I created a Mini Security Operations Center via Azure. I created a virtual machine and intentionally left the RDP (3389) port open. Then I used Sentinel to create a connected workspace to log all security incidents with the virtual machine. For this project I focused on alerting successful logins to the virtual machine.

Table of Contents

Prerequisites

- Active internet connection
- Valid email to sign up for Azure free tier
- Basic familiarity with Azure Portal, resource groups, and virtual machines

---

Architecture Overview

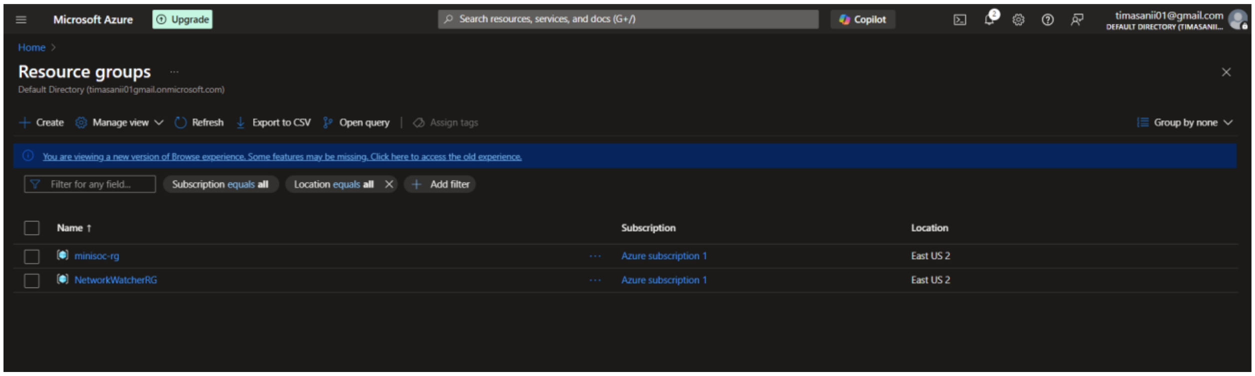
```
+----------------------+     +------------------------+

| Azure Virtual VM     | <---> | Log Analytics Workspace|

| (Windows Pro 11)     |       | + Sentinel (SIEM)       |
+----------------------+    +-------------------------+
```

Setup Steps

1. Create Free Azure Account

2. Create Resource Group

1. In the Azure Portal, go to **Resource groups** > **+ Create**
2. Provide a name (e.g., minisoc-rg) and select a region
3. Click **Review + create**, then **Create**



Resource groups

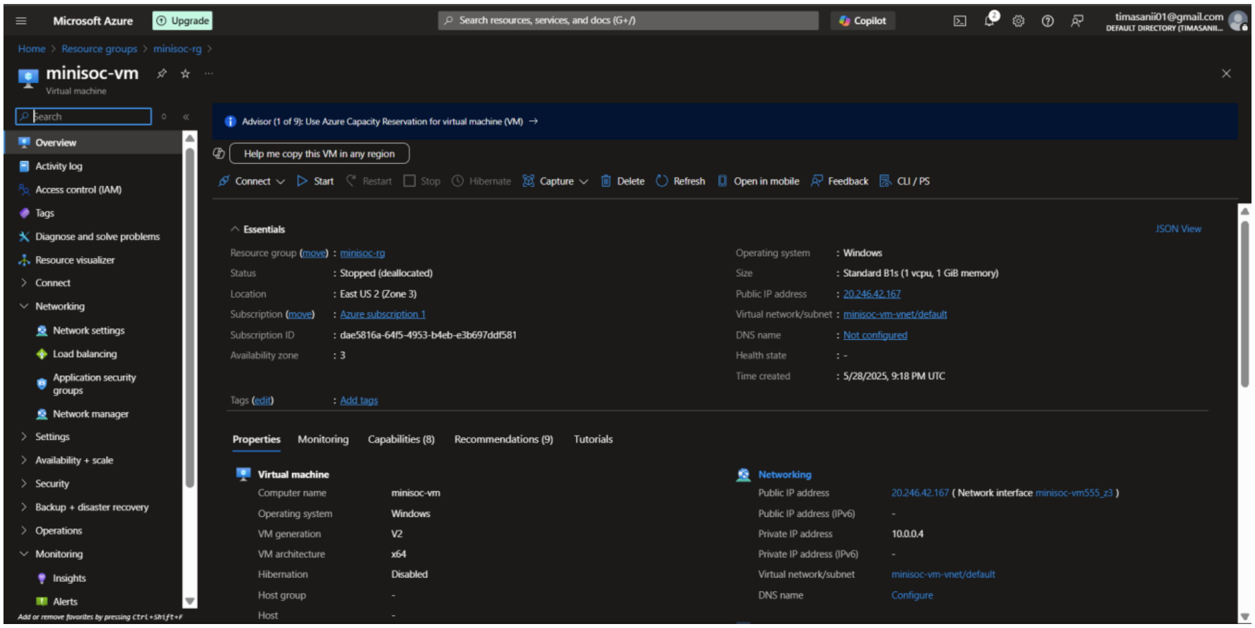
Default Directory (timasanii01gmail.onmicrosoft.com)

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Name ↑	Subscription	Location
minisoc-rg	Azure subscription 1	East US 2
NetworkWatcherRG	Azure subscription 1	East US 2

3. Provision Azure Virtual Machine

1. In the portal, navigate to **Virtual machines** > **+ Create**
2. Select **Azure Resource Manager**
3. Choose the **minisoc-rg** resource group
4. Under Image, pick **Windows 11 Pro**
5. Configure size and credentials
6. Under **Networking**, ensure **RDP (3389)** is open to your IP
7. Click **Review + create**, then **Create**



Essentials

Resource group (move) : minisoc-rg
Status : Stopped (deallocated)
Location : East US 2 (Zone 3)
Subscription (move) : Azure subscription 1
Subscription ID : dae5816a-64f5-4953-b4eb-e3b697ddf581
Availability zone : 3

Operating system : Windows
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : 20.246.42.167
Virtual network/subnet : minisoc-vm-vnet/default
DNS name : Not configured
Health state : -
Time created : 5/28/2025, 9:18 PM UTC

Tags (edit) : Add tags

Virtual machine

Computer name	minisoc-vm
Operating system	Windows
VM generation	V2
VM architecture	x64
Hibernation	Disabled
Host group	-
Host	-

Networking

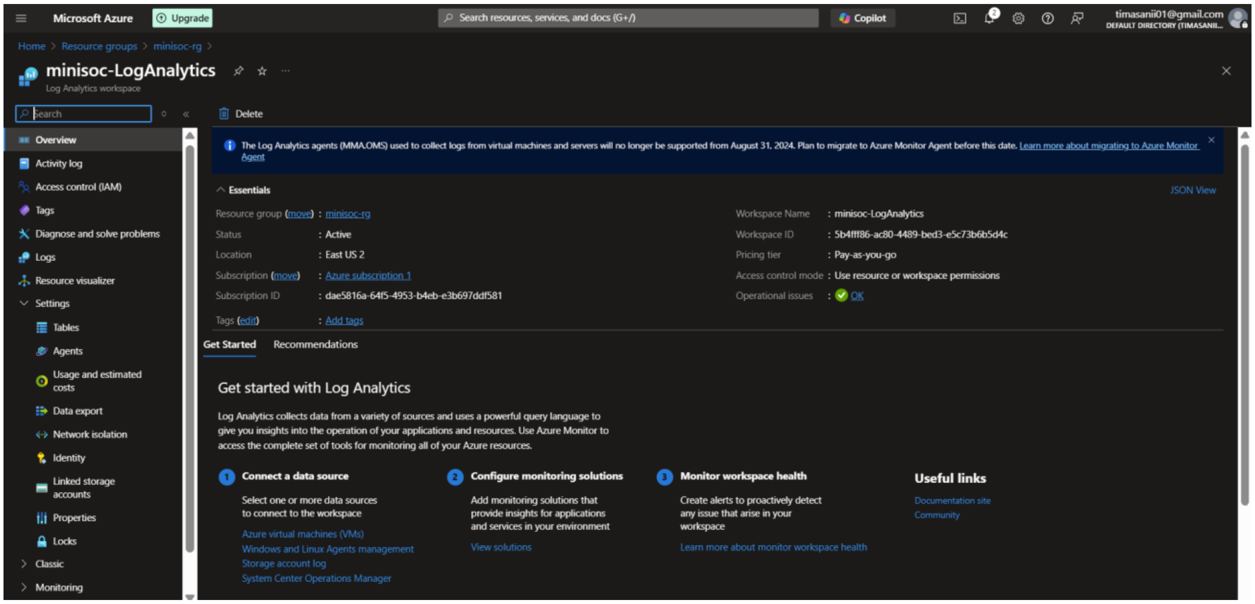
Public IP address	20.246.42.167 (Network interface minisoc-vm555_z3)
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	minisoc-vm-vnet/default
DNS name	Configure

4. Deploy Microsoft Sentinel

1. In the Azure Portal, search for **Microsoft Sentinel**
2. Click **+ Add**
3. Select the target **Log Analytics workspace** (create in next step)

5. Create Log Analytics Workspace

1. Navigate to **Log Analytics workspaces** > **+ Create**
2. Select **mini-soc-rg**
3. Provide a name (e.g., minisoc-LogAnalytics)
4. Choose region and pricing tier
5. Click **Review + create**, then **Create**



The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to Azure Monitor Agent

Resource group (move) : minisoc-rg
Status : Active
Location : East US 2
Subscription (move) : Azure subscription 1
Subscription ID : dae5816a-64f5-4953-b4eb-e3b697ddf581
Tags (edit) : Add tags

Workspace Name : minisoc-LogAnalytics
Workspace ID : 5b4fff86-ac80-4489-bed3-e5c73b6b5d4c
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : ✓ OK

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)
Windows and Linux Agents management
Storage account log
System Center Operations Manager

2 Configure monitoring solutions

Add monitoring solutions that provide insights for applications and services in your environment

View solutions

3 Monitor workspace health

Create alerts to proactively detect any issue that arise in your workspace

Learn more about monitor workspace health

Useful links

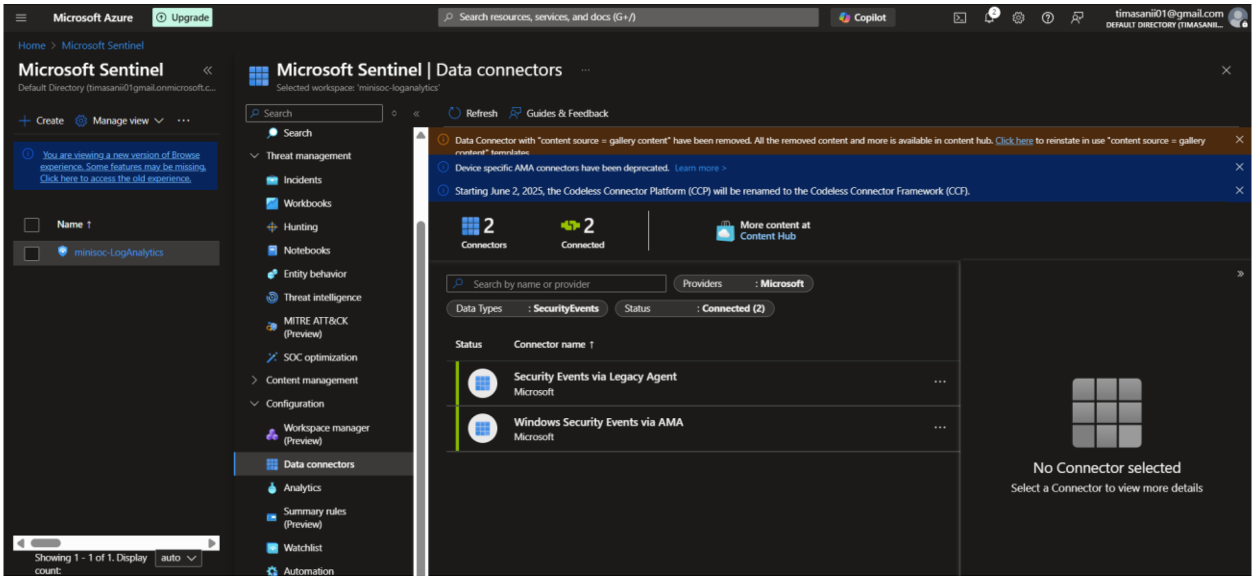
Documentation site
Community

6. Connect Sentinel to Workspace

1. In **Microsoft Sentinel**, under **Settings** > **Workspace settings**
2. Add the newly created **mini-soc-law** workspace

7. Configure Windows Security Events Connector

1. In **Microsoft Sentinel**, go to **Data connectors**
2. Select **Windows Security Events**
3. Click **Open connector page**
4. Under **Data rule name**, enter WinSecEventsConnector
5. Select your VM under **Connected sources**
6. Enable **All security events** (IDs 4624, 4625, etc.)
7. Click **Apply changes**



Microsoft Sentinel | Data connectors

Selected workspace: 'minisoc-loganalytics'

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

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

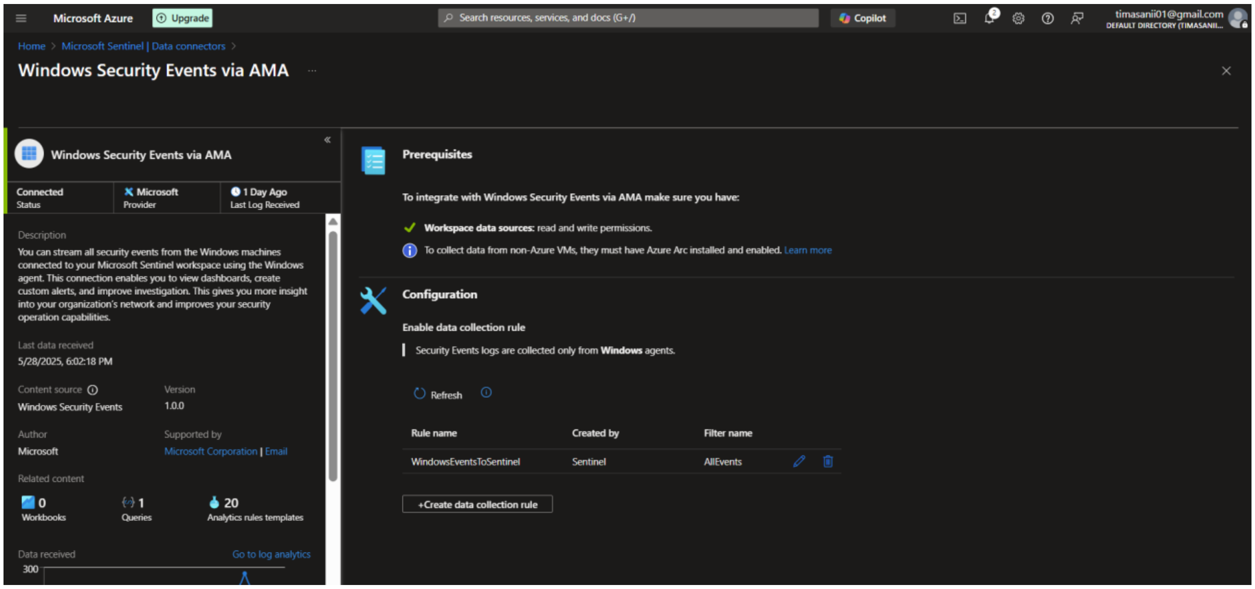
Device specific AMA connectors have been deprecated. Learn more >

Starting June 2, 2025, the Codeless Connector Platform (CCP) will be renamed to the Codeless Connector Framework (CCF).

Status	Connector name ↑
	Security Events via Legacy Agent Microsoft
	Windows Security Events via AMA Microsoft

8. Create Sentinel Alert Rule

1. In **Microsoft Sentinel**, navigate to **Analytics** > **+ Create** > **Scheduled query rule**
2. Name the rule SuccessfulLocalSigninAlert
3. Set **Schedule** to run every **5** minutes, look back **5** minutes
4. Configure alert details, severity, and action groups as needed
5. Click **Create**


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
timasanii01@gmail.com
DEFAULT DIRECTORY (TIMASANII...
Home > Microsoft Sentinel | Data connectors >
Refresh
+Create data collection rule
Go to log analytics
300

Windows Security Events via AMA

Windows Security Events via AMA

Status	Provider	Last Log Received
Connected	Microsoft	1 Day Ago

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

5/28/2025, 6:02:18 PM

Content source: Windows Security Events

Version: 1.0.0

Author: Microsoft

Supported by: Microsoft Corporation | Email

Related content

Workbooks	Queries	Analytics rules templates
0	1	20

Data received

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

✓ **Workspace data sources:** read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more

Configuration

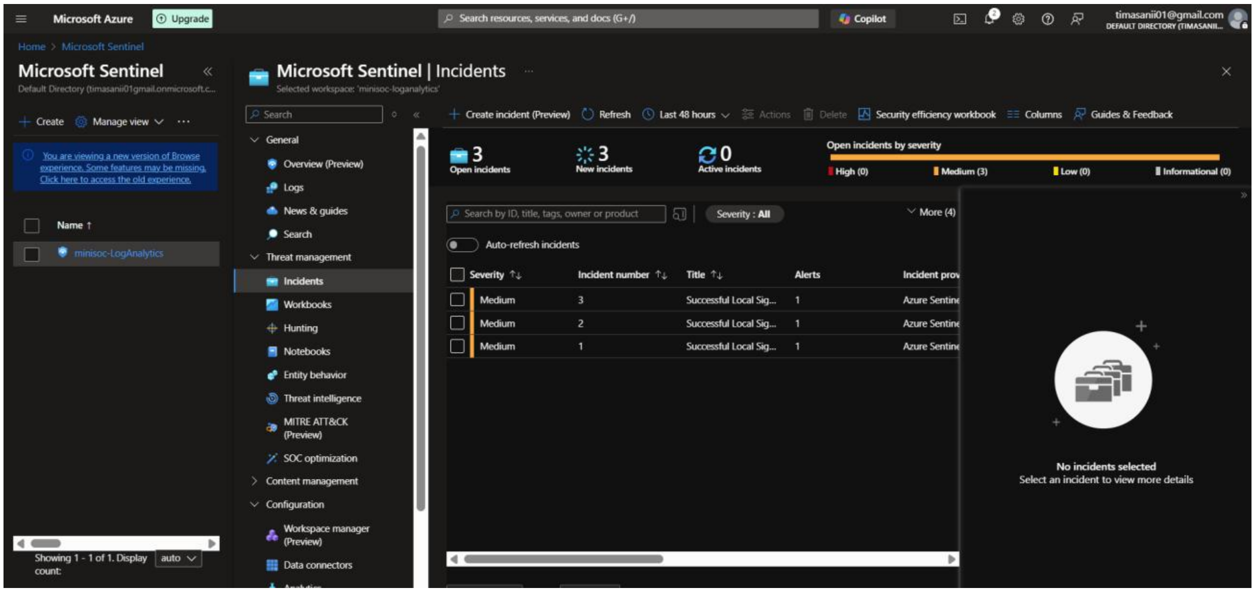
Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Rule name	Created by	Filter name
WindowsEventsToSentinel	Sentinel	AllEvents

Usage

- Monitor incoming alerts via the **Incidents** tab in Microsoft Sentinel
- Investigate by clicking on the alert to view event details



You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Microsoft Sentinel | Incidents

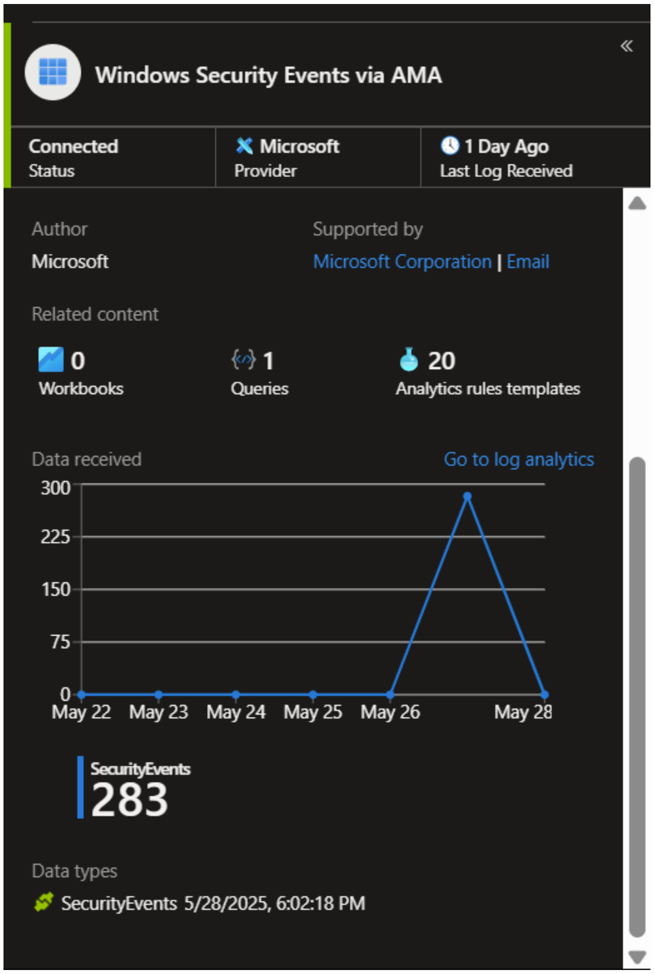
Selected workspace: 'minisoc-loganalytics'

3 Open incidents | 3 New incidents | 0 Active incidents

Open incidents by severity: High (0) | Medium (3) | Low (0) | Informational (0)

Severity	Incident number	Title	Alerts	Incident prov
Medium	3	Successful Local Sig...	1	Azure Sentine
Medium	2	Successful Local Sig...	1	Azure Sentine
Medium	1	Successful Local Sig...	1	Azure Sentine

No incidents selected
Select an incident to view more details



Windows Security Events via AMA

Connected
Status

Microsoft
Provider

1 Day Ago
Last Log Received

Author
Microsoft

Supported by
Microsoft Corporation | Email

Related content

0 Workbooks | 1 Queries | 20 Analytics rules templates

Data received

SecurityEvents
283

Data types

SecurityEvents 5/28/2025, 6:02:18 PM

-