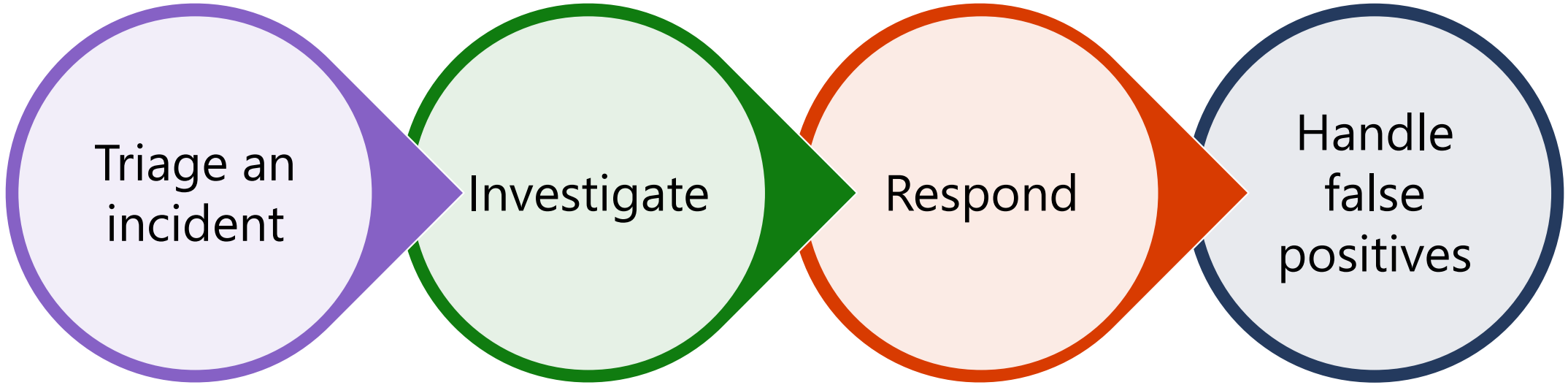
Microsoft

A Day in the life of an Azure Sentinel Analyst

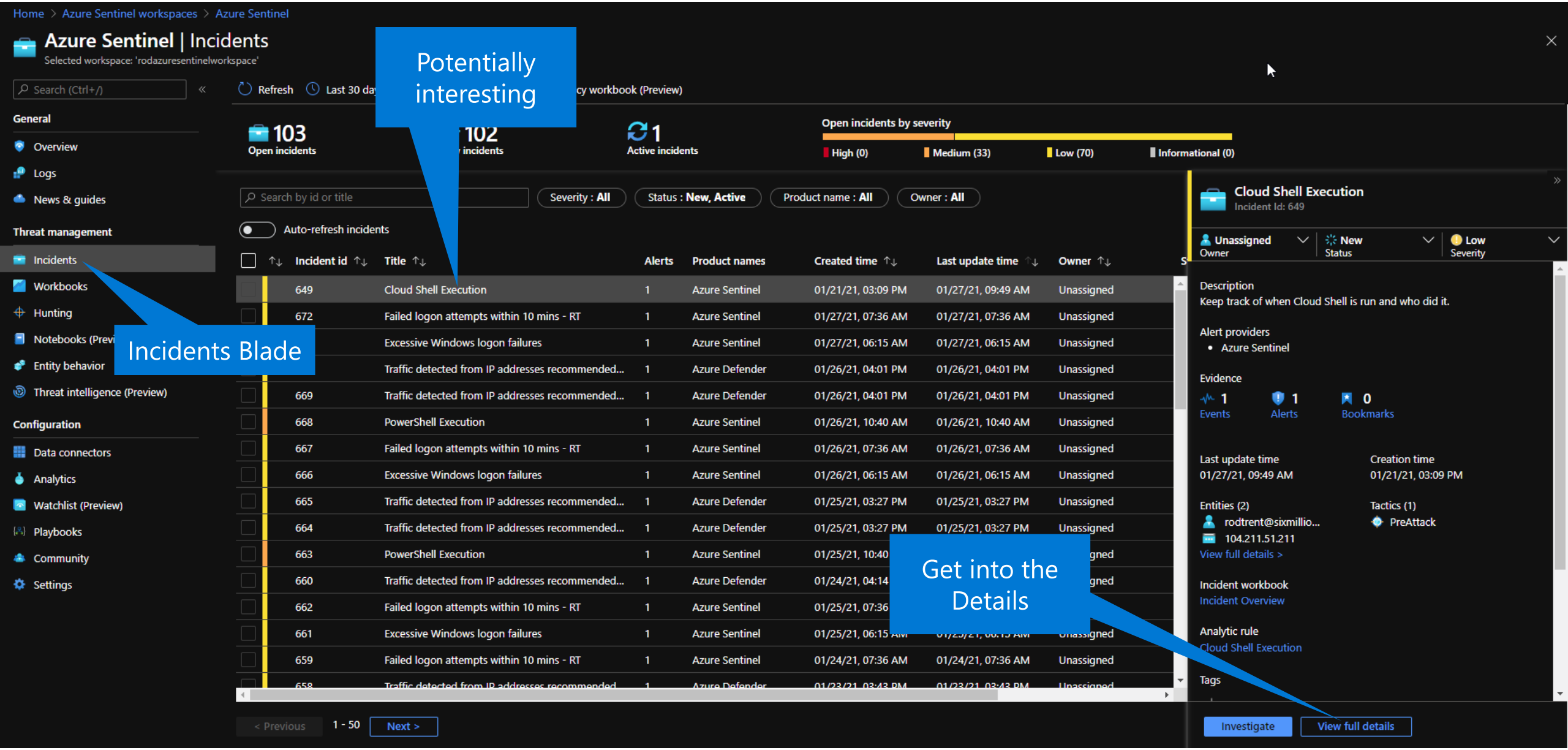
Rod Trent
Cybersecurity CE
Azure Sentinel Global SME

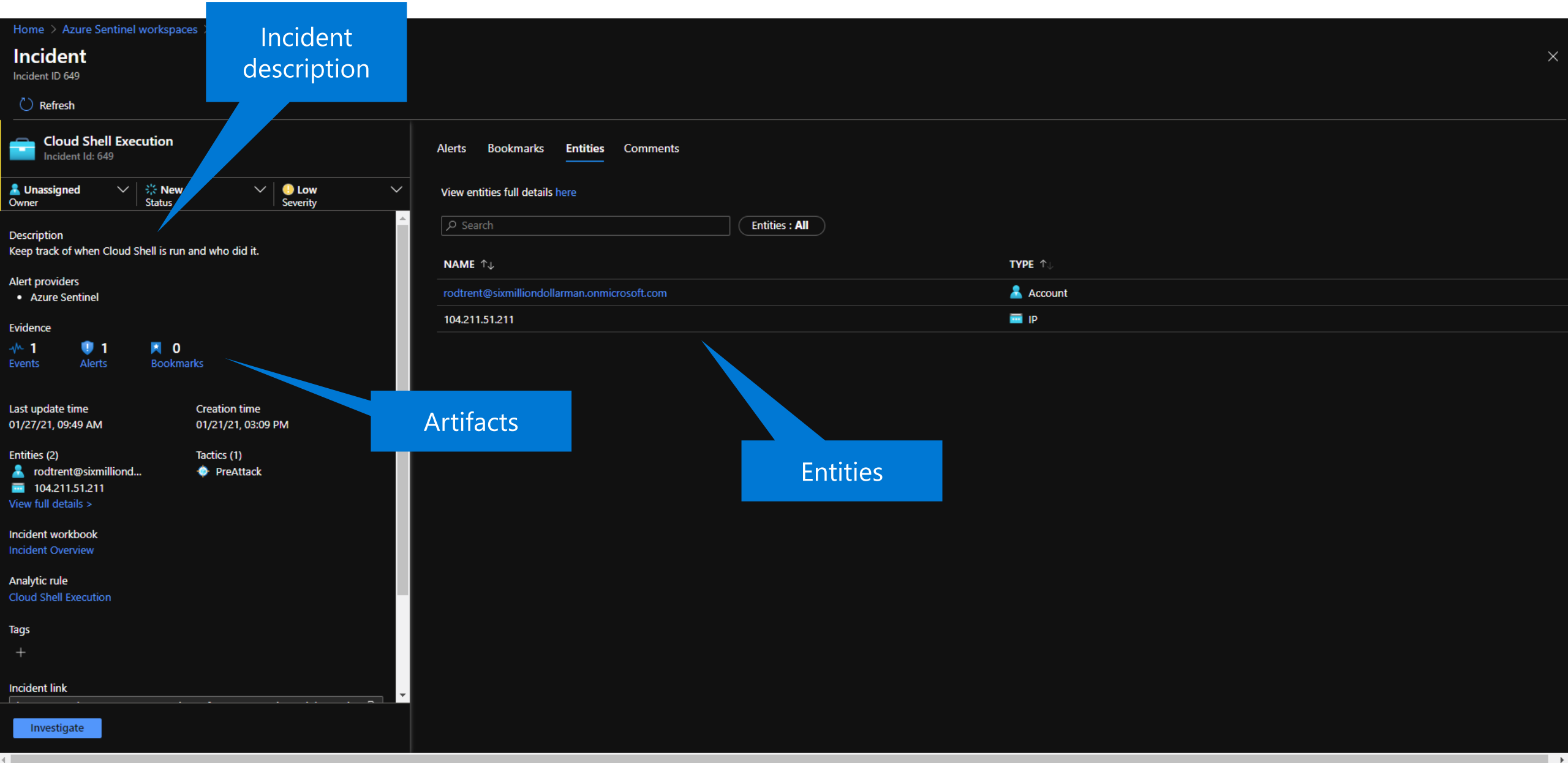
The SOC incident workflow

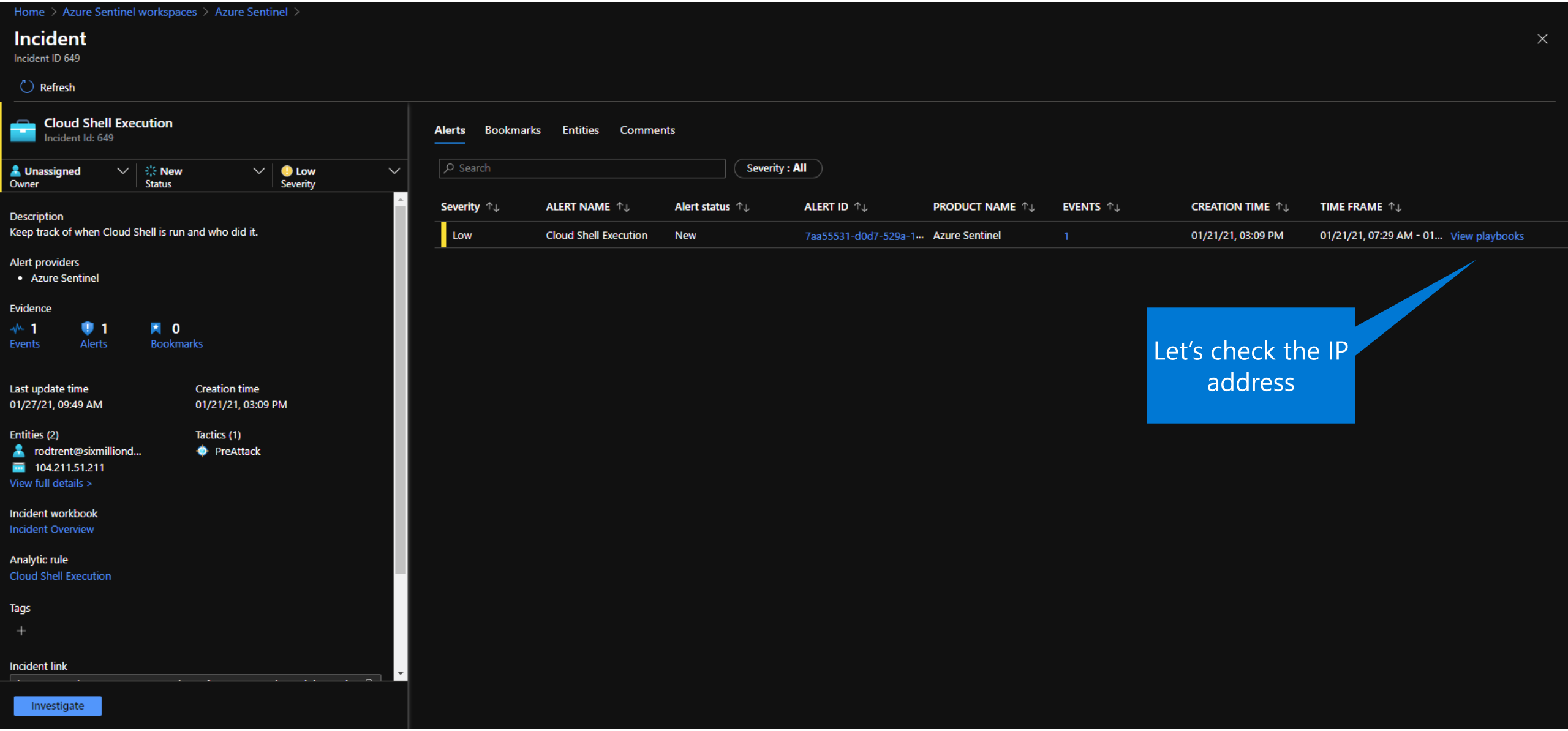


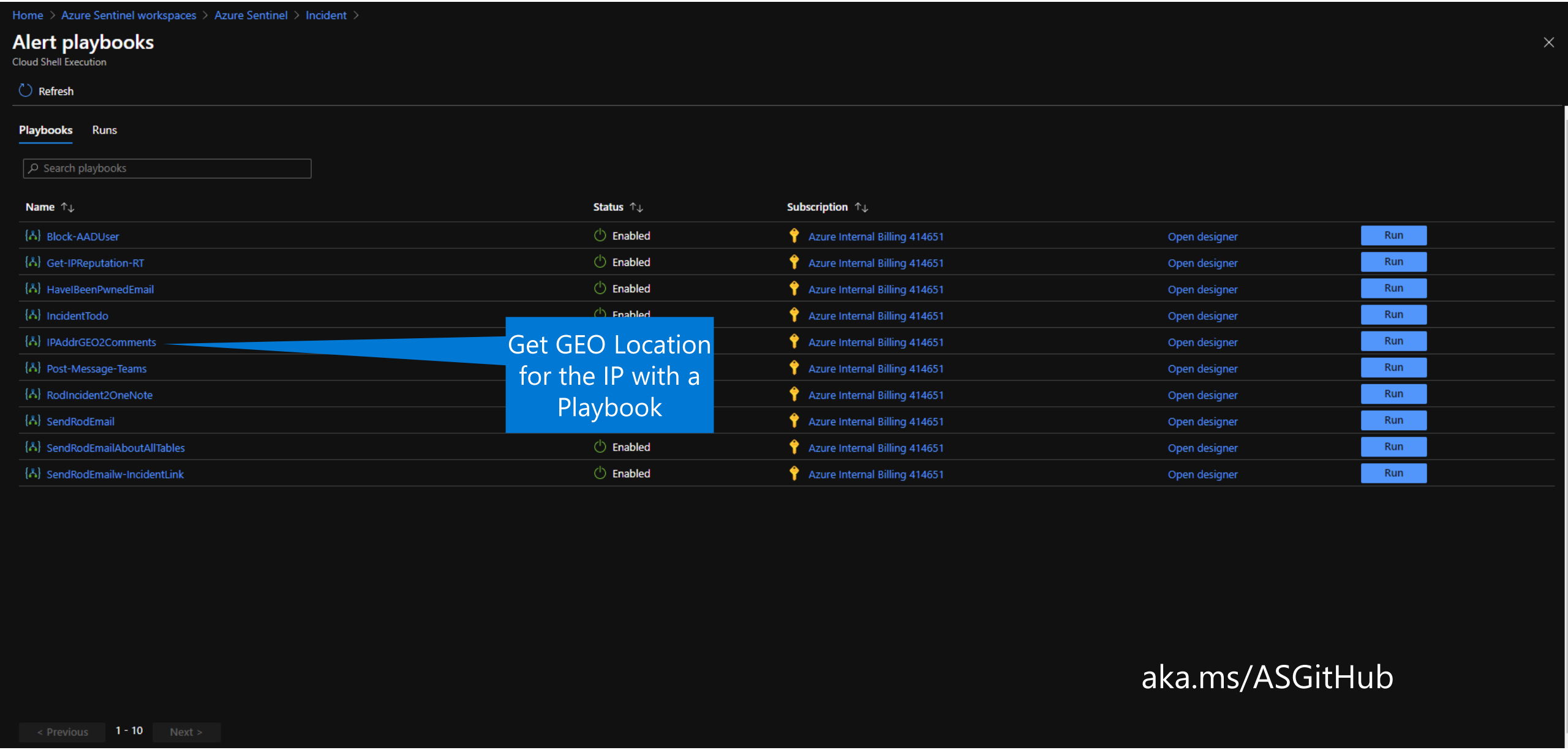
Casting Call

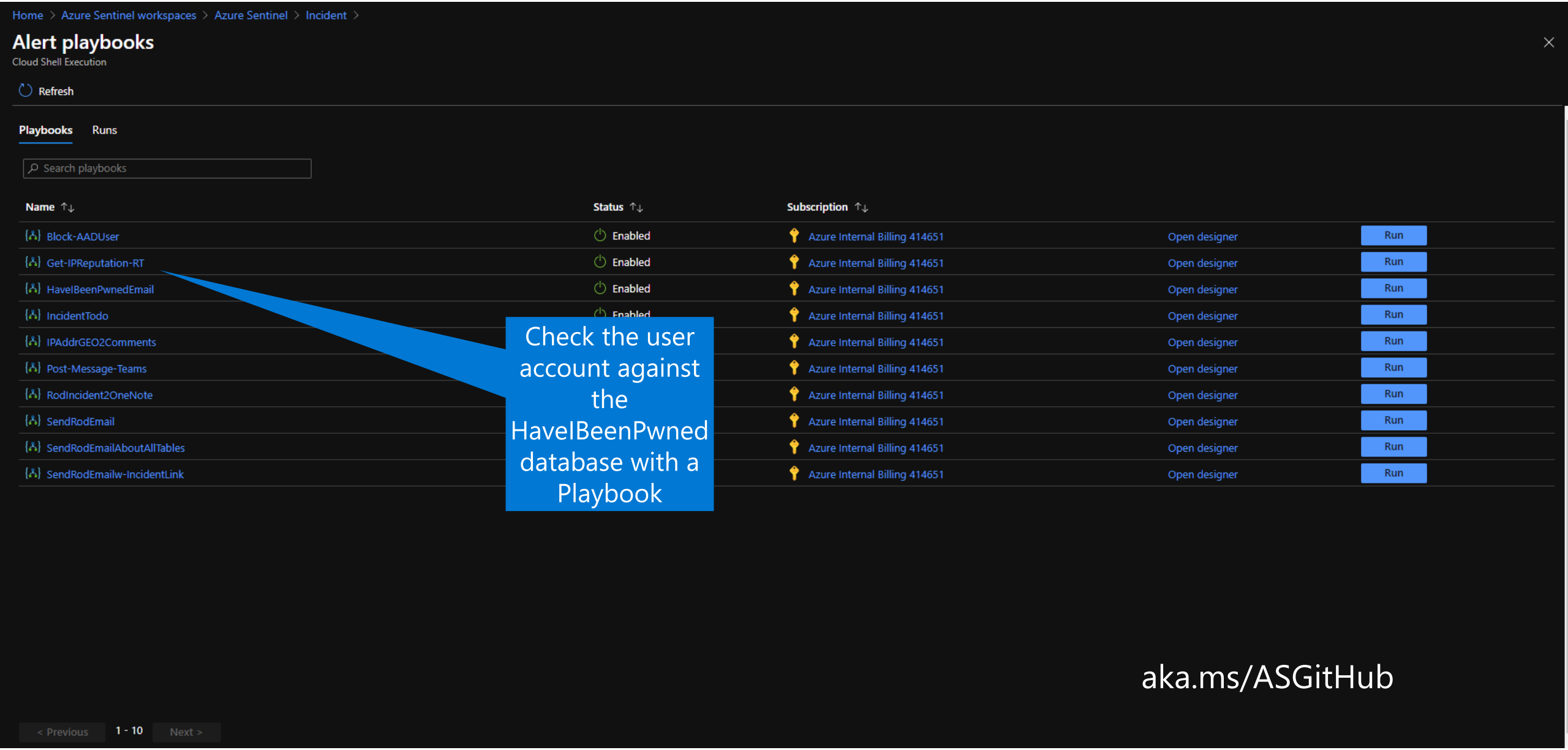
Action!

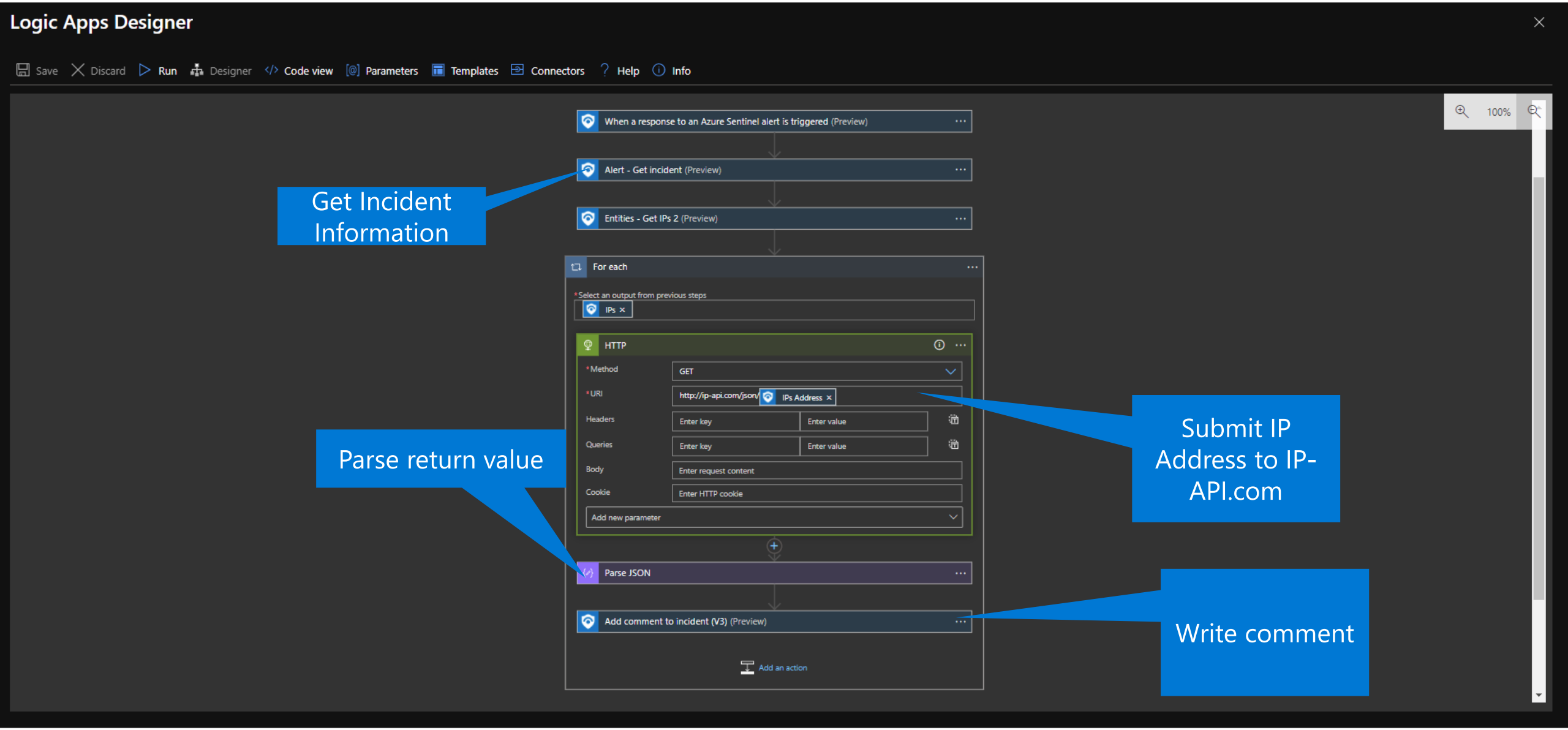


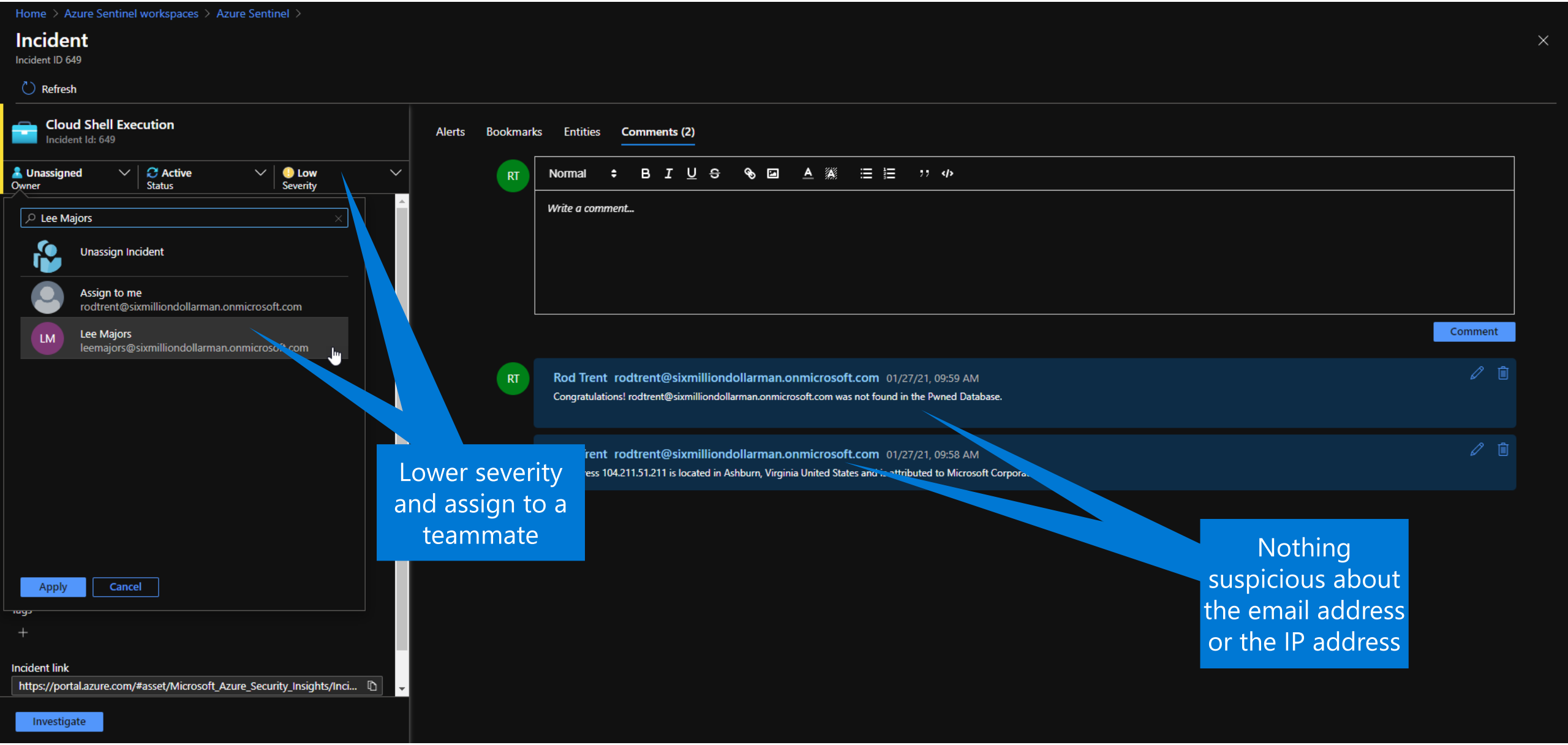


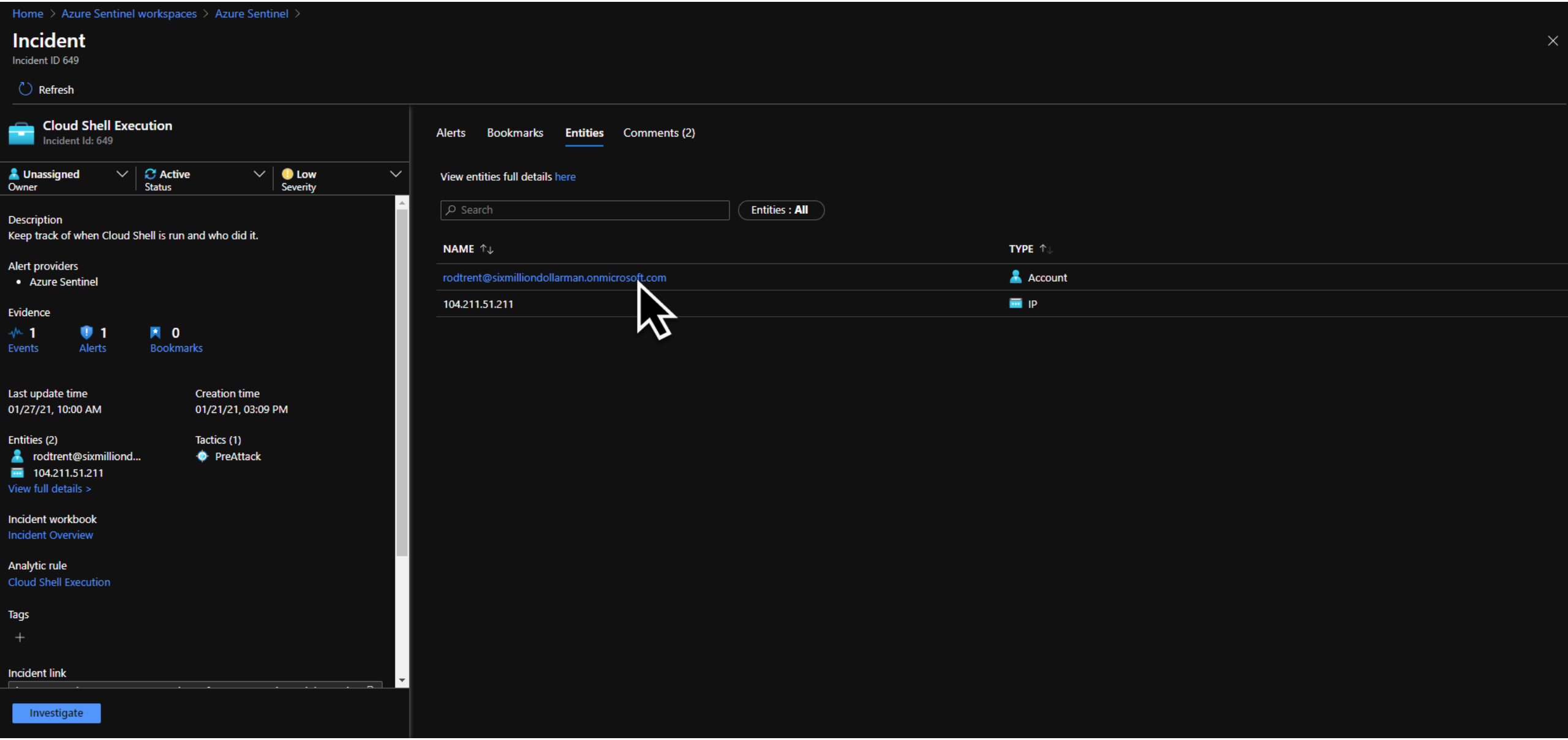


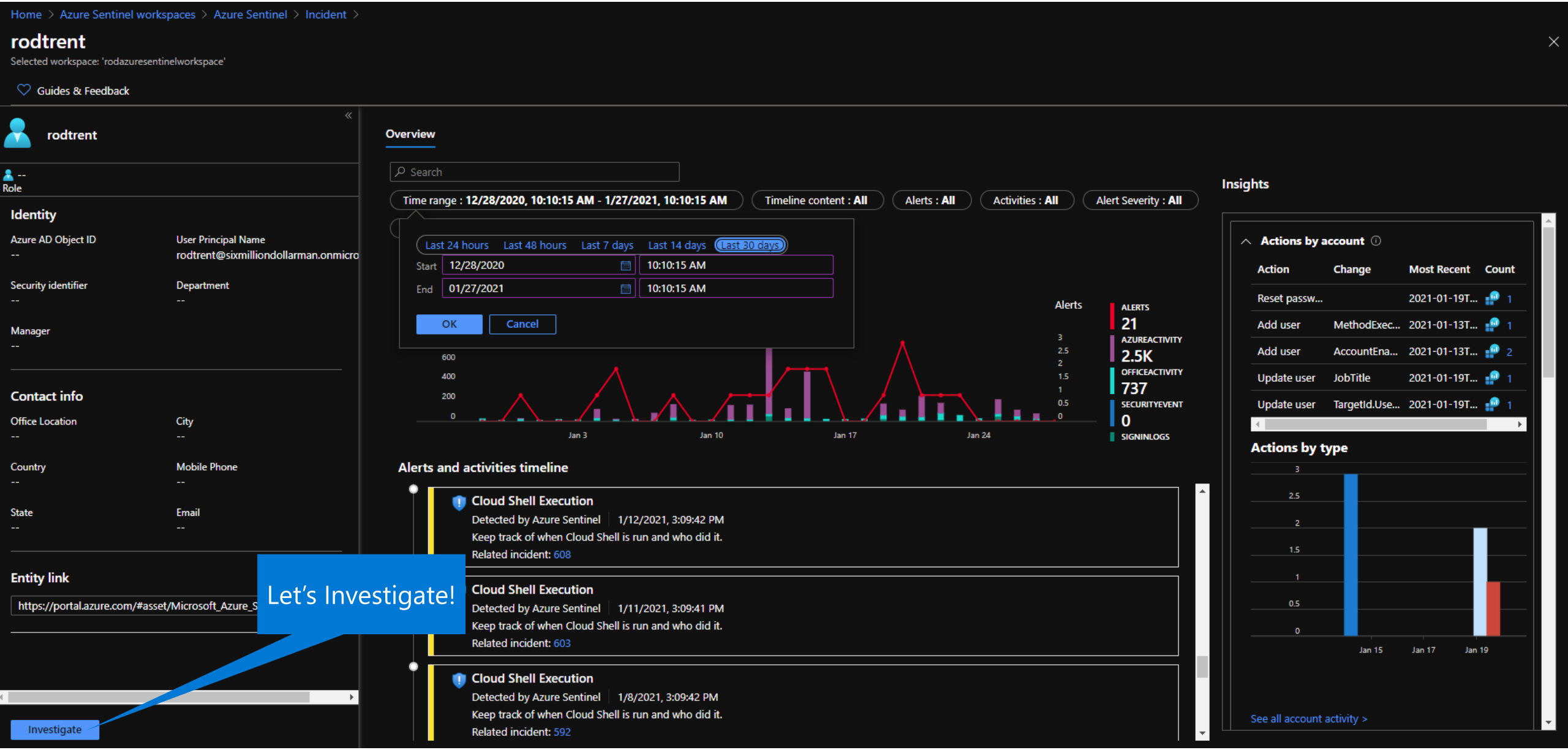


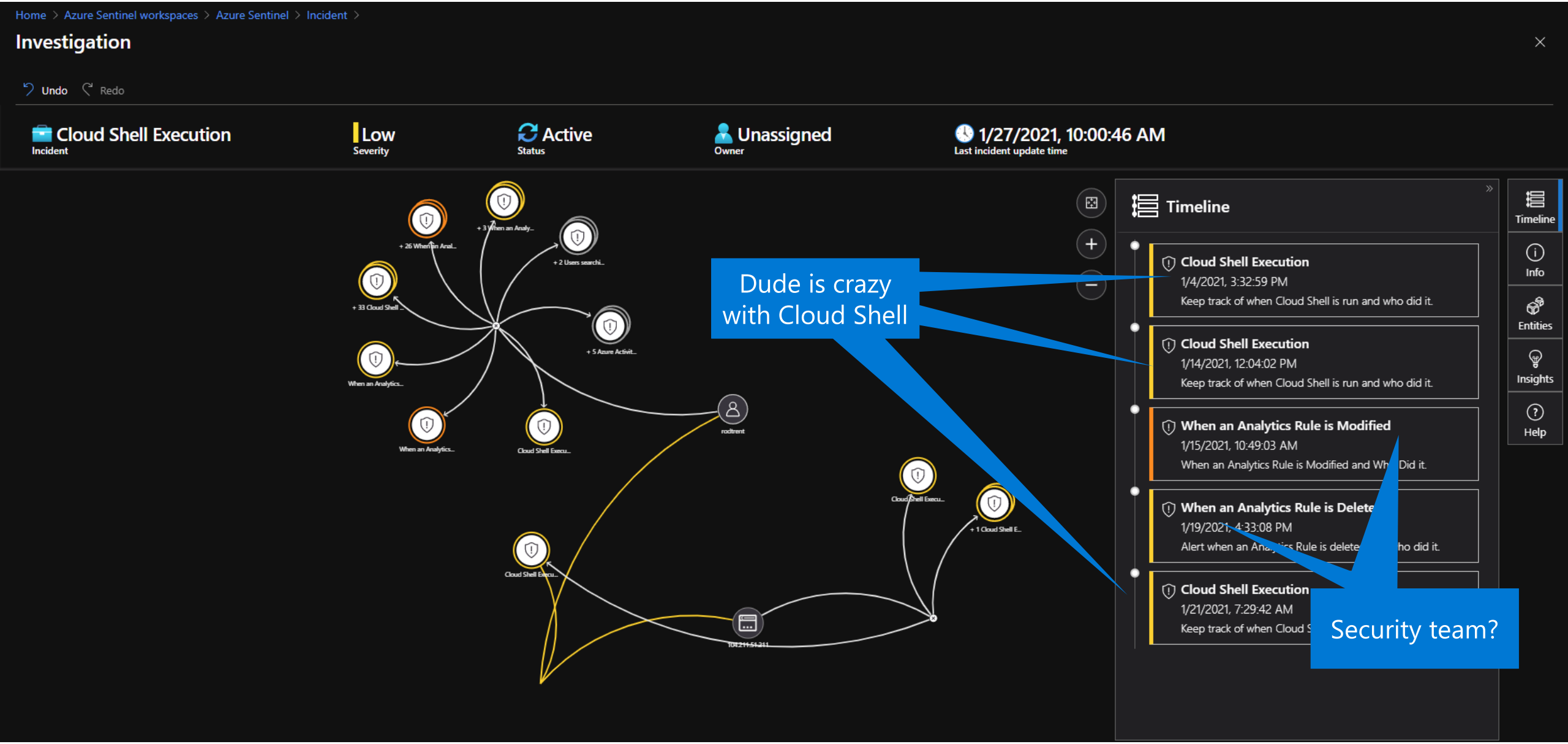












Action!

User And Entity Behavior Analytics - rodazuresentinelworkspace

rodazuresentinelworkspace

Edit

User and Entity Behavior Analytics

Welcome to the User and Entity Behavior Analytics workbook. The workbook provides a guided investigation for entities based on open incidents, alerts and anomalies identified by the UEBA engine.

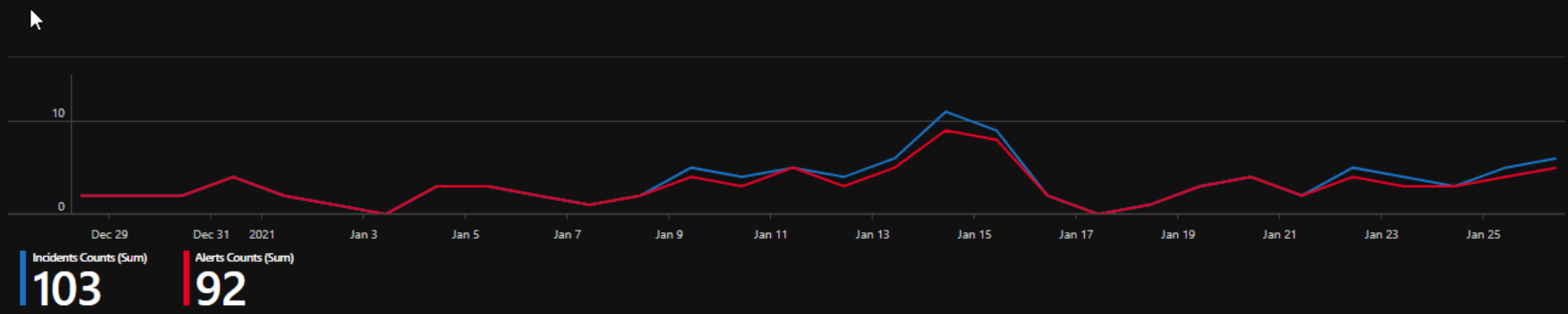
Time Range: Last 30 days

<*unset*>
Last 30 minutes
Last hour
Last 4 hours
Last 12 hours
Last 24 hours
Last 48 hours
Last 3 days
Last 7 days
Last 14 days
Last 28 days
Last 30 days
Last 60 days
Last 90 days

Open Inciden
103

lert Count
92

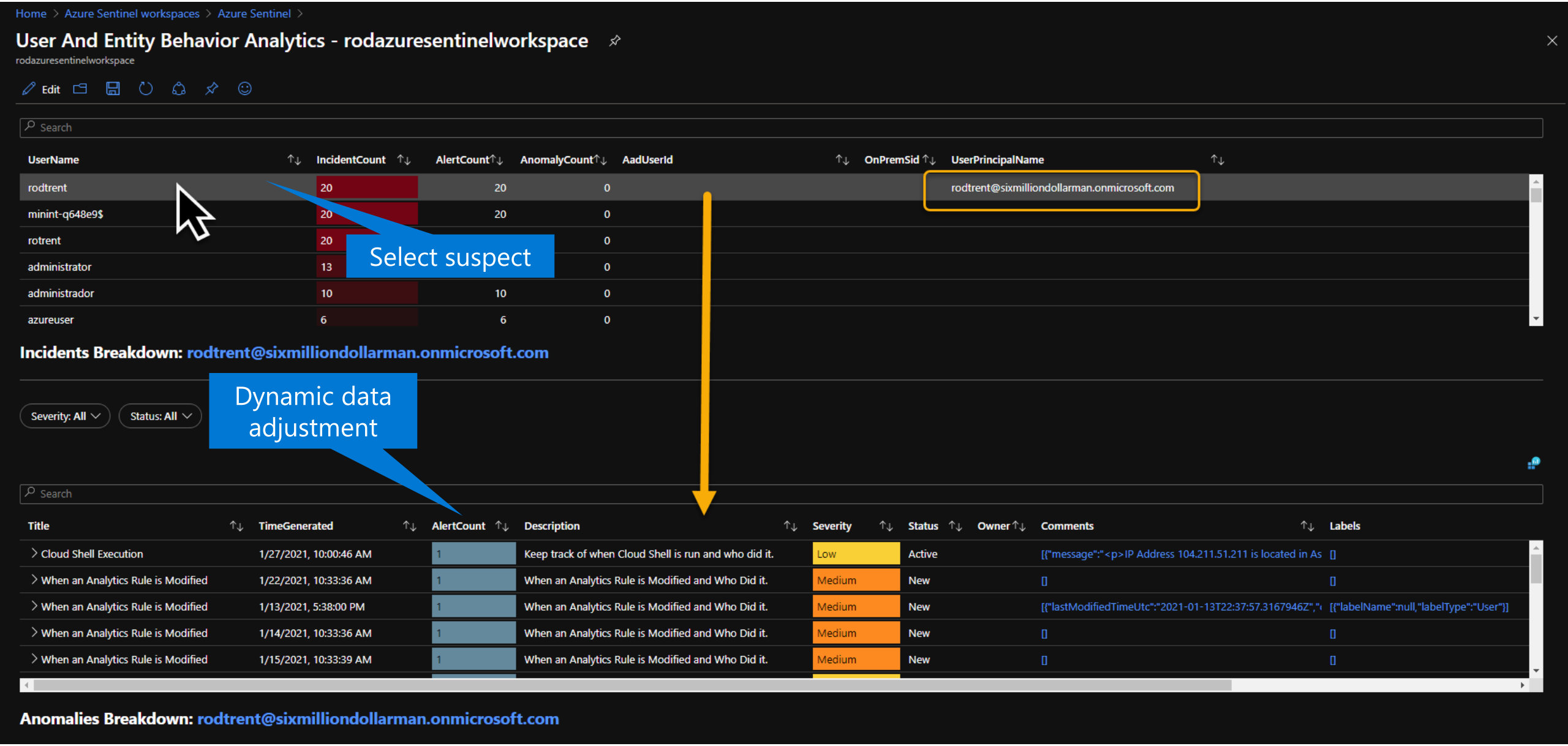
Anomalies Count
0

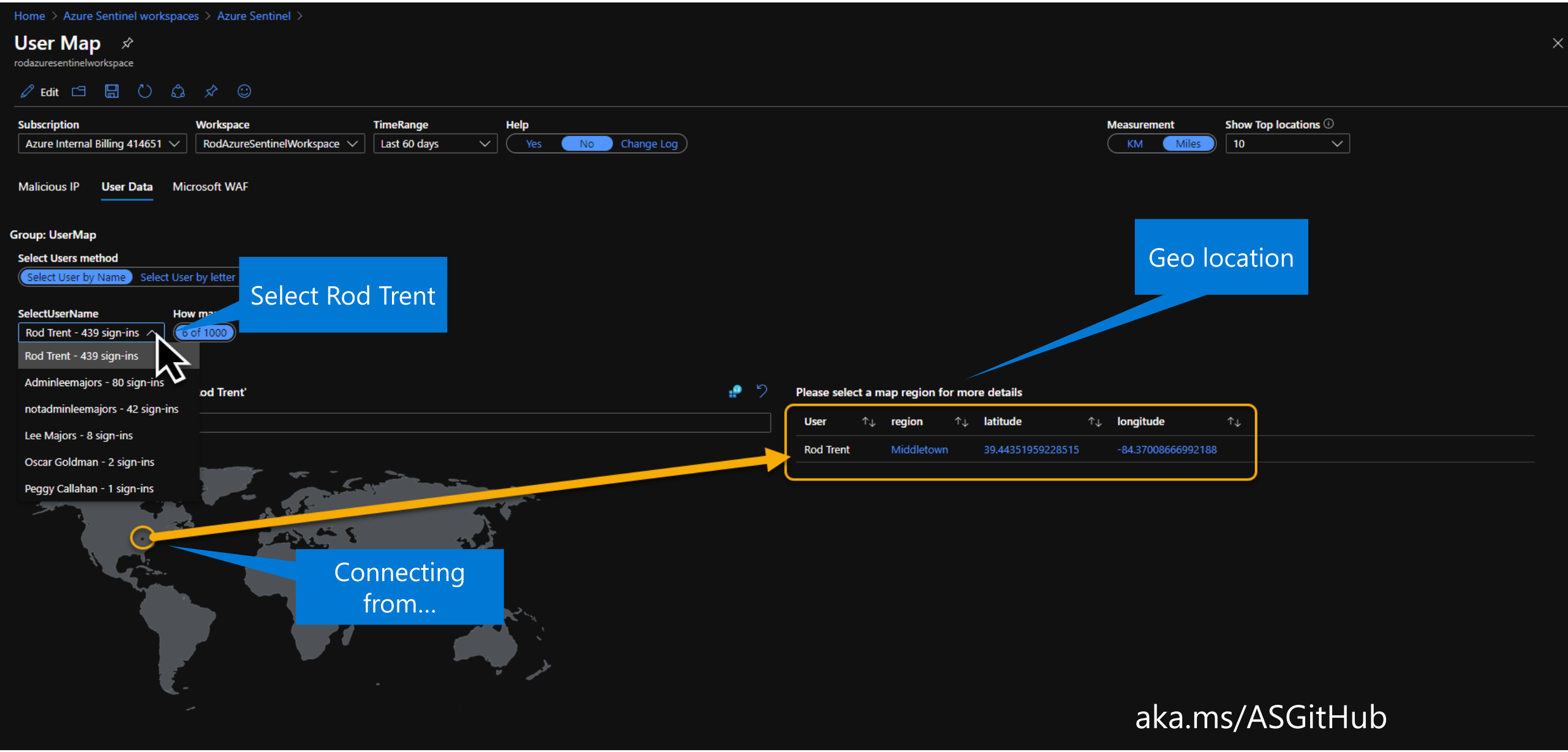


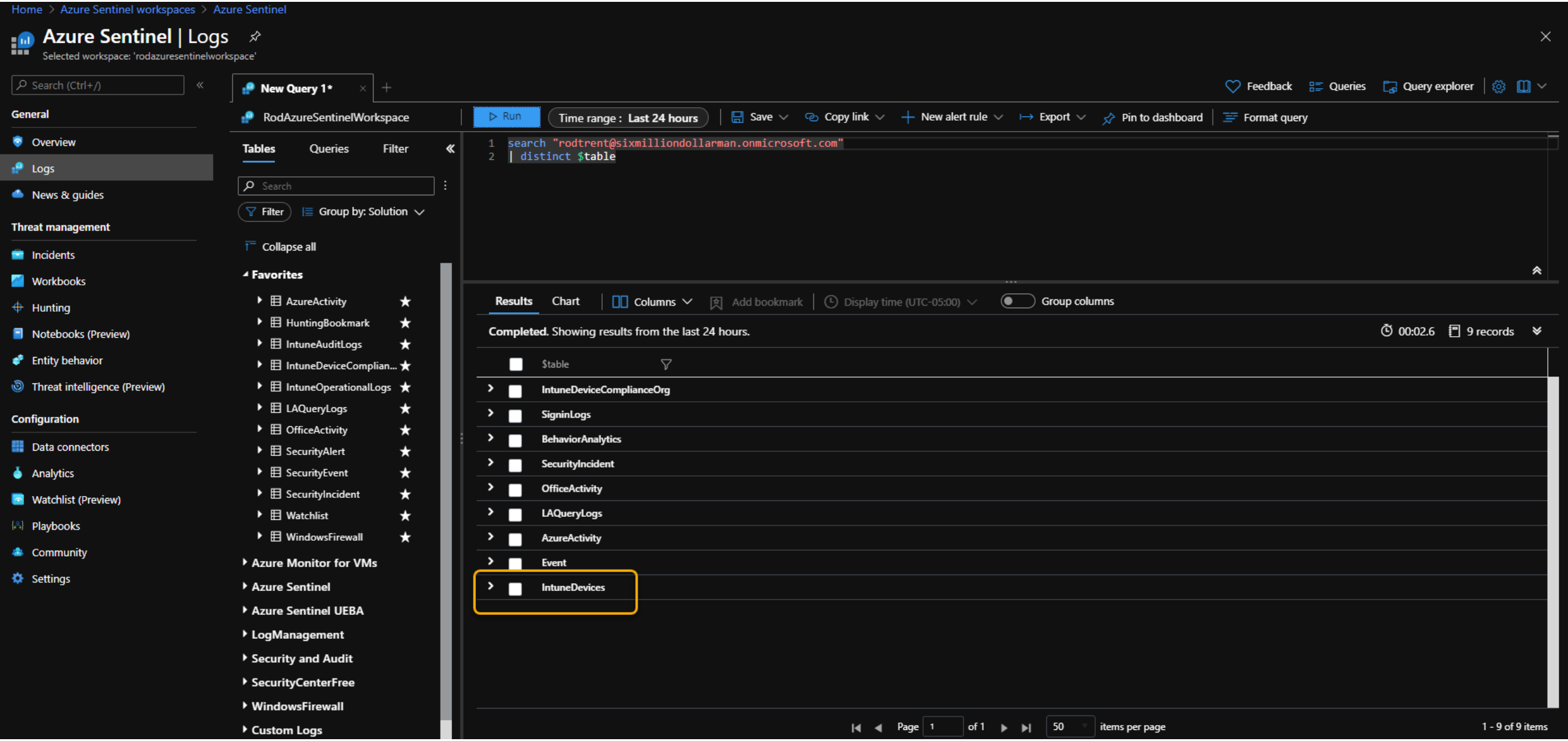
Top users ... - by Incidents, alerts & anomalies

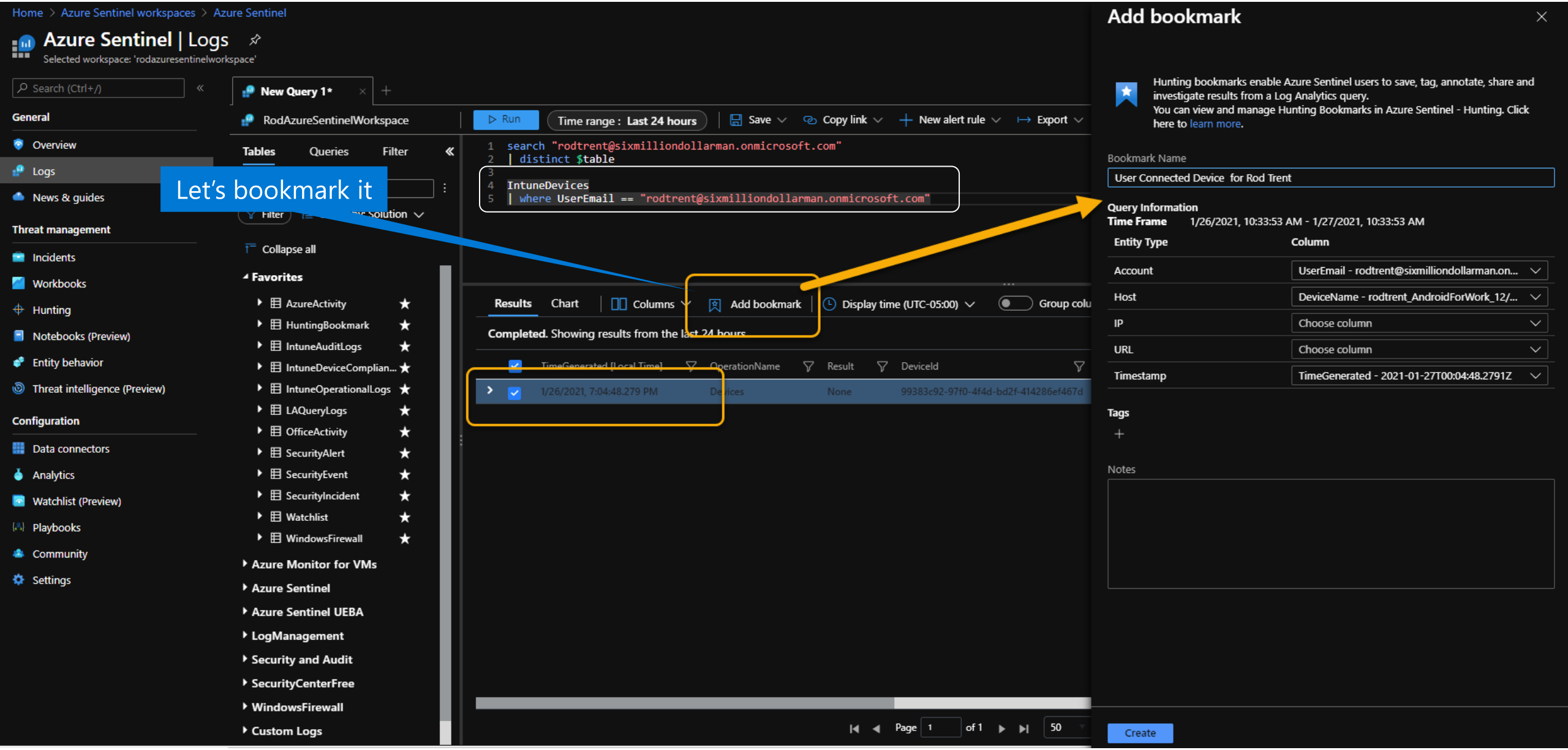
Search

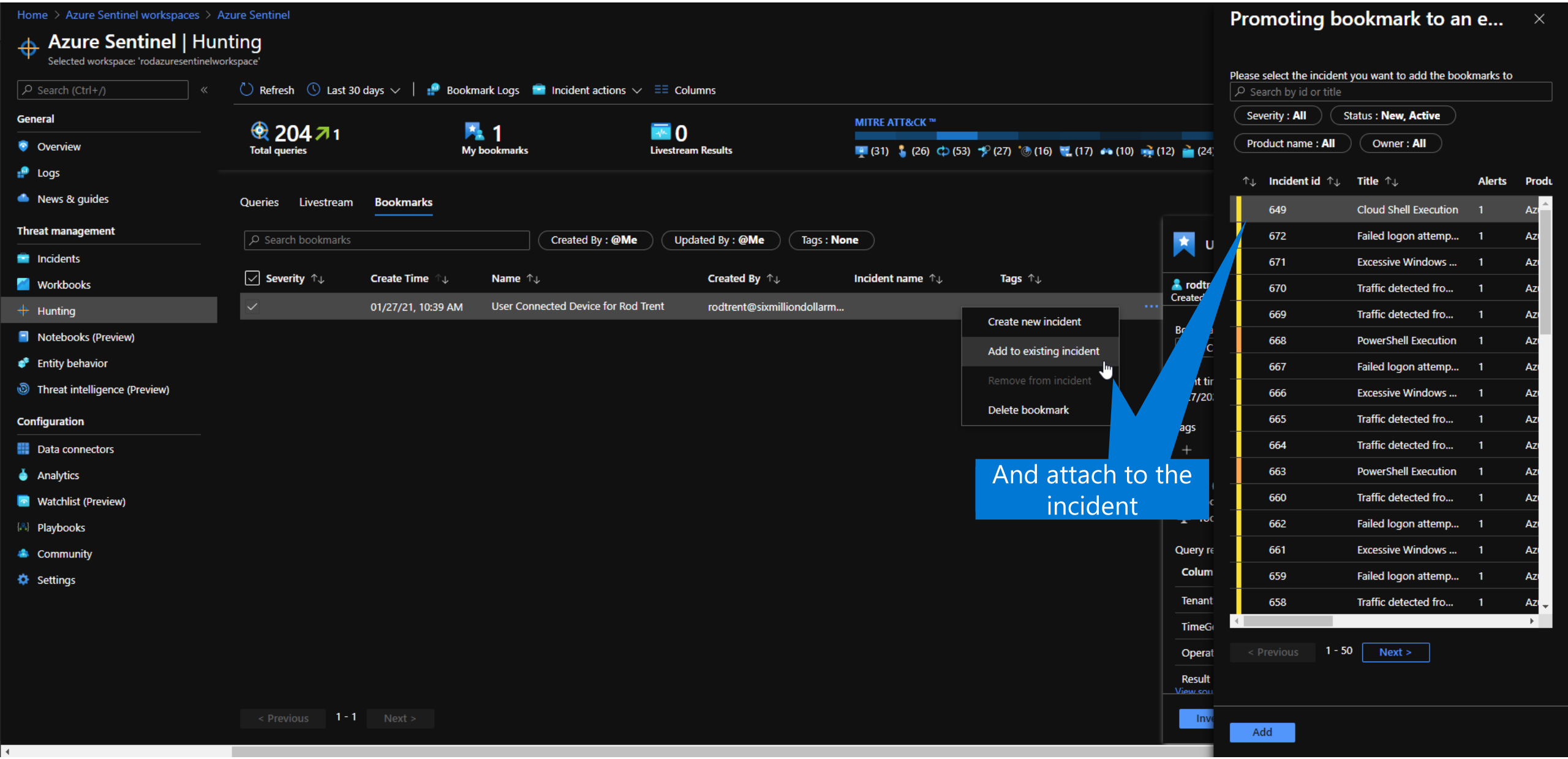
UserName	IncidentCount	AlertCount	AnomalyCount	AadUserId	OnPremSid	UserPrincipalName
rodtrent	20	20	0			rodtrent@sixmilliondollarman.onmicrosoft.com
minint-q648e9$	20	20	0			
rotrent	20	20	0			
administrator	13	13	0			
administrador	10	10	0			
azureuser	6	6	0			



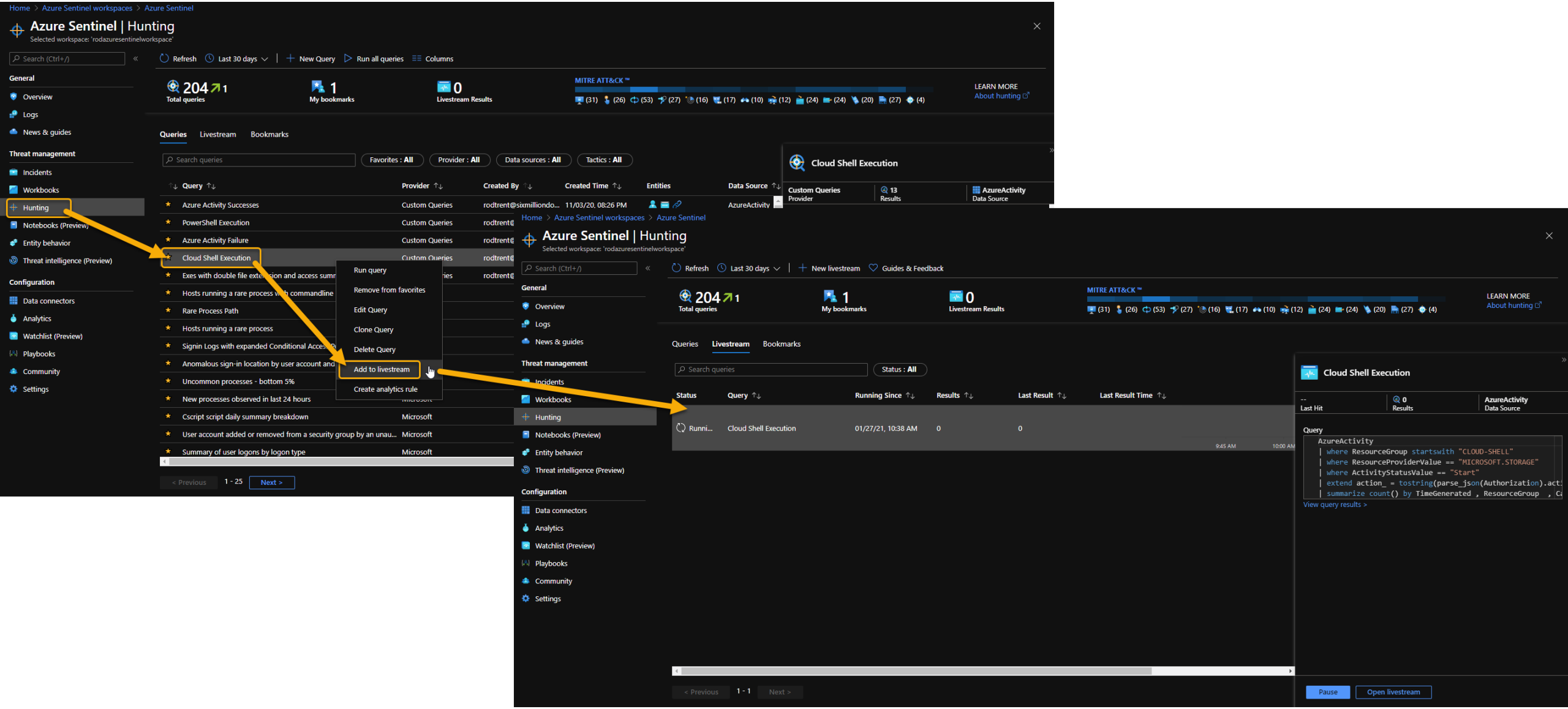


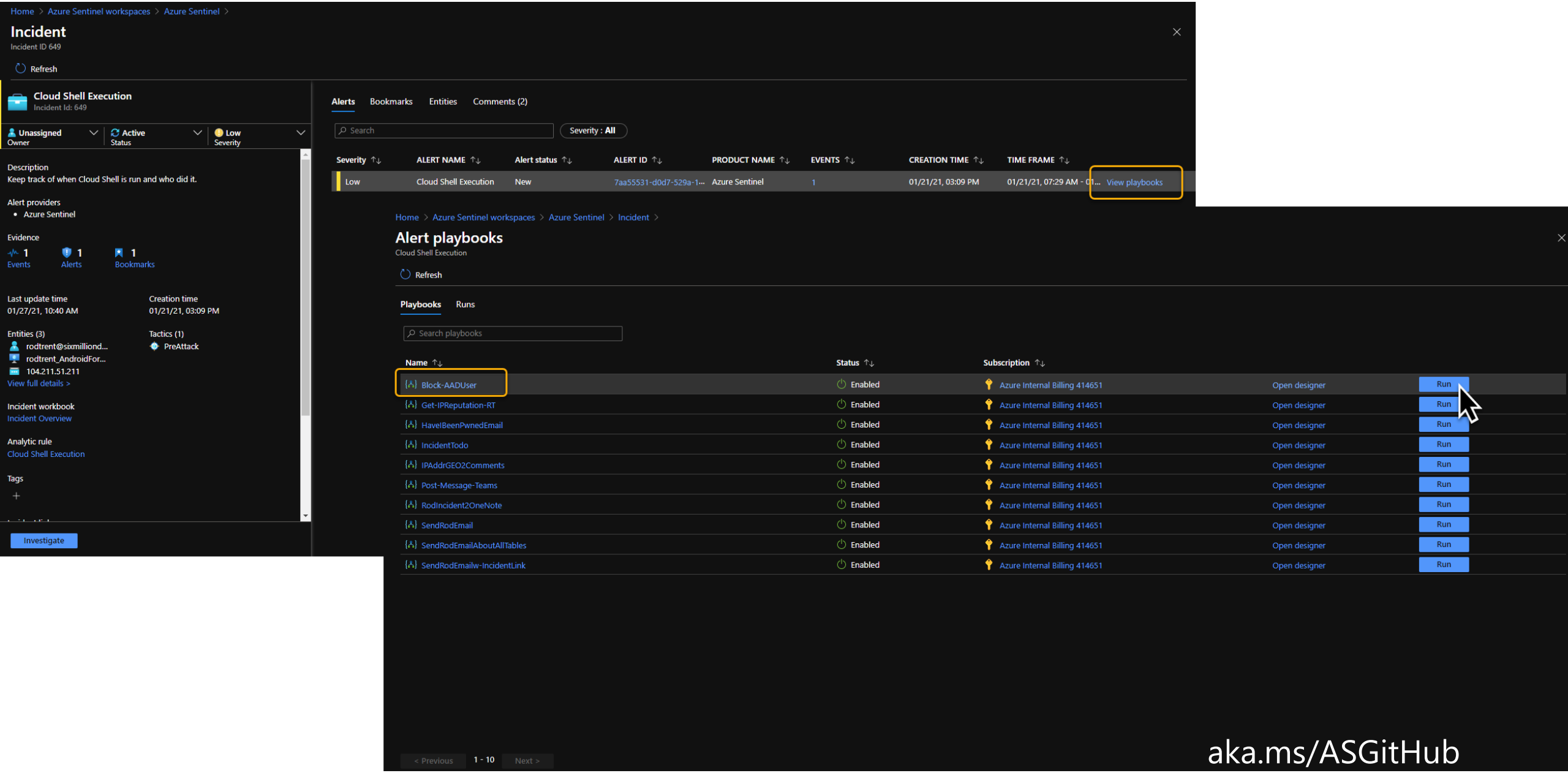






Action!





Analytic rule wizard - Create new rule

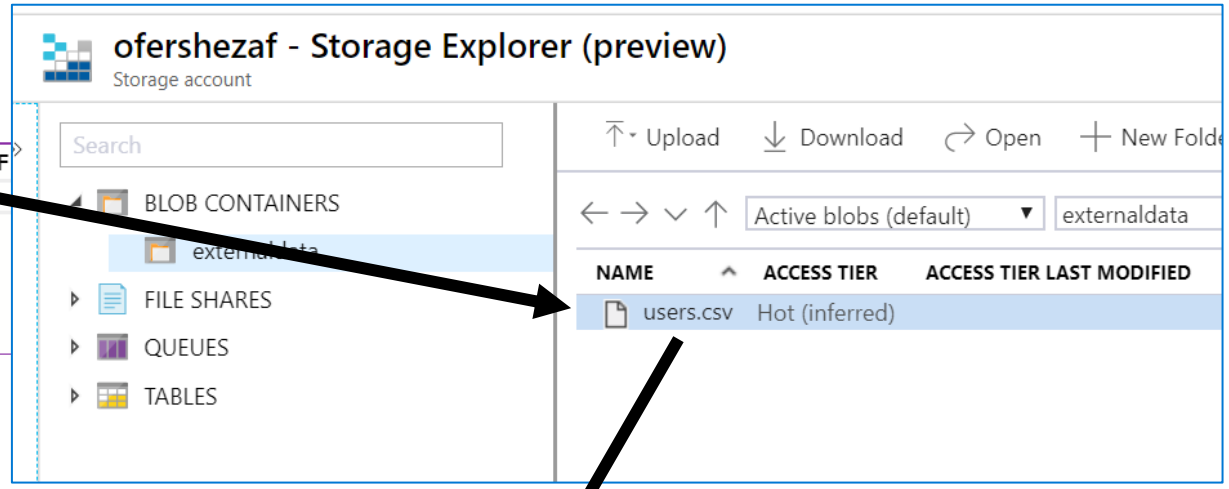
Define the logic for your new analytic rule.

Rule query

```
let whitelist = externaldata (UserPrincipalName: string) [h"https://..."] with (ignoreF
SecurityEvent | where EventID == "1102" and UserPrincipalName !in~ (whitelist)
```

Any time details set here will be within the scope defined below in the Query scheduling fields.

View query results >



Map entities - more entities coming soon!

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

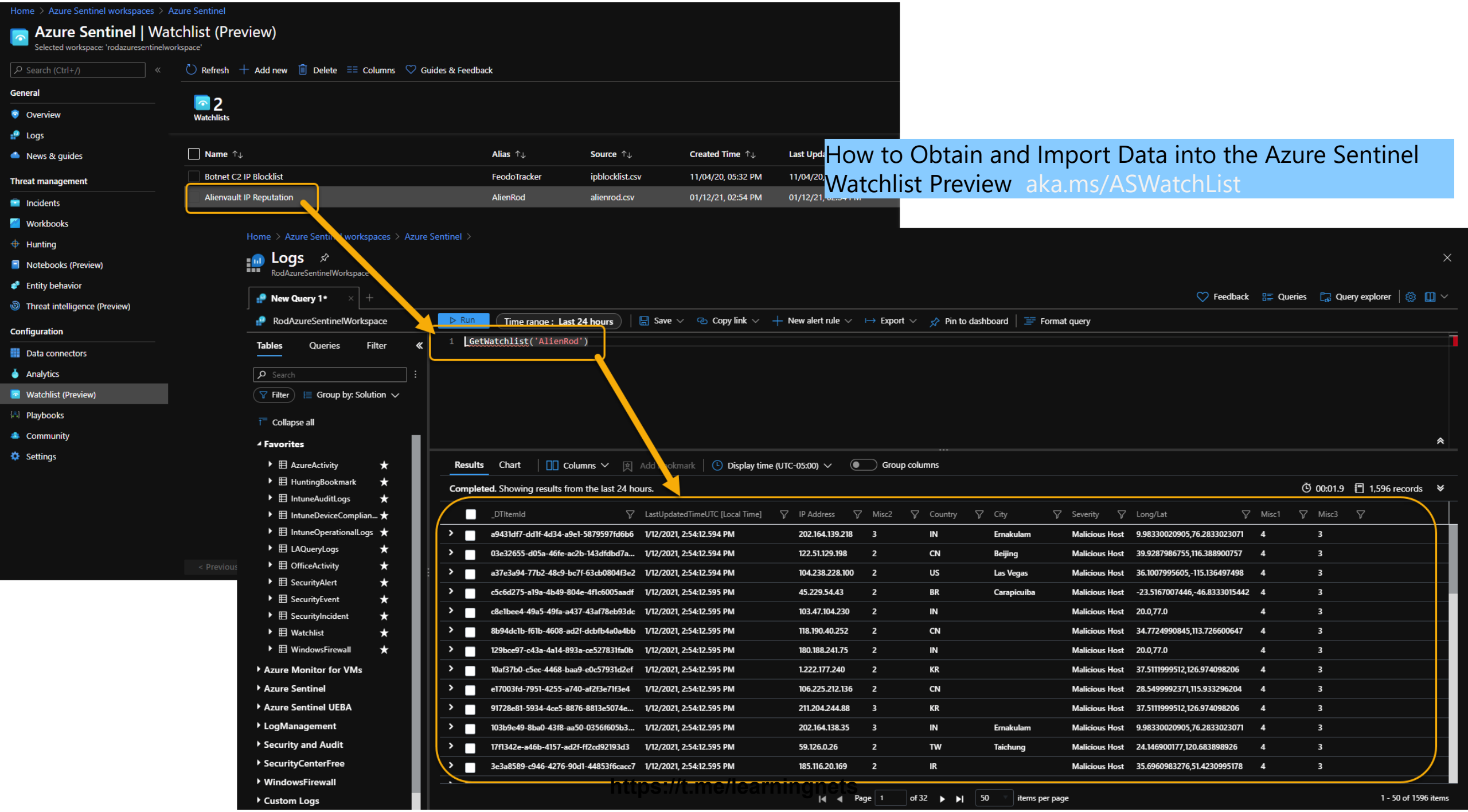
Entity Type
Account
Host
IP
URL

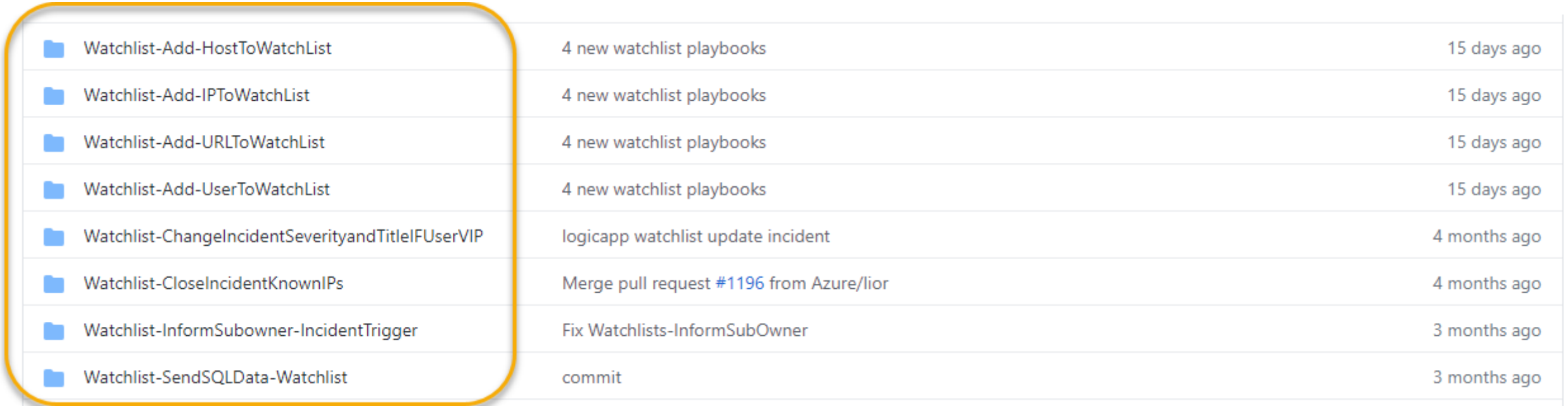
	A	B	C	D
1	UserName	DisplayName	Risk	Location
2	chris@contoso.com	Chris Green	70	{ "City": "Redmond", "State": "Washintgon", "Country": "US" }
3	ben@contoso.com	Ben Andrews	100	{ "City": "Oxford", "State": "Oxfordshare", "Country": "UK" }
4	nir@contoso.com	Nir Cohen	50	{ "City": "Tel-Aviv", "State": "", "Country": "IL" }
5	Gabriela@contoso.com	Cynthia Silva	20	{ "City": "Rio de Janeiro", "State": "Rio de Janeiro", "Country": "BR" }
6	melissa@contoso.com	Chandana Agarwals	100	{ "City": "Mumbai", "State": "Maharashtra", "Country": "IN" }
7	alexw@seccxp.ninja	Alex Wilber	50	{ "City": "Rotterdam", "State": "South Holland", "Country": "NL" }

Query scheduling

Previous | Next : Automated response >

aka.ms/SentinelLookups

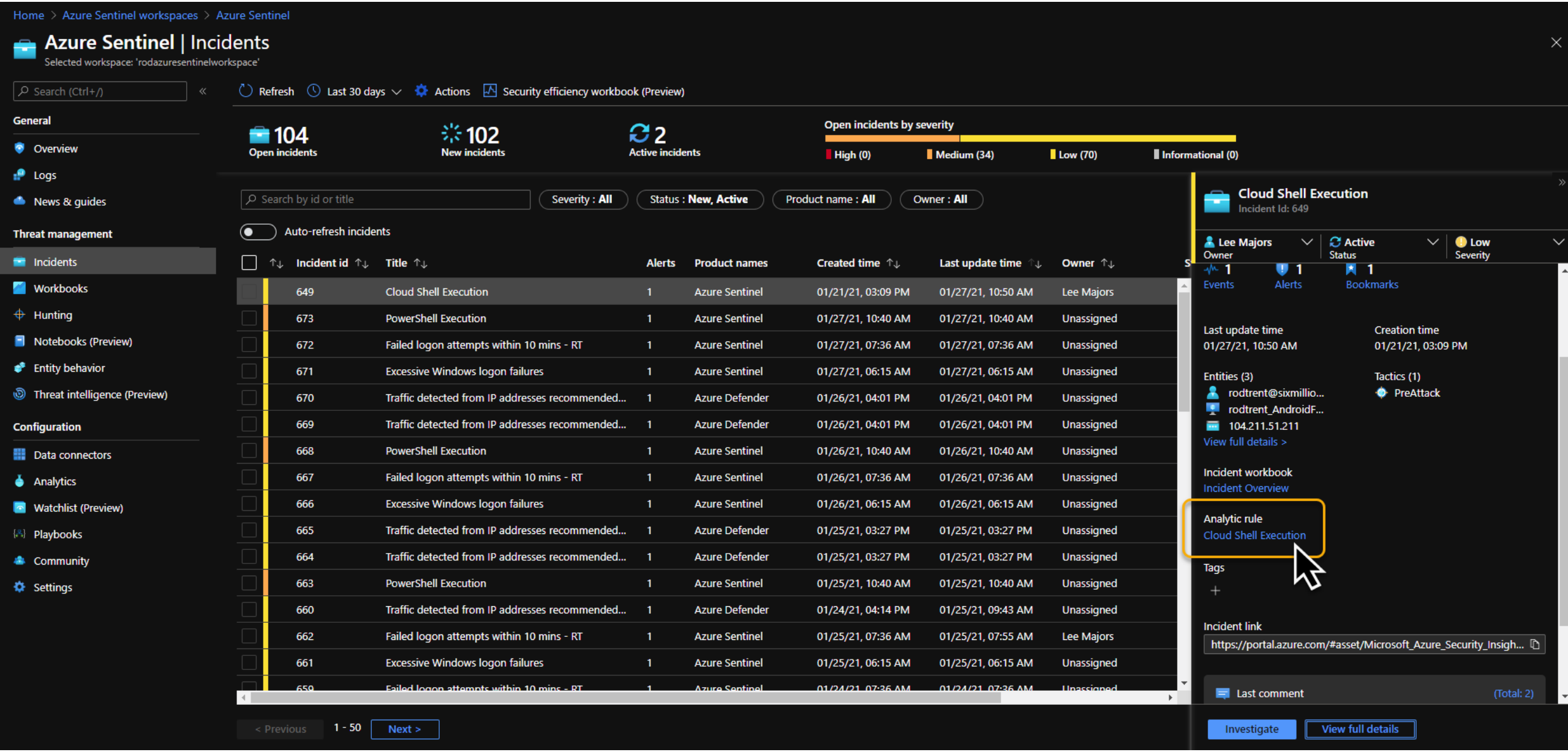

How to Obtain and Import Data into the Azure Sentinel Watchlist Preview aka.ms/ASWatchList
Home > Azure Sentinel workspaces > Azure Sentinel
Azure Sentinel | Watchlist (Preview)
Selected workspace: 'rodazuresentinelworkspace'
Search (Ctrl+/)
Refresh
Add new
Delete
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks (Preview)
Entity behavior
Threat intelligence (Preview)
Configuration
Data connectors
Analytics
Watchlist (Preview)
Playbooks
Community
Settings
2
Watchlists
Name
Alias
Source
Created Time
Last Upda
Botnet C2 IP Blocklist
FeodoTracker
ipblocklist.csv
11/04/20, 05:32 PM
11/04/20,
Alienvault IP Reputation
AlienRod
alienrod.csv
01/12/21, 02:54 PM
01/12/21,
Home > Azure Sentinel workspaces > Azure Sentinel
Logs
RodAzureSentinelWorkspace
New Query 1*
Feedback
Queries
Query explorer
RodAzureSentinelWorkspace
Run
Time range : Last 24 hours
Save
Copy link
New alert rule
Export
Pin to dashboard
Format query
Tables
Queries
Filter
Search
Filter
Group by: Solution
Collapse all
Favorites
AzureActivity
HuntingBookmark
IntuneAuditLogs
IntuneDeviceCompliance...
IntuneOperationalLogs
LAQueryLogs
OfficeActivity
SecurityAlert
SecurityEvent
SecurityIncident
Watchlist
WindowsFirewall
Azure Monitor for VMs
Azure Sentinel
Azure Sentinel UEBA
LogManagement
Security and Audit
SecurityCenterFree
WindowsFirewall
Custom Logs
1 GetWatchlist('AlienRod')
Results
Chart
Columns
Add bookmark
Display time (UTC-05:00)
Group columns
Completed. Showing results from the last 24 hours.
00:01.9
1,596 records
_DTItemId
LastUpdatedTimeUTC [Local Time]
IP Address
Misc2
Country
City
Severity
Long/Lat
Misc1
Misc3
a9431df7-dd1f-4d34-a9e1-5879597fd6b6 1/12/2021, 2:54:12.594 PM 202.164.139.218 3 IN Ernakulam Malicious Host 9.98330020905,76.2833023071 4 3
03e32655-d05a-46fe-ac2b-143dfdbd7a... 1/12/2021, 2:54:12.594 PM 122.51.129.198 2 CN Beijing Malicious Host 39.9287986755,116.388900757 4 3
a37e3a94-77b2-48c9-bc7f-63cb0804f3e2 1/12/2021, 2:54:12.594 PM 104.238.228.100 2 US Las Vegas Malicious Host 36.1007995605,-115.136497498 4 3
c5c6d275-a19a-4b49-804e-4f1c6005aadf 1/12/2021, 2:54:12.595 PM 45.229.54.43 2 BR Carapicuiba Malicious Host -23.5167007446,-46.8333015442 4 3
c8e1bee4-49a5-49fa-a437-43af78eb93dc 1/12/2021, 2:54:12.595 PM 103.47.104.230 2 IN Malicious Host 20.0,77.0 4 3
8b94dc1b-f61b-4608-ad2f-dcbfb4a0a4bb 1/12/2021, 2:54:12.595 PM 118.190.40.252 2 CN Malicious Host 34.7724990845,113.726600647 4 3
129bce97-c43a-4a14-893a-ce527831fa0b 1/12/2021, 2:54:12.595 PM 180.188.241.75 2 IN Malicious Host 20.0,77.0 4 3
10af37b0-c5ec-4468-baa9-e0c57931d2ef 1/12/2021, 2:54:12.595 PM 1.222.177.240 2 KR Malicious Host 37.5111999512,126.974098206 4 3
e17003fd-7951-4255-a740-af2f3e71f3e4 1/12/2021, 2:54:12.595 PM 106.225.212.136 2 CN Malicious Host 28.5499992371,115.933296204 4 3
91728e81-5934-4ce5-8876-8813e5074e... 1/12/2021, 2:54:12.595 PM 211.204.244.88 3 KR Malicious Host 37.5111999512,126.974098206 4 3
103b9e49-8ba0-43f8-aa50-0356f605b3... 1/12/2021, 2:54:12.595 PM 202.164.138.35 3 IN Ernakulam Malicious Host 9.98330020905,76.2833023071 4 3
17f1342e-a46b-4157-ad2f-ff2cd92193d3 1/12/2021, 2:54:12.595 PM 59.126.0.26 2 TW Taichung Malicious Host 24.146900177,120.683898926 4 3
3e3a8589-c946-4276-90d1-44853f6cacc7 1/12/2021, 2:54:12.595 PM 185.116.20.169 2 IR Malicious Host 35.6960983276,51.4230995178 4 3
https://t.me/learningnets
Page 1 of 32
50 items per page
1 - 50 of 1596 items



Watchlist-Add-HostToWatchList	4 new watchlist playbooks	15 days ago
Watchlist-Add-IPToWatchList	4 new watchlist playbooks	15 days ago
Watchlist-Add-URLToWatchList	4 new watchlist playbooks	15 days ago
Watchlist-Add-UserToWatchList	4 new watchlist playbooks	15 days ago
Watchlist-ChangeIncidentSeverityandTitleIFUserVIP	logicapp watchlist update incident	4 months ago
Watchlist-CloseIncidentKnownIPs	Merge pull request #1196 from Azure/lior	4 months ago
Watchlist-InformSubowner-IncidentTrigger	Fix Watchlists-InformSubOwner	3 months ago
Watchlist-SendSQLData-Watchlist	commit	3 months ago

Playbooks folder: https://aka.ms/ASGitHub

Action!



Take actions today - Get started with Azure Sentinel

Start
Microsoft Azure trial

Create Azure Sentinel
instance

Connect
data sources

To learn more, visit https://aka.ms/AzureSentinel

Questions?

Azure Sentinel benefit for Microsoft 365 E5 customers

Save up to USD1500/month on a typical 3,500 seat deployment of Microsoft 365 E51 with Azure credits for up to 100MB per user/month of data ingestion into Azure Sentinel.

aka.ms/SentinelOffer

Azure Sentinel Resources:

Azure Sentinel GitHub Repo: **aka.ms/ASGitHub**
Azure Sentinel Peer Community/Blog: **aka.ms/AzureSentinelMicrosoft**
My Azure Sentinel Blog: **aka.ms/RodBlog**
Azure Sentinel on LinkedIn: **aka.ms/AzureSentinelLinkedIn**
Azure Sentinel on Twitter: **aka.ms/AzureSentinelTwitter**
Follow me on Twitter: **@rodtrent**