

Lab #5: Setup of SIEM & Log Repository

Purpose:

- We'll be setting up our SIEM (Microsoft Sentinel) and central log repository (Log Analytics workspace).
- In our SIEM we'll be creating a watch list that has network blocks with corresponding geo-locations.
- The 3 main sources of logs in Azure: (1) Entra ID logs, (2) Activity logs, (3) Resource logs
 1. **Entra ID logs** → tenant-level logs (e.g., sign-in logs, audit logs). These logs contain a history of sign-in activity and an audit trail of changes made in Entra ID for a given tenant.
 2. **Activity logs** → determined the what, who, and when for any 'write' operation within a given subscription.
 3. **Resource logs** → provide insight into the operations performed from within a given Azure resource.
- Our generated logs will ultimately be captured and aggregated.

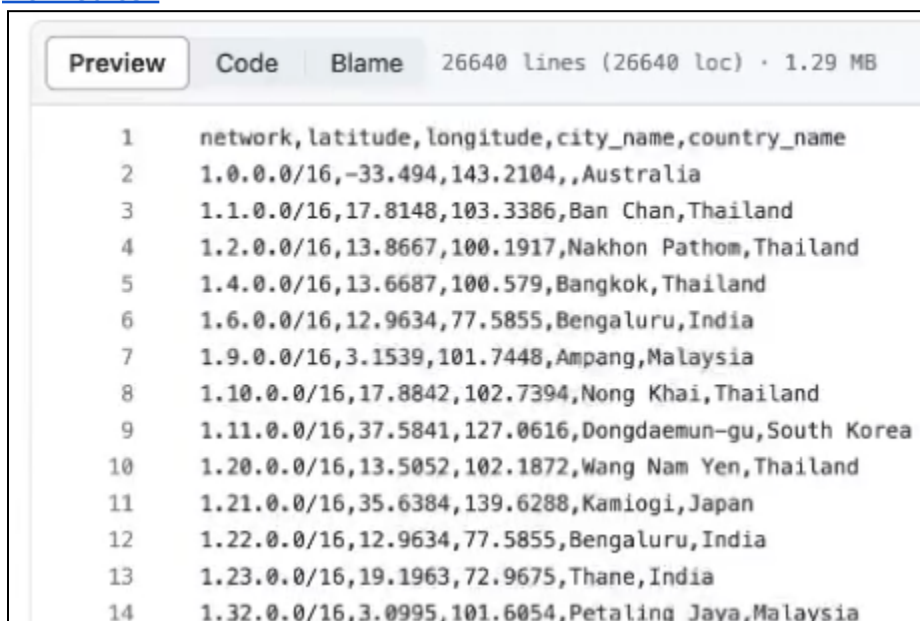
Tasks:

1. Put Large Geo-Data Files in Azure Storage
2. Set up a central log repository (Log Analytics)
3. Set up a SIEM (Microsoft Sentinel)
4. Create the GeolP watchlist (Microsoft Sentinel)
5. Query the watchlist (Log Analytics)

Task 1: Put Large Geo-Data Files in Azure Storage

Note: This will include a long list of network blocks (with associated city and country names). This will be used to derive geolocations of attackers when we inspect logs.

1. Open and download this CSV file to your local PC:
[https://github.com/erichmair/Azure-SOC-Honeynet-Project/blob/main/Sentinel-Maps\(JSON\)/geoip-summarized.csv](https://github.com/erichmair/Azure-SOC-Honeynet-Project/blob/main/Sentinel-Maps(JSON)/geoip-summarized.csv)

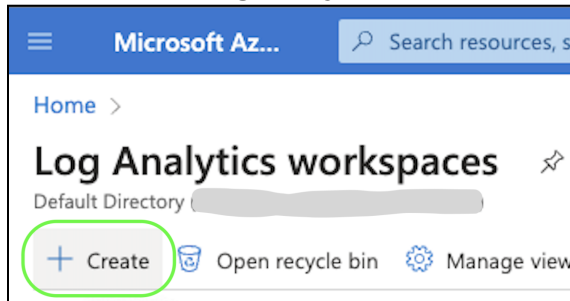


```
Preview Code Blame 26640 lines (26640 loc) · 1.29 MB
1 network, latitude, longitude, city_name, country_name
2 1.0.0.0/16, -33.494, 143.2104, , Australia
3 1.1.0.0/16, 17.8148, 103.3386, Ban Chan, Thailand
4 1.2.0.0/16, 13.8667, 100.1917, Nakhon Pathom, Thailand
5 1.4.0.0/16, 13.6687, 100.579, Bangkok, Thailand
6 1.6.0.0/16, 12.9634, 77.5855, Bengaluru, India
7 1.9.0.0/16, 3.1539, 101.7448, Ampang, Malaysia
8 1.10.0.0/16, 17.8842, 102.7394, Nong Khai, Thailand
9 1.11.0.0/16, 37.5841, 127.0616, Dongdaemun-gu, South Korea
10 1.20.0.0/16, 13.5052, 102.1872, Wang Nam Yen, Thailand
11 1.21.0.0/16, 35.6384, 139.6288, Kamiogi, Japan
12 1.22.0.0/16, 12.9634, 77.5855, Bengaluru, India
13 1.23.0.0/16, 19.1963, 72.9675, Thane, India
14 1.32.0.0/16, 3.0995, 101.6054, Petaling Jaya, Malaysia
```

2. (We'll come back to this geo-data file in **Task 4**)

Task 2: Set up a central log repository (Log Analytics)

1. Azure portal > Log Analytics workspaces > Create log analytics workspace



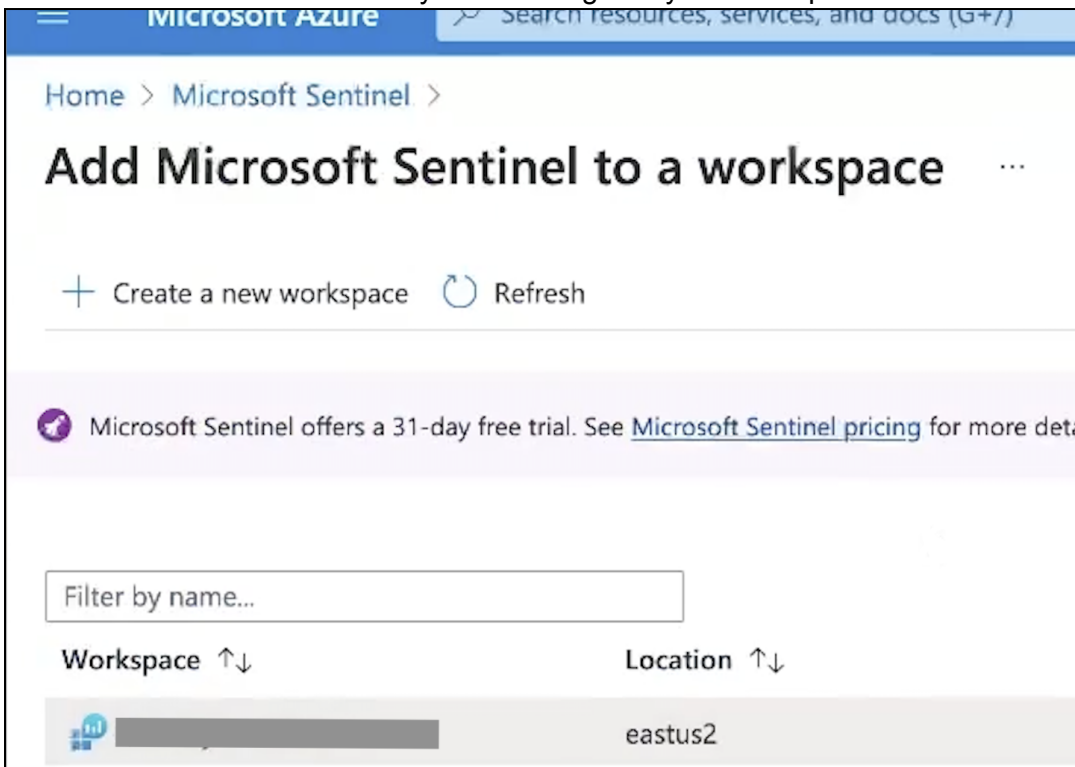
- a. **Resource group:** (same resource group as “Tester” VMs)
- b. **Name:** LAW-Cyber-Lab-01
- c. **Region:** East US 2 (same region as “Tester” VMs)
- d. Select **Review and Create** > select **Create**.

Note: In future labs, we'll connect the “tester” VMs to our Log Analytics workspace so logs will be sent to it.

Task 3: Set up a SIEM (Microsoft Sentinel)

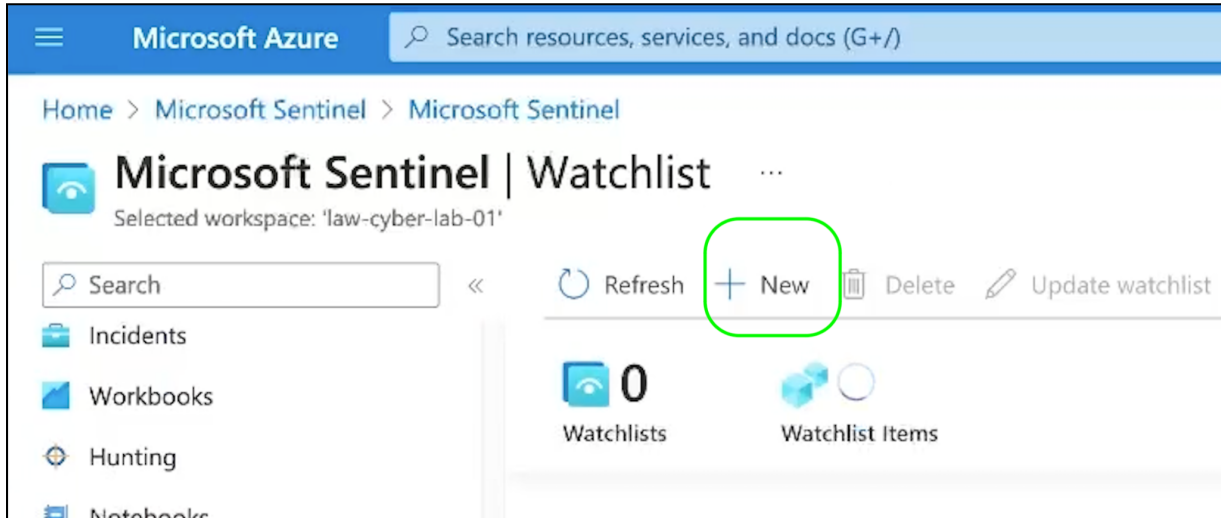
Note: We'll be setting up Microsoft Sentinel and connecting it to our Log Analytics workspace.

1. Azure portal > Microsoft Sentinel > Create Microsoft Sentinel
 - a. Select our recently-created Log Analytics workspace. Done.



Task 4: Create the GeoIP watchlist (Microsoft Sentinel)

1. **Azure** portal > **Microsoft Sentinel** > select our new Sentinel instance > **Watchlist**.
2. Select **+NEW** to create a new watchlist.

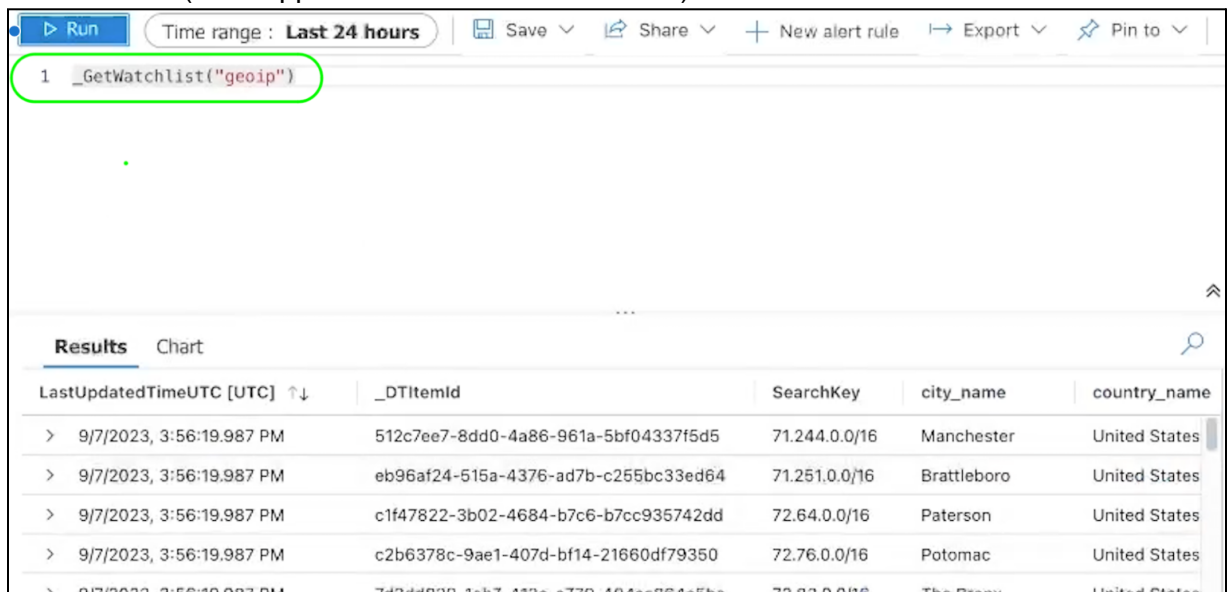


- a. **General tab:** **The Name and Alias should be the same name.**
- b. **Source tab:**
 - i. **Source type** is "Local file", **File type** is "CSV", **Number of lines before row** is "0", uploaded the CSV file (saved to your local Desktop folder), **SearchKey** is "network".
- c. Select **Review and Create** > select **Create**.

Note: This process may take 30-60 min. Let's skip to the next task for now.

Task 5: Query the watchlist (Log Analytics)

1. **Azure** portal > **Log Analytics workspaces** > our workspace > select **Logs**
2. Query the watchlist using this command: **GetWatchlist("geoup")**
 - a. Select **Run** > (rows appeared below under "Results").



End:

- We created a central log repository, created a SIEM instance, and connected them both. We also ingested the GeoIP watchlist into our Sentinel watchlist.