

Microsoft Sentinel SIEM

1) CREATE A SIEM IN AZURE

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

The screenshot shows the GitHub repository for Azure-Sentinel. The main content area displays the 'Sentinel-All-In-One' tool documentation. It includes a sidebar with a file tree showing various Azure Sentinel-related files like 'azure-pipelines', '.github', and 'BYOML'. The main content area lists 'Prerequisites' (Azure Subscription, permissions, and connectors), a 'Try it now!' button with a 'Deploy to Azure' link, and a 'Supported connectors' section with a table.

The screenshot shows the Microsoft Azure portal's 'Custom deployment' wizard. The user is on the second step, 'Instance details'. They have selected 'Subscription 1 (dad78e23-6cb4-4e34-940a-d69ebf721861)' and specified the location as 'East US'. Other fields include 'Resource Group name' (SEC-Monitoring), 'Workspace Name' (SEC-Monitoring), 'Daily ingestion limit in GBs' (10), 'Number of days of retention' (90), and 'Select pricing tier for Sentinel and Log Analytics' (Pay-as-you-go). At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons.

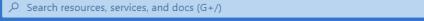
Exploring deployed cybersecurity Artifacts:

The screenshot shows the Microsoft Azure portal interface. The URL is <https://portal.azure.com/#@harshsoni0194outlook.onmicrosoft.com/resource/subscriptions/dad78e23-6cb4-4e34-940a-d69ebf721861/resourceGroups/SEC-Monitoring/overview>. The title bar says "SEC-Monitoring - Microsoft Azure". The left sidebar shows "Resource groups" with "SEC-Monitoring" selected. The main content area is titled "SEC-Monitoring" and shows a table of resources. The table has columns for Name, Type, Deployment Script, Location, and more. Resources listed include "deployRules", "Container instances", "Storage account", "Deployment Script", "Log Analytics workspace", "Solution", and "Deolvement Script".

The screenshot shows the Microsoft Azure portal interface. The URL is <https://portal.azure.com/#@harshsoni0194outlook.onmicrosoft.com/resource/subscriptions/dad78e23-6cb4-4e34-940a-d69ebf721861/resourceGroups/SEC-Monitoring/providers/Microsoft.OperationalInsights/workspaces/SEC-Monitoring>. The title bar says "SEC-Monitoring - Microsoft Azure". The left sidebar shows "Resource groups" and "SEC-Monitoring". The main content area is titled "SEC-Monitoring" and shows an "Overview" section with a message about the deprecation of MMA.OMS. It also shows sections for "Logs", "Monitoring", and "Automation". The "Logs" section is expanded, showing details like "Workspace Name: SEC-Monitoring", "Status: Active", "Location: East US", "Subscription: Subscription 1", and "Tags: Add tags".

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 - har... Online Courses - Le... Python Notes OINP — Captcha My application - Ca... OINP Express Entry... TryHackMe harshsoni0194@outloo... All Bookmarks harshsoni0194@outloo... DEFAULT DIRECTORY /HARSHSO...

Microsoft Azure       

Home > Resource groups > SEC-Monitoring > SEC-Monitoring

SEC-Monitoring | Diagnostic settings

Log Analytics workspace

Search  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](#)

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

Diagnostic settings

- Advisor recommendations
- Workbooks

Automation Help

Microsoft Azure Search resources, services, and docs (G+ /)

Home > Resource groups > SEC-Monitoring > SEC-Monitoring | Diagnostic settings >

Diagnostic setting ...

Save Discard Delete Feedback

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

Diagnostic setting name * Sentinel

Logs

Category groups	Destination details
<input type="checkbox"/> audit	<input checked="" type="checkbox"/> Send to Log Analytics workspace
<input checked="" type="checkbox"/> allLogs	Subscription: Subscription 1
	Log Analytics workspace: SEC-Monitoring (eastus)
	<input type="checkbox"/> Archive to a storage account
	<input type="checkbox"/> Stream to an event hub
	<input type="checkbox"/> Send to partner solution

Metrics

Metrics	Destination details
<input checked="" type="checkbox"/> AllMetrics	

portal.azure.com/#@harshsoni0194outlook.onmicrosoft.com/resource/subscriptions/dad78e23-6cb4-4e34-940a-d69ebf721861/resourceGroups/SEC-Monitoring/providers/Mic... Save Feedback

Home > Resource groups > SEC-Monitoring > SEC-Monitoring

SEC-Monitoring | Diagnostic settings

Log Analytics workspace

Search 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](#)

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
Sentinel	-	-	SEC-Monitoring	-	Edit setting

+ 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.security/insightsarg%2Fsentinel

Microsoft Azure

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

No grouping List view

Showing 1 to 1 of 1 records.

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

Home > Microsoft Sentinel

Microsoft Sentinel

Default Directory (harshsoni0194outlook.onmicrosoft.com)

+ Create Manage view ...

Filter for any field... Name ↑ SEC-Monitoring

Overview (Preview)

General

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 False Positive Benign Positive Undetermined

(0) (0) (0) (1)

Mean time to acknowledge Mean time to close

0 min 0 min 0 min 0 min

Manage incidents > Analyze SOC efficiency >

< Page 1 of 1 >

The screenshot shows the Microsoft Sentinel Logs interface. On the left, a sidebar menu is open under the 'Logs' section, listing various log types such as SEC-Monitoring, AuditLogs_CL, AzureActivity_CL, Cisco_Umbrella_dns_CL, OfficeActivity_CL, SecurityEvent_CL, and Signature_CL. The main area displays a 'New Query 1' window with a search bar, a 'Run' button, and a time range selector set to 'Last 24 hours'. Below these are tabs for 'Tables', 'Queries', and 'Functions'. A large text input field says 'Type your query here or click one of the queries to start'. To the right, there's a 'Query history' section which is currently empty, stating 'No queries history'.

This screenshot shows the Microsoft Sentinel Logs interface after running a query. The results table displays 23 rows of data from the 'AzureActivity_CL' table. The columns shown are TimeGenerated (UTC), _table_s, CallerIPAddress, CategoryValue_s, and CorrelationId. The data includes various Azure activity logs from May 14, 2024, such as AzureActivity entries for different IP addresses and correlation IDs.

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-223f5220e772
> 5/14/2024, 10:13:55.428 PM	AzureActivity	37.142.150.162	Administrative	b62b273a-d336-4ead-b1ac-223f5220e772
> 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
0s 493ms	Display time (UTC +0:00)	Query details 1 - 8 of 23		

The screenshot shows the Microsoft Sentinel Data connectors page. The left sidebar includes links for Threat management, Content management (Content hub, Repositories (Preview), Community), Configuration (Workspace manager (Preview)), and Data connectors (which is selected). The main area displays a summary of 16 connectors and 7 connected ones, with a link to the Content hub for more content. A search bar at the top allows searching by name or provider. Below, a table lists the connectors with columns for Status, Connector name, and Microsoft logo. The connectors listed are Azure Activity, Cisco Umbrella (Preview), Dynamics365, Microsoft 365 (formerly, Office 365), and Microsoft 365 Insider Risk Management (Preview). A large icon of a 3x3 grid is on the right, with the text "No Connector selected Select a Connector to view more details".

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

Microsoft Azure | Microsoft Sentinel | Data connectors

Selected workspace: sec-monitoring

16 Connectors 7 Connected

More content at Content hub

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 Version

Azure Activity 2.0.0

Author Supported by

Microsoft Microsoft Corporation | Email

Open connector page

Search resources, services, and docs (G+)

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

Refresh Guides & Feedback

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

Open connector page

Microsoft Azure | Microsoft Sentinel | Analytics

Selected workspace: sec-monitoring

135 Active rules

More content at Content hub

Rules by severity

High (8) Medium (100) Low (17) Informational (0)

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique Add filter

Severity	Name	Rule type	Status	Tactics	Techniques
High	Solorigate Net...	Scheduled	Enabled	Command ...	
Medium	Sign-ins from I...	Scheduled	Enabled	Initi... +1	
Medium	Malicious Inbox...	Scheduled	Enabled	Pers... +1	
Medium	TI Map IP Entity...	Scheduled	Enabled	Impact	
Medium	TI Map IP Entity...	Scheduled	Enabled	Impact	
Medium	Malware in the ...	Scheduled	Enabled	Defense Ev...	
Medium	TI Map URL Ent...	Scheduled	Enabled	Impact	

No analytics rules selected

Select an analytics rule to view more details

Learn More About analytics rules

Search resources, services, and docs (G+)

Search

Overview (Preview)

Logs

News & guides

Search

Threat management

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Analytics

Watchlist

Automation

Settings

Create Refresh Analytics workbooks Rule runs (Preview) Enable Disable Delete Import Export Columns Guides & Feedback

Microsoft Sentinel - Microsoft | portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/-/Analytics/id/%2fsubscriptions%2fdad78e23-6cb4-4e34-940a-d69ebf721861%2fresourcegroups%2fse... | +

Inbox (3,278) - hs85... Mail - Harsh Soni -... Certifications - har... Online Courses - Le... Python Notes OINP — Captcha My application - Ca... OINP Express Entry... TryHackMe All Bookmarks

Microsoft Azure | Microsoft Sentinel | Analytics

Selected workspace: sec-monitoring

Microsoft Sentinel | Analytics

135 Active rules

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	Status	Tactics	Techniques	Sub techn...
Medium	TI Map IP Entity...	Enabled	Impact		
Medium	TI Map IP Entity...	Enabled	Impact		
Medium	Malware in the ...	Enabled	Defense Ev...		
Medium	TI Map URL Ent...	Enabled	Impact		
High	D365 - Audit lo...	Enabled	Pers... +2		
Medium	D365 - Audit lo...	Enabled	Pers... +2		
Medium	Unauthorized d...	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 Enabled Status

Info Insights

ID: 99d2c64c-a9af-442c-9a13-30bc26e313cc

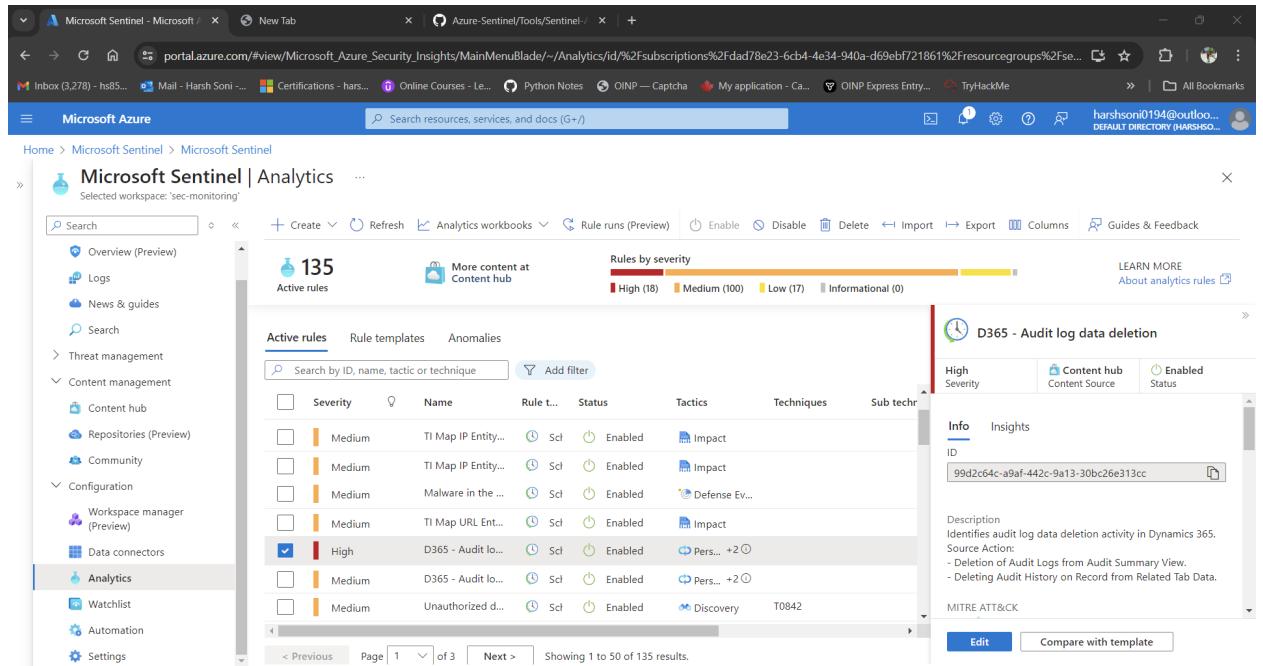
Description: Identifies audit log data deletion activity in Dynamics 365.

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 | portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/-/Analytics/id/%2fsubscriptions%2fdad78e23-6cb4-4e34-940a-d69ebf721861%2fresourcegroups%2fse... | +

Inbox (3,278) - hs85... Mail - Harsh Soni -... Certifications - har... Online Courses - Le... Python Notes OINP — Captcha My application - Ca... OINP Express Entry... TryHackMe All Bookmarks

Microsoft Azure | Microsoft Sentinel | Analytics

Selected workspace: sec-monitoring

Microsoft Sentinel | Analytics

135 Active rules

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	Security Events ...	I... +1	T1190 +1	10/25/2023, 12:00...
Rare privileged pr...	Enabled	Security Events ...	Initial A...	T1078	10/21/2023, 12:00...
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.

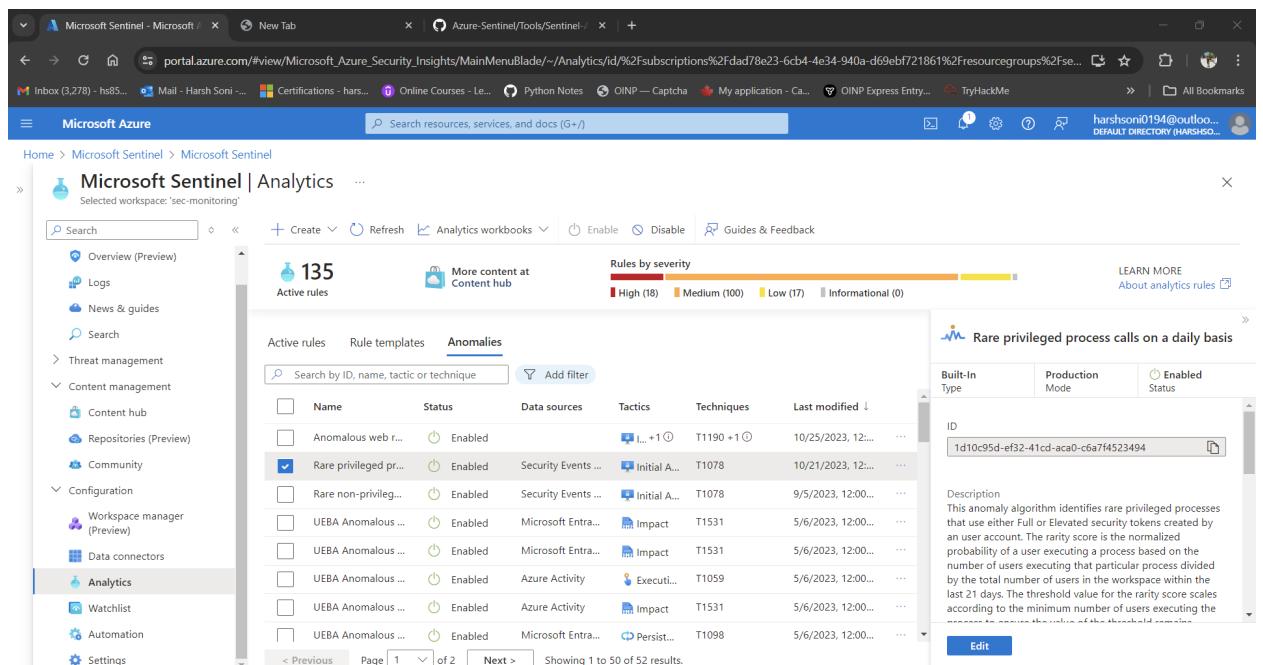
Rare privileged process calls on a daily basis

Built-In Production Mode Enabled Status

ID: 1d10c95d-ef32-41cd-ac40-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 process.

Edit



ENABLE ARTIFICIAL INTELLIGENCE IN SIEM

SET UEBA

The screenshot shows the Microsoft Sentinel Settings page under the 'Entity behavior analytics' section. On the left, a sidebar lists various workspace management options like Overview, Logs, Threat management, Content management, Configuration, and Settings. The main content area has tabs for Pricing, Settings, and Workspace settings, with 'Settings' selected. Under 'Entity behavior analytics', there's a 'What is it?' section describing UEBA's purpose and how it creates comprehensive profiles of users and entities. Below that is a 'How to enable it' section with a 'Set UEBA' button. The 'Anomalies' section is also visible. At the bottom, there's a step-by-step guide for configuration:

- 2. Sync Microsoft Sentinel with at least one of the following directory services**
This will create profiles for the users and entities in your organization and also creates data stores in Microsoft Sentinel.
Only tenants onboarded to Microsoft Defender for Identity can enable Active Directory syncing.
- 3. Select the existing data sources you want to enable for entity behavior analytics**
A list of available data sources includes Audit Logs (Microsoft) and Signin Logs (Microsoft), both of which are checked. An 'Apply' button is present below the list.

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:

The screenshot shows the Microsoft Sentinel Watchlist interface. At the top, there are two counts: 15 Watchlists and 954 Watchlist Items. Below this, a table lists 15 watchlists with columns for Name, Alias, Source, Create..., and Last updated. The table includes rows for D365-SecurityConfig, D365-UserConfig, NetworkSession Monitor Configuration, SOC General IT, SOC Contacts, SOC Email Distribution, SOC Maturity Assessment (CMMI), and SOC External Contacts. The interface also features a sidebar with categories like General, Logs, News & guides, Search, Threat management, Content management, Configuration, Workspace manager (Preview), Data connectors, Analytics, Watchlist, and Automation. The Watchlist category is currently selected. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 2024-05-14 at 6:53 PM.

Name	Alias	Source	Create...	Last updated
D365-SecurityConfig	D365-SecurityConfig	ContentHub	5/14/2024	5/14/2024
D365-UserConfig	D365-UserConfig	ContentHub	5/14/2024	5/14/2024
NetworkSession Monitor Configuration	NetworkSession_Monitor_Config	NetworkSession	5/14/2024	5/14/2024
SOC General IT	SOCgeneralIT	SOCgenerator	5/14/2024	5/14/2024
SOC Contacts	SOCcontacts	SOCContact	5/14/2024	5/14/2024
SOC Email Distribution	SOCEmailDistribution	SOCEmail	5/14/2024	5/14/2024
SOC Maturity Assessment (CMMI)	SOCMA	SOCMA.cs	5/14/2024	5/14/2024
SOC External Contacts	SOCExternalContacts	SOCExternal	5/14/2024	5/14/2024

Upload a TOR FILE:

The screenshot shows the Microsoft Azure Watchlist wizard interface. The 'Source' tab is selected. Under 'Source type', 'Local file' is chosen. Under 'File type', 'CSV file with a header (.csv)' is selected. The 'Number of lines before row with headings' is set to 0. A file named 'Tor+Exit+Nodes.csv' is uploaded. On the right, a 'File preview' section shows the first 50 rows and first 5 columns of the CSV file, which contains IP addresses. Below the preview is a note: 'Drag and drop the files or Browse for files'. At the bottom, there are 'SearchKey' and 'Reset' fields, and navigation buttons: '< Previous' and 'Next : Review + create >'.

Calling Watchlist using KQL:

The screenshot shows the Microsoft Azure Log Analytics workspace under the 'Logs' section. A query is being run: `1 | _GetWatchlist('Tor-IP-Addresses')`. The results table displays a list of items, each with a timestamp, item ID, search key, and IP address. The table has columns: LastUpdatedTimeUTC, DTItemid, SearchKey, and IPAddress. The results show multiple entries for different IP addresses over a 24-hour period. The interface includes a sidebar for navigating between tables, queries, and functions, and various toolbar options like Run, Save, Share, and Export.

LastUpdatedTimeUTC	DTItemid	SearchKey	IPAddress
5/14/2024, 10:56:15.797 PM	4b11a85b-5d68-421a-b24c-c02b90c56de5	213.164.206.124	
5/14/2024, 10:56:15.797 PM	6c4738cd-25ed-4b99-a237-e0e91dff159	23.154.177.23	
5/14/2024, 10:56:15.797 PM	bc2c45fd-2ac3-442d-b13f-e61df679553c	2602:fbec:0fec:2514:0000:0000:0000:0001	
5/14/2024, 10:56:15.797 PM	033cd54-5397-41bc-861f-731166054dd	2602:fc24:0018:1be9:0000:0000:0000:0001	
5/14/2024, 10:56:15.797 PM	7035c619-128a-4651-9fbf-cc47bbc8f1ae	2605:6400:0010:03e0:b11:8981:7151:5d83	
5/14/2024, 10:56:15.797 PM	dcaabf47-ae3a-449r-87a4-db9903e9cf5f	2605:6400:0010:04ed:0001:0001:0001:0001	
5/14/2024, 10:56:15.797 PM	fa3cae1-6f5a-4264-ac12-be17d7a6cab	2605:6400:0030:f5db:25a1:b884:ef2d:8818	

Create Detection Rule for Cybersecurity Threat

The screenshot shows the 'Analytics rule wizard - Create a new Scheduled rule' page. At the top, there are tabs: General, Set rule logic, Incident settings, Automated response, and Review + create. The 'General' tab is selected. Below the tabs, a sub-header says 'Create an analytics rule that will run on your data to detect threats.' Under 'Analytics rule details', there are fields for Name (set to 'Successful Sign-Ins From Tor Network'), Description (set to 'Rule detects successful sign-ins from TOR network a popular tool used by threat actors to anonymize their activity'), Severity (set to 'Medium'), and MITRE ATT&CK (with a dropdown menu showing 'Select tactics techniques and sub-techniques'). A blue button at the bottom left says 'Next : Set rule logic >'.

The screenshot shows the 'Analytics rule wizard - Set rule logic' page. The 'Set rule logic' tab is selected. It contains a section for defining logic with the heading 'Define the logic for your new analytics rule.' Below this is a 'Rule query' section with the sub-heading 'Any time details set here will be within the scope defined below'. A code editor window shows the following Log Query Language (LQL) code:

```
let TorNodes = ( _GetWatchlist('Tor-IP-Addresses')
SigninLogs
```

Below the code editor, there's a link 'View query results >'. To the right, there's a sidebar with sections for 'Tables', 'Queries', 'Functions', and 'Favorites'. The 'Favorites' section includes items like 'LogManagement', 'Microsoft Sentinel', and 'Custom Logs'. At the bottom, there are navigation buttons: '< Previous' and 'Next : Incident settings >'.

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	<input type="button" value="▼"/>	<input type="button" value="Delete"/>		
Sid	<input type="button" value="▼"/>	UserId	<input type="button" value="▼"/>	<input type="button" value="Delete"/>
DisplayName	<input type="button" value="▼"/>	UserDisplayName	<input type="button" value="▼"/>	<input type="button" value="Delete"/>
IP		<input type="button" value="▼"/>	<input type="button" value="Delete"/>	
Address	<input type="button" value="▼"/>	IPAddress	<input type="button" value="▼"/>	<input type="button" value="Delete"/>
+ 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	<input type="button" value="▼"/>	<input type="button" value="Delete"/>
User	UserDisplayName	<input type="button" value="▼"/>	<input type="button" value="Delete"/>
+ Add new			

Alert details

Query scheduling

Run query every *

5	Hours	<input type="button" value="▼"/>
---	-------	----------------------------------

Lookup data from the last *

5	Hours	<input type="button" value="▼"/>
---	-------	----------------------------------

[< Previous](#)

[Next : Incident settings >](#)



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 or 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
Successful Sign in detection from TOR network

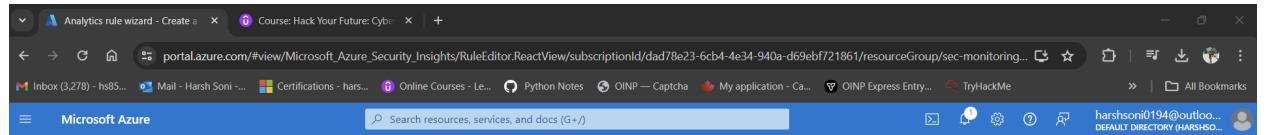
ConfidenceScore RiskState

+ Add new property override

Query scheduling

Run query every *

< Previous Next : Incident settings >



Analytics rule wizard - Create a 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 >



Microsoft Sentinel | Analytics

Selected workspace: 'sec-monitoring'

136 Active rules

Rules by severity:

- High (19)
- Medium (100)
- Low (17)
- Informational (0)

Active rules Rule templates Anomalies

Severity	Name	Rule t...	Status	Tactics
<input checked="" type="checkbox"/> High	Successful Sign-Ins From Tor Network			Enabled
<input type="checkbox"/> High	Solorigate Network Beacon			Enabled
<input type="checkbox"/> Medium	Sign-ins from IPs that attempt sign-ins to disable...			Enabled
<input type="checkbox"/> Medium	Malicious Inbox Rule - custom			Enabled
<input type="checkbox"/> Medium	TI Map IP Entity to DeviceNetworkEvents			Enabled
<input type="checkbox"/> Medium	TI Map IP Entity to AzureActivity			Enabled
<input type="checkbox"/> Medium	Malware in the recycle bin			Enabled

Successful Sign-Ins From Tor Network

High Severity

Custom Content Source

Enabled Status

Rule query:
let TorNodes = (_GetWatchlist('Tor-IP-Addresses'),
\$signinLogs)

Rule frequency: Run query every 5 hours

Rule period: Last 5 hours data

Rule threshold

Edit

Create a USER ACCOUNT in AZURE for SIEM Investigation:

Default Directory | Properties

Technical contact: harshsoni0194@outlook.com

Global privacy contact:

Privacy statement URL:

Access management for Azure resources

Harsh Soni (harshsoni0194@outlook.com) can manage access to all Azure subscriptions and management groups in this tenant.

Save Discard

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically protected from common identity-related attacks.

Your organization is protected by security defaults.

Manage security defaults

Reason for disabling *

This feedback will be used to improve Microsoft products and services. [View privacy statement](#)

My organization is planning to use Conditional Access

My organization is unable to use apps/devices

Too many sign-in multifactor authentication challenges

Too many multifactor authentication sign-up requests

Other

Testing

Save Cancel

Create new user

Create a new internal user in your organization.

Basics

User principal name * Purv @ harshsoni0194outlook... Domain not listed? Learn more

Mail nickname * Purv Derive from user principal name

Display name * Purv

Password * Password strength: Strong Auto-generate password

Account enabled

Review + create < Previous Next: Properties > Give feedback

Add role assignment

Role: Contributor

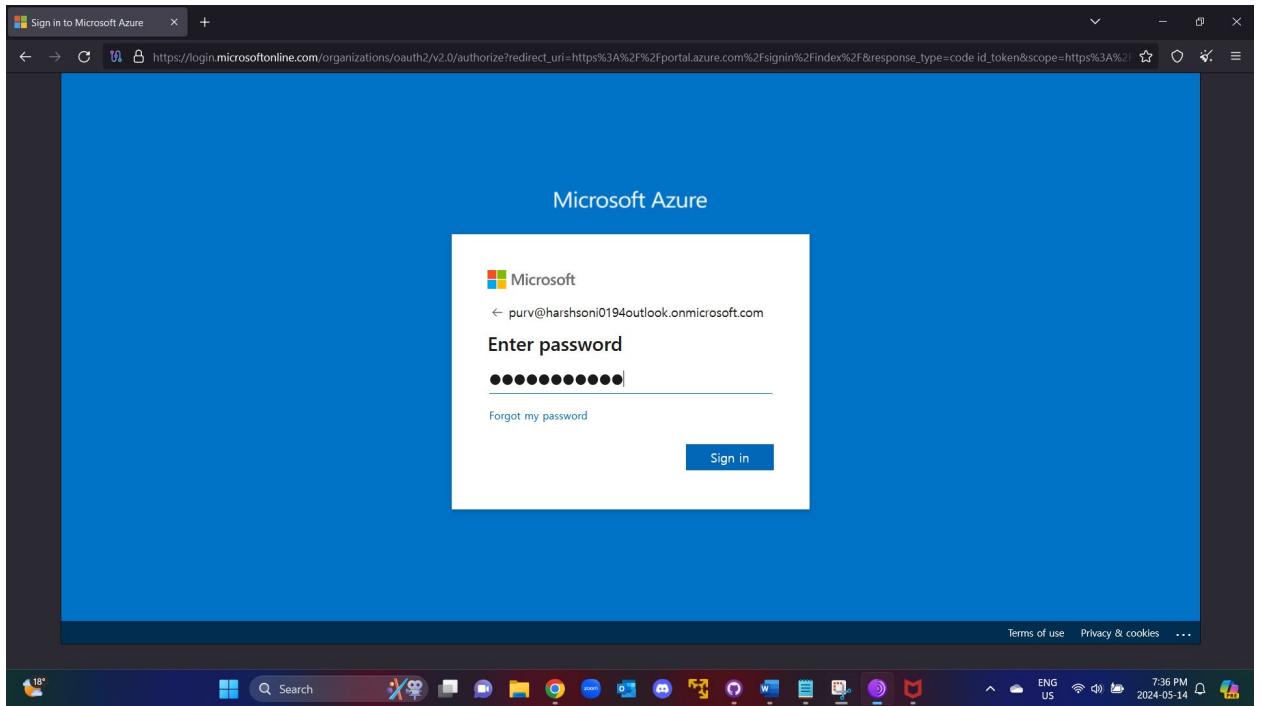
Scope: /subscriptions/dad78e23-6cb4-4e34-940a-d69ebf721861/resourceGroups/SEC-Monitoring/providers/Microsoft.OperationalInsights/workspaces/SEC-Monitoring

Members	Name	Object ID	Type
Purv	3d9d5fac-922a-401b-8db9-84c436407627	User	

Description: No description

Review + assign Previous Next Feedback

Login to the new user account from TOR network:



LOG/INCIDENT DETECTED

A screenshot of the Microsoft Sentinel Incident Page. The URL is portal.azure.com/#view/Microsoft_Azure_Security_Insights/IncidentPage.ReactView/incidentArnid/%2Fsubscriptions%2Fdad78e23-6cb4-4e34-940a-d69ebf721861%2Fres... The page displays an incident titled "Successful Sign-Ins from Tor Network IP {174.89.152.123} ...". The incident number is 5. The timeline shows a single event: "Successful Sign-In f..." on May 14, 19:32:45. The incident details pane shows the following information:

- Description: Successful Sign in detection from TOR network
- Severity: High
- Status: New
- Owner: Unassigned
- Link to LA: https://logAnalytics.microsoft.com/LogAnalytics/Logs/1a929665-db88-e624-a444-8...
- Entities (3): Purv, 89.187.143.31, 174.89.152.123
- Tactics and techniques: Initial Access (1)
- System alert ID: 1a929665-db88-e624-a444-8...
- Rule name: Successful Sign-Ins From Tor ...
- Last update time: 5/14/2024, 07:47:44 PM
- Updates: 0
- Start time: 5/14/2024, 07:32 PM
- End time: 5/14/2024, 07:42 PM

The status bar at the bottom indicates the date as 2024-05-14 and the time as 7:53 PM.

Successful Sign-Ins from Tor Net

```
// The query_now parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert.
2 set query_now = datetime(2024-05-14T23:42:42.7006697Z);
3 let TorNodes = _GetWatchlist('Tor-IP-Addresses')
4 | project TorIP = IpAddress;
5 SigninLogs
```

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	ResultType
ResourceGroup	Microsoft.aadiam				
Identity	Purv				
Level	4				
Location	CZ				
AlternateSignInName	purv@harshsoni0194outlook.onmicrosoft.com				
AppDisplayName	Azure Portal				
ApId	c44b4083-3bb0-49c1-b47d-974e53cbdf3c				

1s 950ms | Display time (UTC+00:00) | 1 - 1 of 8

Investigate | **Done**

Successful Sign-Ins from Tor Net

```
// The query_now parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert.
2 set query_now = datetime(2024-05-14T23:42:42.7006697Z);
3 let TorNodes = _GetWatchlist('Tor-IP-Addresses')
4 | project TorIP = IpAddress;
5 SigninLogs
```

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	ResultType
Id	2037a72b-2325-47e6-b76b-1af8cf8f5101				
IPAddress	89.187.143.31				
LocationDetails	{"city": "Praha", "state": "Hlavn\u00ed Mesto Praha", "countryOrRegion": "CZ", "geoCoordinates": [{"lat": 50.0755, "lon": 14.4378}]} []				
NetworkLocationDetails	[]				
OriginalRequestId	2037a72b-2325-47e6-b76b-1af8cf8f5101				
ProcessingTimeInMilliseconds	100				

1s 950ms | Display time (UTC+00:00) | 1 - 1 of 8

Continue in Log Analytics

IP Reported as abuse and in TOR network:

The screenshot shows the AbuselPDB website interface. At the top, there's a navigation bar with links like Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, Contact, LOGIN, and SIGN UP. Below the navigation is a search bar with placeholder text "Check an IP Address, Domain Name, or Subnet e.g. 174.89.152.123, microsoft.com, or 5.188.10.0/24". A search button labeled "CHECK" is to the right. The main content area displays the result for IP 89.187.143.31, stating it was found 399 times with a confidence of 53%. It also notes that the address is a Tor exit node. Below this, detailed information is provided for the ISP (COOLHOUSING s.r.o.), Usage Type (Data Center/Web Hosting/Transit), Hostname(s) (89.187.143.31.coolhousing.net), and Domain Name (coolhousing.net). A sidebar on the left has a "feedback" button. A sponsor banner for monday.com is visible on the right.

The screenshot shows the Microsoft Azure Sentinel Entity Page for a user named Purv. The page includes a sidebar with Purv's profile picture, name, and status. The main content area features a chart titled "Alerts, events and anomalies over time" showing a single sharp peak at index 1. Below the chart, five categories are displayed with counts: SecurityAlert (1), Anomalies (0), AzureActivity (0), OfficeActivity (0), and SecurityEvent (0). To the right, an "Insights" panel is open, showing sections for UEBA Insights, Actions by account, Actions on account, and Event Logs cleared by user, all of which show no results. The bottom of the screen shows the Windows taskbar with various pinned icons.

REMEDIATION

DISABLE THE ACCOUNT

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and a user profile for 'harshsoni0194@outlook.com'. Below the header, the URL 'Home > Default Directory | Users > Users >' is visible. The main content area displays a user named 'Purv' with a green profile picture containing a white letter 'P'. The user's email is listed as 'Purv@harshsoni0194outlook.onmicrosoft.com' and their status is 'Member'. A sidebar on the left provides navigation links for 'Overview', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', 'Custom security attributes', 'Assigned roles', 'Administrative units', 'Groups', 'Applications', 'Licenses', 'Devices', 'Azure role assignments', 'Authentication methods', and 'Troubleshooting + Support'. The 'Overview' section is currently selected. On the right, detailed user information is shown, including 'User principal name' (Purv@harshsoni0194outlook.onmicrosoft.com), 'Object ID' (3d9d5fac-922a-401b-8db9-84c436407627), 'Created date time' (May 14, 2024, 7:26 PM), 'User type' (Member), 'Identities' (harshsoni0194outlook.onmicrosoft.com), 'Group memberships' (0), 'Applications' (0), 'Assigned roles' (1), and 'Assigned licenses' (0). Below this, there are sections for 'My Feed' (Account status: Disabled, Edit) and 'B2B invitation' (Convert to external user). At the bottom, there is a 'Quick actions' bar with various icons and a taskbar at the very bottom.

Turn on Diagnostic Settings:

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and a user profile for 'harshsoni0194@outlook.com'. Below the header, the URL 'Home > SEC-Monitoring | Diagnostic settings >' is visible. The main content area displays a 'Diagnostic setting' page for 'SEC-Monitoring'. It includes a 'Save' button, a 'Discard' button, a 'Delete' button, and a 'Feedback' link. A note states: 'A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs.' The 'Diagnostic setting name' is set to 'Diagnostics'. Under the 'Logs' section, 'audit' and 'allLogs' are selected under 'Category groups'. Under 'Categories', 'Audit' and 'Summary Logs' are checked. Under the 'Metrics' section, 'AllMetrics' is checked. In the 'Destination details' section, 'Send to Log Analytics workspace' is checked, and 'Subscription' is set to 'Subscription 1' with 'Log Analytics workspace' set to 'SEC-Monitoring (eastus)'. There are also options for 'Archive to a storage account', 'Stream to an event hub', and 'Send to partner solution'. At the bottom, there is a 'Quick actions' bar with various icons and a taskbar at the very bottom.

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 >](#)