Lab #11: **Construction of Sentinel Attack Maps**

Purpose:

- We'll be creating 4 different workbooks in Sentinel, which should help with displaying varying types of malicious traffic that are targeting our resources. This malicious traffic will be coming from different geographical locations.
- Here are the 4 maps we'll be creating, as well as their use cases:

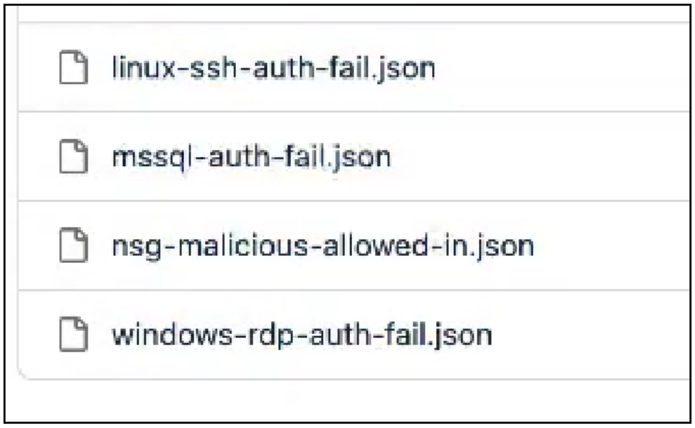
#	Map	Use Case
1	Windows VMs	RDP, SMB, general authentication failures
2	Linux VMs	SSH authentication failures
3	MS SQL Server (in windows-vm)	Authentication failures
4	NSGs	Attack map that displays inbound malicious flows

Tasks:

1. **Prepare the pre-built JSON files**
2. **Configure the 4 workbooks (attack maps)**
   - ○ Attack map #1: Linux-ssh-auth-fail
   - ○ Attack map #2: mssql-auth-fail
   - ○ Attack map #3: nsg-malicious-allowed-in
   - ○ Attack map #4: windows-rdp-auth-fail

Task 1: **Prepare the pre-built JSON files**

1. Open this link to view the four pre-built JSON files: https://github.com/erichmair/Azure-SOC-Honeynet-Project/tree/main/Sentinel-Maps(JSON)



linux-ssh-auth-fail.json
mssql-auth-fail.json
nsg-malicious-allowed-in.json
windows-rdp-auth-fail.json

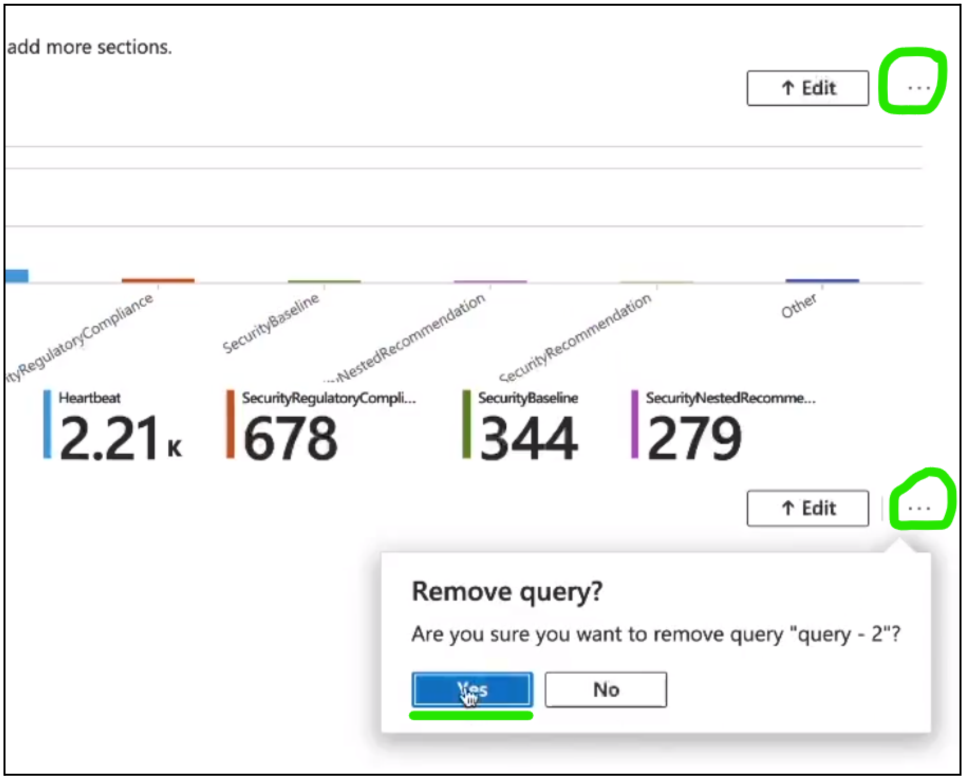
2. Open each JSON file in separate tabs. We'll come back to the files when creating each workbook.

Task 2: **Configure the 4 workbooks (attack maps)**

Attack map #1: Linux-ssh-auth-fail:

1. Open our **Azure** account > **Sentinel** > (open our workspace) > **Workbooks** >
2. Select **Add Workbook** > **Edit**:

a. Remove both default query sections.

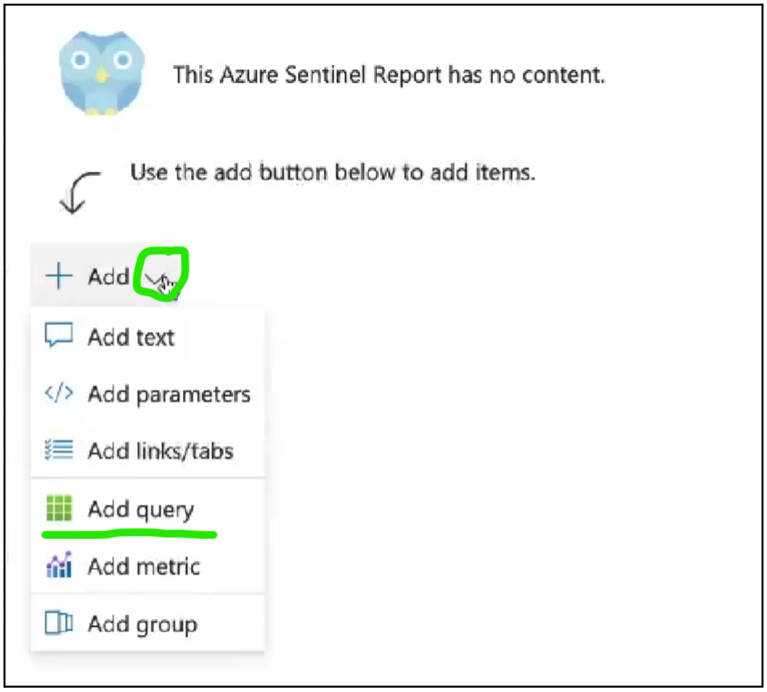


add more sections.

Remove query?

Are you sure you want to remove query "query - 2"?

b. Select **Add Query**

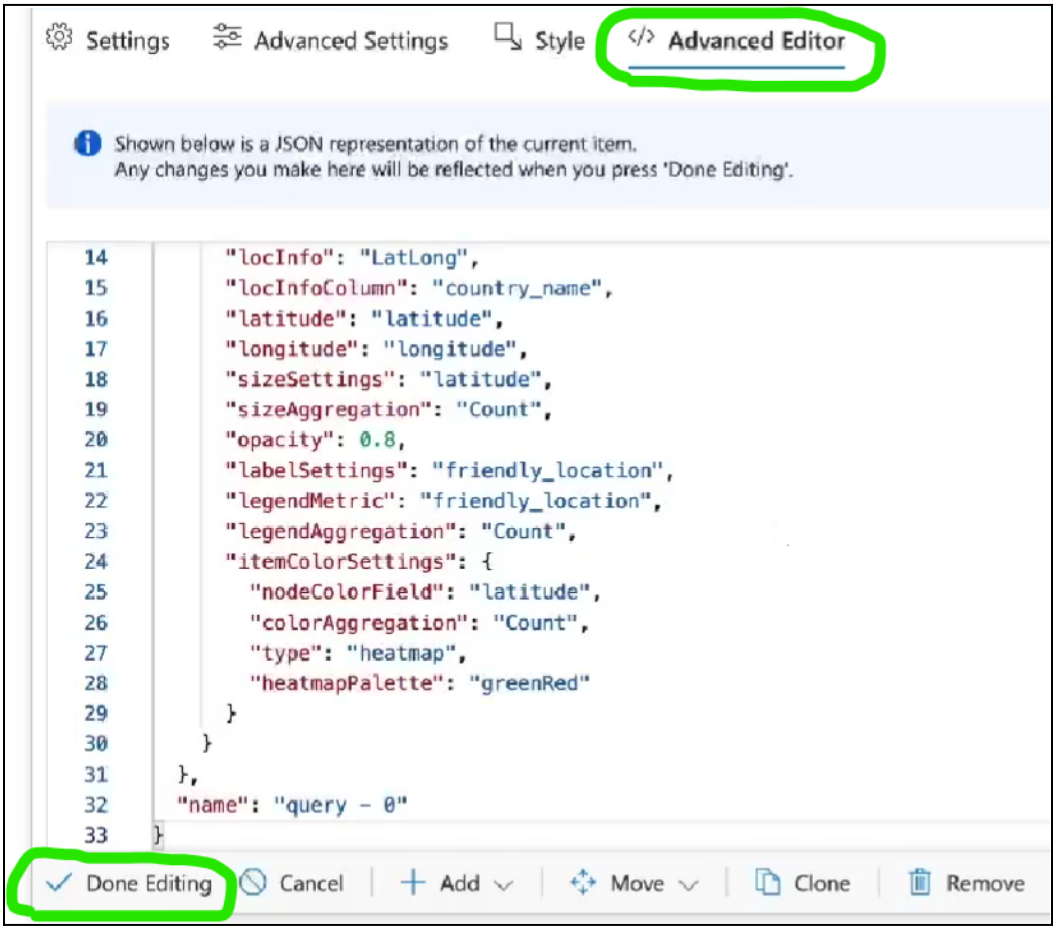


This Azure Sentinel Report has no content.

Use the add button below to add items.

c. Select **Advanced Editor** >

i. Erase the pre-filled query script from the query box. Afterward, copy + paste the contents of the **linux-ssh-auth-fail.json** file into the empty query box > **Done Editing**.



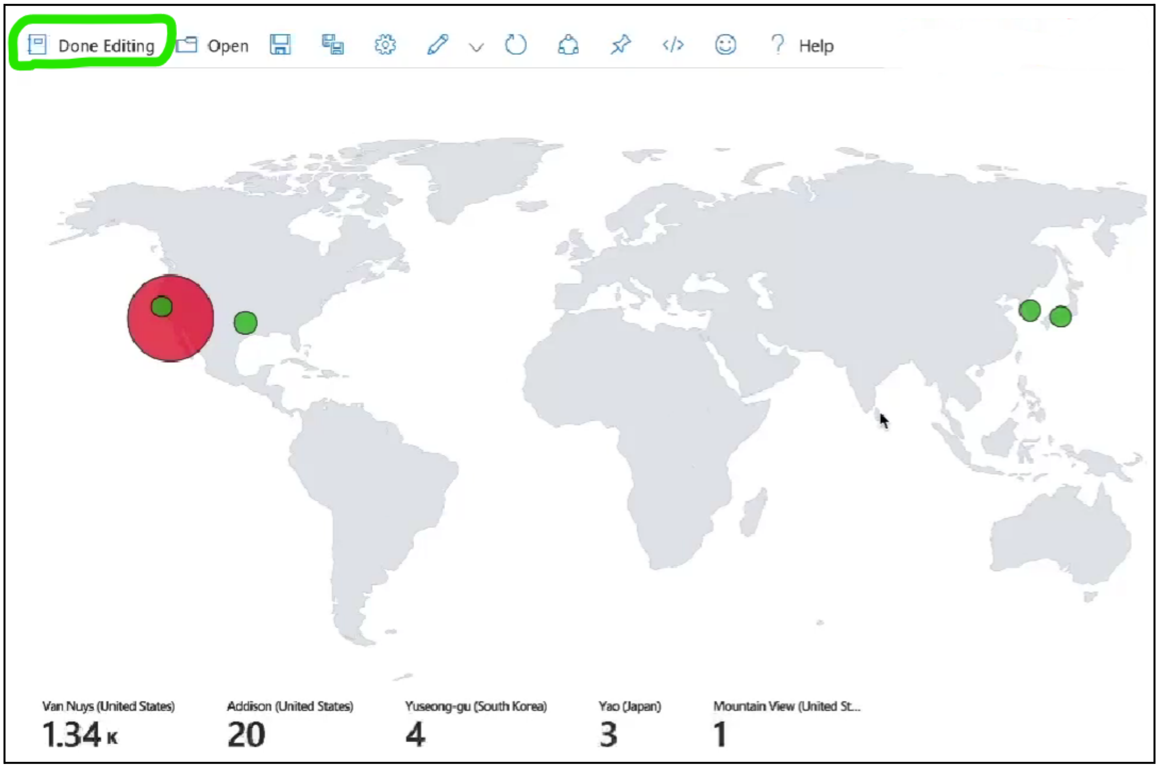
Shown below is a JSON representation of the current item.
Any changes you make here will be reflected when you press 'Done Editing'.

```
        "locInfo": "LatLong",
        "locInfoColumn": "country_name",
        "latitude": "latitude",
        "longitude": "longitude",
        "sizeSettings": "latitude",
        "sizeAggregation": "Count",
        "opacity": 0.8,
        "labelSettings": "friendly_location",
        "legendMetric": "friendly_location",
        "legendAggregation": "Count",
        "itemColorSettings": {
          "nodeColorField": "latitude",
          "colorAggregation": "Count",
          "type": "heatmap",
          "heatmapPalette": "greenRed"
        }
      }
    }
  },
  "name": "query - 0"
}
```

d. The **linux-ssh-auth-fail** attack map is now generated.

i. Update the name to "linux-ssh-auth-fail" (select the **Save As** icon).

ii. Select **Done Editing**.



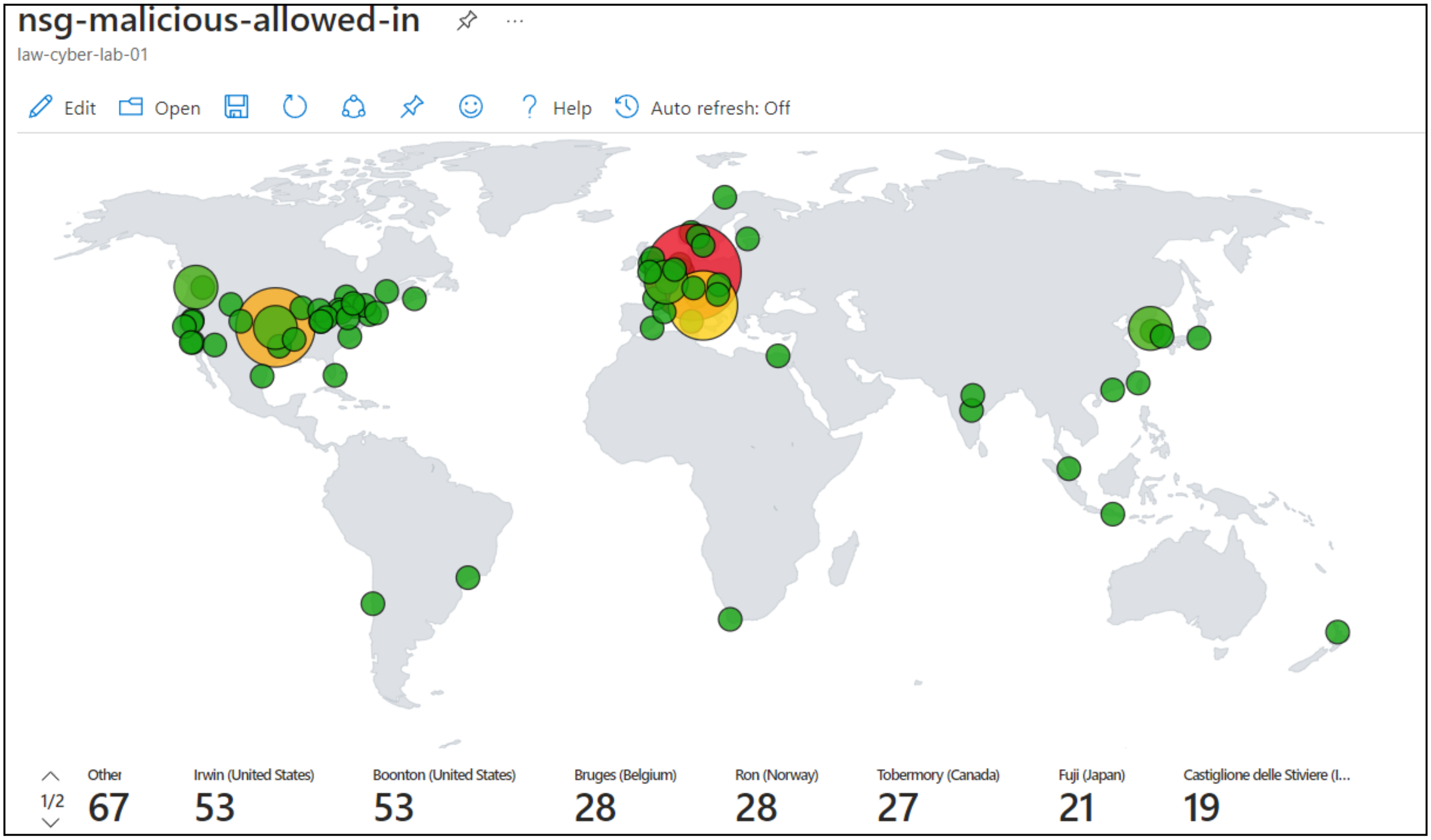
```
Van Nuys (United States)   Addison (United States)   Yuseong-gu (South Korea)   Yao (Japan)   Mountain View (United St...
1.34 K                     20                        4                          3             1
```

Attack map #2: mssql-auth-fail:

1. **Azure** account > **Sentinel** > (open our workspace) > **Workbooks** >
2. Select **Add Workbook** > **Edit**:
   a. Remove both default query sections.
   b. Select **Add Query** > **Advanced Editor** >
      i. Erase the pre-filled query script from the query box. Afterward, copy + paste the contents of the **mssql-auth-fail.json** file into the empty query box > **Done Editing**.
   c. The **mssql-auth-fail** attack map is now generated.
      i. Update the name to “mssql-auth-fail” (select the **Save As** icon).
      ii. Select **Done Editing**.

Attack map #3: nsg-malicious-allowed-in:

1. **Azure** account > **Sentinel** > (open our workspace) > **Workbooks** >
2. Select **Add Workbook** > **Edit**:
   a. Remove both default query sections.
   b. Select **Add Query** > **Advanced Editor** >
      i. Erase the pre-filled query script from the query box. Afterward,copy + paste the contents of the **nsg-malicious-allowed-in.json** file into the empty query box > **Done Editing**.
   c. The **nsg-malicious-allowed-in** attack map is now generated.
      i. Update the name to “nsg-malicious-allowed-in” (select the **Save As** icon).
      ii. Select **Done Editing**.



nsg-malicious-allowed-in

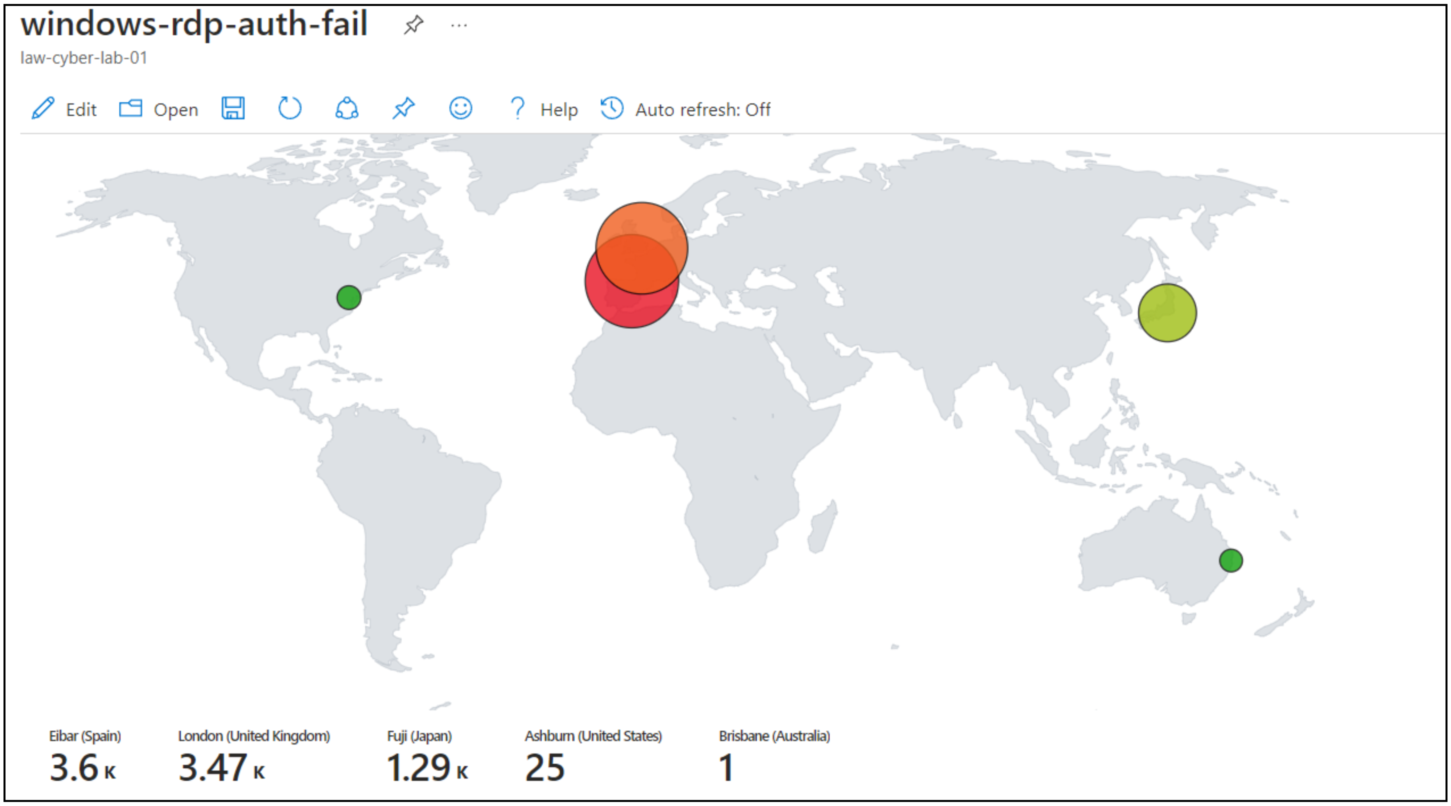
law-cyber-lab-01

Other	Irwin (United States)	Boonton (United States)	Bruges (Belgium)	Ron (Norway)	Tobermory (Canada)	Fuji (Japan)	Castiglione delle Stiviere (I...
67	53	53	28	28	27	21	19

Attack map #4: windows-rdp-auth-fail:

1. **Azure** account > **Sentinel** > (open our workspace) > **Workbooks** >
2. Select **Add Workbook** > **Edit**:
   a. Removed both default query sections.
   b. Selected **Add Query** > **Advanced Editor** >
      i. Erase the pre-filled query script from the query box. Afterward, copy + paste the contents of the **windows-rdp-auth-fail.json** file into the empty query box > **Done Editing**.
   c. The **windows-rdp-auth-fail** attack map is now generated.

i. Update the name to “windows-rdp-auth-fail” (select the **Save As** icon).
ii. Select **Done Editing**.



windows-rdp-auth-fail

law-cyber-lab-01

Eibar (Spain)	London (United Kingdom)	Fuji (Japan)	Ashburn (United States)	Brisbane (Australia)
3.6 K	3.47 K	1.29 K	25	1

End:

- Our SIEM (Microsoft Sentinel) is querying our Log Analytics workspace and producing attack maps. These maps utilize the GeoIP watchlist to better map the geographical location of malicious IP addresses.