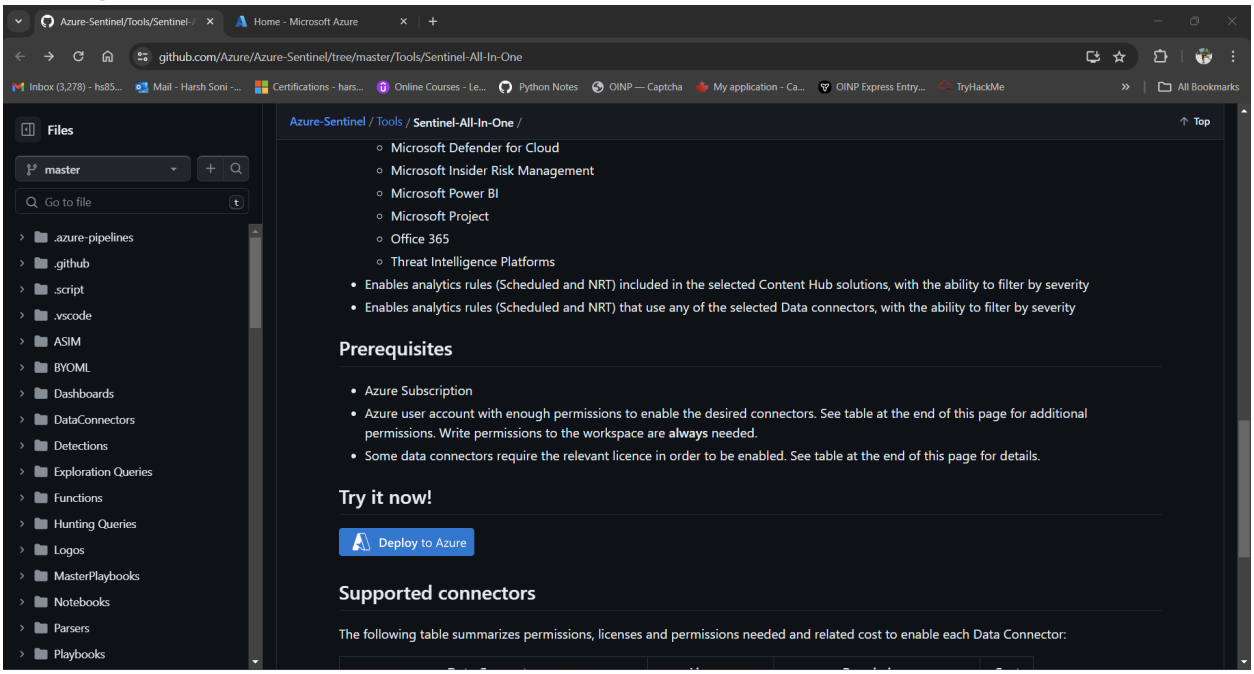
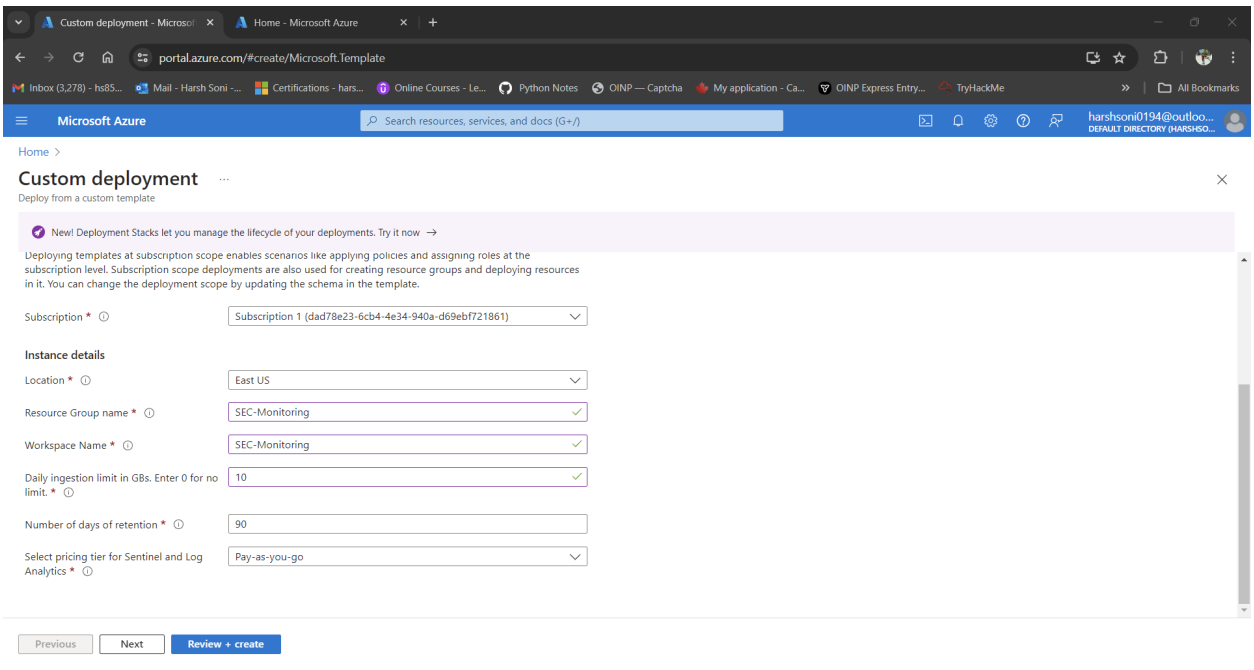
Microsoft Sentinel SIEM

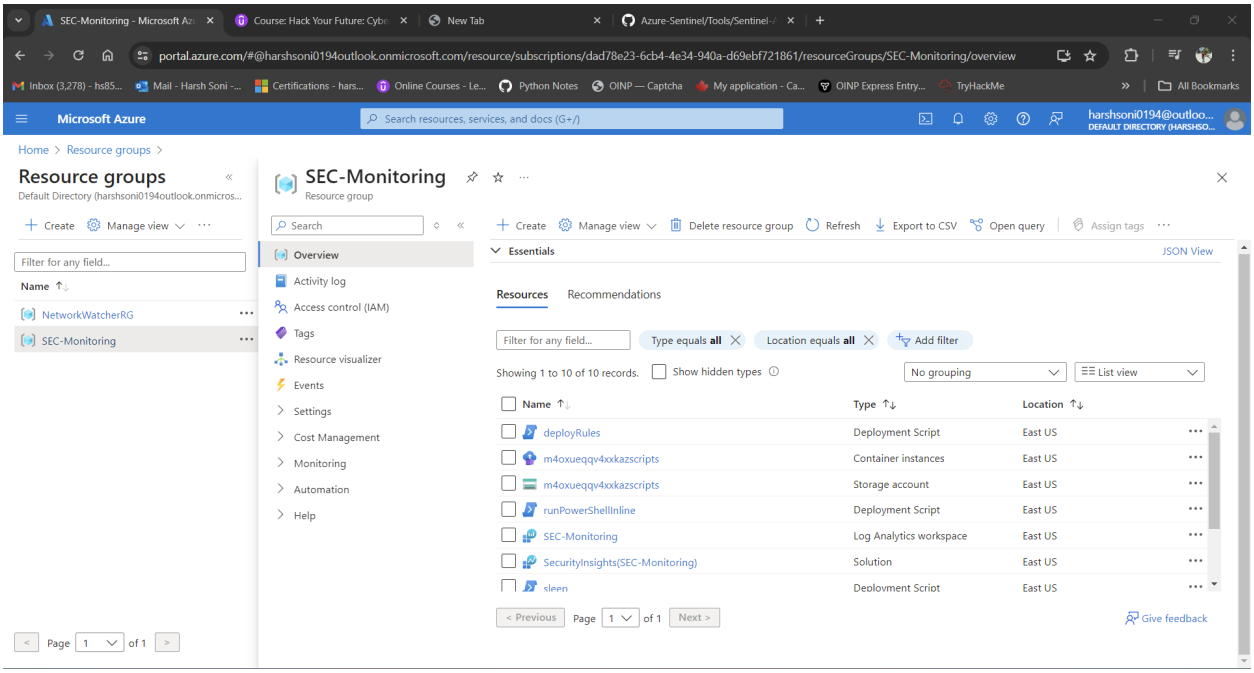
1) CREATE A SIEM IN AZURE

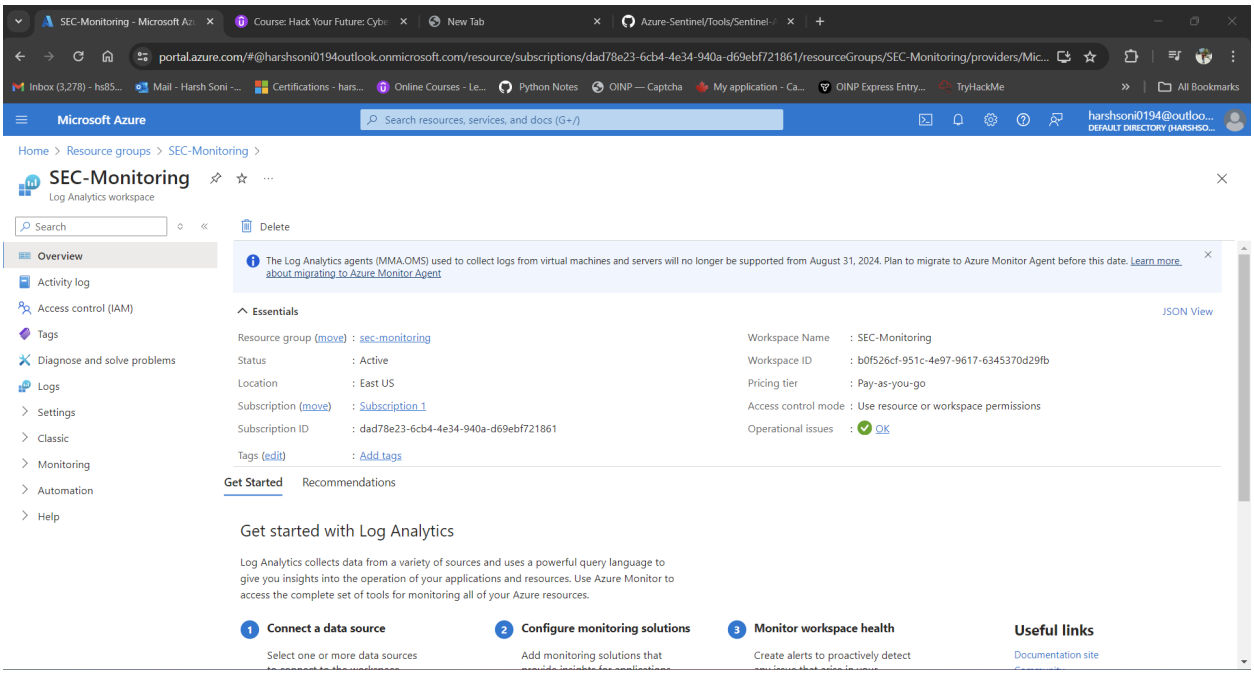
https://github.com/Azure/Azure-Sentinel/tree/master/Tools/Sentinel-All-In-One

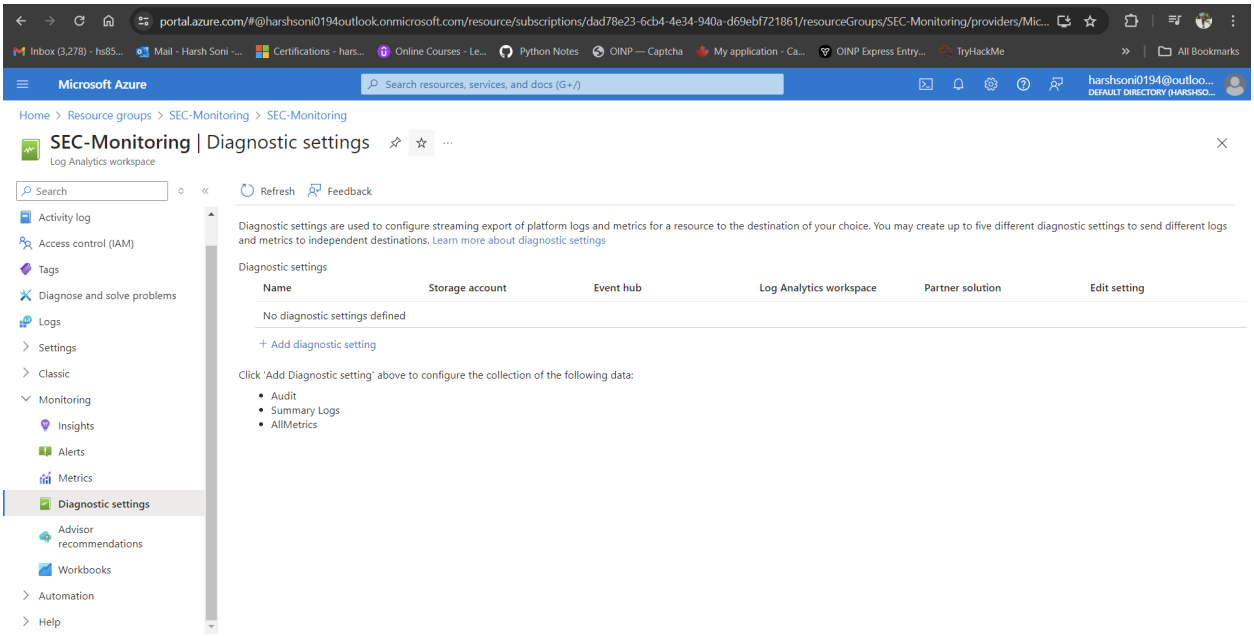


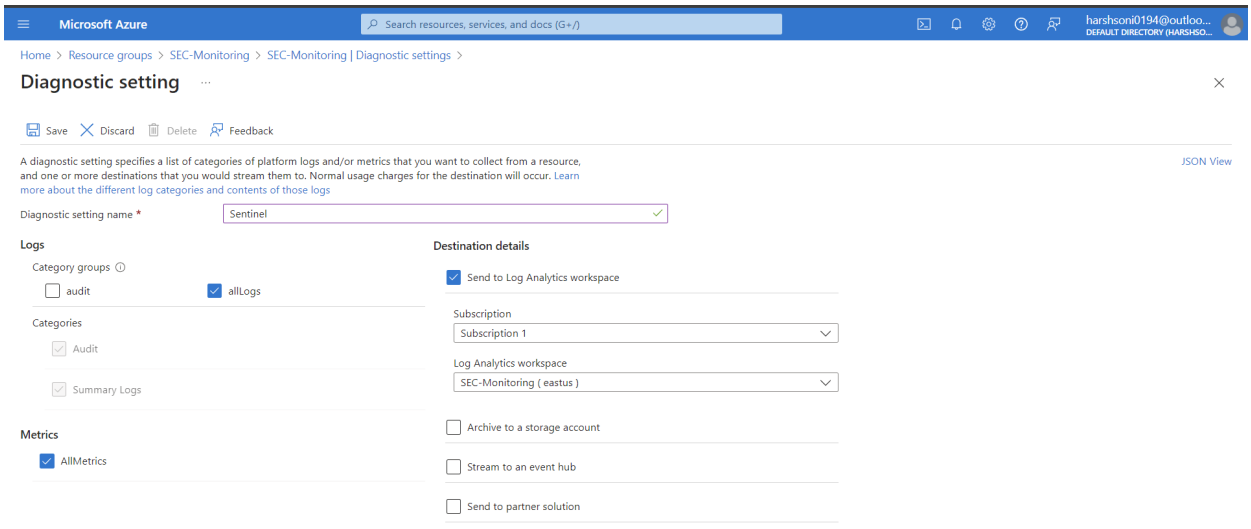


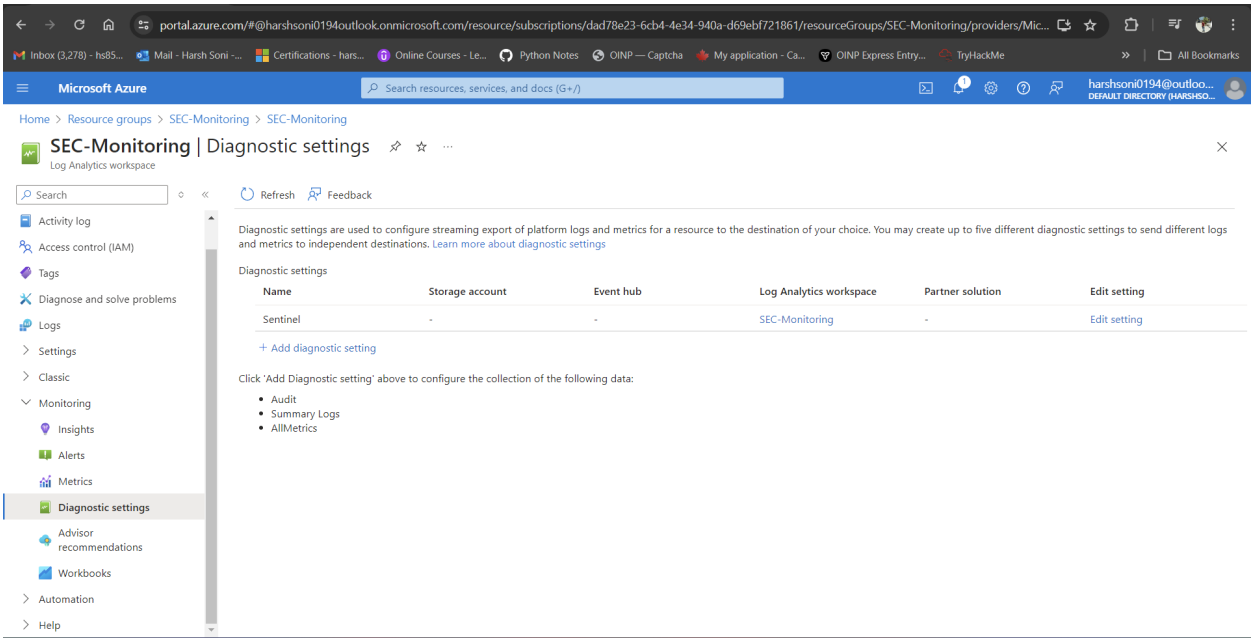
Exploring deployed cybersecurity Artifacts:



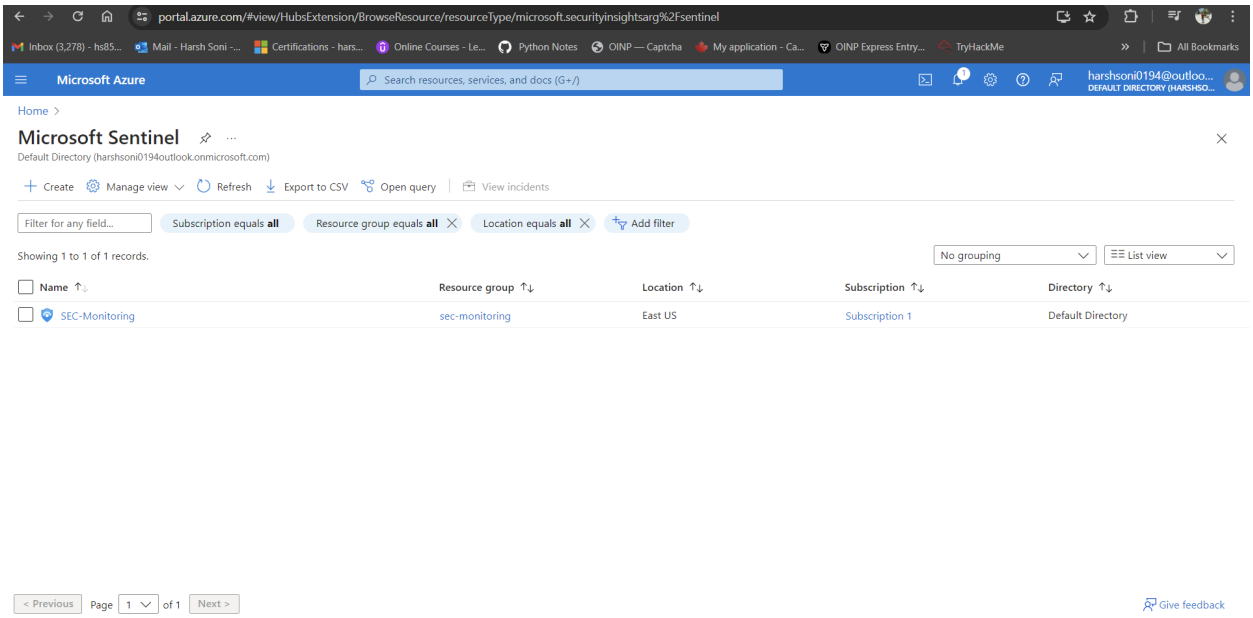


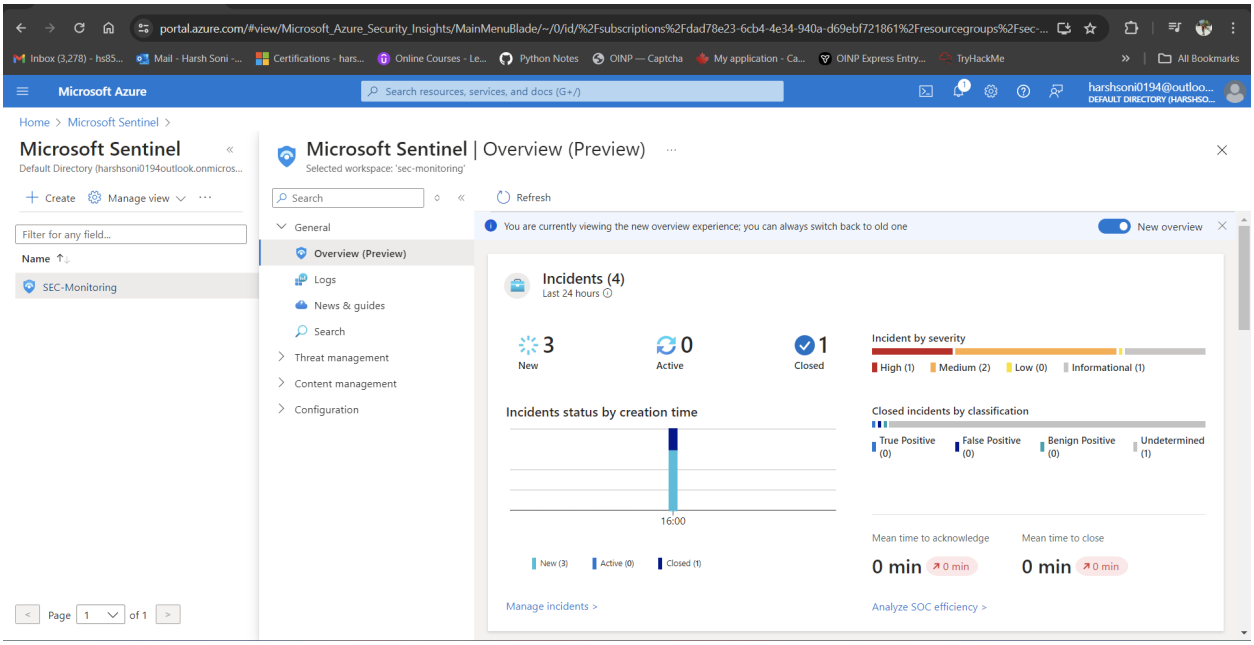

portal.azure.com/#@harshsoni0194outlook.onmicrosoft.com/resource/subscriptions/dad78e23-6cb4-4e34-940a-d69ebf721861/resourceGroups/SEC-Monitoring/providers/Mic...
Inbox (3,278) - hs85...
Mail - Harsh Soni -...
Certifications - hars...
Online Courses - Le...
Python Notes
OINP — Captcha
My application - Ca...
OINP Express Entry...
TryHackMe
All Bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
harshsoni0194@outloo...
DEFAULT DIRECTORY (HARSHSO...
Home > Resource groups > SEC-Monitoring > SEC-Monitoring
SEC-Monitoring | Diagnostic settings
Log Analytics workspace
Search
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Settings
Classic
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Advisor recommendations
Workbooks
Automation
Help
Refresh
Feedback
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:
Audit
Summary Logs
AllMetrics

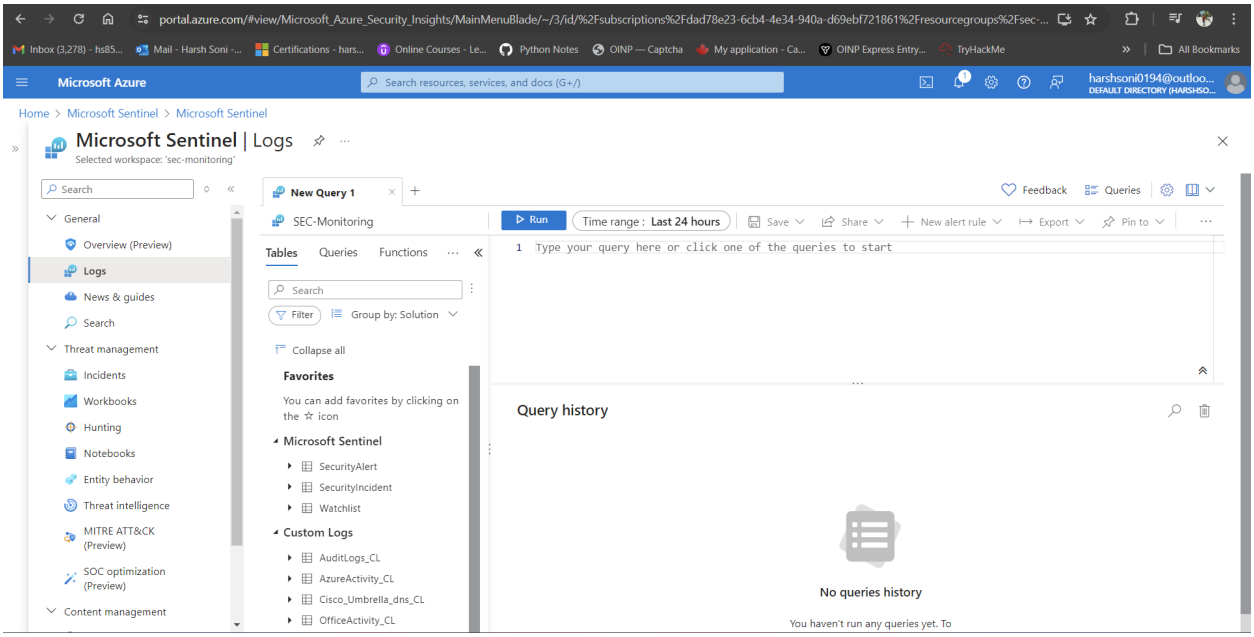


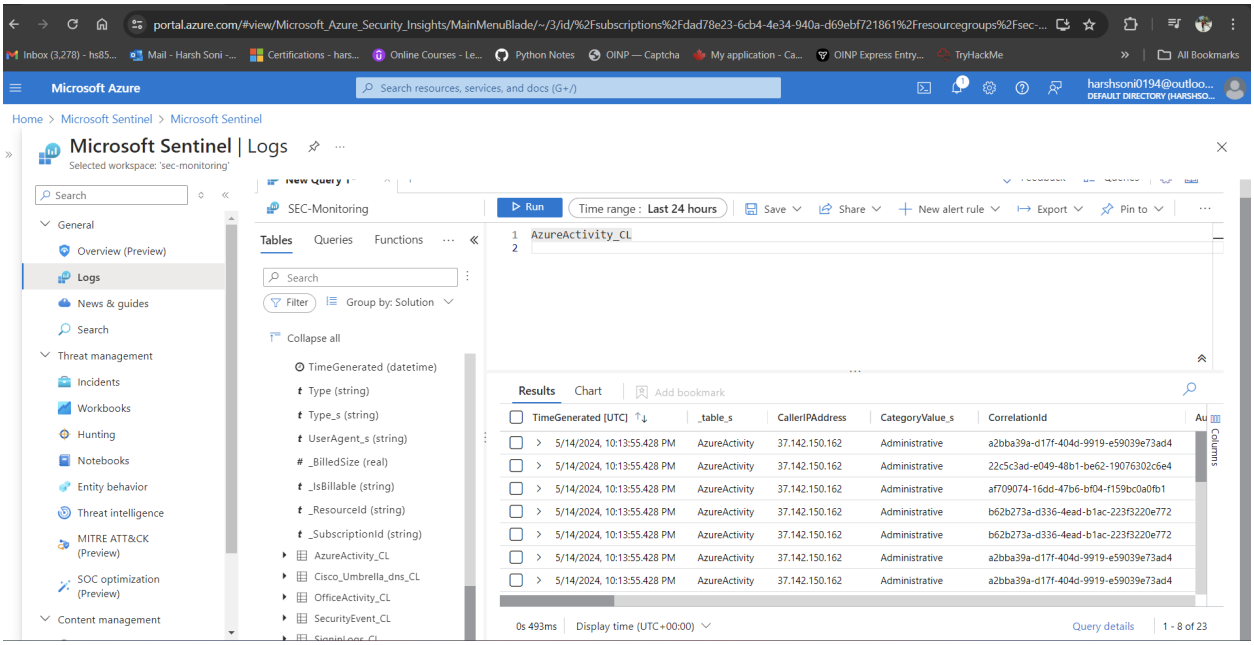


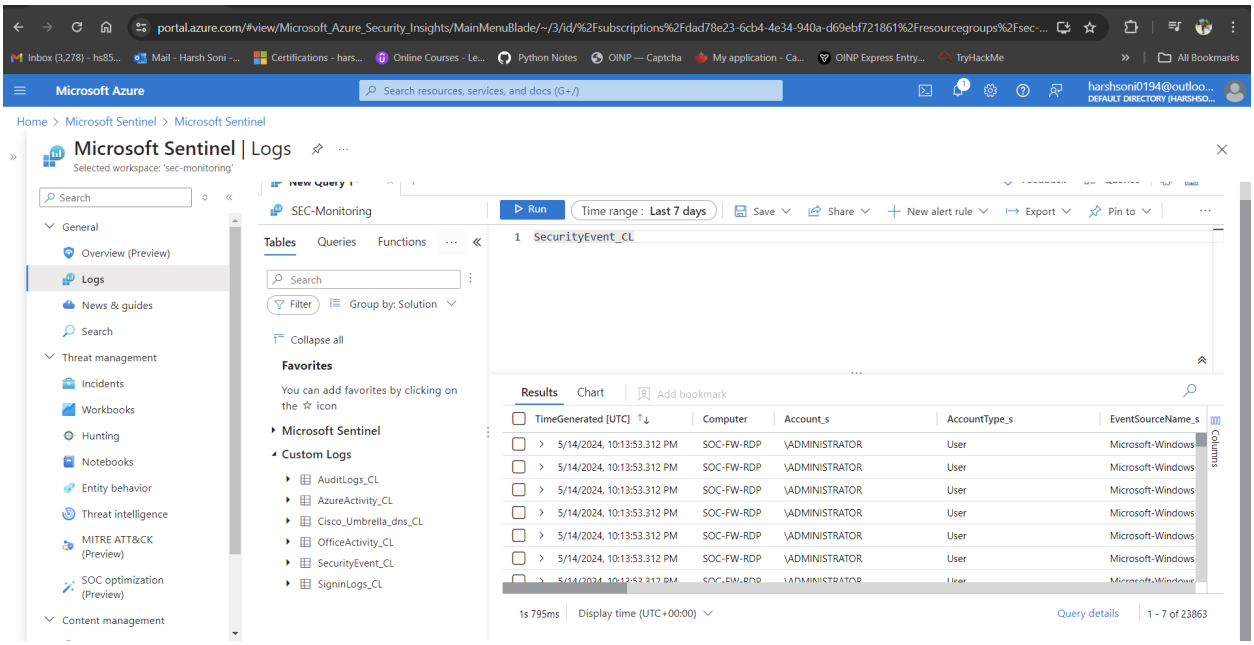
Exploring created Cloud SIEM solution

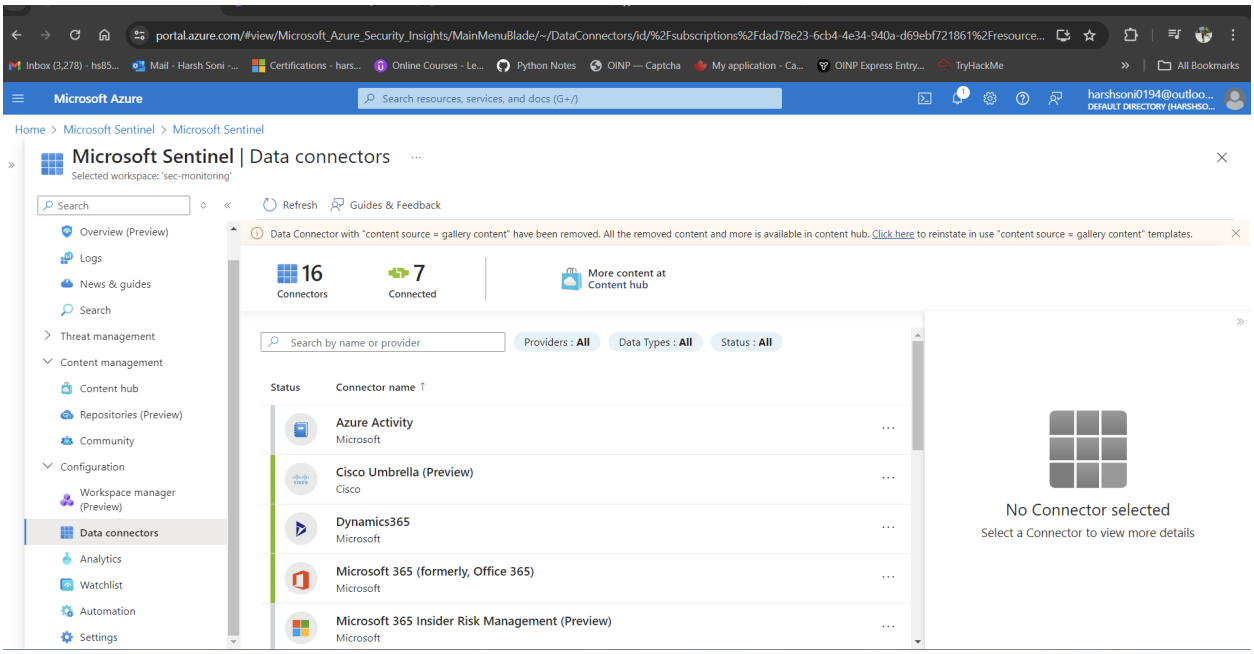

portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel
Microsoft Azure
Search resources, services, and docs (G+/)
Home
Microsoft Sentinel
Default Directory (harshsoni0194outlook.onmicrosoft.com)
Create
Manage view
Refresh
Export to CSV
Open query
View incidents
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 1 to 1 of 1 records.
No grouping
List view
Name
Resource group
Location
Subscription
Directory
SEC-Monitoring
sec-monitoring
East US
Subscription 1
Default Directory
< Previous
Page 1 of 1
Next >
Give feedback

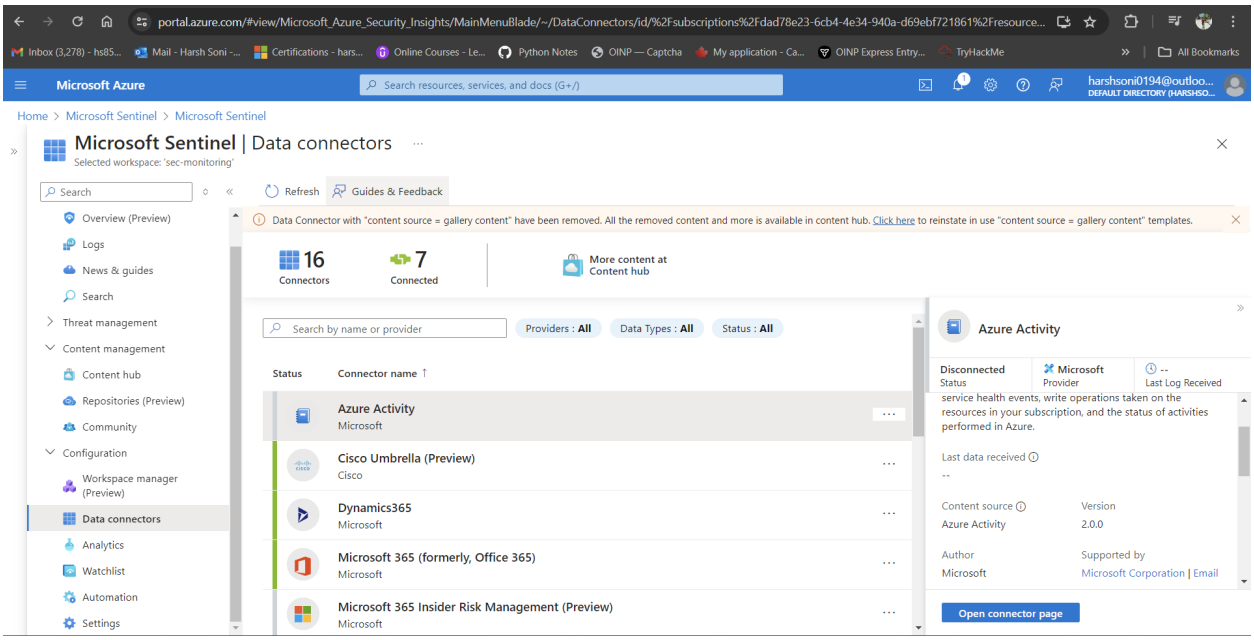

portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/0/id/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fresourcegroups%2Fsec-...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel
Microsoft Sentinel
Default Directory (harshsoni0194outlook.onmicros...
Create
Manage view
Filter for any field...
Name
SEC-Monitoring
Page 1 of 1
Microsoft Sentinel | Overview (Preview)
Selected workspace: 'sec-monitoring'
Search
Refresh
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Content management
Configuration
You are currently viewing the new overview experience; you can always switch back to old one
New overview
Incidents (4)
Last 24 hours
3
New
0
Active
1
Closed
Incident by severity
High (1)
Medium (2)
Low (0)
Informational (1)
Incidents status by creation time
16:00
New (3)
Active (0)
Closed (1)
Closed incidents by classification
True Positive (0)
False Positive (0)
Benign Positive (0)
Undetermined (1)
Mean time to acknowledge
0 min
0 min
Mean time to close
0 min
0 min
Manage incidents >
Analyze SOC efficiency >

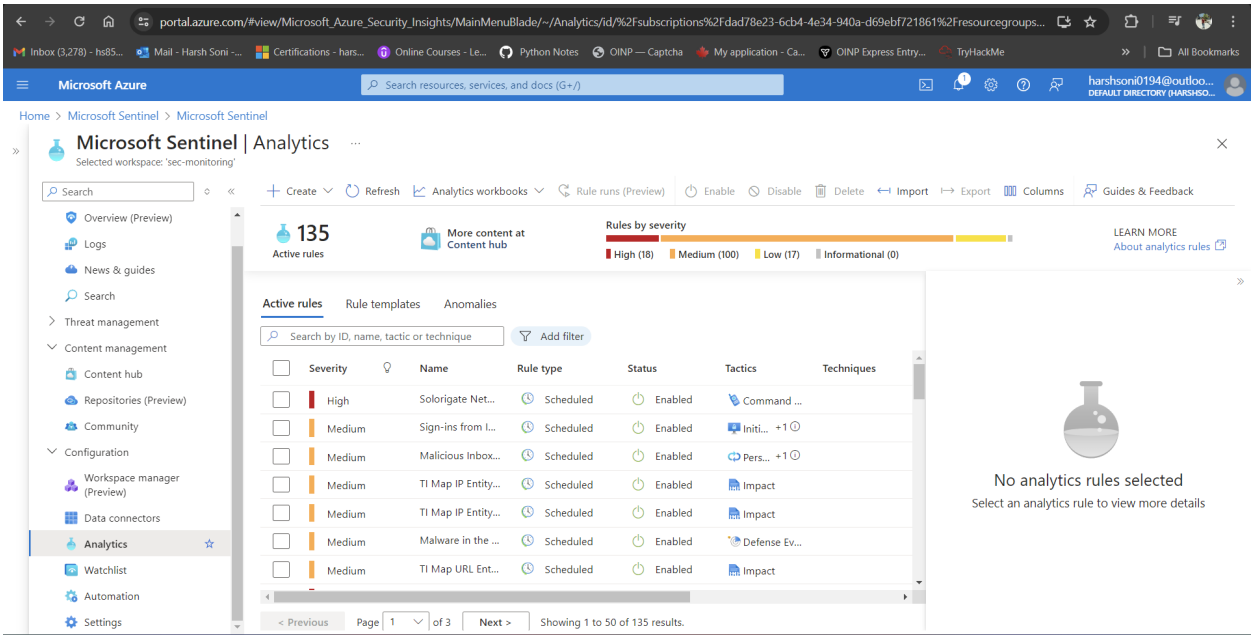

portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/3/id/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fresourcegroups%2Fsec-...
Microsoft Azure
Search resources, services, and docs (G+/)
harshsoni0194@outloo...
DEFAULT DIRECTORY (HARSHSO...
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'sec-monitoring'
New Query 1
SEC-Monitoring
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
Pin to
Feedback
Queries
Tables
Queries
Functions
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
Microsoft Sentinel
SecurityAlert
SecurityIncident
Watchlist
Custom Logs
AuditLogs_CL
AzureActivity_CL
Cisco_Umbrella_dns_CL
OfficeActivity_CL
1 Type your query here or click one of the queries to start
Query history
No queries history
You haven't run any queries yet. To
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization (Preview)
Content management

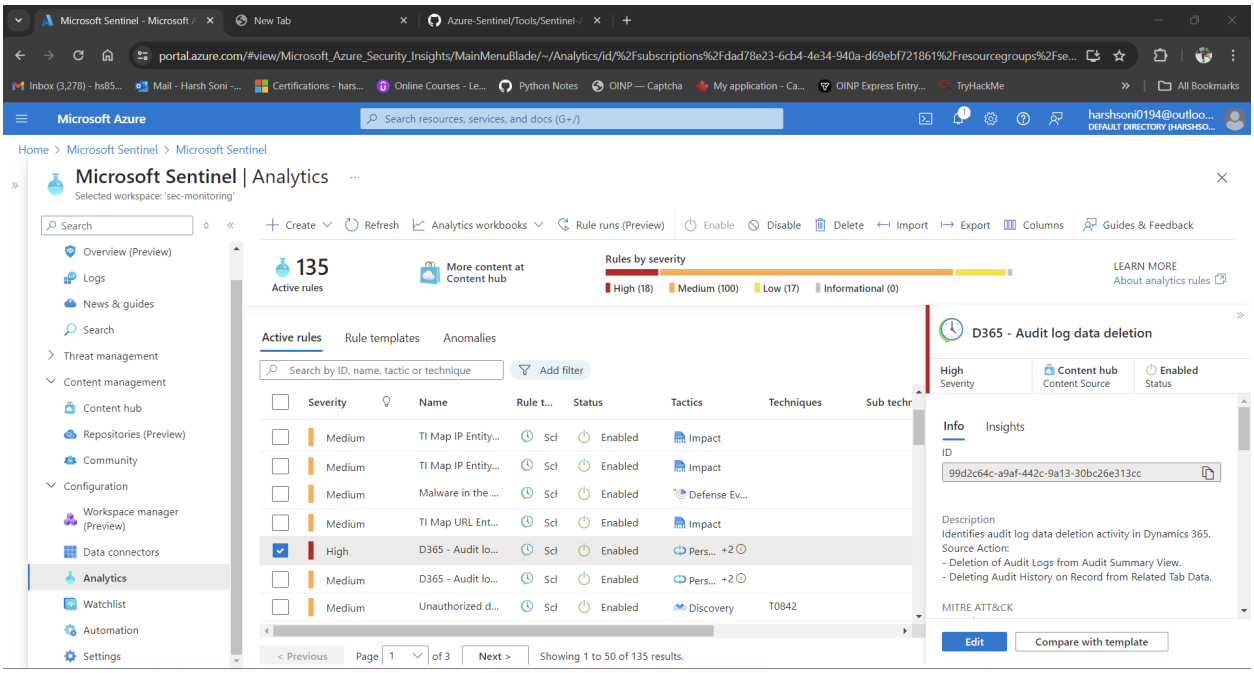

portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/3/id/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fresourcegroups%2Fsec-...
Microsoft Azure
Search resources, services, and docs (G+/)
harshsoni0194@outloo...
DEFAULT DIRECTORY (HARSHSO...
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'sec-monitoring'
SEC-Monitoring
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
Pin to
Tables
Queries
Functions
Filter
Group by: Solution
Collapse all
1 AzureActivity_CL
2
TimeGenerated (datetime)
Type (string)
Type_s (string)
UserAgent_s (string)
_BilledSize (real)
_IsBillable (string)
_ResourceId (string)
_SubscriptionId (string)
AzureActivity_CL
Cisco_Umbrella_dns_CL
OfficeActivity_CL
SecurityEvent_CL
Results
Chart
Add bookmark
TimeGenerated [UTC]
_table_s
CallerIPAddress
CategoryValue_s
CorrelationId
5/14/2024, 10:13:55.428 PM AzureActivity 37.142.150.162 Administrative a2bba39a-d17f-404d-9919-e59039e73ad4
5/14/2024, 10:13:55.428 PM AzureActivity 37.142.150.162 Administrative 22c5c3ad-e049-48b1-be62-19076302c6e4
5/14/2024, 10:13:55.428 PM AzureActivity 37.142.150.162 Administrative af709074-16dd-47b6-bf04-f159bc0a0fb1
5/14/2024, 10:13:55.428 PM AzureActivity 37.142.150.162 Administrative b62b273a-d336-4ead-b1ac-223f3220e772
5/14/2024, 10:13:55.428 PM AzureActivity 37.142.150.162 Administrative b62b273a-d336-4ead-b1ac-223f3220e772
5/14/2024, 10:13:55.428 PM AzureActivity 37.142.150.162 Administrative a2bba39a-d17f-404d-9919-e59039e73ad4
5/14/2024, 10:13:55.428 PM AzureActivity 37.142.150.162 Administrative a2bba39a-d17f-404d-9919-e59039e73ad4
Columns
0s 493ms
Display time (UTC+00:00)
Query details
1 - 8 of 23

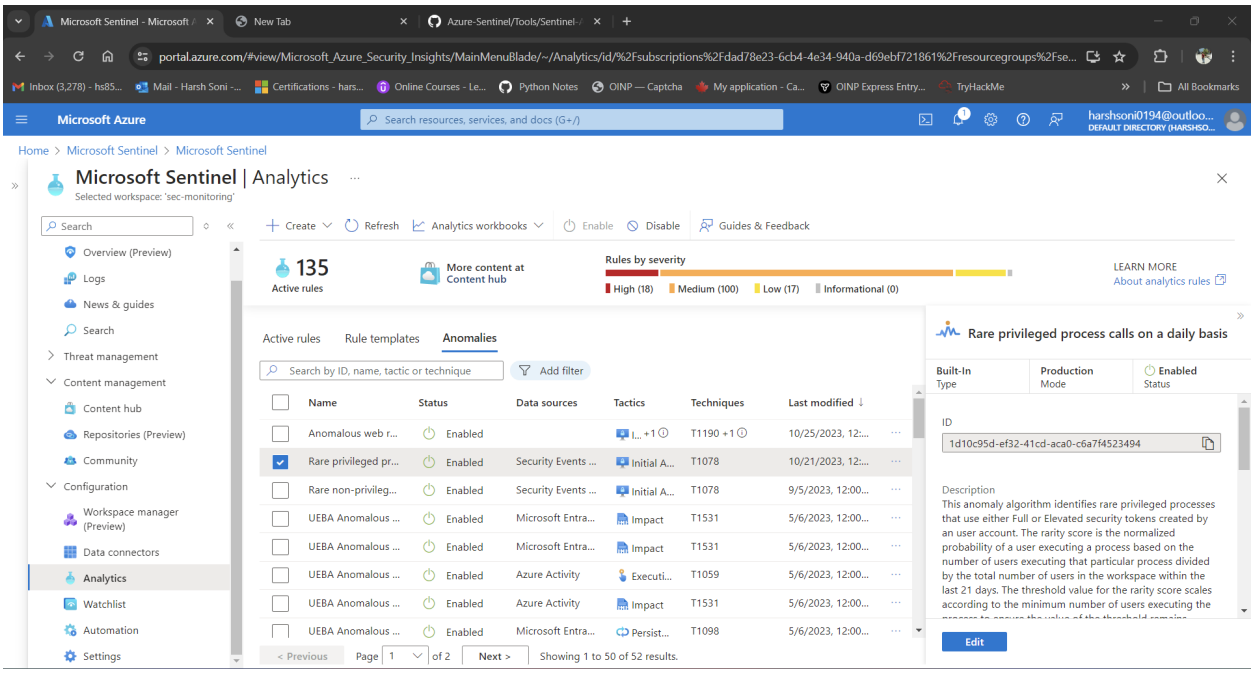

portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/3/id/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fresourcegroups%2Fsec-...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'sec-monitoring'
SEC-Monitoring
Run
Time range : Last 7 days
Save
Share
New alert rule
Export
Pin to
Tables
Queries
Functions
Favorites
You can add favorites by clicking on the ☆ icon
Microsoft Sentinel
Custom Logs
AuditLogs_CL
AzureActivity_CL
Cisco_Umbrella_dns_CL
OfficeActivity_CL
SecurityEvent_CL
SigninLogs_CL
1 SecurityEvent_CL
Results
Chart
TimeGenerated [UTC]
Computer
Account_s
AccountType_s
EventSourceName_s
5/14/2024, 10:13:53.312 PM
SOC-FW-RDP
\ADMINISTRATOR
User
Microsoft-Windows
1s 795ms
Display time (UTC+00:00)
Query details
1 - 7 of 23863


portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/DataConnectors/id/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fresource...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Data connectors
Selected workspace: 'sec-monitoring'
Refresh
Guides & Feedback
Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.
16
Connectors
7
Connected
More content at
Content hub
Search by name or provider
Providers : All
Data Types : All
Status : All
Status
Connector name
Azure Activity
Microsoft
Cisco Umbrella (Preview)
Cisco
Dynamics365
Microsoft
Microsoft 365 (formerly, Office 365)
Microsoft
Microsoft 365 Insider Risk Management (Preview)
Microsoft
No Connector selected
Select a Connector to view more details


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Data connectors
Selected workspace: 'sec-monitoring'
Refresh
Guides & Feedback
Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.
16 Connectors
7 Connected
More content at Content hub
Search by name or provider
Providers : All
Data Types : All
Status : All
Status
Connector name
Azure Activity
Microsoft
Cisco Umbrella (Preview)
Cisco
Dynamics365
Microsoft
Microsoft 365 (formerly, Office 365)
Microsoft
Microsoft 365 Insider Risk Management (Preview)
Microsoft
Azure Activity
Disconnected
Status
Microsoft
Provider
Last Log Received
service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.
Last data received
Content source
Azure Activity
Version
2.0.0
Author
Microsoft
Supported by
Microsoft Corporation | Email
Open connector page
Overview (Preview)
Logs
News & guides
Search
Threat management
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Watchlist
Automation
Settings

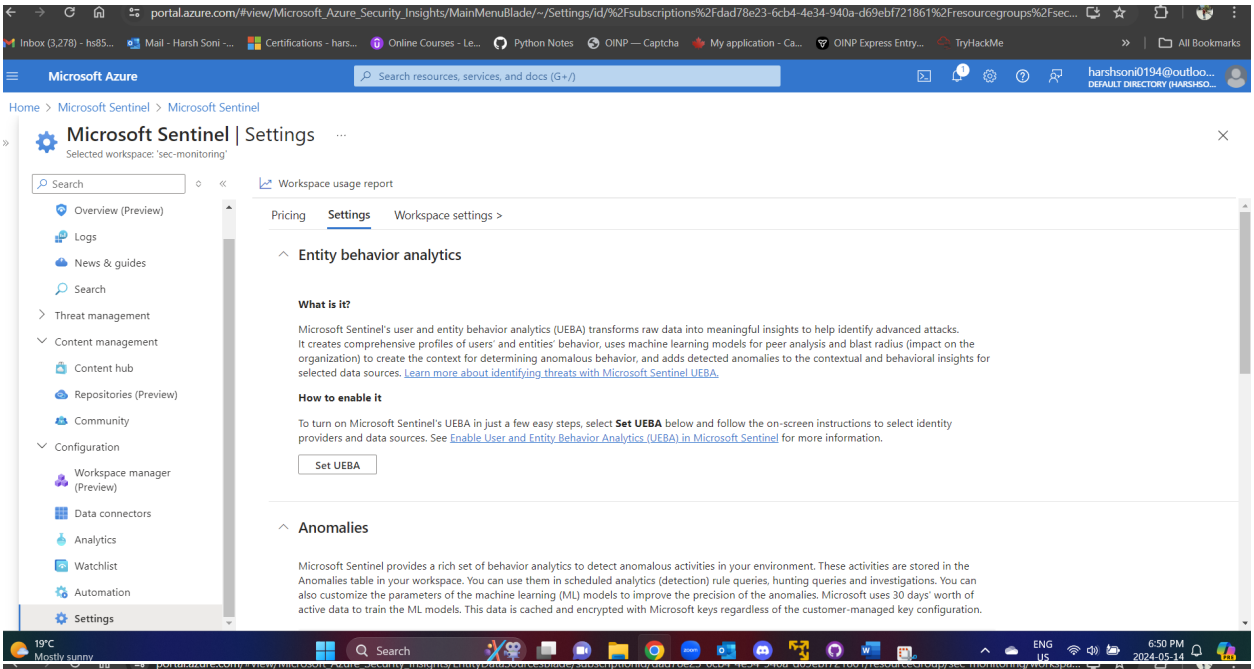

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Analytics
Selected workspace: 'sec-monitoring'
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Import
Export
Columns
Guides & Feedback
135 Active rules
More content at Content hub
Rules by severity
High (18)
Medium (100)
Low (17)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule type
Status
Tactics
Techniques
High
Sologate Net...
Medium
Sign-ins from I...
Medium
Malicious Inbox...
Medium
TI Map IP Entity...
Medium
TI Map IP Entity...
Medium
Malware in the ...
Medium
TI Map URL Ent...
Scheduled
Enabled
Command ...
Initi... +1
Pers... +1
Impact
Defense Ev...
< Previous
Page 1 of 3
Next >
Showing 1 to 50 of 135 results.
No analytics rules selected
Select an analytics rule to view more details
Overview (Preview)
Logs
News & guides
Search
Threat management
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Watchlist
Automation
Settings

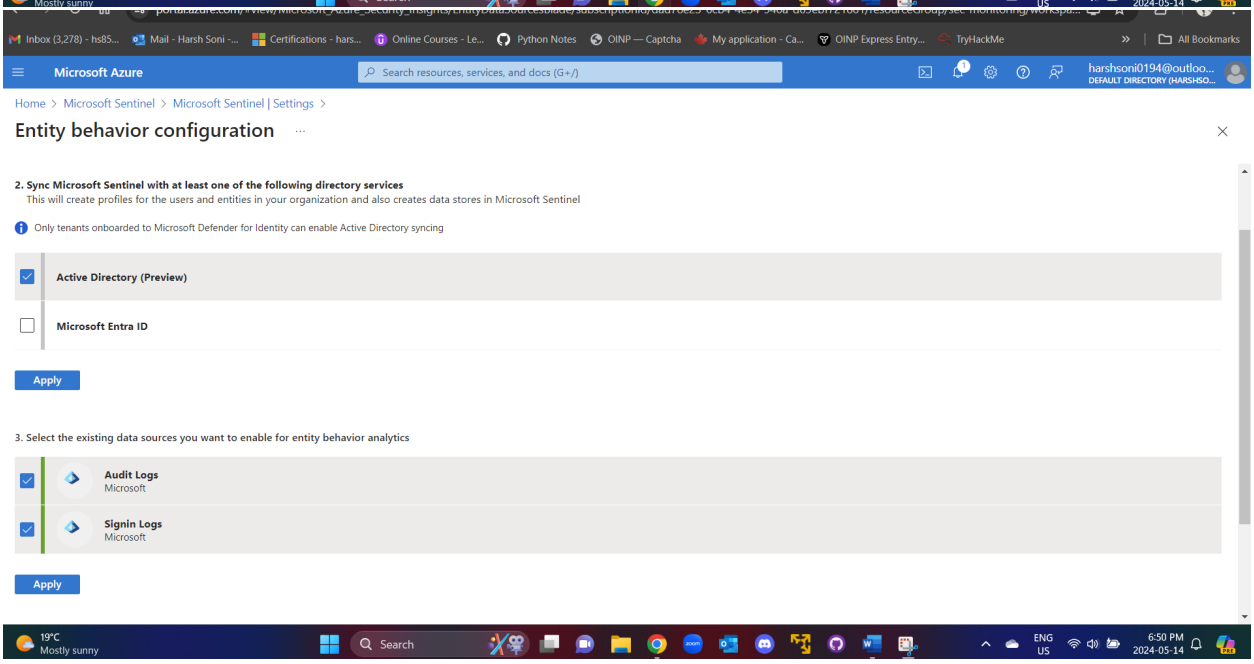

Microsoft Sentinel - Microsoft
New Tab
Azure-Sentinel/Tools/Sentinel-
portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/Analytics/id/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fresourcegroups%2Fse...
Microsoft Azure
Search resources, services, and docs (G+/)
harshsoni0194@outloo...
DEFAULT DIRECTORY (HARSHSO...
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Analytics
Selected workspace: 'sec-monitoring'
Search
Overview (Preview)
Logs
News & guides
Search
Threat management
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Watchlist
Automation
Settings
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
Disable
Delete
Import
Export
Columns
Guides & Feedback
135
Active rules
More content at Content hub
Rules by severity
High (18)
Medium (100)
Low (17)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule t...
Status
Tactics
Techniques
Sub techr
Medium
TI Map IP Entity...
Scl
Enabled
Impact
Medium
TI Map IP Entity...
Scl
Enabled
Impact
Medium
Malware in the ...
Scl
Enabled
Defense Ev...
Medium
TI Map URL Ent...
Scl
Enabled
Impact
High
D365 - Audit lo...
Scl
Enabled
Pers... +2
Medium
D365 - Audit lo...
Scl
Enabled
Pers... +2
Medium
Unauthorized d...
Scl
Enabled
Discovery
T0842
< Previous
Page 1 of 3
Next >
Showing 1 to 50 of 135 results.
D365 - Audit log data deletion
High
Severity
Content hub
Content Source
Enabled
Status
Info
Insights
ID
99d2c64c-a9af-442c-9a13-30bc26e313cc
Description
Identifies audit log data deletion activity in Dynamics 365.
Source Action:
- Deletion of Audit Logs from Audit Summary View.
- Deleting Audit History on Record from Related Tab Data.
MITRE ATT&CK
Edit
Compare with template


Microsoft Sentinel - Microsoft
New Tab
Azure-Sentinel/Tools/Sentinel-
portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/Analytics/id/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fresourcegroups%2Fse...
Microsoft Azure
Search resources, services, and docs (G+/)
harshsoni0194@outloo...
DEFAULT DIRECTORY (HARSHSO...
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Analytics
Selected workspace: 'sec-monitoring'
Search
Overview (Preview)
Logs
News & guides
Search
Threat management
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Watchlist
Automation
Settings
Create
Refresh
Analytics workbooks
Enable
Disable
Guides & Feedback
135
Active rules
More content at Content hub
Rules by severity
High (18)
Medium (100)
Low (17)
Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Name
Status
Data sources
Tactics
Techniques
Last modified
Anomalous web r...
Enabled
I... +1
T1190 +1
10/25/2023, 12:...
Rare privileged pr...
Enabled
Security Events ...
Initial A...
T1078
10/21/2023, 12:...
Rare non-privileg...
Enabled
Security Events ...
Initial A...
T1078
9/5/2023, 12:00...
UEBA Anomalous ...
Enabled
Microsoft Entra...
Impact
T1531
5/6/2023, 12:00...
UEBA Anomalous ...
Enabled
Microsoft Entra...
Impact
T1531
5/6/2023, 12:00...
UEBA Anomalous ...
Enabled
Azure Activity
Executi...
T1059
5/6/2023, 12:00...
UEBA Anomalous ...
Enabled
Azure Activity
Impact
T1531
5/6/2023, 12:00...
UEBA Anomalous ...
Enabled
Microsoft Entra...
Persist...
T1098
5/6/2023, 12:00...
< Previous
Page 1 of 2
Next >
Showing 1 to 50 of 52 results.
Rare privileged process calls on a daily basis
Built-In
Type
Production
Mode
Enabled
Status
ID
1d10c95d-ef32-41cd-aca0-c6a7f4523494
Description
This anomaly algorithm identifies rare privileged processes that use either Full or Elevated security tokens created by an user account. The rarity score is the normalized probability of a user executing a process based on the number of users executing that particular process divided by the total number of users in the workspace within the last 21 days. The threshold value for the rarity score scales according to the minimum number of users executing the
Edit

ENABLE ARTIFICIAL INTELLIGENCE IN SIEM

SET UEBA





Playbook permissions

What is it?

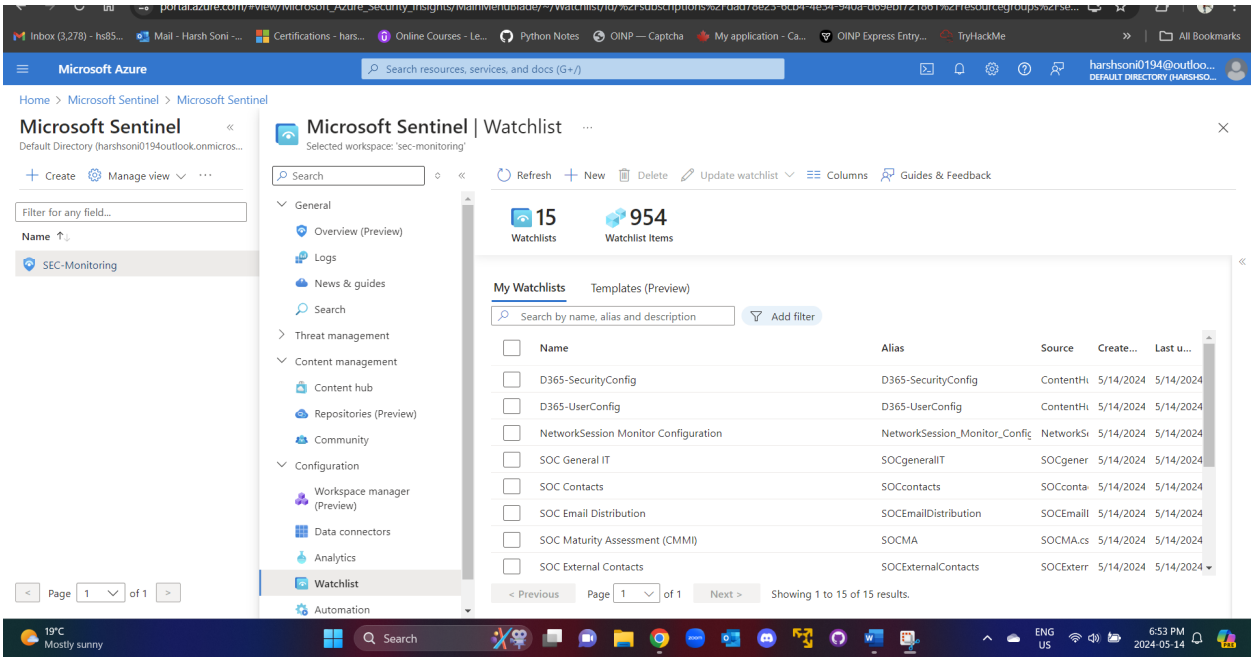
Automation rules allow you to centrally manage all the automation of incident handling. Automation rules streamline automation use in Microsoft Sentinel and enable you to simplify complex workflows for your incident orchestration processes.

Playbook permissions

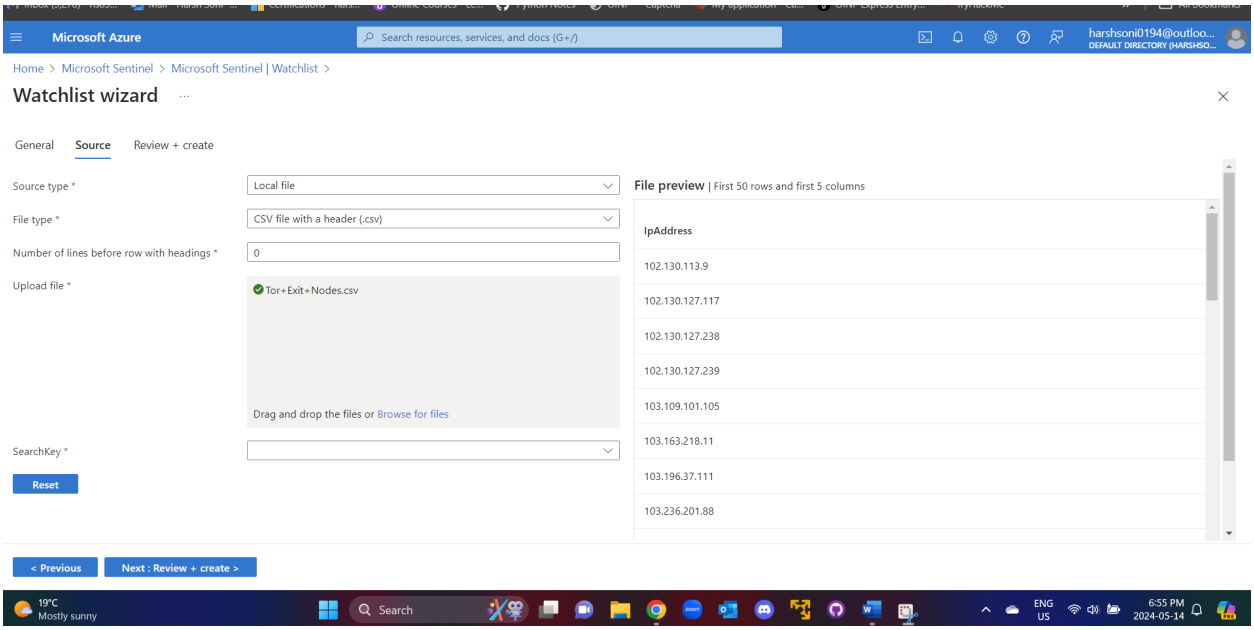
Microsoft Sentinel automation rules can run Logic App playbooks to integrate with other services or create complex logic chains for incident handling. Explicit permissions are required to use this functionality.

Configure permissions

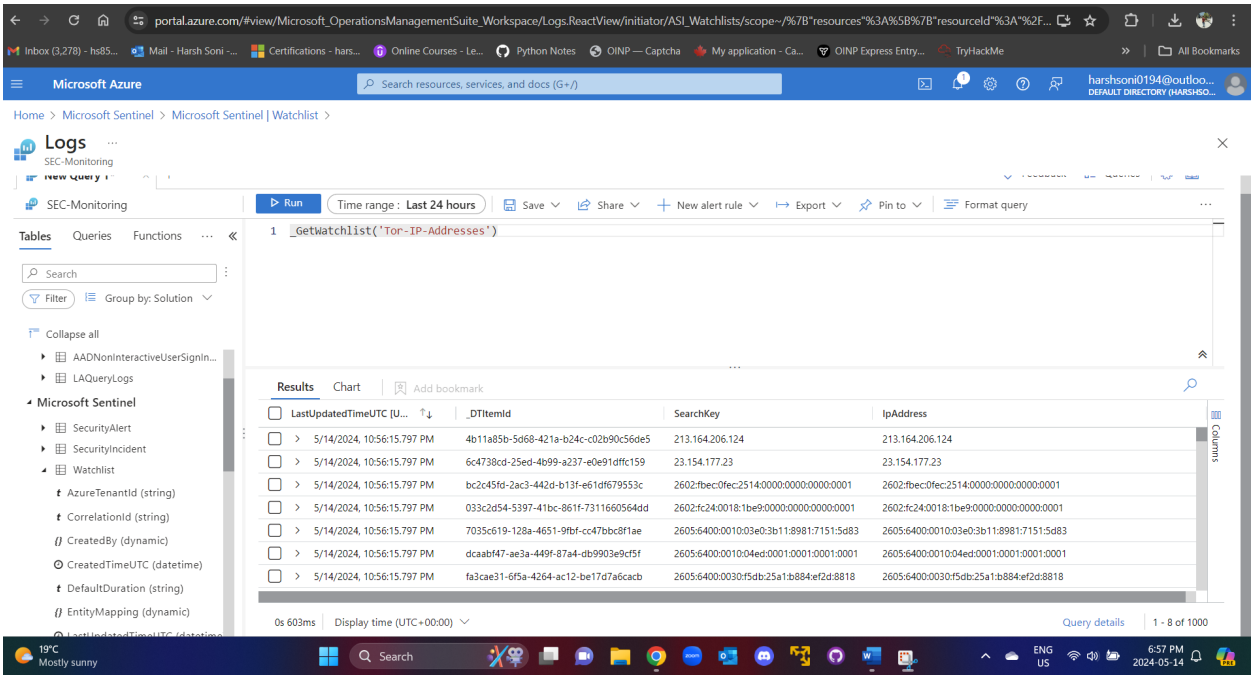
Create a Watchlist to Detect Cybersecurity Threats:



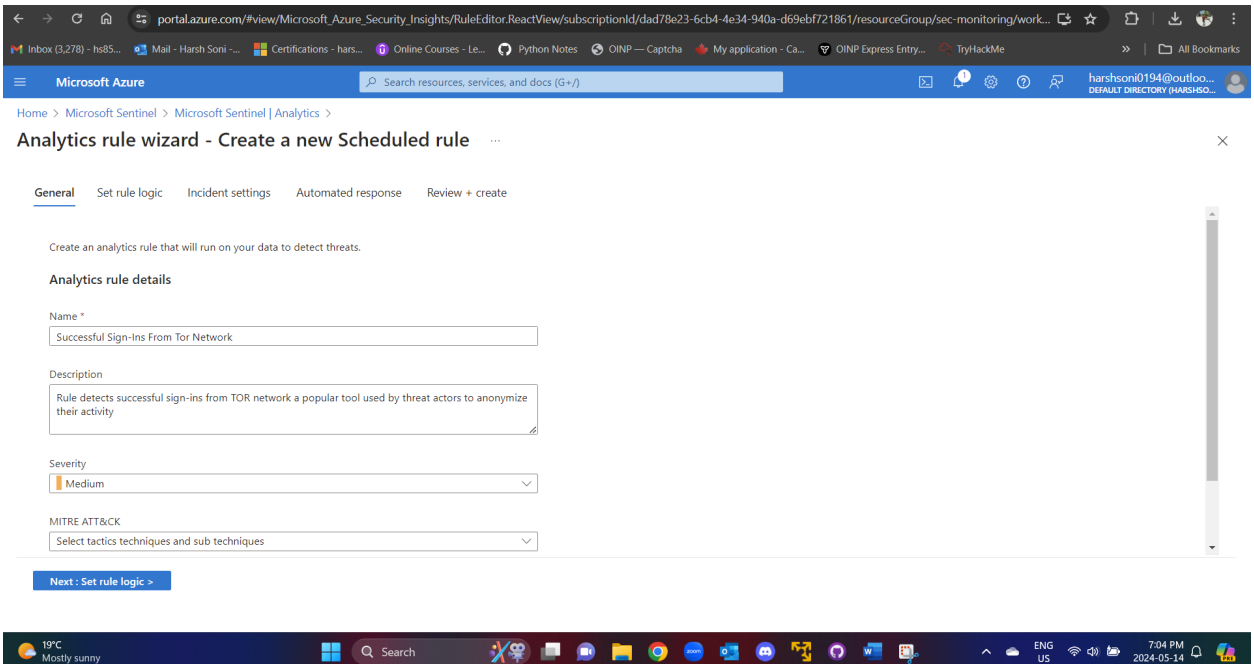
Upload a TOR FILE:

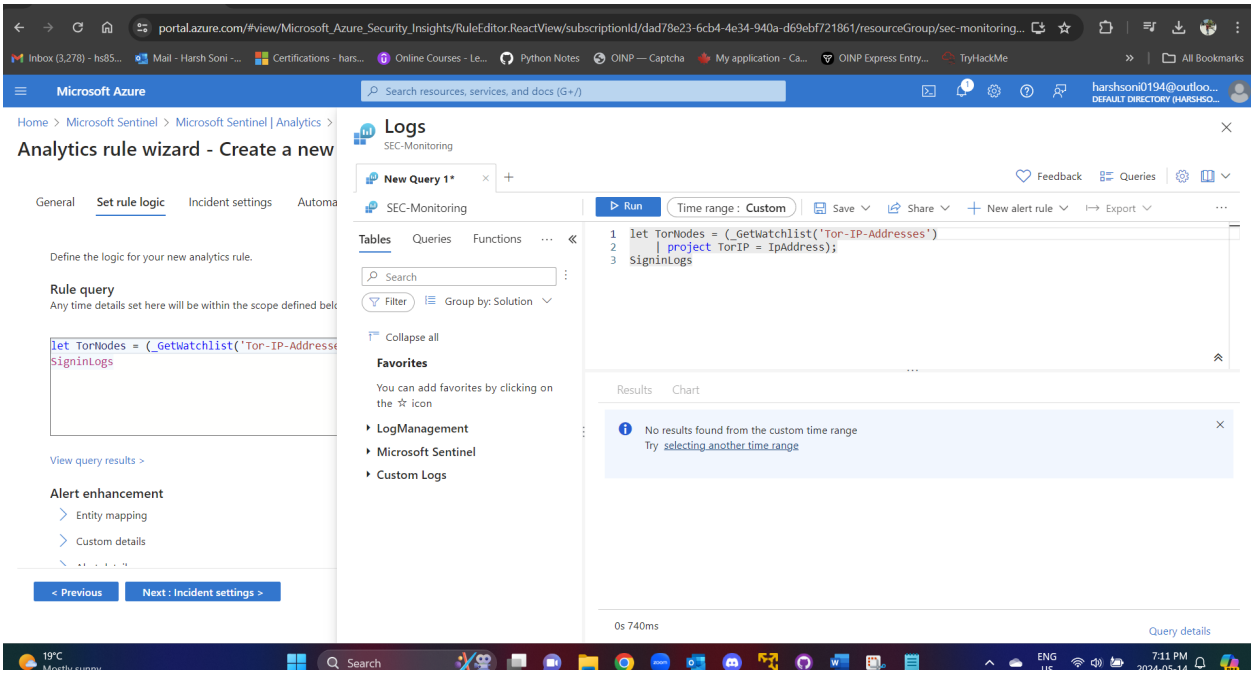


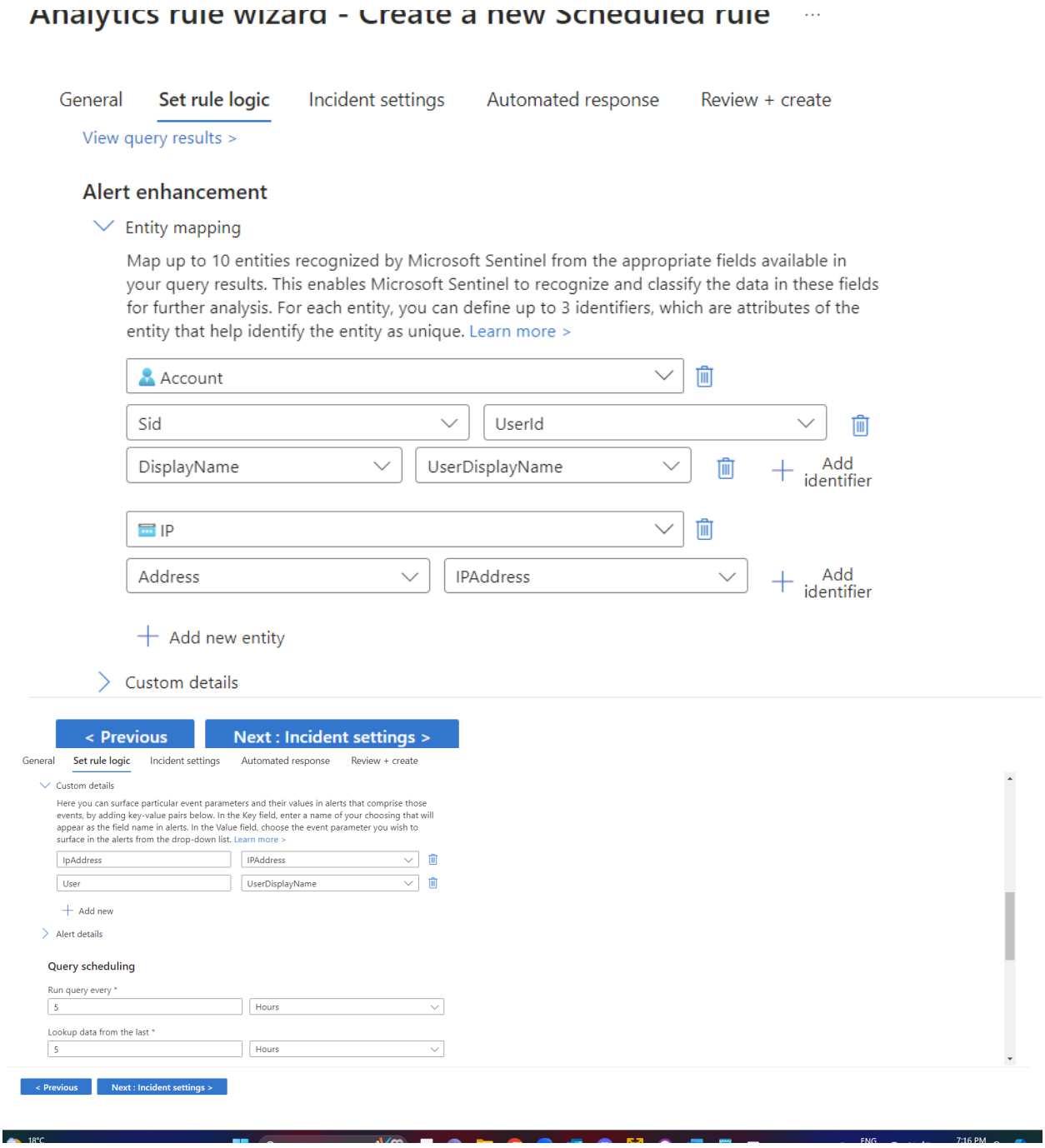
Calling Watchlist using KQL:

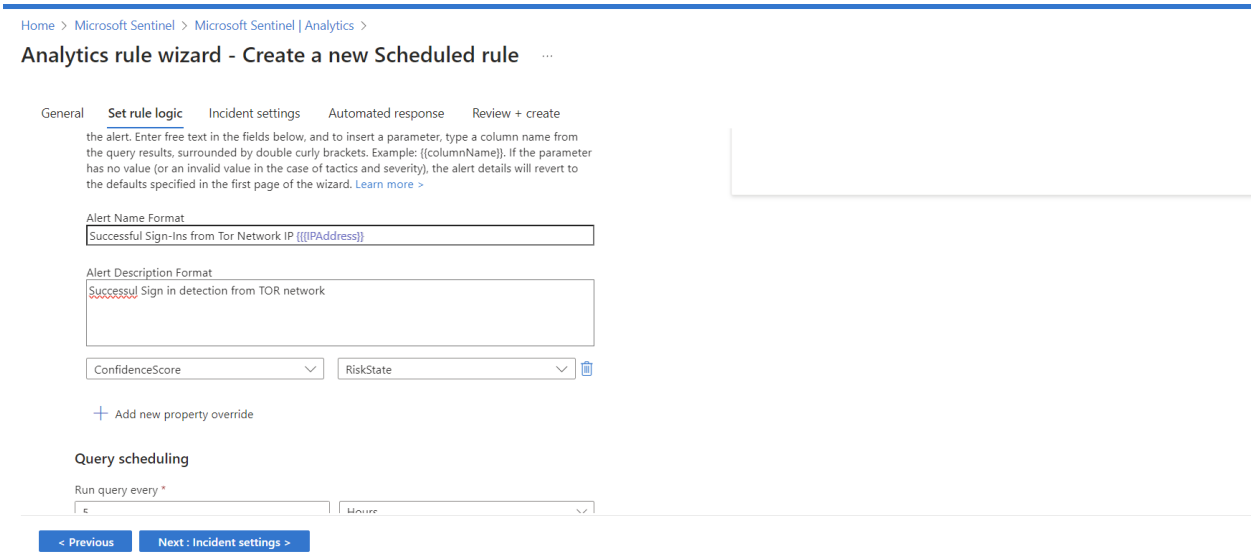


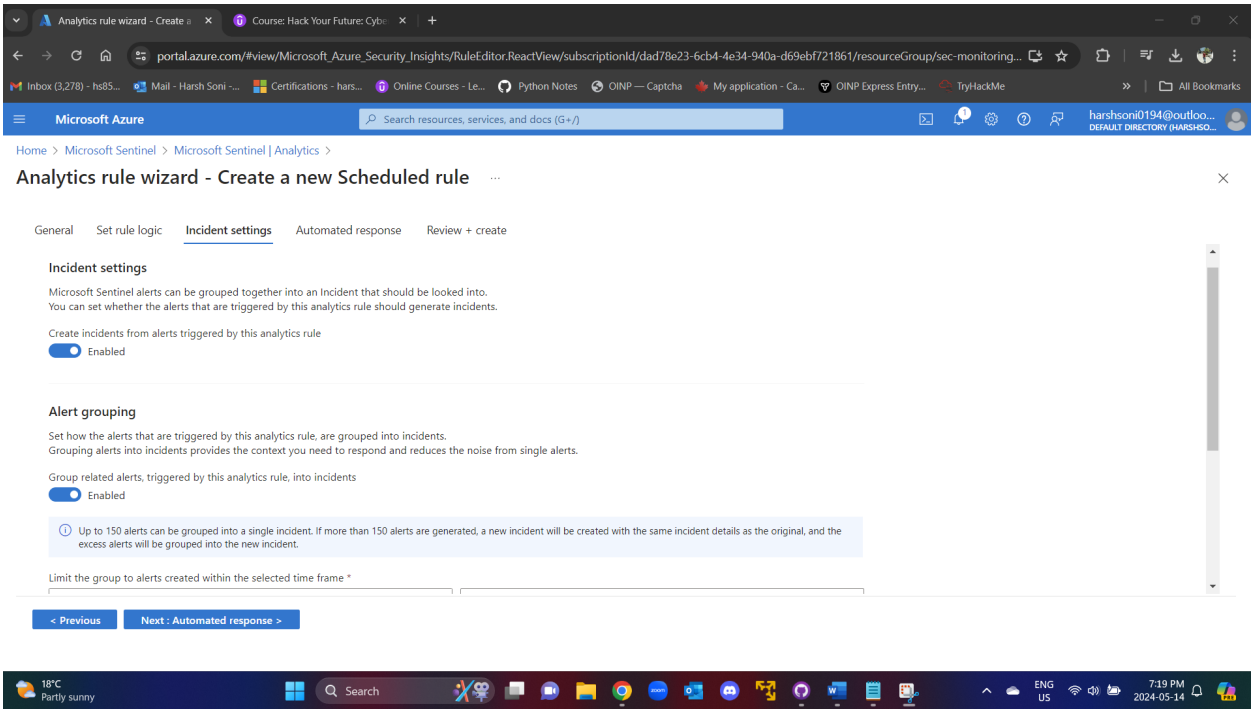
Create Detection Rule for Cybersecurity Threat

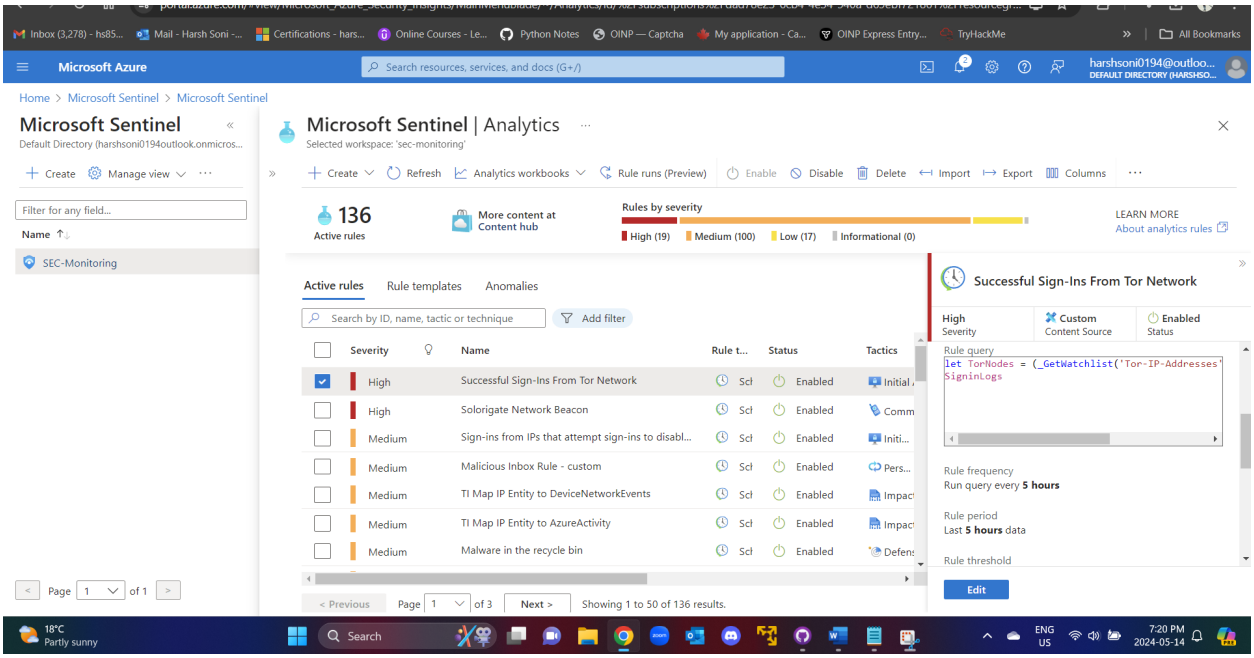

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
Create an analytics rule that will run on your data to detect threats.
Analytics rule details
Name *
Successful Sign-Ins From Tor Network
Description
Rule detects successful sign-ins from TOR network a popular tool used by threat actors to anonymize their activity
Severity
Medium
MITRE ATT&CK
Select tactics techniques and sub techniques
Next : Set rule logic >


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new
General
Set rule logic
Incident settings
Define the logic for your new analytics rule.
Rule query
Any time details set here will be within the scope defined bel
let TorNodes = (_GetWatchlist('Tor-IP-Addresse
SigninLogs
View query results >
Alert enhancement
Entity mapping
Custom details
< Previous
Next : Incident settings >
Logs
SEC-Monitoring
New Query 1*
SEC-Monitoring
Run
Time range : Custom
Save
Share
New alert rule
Export
Feedback
Queries
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
LogManagement
Microsoft Sentinel
Custom Logs
let TorNodes = (_GetWatchlist('Tor-IP-Addresses')
| project TorIP = IpAddress);
SigninLogs
Results
Chart
No results found from the custom time range
Try selecting another time range
0s 740ms
Query details

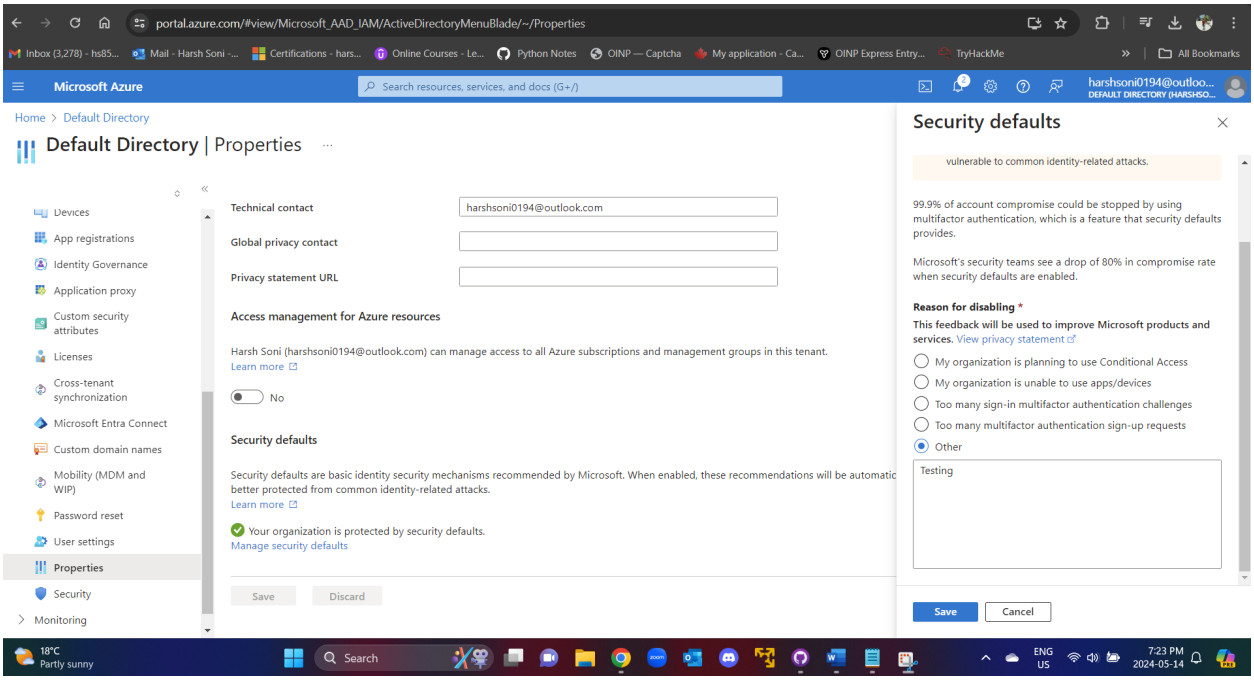

Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
View query results >
Alert enhancement
Entity mapping
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. Learn more >
Account
Sid
UserId
DisplayName
UserDisplayName
Add identifier
IP
Address
IPAddress
Add identifier
Add new entity
Custom details
< Previous
Next : Incident settings >
General
Set rule logic
Incident settings
Automated response
Review + create
Custom details
Here you can surface particular event parameters and their values in alerts that comprise those events, by adding key-value pairs below. In the Key field, enter a name of your choosing that will appear as the field name in alerts. In the Value field, choose the event parameter you wish to surface in the alerts from the drop-down list. Learn more >
IpAddress
IPAddress
User
UserDisplayName
Add new
Alert details
Query scheduling
Run query every *
5
Hours
Lookup data from the last *
5
Hours
< Previous
Next : Incident settings >

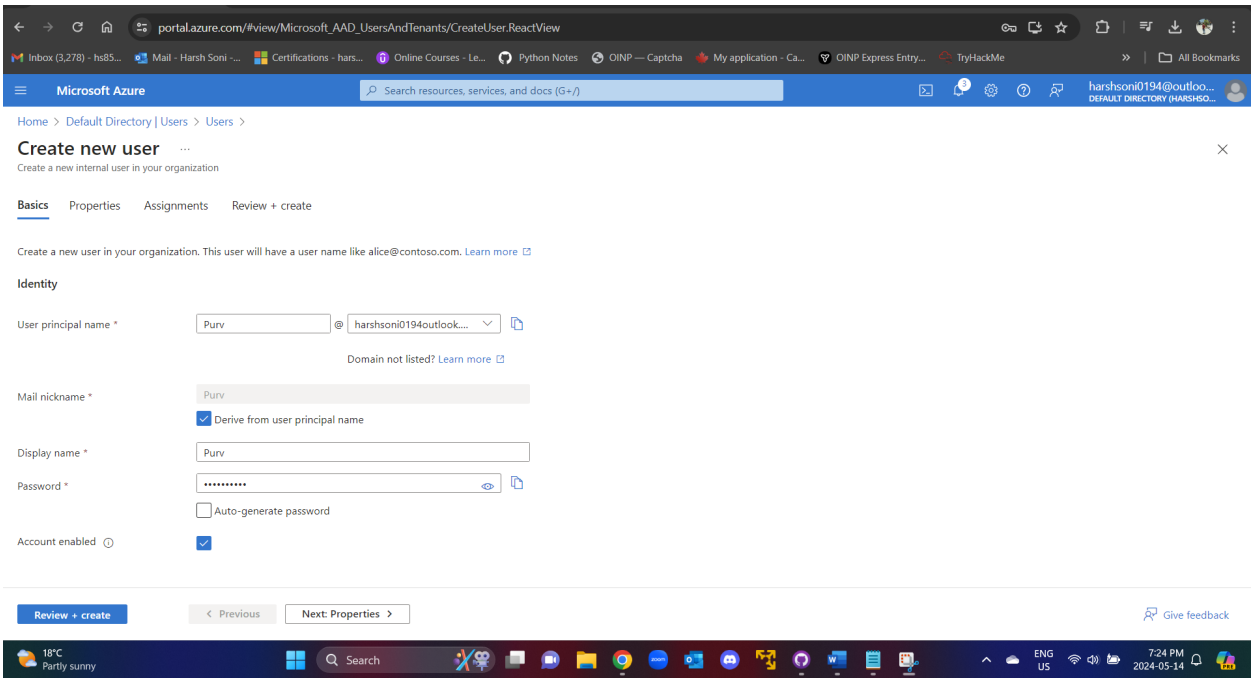

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
the alert. Enter free text in the fields below, and to insert a parameter, type a column name from the query results, surrounded by double curly brackets. Example: {{columnName}}. If the parameter has no value (or an invalid value in the case of tactics and severity), the alert details will revert to the defaults specified in the first page of the wizard. Learn more >
Alert Name Format
Successful Sign-Ins from Tor Network IP {{IPAddress}}
Alert Description Format
Successul Sign in detection from TOR network
ConfidenceScore
RiskState
Add new property override
Query scheduling
Run query every *
< Previous
Next : Incident settings >

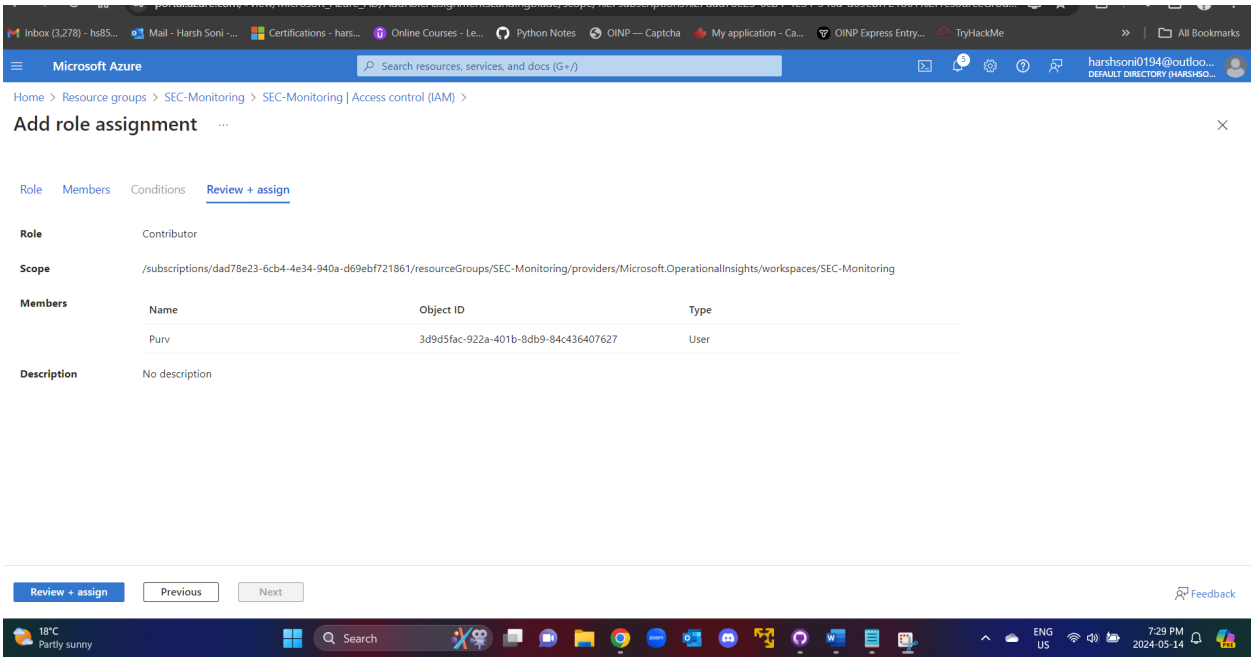

Analytics rule wizard - Create a
Course: Hack Your Future: Cybe
portal.azure.com/#view/Microsoft_Azure_Security_Insights/RuleEditor.ReactView/subscriptionId/dad78e23-6cb4-4e34-940a-d69ebf721861/resourceGroup/sec-monitoring...
Microsoft Azure
Search resources, services, and docs (G+/)
harshsoni0194@outloo...
DEFAULT DIRECTORY (HARSHSO...
Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create
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
Alert grouping
Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.
Group related alerts, triggered by this analytics rule, into incidents
Enabled
Up to 150 alerts can be grouped into a single incident. If more than 150 alerts are generated, a new incident will be created with the same incident details as the original, and the excess alerts will be grouped into the new incident.
Limit the group to alerts created within the selected time frame *
< Previous
Next : Automated response >
18°C
Partly sunny
Search
ENG
US
7:19 PM
2024-05-14



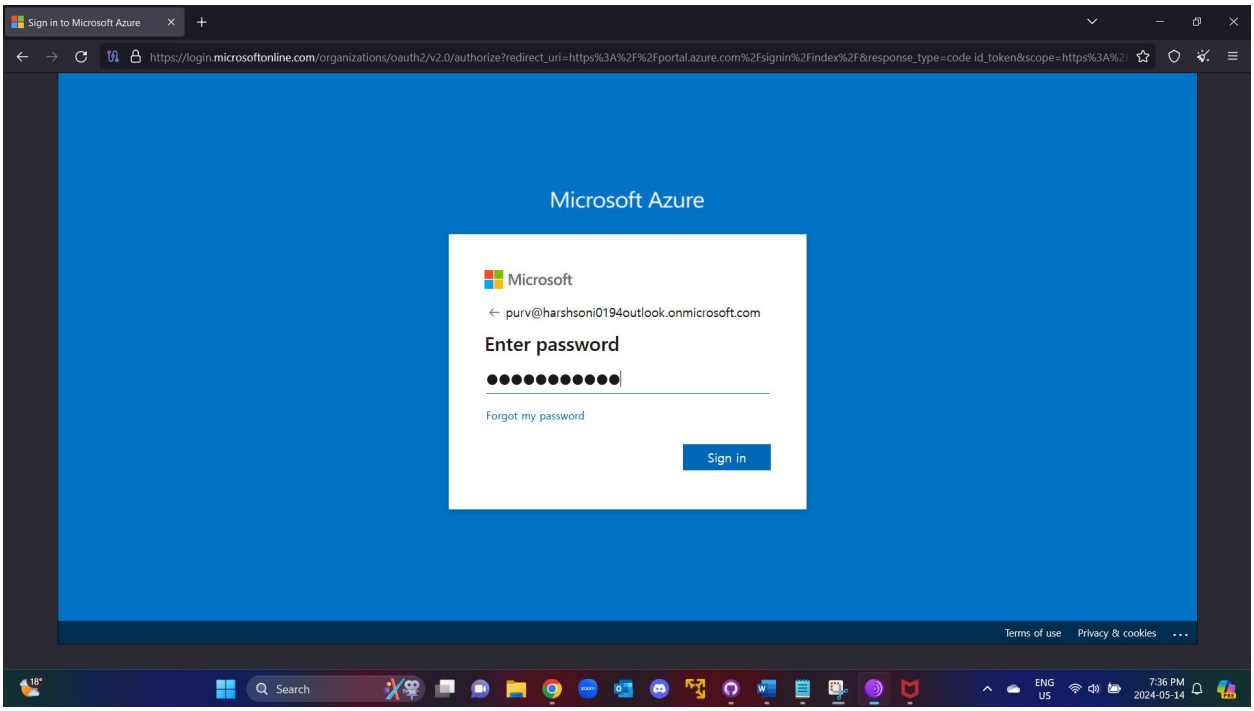
Create a USER ACCOUNT in AZURE for SIEM Investigation:



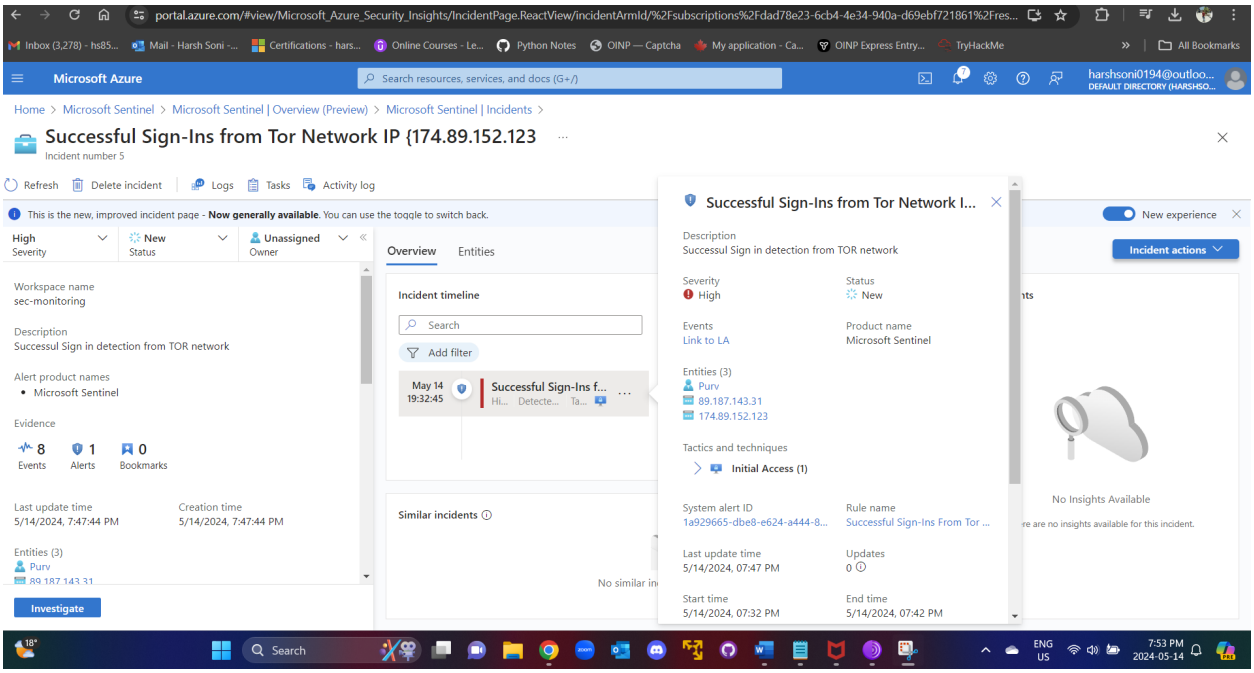


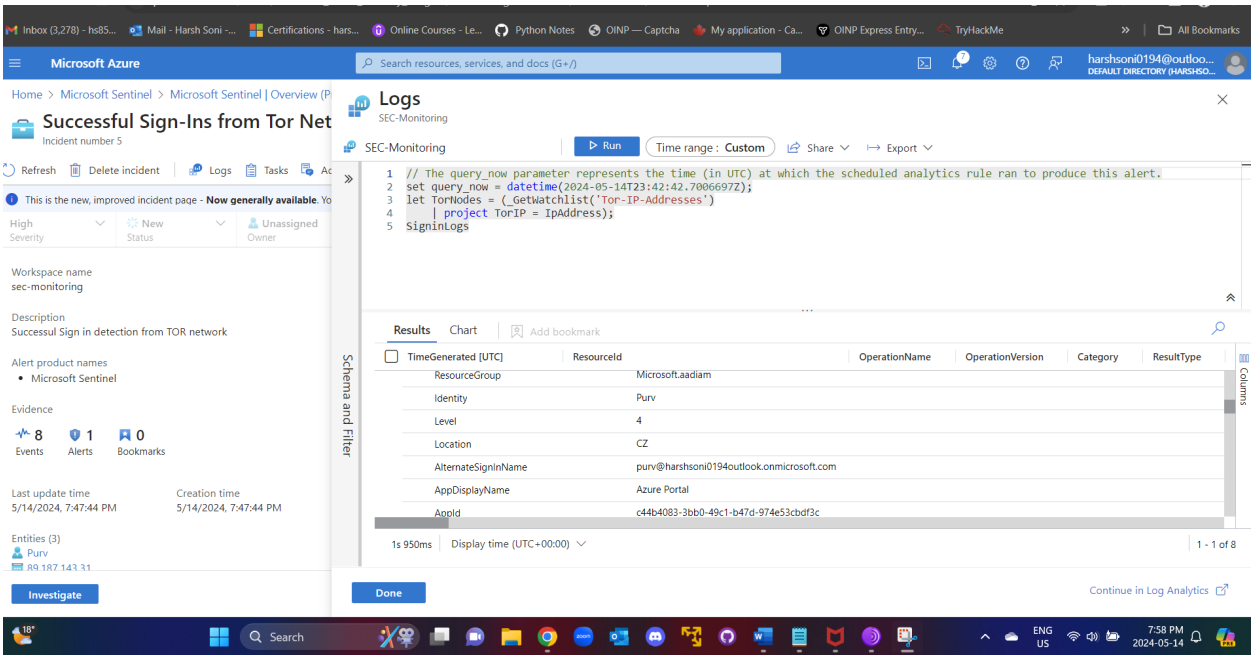


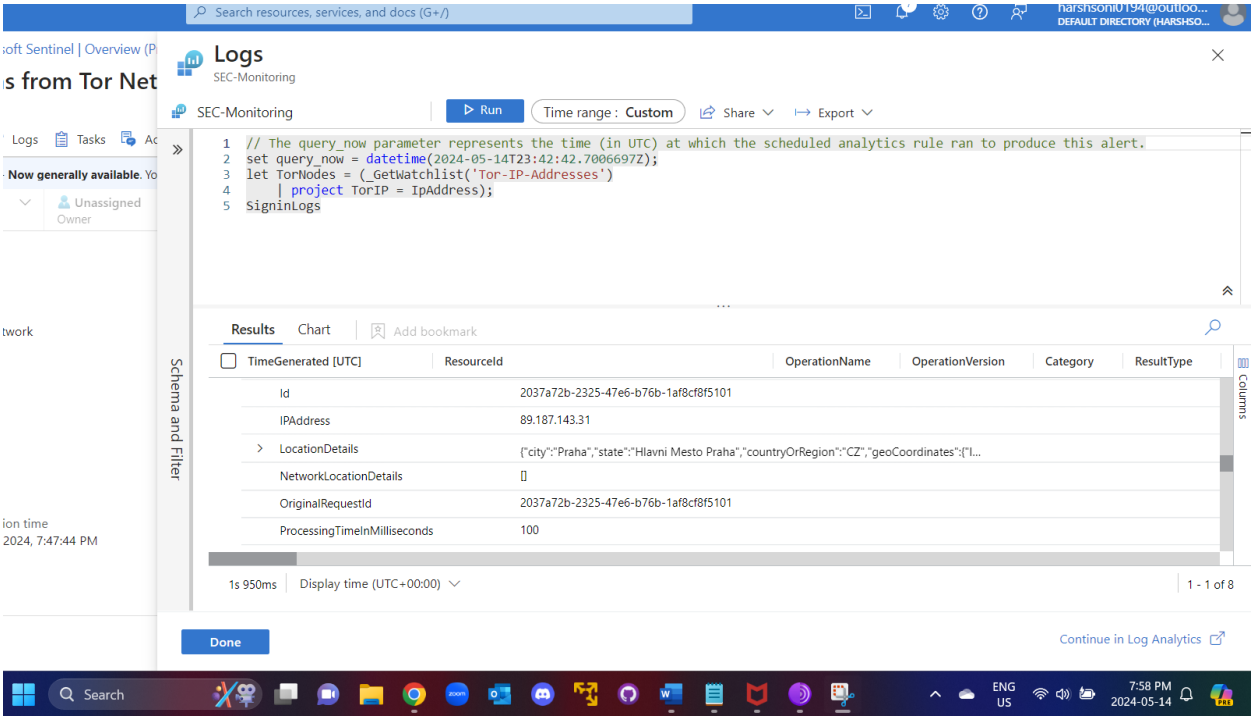
Login to the new user account from TOR network:



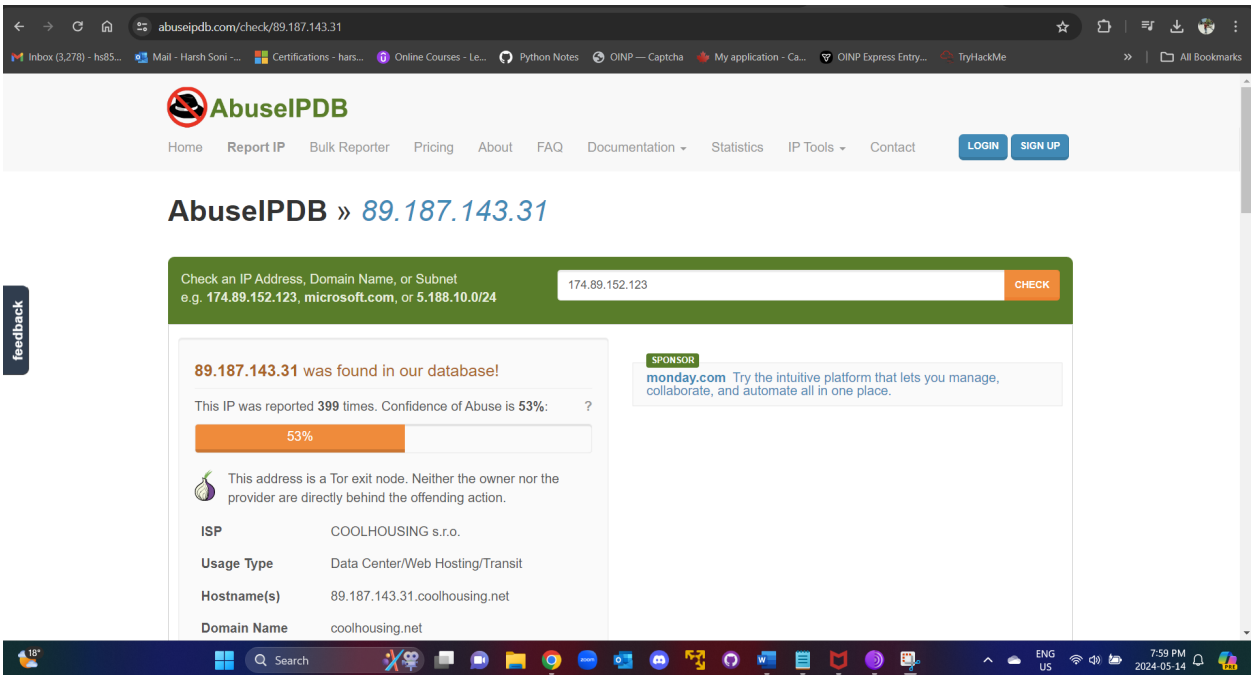
LOG/INCIDENT DETECTED

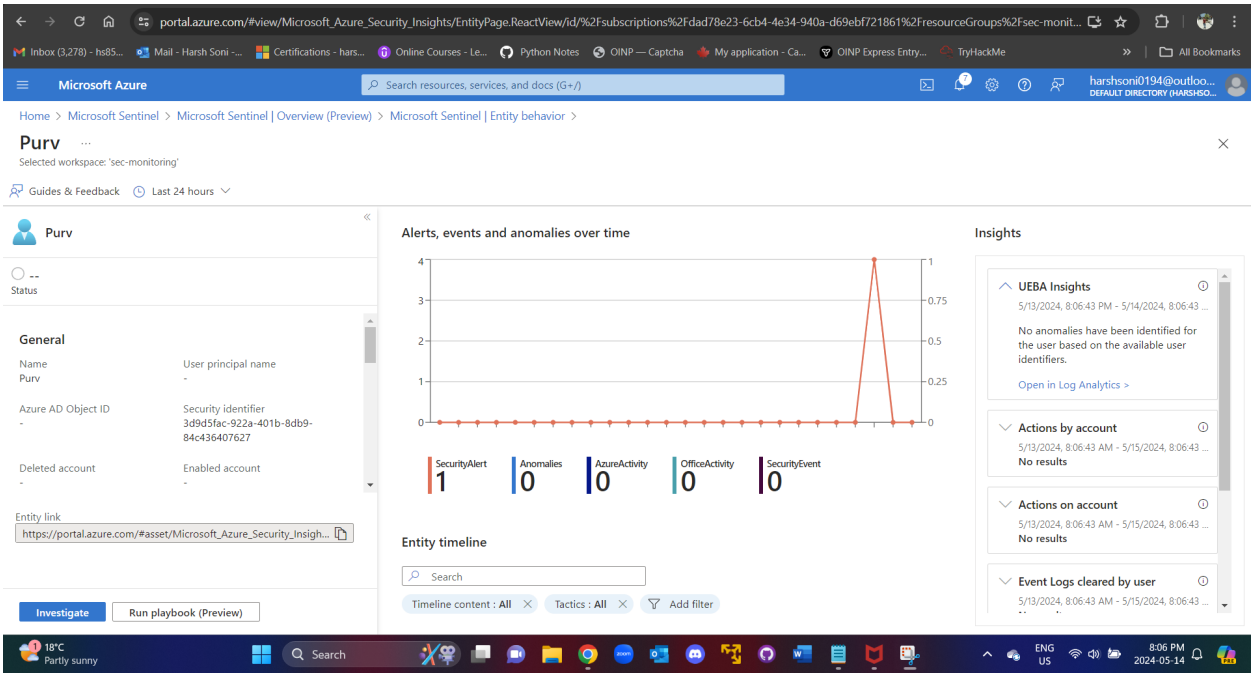






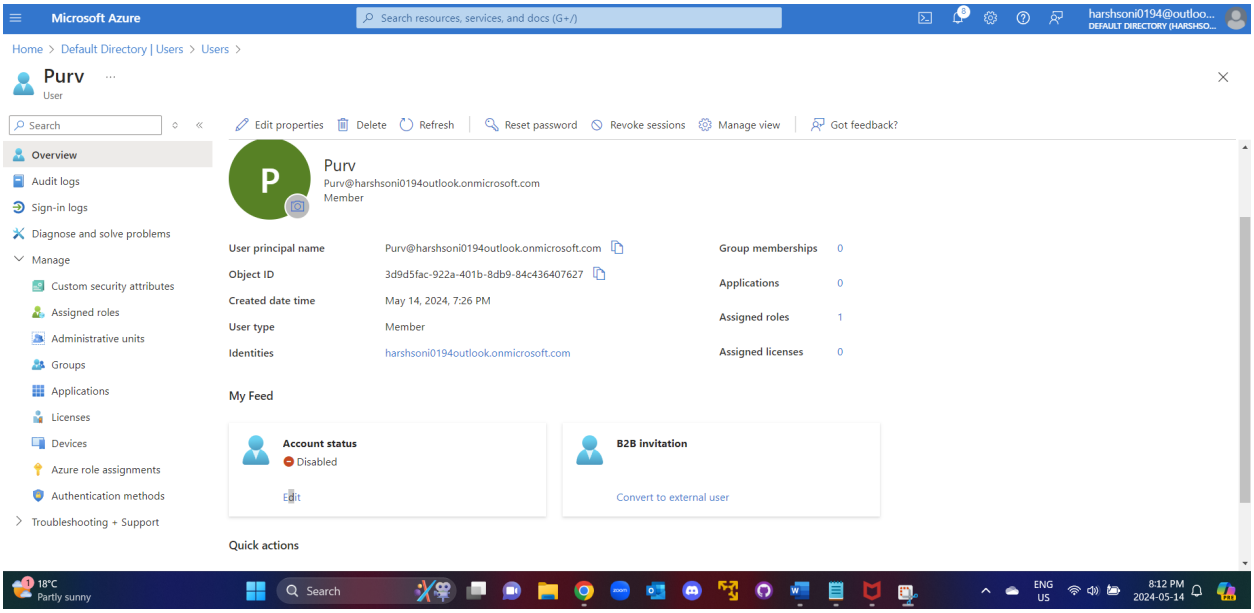
IP Reported as abuse and in TOR network:



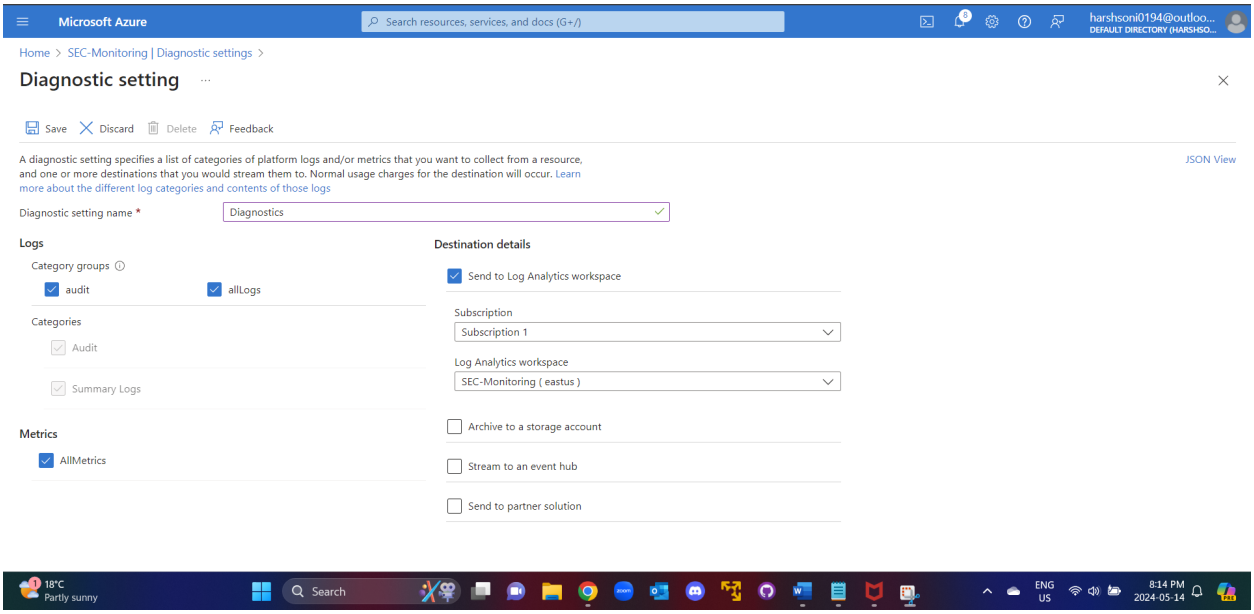


REMEDIATION

DISABLE THE ACCOUNT



Turn on Diagnostic Settings:



Enable Auditing and Health Monitoring

Auditing and health monitoring

What is it?

With the Microsoft Sentinel health and audit feature, you can keep an eye on the availability and health of system resources.

How to enable it?

Select **Enable** to enable health monitoring for all resources, or select Configure diagnostic settings for advanced configuration. Learn more >

Enabled Configure diagnostic settings >