



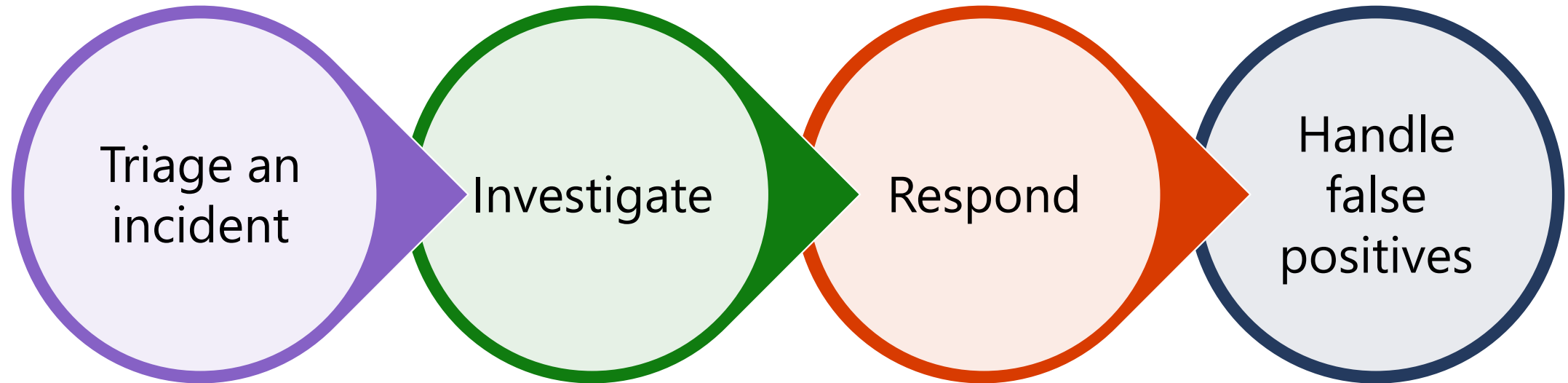
A Day in the life of an Azure Sentinel Analyst

Rod Trent
Cybersecurity CE
Azure Sentinel Global SME



<https://t.me/learningnets>

The SOC incident workflow





Casting Call

Action!

<https://t.me/learningnets>



Azure Sentinel | Incidents

Selected workspace: 'rodazuresentinelworkspace'

Search (Ctrl+/)

Refresh Last 30 days Policy workbook (Preview)

Potentially interesting

- 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

103 Open incidents

102 Incidents

1 Active incidents



Search by id or title

Severity: All Status: New, Active Product name: All Owner: All

Auto-refresh incidents

Incident id	Title	Alerts	Product names	Created time	Last update time	Owner
649	Cloud Shell Execution	1	Azure Sentinel	01/21/21, 03:09 PM	01/27/21, 09:49 AM	Unassigned
672	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/27/21, 07:36 AM	01/27/21, 07:36 AM	Unassigned
	Excessive Windows logon failures	1	Azure Sentinel	01/27/21, 06:15 AM	01/27/21, 06:15 AM	Unassigned
	Traffic detected from IP addresses recommended...	1	Azure Defender	01/26/21, 04:01 PM	01/26/21, 04:01 PM	Unassigned
669	Traffic detected from IP addresses recommended...	1	Azure Defender	01/26/21, 04:01 PM	01/26/21, 04:01 PM	Unassigned
668	PowerShell Execution	1	Azure Sentinel	01/26/21, 10:40 AM	01/26/21, 10:40 AM	Unassigned
667	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/26/21, 07:36 AM	01/26/21, 07:36 AM	Unassigned
666	Excessive Windows logon failures	1	Azure Sentinel	01/26/21, 06:15 AM	01/26/21, 06:15 AM	Unassigned
665	Traffic detected from IP addresses recommended...	1	Azure Defender	01/25/21, 03:27 PM	01/25/21, 03:27 PM	Unassigned
664	Traffic detected from IP addresses recommended...	1	Azure Defender	01/25/21, 03:27 PM	01/25/21, 03:27 PM	Unassigned
663	PowerShell Execution	1	Azure Sentinel	01/25/21, 10:40 AM	01/25/21, 10:40 AM	Unassigned
660	Traffic detected from IP addresses recommended...	1	Azure Defender	01/24/21, 04:14 AM	01/24/21, 04:14 AM	Unassigned
662	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/25/21, 07:36 AM	01/25/21, 07:36 AM	Unassigned
661	Excessive Windows logon failures	1	Azure Sentinel	01/25/21, 06:15 AM	01/25/21, 06:15 AM	Unassigned
659	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/24/21, 07:36 AM	01/24/21, 07:36 AM	Unassigned
658	Traffic detected from IP addresses recommended...	1	Azure Defender	01/23/21, 03:43 PM	01/23/21, 03:43 PM	Unassigned

Incidents Blade

Get into the Details

Cloud Shell Execution

Incident Id: 649

Unassigned New Low Severity

Description: Keep track of when Cloud Shell is run and who did it.

Alert providers: Azure Sentinel

Evidence: 1 Events, 1 Alerts, 0 Bookmarks

Last update time: 01/27/21, 09:49 AM | Creation time: 01/21/21, 03:09 PM

Entities (2): rodrent@sixmillio..., 104.211.51.211 | Tactics (1): PreAttack

Incident workbook: Incident Overview

Analytic rule: Cloud Shell Execution

Tags

Investigate View full details

< Previous 1 - 50 Next >

Home > Azure Sentinel workspaces

Incident

Incident ID 649

Refresh

Cloud Shell Execution

Incident Id: 649

Unassigned Owner | New Status | Low Severity

Description
Keep track of when Cloud Shell is run and who did it.

Alert providers
• Azure Sentinel

Evidence
1 Events | 1 Alerts | 0 Bookmarks

Last update time: 01/27/21, 09:49 AM
Creation time: 01/21/21, 03:09 PM

Entities (2)
• rodrent@sixmilliond...
• 104.211.51.211
[View full details >](#)

Tactics (1)
• PreAttack

Incident workbook
[Incident Overview](#)

Analytic rule
Cloud Shell Execution

Tags
+

Incident link

Investigate

Incident description

Alerts | Bookmarks | **Entities** | Comments

[View entities full details here](#)

Search

Entities : All

NAME ↑↓	TYPE ↑↓
rodrent@sixmilliondollarman.onmicrosoft.com	Account
104.211.51.211	IP

Artifacts

Entities

Incident

Incident ID 649

Refresh

Cloud Shell Execution

Incident Id: 649

Unassigned Owner | New Status | Low Severity

Description
Keep track of when Cloud Shell is run and who did it.

Alert providers
• Azure Sentinel

Evidence
1 Events | 1 Alerts | 0 Bookmarks

Last update time: 01/27/21, 09:49 AM
Creation time: 01/21/21, 03:09 PM

Entities (2): rodrent@sixmilliond..., 104.211.51.211
Tactics (1): PreAttack

Incident workbook
Incident Overview

Analytic rule
Cloud Shell Execution

Tags
+

Incident link

Investigate

Alerts | Bookmarks | Entities | Comments

Search | Severity: All

Severity	ALERT NAME	Alert status	ALERT ID	PRODUCT NAME	EVENTS	CREATION TIME	TIME FRAME
Low	Cloud Shell Execution	New	7aa55531-d0d7-529a-1...	Azure Sentinel	1	01/21/21, 03:09 PM	01/21/21, 07:29 AM - 01... View playbooks

Let's check the IP address

Alert playbooks

Cloud Shell Execution



Refresh

Playbooks Runs

Search playbooks

Name ↑↓	Status ↑↓	Subscription ↑↓		
Block-AADUser	Enabled	Azure Internal Billing 414651	Open designer	Run
Get-IPReputation-RT	Enabled	Azure Internal Billing 414651	Open designer	Run
HavelBeenPwnedEmail	Enabled	Azure Internal Billing 414651	Open designer	Run
IncidentTodo	Enabled	Azure Internal Billing 414651	Open designer	Run
IPAddrGEO2Comments		Azure Internal Billing 414651	Open designer	Run
Post-Message-Teams		Azure Internal Billing 414651	Open designer	Run
RodIncident2OneNote		Azure Internal Billing 414651	Open designer	Run
SendRodEmail		Azure Internal Billing 414651	Open designer	Run
SendRodEmailAboutAllTables	Enabled	Azure Internal Billing 414651	Open designer	Run
SendRodEmailw-IncidentLink	Enabled	Azure Internal Billing 414651	Open designer	Run

Get GEO Location
for the IP with a
Playbook

aka.ms/ASGitHub

Alert playbooks

Cloud Shell Execution



Refresh

Playbooks Runs

Search playbooks

Name ↑↓	Status ↑↓	Subscription ↑↓		
Block-AADUser	Enabled	Azure Internal Billing 414651	Open designer	Run
Get-IPReputation-RT	Enabled	Azure Internal Billing 414651	Open designer	Run
HaveIBeenPwnedEmail	Enabled	Azure Internal Billing 414651	Open designer	Run
IncidentTodo	Enabled	Azure Internal Billing 414651	Open designer	Run
IPAddrGEO2Comments		Azure Internal Billing 414651	Open designer	Run
Post-Message-Teams		Azure Internal Billing 414651	Open designer	Run
RodIncident2OneNote		Azure Internal Billing 414651	Open designer	Run
SendRodEmail		Azure Internal Billing 414651	Open designer	Run
SendRodEmailAboutAllTables		Azure Internal Billing 414651	Open designer	Run
SendRodEmailw-IncidentLink		Azure Internal Billing 414651	Open designer	Run

Check the user account against the HaveIBeenPwned database with a Playbook

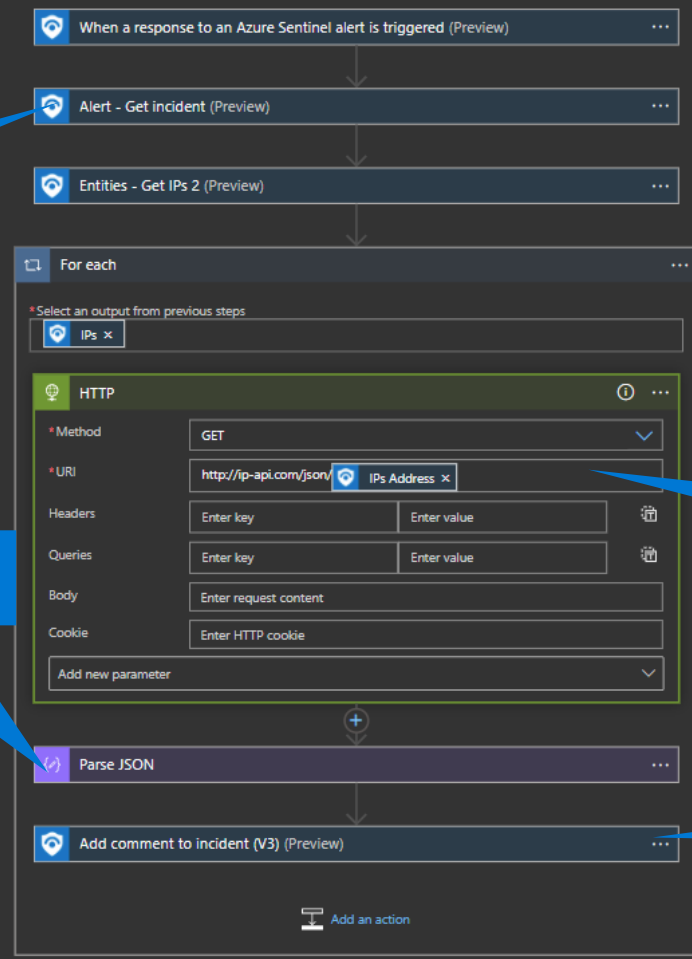
aka.ms/ASGitHub

Get Incident Information

Parse return value

Submit IP Address to IP-API.com

Write comment



Incident

Incident ID 649

Refresh

Cloud Shell Execution

Incident Id: 649

Unassigned Owner | Active Status | Low Severity

- Lee Majors
- Unassign Incident
- Assign to me
rodtrent@sixmilliondollarman.onmicrosoft.com
- Lee Majors**
leemajors@sixmilliondollarman.onmicrosoft.com

Apply Cancel

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Inci...

Investigate

Alerts | Bookmarks | Entities | **Comments (2)**

RT

Normal

Write a comment...

Comment

RT Rod Trent rodtrent@sixmilliondollarman.onmicrosoft.com 01/27/21, 09:59 AM
Congratulations! rodtrent@sixmilliondollarman.onmicrosoft.com was not found in the Pwned Database.

RT Rod Trent rodtrent@sixmilliondollarman.onmicrosoft.com 01/27/21, 09:58 AM
Address 104.211.51.211 is located in Ashburn, Virginia United States and is attributed to Microsoft Corpora...

Lower severity and assign to a teammate

Nothing suspicious about the email address or the IP address

Incident

Incident ID 649



Refresh

Cloud Shell Execution

Incident Id: 649

Unassigned Active Status Low Severity

Description
Keep track of when Cloud Shell is run and who did it.

Alert providers
• Azure Sentinel

Evidence
 1 Events 1 Alerts 0 Bookmarks

Last update time: 01/27/21, 10:00 AM
Creation time: 01/21/21, 03:09 PM

Entities (2): rodtre... 104.211.51.211
Tactics (1): PreAttack

[View full details >](#)

Incident workbook
[Incident Overview](#)

Analytic rule
Cloud Shell Execution

Tags
+

Incident link

Investigate

Alerts Bookmarks Entities Comments (2)

[View entities full details here](#)

Entities : All

NAME ↑↓	TYPE ↑↓
rodtre@sixmilliondollarman.onmicrosoft.com	Account
104.211.51.211	IP



rodrent

Selected workspace: 'rodazuresentinelworkspace'

Guides & Feedback

rodrent

Role

Identity

Azure AD Object ID -- User Principal Name rodrent@sixmilliondollarman.onmicro

Security identifier -- Department --

Manager --

Contact info

Office Location -- City --

Country -- Mobile Phone --

State -- Email --

Entity link

https://portal.azure.com/#asset/Microsoft_Azure_S...

Investigate

Overview

Search

Time range : 12/28/2020, 10:10:15 AM - 1/27/2021, 10:10:15 AM

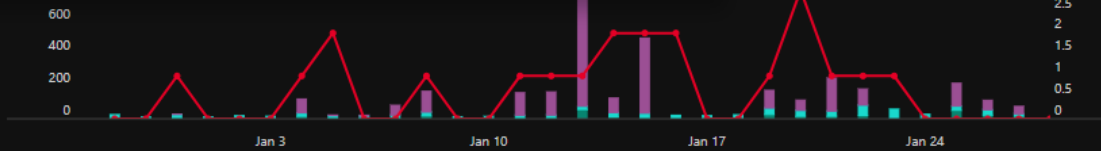
Timeline content : All Alerts : All Activities : All Alert Severity : All

Last 24 hours Last 48 hours Last 7 days Last 14 days **Last 30 days**

Start 12/28/2020 10:10:15 AM

End 01/27/2021 10:10:15 AM

OK Cancel



Alerts and activities timeline

Cloud Shell Execution
 Detected by Azure Sentinel | 1/12/2021, 3:09:42 PM
 Keep track of when Cloud Shell is run and who did it.
 Related incident: 608

Cloud Shell Execution
 Detected by Azure Sentinel | 1/11/2021, 3:09:41 PM
 Keep track of when Cloud Shell is run and who did it.
 Related incident: 603

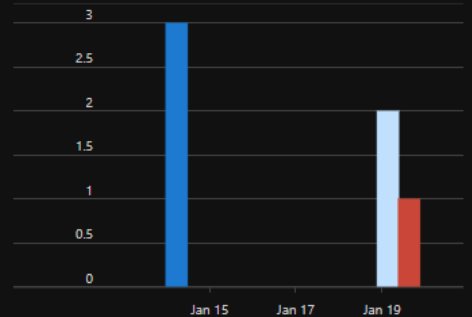
Cloud Shell Execution
 Detected by Azure Sentinel | 1/8/2021, 3:09:42 PM
 Keep track of when Cloud Shell is run and who did it.
 Related incident: 592

Insights

Actions by account

Action	Change	Most Recent	Count
Reset passw...		2021-01-19T...	1
Add user	MethodExec...	2021-01-13T...	1
Add user	AccountEna...	2021-01-13T...	2
Update user	JobTitle	2021-01-19T...	1
Update user	Targetid.Use...	2021-01-19T...	1

Actions by type



[See all account activity >](#)

Let's Investigate!

Investigation

Undo Redo

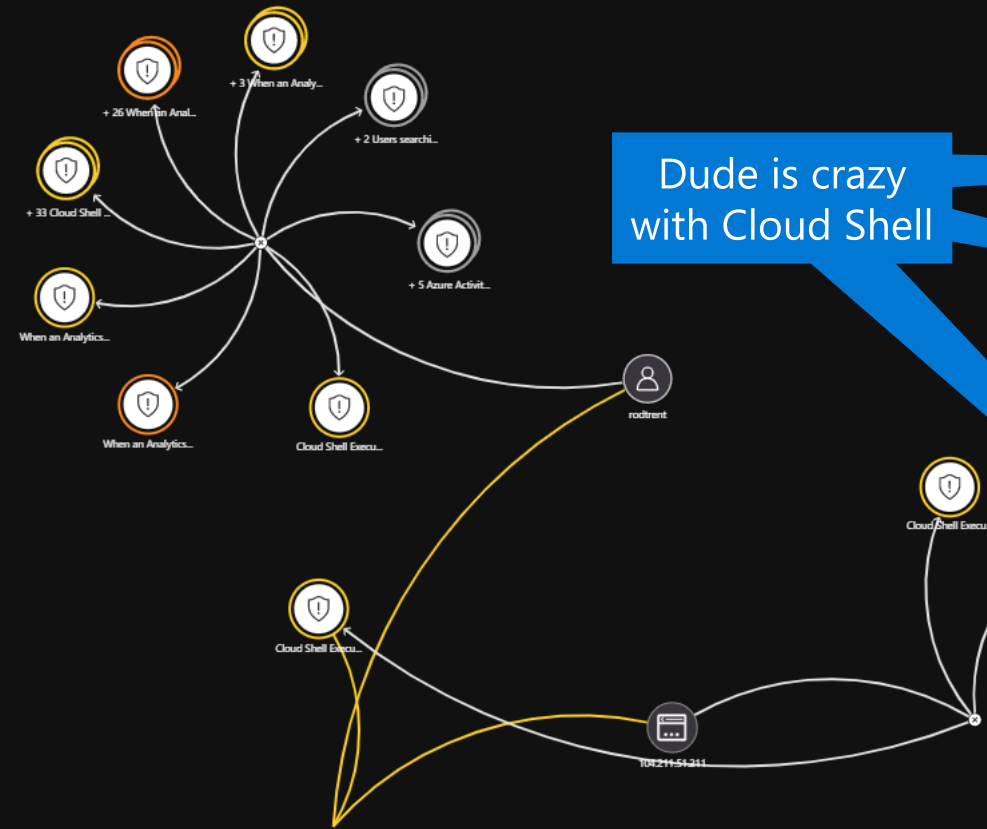
Cloud Shell Execution
Incident

Low
Severity

Active
Status

Unassigned
Owner

1/27/2021, 10:00:46 AM
Last incident update time



Dude is crazy with Cloud Shell

Timeline

- Cloud Shell Execution**
1/4/2021, 3:32:59 PM
Keep track of when Cloud Shell is run and who did it.
- Cloud Shell Execution**
1/14/2021, 12:04:02 PM
Keep track of when Cloud Shell is run and who did it.
- When an Analytics Rule is Modified**
1/15/2021, 10:49:03 AM
When an Analytics Rule is Modified and Who Did it.
- When an Analytics Rule is Deleted**
1/19/2021, 4:33:08 PM
Alert when an Analytics Rule is deleted and who did it.
- Cloud Shell Execution**
1/21/2021, 7:29:42 AM
Keep track of when Cloud S

Security team?

Cut!

<https://t.me/learningnets>

Action!

<https://t.me/learningnets>



User And Entity Behavior Analytics - rodazuresentinelworkspace

rodazuresentinelworkspace



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

Open Incident **103** <unset>

Last 30 minutes **Alert Count 92**

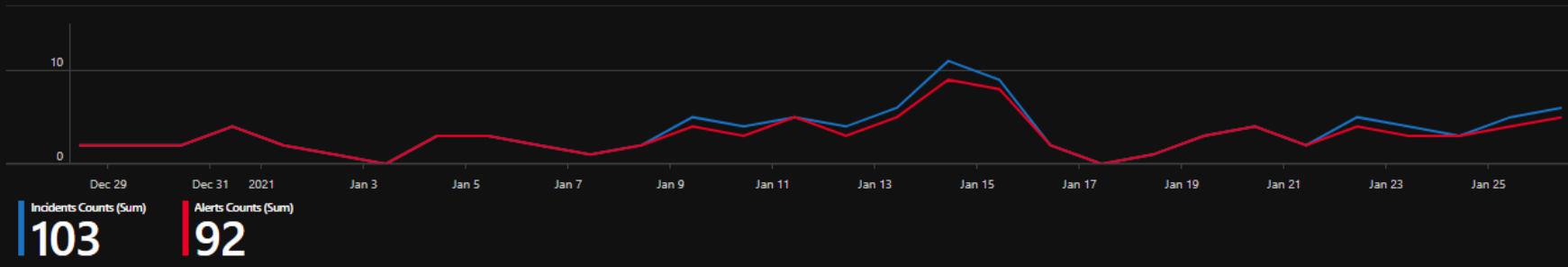
Last hour **Anomalies Count 0**

Last 4 hours

Last 12 hours

Last 24 hours

Last 48 hours



Top users - by Incidents, alerts & anomalies

- Last 3 days
- Last 7 days
- Last 14 days
- Last 28 days
- Last 30 days**
- Last 60 days
- Last 90 days

UserName	IncidentCount	AlertCount	AnomalyCount	AadUserId	OnPremSid	UserPrincipalName
rodtrent	20	20	0			rodtrent@sixmilliondollarman.onmicrosoft.com
minint-q648e93	20	20	0			
rotrent	20	20	0			
administrator	13	13	0			
administrador	10	10	0			
azureuser	6	6	0			

User And Entity Behavior Analytics - rodazuresentinelworkspace

rodazuresentinelworkspace



Search

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



Select suspect

Dynamic data adjustment

Incidents Breakdown: rodtrrent@sixmilliondollarman.onmicrosoft.com

Severity: All Status: All

Search

Title	TimeGenerated	AlertCount	Description	Severity	Status	Owner	Comments	Labels
> Cloud Shell Execution	1/27/2021, 10:00:46 AM	1	Keep track of when Cloud Shell is run and who did it.	Low	Active		["message":"<p>IP Address 104.211.51.211 is located in As	
> When an Analytics Rule is Modified	1/22/2021, 10:33:36 AM	1	When an Analytics Rule is Modified and Who Did it.	Medium	New			
> When an Analytics Rule is Modified	1/13/2021, 5:38:00 PM	1	When an Analytics Rule is Modified and Who Did it.	Medium	New		["lastModifiedTimeUtc":"2021-01-13T22:37:57.3167946Z",	["labelName":null,"labelType":"User"]
> When an Analytics Rule is Modified	1/14/2021, 10:33:36 AM	1	When an Analytics Rule is Modified and Who Did it.	Medium	New			
> When an Analytics Rule is Modified	1/15/2021, 10:33:39 AM	1	When an Analytics Rule is Modified and Who Did it.	Medium	New			

Anomalies Breakdown: rodtrrent@sixmilliondollarman.onmicrosoft.com

User Map

rodazuresentinelworkspace



Subscription: Azure Internal Billing 414651 | Workspace: RodAzureSentinelWorkspace | TimeRange: Last 60 days | Help: Yes No Change Log

Measurement: KM Miles | Show Top locations: 10

Malicious IP **User Data** Microsoft WAF

Group: UserMap

Select Users method: Select User by Name Select User by letter

Select Rod Trent

- SelectUserName: Rod Trent - 439 sign-ins (6 of 1000)
- Rod Trent - 439 sign-ins
- Adminleemajors - 80 sign-ins
- notadminleemajors - 42 sign-ins
- Lee Majors - 8 sign-ins
- Oscar Goldman - 2 sign-ins
- Peggy Callahan - 1 sign-ins

Geo location

Please select a map region for more details

User	region	latitude	longitude
Rod Trent	Middletown	39.44351959228515	-84.37008666992188

Connecting from...

aka.ms/ASGitHub

Azure Sentinel | Logs

Selected workspace: 'rodazuresentinelworkspace'

Search (Ctrl+/)

New Query 1*

RodAzureSentinelWorkspace

Time range: Last 24 hours

Feedback | Queries | Query explorer | Settings | Help

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

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 search "rodtrent@sixmilliondollarman.onmicrosoft.com"
2 | distinct $table
```

Results | Chart | Columns | Add bookmark | Display time (UTC-05:00) | Group columns

Completed. Showing results from the last 24 hours. 00:02.6 9 records

\$table
IntuneDeviceComplianceOrg
SigninLogs
BehaviorAnalytics
SecurityIncident
OfficeActivity
LAQueryLogs
AzureActivity
Event
IntuneDevices

Search (Ctrl+/)

New Query 1*

RodAzureSentinelWorkspace

Run Time range: Last 24 hours Save Copy link New alert rule Export

Let's bookmark it

```
1 search "rod trent@sixmilliondollarman.onmicrosoft.com"
2 | distinct $table
3
4 IntuneDevices
5 | where userEmail == "rod trent@sixmilliondollarman.onmicrosoft.com"
```

Add bookmark

Completed. Showing results from the last 24 hours

TimeGenerated [Local Time]	OperationName	Result	DeviceId
1/26/2021, 7:04:48.279 PM	Devices	None	99383c92-97f0-4f4d-bd2f-414286ef467d

Add bookmark

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

Bookmark Name
User Connected Device for Rod Trent

Query Information
Time Frame 1/26/2021, 10:33:53 AM - 1/27/2021, 10:33:53 AM

Entity Type	Column
Account	UserEmail - rod trent@sixmilliondollarman.on...
Host	DeviceName - rod trent_AndroidForWork_12/...
IP	Choose column
URL	Choose column
Timestamp	TimeGenerated - 2021-01-27T00:04:48.2791Z

Tags
+

Notes

Create

Azure Sentinel | Hunting

Selected workspace: 'rodazuresentinelworkspace'

Search (Ctrl+/) Refresh Last 30 days Bookmark Logs Incident actions Columns

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

204 Total queries 1 My bookmarks 0 Livestream Results MITRE ATT&CK™

Queries Livestream Bookmarks

Search bookmarks Created By: @Me Updated By: @Me Tags: None

Severity	Create Time	Name	Created By	Incident name	Tags
✓	01/27/21, 10:39 AM	User Connected Device for Rod Trent	rodtrrent@sixmilliondollarm...		

- Create new incident
- Add to existing incident
- Remove from incident
- Delete bookmark

And attach to the incident

Promoting bookmark to an e...

Please select the incident you want to add the bookmarks to

Search by id or title

Severity: All Status: New, Active

Product name: All Owner: All

Incident id	Title	Alerts	Produ
649	Cloud Shell Execution	1	Az
672	Failed logon attemp...	1	Az
671	Excessive Windows ...	1	Az
670	Traffic detected fro...	1	Az
669	Traffic detected fro...	1	Az
668	PowerShell Execution	1	Az
667	Failed logon attemp...	1	Az
666	Excessive Windows ...	1	Az
665	Traffic detected fro...	1	Az
664	Traffic detected fro...	1	Az
663	PowerShell Execution	1	Az
660	Traffic detected fro...	1	Az
662	Failed logon attemp...	1	Az
661	Excessive Windows ...	1	Az
659	Failed logon attemp...	1	Az
658	Traffic detected fro...	1	Az

< Previous 1 - 50 Next >

Add

Cut!

<https://t.me/learningnets>

Action!



<https://t.me/learningnets>

Home > Azure Sentinel workspaces > Azure Sentinel

Azure Sentinel | Hunting

Selected workspace: 'rodazuresentinelworkspace'

Search (Ctrl+/) Refresh Last 30 days New Query Run all queries Columns

General

204 Total queries 1 My bookmarks 0 Livestream Results

MITRE ATT&CK™

Cloud Shell Execution

Custom Queries Provider 13 Results AzureActivity Data Source

Query	Provider	Created By	Created Time	Entities	Data Source
Azure Activity Successes	Custom Queries	rodtrent@sixmilliondo...	11/03/20, 08:26 PM		AzureActivity
PowerShell Execution	Custom Queries	rodtrent@			
Azure Activity Failure	Custom Queries	rodtrent@			
Cloud Shell Execution	Custom Queries	rodtrent@			
Exes with double file extension and access sum...	ies	rodtrent@			
Hosts running a rare process with commandline					
Rare Process Path					
Hosts running a rare process					
Signin Logs with expanded Conditional Access					
Anomalous sign-in location by user account and					
Uncommon processes - bottom 5%					
New processes observed in last 24 hours					
Cscript script daily summary breakdown	Microsoft				
User account added or removed from a security group by an unau...	Microsoft				
Summary of user logons by logon type	Microsoft				

Run query
Remove from favorites
Edit Query
Clone Query
Delete Query
Add to livestream
Create analytics rule

Cloud Shell Execution

204 Total queries 1 My bookmarks 0 Livestream Results

MITRE ATT&CK™

Cloud Shell Execution

AzureActivity Data Source

Status	Query	Running Since	Results	Last Result	Last Result Time
Runni...	Cloud Shell Execution	01/27/21, 10:38 AM	0	0	9:45 AM 10:00 AM

```
AzureActivity
| where ResourceGroup startswith "CLOUD-SHELL"
| where ResourceProviderValue == "MICROSOFT.STORAGE"
| where ActivityStatusValue == "Start"
| extend action_ = tostring(parse_json(Authorization).acti...)
| summarize count() by TimeGenerated, ResourceGroup, C...
```

View query results >

Pause Open livestream

<https://t.me/learningnets>

Incident

Incident ID: 649

Refresh

Cloud Shell Execution

Incident ID: 649

Unassigned Owner | Active Status | Low Severity

Description: Keep track of when Cloud Shell is run and who did it.

Alert providers: Azure Sentinel

Evidence: 1 Events, 1 Alerts, 1 Bookmarks

Last update time: 01/27/21, 10:40 AM | Creation time: 01/21/21, 03:09 PM

Entities (3): rodtrent@sixmilliond..., rodtrent_AndroidFor..., 104.211.51.211

Tactics (1): PreAttack

Incident workbook: Incident Overview

Analytic rule: Cloud Shell Execution

Tags: +

Investigate

Alerts | Bookmarks | Entities | Comments (2)

Search | Severity: All

Severity	ALERT NAME	Alert status	ALERT ID	PRODUCT NAME	EVENTS	CREATION TIME	TIME FRAME	
Low	Cloud Shell Execution	New	7aa55531-d0d7-529a-1...	Azure Sentinel	1	01/21/21, 03:09 PM	01/21/21, 07:29 AM - 01...	View playbooks

Alert playbooks

Cloud Shell Execution

Refresh

Playbooks | Runs

Search playbooks

Name	Status	Subscription		
{A} Block-AADUser	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} Get-IPReputation-RT	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} HavelBeenPwnedEmail	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} IncidentTodo	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} IPAddrGEO2Comments	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} Post-Message-Teams	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} RodIncident2OneNote	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} SendRodEmail	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} SendRodEmailAboutAllTables	Enabled	Azure Internal Billing 414651	Open designer	Run
{A} SendRodEmailw-IncidentLink	Enabled	Azure Internal Billing 414651	Open designer	Run

Analytic rule wizard - Create new rule

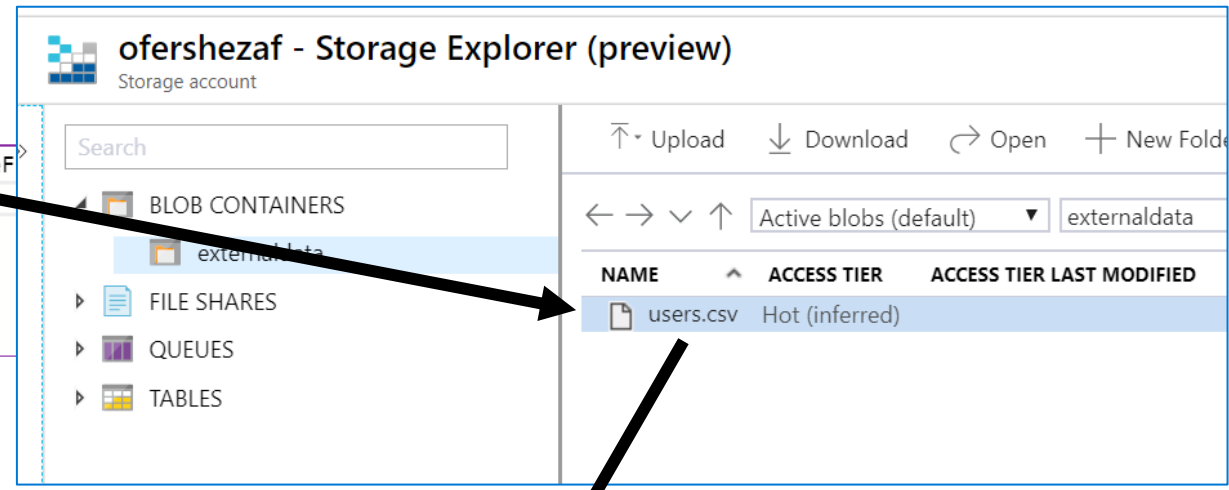
General Set rule logic Automated response Review and create

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	A	B	C	D
	1	UserName	DisplayName	Risk Location
Account	2	chris@contoso.com	Chris Green	70 { "City": "Redmond", "State": "Washintgon", "Country": "US" }
Host	3	ben@contoso.com	Ben Andrews	100 { "City": "Oxford", "State": "Oxfordshare", "Country": "UK" }
IP	4	nir@contoso.com	Nir Cohen	50 { "City": "Tel-Aviv", "State": "", "Country": "IL" }
URL	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

aka.ms/SentinelLookups

Azure Sentinel | Watchlist (Preview)

Selected workspace: 'rodazuresentinelworkspace'

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

General

2 Watchlists

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

Name	Alias	Source	Created Time	Last Updated
Botnet C2 IP Blocklist	FeodoTracker	ipblocklist.csv	11/04/20, 05:32 PM	11/04/20, 05:32 PM
Alienvault IP Reputation	AlienRod	alienrod.csv	01/12/21, 02:54 PM	01/12/21, 02:54 PM

How to Obtain and Import Data into the Azure Sentinel Watchlist Preview aka.ms/ASWatchList

Logs

RodAzureSentinelWorkspace

New Query 1*

RodAzureSentinelWorkspace

Run Time range: Last 24 hours

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
10a37b0-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-f2cd92193d3	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

 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>

<https://t.me/learningnets>

Cut!

<https://t.me/learningnets>

Action!



<https://t.me/learningnets>

Azure Sentinel | Incidents

Selected workspace: 'rodazuresentinelworkspace'

Search (Ctrl+/) Refresh Last 30 days Actions Security efficiency workbook (Preview)

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

104 Open incidents

102 New incidents

2 Active incidents

Open incidents by severity



Search by id or title

Severity: All

Status: New, Active

Product name: All

Owner: All

Auto-refresh incidents

Incident id	Title	Alerts	Product names	Created time	Last update time	Owner
649	Cloud Shell Execution	1	Azure Sentinel	01/21/21, 03:09 PM	01/27/21, 10:50 AM	Lee Majors
673	PowerShell Execution	1	Azure Sentinel	01/27/21, 10:40 AM	01/27/21, 10:40 AM	Unassigned
672	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/27/21, 07:36 AM	01/27/21, 07:36 AM	Unassigned
671	Excessive Windows logon failures	1	Azure Sentinel	01/27/21, 06:15 AM	01/27/21, 06:15 AM	Unassigned
670	Traffic detected from IP addresses recommended...	1	Azure Defender	01/26/21, 04:01 PM	01/26/21, 04:01 PM	Unassigned
669	Traffic detected from IP addresses recommended...	1	Azure Defender	01/26/21, 04:01 PM	01/26/21, 04:01 PM	Unassigned
668	PowerShell Execution	1	Azure Sentinel	01/26/21, 10:40 AM	01/26/21, 10:40 AM	Unassigned
667	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/26/21, 07:36 AM	01/26/21, 07:36 AM	Unassigned
666	Excessive Windows logon failures	1	Azure Sentinel	01/26/21, 06:15 AM	01/26/21, 06:15 AM	Unassigned
665	Traffic detected from IP addresses recommended...	1	Azure Defender	01/25/21, 03:27 PM	01/25/21, 03:27 PM	Unassigned
664	Traffic detected from IP addresses recommended...	1	Azure Defender	01/25/21, 03:27 PM	01/25/21, 03:27 PM	Unassigned
663	PowerShell Execution	1	Azure Sentinel	01/25/21, 10:40 AM	01/25/21, 10:40 AM	Unassigned
660	Traffic detected from IP addresses recommended...	1	Azure Defender	01/24/21, 04:14 PM	01/25/21, 09:43 AM	Unassigned
662	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/25/21, 07:36 AM	01/25/21, 07:55 AM	Lee Majors
661	Excessive Windows logon failures	1	Azure Sentinel	01/25/21, 06:15 AM	01/25/21, 06:15 AM	Unassigned
659	Failed logon attempts within 10 mins - RT	1	Azure Sentinel	01/24/21, 07:36 AM	01/24/21, 07:36 AM	Unassigned

< Previous 1 - 50 Next >

Cloud Shell Execution

Incident Id: 649

Lee Majors Owner

Active Status

Low Severity

1 Events 1 Alerts 1 Bookmarks

Last update time
01/27/21, 10:50 AM

Creation time
01/21/21, 03:09 PM

Entities (3)

- rodtrrent@sixmillio...
- rodtrrent_AndroidF...
- 104.211.51.211

Tactics (1)

- PreAttack

[View full details >](#)

Incident workbook
[Incident Overview](#)

Analytic rule
[Cloud Shell Execution](#)

Tags

+

Incident link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Insig...

Last comment

(Total: 2)

Investigate

View full details



That's a wrap!

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>

<https://t.me/learningnets>

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: [@rod trent](https://twitter.com/rod trent)

<https://t.me/learninghubs>

