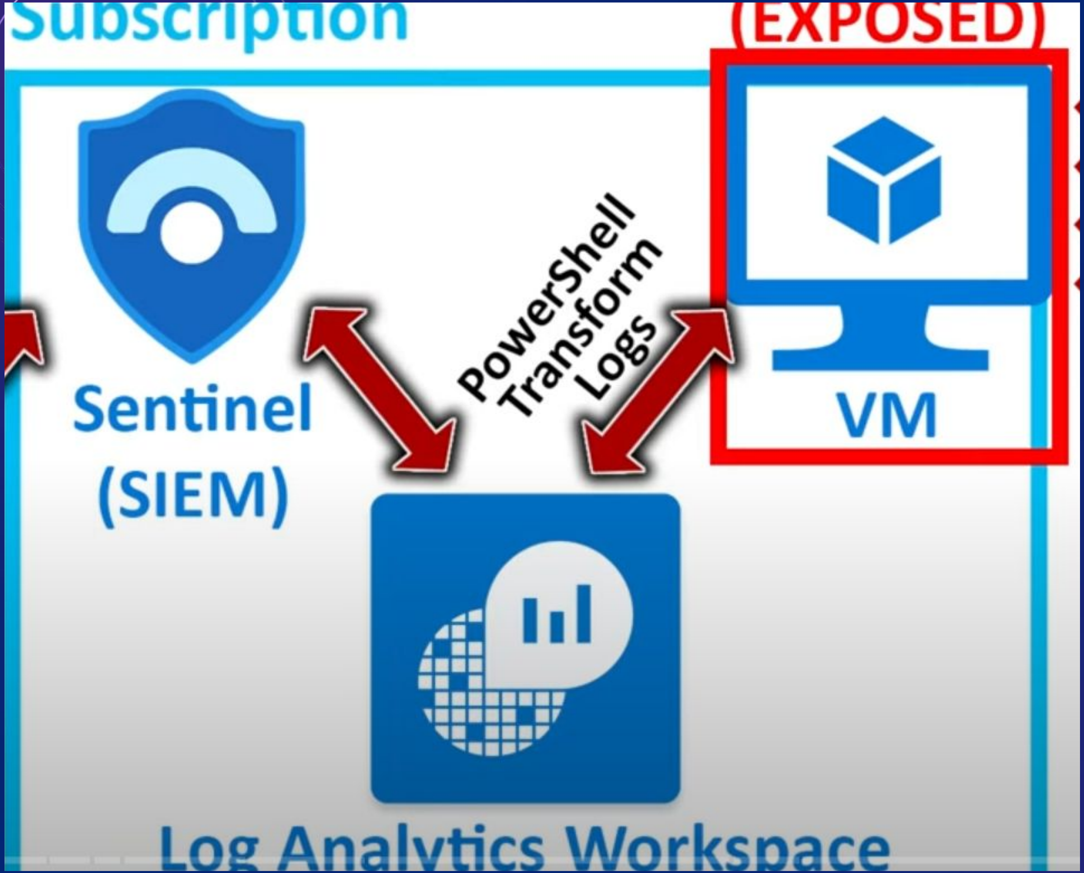
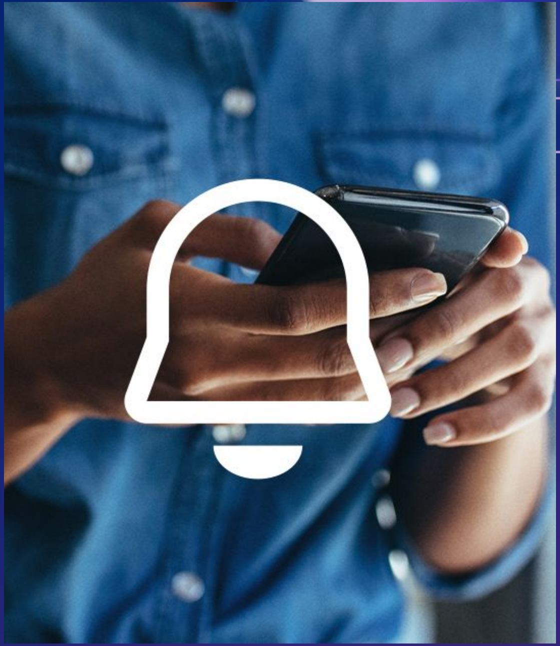
Azure SIEM With Live Map Integration

Rogelio Perez Montero

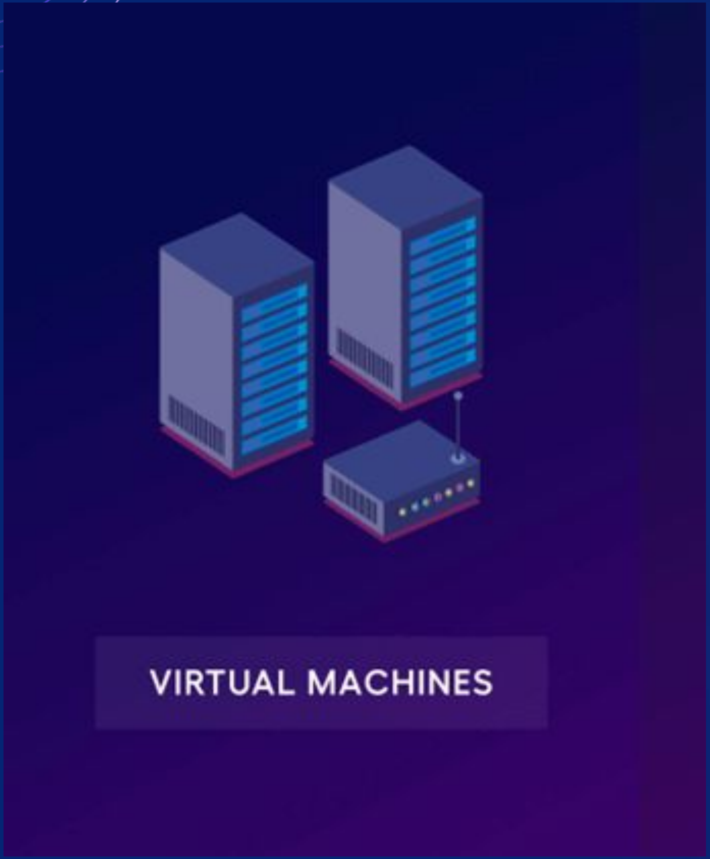
What is a S.I.E.M?

- Security Information and Event Management
- Primary function of a SIEM system is to collect, analyze, correlate, and manage security data from various sources within an organization's IT infrastructure.
- Creates real time correlation analysis
- Provides alerts, automated responses, and forensic capabilities





Introduction

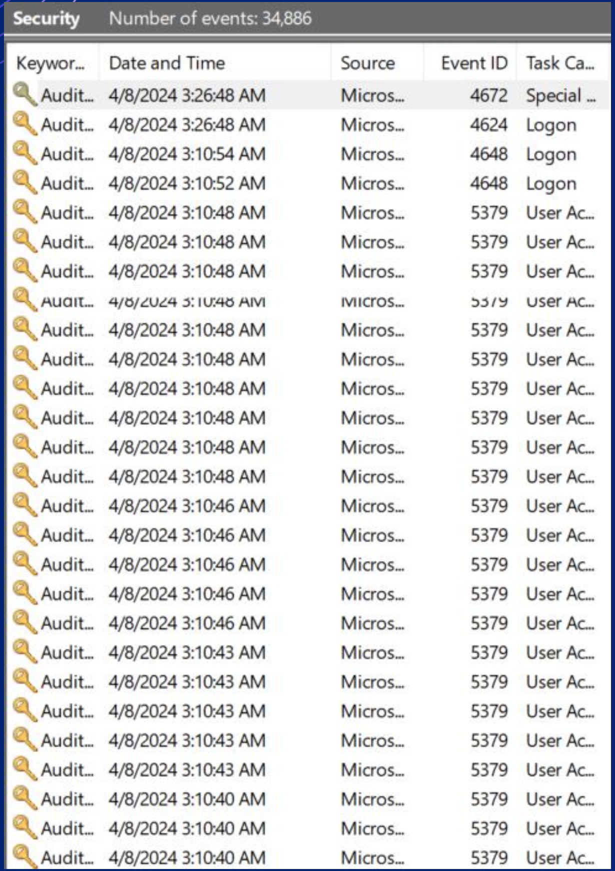


Azure Virtual Machine

- Windows 10 as operating system
- Expose to the internet by allowing all traffic inbound rules, to gather data on people trying to “remote desktop connect”
- Took off all firewalls to be the most vulnerable and discoverable
- Tested by pinging the vm multiple times

Azure Log Analytics

- Collects and aggregates log data from various sources across Azure resources and on-premises environments
- Has tools to analyze log data, identify trends, and potential issues
- Has real time alerts and monitoring
- Responsible for collecting all the failed login data from the virtual machine

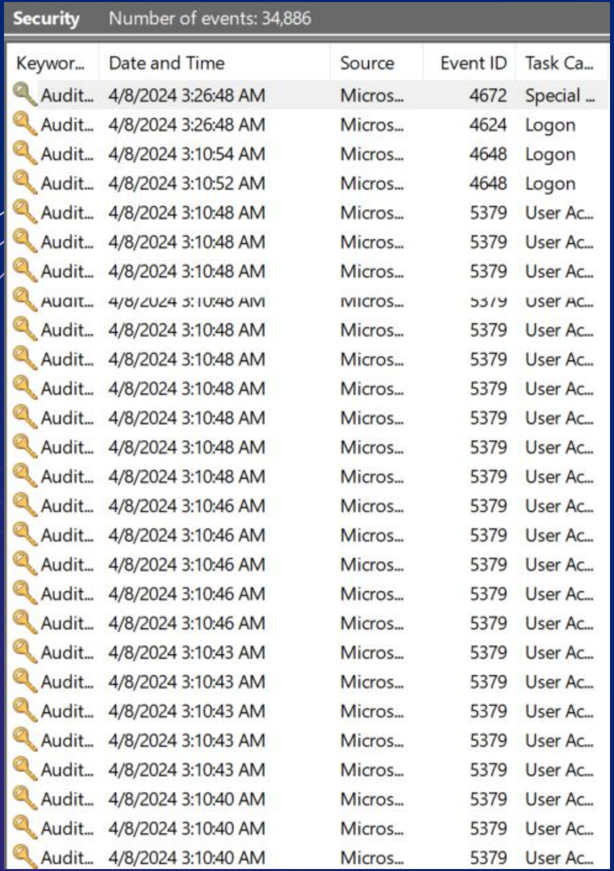


Security Number of events: 34,886

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	4/8/2024 3:26:48 AM	Micros...	4672	Special ...
Audit...	4/8/2024 3:26:48 AM	Micros...	4624	Logon
Audit...	4/8/2024 3:10:54 AM	Micros...	4648	Logon
Audit...	4/8/2024 3:10:52 AM	Micros...	4648	Logon
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:40 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:40 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:40 AM	Micros...	5379	User Ac...

Combining VM & Logs

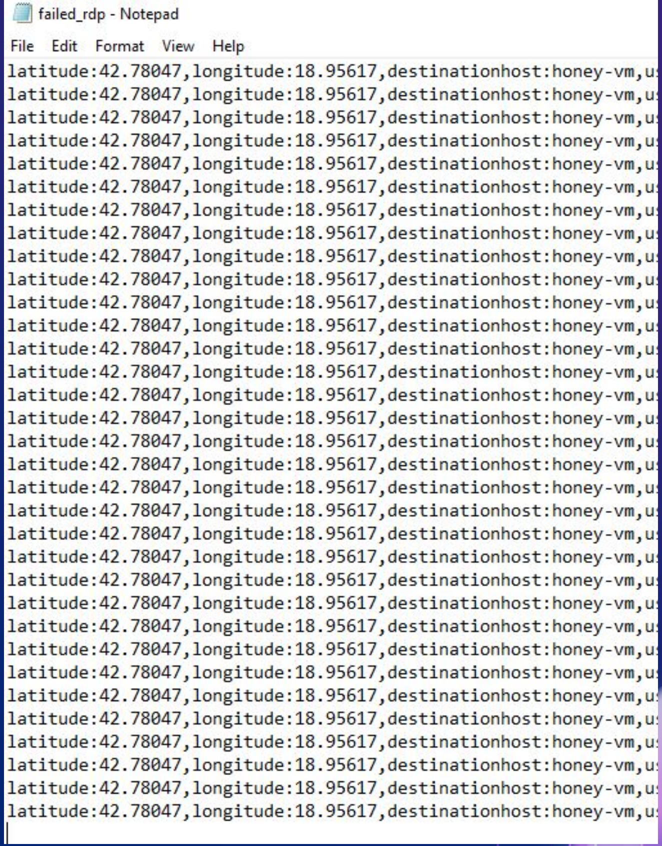
- Data comes from the Event Viewer failed login logs. (Event ID: 4625)
- Using a powershell Script, they are converted into readable data
- IP geolocation API converts the IP addresses of failed login attempts into countries and cities
- The Work Logs tool takes the output file of the script and stores it in a database which can be manipulated in their GUI



Security Number of events: 34,886

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	4/8/2024 3:26:48 AM	Micros...	4672	Special ...
Audit...	4/8/2024 3:26:48 AM	Micros...	4624	Logon
Audit...	4/8/2024 3:10:54 AM	Micros...	4648	Logon
Audit...	4/8/2024 3:10:52 AM	Micros...	4648	Logon
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:48 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:46 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:43 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:40 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:40 AM	Micros...	5379	User Ac...
Audit...	4/8/2024 3:10:40 AM	Micros...	5379	User Ac...

PowerShell ISE



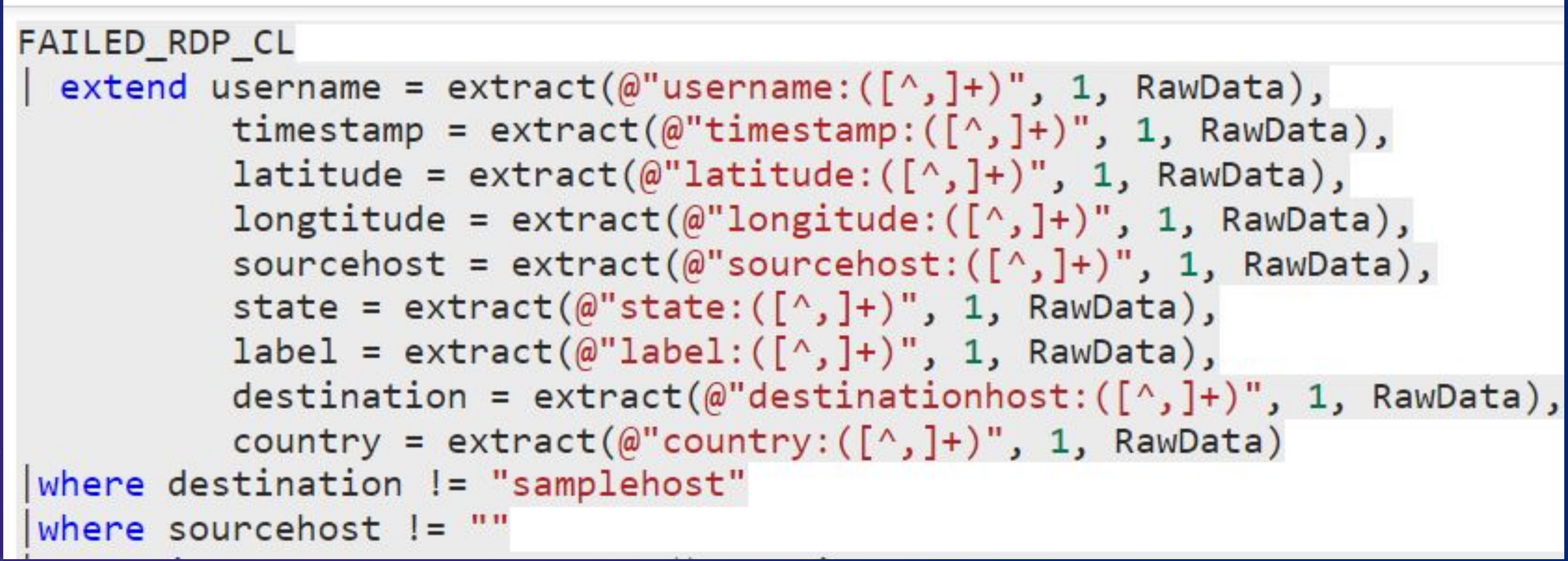
failed_rdp - Notepad

```
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
latitude:42.78047,longitude:18.95617,destinationhost:honey-vm,u
```

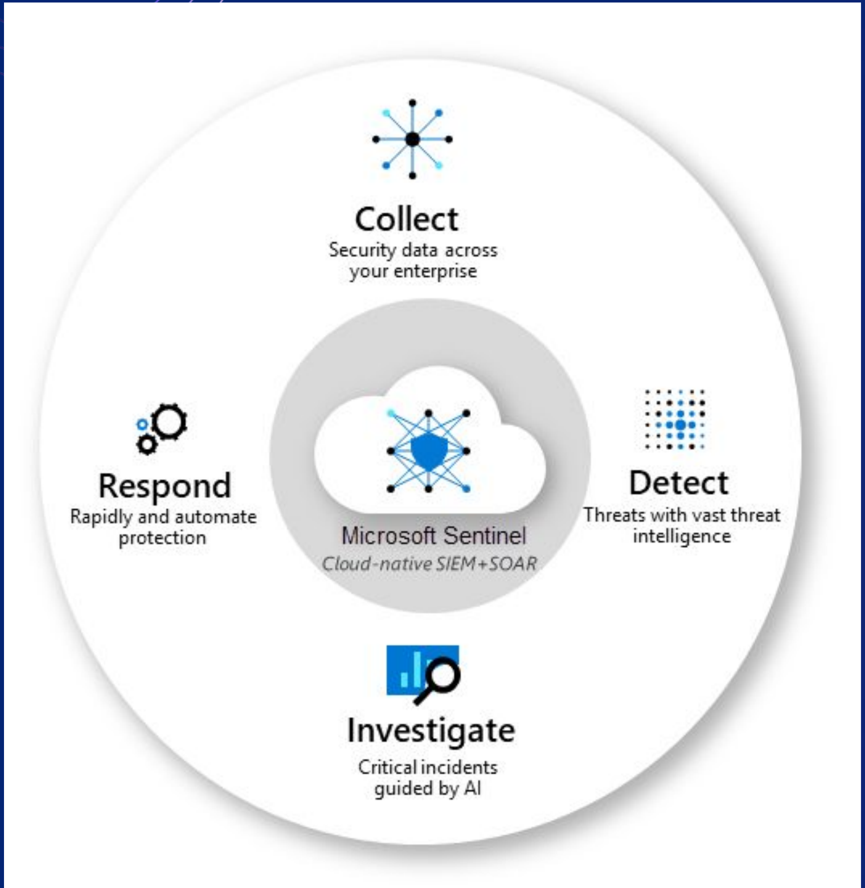
Refining Data

- Text file is still set as raw data without any labels for countries or state/city
- Using queries, the data was refined to extract the labels need to make a live map
- After cleaning the data, 17,400 failed Remote Desktop Connections

Query

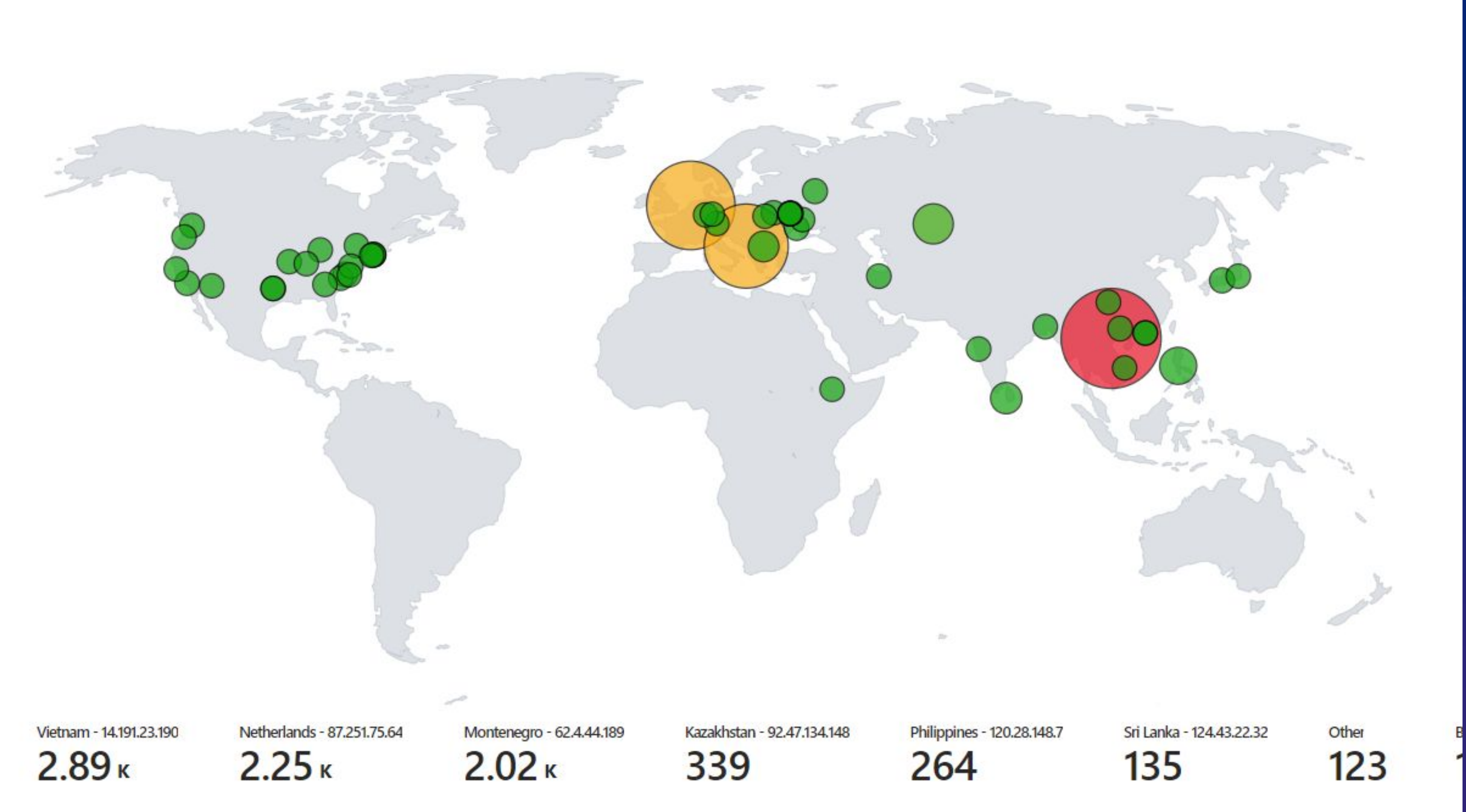


```
FAILED_RDP_CL
| extend username = extract(@"username:([^,]+)", 1, RawData),
          timestamp = extract(@"timestamp:([^,]+)", 1, RawData),
          latitude = extract(@"latitude:([^,]+)", 1, RawData),
          longtitude = extract(@"longitude:([^,]+)", 1, RawData),
          sourcehost = extract(@"sourcehost:([^,]+)", 1, RawData),
          state = extract(@"state:([^,]+)", 1, RawData),
          label = extract(@"label:([^,]+)", 1, RawData),
          destination = extract(@"destinationhost:([^,]+)", 1, RawData),
          country = extract(@"country:([^,]+)", 1, RawData)
|where destination != "samplehost"
|where sourcehost != ""
```


Collect
Security data across your enterprise
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI
Respond
Rapidly and automate protection
Microsoft Sentinel
Cloud-native SIEM+SOAR

Azure Sentinel

- provides attack detection, threat visibility, proactive hunting, and threat response to help you stop threats
- Used Analytics tool to create a incident rule
- When EventID 4625 is greater than 10, alert is send with customized automated response
- Used workbook tool to connect the Log workspace data and make a live map of all login attempts



Vietnam - 14.191.23.190	Netherlands - 87.251.75.64	Montenegro - 62.4.44.189	Kazakhstan - 92.47.134.148	Philippines - 120.28.148.7	Sri Lanka - 124.43.22.32	Other	B
2.89 K	2.25 K	2.02 K	339	264	135	123	1

Thank you

Questions?