

# HONEYPOTLAB

Craig Kovalcheck


## OBJECTIVE

- My objective for this homelab was to gain practical experience and develop a greater insight into Microsoft Sentinel, and Azure as a whole.
- I utilized Josh Madakor's Azure Sentinel Tutorial which I found on Youtube.
- I spun up a VM, made it intentionally vulnerable, fed logs through an IP geolocation API and use the data to generate a heat map with latitude/longitude coordinates on Microsoft Sentinel.






# CREATING THE VM

- Using Microsoft Azure I deployed a Windows 10 VM which I labeled as “honeypot-vm”.
- On Azure I created a firewall rule labeled “DANGER\_ANY\_IN” set to allow everything (“\*”) through, to open honeypot-vm to the Internet.
- This is meant to make honeypot-vm easier for attackers to find.

Deployment is in progress

Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows... Start time: 12/31/2022, 11:21:28 AM  
Subscription: [Azure subscription 1](#) Correlation ID: c542ef23-d0cf-405e-8d3e-ca30cf5244b   
Resource group: [honeypotlab](#)

Deployment details

Resource	Type	Status
 honeypot-vm	Microsoft.Compute/virtualMachines	Created
 <a href="#">honeypot-vm333_z1</a>	Microsoft.Network/networkInterfaces	Created
 <a href="#">honeypotlab-vnet</a>	Microsoft.Network/virtualNetworks	OK
 <a href="#">honeypot-vm-nsg</a>	Microsoft.Network/networkSecurityGroups	OK
 <a href="#">honeypot-vm-ip</a>	Microsoft.Network/publicIpAddresses	OK


## VM CON'T

- Went ahead and disabled the firewall completely in the domain, private, and public profiles.
- I pinged honeypot-vm to verify the firewalls were off and an attacker would be able to ping the machine.




# LOGGING

- I created a Log Analytics Workspace (law-honeypot) in Azure to allow the ingestion of the Windows Event logs from the vulnerable VM.
- This will also allow me to display the events on a heatmap later on by using a custom log with the geodata in it, which Sentinel will use for the heatmap.

**Log Analytics workspace**  
by Microsoft

Basics	
Subscription	Azure subscription 1
Resource group	honeypotlab
Name	law-honeypot
Region	East US

**No log analytics workspaces to display**  
Try changing or clearing your filters.  
[Create log analytics workspace](#)

# LOGGING CON'T

- Enable Defender for law-honeypot and enable data collection for all events.
- Then connect our law-honeypot to our honeypot-vm.

The screenshot shows the Azure Log Analytics workspace interface for 'law-honeypot | Virtual machines'. The left sidebar contains navigation links: Overview, Activity log, and Access control (IAM). The main area displays a table of virtual machines with a search bar, a refresh button, and a filter input. One VM, 'honeypot-vm', is shown with a 'Connecting' status.

Name	Log Analytics Connection
honeypot-vm	Connecting

## CREATING THE SIEM

- I searched for “Microsoft Sentinel” in the search bar, this is the SIEM available for use on Azure.
- I add/connect Sentinel to law-honeypot, where the logs will be located.












### No Microsoft Sentinel to display

See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise.

[Create Microsoft Sentinel](#)

# VM EVENT LOGS





- I opened Event Viewer on honeypot-vm and I focused on the Security Logs looking for “Audit Failure” or “Event ID 4625”.
- These initial events are me failing to login to honeypot-vm through RDP.
- These are the logs that I will gather

Keywords	Date and Time	Source	Event ID	Task Category
 Audit Failure	12/31/2022 5:58:57 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:55:59 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:52:14 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:51:57 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:51:51 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:51:36 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:51:11 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:50:09 PM	Microsoft Windows security auditing.	4625	Logon
 Audit Failure	12/31/2022 5:48:33 PM	Microsoft Windows security auditing.	4625	Logon



# LOG EXPORTER

- I used Josh Madakor's Custom\_Security\_Log\_Exporter script located at <https://github.com/joshmadakor1/Sentinel-Lab>.
- I saved it to the honeypot-vm's Desktop and ran it from Powershell ISE.
- I had to get an API key from <https://ipgeolocation.io> so the script can actually get the lat/long coordinates for the attacker IP address in the Security logs.

 main ▾ Sentinel-Lab / Custom_Security_Log_Exporter.ps1	 API Keys  Add	
 joshmadakor1 Update Custom_Security_Log_Exporter.ps1	99f0282a18564bb6a5b4a3a43e38c924	<pre>1 # Get API key from here: https://ipgeolocation.io/ 2 \$API_KEY      = "d4600b4efdef42b39828f5155041a457" 3 \$LOGFILE_NAME = "failed_rdp.log" 4 \$LOGFILE_PATH = "C:\ProgramData\\${\$LOGFILE_NAME}"</pre>

# RUNNING SCRIPT

- Ran the Log\_Exporter.ps1 script through Powershell ISE and I attempted some failed RDP logins to verify the script was running correctly.
- As long as the script is running it will filter failed RDP events and creates a new log file located at “C:\ProgramData\failed\_rdp.log”
- Failed logins are also displayed in Powershell, seen below.

```
PS C:\Users\craigmin> C:\Users\craigmin\Desktop\Log_Exporter.ps1
```

```
Directory: C:\ProgramData
```

Mode	LastWriteTime	Length	Name
-a----	12/31/2022 8:12 PM	0	failed_rdp.log

```
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:58:57  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:55:59  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigadmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:52:14  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigadmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:51:57  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigadmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:51:51  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:Craigadmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:51:36  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:51:11  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigadmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:50:09  
latitude:38.62775,longitude:-90.19956,destinationhost:honey-pot-vm,username:craigmin,sourcehost:148.72.165.211,state:Missouri,label:United States - 148.72.165.211,timestamp:2022-12-31 17:48:33
```

# CUSTOM LOG

- Created custom log on Log Analytics to collect the log file from honeypot-vm and fed it a sample log from the VM to train Log Analytics what to look for.
- Created custom fields for our custom log.
- Have to create extractions to help further teach the algorithm, as more logs are ingested these extractions may need adjustment.

country_CF	state_CF	sourcehost_CF	username_CF	destinationhost_CF	latitude_CF	longitude_CF
Turkey	Adana	213.238.167.50	ALCADMIN	honeypot-vm	36.976	35.313

## FAILED\_RDP\_WITH\_GEO\_CL

Description

Description

Collection paths

Type	Path
Windows	C:\ProgramData\failed_rdp.log

☐ Custom field name ↑↓

☐ country\_CF

☐ destinationhost\_CF

☐ label\_CF

☐ latitude\_CF

☐ longitude\_CF

☐ sourcehost\_CF

☐ state\_CF

☐ timestamp\_CF

☐ username\_CF

# SENTINEL SIEM

- Created a custom workbook in Sentinel, labeled “Failed RDP”, I did this to be able to generate a heatmap on the Sentinel Dashboard.
- With the FAILED\_RDP\_WITH\_GEO\_CL query I used some of the custom log fields I created earlier as parameters.

Log Analytics workspace Logs 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 != ""
```

Workbook name ↑↓

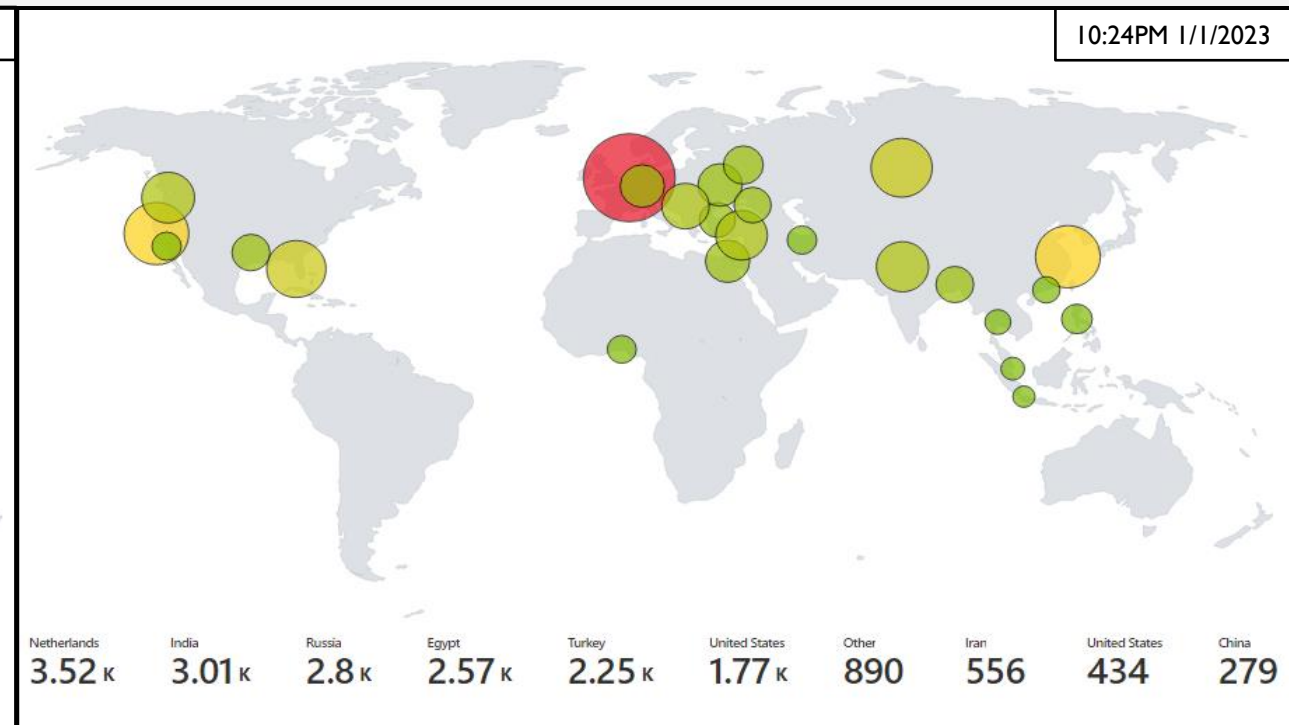
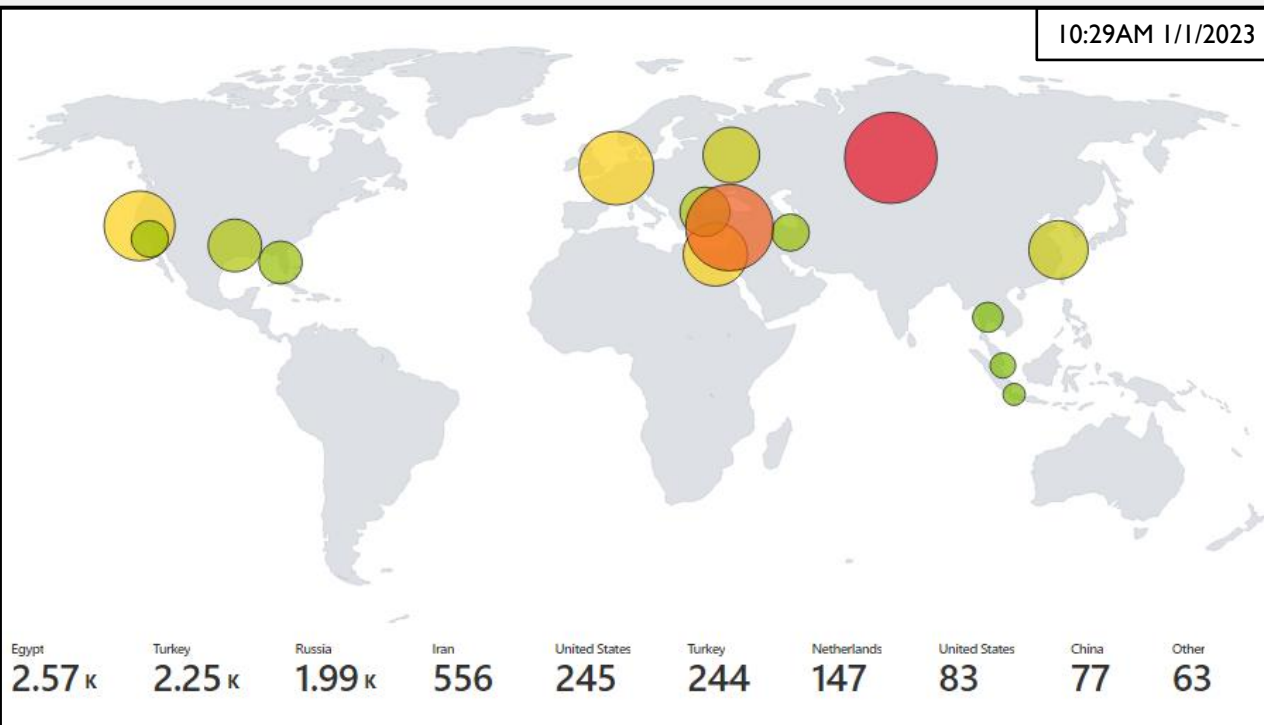


Failed RDP



# HEATMAP

- A large portion of the initial attacks originated from Turkey and Egypt followed by Russia.
- Later we see an increase in attacks from Europe and India. Time Zones?



## TAKEAWAYS

- Do not use default configurations (username/password), attackers tried variations of “admin/administrator”.
- Multifactor Authentication (MFA) could help with this type of attack.
- Got some practical experience using Azure to create a VM, LAW, and SIEM.
- Take more screenshots before deleting your resources.

## TOOLS/SOURCES

- Josh Madakor - <https://www.youtube.com/watch?v=RoZeVbbZ0o0>
- PowerShell Script - [https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom\\_Security\\_Log\\_Exporter.ps1](https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1)
- Microsoft Azure - <https://azure.microsoft.com/en-us/>
- IP Geolocation API <https://ipgeolocation.io/>