**TO MAP LIVE CYBER ATTACKS USING SECURITY INFORMATION AND EVENT MANAGER(SIEM)**

Objective : Setting up Azure Sentinel(cloud based SIEM) to map live cyber attacks .

In this project we use a Virtual Machine in the cloud which is going to be a honey pot(Make it vulnerable) and we collect the records of ip addresses of the attackers using powershell script and send the data to the third party API to geolocate the attacks.

* Create a VM (exposed)
* We use Log Analytics Workspace(To collect the data)
* Setup Azure Sentinel(SIEM) (To create a map to map the attacker data)
* We use Powershell (To extract ip addresses from the windows) and send it to third party API(will derive the latitude , longitude and send it to VM)

STEPS :  
In Azure Portal:

Create all the resources under same resource group

1. Create a VM - create a new inbound rule in Networking section (windows)
2. Create Log Analytic Workspace
3. Security Centre - setting - defender plans on - servers on, sql off then -data collection - All events
4. Connect Log analytics - VM and connect
5. Create Sentinel - pick log analytics
6. Open VM and copy IP - Open Remote Desktop

In Remote Desktop :

1. Open Event Viewer - Here we can find the people who fail to login to our vm
2. We collect those ip addresses systematically(using PowerShell)
3. Now turn off the firewall protection on VM(remote desktop)
4. Open PowerShell and run the following PowerShell script{Hyperlink}
5. In this script you need get your own API\_KEY from the website{Hyperlink}(ipgeolocation.io)
6. By using the PowerShell script we can grab all the logs(failed) and send them to the API and get the geolocation from the API and create log files. (Stores in $LOGFILE\_PATH )

Again we go back to Azure Portal:

1. Go to Log analytics - Custom log - create a custom log
2. Copy the LOGFILE from remote desktop and Create a file(failed\_rdp\_log) in your desktop Note : this failed\_rdp\_log will be used in “creating custom log” in azure
3. “In Collection paths'' select windows and paste the path of the LOGFILE from Remote Desktop(VM).
4. Next fill the details section and Create Custom Log(cl)
5. Then go to “logs” and run the custom log(cl) - We run the logs from the LOGFILE generated by PowerShell.
6. Expand one of the Logs and Click the Actions(“...”) then we need to extract each field (attributes such as latitude , longitude) and save each extractions(custom fields).
7. And finally run the Custom log again - we can find each extraction(custom field) as column in the logs section.

Note: Each Custom field can be modified in Custom Logs section

1. Create a “New workbook” in Azure Sentinel
2. Run the following query - FAILED\_RDP\_WITH\_GEO\_CL | summarize event\_count=count() by sourcehost\_CF, latitude\_CF, longitude\_CF, country\_CF, label\_CF, destinationhost\_CF

| where destinationhost\_CF != "samplehost"

| where sourcehost\_CF != ""

1. Select Visualisation as “Map”
2. Set the Map Setting according to our purpose
3. Save the Map and wait for the attacks.
4. After a while we get the attacks from various countries.
5. Collect the data from the map.

Conclusion :

* SIEM makes it easier for enterprises to manage security by filtering massive amounts of security data and prioritising the security alerts the software generates.SIEM software enables organisations to detect incidents that may otherwise go undetected..
* SIEM system also enhances incident management by enabling the company's security team to uncover the route an attack takes across the network, identify the sources that were compromised and provide the automated tools to prevent the attacks in progress.
* In this Project with the help of SIEM analytics of Azure Sentinel we are able to demonstrate and map a live cyber attack on our Virtual Machine.