

Home Lab: Basic Security Operations Center

Writeup by: Joseph Elbert

Email: Josephelb@comcast.net

LinkedIn: [LinkedIn Profile](#)

Project Overview

Overview:

- Set up a Windows 10 honeypot VM in Azure
- Ingest logs into Microsoft Sentinel using Log Analytics Workspace
- Perform a basic attack simulation (failed logon attempts)
- Visualize and query logs using KQL
- Enrich data with geolocation for better analysis

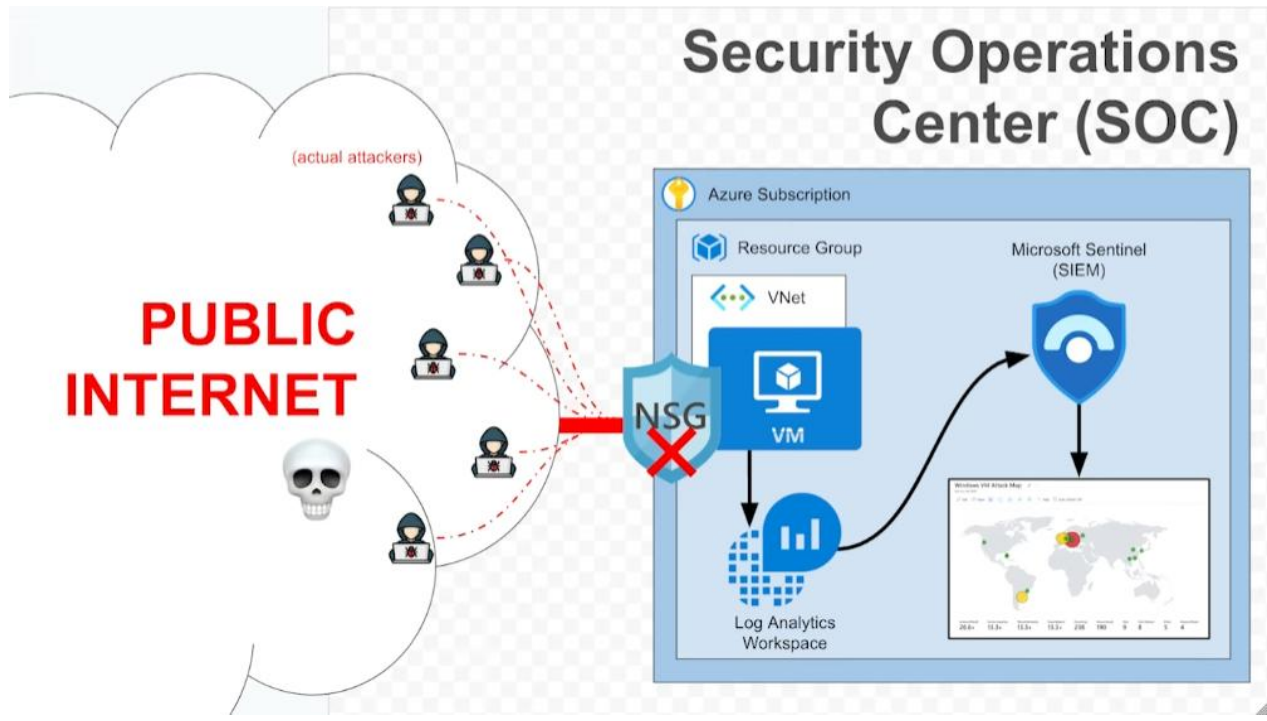
This lab simulates core SIEM tasks and it will eventually introduce the concept of integrating XDR using Microsoft Defender, which can be connected to Sentinel in future projects for extended detection and response capabilities.

Lab Goals and Objectives

My Goals for this lab:

- Understand how to deploy an Azure VM for monitoring
- Set up a Log Analytics Workspace and Microsoft Sentinel
- Ingest and analyze Windows security logs
- Write and run KQL queries to investigate specific events
- Enrich logs with external geolocation data using watchlists
- Visualize alerts and log trends in an interactive dashboard

Network Map



Resource Group

To begin, I will be making a resource group in order to keep all of our resources together for this project. Below is what I began with. First, I will click on create. I named my group **Joe-SOC-Lab**.

The image shows two screenshots of the Microsoft Azure portal. The top screenshot displays the 'Resource groups' page, which is currently empty, showing a message 'No resource groups to display' and a '+ Create' button. The bottom screenshot shows the 'Create a resource group' form, where the user has entered 'Joe-SOC-Lab' as the resource group name and selected '(US) East US' as the region. The form also shows the subscription as 'Azure for Students'.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home >

Resource groups

Augusta University (augedu.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags

Group by none

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

Filter for any field... Subscription equals all Location equals all Add filter

No resource groups to display

Resource groups provide a logical container to manage and organize Azure resources, simplifying administration and enabling efficient resource management.

+ Create

Learn more

Showing 1 - 0 of 0. Display count: auto

Give feedback

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Resource groups >

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

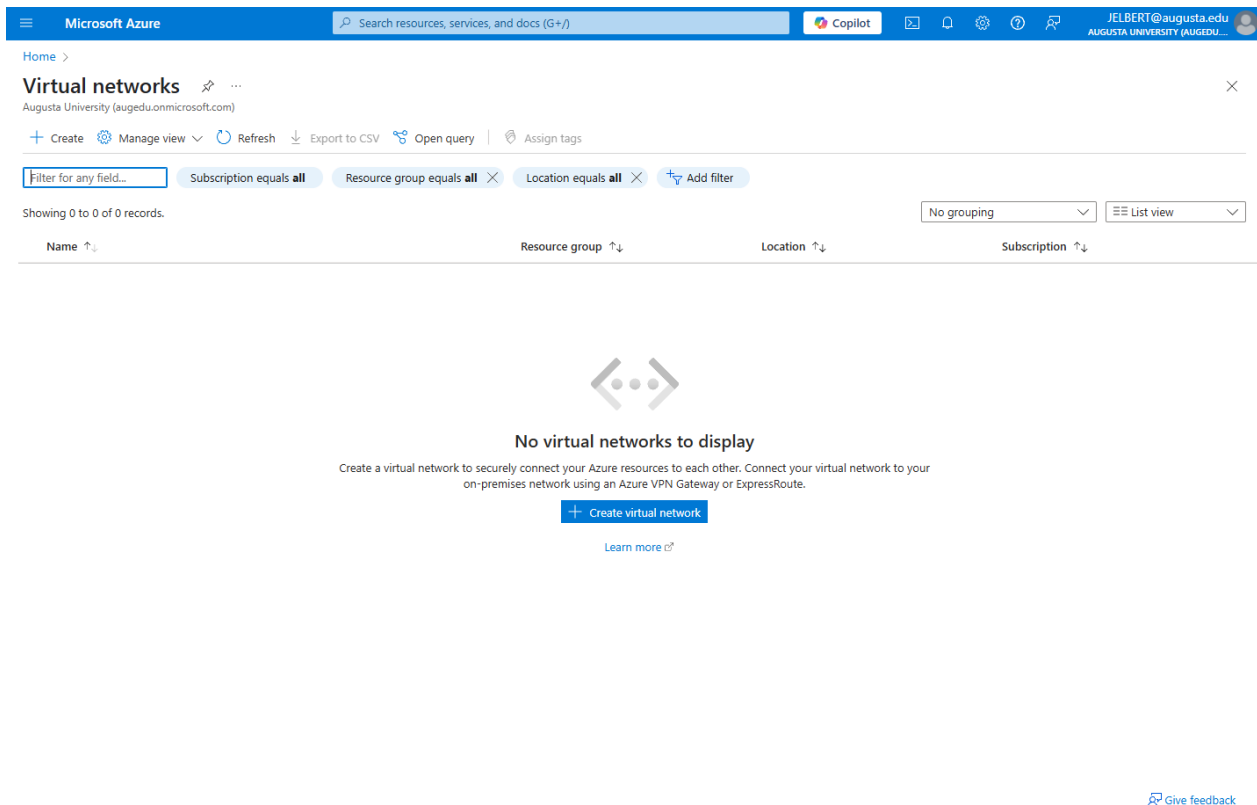
Subscription * Azure for Students

Resource group name * Joe-SOC-Lab

Region * (US) East US

Previous Next Review + create

Next, I will be making a virtual network for a virtual machine honeypot and the Microsoft Sentinel instance. The honeypot will be accessible to anyone in the world, which will help me discover different types of attacks that will attempt to access my system.



If you would like to see a tutorial on how I set up my virtual network, visit this quick video.

[Creating Virtual Network.mp4](#)

It is now time to setup the virtual machine honeypot.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Basics' tab. The interface includes a top navigation bar with the Azure logo, a search bar, and user information. Below the navigation bar, there are tabs for 'Project details', 'Instance details', 'Disks', 'Networking', 'Management', 'Monitoring', 'Advanced', 'Tags', and 'Review + create'. The 'Project details' section includes a message about subscription eligibility and a 'Project details' section with dropdowns for 'Subscription' (Azure for Students) and 'Resource group' ((New) Resource group). The 'Instance details' section includes a 'Virtual machine name' field, a 'Region' dropdown (US East US), an 'Availability zone' dropdown (Zone 1), and 'Zone options' (Self-selected zone). At the bottom, there are buttons for '< Previous', 'Next : Disks >', and 'Review + create'. A 'Give feedback' link is also present.

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ☐ Azure for Students

Resource group * ☐ (New) Resource group

[Create new](#)

Instance details

Virtual machine name *

Region * ☐ (US) East US

Availability options ☐ Availability zone

Zone options ☒ Self-selected zone
Choose up to 3 availability zones, one VM per zone

☐ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

Availability zone * ☐ Zone 1

[Using an Azure-selected zone is not supported in region 'East US'.](#)

[You can now select multiple zones. Selecting multiple zones will create one VM.](#)

< Previous | Next : Disks > | **Review + create**

[Give feedback](#)

These are the settings I used for my virtual machine honeypot. I will include the tabs and their required information. The tabs are down below.

Basics

Subscription	Azure for Students
Resource group	Joe-SOC-Lab
Virtual machine name	CORP-NET-EAST-1
Region	East US
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Standard
Image	Windows 10 Pro, version 22H2 - Gen1
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	labuser
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Client
Azure Spot	No

Disks

OS disk size	Image default
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	Vnet-soc-lab
Subnet	default (10.0.0.0/24)
Public IP	(new) CORP-NET-EAST-1-ip
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Enabled

Management

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Site Recovery	Disabled
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching; patches will be installed by OS

Monitoring

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	-
Proximity placement group	None
Capacity reservation group	None

This is what my Joe-SOC-Lab network looks like after I installed the VM with the settings I configured right before this.

Resource groups
Augusta University (augeduonmicrosoft.com)

Joe-SOC-Lab
Resource group

Overview

Essentials

Subscription (move): [Azure for Students](#)
Subscription ID: f7d0ffab-a00b-4640-be9d-7f0581db89b2
Deployments: [1 Deploying 1 Succeeded](#)
Location: East US
Tags (edit): [Add tags](#)

Resources

Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 6 of 6 records. Show hidden types No grouping List view

Name	Type	Location
CORP-NET-EAST-1	Virtual machine	East US
CORP-NET-EAST-1-ip	Public IP address	East US
CORP-NET-EAST-1-nsg	Network security group	East US
corp-net-east-1632_z1	Network Interface	East US
CORP-NET-EAST-1_OsDisk_1_35ae155c6dca490e87ef150...	Disk	East US
Vnet-soc-lab	Virtual network	East US

Showing 1 - 2 of 2. Display count: auto

Page 1 of 1

Give feedback

Now, its time to configure the firewall so anyone can attacker this VM on the internet. This makes this a honeypot. I went to the inbound security rules and set it where all inbound connections are allowed.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open, showing the 'Inbound security rules' section for the 'CORP-NET-EAST-1-nsg' network security group. The main pane displays a table of existing security rules:

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc--	Any	Any
65500	DenyAllInBound	Any	Any

The 'Add inbound security rule' dialog is open on the right. It is configured as follows:

- Source: Any
- Source port ranges: *
- Destination: Any
- Service: Custom
- Destination port ranges: 8080
- Protocol: Any
- Action: Allow
- Priority: 100
- Name: AllowAnyCustom8080Inbound
- Description: (empty)

The 'Add' button is highlighted in blue.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open, showing the 'Inbound security rules' section for the 'CORP-NET-EAST-1-nsg' network security group. The main pane displays a table of existing security rules:

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc--	Any	Any
65500	DenyAllInBound	Any	Any

The 'Add inbound security rule' dialog is open on the right. It is configured as follows:

- Source: Any
- Source port ranges: *
- Destination: Any
- Service: Custom
- Destination port ranges: *
- Protocol: Any
- Action: Allow
- Priority: 100
- Name: DANGER_AllowAnyCustomAnyInbound
- Description: (empty)

The 'Add' button is highlighted in blue.

The virtual machine is ready. We can now connect to the virtual machine via Remote Desktop Protocol (RDP) on port 3389.

The screenshot displays the Microsoft Azure portal interface. On the left, the navigation pane shows the 'Virtual machines' section under 'Compute infrastructure'. The main pane shows the details for the virtual machine 'CORP-NET-EAST-1'. On the right, a 'Native RDP' connection window is open, providing instructions for connecting to the VM. The window includes a 'Switch local machine OS' dropdown and three main steps: 1. 'Configure prerequisites for Native RDP', which shows that port 3389 access is configured and the public IP address is 40.76.121.134; 2. 'Open Remote Desktop Connection (on Windows)', which instructs the user to open RDP from their local machine; and 3. 'Download and open the RDP file', which provides a button to download the RDP file. The 'Other Information' section includes a link to 'Reset password'.

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Compute infrastructure | Virtual machines > CORP-NET-EAST-1

Compute infrastructure | Virtual machines

Overview

All resources

Infrastructure

Virtual machines

Virtual Machine Scale Set (VMSS)

Compute Fleet

Disks + images

Capacity + placement

Related services

Help

Virtual machines

Get started

+ Create

Switch to classic

Filter for any field...

Name

CORP-NET-EAST-1

CORP-NET-EAST-1 | Connect

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Connect

Bastion

Windows Admin Center

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

Automation

Help

Native RDP

Connect from your local machine (Windows)

Switch local machine OS

1 Configure prerequisites for Native RDP

Azure needs to configure some features in order to connect to the VM.

Prerequisites configured

Port 3389 access

Port 3389 on this virtual machine is accessible from the local machine IP (174.50.101.149). [Learn more](#)

Change the port for connecting to this virtual machine on the Connect page of the virtual machine.

Public IP address: 40.76.121.134

A public IP address is required to connect via this connection method.

Configured

2 Open Remote Desktop Connection (on Windows)

Open Remote Desktop Connection. Or change your local machine operating system to view more instructions. [Learn more](#)

3 Download and open the RDP file

Download and open the RDP file to connect to the virtual machine.

Username

labuser

Download RDP file

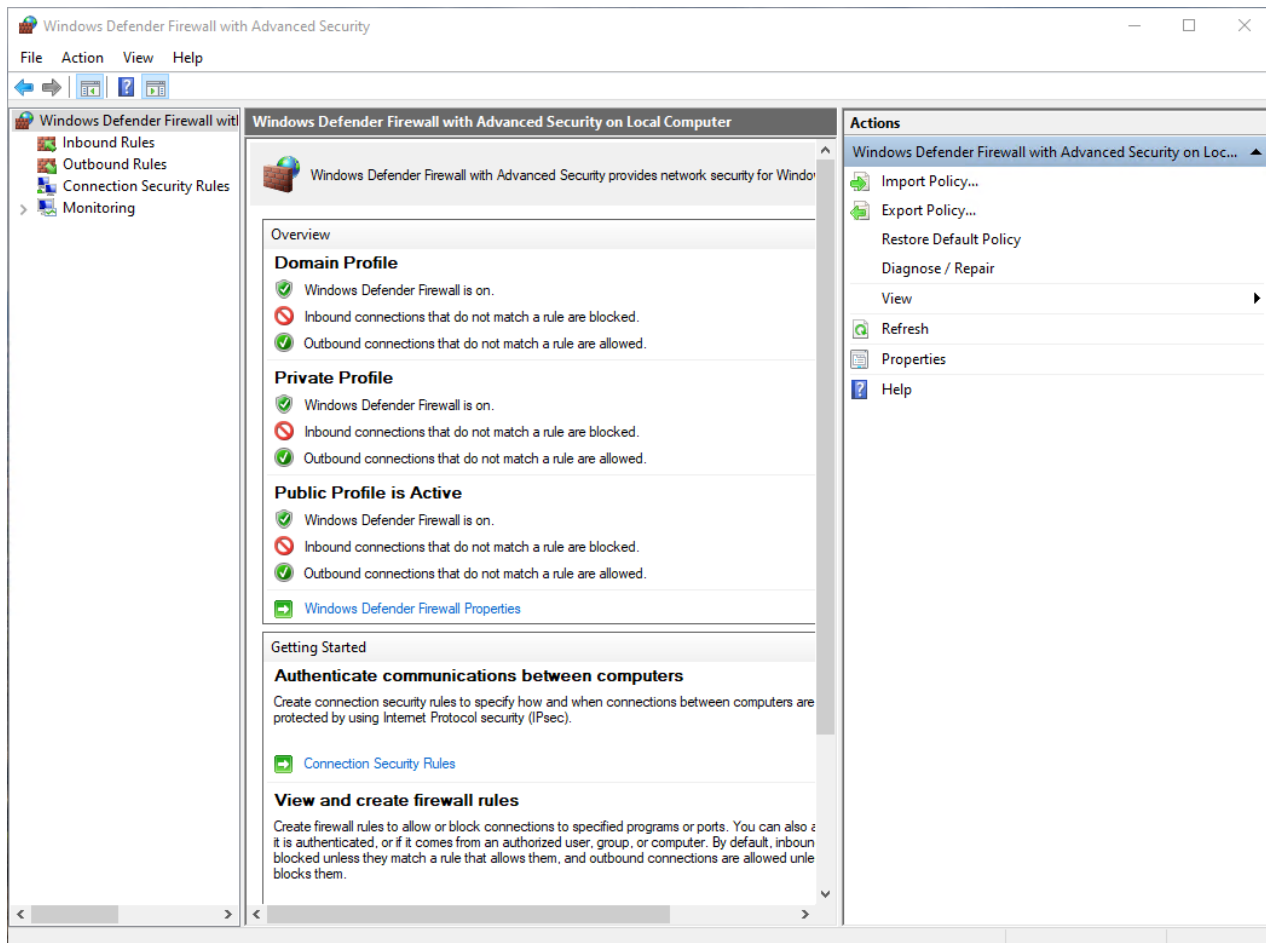
Other Information

Forgot password?

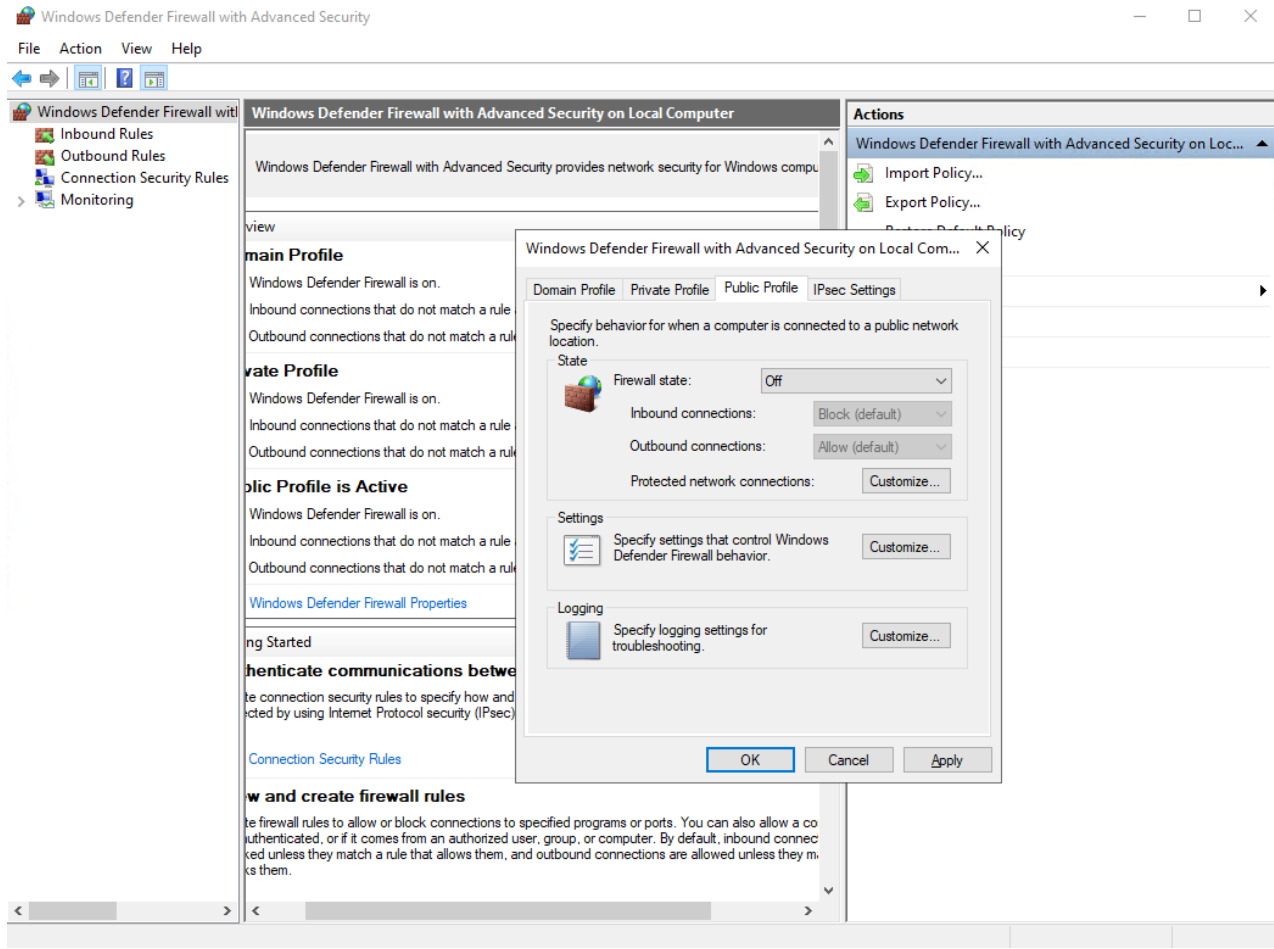
[Reset password](#)

Close Troubleshooting Give feedback

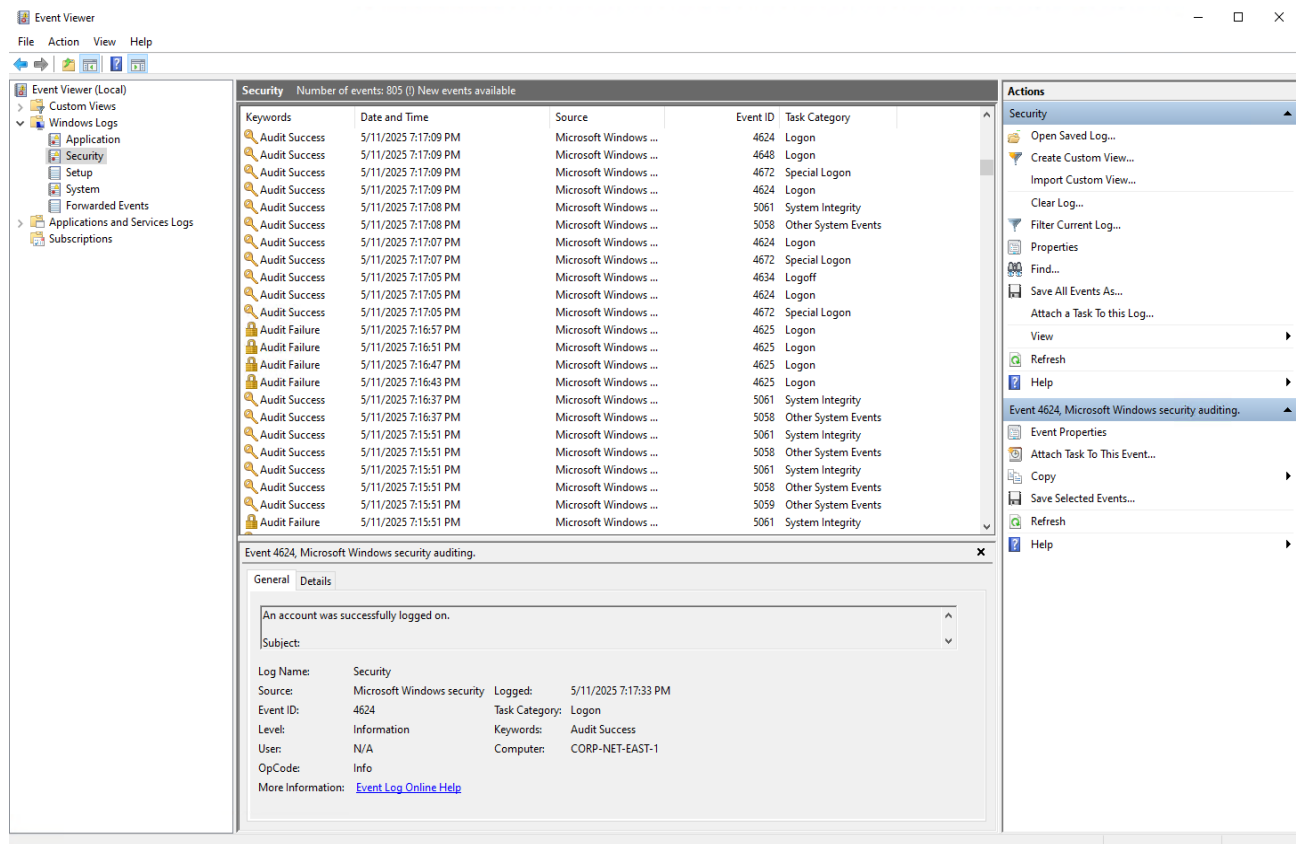
Once logged into the virtual machine, it is time to open the Windows Defender Firewall settings. We need to do this in order to make it a honeypot for remote attackers to connect to it. Type in the search bar: “**wf.msc**” to open this menu.



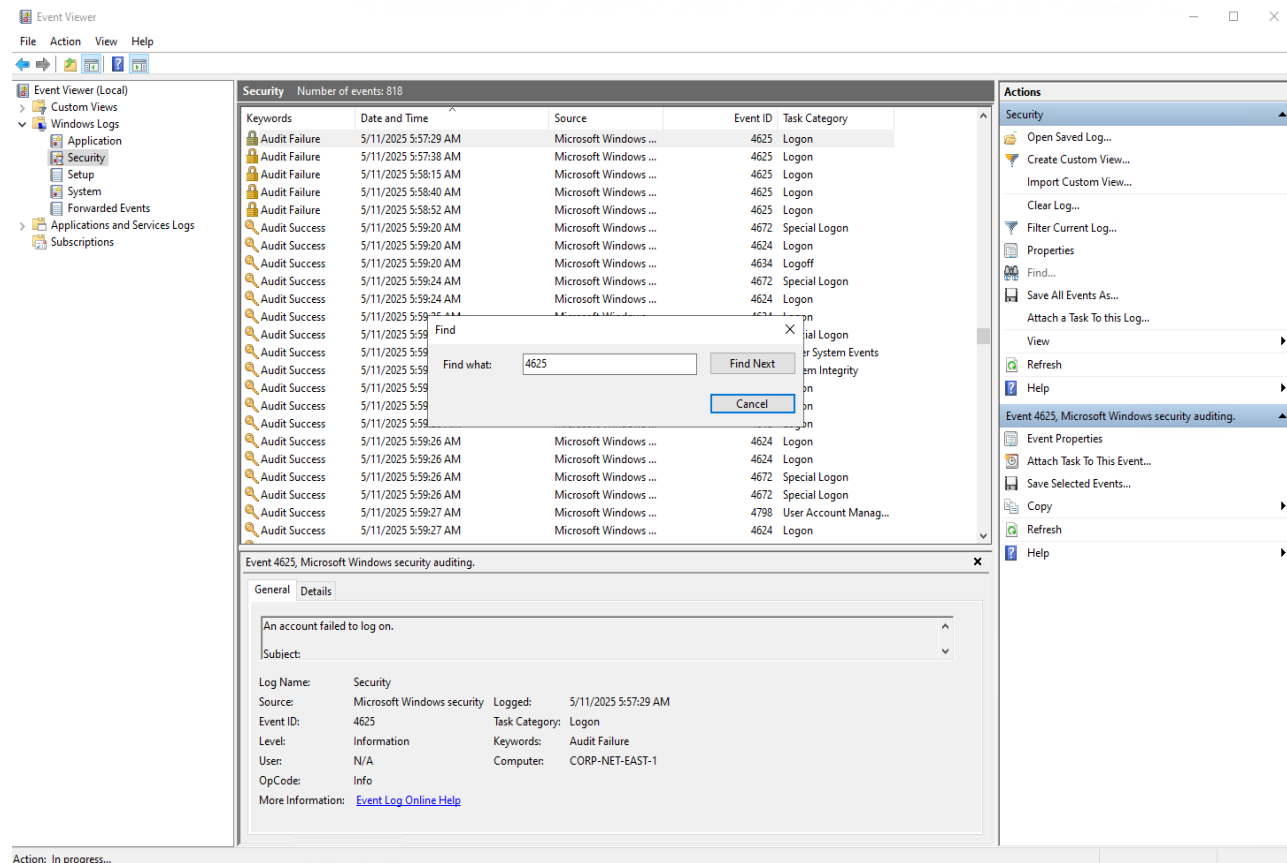
In the middle of the screen, go to “Windows Defender Firewall Properties” and you should see the box below pop up. On the first 3 tabs, press the “o” key to turn all of the settings off on each of the tabs. Click apply and then exit out.



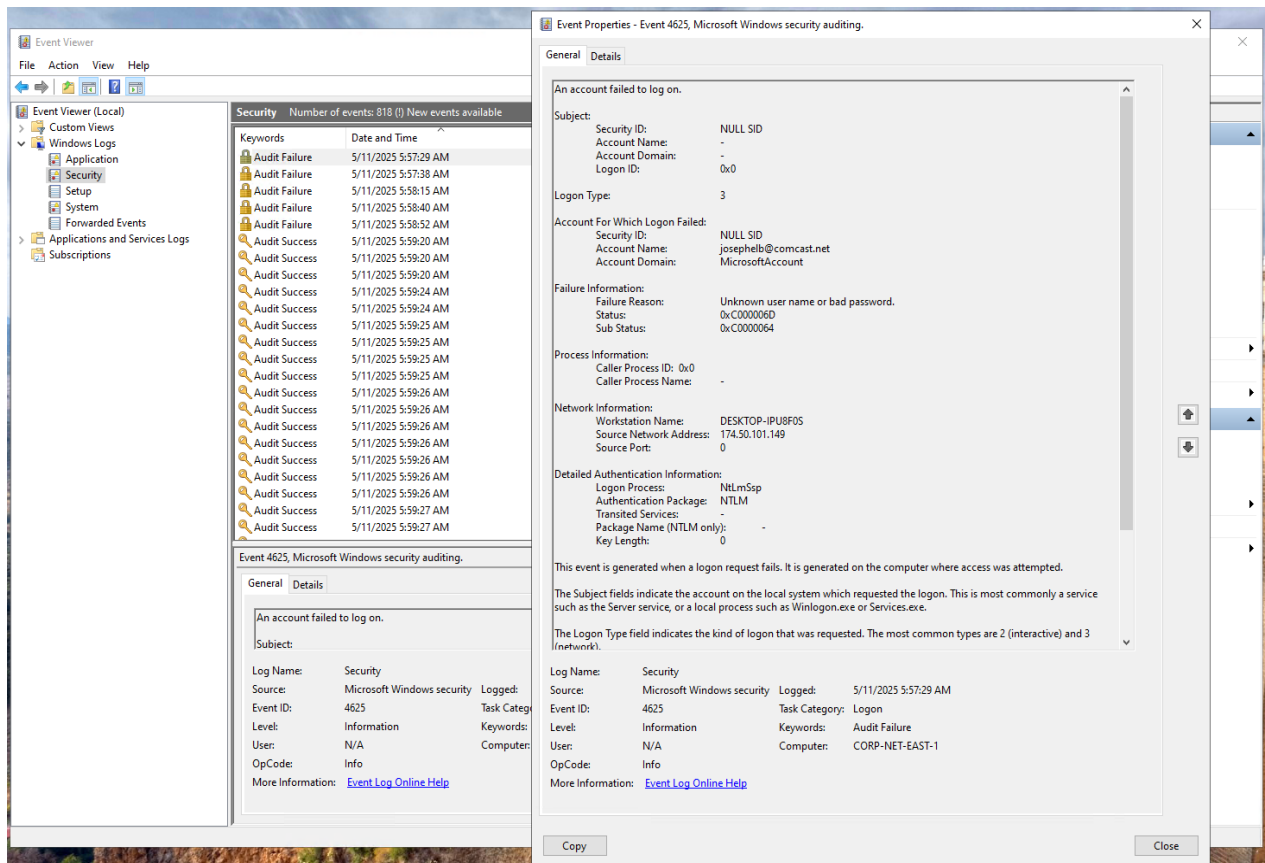
Now, its time to go into Event Viewer to learn about system logs. Once in Event Viewer, go to the “Windows Logs” folder. Then go to the “Security” tab to view windows security event logs.



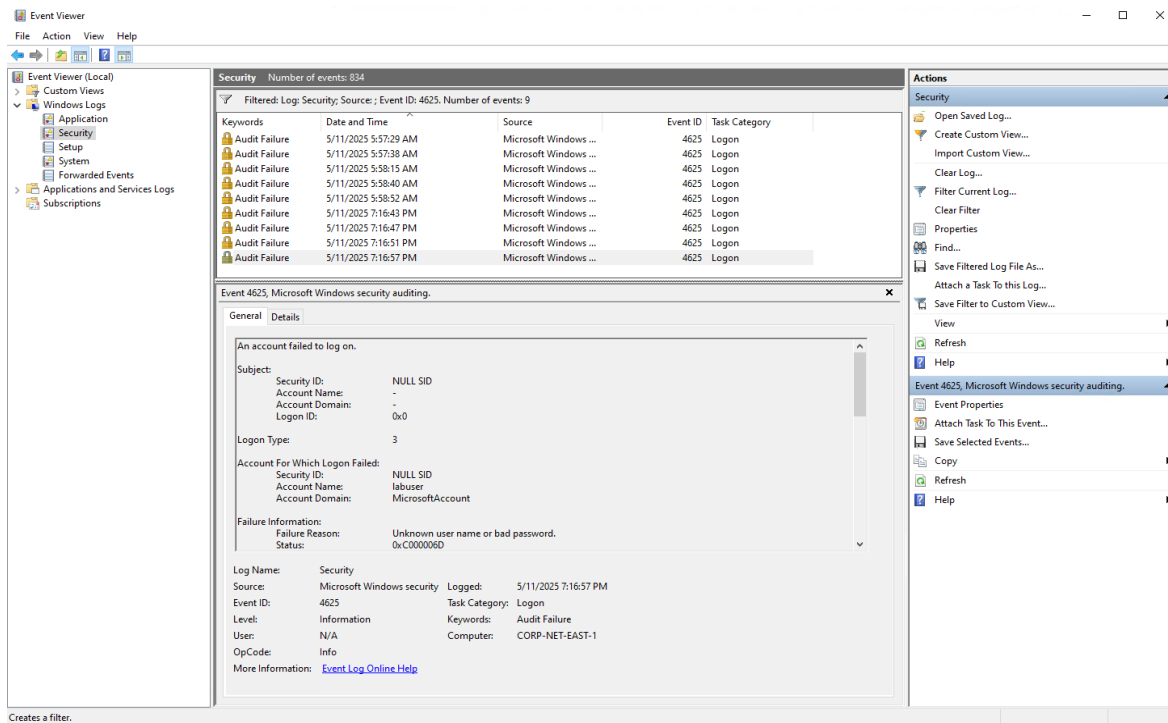
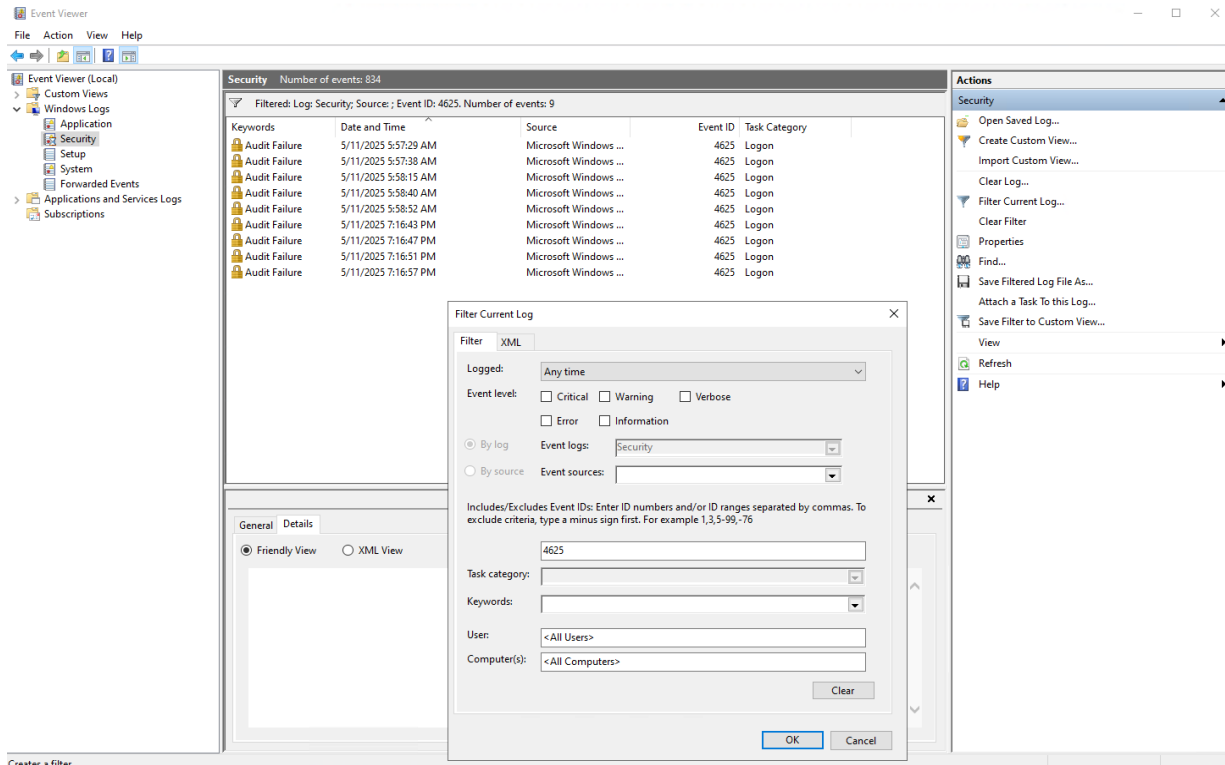
Press “ctrl + f” in order to search for certain EventID numbers. The EventID below is 4625 and it has to do with events related to system logon’s.



Click on any file and you will be able to see all of the information for the security event log. You can see things like account name, failure reason, and the IP address it came from.



You can also filter the list of logs based on the currently selected log. You do this in order to see logs that have the same exact EventID, which can help map attack patterns.



Next, it is time to create a log analytics workspace. This is needed in order to connect our VM to our Microsoft Sentinel Security Information and Event Management (SIEM) system.

The screenshot shows the Microsoft Azure portal interface for 'Log Analytics workspaces'. The header includes the Microsoft Azure logo, a search bar, and the user profile 'JELBERT@augusta.edu'. The main content area displays 'Log Analytics workspaces' with a sub-header 'Augusta University (augedu.onmicrosoft.com)'. Below this are navigation links: '+ Create', 'Open recycle bin', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A filter bar shows 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. The table below the filter bar is empty, with columns for Name, Resource group, Location, and Subscription. A message states 'No log analytics workspaces to display' and explains that workspaces leverage unique environments for log data from Azure Monitor and other Azure services. A button '+ Create log analytics workspace' is prominently displayed, along with a 'Learn more' link.

The screenshot shows the Microsoft Azure portal interface for 'Microsoft Sentinel'. The header includes the Microsoft Azure logo, a search bar, and the user profile 'JELBERT@augusta.edu'. The main content area displays 'Microsoft Sentinel' with a sub-header 'Augusta University (augedu.onmicrosoft.com)'. Below this are navigation links: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'View incidents'. A filter bar shows 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. The table below the filter bar is empty, with columns for Name, Resource group, Location, Subscription, and Directory. A message states 'No Microsoft Sentinel to display' and explains that Sentinel is used to see and stop threats before they cause harm. A button '+ Create Microsoft Sentinel' is prominently displayed, along with a 'Learn more' link.

Here, I will be linking the Microsoft Sentinel instance to my Log analytics workspace: LAW-soc-lab workspace.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace

+ Create a new workspace Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...				
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
LAW-soc-lab-0000	eastus	joe-soc-lab	Azure for Students	Augusta University

Add Cancel

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | News & guides

Selected workspace: 'law-soc-lab-0000'

Search Documentation

General

- Overview
- Logs
- News & guides**
- Search
- Threat management
- Content management
- Configuration

Get started Free trial

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

Install your first content hub solution

Discover and install Microsoft Sentinel content, which includes data connectors, workbooks, analytics, and automation with a single deployment step.

[Go to content hub](#)

1. Collect data

Collect data at cloud scale across the enterprise from on-premises to multiple clouds.

Documentation

Data connectors documentation

[Documentation](#)

Add or remove favorites by pressing Ctrl+Shift+F

Once Microsoft Sentinel was connected, it was time to install some addons. I needed to add Windows Security Events to the Microsoft Sentinel instance. Here, you can also add other things like **Cisco Umbrella**, **Amazon Web Services (AWS)**, **Log4j Vulnerability Detection**, and many other Microsoft integrations.

The screenshot shows the Microsoft Sentinel Content Hub interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the 'Content hub' section is active, showing a search for 'security event'. The results table lists various solutions, with 'Windows Security Events' highlighted as 'In progress'. A right-hand pane provides details for 'Windows Security Events', including a note about the installation process and a list of data connectors.

Content title	Status	Content source	Provider	Support
SlashNext Security Events	Not installed	Solution	SlashNext	SlashNext
SlashNextSecurityEventsforMicrosoftSentinel	Not installed	Solution	SlashNext	SlashNext
Windows Security Events	In progress	Solution	Microsoft	Microsoft
Security Events via Legacy Agent	In progress	Solution	Microsoft	Microsoft
Windows Security Events via AMA	In progress	Solution	Microsoft	Microsoft
NRT Security Event log cleared	In progress	Solution	Microsoft	Microsoft
Event Analyzer	In progress	Solution	Microsoft	Microsoft
New EXE deployed via Default Domain or ...	In progress	Solution	Microsoft	Microsoft
Gain Code Execution on ADFS Server via S...	In progress	Solution	Microsoft	Microsoft
Excessive Windows Logon Failures	In progress	Solution	Microsoft	Microsoft
Starting or Stopping HealthService to Avoi...	In progress	Solution	Microsoft	Microsoft

Windows Security Events

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20

[Install](#) [View details](#)

It is now time to configure the windows security events I just installed. The one that I edited was the Windows Security Events via AMA (Azure Monitoring Agent).

Microsoft Azure

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

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Microsoft Sentinel | Content hub >

Windows Security Events

Refresh Delete Reinstall

74 Installed content items 22 Configuration needed

Windows Security Events

Microsoft Provider Microsoft Support 3.0.9 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Manage Actions View details

Search...

Content name	Create...	Conte...	Ve...
<input type="checkbox"/> Security Events via Legacy Agent	▲ 1 items	Data c...	1.0
<input type="checkbox"/> Windows Security Events via AMA	▲ 1 items	Data c...	1.0
<input type="checkbox"/> AD FS Remote Auth Sync Connection	▲ --	Analyti...	1.0
<input type="checkbox"/> AD FS Remote HTTP Network Connection	▲ --	Analyti...	1.0
<input type="checkbox"/> AD user enabled and password not set within 48 hours	▲ --	Analyti...	1.0
<input type="checkbox"/> ADFS Database Named Pipe Connection	▲ --	Analyti...	1.0
<input type="checkbox"/> Excessive Windows Logon Failures	▲ --	Analyti...	2.0
<input type="checkbox"/> Exchange OAB Virtual Directory Attribute Containing Potential Webshell	▲ --	Analyti...	1.0
<input type="checkbox"/> Gain Code Execution on ADFS Server via SMB + Remote Service or Schedule	--	Analyti...	1.0
<input type="checkbox"/> Microsoft Entra ID Local Device Join Information and Transport Key Registry	--	Analyti...	1.0
<input type="checkbox"/> New EXE deployed via Default Domain or Default Domain Controller Policies	--	Analyti...	1.0
<input type="checkbox"/> Non Domain Controller Active Directory Replication	▲ --	Analyti...	1.0
<input type="checkbox"/> NRT Base64 Encoded Windows Process Command-lines	▲ --	Analyti...	1.0
<input type="checkbox"/> NRT Process executed from binary hidden in Base64 encoded file	▲ --	Analyti...	1.0
<input type="checkbox"/> NRT Security Event log cleared	▲ --	Analyti...	1.0
<input type="checkbox"/> Potential Fodhelper UAC Bypass	▲ --	Analyti...	1.0

< Previous Page 1 of 3 Next > Showing 1 to 30 of 74 results.

No templates selected
Select templates to view more details

Microsoft Azure

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

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Microsoft Sentinel | Content hub >

Windows Security Events

Refresh Delete Reinstall

74 Installed content items 22 Configuration needed

Windows Security Events

Microsoft Provider Microsoft Support 3.0.9 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Manage Actions View details

Search...

Content name	Create...	Conte...	Ve...
<input type="checkbox"/> Security Events via Legacy Agent	▲ 1 items	Data c...	1.0
<input checked="" type="checkbox"/> Windows Security Events via AMA	▲ 1 items	Data c...	1.0
<input type="checkbox"/> AD FS Remote Auth Sync Connection	▲ --	Analyti...	1.0
<input type="checkbox"/> AD FS Remote HTTP Network Connection	▲ --	Analyti...	1.0
<input type="checkbox"/> AD user enabled and password not set within 48 hours	▲ --	Analyti...	1.0
<input type="checkbox"/> ADFS Database Named Pipe Connection	▲ --	Analyti...	1.0
<input type="checkbox"/> Excessive Windows Logon Failures	▲ --	Analyti...	2.0
<input type="checkbox"/> Exchange OAB Virtual Directory Attribute Containing Potential Webshell	▲ --	Analyti...	1.0
<input type="checkbox"/> Gain Code Execution on ADFS Server via SMB + Remote Service or Schedule	--	Analyti...	1.0
<input type="checkbox"/> Microsoft Entra ID Local Device Join Information and Transport Key Registry	--	Analyti...	1.0
<input type="checkbox"/> New EXE deployed via Default Domain or Default Domain Controller Policies	--	Analyti...	1.0
<input type="checkbox"/> Non Domain Controller Active Directory Replication	▲ --	Analyti...	1.0
<input type="checkbox"/> NRT Base64 Encoded Windows Process Command-lines	▲ --	Analyti...	1.0
<input type="checkbox"/> NRT Process executed from binary hidden in Base64 encoded file	▲ --	Analyti...	1.0
<input type="checkbox"/> NRT Security Event log cleared	▲ --	Analyti...	1.0
<input type="checkbox"/> Potential Fodhelper UAC Bypass	▲ --	Analyti...	1.0

< Previous Page 1 of 3 Next > Showing 1 to 30 of 74 results.

Windows Security Events via AMA

Disconnected Status Microsoft Provider -- Last Log Received

Content source Windows Security Events Version 1.0.0

Author Microsoft Supported by Microsoft Corporation | Email

Data received

Go to query

0

Data types SecurityEvents --

Open connector page

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Microsoft Sentinel | Content hub > Windows Security Events >

Windows Security Events via AMA

Windows Security Events via AMA

Disconnected Status

Microsoft Provider

Last Log Received

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

--

Content source

Version

Windows Security Events

1.0.0

Author

Supported by

Microsoft

Microsoft Corporation | Email

Related content

0 Workbooks

1 Queries

20 Analytics rules templates

Data received

Go to log analytics

4

3

2

1

0

May 4

May 5

May 6

May 7

May 8

May 10

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.

Refresh

Rule name

Created by

Filter name

No results

+Create data collection rule

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY (AUGEDU...)

Home > Microsoft Sentinel | Content hub > Windows Security Events >

Windows Security Events via AMA

Windows Security Events via AMA

Disconnected Status

Microsoft Provider

Last Log Received

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

--

Content source

Version

Windows Security Events

1.0.0

Author

Supported by

Microsoft

Microsoft Corporation | Email

Related content

0 Workbooks

1 Queries

20 Analytics rules templates

Data received

Go to log analytics

4

3

2

1

0

May 4

May 5

May 6

May 7

May 8

May 10

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.

Refresh

Rule name

Created by

Filter name

No results

+Create data collection rule

Create Data Collection Rule

Data collection rule management

Basic Resources Collect Review + create

Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned identity for all other applications. [Learn more](#)

Subscriptions

Resource Groups

Resource Types

Locations

Selected: All

Selected: All

Selected: All

Selected: All

Search to filter items...

Show Selected

Scope

Resource Type

Location

Azure for Students

Joe-SOC-Lab

CORP-NET-EAST-1

microsoft.compute/virtualmachines

East US

< Previous

Next: Collect >

I went into my VM and I needed to install an Azure monitoring agent in order for the logs to be sent to the Log Analytics Workspace, and then to the Microsoft Sentinel instance.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user profile for JELBERT@augusta.edu. The main content area is titled 'CORP-NET-EAST-1 | Extensions + applications'. On the left, a sidebar menu lists various VM management options, with 'Extensions + applications' selected. The main panel shows a table of installed extensions. The table has columns for Name, Type, Version, Latest Version, Status, and Automatic upgrade status. One extension is listed: 'AzureMonitorWindowsAgent' of type 'Microsoft.Azure.Monitor...' with version '1.34.0.0'. The status is 'Provisioning succeeded' and the automatic upgrade status is 'Disabled'.

Name	Type	Version	Latest Version	Status	Automatic upgrade status
AzureMonitorWindowsAgent	Microsoft.Azure.Monitor...	1.34.0.0	1.34.0.0	Provisioning succeeded	Disabled

Once it was connected, I had to wait like 5-10 minutes in order to receive my first set of logs. Microsoft Sentinel uses KQL which is similar to SQL (The language I am familiar with), and it helps query the results of the logs in order to find specific logs easier.

The screenshot shows the Microsoft Azure portal interface for a Log Analytics workspace named 'LAW-soc-lab-0000'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Resource visualizer, Settings, Classic, Monitoring, Automation, and Help. The main pane displays a KQL query named 'SecurityEvent' with a time range of 'Last 24 hours' and 'Show: 1000 results'. The query results are shown in a table with columns: TimeGenerated [UTC], Account, AccountType, Computer, and EventSourceName. The results show several log entries for 'Microsoft-Windows-Security-Auditing' events.

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName
> 5/11/2025, 8:09:07:507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing
> 5/11/2025, 8:09:07:507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing
> 5/11/2025, 8:05:31:770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing
> 5/11/2025, 8:05:31:770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing
> 5/11/2025, 8:05:31:710 PM	WORKGROUP\CORP-NET-EAST-1	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing
> 5/11/2025, 8:05:31:709 PM	WORKGROUP\CORP-NET-EAST-1	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing
> 5/11/2025, 8:05:27:533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing
> 5/11/2025, 8:05:27:533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing

This screenshot shows the same Microsoft Azure Log Analytics workspace, but with a more detailed KQL query. The query results table includes additional columns: Channel and Task. The results show several log entries for 'Microsoft-Windows-Security-Auditing' events, including details about the channel and task.

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task
> 5/11/2025, 8:09:07:507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	12548
> 5/11/2025, 8:09:07:507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	12544
> 5/11/2025, 8:05:31:770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	12548
> 5/11/2025, 8:05:31:770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	12544
> 5/11/2025, 8:05:31:710 PM	WORKGROUP\CORP-NET-EAST-1	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	13826
> 5/11/2025, 8:05:31:709 PM	WORKGROUP\CORP-NET-EAST-1	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	13826
> 5/11/2025, 8:05:27:533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	12548
> 5/11/2025, 8:05:27:533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-Auditing	Security	12544

This was my first official KQL query. It searches the SecurityEvent logs table and has parameters that are specified with each | character.

The screenshot shows the Microsoft Azure portal interface for a Log Analytics workspace named 'LAW-soc-lab-0000'. A KQL query is entered in the editor:

```
1 SecurityEvent
2 | where Account == "NT AUTHORITY\SYSTEM"
```

The query is executed, and the results are displayed in a table. The table has columns: TimeGenerated [UTC], Account, AccountType, Computer, EventSourceName, Channel, and Task. The results show 10 entries for the 'NT AUTHORITY\SYSTEM' account, all with a Task ID of 12548.

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task
5/11/2025, 8:10:58.313 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:10:58.313 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:10:48.215 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:10:48.215 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:10:41.625 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:10:41.625 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:09:07.507 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:05:31.770 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12548
5/11/2025, 8:05:27.533 PM	NT AUTHORITY\SYSTEM	Machine	CORP-NET-EAST-1	Microsoft-Windows-Security-A...	Security	12544

The screenshot shows the Microsoft Azure portal interface for a Log Analytics workspace named 'LAW-soc-lab-0000'. A KQL query is entered in the editor:

```
1 SecurityEvent
2 | where Account == "NT AUTHORITY\SYSTEM"
3 | project Account, TimeGenerated, Computer, EventID, Activity, IPAddress
```

The query is executed, and the results are displayed in a table. The table has columns: Account, TimeGenerated [UTC], Computer, EventID, Activity, and IPAddress. The results show 10 entries for the 'NT AUTHORITY\SYSTEM' account, with EventID 4672 and 4624, and Activity descriptions.

Account	TimeGenerated [UTC]	Computer	EventID	Activity	IPAddress
NT AUTHORITY\SYSTEM	5/11/2025, 8:15:11.206 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:15:11.206 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:58.313 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:58.313 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:48.215 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:48.215 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:41.625 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:10:41.625 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:09:07.507 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:09:07.507 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:31.770 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:31.770 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:27.533 PM	CORP-NET-EAST-1	4672	4672 - Special privileges assigned to new logon.	-
NT AUTHORITY\SYSTEM	5/11/2025, 8:05:27.533 PM	CORP-NET-EAST-1	4624	4624 - An account was successfully logged on.	-

This query lets me use “**project**” in order to only show columns in the query results that I want to see. This shows that a user tried to logon to the system 3 times and failed each time.

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'JELBERT@augusta.edu AUGUSTA UNIVERSITY'. The main workspace is titled 'LAW-soc-lab-0000 | Logs'. A new query is being edited in the 'New Query 1' tab. The query is as follows:

```
1 SecurityEvent
2 | where EventID == 4625
3 | project TimeGenerated, Account, Computer, EventID, Activity, IPAddress
```

The query results are displayed in a table with the following columns: TimeGenerated [UTC], Account, Computer, EventID, Activity, and IPAddress. The results show three failed login attempts for the account 'MicrosoftAccount\CrypTicXz' on the computer 'CORP-NET-EAST-1' with EventID 4625. The activity for all three is '4625 - An account failed to log on.' and the IP address is '174.50.101.149'.

TimeGenerated [UTC]	Account	Computer	EventID	Activity	IPAddress
> 5/11/2025, 8:20:28.718 PM	MicrosoftAccount\CrypTicXz	CORP-NET-EAST-1	4625	4625 - An account failed to log on.	174.50.101.149
> 5/11/2025, 8:20:22.029 PM	MicrosoftAccount\CrypTicXz	CORP-NET-EAST-1	4625	4625 - An account failed to log on.	174.50.101.149
> 5/11/2025, 8:20:17.401 PM	MicrosoftAccount\CrypTicXz	CORP-NET-EAST-1	4625	4625 - An account failed to log on.	174.50.101.149

The bottom status bar shows '0s 376ms | Display time (UTC+00:00)' and 'Query details | 1 - 3 of 3'.

Now, I need to setup a watchlist to make it easier to see where IP addresses are connecting from. Information like their country, city, and coordinates.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu

Home > Microsoft Sentinel

Microsoft Sentinel

Augusta University

Create Manage view

Filter for any field...

Name

LAW-soc-lab-0000

Microsoft Sentinel | Watchlist

Selected workspace: 'law-soc-lab-0000'

Search Refresh New Delete Update watchlist Columns Guides & Feedback

General

Overview (Preview)

Logs

News & guides

Search

Threat management

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Summary rules (Preview)

Watchlist

Automation

Settings

0 Watchlists

0 Watchlist Items

My Watchlists Templates (Preview)

Watchlist

What is it?

Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.

How does it work?

Create a new watchlist by selecting 'Add new' and follow the steps in the new watchlist wizard. You will receive a notification in the notifications area within in the Azure portal that your watchlist was created. Watchlists are stored within your Microsoft Sentinel workspace as name value pairs and are cached for optimal query performance and low latency.

This is what you can do with watchlists

Investigate threats and respond to incidents quickly with fast import of IP addresses, file hashes, etc. from external threat intelligence.

Import business data, such as user lists with privileged system access as a watchlist. Then use the watchlist to create alerts and dashboards.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu

Home > Microsoft Sentinel | Watchlist

Watchlist wizard

General Source Review + create

Source type *

Local file

File type *

CSV file with a header (.csv)

Number of lines before row with headings *

0

Upload file *

geoiip-summarized.csv

Drag and drop the files or Browse for files

SearchKey *

network

Reset

File preview | First 50 rows and first 5 columns

network	latitude	longitude	cityname	countryname
1.0.0/16	-33.494	143.2104		Australia
1.1.0/16	17.8148	103.3386	Ban Chan	Thailand
1.2.0/16	13.8667	100.1917	Nakhon Pathom	Thailand
1.3.0/16	13.8679	100.1891	Nakhon Pathom	Thailand
1.4.0/16	13.6687	100.579	Bangkok	Thailand
1.5.0/16	13.6659	100.5882	Bangkok	Thailand
1.6.0/16	12.9634	77.5855	Bengaluru	India
1.7.0/16	12.9691	77.5902	Bengaluru	India
1.8.0/16	12.9557	77.5843	Bengaluru	India
1.9.0/16	3.1539	101.7448	Ampang	Malaysia

< Previous

Next: Review + create >

Give feedback

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

JELBERT@augusta.edu
AUGUSTA UNIVERSITY

Home > Microsoft Sentinel

Microsoft Sentinel

Augusta University

+ Create Manage view ...

Filter for any field...

Name ↑

LAW-soc-lab-0000

Microsoft Sentinel | Watchlist

Selected workspace: 'law-soc-lab-0000'

Search

Refresh

+ New

Delete

Update watchlist

Columns

Guides & Feedback

General

Overview (Preview)

Logs

News & guides

Search

Threat management

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Summary rules (Preview)

Watchlist

Automation

Settings

1 Watchlists

51K Watchlist Items

My Watchlists

Templates (Preview)

Search by name, alias and description

Add filter

<input checked="" type="checkbox"/>	Name	Alias
<input checked="" type="checkbox"/>	geoup	geoup

< Previous

Page 1 of 1

Next >

Showing 1 to 1 of 1 results.

geoup

Microsoft Provider

51K Rows

5/11/20... Created time

Description

Source

geoup-summarized.csv

Created by

JELBERT@augusta.edu

Last updated

5/11/2025, 4:32:14 PM

SearchKey

network

Status (Preview)

Succeeded

View in logs

Update watchlist

The watchlist is uploaded, so now I can filter through the logs again to find exactly where the user is trying to login from. This is a more advanced KQL query.

The screenshot shows the Microsoft Azure Log Analytics workspace interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'JELBERT@augusta.edu'. The main header indicates the workspace is 'LAW-soc-lab-0000 | Logs'. Below this, a 'New Query 1' tab is active, showing a KQL query. The query is designed to filter security events based on a watchlist of IP addresses and then look up the geographic location of the attacker.

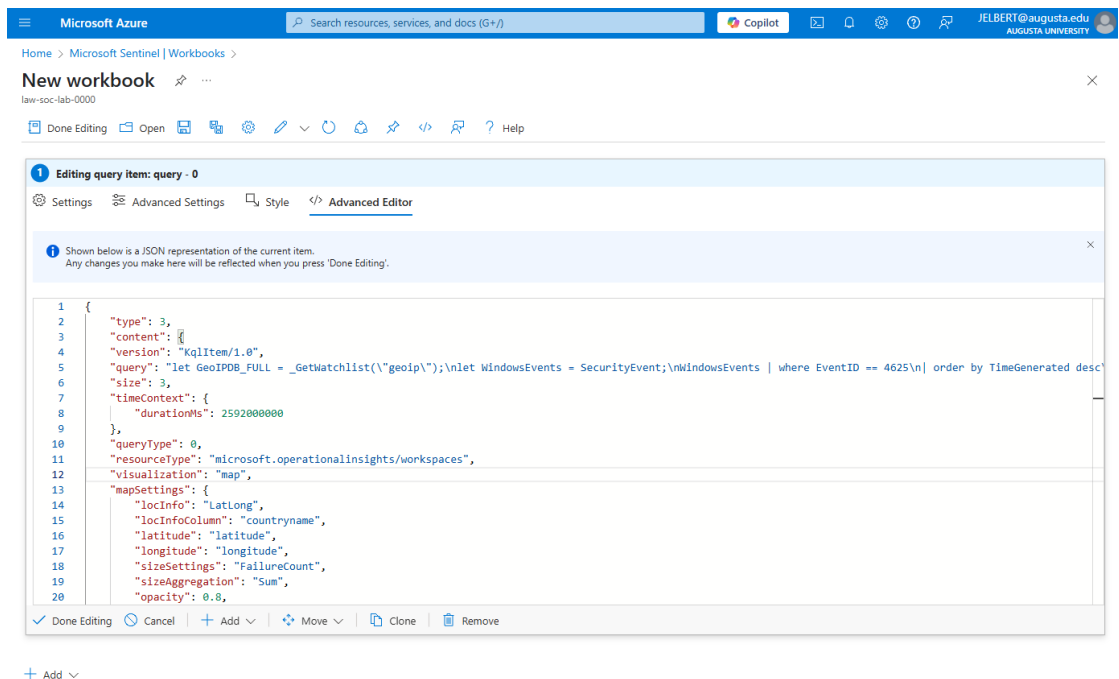
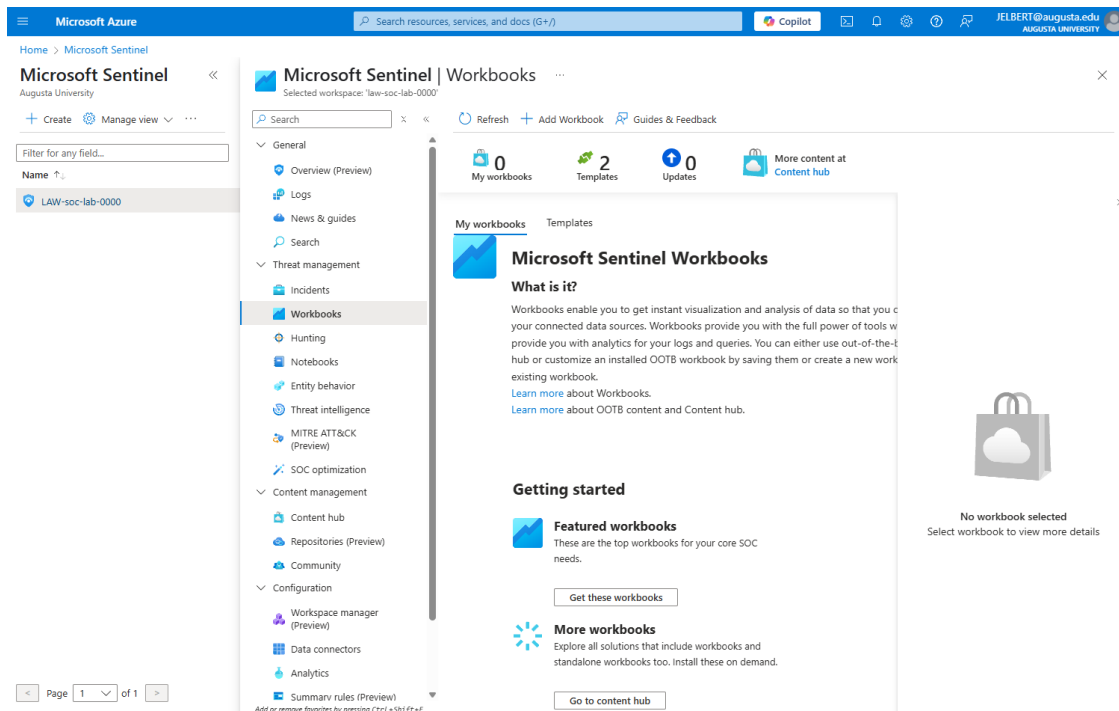
```
1 let GeoIPDB_FULL = _GetWatchlist("geoip");
2 let WindowsEvents = SecurityEvent
3   | where IPAddress == "174.50.101.149"
4   | where EventID == 4625
5   | order by TimeGenerated desc
6   | evaluate ipv4_lookup(GeoIPDB_FULL, IPAddress, network);
7 WindowsEvents
8 | project TimeGenerated, Computer, AttackerIp = IPAddress, cityname, countryname, latitude, longitude
9
```

The query results are displayed in a table with the following columns: TimeGenerated [UTC], Computer, AttackerIp, cityname, countryname, latitude, and longitude. The results show five entries, all from the computer 'CORP-NET-EAST-1' at the IP address '174.50.101.149', located in Chula Vista, United States.

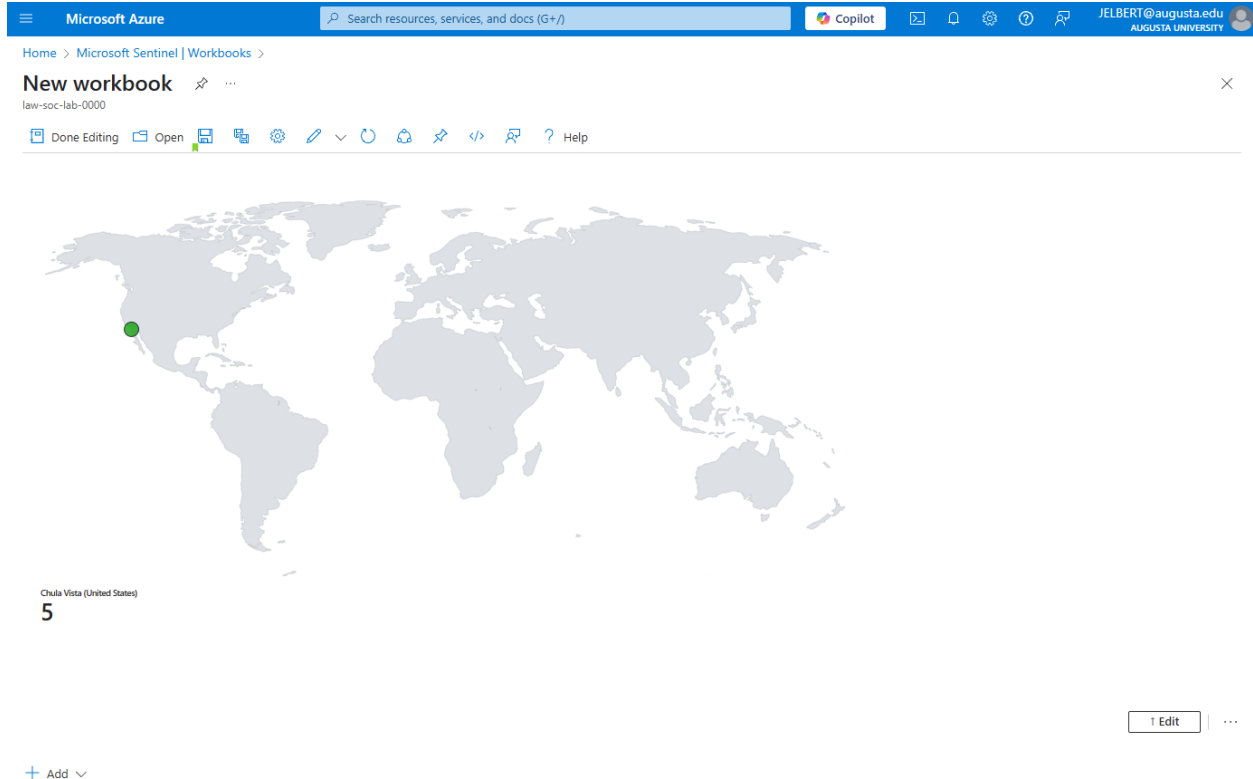
TimeGenerated [UTC]	Computer	AttackerIp	cityname	countryname	latitude	longitude
> 5/11/2025, 8:54:32.921 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
> 5/11/2025, 8:54:17.012 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
> 5/11/2025, 8:20:28.718 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
> 5/11/2025, 8:20:22.029 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801
> 5/11/2025, 8:20:17.401 PM	CORP-NET-EAST-1	174.50.101.149	Chula Vista	United States	32.6387	-117.0801

The bottom of the interface shows the query execution time as '0s 463ms' and the display time as 'Display time (UTC+00:00)'. There are also links for 'Query details' and a page indicator '1 - 5 of 5'.

After running that query to confirm that the watchlist was successfully uploaded. I then had to make a workbook in order to help me map the attacks. In the workbook advanced editor, I pasted some JSON that will help draw a map on the screen and help me visualize the attacks.



Since I don't have many attackers connecting to my VM honeypot, I only have one attacker that has tried to logon to my system so far. It is displayed on the map below. Once more attackers try to logon or attack my VM honeypot, more circles will start to appear. The circles will be colored based on the severity of the attack. Green will be the lowest, yellow medium is a medium rating, and red will be a critical rating.



I can also edit the map settings even further if I wanted to.

The screenshot displays the Microsoft Sentinel interface for a workspace named 'Windows VM Attack Map'. The main area shows a world map with a single green dot located in Mexico, representing a data point from the query. The query is as follows:

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent;
WindowsEvents | where EventID == 4625
| order by TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL, IPAddress, network)
| summarize FailureCount = count() by IPAddress, latitude, longitude, cityname, countryname
| project FailureCount, AttackerIp = IPAddress, latitude, longitude, city = cityname, country = countryname,
friendly_location = strcat(cityname, " (", countryname, ")");
```

The 'Map Settings' panel on the right is open, showing various configuration options:

- Layout Settings:**
 - Location Info using: Latitude/Longitude
 - Latitude: Latitude
 - Longitude: Longitude
 - Size by: FailureCount
 - Aggregation for location: Sum of values
 - Minimum region size: 20
 - Maximum region size: 70
 - Default region size: 10
 - Minimum value: (auto)
 - Maximum value: (auto)
 - Opacity of items on Map: 0.8
- Color Settings:**
 - Coloring Type: Heatmap
 - Color by: FailureCount
 - Aggregation for color: Sum of values
 - Color palette: Green to Red
 - Minimum value: (auto)

Buttons at the bottom of the panel include 'Apply', 'Save and Close', and 'Cancel'.

Future Goals

Optional Integration: Microsoft Defender for Cloud:

Although Defender for Cloud was not connected during this lab, Microsoft Sentinel can be integrated with Defender to enable **SIEM + XDR** functionality. This allows for correlation of Defender alerts, asset risk scoring, and cross-platform visibility across cloud workloads and endpoints.

The main future improvement I want to add are automated alerts or setting detection thresholds for alerts. I also want to configure plans for incidents as well.

Key Outcomes and Lessons Learned

- Built Cloud Infrastructure from Scratch: Successfully configured an Azure-based virtual environment using best practices around resource groups, VMs, NSGs, and agent installation.
- Gained Experience with Microsoft Sentinel SIEM: Explored Sentinel's capabilities including data connectors, event ingestion, querying, enrichment, and dashboarding.
- Mastered KQL Basics for Log Analysis: Practiced querying large sets of security event data to filter, project, and sort log entries using SecurityEvent logs and Event ID filters (e.g., 4625 - failed logins).
- Learned Log Enrichment through Watchlists: Imported a GeoIP dataset to enrich logs with geographic information, allowing correlation between attack origin and event type.
- Visualized Security Data in Workbooks: Created a dynamic workbook and customized JSON queries to map attack attempts in a visual format, simulating analyst reporting techniques.

- Learned the Role of SIEM in Modern SOC: Understood how SIEMs fit into the broader detection and response ecosystem, and the value of future XDR integrations with tools like Microsoft Defender.

Conclusion

This lab gave me hands-on experience with **real-world cloud security operations** by deploying and managing a basic SIEM solution using **Microsoft Sentinel** in **Azure**. I configured an open honeypot to simulate live attack scenarios, practiced querying logs using **Kusto Query Language (KQL)**, enriched raw log data with geolocation context using a **Sentinel watchlist**, and visualized events using **workbooks** and **custom dashboards**.

Through this experience, I gained firsthand understanding of how SIEM tools ingest and correlate data, how security analysts monitor activity, and how incident detection workflows are built in modern cloud environments. I also learned how to transform raw logs into actionable intelligence—a skill that’s critical for **SOC analysts, cybersecurity engineers, and threat hunters**.

This lab has not only improved my technical skills but also prepared me to contribute meaningfully to a **Security Operations Center (SOC)** or a **cloud security team** by demonstrating:

- Basic Cloud infrastructure setup (Azure)
- Security event ingestion and correlation (Sentinel + Log Analytics)
- Basic threat detection through log analysis
- SIEM dashboard creation for visibility and reporting

This project sets a strong foundation for more advanced work in incident response, threat detection, and SIEM/XDR integration in my studies.