Part 1. Setup Azure Subscription

Create Free Azure Subscription:
https://azure.microsoft.com/en-us/pricing/purchase-options/azure-account

If Azure doesn't let you create a free account, you can either

1. Create a paid subscription and be mindful of shutting down/deleting your resources when you are done, or
2. Sign up for the Cyber Range, where you pay a flat fee and get access to Azure, Tenable, Defender for Endpoint, Courses, Labs, Weekly lives, optional Cyber Internship: https://skool.com/cyber-range

After your subscription is created, you can login at:
https://portal.azure.com

Part 2. Create the Honey Pot (Azure Virtual Machine)

Go to: https://portal.azure.com and search for virtual machines

Create a new Windows 10 virtual machine (choose an appropriate size. If you are in the Cyber Range, the size will be limited. You notice the monthly cost of leaving the VM on 24/7. Be mindful of shutting this off when you are done, or just join the cyber range and we handle the back end expense). Remember the username and password

Go to the Network Security Group for your virtual machine and create a rule that allows all traffic inbound

Log into your virtual machine and turn off the windows firewall (start -> wf.msc -> properties -> all off)

Part 3. Logging into the VM and inspecting logs

Fail 3 logins as "employee" (or some other username)

Login to your virtual machine

Open up Event Viewer and inspect the security logs

See the 3 failed logins as "employee", event ID 4625

Next, we are going to create a central log repository called a LAW

Part 4. Log Forwarding and KQL

Create Log Analytics Workspace

Create a Sentinel Instance and connect it to Log Analytics

(observe architecture)

Configure the “Windows Security Events via AMA” connector

Create the DCR within sentinel, watch for extension creation

Query for logs within the LAW

We can now query the Log analytics workspace as well as the SIEM, sentinel directly, which we will do soon

> Note: Querying logs in here is a really important skill that you MUST have if you want to work in security operations. Depending on where you work, you need to know SQL, KQL, or SPL, but these are all basically the same thing. If you know one, you can easily learn the others. Microsoft and Sentinel uses KQL, which you can learn in the Cyber Range https://skool.com/cyber-range, or from here https://kc7cyber.com/ (free)
>
> Tip: The Cyber Range is basically a full production environment with *hundreds* of users and Virtual Machines in it, which are all producing a ton of logs. It’s a really good place to practice just sifting through logs and seeing what you can see.

Observe some of your VM logs:

```
SecurityEvent
| where EventId == 4625
```

(observe architecture)

Part 5. Log Enrichment and Finding Location Data

Observe the SecurityEvent logs in the Log Analytics Workspace; there is no location data, only IP address, which we can use to derive the location data.

We are going to import a spreadsheet (as a “Sentinel Watchlist”) which contains geographic information for each block of IP addresses.

Download: geoip-summarized.csv

Within Sentinel, create the watchlist:

Name/Alias: geoip
Source type: Local File
Number of lines before row: 0
Search Key: network

Allow the watchlist to fully import, there should be a total of roughly 54,000 rows.

In real life, this location data would come from a live source or it would be updated automatically on the back end by your service provider.

(observe architecture)

Observe the logs now have geographic information, so you can see where the attacks are coming from

```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent
    | where IpAddress == <attacker IP address>
    | where EventID == 4625
    | order by TimeGenerated desc
    | evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
WindowsEvents
```

(observe architecture)

Part 6. Attack Map Creation

Within Sentine, create a new Workbook

Delete the prepopulated elements and add a “Query” element

Go to the advanced editor tab, and paste the JSON

Workbook (Attack map):
map.json

Observe the query
Observe the map settings

Observe the map

Finished!

If you liked this lab, join the Cyber Range: https://skool.com/cyber-range

- Access to an actual work environment with licensed enterprise security tools
- Weekly live calls with me
- Internships
- Community
- Threat hunts with cash prizes