**SIEM in Azure with Live Worldwide Cyber Attacks**

In this tutorial I will be describing the process of setting up Azure Sentinel (SIEM) as well as a Virtual Machine (VM) in the cloud which will function as our honeypot. This honeypot will be vulnerable to the internet, and we will be monitoring and logging attacks from different IP addresses from various countries around the world. We will then take that data and display it on a map so we can visually see where the attacks are coming from. The logging attacks will consist of failed Remote Desktop Protocol (RDP) attacks.

This is tutorial will take 1-1.5 hours to complete.

A picture containing graphical user interface

Description automatically generated

This tutorial allowed me to gain knowledge to the following:

1. Azure Portal
2. Azure Sentinel
3. Kusto Query Language (KQL)
4. Network Security Groups

**Index**

**Prerequisites**

1. **PowerShell Script for the Lab:** https://github.com/joshmadakor1/Senti...
2. **Azure Trial:** <https://azure.microsoft.com/en-us/free/>
3. **Sentinel Map Query:**

FAILED\_RDP\_WITH\_GEO\_CL | summarize event\_count=count() by sourcehost\_CF, latitude\_CF, longitude\_CF, country\_CF, label\_CF, destinationhost\_CF

| where destinationhost\_CF != "samplehost"

| where sourcehost\_CF != ""

**Steps**

1. **Create a free Azure subscription**
2. A picture containing graphical user interface

   Description automatically generatedFirst start by setting up a free Azure account (<https://azure.microsoft.com/en-us/free/>). A $200 Azure credit will be assigned to your account for up to 30 days.
3. **Create a Virtual Machine**
4. A screenshot of a computer

   Description automatically generatedThis is the machine that will be exposed on the internet. To create one, open -> <https://portal.azure.com/#home> and input “Virtual machines” and select it on the search bar.
5. Click on the “Create” button on the top right and select “Virtual machine”

Graphical user interface, text, application, email

Description automatically generated

1. In the “Create a virtual machine” screen, input the following info on the “Basics” tab:

Instance details

Virtual machine name: honeypot1-vm  
Leave everything as default

Administrator account

Username: davidadmin (You can use your name + admin)  
Password: Password123! (You can input any password you wish. This will be used to log into the virtual machine)

Licensing

Check the box (Windows 10 license with multi-tenant hosting rights)

1. Click on the “Next: Disks” button
2. On the “Disks” tab, click on the “Next: Networking” button
3. On the “Networking” tab ->

Network Interface

NIC network security group: Click on the “Advanced” toggle  
Configure network security group: Click on the “Create new” button

In the “Create network security group” screen remove the default “Inbound rules”

Click on “Add an inbound rule” and input the following. Click on the “Add” button. This will allow all traffic from the internet to enter our VM.

Destination port ranges: \*  
Priority: 100  
Name: DANGER\_ANY\_IN

1. Graphical user interface, text, application

   Description automatically generatedClick on “Review and create” and you will see the image below:

Click “Create”. We want to make our VM discoverable by any means necessary, whether it be PCP pings, SYN scans, etc. For this tutorial we will measure by failed RDP login attempts.

Once deployment of the VM is completed it will look like this:

Graphical user interface, text, application, email

Description automatically generated

1. **Create Log Analytics Workspace**

The purpose of creating a Log Analytics workspace is to ingest logs from the VM. The window events logs from the VM will be ingested to the workspace and it will be converted to custom logs which will contain geographic information. This geographic information allows us to determine the location of where the attacks are coming from. Also, our SIEM (Azure sentinel) will connect to this workspace to be able to display the attacks through a map

1. Graphical user interface, text, application

   Description automatically generatedSearch for and select “Log Analytics workspaces” in the Search bar
2. On the “Create Log Analytics Workspace” screen, click on the “Create” button
3. Input the following:

Resource group: honeypot1-vm\_group (Resource group name created from -> **2) Create a Virtual Machine**)

Name: law-honeypot1

1. Click on “Review + Create” button, and click on the “Create” button

Graphical user interface, text, application

Description automatically generated

1. **Enable gathering VM logs in Security Center**

We will enable the ability to gather logs from the VM into the log analytics workspace

1. Search for and select “Microsoft Defender for Cloud” in the Search bar

Graphical user interface, text, application

Description automatically generated

1. On the “Microsoft Defender for Cloud”, on bottom left side, click on “Environment settings”
2. Expand all the options under “Azure” and select the Log Analytics you just made -> “law-honeypot1”
3. Click on “Enable all Microsoft Defender for Cloud plans” and toggle “SQL servers on machines” to Off. Click “Save”

Graphical user interface, text, application, email

Description automatically generated

1. On the left-hand side, click on the “Data collection” tab and toggle to “All Events”. Click “Save”
2. Go back to the “Log Analytics Workspace”. We will now connect it to the VM. Click on your workspace, “law-honeypot1”
3. On the left-hand side, scroll down and click on “Virtual machines”
4. Graphical user interface, application, Word

   Description automatically generatedClick on the VM, “honeypot1-vm”
5. Click on “Connect”Graphical user interface, application, Word

   Description automatically generated
6. After its finished it should look like the following:

Graphical user interface, application, Word

Description automatically generated

1. **Setup Azure Sentinel**

This is our SIEM we will use to visualize the attack data

1. Search for and select “Microsoft Sentinel” in the Search bar
2. Graphical user interface, application

   Description automatically generatedClick on “Create” and select the log analytics workspace we created, “law-honeypot1”
3. **Log into VM with Remote Desktop**
4. Search for and select “Virtual machines” in the Search bar. Select the VM, “[honeypot1-vm](https://portal.azure.com/#@daviddiciocogmail.onmicrosoft.com/resource/subscriptions/c8bc1057-a16b-47a5-968e-847f30a95405/resourceGroups/honeypot1-vm_group/providers/Microsoft.Compute/virtualMachines/honeypot1-vm)”
5. Copy the “Public IP address”

Graphical user interface, text, application, email

Description automatically generated

1. Click your Start Menu and type and open “Remote Desktop Connection”. Input the IP address in the “Computer” field and click on “Connect”
2. Type in an incorrect username and password and click “OK”. We want to first log a failed login attempt in the “Event Viewer”. Next, type in the correct username (davidadmin) and password (Password123!) you previously created

A screenshot of a computer

Description automatically generated

1. Accept the certification warning. The VM will now begin to open
2. Toggle off all the Privacy settings and click on “Accept”
3. Click on “Microsoft Edge” and complete setting it up
4. Click on the Start Menu in the VM and type and select “Event Viewer”
5. Navigate to “Windows Logs” -> “Security”. These are all the security events on this VM. We will be focusing on Event ID: 4625

We will be gathering all login failures that try to login to the VM. Doubling click this record will display Network info regarding what Workstation and its Source Network Address that tried logging in. With the Source Network Addresses/IP addresses, we can determine the location of the users attempting to log in. Programmatically we will use an API geolocation (<https://ipgeolocation.io/>) which will return location information back to us. Using this info, will then create our own custom log and send it to our log analytics workspace in Azure and use Sentinel to read the longitude and latitude to plot them out to a map.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

1. **Turn off Windows Firewall on the VM**
2. Next, we will turn off the firewall off on the VM so it can respond to ICMP echo requests so people can discover it on the internet faster. In the VM’s start menu, type in and select “wf.msc”
3. Click on “Windows Defender Firewall Properties”.

* On the “Domain Profile” tab, set “Firewall state” to “Off”
* On the “Private Profile” tab, set “Firewall state” to “Off”
* On the “Public Profile” tab, set “Firewall state” to “Off”

Click on “Apply” and “OK”

1. Close “wf.msc” application and the “Event Viewer”
2. On “Microsoft Edge” open this link, <https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1>, and download the PowerShell script
3. Graphical user interface, application

   Description automatically generatedIn the VM’s start menu, type in and select “Windows Powershell ISE”. On the top left, click on “New Script” and paste the script. Save it on the Desktop with the name, “Log\_Exporter”
4. Navigate to: <https://ipgeolocation.io/> , and create a new account. Once that is completed retrieve the API\_KEY and replace with the one in the script
5. In, “Windows Powershell ISE”, click on the “Run” button. Essentially, the custom script will continuously keeps checking the “Event Viewer” Security logs, checks who failed to log in, and gets their IP address and creates a new log file

Graphical user interface, application

Description automatically generatedThe purple records below indicate failed log ins from the “Event Viewer”. It will then send the IP addresses to the Geolocation API and creates a “failed\_rdp” file in “C:\ProgramData\”

1. **Create custom log in Log Analytics Workspace to bring in our custom log with geodata**
2. In Azure, search for and select “Log Analytics Workspace” in the Search bar. Select the workspace, “law-honeypot1”
3. Click on “Custom Logs” and click on “Add custom logs”
4. Go back to the VM and under “C:\ProgramData\” copy the contents of the “failed\_rdp” file. In your local computer, open “Notepad” and paste the contents. Save it to your “Desktop” and name it, “failed\_rdp.log” (Save type as “All Files”)
5. In Azure, upload “failed\_rdp.log”. This will be used to train Log Analytics on what to look for in the log file
6. Click on “Next” and on “Record delimiter” click on “Next”
7. Graphical user interface, application, Word

   Description automatically generatedOn “Collection Paths”, select type “Windows” and input “C:\ProgramData\failed\_rdp.log”. Click on “Next”
8. On “Details”, input “FAILED\_RDP\_GEO” in the “Custom log name” field. Click on “Next”
9. Click on “Create”
10. It will take a while for the log analytics workspace and the VM to sync up and bring the logs in (15-30 min). To verify the sync is complete, click on “Logs”, close the “Query” pop-up and type in “FAILED\_RDP\_WITH\_GEO\_CL” (remove any additional characters after it). Click on the “Run” button. If logs are displayed, the sync is complete

Graphical user interface, text, application, email

Description automatically generated

The “RawData” column contains a whole line from the “failed\_rdp” file in the VM. Next we will extract fields from the “Raw Data” column so we can create their own field (Ex. Fields for latitude, longitude, etc.)

1. **Create custom fields/extract fields from RawData custom log**
2. Expand one of the logs and click on “Extract fields from ….”

Graphical user interface, text, application, email

Description automatically generated

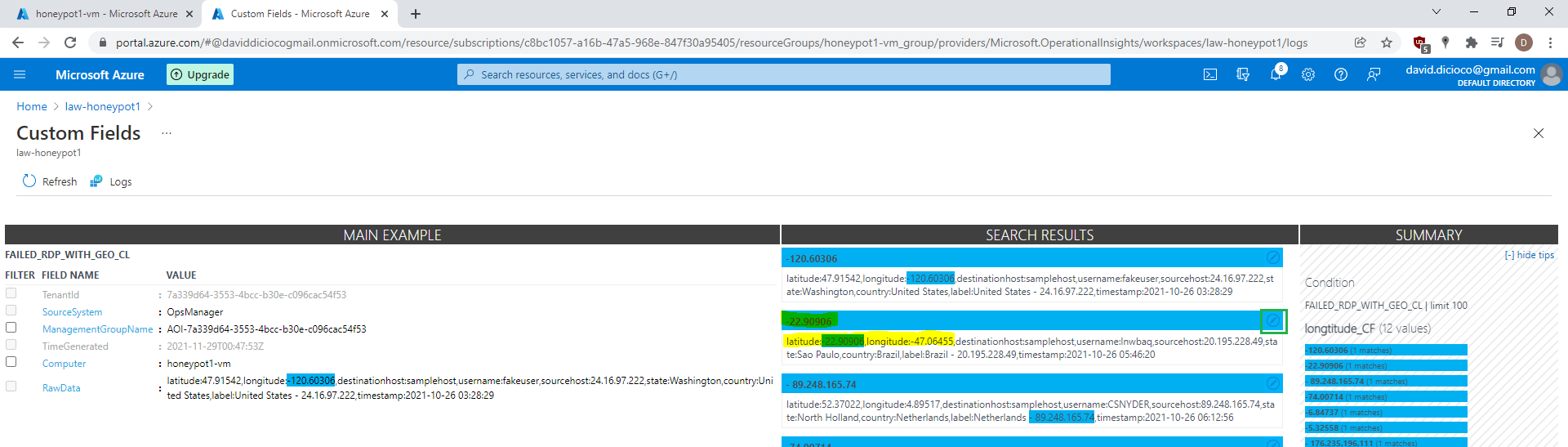
1. Graphical user interface, text, application

   Description automatically generatedHighlight the value of “Latitude”. In “Field Title”, input, “latitude1”, and for “Field Type” select “Numeric”
2. Under “Search Results”, verify all the latitude fields are getting its latitude values. If so, click on the “Save Extraction” button

Graphical user interface, text, application, email

Description automatically generated

The sample data allows us to train the extract process.

1. On the same log and click on “Extract fields from ….” and do the same for longitude. If there are any highlight issues like the one below:

Click on the “Edit” button and click “Modify this highlight”. Highlight the correct value and click “Extract”. Do that for every record that is highlighting an incorrect value.

Once all records under “Search Results” are verified, click on the “Save Extraction” button

1. Repeat the process for every field in “RawData”. Input/Select the following for each fields  
     
   destinationhost

Field Title: destinationhost

Field Type: Text

username

Field Title: destinationhost

Field Type: Text

sourcehost

Field Title: sourcehost

Field Type: Text

state

Field Title: state

Field Type: Text

country

Field Title: country

Field Type: Text

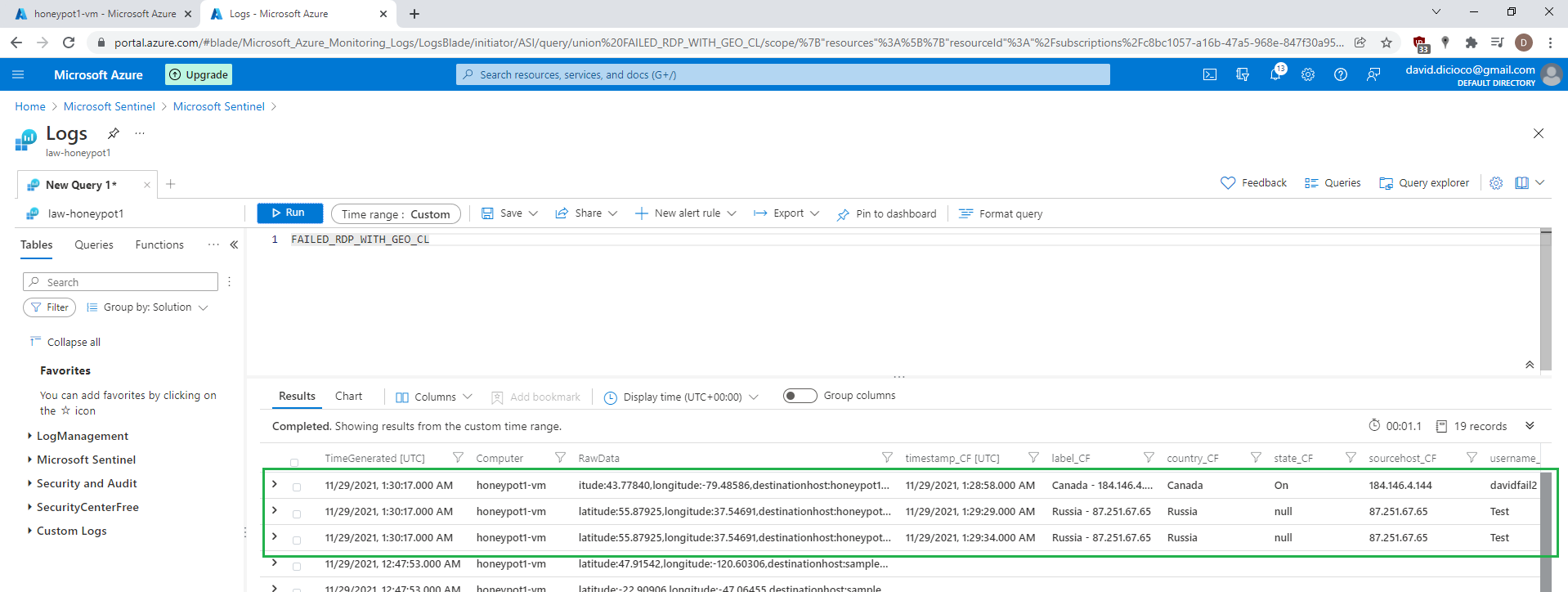
label

Field Title: label

Field Type: Text

timestamp  
Field Title: timestamp  
Field Type: Date/Time

The sample records you have, the more accurate the extract process will be.

1. To verify the logs are parsed out correctly, you can do another failed login attempt on your local computer. Running the query again shows the logs are parsed out correctly
2. **Setup a Map in Sentinel (using Latitude and Longitude)**

We will now setup a map within Sentinel which is currently linked to FAILED\_RDP\_WITH\_GEO\_CL

1. In Azure, search for and select “Microsoft Sentinel” in the Search bar. Select the workspace, “law-honeypot1”
2. Click on “Workbooks” and click on “Add workbook”
3. Click on “Edit” and remove the two default widgets
4. Click on “Add” -> “Add query”. Paste the following query:

FAILED\_RDP\_WITH\_GEO\_CL | summarize event\_count=count() by sourcehost\_CF, latitude\_CF, longitude\_CF, country\_CF, label\_CF, destinationhost\_CF

| where destinationhost\_CF != "samplehost"

| where sourcehost\_CF != ""

1. Set “Visualization” to “Map”, and “Map Size” to “Full”
2. In the “Map Settings” set the fields to the following:

“Latitude”: latitude\_CF

“Longitude”: longitude\_CF  
“Size by”: event\_count  
“Metric Label”: label\_CF

1. Click on “Done Editing”. Set “Auto refresh” to “5 minutes”
2. **Waiting for attacks from the internet**

By waiting for a couple hours (12-24), the map with automatically refresh every 5 minutes and display when a user from the internet tried and failed to log in.

In this example, I ran it overnight and the map displayed the following:

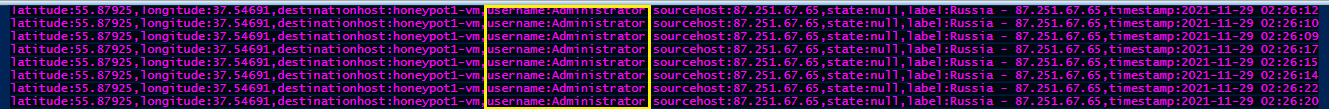
Map

Description automatically generated with medium confidence

Substantial amounts of activity were logged for both Vietnam (5000+) and the United States (1000+)

**IMPORTANT NOTE:** Delete the resource group in Azure once you have completed this tutorial! Otherwise, they will consume your free $200 Azure credit and potentially cost money if the 30 days from your free trial is expired

**Final Thoughts**

By going through this tutorial its evident that as soon as anything is put up on the internet (for this example -> an open VM), people from around the world will attempt to access it. You become a target of opportunity if anything is open. Secondly, by going through the logs of the VM, it was clear that you should avoid using the username of “Administrator”. The username was found to be one of the most guessed. By disabling common usernames, you can avoid this risk. Password strength was also found to be important considering the large amount of log in attempts made overnight (less than 24 hours). By having a strong password, it adds another layer of defence