Lab #15: **Expose Environment to Malicious Traffic #1 (‘Before’ Hardening)**

Purpose:

- We’ll expose our lab environment to malicious traffic for 24 hours. We’ll then analyze all of the alerts/etc that were generated during that period.

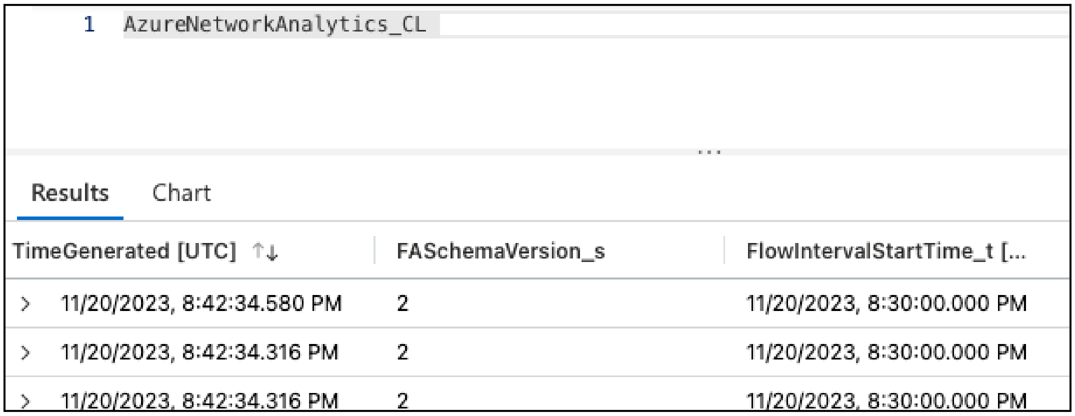
Tasks:

1. **Perform pre-lab steps**
   - Ensure that queries are returning results
   - Power on both “Tester” VMs (leave on for 24 hours)
2. **Analyze the environment ‘Before’ hardening**
   - Obtain the ‘Before’ results
     - Start and End time; Security Events (Windows VMs); Syslog (Linux VMs); SecurityAlert (Microsoft Defender for Cloud); Security Incident (Sentinel Incidents); NSG Inbound Malicious Flows Allowed.
   - Analyze the ‘Before’ attack maps
     - Mssql-auth-fail; Nsg-malicious-allowed-in; Linux-ssh-auth-fail; Windows-rdp-smb-auth-fail.

Task 1: **Perform pre-lab steps**

Ensure that queries are returning results:

1. Azure **portal** > **Log Analytics workspace** > (select workspace) > **Logs** > **New Query**
2. Run each query separately:
   a. **SecurityEvent**, **Syslog**, **SecurityAlert**, **SecurityIncident**, **AzureNetworkAnalytics_CL**



```
AzureNetworkAnalytics_CL
```

TimeGenerated [UTC]	FASchemaVersion_s	FlowIntervalStartTime_t [...
11/20/2023, 8:42:34.580 PM	2	11/20/2023, 8:30:00.000 PM
11/20/2023, 8:42:34.316 PM	2	11/20/2023, 8:30:00.000 PM
11/20/2023, 8:42:34.316 PM	2	11/20/2023, 8:30:00.000 PM

> ***Note**: We want to ensure that these queries return results before we begin this lab. These results will be how we’ll measure our metrics.*

Power on both “Tester” VMs (leave on for 24 hours):

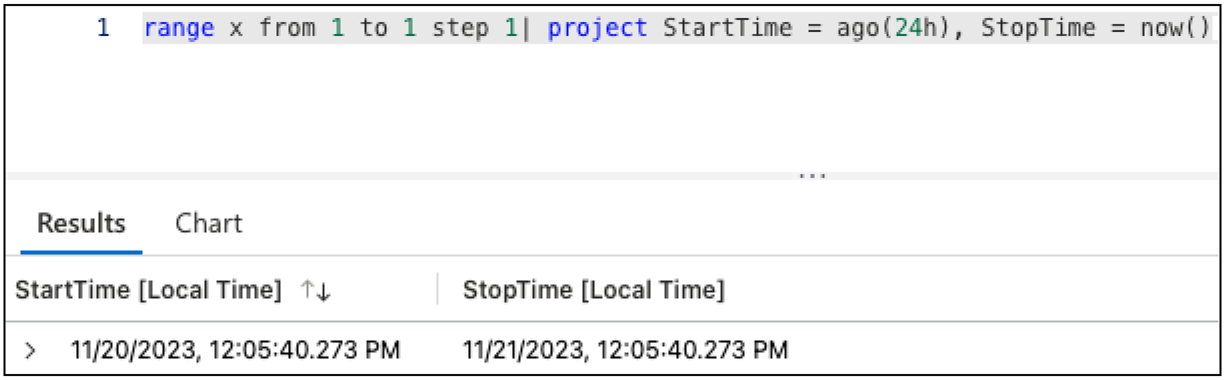
1. **Azure portal** > **Virtual Machines** > power on both “Tester” VMs (windows-vm, linux-vm).
2. Leave these VMs on for 24 hours.

Task 2: Analyze the environment ‘Before’ hardening

Results (‘Before’)	
Start Time:	11/20/2023, 12:05:40 PM
Stop Time:	11/21/2023, 12:05:40 PM
Security Events (Windows VMs):	22540
Syslog (Linux VMs):	998
SecurityAlert (Microsoft Defender for Cloud):	7
SecurityIncident (Sentinel Incidents):	152
NSG Inbound Malicious Flows Allowed:	2385

Obtain the ‘Before’ security events:

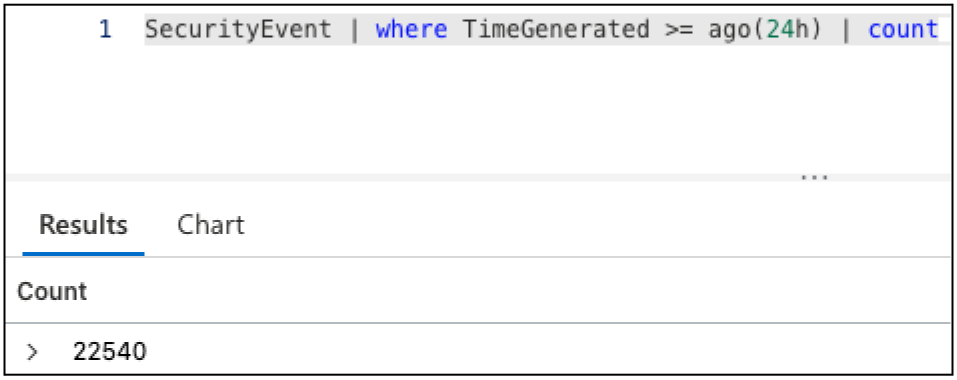
1. Start and End time → ran this query:
   range x from 1 to 1 step 1| project StartTime = ago(24h), StopTime = now()



```
range x from 1 to 1 step 1| project StartTime = ago(24h), StopTime = now()
```

StartTime [Local Time] ↑↓	StopTime [Local Time]
› 11/20/2023, 12:05:40.273 PM	11/21/2023, 12:05:40.273 PM

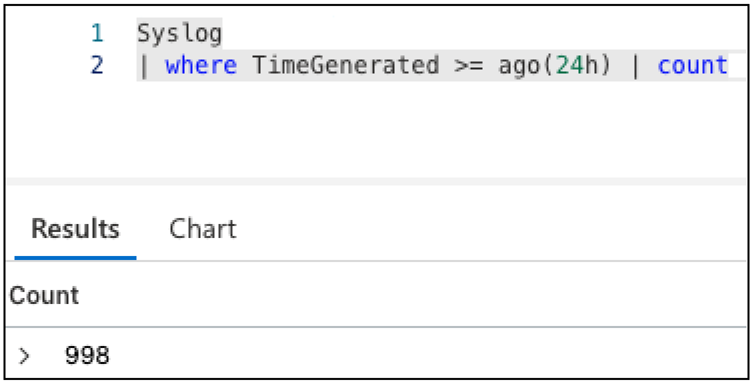
2. Security Events (Windows VMs) → ran this query:
   SecurityEvent | where TimeGenerated >= ago(24h) | count



```
SecurityEvent | where TimeGenerated >= ago(24h) | count
```

Count
› 22540

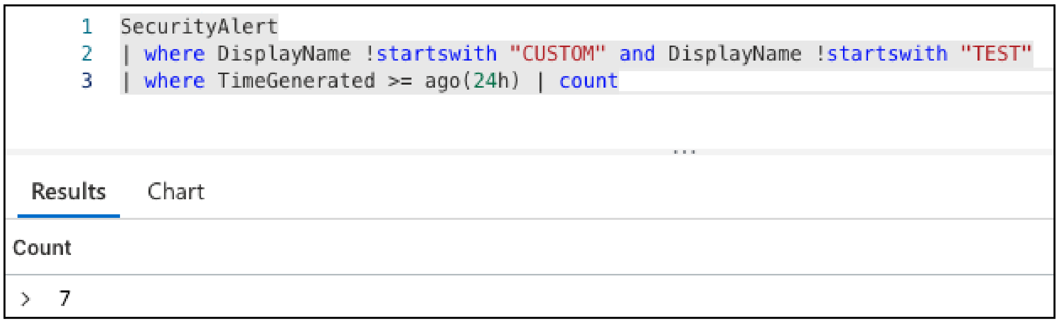
3. Syslog (Linux VMs) → ran this query:
Syslog | where TimeGenerated >= ago(24h) | count



```
Syslog
| where TimeGenerated >= ago(24h) | count
```

```
Count
> 998
```

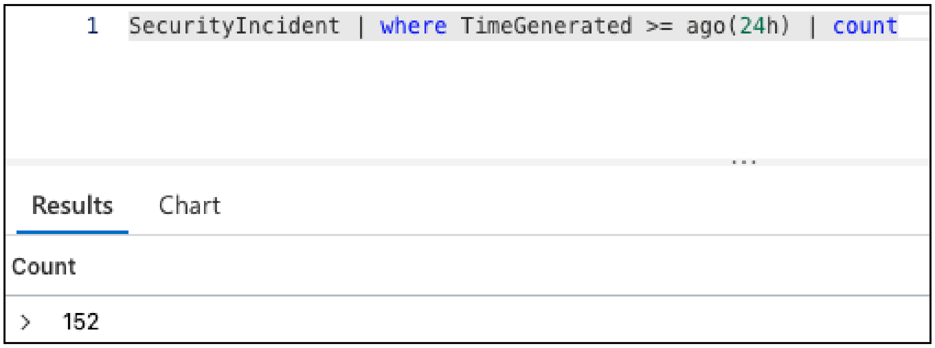
4. SecurityAlert (Microsoft Defender for Cloud) → ran this query:
SecurityAlert | where DisplayName !startswith "CUSTOM" and DisplayName !startswith "TEST" | where TimeGenerated >= ago(24h) | count



```
SecurityAlert
| where DisplayName !startswith "CUSTOM" and DisplayName !startswith "TEST"
| where TimeGenerated >= ago(24h) | count
```

```
Count
> 7
```

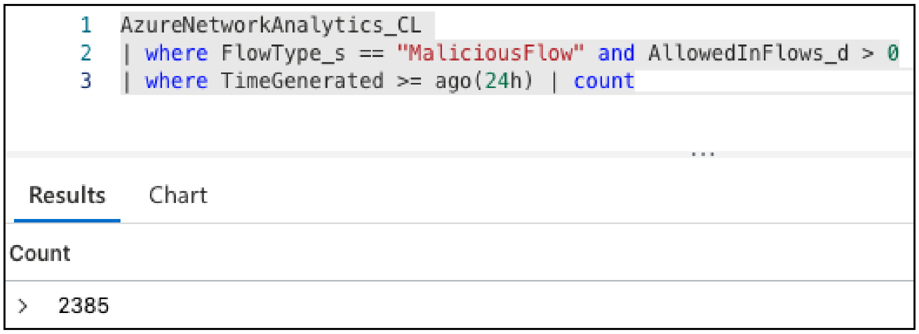
5. Security Incident (Sentinel Incidents) → ran this query:
SecurityIncident | where TimeGenerated >= ago(24h) | count



```
SecurityIncident | where TimeGenerated >= ago(24h) | count
```

```
Count
> 152
```

6. NSG Inbound Malicious Flows Allowed → ran this query:
AzureNetworkAnalytics_CL | where FlowType_s == "MaliciousFlow" and AllowedInFlows_d > 0 | where TimeGenerated >= ago(24h) | count

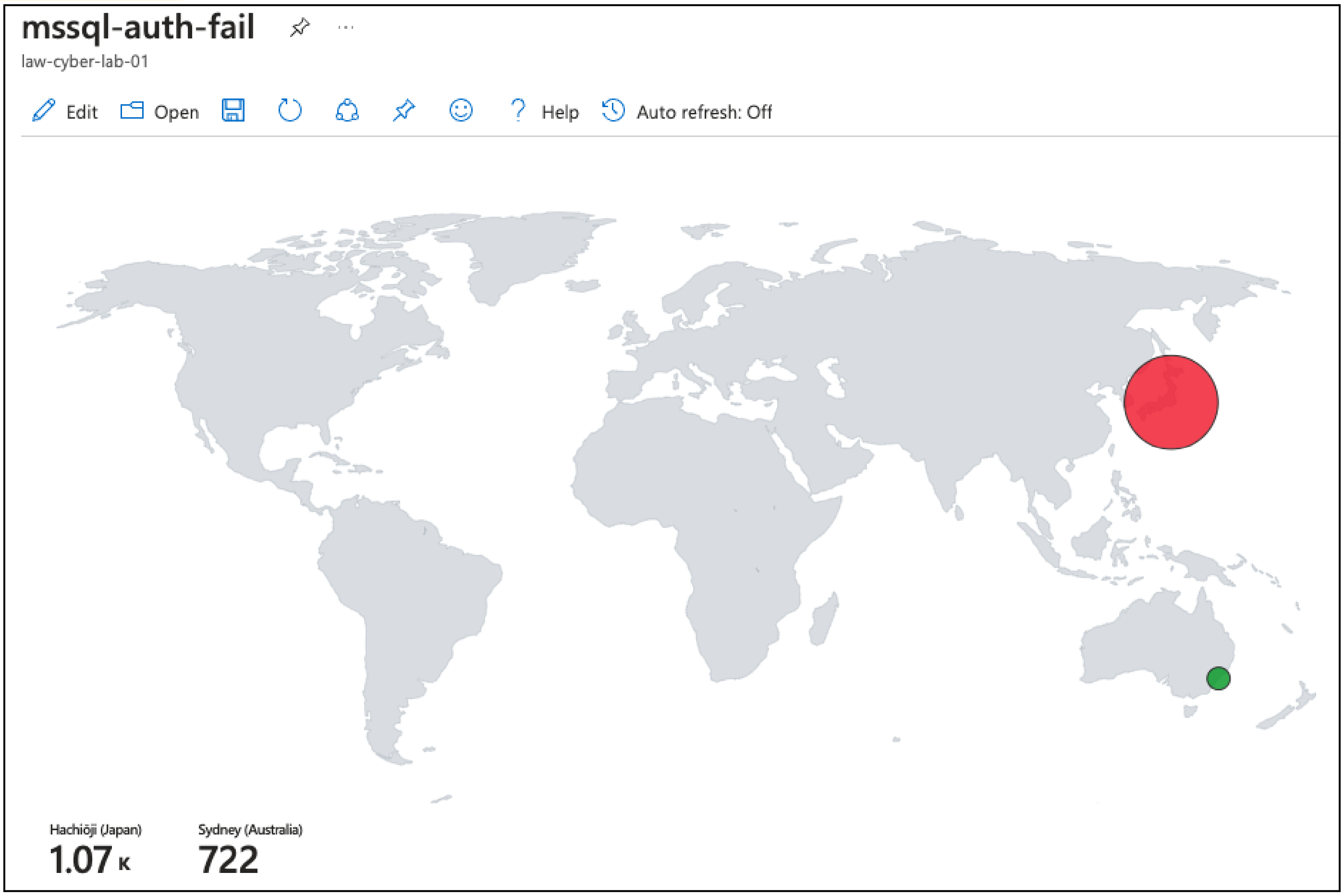


```
AzureNetworkAnalytics_CL
| where FlowType_s == "MaliciousFlow" and AllowedInFlows_d > 0
| where TimeGenerated >= ago(24h) | count
```

```
Count
> 2385
```

Analyze the ‘Before’ attack maps:

1. **Azure** portal > **Sentinel** > **Workbooks** > **My Workbooks**.
2. Mssql-auth-fail:

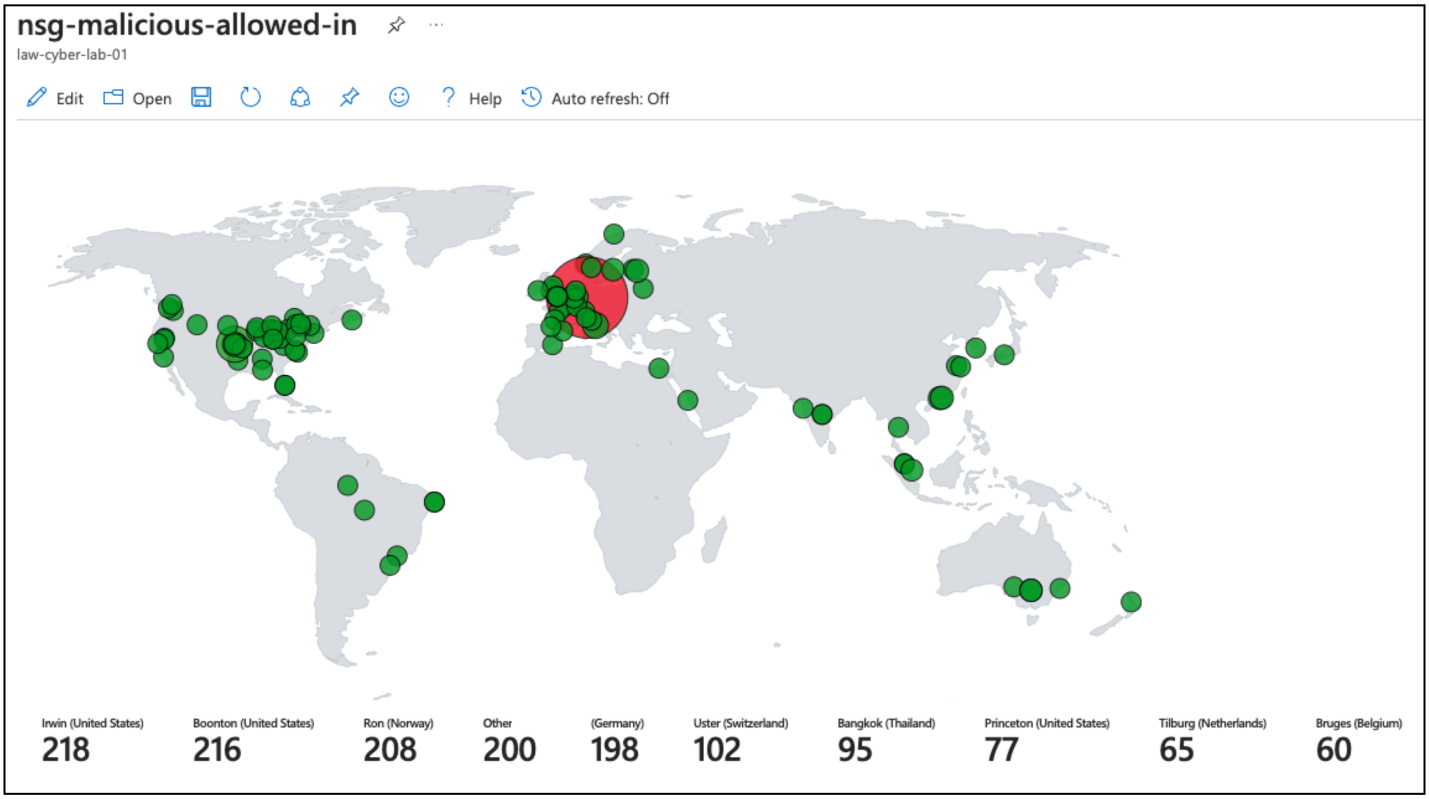


mssql-auth-fail

law-cyber-lab-01

Hachiōji (Japan)	Sydney (Australia)
1.07 K	722

3. Nsg-malicious-allowed-in:

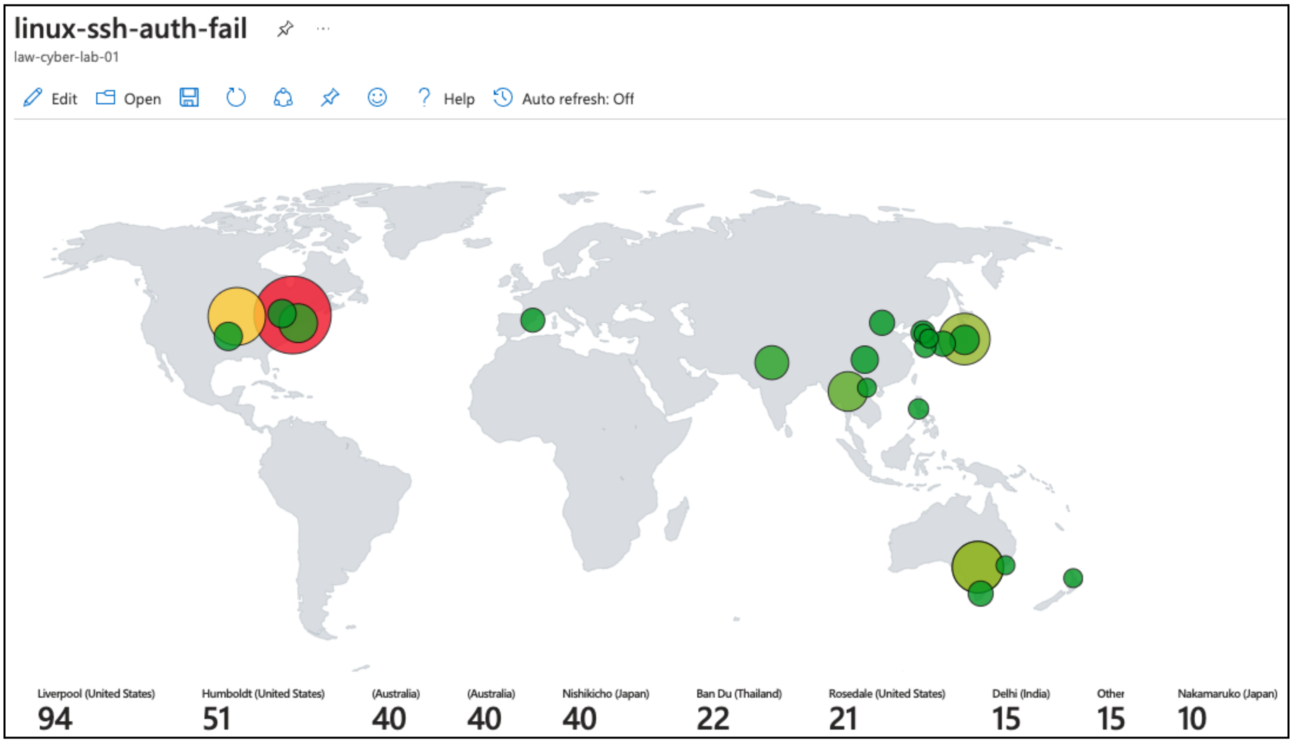


nsg-malicious-allowed-in

law-cyber-lab-01

Irwin (United States)	Boonton (United States)	Ron (Norway)	Other	(Germany)	Uster (Switzerland)	Bangkok (Thailand)	Princeton (United States)	Tilburg (Netherlands)	Bruges (Belgium)
218	216	208	200	198	102	95	77	65	60

4. Linux-ssh-auth-fail:

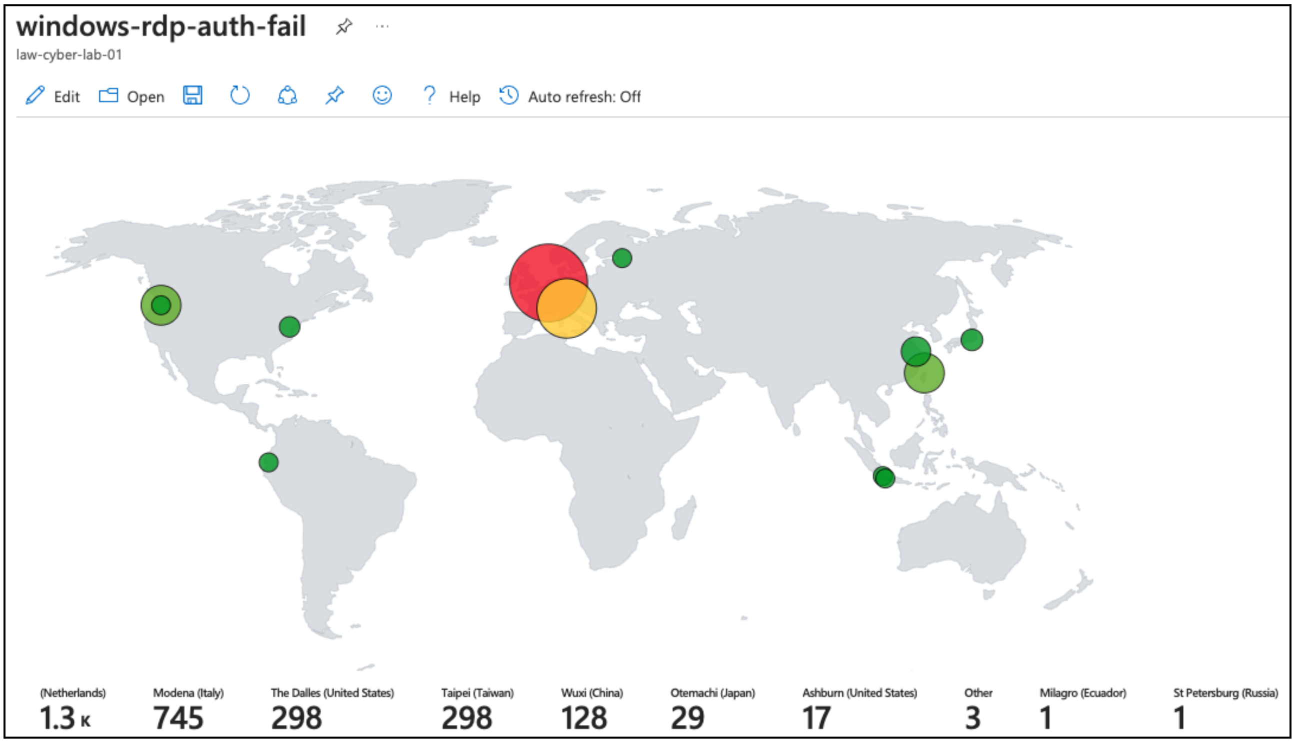


linux-ssh-auth-fail

law-cyber-lab-01

Liverpool (United States)	Humboldt (United States)	(Australia)	(Australia)	Nishikicho (Japan)	Ban Du (Thailand)	Rosedale (United States)	Delhi (India)	Other	Nakamaruko (Japan)
94	51	40	40	40	22	21	15	15	10

5. Windows-rdp-smb-auth-fail:



windows-rdp-auth-fail

law-cyber-lab-01

(Netherlands)	Modena (Italy)	The Dalles (United States)	Taipei (Taiwan)	Wuxi (China)	Otemachi (Japan)	Ashburn (United States)	Other	Milagro (Ecuador)	St Petersburg (Russia)
1.3 K	745	298	298	128	29	17	3	1	1

End:

- We've left our lab environment exposed for 24 hours and then analyzed the results that were generated. In the next lab we'll investigate the incidents and start performing steps to secure our environment.
- We'll ultimately expose our lab environment again for 24 hours 'After' remediating vulnerabilities. We'll then compare the 'Before' and 'After' results.