FALL SEMESTER 2022-23

CSE3501-INFORMATION SECURITY ANALYSIS AND AUDIT

TOPIC: MAPPING CYBER ATTACKS USING AZURE SENTINEL

TEAM NO: 18

TEAM MEMBERS:

THEO DANIEL M - 20BCB0122

KISHORE R - 20BCE2411

PRANSHU BHARGAVA - 20BCB0137

COURSE CODE: CSE3501

SLOT: G1

Under the supervision of

Dr. Saritha Murali

ABSTRACT

The ever-increasing amount of major security incidents has led to an emerging interest in cooperative approaches to encounter cyber threats. The protection of corporate IT infrastructures against cyber attacks is becoming a more and more demanding task.

In order to achieve a high level of cyber security awareness most mid to large sized companies use Security Information and Event Management (SIEM) embedded into a Security Operations Center. These systems enable the centralized collection and analysis of security relevant information generated by a variety of different systems, to detect advanced threats and to improve reaction time in case of an incident.

Security information and event management systems are the industry-specific word in Computer Security talking for the type of info that an average of log documents or celebration logs out of multiple sources into a centralized repository for further analysis. Occasion logs are produced by numerous internet sites, apparatus, programs and computer software Updates.

Currently, SIEM systems and related solutions are slowly converging with big data analytics tools.

Our project is an overview about the security information event management system and how it can be used to locate cyber attacks from different parts of the world. The aim of our project is to monitor and log cyber-attacks from different IP addresses, use that data and display the location of the source of the attack and the magnitude of the attack. This can be achieved using azure sentinel which is a cloud-based SIEM as well as a virtual machine in the cloud. we're going to make it super vulnerable to the internet and then essentially we're going to monitor and log the cyber attacks from different IP addresses from different places all over the world.

INTRODUCTION

Cybersecurity risks affecting industrial control systems (ICT) have grown enormously during the past couple of years, mainly due to increased activity by nation-states and cyber criminals. Attackers have become more sophisticated and dangerous and their appropriate and timely detection has become a real challenge.

Examples of current cybersecurity incidents affecting IT and ICT include : ransomware attacks; malware having impact on the utility's ability to conduct business and operations; phishing campaigns directed to executives, executive assistants, SCADA engineers, IT administrators or other privileged users; business email compromise incidents, including account takeover or impersonation of executives; data leakage and thefts; social engineering to gather sensitive information from personnel.

The aim of our project is to monitor and log cyber-attacks from different IP addresses, use that data and display the location of the source of the attack and the magnitude of the attack.

Our project is performed in the Microsoft sentinel environment entirely.

To monitor and log cyber-attacks from different IP addresses, use that data and display the location of the source of the attack and the magnitude of the attack, we do it in three steps :

1. Get the attacker's IP address.
2. Getting geo data from it.
3. Sending it to azure mapping.

Azure Sentinel – cloud-based Microsoft native SIEM - security information and event management platform that uses built-in AI to help analyse large volumes of data across an enterprise fast. Microsoft Sentinel natively incorporates Azure services, like Log Analytics which we use in our project.

In our project we will be inspecting the failed RDP logs.

To do this we will be using a custom PowerShell script to extract the IP address from the windows event viewer and send it to a third-party API to derive the geographic data like the latitude, and longitude.

PowerShell - is a task automation and configuration management program from Microsoft, consisting of a command-line shell and the associated scripting language.

Followed by this, we send the geographical data back to the Virtual machine which in turn creates a custom log with the geographic data.
Create a log repository called log analytics workspace in azure, to ingest logs from the virtual machine.
Set up azure sentinel, where we configure Azure Sentinel workbook (Microsoft's cloud SIEM) to display the global attack data on the world map according to the physical location and magnitude of attacks.

In Microsoft Sentinel each workspace has its own data repository and configuration and can combine data from multiple services. In our project we, :

- Configure Log Analytics Workspace in Azure to ingest custom logs containing geographic information (Latitude, state/province, and country etc).
- Configure Custom Fields in Log Analytics workspace with the intent of mapping geo data in azure sentinel.
- Configure Azure sentinel (Microsoft's cloud SIEM) workbook to display attack data (RDP brute force) on the world map according to physical location and magnitude attacks.

2. Literature Study

Some recent works in the related areas

- Global Mapping of Cyber Attacks by Ghita Mezzour, L. Richard Carley, Kathleen M. Carley (2014)

In this work, Symantec's World Intelligence Network Environment (WINE) Intrusion Prevention System (IPS) is used , elemetry data which contain attack reports from more than 10 million customer computers worldwide. Regression analysis is used to test for the relevance of multiple factors including monetary and computing resources, cyber-security research and institutions, and corruption which helps in confirming some hypotheses and disproves others.
It was found that many countries in Eastern Europe extensively host attacking computers because of a combination of good computing infrastructure and high corruption rate. And also found that web attacks and fake applications are most prevalent in rich countries because attacks on these countries are more lucrative. Whereas it was found that computers in Africa launch the lowest rates of cyber-attacks.

- A STUDY ON TYPES OF CYBER CRIMES AND CYBER ATTACKS IN INDIA by Bhavika Pandita Hakhroo

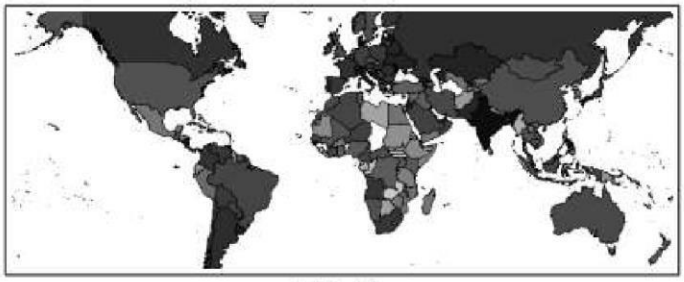
The study was aimed to understand the types of cybercrimes and cyber-attacks in India. The Information Technology Act has had a significant impact on dealings with crimes related to the cyber / virtual world. The cyber crime rate in India has been increasing. To understand cybercrime, an understanding of the types of cyber crimes is crucial. The preventive measures are necessary to safeguard against the nature of these crimes. It is important to undertake preventive measures and safeguard yourself beforehand and be aware of these types of crimes. The basic measure to prevent cybercrime are to ensure regular computer updates, keep strong passwords and to avoid using public wifi networks

- Cyber Attack Prevention Based on Evolutionary Cybernetics Approach by Dmitry Zegzhda,Daria Lavrova *,Evgeny PavlenkoORCID andAnna Shtyrkina

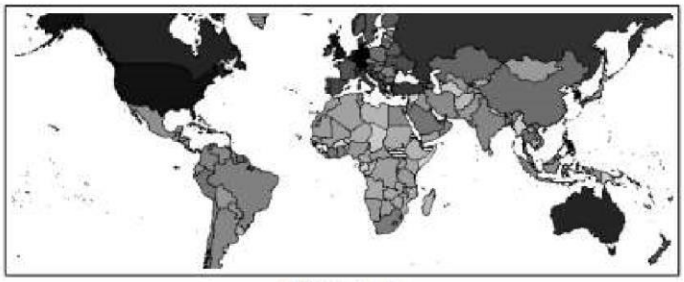
The paper looks at the problem of cybersecurity in modern cyber–physical systems and proposes an evolutionary model approach to counteract cyber attacks by self-regulating the structure of the system, as well as several evolutionary indicators to assess the state of the system.. The methodological approach consists of using evolutionary models to describe how modern cyber–physical systems can counteract cyber attacks and evolve, building on the experience of past security incidents.

Some statistical data and figure

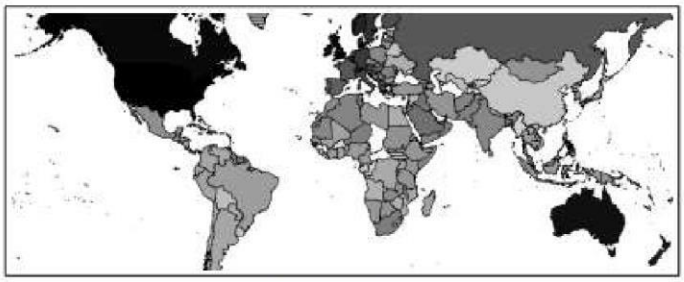
1. Attacks encountered per computer. Vizualization



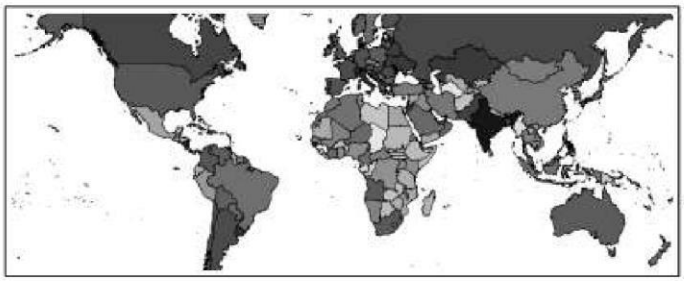
(a) Exploits



(b) Web attacks



(c) fake applications



(d) Total attacks

2. Attacks encountered per computer. Correlation table of variables used in the regression

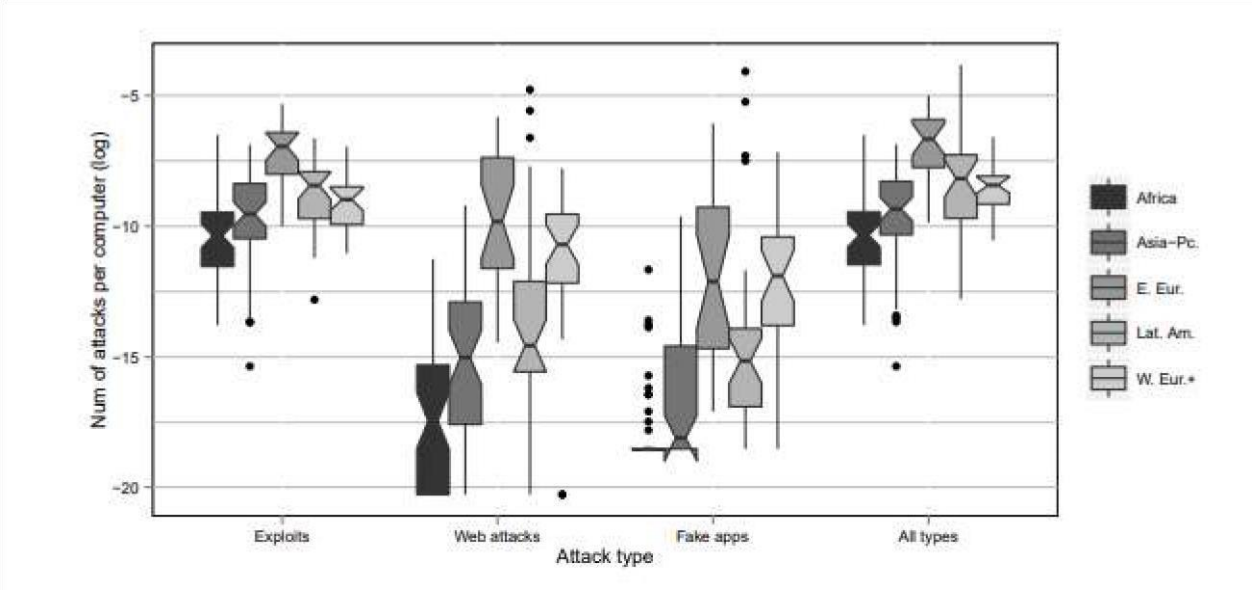
	Exploits enc.	Web atcks enc.	Fake apps enc.	All types enc.	Bandwith	ICT	GDP PC	Web viz.	Research	Institutions	Alliance btw	Hostility btw
Exploits enc.												
Web atks enc.	0.46***											
Fake apps enc.	0.28***	0.71***										
All types enc.	0.88***	0.62***	0.43***									
Bandwidth	0.16*	0.39***	0.44***	0.26***								
ICT	0.36***	0.70***	0.65***	0.51***	0.60***							
GDP PC	0.28***	0.61***	0.64***	0.42***	0.52***	0.92***						
Web viz.	0.02	0.15*	0.16*	0.04	0.02	0.16*	0.17*					
Research	0.11	0.33***	0.20**	0.16*	0.09	0.23**	0.20**	0.64***				
Institutions	0.44***	0.51***	0.35***	0.50***	0.34***	0.56***	0.47***	0.15*	0.27***			
Alliance btw	0.10	0.32***	0.31***	0.15*	0.10	0.21**	0.18*	0.48***	0.46***	0.20**		
Hostility btw	-0.02	0.10	0.11	-0.01	0.03	0.02	0.00	0.40***	0.38***	0.07	0.30***	
Extradition btw	0.04	0.22**	0.22**	0.08	0.03	0.13	0.12	0.78***	0.70***	0.12	0.58***	0.55***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

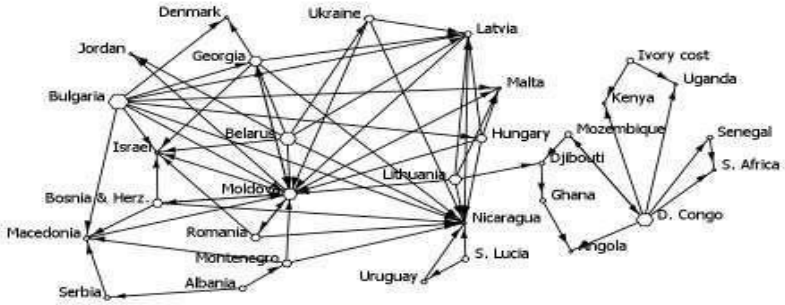
3. Attacks encountered per computer. Top countries

Exploits		Web attacks		Fake applications		All types	
Country	Value	Country	Value	Country	Value	Country	Value
Belarus	4.85	Belize	8.41	Dominica	13.82	Dominica	21.66
Moldova	2.88	Dominica	3.76	Trinidad & Tobago	5.27	Belize	9.08
Georgia	2.68	Moldova	2.97	Latvia	2.31	Trinidad & Tobago	7.29
Bulgaria	2.52	Ukraine	1.99	Bosnia & Herz.	1.01	Moldova	6.75
Bosnia & Herz.	1.96	Latvia	1.57	Moldova	0.81	Latvia	5.63
Ukraine	1.96	Trinidad & Tobago	1.33	Luxembourg	0.76	Belarus	4.91
Latvia	1.56	Lithuania	0.92	Panama	0.67	Ukraine	4.06
Congo	1.49	Bosnia & Herz.	0.75	Belize	0.55	Bosnia & Herz.	3.77
Hungary	1.42	Romania	0.74	Romania	0.50	Georgia	2.72
Romania	1.39	Russia	0.52	Ukraine	0.35	Romania	2.67

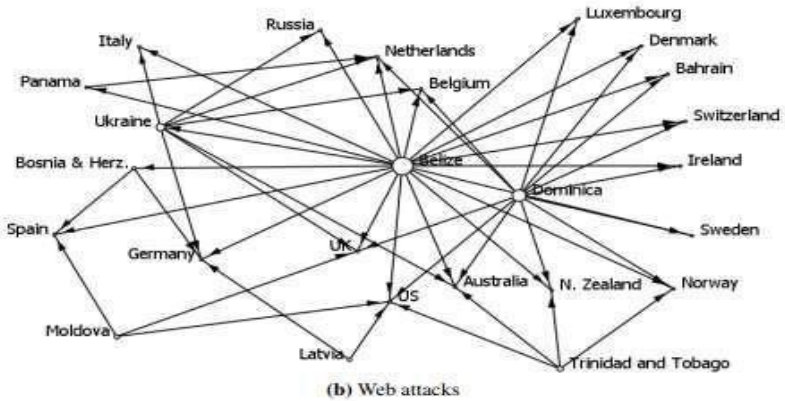
4. Attacks encountered per computer . Regional distribution



5. Cyber attack network



(a) Exploits



(b) Web attacks

.

PROBLEM STATEMENT AND OBJECTIVES :

1. ***From where the attackers hack our Virtual Machine ?***

By creating a Virtual machine and deactivating the Firewalls for the VM will make it exposed to the World. If an attacker tries to attack our VM, we get their IP Address using the failed RDP logs in our system.

We configure Custom Fields in Log Analytics workspace with the intend of mapping geo data in azure sentinel.

2. ***How to store that information ?***

By using Log data (PowerShell Transform log), A Log Analytics workspace is a unique environment for log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Each workspace has its own data repository and configuration but might combine data from multiple services.

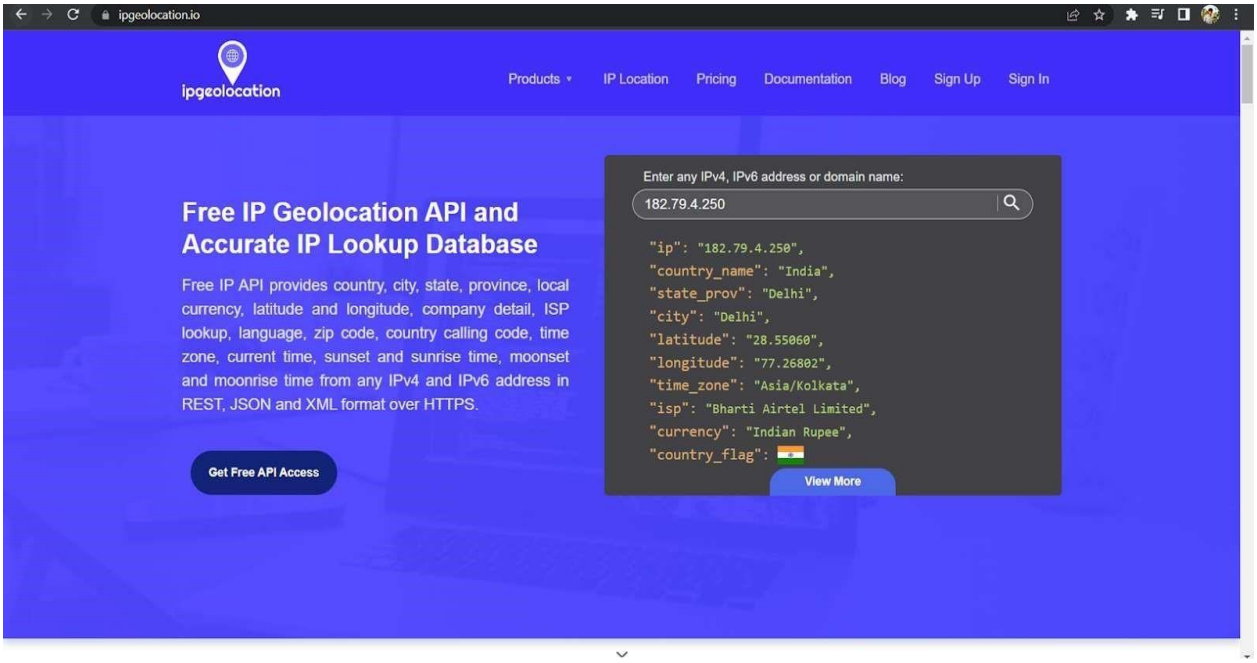
3. ***How to map the location of the IP addresses of the hackers ?***

Configure Azure sentinel (Microsoft's cloud SIEM) workbook to display attack data (RDP brute force) on the world map according to physical location and magnitude attacks.

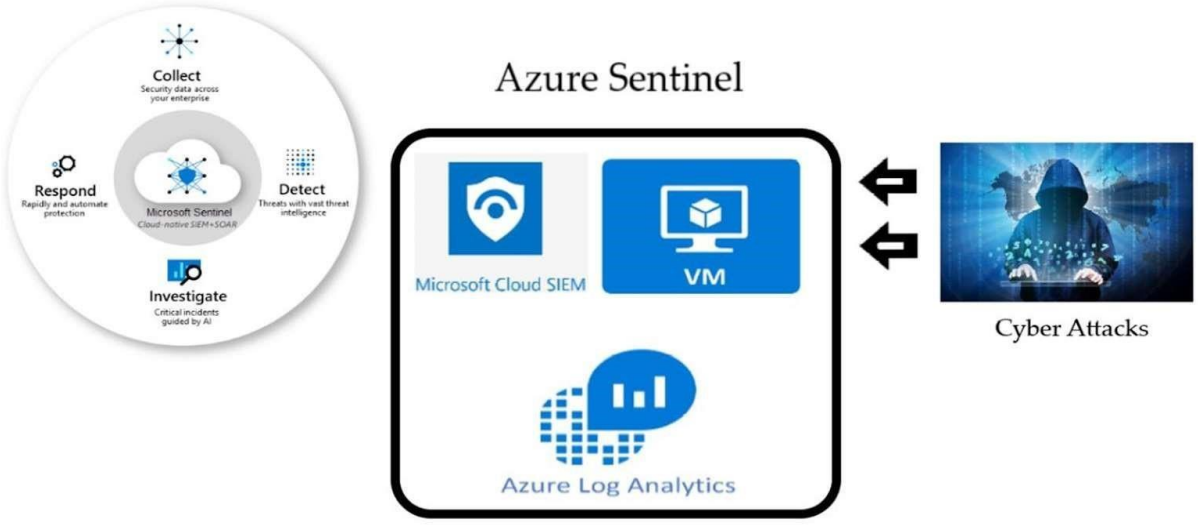
With Azure Event Hub you can stream Azure Monitor data to external SIEM (Security Information and Event Management) and monitoring tools, using its event ingestion and data streaming capabilities.

4. ***How to find the geographical location of the attacker ?***

The following is an example of a third party to derive the geographical data from the IP address.


ipgeolocation.io
ipgeolocation
Products
IP Location
Pricing
Documentation
Blog
Sign Up
Sign In
Free IP Geolocation API and Accurate IP Lookup Database
Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonset and moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.
Get Free API Access
Enter any IPv4, IPv6 address or domain name:
182.79.4.250
"ip": "182.79.4.250",
"country_name": "India",
"state_prov": "Delhi",
"city": "Delhi",
"latitude": "28.55060",
"longitude": "77.26802",
"time_zone": "Asia/Kolkata",
"isp": "Bharti Airtel Limited",
"currency": "Indian Rupee",
"country_flag":
View More

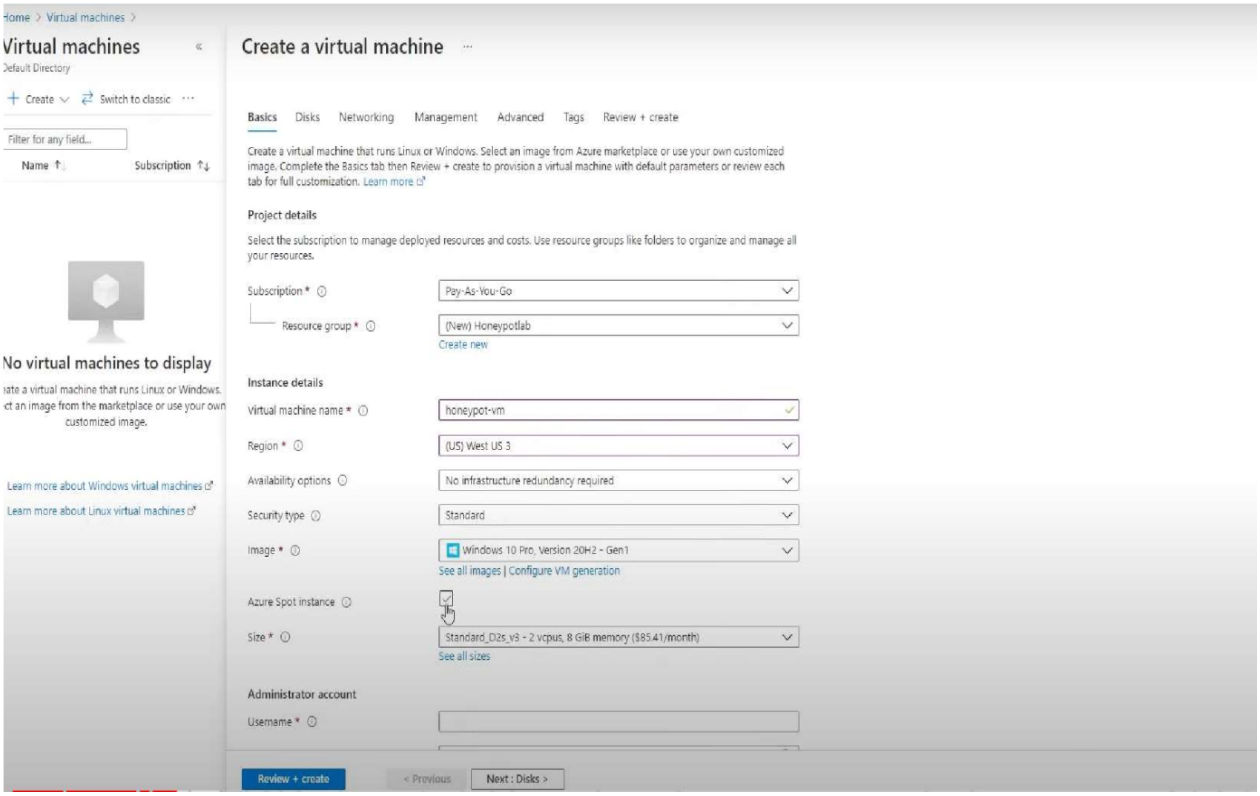
DESIGN :


Collect
Security data across your enterprise
Respond
Rapidly end automate protection
Microsoft Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI
Azure Sentinel
Microsoft Cloud SIEM
VM
Azure Log Analytics
Cyber Attacks

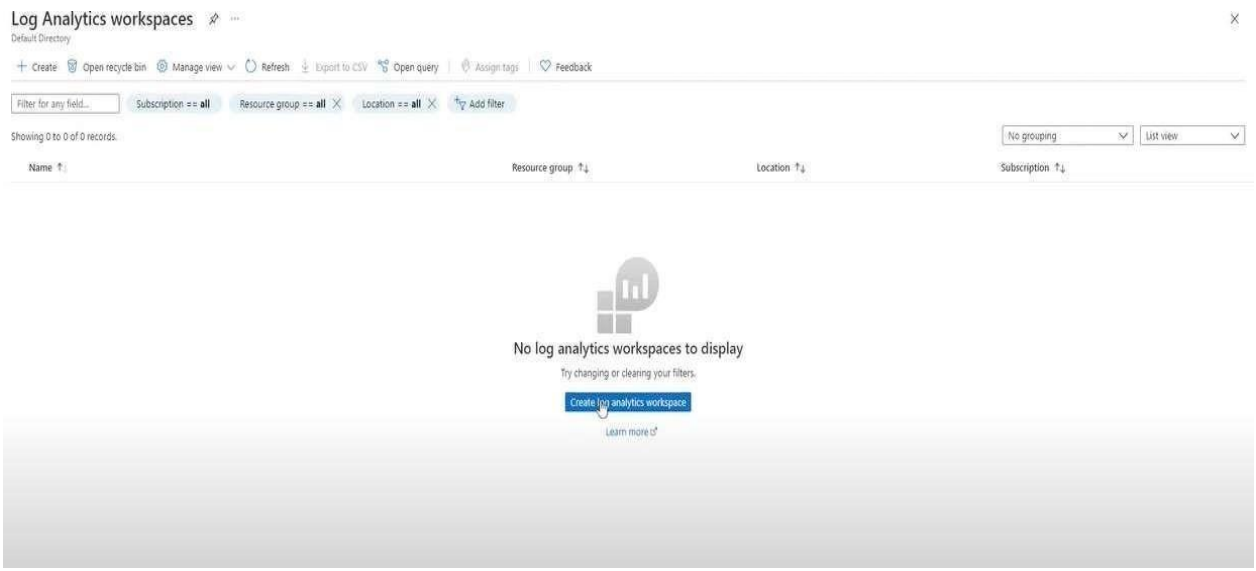
5. Implementation

RESULTS AND DISCUSSIONS:

- Creating a virtual machine



- Creating log analytic workspace

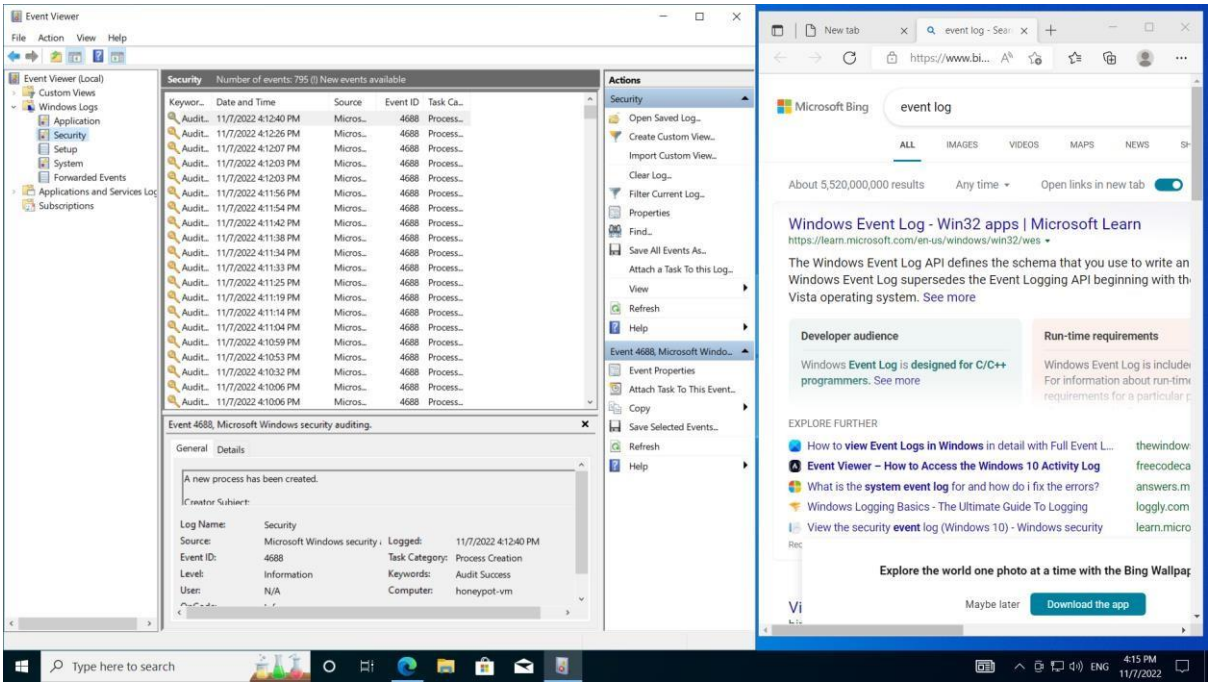


WINDOWS SECURITY AUDIT:

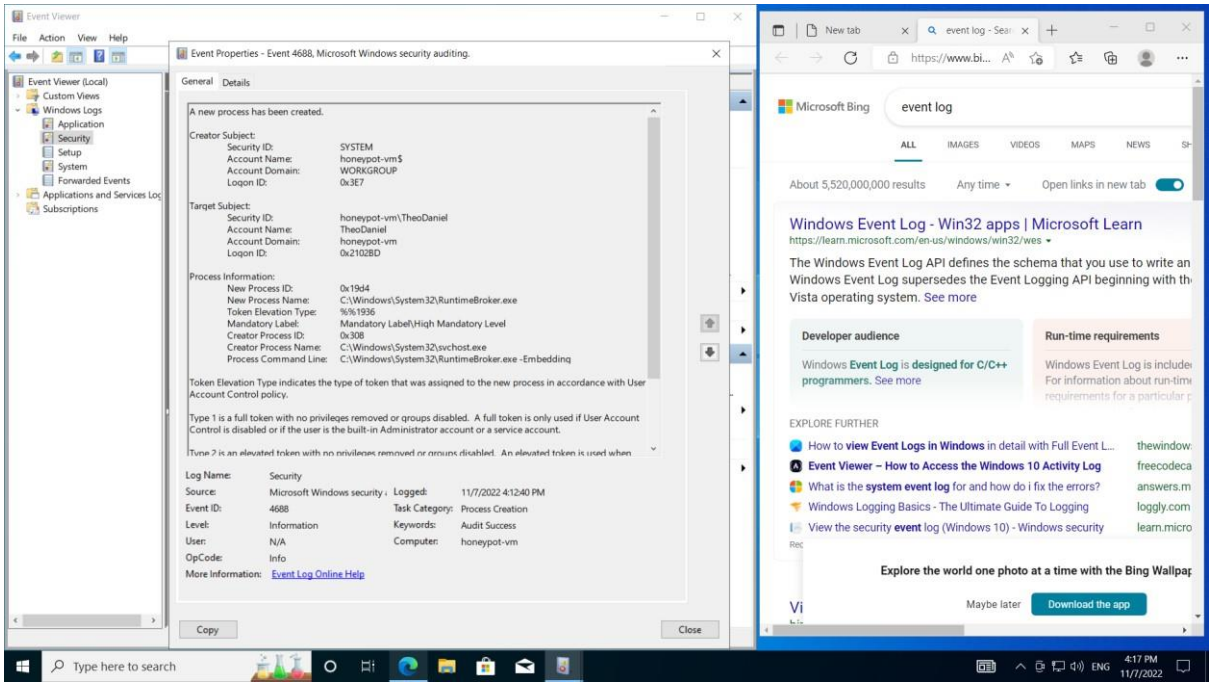
Windows security auditing is a Windows feature that helps to maintain the security on the computer and in corporate networks. Windows auditing is intended to monitor user activity, perform forensic analysis and incident investigation, and troubleshooting.

Windows security auditing lets you audit user logons and invalid logon attempts to your system. Windows generate these events not only when a user physically logons the system, but even when accessing a shared resource from a remote computer.

To log logon events run Local Security Policy. Open Local Policies branch and select Audit Policy. Double click on “Audit logon events” and enable Success and Failure options. After that, all user logons and invalid logon attempts will be logged to security event log.

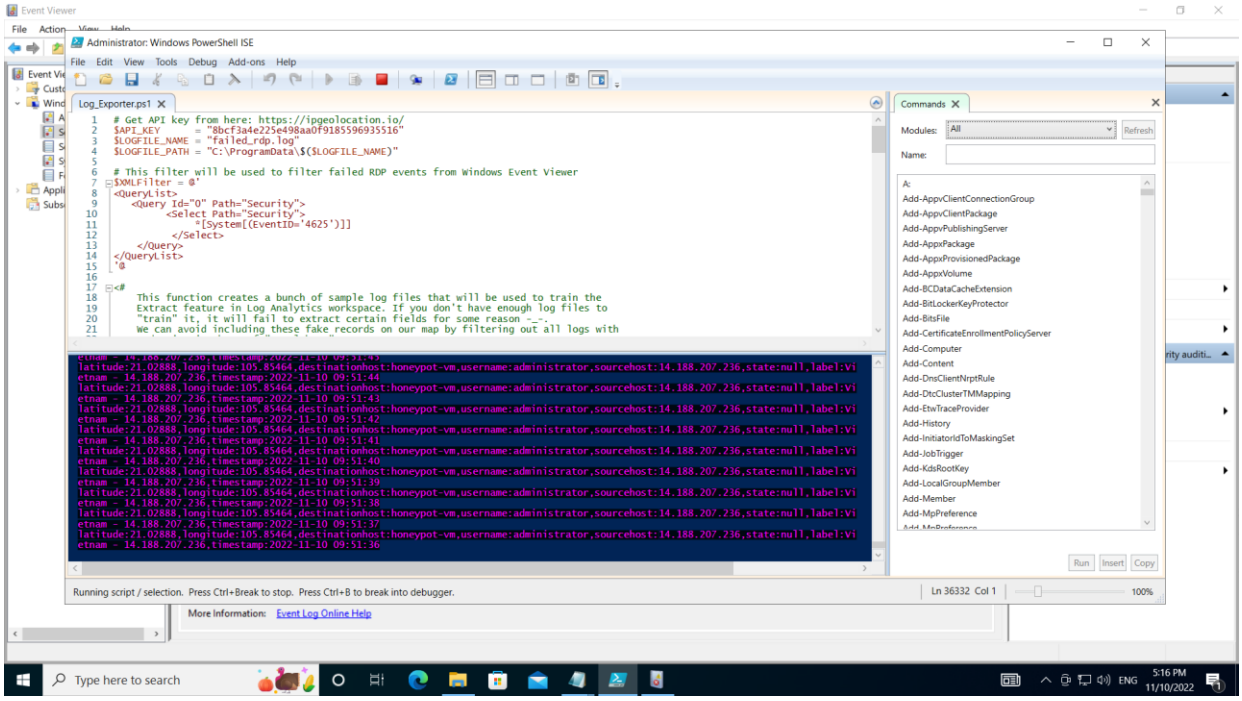


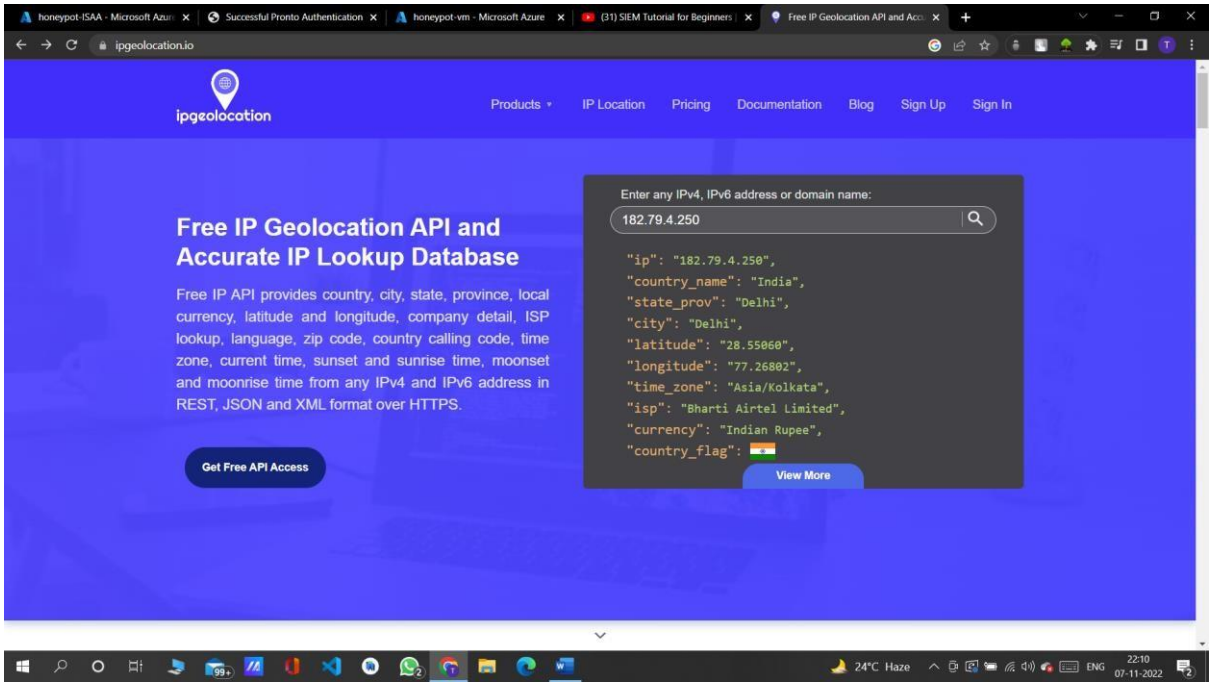
This is the Screenshot of the Audit user logon details which is saved in the Virtual Machine (Azure VM Windows). Open the software Event Viewer – Windows Logs- Security , User can able to see all logon details.



In the Network Information, the workstation Name, Source Network Address (which is IP Address) and Source Port are available in the Event viewer which we can use it to find the latitude and longitude of the User Location in the Real World.

Event ID	Event message
4624	An account was successfully logged on
4625	An account failed to log on
4648	A logon was attempted using explicit credentials
4675	SIDs were filtered
4656	A handle to an object was requested
4658	The handle to an object was closed
4660	An object was deleted
4663	An attempt was made to access an object
4685	The state of a transaction has changed
4985	The state of a transaction has changed





Code to Update Custom Security Log Exporter:

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY     = "d4600b4efdef42b39828f5155041a457"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
  <Query Id="0" Path="Security">
      <Select Path="Security">
          *[System[(EventID='4625')]]
       </Select>
   </Query>
</QueryList>
'@

<#
   This function creates a bunch of sample log files that will be used to train the
Extract feature in Log Analytics workspace. If you don't have enough log files to
"train" it, it will fail to extract certain fields for some reason -_-.
   We can avoid including these fake records on our map by filtering out all logs with
a destination host of "samplehost"
```

```
#>
Function write-Sample-Log() {
   "latitude:47.91542,longitude:-
120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washingt
on,country:United States,label:United States - 24.16.97.222,timestamp:2021-10-26 03:28:29" |
OutFile $LOGFILE_PATH -Append -Encoding utf8
   "latitude:-22.90906,longitude:-
47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao
Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:20" | Out-File
$LOGFILE_PATH -Append -Encoding utf8

"latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:8
9.248.165.74,state:North Holland,country:Netherlands,label:Netherlands -
89.248.165.74,timestamp:2021-10-26 06:12:56" | Out-File $LOGFILE_PATH -Append -Encoding utf8
   "latitude:40.71455,longitude:-
74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:N
ew York,country:United States,label:United States - 72.45.247.218,timestamp:2021-10-26 10:44:07"
| Out-File $LOGFILE_PATH -Append -Encoding utf8
   "latitude:33.99762,longitude:-
6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:RabatS
alé-Kénitra,country:Morocco,label:Morocco - 102.50.242.216,timestamp:2021-10-26 11:03:13" |
Out-File $LOGFILE_PATH -Append -Encoding utf8
   "latitude:-
5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,stat
e:Penang,country:Malaysia,label:Malaysia - 42.1.62.34,timestamp:2021-10-26 11:04:45" | Out-File
$LOGFILE_PATH -Append -Encoding utf8

"latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourceho
st:176.235.196.111,state:Istanbul,country:Turkey,label:Turkey -
176.235.196.111,timestamp:202110-26 11:50:47" | Out-File $LOGFILE_PATH -Append -Encoding utf8

"latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.25
1.67.98,state:null,country:Russia,label:Russia - 87.251.67.98,timestamp:2021-10-26 12:13:45" | Out-
File $LOGFILE_PATH -Append -Encoding utf8

"latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehos
t:20.86.161.127,state:North Holland,country:Netherlands,label:Netherlands -
20.86.161.127,timestamp:2021-10-26 12:33:46" | Out-File $LOGFILE_PATH -Append -Encoding utf8
   "latitude:17.49163,longitude:-
88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Bel
ize,label:Belize - 45.227.254.8,timestamp:2021-10-26 13:13:25" | Out-File $LOGFILE_PATH -Append
Encoding utf8    "latitude:-
55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,
state:Central Federal District,country:Russia,label:Russia - 94.232.47.130,timestamp:2021-10-26
14:25:33" | Out-File $LOGFILE_PATH -Append -Encoding utf8
}

# This block of code will create the log file if it doesn't already exist
```

```
if ((Test-Path $LOGFILE_PATH) -eq $false) {     New-
Item -ItemType File -Path $LOGFILE_PATH
   write-Sample-Log
}

# Infinite Loop that keeps checking the Event Viewer logs. while
($true)
{

   Start-Sleep -Seconds 1
   # This retrieves events from Windows EVent Viewer based on the filter
$events = Get-WinEvent -FilterXml $XMLFilter -ErrorAction SilentlyContinue     if
($Error) {
      #Write-Host "No Failed Logons found. Re-run script when a login has failed."
   }

   # Step through each event collected, get geolocation     #
for the IP Address, and add new events to the custom log
foreach ($event in $events) {


      # $event.properties[19] is the source IP address of the failed logon
      # This if-statement will proceed if the IP address exists (>= 5 is arbitrary, just saying if it's not
empty)
      if ($event.properties[19].Value.Length -ge 5) {

         # Pick out fields from the event. These will be inserted into our new custom log
         $timestamp = $event.TimeCreated
         $year = $event.TimeCreated.Year

         $month = $event.TimeCreated.Month
         if ("$($event.TimeCreated.Month)".Length -eq 1) {
            $month = "0$($event.TimeCreated.Month)"
         }

         $day = $event.TimeCreated.Day            if
("$($event.TimeCreated.Day)".Length -eq 1) {
            $day = "0$($event.TimeCreated.Day)"
         }

         $hour = $event.TimeCreated.Hour
         if ("$($event.TimeCreated.Hour)".Length -eq 1) {
            $hour = "0$($event.TimeCreated.Hour)"
         }

         $minute = $event.TimeCreated.Minute
         if ("$($event.TimeCreated.Minute)".Length -eq 1) {
            $minute = "0$($event.TimeCreated.Minute)"
```

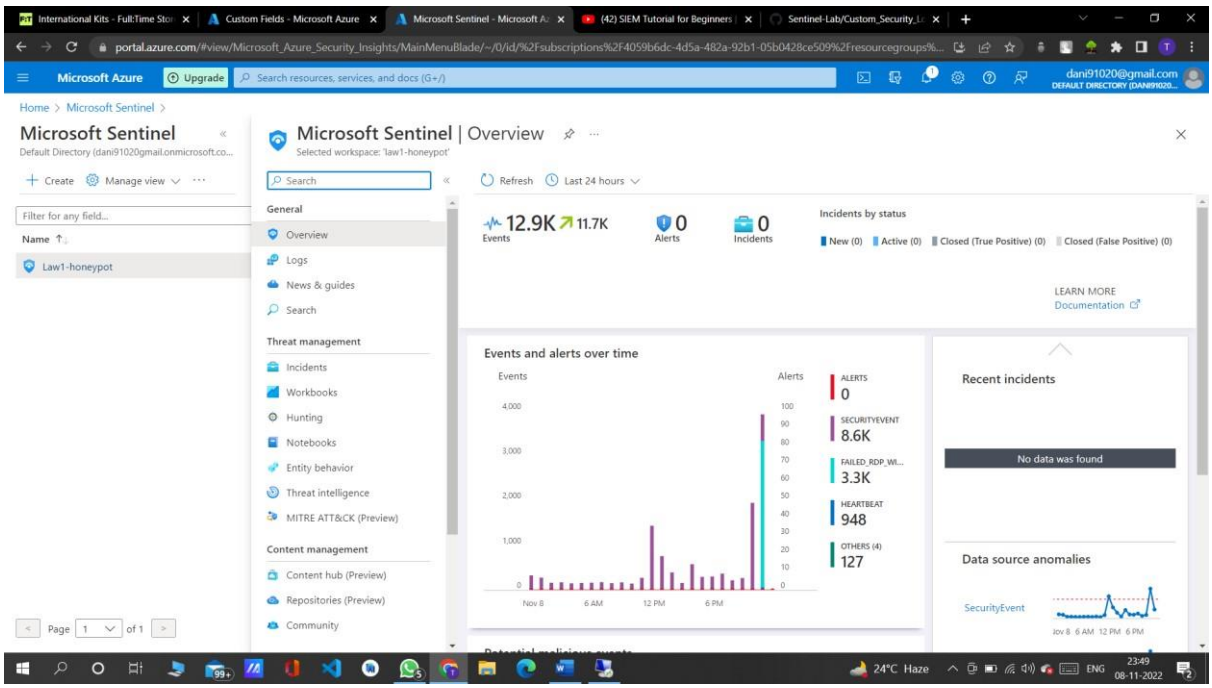
```
        }


        $second = $event.TimeCreated.Second
        if ("$($event.TimeCreated.Second)".Length -eq 1) {
           $second = "0$($event.TimeCreated.Second)"
        }

        $timestamp = "$($year)-$($month)-$($day) $($hour):$($minute):$($second)"
$eventId = $event.Id
        $destinationHost = $event.MachineName# Workstation Name (Destination)
        $username = $event.properties[5].Value # Account Name (Attempted Logon)
        $sourceHost = $event.properties[11].Value # Workstation Name (Source)
        $sourceIp = $event.properties[19].Value # IP Address

        # Get the current contents of the Log file!
        $log_contents = Get-Content -Path $LOGFILE_PATH

        # Do not write to the log file if the log already exists.
        if (-Not ($log_contents -match "$($timestamp)") -or ($log_contents.Length -eq 0)) {

           # Announce the gathering of geolocation data and pause for a second as to not rate-limit
the API
           #Write-Host "Getting Latitude and Longitude from IP Address and writing to log"
ForegroundColor Yellow -BackgroundColor Black
           Start-Sleep -Seconds 1

           # Make web request to the geolocation API
           # For more info: https://ipgeolocation.io/documentation/ip-geolocation-api.html
$API_ENDPOINT =
"https://api.ipgeolocation.io/ipgeo?apiKey=$($API_KEY)&ip=$($sourceIp)"
           $response = Invoke-WebRequest -UseBasicParsing -Uri $API_ENDPOINT

           # Pull Data from the API response, and store them in variables
           $responseData = $response.Content | ConvertFrom-Json
           $latitude = $responseData.latitude
           $longitude = $responseData.longitude
$state_prov = $responseData.state_prov              if
($state_prov -eq "") { $state_prov = "null" }
$country = $responseData.country_name               if
($country -eq "") {$country -eq "null"}

           # Write all gathered data to the custom log file. It will look something like this:
           #

"latitude:$($latitude),longitude:$($longitude),destinationhost:$($destinationHost),username:$($use
rname),sourcehost:$($sourceIp),state:$($state_prov),      country:$($country),label:$($country)      -
$($sourceIp),timestamp:$($timestamp)" | Out-File $LOGFILE_PATH -Append -Encoding utf8
```

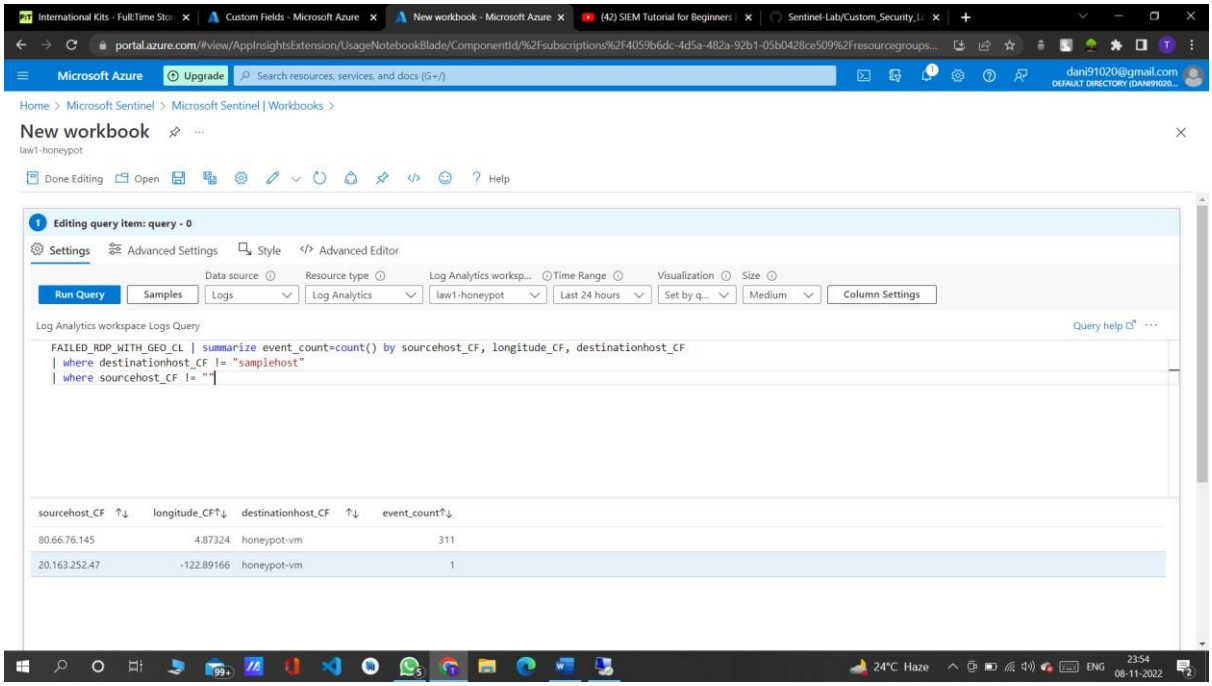
```
            Write-Host -BackgroundColor Black -ForegroundColor Magenta
"latitude:$($latitude),longitude:$($longitude),destinationhost:$($destinationHost),username:$($use
rname),sourcehost:$($sourceIp),state:$($state_prov),label:$($country) -
$($sourceIp),timestamp:$($timestamp)"
        }
else {
            # Entry already exists in custom log file. Do nothing, optionally, remove the # from the line
below for output
            # Write-Host "Event already exists in the custom log. Skipping." -ForegroundColor Gray
BackgroundColor Black
        }
      }
   }
}
```

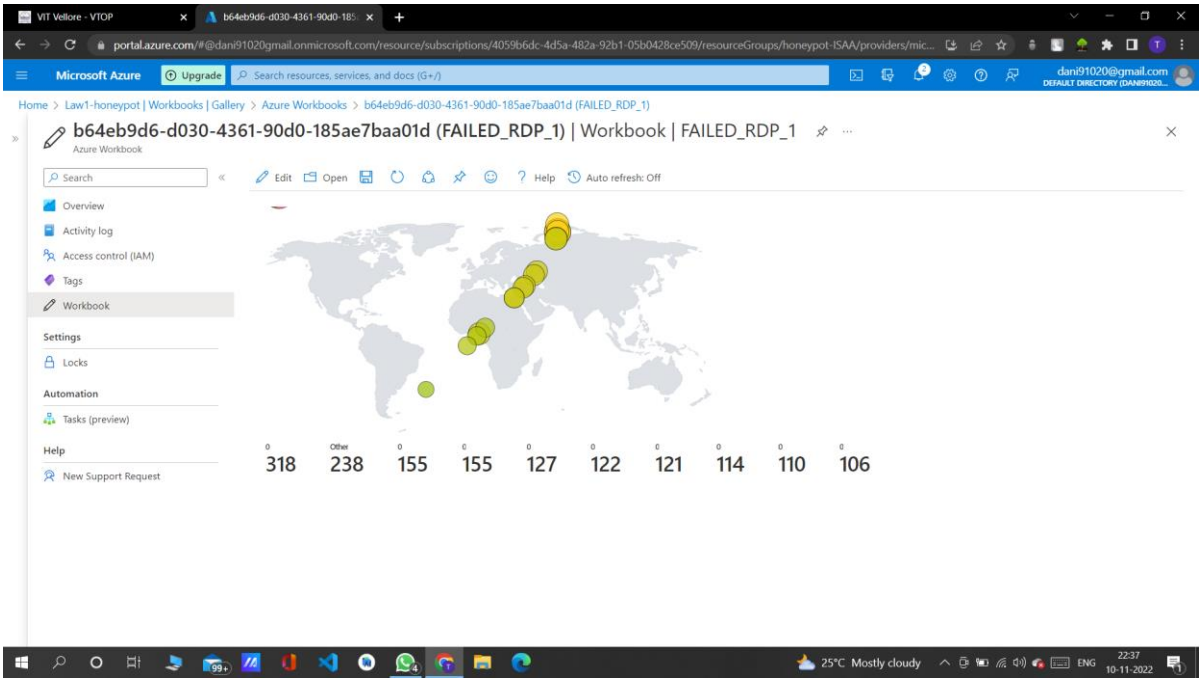
Microsoft Sentinel:

Microsoft Sentinel is a scalable, cloud-native solution which provides

- Security information and event management (SIEM)
- Security orchestration, automation and response (SOAR)




New workbook
law1-honeypot
Done Editing
Open
Help
Editing query item: query - 0
Settings
Advanced Settings
Style
Advanced Editor
Run Query
Samples
Data source
Logs
Resource type
Log Analytics
Log Analytics worksp...
law1-honeypot
Time Range
Last 24 hours
Visualization
Set by q...
Size
Medium
Column Settings
Log Analytics workspace Logs Query
Query help
FAILED_RDP_WITH_GEO_CL | summarize event_count=count() by sourcehost_CF, longitude_CF, destinationhost_CF
| where destinationhost_CF != "samplehost"
| where sourcehost_CF != ""
sourcehost_CF
longitude_CF
destinationhost_CF
event_count
80.66.76.145
4.87324
honeypot-vm
311
20.163.252.47
-122.89166
honeypot-vm
1


b64eb9d6-d030-4361-90d0-185ae7baa01d (FAILED_RDP_1) | Workbook | FAILED_RDP_1
Azure Workbook
Edit
Open
Help
Auto refresh: Off
Overview
Activity log
Access control (IAM)
Tags
Workbook
Settings
Locks
Automation
Tasks (preview)
Help
New Support Request
318
Other
238
155
155
127
122
121
114
110
106

Bibliography

[1] Yan, F., Gu, Y., Wang, Y., Wang, C., Hu, X., Peng, H., Yao, Z., Wang, Z. and Shen, Y., 2013. Study on the interaction mechanism between laser and rock during perforation. *Optics & Laser Technology*, *54*, pp.303-308.

[2] Akamai. Akamai's state of the internet report, Q1 2014.

[3] Alexa. The top 500 sites in each country or territory. www.alexa.com/topsites/countries, 2013. Last accessed: October 2013.

[4] M. Bailey, J. Oberheide, J. Anderen, Z. M. Mao, F. Jahanian, and J. Nezario. Automated classification and analysis of internet malware. In International Symposium on Research in Attacks, Instrusions and Defenses (RAID), September 2007.

[5] A. Vazão, L. Santos, M. B. Piedade and C. Rabadão, "SIEM Open Source Solutions: A Comparative Study," *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 2019, pp. 1-5, doi: 10.23919/CISTI.2019.8760980.

[6] González-Granadillo G, González-Zarzosa S, Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel). 2021 Jul 12;21(14):4759. doi: 10.3390/s21144759. PMID: 34300500; PMCID: PMC8309804.