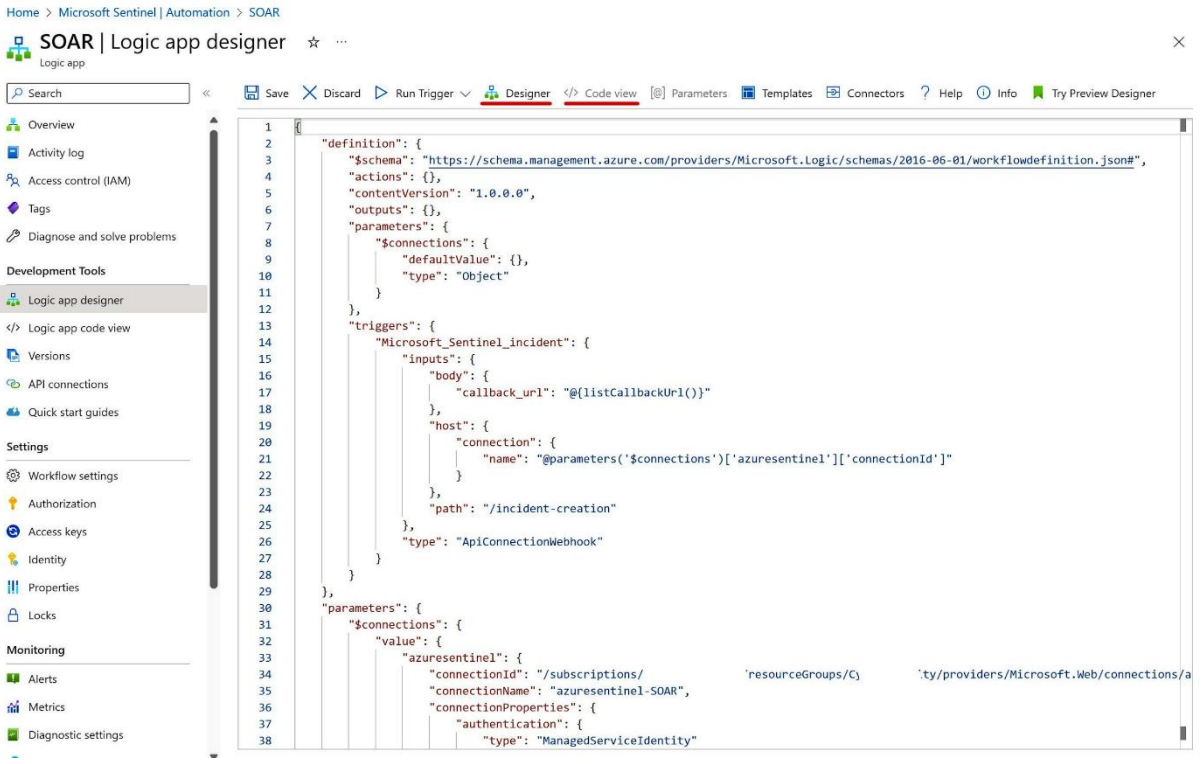
Microsoft Sentinel

Connect with managed identity

Note: Grant permissions to the managed identity after deployment.

Previous | Create and continue to designer


Home > Microsoft Sentinel | Automation > SOAR
SOAR | Logic app designer
Logic app
Search
Save
Discard
Run Trigger
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
100%
Microsoft Sentinel incident (Preview)
+ New step


Home > Microsoft Sentinel | Automation > SOAR
SOAR | Logic app designer
Logic app
Search
Save
Discard
Run Trigger
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Try Preview Designer
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
{
"definition": {
"$schema": "https://schema.management.azure.com/providers/Microsoft.Logic/schemas/2016-06-01/workflowdefinition.json#",
"actions": {},
"contentVersion": "1.0.0.0",
"outputs": {},
"parameters": {
"$connections": {
"defaultValue": {},
"type": "Object"
}
},
"triggers": {
"Microsoft_Sentinel_incident": {
"inputs": {
"body": {
"callback_url": "@{listCallbackUrl()}"
},
"host": {
"connection": {
"name": "@parameters('$connections')['azuresentinel']['connectionId']"
}
},
"path": "/incident-creation"
},
"type": "ApiConnectionWebhook"
}
}
},
"parameters": {
"$connections": {
"value": {
"azuresentinel": {
"connectionId": "/subscriptions/ 'resourceGroups/C ty/providers/Microsoft.Web/connections/a
"connectionName": "azuresentinel-SOAR",
"connectionProperties": {
"authentication": {
"type": "ManagedServiceIdentity"

Home >

Create Logic App ...

Basics | Hosting | Monitoring | Tags | Review + create

Create a logic app, which lets you group workflows as a logical unit for easier management, deployment and sharing of resources. Workflows let you connect your business-critical apps and services with Azure Logic Apps, automating your workflows without writing a single line of code.

Project Details

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

Subscription * : VS FTE

Resource Group * : CyberSecurity

Create new

Instance Details

Logic App name * : SOARStandard .azurewebsites.net

Publish * : (•) Workflow ( ) Docker Container

Region * : Central US

Not finding your App Service Plan? Try a different region or select your App Service Environment.

Plan

The plan type you choose dictates how your app scales, what features are enabled, and how it is priced. Learn more

Plan type * :

(•) **Standard:** Best for enterprise-level, serverless applications, with event-based scaling and networking isolation.

( ) **Consumption:** Best for entry-level. Pay only as much as your workflow runs.

Windows Plan (Central US) * : (New) ASP-CyberSecurity-8dfe

Create new

Pricing plan * :

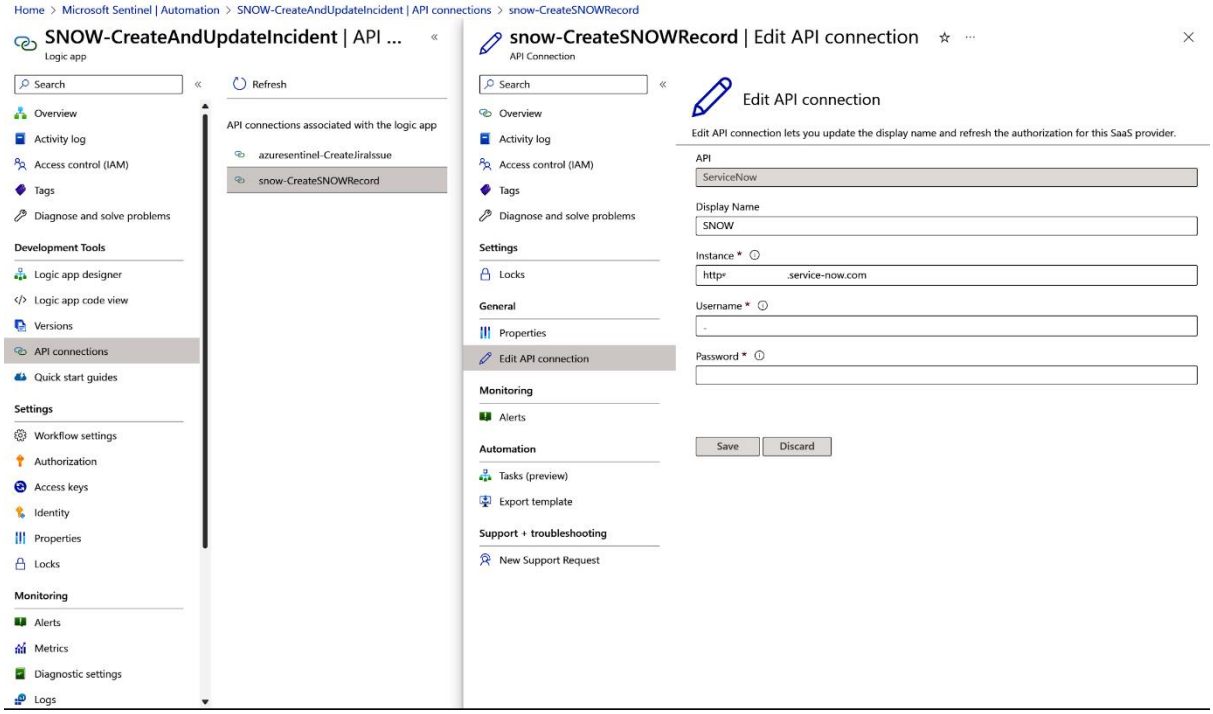
Workflow Standard WS1
210 total ACU, 3.5 GB memory
Change size

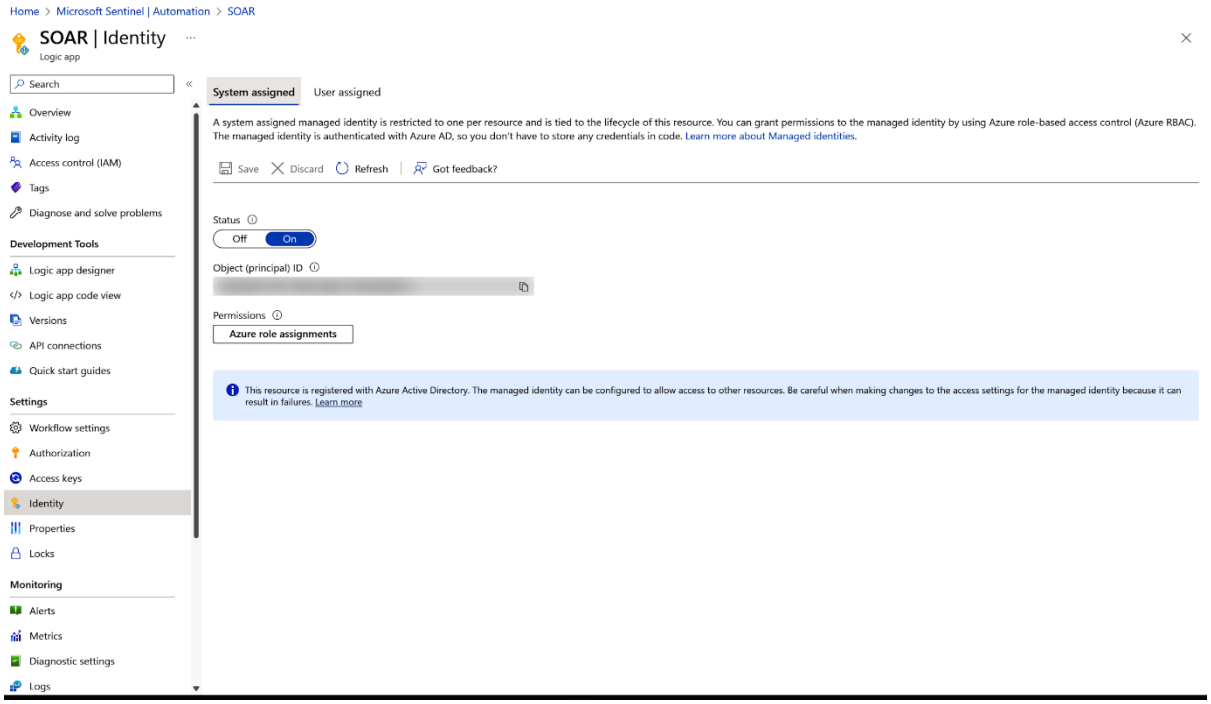
Zone redundancy

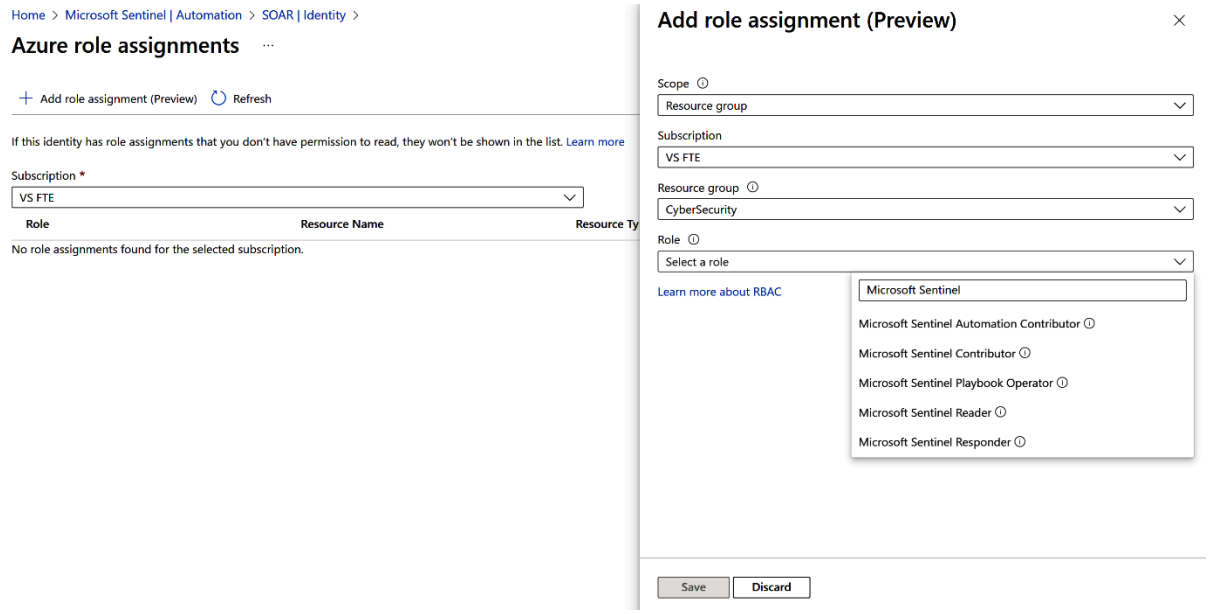
An App Service plan can be deployed as a zone redundant service in the regions that support it. This is a deployment time only decision. You can't make an App Service plan zone redundant after it has been deployed Learn more

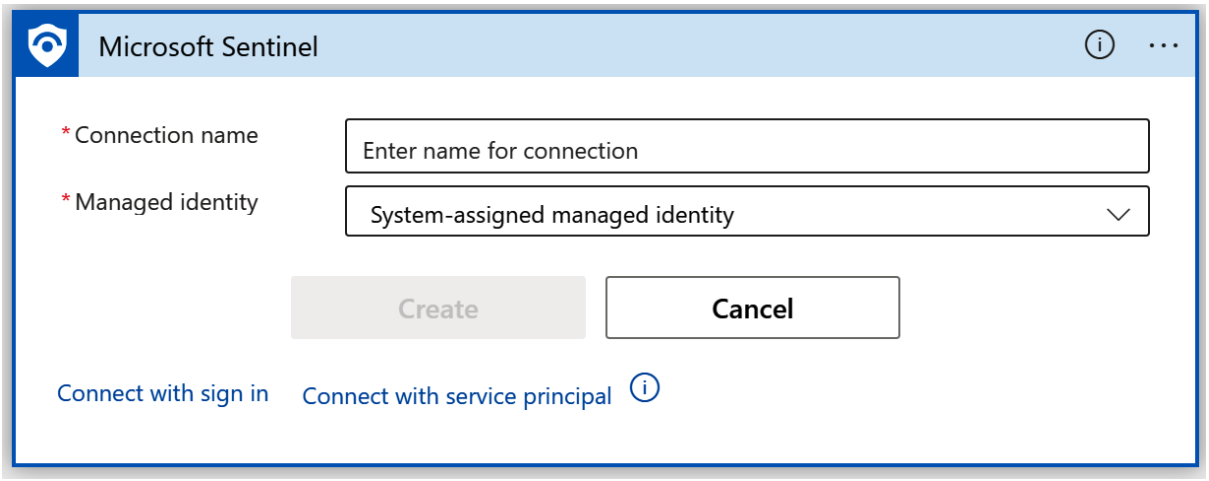
( )

Review + create | < Previous | Next : Hosting >


Home > Microsoft Sentinel | Automation > SNOW-CreateAndUpdateIncident | API connections > snow-CreateSNOWRecord
SNOW-CreateAndUpdateIncident | API ...
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Refresh
API connections associated with the logic app
azuresentinel-CreateJiralssue
snow-CreateSNOWRecord
snow-CreateSNOWRecord | Edit API connection
API Connection
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
General
Properties
Edit API connection
Monitoring
Alerts
Automation
Tasks (preview)
Export template
Support + troubleshooting
New Support Request
Edit API connection
Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.
API
ServiceNow
Display Name
SNOW
Instance *
http .service-now.com
Username *
Password *
Save
Discard


Home > Microsoft Sentinel | Automation > SOAR
SOAR | Identity
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
System assigned
User assigned
A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code. Learn more about Managed identities.
Save
Discard
Refresh
Got feedback?
Status
Off
On
Object (principal) ID
Permissions
Azure role assignments
This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more


Home > Microsoft Sentinel | Automation > SOAR | Identity >
Azure role assignments
Add role assignment (Preview)
Refresh
If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more
Subscription *
VS FTE
Role
Resource Name
Resource Ty
No role assignments found for the selected subscription.
Add role assignment (Preview)
Scope
Resource group
Subscription
VS FTE
Resource group
CyberSecurity
Role
Select a role
Learn more about RBAC
Microsoft Sentinel
Microsoft Sentinel Automation Contributor
Microsoft Sentinel Contributor
Microsoft Sentinel Playbook Operator
Microsoft Sentinel Reader
Microsoft Sentinel Responder
Save
Discard


Microsoft Sentinel
* Connection name
Enter name for connection
* Managed identity
System-assigned managed identity
Create
Cancel
Connect with sign in
Connect with service principal

Dashboard > CybSec Guru | App registrations >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

SOAR

Supported account types

Who can use this application or access this API?

- (•) Accounts in this organizational directory only (CybSec Guru only - Single tenant)
- ( ) Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ( ) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ( ) Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

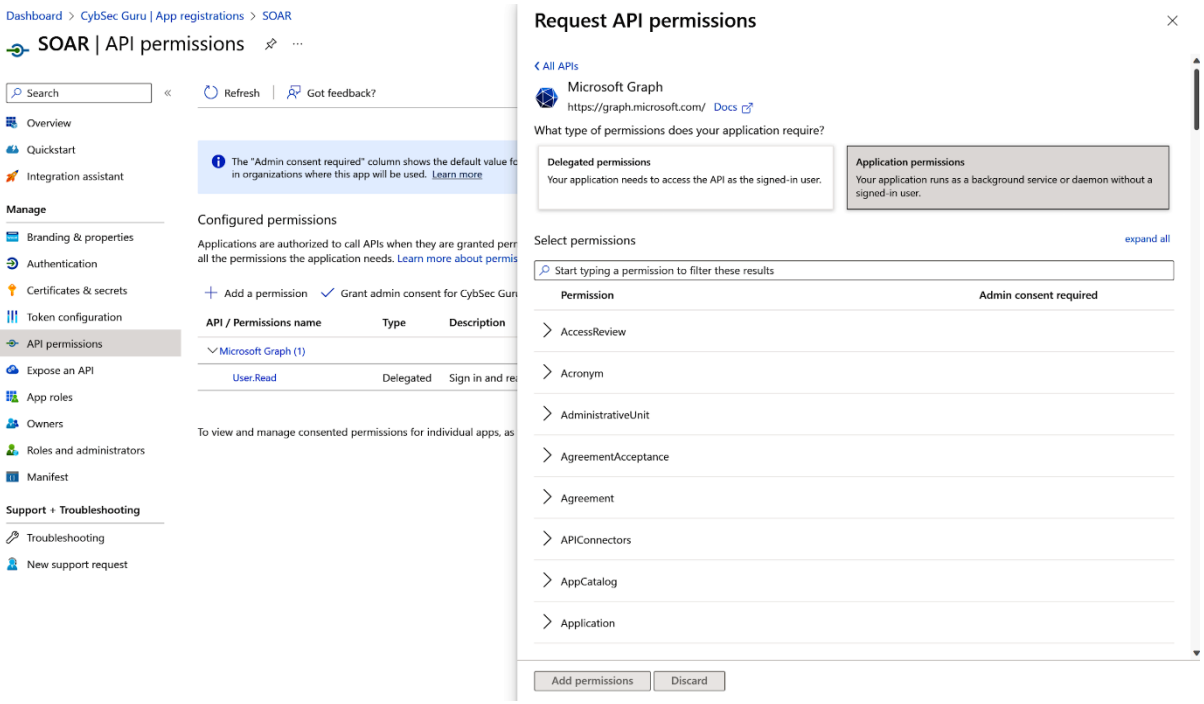
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

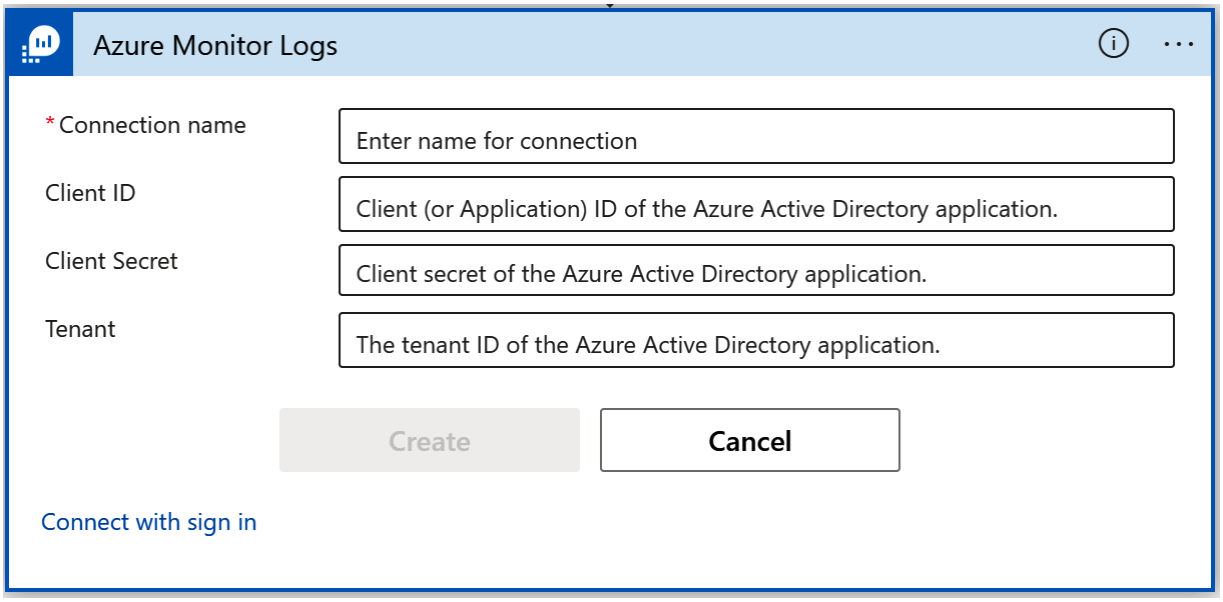
Select a platform | e.g. https://example.com/auth

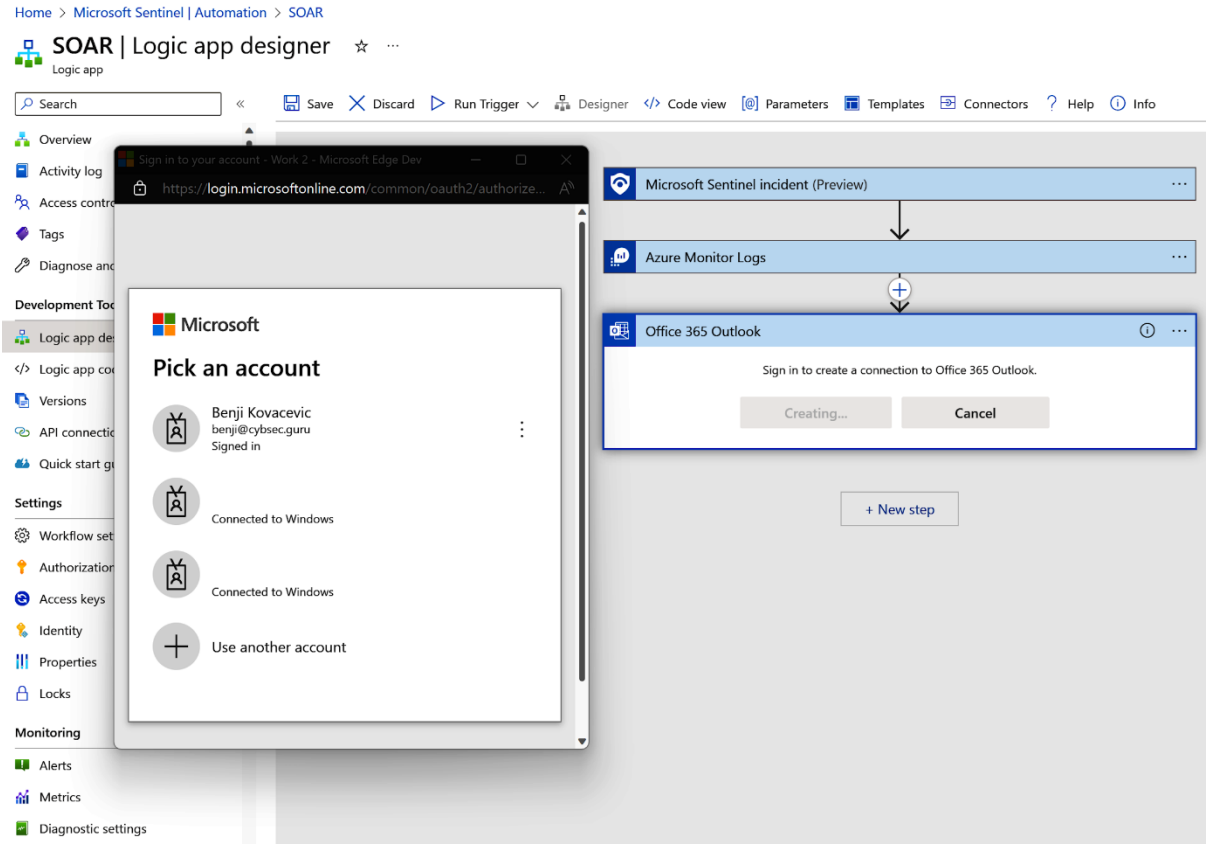
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

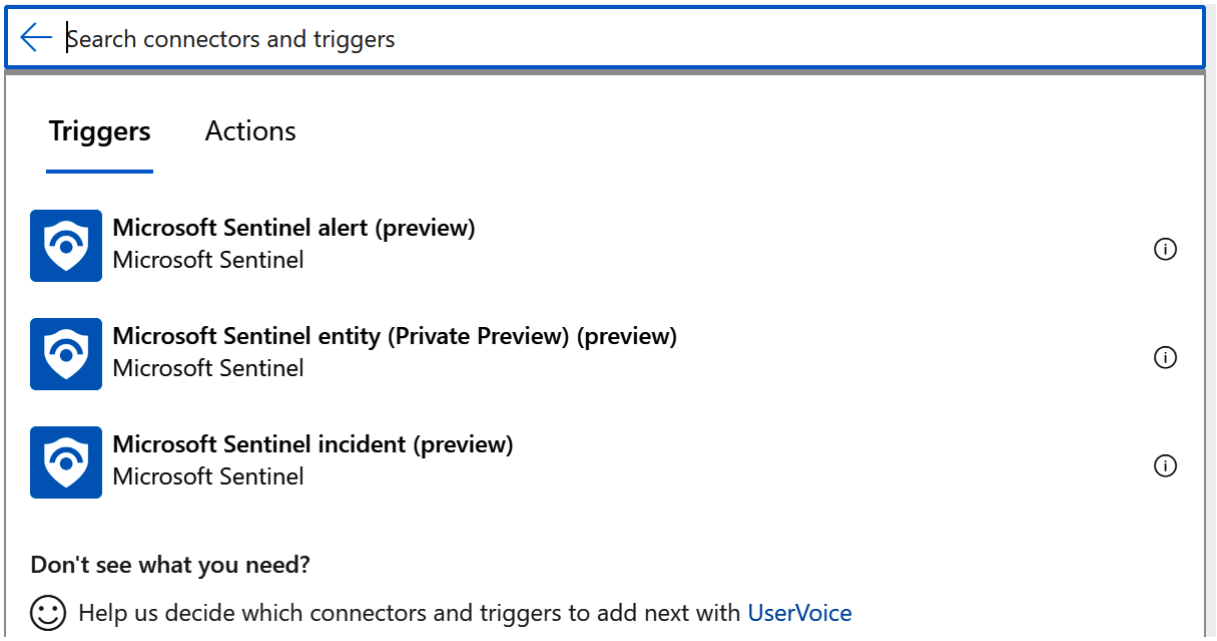
By proceeding, you agree to the Microsoft Platform Policies

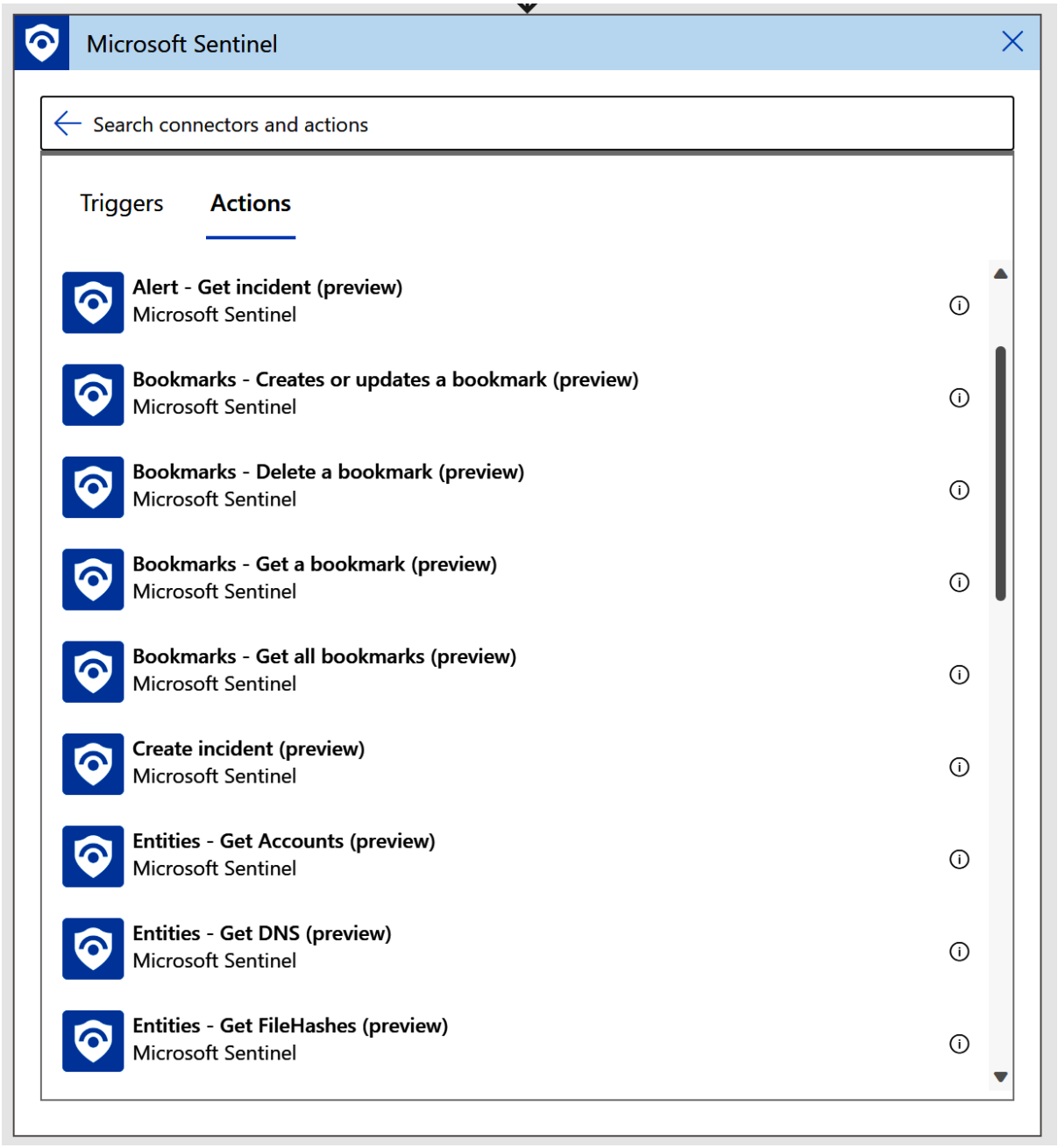
Register

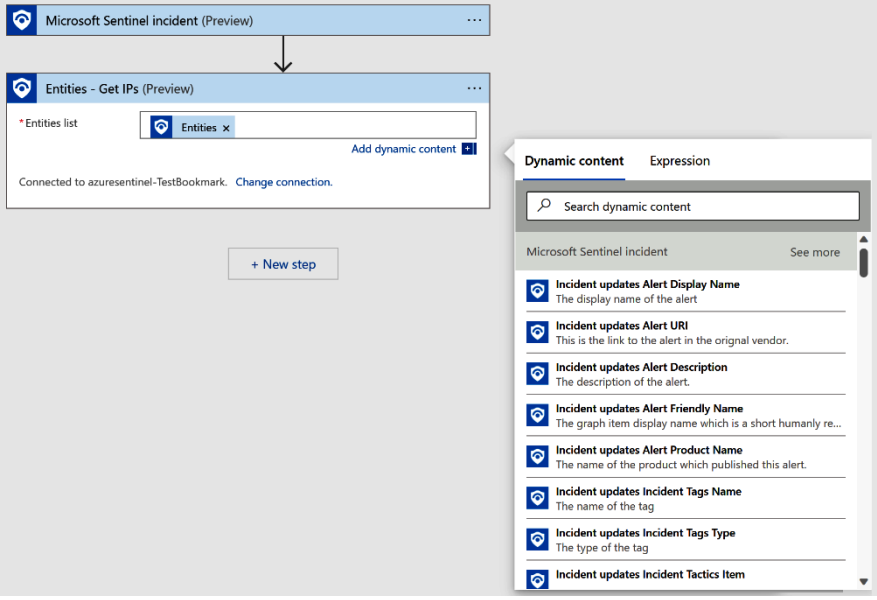


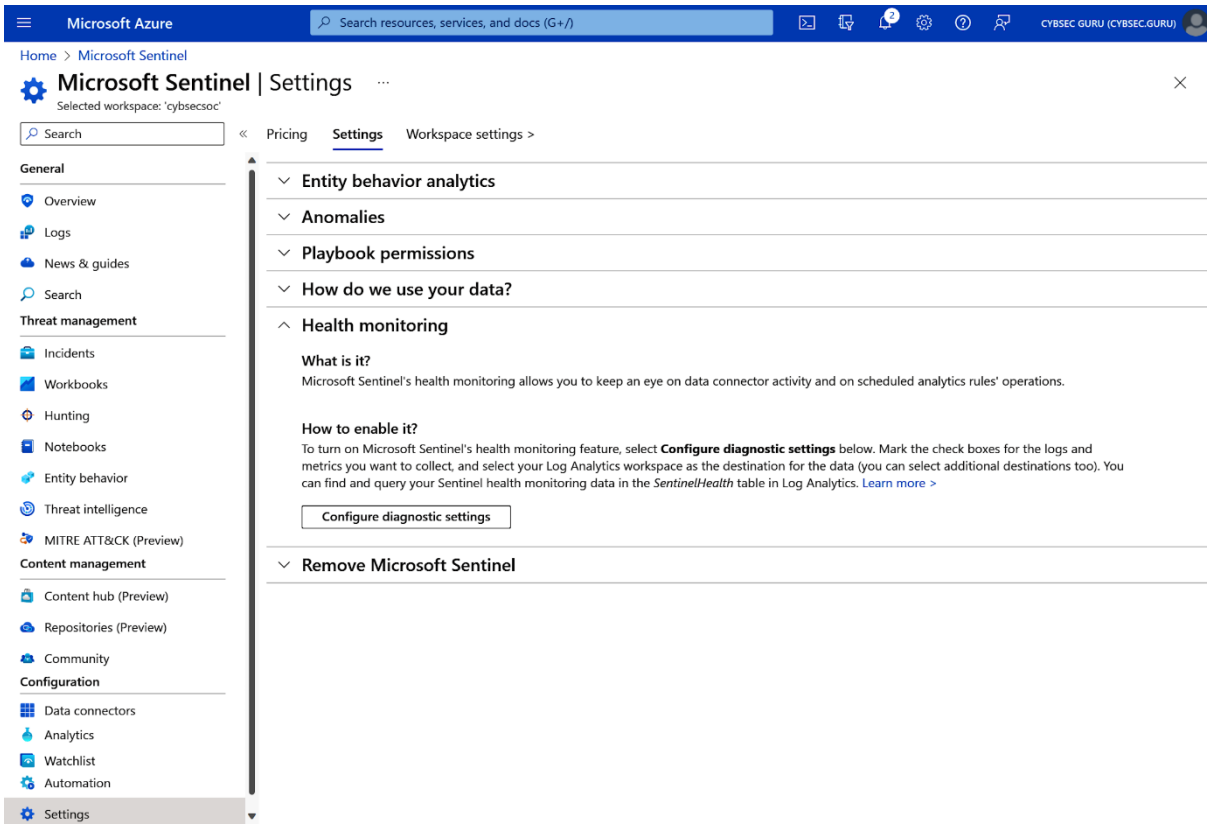

Azure Monitor Logs
* Connection name
Enter name for connection
Client ID
Client (or Application) ID of the Azure Active Directory application.
Client Secret
Client secret of the Azure Active Directory application.
Tenant
The tenant ID of the Azure Active Directory application.
Create
Cancel
Connect with sign in


Home > Microsoft Sentinel | Automation > SOAR
SOAR | Logic app designer
Logic app
Search
Save
Discard
Run Trigger
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Tags
Development Tools
Logic app designer
Versions
Settings
Workflow settings
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Microsoft Sentinel incident (Preview)
Azure Monitor Logs
Office 365 Outlook
Sign in to create a connection to Office 365 Outlook.
Creating...
Cancel
+ New step
Microsoft
Pick an account
Benji Kovacevic
benji@cybsec.guru
Signed in
Connected to Windows
Connected to Windows
Use another account


Search connectors and triggers
Triggers
Actions
Microsoft Sentinel alert (preview)
Microsoft Sentinel
Microsoft Sentinel entity (Private Preview) (preview)
Microsoft Sentinel
Microsoft Sentinel incident (preview)
Microsoft Sentinel
Don't see what you need?
Help us decide which connectors and triggers to add next with UserVoice


Microsoft Sentinel
Search connectors and actions
Triggers
Actions
Alert - Get incident (preview)
Microsoft Sentinel
Bookmarks - Creates or updates a bookmark (preview)
Microsoft Sentinel
Bookmarks - Delete a bookmark (preview)
Microsoft Sentinel
Bookmarks - Get a bookmark (preview)
Microsoft Sentinel
Bookmarks - Get all bookmarks (preview)
Microsoft Sentinel
Create incident (preview)
Microsoft Sentinel
Entities - Get Accounts (preview)
Microsoft Sentinel
Entities - Get DNS (preview)
Microsoft Sentinel
Entities - Get FileHashes (preview)
Microsoft Sentinel


Microsoft Sentinel incident (Preview)
Entities - Get IPs (Preview)
*Entities list
Entities
Add dynamic content
Connected to azuresentinel-TestBookmark. Change connection.
+ New step
Dynamic content
Expression
Search dynamic content
Microsoft Sentinel incident
See more
Incident updates Alert Display Name
The display name of the alert
Incident updates Alert URI
This is the link to the alert in the orignal vendor.
Incident updates Alert Description
The description of the alert.
Incident updates Alert Friendly Name
The graph item display name which is a short humanly re...
Incident updates Alert Product Name
The name of the product which published this alert.
Incident updates Incident Tags Name
The name of the tag
Incident updates Incident Tags Type
The type of the tag
Incident updates Incident Tactics Item


Microsoft Azure
Search resources, services, and docs (G+/)
CYBSEC GURU (CYBSEC.GURU)
Home > Microsoft Sentinel
Microsoft Sentinel | Settings
Selected workspace: 'cybsecsoc'
Search
Pricing
Settings
Workspace settings >
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Entity behavior analytics
Anomalies
Playbook permissions
How do we use your data?
Health monitoring
What is it?
Microsoft Sentinel's health monitoring allows you to keep an eye on data connector activity and on scheduled analytics rules' operations.
How to enable it?
To turn on Microsoft Sentinel's health monitoring feature, select Configure diagnostic settings below. Mark the check boxes for the logs and metrics you want to collect, and select your Log Analytics workspace as the destination for the data (you can select additional destinations too). You can find and query your Sentinel health monitoring data in the SentinelHealth table in Log Analytics. Learn more >
Configure diagnostic settings
Remove Microsoft Sentinel

Home > Microsoft Sentinel | Settings > Diagnostic settings >

Diagnostic setting

Save | Discard | Delete | Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

JSON View

Diagnostic setting name * Automation Health

Logs

Category groups

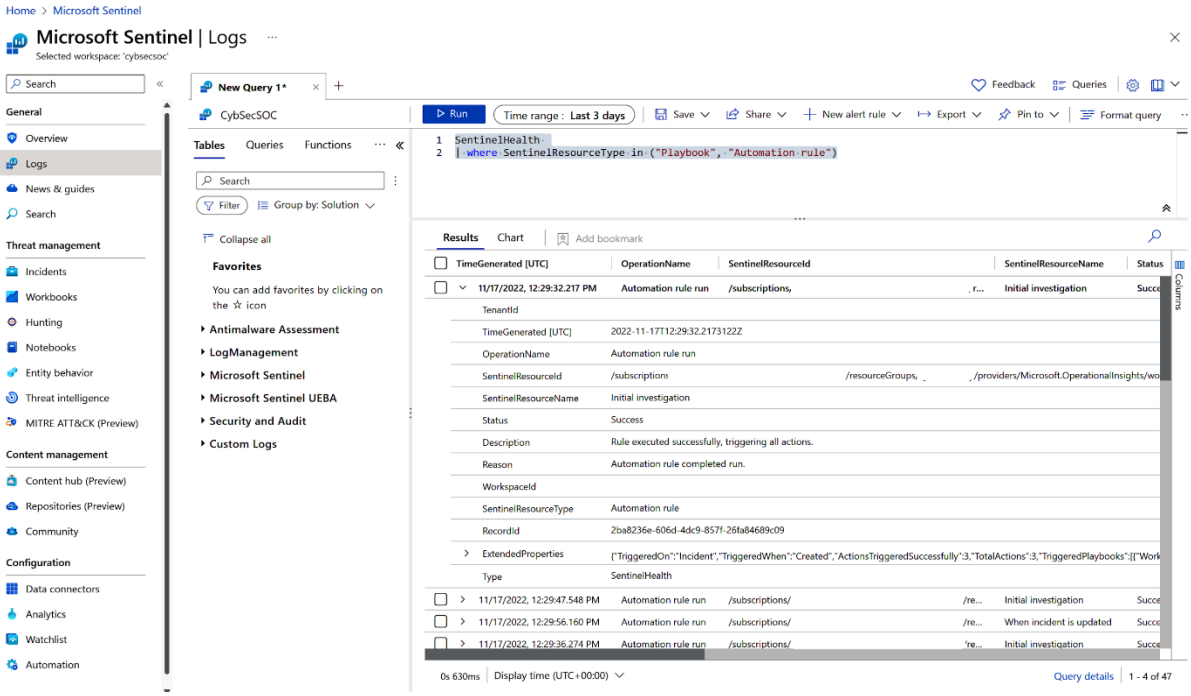
- [ ] allLogs

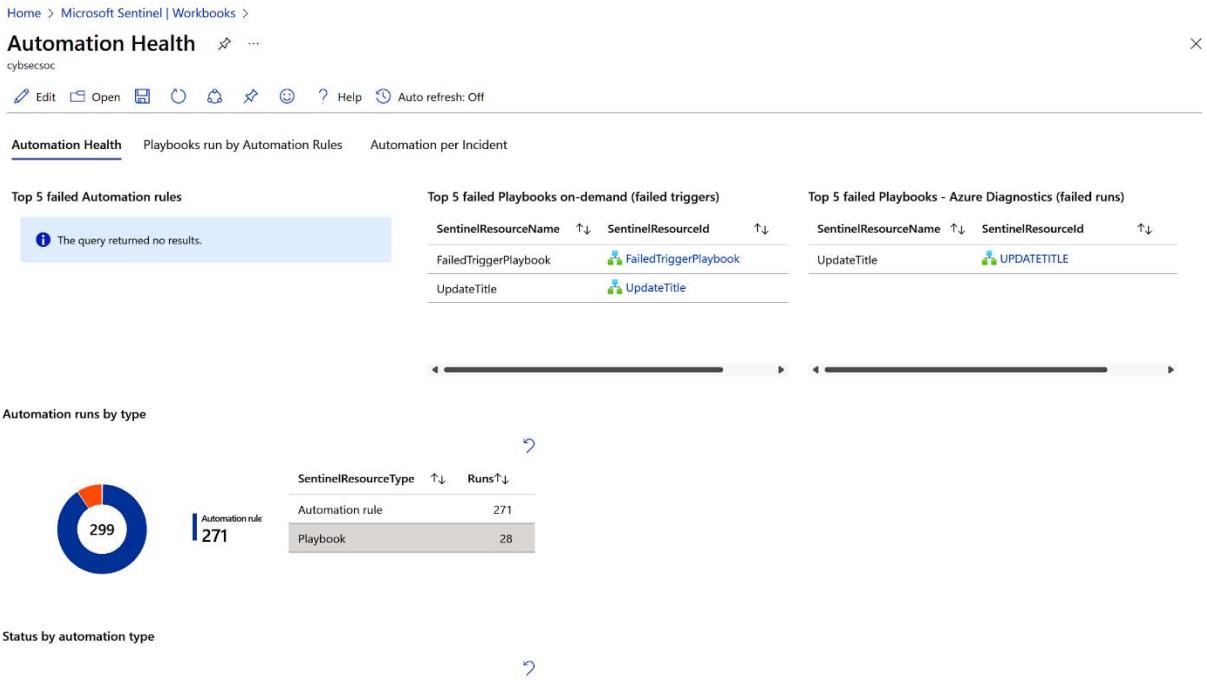
Categories

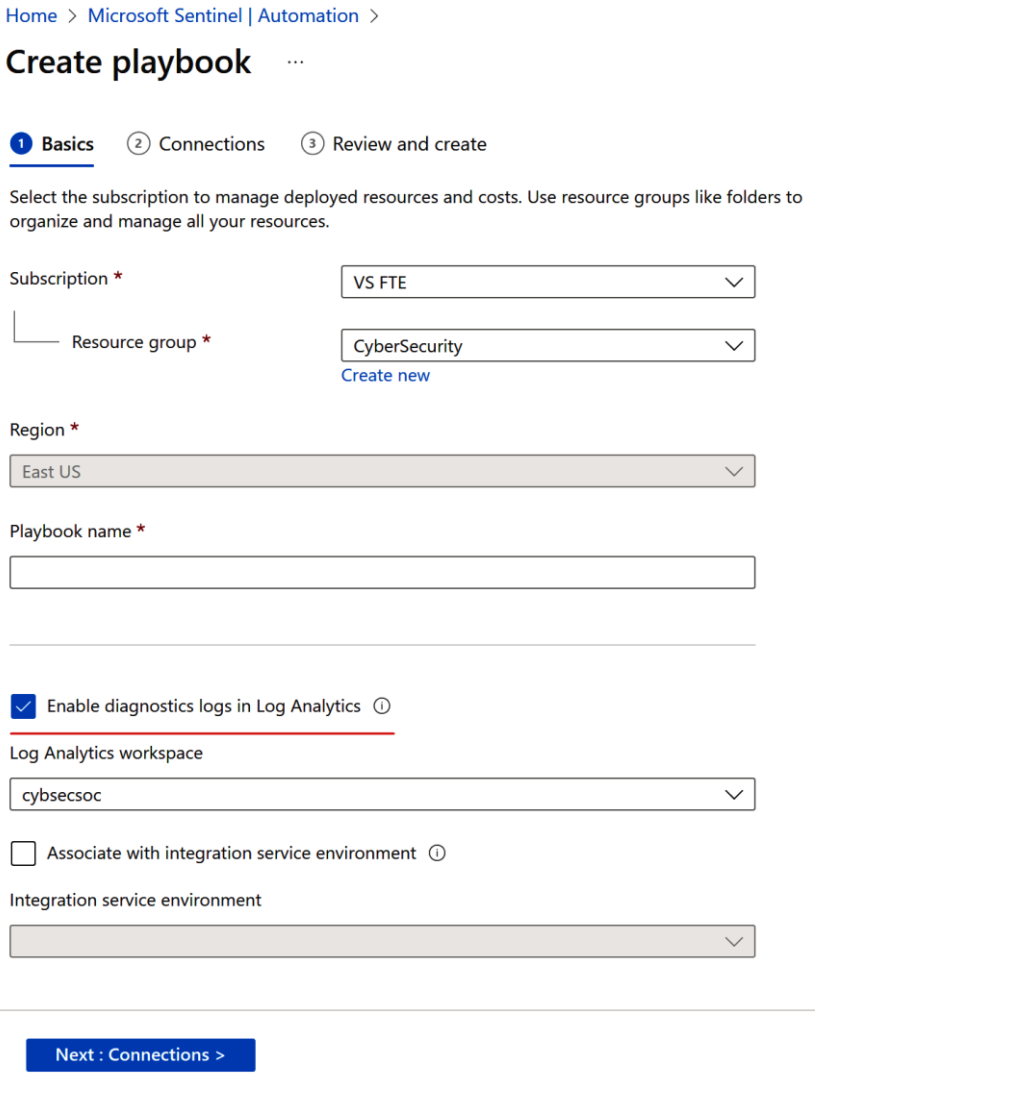
- [x] Automation
- [ ] Data Collection - Connectors

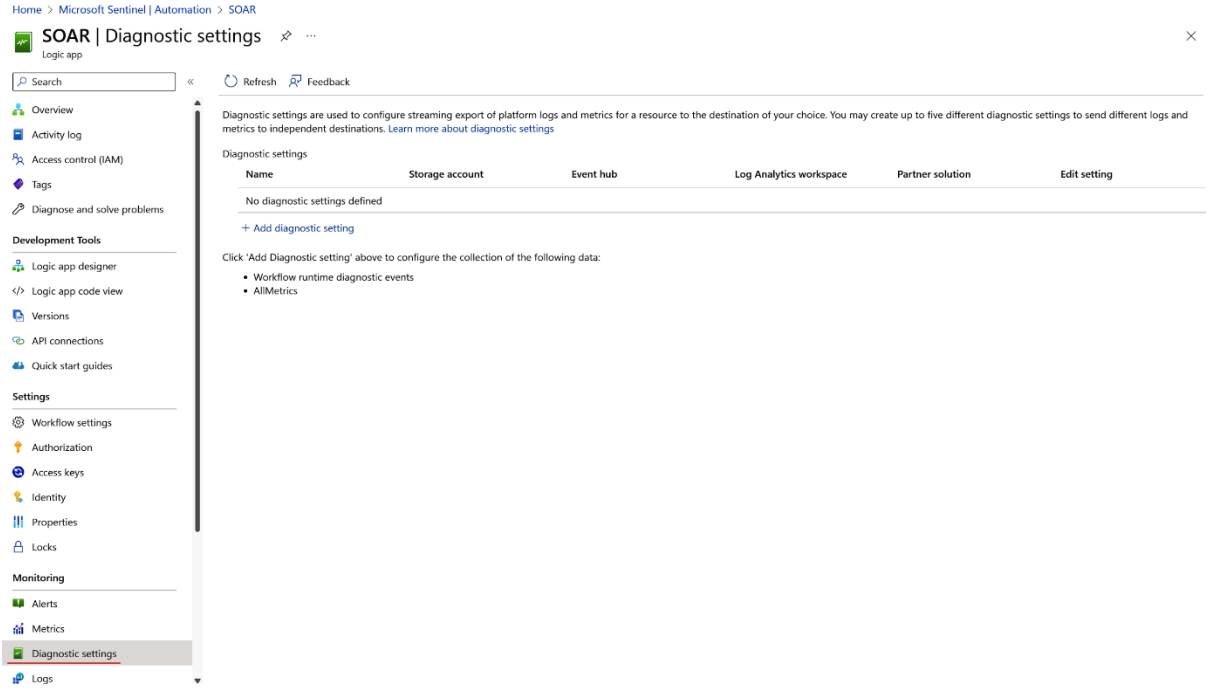
Destination details

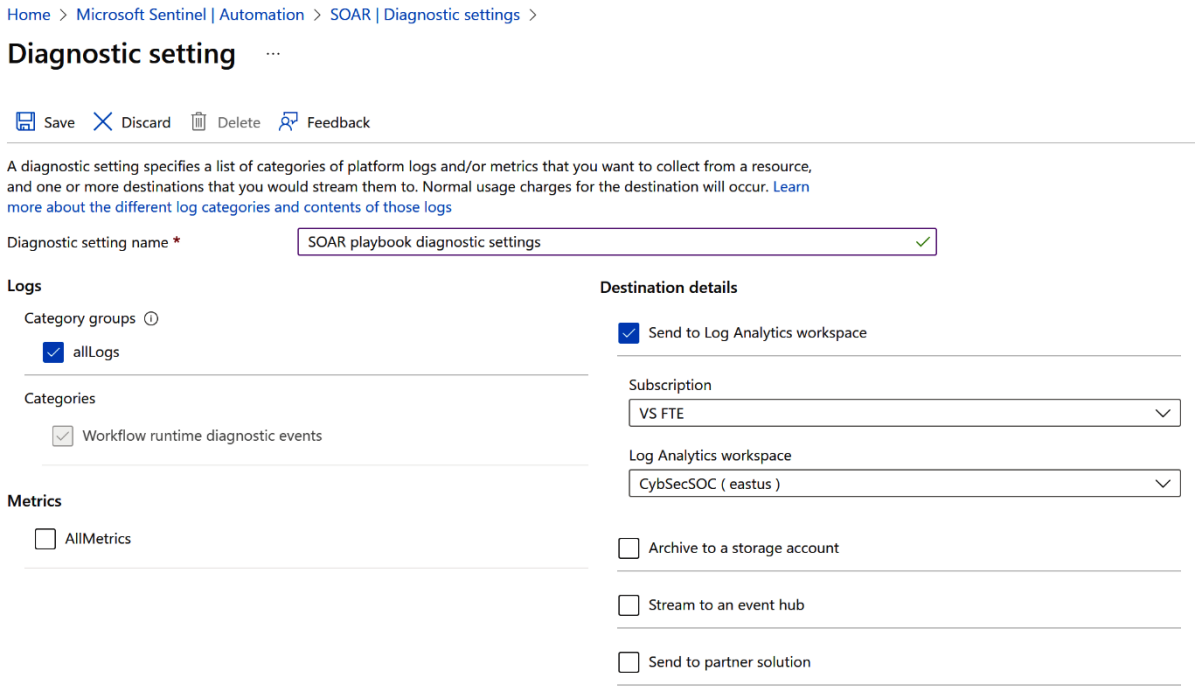
- [x] Send to Log Analytics workspace
  - Subscription: VS FTE
  - Log Analytics workspace: CybSecSOC (eastus)
- [ ] Archive to a storage account
- [ ] Stream to an event hub
- [ ] Send to partner solution

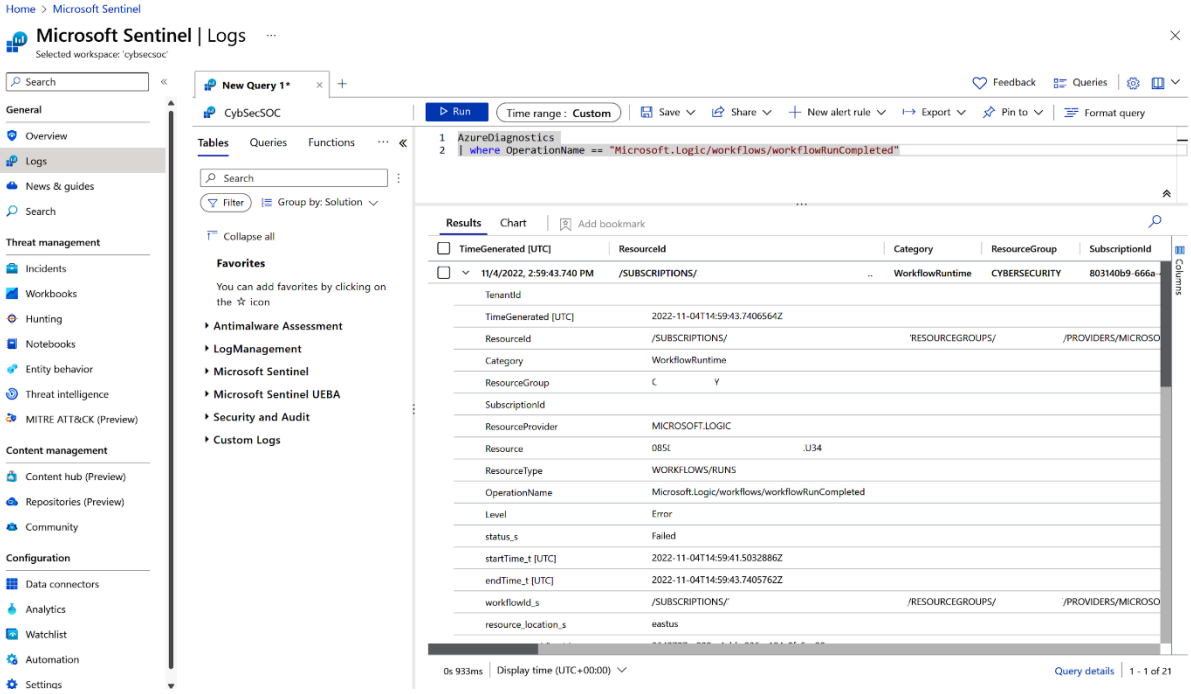


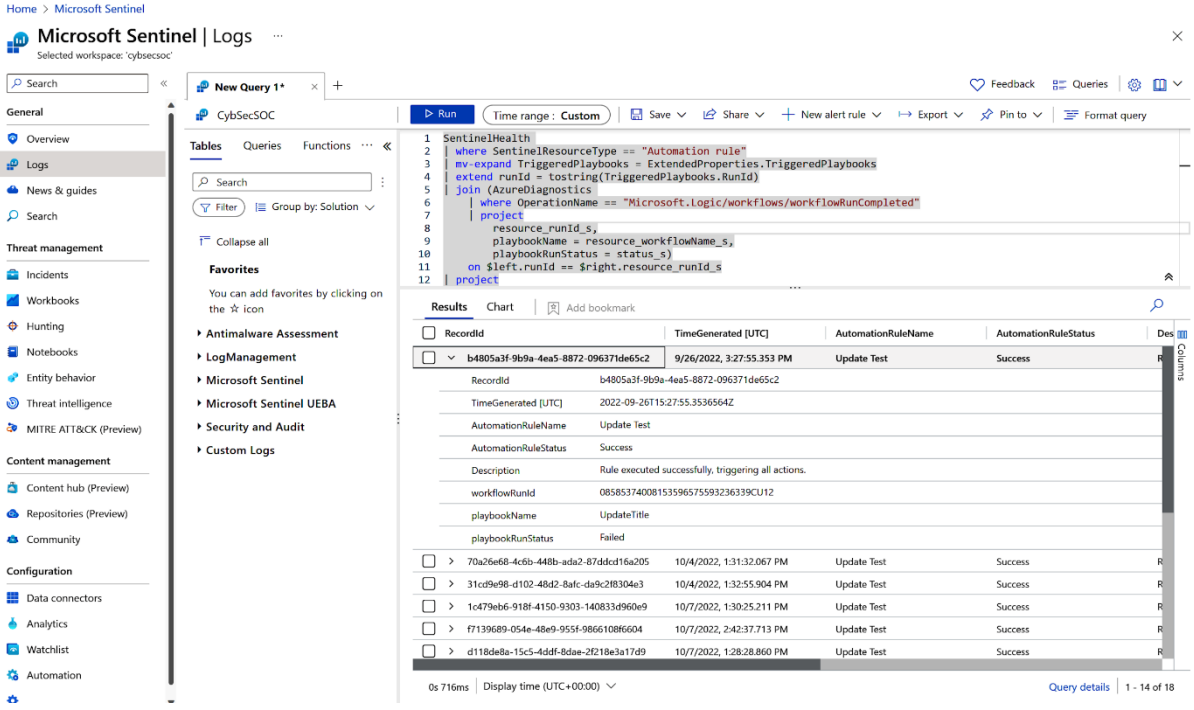

Home > Microsoft Sentinel | Workbooks >
Automation Health
cybsecsoc
Edit
Open
Help
Auto refresh: Off
Automation Health
Playbooks run by Automation Rules
Automation per Incident
Top 5 failed Automation rules
The query returned no results.
Top 5 failed Playbooks on-demand (failed triggers)
SentinelResourceName
SentinelResourceId
FailedTriggerPlaybook
FailedTriggerPlaybook
UpdateTitle
UpdateTitle
Top 5 failed Playbooks - Azure Diagnostics (failed runs)
SentinelResourceName
SentinelResourceId
UpdateTitle
UPDATETITLE
Automation runs by type
299
Automation rule
271
SentinelResourceType
Runs
Automation rule
271
Playbook
28
Status by automation type


Home > Microsoft Sentinel | Automation >
Create playbook
1 Basics
2 Connections
3 Review and create
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
VS FTE
Resource group *
CyberSecurity
Create new
Region *
East US
Playbook name *
Enable diagnostics logs in Log Analytics
Log Analytics workspace
cybsecsoc
Associate with integration service environment
Integration service environment
Next : Connections >

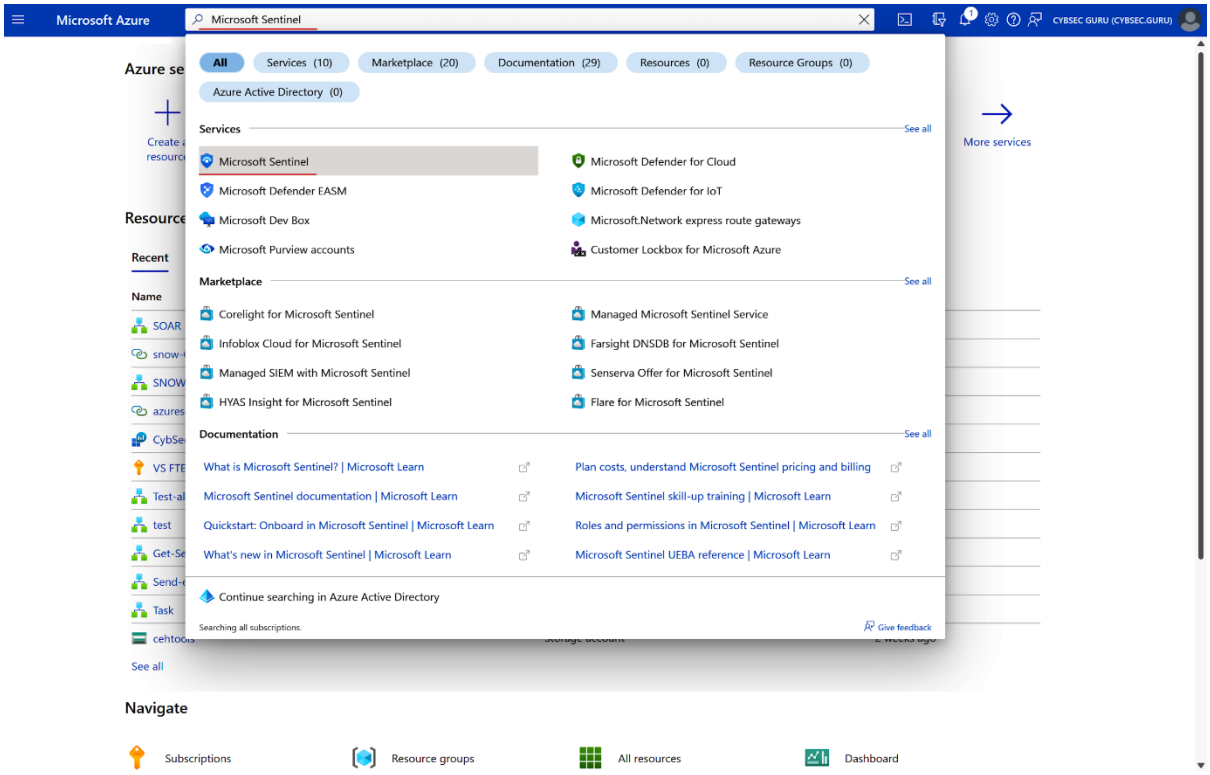

Home > Microsoft Sentinel | Automation > SOAR
SOAR | Diagnostic settings
Logic app
Search
Refresh
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings
Diagnostic settings
Name
Storage account
Event hub
Log Analytics workspace
Partner solution
Edit setting
No diagnostic settings defined
+ Add diagnostic setting
Click 'Add Diagnostic setting' above to configure the collection of the following data:
Workflow runtime diagnostic events
AllMetrics

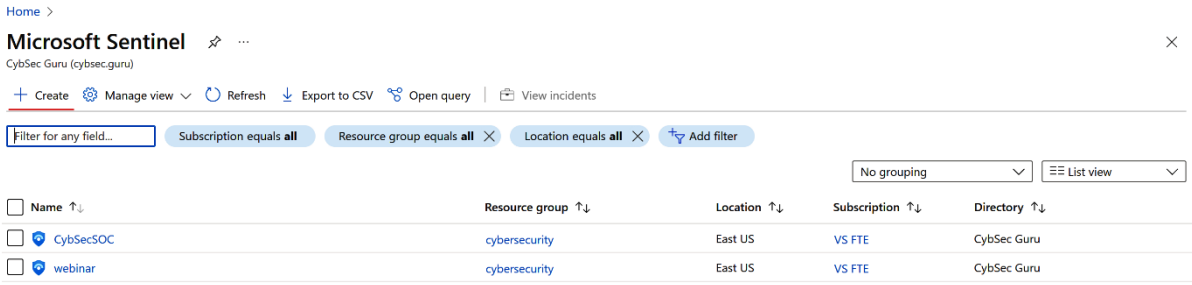

Home > Microsoft Sentinel | Automation > SOAR | Diagnostic settings >
Diagnostic setting
Save
Discard
Delete
Feedback
A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs
Diagnostic setting name *
SOAR playbook diagnostic settings
Logs
Category groups
allLogs
Categories
Workflow runtime diagnostic events
Metrics
AllMetrics
Destination details
Send to Log Analytics workspace
Subscription
VS FTE
Log Analytics workspace
CybSecSOC (eastus)
Archive to a storage account
Stream to an event hub
Send to partner solution

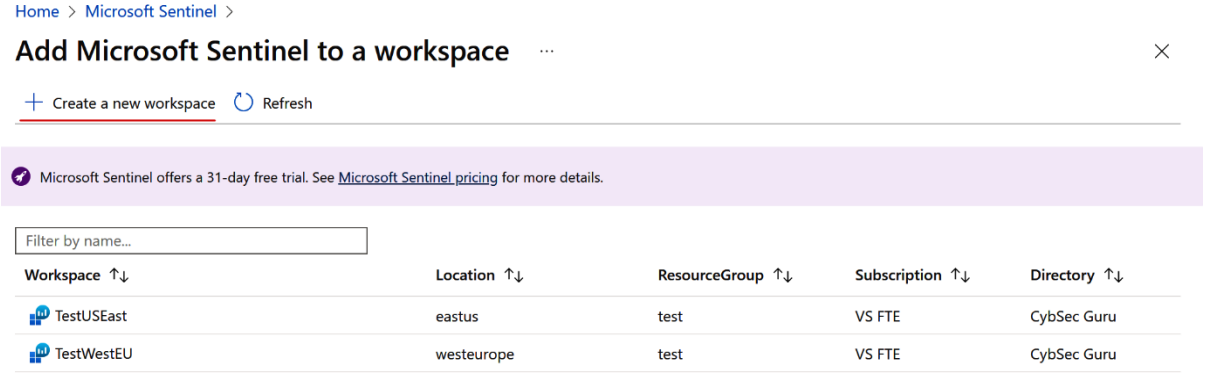

Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'cybsecsoc'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
New Query 1*
Feedback
Queries
CybSecSOC
Run
Time range : Custom
Save
Share
New alert rule
Export
Pin to
Format query
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
Antimalware Assessment
LogManagement
Microsoft Sentinel
Microsoft Sentinel UEBA
Security and Audit
Custom Logs
1 AzureDiagnostics
2 | where OperationName == "Microsoft.Logic/workflows/workflowRunCompleted"
Results
Chart
Add bookmark
TimeGenerated [UTC]
ResourceId
Category
ResourceGroup
SubscriptionId
11/4/2022, 2:59:43.740 PM
/SUBSCRIPTIONS/
WorkflowRuntime
CYBERSECURITY
803140b9-666a
TenantId
TimeGenerated [UTC] 2022-11-04T14:59:43.7406564Z
ResourceId /SUBSCRIPTIONS/ /RESOURCEGROUPS/ /PROVIDERS/MICROSO
Category WorkflowRuntime
ResourceGroup
SubscriptionId
ResourceProvider MICROSOFT.LOGIC
Resource
ResourceType WORKFLOWS/RUNS
OperationName Microsoft.Logic/workflows/workflowRunCompleted
Level Error
status_s Failed
startTime_t [UTC] 2022-11-04T14:59:41.5032886Z
endTime_t [UTC] 2022-11-04T14:59:43.7405762Z
workflowId_s /SUBSCRIPTIONS/ /RESOURCEGROUPS/ /PROVIDERS/MICROSO
resource_location_s eastus
Columns
0s 933ms
Display time (UTC+00:00)
Query details
1 - 1 of 21


Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'cybsecsoc'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
New Query 1*
Feedback
Queries
CybSecSOC
Run
Time range : Custom
Save
Share
New alert rule
Export
Pin to
Format query
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
Antimalware Assessment
LogManagement
Microsoft Sentinel
Microsoft Sentinel UEBA
Security and Audit
Custom Logs
1 SentinelHealth
2 | where SentinelResourceType == "Automation rule"
3 | mv-expand TriggeredPlaybooks = ExtendedProperties.TriggeredPlaybooks
4 | extend runId = tostring(TriggeredPlaybooks.RunId)
5 | join (AzureDiagnostics
6 | where OperationName == "Microsoft.Logic/workflows/workflowRunCompleted"
7 | project
8 resource_runId_s,
9 playbookName = resource_workflowName_s,
10 playbookRunStatus = status_s)
11 on $left.runId == $right.resource_runId_s
12 | project
Results
Chart
Add bookmark
RecordId
TimeGenerated [UTC]
AutomationRuleName
AutomationRuleStatus
b4805a3f-9b9a-4ea5-8872-096371de65c2
9/26/2022, 3:27:55.353 PM
Update Test
Success
RecordId b4805a3f-9b9a-4ea5-8872-096371de65c2
TimeGenerated [UTC] 2022-09-26T15:27:55.3536564Z
AutomationRuleName Update Test
AutomationRuleStatus Success
Description Rule executed successfully, triggering all actions.
workflowRunId
playbookName UpdateTitle
playbookRunStatus Failed
70a26e68-4c6b-448b-ada2-87ddcd16a205 10/4/2022, 1:31:32.067 PM Update Test Success
31cd9e98-d102-48d2-8afc-da9c2f8304e3 10/4/2022, 1:32:55.904 PM Update Test Success
1c479eb6-918f-4150-9303-140833d960e9 10/7/2022, 1:30:25.211 PM Update Test Success
f7139689-054e-48e9-955f-9866108f6604 10/7/2022, 2:42:37.713 PM Update Test Success
d118de8a-15c5-4ddf-8dae-2f218e3a17d9 10/7/2022, 1:28:28.860 PM Update Test Success
Columns
0s 716ms
Display time (UTC+00:00)
Query details
1 - 14 of 18

Chapter 6: Enriching Incidents Using Automation







Create Log Analytics workspace ...

Basics | Tags | Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * : VS FTE

Resource group * : (New) SOAR

Create new

Instance details

Name * : SOAR

Region * : West Europe

Review + Create | « Previous | Next : Tags >

Create Log Analytics workspace ...

Validation passed

Basics Tags **Review + Create**

Log Analytics workspace
by Microsoft

Basics

Subscription	VS FTE
Resource group	SOAR
Name	SOAR
Region	West Europe

Pricing

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

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the Azure Monitor pricing page. You can change to a different pricing tier after the workspace is created. Learn more about Log Analytics pricing models.

Tags

(none)

Create « Previous Download a template for automation

Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace ···

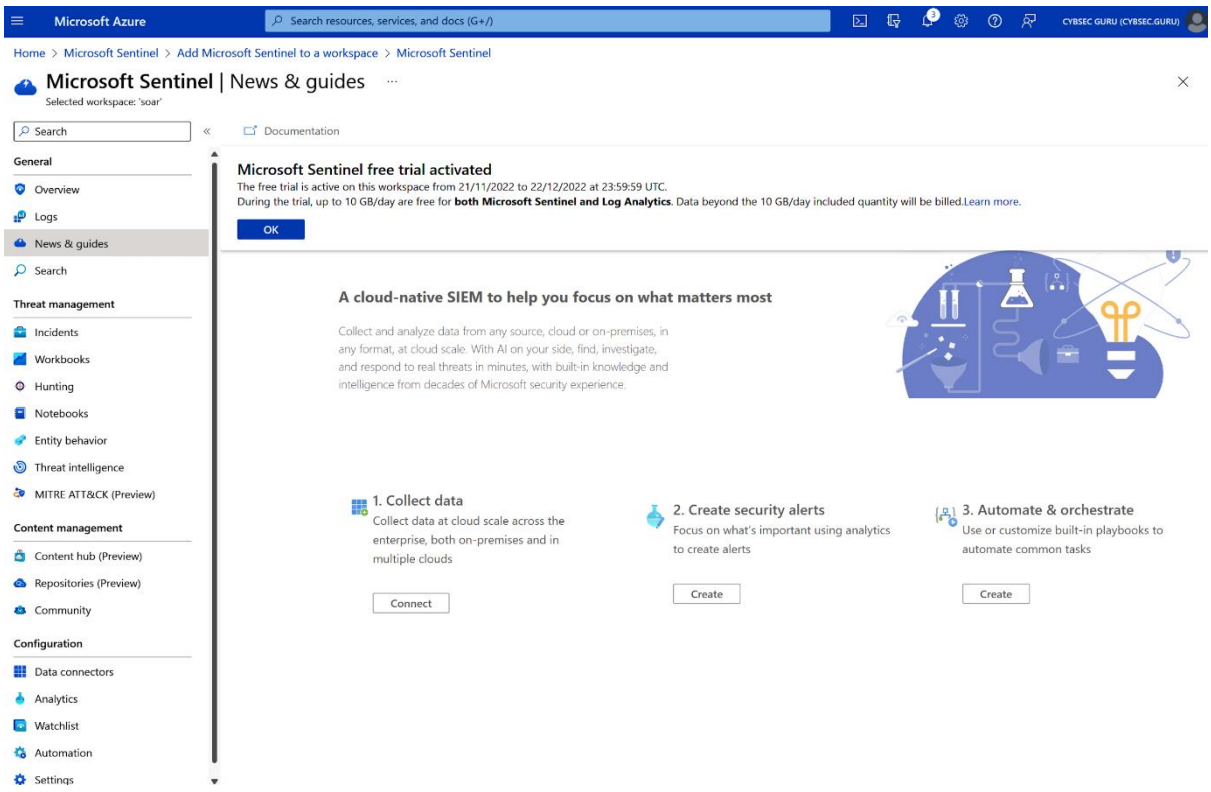
+ Create a new workspace Refresh

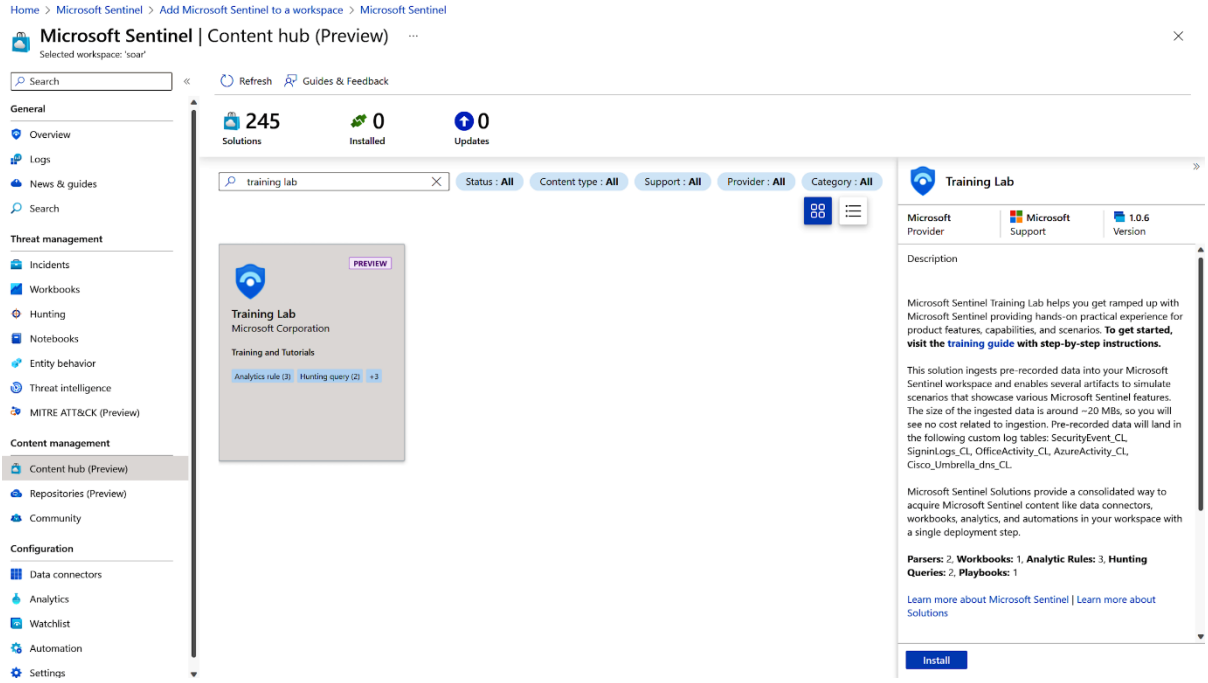
Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

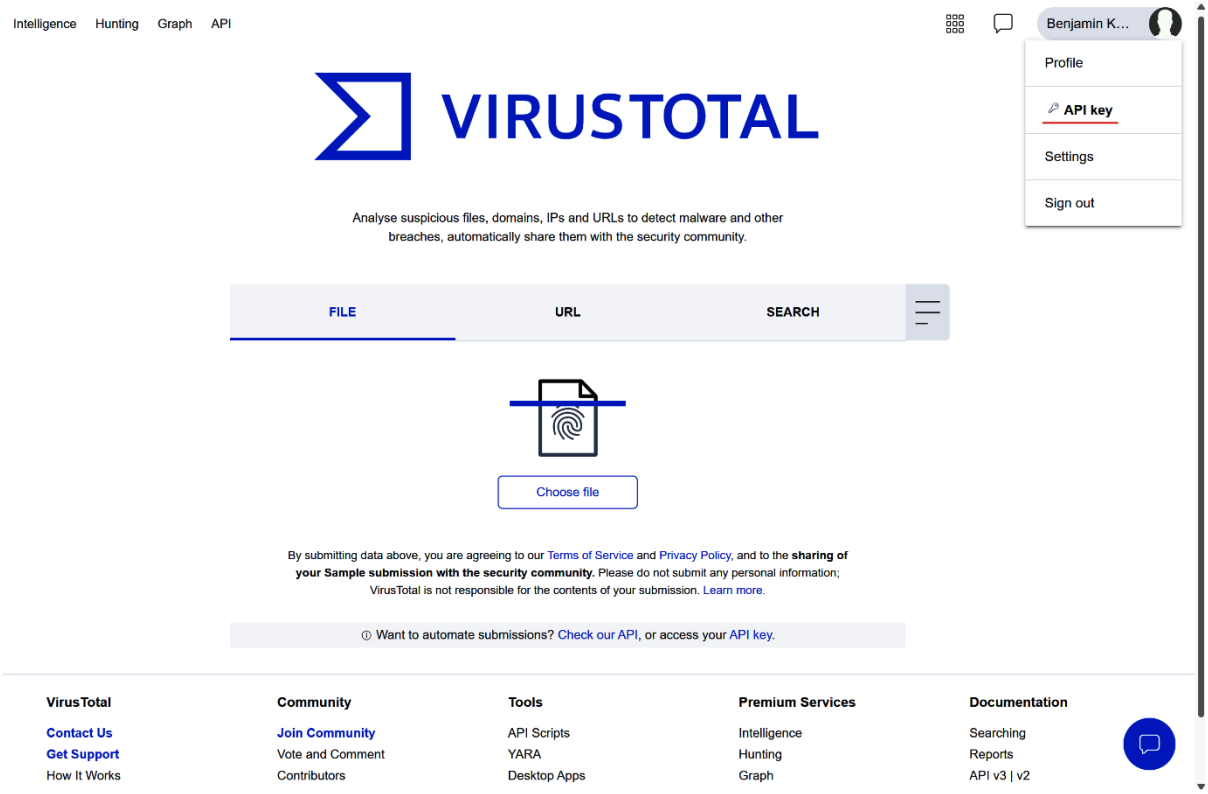
Filter by name...

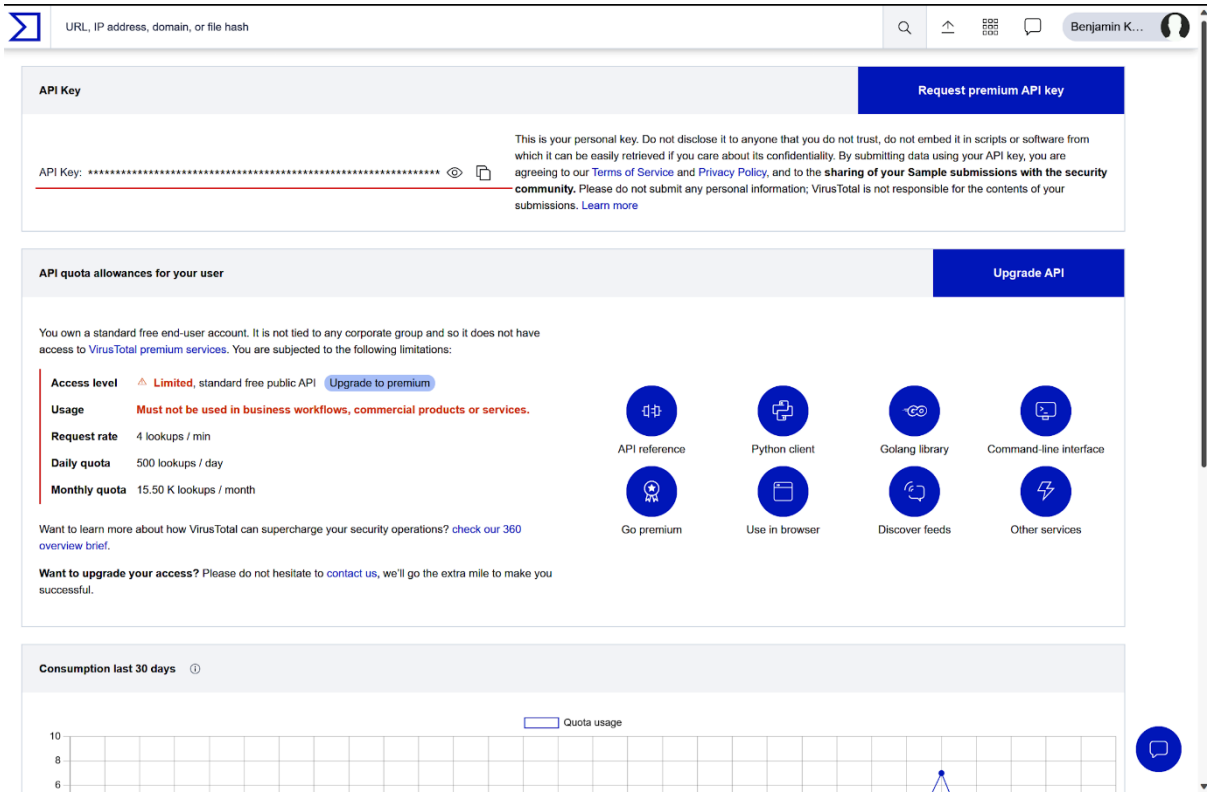
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
SOAR	westeurope	soar	VS FTE	CybSec Guru
TestUSEast	eastus	test	VS FTE	CybSec Guru
TestWestEU	westeurope	test	VS FTE	CybSec Guru

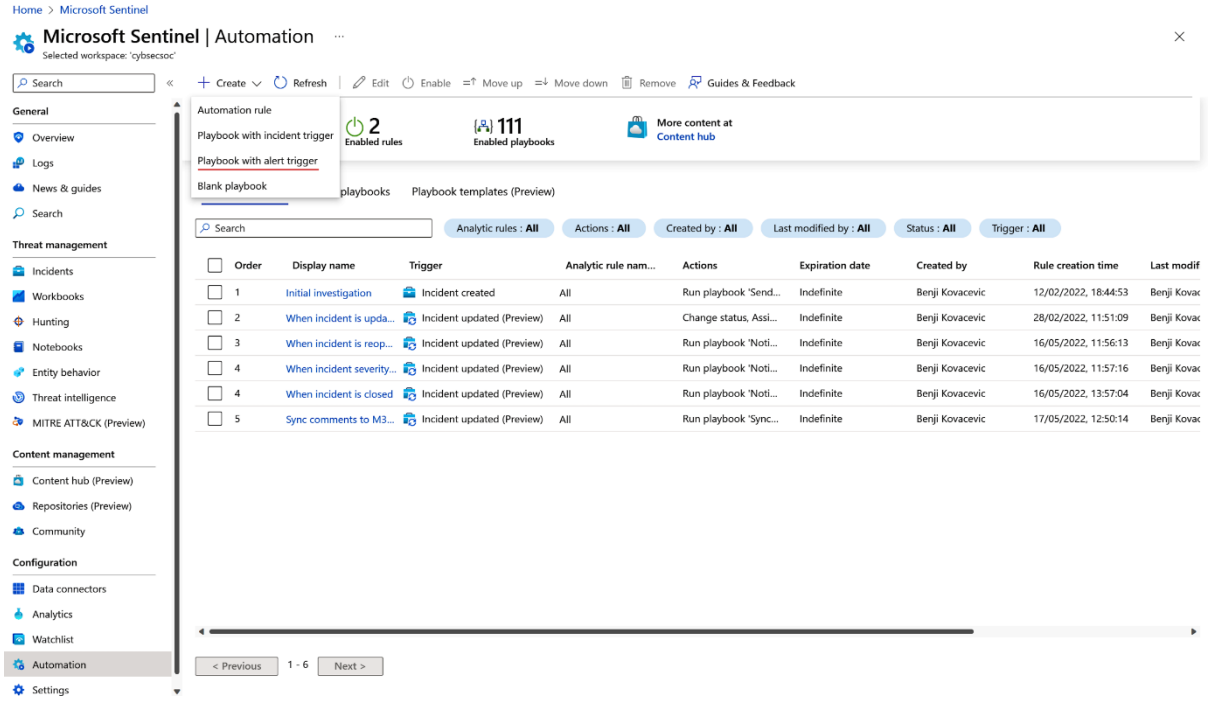
Add Cancel




Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel
Microsoft Sentinel | Content hub (Preview)
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Refresh
Guides & Feedback
245
Solutions
0
Installed
0
Updates
training lab
Status : All
Content type : All
Support : All
Provider : All
Category : All
PREVIEW
Training Lab
Microsoft Corporation
Training and Tutorials
Analytics rule (3)
Hunting query (2)
+3
Training Lab
Microsoft
Provider
Microsoft
Support
1.0.6
Version
Description
Microsoft Sentinel Training Lab helps you get ramped up with Microsoft Sentinel providing hands-on practical experience for product features, capabilities, and scenarios. To get started, visit the training guide with step-by-step instructions.
This solution ingests pre-recorded data into your Microsoft Sentinel workspace and enables several artifacts to simulate scenarios that showcase various Microsoft Sentinel features. The size of the ingested data is around ~20 MBs, so you will see no cost related to ingestion. Pre-recorded data will land in the following custom log tables: SecurityEvent_CL, SigninLogs_CL, OfficeActivity_CL, AzureActivity_CL, Cisco_Umbrella_dns_CL.
Microsoft Sentinel Solutions provide a consolidated way to acquire Microsoft Sentinel content like data connectors, workbooks, analytics, and automations in your workspace with a single deployment step.
Parsers: 2, Workbooks: 1, Analytic Rules: 3, Hunting Queries: 2, Playbooks: 1
Learn more about Microsoft Sentinel | Learn more about Solutions
Install


Intelligence
Hunting
Graph
API
Benjamin K...
Profile
API key
Settings
Sign out
VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Choose file
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.
VirusTotal
Contact Us
Get Support
How It Works
Community
Join Community
Vote and Comment
Contributors
Tools
API Scripts
YARA
Desktop Apps
Premium Services
Intelligence
Hunting
Graph
Documentation
Searching
Reports
API v3 | v2


URL, IP address, domain, or file hash
Benjamin K...
API Key
Request premium API key
API Key: ••
This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submissions with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submissions. Learn more
API quota allowances for your user
Upgrade API
You own a standard free end-user account. It is not tied to any corporate group and so it does not have access to VirusTotal premium services. You are subjected to the following limitations:
Access level Limited, standard free public API Upgrade to premium
Usage Must not be used in business workflows, commercial products or services.
Request rate 4 lookups / min
Daily quota 500 lookups / day
Monthly quota 15.50 K lookups / month
Want to learn more about how VirusTotal can supercharge your security operations? check our 360 overview brief.
Want to upgrade your access? Please do not hesitate to contact us, we'll go the extra mile to make you successful.
API reference
Python client
Golang library
Command-line interface
Go premium
Use in browser
Discover feeds
Other services
Consumption last 30 days
Quota usage
10
8
6


Home > Microsoft Sentinel
Microsoft Sentinel | Automation
Selected workspace: 'cybsecsoc'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Create
Refresh
Edit
Enable
Move up
Move down
Remove
Guides & Feedback
Automation rule
Playbook with incident trigger
Playbook with alert trigger
Blank playbook
2
Enabled rules
111
Enabled playbooks
More content at
Content hub
playbooks
Playbook templates (Preview)
Search
Analytic rules : All
Actions : All
Created by : All
Last modified by : All
Status : All
Trigger : All
Order
Display name
Trigger
Analytic rule nam...
Actions
Expiration date
Created by
Rule creation time
Last modif
1 Initial investigation Incident created All Run playbook 'Send... Indefinite Benji Kovacevic 12/02/2022, 18:44:53 Benji Kovac
2 When incident is upda... Incident updated (Preview) All Change status, Assi... Indefinite Benji Kovacevic 28/02/2022, 11:51:09 Benji Kovac
3 When incident is reop... Incident updated (Preview) All Run playbook 'Noti... Indefinite Benji Kovacevic 16/05/2022, 11:56:13 Benji Kovac
4 When incident severity... Incident updated (Preview) All Run playbook 'Noti... Indefinite Benji Kovacevic 16/05/2022, 11:57:16 Benji Kovac
4 When incident is closed Incident updated (Preview) All Run playbook 'Noti... Indefinite Benji Kovacevic 16/05/2022, 13:57:04 Benji Kovac
5 Sync comments to M3... Incident updated (Preview) All Run playbook 'Sync... Indefinite Benji Kovacevic 17/05/2022, 12:50:14 Benji Kovac
< Previous
1 - 6
Next >

Home > Microsoft Sentinel | Automation >

Create playbook ...

1 Basics 2 Connections 3 Review and create

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

Subscription *: VS FTE

Resource group *: CyberSecurity

Create new

Region *: East US

Playbook name *: VirusTotal-IPEnrichment-alertTrigger

Enable diagnostics logs in Log Analytics

Log Analytics workspace: cybsecsoc

Associate with integration service environment

Integration service environment:

Next : Connections >

Home > Microsoft Sentinel | Automation >

Create playbook ...

Basics 2 Connections 3 Review and create

For each connector this playbook uses, you can choose to use an existing connection from another playbook. Otherwise, you must create a new connection and authenticate when you are brought to the Logic Apps designer after your playbook is deployed.

Microsoft Sentinel Connect with managed identity

Previous Next : Review and create >

Home > Microsoft Sentinel | Automation >

Create playbook ...

Basics | Connections | 3 Review and create

Basics

Subscription	VS FTE
Resource group	CyberSecurity
Region	East US
Playbook name	VirusTotal-IPEnrichment-alertTrigger
Diagnostics logs workspace	Disabled
Integration service environment	Disabled

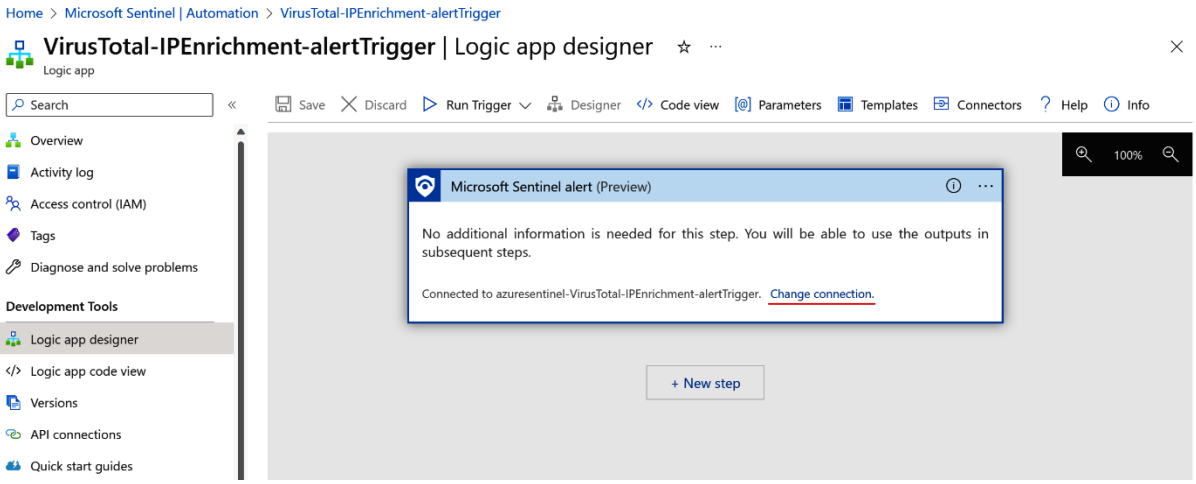
Connections

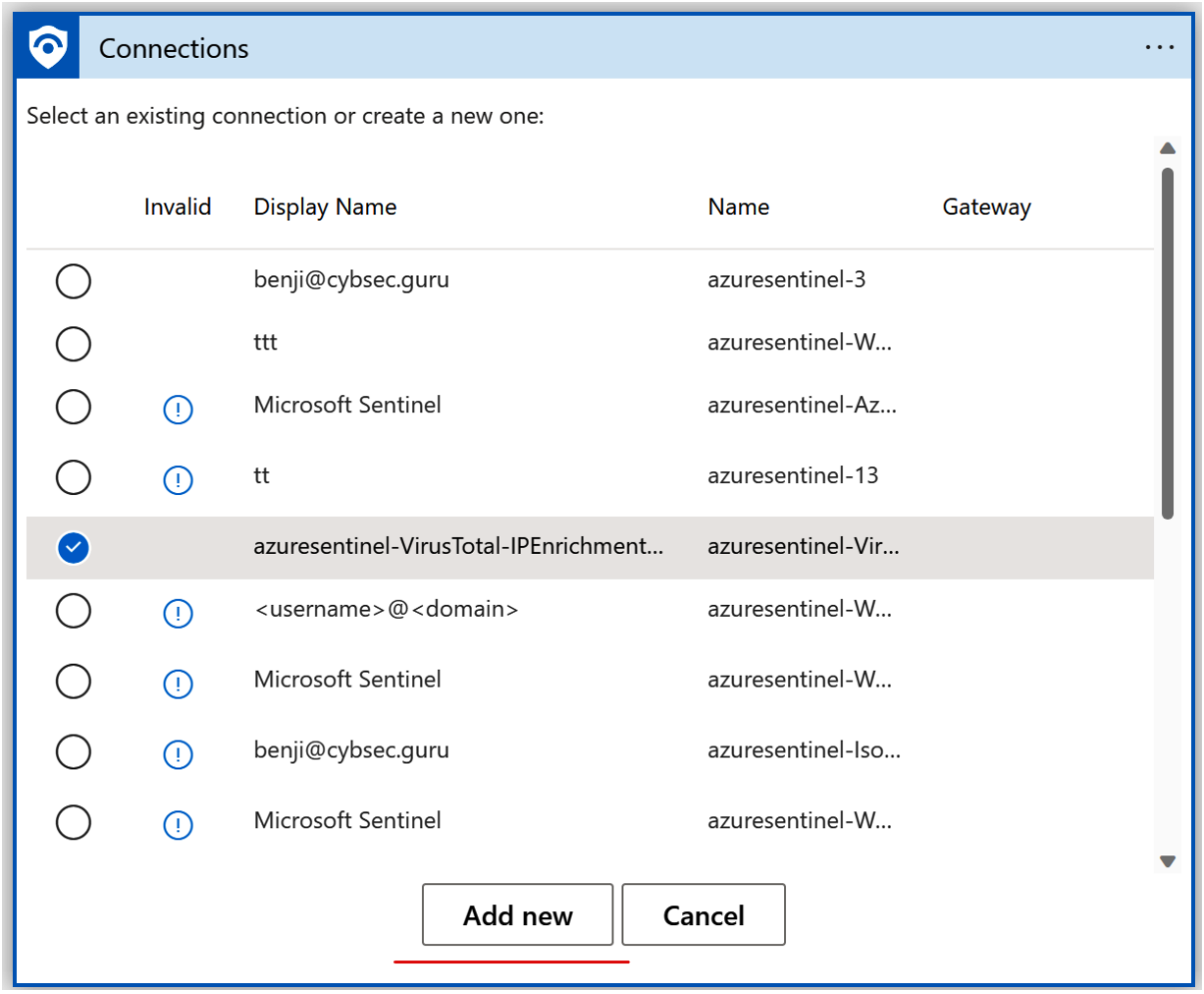
Microsoft Sentinel

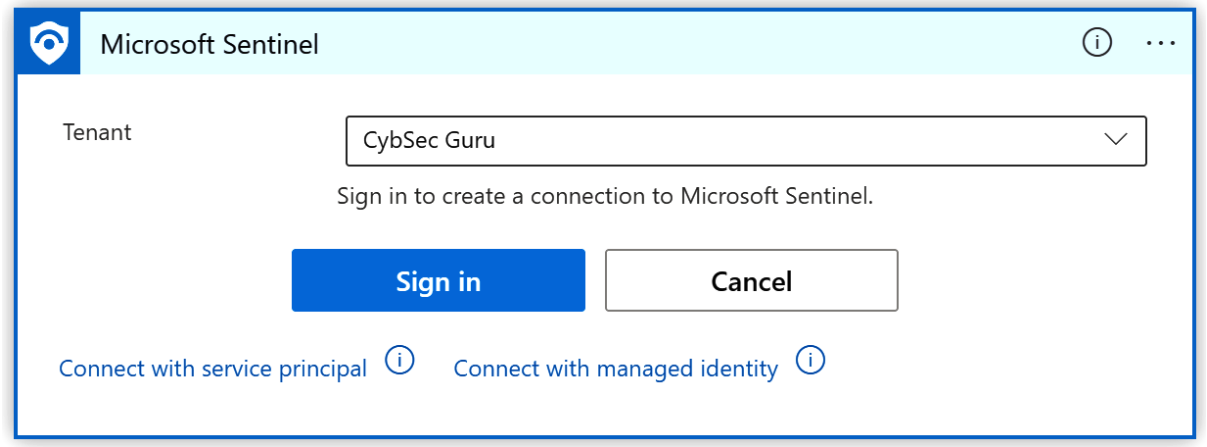
Connect with managed identity

Note: Grant permissions to the managed identity after deployment.

Previous | Create and continue to designer



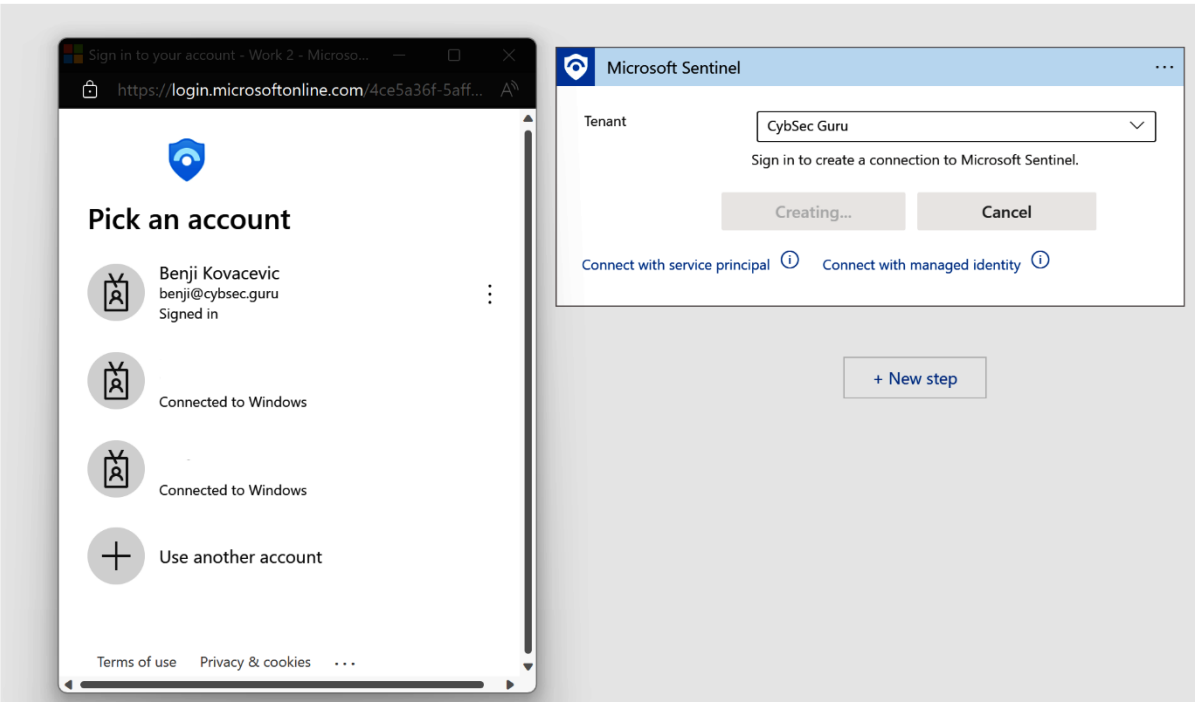

Connections
Select an existing connection or create a new one:
Invalid
Display Name
Name
Gateway
benji@cybsec.guru
azuresentinel-3
ttt
azuresentinel-W...
Microsoft Sentinel
azuresentinel-Az...
tt
azuresentinel-13
azuresentinel-VirusTotal-IPEnrichment...
azuresentinel-Vir...
<username>@<domain>
azuresentinel-W...
Microsoft Sentinel
azuresentinel-W...
benji@cybsec.guru
azuresentinel-Iso...
Microsoft Sentinel
azuresentinel-W...
Add new
Cancel

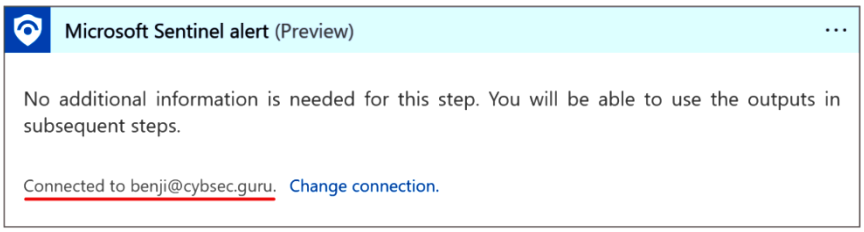

Microsoft Sentinel
Tenant
CybSec Guru
Sign in to create a connection to Microsoft Sentinel.
Sign in
Cancel
Connect with service principal
Connect with managed identity

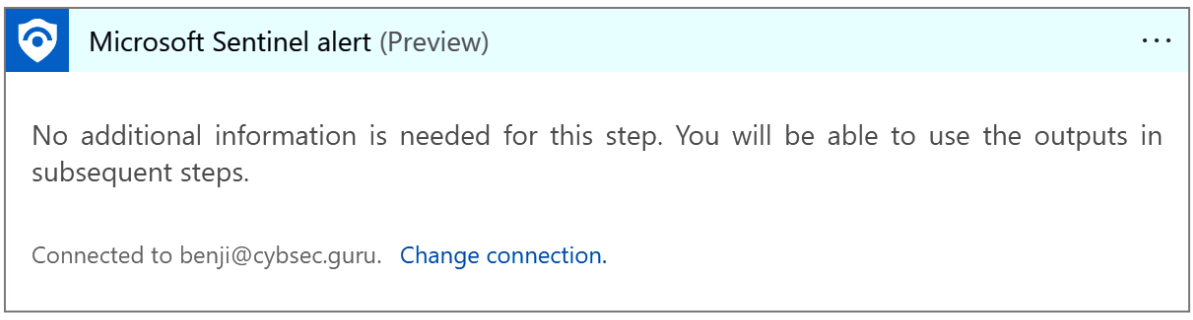
Home > Microsoft Sentinel | Automation > VirusTotal-IPEnrichment-alertTrigger >

Logic Apps Designer ...

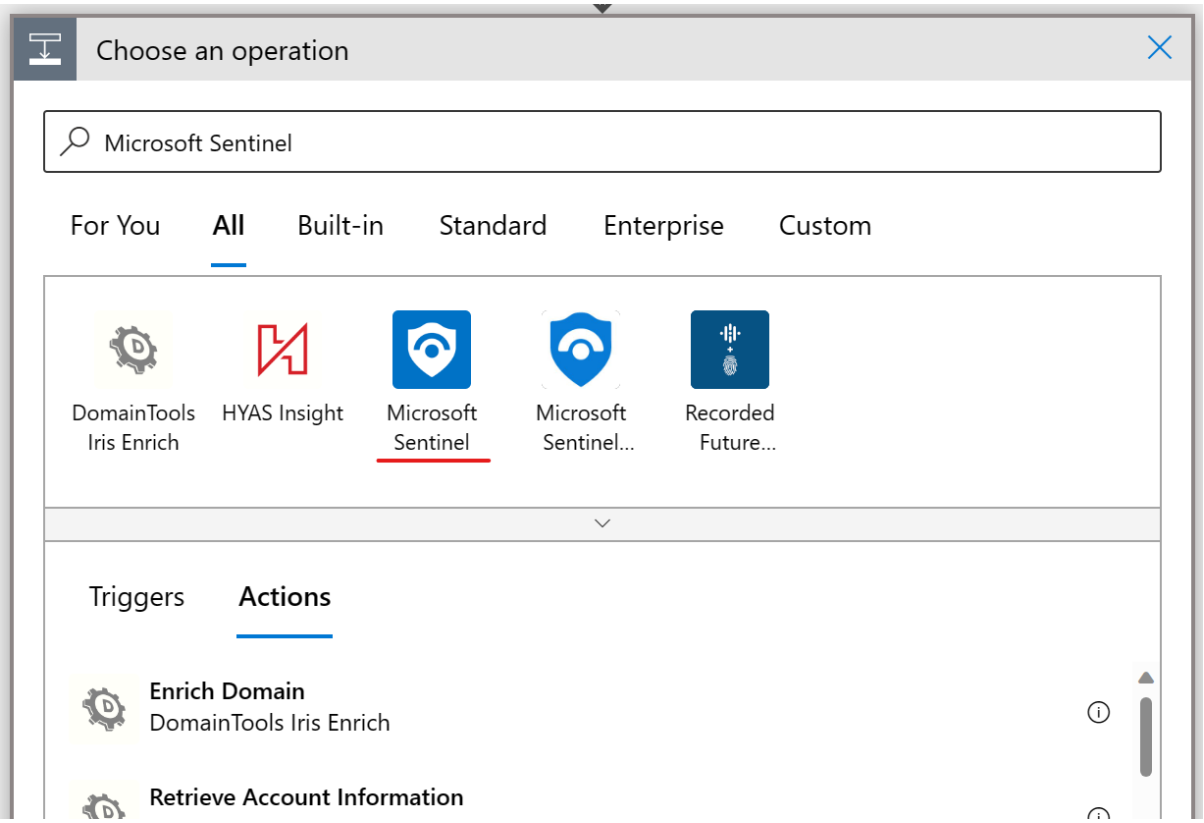
Save | Discard | Run Trigger | Designer | Code view | Parameters | Templates | Connectors | Help | Info

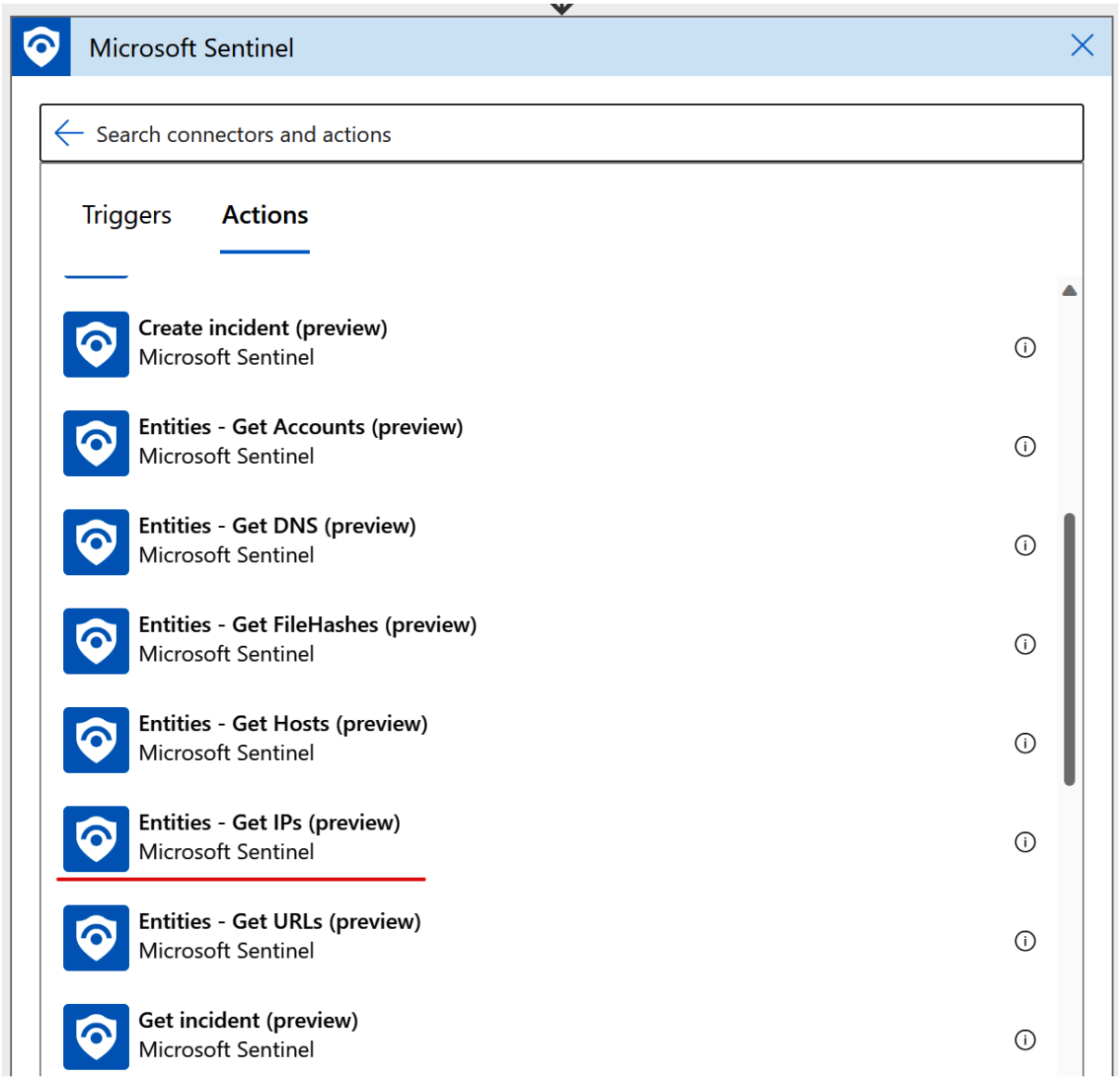


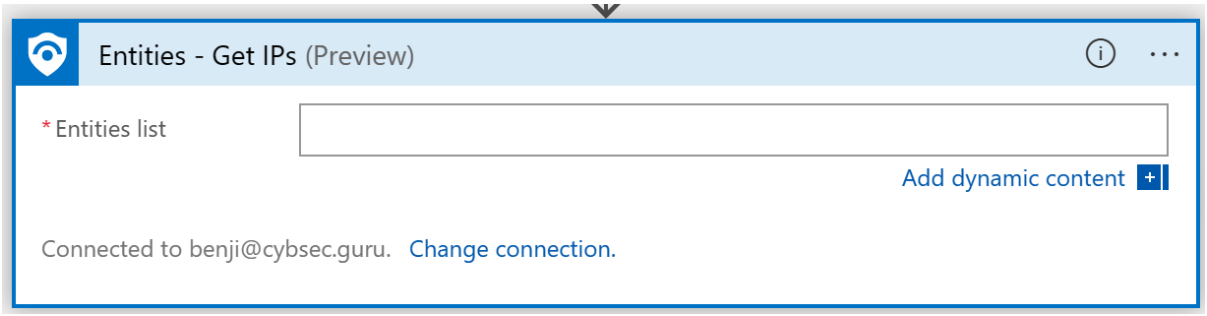


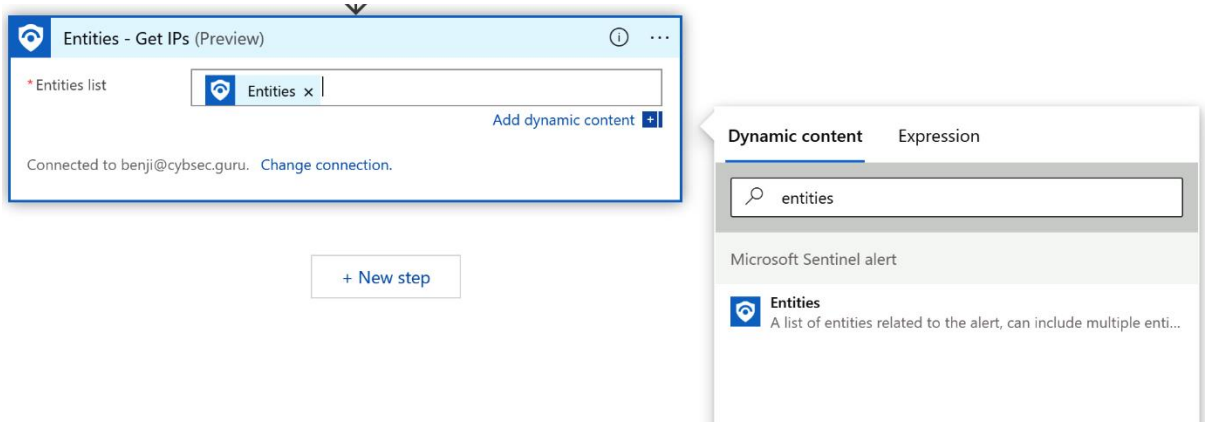


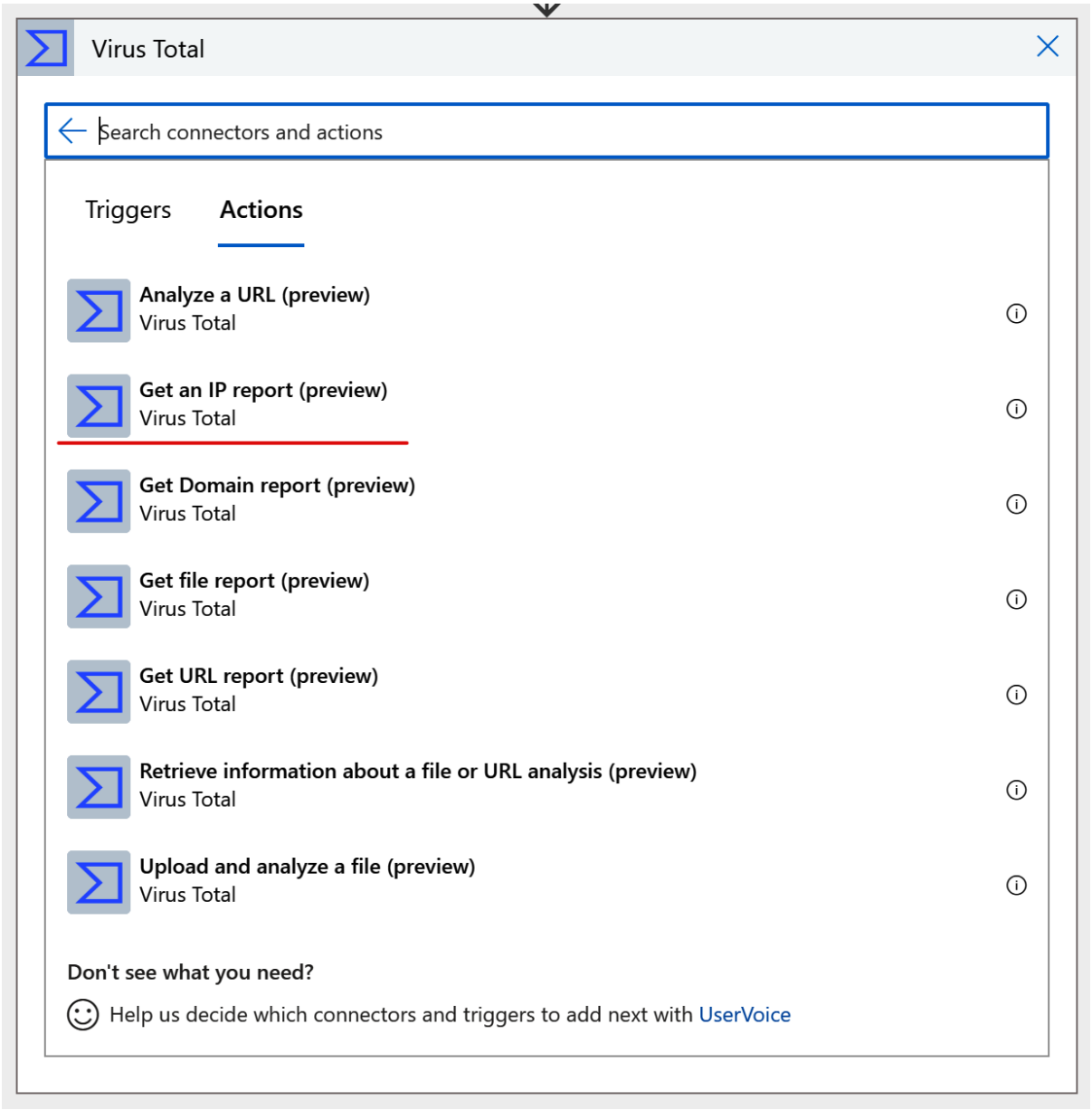
+ New step

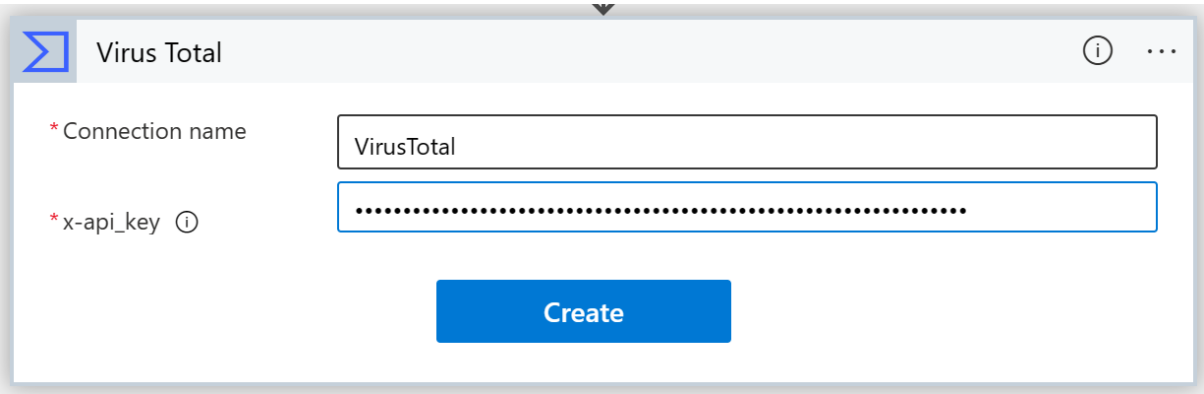

Choose an operation
Microsoft Sentinel
For You
All
Built-in
Standard
Enterprise
Custom
DomainTools Iris Enrich
HYAS Insight
Microsoft Sentinel
Microsoft Sentinel...
Recorded Future...
Triggers
Actions
Enrich Domain
DomainTools Iris Enrich
Retrieve Account Information

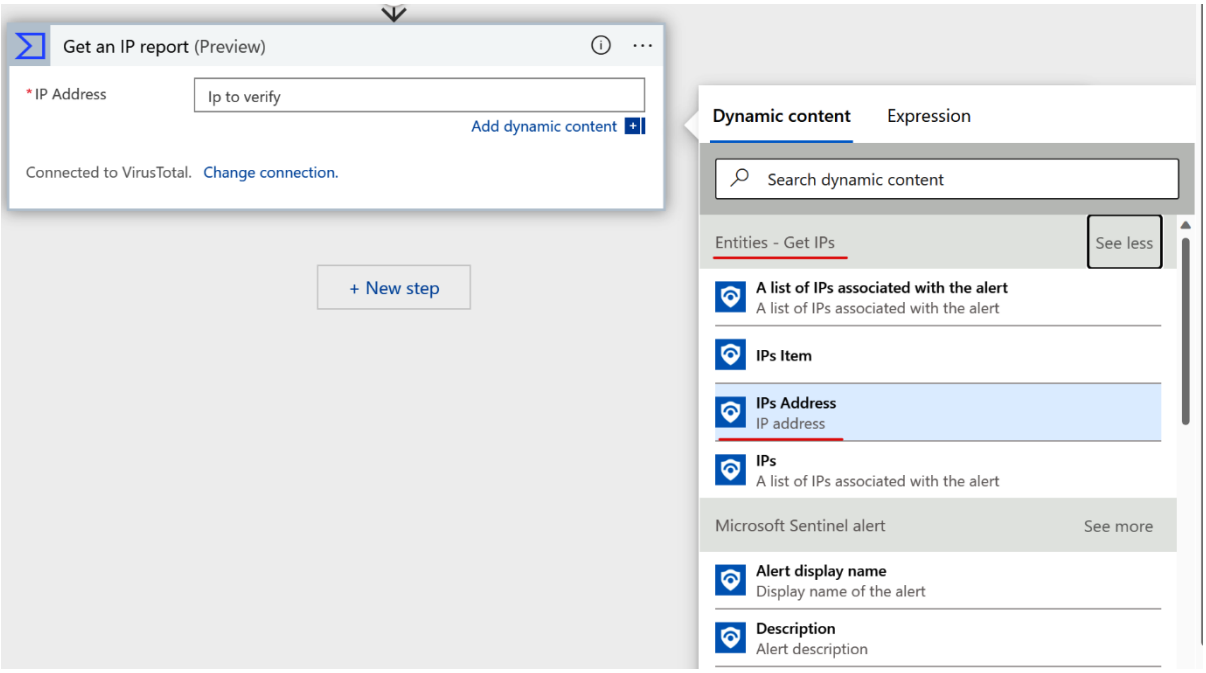

Microsoft Sentinel
Search connectors and actions
Triggers
Actions
Create incident (preview)
Microsoft Sentinel
Entities - Get Accounts (preview)
Microsoft Sentinel
Entities - Get DNS (preview)
Microsoft Sentinel
Entities - Get FileHashes (preview)
Microsoft Sentinel
Entities - Get Hosts (preview)
Microsoft Sentinel
Entities - Get IPs (preview)
Microsoft Sentinel
Entities - Get URLs (preview)
Microsoft Sentinel
Get incident (preview)
Microsoft Sentinel

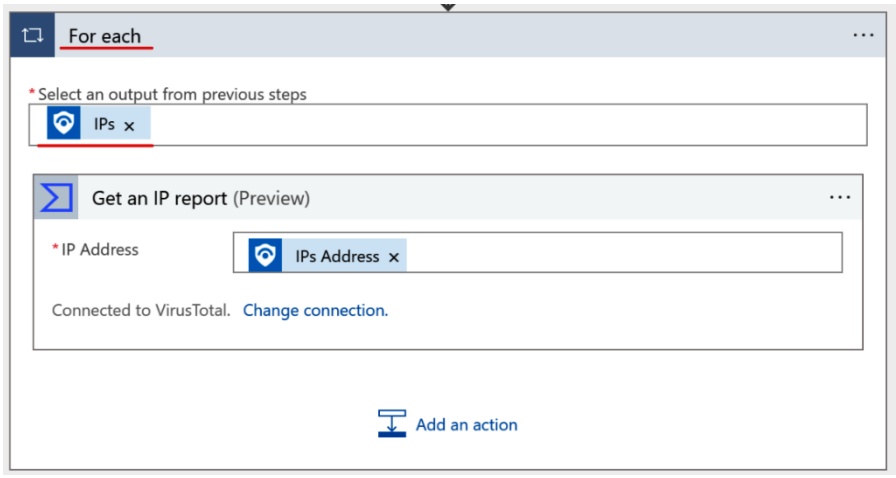

Entities - Get IPs (Preview)
* Entities list
Add dynamic content
Connected to benji@cybsec.guru.
Change connection.

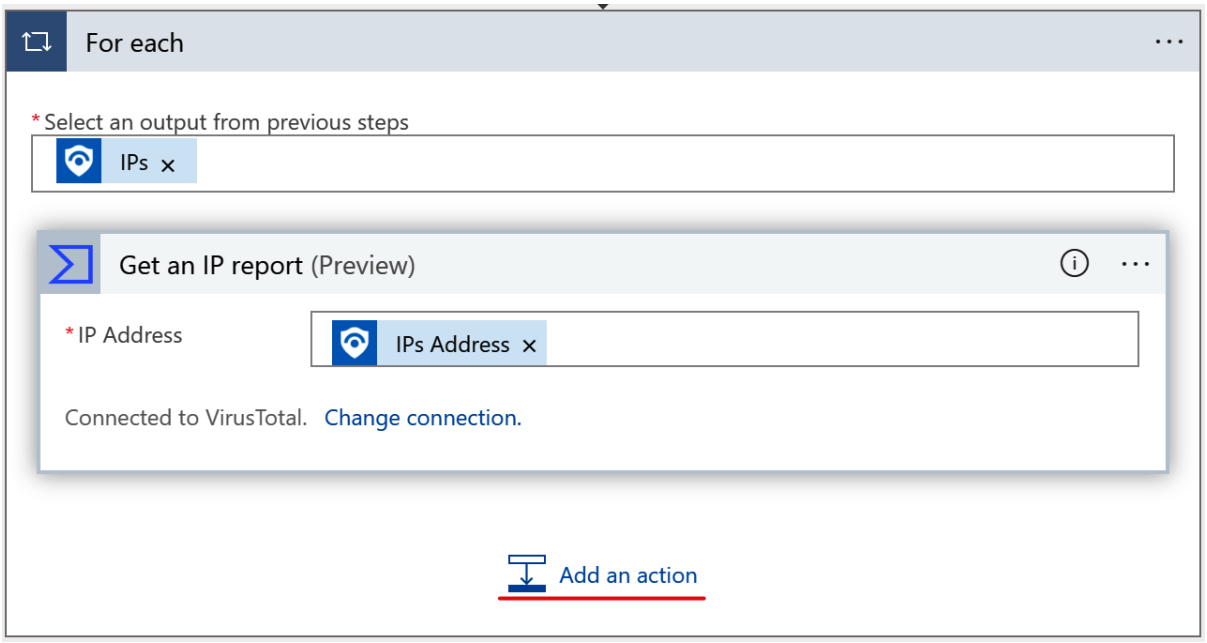

Entities - Get IPs (Preview)
* Entities list
Entities
Add dynamic content
Connected to benji@cybsec.guru. Change connection.
+ New step
Dynamic content
Expression
entities
Microsoft Sentinel alert
Entities
A list of entities related to the alert, can include multiple enti...

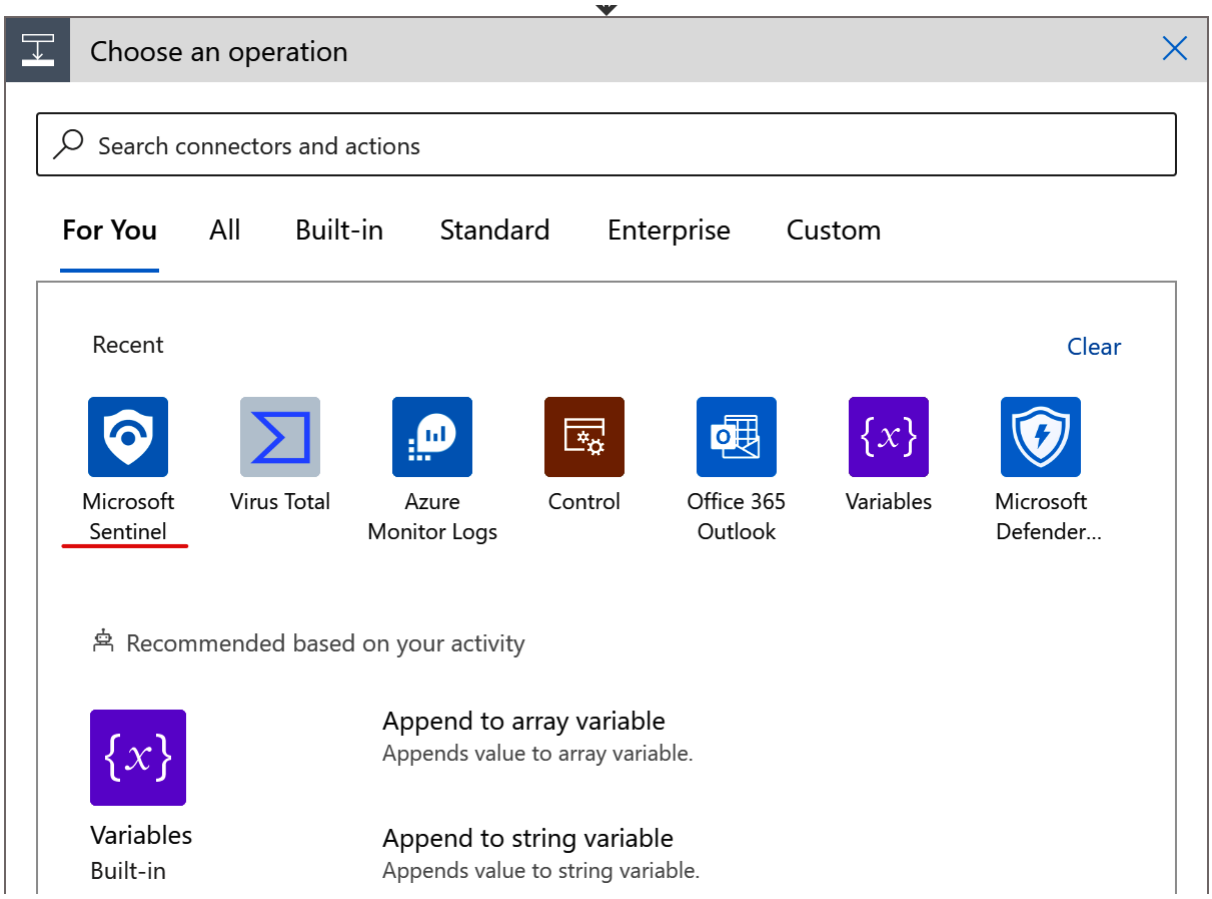

Virus Total
Search connectors and actions
Triggers
Actions
Analyze a URL (preview)
Virus Total
Get an IP report (preview)
Virus Total
Get Domain report (preview)
Virus Total
Get file report (preview)
Virus Total
Get URL report (preview)
Virus Total
Retrieve information about a file or URL analysis (preview)
Virus Total
Upload and analyze a file (preview)
Virus Total
Don't see what you need?
Help us decide which connectors and triggers to add next with UserVoice

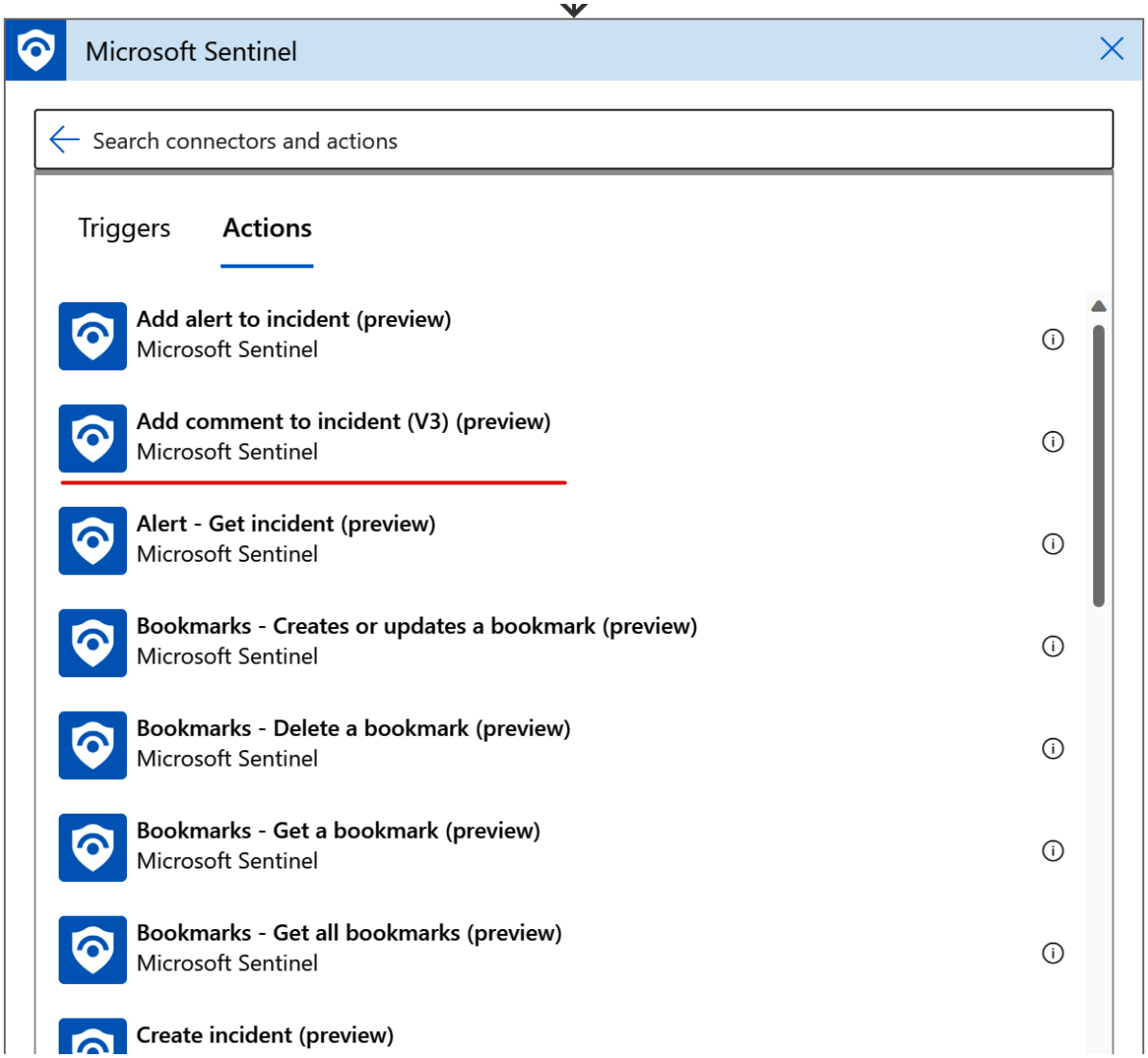

Virus Total
* Connection name
VirusTotal
* x-api_key
Create

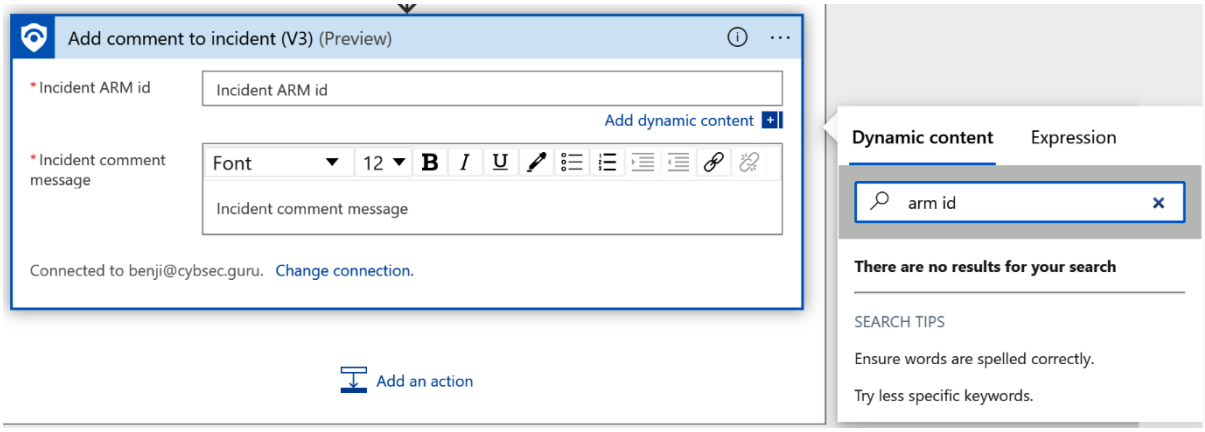

Get an IP report (Preview)
* IP Address
Ip to verify
Add dynamic content
Connected to VirusTotal. Change connection.
+ New step
Dynamic content
Expression
Search dynamic content
Entities - Get IPs
See less
A list of IPs associated with the alert
A list of IPs associated with the alert
IPs Item
IPs Address
IP address
IPs
A list of IPs associated with the alert
Microsoft Sentinel alert
See more
Alert display name
Display name of the alert
Description
Alert description

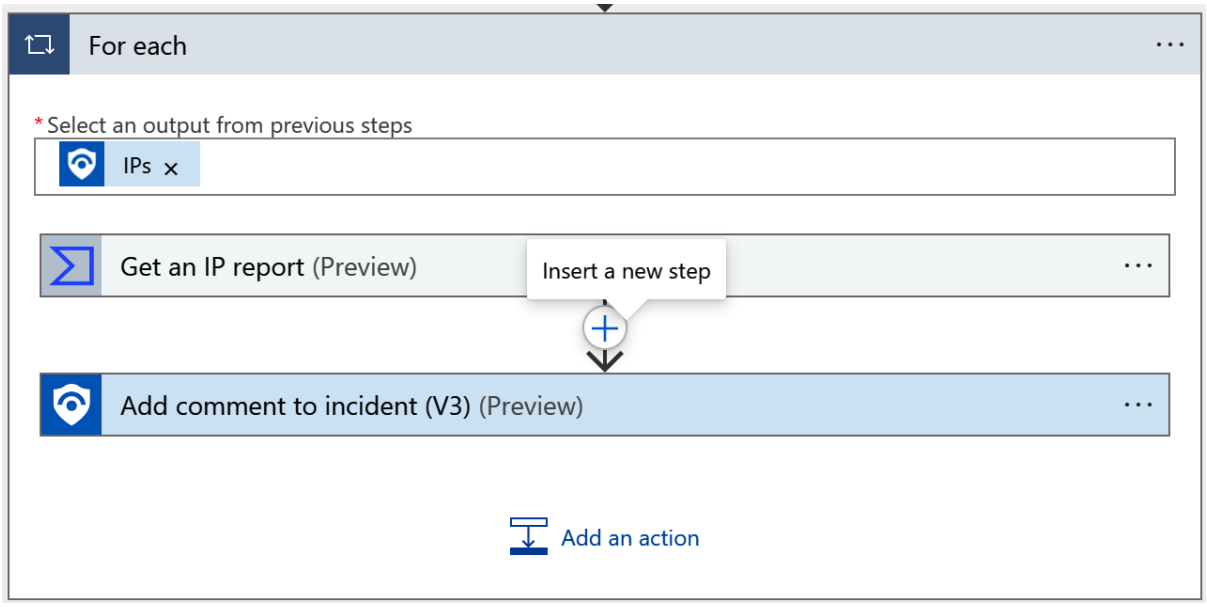

For each
* Select an output from previous steps
IPs
Get an IP report (Preview)
* IP Address
IPs Address
Connected to VirusTotal. Change connection.
Add an action

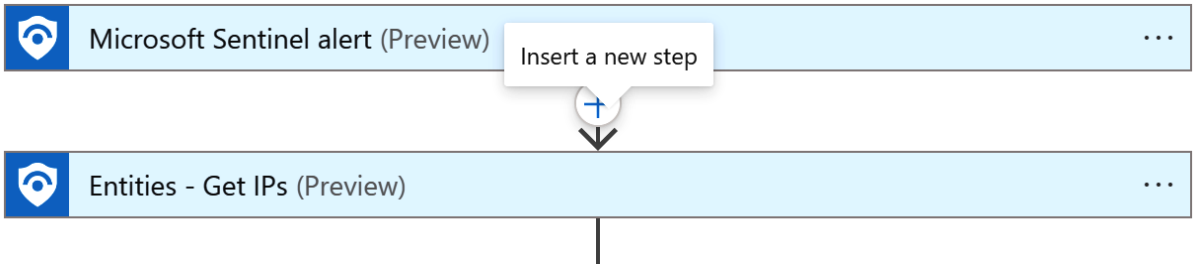

For each
* Select an output from previous steps
IPs
Get an IP report (Preview)
* IP Address
IPs Address
Connected to VirusTotal. Change connection.
Add an action

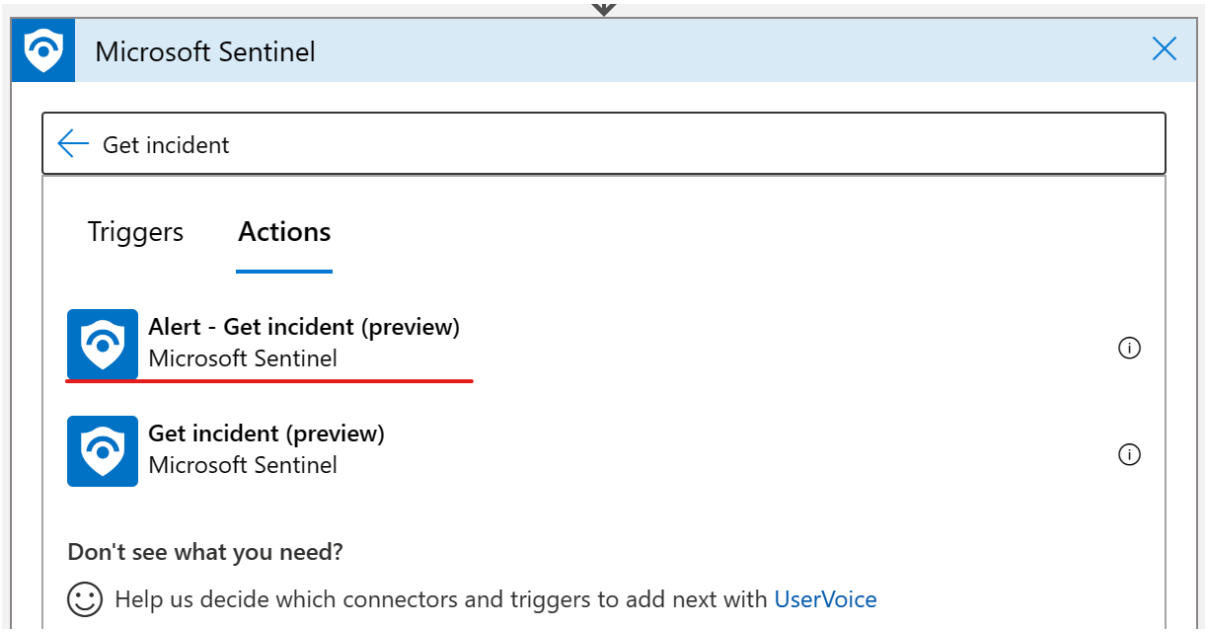

Choose an operation
Search connectors and actions
For You
All
Built-in
Standard
Enterprise
Custom
Recent
Clear
Microsoft Sentinel
Virus Total
Azure Monitor Logs
Control
Office 365 Outlook
Variables
Microsoft Defender...
Recommended based on your activity
Variables
Built-in
Append to array variable
Appends value to array variable.
Append to string variable
Appends value to string variable.

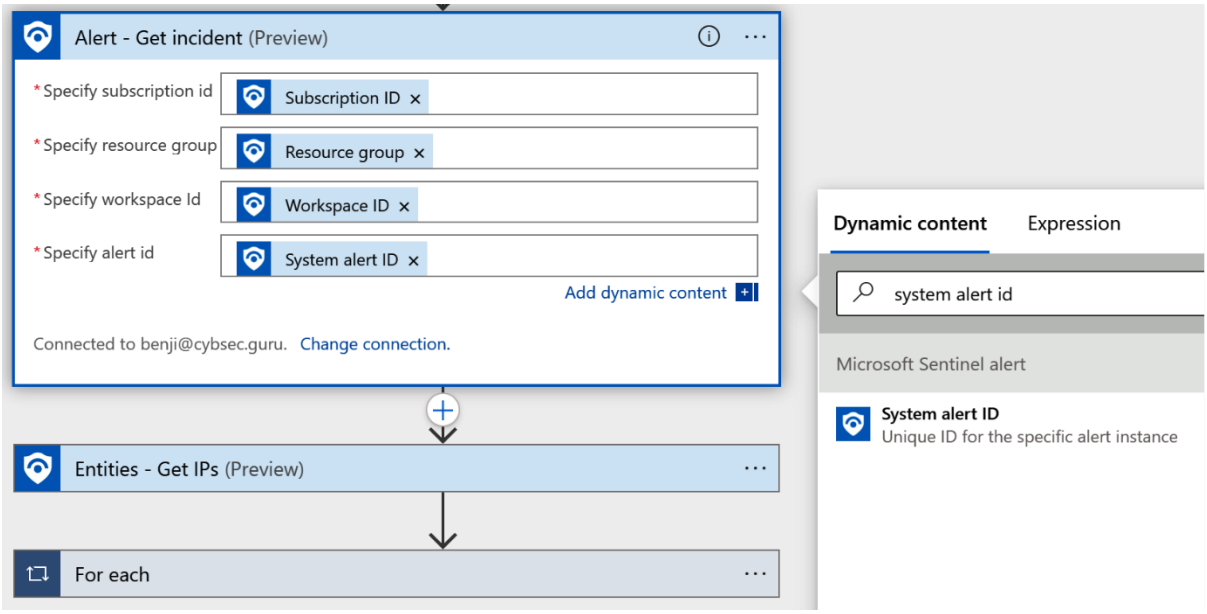

Microsoft Sentinel
Search connectors and actions
Triggers
Actions
Add alert to incident (preview)
Microsoft Sentinel
Add comment to incident (V3) (preview)
Microsoft Sentinel
Alert - Get incident (preview)
Microsoft Sentinel
Bookmarks - Creates or updates a bookmark (preview)
Microsoft Sentinel
Bookmarks - Delete a bookmark (preview)
Microsoft Sentinel
Bookmarks - Get a bookmark (preview)
Microsoft Sentinel
Bookmarks - Get all bookmarks (preview)
Microsoft Sentinel
Create incident (preview)

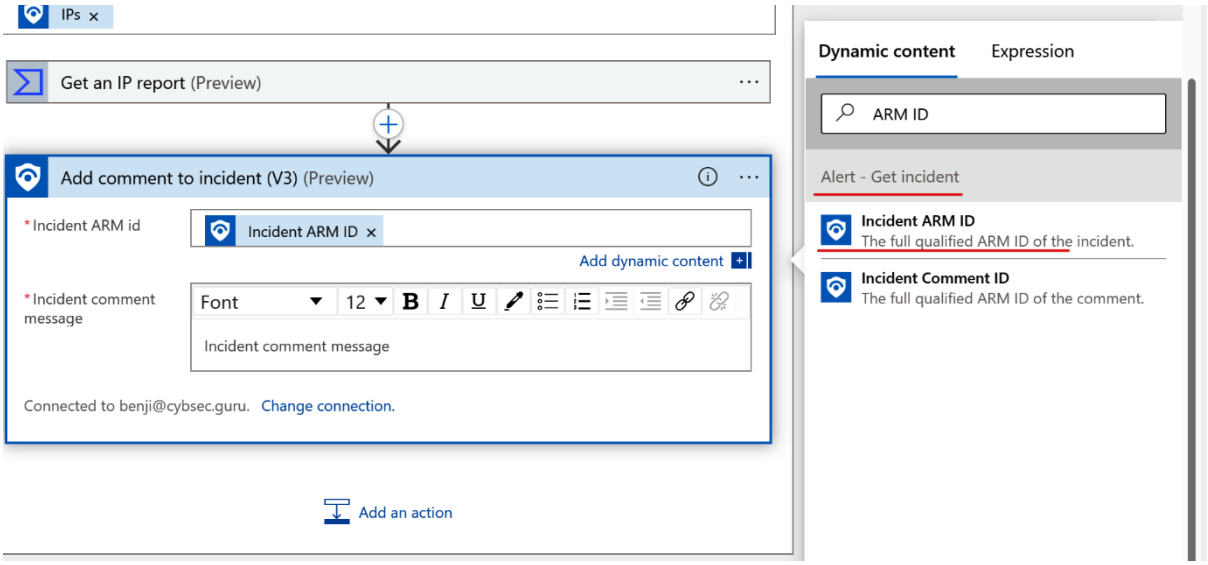

Add comment to incident (V3) (Preview)
* Incident ARM id
Incident ARM id
Add dynamic content
* Incident comment message
Font
12
Incident comment message
Connected to benji@cybsec.guru. Change connection.
Add an action
Dynamic content
Expression
arm id
There are no results for your search
SEARCH TIPS
Ensure words are spelled correctly.
Try less specific keywords.

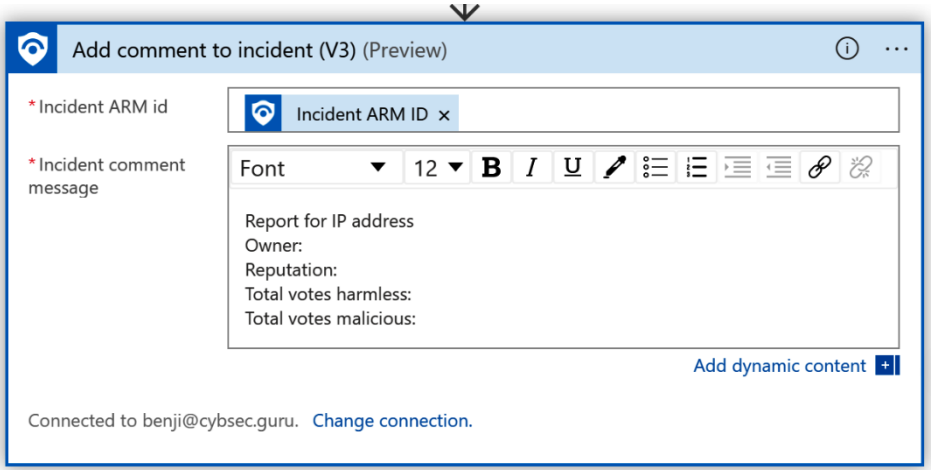

For each
* Select an output from previous steps
IPs
Get an IP report (Preview)
Insert a new step
Add comment to incident (V3) (Preview)
Add an action

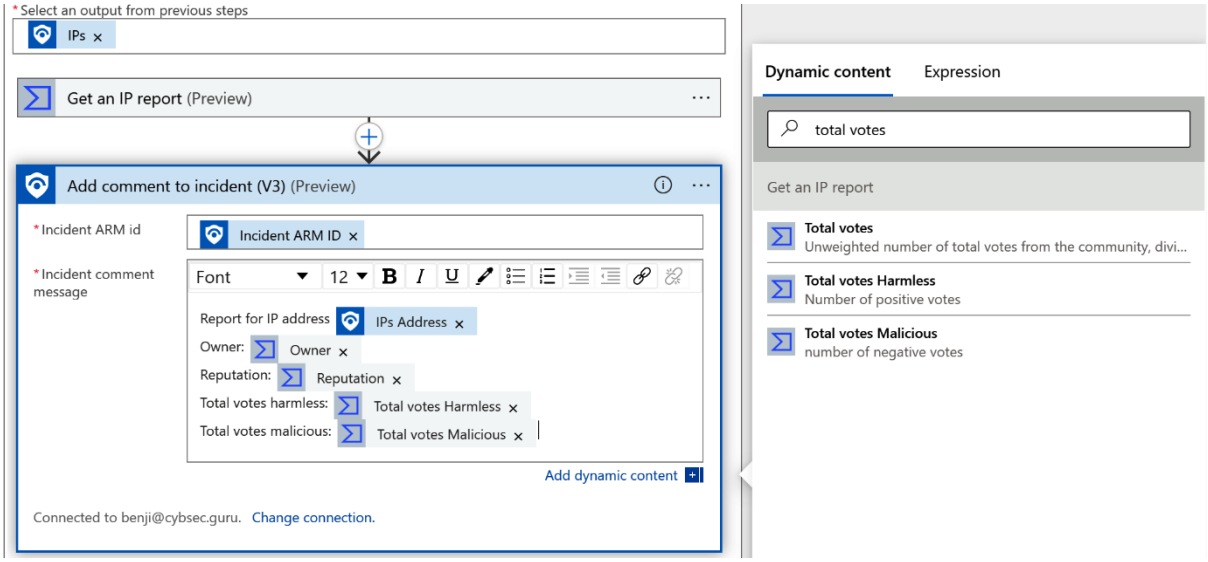

Microsoft Sentinel alert (Preview)
Insert a new step
Entities - Get IPs (Preview)

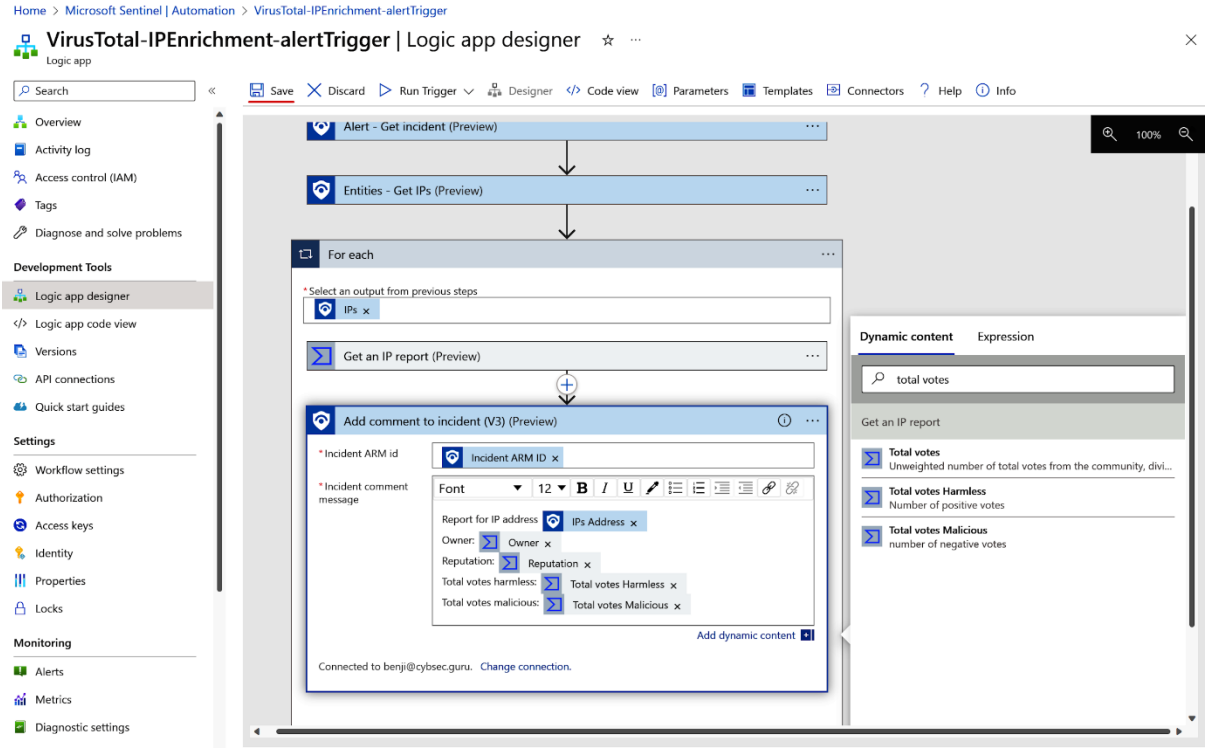

Microsoft Sentinel
Get incident
Triggers
Actions
Alert - Get incident (preview)
Microsoft Sentinel
Get incident (preview)
Microsoft Sentinel
Don't see what you need?
Help us decide which connectors and triggers to add next with UserVoice

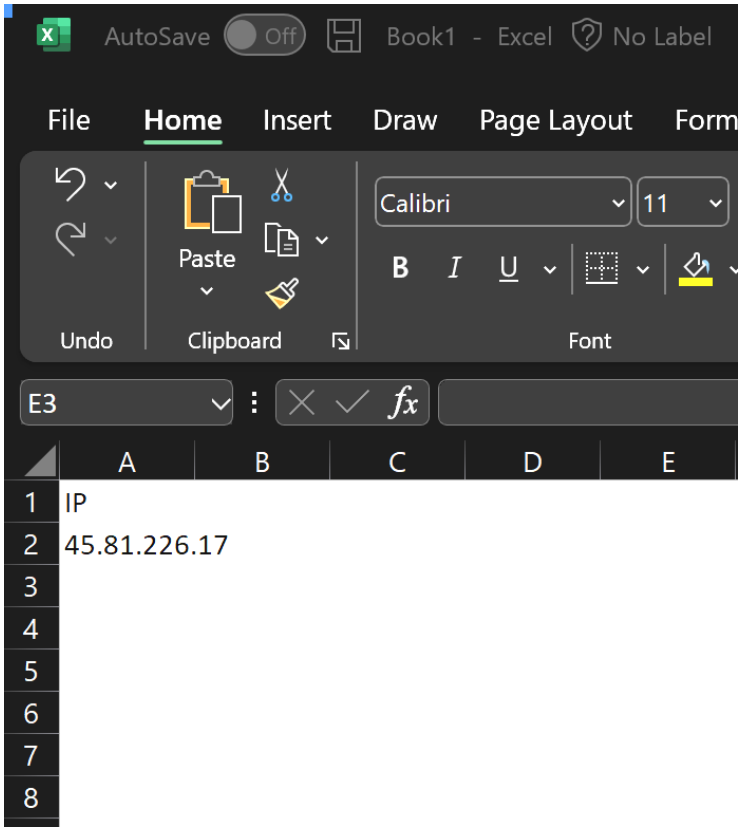

Alert - Get incident (Preview)
*Specify subscription id
Subscription ID ×
*Specify resource group
Resource group ×
*Specify workspace Id
Workspace ID ×
*Specify alert id
System alert ID ×
Add dynamic content
Connected to benji@cybsec.guru. Change connection.
Entities - Get IPs (Preview)
For each
Dynamic content
Expression
system alert id
Microsoft Sentinel alert
System alert ID
Unique ID for the specific alert instance

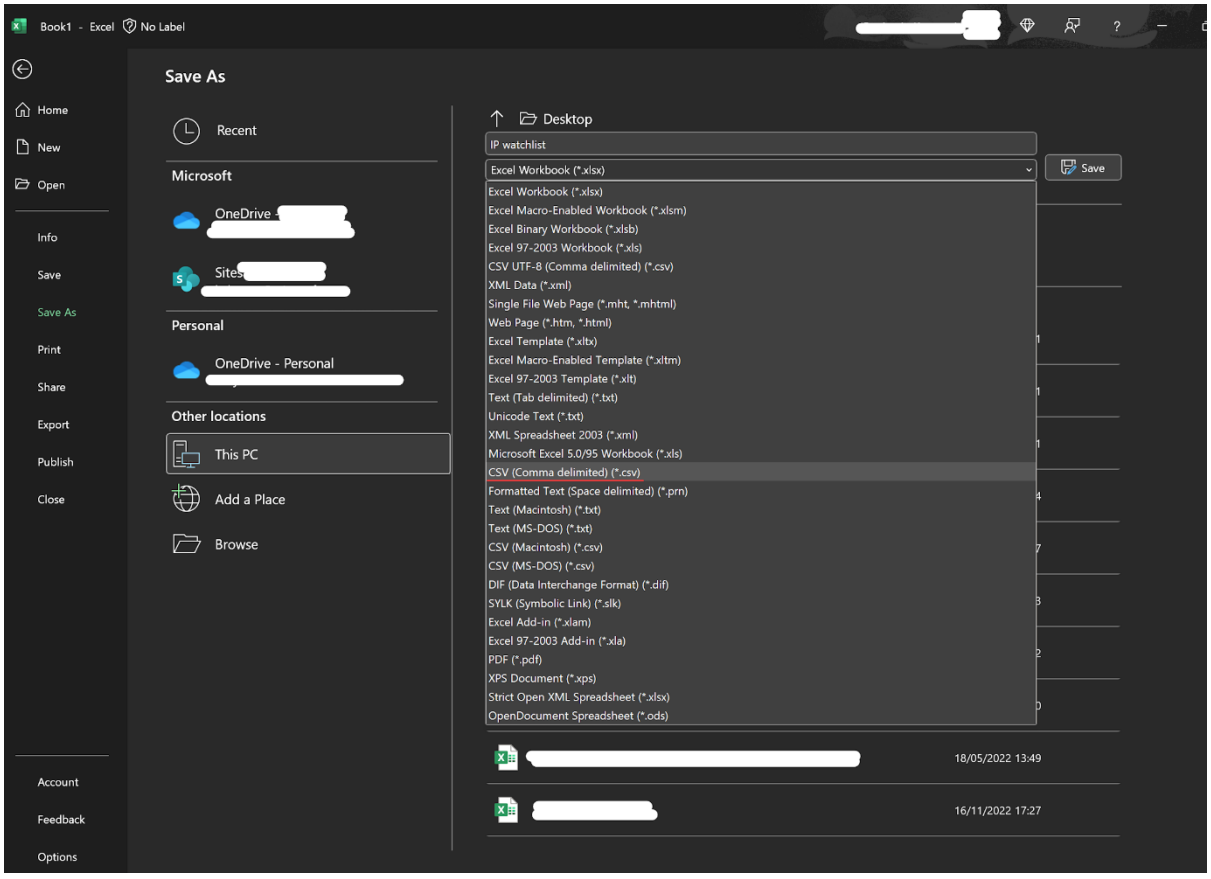

IPs ×
Get an IP report (Preview)
Add comment to incident (V3) (Preview)
*Incident ARM id
Incident ARM ID ×
Add dynamic content
*Incident comment message
Font
12
Incident comment message
Connected to benji@cybsec.guru. Change connection.
Add an action
Dynamic content
Expression
ARM ID
Alert - Get incident
Incident ARM ID
The full qualified ARM ID of the incident.
Incident Comment ID
The full qualified ARM ID of the comment.

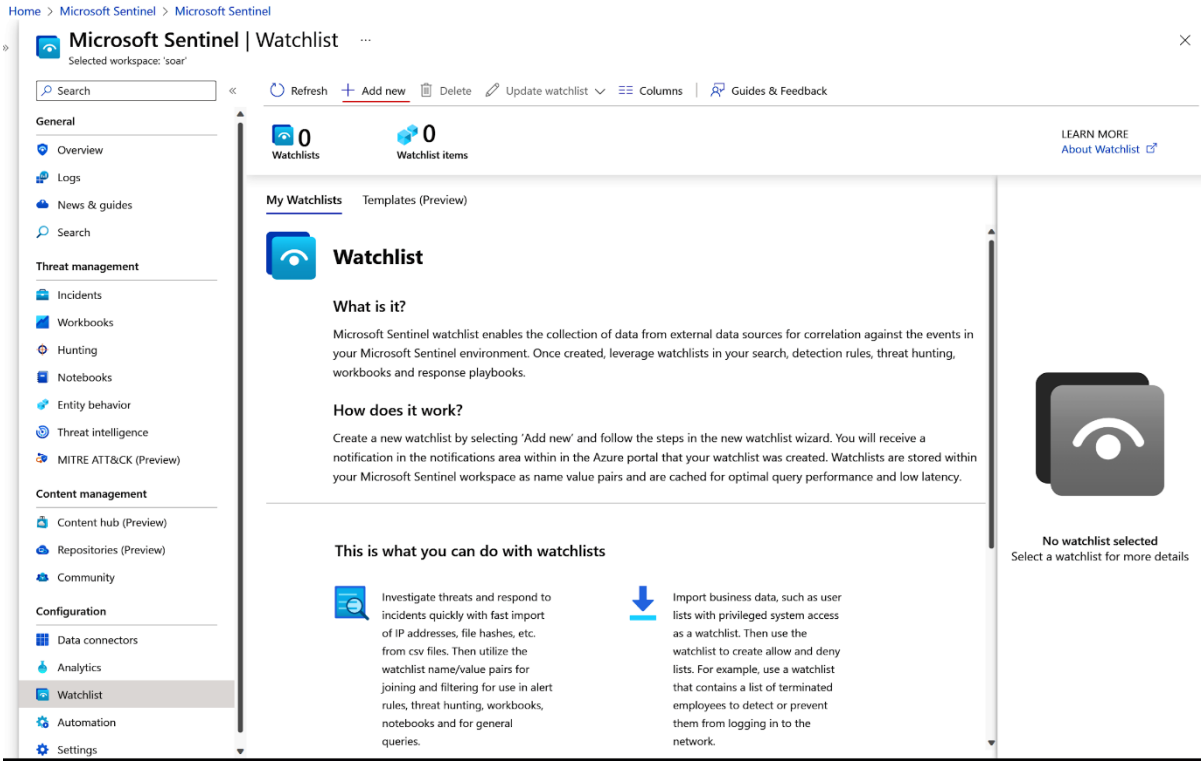

Add comment to incident (V3) (Preview)
*Incident ARM id
Incident ARM ID ×
*Incident comment message
Font
12
Report for IP address
Owner:
Reputation:
Total votes harmless:
Total votes malicious:
Add dynamic content
Connected to benji@cybsec.guru. Change connection.

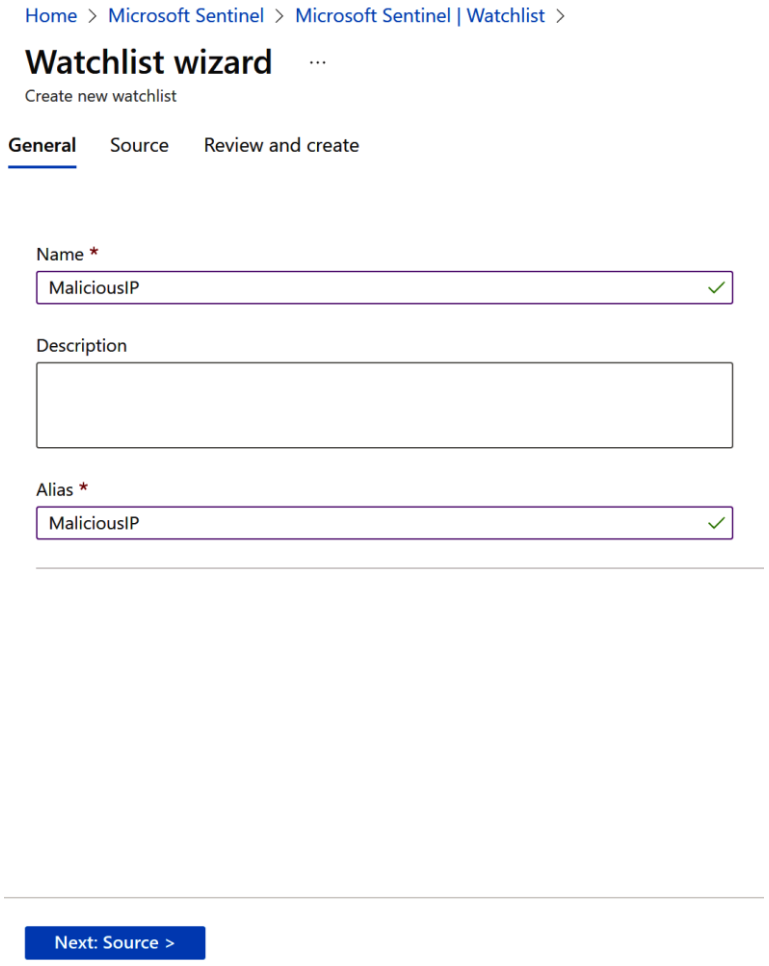

*Select an output from previous steps
IPs
Get an IP report (Preview)
Add comment to incident (V3) (Preview)
*Incident ARM id
Incident ARM ID
*Incident comment message
Font
12
Report for IP address
IPs Address
Owner:
Owner
Reputation:
Reputation
Total votes harmless:
Total votes Harmless
Total votes malicious:
Total votes Malicious
Add dynamic content
Connected to benji@cybsec.guru.
Change connection.
Dynamic content
Expression
total votes
Get an IP report
Total votes
Unweighted number of total votes from the community, divi...
Total votes Harmless
Number of positive votes
Total votes Malicious
number of negative votes

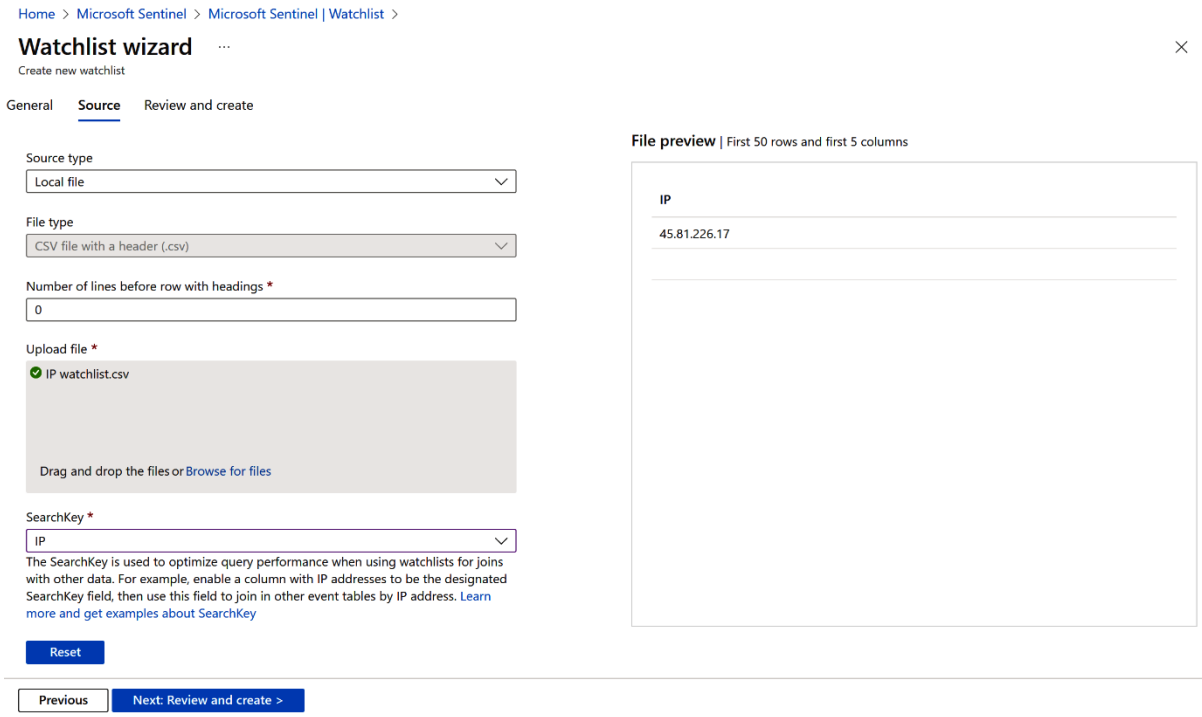

Home > Microsoft Sentinel | Automation > VirusTotal-IPEnrichment-alertTrigger
VirusTotal-IPEnrichment-alertTrigger | Logic app designer
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Save
Discard
Run Trigger
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Alert - Get incident (Preview)
Entities - Get IPs (Preview)
For each
*Select an output from previous steps
IPs
Get an IP report (Preview)
Add comment to incident (V3) (Preview)
*Incident ARM id
Incident ARM ID
*Incident comment message
Font
12
Report for IP address
IPs Address
Owner:
Owner
Reputation:
Reputation
Total votes harmless:
Total votes Harmless
Total votes malicious:
Total votes Malicious
Add dynamic content
Connected to benji@cybsec.guru.
Change connection.
100%
Dynamic content
Expression
total votes
Get an IP report
Total votes
Unweighted number of total votes from the community, divi...
Total votes Harmless
Number of positive votes
Total votes Malicious
number of negative votes

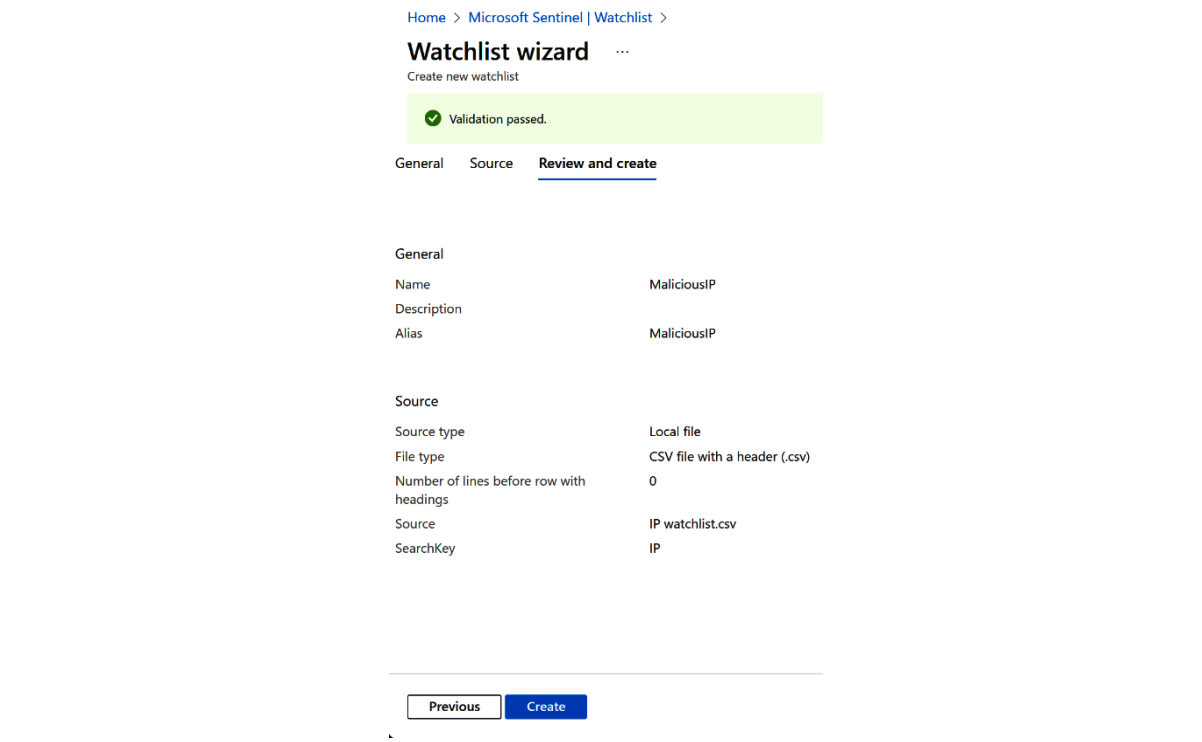

AutoSave Off
Book1 - Excel
No Label
File
Home
Insert
Draw
Page Layout
Form
Paste
Calibri
11
Undo
Clipboard
Font
E3
A
B
C
D
E
1
IP
2
45.81.226.17
3
4
5
6
7
8

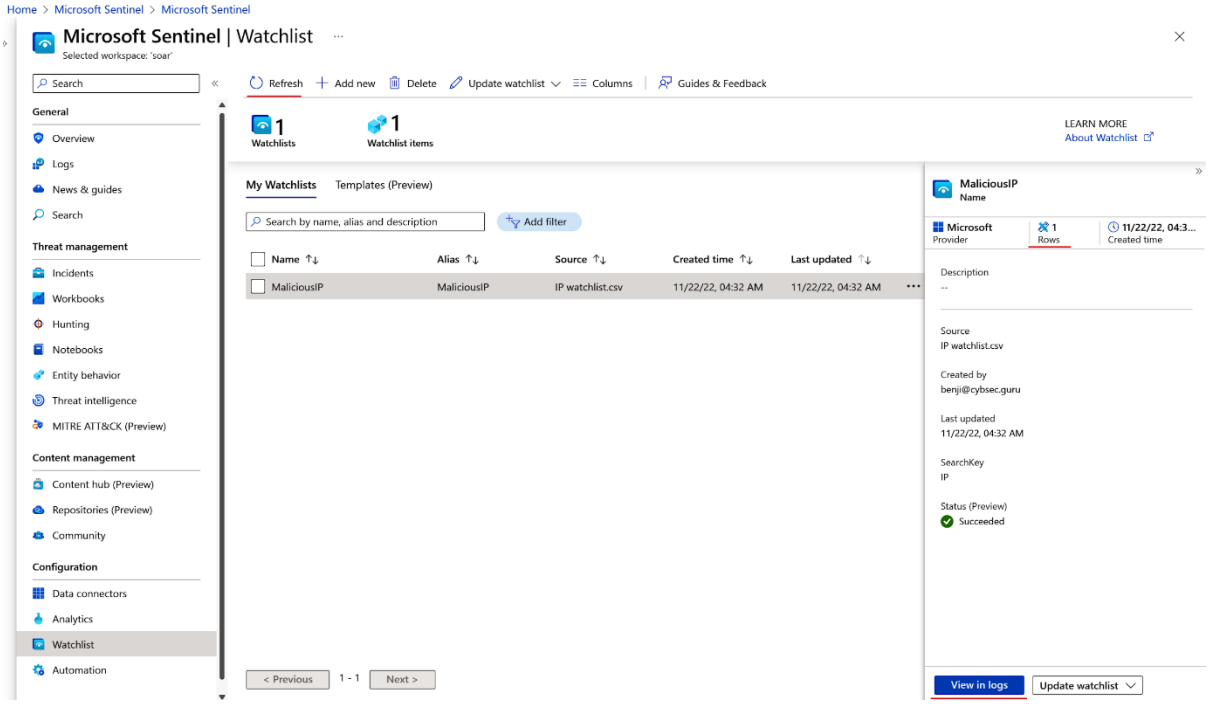

Book1 - Excel
No Label
Save As
Home
New
Open
Info
Save
Save As
Print
Share
Export
Publish
Close
Account
Feedback
Options
Recent
Microsoft
OneDrive
Sites
Personal
OneDrive - Personal
Other locations
This PC
Add a Place
Browse
Desktop
IP watchlist
Excel Workbook (*.xlsx)
Save
Excel Workbook (*.xlsx)
Excel Macro-Enabled Workbook (*.xlsm)
Excel Binary Workbook (*.xlsb)
Excel 97-2003 Workbook (*.xls)
CSV UTF-8 (Comma delimited) (*.csv)
XML Data (*.xml)
Single File Web Page (*.mht, *.mhtml)
Web Page (*.htm, *.html)
Excel Template (*.xltx)
Excel Macro-Enabled Template (*.xltm)
Excel 97-2003 Template (*.xlt)
Text (Tab delimited) (*.txt)
Unicode Text (*.txt)
XML Spreadsheet 2003 (*.xml)
Microsoft Excel 5.0/95 Workbook (*.xls)
CSV (Comma delimited) (*.csv)
Formatted Text (Space delimited) (*.prn)
Text (Macintosh) (*.txt)
Text (MS-DOS) (*.txt)
CSV (Macintosh) (*.csv)
CSV (MS-DOS) (*.csv)
DIF (Data Interchange Format) (*.dif)
SYLK (Symbolic Link) (*.slk)
Excel Add-in (*.xlam)
Excel 97-2003 Add-in (*.xla)
PDF (*.pdf)
XPS Document (*.xps)
Strict Open XML Spreadsheet (*.xlsx)
OpenDocument Spreadsheet (*.ods)
18/05/2022 13:49
16/11/2022 17:27

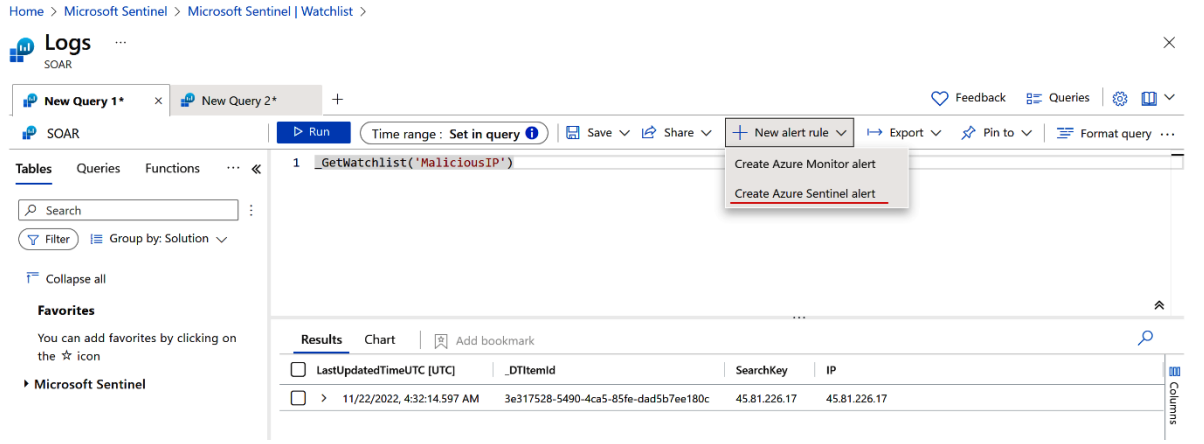

Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Watchlist
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Refresh
Add new
Delete
Update watchlist
Columns
Guides & Feedback
0
Watchlists
0
Watchlist items
LEARN MORE
About Watchlist
My Watchlists
Templates (Preview)
Watchlist
What is it?
Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.
How does it work?
Create a new watchlist by selecting 'Add new' and follow the steps in the new watchlist wizard. You will receive a notification in the notifications area within in the Azure portal that your watchlist was created. Watchlists are stored within your Microsoft Sentinel workspace as name value pairs and are cached for optimal query performance and low latency.
This is what you can do with watchlists
Investigate threats and respond to incidents quickly with fast import of IP addresses, file hashes, etc. from csv files. Then utilize the watchlist name/value pairs for joining and filtering for use in alert rules, threat hunting, workbooks, notebooks and for general queries.
Import business data, such as user lists with privileged system access as a watchlist. Then use the watchlist to create allow and deny lists. For example, use a watchlist that contains a list of terminated employees to detect or prevent them from logging in to the network.
No watchlist selected
Select a watchlist for more details


Home > Microsoft Sentinel > Microsoft Sentinel | Watchlist >
Watchlist wizard
Create new watchlist
General
Source
Review and create
Name *
MaliciousIP
Description
Alias *
MaliciousIP
Next: Source >


Home > Microsoft Sentinel > Microsoft Sentinel | Watchlist >
Watchlist wizard
Create new watchlist
General
Source
Review and create
Source type
Local file
File type
CSV file with a header (.csv)
Number of lines before row with headings *
0
Upload file *
IP watchlist.csv
Drag and drop the files or Browse for files
SearchKey *
IP
The SearchKey is used to optimize query performance when using watchlists for joins with other data. For example, enable a column with IP addresses to be the designated SearchKey field, then use this field to join in other event tables by IP address. Learn more and get examples about SearchKey
Reset
File preview | First 50 rows and first 5 columns
IP
45.81.226.17
Previous
Next: Review and create >


Home > Microsoft Sentinel | Watchlist >
Watchlist wizard
Create new watchlist
Validation passed.
General
Source
Review and create
General
Name
MaliciousIP
Description
Alias
MaliciousIP
Source
Source type
Local file
File type
CSV file with a header (.csv)
Number of lines before row with headings
0
Source
IP watchlist.csv
SearchKey
IP
Previous
Create


Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Watchlist
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Refresh
Add new
Delete
Update watchlist
Columns
Guides & Feedback
1
Watchlists
1
Watchlist items
LEARN MORE
About Watchlist
My Watchlists
Templates (Preview)
Search by name, alias and description
Add filter
Name
Alias
Source
Created time
Last updated
MaliciousIP
MaliciousIP
IP watchlist.csv
11/22/22, 04:32 AM
11/22/22, 04:32 AM
< Previous
1 - 1
Next >
MaliciousIP
Name
Microsoft
Provider
1
Rows
11/22/22, 04:3...
Created time
Description
--
Source
IP watchlist.csv
Created by
benji@cybsec.guru
Last updated
11/22/22, 04:32 AM
SearchKey
IP
Status (Preview)
Succeeded
View in logs
Update watchlist


Home > Microsoft Sentinel > Microsoft Sentinel | Watchlist >
Logs
SOAR
New Query 1*
New Query 2*
Feedback
Queries
SOAR
Run
Time range : Set in query
Save
Share
New alert rule
Export
Pin to
Format query
Create Azure Monitor alert
Create Azure Sentinel alert
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
Microsoft Sentinel
1 _GetWatchlist('MaliciousIP')
Results
Chart
Add bookmark
LastUpdatedTimeUTC [UTC]
_DTItemId
SearchKey
IP
11/22/2022, 4:32:14.597 AM
3e317528-5490-4ca5-85fe-dad5b7ee180c
45.81.226.17
45.81.226.17
Columns

Home > Microsoft Sentinel > Microsoft Sentinel | Watchlist > Logs >

Analytics rule wizard - Create a new scheduled rule

General | Set rule logic | Incident settings | Automated response | Review and create

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

Analytics rule details

Name *

Test - Malicious IP

Description

Tactics and techniques

0 selected

Severity

Medium

Status

Enabled | Disabled

Next : Set rule logic >

Analytics rule wizard - Create a new scheduled rule ...

General | **Set rule logic** | Incident settings | 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.

```
_GetWatchlist('MaliciousIP')
```

View query results >

Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results.
This enables Microsoft 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 >

ℹ 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 old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. Learn more >

IP

Address | IP | Add identifier

+ Add new entity

Analytics rule wizard - Create a new scheduled rule ...

+ Add new entity

Custom details

Alert details

Query scheduling

Run query every *

5 | Minutes

Lookup data from the last * ⓘ

5 | Hours

Alert threshold

Generate alert when number of query results *

Is greater than | 0

Event grouping

Configure how rule query results are grouped into alerts

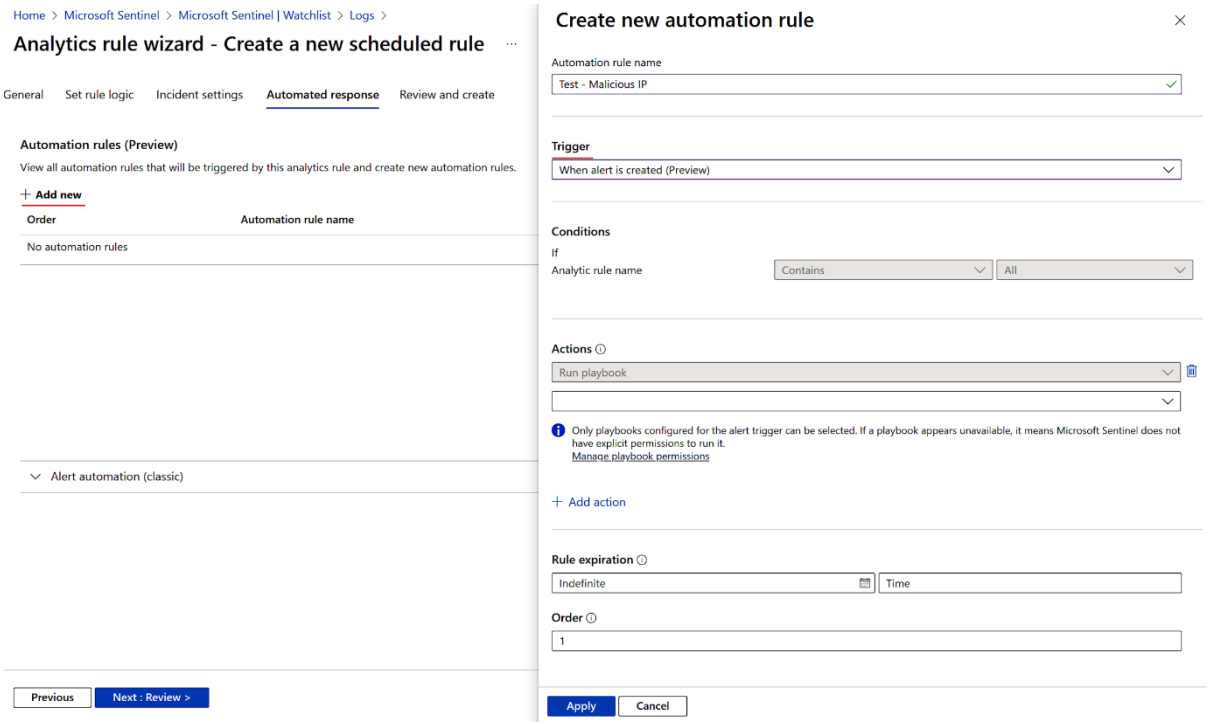
- (•) Group all events into a single alert
- ( ) Trigger an alert for each event

Suppression

Stop running query after alert is generated ⓘ

On | Off

Previous | Next : Incident settings >



Actions

Run playbook

Only playbooks configured for the alert trigger can be selected. If a playbook appears unavailable, it means Microsoft Sentinel does not have explicit permissions to run it.
Manage playbook permissions

Manage permissions

Choose the resource groups that contain the playbooks you want to give Microsoft Sentinel permissions to run

Browse | Current permissions

Search

Name	Subscription
Built-In-Identity-RG	VS FTE
cloud-shell-storage-n...	VS FTE
cloud-shell-storage-w...	VS FTE
DefaultResourceGrou...	VS FTE
NetworkWatcherRG	VS FTE
SOAR	VS FTE
Test	VS FTE

Apply | Cancel

Create new automation rule

Automation rule name

Test - Malicious IP

Trigger

When alert is created (Preview)

Conditions

If

Analytic rule name | Contains | All

Actions

Run playbook

VirusTotal-IPEnrichment-alertTrigger
VS FTE / SOAR

+ Add action

Rule expiration

Indefinite | Time

Order

1

Apply | Cancel

Home > Microsoft Sentinel > Microsoft Sentinel | Watchlist > Logs >

Analytics rule wizard - Create a new scheduled rule

General | Set rule logic | Incident settings | Automated response | Review and create

Automation rules (Preview)

View all automation rules that will be triggered by this analytics rule and create new automation rules.

+ Add new

Order	Automation rule name	Trigger	Action	Status
1	Test - Malicious IP	Alert created (Preview)	Run playbook 'VirusTotal-IPEnrichment-...	Enabled

Analytics rule wizard - Create a new scheduled rule

Validation passed.

General | Set rule logic | Incident settings | Automated response | **Review and create**

Analytics rule details

Name	Test - Malicious IP
Description	
Tactics and techniques	
Severity	Medium
Status	Enabled

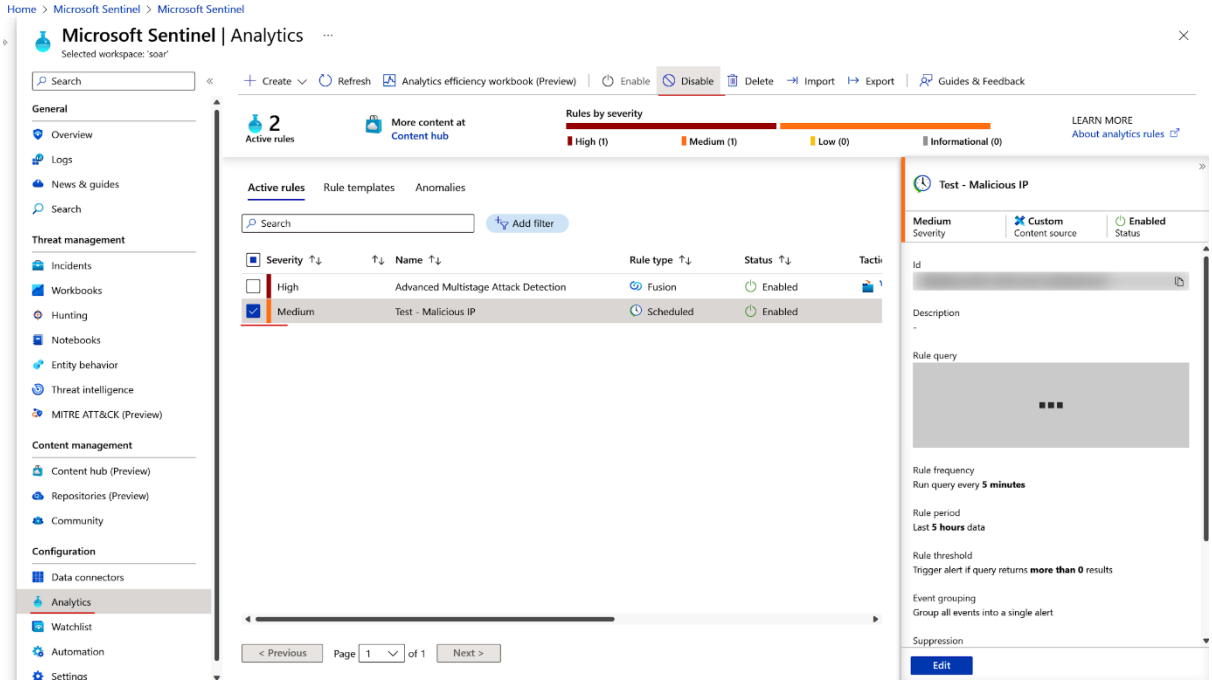
Analytics rule settings

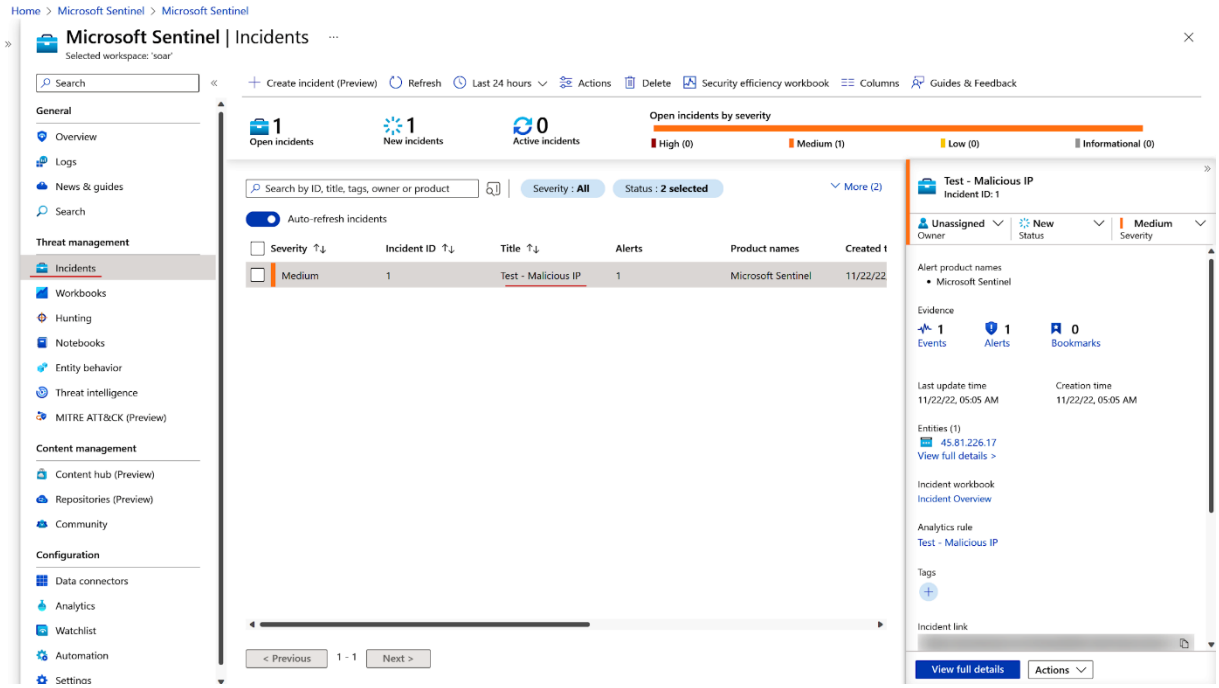
Rule query	_GetWatchlist('MaliciousIP')
Rule frequency	Run query every **5 minutes**
Rule period	Last **5 hours** data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns **more than 0** results
Event grouping	Group all events into a single alert
Suppression	Not configured

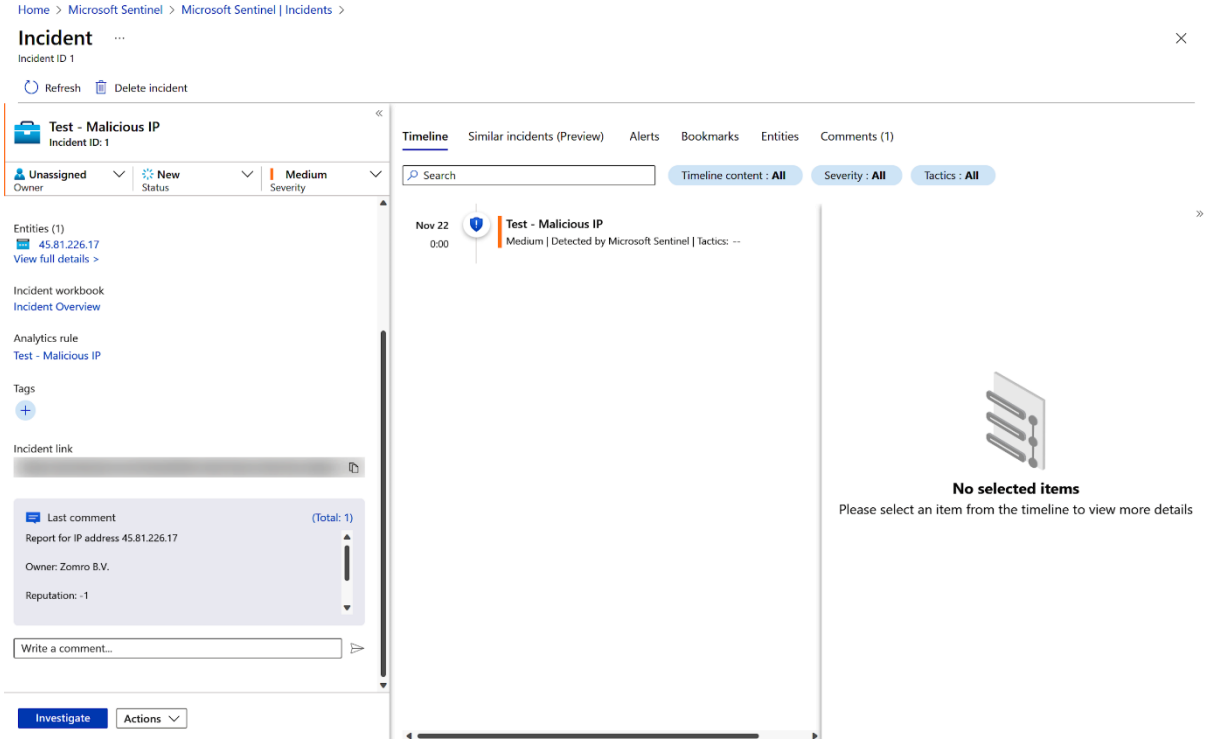
Entity mapping

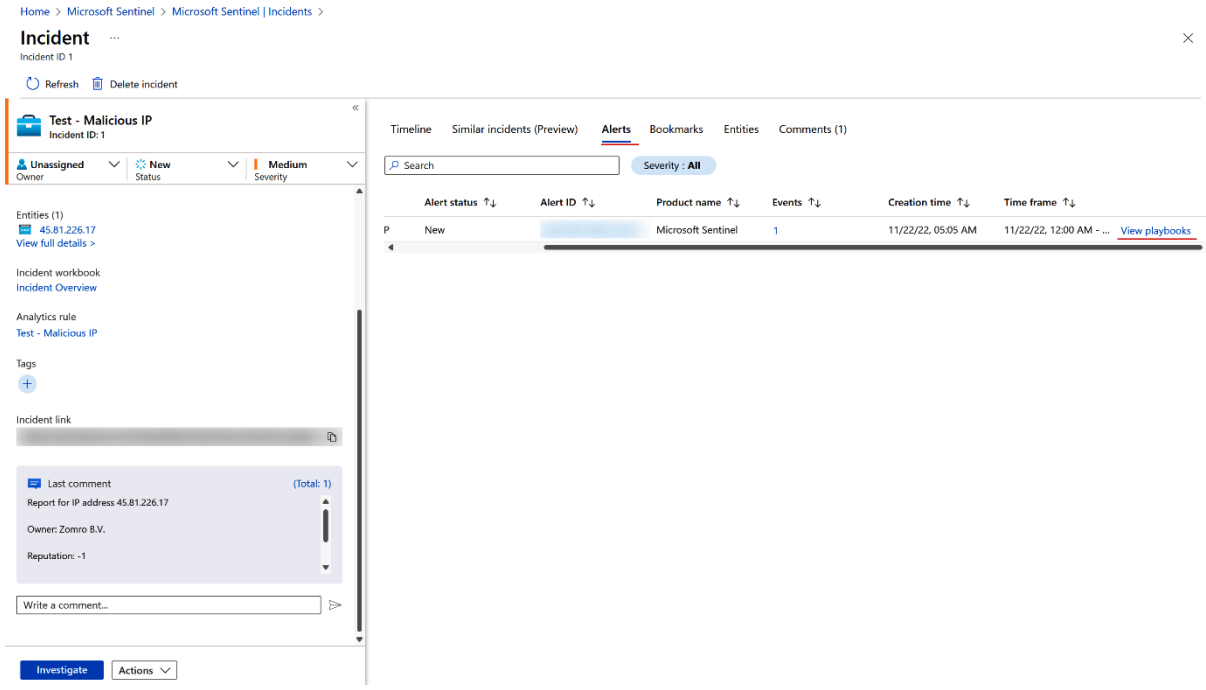
Entity 1:	**IP** Identifier: Address, Value: IP

Previous | Create


Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Analytics
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Create
Refresh
Analytics efficiency workbook (Preview)
Enable
Disable
Delete
Import
Export
Guides & Feedback
2
Active rules
More content at
Content hub
Rules by severity
High (1)
Medium (1)
Low (0)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search
Add filter
Severity
Name
Rule type
Status
High
Advanced Multistage Attack Detection
Fusion
Enabled
Medium
Test - Malicious IP
Scheduled
Enabled
< Previous
Page 1 of 1
Next >
Test - Malicious IP
Medium
Severity
Custom
Content source
Enabled
Status
Id
Description
-
Rule query
Rule frequency
Run query every 5 minutes
Rule period
Last 5 hours data
Rule threshold
Trigger alert if query returns more than 0 results
Event grouping
Group all events into a single alert
Suppression
Edit


Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
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 : 2 selected
More (2)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created t
Medium
1
Test - Malicious IP
1
Microsoft Sentinel
11/22/22
< Previous
1 - 1
Next >
Test - Malicious IP
Incident ID: 1
Unassigned
Owner
New
Status
Medium
Severity
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
11/22/22, 05:05 AM
Creation time
11/22/22, 05:05 AM
Entities (1)
45.81.226.17
View full details >
Incident workbook
Incident Overview
Analytics rule
Test - Malicious IP
Tags
Incident link
View full details
Actions


Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >
Incident
Incident ID 1
Refresh
Delete incident
Test - Malicious IP
Incident ID: 1
Unassigned
Owner
New
Status
Medium
Severity
Entities (1)
45.81.226.17
View full details >
Incident workbook
Incident Overview
Analytics rule
Test - Malicious IP
Tags
Incident link
Last comment
(Total: 1)
Report for IP address 45.81.226.17
Owner: Zomro B.V.
Reputation: -1
Write a comment...
Investigate
Actions
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities
Comments (1)
Search
Timeline content : All
Severity : All
Tactics : All
Nov 22
0:00
Test - Malicious IP
Medium | Detected by Microsoft Sentinel | Tactics: --
No selected items
Please select an item from the timeline to view more details


Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >
Incident
Incident ID 1
Refresh
Delete incident
Test - Malicious IP
Incident ID: 1
Unassigned
Owner
New
Status
Medium
Severity
Entities (1)
45.81.226.17
View full details >
Incident workbook
Incident Overview
Analytics rule
Test - Malicious IP
Tags
Incident link
Last comment
(Total: 1)
Report for IP address 45.81.226.17
Owner: Zomro B.V.
Reputation: -1
Write a comment...
Investigate
Actions
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities
Comments (1)
Search
Severity : All
Alert status
Alert ID
Product name
Events
Creation time
Time frame
P
New
Microsoft Sentinel
1
11/22/22, 05:05 AM
11/22/22, 12:00 AM - ...
View playbooks

Home > Microsoft Sentinel > Microsoft Sentinel | Incidents > Incident >

Alert playbooks

Test - Malicious IP

Refresh

Playbooks Runs

VirusTotal

Name	Status	Plan	Subscription		
VirusTotal-IPEnrichment-alertTrigger	Enabled	Consumption	VS FTE	Open designer	Run

Home > Microsoft Sentinel > Microsoft Sentinel | Incidents > Incident >

Alert playbooks

Test - Malicious IP

Refresh

Playbooks Runs

Search playbooks runs

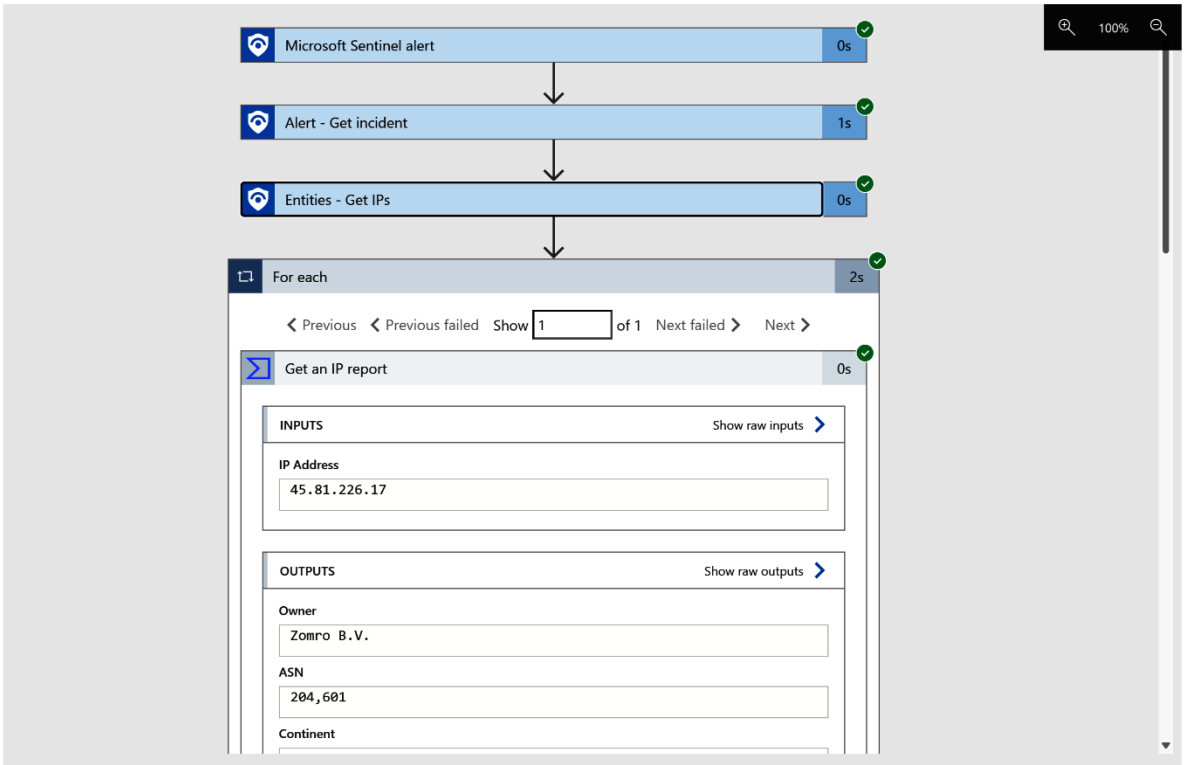
Name	Status	Start time	End time	
VirusTotal-IPEnrichment-alertTrigger	Succeeded	11/22/22, 05:20 AM	11/22/22, 05:20 AM	View run
VirusTotal-IPEnrichment-alertTrigger	Succeeded	11/22/22, 05:05 AM	11/22/22, 05:05 AM	View run

Home > Microsoft Sentinel > Microsoft Sentinel | Incidents > Incident > Alert playbooks >

Logic app run

08585325124618903063359928689CU225

Run Details Resubmit Cancel Run Refresh Info



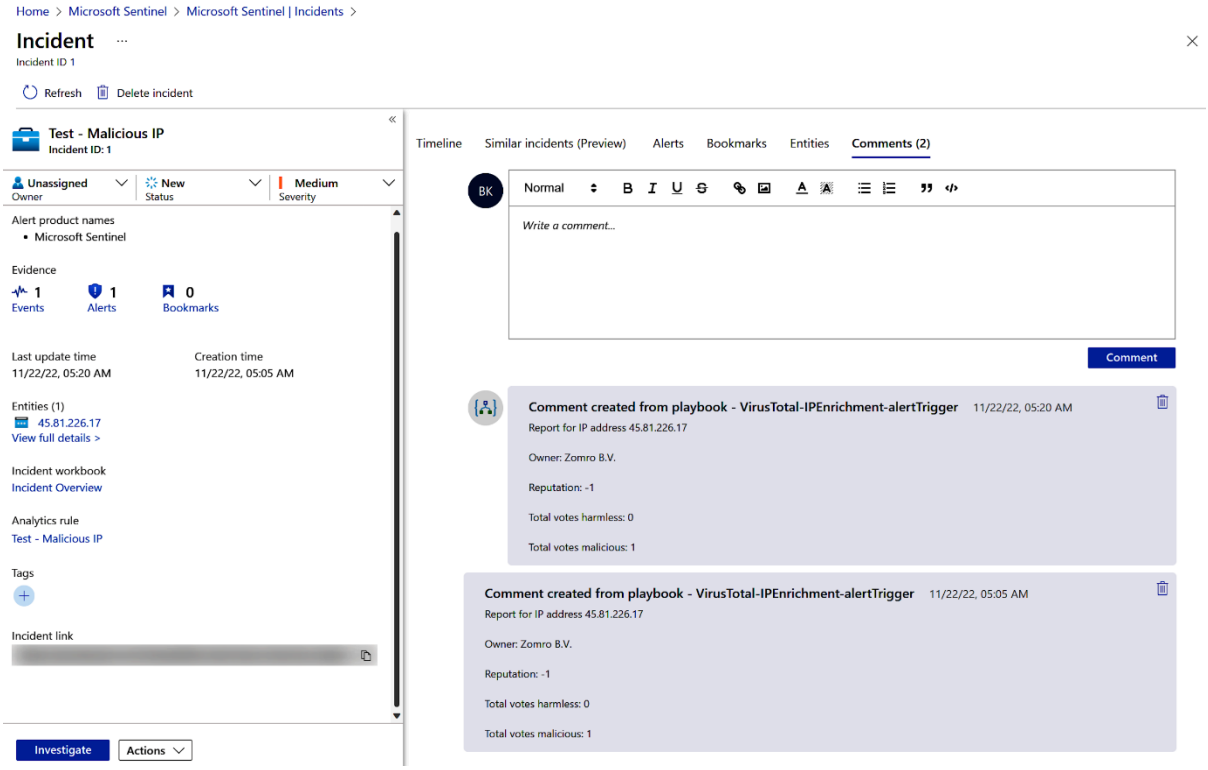
Home > Microsoft Sentinel > Microsoft Sentinel | Incidents > Incident > Alert playbooks >

Logic app run ...

085853251246189030633599286 89CU225

Run Details | Resubmit | Cancel Run | Refresh | Info

Microsoft Sentinel alert



Home > Microsoft Sentinel | Analytics >

Analytics rule wizard - Edit existing scheduled rule

Test - Malicious IP

General | Set rule logic | **Incident settings** | Automated response | Review and update

Incident settings

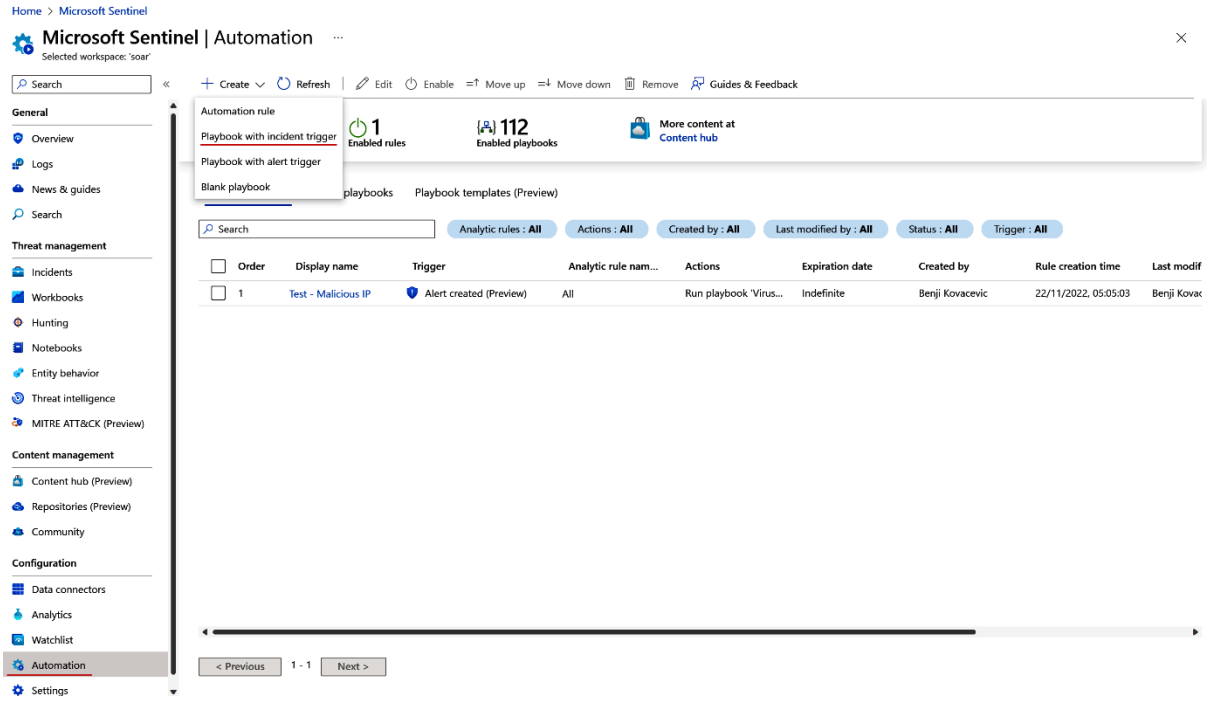
Microsoft Sentinel alerts can be grouped together into an Incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

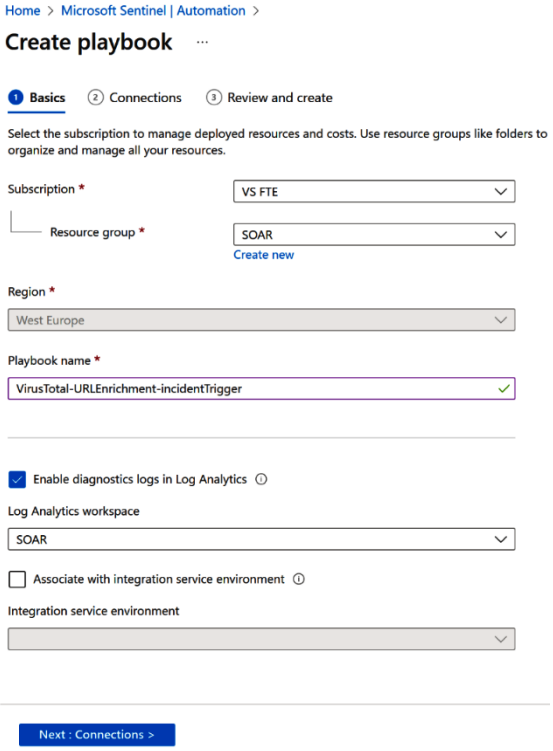
Create incidents from alerts triggered by this analytics rule

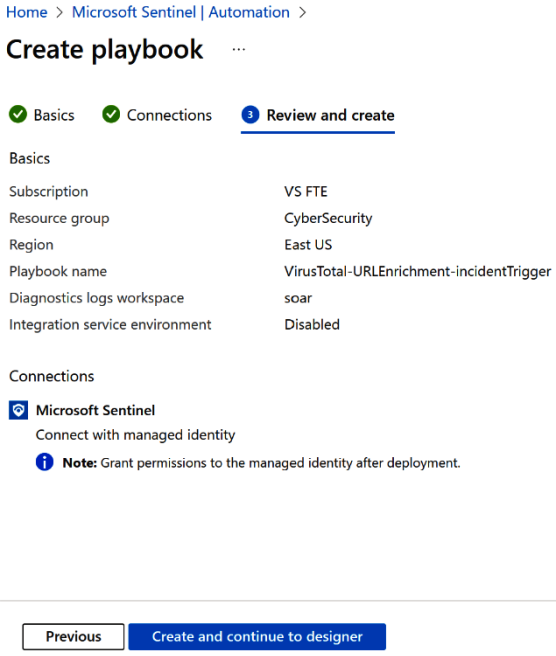
Enabled | Disabled

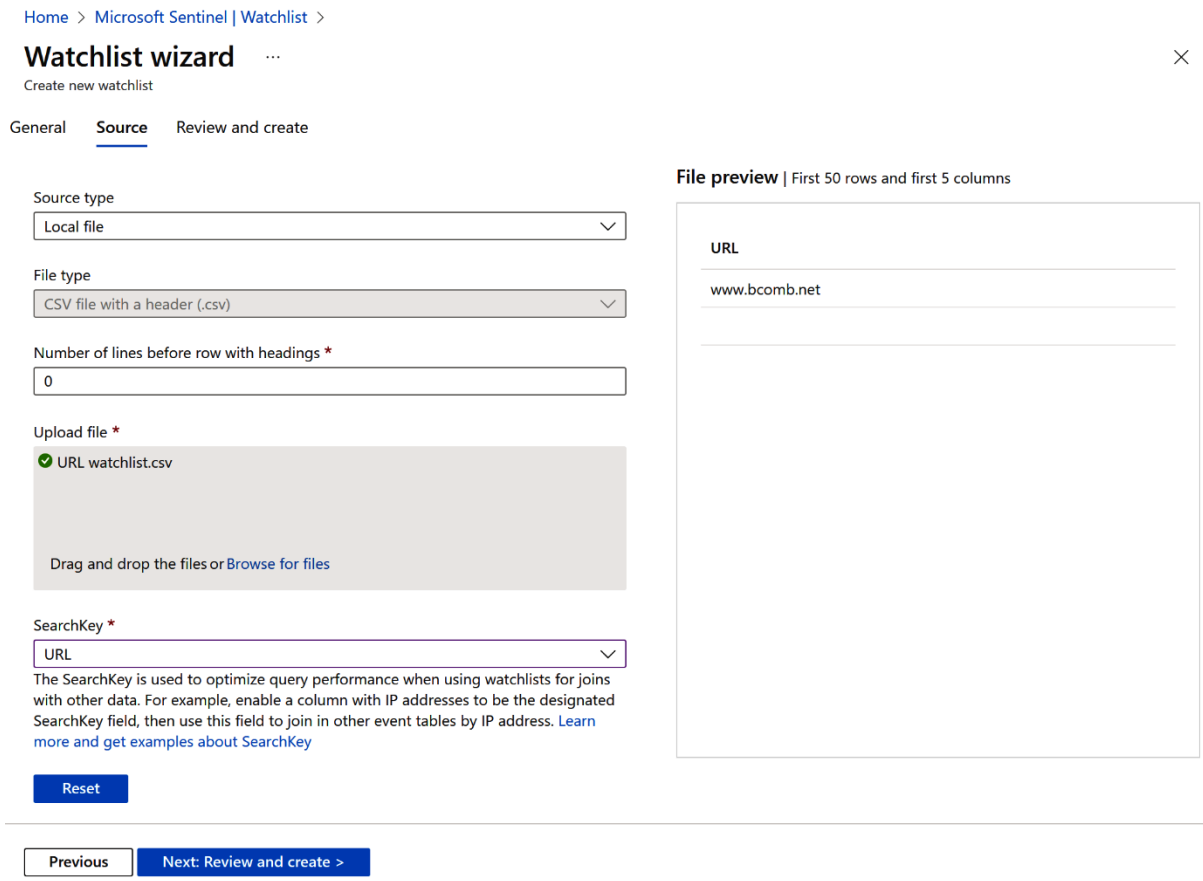
Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents.




Home > Microsoft Sentinel | Automation >
Create playbook
Basics
Connections
Review and create
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
VS FTE
Resource group *
SOAR
Create new
Region *
West Europe
Playbook name *
VirusTotal-URLEnrichment-incidentTrigger
Enable diagnostics logs in Log Analytics
Log Analytics workspace
SOAR
Associate with integration service environment
Integration service environment
Next : Connections >


Home > Microsoft Sentinel | Automation >
Create playbook
Basics
Connections
Review and create
Basics
Subscription VS FTE
Resource group CyberSecurity
Region East US
Playbook name VirusTotal-URLEnrichment-incidentTrigger
Diagnostics logs workspace soar
Integration service environment Disabled
Connections
Microsoft Sentinel
Connect with managed identity
Note: Grant permissions to the managed identity after deployment.
Previous
Create and continue to designer


Home > Microsoft Sentinel | Watchlist >
Watchlist wizard
Create new watchlist
General
Source
Review and create
Source type
Local file
File type
CSV file with a header (.csv)
Number of lines before row with headings *
0
Upload file *
URL watchlist.csv
Drag and drop the files or Browse for files
SearchKey *
URL
The SearchKey is used to optimize query performance when using watchlists for joins with other data. For example, enable a column with IP addresses to be the designated SearchKey field, then use this field to join in other event tables by IP address. Learn more and get examples about SearchKey
Reset
File preview | First 50 rows and first 5 columns
URL
www.bcomb.net
Previous
Next: Review and create >

Home > Microsoft Sentinel | Watchlist > Logs >

Analytics rule wizard - Create a new scheduled 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.

```
_GetWatchlist('MaliciousURL')
```

View query results >

Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results.
This enables Microsoft 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 old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. Learn more >

URL

Url | URL | Add identifier

Add new entity

Custom details

Alert details

Previous | Next : Incident settings >

Analytics rule wizard - Create a new scheduled rule ...

Validation passed.

General | Set rule logic | Incident settings | Automated response | **Review and create**

Analytics rule details

Name	Test – Malicious URL
Description	
Tactics and techniques	
Severity	Medium
Status	Enabled

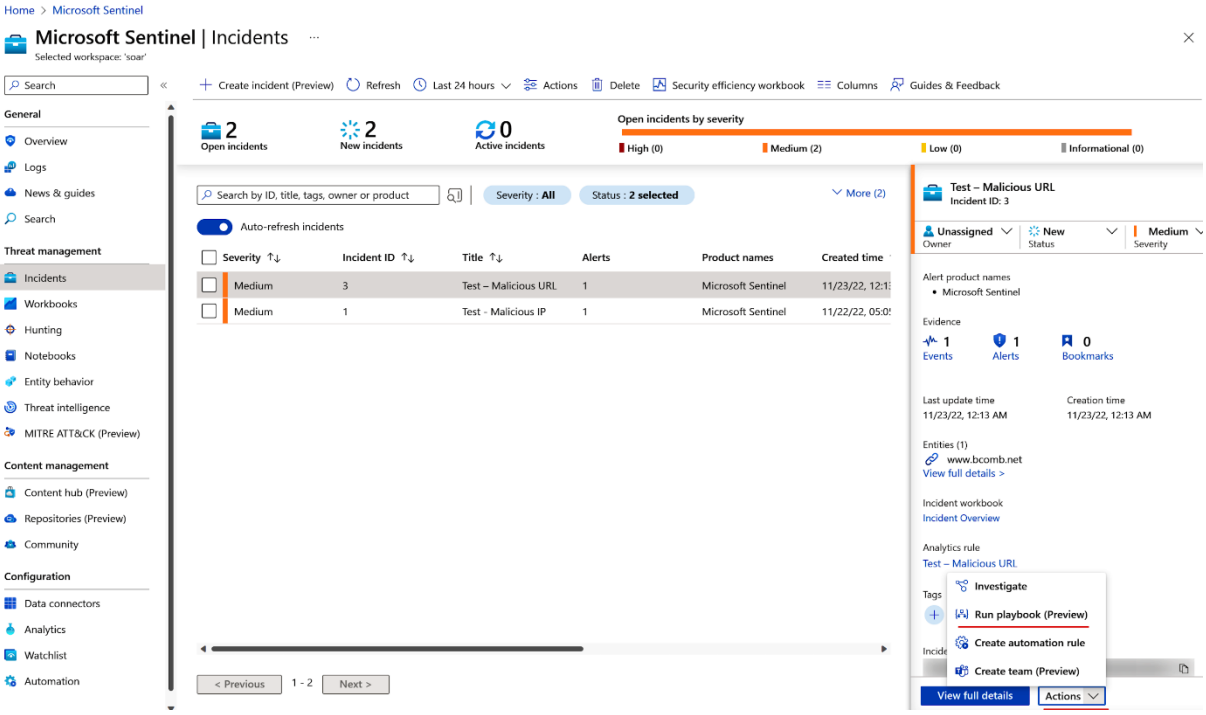
Analytics rule settings

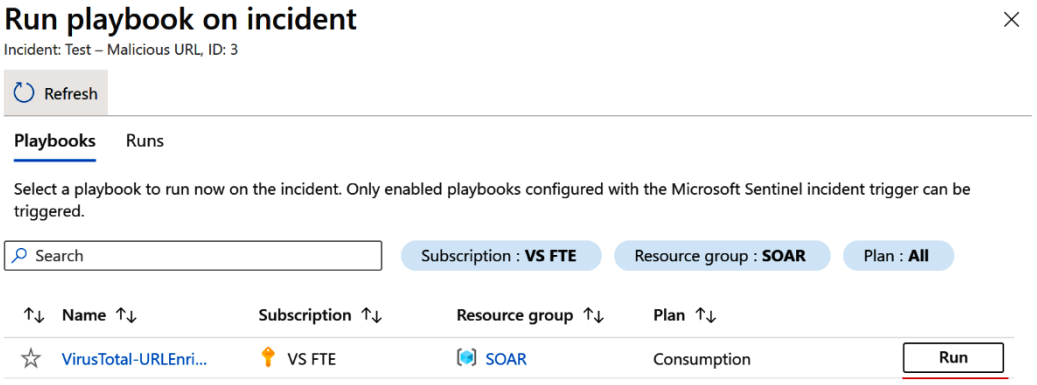
Rule query	_GetWatchlist('MaliciousURL')
Rule frequency	Run query every **5 minutes**
Rule period	Last **5 hours** data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns **more than 0** results
Event grouping	Group all events into a single alert
Suppression	Not configured

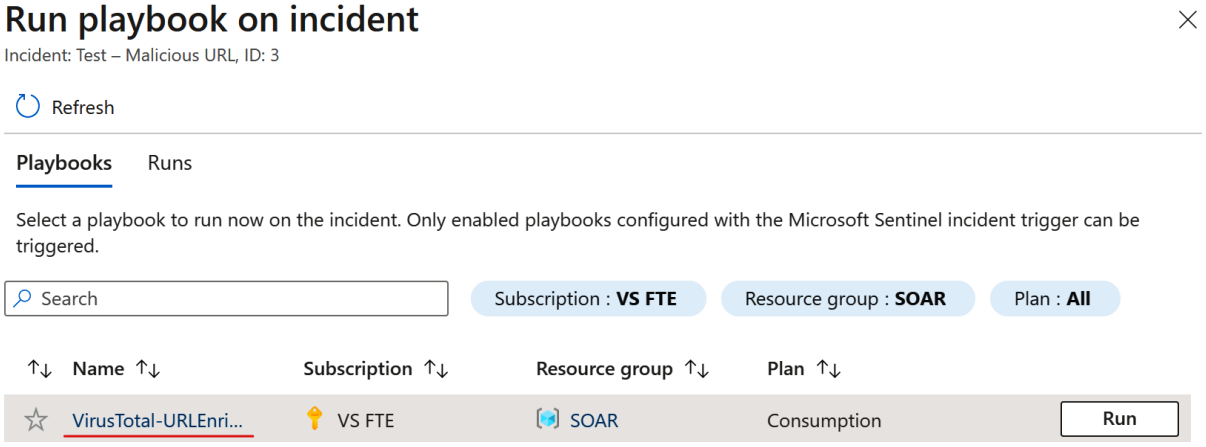
Entity mapping

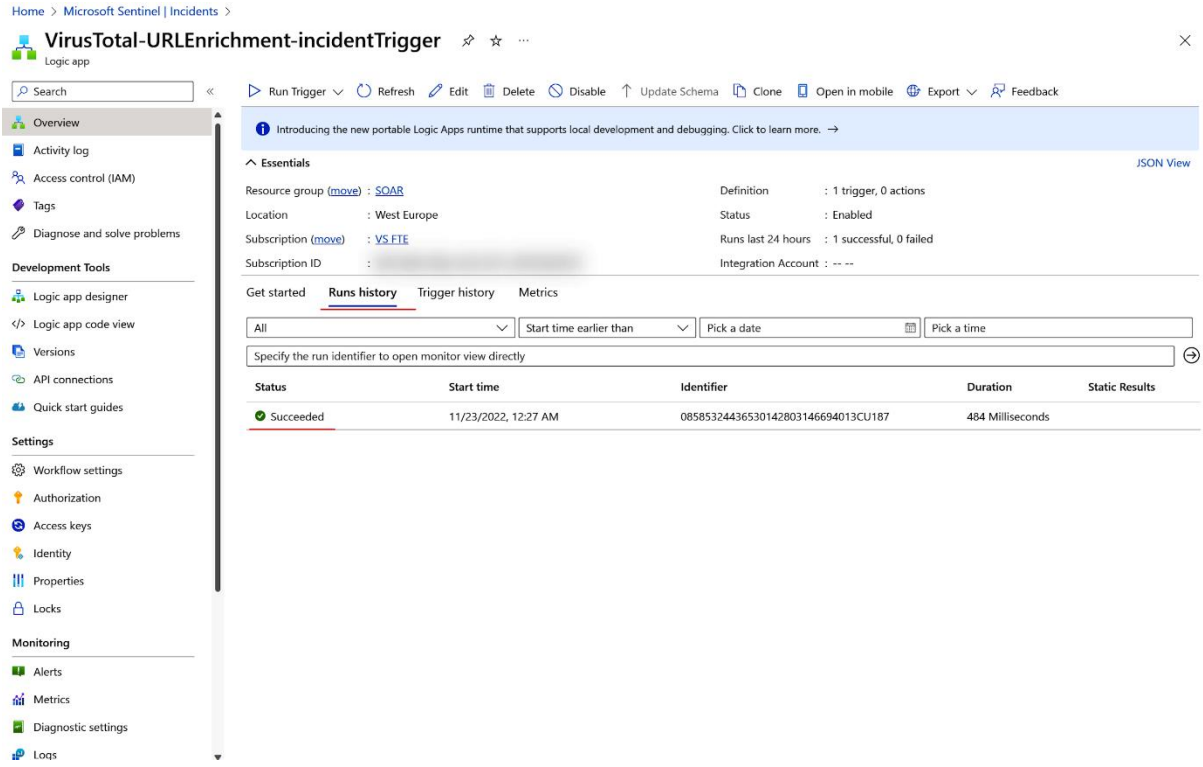
Entity 1:	**URL** Identifier: Url, Value: URL

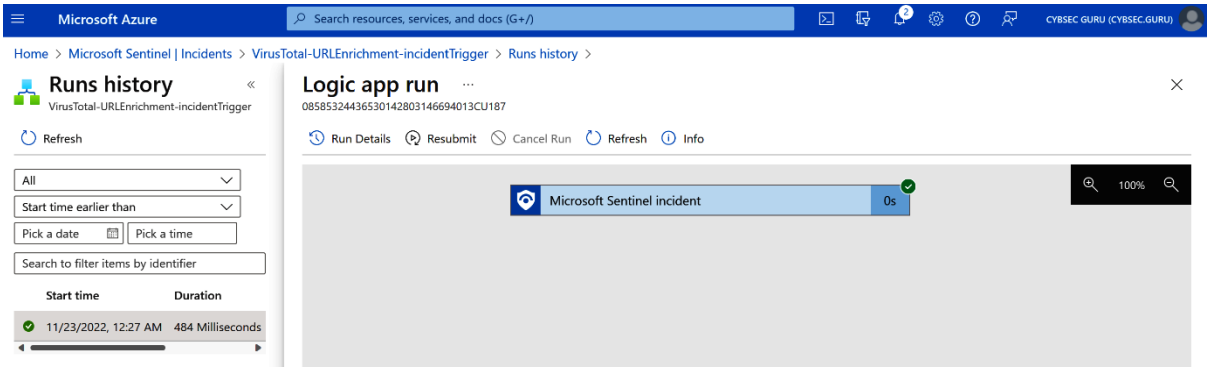
Previous | Create

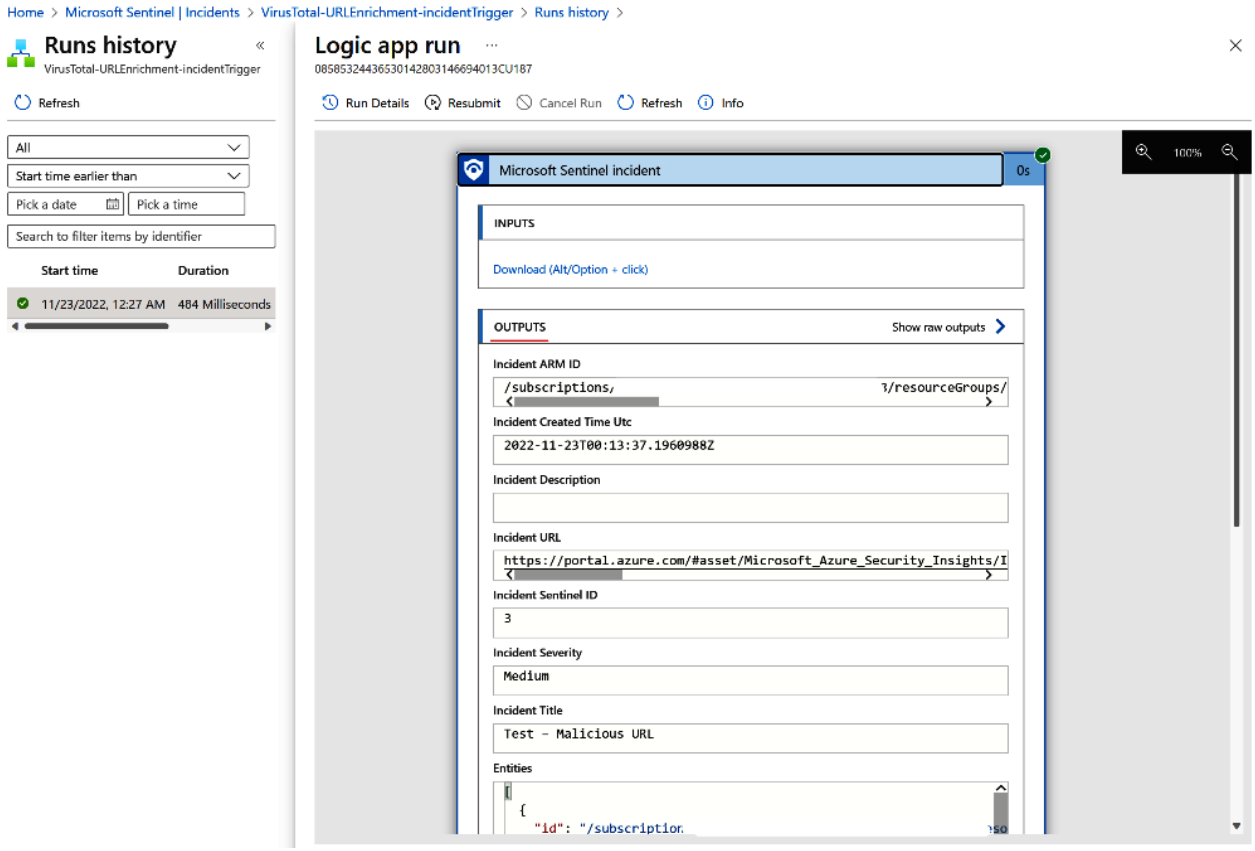

Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
2
Open incidents
2
New incidents
0
Active incidents
Open incidents by severity
High (0)
Medium (2)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
More (2)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
3
Test – Malicious URL
1
Microsoft Sentinel
11/23/22, 12:1
Medium
1
Test - Malicious IP
1
Microsoft Sentinel
11/22/22, 05:0
< Previous
1 - 2
Next >
Test – Malicious URL
Incident ID: 3
Unassigned
Owner
New
Status
Medium
Severity
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
11/23/22, 12:13 AM
Creation time
11/23/22, 12:13 AM
Entities (1)
www.bcomb.net
View full details >
Incident workbook
Incident Overview
Analytics rule
Test – Malicious URL
Tags
Investigate
Run playbook (Preview)
Create automation rule
Create team (Preview)
View full details
Actions

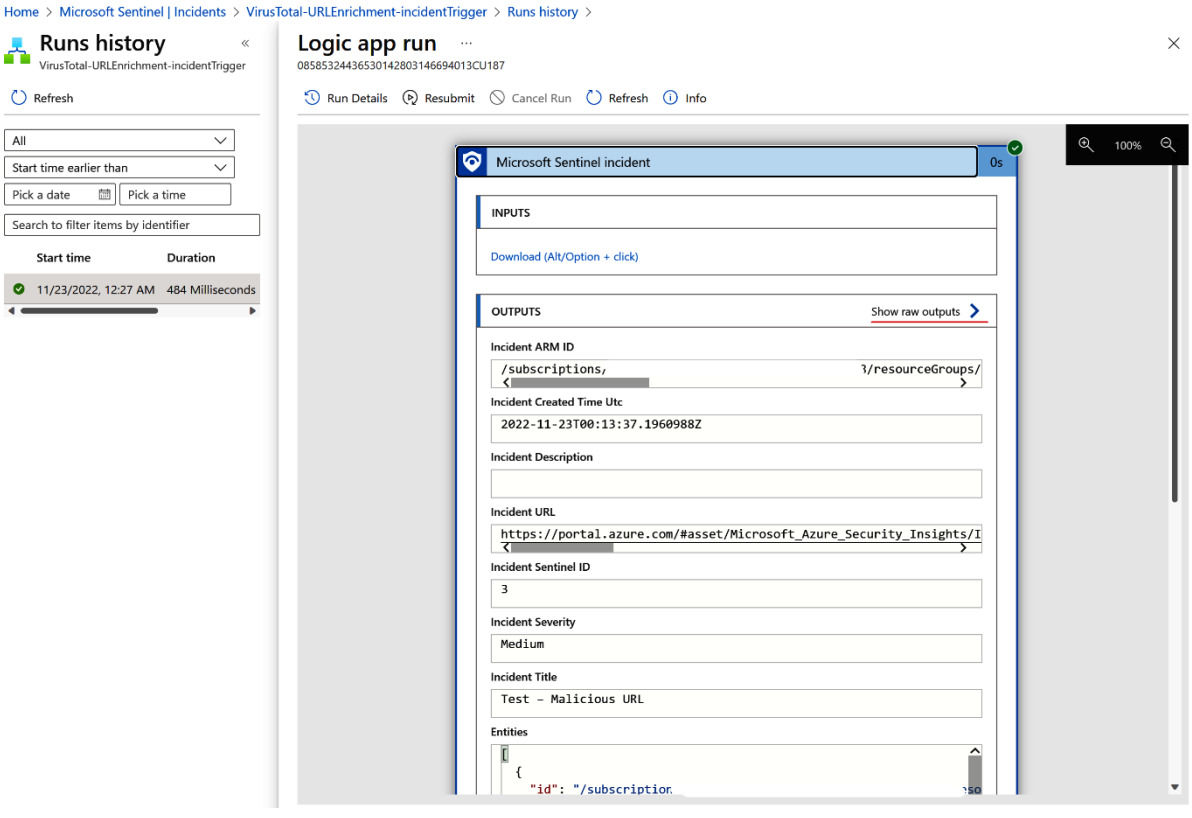

Run playbook on incident
Incident: Test – Malicious URL, ID: 3
Refresh
Playbooks
Runs
Select a playbook to run now on the incident. Only enabled playbooks configured with the Microsoft Sentinel incident trigger can be triggered.
Search
Subscription : VS FTE
Resource group : SOAR
Plan : All
Name
Subscription
Resource group
Plan
VirusTotal-URLEnri...
VS FTE
SOAR
Consumption
Run

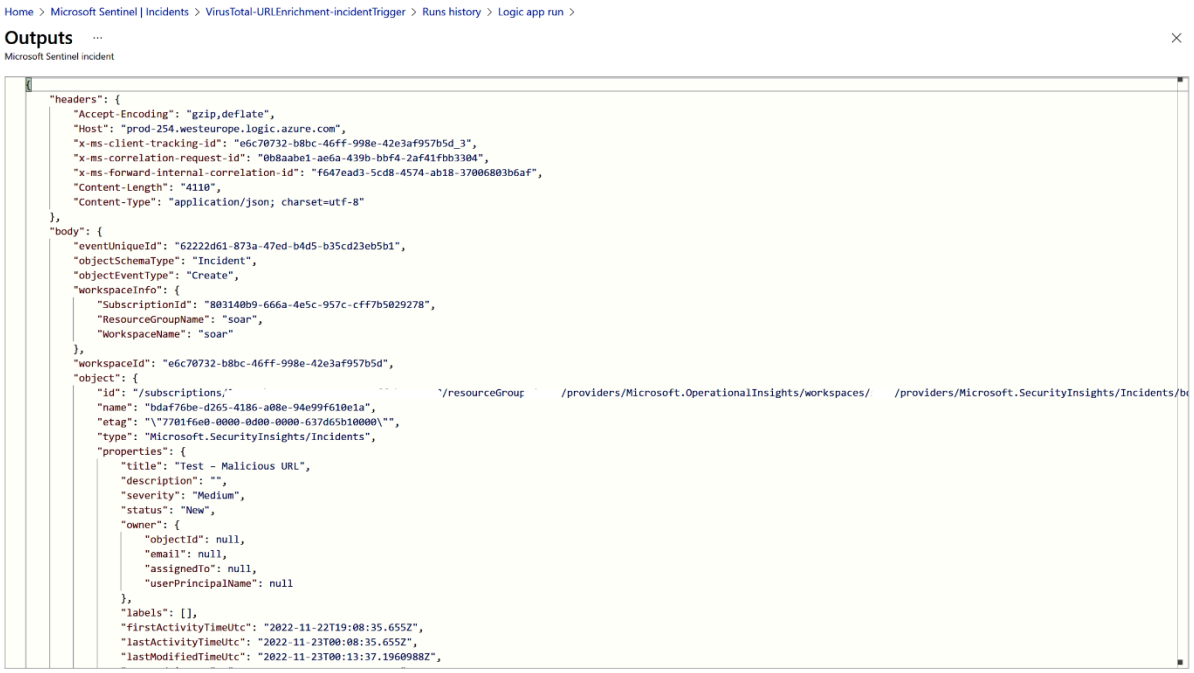

Run playbook on incident
Incident: Test – Malicious URL, ID: 3
Refresh
Playbooks
Runs
Select a playbook to run now on the incident. Only enabled playbooks configured with the Microsoft Sentinel incident trigger can be triggered.
Search
Subscription : VS FTE
Resource group : SOAR
Plan : All
Name
Subscription
Resource group
Plan
VirusTotal-URLEnri...
VS FTE
SOAR
Consumption
Run

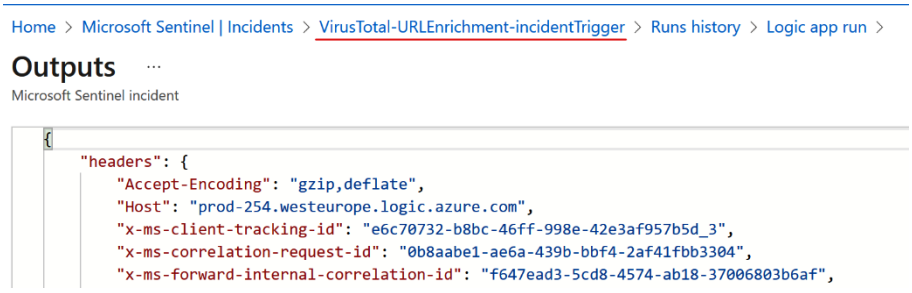

Home > Microsoft Sentinel | Incidents >
VirusTotal-URLEnrichment-incidentTrigger
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Run Trigger
Refresh
Edit
Delete
Disable
Update Schema
Clone
Open in mobile
Export
Feedback
Introducing the new portable Logic Apps runtime that supports local development and debugging. Click to learn more.
Essentials
JSON View
Resource group (move) : SOAR
Location : West Europe
Subscription (move) : VS FTE
Subscription ID :
Definition : 1 trigger, 0 actions
Status : Enabled
Runs last 24 hours : 1 successful, 0 failed
Integration Account : -- --
Get started
Runs history
Trigger history
Metrics
All
Start time earlier than
Pick a date
Pick a time
Specify the run identifier to open monitor view directly
Status
Start time
Identifier
Duration
Static Results
Succeeded
11/23/2022, 12:27 AM
08585324436530142803146694013CU187
484 Milliseconds

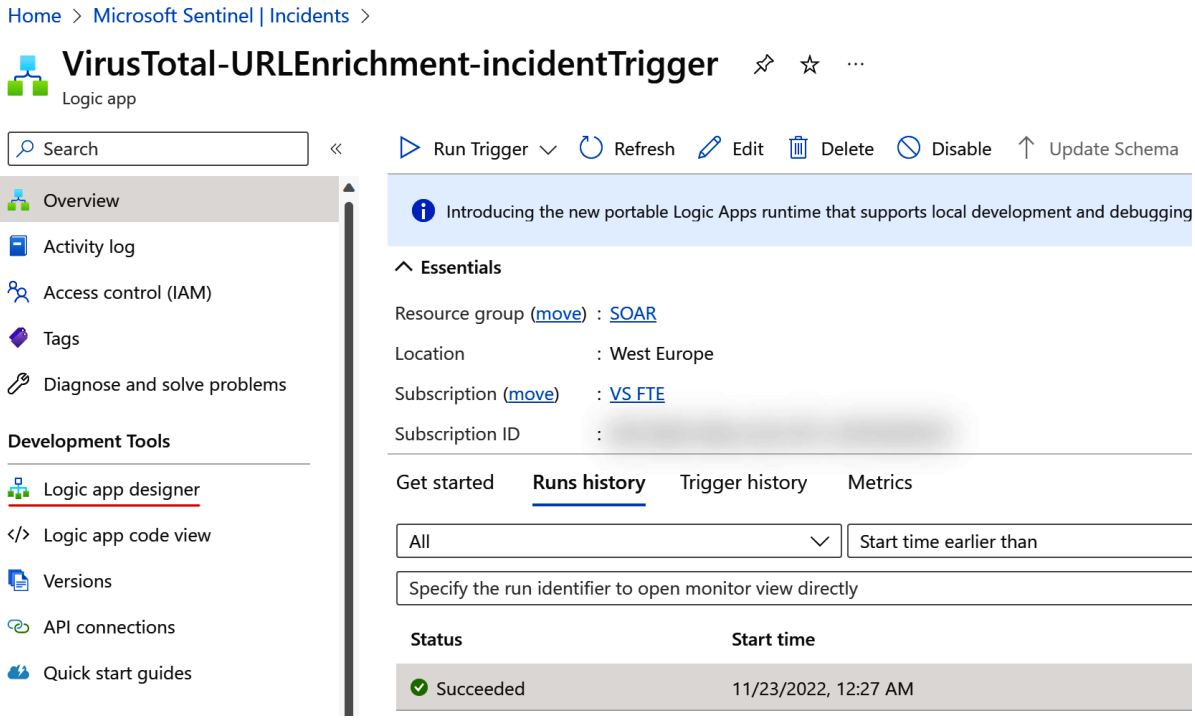

Microsoft Azure
Search resources, services, and docs (G+/)
CYBSEC GURU (CYBSEC.GURU)
Home > Microsoft Sentinel | Incidents > VirusTotal-URLEnrichment-incidentTrigger > Runs history >
Runs history
VirusTotal-URLEnrichment-incidentTrigger
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
11/23/2022, 12:27 AM
484 Milliseconds
Logic app run
08585324436530142803146694013CU187
Run Details
Resubmit
Cancel Run
Refresh
Info
Microsoft Sentinel incident
0s
100%

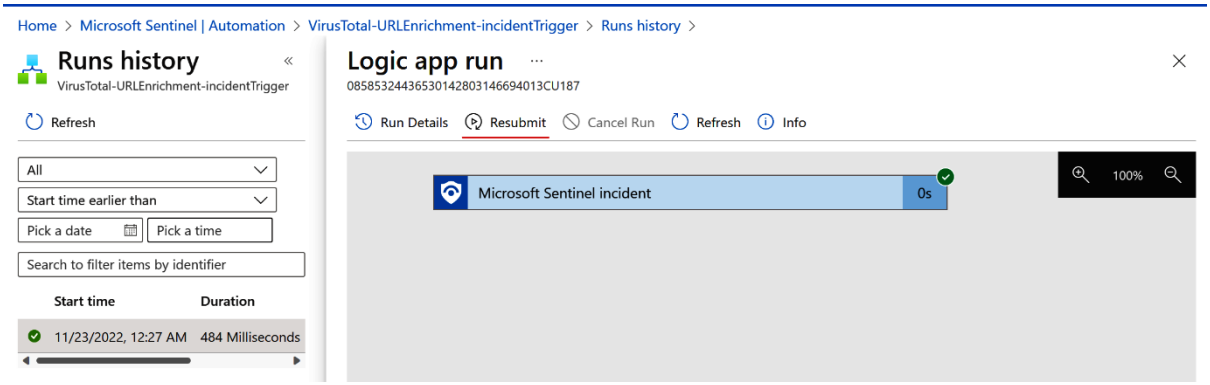

Home > Microsoft Sentinel | Incidents > VirusTotal-URLEnrichment-incidentTrigger > Runs history >
Runs history
VirusTotal-URLEnrichment-incidentTrigger
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
11/23/2022, 12:27 AM
484 Milliseconds
Logic app run
08585324436530142803146694013CU187
Run Details
Resubmit
Cancel Run
Refresh
Info
100%
Microsoft Sentinel incident
0s
INPUTS
Download (Alt/Option + click)
OUTPUTS
Show raw outputs
Incident ARM ID
/subscriptions/
3/resourceGroups/
Incident Created Time Utc
2022-11-23T00:13:37.1960988Z
Incident Description
Incident URL
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/I
Incident Sentinel ID
3
Incident Severity
Medium
Incident Title
Test - Malicious URL
Entities
{
"id": "/subscriptior

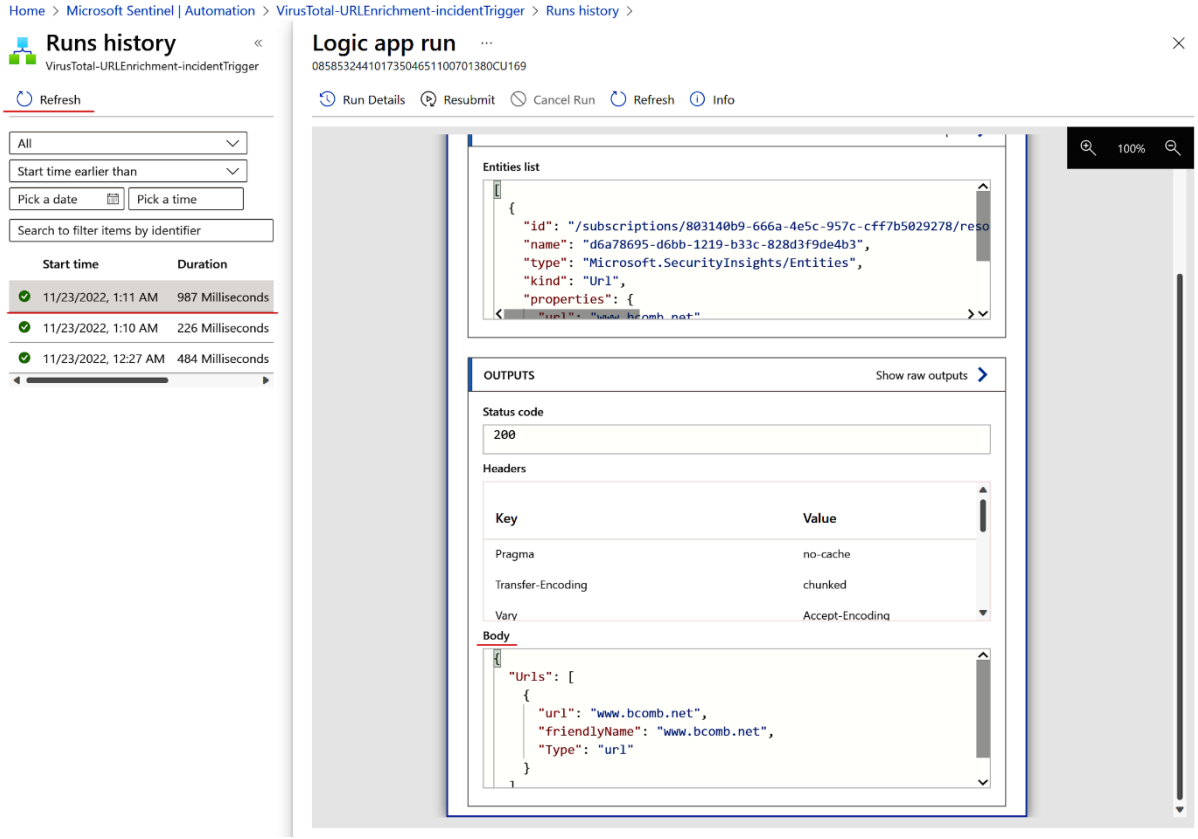

Home > Microsoft Sentinel | Incidents > VirusTotal-URLEnrichment-incidentTrigger > Runs history >
Runs history
VirusTotal-URLEnrichment-incidentTrigger
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
11/23/2022, 12:27 AM
484 Milliseconds
Logic app run
08585324436530142803146694013CU187
Run Details
Resubmit
Cancel Run
Refresh
Info
100%
Microsoft Sentinel incident
0s
INPUTS
Download (Alt/Option + click)
OUTPUTS
Show raw outputs
Incident ARM ID
/subscriptions/
3/resourceGroups/
Incident Created Time Utc
2022-11-23T00:13:37.1960988Z
Incident Description
Incident URL
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/I
Incident Sentinel ID
3
Incident Severity
Medium
Incident Title
Test - Malicious URL
Entities
{
"id": "/subscriptior

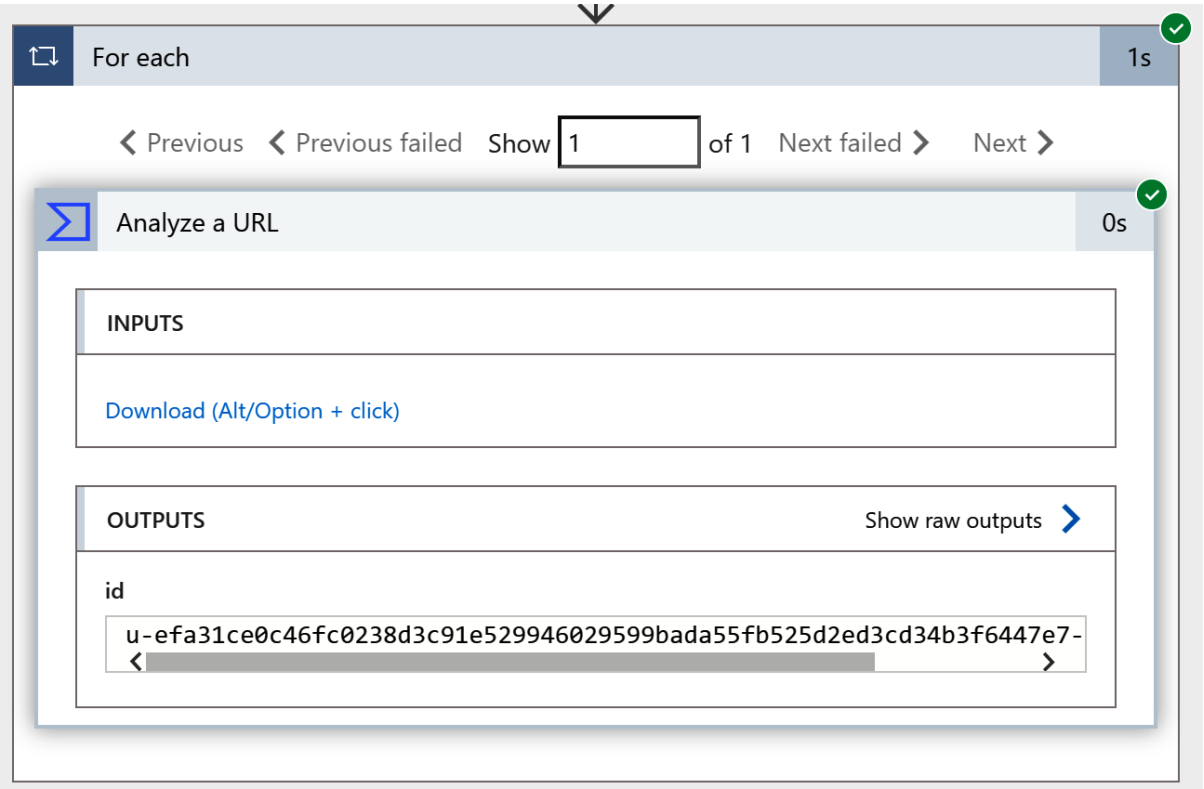

Home > Microsoft Sentinel | Incidents > VirusTotal-URLEnrichment-incidentTrigger > Runs history > Logic app run >
Outputs
Microsoft Sentinel incident
{
"headers": {
"Accept-Encoding": "gzip,deflate",
"Host": "prod-254.westeurope.logic.azure.com",
"x-ms-client-tracking-id": "e6c70732-b8bc-46ff-998e-42e3af957b5d_3",
"x-ms-correlation-request-id": "0b8aabe1-ae6a-439b-bbf4-2af41fbb3304",
"x-ms-forward-internal-correlation-id": "f647ead3-5cd8-4574-ab18-37006803b6af",
"Content-Length": "4110",
"Content-Type": "application/json; charset=utf-8"
},
"body": {
"eventUniqueId": "62222d61-873a-47ed-b4d5-b35cd23eb5b1",
"objectSchemaType": "Incident",
"objectEventType": "Create",
"workspaceInfo": {
"SubscriptionId": "803140b9-666a-4e5c-957c-cff7b5029278",
"ResourceGroupName": "soar",
"WorkspaceName": "soar"
},
"workspaceId": "e6c70732-b8bc-46ff-998e-42e3af957b5d",
"object": {
"id": "/subscriptions/
/providers/Microsoft.OperationalInsights/workspaces/
/providers/Microsoft.SecurityInsights/Incidents/b
"name": "bdaf76be-d265-4186-a08e-94e99f610e1a",
"etag": "\"7701f6e0-0000-0d00-0000-637d65b10000\"",
"type": "Microsoft.SecurityInsights/Incidents",
"properties": {
"title": "Test - Malicious URL",
"description": "",
"severity": "Medium",
"status": "New",
"owner": {
"objectId": null,
"email": null,
"assignedTo": null,
"userPrincipalName": null
},
"labels": [],
"firstActivityTimeUtc": "2022-11-22T19:08:35.655Z",
"lastActivityTimeUtc": "2022-11-23T00:08:35.655Z",
"lastModifiedTimeUtc": "2022-11-23T00:13:37.1960988Z",

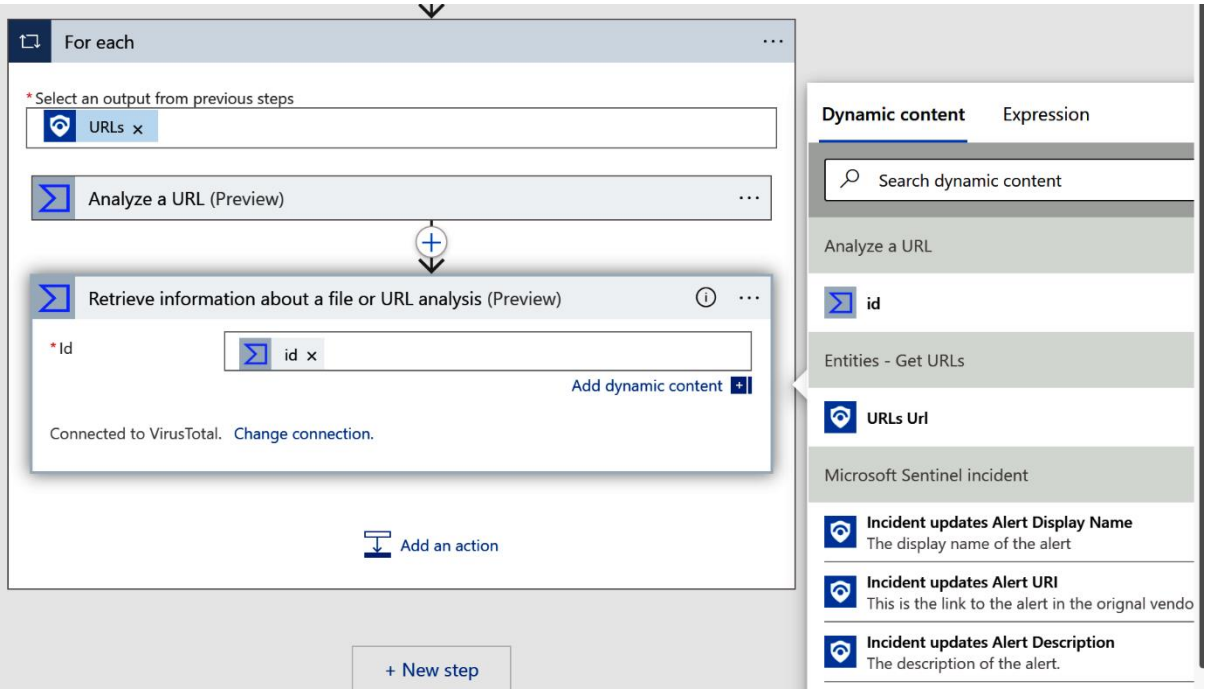

Home > Microsoft Sentinel | Incidents > VirusTotal-URLEnrichment-incidentTrigger > Runs history > Logic app run >
Outputs
Microsoft Sentinel incident
{
"headers": {
"Accept-Encoding": "gzip,deflate",
"Host": "prod-254.westeurope.logic.azure.com",
"x-ms-client-tracking-id": "e6c70732-b8bc-46ff-998e-42e3af957b5d_3",
"x-ms-correlation-request-id": "0b8aabe1-ae6a-439b-bbf4-2af41fbb3304",
"x-ms-forward-internal-correlation-id": "f647ead3-5cd8-4574-ab18-37006803b6af",


Home > Microsoft Sentinel | Incidents >
VirusTotal-URLEnrichment-incidentTrigger
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Run Trigger
Refresh
Edit
Delete
Disable
Update Schema
Introducing the new portable Logic Apps runtime that supports local development and debugging
Essentials
Resource group (move) : SOAR
Location : West Europe
Subscription (move) : VS FTE
Subscription ID :
Get started
Runs history
Trigger history
Metrics
All
Start time earlier than
Specify the run identifier to open monitor view directly
Status
Start time
Succeeded
11/23/2022, 12:27 AM


Home > Microsoft Sentinel | Automation > VirusTotal-URLEnrichment-incidentTrigger > Runs history >
Runs history
VirusTotal-URLEnrichment-incidentTrigger
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
11/23/2022, 12:27 AM
484 Milliseconds
Logic app run
08585324436530142803146694013CU187
Run Details
Resubmit
Cancel Run
Refresh
Info
Microsoft Sentinel incident
0s
100%


Home > Microsoft Sentinel | Automation > VirusTotal-URLEnrichment-incidentTrigger > Runs history >
Runs history
VirusTotal-URLEnrichment-incidentTrigger
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
11/23/2022, 1:11 AM
987 Milliseconds
11/23/2022, 1:10 AM
226 Milliseconds
11/23/2022, 12:27 AM
484 Milliseconds
Logic app run
08585324410173504651100701380CU169
Run Details
Resubmit
Cancel Run
Refresh
Info
100%
Entities list
{
"id": "/subscriptions/803140b9-666a-4e5c-957c-cff7b5029278/reso
"name": "d6a78695-d6bb-1219-b33c-828d3f9de4b3",
"type": "Microsoft.SecurityInsights/Entities",
"kind": "Url",
"properties": {
OUTPUTS
Show raw outputs
Status code
200
Headers
Key
Value
Pragma
no-cache
Transfer-Encoding
chunked
Vary
Accept-Encoding
Body
{
"Urls": [
{
"url": "www.bcomb.net",
"friendlyName": "www.bcomb.net",
"Type": "url"
}

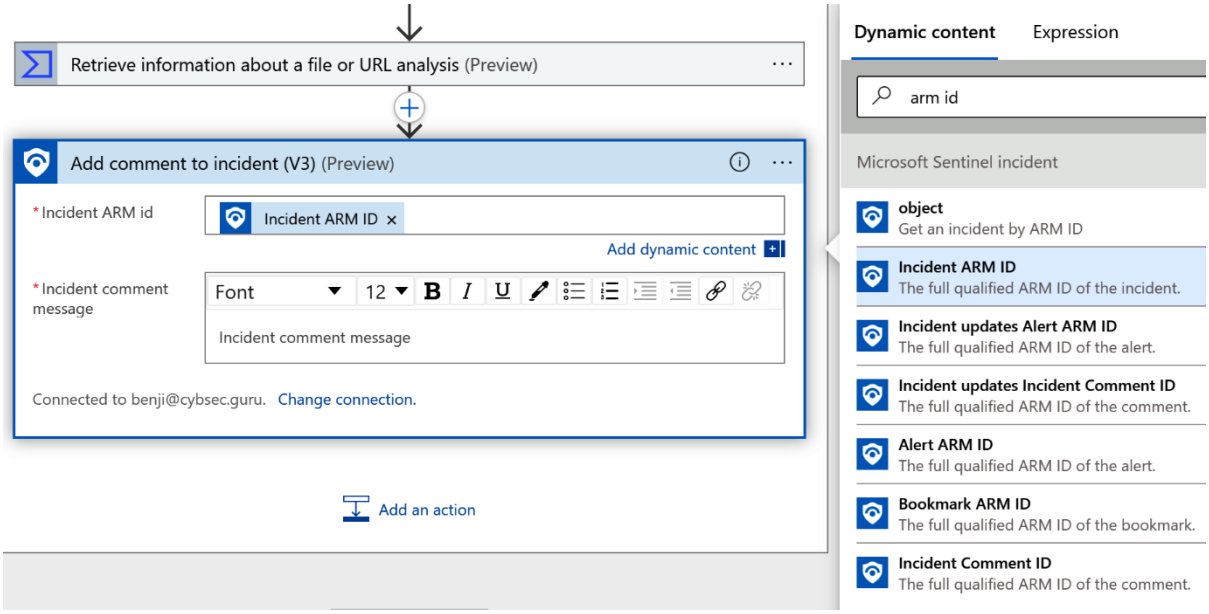

For each
1s
Previous
Previous failed
Show 1 of 1
Next failed
Next
Analyze a URL
0s
INPUTS
Download (Alt/Option + click)
OUTPUTS
Show raw outputs
id
u-efa31ce0c46fc0238d3c91e529946029599bada55fb525d2ed3cd34b3f6447e7-

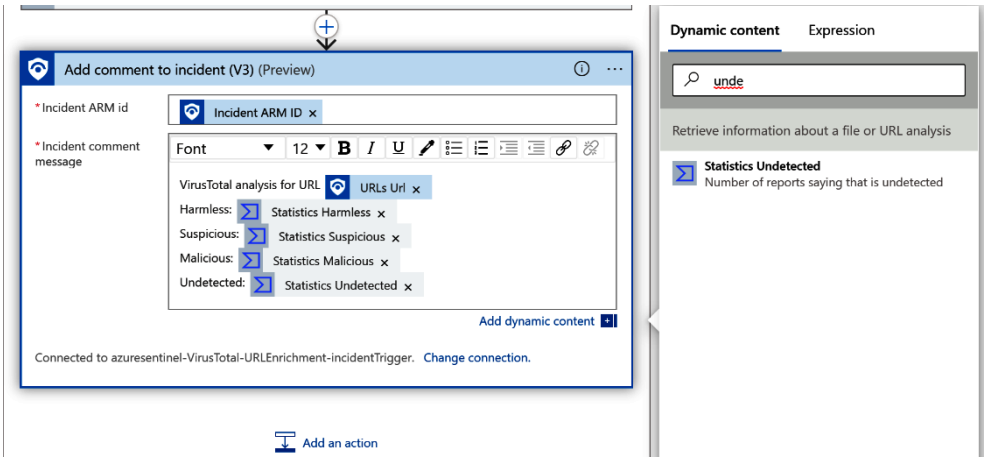

For each
*Select an output from previous steps
URLs
Analyze a URL (Preview)
Retrieve information about a file or URL analysis (Preview)
*Id
id
Add dynamic content
Connected to VirusTotal. Change connection.
Add an action
+ New step
Dynamic content
Expression
Search dynamic content
Analyze a URL
id
Entities - Get URLs
URLs Url
Microsoft Sentinel incident
Incident updates Alert Display Name
The display name of the alert
Incident updates Alert URI
This is the link to the alert in the orignal vendo
Incident updates Alert Description
The description of the alert.

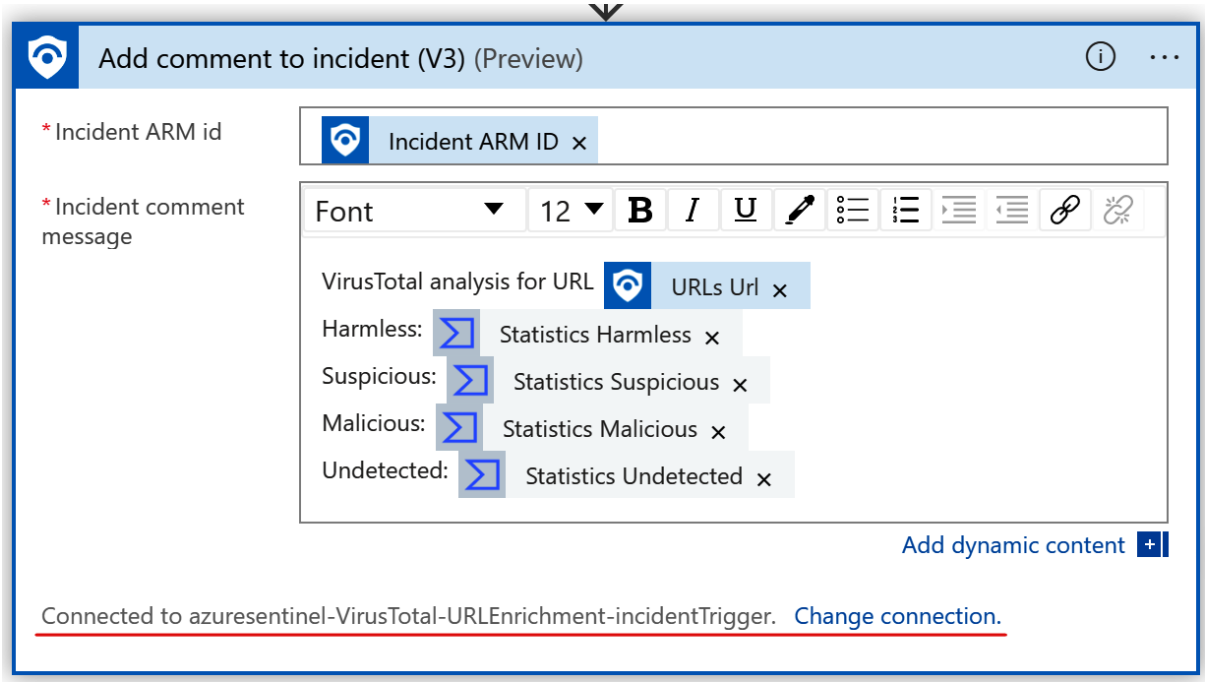
Outputs

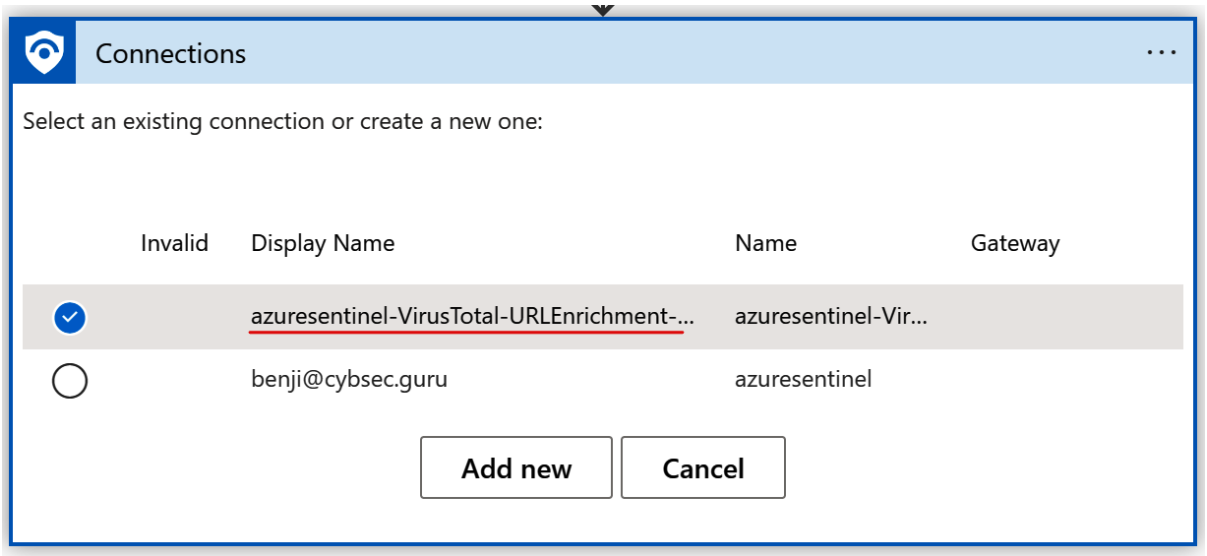
Retrieve information about a file or URL analysis

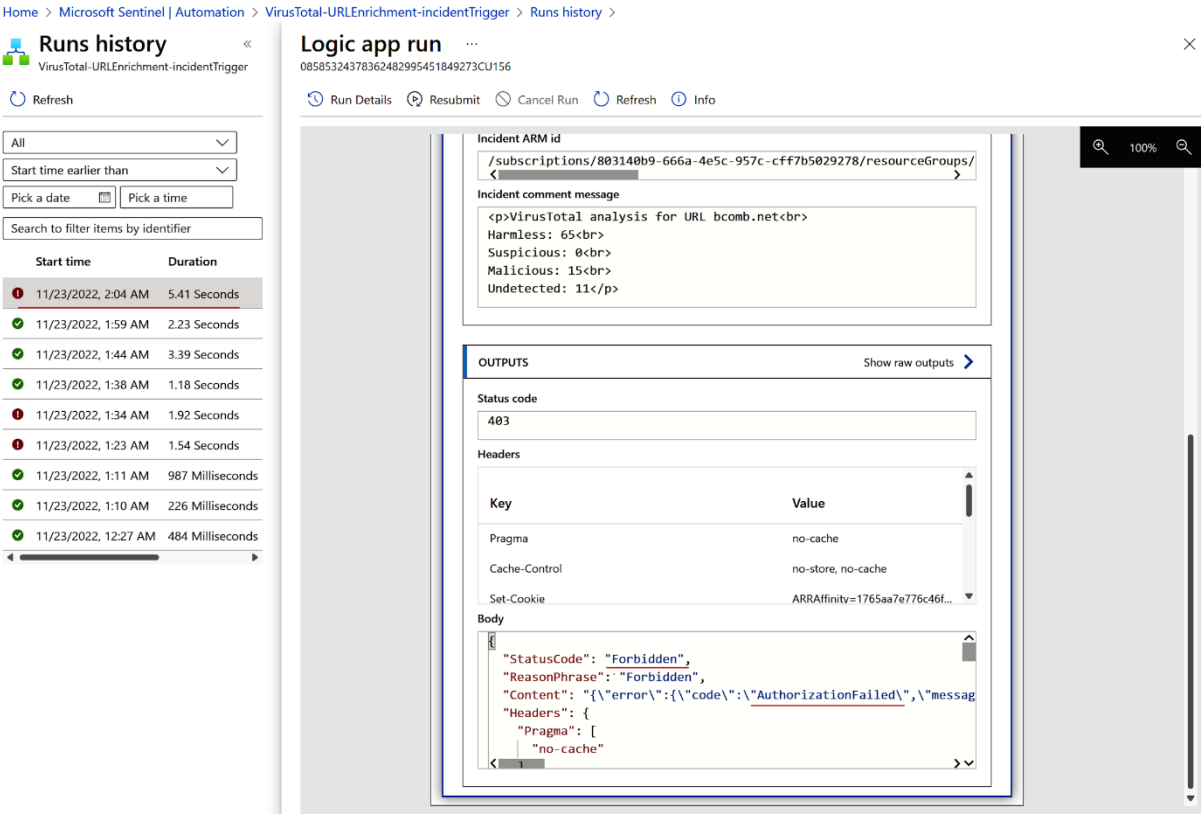

```
{
    "statusCode": 200,
    "headers": {
        "X-Cloud-Trace-Context": "64690eab866b59865a970da31b0181dc",
        "Timing-Allow-Origin": "*",
        "x-ms-apihub-cached-response": "true",
        "x-ms-apihub-obo": "false",
        "Date": "Wed, 23 Nov 2022 01:44:24 GMT",
        "Content-Length": "21698",
        "Content-Type": "application/json"
    },
    "body": {
        "meta": {
            "url_info": {
                "url": "http://bcomb.net/",
                "id": "efa31ce0c46fc0238d3c91e529946029599bada55fb525d2ed3cd34b3f6447e7"
            }
        },
        "data": {
            "attributes": {
                "date": 1669167505,
                "status": "completed",
                "stats": {
                    "harmless": 65,
                    "malicious": 15,
                    "suspicious": 0,
                    "undetected": 11,
                    "timeout": 0
                },
                "results": {
                    "Bkav": {
                        "category": "undetected",
                        "result": "unrated",
                        "method": "blacklist",
                        "engine_name": "Bkav"
                    },
                    "CMC Threat Intelligence": {
                        "category": "harmless",
                        "result": "clean",
                        "method": "blacklist",
```

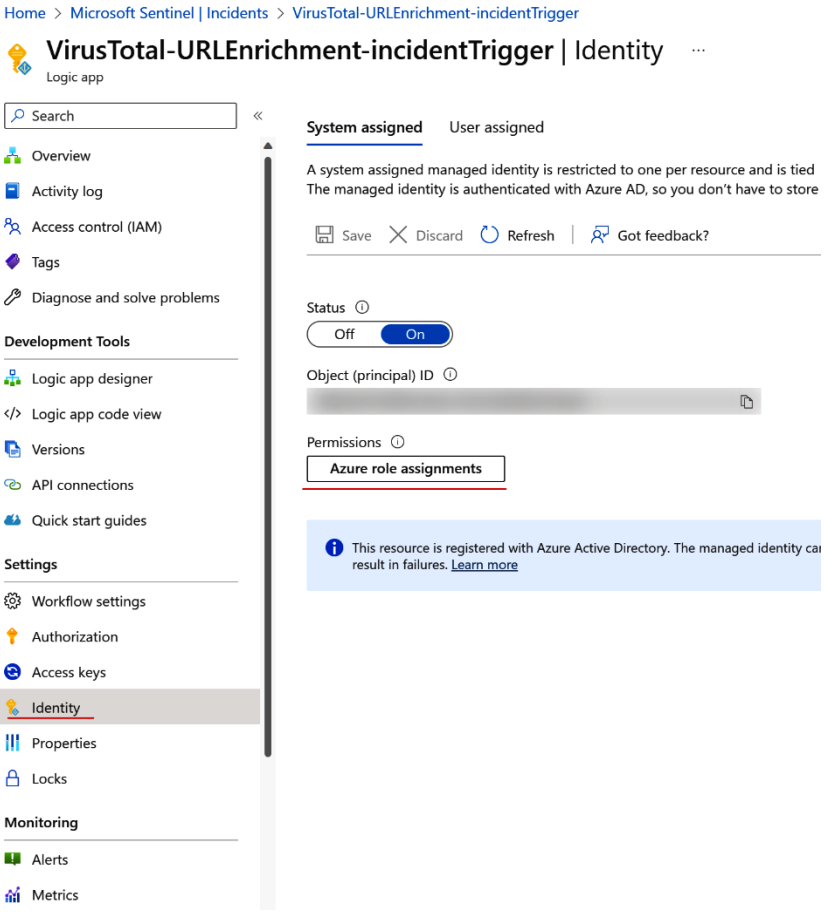

Retrieve information about a file or URL analysis (Preview)
Add comment to incident (V3) (Preview)
*Incident ARM id
Incident ARM ID
Add dynamic content
*Incident comment message
Font
12
Incident comment message
Connected to benji@cybsec.guru. Change connection.
Add an action
Dynamic content
Expression
arm id
Microsoft Sentinel incident
object
Get an incident by ARM ID
Incident ARM ID
The full qualified ARM ID of the incident.
Incident updates Alert ARM ID
The full qualified ARM ID of the alert.
Incident updates Incident Comment ID
The full qualified ARM ID of the comment.
Alert ARM ID
The full qualified ARM ID of the alert.
Bookmark ARM ID
The full qualified ARM ID of the bookmark.
Incident Comment ID
The full qualified ARM ID of the comment.

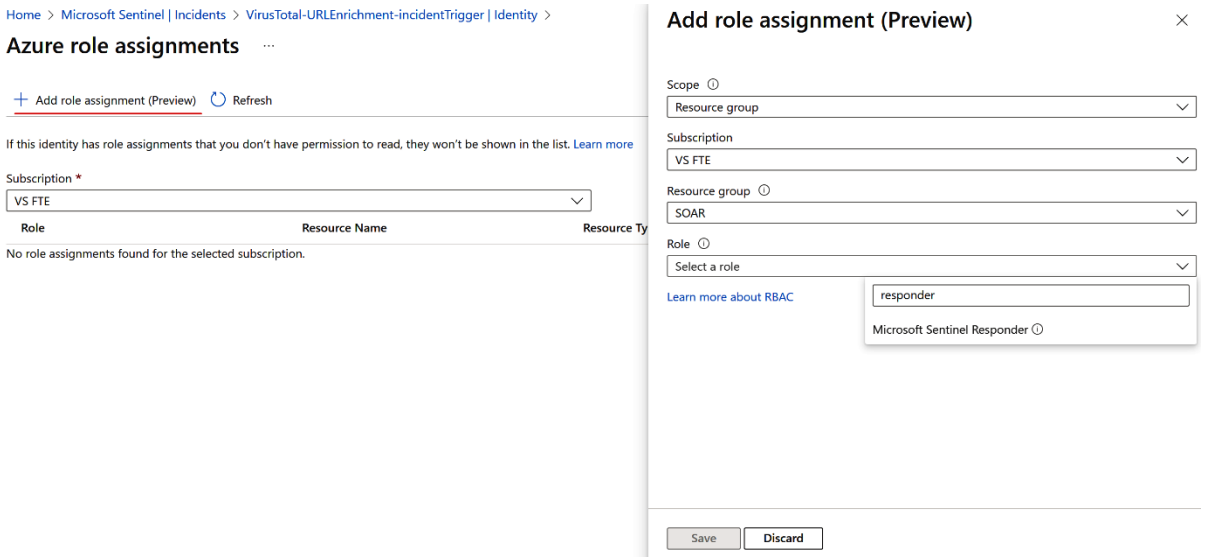

Add comment to incident (V3) (Preview)
*Incident ARM id
Incident ARM ID
*Incident comment message
Font
12
VirusTotal analysis for URL
URLs Url
Harmless:
Statistics Harmless
Suspicious:
Statistics Suspicious
Malicious:
Statistics Malicious
Undetected:
Statistics Undetected
Add dynamic content
Connected to azuresentinel-VirusTotal-URLEnrichment-incidentTrigger. Change connection.
Add an action
Dynamic content
Expression
unde
Retrieve information about a file or URL analysis
Statistics Undetected
Number of reports saying that is undetected

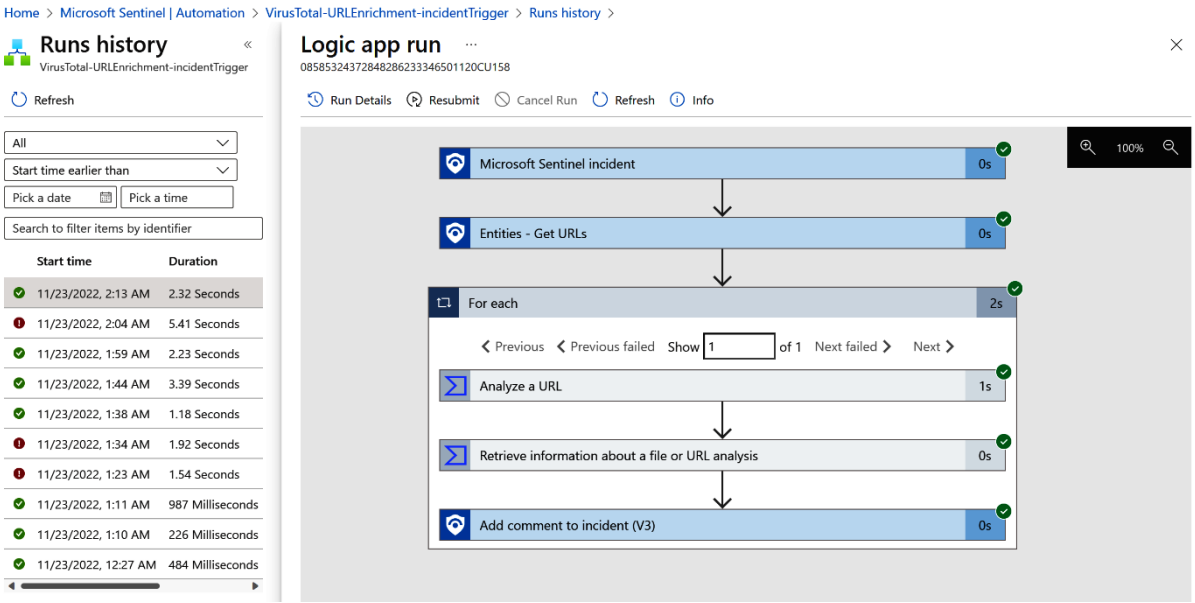

Add comment to incident (V3) (Preview)
* Incident ARM id
Incident ARM ID
* Incident comment message
Font
12
VirusTotal analysis for URL
URLs Url
Harmless:
Statistics Harmless
Suspicious:
Statistics Suspicious
Malicious:
Statistics Malicious
Undetected:
Statistics Undetected
Add dynamic content
Connected to azuresentinel-VirusTotal-URLEnrichment-incidentTrigger. Change connection.

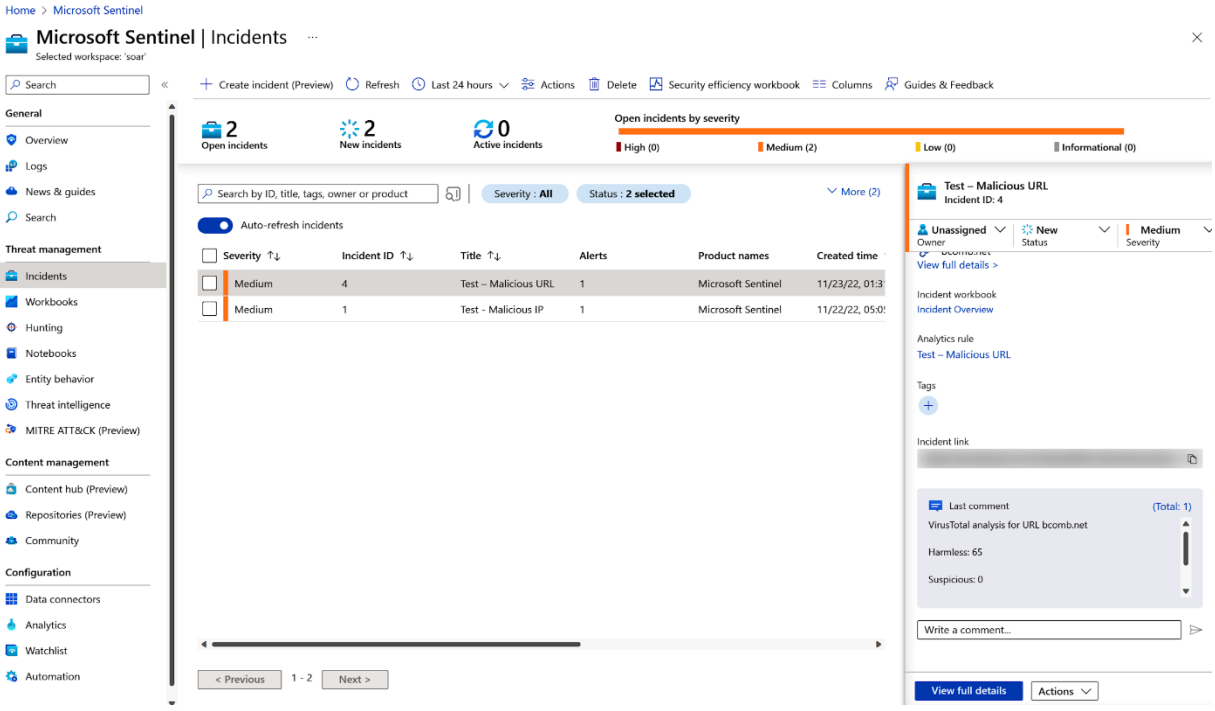

Connections
Select an existing connection or create a new one:
Invalid
Display Name
Name
Gateway
azuresentinel-VirusTotal-URLEnrichment-...
azuresentinel-Vir...
benji@cybsec.guru
azuresentinel
Add new
Cancel

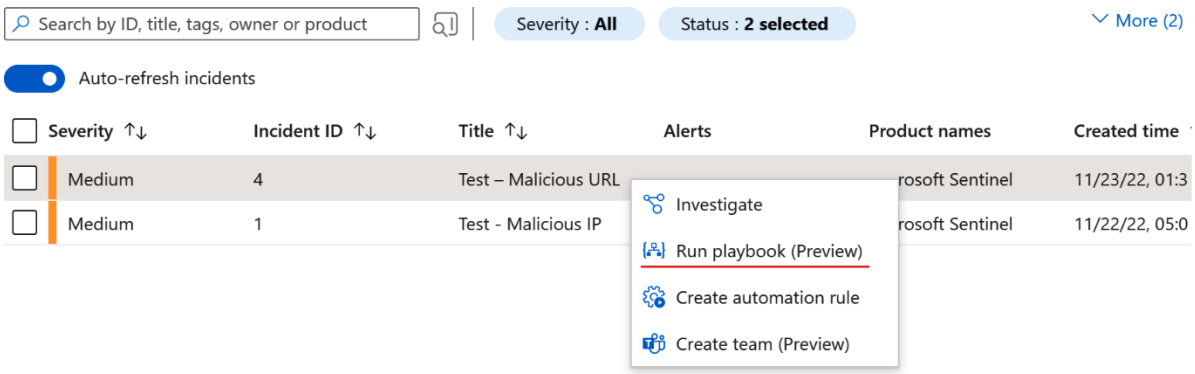

Home > Microsoft Sentinel | Automation > VirusTotal-URLEnrichment-incidentTrigger > Runs history >
Runs history
VirusTotal-URLEnrichment-incidentTrigger
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
11/23/2022, 2:04 AM 5.41 Seconds
11/23/2022, 1:59 AM 2.23 Seconds
11/23/2022, 1:44 AM 3.39 Seconds
11/23/2022, 1:38 AM 1.18 Seconds
11/23/2022, 1:34 AM 1.92 Seconds
11/23/2022, 1:23 AM 1.54 Seconds
11/23/2022, 1:11 AM 987 Milliseconds
11/23/2022, 1:10 AM 226 Milliseconds
11/23/2022, 12:27 AM 484 Milliseconds
Logic app run
085853243783624829954518492 73CU156
Run Details
Resubmit
Cancel Run
Refresh
Info
100%
Incident ARM id
/subscriptions/803140b9-666a-4e5c-957c-cff7b5029278/resourceGroups/
Incident comment message
VirusTotal analysis for URL bcomb.net
Harmless: 65
Suspicious: 0
Malicious: 15
Undetected: 11
OUTPUTS
Show raw outputs
Status code
403
Headers
Key
Value
Pragma
no-cache
Cache-Control
no-store, no-cache
Set-Cookie
ARRAffinity=1765aa7e776c46f...
Body
{
"StatusCode": "Forbidden",
"ReasonPhrase": "Forbidden",
"Content": "{\"error\":{\"code\":\"AuthorizationFailed\",\"messag
"Headers": {
"Pragma": [
"no-cache"

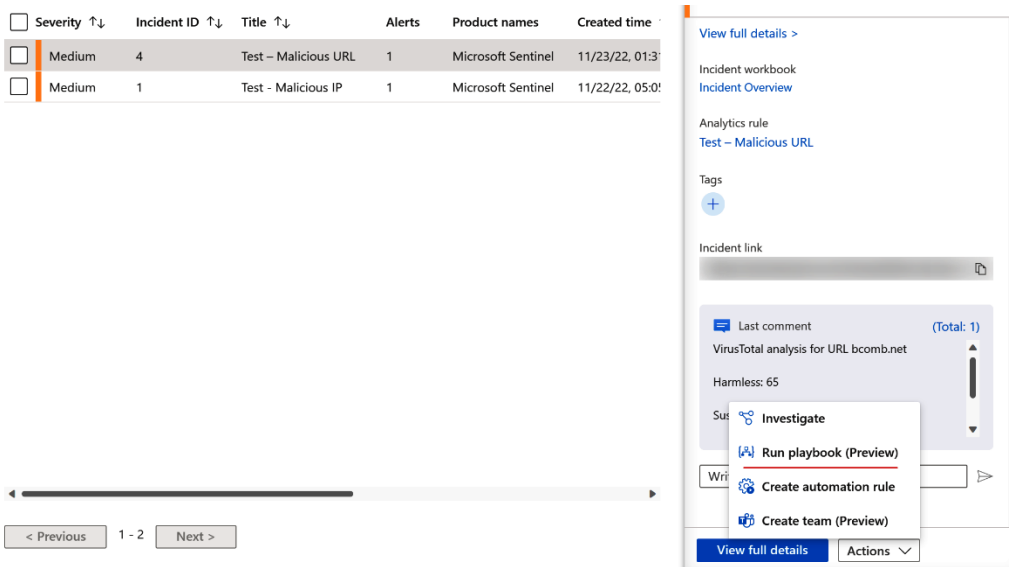

Home > Microsoft Sentinel | Incidents > VirusTotal-URLEnrichment-incidentTrigger
VirusTotal-URLEnrichment-incidentTrigger | Identity
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Metrics
System assigned
User assigned
A system assigned managed identity is restricted to one per resource and is tied
The managed identity is authenticated with Azure AD, so you don't have to store
Save
Discard
Refresh
Got feedback?
Status
Off
On
Object (principal) ID
Permissions
Azure role assignments
This resource is registered with Azure Active Directory. The managed identity ca
result in failures. Learn more

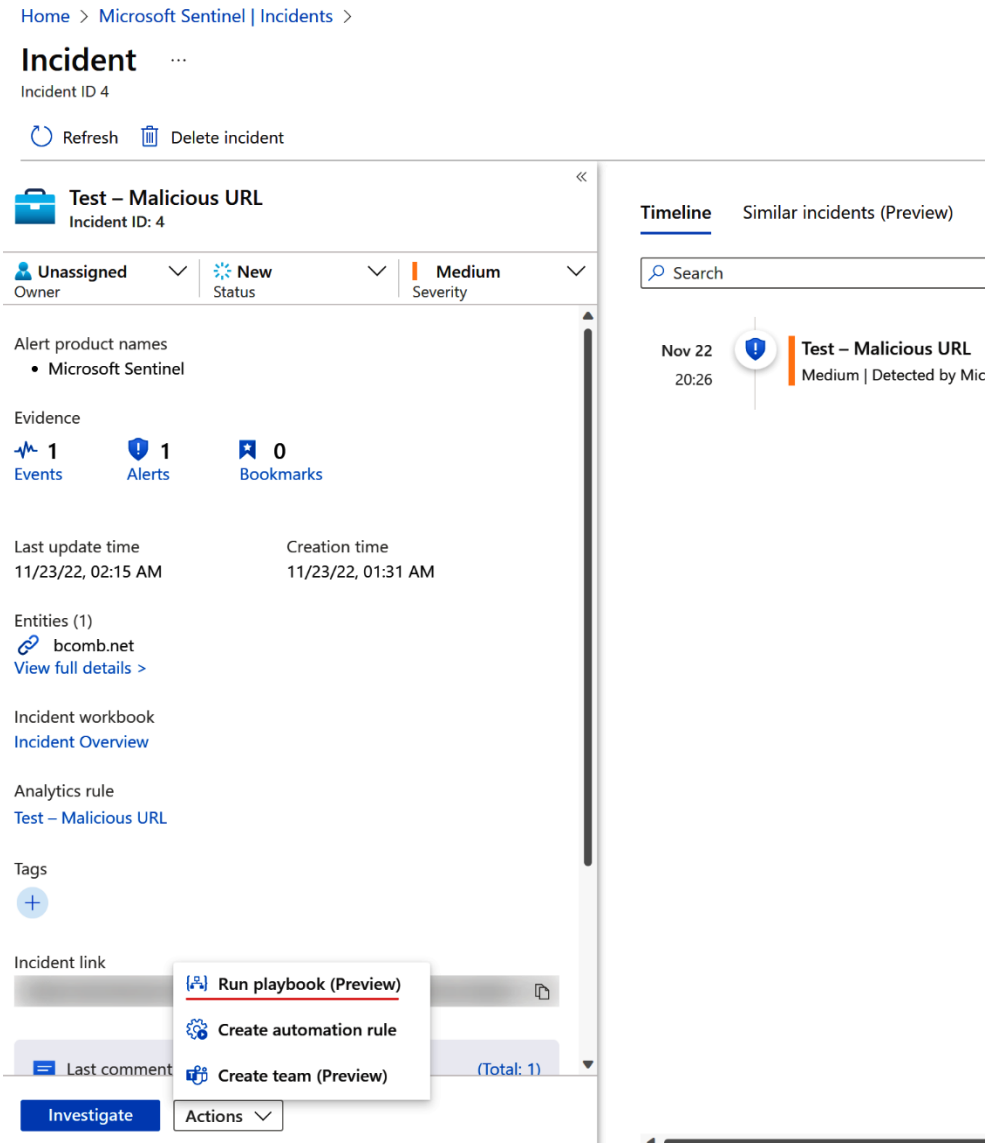

Home > Microsoft Sentinel | Incidents > VirusTotal-URLEnrichment-incidentTrigger | Identity >
Azure role assignments
Add role assignment (Preview)
Refresh
If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more
Subscription *
VS FTE
Role
Resource Name
Resource Ty
No role assignments found for the selected subscription.
Add role assignment (Preview)
Scope
Resource group
Subscription
VS FTE
Resource group
SOAR
Role
Select a role
Learn more about RBAC
responder
Microsoft Sentinel Responder
Save
Discard


Home > Microsoft Sentinel | Automation > VirusTotal-URLEnrichment-incidentTrigger > Runs history >
Runs history
VirusTotal-URLEnrichment-incidentTrigger
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
11/23/2022, 2:13 AM 2.32 Seconds
11/23/2022, 2:04 AM 5.41 Seconds
11/23/2022, 1:59 AM 2.23 Seconds
11/23/2022, 1:44 AM 3.39 Seconds
11/23/2022, 1:38 AM 1.18 Seconds
11/23/2022, 1:34 AM 1.92 Seconds
11/23/2022, 1:23 AM 1.54 Seconds
11/23/2022, 1:11 AM 987 Milliseconds
11/23/2022, 1:10 AM 226 Milliseconds
11/23/2022, 12:27 AM 484 Milliseconds
Logic app run
085853243728482862333465011 20CU158
Run Details
Resubmit
Cancel Run
Refresh
Info
100%
Microsoft Sentinel incident 0s
Entities - Get URLs 0s
For each 2s
Previous
Previous failed
Show 1 of 1
Next failed
Next
Analyze a URL 1s
Retrieve information about a file or URL analysis 0s
Add comment to incident (V3) 0s


Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
2
Open incidents
2
New incidents
0
Active incidents
Open incidents by severity
High (0)
Medium (2)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
More (2)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
4
Test – Malicious URL
1
Microsoft Sentinel
11/23/22, 01:3
Medium
1
Test - Malicious IP
1
Microsoft Sentinel
11/22/22, 05:0
< Previous
1 - 2
Next >
Test – Malicious URL
Incident ID: 4
Unassigned
Owner
New
Status
Medium
Severity
View full details >
Incident workbook
Incident Overview
Analytics rule
Test – Malicious URL
Tags
Incident link
Last comment
(Total: 1)
VirusTotal analysis for URL bcomb.net
Harmless: 65
Suspicious: 0
Write a comment...
View full details
Actions


Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
More (2)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
4
Test – Malicious URL
rosoft Sentinel
11/23/22, 01:3
Medium
1
Test - Malicious IP
rosoft Sentinel
11/22/22, 05:0
Investigate
Run playbook (Preview)
Create automation rule
Create team (Preview)


Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
4
Test – Malicious URL
1
Microsoft Sentinel
11/23/22, 01:3
Medium
1
Test - Malicious IP
1
Microsoft Sentinel
11/22/22, 05:0
< Previous
1 - 2
Next >
View full details >
Incident workbook
Incident Overview
Analytics rule
Test – Malicious URL
Tags
Incident link
Last comment
(Total: 1)
VirusTotal analysis for URL bcomb.net
Harmless: 65
Investigate
Run playbook (Preview)
Create automation rule
Create team (Preview)
View full details
Actions


Home > Microsoft Sentinel | Incidents >
Incident
Incident ID 4
Refresh
Delete incident
Test – Malicious URL
Incident ID: 4
Unassigned
Owner
New
Status
Medium
Severity
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
11/23/22, 02:15 AM
Creation time
11/23/22, 01:31 AM
Entities (1)
bcomb.net
View full details >
Incident workbook
Incident Overview
Analytics rule
Test – Malicious URL
Tags
Incident link
Run playbook (Preview)
Create automation rule
Create team (Preview)
Last comment
(Total: 1)
Investigate
Actions
Timeline
Similar incidents (Preview)
Search
Nov 22
20:26
Test – Malicious URL
Medium | Detected by Mic

Create new automation rule

Automation rule name

Test - Malicious URL

Trigger

When incident is created

Conditions

If

Analytic rule name | Contains | All

+ Add

Actions

Run playbook

VirusTotal-URLEnrichment-incidentTrigger
VS FTE / SOAR

+ Add action

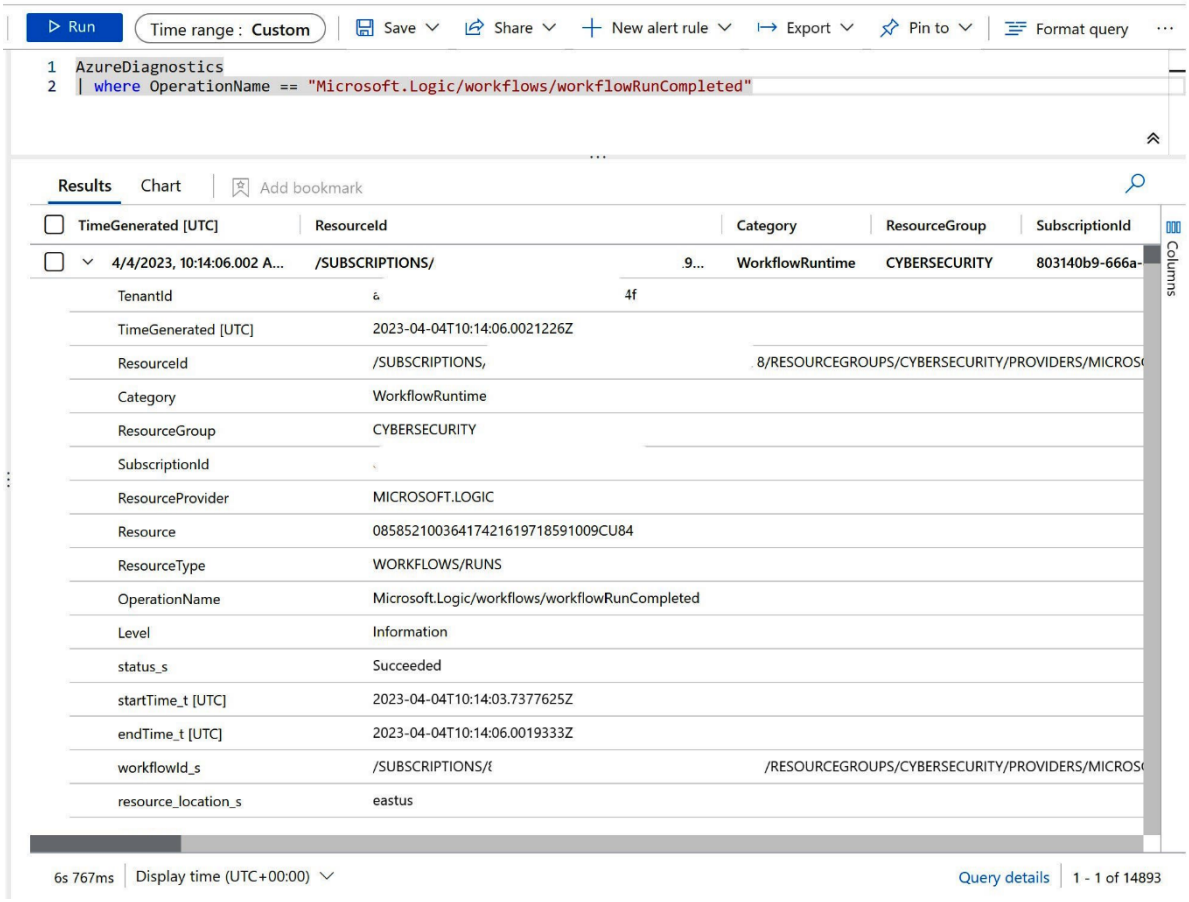
Rule expiration

Indefinite | Time

Order

1

Apply | Cancel


Run
Time range : Custom
Save
Share
New alert rule
Export
Pin to
Format query
1 AzureDiagnostics
2 | where OperationName == "Microsoft.Logic/workflows/workflowRunCompleted"
Results
Chart
Add bookmark
TimeGenerated [UTC]
ResourceId
Category
ResourceGroup
SubscriptionId
4/4/2023, 10:14:06.002 A...
/SUBSCRIPTIONS/
9...
WorkflowRuntime
CYBERSECURITY
803140b9-666a-
TenantId
4f
TimeGenerated [UTC]
2023-04-04T10:14:06.0021226Z
ResourceId
/SUBSCRIPTIONS/
8/RESOURCEGROUPS/CYBERSECURITY/PROVIDERS/MICROS
Category
WorkflowRuntime
ResourceGroup
CYBERSECURITY
SubscriptionId
ResourceProvider
MICROSOFT.LOGIC
Resource
08585210036417421619718591009CU84
ResourceType
WORKFLOWS/RUNS
OperationName
Microsoft.Logic/workflows/workflowRunCompleted
Level
Information
status_s
Succeeded
startTime_t [UTC]
2023-04-04T10:14:03.7377625Z
endTime_t [UTC]
2023-04-04T10:14:06.0019333Z
workflowId_s
/SUBSCRIPTIONS/
/RESOURCEGROUPS/CYBERSECURITY/PROVIDERS/MICROS
resource_location_s
eastus
Columns
6s 767ms
Display time (UTC+00:00)
Query details
1 - 1 of 14893

Chapter 7: Managing Incidents with Automation

Home >

Create Logic App ...

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

Subscription * ⓘ — VS FTE

Resource Group * ⓘ — SOAR

Create new

Instance Details

Logic App name * — SOARIncidentManagement

.azurewebsites.net

Publish * — (•) Workflow ( ) Docker Container

Region * — East US

ⓘ Not finding your App Service Plan? Try a different region or select your App Service Environment.

Plan

The plan type you choose dictates how your app scales, what features are enabled, and how it is priced. Learn more

Plan type * —

(•) **Standard:** Best for enterprise-level, serverless applications, with event-based scaling and networking isolation.

( ) **Consumption:** Best for entry-level. Pay only as much as your workflow runs.

Windows Plan (East US) * ⓘ — (New) ASP-SOAR-8feb

Create new

Pricing plan * —

Workflow Standard WS1
210 total ACU, 3.5 GB memory
Change size

Review + create | < Previous | Next : Hosting >

Home >

Create Logic App ...

Basics **Hosting** Monitoring Tags Review + create

Storage

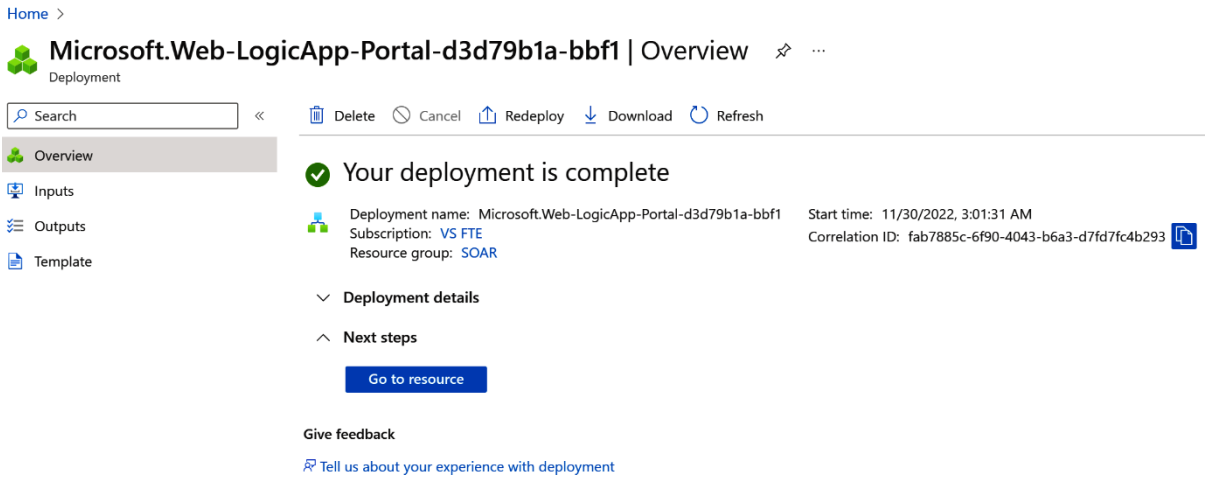
When creating a logic app, you must create or link to an external storage, which is used to store workflow state, run history, and artifacts.

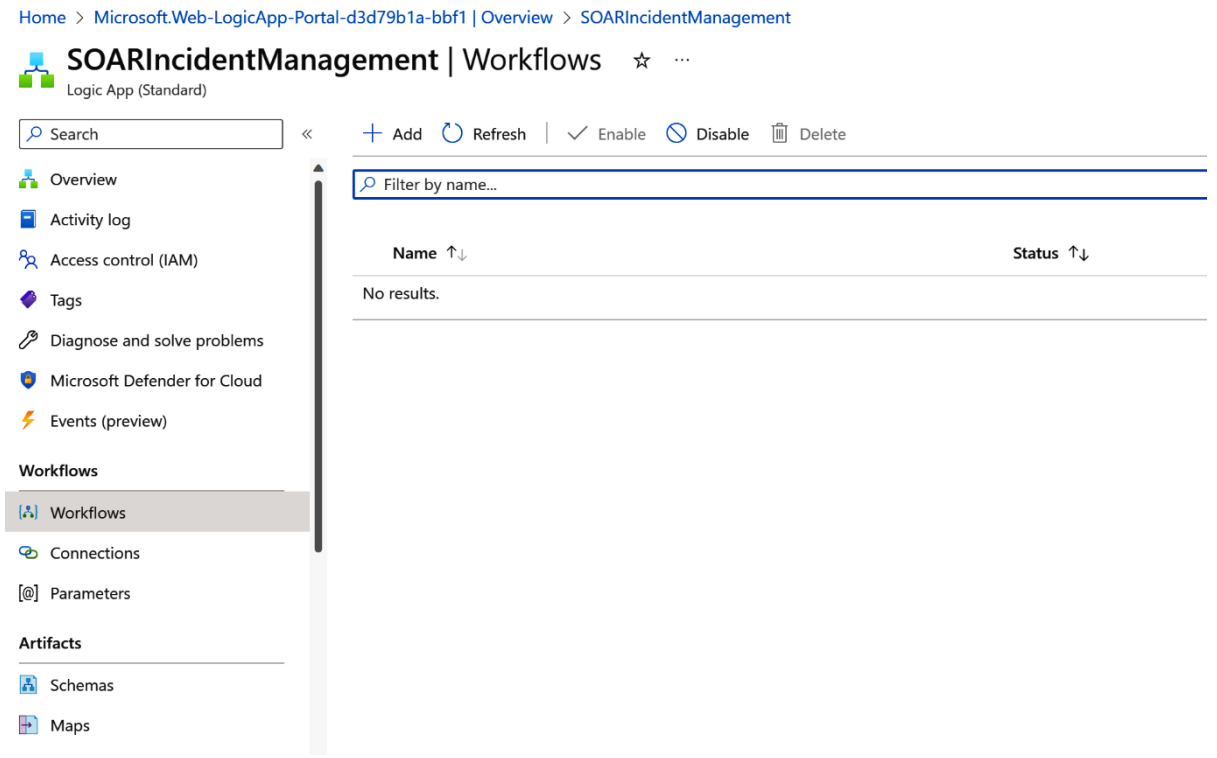
Storage type * Azure Storage

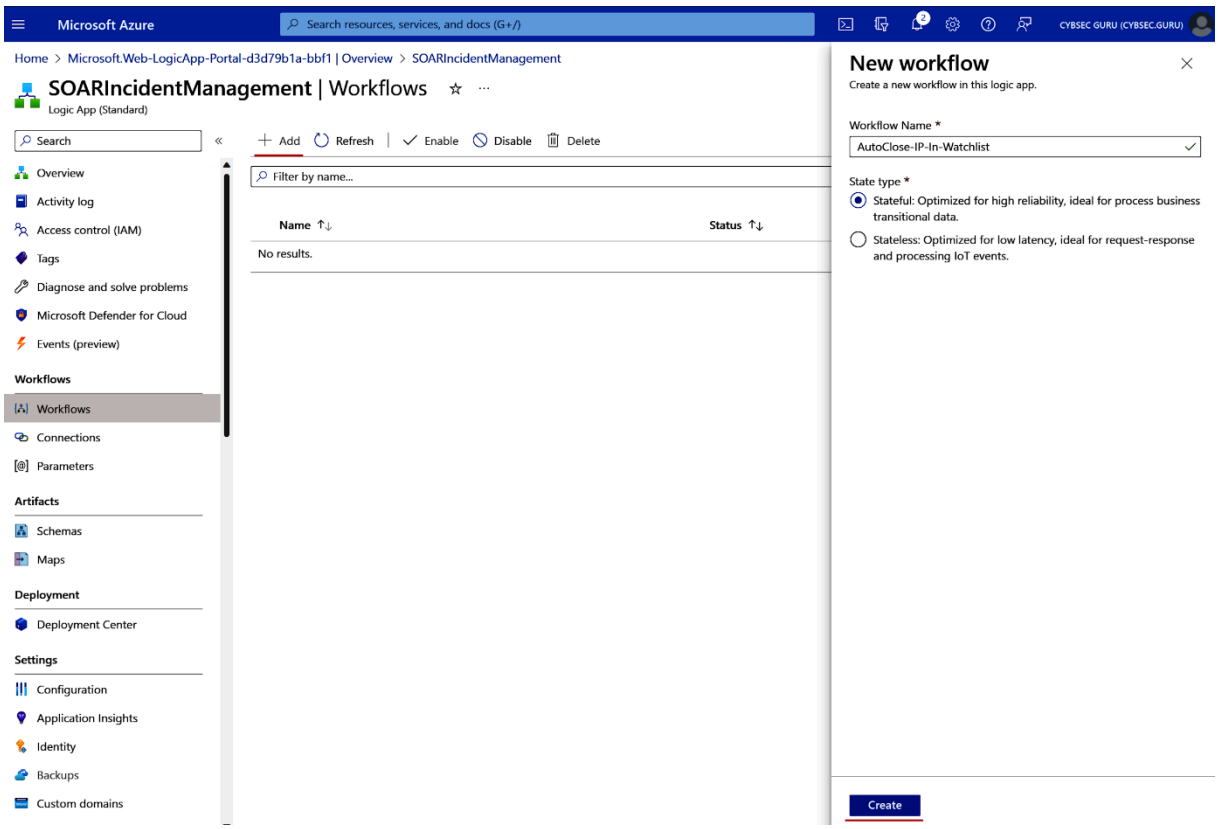
Storage account * (New) soarab4d

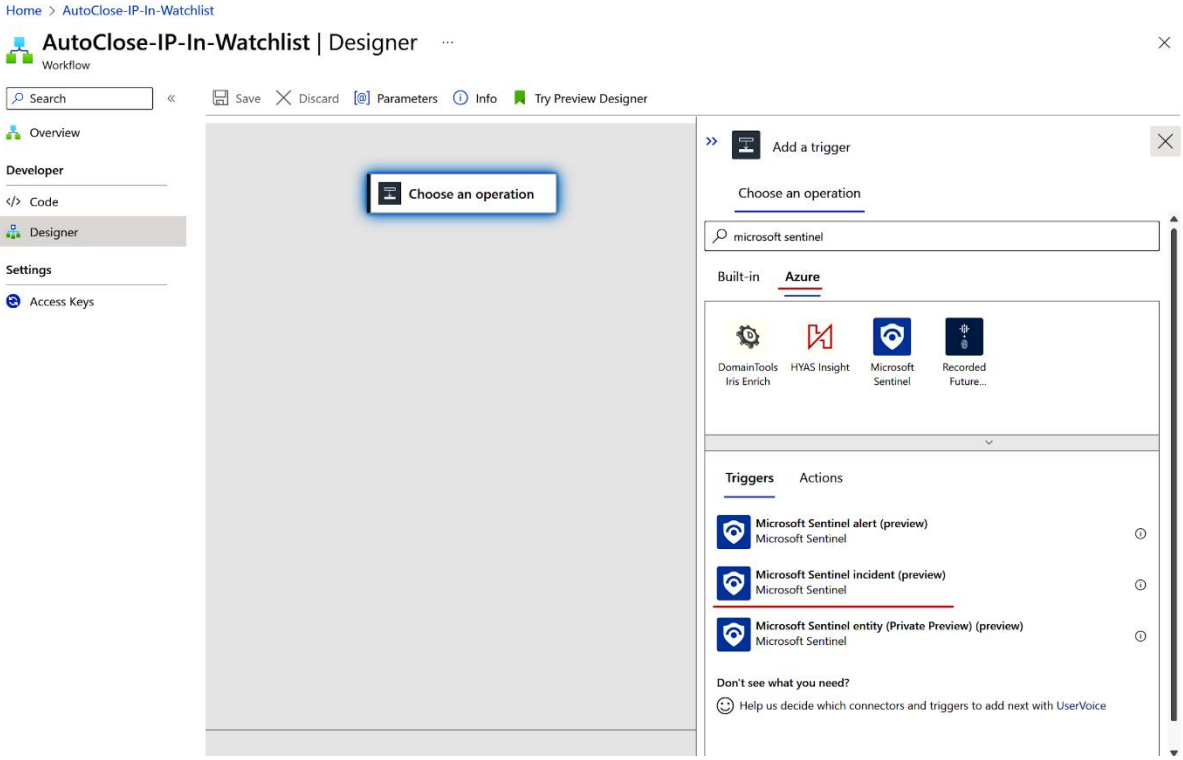
Create new

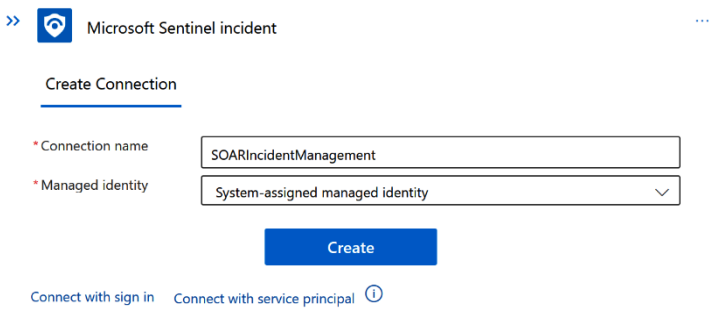
Review + create < Previous Next : Monitoring >

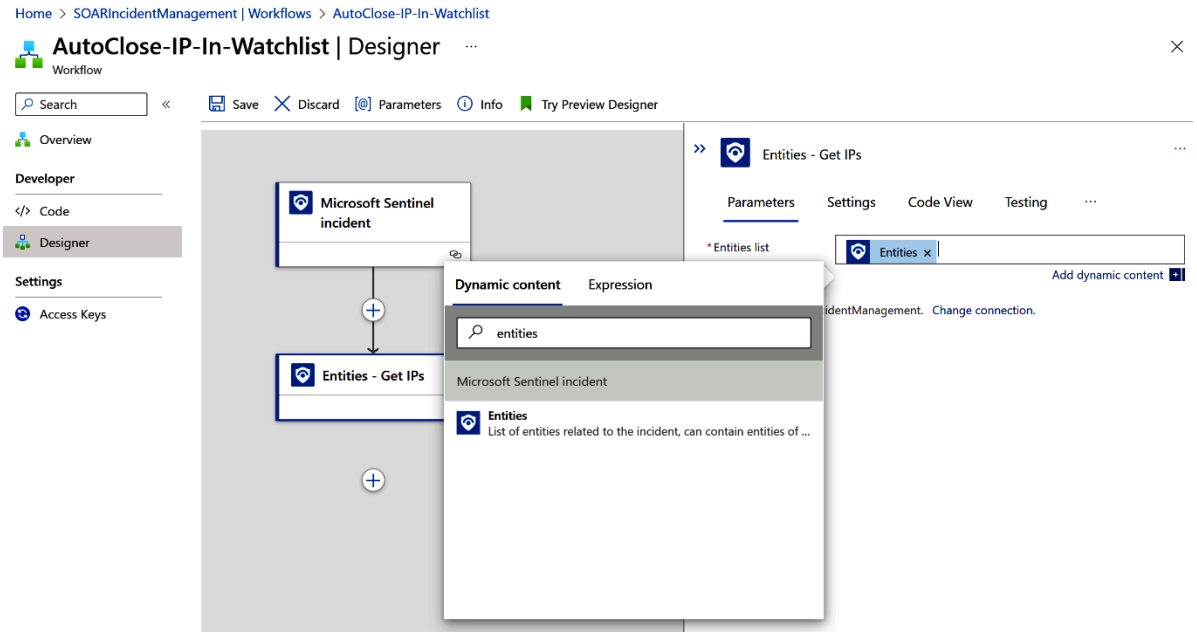


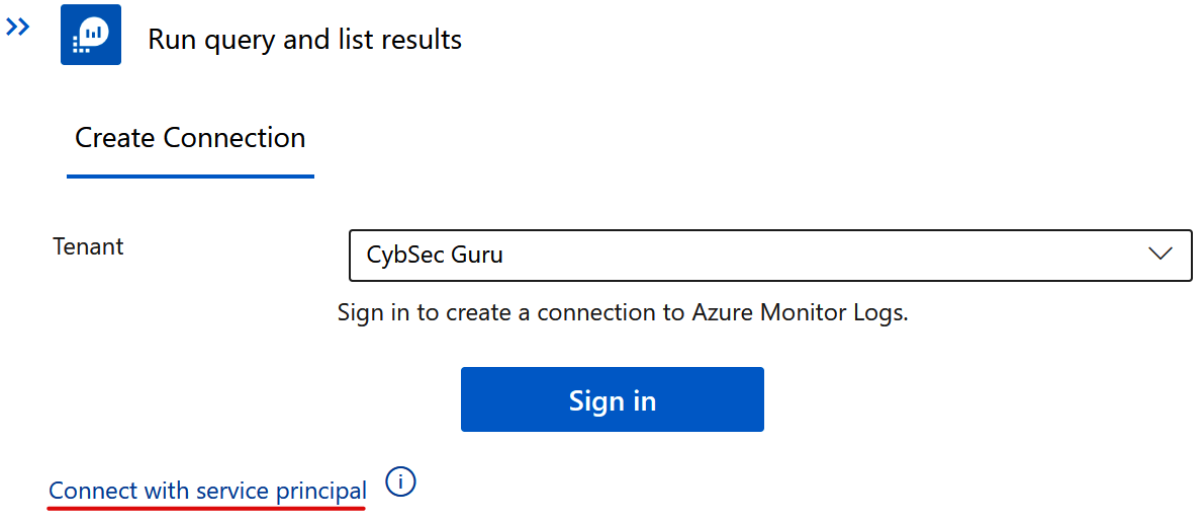

Home > Microsoft.Web-LogicApp-Portal-d3d79b1a-bbf1 | Overview > SOARIncidentManagement
SOARIncidentManagement | Workflows
Logic App (Standard)
Search
Add
Refresh
Enable
Disable
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Workflows
Workflows
Connections
Parameters
Artifacts
Schemas
Maps
Filter by name...
Name
Status
No results.

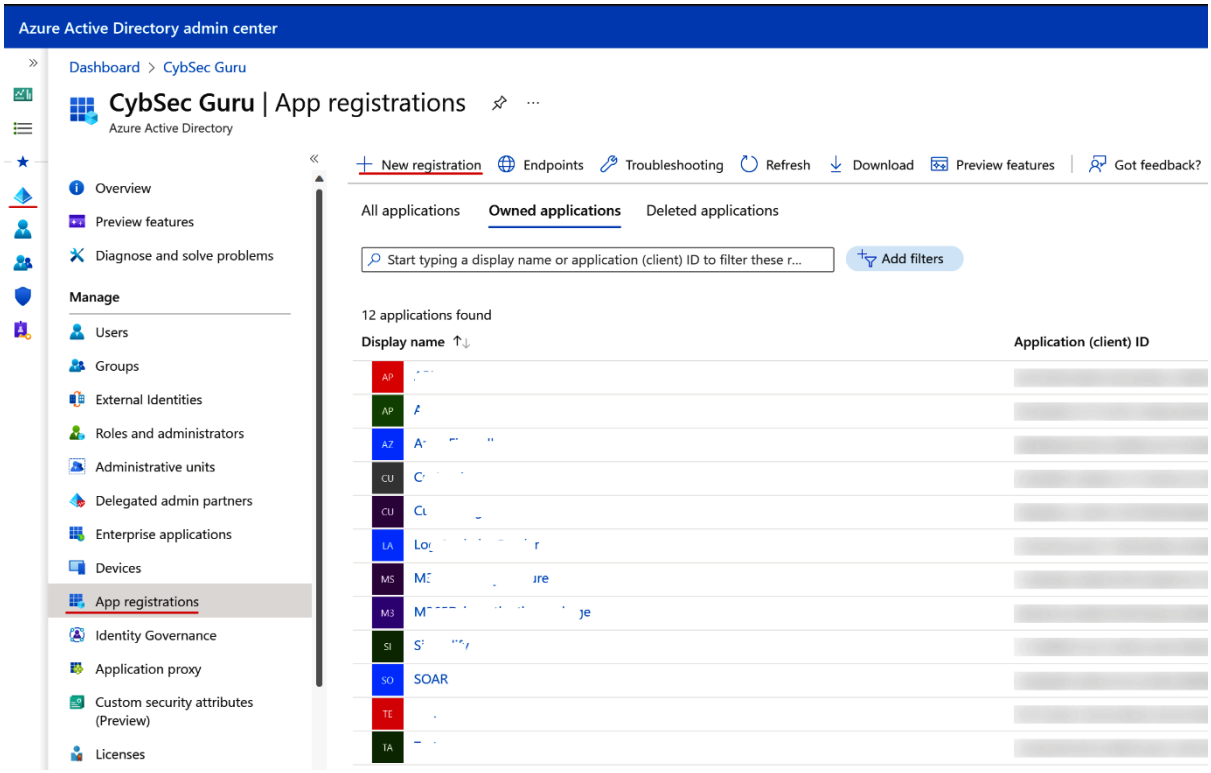

Microsoft Azure
Search resources, services, and docs (G+/)
CYBSEC GURU (CYBSEC.GURU)
Home > Microsoft.Web-LogicApp-Portal-d3d79b1a-bbf1 | Overview > SOARIncidentManagement
SOARIncidentManagement | Workflows
Logic App (Standard)
Search
Add
Refresh
Enable
Disable
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Workflows
Workflows
Connections
Parameters
Artifacts
Schemas
Maps
Deployment
Deployment Center
Settings
Configuration
Application Insights
Identity
Backups
Custom domains
Filter by name...
Name
Status
No results.
New workflow
Create a new workflow in this logic app.
Workflow Name *
AutoClose-IP-In-Watchlist
State type *
Stateful: Optimized for high reliability, ideal for process business transitional data.
Stateless: Optimized for low latency, ideal for request-response and processing IoT events.
Create

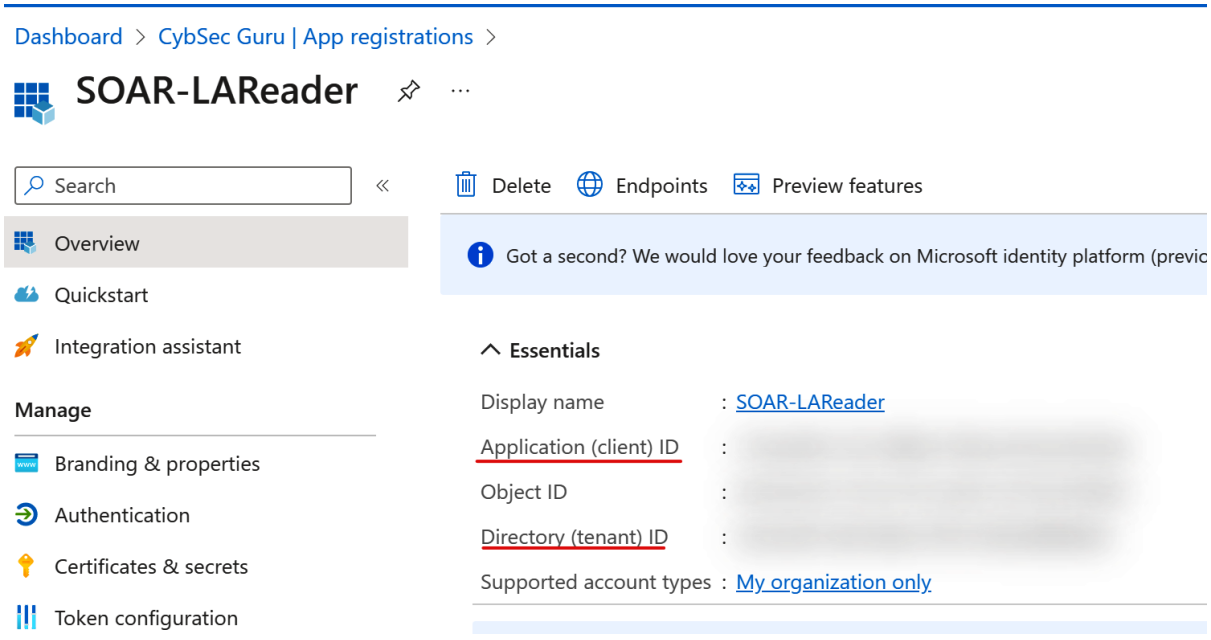

Home > AutoClose-IP-In-Watchlist
AutoClose-IP-In-Watchlist | Designer
Workflow
Search
Overview
Developer
Code
Designer
Settings
Access Keys
Save
Discard
Parameters
Info
Try Preview Designer
Choose an operation
Add a trigger
Choose an operation
microsoft sentinel
Built-in
Azure
DomainTools Iris Enrich
HYAS Insight
Microsoft Sentinel
Recorded Future...
Triggers
Actions
Microsoft Sentinel alert (preview)
Microsoft Sentinel
Microsoft Sentinel incident (preview)
Microsoft Sentinel
Microsoft Sentinel entity (Private Preview) (preview)
Microsoft Sentinel
Don't see what you need?
Help us decide which connectors and triggers to add next with UserVoice


Microsoft Sentinel incident
Create Connection
* Connection name
SOARIncidentManagement
* Managed identity
System-assigned managed identity
Create
Connect with sign in
Connect with service principal


Home > SOARIncidentManagement | Workflows > AutoClose-IP-In-Watchlist
AutoClose-IP-In-Watchlist | Designer
Workflow
Search
Overview
Developer
Code
Designer
Settings
Access Keys
Save
Discard
Parameters
Info
Try Preview Designer
Microsoft Sentinel incident
Entities - Get IPs
Dynamic content
Expression
entities
Microsoft Sentinel incident
Entities
List of entities related to the incident, can contain entities of ...
Entities - Get IPs
Parameters
Settings
Code View
Testing
* Entities list
Entities
Add dynamic content
Change connection.


Run query and list results
Create Connection
Tenant
CybSec Guru
Sign in to create a connection to Azure Monitor Logs.
Sign in
Connect with service principal


Azure Active Directory admin center
Dashboard > CybSec Guru
CybSec Guru | App registrations
Azure Active Directory
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security attributes (Preview)
Licenses
New registration
Endpoints
Troubleshooting
Refresh
Download
Preview features
Got feedback?
All applications
Owned applications
Deleted applications
Start typing a display name or application (client) ID to filter these r...
Add filters
12 applications found
Display name
Application (client) ID
SOAR


Dashboard > CybSec Guru | App registrations >
SOAR-LAReader
Search
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
Delete
Endpoints
Preview features
Got a second? We would love your feedback on Microsoft identity platform (previc
Essentials
Display name : SOAR-LAReader
Application (client) ID :
Object ID :
Directory (tenant) ID :
Supported account types : My organization only

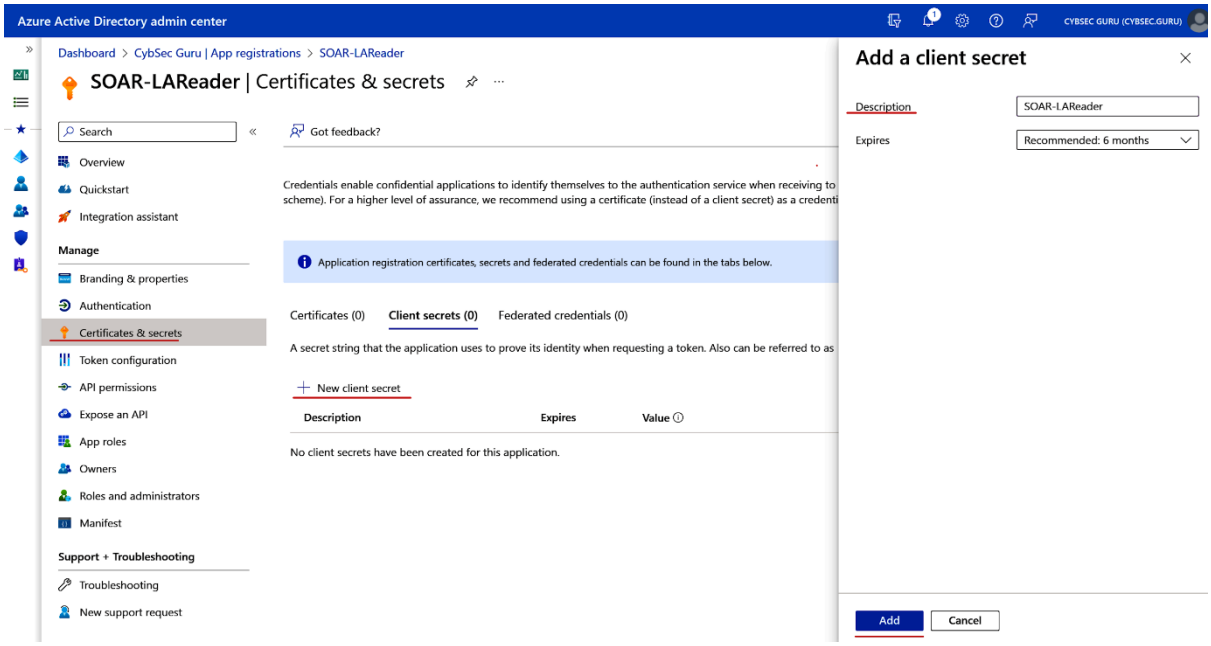
Run query and list results

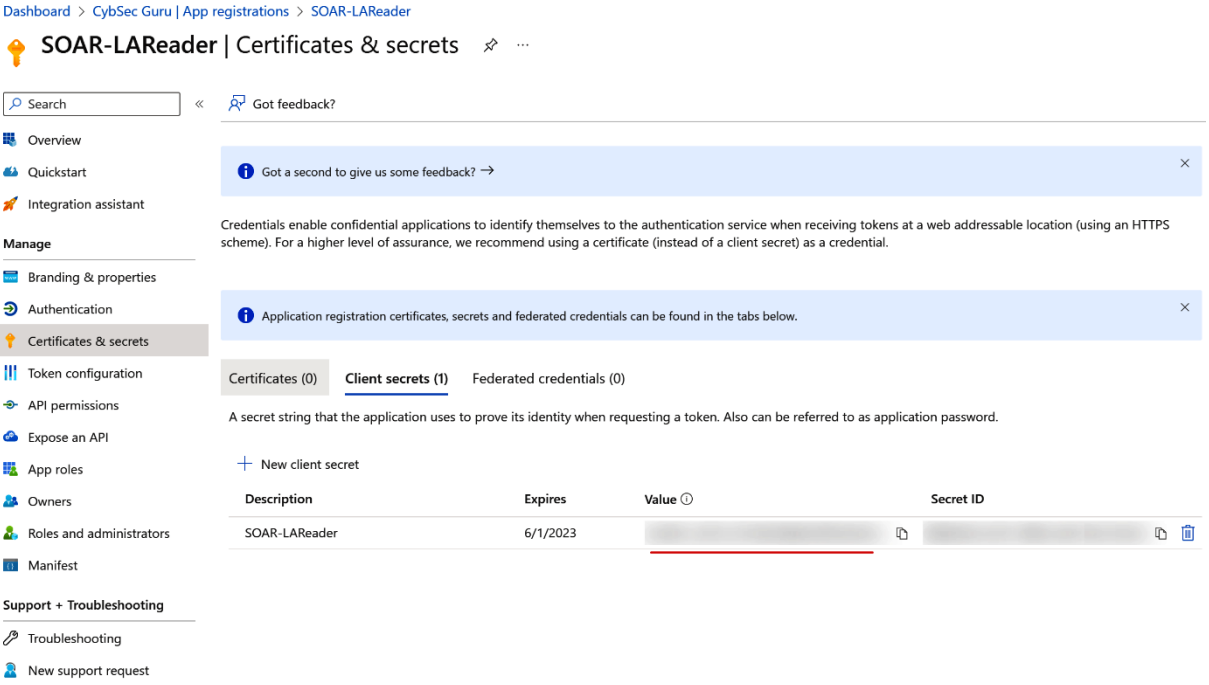
Create Connection

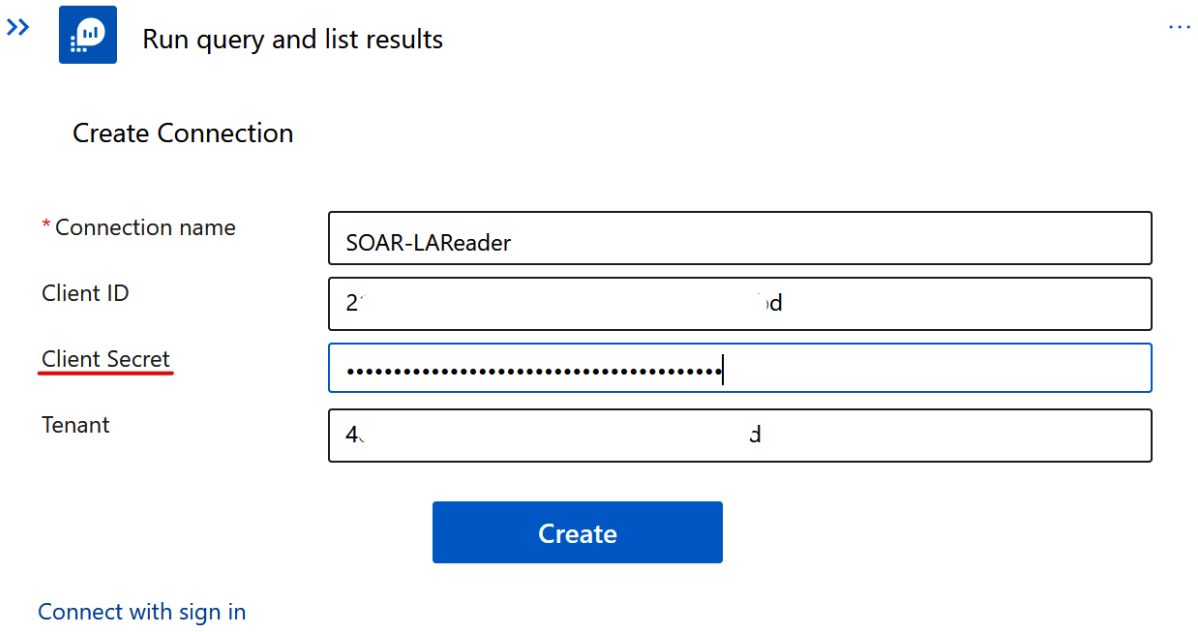
* Connection name	SOAR-LAReader
Client ID	2 d
Client Secret	Client secret of the Azure Active Directory application.
Tenant	4 5d

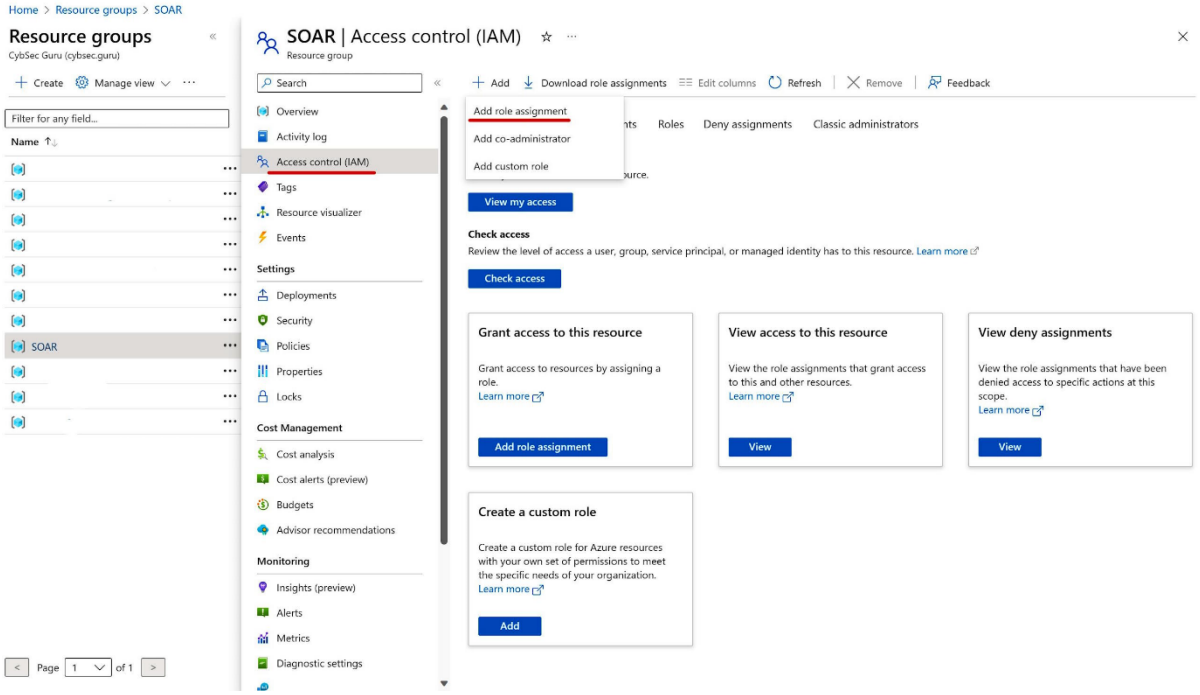
Create

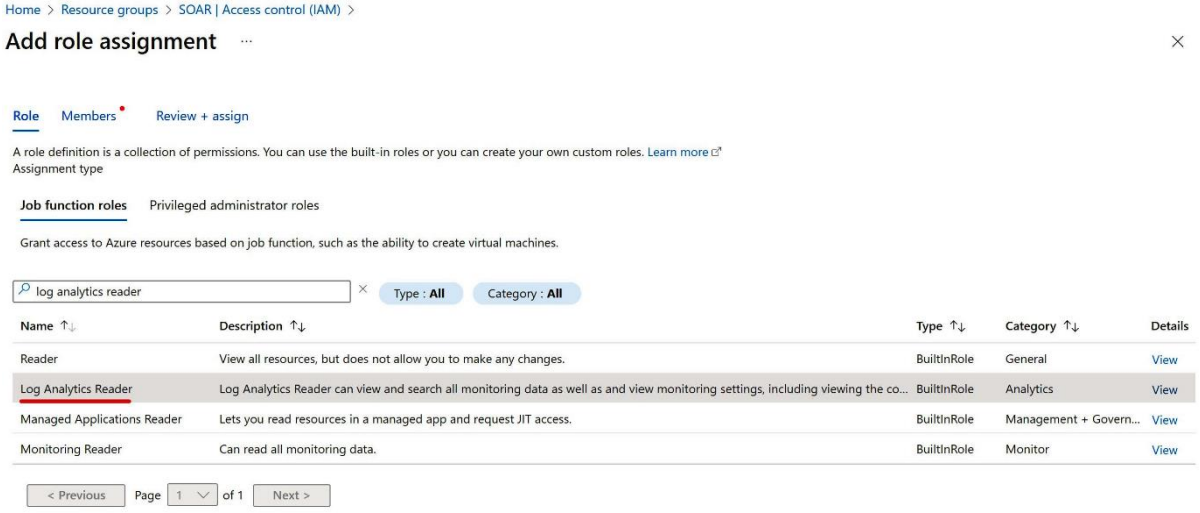
Connect with sign in

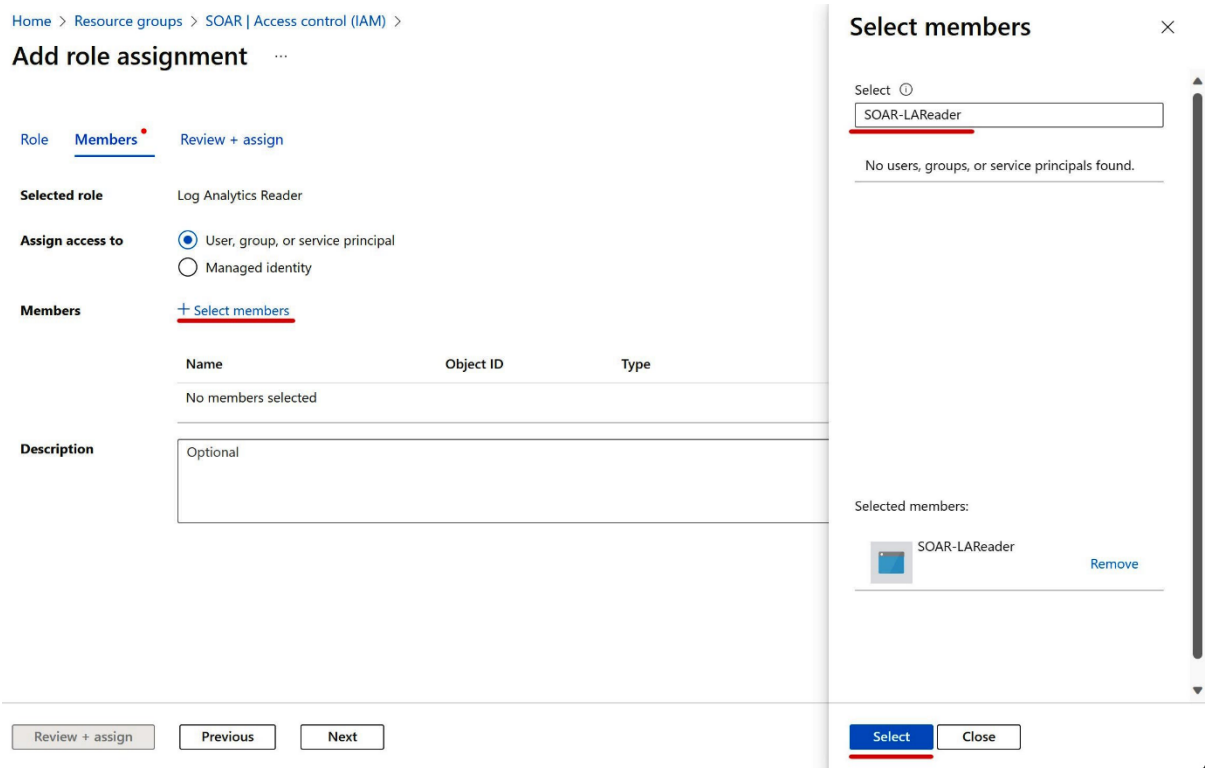


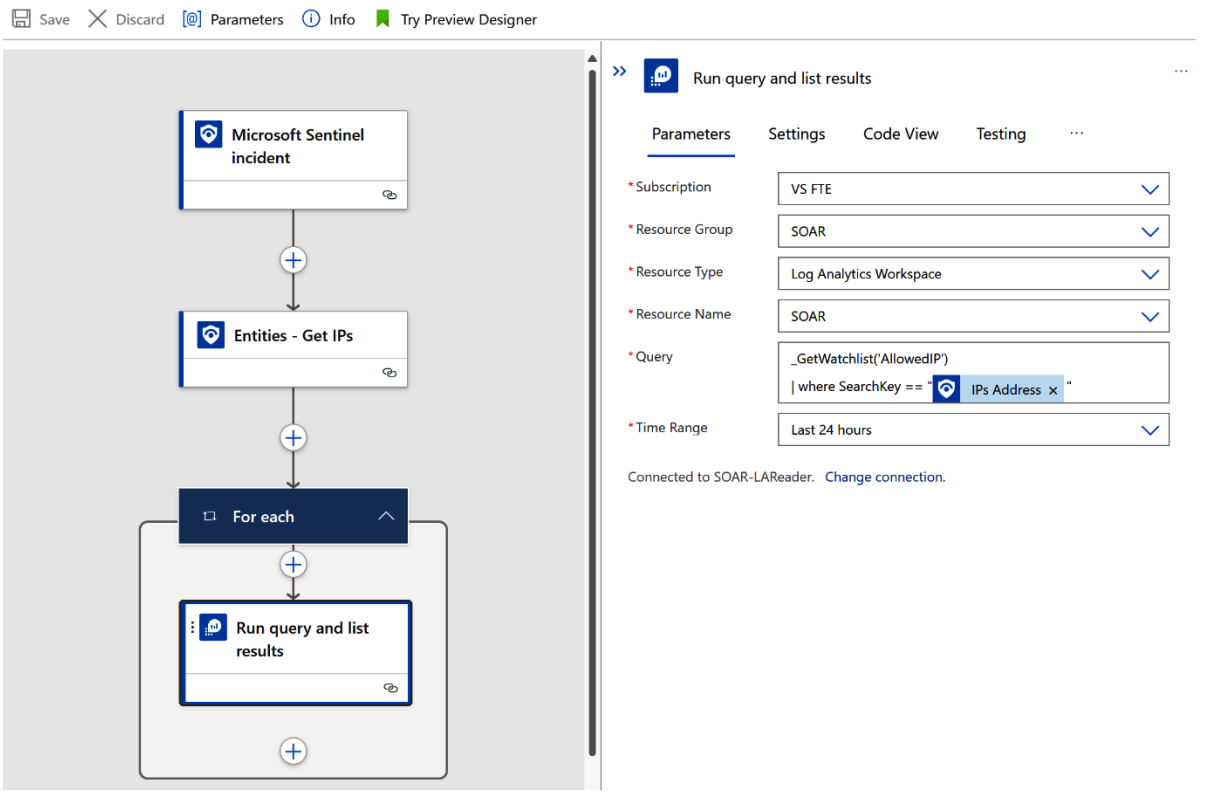

Dashboard > CybSec Guru | App registrations > SOAR-LAReader
SOAR-LAReader | Certificates & secrets
Search
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Got a second to give us some feedback?
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
Application registration certificates, secrets and federated credentials can be found in the tabs below.
Certificates (0)
Client secrets (1)
Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
New client secret
Description
Expires
Value
Secret ID
SOAR-LAReader
6/1/2023

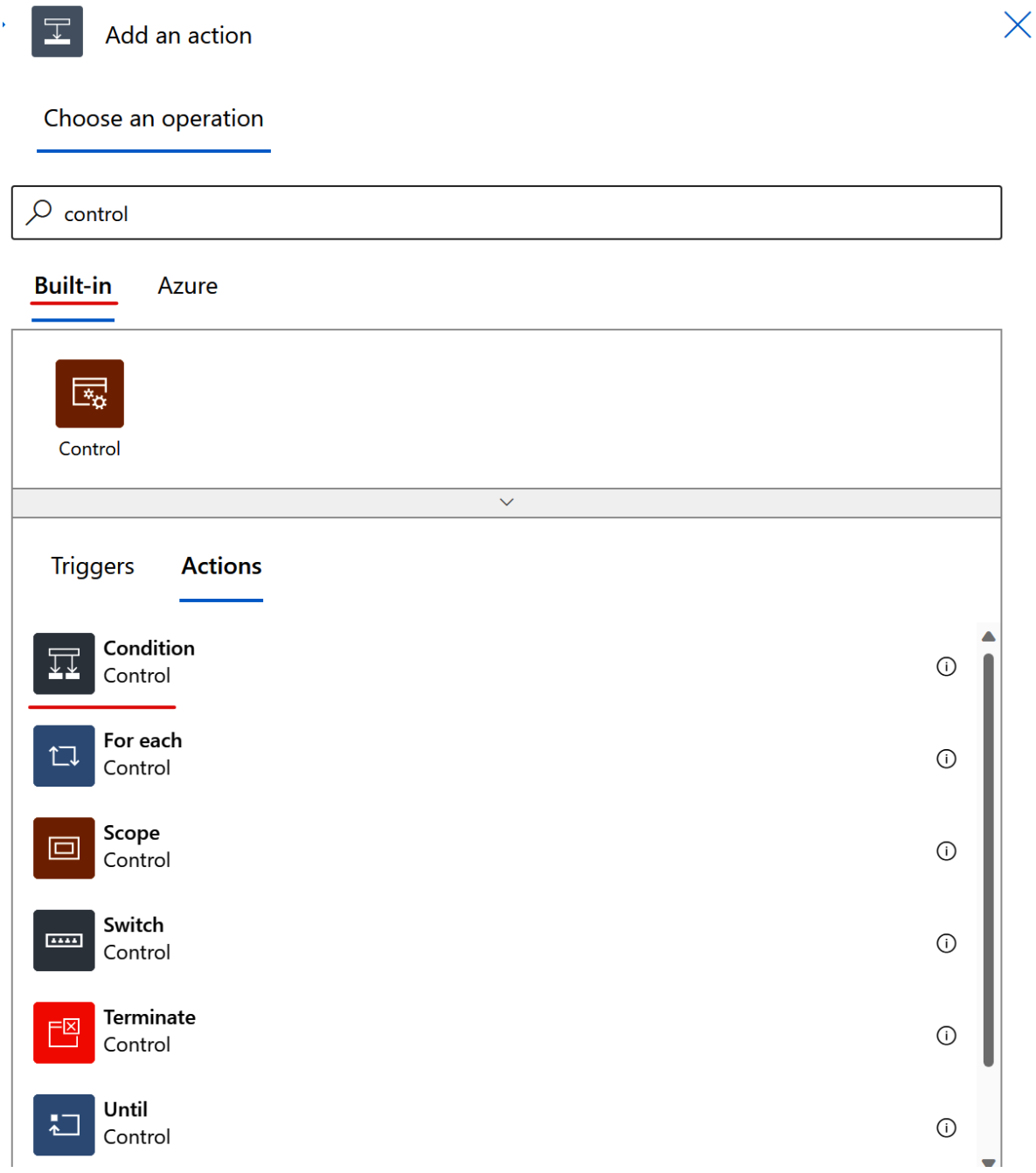

Run query and list results
Create Connection
*Connection name
SOAR-LAReader
Client ID
Client Secret
Tenant
Create
Connect with sign in

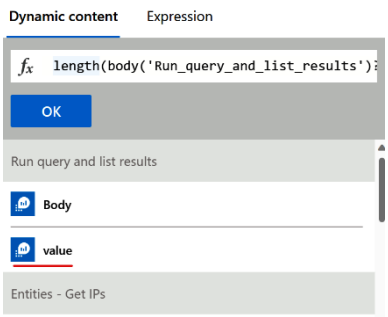

Home > Resource groups > SOAR
Resource groups
CybSec Guru (cybsec.guru)
Create
Manage view
Filter for any field...
Name
SOAR
Page 1 of 1
SOAR | Access control (IAM)
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Policies
Properties
Locks
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Advisor recommendations
Monitoring
Insights (preview)
Alerts
Metrics
Diagnostic settings
Add
Download role assignments
Edit columns
Refresh
Remove
Feedback
Add role assignment
Add co-administrator
Add custom role
Roles
Deny assignments
Classic administrators
View my access
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Check access
Grant access to this resource
Grant access to resources by assigning a role.
Learn more
Add role assignment
View access to this resource
View the role assignments that grant access to this and other resources.
Learn more
View
View deny assignments
View the role assignments that have been denied access to specific actions at this scope.
Learn more
View
Create a custom role
Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization.
Learn more
Add

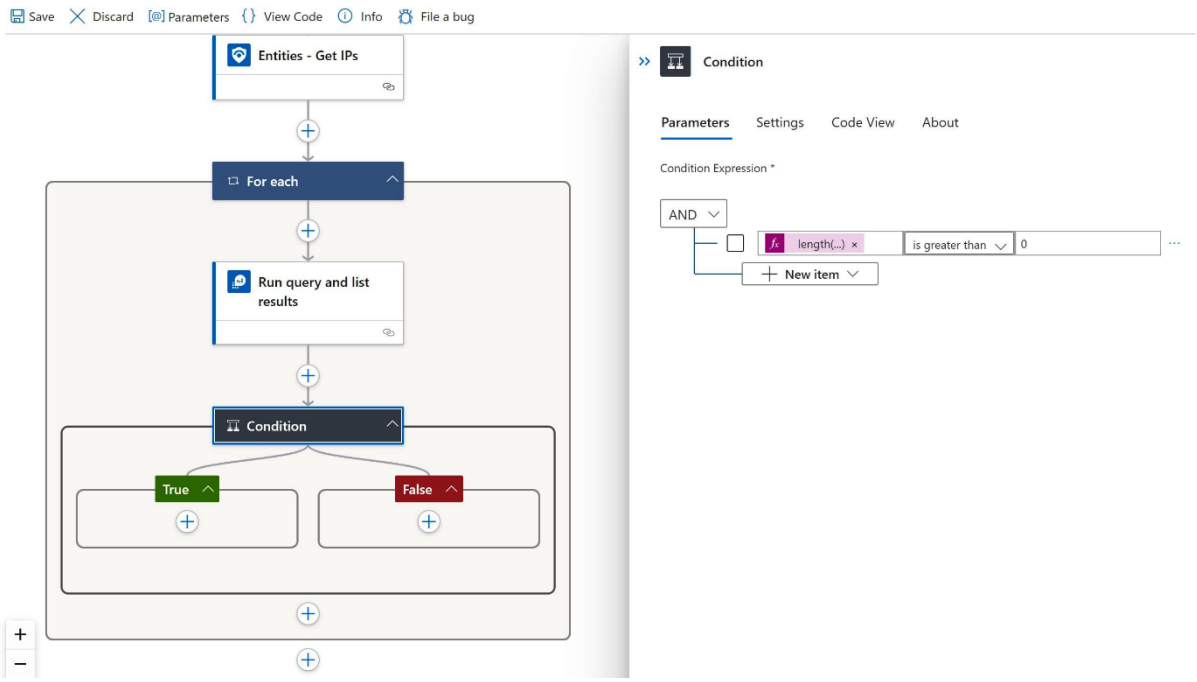

Home > Resource groups > SOAR | Access control (IAM) >
Add role assignment
Role
Members
Review + assign
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more
Assignment type
Job function roles
Privileged administrator roles
Grant access to Azure resources based on job function, such as the ability to create virtual machines.
log analytics reader
Type : All
Category : All
Name
Description
Type
Category
Details
Reader
View all resources, but does not allow you to make any changes.
BuiltInRole
General
View
Log Analytics Reader
Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the co...
BuiltInRole
Analytics
View
Managed Applications Reader
Lets you read resources in a managed app and request JIT access.
BuiltInRole
Management + Govern...
View
Monitoring Reader
Can read all monitoring data.
BuiltInRole
Monitor
View
< Previous
Page 1 of 1
Next >

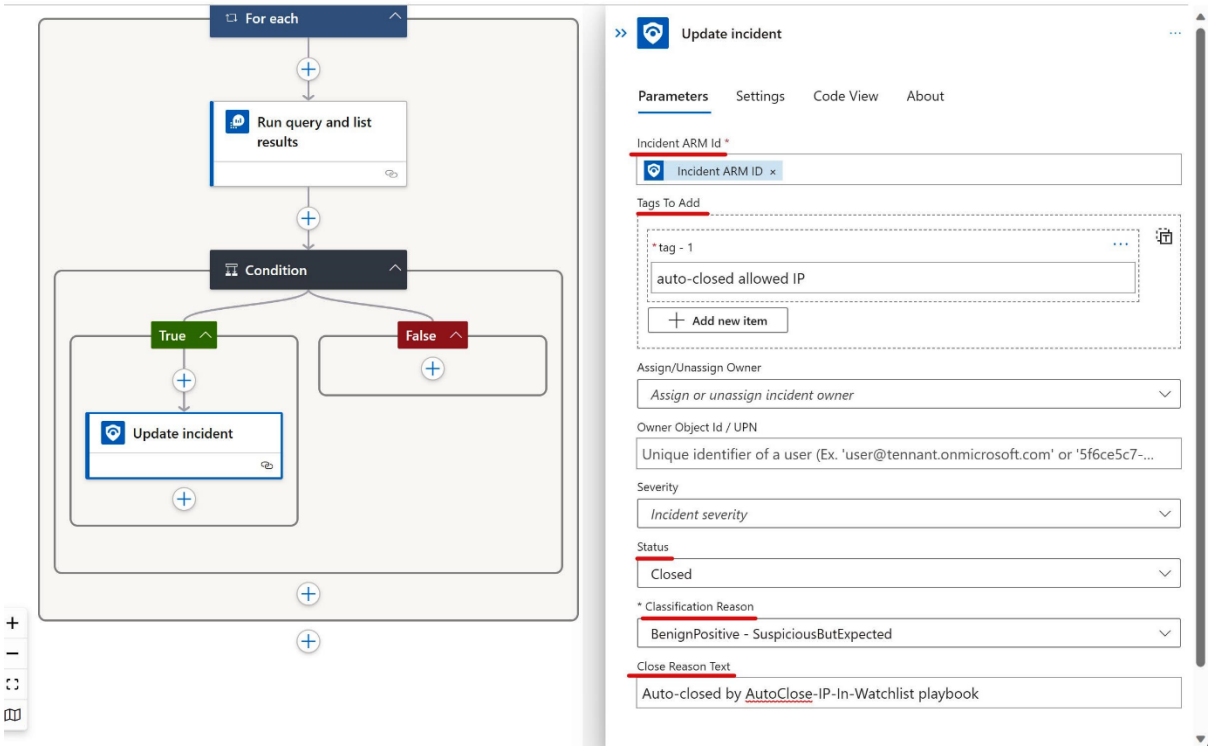

Home > Resource groups > SOAR | Access control (IAM) >
Add role assignment
Role
Members
Review + assign
Selected role
Log Analytics Reader
Assign access to
User, group, or service principal
Managed identity
Members
+ Select members
Name
Object ID
Type
No members selected
Description
Optional
Review + assign
Previous
Next
Select members
Select
SOAR-LAReader
No users, groups, or service principals found.
Selected members:
SOAR-LAReader
Remove
Select
Close

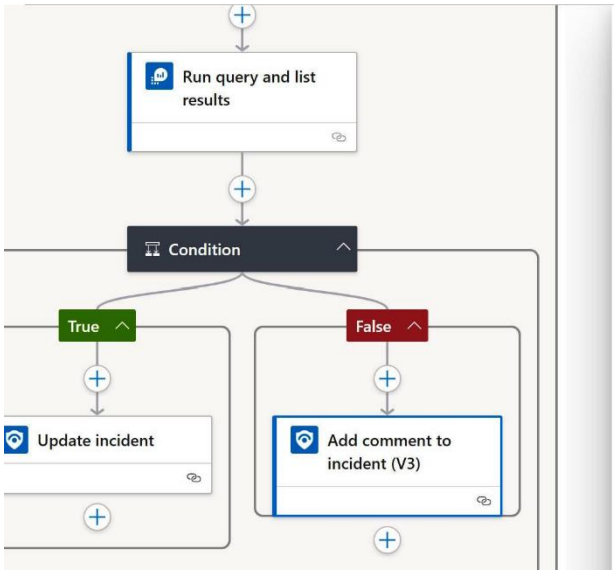

Save
Discard
Parameters
Info
Try Preview Designer
Microsoft Sentinel incident
Entities - Get IPs
For each
Run query and list results
Run query and list results
Parameters
Settings
Code View
Testing
*Subscription
VS FTE
*Resource Group
SOAR
*Resource Type
Log Analytics Workspace
*Resource Name
SOAR
*Query
_GetWatchlist('AllowedIP')
| where SearchKey == "
IPs Address
"
*Time Range
Last 24 hours
Connected to SOAR-LAReader.
Change connection.

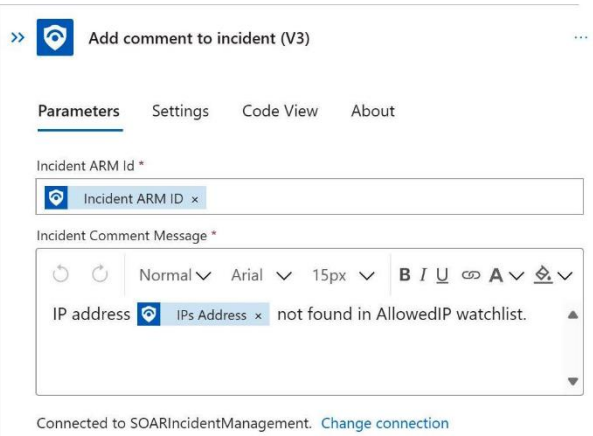

Add an action
Choose an operation
control
Built-in
Azure
Control
Triggers
Actions
Condition
Control
For each
Control
Scope
Control
Switch
Control
Terminate
Control
Until
Control

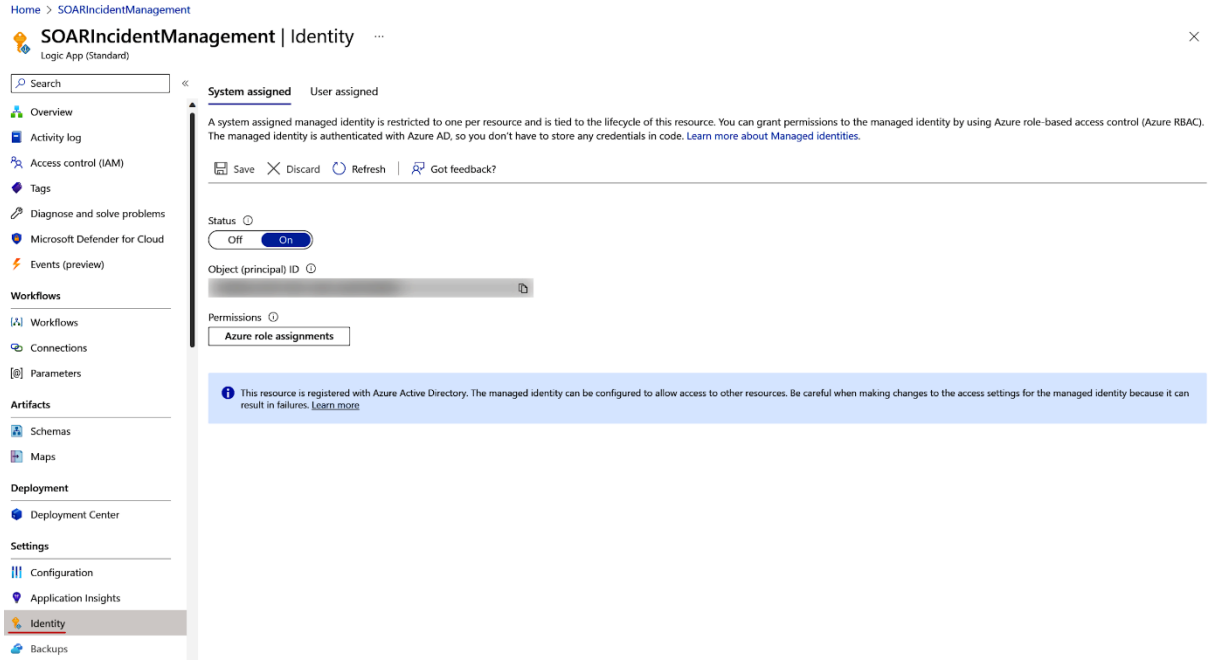

Dynamic content
Expression
length(body('Run_query_and_list_results'))
OK
Run query and list results
Body
value
Entities - Get IPs


Save
Discard
Parameters
View Code
Info
File a bug
Entities - Get IPs
For each
Run query and list results
Condition
True
False
Condition
Parameters
Settings
Code View
About
Condition Expression *
AND
length(...)
is greater than
0
New item


For each
Run query and list results
Condition
True
False
Update incident
Update incident
Parameters
Settings
Code View
About
Incident ARM Id *
Incident ARM ID
Tags To Add
*tag - 1
auto-closed allowed IP
Add new item
Assign/Unassign Owner
Assign or unassign incident owner
Owner Object Id / UPN
Unique identifier of a user (Ex. 'user@tennant.onmicrosoft.com' or '5f6ce5c7-...
Severity
Incident severity
Status
Closed
* Classification Reason
BenignPositive - SuspiciousButExpected
Close Reason Text
Auto-closed by AutoClose-IP-In-Watchlist playbook


Run query and list results
Condition
True
False
Update incident
Add comment to incident (V3)


Add comment to incident (V3)
Parameters
Settings
Code View
About
Incident ARM Id *
Incident ARM ID ×
Incident Comment Message *
Normal
Arial
15px
IP address
IPs Address ×
not found in AllowedIP watchlist.
Connected to SOARIncidentManagement. Change connection


Home > SOARIncidentManagement
SOARIncidentManagement | Identity
Logic App (Standard)
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Workflows
Workflows
Connections
Parameters
Artifacts
Schemas
Maps
Deployment
Deployment Center
Settings
Configuration
Application Insights
Identity
Backups
System assigned
User assigned
A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code. Learn more about Managed identities.
Save
Discard
Refresh
Got feedback?
Status
Off
On
Object (principal) ID
Permissions
Azure role assignments
This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more

Run playbook on incident

Incident: Test - Malicious IP, ID: 5

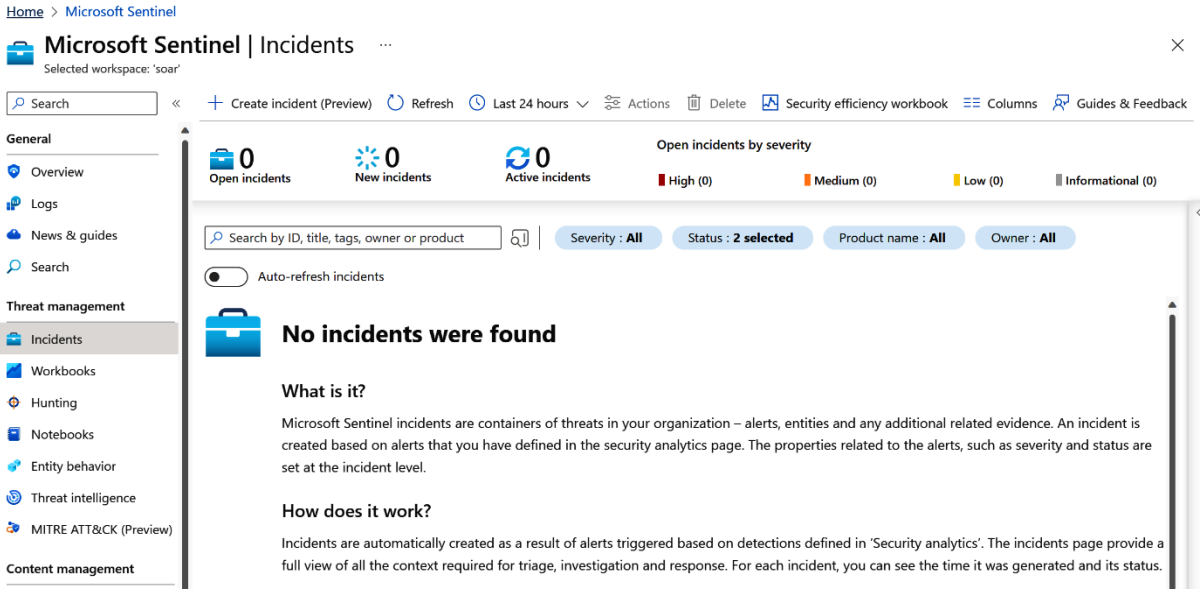
Refresh

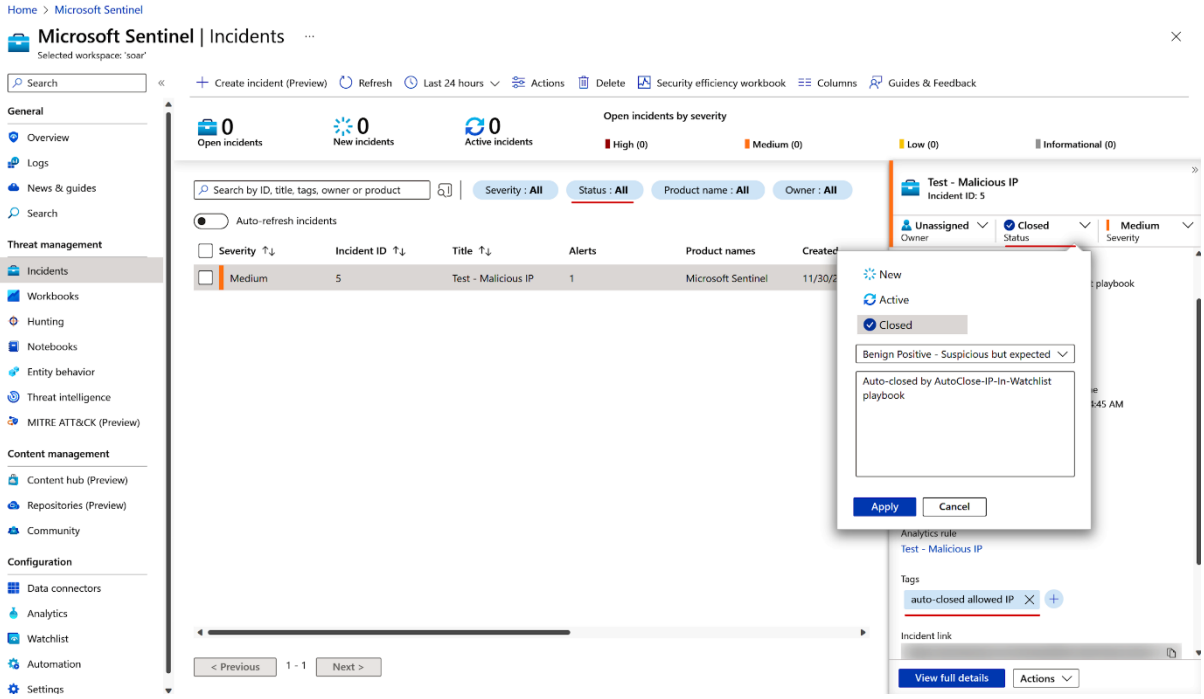
Playbooks Runs

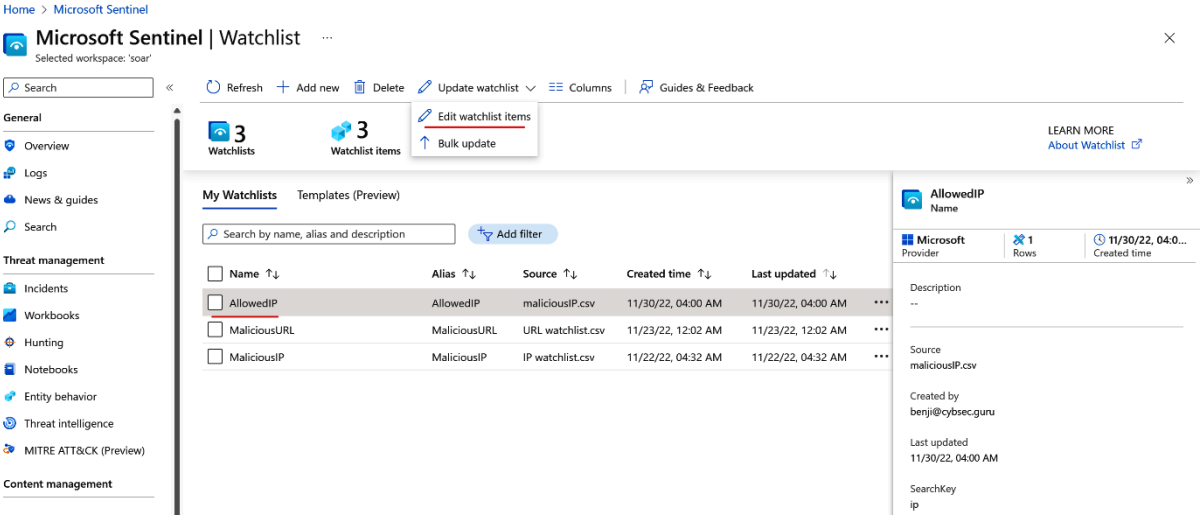
Select a playbook to run now on the incident. Only enabled playbooks configured with the Microsoft Sentinel incident trigger can be triggered.

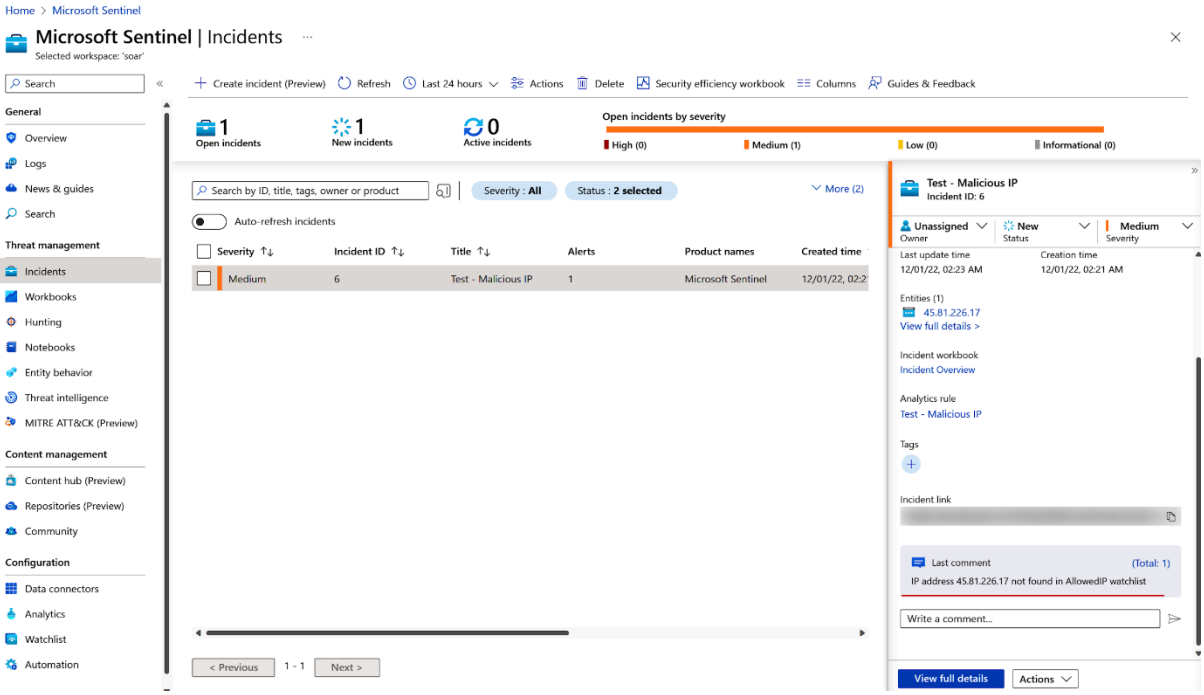
Search | Subscription : **VS FTE** | Resource group : **SOAR** | Plan : **All**

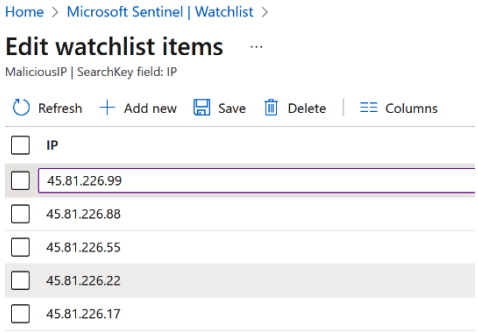
Name	Subscripti...	Resource gr...	Plan	
VirusTotal-URLEnrichment-incidentTrigger	VS FTE	SOAR	Consumption	Run
SOARIncidentManagement/AutoClose-I...	VS FTE	SOAR	Standard	Run

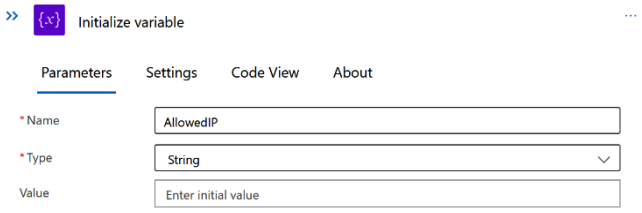


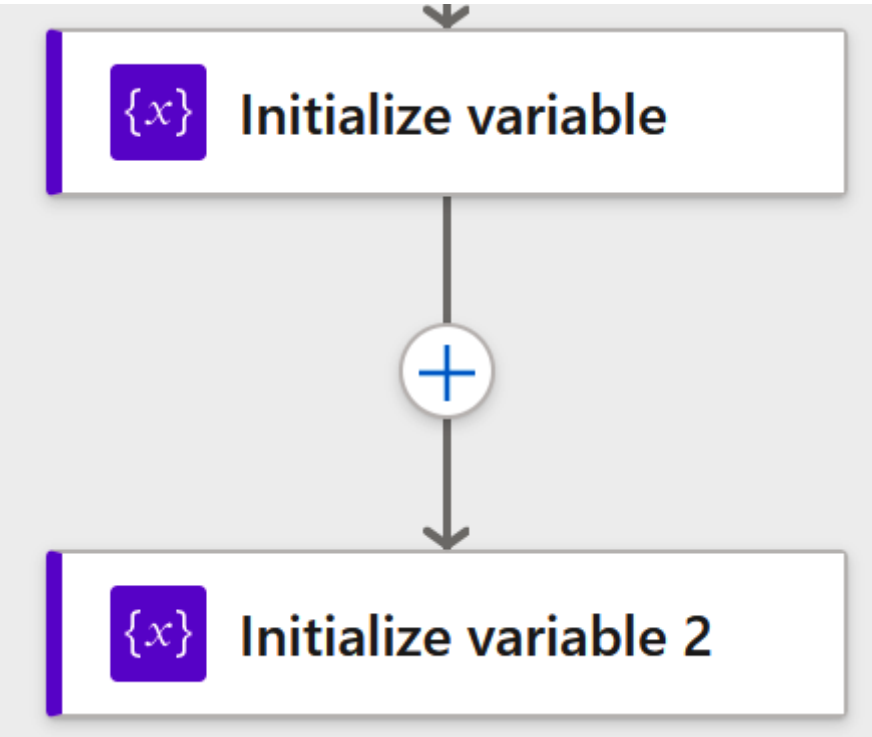

Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
0 Open incidents
0 New incidents
0 Active incidents
Open incidents by severity
High (0)
Medium (0)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : All
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created
Medium
5
Test - Malicious IP
1
Microsoft Sentinel
11/30/2
< Previous
1 - 1
Next >
Test - Malicious IP
Incident ID: 5
Unassigned
Owner
Closed
Status
Medium
Severity
New
Active
Closed
Benign Positive - Suspicious but expected
Auto-closed by AutoClose-IP-In-Watchlist playbook
Apply
Cancel
Analytics rule
Test - Malicious IP
Tags
auto-closed allowed IP
Incident link
View full details
Actions

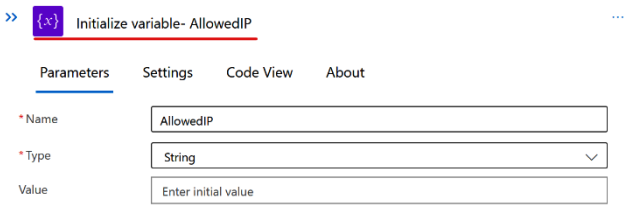

Home > Microsoft Sentinel
Microsoft Sentinel | Watchlist
Selected workspace: 'soar'
Search
Refresh
Add new
Delete
Update watchlist
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
3 Watchlists
3 Watchlist items
Edit watchlist items
Bulk update
LEARN MORE
About Watchlist
My Watchlists
Templates (Preview)
Search by name, alias and description
Add filter
Name
Alias
Source
Created time
Last updated
AllowedIP
AllowedIP
maliciousIP.csv
11/30/22, 04:00 AM
11/30/22, 04:00 AM
MaliciousURL
MaliciousURL
URL watchlist.csv
11/23/22, 12:02 AM
11/23/22, 12:02 AM
MaliciousIP
MaliciousIP
IP watchlist.csv
11/22/22, 04:32 AM
11/22/22, 04:32 AM
AllowedIP
Name
Microsoft
Provider
1
Rows
11/30/22, 04:0...
Created time
Description
--
Source
maliciousIP.csv
Created by
benji@cybsec.guru
Last updated
11/30/22, 04:00 AM
SearchKey
ip

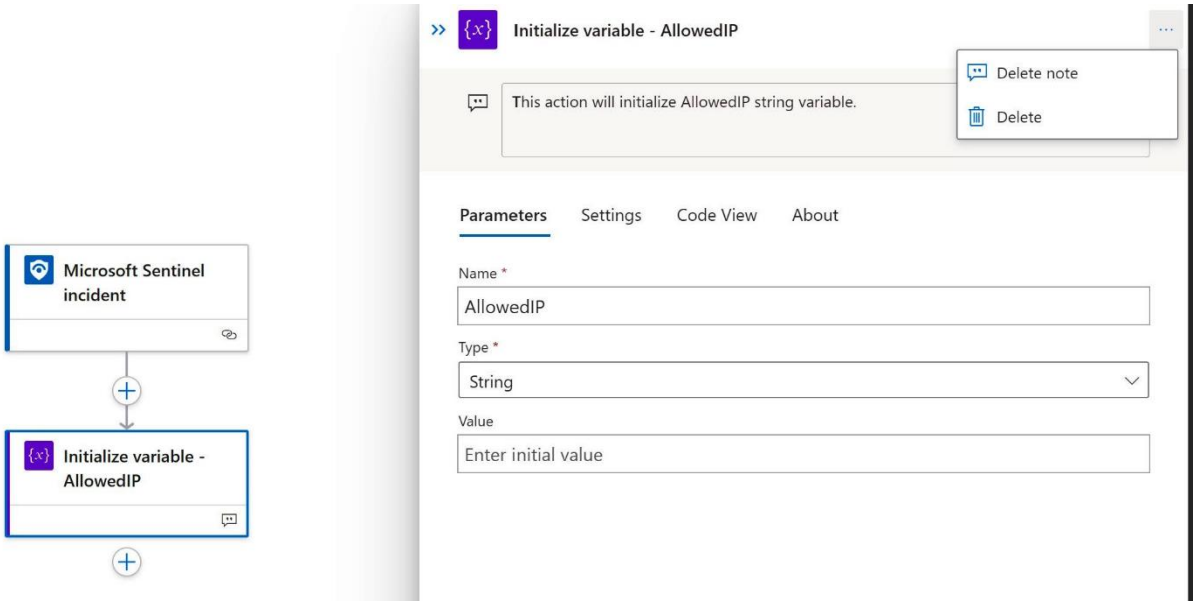

Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
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 : 2 selected
More (2)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
6
Test - Malicious IP
1
Microsoft Sentinel
12/01/22, 02:2
< Previous
1 - 1
Next >
Test - Malicious IP
Incident ID: 6
Unassigned
Owner
New
Status
Medium
Severity
Last update time
12/01/22, 02:23 AM
Creation time
12/01/22, 02:21 AM
Entities (1)
45.81.226.17
View full details >
Incident workbook
Incident Overview
Analytics rule
Test - Malicious IP
Tags
Incident link
Last comment
(Total: 1)
IP address 45.81.226.17 not found in AllowedIP watchlist
Write a comment...
View full details
Actions


Home > Microsoft Sentinel | Watchlist >
Edit watchlist items
MaliciousIP | SearchKey field: IP
Refresh
Add new
Save
Delete
Columns
IP
45.81.226.99
45.81.226.88
45.81.226.55
45.81.226.22
45.81.226.17


Initialize variable
Parameters
Settings
Code View
About
*Name
AllowedIP
*Type
String
Value
Enter initial value


Initialize variable
Initialize variable 2


Initialize variable- AllowedIP
Parameters
Settings
Code View
About
* Name
AllowedIP
* Type
String
Value
Enter initial value


Microsoft Sentinel incident
Initialize variable - AllowedIP
Initialize variable - AllowedIP
Delete note
Delete
This action will initialize AllowedIP string variable.
Parameters
Settings
Code View
About
Name *
AllowedIP
Type *
String
Value
Enter initial value

Condition

Parameters Settings Run After About

And

length(...) ×

is greater than

0

Add

Append to string variable - AllowedIP

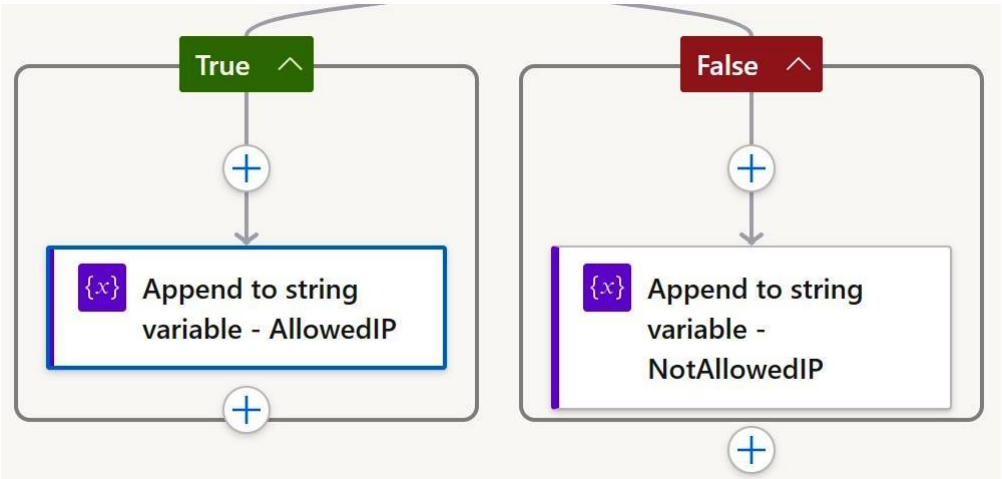
Parameters Settings Code View About

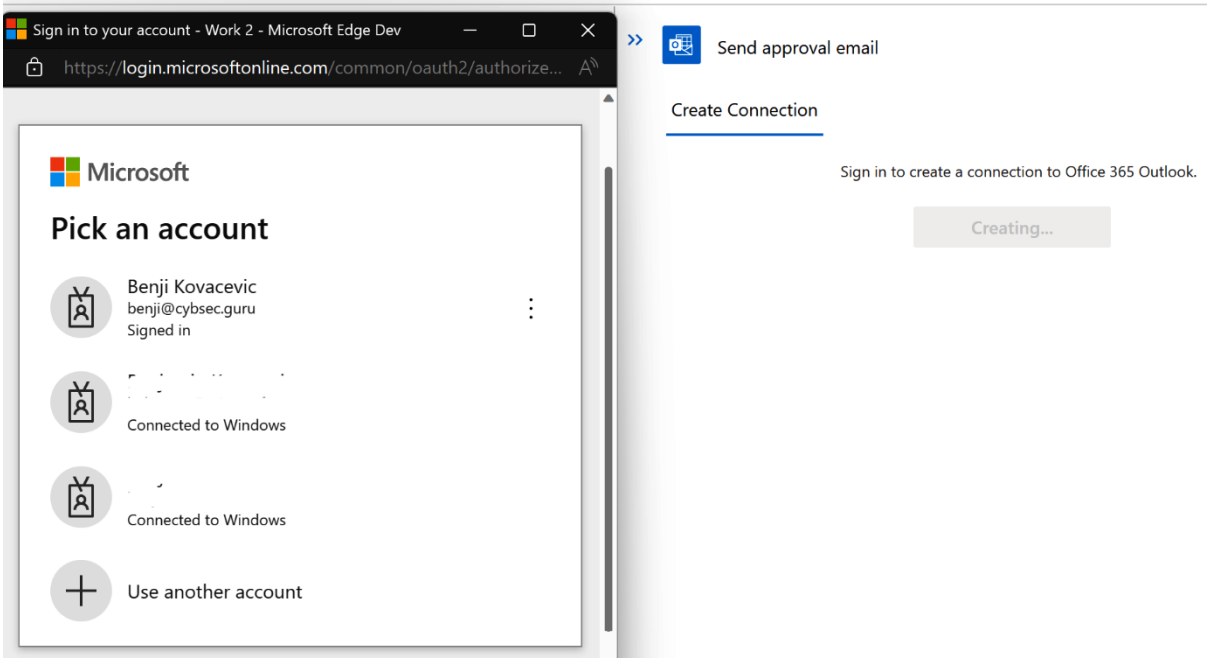
Name *

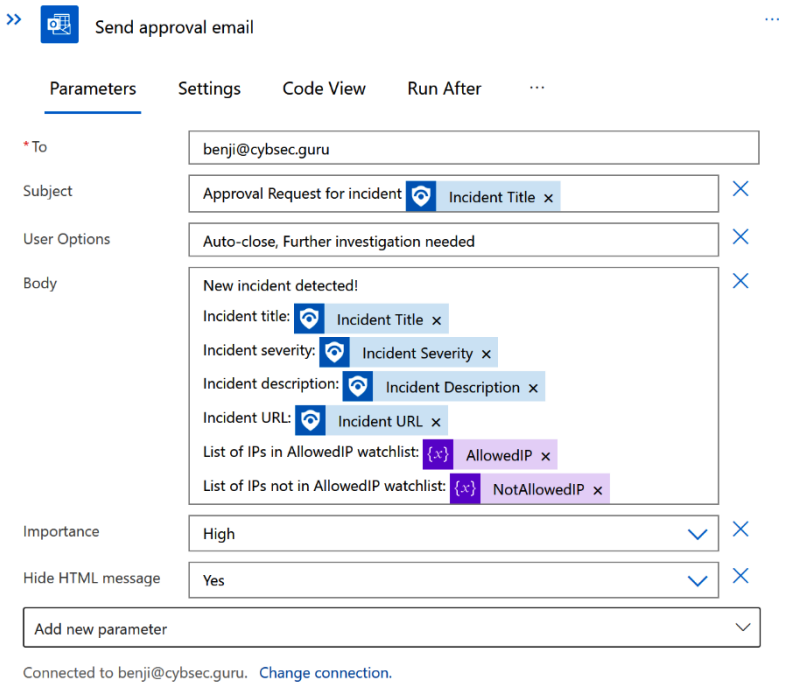
AllowedIP

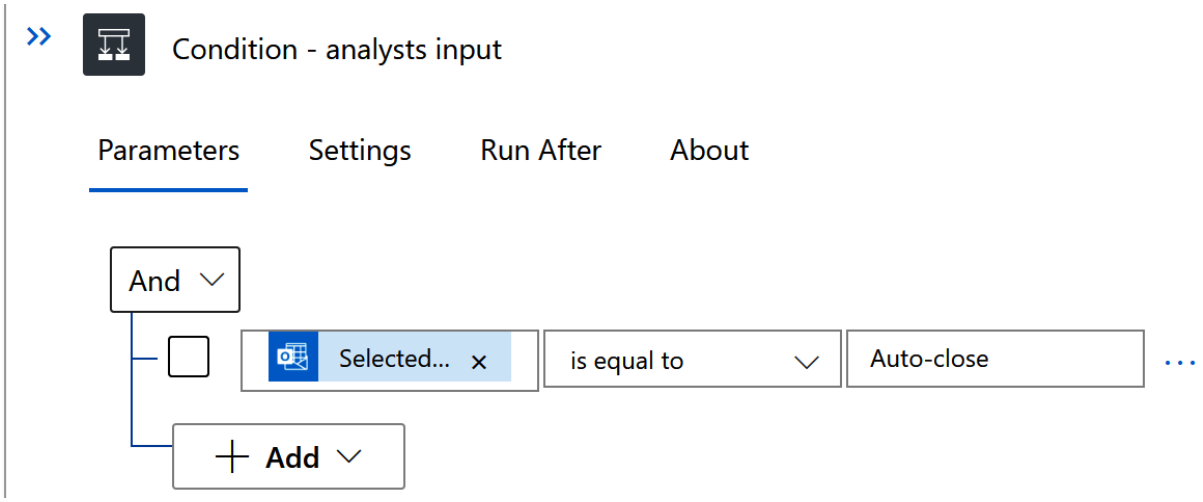
Value *

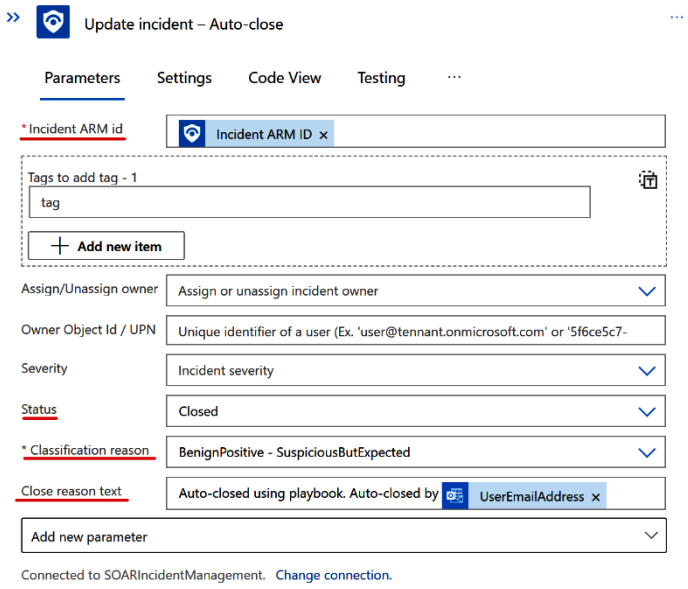
IPs Address ×

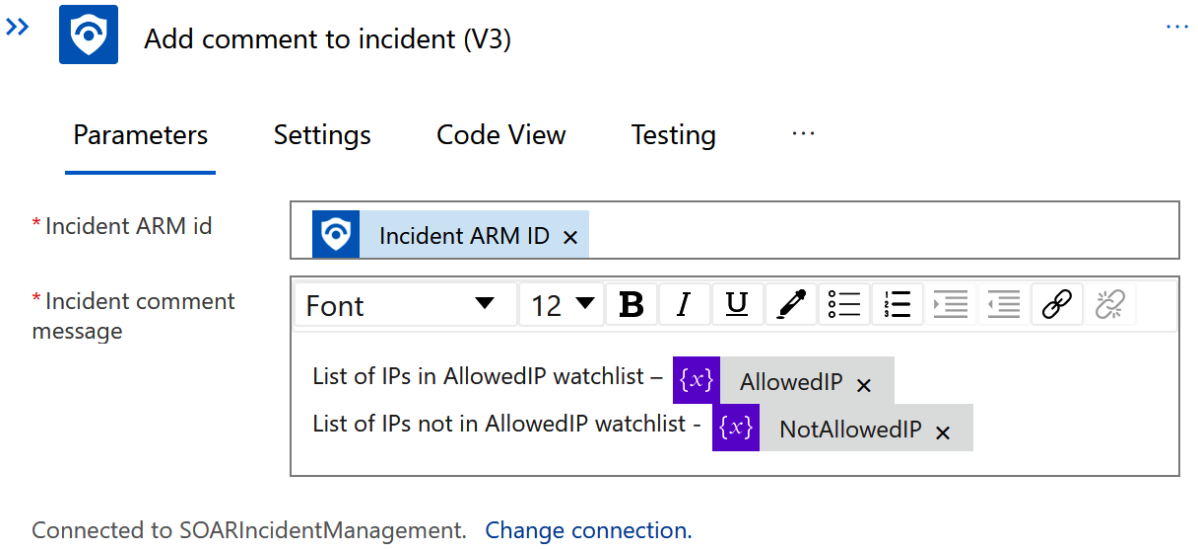


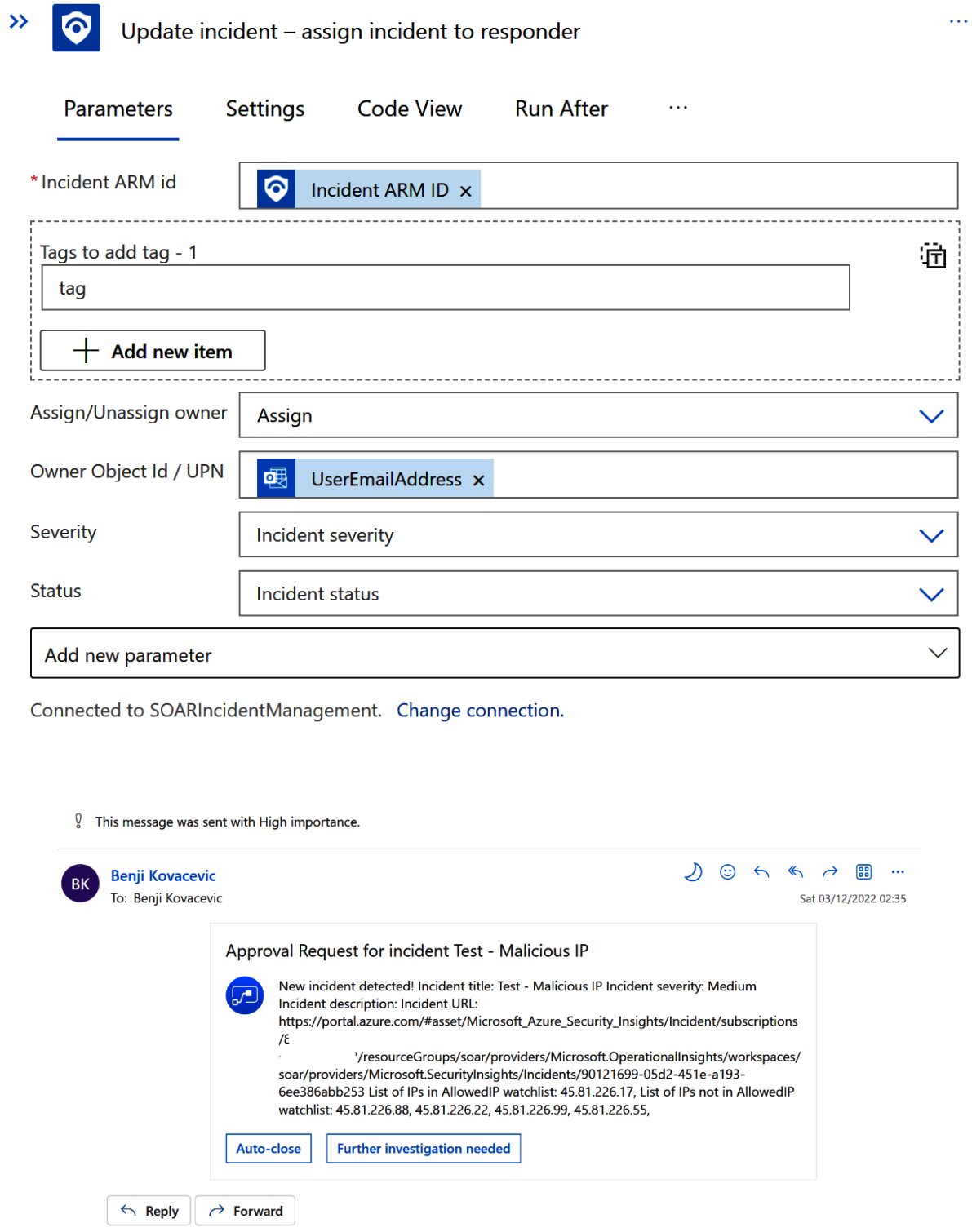

Sign in to your account - Work 2 - Microsoft Edge Dev
https://login.microsoftonline.com/common/oauth2/authorize...
Microsoft
Pick an account
Benji Kovacevic
benji@cybsec.guru
Signed in
Connected to Windows
Connected to Windows
Use another account
Send approval email
Create Connection
Sign in to create a connection to Office 365 Outlook.
Creating...

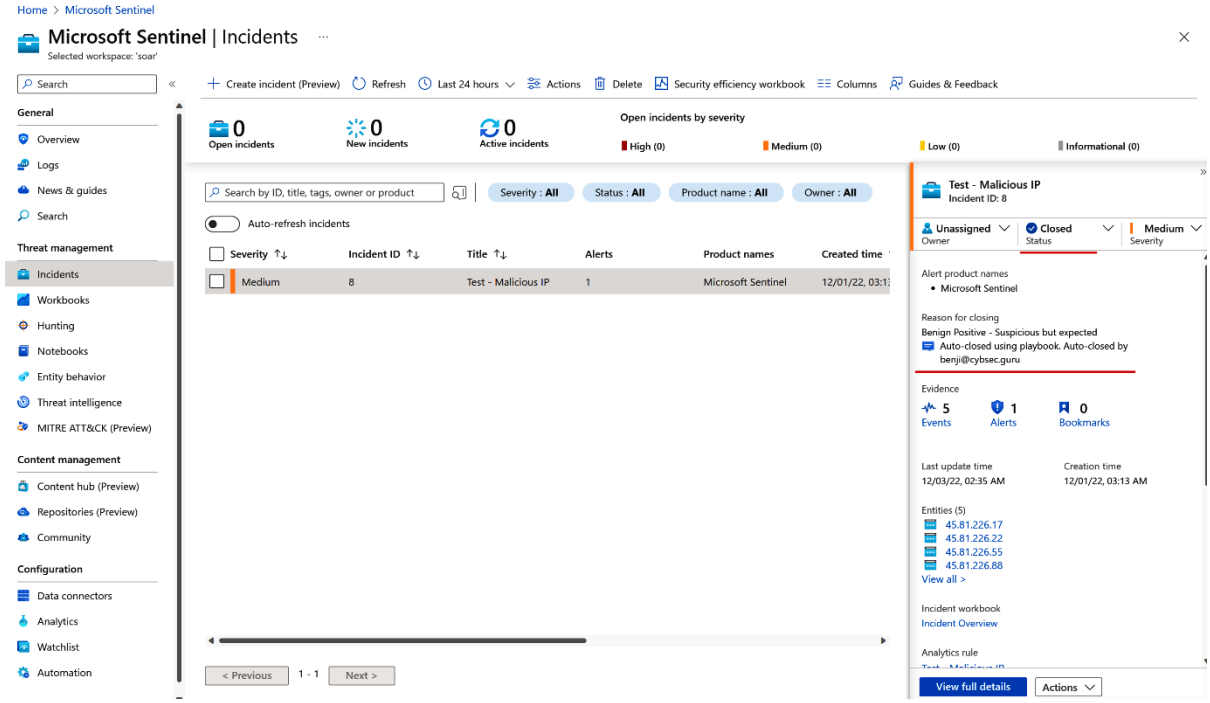

Send approval email
Parameters
Settings
Code View
Run After
*To
benji@cybsec.guru
Subject
Approval Request for incident
Incident Title
User Options
Auto-close, Further investigation needed
Body
New incident detected!
Incident title:
Incident Title
Incident severity:
Incident Severity
Incident description:
Incident Description
Incident URL:
Incident URL
List of IPs in AllowedIP watchlist:
AllowedIP
List of IPs not in AllowedIP watchlist:
NotAllowedIP
Importance
High
Hide HTML message
Yes
Add new parameter
Connected to benji@cybsec.guru.
Change connection.

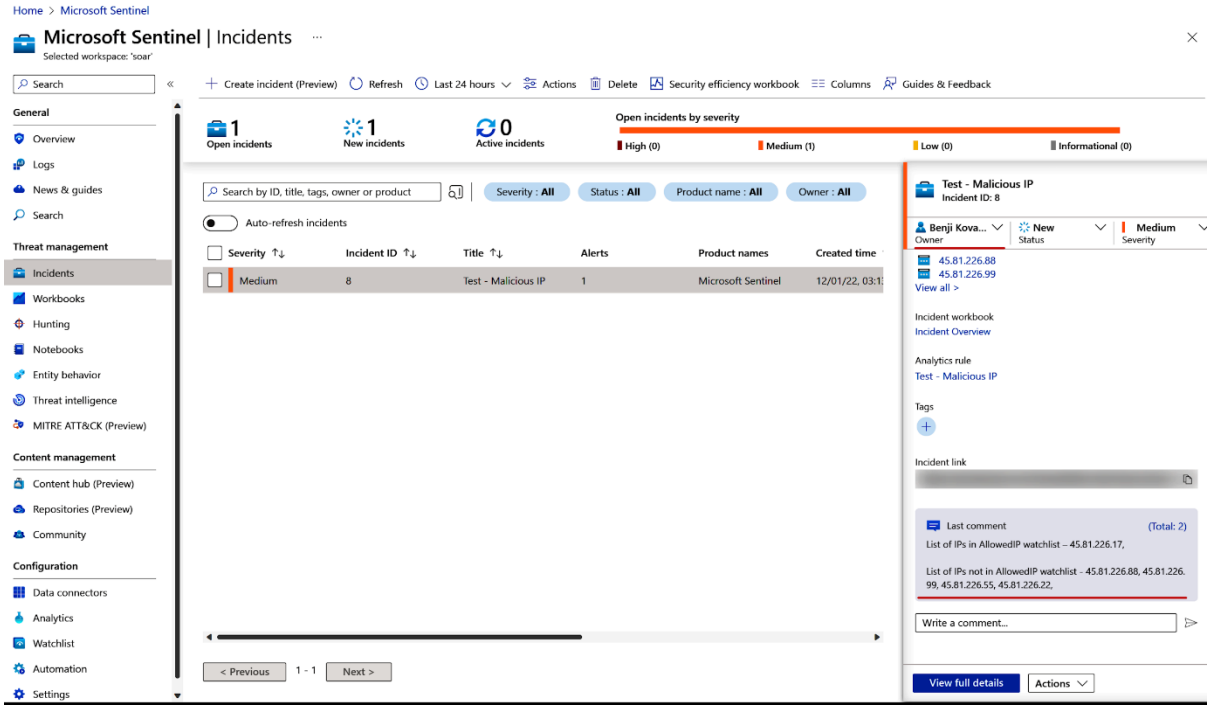

Condition - analysts input
Parameters
Settings
Run After
About
And
Selected... ×
is equal to
Auto-close
Add


Update incident – Auto-close
Parameters
Settings
Code View
Testing
* Incident ARM id
Incident ARM ID ×
Tags to add tag - 1
tag
Add new item
Assign/Unassign owner
Assign or unassign incident owner
Owner Object Id / UPN
Unique identifier of a user (Ex. 'user@tennant.onmicrosoft.com' or '5f6ce5c7-
Severity
Incident severity
Status
Closed
* Classification reason
BenignPositive - SuspiciousButExpected
Close reason text
Auto-closed using playbook. Auto-closed by
UserEmailAddress ×
Add new parameter
Connected to SOARIncidentManagement. Change connection.


Add comment to incident (V3)
Parameters
Settings
Code View
Testing
* Incident ARM id
Incident ARM ID ×
* Incident comment message
Font
12
List of IPs in AllowedIP watchlist –
AllowedIP ×
List of IPs not in AllowedIP watchlist -
NotAllowedIP ×
Connected to SOARIncidentManagement. Change connection.


Update incident – assign incident to responder
Parameters
Settings
Code View
Run After
* Incident ARM id
Incident ARM ID
Tags to add tag - 1
tag
Add new item
Assign/Unassign owner
Assign
Owner Object Id / UPN
UserEmailAddress
Severity
Incident severity
Status
Incident status
Add new parameter
Connected to SOARIncidentManagement. Change connection.
This message was sent with High importance.
BK
Benji Kovacevic
To: Benji Kovacevic
Sat 03/12/2022 02:35
Approval Request for incident Test - Malicious IP
New incident detected! Incident title: Test - Malicious IP Incident severity: Medium Incident description: Incident URL: https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Incident/subscriptions/
'/resourceGroups/soar/providers/Microsoft.OperationalInsights/workspaces/soar/providers/Microsoft.SecurityInsights/Incidents/90121699-05d2-451e-a193-6ee386abb253 List of IPs in AllowedIP watchlist: 45.81.226.17, List of IPs not in AllowedIP watchlist: 45.81.226.88, 45.81.226.22, 45.81.226.99, 45.81.226.55,
Auto-close
Further investigation needed
Reply
Forward


Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
0 Open incidents
0 New incidents
0 Active incidents
Open incidents by severity
High (0)
Medium (0)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : All
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
8
Test - Malicious IP
1
Microsoft Sentinel
12/01/22, 03:1
< Previous
1 - 1
Next >
Test - Malicious IP
Incident ID: 8
Unassigned
Owner
Closed
Status
Medium
Severity
Alert product names
Microsoft Sentinel
Reason for closing
Benign Positive - Suspicious but expected
Auto-closed using playbook. Auto-closed by benji@cybsec.guru
Evidence
5 Events
1 Alerts
0 Bookmarks
Last update time
12/03/22, 02:35 AM
Creation time
12/01/22, 03:13 AM
Entities (5)
45.81.226.17
45.81.226.22
45.81.226.55
45.81.226.88
View all >
Incident workbook
Incident Overview
Analytics rule
View full details
Actions


Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
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 : All
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
8
Test - Malicious IP
1
Microsoft Sentinel
12/01/22, 03:1
< Previous
1 - 1
Next >
Test - Malicious IP
Incident ID: 8
Benji Kova...
Owner
New
Status
Medium
Severity
45.81.226.88
45.81.226.99
View all >
Incident workbook
Incident Overview
Analytics rule
Test - Malicious IP
Tags
Incident link
Last comment
(Total: 2)
List of IPs in AllowedIP watchlist – 45.81.226.17,
List of IPs not in AllowedIP watchlist - 45.81.226.88, 45.81.226.99, 45.81.226.55, 45.81.226.22,
Write a comment...
View full details
Actions


Conditions
If
Analytic rule name
Contains
Test - Malicious IP
AND
IP address
Contains
45.81.226.17
+ Add

Actions ⓘ

Change status

Closed

Benign Positive - Suspicious but expected

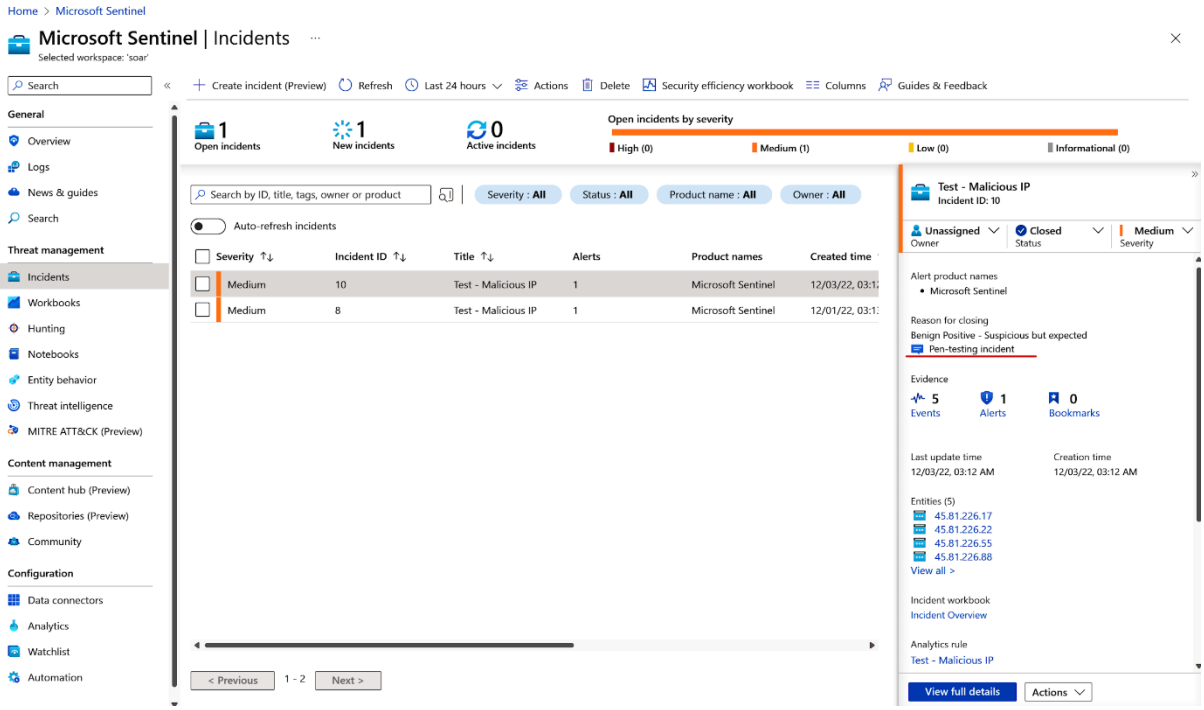
Pen-testing incident

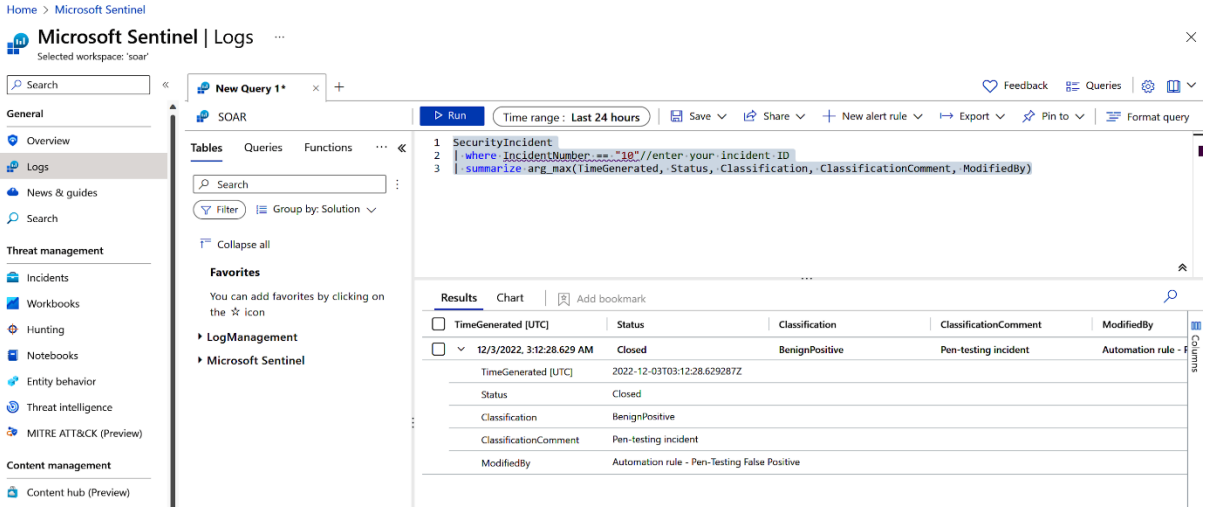
Rule expiration ⓘ

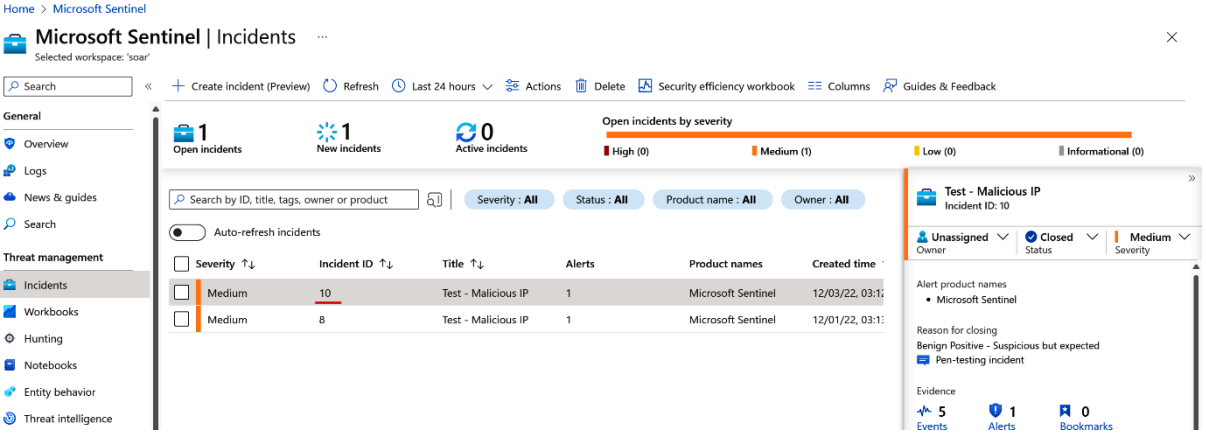
12/03/2022 | 3:15 AM

Order ⓘ

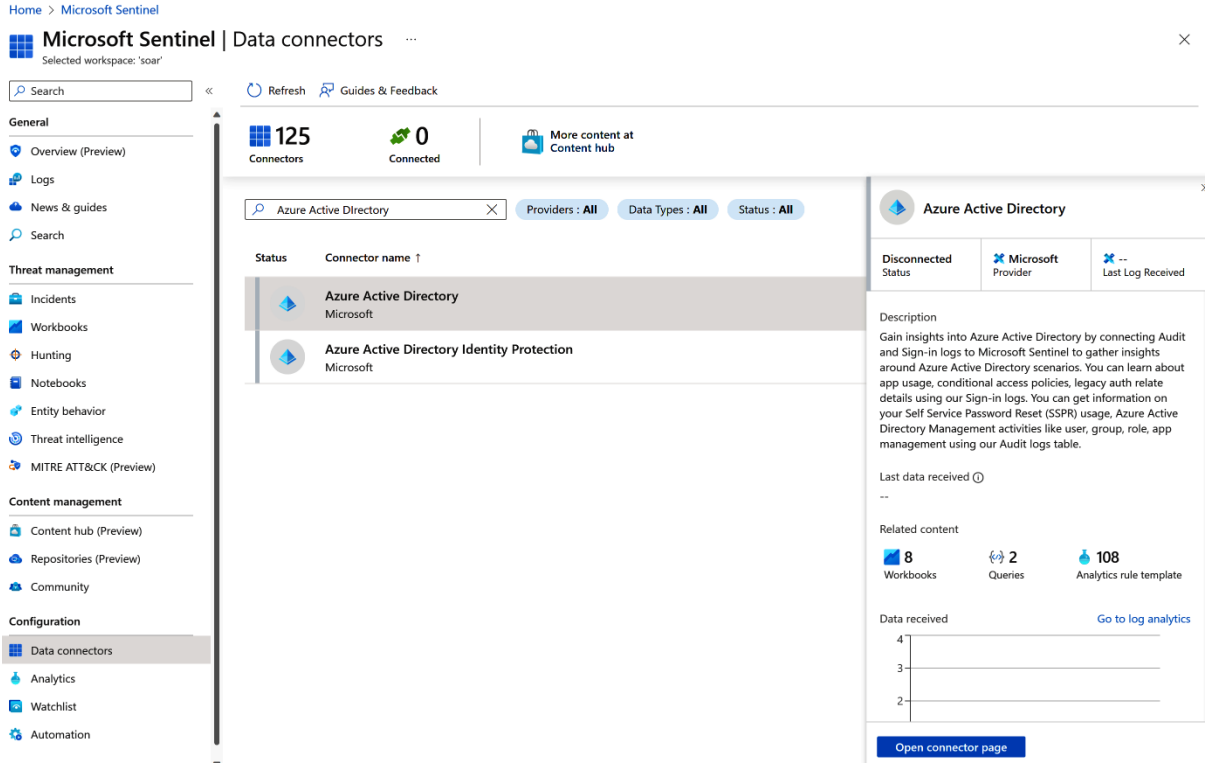
1

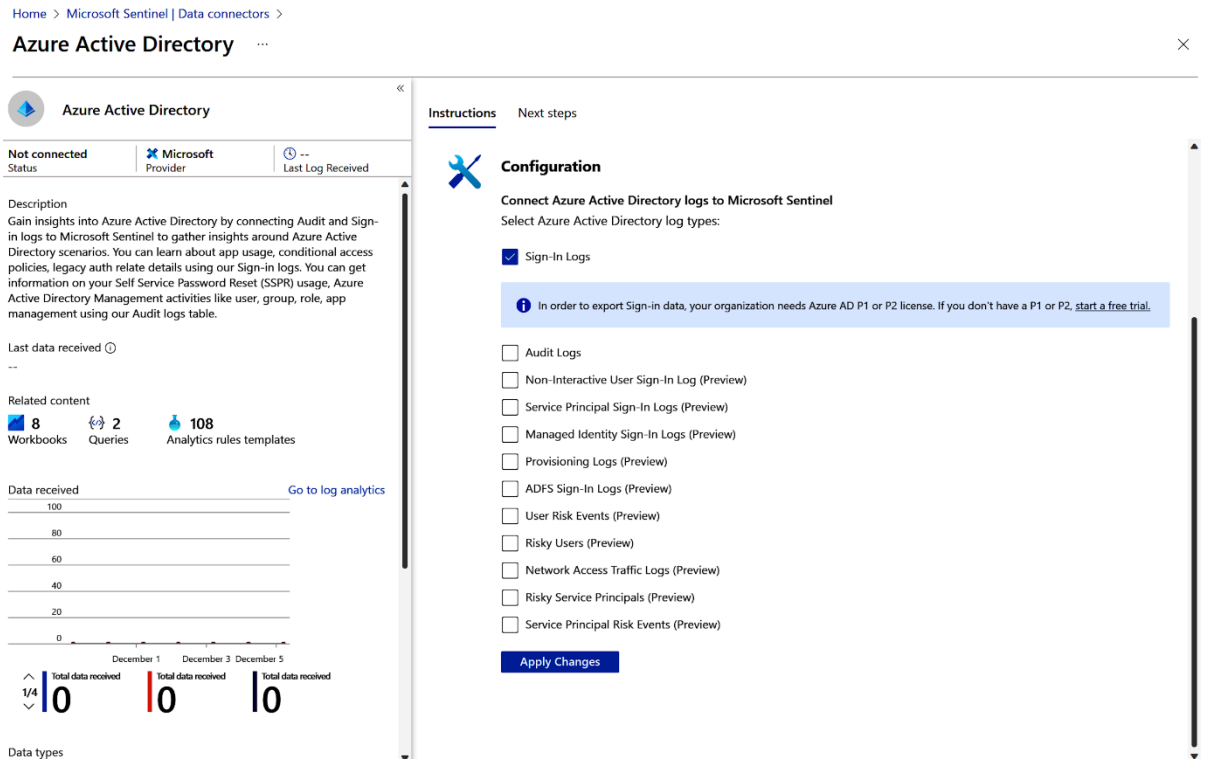


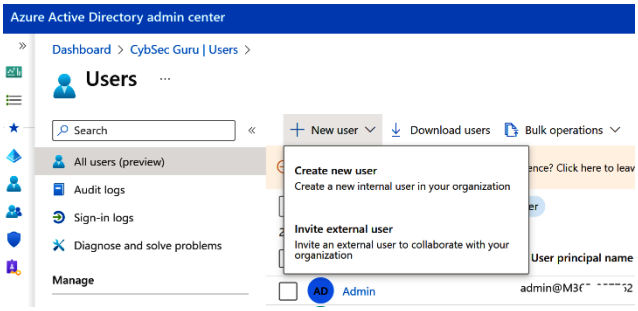

Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
New Query 1*
SOAR
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
Pin to
Format query
Feedback
Queries
Tables
Queries
Functions
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
LogManagement
Microsoft Sentinel
1 SecurityIncident
2 | where IncidentNumber == "10"//enter your incident ID
3 | summarize arg_max(TimeGenerated, Status, Classification, ClassificationComment, ModifiedBy)
Results
Chart
Add bookmark
TimeGenerated [UTC]
Status
Classification
ClassificationComment
ModifiedBy
12/3/2022, 3:12:28.629 AM
Closed
BenignPositive
Pen-testing incident
Automation rule -
TimeGenerated [UTC]
2022-12-03T03:12:28.6292877Z
Status
Closed
Classification
BenignPositive
ClassificationComment
Pen-testing incident
ModifiedBy
Automation rule - Pen-Testing False Positive
Columns


Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'soar'
Search
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
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 : All
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium
10
Test - Malicious IP
1
Microsoft Sentinel
12/03/22, 03:1
Medium
8
Test - Malicious IP
1
Microsoft Sentinel
12/01/22, 03:1
Test - Malicious IP
Incident ID: 10
Unassigned
Owner
Closed
Status
Medium
Severity
Alert product names
Microsoft Sentinel
Reason for closing
Benign Positive - Suspicious but expected
Pen-testing incident
Evidence
5
Events
1
Alerts
0
Bookmarks

Chapter 8: Responding to Incidents Using Automation







Dashboard > CybSec Guru | Users > Users >

New user

CybSec Guru

Got feedback?

Select template

- **Create user**
  Create a new user in your organization.
- **Invite user**
  Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they ca

Help me decide

Identity

User name * : SOARTest @ cybsec.guru

The domain name I need isn't shown here

Name * : SOAR Test user

First name :

Last name :

Password

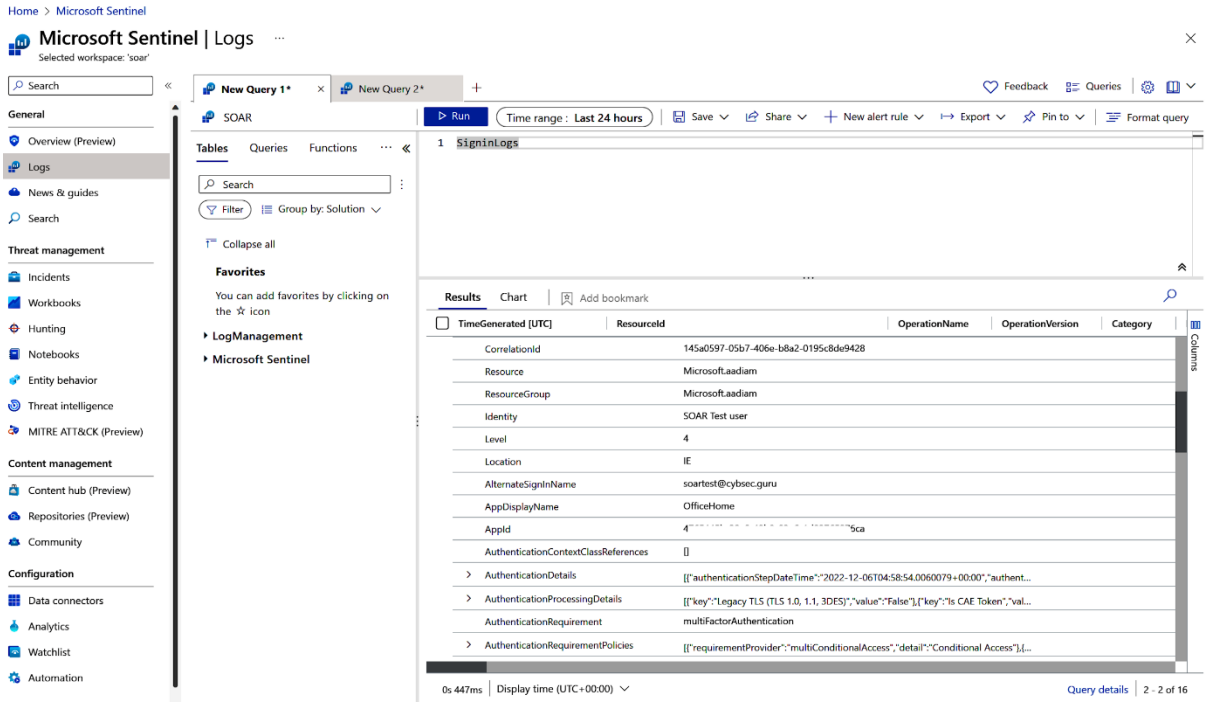
- Auto-generate password
- Let me create the password

Initial password * : ••••••••

Groups and roles

Groups: 0 groups selected

Create



Analytics rule wizard - Create a new scheduled 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.

```
_GetWatchlist('MaliciousIP')
| extend UsrAccount = "SOARTest"
| extend UPNSuffix = "cybsec.guru"
```

View query results >

Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results.
This enables Microsoft 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 old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. Learn more >

IP

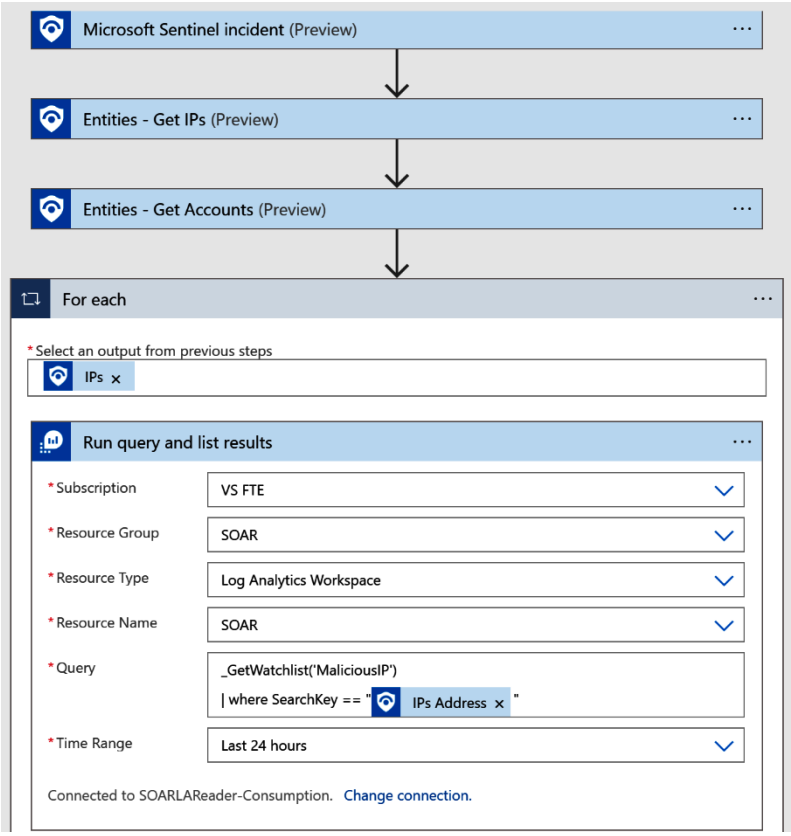
Address — SearchKey — + Add identifier

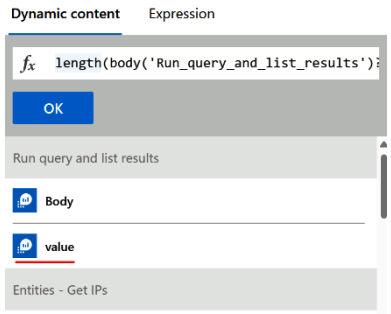
Account

Name — UsrAccount — + Add identifier

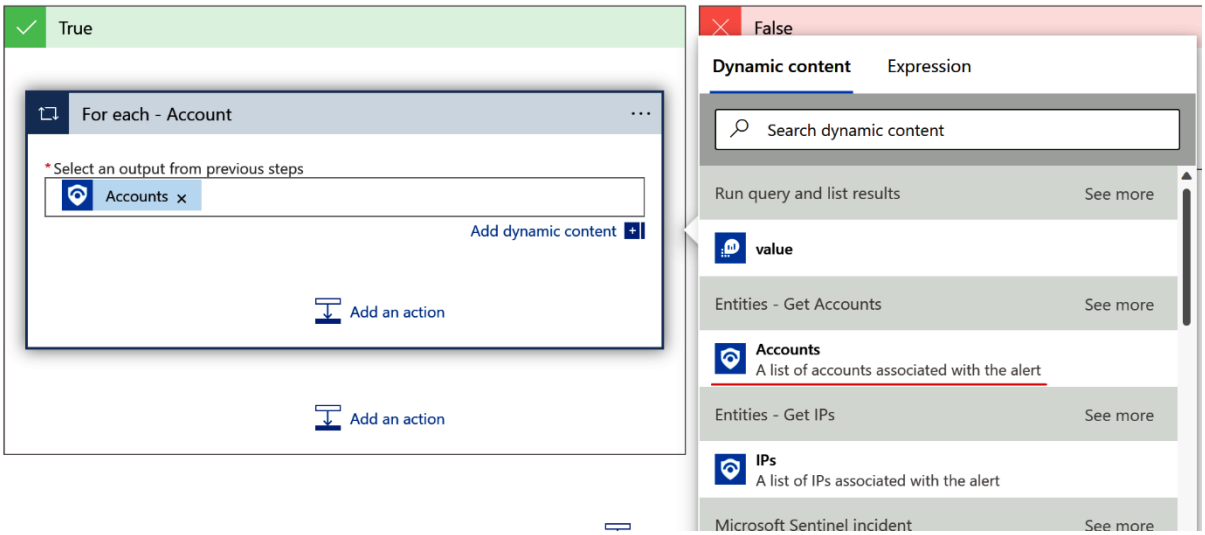
UPNSuffix — UPNSuffix

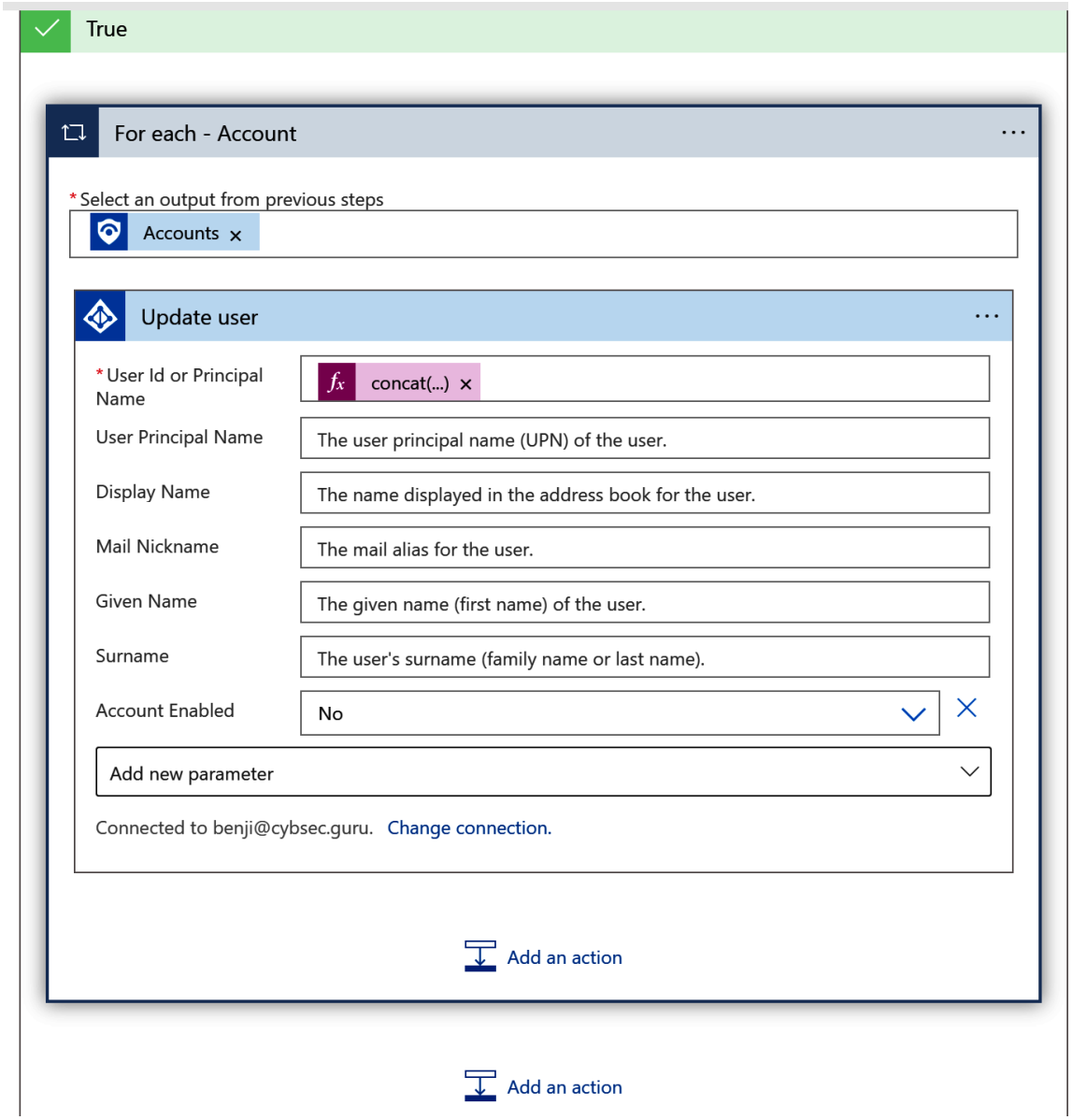
Previous | Next : Incident settings >

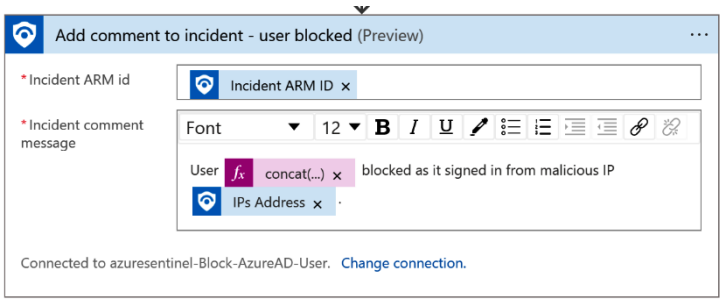

Microsoft Sentinel incident (Preview)
Entities - Get IPs (Preview)
Entities - Get Accounts (Preview)
For each
* Select an output from previous steps
IPs
Run query and list results
* Subscription
VS FTE
* Resource Group
SOAR
* Resource Type
Log Analytics Workspace
* Resource Name
SOAR
* Query
_GetWatchlist('MaliciousIP')
| where SearchKey == "
IPs Address
"
* Time Range
Last 24 hours
Connected to SOARLAReader-Consumption.
Change connection.

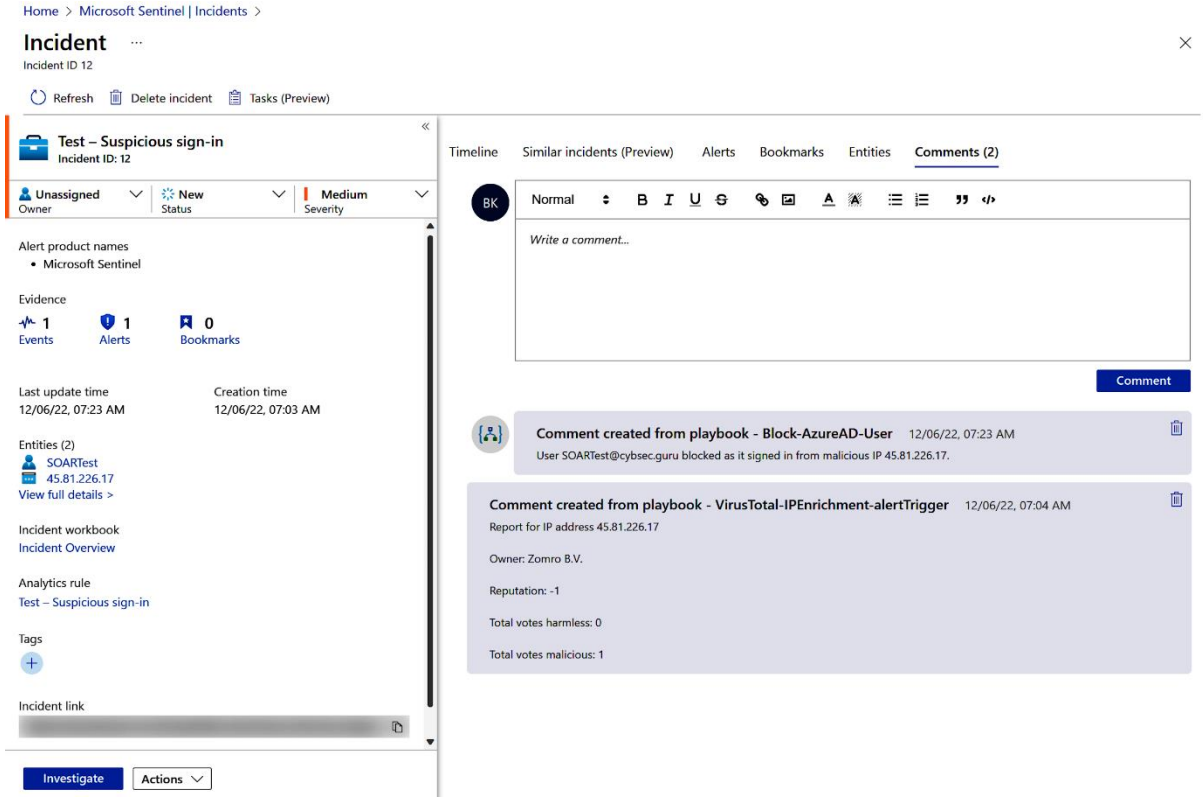

Dynamic content
Expression
length(body('Run_query_and_list_results'))
OK
Run query and list results
Body
value
Entities - Get IPs

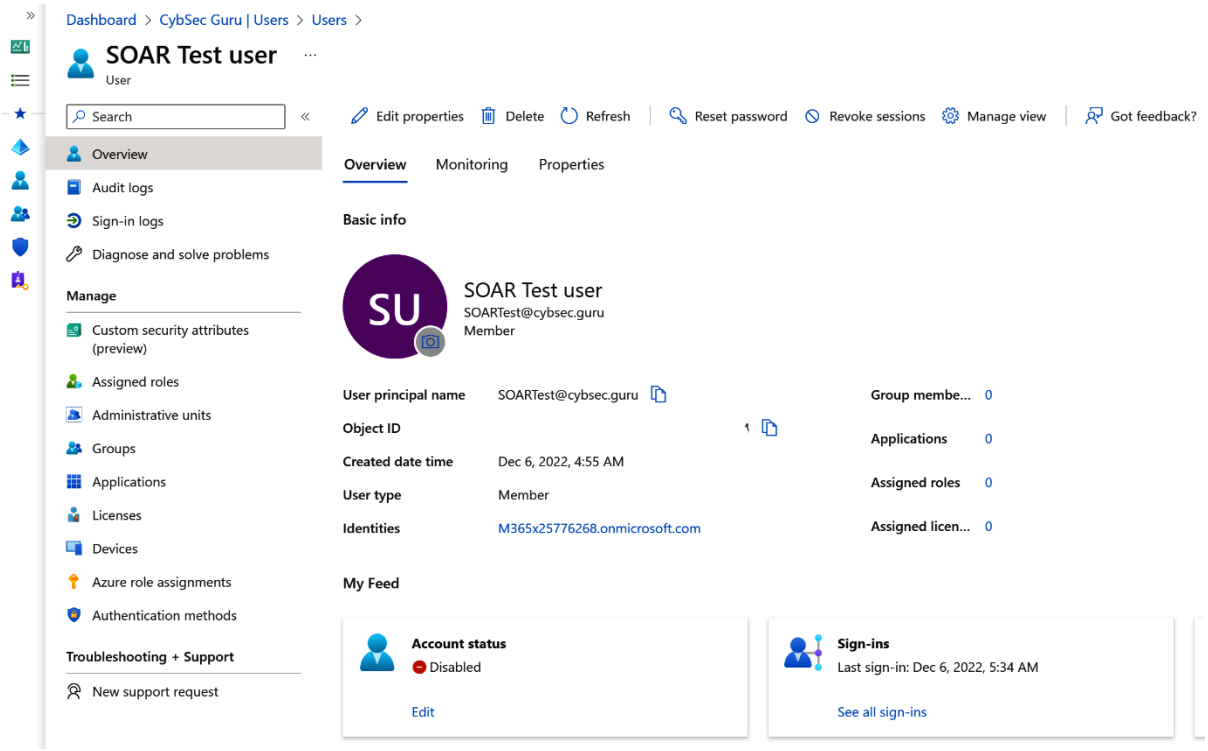

For each - Account
* Select an output from previous steps
Rename
Add a comment

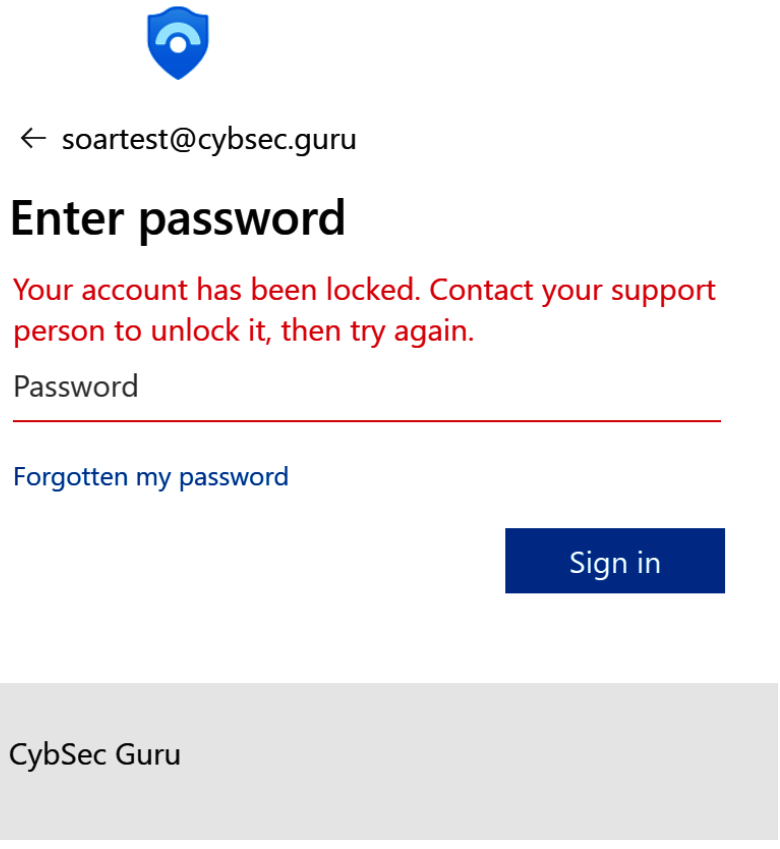

True
For each - Account
*Select an output from previous steps
Accounts
Add dynamic content
Add an action
Add an action
False
Dynamic content
Expression
Search dynamic content
Run query and list results
See more
value
Entities - Get Accounts
See more
Accounts
A list of accounts associated with the alert
Entities - Get IPs
See more
IPs
A list of IPs associated with the alert
Microsoft Sentinel incident
See more

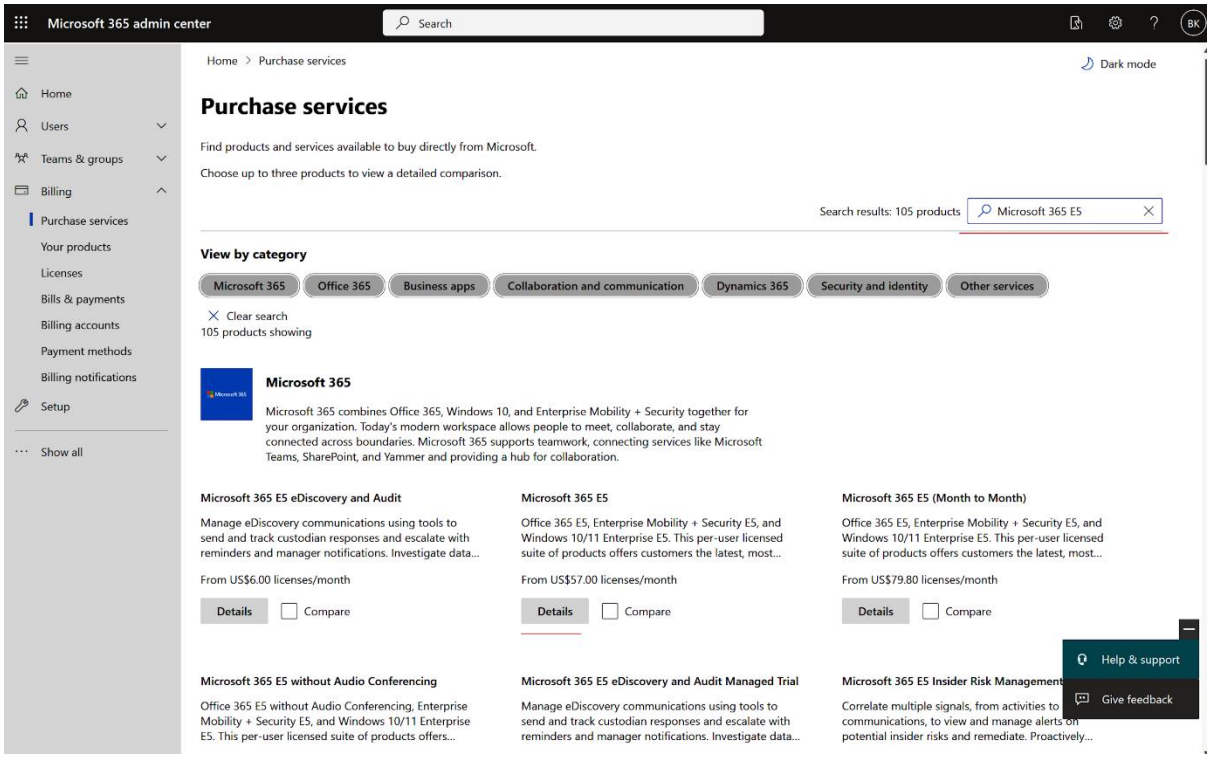

True
For each - Account
*Select an output from previous steps
Accounts
Update user
*User Id or Principal Name
concat(...)
User Principal Name
The user principal name (UPN) of the user.
Display Name
The name displayed in the address book for the user.
Mail Nickname
The mail alias for the user.
Given Name
The given name (first name) of the user.
Surname
The user's surname (family name or last name).
Account Enabled
No
Add new parameter
Connected to benji@cybsec.guru.
Change connection.
Add an action
Add an action

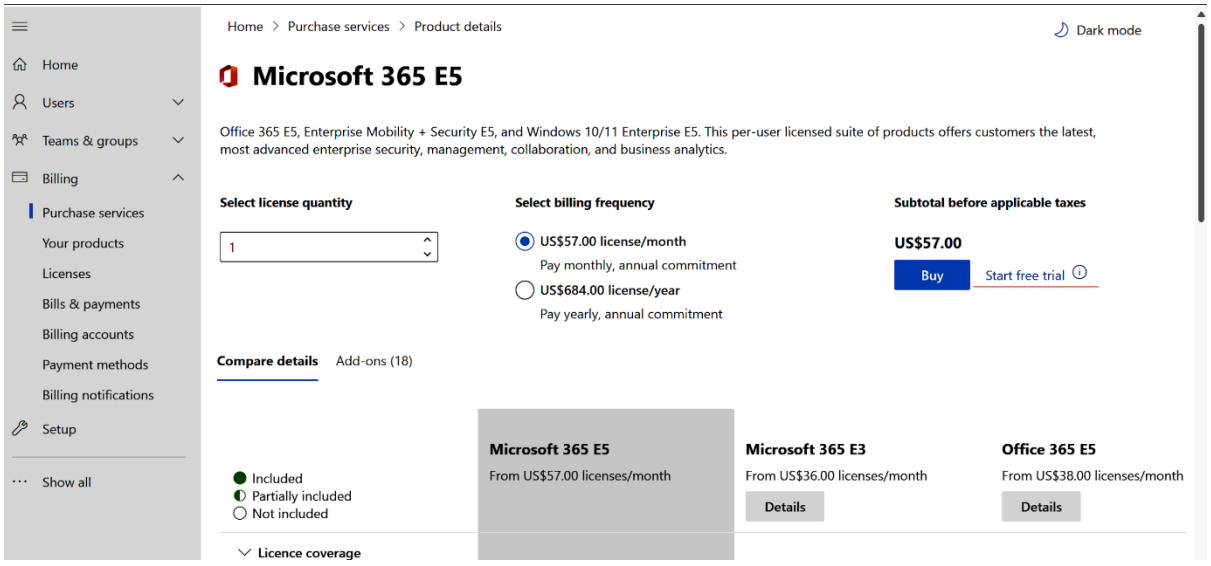

Add comment to incident - user blocked (Preview)
*Incident ARM id
Incident ARM ID
*Incident comment message
Font
12
User
concat(...)
blocked as it signed in from malicious IP
IPs Address
Connected to azuresentinel-Block-AzureAD-User.
Change connection.

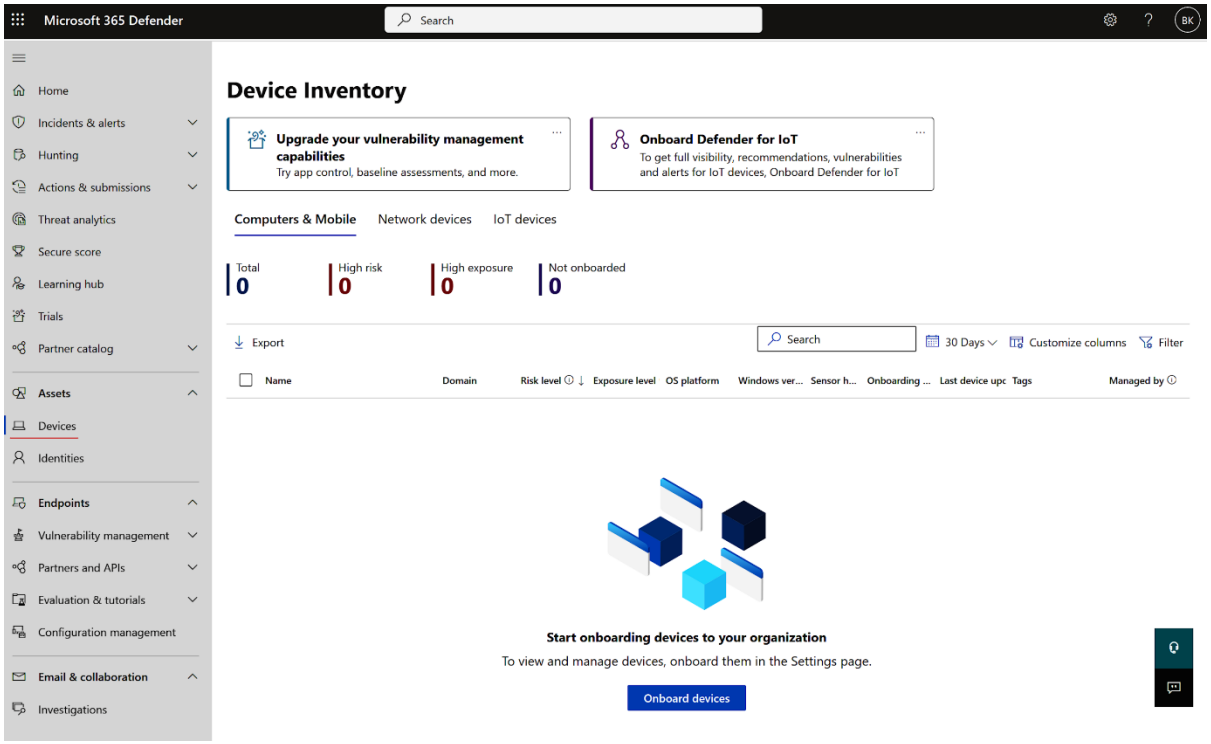

Home > Microsoft Sentinel | Incidents >
Incident
Incident ID 12
Refresh
Delete incident
Tasks (Preview)
Test – Suspicious sign-in
Incident ID: 12
Unassigned
Owner
New
Status
Medium
Severity
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
12/06/22, 07:23 AM
Creation time
12/06/22, 07:03 AM
Entities (2)
SOARTest
45.81.226.17
View full details >
Incident workbook
Incident Overview
Analytics rule
Test – Suspicious sign-in
Tags
Incident link
Investigate
Actions
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities
Comments (2)
BK
Normal
Write a comment...
Comment
Comment created from playbook - Block-AzureAD-User
12/06/22, 07:23 AM
User SOARTest@cybsec.guru blocked as it signed in from malicious IP 45.81.226.17.
Comment created from playbook - VirusTotal-IPEnrichment-alertTrigger
12/06/22, 07:04 AM
Report for IP address 45.81.226.17
Owner: Zomro B.V.
Reputation: -1
Total votes harmless: 0
Total votes malicious: 1

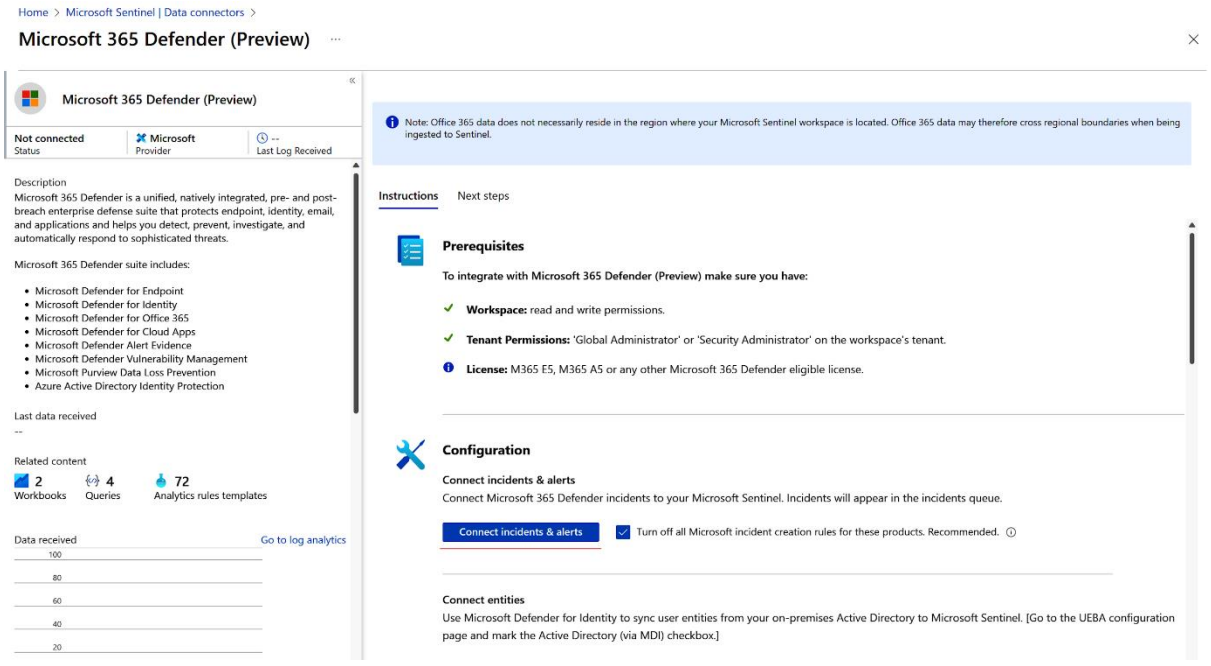

Dashboard > CybSec Guru | Users > Users >
SOAR Test user
User
Search
Edit properties
Delete
Refresh
Reset password
Revoke sessions
Manage view
Got feedback?
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
Troubleshooting + Support
New support request
Overview
Monitoring
Properties
Basic info
SU
SOAR Test user
SOARTest@cybsec.guru
Member
User principal name
SOARTest@cybsec.guru
Object ID
Created date time
Dec 6, 2022, 4:55 AM
User type
Member
Identities
M365x25776268.onmicrosoft.com
Group membe... 0
Applications 0
Assigned roles 0
Assigned licen... 0
My Feed
Account status
Disabled
Edit
Sign-ins
Last sign-in: Dec 6, 2022, 5:34 AM
See all sign-ins

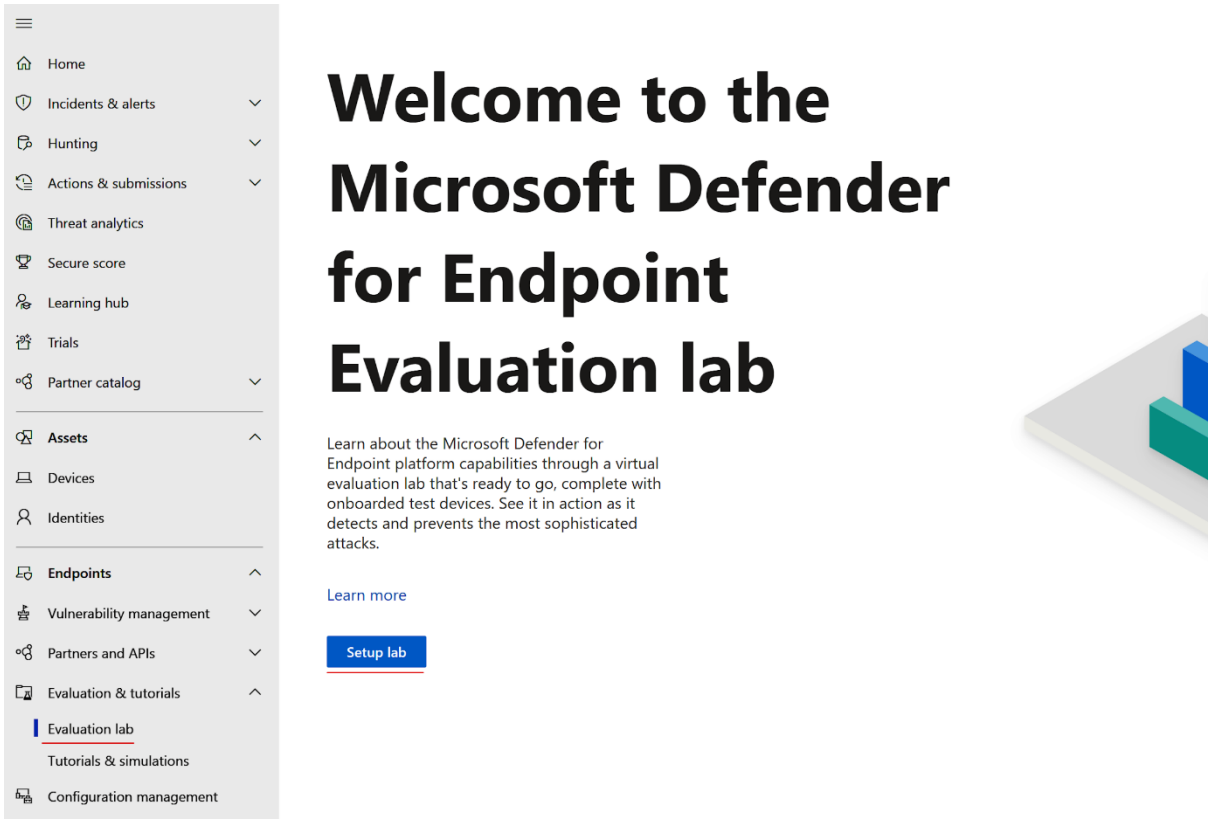

soartest@cybsec.guru
Enter password
Your account has been locked. Contact your support person to unlock it, then try again.
Password
Forgotten my password
Sign in
CybSec Guru

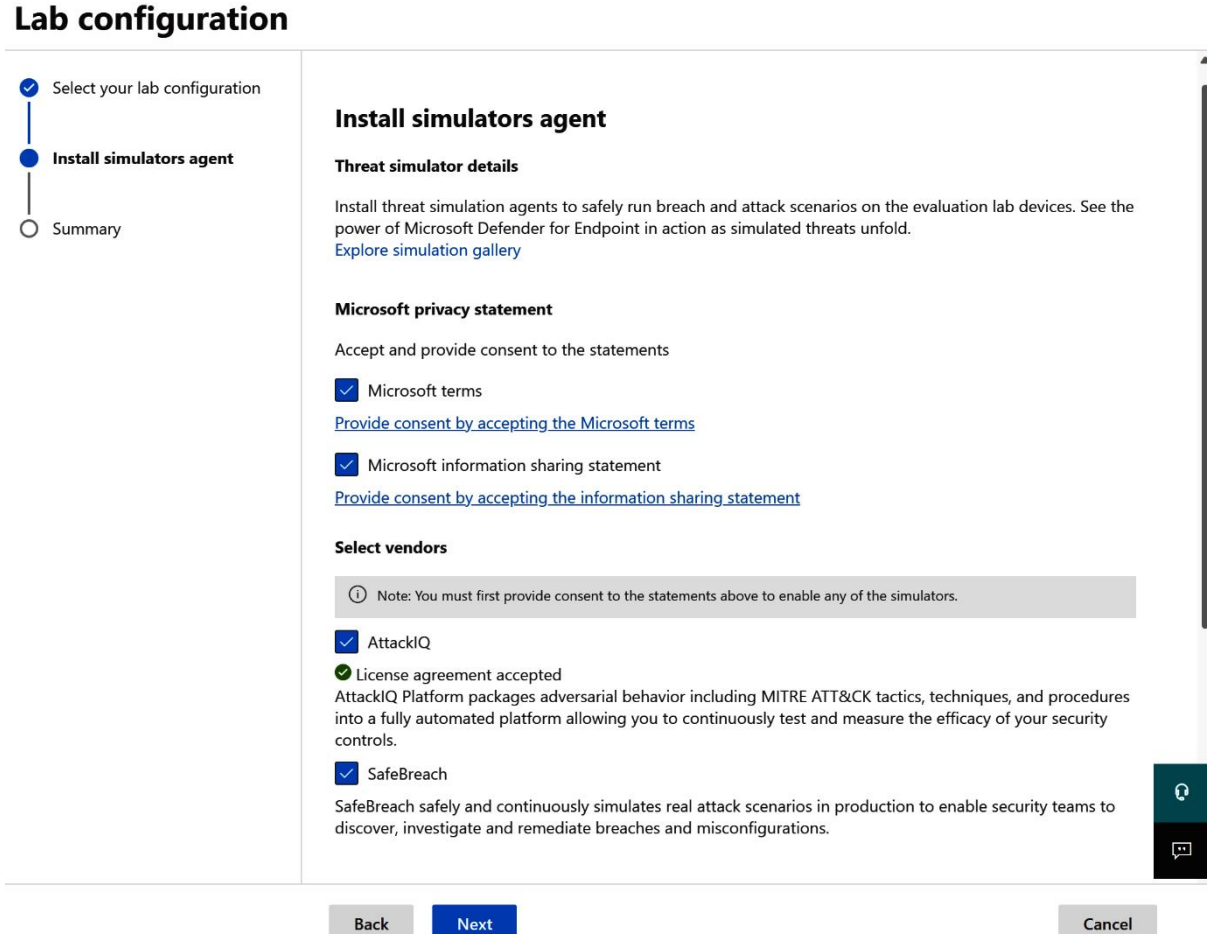

Microsoft 365 admin center
Search
Home
Users
Teams & groups
Billing
Purchase services
Your products
Licenses
Bills & payments
Billing accounts
Payment methods
Billing notifications
Setup
Show all
Home > Purchase services
Dark mode
Purchase services
Find products and services available to buy directly from Microsoft.
Choose up to three products to view a detailed comparison.
Search results: 105 products
Microsoft 365 E5
View by category
Microsoft 365
Office 365
Business apps
Collaboration and communication
Dynamics 365
Security and identity
Other services
Clear search
105 products showing
Microsoft 365
Microsoft 365 combines Office 365, Windows 10, and Enterprise Mobility + Security together for your organization. Today's modern workspace allows people to meet, collaborate, and stay connected across boundaries. Microsoft 365 supports teamwork, connecting services like Microsoft Teams, SharePoint, and Yammer and providing a hub for collaboration.
Microsoft 365 E5 eDiscovery and Audit
Manage eDiscovery communications using tools to send and track custodian responses and escalate with reminders and manager notifications. Investigate data...
From US$6.00 licenses/month
Details
Compare
Microsoft 365 E5
Office 365 E5, Enterprise Mobility + Security E5, and Windows 10/11 Enterprise E5. This per-user licensed suite of products offers customers the latest, most...
From US$57.00 licenses/month
Details
Compare
Microsoft 365 E5 (Month to Month)
Office 365 E5, Enterprise Mobility + Security E5, and Windows 10/11 Enterprise E5. This per-user licensed suite of products offers customers the latest, most...
From US$79.80 licenses/month
Details
Compare
Microsoft 365 E5 without Audio Conferencing
Office 365 E5 without Audio Conferencing, Enterprise Mobility + Security E5, and Windows 10/11 Enterprise E5. This per-user licensed suite of products offers...
Microsoft 365 E5 eDiscovery and Audit Managed Trial
Manage eDiscovery communications using tools to send and track custodian responses and escalate with reminders and manager notifications. Investigate data...
Microsoft 365 E5 Insider Risk Management
Correlate multiple signals, from activities to communications, to view and manage alerts on potential insider risks and remediate. Proactively...
Help & support
Give feedback

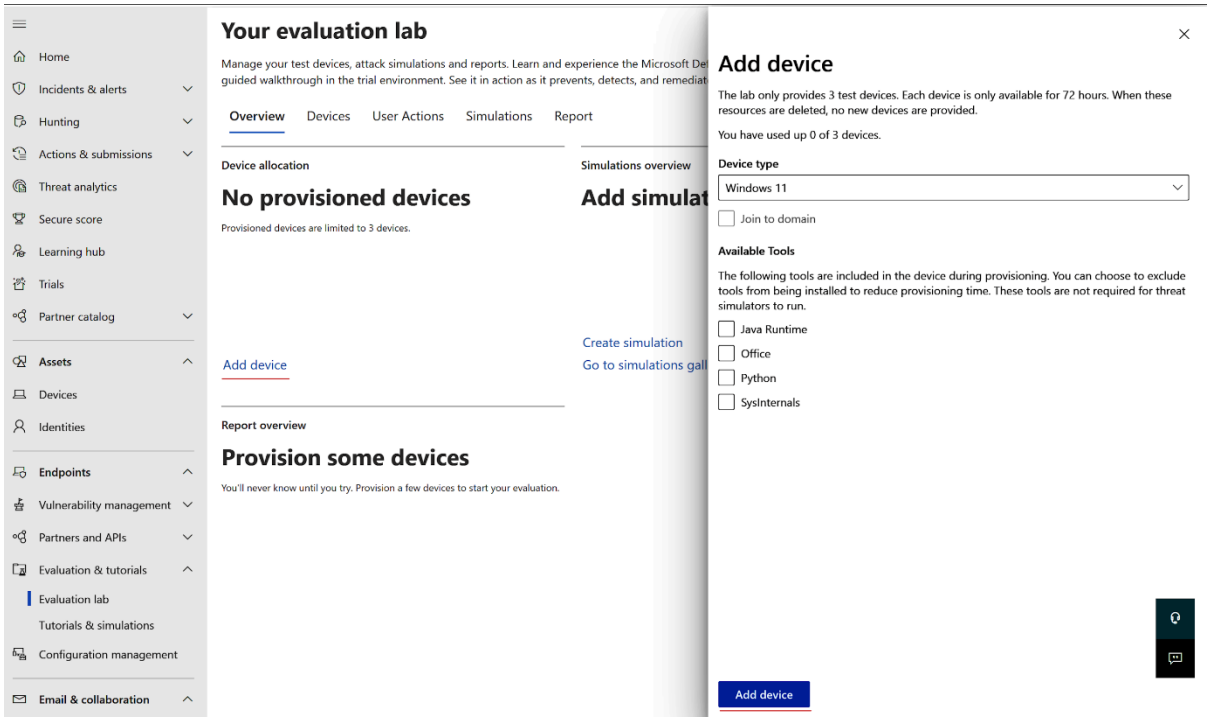

Home
Users
Teams & groups
Billing
Purchase services
Your products
Licenses
Bills & payments
Billing accounts
Payment methods
Billing notifications
Setup
Show all
Home > Purchase services > Product details
Dark mode
Microsoft 365 E5
Office 365 E5, Enterprise Mobility + Security E5, and Windows 10/11 Enterprise E5. This per-user licensed suite of products offers customers the latest, most advanced enterprise security, management, collaboration, and business analytics.
Select license quantity
1
Select billing frequency
US$57.00 license/month
Pay monthly, annual commitment
US$684.00 license/year
Pay yearly, annual commitment
Subtotal before applicable taxes
US$57.00
Buy
Start free trial
Compare details
Add-ons (18)
Included
Partially included
Not included
Microsoft 365 E5
From US$57.00 licenses/month
Microsoft 365 E3
From US$36.00 licenses/month
Details
Office 365 E5
From US$38.00 licenses/month
Details
Licence coverage


Microsoft 365 Defender
Search
BK
Home
Incidents & alerts
Hunting
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Device Inventory
Upgrade your vulnerability management capabilities
Try app control, baseline assessments, and more.
Onboard Defender for IoT
To get full visibility, recommendations, vulnerabilities and alerts for IoT devices, Onboard Defender for IoT
Computers & Mobile
Network devices
IoT devices
Total 0
High risk 0
High exposure 0
Not onboarded 0
Export
Search
30 Days
Customize columns
Filter
Name
Domain
Risk level
Exposure level
OS platform
Windows ver...
Sensor h...
Onboarding ...
Last device upc
Tags
Managed by
Start onboarding devices to your organization
To view and manage devices, onboard them in the Settings page.
Onboard devices


Home > Microsoft Sentinel | Data connectors >
Microsoft 365 Defender (Preview)
Microsoft 365 Defender (Preview)
Not connected
Status
Microsoft
Provider
--
Last Log Received
Description
Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.
Microsoft 365 Defender suite includes:
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365
Microsoft Defender for Cloud Apps
Microsoft Defender Alert Evidence
Microsoft Defender Vulnerability Management
Microsoft Purview Data Loss Prevention
Azure Active Directory Identity Protection
Last data received
--
Related content
2 Workbooks
4 Queries
72 Analytics rules templates
Data received
Go to log analytics
100
80
60
40
20
Note: Office 365 data does not necessarily reside in the region where your Microsoft Sentinel workspace is located. Office 365 data may therefore cross regional boundaries when being ingested to Sentinel.
Instructions
Next steps
Prerequisites
To integrate with Microsoft 365 Defender (Preview) make sure you have:
Workspace: read and write permissions.
Tenant Permissions: 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
License: M365 E5, M365 A5 or any other Microsoft 365 Defender eligible license.
Configuration
Connect incidents & alerts
Connect Microsoft 365 Defender incidents to your Microsoft Sentinel. Incidents will appear in the incidents queue.
Connect incidents & alerts
Turn off all Microsoft incident creation rules for these products. Recommended.
Connect entities
Use Microsoft Defender for Identity to sync user entities from your on-premises Active Directory to Microsoft Sentinel. [Go to the UEBA configuration page and mark the Active Directory (via MDI) checkbox.]


Home
Incidents & alerts
Hunting
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Evaluation & tutorials
Evaluation lab
Tutorials & simulations
Configuration management
Welcome to the Microsoft Defender for Endpoint Evaluation lab
Learn about the Microsoft Defender for Endpoint platform capabilities through a virtual evaluation lab that's ready to go, complete with onboarded test devices. See it in action as it detects and prevents the most sophisticated attacks.
Learn more
Setup lab


Lab configuration
Select your lab configuration
Install simulators agent
Summary
Install simulators agent
Threat simulator details
Install threat simulation agents to safely run breach and attack scenarios on the evaluation lab devices. See the power of Microsoft Defender for Endpoint in action as simulated threats unfold.
Explore simulation gallery
Microsoft privacy statement
Accept and provide consent to the statements
Microsoft terms
Provide consent by accepting the Microsoft terms
Microsoft information sharing statement
Provide consent by accepting the information sharing statement
Select vendors
Note: You must first provide consent to the statements above to enable any of the simulators.
AttackIQ
License agreement accepted
AttackIQ Platform packages adversarial behavior including MITRE ATT&CK tactics, techniques, and procedures into a fully automated platform allowing you to continuously test and measure the efficacy of your security controls.
SafeBreach
SafeBreach safely and continuously simulates real attack scenarios in production to enable security teams to discover, investigate and remediate breaches and misconfigurations.
Back
Next
Cancel



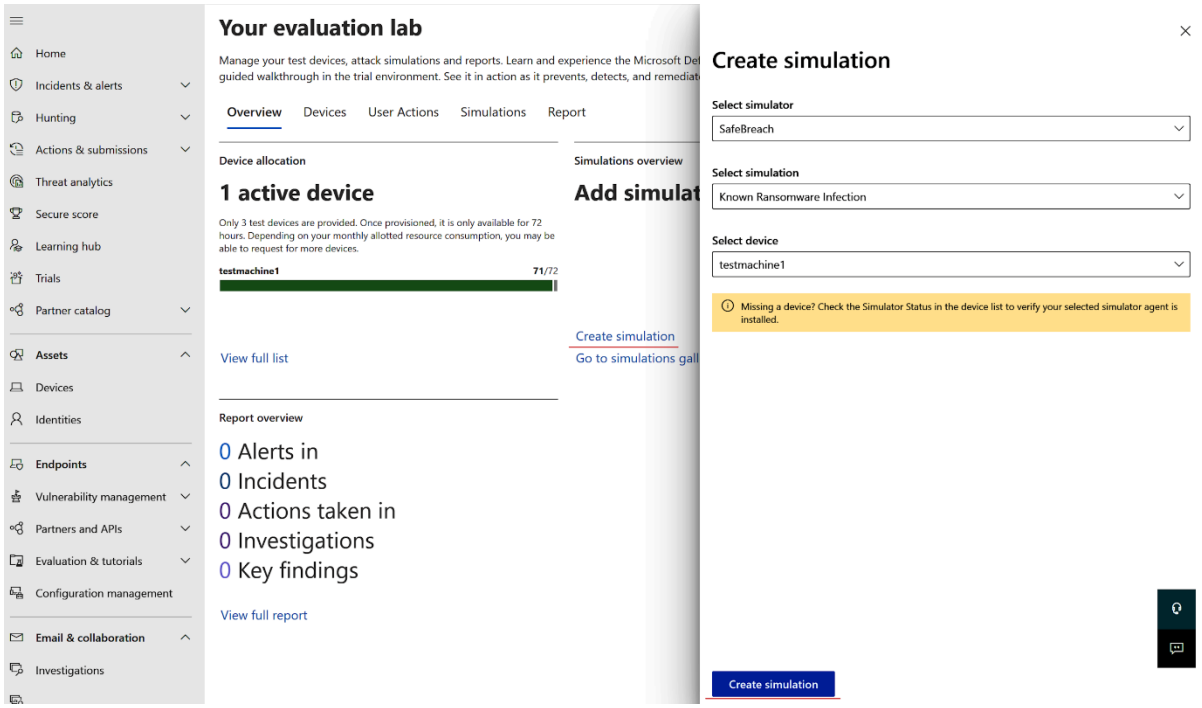
Device allocation

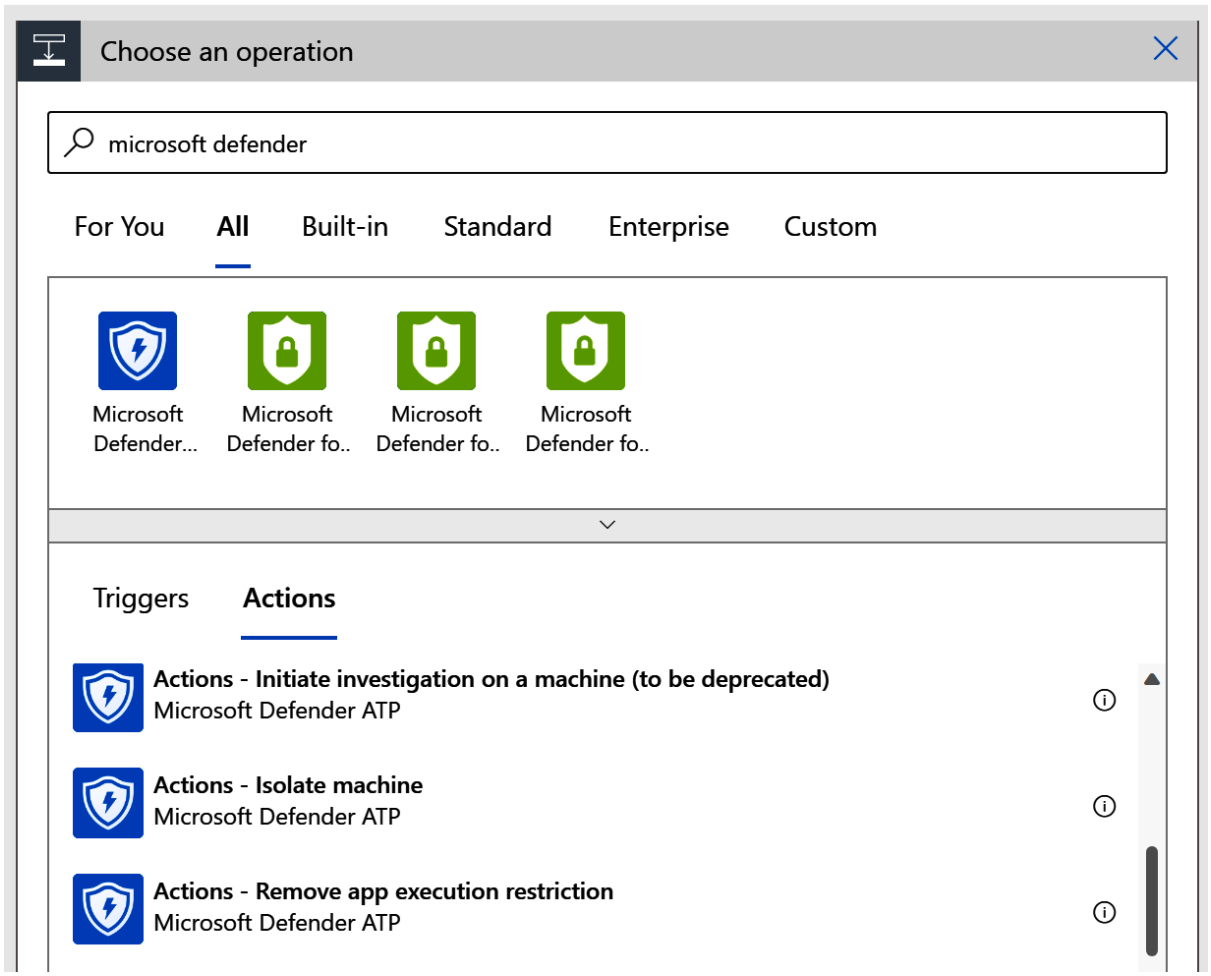
1 active device

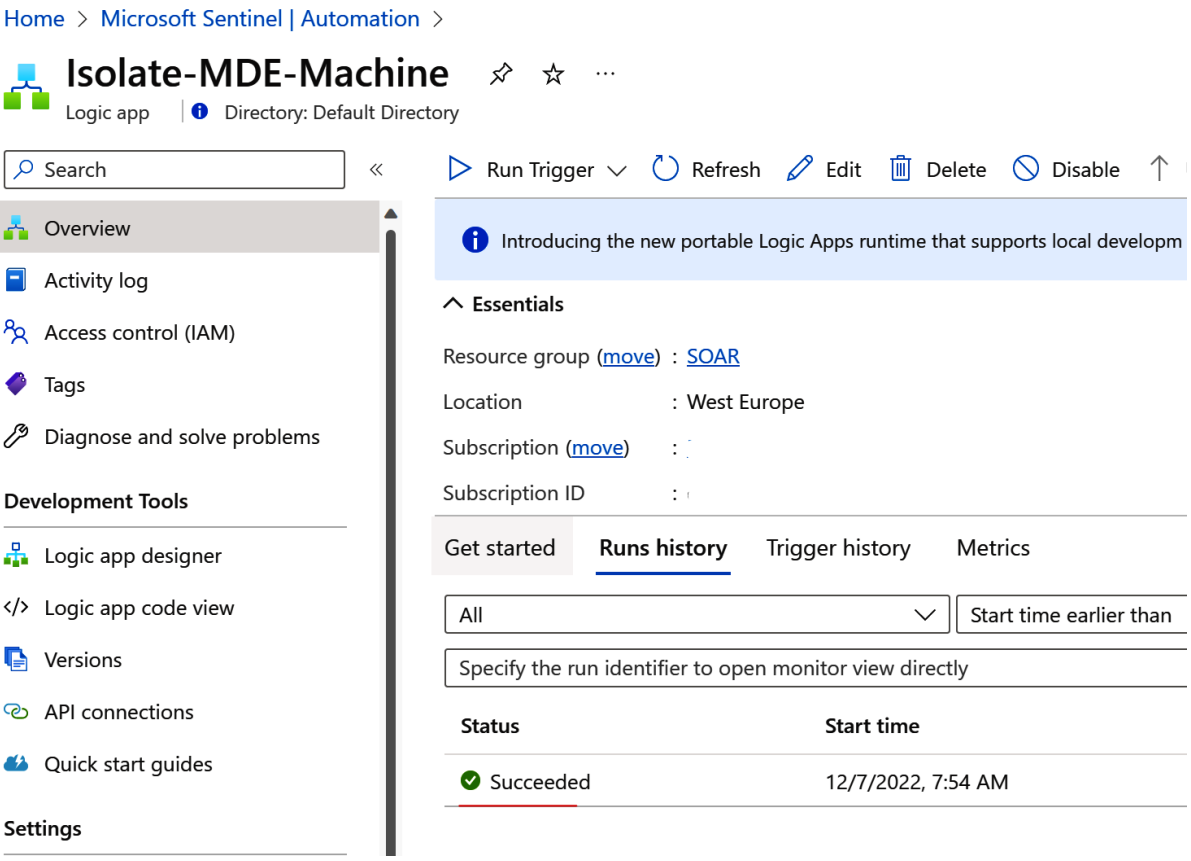
Only 3 test devices are provided. Once provisioned, it is only available for 72 hours. Depending on your monthly allotted resource consumption, you may be able to request for more devices.

testmachine1 **71**/72

View full list


Your evaluation lab
Manage your test devices, attack simulations and reports. Learn and experience the Microsoft De
guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediat
Overview
Devices
User Actions
Simulations
Report
Device allocation
1 active device
Only 3 test devices are provided. Once provisioned, it is only available for 72 hours. Depending on your monthly allotted resource consumption, you may be able to request for more devices.
testmachine1
71/72
View full list
Simulations overview
Add simulat
Create simulation
Go to simulations gall
Report overview
0 Alerts in
0 Incidents
0 Actions taken in
0 Investigations
0 Key findings
View full report
Home
Incidents & alerts
Hunting
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Create simulation
Select simulator
SafeBreach
Select simulation
Known Ransomware Infection
Select device
testmachine1
Missing a device? Check the Simulator Status in the device list to verify your selected simulator agent is installed.
Create simulation


Choose an operation
microsoft defender
For You
All
Built-in
Standard
Enterprise
Custom
Microsoft Defender...
Microsoft Defender fo..
Microsoft Defender fo..
Microsoft Defender fo..
Triggers
Actions
Actions - Initiate investigation on a machine (to be deprecated)
Microsoft Defender ATP
Actions - Isolate machine
Microsoft Defender ATP
Actions - Remove app execution restriction
Microsoft Defender ATP


Home > Microsoft Sentinel | Automation >
Isolate-MDE-Machine
Logic app
Directory: Default Directory
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Run Trigger
Refresh
Edit
Delete
Disable
Introducing the new portable Logic Apps runtime that supports local developm
Essentials
Resource group (move) : SOAR
Location : West Europe
Subscription (move) :
Subscription ID :
Get started
Runs history
Trigger history
Metrics
All
Start time earlier than
Specify the run identifier to open monitor view directly
Status
Start time
Succeeded
12/7/2022, 7:54 AM

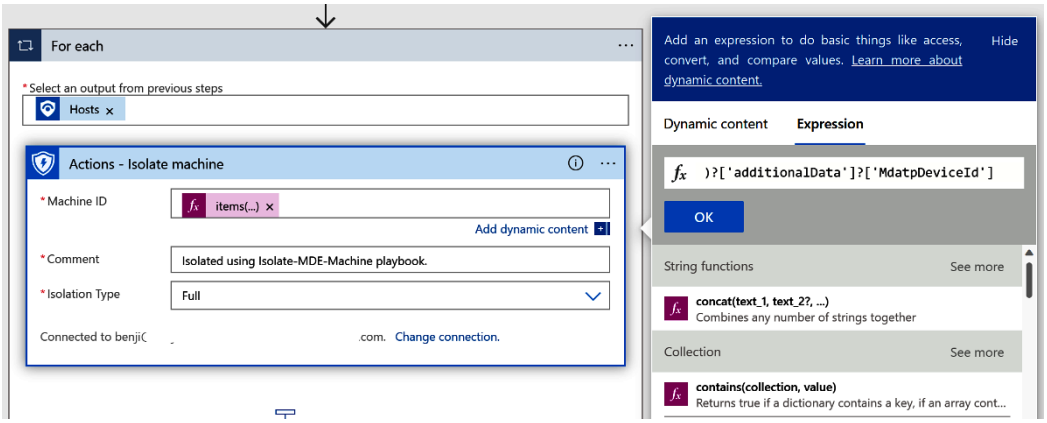
Outputs

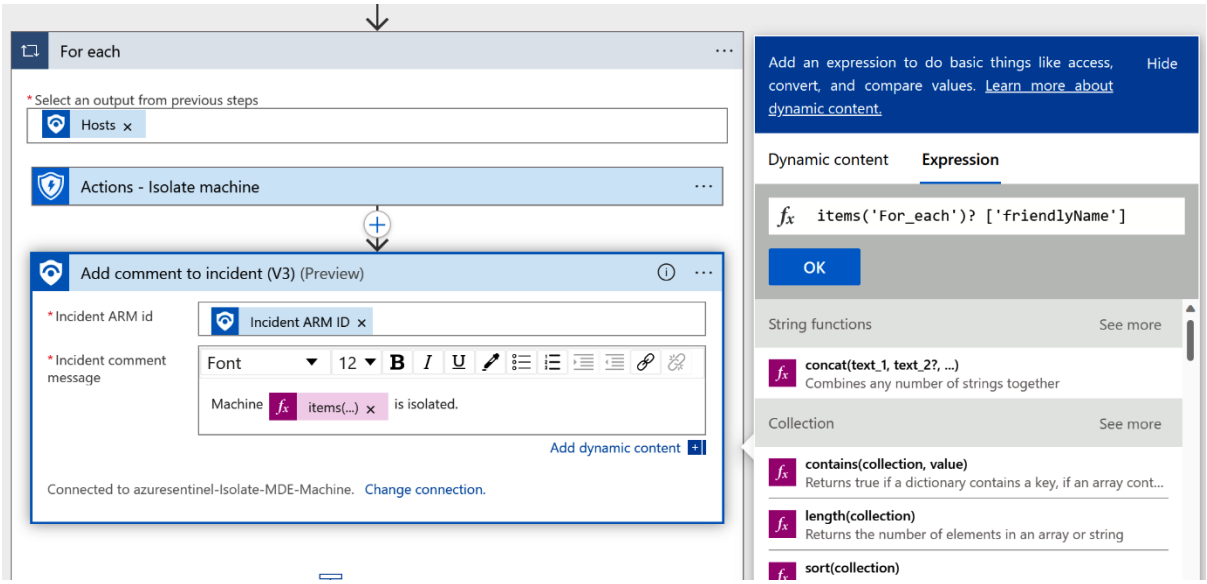
Entities - Get Hosts

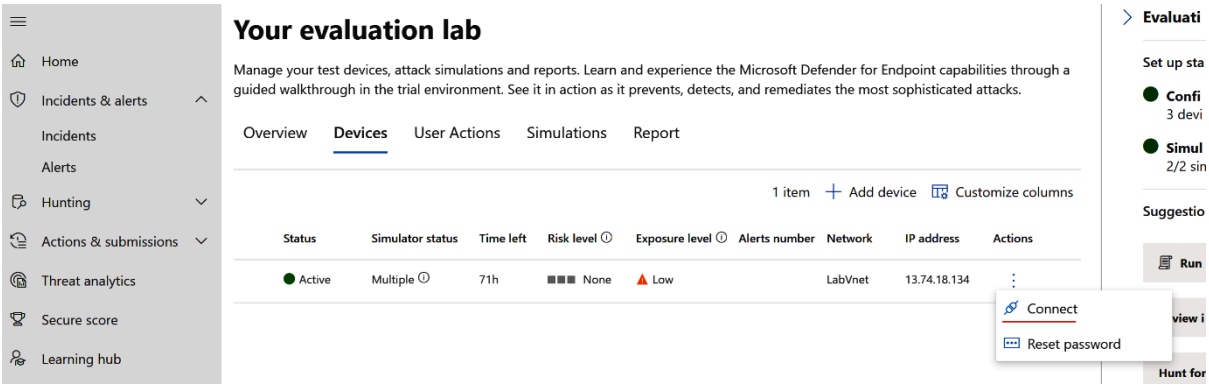

```
{
    "statusCode": 200,
    "headers": {
        "Pragma": "no-cache",
        "Transfer-Encoding": "chunked",
        "Vary": "Accept-Encoding",
        "Cache-Control": "no-store, no-cache"
        "Set-Cookie": "A                                                                                    ,HttpOnly;
        "x-ms-request-id": "b0                                          /".
        "Strict-Transport-Security": "                                        ns",
        "X-Content-Type-Options": "nosniff",
        "X-Frame-Options": "DENY",
        "Timing-Allow-Origin": "*",
        "x-ms-apihub-cached-response": "false",
        "x-ms-apihub-obo": "false",
        "Date": "Wed, 07 Dec 2022 07:54:38 GMT",
        "Content-Type": "application/json; charset=utf-8",
        "Expires": "-1",
        "Content-Length": "516"
    },
    "body": {
        "Hosts": [
            {
                "hostName": "testmachine1",
                "osFamily": "Windows",
                "osVersion": "21H2",
                "additionalData": {
                    "MdatpDeviceId": "c27a373660a3b534c032d70f204067c49d793e54",
                    "FQDN": "testmachine1",
                    "RiskScore": "High",
                    "HealthStatus": "Active",
                    "LastSeen": "2022-12-07T07:27:11.2020735Z",
                    "LastExternalIpAddress": "13.74.18.134",
                    "LastIpAddress": "10.1.1.68",
                    "AvStatus": "Unknown",
                    "OnboardingStatus": "Onboarded",
                    "LoggedOnUsers": "[{\"AccountName\":\"administrator1\",\"DomainName\":\"TestMachine1\"}]"
                },
                "friendlyName": "testmachine1",
                "Type": "host"
```



```
"body": {
    "Hosts": [
        {
            "hostName": "testmachine1",
            "osFamily": "Windows",
            "osVersion": "21H2",
            "additionalData": {
                "MdatpDeviceId": "c27a373660a3b534c032d70f204067c49d793e54",
                "FQDN": "testmachine1",
                "RiskScore": "High",
                "HealthStatus": "Active",
                "LastSeen": "2022-12-07T07:27:11.2020735Z",
                "LastExternalIpAddress": "13.74.18.134",
                "LastIpAddress": "10.1.1.68",
                "AvStatus": "Unknown",
                "OnboardingStatus": "Onboarded",
                "LoggedOnUsers": "[{\"AccountName\":\"administrator1\",\"DomainNa
            },
            "friendlyName": "testmachine1",
```


For each
*Select an output from previous steps
Hosts
Actions - Isolate machine
*Machine ID
items(...)
Add dynamic content
*Comment
Isolated using Isolate-MDE-Machine playbook.
*Isolation Type
Full
Connected to benji(
.com. Change connection.
Add an expression to do basic things like access, convert, and compare values. Learn more about dynamic content.
Hide
Dynamic content
Expression
)?['additionalData']?['MdatpDeviceId']
OK
String functions
See more
concat(text_1, text_2?, ...)
Combines any number of strings together
Collection
See more
contains(collection, value)
Returns true if a dictionary contains a key, if an array cont...

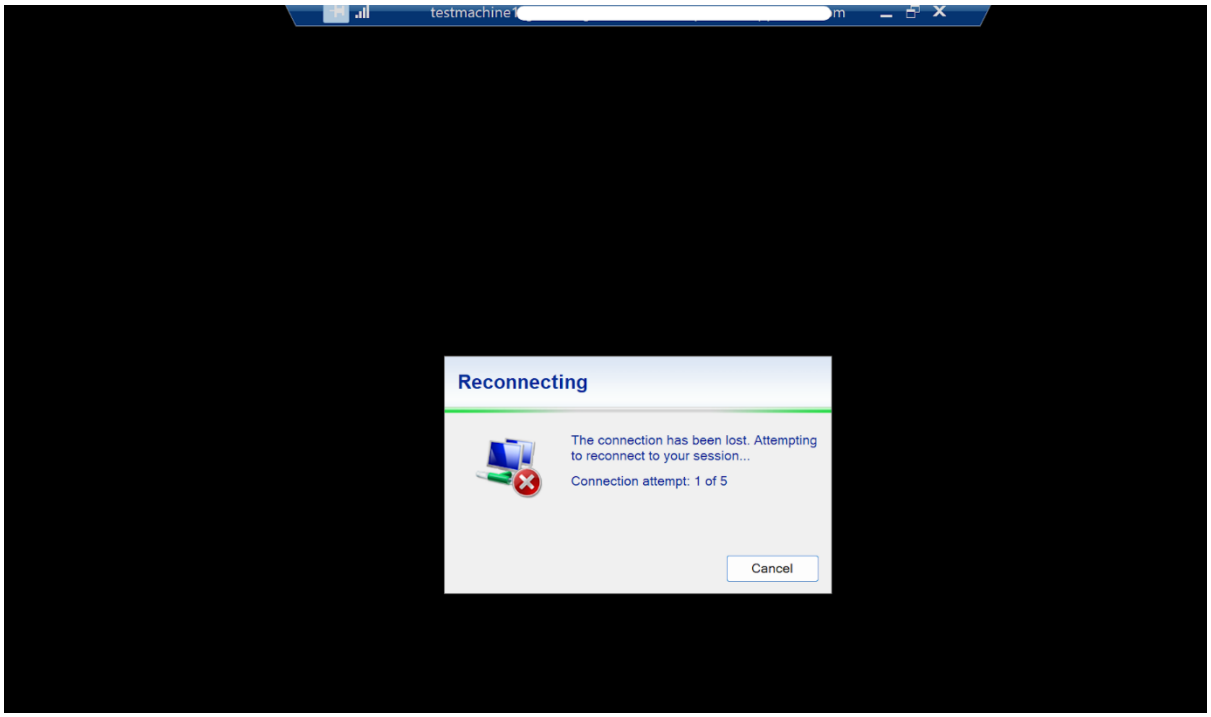

For each
*Select an output from previous steps
Hosts
Actions - Isolate machine
Add comment to incident (V3) (Preview)
*Incident ARM id
Incident ARM ID
*Incident comment message
Font
12
Machine
items(...)
is isolated.
Add dynamic content
Connected to azuresentinel-Isolate-MDE-Machine. Change connection.
Add an expression to do basic things like access, convert, and compare values. Learn more about dynamic content.
Hide
Dynamic content
Expression
items('For_each')? ['friendlyName']
OK
String functions
See more
concat(text_1, text_2?, ...)
Combines any number of strings together
Collection
See more
contains(collection, value)
Returns true if a dictionary contains a key, if an array cont...
length(collection)
Returns the number of elements in an array or string
sort(collection)

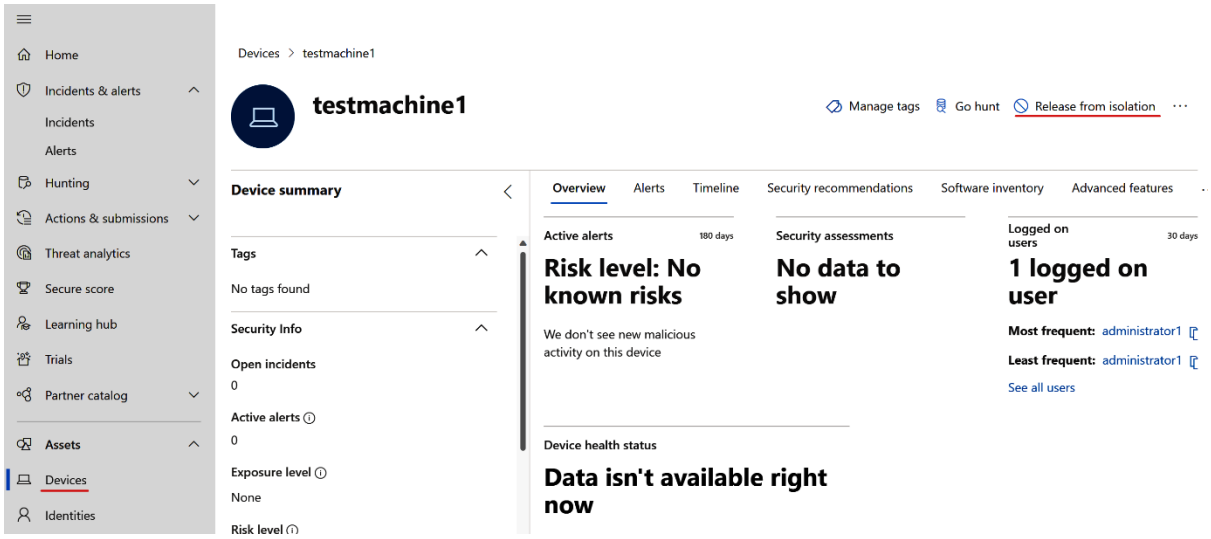

Home
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Threat analytics
Secure score
Learning hub
Your evaluation lab
Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender for Endpoint capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.
Overview
Devices
User Actions
Simulations
Report
1 item
Add device
Customize columns
Status
Simulator status
Time left
Risk level
Exposure level
Alerts number
Network
IP address
Actions
Active
Multiple
71h
None
Low
LabVnet
13.74.18.134
Connect
Reset password
Evaluati
Set up sta
Confi
3 devi
Simul
2/2 sin
Suggestio
Run
Hunt for

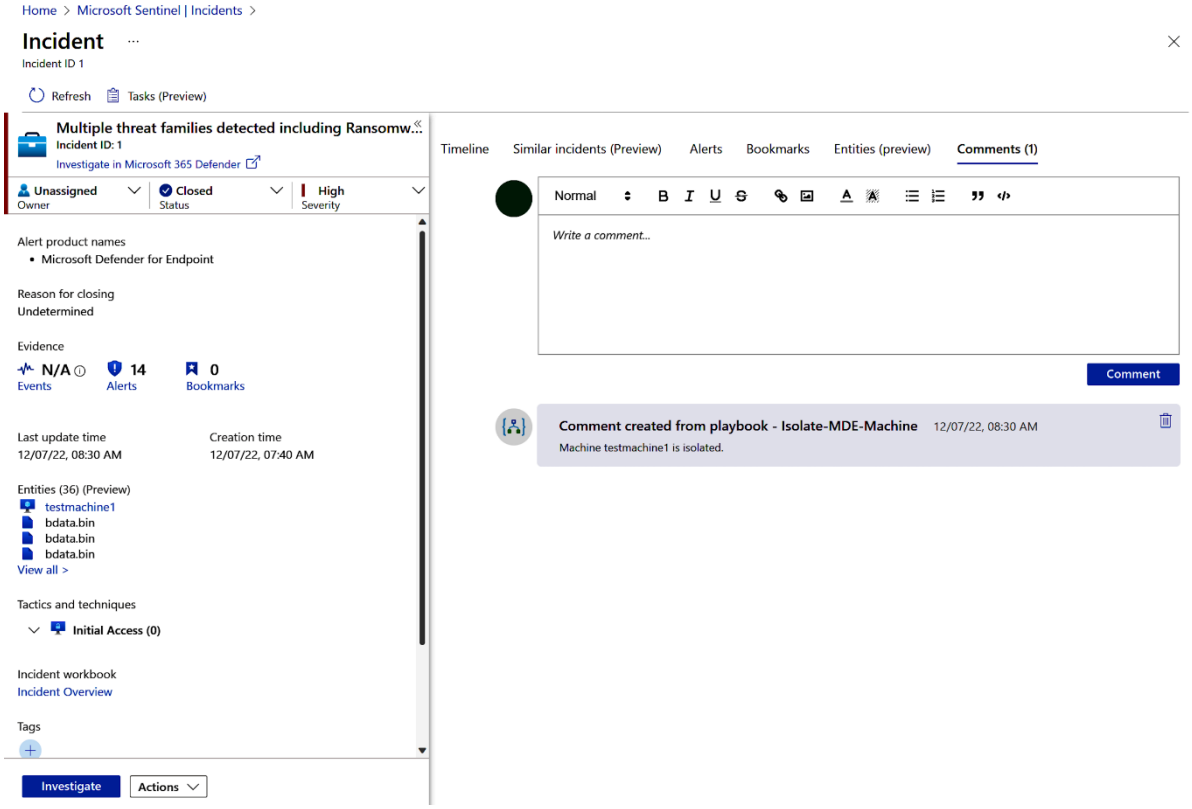
Search by ID, title, tags, owner or product | Severity : **All** | Status : **All** | Product name : **All** | Owner : **All**

Auto-refresh incidents

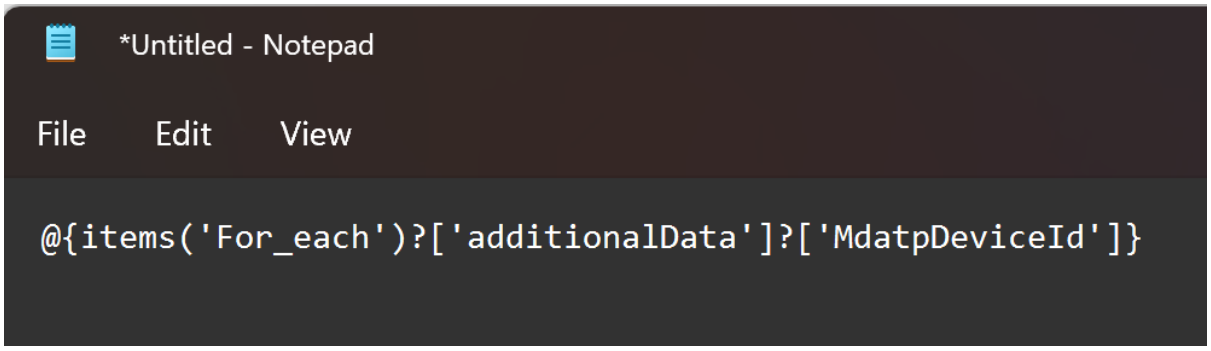
Severity	Incident ID	Title	Alerts	Product names	Create
High	1	Multiple threat families detected inclu...	14	Microsoft 365 Defe...	12/07/
High	2	Multi-stage incident including Ranso...	0	Microsoft 365 Defe...	12/07/

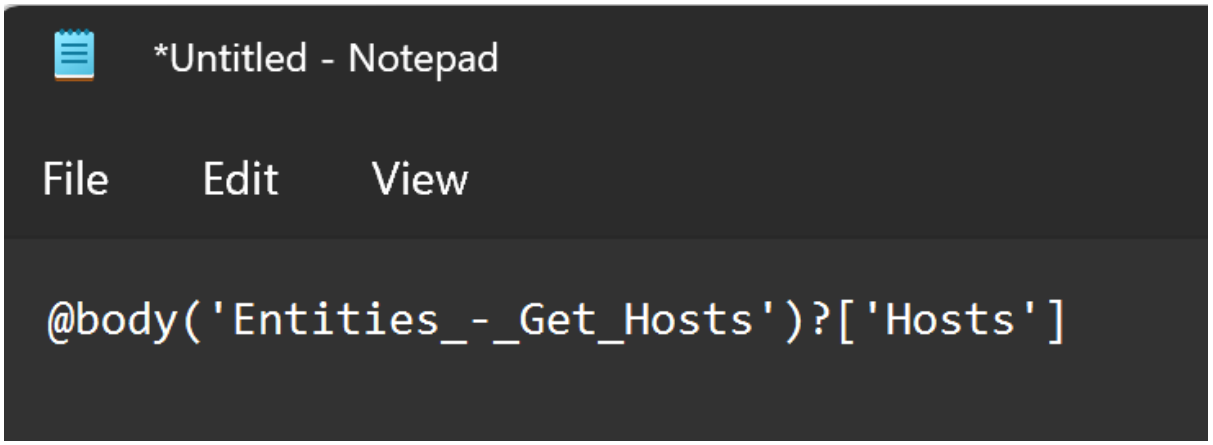




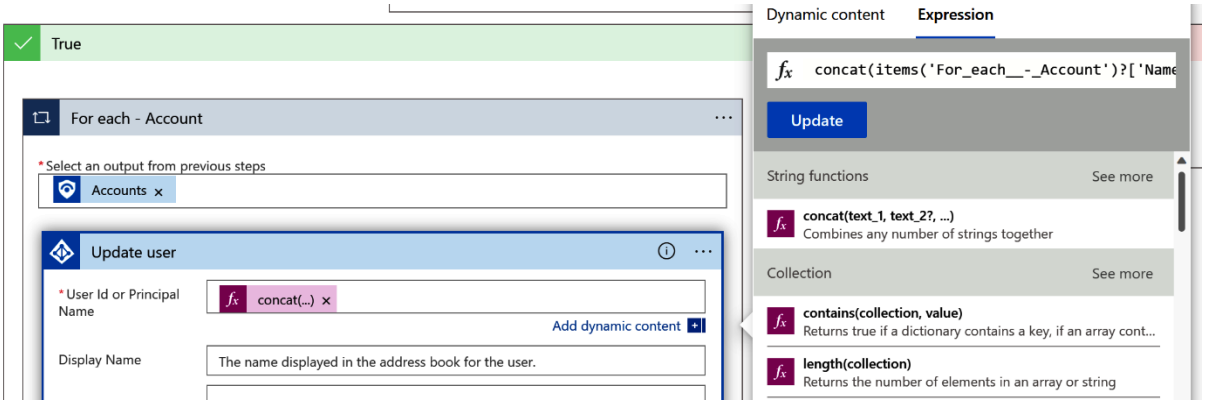

Home > Microsoft Sentinel | Incidents >
Incident
Incident ID 1
Refresh
Tasks (Preview)
Multiple threat families detected including Ransomw...
Incident ID: 1
Investigate in Microsoft 365 Defender
Unassigned
Owner
Closed
Status
High
Severity
Alert product names
• Microsoft Defender for Endpoint
Reason for closing
Undetermined
Evidence
N/A
Events
14
Alerts
0
Bookmarks
Last update time
12/07/22, 08:30 AM
Creation time
12/07/22, 07:40 AM
Entities (36) (Preview)
testmachine1
bdata.bin
bdata.bin
bdata.bin
View all >
Tactics and techniques
Initial Access (0)
Incident workbook
Incident Overview
Tags
Investigate
Actions
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities (preview)
Comments (1)
Normal
Write a comment...
Comment
Comment created from playbook - Isolate-MDE-Machine
12/07/22, 08:30 AM
Machine testmachine1 is isolated.

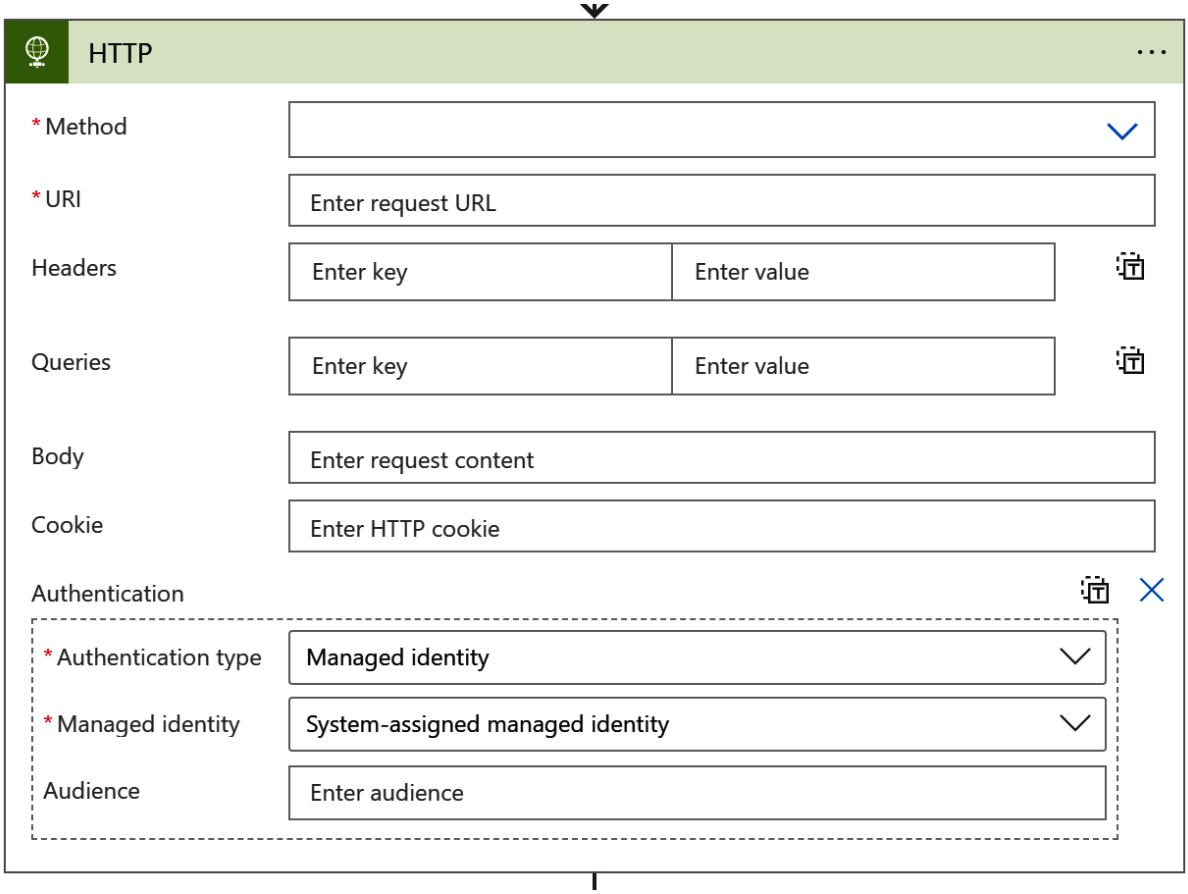
Chapter 9: Mastering Microsoft Sentinel Automation: Tips and Tricks

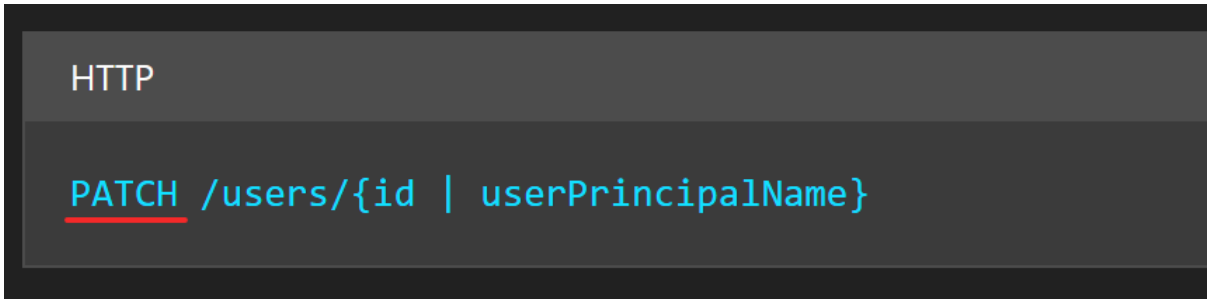





```
"body": {
    "Hosts": [
        {
            "hostName": "testmachine1",
            "osFamily": "Windows",
            "osVersion": "21H2",
            "additionalData": {
                "MdatpDeviceId": "c27a373660a3b534c032d70f204067c49d793e54",
                "FQDN": "testmachine1",
                "RiskScore": "None",
                "HealthStatus": "Active",
                "LastSeen": "2022-12-07T07:27:11.2020735Z",
                "LastExternalIpAddress": "13.74.18.134",
                "LastIpAddress": "10.1.1.68",
                "AvStatus": "Unknown",
                "OnboardingStatus": "Onboarded",
                "LoggedOnUsers": "[{\"AccountName\":\"administrator1\",\"DomainName\":\"TestMachine1\"}]"
            },
            "friendlyName": "testmachine1",
```


True
For each - Account
*Select an output from previous steps
Accounts
Update user
*User Id or Principal Name
concat(...)
Add dynamic content
Display Name
The name displayed in the address book for the user.
Dynamic content
Expression
concat(items('For_each__-_Account')?['Name
Update
String functions
See more
concat(text_1, text_2?, ...)
Combines any number of strings together
Collection
See more
contains(collection, value)
Returns true if a dictionary contains a key, if an array cont...
length(collection)
Returns the number of elements in an array or string


HTTP
* Method
* URI
Enter request URL
Headers
Enter key
Enter value
Queries
Enter key
Enter value
Body
Enter request content
Cookie
Enter HTTP cookie
Authentication
* Authentication type
Managed identity
* Managed identity
System-assigned managed identity
Audience
Enter audience


HTTP
PATCH /users/{id | userPrincipalName}

HTTP Copy

```
PATCH https://graph.microsoft.com/v1.0/me
Content-type: application/json

{
```

Header	Value
Authorization	Bearer {token}. Required.
Content-Type	application/json

Request body

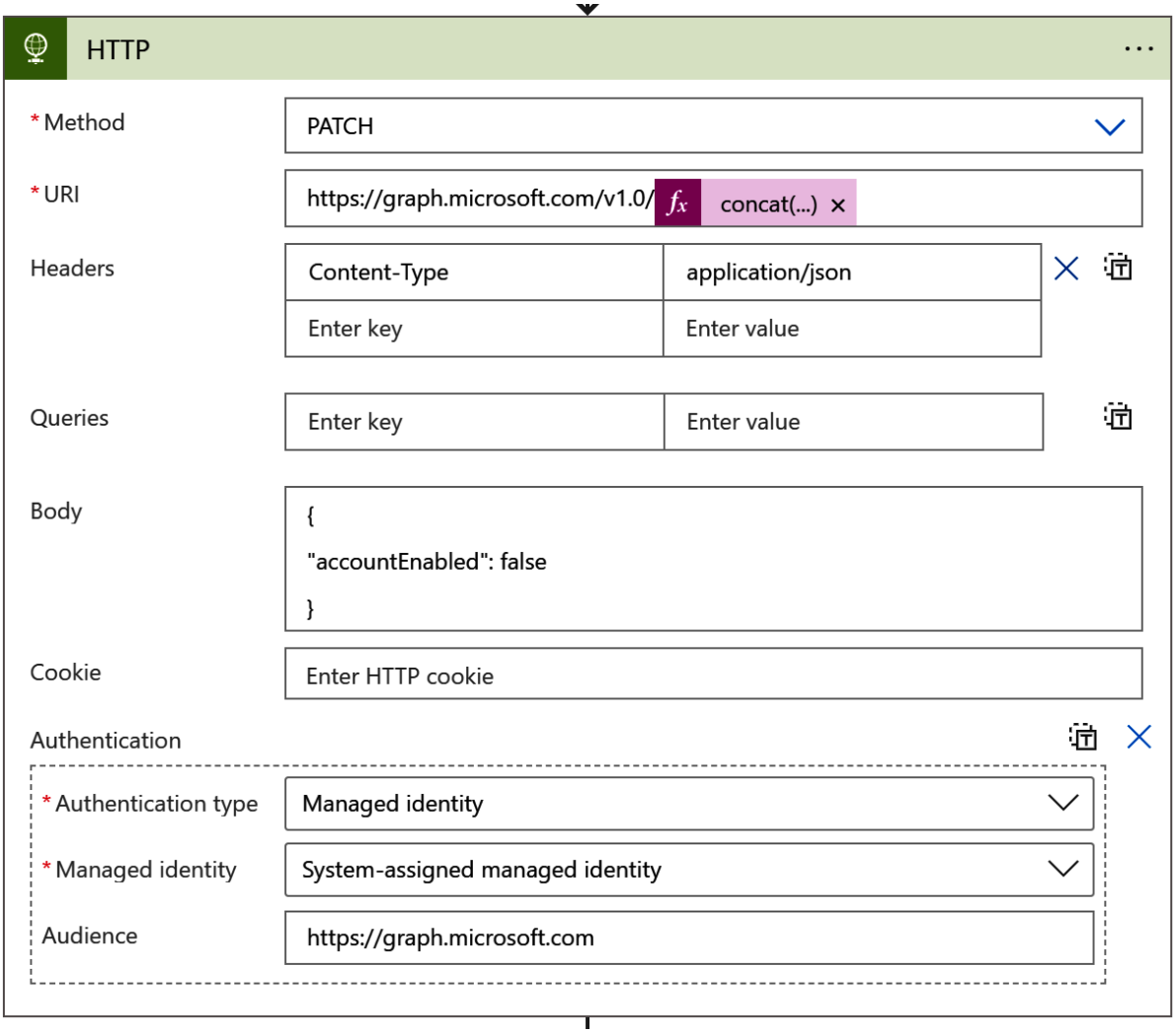
In the request body, supply the values for relevant fields that should be updated. Existing properties that are not included in the request body will maintain their previous values or be recalculated based on changes to other property values. For best performance you shouldn't include existing values that haven't changed.

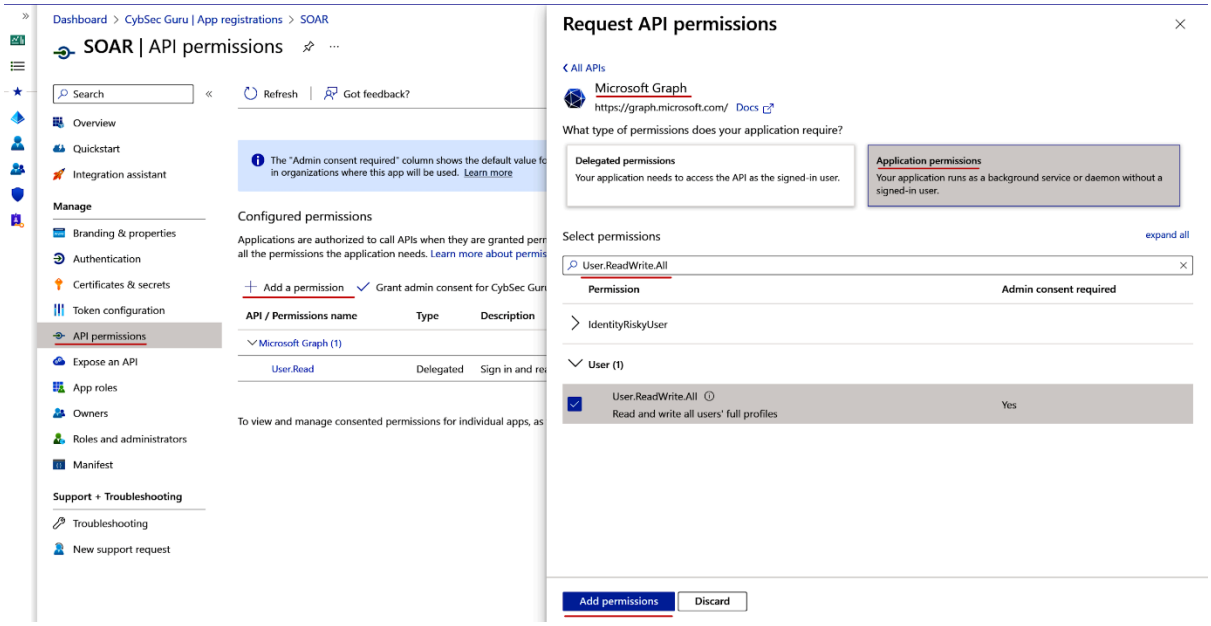
Property	Type	Description
aboutMe	String	A freeform text entry field for the user to describe themselves.
accountEnabled	Boolean	`true` if the account is enabled; otherwise, `false`. This property is required when a user is created. A global administrator assigned the *Directory.AccessAsUser.All* delegated permission can update the **accountEnabled** status of all administrators in the tenant.
ageGroup	ageGroup	Sets the age group of the user. Allowed values: `null`, `Minor`, `NotAdult` and `Adult`. Refer to the legal age group property definitions for further information.
birthday	DateTimeOffset	The birthday of the user. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is `2014-01-01T00:00:00Z`
businessPhones	String collection	The telephone numbers for the user. NOTE: Although this is a string collection, only one

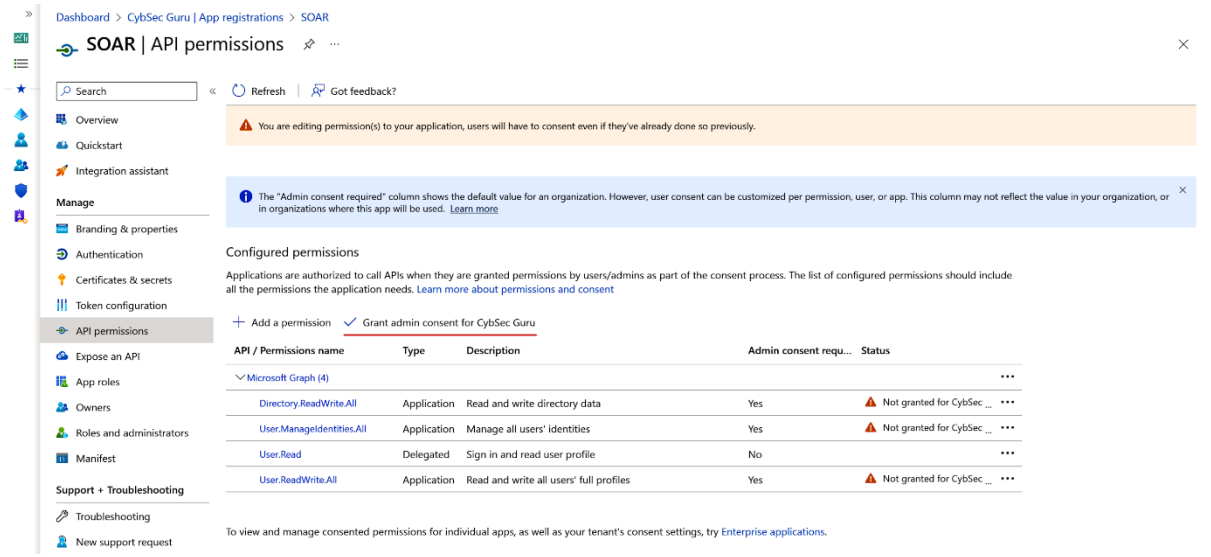
Permissions

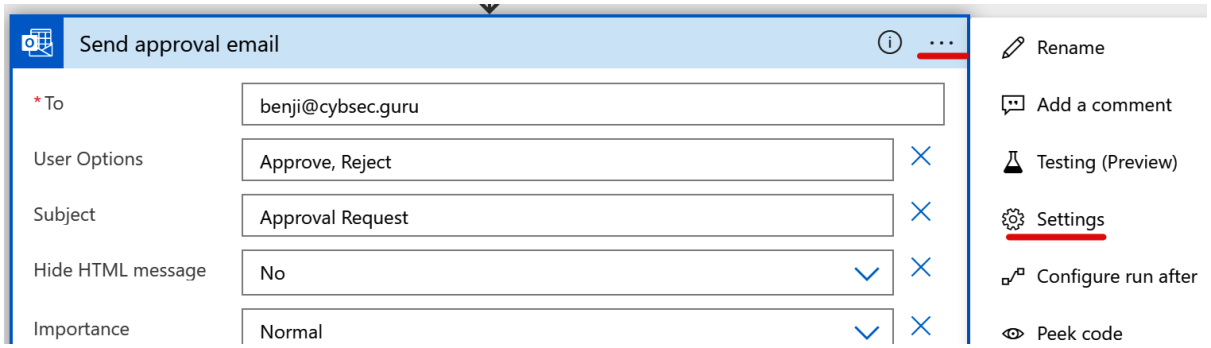
One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	User.ReadWrite, User.ReadWrite.All, User.ManageIdentities.All, Directory.ReadWrite.All
Delegated (personal Microsoft account)	User.ReadWrite
Application	User.ReadWrite.All, User.ManageIdentities.All, Directory.ReadWrite.All




Dashboard > CybSec Guru | App registrations > SOAR
SOAR | API permissions
Search
Refresh
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Configured permissions
Add a permission
Grant admin consent for CybSec Guru
API / Permissions name
Type
Description
Microsoft Graph (1)
User.Read
Delegated
Request API permissions
All APIs
Microsoft Graph
https://graph.microsoft.com/ Docs
What type of permissions does your application require?
Delegated permissions
Your application needs to access the API as the signed-in user.
Application permissions
Your application runs as a background service or daemon without a signed-in user.
Select permissions
expand all
User.ReadWrite.All
Permission
Admin consent required
IdentityRiskyUser
User (1)
User.ReadWrite.All
Read and write all users' full profiles
Yes
Add permissions
Discard


Dashboard > CybSec Guru | App registrations > SOAR
SOAR | API permissions
Search
Refresh
Got feedback?
You are editing permission(s) to your application, users will have to consent even if they've already done so previously.
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more
Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent
Add a permission
Grant admin consent for CybSec Guru
API / Permissions name
Type
Description
Admin consent requ...
Status
Microsoft Graph (4)
Directory.ReadWrite.All
Application
Read and write directory data
Yes
Not granted for CybSec ...
User.ManageIdentities.All
Application
Manage all users' identities
Yes
Not granted for CybSec ...
User.Read
Delegated
Sign in and read user profile
No
User.ReadWrite.All
Application
Read and write all users' full profiles
Yes
Not granted for CybSec ...
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.


Send approval email
*To
benji@cybsec.guru
User Options
Approve, Reject
Subject
Approval Request
Hide HTML message
No
Importance
Normal
Rename
Add a comment
Testing (Preview)
Settings
Configure run after
Peek code

Settings for 'Send approval email'

Secure Inputs

Secure inputs of the operation.

Secure Inputs

Off

Secure Outputs

Secure outputs of the operation and references of output properties.

Secure Outputs

Off

Action Timeout

Limit the maximum duration between the retries and asynchronous responses for this action. Note: This does not alter the request timeout of a single request.

Duration ⓘ PT10M

Retry Policy

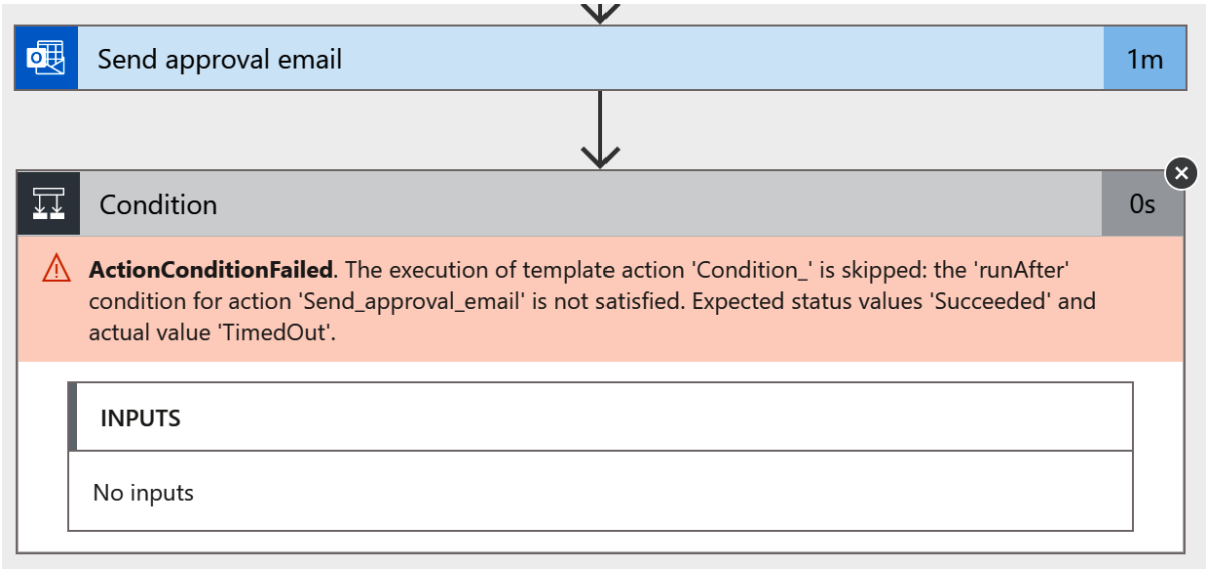
A retry policy applies to intermittent failures, characterized as HTTP status codes 408, 429, and 5xx, in addition to any connectivity exceptions. The default is an exponential interval policy set to retry 4 times.

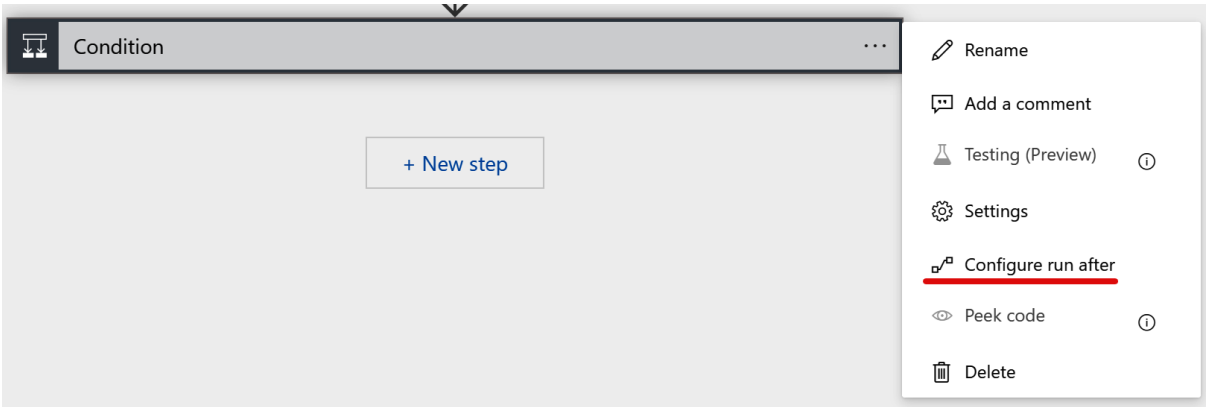
Type Default

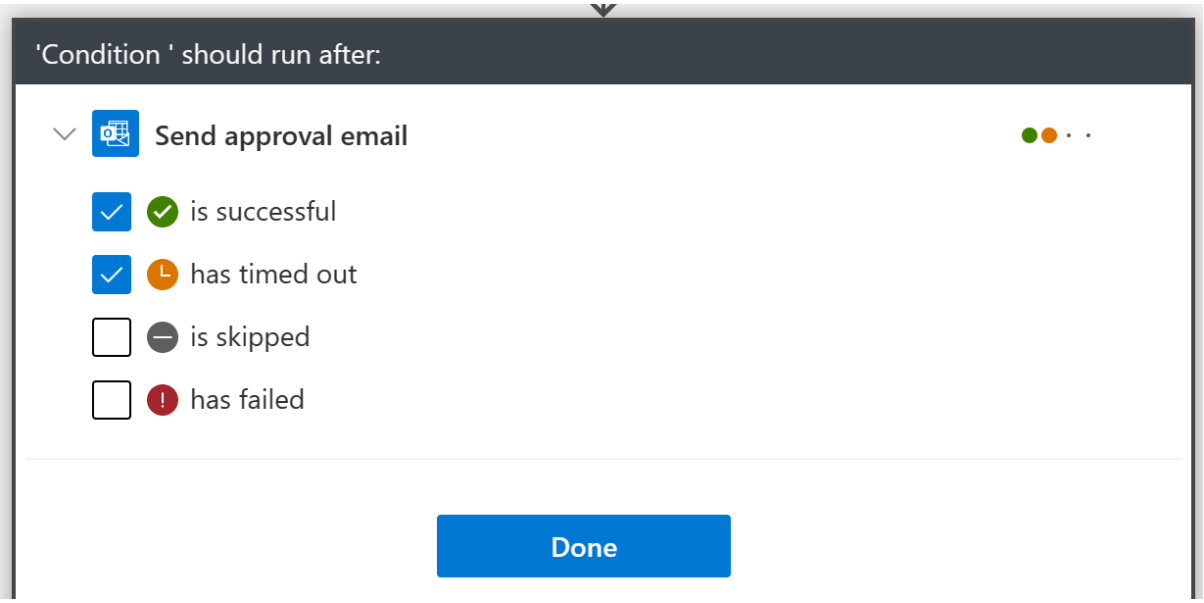
Tracked Properties

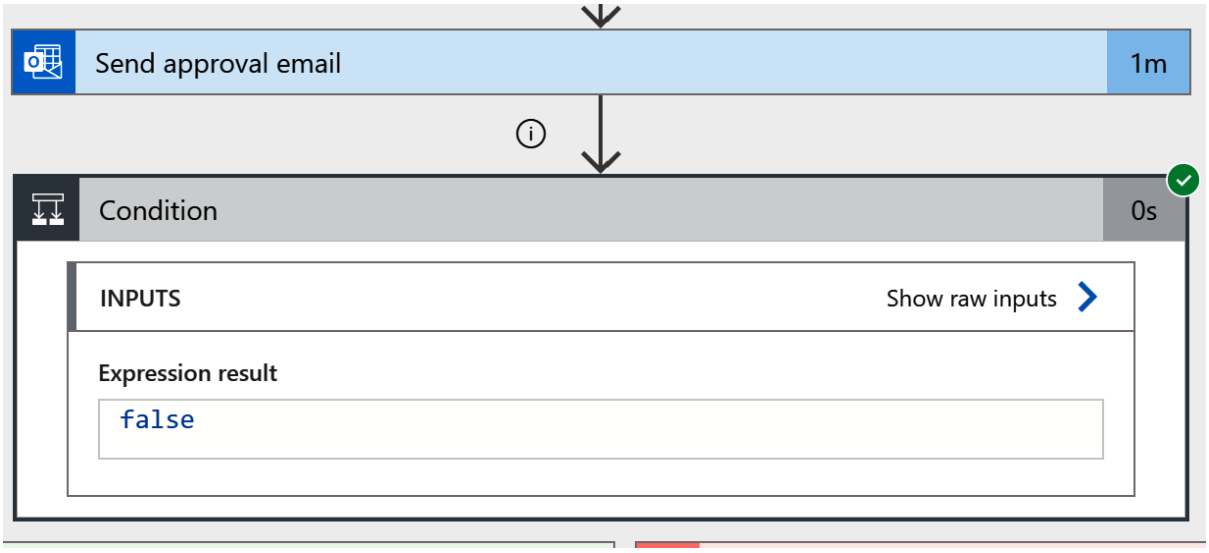
Key	Value

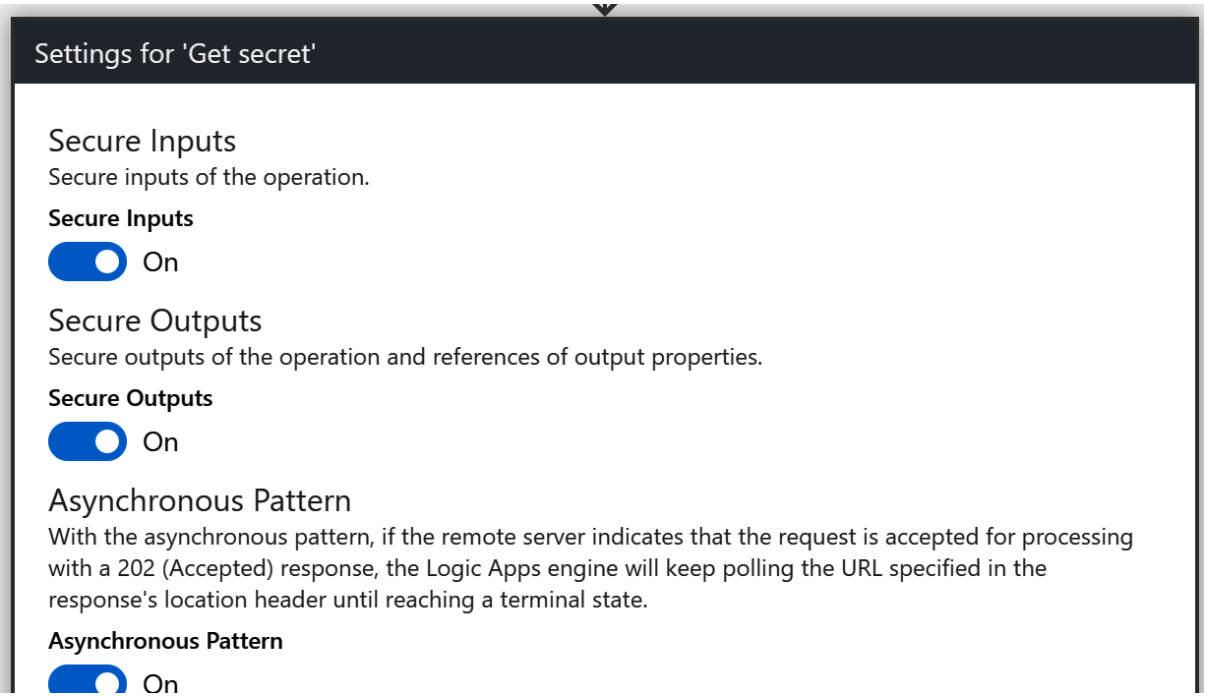
Done Cancel

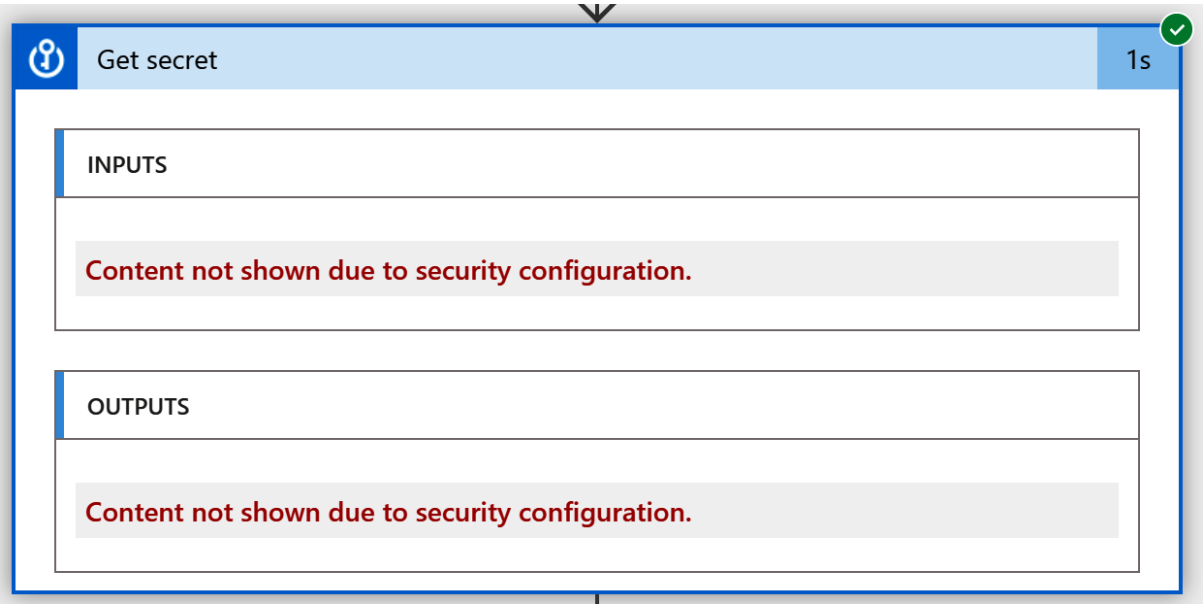


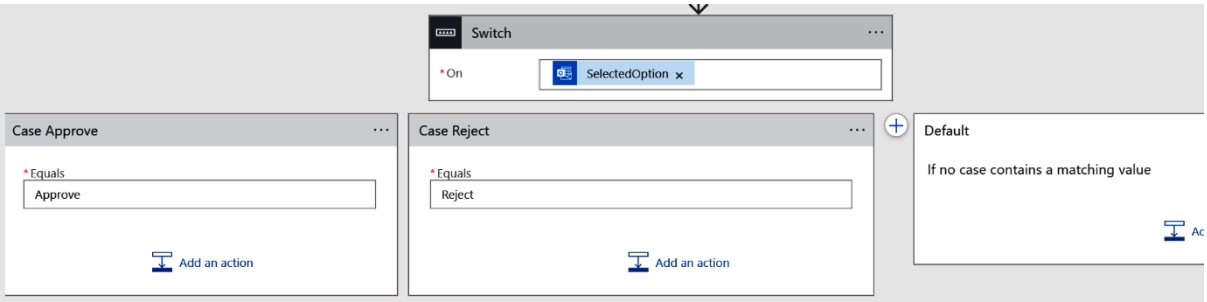

Condition
+ New step
Rename
Add a comment
Testing (Preview)
Settings
Configure run after
Peek code
Delete

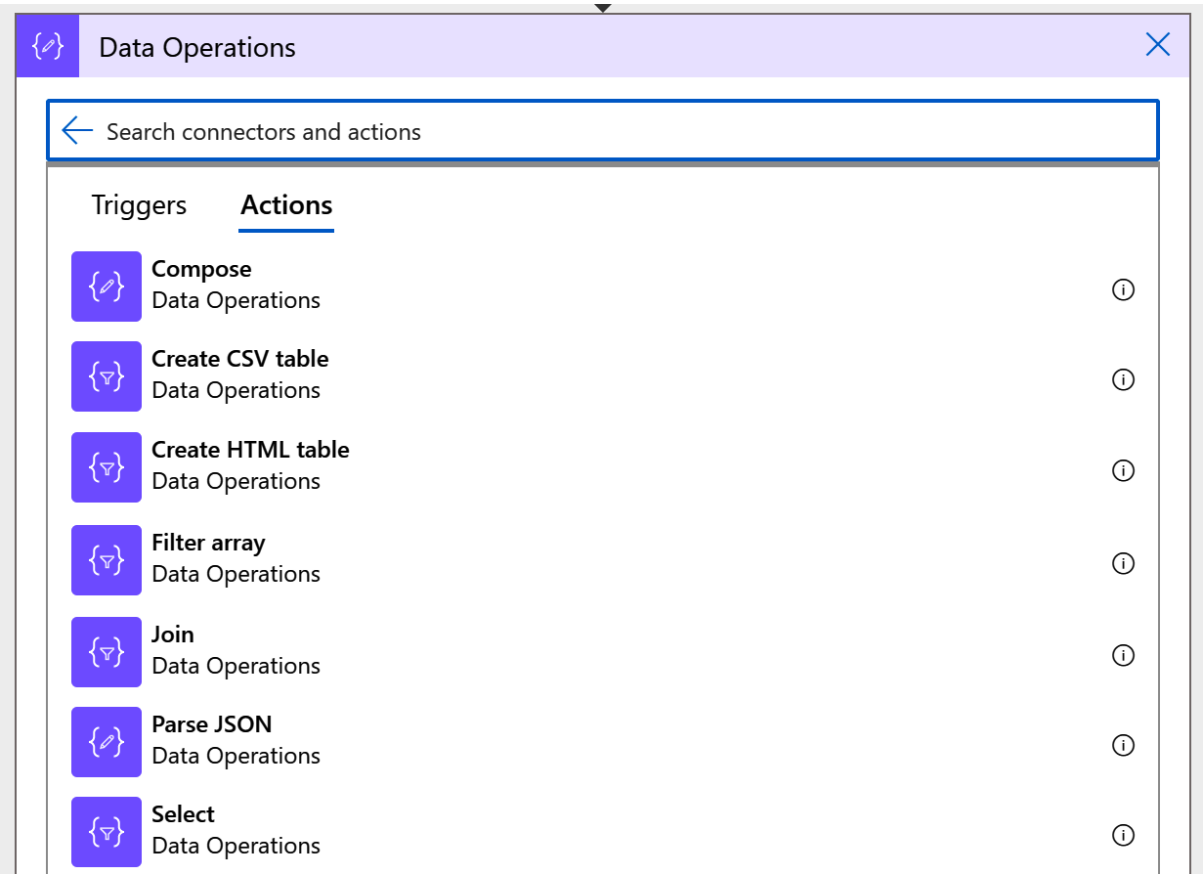

'Condition ' should run after:
Send approval email
is successful
has timed out
is skipped
has failed
Done

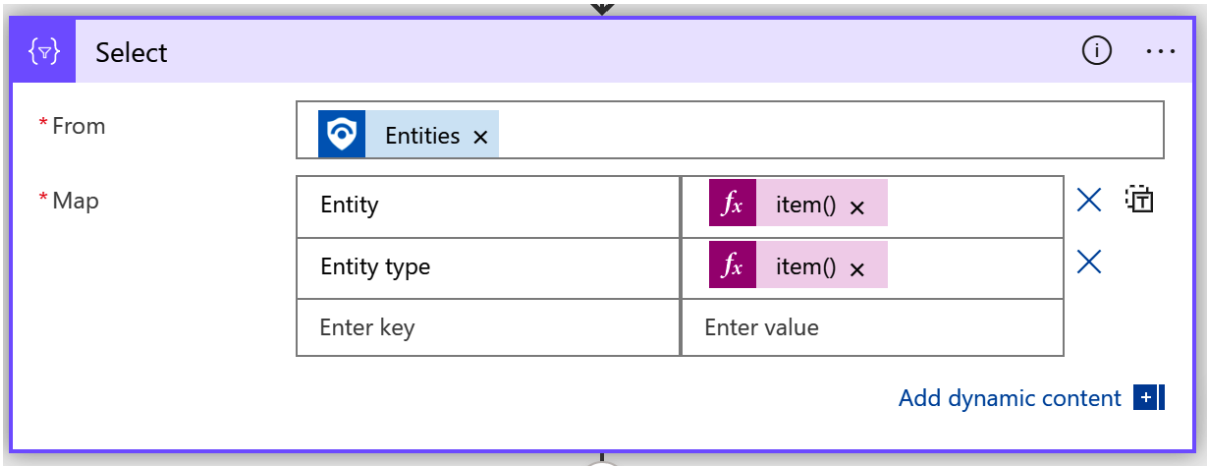

Send approval email
1m
Condition
0s
INPUTS
Show raw inputs
Expression result
false

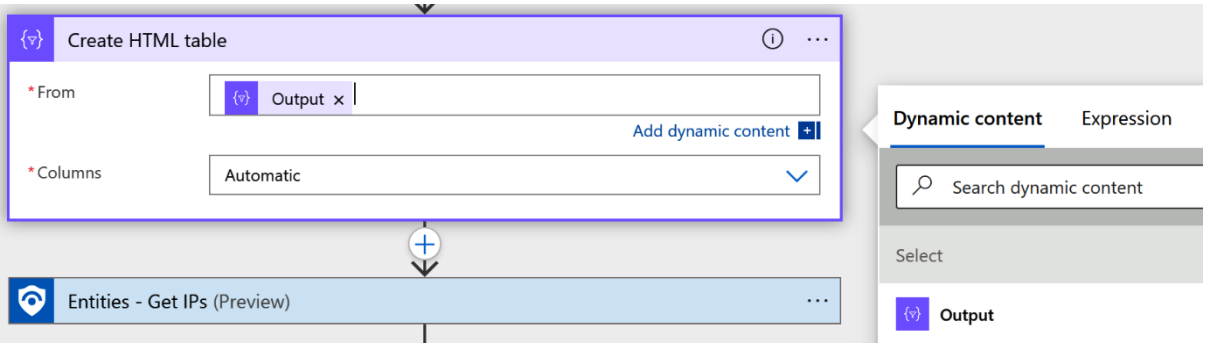

Settings for 'Get secret'
Secure Inputs
Secure inputs of the operation.
Secure Inputs
On
Secure Outputs
Secure outputs of the operation and references of output properties.
Secure Outputs
On
Asynchronous Pattern
With the asynchronous pattern, if the remote server indicates that the request is accepted for processing with a 202 (Accepted) response, the Logic Apps engine will keep polling the URL specified in the response's location header until reaching a terminal state.
Asynchronous Pattern
On

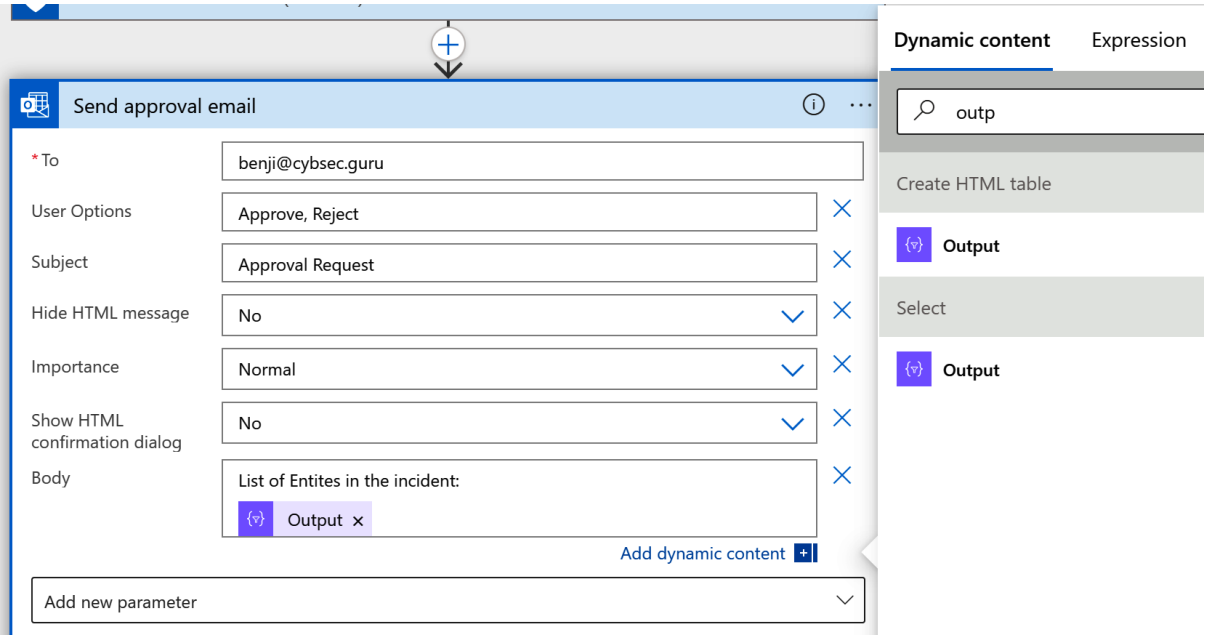

Get secret
1s
INPUTS
Content not shown due to security configuration.
OUTPUTS
Content not shown due to security configuration.

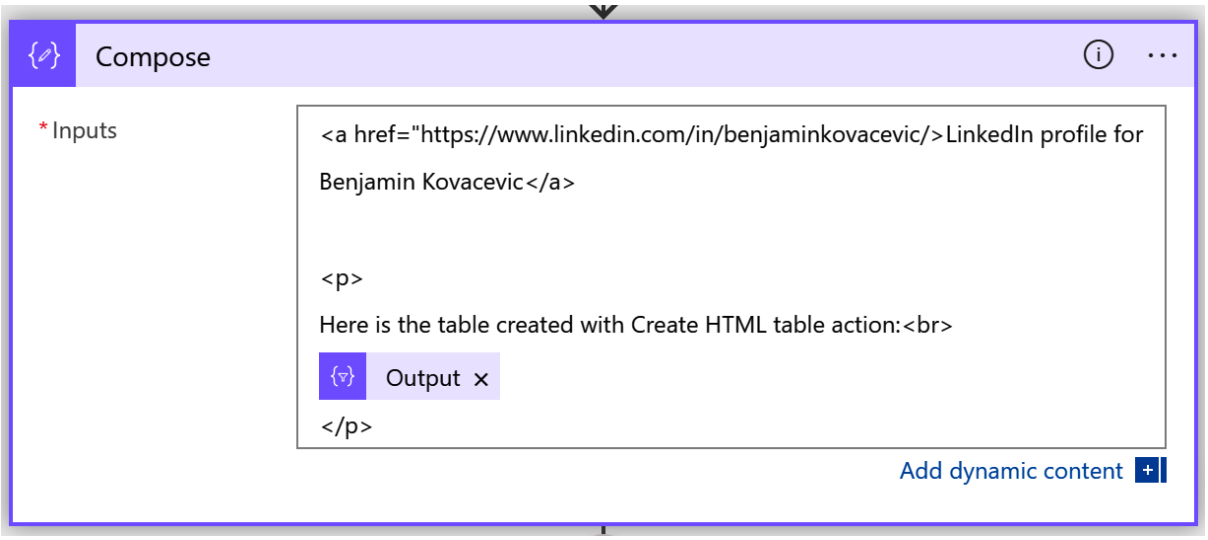

Switch
* On
SelectedOption
Case Approve
* Equals
Approve
Add an action
Case Reject
* Equals
Reject
Add an action
Default
If no case contains a matching value


Data Operations
Search connectors and actions
Triggers
Actions
Compose
Data Operations
Create CSV table
Data Operations
Create HTML table
Data Operations
Filter array
Data Operations
Join
Data Operations
Parse JSON
Data Operations
Select
Data Operations


Select
* From
Entities
* Map
Entity
item()
Entity type
item()
Enter key
Enter value
Add dynamic content

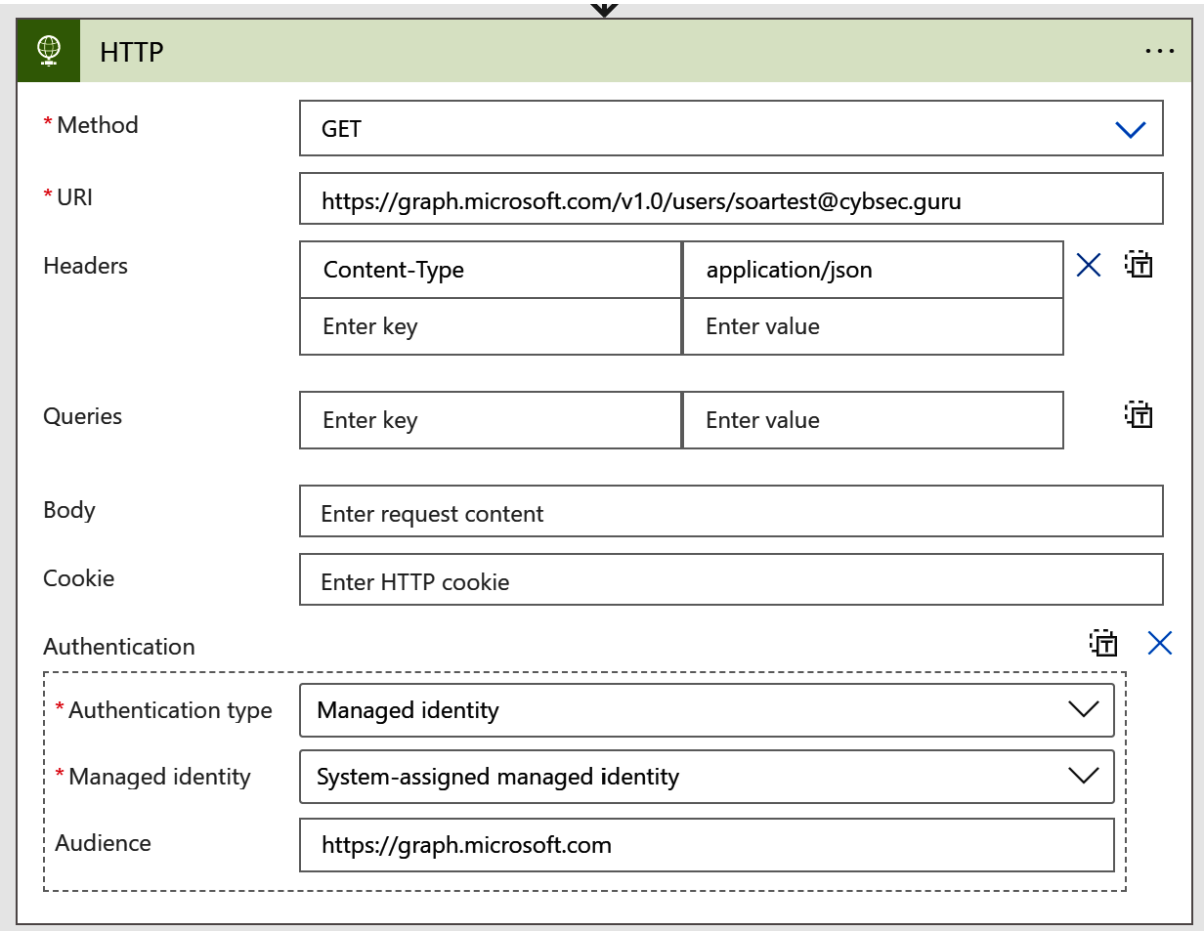

Create HTML table
* From
Output
Add dynamic content
* Columns
Automatic
Entities - Get IPs (Preview)
Dynamic content
Expression
Search dynamic content
Select
Output

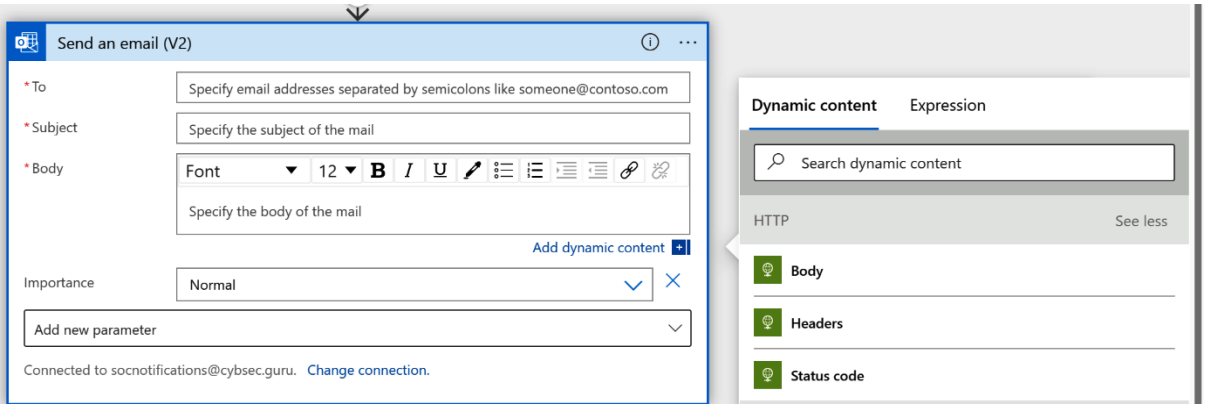

Send approval email
*To
benji@cybsec.guru
User Options
Approve, Reject
Subject
Approval Request
Hide HTML message
No
Importance
Normal
Show HTML confirmation dialog
No
Body
List of Entites in the incident:
Output
Add dynamic content
Add new parameter
Dynamic content
Expression
outp
Create HTML table
Output
Select
Output


Compose
*Inputs
LinkedIn profile for Benjamin Kovacevic

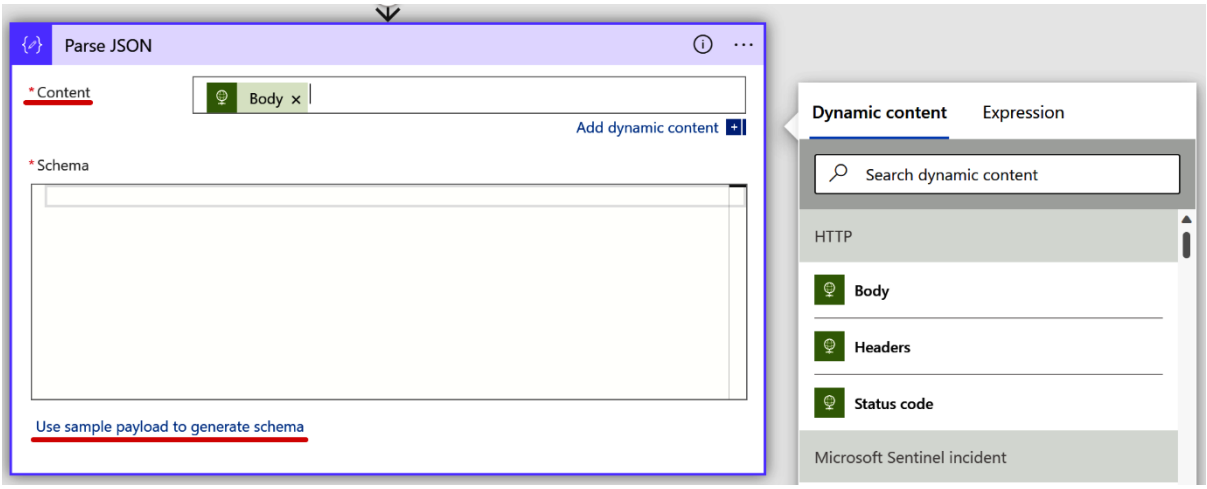
Here is the table created with Create HTML table action:
Output

Add dynamic content


HTTP
* Method
GET
* URI
https://graph.microsoft.com/v1.0/users/soartest@cybsec.guru
Headers
Content-Type
application/json
Enter key
Enter value
Queries
Enter key
Enter value
Body
Enter request content
Cookie
Enter HTTP cookie
Authentication
* Authentication type
Managed identity
* Managed identity
System-assigned managed identity
Audience
https://graph.microsoft.com


Send an email (V2)
* To
Specify email addresses separated by semicolons like someone@contoso.com
* Subject
Specify the subject of the mail
* Body
Font
12
Specify the body of the mail
Add dynamic content
Importance
Normal
Add new parameter
Connected to socnotifications@cybsec.guru. Change connection.
Dynamic content
Expression
Search dynamic content
HTTP
See less
Body
Headers
Status code

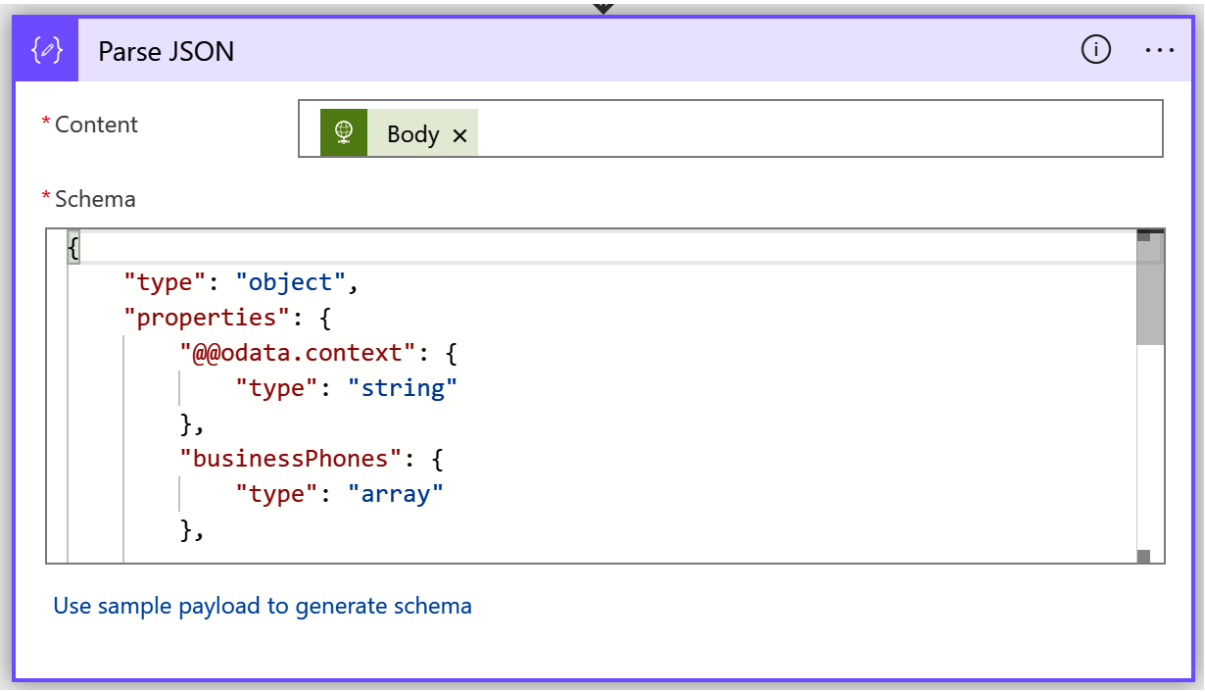
```
"body": {
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
    "businessPhones": [],
    "displayName": "SOAR Test user",
    "givenName": null,
    "jobTitle": null,
    "mail": null,
    "mobilePhone": null,
    "officeLocation": null,
    "preferredLanguage": null,
    "surname": null,
    "userPrincipalName": "SOARTest@cybsec.guru",
    "id": "46f7b9a7-0a1f-44d2-a345-47ed303b8d94"
}
```

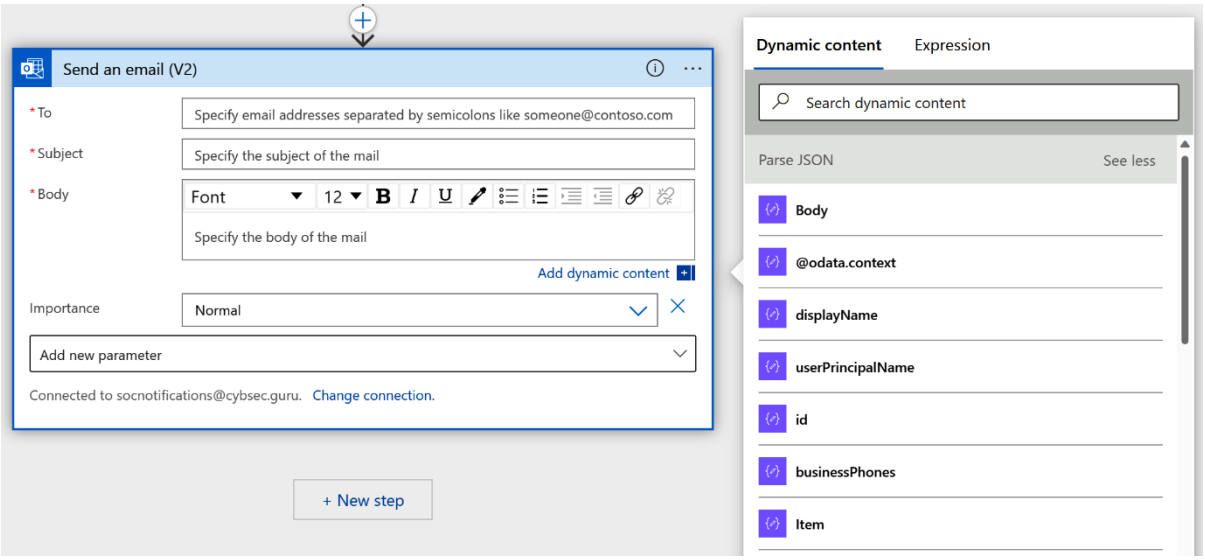



Enter or paste a sample JSON payload.


```
    "jobTitle": null,
    "mail": null,
    "mobilePhone": null,
    "officeLocation": null,
    "preferredLanguage": null,
    "surname": null,
    "userPrincipalName": "SOARTest@cybsec.guru",
    "id": "46f7b9a7-0a1f-44d2-a345-47ed303b8d94"
}
```


Done


Parse JSON
* Content
Body
* Schema
{
"type": "object",
"properties": {
"@@odata.context": {
"type": "string"
},
"businessPhones": {
"type": "array"
},
Use sample payload to generate schema


Send an email (V2)
* To
Specify email addresses separated by semicolons like someone@contoso.com
* Subject
Specify the subject of the mail
* Body
Font
12
Specify the body of the mail
Add dynamic content
Importance
Normal
Add new parameter
Connected to socnotifications@cybsec.guru. Change connection.
+ New step
Dynamic content
Expression
Search dynamic content
Parse JSON
See less
Body
@odata.context
displayName
userPrincipalName
id
businessPhones
Item