International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 05 | May 2024 www.irjet.net p-ISSN: 2395-0072

Using Azure Sentinel (SIEM) to track live cyber threats via Honey pot.

Shivangi Gandhi[1], Dinesh Kamani[2], Sravan Gavara[3], K.S Ayush [4]

[1]*Assistant Professor, Dept. of computer science, Parul University, Gujarat, India*
[2345]*UG student, Dept. of computer science, Parul University, Gujarat, India*

Abstract – *Data theft is a big problem in current tech world as many cyber threats are increasing day to day. How and why these thefts are happening after having some many protections in this modern world. In this paper we will begin by going over how we created the essential resource group for the honeypot. After that, we will walk you through setting up a log analytics workspace and a virtual honeypot computer to collect data from the honeypot. After the data has been collected, we will walk you through configuring Sentinel to interact with the Log Analytics Workspace and retrieve the information. Subsequently, we will utilize the IP geolocation of the unsuccessful login attempts from all across the world to create a Sentinel dashboard.*

***Key Words*: sentinel, Log Analytics workspace, honeypot, IP geolocation**

1. INTRODUCTION

Using Microsoft's Azure platform, we will build up a lab for a honeypot in this project. We will also cover how to aggregate the data collected by the honeypot into Microsoft Sentinel a security information and event management (SIEM) application. A security tool called a honeypot is designed to entice and apprehend possible attackers by seeming to be a helpful network component. By putting up a honeypot lab on Azure, you can simulate a network environment and obtain insightful data about potential dangers and malicious activity. After the data has been collected, it can be sent to Microsoft Sentinel for analysis and storage. Sentinel is a cloud-based SIEM application that helps you monitor and manage security threats throughout your company.[1] The honeypot system records and tracks the movements of intruders within the system, sending the information to the system administrator and security staff who have deployed and set up the spyhole. The information gathered may be essential for establishing defenses against different kinds of attacks, particularly those that are more recent. The use of honeypots offers a practical way to improve a system's security and dependability and aids engineers, scientists, and researchers in developing a plan of defense against cyberattacks.[2] A honeypot is a security tool designed to be probed, attacked, or compromised. It was suggested that any interaction detected be automatically interpreted as malicious activity, and the administrator network uses the reports generated by the malicious source to ascertain the identity, reasons for the intrusion, and methods of the hacker.[3] A honeypot is akin to the wet cement used to find footprints in your home; you may use it to see if burglars are testing your home security by rattling your door locks.[4] Depending on the type of Honeypot system installed within infrastructure, its goal is to record any potential destructive action by an attacker. Honeypot systems can be used to detect several forms of malicious activity, including automated attacks by malicious bots, known vulnerability exploitation, web application attacks, and the exploitation of out-of-date software and systems.[5] Industrial control systems (ICT) are at much greater danger from cybersecurity threats in the last several years, mostly as a result of nation-states and cybercriminals becoming more active. Attackers are now more dangerous and skilled than ever, and it can be difficult to identify them in time for action.

1.1 Related Work

Before We configured Azure Sentinel (SIEM) and linked it to an operational virtual machine that acts as a honeypot in order to finish this project. The project comprises of an Azure Sentinel on SIEM framework Cyber Attacks map configure the Azure Log Analytics Workspace so that geographic data from custom logs can be imported. (country, state or province, latitude, and longitude). to map geodata in Azure Sentinel, Log Analytics Workspace custom fields were arranged. Configure the Azure Sentinel spreadsheet (Microsoft's SIEM) to display global attack data (RDP brute force) based on the precise location and scale of the strike on a global map.[1][2][3] Any honeypot system's primary goal is to detect intrusions and gain detailed knowledge about them. It may also involve mitigating attacks. One method for a handful of these can be accomplished by integrating the honeypot idea into IDS and IPS.[6] A honeynet is an assortment of different honeypots. These are unique networks designed to entice potential attackers. A honeynet's purpose is to gather data regarding malicious activity. The investigators subsequently examine this recorded data to obtain the pertinent information.[5] SIEMs may typically gather, compile, store, and correlate events produced by a managed infrastructure. As they collect events from various sensors (firewalls, intrusion detection systems, antivirus software, etc.), correlate these events, and provide synthetic views of the alerts for threat handling and security reporting, they serve as the foundation of contemporary security operations centers [4,5]. Aside from these essential features, the current systems differ greatly from one another, which typically reflects the various markets in which SIEMs are found.

1.2 Challenge

Typically, there are several ways to carry out a particular operation or launch an attack in the field of cyber security. It is crucial to determine the type of route that an intruder would have taken to complete the mission. Finding the potential entrances to the virtual machine was somewhat difficult for us. Or what are the chances that un authorized individuals were picked to compromise the VM's credentials

2. ANALYSIS

The below figure describes Setting tup the Azure Sentinel (SIEM) and connect it to a live virtual machine acting as a honey pot. We will observe live attacks (RDP Brute Force) from all around the world. We will use a custom PowerShell script to look up the attackers Geolocation information and plot it on the Azure sentinel Map.

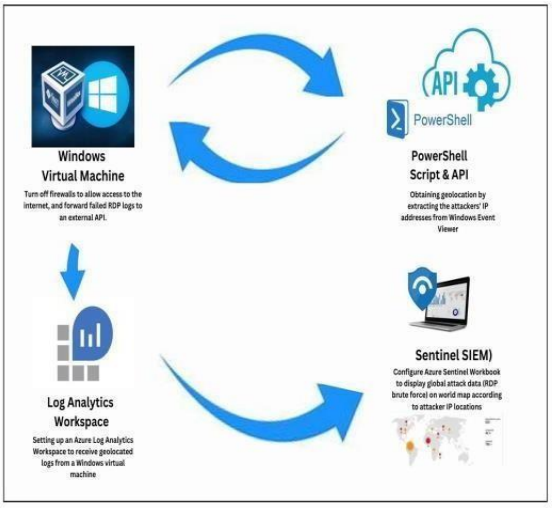

Fig -1: Flow

Now a days we are seeing so many cyber attackers are going to steal our data by entering in to our network we prevent this by using this project.

3. IMPLEMENTATION

Step 1: Create Azure Subscription It's easy to sign up for an Azure subscription; just visit **https://azure.microsoft.com** and start a free trial. I signed in after creating it to view the Azure Dashboard.

Step 2: The resource group enables the grouping of all the resources for this lab so that they all have the same lifecycle. Understanding this is crucial because, once the lab was finished, I would have to deactivate the resource group in order to stop the resources from billing me for services. In the Azure Dashboard, the resource group can be created separately or at the same time as the virtual machine. The formation of the Resource Group and the VM are depicted in the next graphic as occurring simultaneously.

Step 3: The next step was to disable the firewalls and design a special network security group that would make the virtual machine discoverable to hackers everywhere. By opening all the ports, this honeypot will be visible to attackers doing reconnaissance around the globe, leaving it vulnerable to attacks. They will then make several different attempts to hack the system from there. Most people will attempt Brute Force attacks. I'll be using those to gather more information from the attacks, such as the Latitude and Longitude depending on the IP, and more, since these attacks will result in a significant number of failed authentication audits.

Step 4: The virtual machine will take a while to deploy once it has been created. I'm going to be putting up the resource that will store those unsuccessful RDP logon attempts from the Brute force attacks throughout this period. A log analytics workspace is what this is. This resource will also let us to use Sentinel, which will build a spreadsheet that maps the information acquired using the logs in this workspace.

Step 5: After the VM was established, I had to turn on Defender for Cloud so that it could gather all of the VM's logs. The "All Events" collection was enabled in the Data Collection settings after I activated Defender for Cloud on the Log Analytics Workspace.

Step 6: Now all I had to do was click "Connect" after selecting the virtual machine from the list of workspace data sources in the virtual machine and connecting it to the log analytics workspace.

Step 7: I connected to the virtual machine using RDP and a strong password to begin collecting the live attacks. Then I had to set it up to gather the failed logon events from Event Viewer and gather the IP address, hostname, attempted username, and other information for each event. Also, I had to ask for the latitude and longitude data based on the IP address in order to get this data from each occurrence in real time. I accomplished this by making the following API queries to an IP geolocation provider

Step 8: Observe Event viewer Logs in VM. And Turn of Windows Firewall on VM.

Step 9: A PowerShell script written by us carried out the entire procedure by searching for Event 4625 (Audit Failure) in the Event Viewer logon event through an XML filter, then grabbing the necessary data. The exact same script would then make an API request based on the IP, obtain the returned values, and add them to a single line, comma-separated entry on a private log file.

Step 10: Get Geolocation.io API Key 13 Run Script To get Geo Data from attackers.

```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "4901c34bcbd548568f63aee31d90ca1b"
$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
```

Fig -2: API Key Used in power shell script

Step 11: I had to import the custom log into LAW after it had been established and was ready for connections to be made in order to save it and train LAW to separate the raw data into custom fields for processing. I imported them by selecting "make new custom log" from the "Custom Logs" tab in the LAW.

- You can provide a sample log when asked for one by providing a.txt or.log file containing sample entries produced by the Powershell log in the virtual machine.
- The following step displays some sample log entries after importation. I will choose the location of the custom log on the VM under "collection pathways" so that the LAW may access it in real-time and store it there. The location of my personal log, called failed rdp.log.

Step 12: I had to extract the data from the custom log consistently after it was imported into the LAW so that the LAW would know which sets of data matched which. For instance, I needed to quickly extract the Latitude and Longitude so that I could simply map this data on Sentinel using a Kusto-Query Language (KQL) query. The following screenshot illustrates the query returning all of the raw data collected into that custom log. I then picked the "Raw Data" column with the right mouse button and chose "New Custom Field"

- Although the extractions do not effect the entries retrospectively, in my instance I waited too long to construct the extractions for the custom fields, which resulted in some of the entries not being properly mapped. To fix this, I simply made a new custom log, inserted the identical sample, and extracted the data for latitude, longitude, etc. in the samemanner. Finally, I just copied the fresh entries from the old log into the new log so that the LAW could also extract those fields.

Step 13: Now that I had the Application importing, saving, and extracting the raw data from the custom log, the script writing the custom log, and the VM waiting for connections, I simply used all of those components to construct a Sentinel Worksheet that connected it all together. I made the spreadsheet in Sentinel, and then I started selecting everything to display the attacks on a map using KQL. Sentinel offers a variety of data visualization options, but for this lab I choose the Map visualization, which opens a rightsettingssidebar where custom fields may be entered to control how the data is mapped in realtime. Following are some illustrations of what that procedure entails: This KQL query was the last one that I used to summarize the information in the Sentinel worksheet

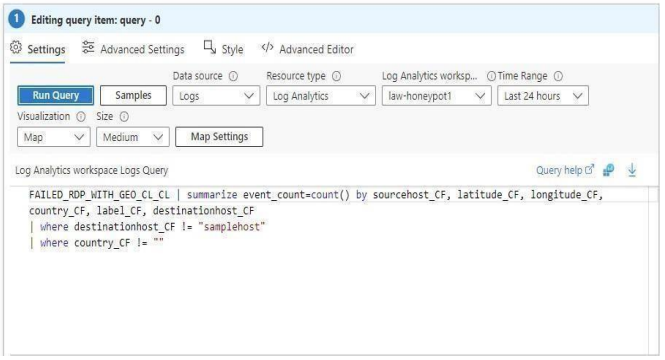

Fig -3: KQL query

4. OUTLOOK

The final check on the sentinel map looks like this:

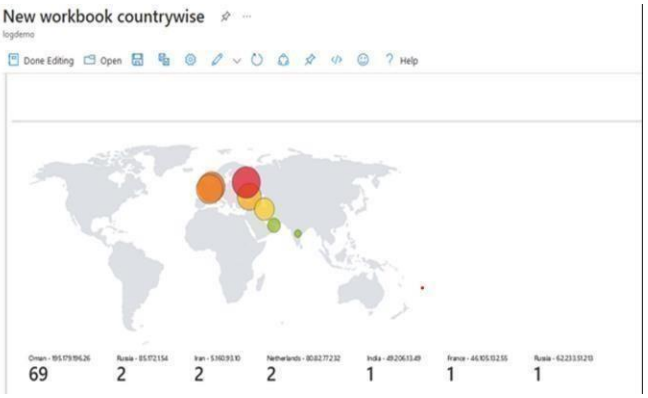

Fig -3: Azure sentinel world map

5. CONCLUSION

Security detections can still be improved dynamically with this knowledge. For example, workbooks can be set up to automatically activate specific defenses and adjust them in real time based on the amount of threats that Microsoft Sentinel's honeypot detects. For example, one may create a blacklist to block all connections from a specific IP address or a subset of IP addresses if they are persistently trying to break into the honeypot using brute force attacks.

The company would be protected against brute force and password spraying assaults because it would be hosting Businesses take action against these assailants. The IP could be taken off the network by the SIEM. blacklist should the attackers move to other resources using distinct IP addresses.

6. WORKING INFORMATION

1. What is Microsoft Azure Sentinel-SIEM: Microsoft Sentinel is a cloud-native security information And event management (SIEM) software that leverages artificial intelligence (AI) built-in to assist in quickly analyzing massive amounts of data across an organization. With Microsoft Sentinel, you can quickly analyze millions of records by combining data from many sources, such as users, servers, apps, devices, and apps that are hosted on-site or in the cloud. For simple onboarding of well-known security solutions, it has built-in connectors. With support for open standard formats like CEF and Syslog, you may get data from any source.

- **Collect** data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds
- **Detect** previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft
- **Investigate** threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft
- **Respond** to incidents rapidly with built-in orchestration and automation of common tasks

You can use Microsoft Sentinel for security event analysis in cloud and on-premises environments. Common use cases include:

- Visualization of log data
- Anomaly detection and alerting
- Investigation of security incidents
- Pro active threat hunting
- Automated response to security events

7. FUTURE WORK

All data, including entries made by unauthorized parties, can be sent. Triage all entries first, then send the highest-ranking government personnel, such as police departments or cybercrime authorities, the entries that pose the greatest risk and harm.

- Make sure you communicate all relevant information to higher authorities in accordance with the level of danger.
- One can also use this project to get expertise in the SIEM field or log events triage analysis.

REFERENCES

[1] Praful Nair, Vishak Nair, Karan Nair, Prof. K.S Charumathi (2020). Implementation of Honeypot to Trap and Track Cyber Attacks ((IRJET), Volume: 07, Issue: 11.

[2] Nadiya El Kamel, Mohamed Eddabbah, Youssef Lmoumen, and Raja Touahni (2020). A Smart Agent Design for Cyber Security Based on Honeypot and Machine Learning (WILEY, HINDAWI), Volume 2020, Article ID 8865474.

[3] C. MooreA. Al-NemratC. MooreA. Al-Nemrat (1January 2015).An Analysis of Honeypot Programs and the Attack Data Collected(Springer International Publishing),Available at https://core.ac.uk/reader/219374523.

[4] Rahul koul, J. W. Bakal, Sahil Dhar (July- 2017) Modern Attack Detection Using Intelligent Honeypot (IRJET), Volume: 04 Issue: 07.

[5] Gustavo Gonzalez-Granadillo, Susana Gonz ´ alez-Zarzosa and Rodrigo Diaz(12 July ´ 2021).Security Information and Event Management (SIEM): Analysis, Trends, and Critical Infrastructures(MDPI),Sensors 2021, 21, 4759. available at https://www.mdpi.com/1424- 8220/21/14/4759.

[6] Abhishek Mairh, Debabrat Barik, Kanchan Verma, Debasish Jena(January 2011).Honeypot in network security: A survey (researchgate.net), DOI:10.1145/1947940.19480 Available https://dl.acm.org/doi/10.1145/1947940.1948065.

[7] Manikandan K, Shambhavi Rai(February 15 2020). A Review on Honeypots (IRJET), Volume: 07 Issue: 01Avaliable https://www.slideshare.net/irjetjournal/irjet-a-review- on- honeypot

[8] Maitri Shukla, 2Pranav Verma, 1 ME Research Scholar, Assistant Professor 1Department of Computer Engineering SOCET, Ahmedabad, India. Honeypot: Concepts, Types and Working . Available at IJEDR1504100.pdf.

BIOGRAPHIES

Shivangi Gandhi
Assistant professor
School of computer science
Parul University

Venkata Dinesh Kamani
Student
School of computer science
Specialized in cyber security
Parul University

Srinivashan Ayush Kalapaurical
Student
School of computer science
Specialized in cyber security
Parul University

Sravan Kumar Gavara
Student
School of computer science
Specialized in cyber security
Parul University