Lab #19: **Expose Environment to Malicious Traffic #2 ('Before' Hardening)**

Purpose:

- We'll expose our lab environment [again] to malicious traffic for 24 hours. We'll then analyze all of the alerts/etc that were generated during that period.
- But this time, we'll expect fewer incidents because of our recent hardening steps:
  - Hardened the NSGs by removing the rule that allowed any inbound traffic to our VMs.
  - We've enabled the NIST SP 800-53 option to the Regulatory Compliance section of Microsoft Defender for Cloud, allowing us to view the recommended security controls. This included implementing the "Boundary Protection" controls of 800-53 (SC-7).

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 'After' hardening**
   - Obtain the 'After' 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 'After' 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**

```
1  AzureNetworkAnalytics_CL
```

Results Chart

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 (‘After’)	
Start Time:	11/25/2023, 10:41:17 AM
Stop Time:	11/25/2023, 10:41:17 PM
Security Events (Windows VMs):	9061
Syslog (Linux VMs):	1
SecurityAlert (Microsoft Defender for Cloud):	0
SecurityIncident (Sentinel Incidents):	0
NSG Inbound Malicious Flows Allowed:	0

Obtain the ‘After’ 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()
```

Results Chart

StartTime [Local Time]	StopTime [Local Time]
11/25/2023, 10:41:17.795 AM	11/26/2023, 10:41:17.795 AM

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

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

Results Chart

Count
9061

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

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

Results Chart

Count
1

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

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

Results Chart

Count
0

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

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

Results Chart

Count
0

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

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

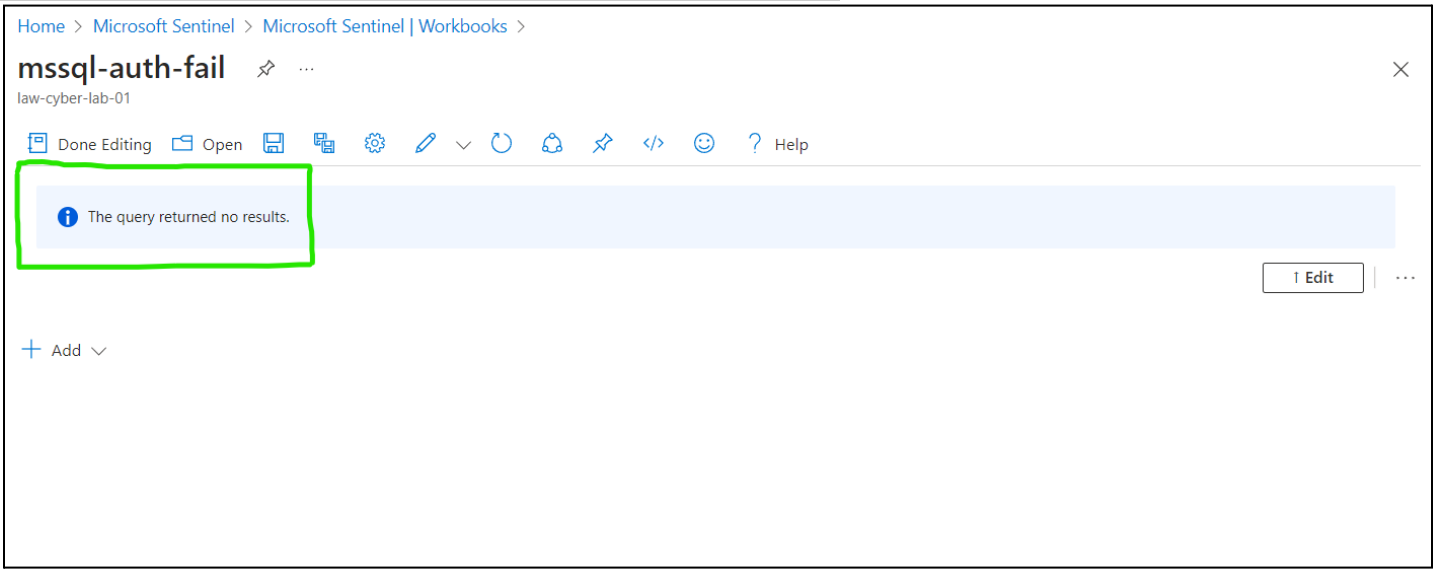
Results Chart

Count
0

Analyze the 'After' attack maps:

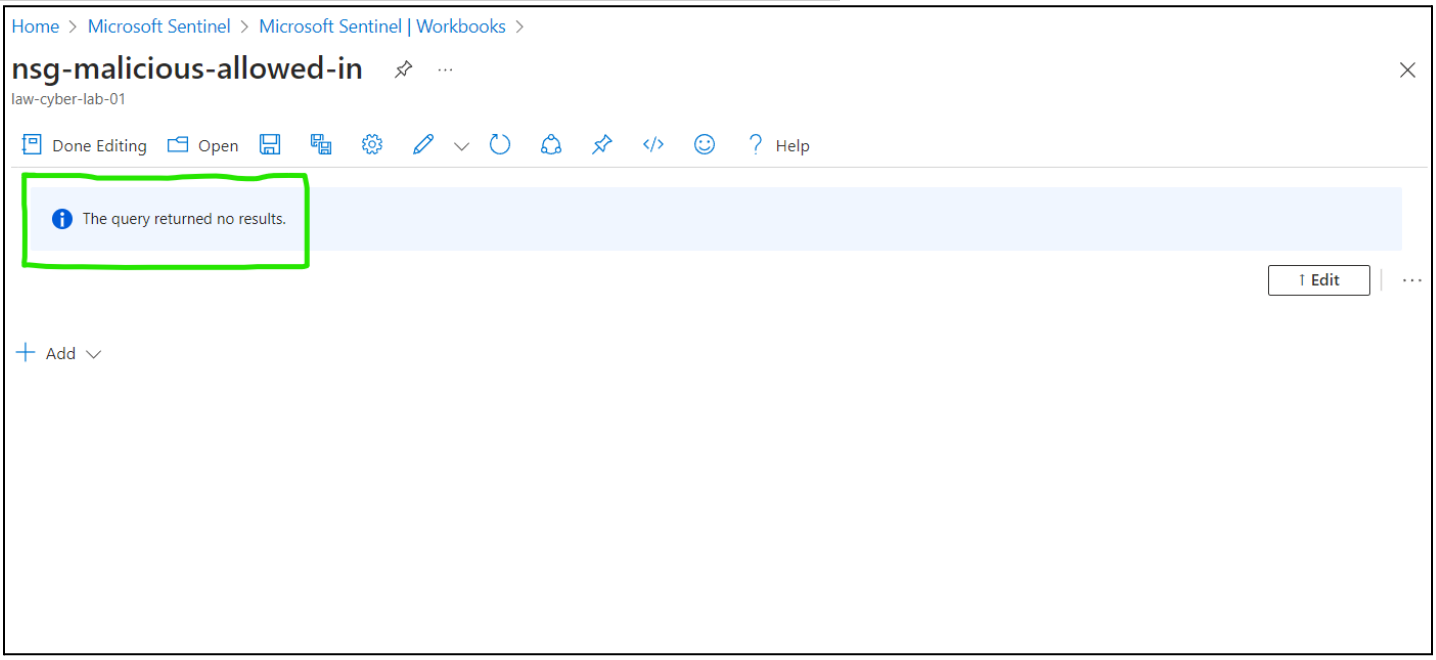
1. **Azure** portal > **Sentinel** > **Workbooks** > **My Workbooks**.
2. Mssql-auth-fail:

   Note: *This attack map is **blank** because it returned no results.*



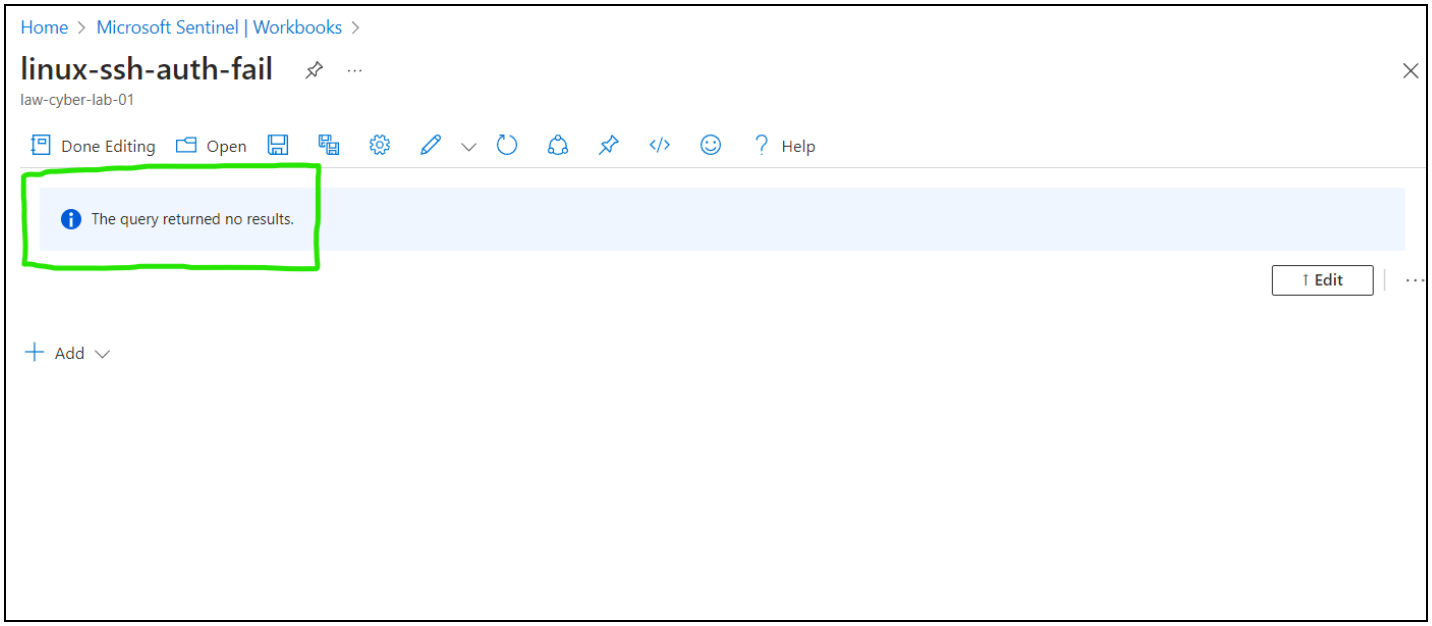
3. Nsg-malicious-allowed-in:

   Note: *This attack map is **blank** because it returned no results.*



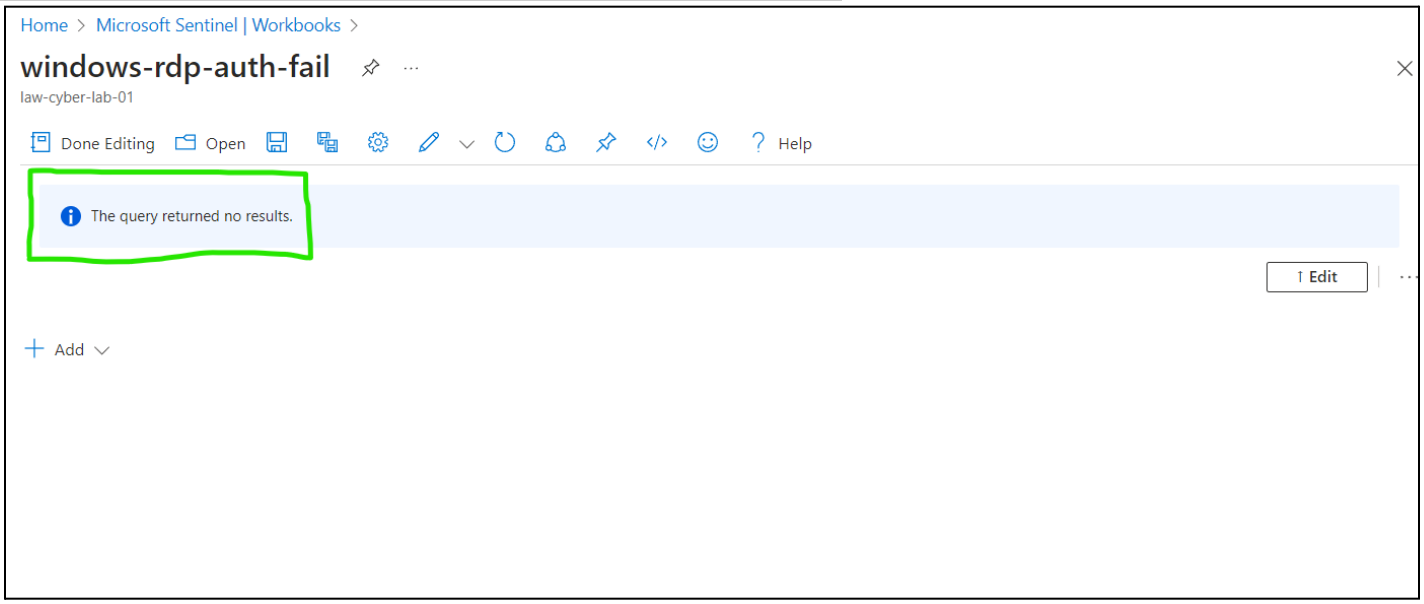
4. Linux-ssh-auth-fail:

   Note: *This attack map is **blank** because it returned no results.*



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

***Note**: This attack map is **blank** because it returned no results.*



End:

- Following our last 24-hour lab exposure, we've enhanced the security posture of our environment by hardening it. We've analyzed the new 24-hour results after [again] exposing our lab environment to external traffic.