Detection Engineering and Automation in Security Operations

Sentinel, Logic Apps, Workbooks, Functions, AND MORE!

INTRO & IDEAS





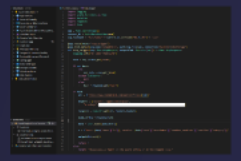
EXAMPLE 1


EXAMPLE 2




EXAMPLE 3





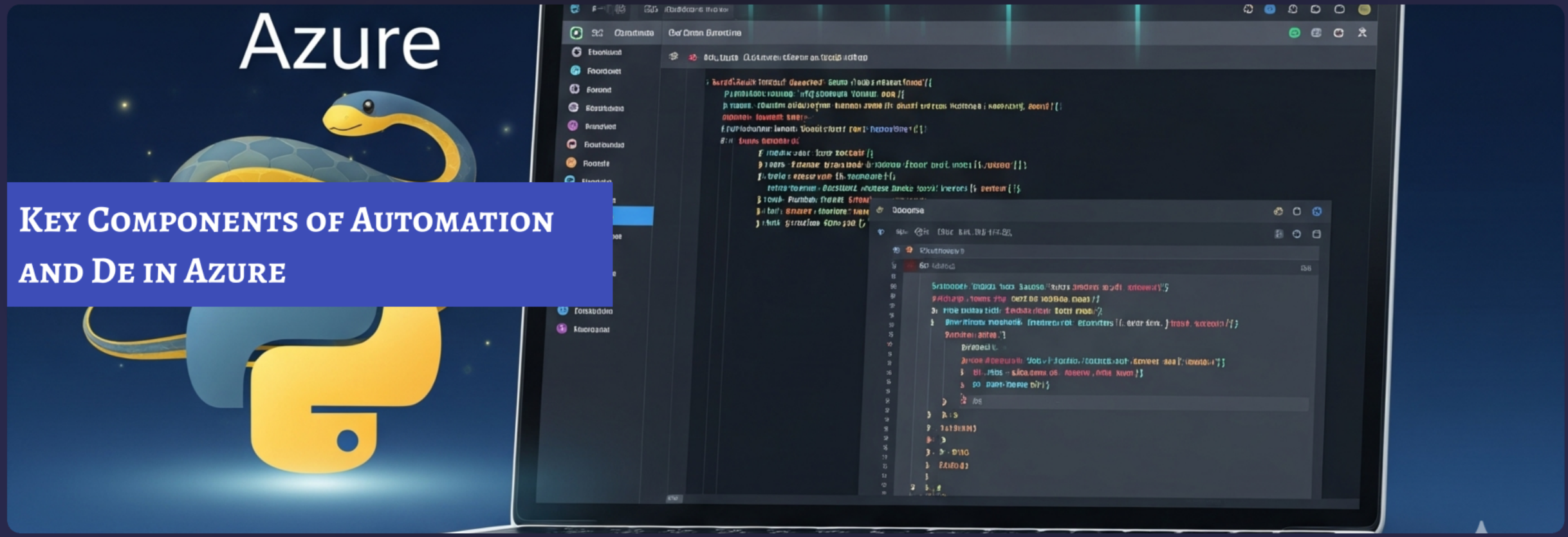

WHOAMI

Sentinel

Logic Apps

Workbooks

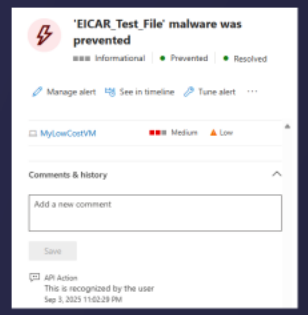
Functions



Key Components of Automation and De in Azure

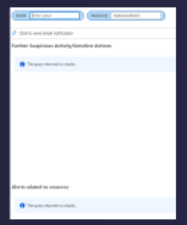
Detection Engineering

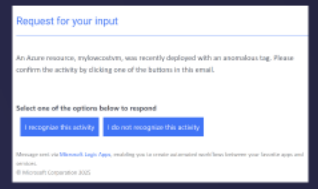
- Slow down, don't speed up
- Policy/Procedure-as-Detection
- Dynamic Detections


'EICAR_Test_File' malware was prevented
Informational
Prevented
Resolved
Manage alert
See in timeline
Tune alert
MyLowCostVM
Medium
Low
Comments & history
Add a new comment
Save
API Action
This is recognized by the user
Sep 3, 2025 11:02:29 PM


API Explorer

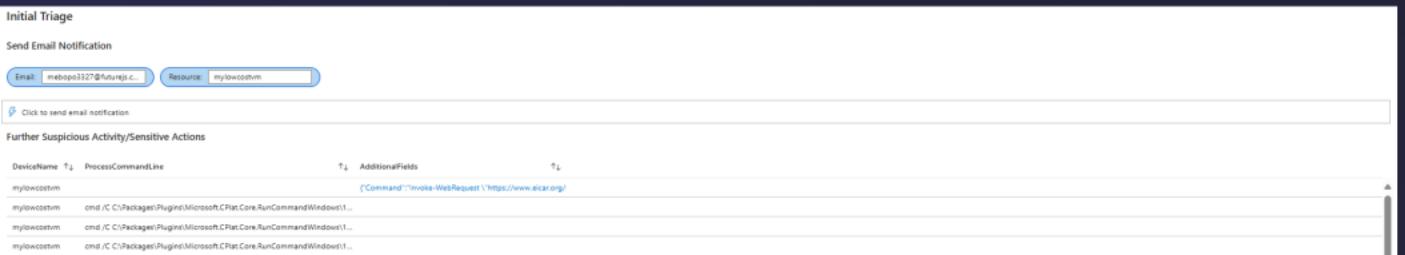
EXAMPLE 1

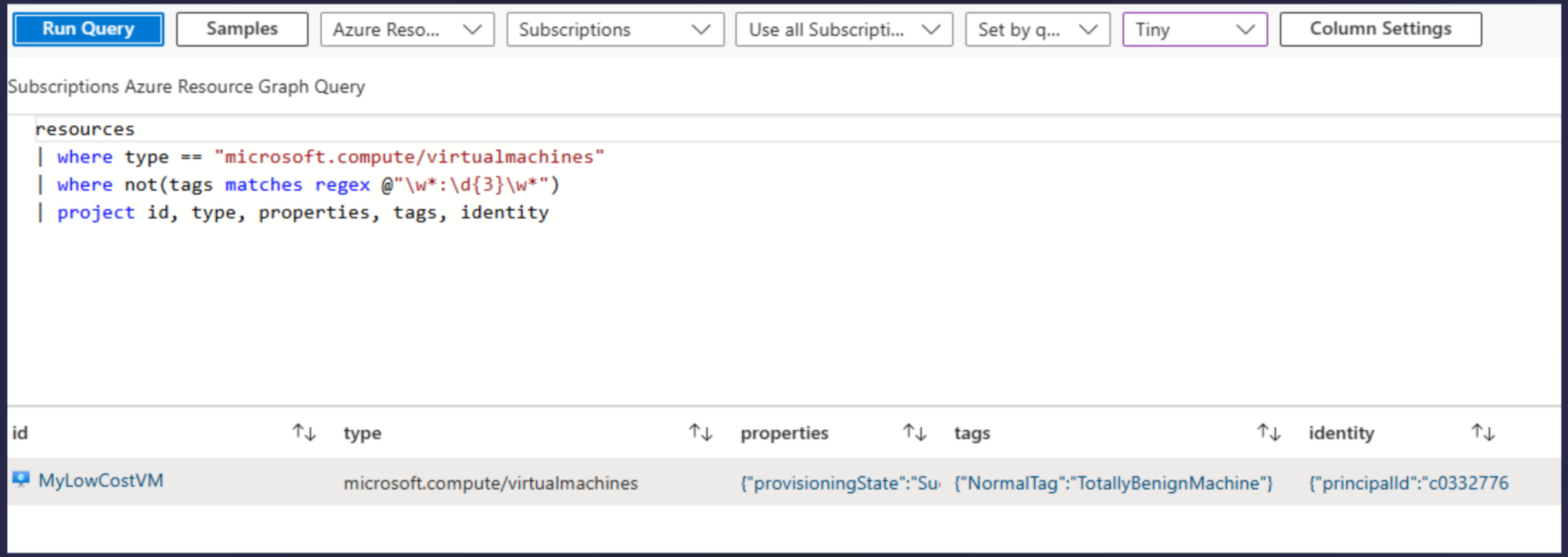



Request for your input
An Azure resource, mylowcostvm, was recently deployed with an anomalous tag. Please confirm the activity by clicking one of the buttons in this email.
Select one of the options below to respond
I recognize this activity
I do not recognize this activity

VMs with Anomalous Tags

id	type	properties	tags	identity
MyLowCostVM	microsoft.compute/virtualmachines	{"provisioningState":"Su	{"NormalTag":"TotallyBenignMachine"}	{"principalId":"c0332776




Run Query
Samples
Azure Reso...
Subscriptions
Use all Subscripti...
Set by q...
Tiny
Column Settings
Subscriptions Azure Resource Graph Query
resources
| where type == "microsoft.compute/virtualmachines"
| where not(tags matches regex @"\w*:\d{3}\w*")
| project id, type, properties, tags, identity
id
type
properties
tags
identity
MyLowCostVM
microsoft.compute/virtualmachines
{"provisioningState":"Su
{"NormalTag":"TotallyBenignMachine"}
{"principalId":"c0332776

Initial Triage

Send Email Notification

Email: mebopo3327@futurejs.c...

Resource: mylowcostvm

Click to send email notification

Further Suspicious Activity/Sensitive Actions

DeviceName	ProcessCommandLine	AdditionalFields
mylowcostvm		{"Command":"Invoke-WebRequest \"https://www.eicar.org/
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	"cmd.exe" /c echo " systeminfo && systeminfo && del "	{"DesktopName":"Winsta0\\Default"}
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	"ipconfig.exe" /all	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	

Alerts related to resource

TenantId	TimeGenerated	DisplayName	AlertName	AlertSeverity	Description	ProviderName	VendorNa...	VendorOriginalId	SystemAlertId
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:34:27.496 PM	'EICAR_Test_File' malware was detected	'EICAR_Test_File' malware was detected	Informational	Malware and unwanted software are undesirable applicat...	MDATP	Microsoft	485ee30e-3fa4-47ac-9acd-8a8e85fea452_1	8f4a1d17-5
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:37:16.943 PM	Suspicious Process Discovery	Suspicious Process Discovery	Low	A known tool or technique was used to gather informatio...	MDATP	Microsoft	db650d8d-47d9-4991-a8a8-d6f8a823e1a4_1	51318f56-7
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:37:16.953 PM	'EICAR_Test_File' malware was prevented	'EICAR_Test_File' malware was prevented	Informational	Malware and unwanted software are undesirable applicat...	MDATP	Microsoft	a7344cbd-0a98-4e88-8eff-43fc11bae3b9_1	50c19c92-7
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:43:20.769 PM	'EICAR_Test_File' malware was prevented	'EICAR_Test_File' malware was prevented	Informational	Malware and unwanted software are undesirable applicat...	MDATP	Microsoft	a7344cbd-0a98-4e88-8eff-43fc11bae3b9_1	50c19c92-7
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:25:18.041 PM	'EICAR_Test_File' malware was detected	'EICAR_Test_File' malware was detected	Informational	Malware and unwanted software are undesirable applicat...	MDATP	Microsoft	485ee30e-3fa4-47ac-9acd-8a8e85fea452_1	8f4a1d17-5

Email: Enter value

Resource: mylowcostvm2

Click to send email notification

Further Suspicious Activity/Sensitive Actions

The query returned no results.

Alerts related to resource

The query returned no results.

Edit | Help | Auto refresh: Off

Initial Triage

Send Email Notification

Email: gayip56051@futurejs.com

Resource: mylowcostvm

Click to send email notification

Further Suspicious Activity/Sensitive Actions

DeviceName	ProcessCommandLine	AdditionalFields
mylowcostvm		{"Command":"Invoke-WebRequest \"https://www.eicar.org/
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	"cmd.exe" /c echo " systeminfo && systeminfo && del "	{"DesktopName":"Winsta0\\Default"}
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	
mylowcostvm	"ipconfig.exe" /all	
mylowcostvm	cmd /C C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1...	

Alerts related to resource

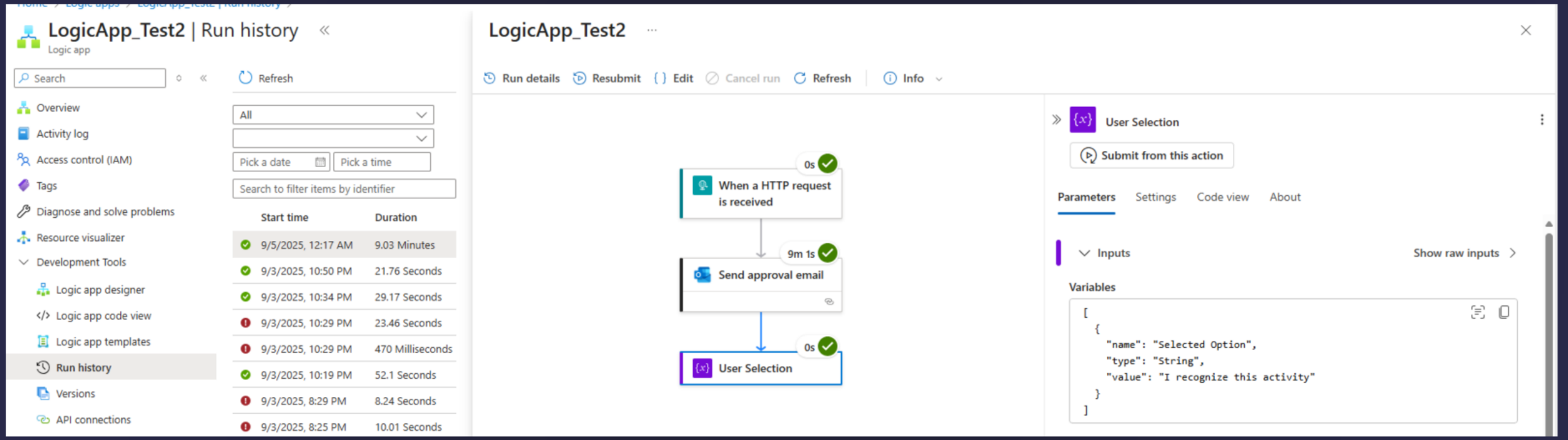
TenantId	TimeGenerated	DisplayName	AlertName	AlertSeverity	Description	ProviderName
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:34:27.496 PM	'EICAR_Test_File' malware was detected	'EICAR_Test_File' malware was detected	Informational	Malware and unwanted software are undesirable applicat...	MDATP
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:37:16.943 PM	Suspicious Process Discovery	Suspicious Process Discovery	Low	A known tool or technique was used to gather informatio...	MDATP
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:37:16.953 PM	'EICAR_Test_File' malware was prevented	'EICAR_Test_File' malware was prevented	Informational	Malware and unwanted software are undesirable applicat...	MDATP
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:43:20.769 PM	'EICAR_Test_File' malware was prevented	'EICAR_Test_File' malware was prevented	Informational	Malware and unwanted software are undesirable applicat...	MDATP
a9663546-fdba-4420-93f8-50070cc04eec	9/1/2025, 10:25:18.041 PM	'EICAR_Test_File' malware was detected	'EICAR_Test_File' malware was detected	Informational	Malware and unwanted software are undesirable applicat...	MDATP

⚠ This action is going to modify one or more Azure resources.

The author of this template has not provided a description for this action, so verify the request details below before continuing.

View request details

Run ARM action | Cancel


LogicApp_Test2 | Run history
Logic app
Search
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Development Tools
Logic app designer
Logic app code view
Logic app templates
Run history
Versions
API connections
All
Pick a date
Pick a time
Search to filter items by identifier
Start time
Duration
9/5/2025, 12:17 AM 9.03 Minutes
9/3/2025, 10:50 PM 21.76 Seconds
9/3/2025, 10:34 PM 29.17 Seconds
9/3/2025, 10:29 PM 23.46 Seconds
9/3/2025, 10:29 PM 470 Milliseconds
9/3/2025, 10:19 PM 52.1 Seconds
9/3/2025, 8:29 PM 8.24 Seconds
9/3/2025, 8:25 PM 10.01 Seconds
LogicApp_Test2
Run details
Resubmit
Edit
Cancel run
Refresh
Info
0s
When a HTTP request is received
9m 1s
Send approval email
0s
User Selection
User Selection
Submit from this action
Parameters
Settings
Code view
About
Inputs
Show raw inputs
Variables
[
{
"name": "Selected Option",
"type": "String",
"value": "I recognize this activity"
}
]

Request for your input

An Azure resource, mylowcostvm, was recently deployed with an anomalous tag. Please confirm the activity by clicking one of the buttons in this email.

Select one of the options below to respond

I recognize this activity | I do not recognize this activity

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

API Explorer

Use the API explorer to test Microsoft Defender for Endpoint capabilities. Use the sample queries to get started.

Run query | PATCH | https://api-us3.securitycenter.microsoft.com/api/alerts/daeb4760a2-09fa-421a-841c-89ec1552cd77_1

```
1  {
2      "comment": "This is recognized by the user"
3  }
```

Success - Status code 200, 540ms

Response body:


```
1  {
2    "@odata.context": "https://api-us3.securitycenter.microsoft.com/api/$metadata#Alerts/$entity",
3    "id": "daeb4760a2-09fa-421a-841c-89ec1552cd77_1",
4    "incidentId": 1,
5    "investigationId": 1,
6    "assignedTo": "API-Automated Investigation and Response",
```

'EICAR_Test_File' malware was prevented

Informational | Prevented | Resolved

Manage alert | See in timeline | Tune alert | ...

MyLowCostVM | Medium | Low

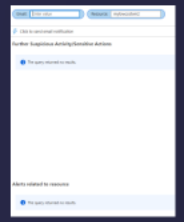
Comments & history

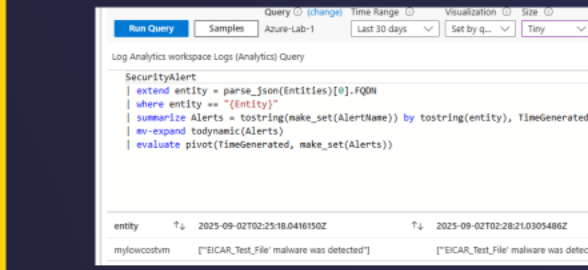
Add a new comment

Save

API Action
This is recognized by the user
Sep 3, 2025 11:02:29 PM

EXAMPLE 2




Query (change)
Time Range
Visualization
Size
Run Query
Samples
Azure-Lab-1
Last 30 days
Set by q...
Tiny
Log Analytics workspace Logs (Analytics) Query
SecurityAlert
| extend entity = parse_json(Entities)[0].FQDN
| where entity == "{Entity}"
| summarize Alerts = tostring(make_set(AlertName)) by tostring(entity), TimeGenerated
| mv-expand todynamic(Alerts)
| evaluate pivot(TimeGenerated, make_set(Alerts))
entity
2025-09-02T02:25:18.0416150Z
2025-09-02T02:28:21.0305486Z
mylowcostvm
["EICAR_Test_File' malware was detected"]
["EICAR_Test_File' malware was detec

Workbook to Logic App

Entity: mylowcostvm

Click to add item to Watchlist

Watchlist

entity	2025-09-02T02:25:18.0416150Z	2025-09-02T02:28:21.0305486Z	2025-09-02T02:34:27.4964434Z	2025-09-02T02:37:16.9438697Z	2025-09-02T02:37:16.9531702Z	2025-09-0
mylowcostvm	["'EICAR_Test_File' malware was detected"]	["'EICAR_Test_File' malware was detected"]	["'EICAR_Test_File' malware was detected"]	["Suspicious Process Discovery"]	["'EICAR_Test_File' malware was prevented"]	["'EICAR_Te

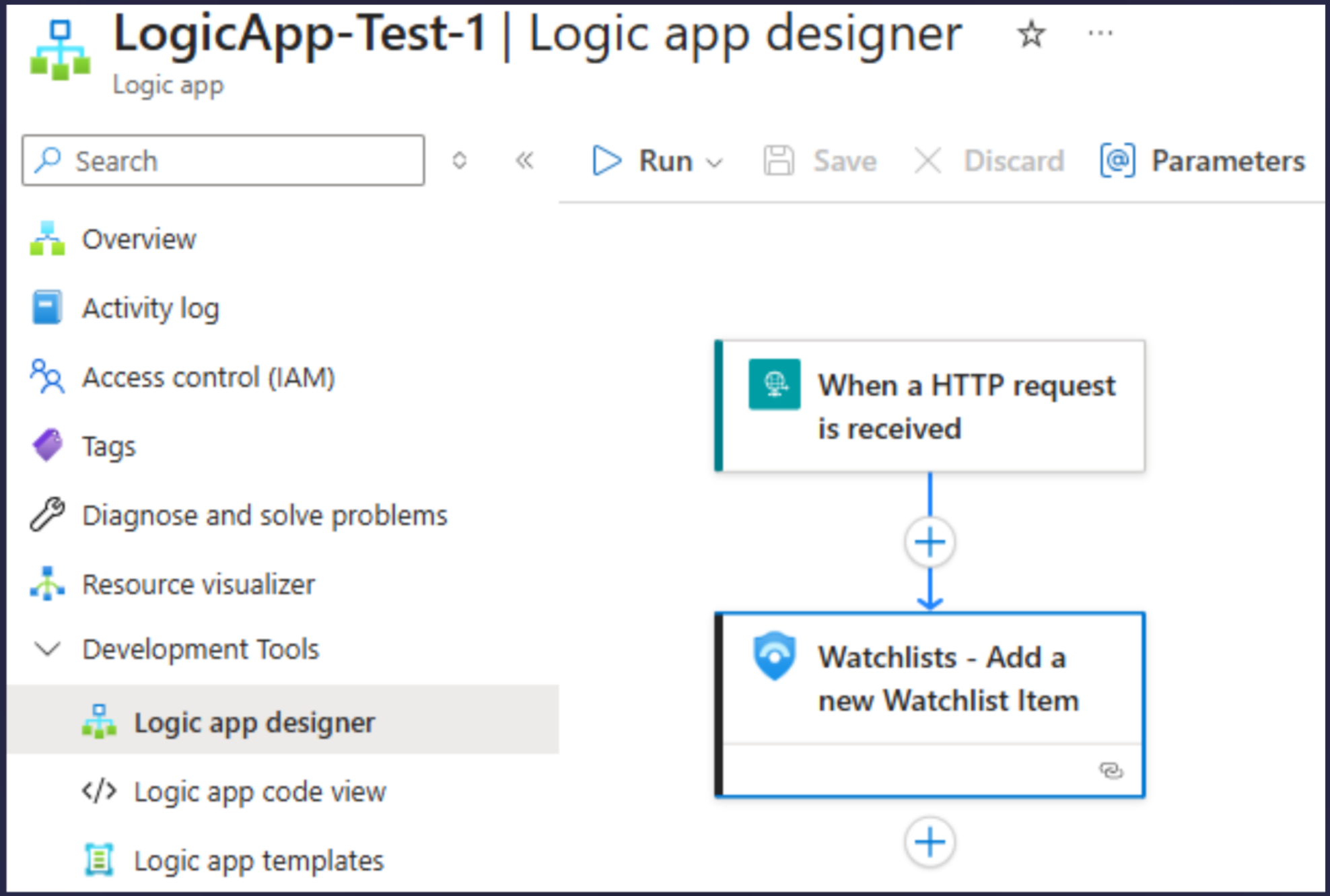
Query (change) | Time Range | Visualization | Size

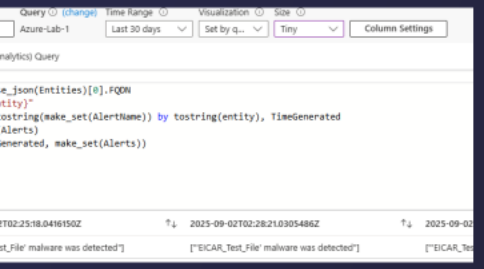
Run Query | Samples | Azure-Lab-1 | Last 30 days | Set by q... | Tiny | Column Settings

Log Analytics workspace Logs (Analytics) Query

```
SecurityAlert
| extend entity = parse_json(Entities)[0].FQDN
| where entity == "{Entity}"
| summarize Alerts = tostring(make_set(AlertName)) by tostring(entity), TimeGenerated
| mv-expand todynamic(Alerts)
| evaluate pivot(TimeGenerated, make_set(Alerts))
```

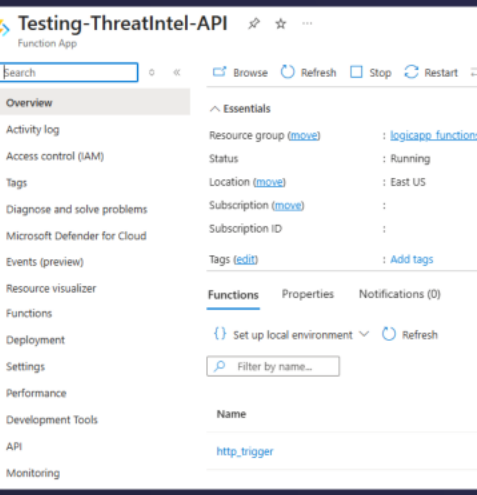
entity	2025-09-02T02:25:18.0416150Z	2025-09-02T02:28:21.0305486Z	2025-09-02
mylowcostvm	["'EICAR_Test_File' malware was detected"]	["'EICAR_Test_File' malware was detected"]	["'EICAR_Tes

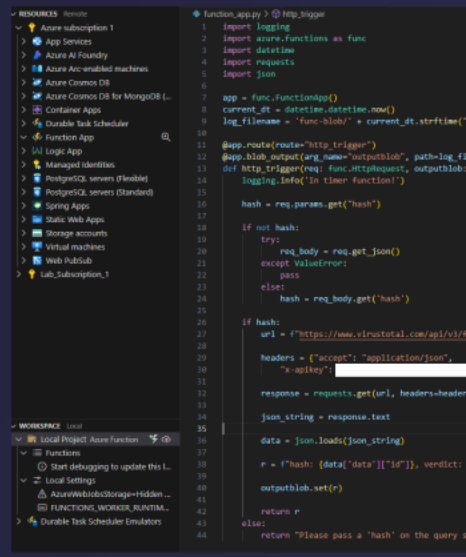

LogicApp-Test-1 | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Development Tools
Logic app designer
Logic app code view
Logic app templates
When a HTTP request is received
Watchlists - Add a new Watchlist Item


Query (change)
Time Range
Visualization
Size
Azure-Lab-1
Last 30 days
Set by q...
Tiny
Column Settings
nalytics) Query
e_json(Entities)[0].FQDN
tity)"
ostring(make_set(AlertName)) by tostring(entity), TimeGenerated
Alerts)
enerated, make_set(Alerts))
2T02:25:18.0416150Z
2025-09-02T02:28:21.0305486Z
2025-09-02
st_File' malware was detected"]
["EICAR_Test_File' malware was detected"]


METRICS
WE'RE GONNA NEED...
MORE METRICS

EXAMPLE 3


Testing-ThreatIntel-API
Function App
Search
Browse
Refresh
Stop
Restart
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Resource visualizer
Functions
Deployment
Settings
Performance
Development Tools
API
Monitoring
Essentials
Resource group (move) : logicapp_function
Status : Running
Location (move) : East US
Subscription (move) :
Subscription ID :
Tags (edit) : Add tags
Functions
Properties
Notifications (0)
Set up local environment
Refresh
Filter by name...
Name
http_trigger


RESOURCES
Azure subscription 1
App Services
Azure AI Foundry
Azure Arc-enabled machines
Azure Cosmos DB
Azure Cosmos DB for MongoDB (...
Container Apps
Durable Task Scheduler
Function App
Logic App
Managed Identities
PostgreSQL servers (Flexible)
PostgreSQL servers (Standard)
Spring Apps
Static Web Apps
Storage accounts
Virtual machines
Web PubSub
Lab_Subscription_1
WORKSPACE
Local Project: Azure Function
Functions
Start debugging to update this l...
Local Settings
AzureWebJobsStorage=Hidden ...
FUNCTIONS_WORKER_RUNTIM...
Durable Task Scheduler Emulators
function_app.py
http_trigger
import logging
import azure.functions as func
import datetime
import requests
import json
app = func.FunctionApp()
current_dt = datetime.datetime.now()
log_filename = 'func-blob/' + current_dt.strftime(
@app.route(route="http_trigger")
@app.blob_output(arg_name="outputblob", path=log_f
def http_trigger(req: func.HttpRequest, outputblob:
logging.info('In timer function!')
hash = req.params.get("hash")
if not hash:
try:
req_body = req.get_json()
except ValueError:
pass
else:
hash = req_body.get('hash')
if hash:
url = f"https://www.virustotal.com/api/v3/
headers = {"accept": "application/json",
"x-apikey":
response = requests.get(url, headers=header
json_string = response.text
data = json.loads(json_string)
r = f"hash: {data['data']['id']}, verdict:
outputblob.set(r)
return r
else:
return "Please pass a 'hash' on the query

Workbook to Azure Function

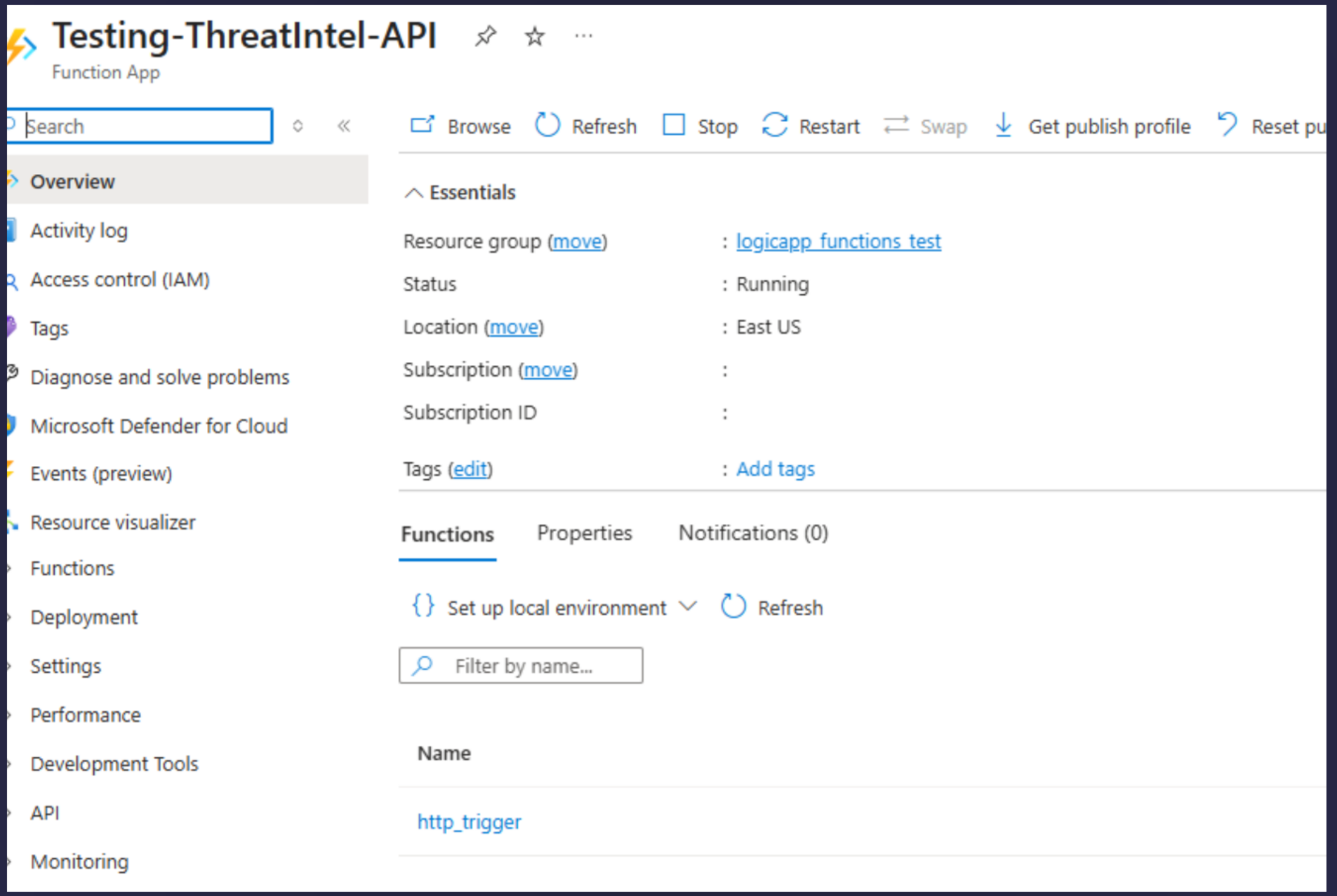
hash: 178ba564b39bd07577e...

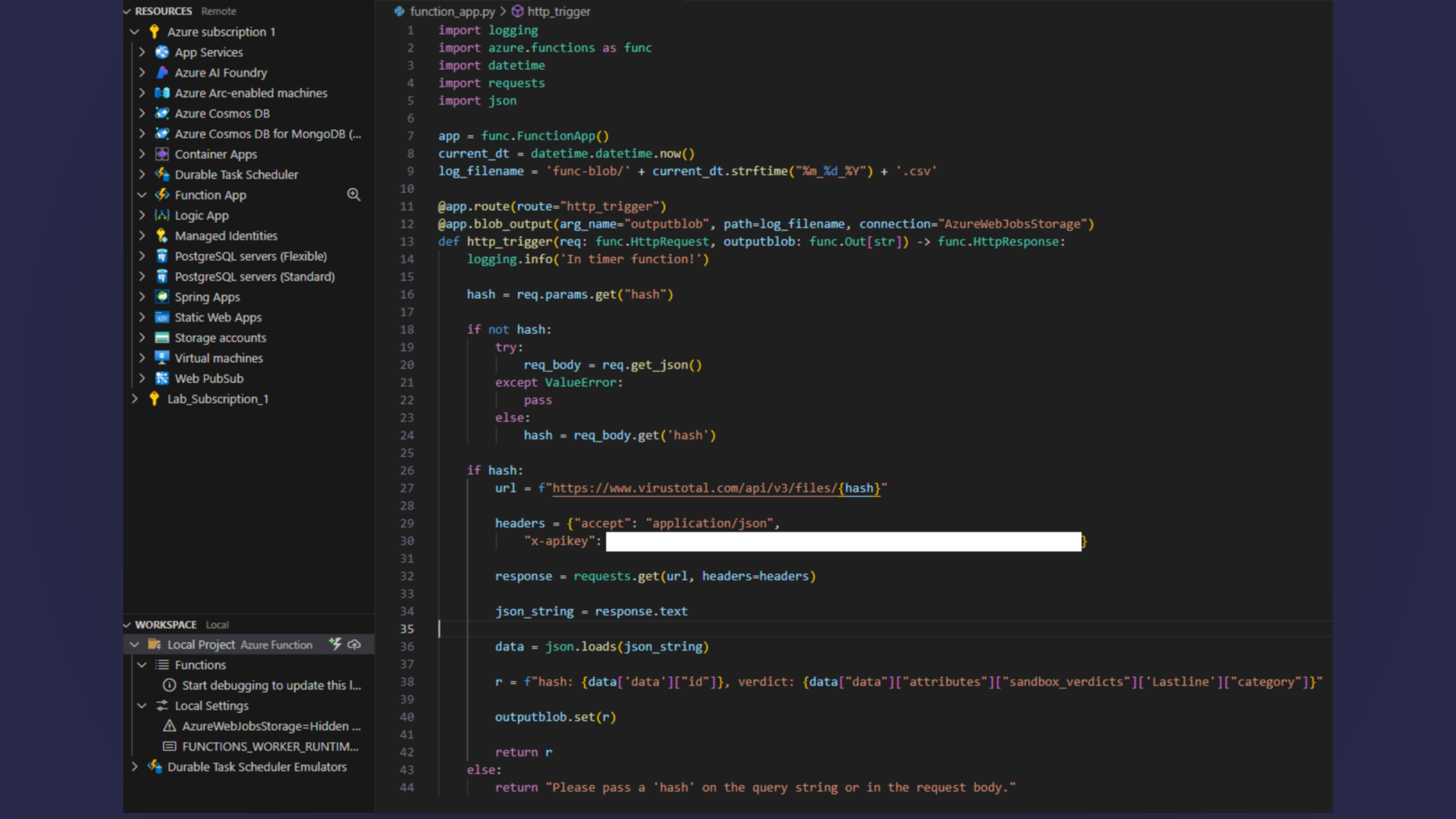
Press the refresh button to the left to submit new hash

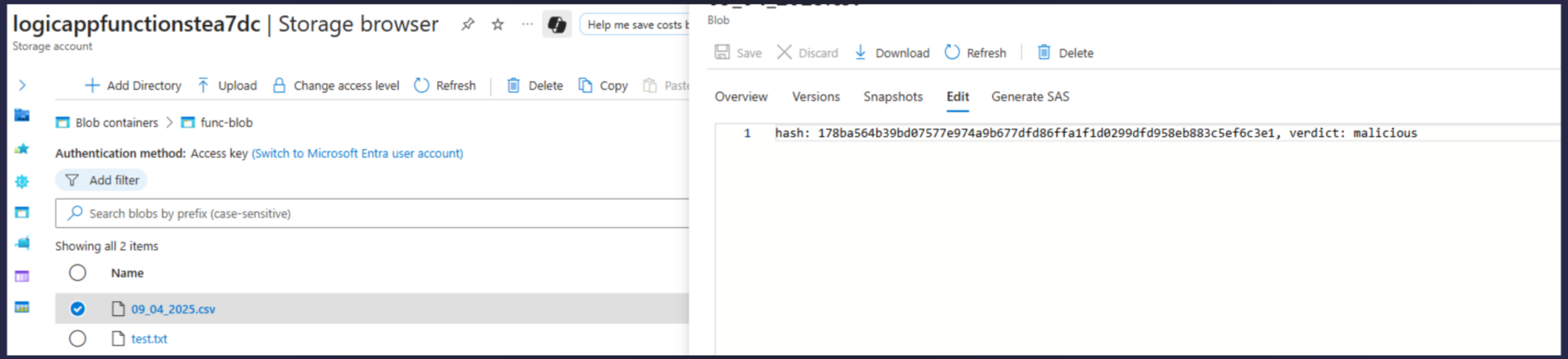
Column
hash: 178ba564b39bd07577e974a9b677dfd86ffa1f1d0299dfd958eb883c5ef6c3e1, verdict: malicious

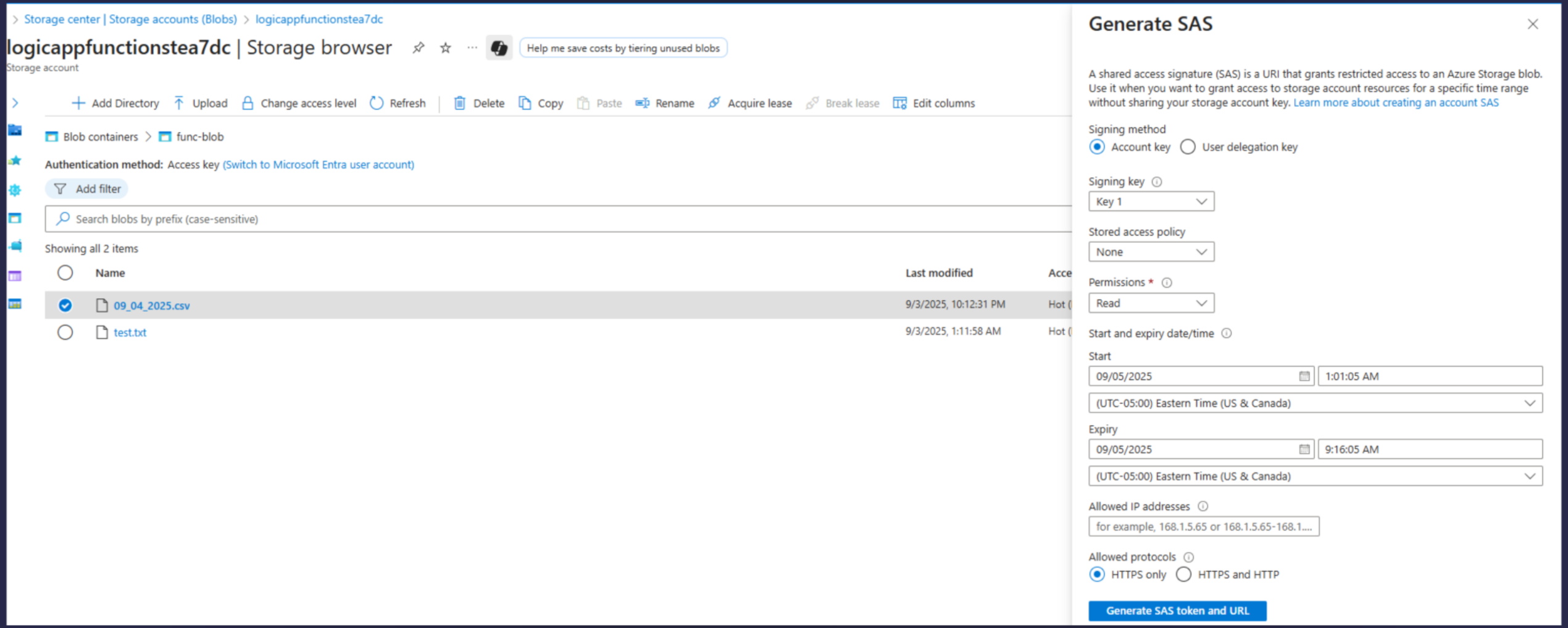
Storage Container

Column
hash: 178ba564b39bd07577e974a9b677dfd86ffa1f1d0299dfd958eb883c5ef6c3e1, verdict: malicious


Testing-ThreatIntel-API
Function App
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Resource visualizer
Functions
Deployment
Settings
Performance
Development Tools
API
Monitoring
Browse
Refresh
Stop
Restart
Swap
Get publish profile
Reset pu
Essentials
Resource group (move) : logicapp_functions_test
Status : Running
Location (move) : East US
Subscription (move) :
Subscription ID :
Tags (edit) : Add tags
Functions
Properties
Notifications (0)
Set up local environment
Refresh
Filter by name...
Name
http_trigger


RESOURCES Remote
Azure subscription 1
App Services
Azure AI Foundry
Azure Arc-enabled machines
Azure Cosmos DB
Azure Cosmos DB for MongoDB (...
Container Apps
Durable Task Scheduler
Function App
Logic App
Managed Identities
PostgreSQL servers (Flexible)
PostgreSQL servers (Standard)
Spring Apps
Static Web Apps
Storage accounts
Virtual machines
Web PubSub
Lab_Subscription_1
WORKSPACE Local
Local Project Azure Function
Functions
Start debugging to update this l...
Local Settings
AzureWebJobsStorage=Hidden ...
FUNCTIONS_WORKER_RUNTIM...
Durable Task Scheduler Emulators
function_app.py > http_trigger
import logging
import azure.functions as func
import datetime
import requests
import json
app = func.FunctionApp()
current_dt = datetime.datetime.now()
log_filename = 'func-blob/' + current_dt.strftime("%m_%d_%Y") + '.csv'
@app.route(route="http_trigger")
@app.blob_output(arg_name="outputblob", path=log_filename, connection="AzureWebJobsStorage")
def http_trigger(req: func.HttpRequest, outputblob: func.Out[str]) -> func.HttpResponse:
logging.info('In timer function!')
hash = req.params.get("hash")
if not hash:
try:
req_body = req.get_json()
except ValueError:
pass
else:
hash = req_body.get('hash')
if hash:
url = f"https://www.virustotal.com/api/v3/files/{hash}"
headers = {"accept": "application/json",
"x-apikey":
response = requests.get(url, headers=headers)
json_string = response.text
data = json.loads(json_string)
r = f"hash: {data['data']["id"]}, verdict: {data["data"]["attributes"]["sandbox_verdicts"]['Lastline']["category"]}"
outputblob.set(r)
return r
else:
return "Please pass a 'hash' on the query string or in the request body."


logicappfunctionstea7dc | Storage browser
Storage account
Help me save costs b
Add Directory
Upload
Change access level
Refresh
Delete
Copy
Blob containers
func-blob
Authentication method: Access key (Switch to Microsoft Entra user account)
Add filter
Search blobs by prefix (case-sensitive)
Showing all 2 items
Name
09_04_2025.csv
test.txt
Blob
Save
Discard
Download
Refresh
Delete
Overview
Versions
Snapshots
Edit
Generate SAS
1
hash: 178ba564b39bd07577e974a9b677dfd86ffa1f1d0299dfd958eb883c5ef6c3e1, verdict: malicious


Storage center | Storage accounts (Blobs) > logicappfunctionstea7dc
logicappfunctionstea7dc | Storage browser
Storage account
Help me save costs by tiering unused blobs
Add Directory
Upload
Change access level
Refresh
Delete
Copy
Paste
Rename
Acquire lease
Break lease
Edit columns
Blob containers > func-blob
Authentication method: Access key (Switch to Microsoft Entra user account)
Add filter
Search blobs by prefix (case-sensitive)
Showing all 2 items
Name
Last modified
09_04_2025.csv
9/3/2025, 10:12:31 PM
test.txt
9/3/2025, 1:11:58 AM
Generate SAS
A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. Learn more about creating an account SAS
Signing method
Account key
User delegation key
Signing key
Key 1
Stored access policy
None
Permissions *
Read
Start and expiry date/time
Start
09/05/2025
1:01:05 AM
(UTC-05:00) Eastern Time (US & Canada)
Expiry
09/05/2025
9:16:05 AM
(UTC-05:00) Eastern Time (US & Canada)
Allowed IP addresses
for example, 168.1.5.65 or 168.1.5.65-168.1....
Allowed protocols
HTTPS only
HTTPS and HTTP
Generate SAS token and URL

Query (change) Http Method Size

Run Query Custom Endpoint GET Tiny Column Settings

URL

https://logicappfunctio...

Custom Endpoint Query

URL Parameters Headers Result Settings

URL PARAMETER

Column

hash: 178ba564b39bd07577e974a9b677dfd86ffa1f1d0299dfd958eb883c5ef6c3e1, verdict: malicious

FIN

Metrics

- % of rollbacks
- % of alerts resolved by the end user
- % of reports that become alerts/ notifications

Detection Engineering and Automation in Security Operations

Sentinel, Logic Apps, Workbooks, Functions, AND MORE!

INTRO & IDEAS





EXAMPLE 1


EXAMPLE 2




EXAMPLE 3