Security Information and Event Management(SIEM) by Azure Sentinel

Vineeth Mathangi,

B00828528 ,

Mathangi-V@ulster.ac.uk,

MSc Internet of things,

The University of Ulster,

Jordanstown.

***Abstract*—Cybersecurity has become one of the major challenges in the modern world because of its complexity in technology and political practices. Organizations understand and recognize the security Attacks, threats, and vulnerabilities before attackers mess -up business strategies. The state-of-the-art in handling diverse data sources for security analysis is Security Information and Event Management (SIEM). It offers real-time analysis and monitoring of the log events and tracking and securing the data for compliance and the purpose of auditing. This paper investigates the failed authentication of log events with the help of Azure Sentinel, a SIEM tool, and by setting up an active Virtual machine that acts as a honeypot, capturing the live attacks, specifically called RDP brute-force, will be monitored the attackers across the world. Moreover, using a third-party API will capture the geolocation of hackers within windows PowerShell ISE and then later extract it to Azure Sentinel. Using machine learning techniques makes decisions as per the collected data.**

Keywords— Microsoft Azure, virtual machine(honeypot), Log Analytics workspace, Microsoft cloud defender, event viewer, windows PowerShell ISE, IP Geolocation API, Azure Sentinel., Jupyter notebook, Machine learning -KNN.

I. Introduction

At present, organizations and banking websites are considered at high risk, and overall security has become a major concern around the world as both are dealing with users'
personal data, secured accounts, transaction histories as well as card details. However, due to the increase of users or customers, it has become a significant issue in these several years. For instance, around 25 million people all over the United Kingdom opted to use e-banking and other electronic resources. So, the authentication mechanism plays an essential role in financial services and organizations it uses to identify the user's identity [2]. Here comes the interesting part, Authentication vulnerabilities are kind of minor issues that are understandable, but they carry the most critical relationship between security and authentication. However, Vulnerabilities can act as a gateway and allow the attackers to access customers' sensitive data. They can completely take over the entire application heads to internal infrastructure, putting the organization or the governance at risk. For example, back then 1940's to present many things evolve simultaneously. As cybersecurity and the other emerging technologies have evolved, do criminals and 'bad actors' come into action. So, securing and monitoring the sensitive data is essential with the help of security information, and event manager and the next generation SIEM is (UEBA) User Entity Behavioral Analytics technology makes it possible to detect insider threats, perform more sophisticated threat hunting, prevent data exfiltration, and mitigate IoT threats, even when traditional security tools don't raise a single alert [3]

Today's SIEM deployments are primarily concerned with using correlation rules to generate ad-hoc data collectors and compromise indicators. On the other side, making it difficult for employees to keep up with massive amounts of data might lead to unforeseen vulnerability issues. Despite major technological advancements, SIEM is strongly reliant on various cognitive human processes because setting up well-crafted indications requires a high level of threat expertise from subject experts. The value of human analysts in creating accurate computer definitions is well acknowledged.[4] in short, the focus of SIEM is on security-related incidents and events, such as succeeded or failed logins, malware activities, or escalation of privileges.

This research paper strongly investigates the failed RDP brute forces by involving the cloud platform Microsoft Azure and creating the honeypot (Virtual Machine), a network-attached system used as a proper trap for cyber-attackers detect and study the tricks. Detecting failed log events on the servers of Azure will trigger an alert by creating a log analytics workspace with the query in the Azure sentinel. Moreover, this incident will automatically trigger an alert to the SOC's (security operation center) team.[5]

II. Existing Work

Nowadays, a business organization may produce millions of data points regarding events quickly since it thrives on producing value through events like sales, client, and marketing support. Whenever an event occurs, there will be a specific space for logging the events. However, Logs are like a helping hand to the information systems value chain. For instance, managerial account ting, financial support, and users' data are completely dependent upon logging all economic events of the entity and producing the audit trail process to provide essential support for the guarantee of events and their consequences.

Examination *:*

The analysis should consider the log source and the logged field entries and their consequence in terms of threat detection. A tough-level examination of log source threat detection versus volumes value is discussed in a detailed analysis.

Firewall traffic: *Volume*: Well, an organization may produce around 20 GB -30 GB firewall logs each day with approximately 1000 end-users; log data can be collected in

source IP, destination IP, traffic, Timestamp, firewall(interfaces), firewall rules, and users.

Threat detection: mostly malicious actors disturb the cages of the internet for probing vulnerabilities all the time. paired with dynamic IP address assignment, it provides a situation where several hit matches from known malicious IPs can be expected to be incoming.

Windows security events:
Volume: The volume is completely dependent upon the business or organization's requirement, whereas collecting data for user identity governance and the required logs may vary. Moreover, data can be collected in the form of user sign-in and sign-outs, user disabled-enabled, password changes, group creation, user creation, file access audit, etc.,

Threat detection: typical alert rules are pattern matching, Anomalous user logins, brute force attacks (password spraying), user creation, activation of disabled users, and suspicious processes. However, we can optimize by filtering the collected security events, the configuration of logging policies (via group policies), filtering the connector level, and filtering at the SIEM solution – level.

Windows Security Event logs detection process is typically intersecting with the detections provided by the EDR (Endpoint Detection & Response) solutions where an organization can disable the logging process created on windows server Azure Defender . Servers is being deployed and is now covering potential harmful actions based on process monitoring.

Disabling the process creation audit could result in a 50 -70 percent increase in the number of Windows Security event logs. Compensating controls, in many circumstances, provide better detection alerts and are updated more regularly by the solution vendor.

Case-study: Basically, log analytics/collection are usually found in smaller companies with a limited security budget or larger organizations with a raw log collection infrastructure in place but need to add advanced security analytics capabilities. And for new deployment security value of each type of log source should be evaluated, and the ingestion of raw logs into the new SIEM must be prioritized based on cost. Let's discuss a case -study based on business considerations on SIEM [6]

. unexpectedly, a suspicious attack was launched against the organization shortly after it was mounted, and as a result, a massive amount of unexpected log volumes was significantly increased. There have been instances when some users in azure sentinel have been subjected to suspicious attacks and implemented mitigation procedures. . however, suspicious hackers run a wide ranging scan from a large number of remote hosts against the customer's public Ip addresses, whereas the scan may hit the user firewall by activating the massive number of denials in the logs and the firewall logs are sent to the azure sentinel (SIEM) . causes a significant increase in log ingestions. As a result, cost increases in Azure.[7]

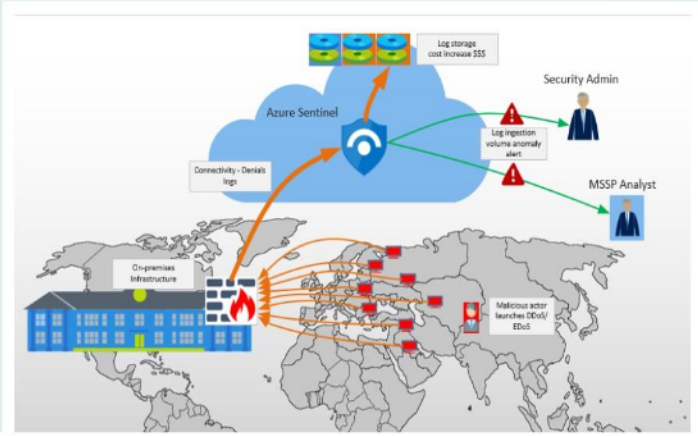


Figure 1: Illustrates the attack that causes log ingestion.

III. Methodology

computing, in simple terms, provides a wide range of services such as storage, databases, networking, software, tools, analytics, servers, virtual machines, and bits of intelligence over the internet to enable user-friendly innovation and more flexible resources.

Microsoft Azure: Azure is a well-known service for cloud computing and a web resources platform that allows operators to retrieve and manage the cloud services and other technologies. In addition, these essential services involve altering the database and storage depending on users' requirements, and it offers around 100+ cloud computing services,80 percent of fortune for customers' needs. secondly, Azure is compatible with programming languages such as java, python, Node-Js, and C. Finally, Azure offers over 54 data centers worldwide.[8]

Honeypot (Virtual Machine): It is a trick for trapping the suspicious hackers and discovering the attacks in which the intrusion information is made available. On the other hand, deception is a practical method and the core principle of honeypots. These technologies might give attackers the impression that they are fighting with a live and real system by delivering defensive and misleading methods.[9]

Microsoft defender cloud: Cloud defender is a tool that protects from threats and security posture management. It strengthens the security of the resources in the cloud. moreover, it is integrated with defender plans, protects workload, hardens the resources, tracks your security posture, protects against cyber-attacks.[10]
Log analytics workspace: In Azure portal analytics, a workspace is a tool that allows us to edit and run the queries log using Azure monitor logs data and interactively examine the logs .in. In additionIn addition, queries are used to find the stored data records that fit specific criteria, analyzeatterns, a, and provideifferent kindskindsf data insights.[11]

Event viewer: It records all the events in the system and stores them. The windows log has Application, security, setup, system, and forward events. We focus on security Audit failures which store the failed login attempts in windows.[12]

Windows PowerShell ISE: Windows power shell ISE is an editor for PowerShell that gives graphical UI (user interface). On the other hand, ISE (Integrated Scripting Environment) is a graphical UI that runs the command, testing, writing, and debugging the scripts without typing all the commands in the command line. Using the IP Geolocation (a third party), the API key will run the scripting to detect the geolocation (latitude and longitude) of malicious actors throughout the world.[13].

Figure 2 :shows the complete architecture of Azure.

The above figure represents the architecture of Infrastructure monitoring.
In short, identifying risks and their potential may impact the business. Whether a compromised entity or a malicious insider, the organization has always been a time-consuming procedure. However, examining through warnings and active hunting puts a lot of effort and time spent with little payoff and the risk of sophisticated threats slipping past detection. But Microsoft sentinel alleviates the analysts' workloads' ambiguity and drudgery by providing actionable intelligence and high fidelity and allows them to focus and repair. All the failed logs data and alerts such as users, source host, latitude, and longitude are pushed away to the analytics workspace called Raw data ingestion. The workspace sentinel can thoroughly identify the strange activities and helps to determine that any assets are compromised. Moreover, the sentinel can effectively proceed with the investigation, hunting, and Entity behaviors with the information.

Risk Factor: Considering the valuable resources, always risk securing the most sensitive data of taken credentials, insider threats, and external threats. Internal threats: Cybersecurity risks arise from within the organization to cause harm. However, based on the most common incidents has been discovered that misuse of powers granted to firms is trusted employees. External threats: adversaries attempting to get inside the organization illegally to control or steal the sensitive data are clearly named external threats, and attackers mostly use viruses and malware to steal the information.

from the beginning, by creating a free trial account in Microsoft Azure which allows us to utilize the tools and technologies . in this research process, several tools were used, such as Virtual Machines, log analytics workspace, Microsoft defender cloud, and Microsoft Sentinel .firstly, create a new resource called (Honeypot-lab)virtual machine. Generally, Virtual machines are used to host applications and manage the typical tasks correlated to the servers. Moreover, by deploying the Windows OS environment, we will test the failed login activities. Secondly, the same procedure search for the log analytics and create a workspace by setting all the regions and advanced features associated with VMs. The next procedure is by enabling the Microsoft cloud defender used to track the security posture, harden the resources, and protect against cyber-attacks. Defender for the cloud has three major roles that manage their workloads and resources: Defend, secure, and continuously assess. However, defender is securing the resources by its default, and it helps to push the logs from VM to the analytics workspace. Finally, Microsoft sentinel, a SIEM tool, delivers intelligent security analytics and threat intelligence and provides a single solution for attack detection, threat visibility, proactive hunting, and entity behavior.

The interesting part begins by copying the honeypot -VM (virtual machine) Ip address (51.143.103.103), pasting it into the Remote desktop, and hitting the connect. Then automatically honeypot connects to the remote environment. However, before connecting desktop asks for a username and password, which is created in the Virtual machine, but before successful log in, fail to log in and attempt to test the environment. For example, I have generated a username as a project and some random password that is genuine, but for the testing audit failure purpose entered the wrong username called 'ulster .'It instantly generates the audit failure in the security events. The following figure illustrates the logon failed attempt.

Figure 3 :testbed by using wrong credential.

So, for testbed purposes, the credentials that we used did work. Later by logging in with suitable authentication, can operate a remote desktop. A further step is open Event viewer helps scan the text log files and aggregate them, and it acts as a database reporting programmer. However, our aim to analyze the security events, also called 'audits, 'shows the action of security results either can be failed or the successful based on the user or adversaries trying to get inside. All the audits are being pushed to windows PowerShell ISE with support of a third-party (IP Geolocation) API key to grab all the logs and geolocations of the attackers or the users. But windows firewall acts as a defender to the audits for pushing

the third-party applications. To get geo information firewall must turn off. The next procedure is to create a new script in ISE, paste the copied from GITHUB resources, grab the personal API key provided by the IP Geolocation application, and then run the script. ISE collects all the audit failure information to the security events then all the collected live data is split into a text file called "Failed_RDP ."The example log files in the unsuccessful RDP log are used to train the Extract feature in the workspace we've created. However, due to the failed login attempt, I have addressed the geolocation of the wrong username (ulster) credentials shown below with latitude, longitude, username, and the source host (I\P address), and country.

"latitude:54.61002, longitude: -5.90277, destination host: honeypot-vm , username :ulster ,sourcehost:51.143.103.103,state:Northern Ireland, country: United Kingdom , timestamp:2022-04-25 14:40:33 ".

Well, from analytics workspace created a custom log to select the collection of paths which pushes all the captured data from the virtual machine(honeypot) to the log analytics workspace.

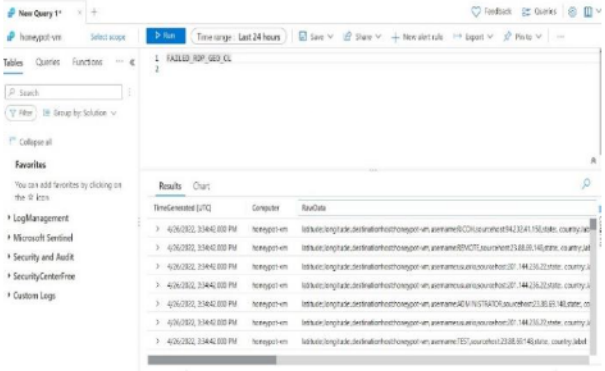


Figure 4 : running query on workspace.

The above picture illustrates the outcome of raw data ingested after performing the query with the name 'FAILED RDP GEO .'It has captured the end-to-end audit success and failures. On the other hand, Workspace simply collects raw data and not the extracted data, which is broken into latitude, longitude, source host, country, timestamp, and label.

Now, create a custom field where log analytics need to understand which sort of data value must pop up. The second step is to verify the precise field that needs to be extracted. For example, below figure shows the extraction of longitude by verifying the data whether all belong to longitude or not. And if any extracts initially are not correct, then need to rectify and edit by using the modification column.

Custom field name	Table name	Field type
country_CF	FAILED_RDP_GEO_CL	Text
destinationhost_CF	FAILED_RDP_GEO_CL	Text
label_CF	FAILED_RDP_GEO_CL	Text
latitude_CF	FAILED_RDP_GEO_CL	Text
longitude_CF	FAILED_RDP_GEO_CL	Text
sourcehost_CF	FAILED_RDP_GEO_CL	Text
state_CF	FAILED_RDP_GEO_CL	Text
timestamp_CF	FAILED_RDP_GEO_CL	Text
username_CF	FAILED_RDP_GEO_CL	Text

Figure 5: demonstrates how fields in analytics are made.

Figure 6: show the extraction of longitude

Overall, the Custom field accepts only collected data after the extraction of fields created, as records match the specified criteria that are added to the Analytics workspace. However, after extracting fields, only live log data can be monitored or stored. A strong investigation has been made in hunting by sentinel, whereas it proactively identifies the behavior of threats and entities by using queries.

Lastly, by capturing all the normalized data exported into a CSV file to perform a better prediction analysis, I have used a few techniques such as KNN and Naïve Bayes.

IV. RESULTS

The project aims to capture the live attacks, investigation, Entity-behaviors, and geolocation of all the failed RDP. Moreover, some prediction analysis has been used based on the collected events(data). The required data has been divided into visualization, investigation, and prediction.

By the results of geodata, sentinel has the workbook, which allows getting precise visualization after building the query.

Figure 7: mapping of geodata.

So manually, after refreshing the Power Shell ISE, data has directly driven into Sentinel mapping visualization and allows all the coordinates of the attackers all over the world. So they are easily detectable. Overall, 2 hours of live attacks mapping tells each event occurs in a different location with different IP addresses. Russia is with the greater number of log events, approximately 5k, in that monitored with three different Ip addresses such as 2.13k(events) - 94.232.41.158(IP), 1.09k (Events)– 45.141.84.54(IP), and 760(Events) – 87.251.67.98(IP). However, Hong Kong has

found the lowest number of events, and can accurately say this country has fewer adversaries.

Hunting: when security appliances and numerous systems generate massive data that can be hard to filter and capture the meaning of full events and look proactively for suspicious characters, hunting is a powerful tool for security threats that protect the organization. Hunting helps us find out the threat actor's next move so that defenders can protect their organization as a wall.

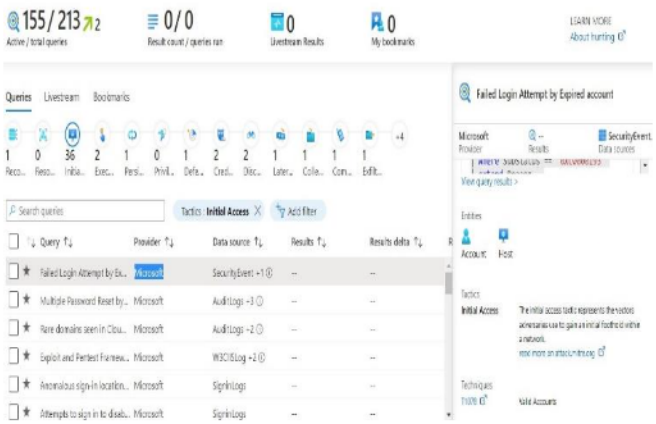


Figure 8:hunting the initial access.

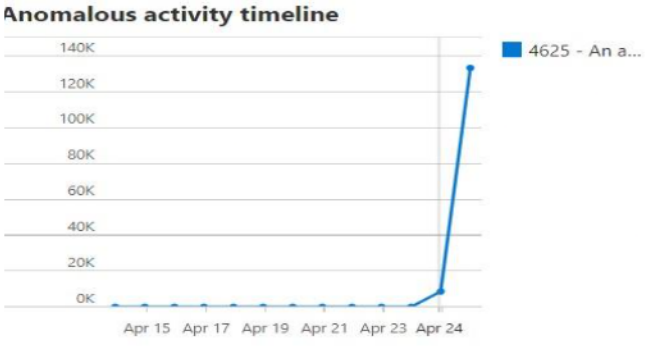
The above figure evident that from all the events, only 155 are active queries out of 213 queries. The initial access tactics refer to the various entry of vectors used to gain control over a network. After running an inbuilt query, entities are Account and Host, which means attackers are trying to gain access from a random account as a valid account through a virtual machine. In addition, the T1078 (Valid accounts) technique says that adversaries from existing accounts attackers may obtain and use credentials to gain initial access or Defense Evasion. For instance, the credentials which the attackers use may no longer be part of a particular organization, and by using these authentications, they pretend to be the original account of the user.

Anomalous Activity: Many audit logs contain numerous entries considered a related sequence activity or a session.

Activity	expectedCount	actualCount	anomalyScore
4625 - An account failed to log on.	1,363.41	133,388	176.55
4634 - An account was logged off.	4.61	122	45.26
4798 - A user's local group membership was enumerated.	10.02	204	34.06
8002 - A process was allowed to run.	257.09	5,178	33.67
4688 - A new process has been created.	274.27	5,244	31.79
4647 - User initiated logoff.	0.16	3	31.31
4696 - A primary token was assigned to process.	0.16	3	31.31

Figure 9:All the generated ID's

Each audit activity contains a specific code that defines the usual behavior. For example, 4625 – is a failed login attempt, and 4624 – is an account log-off. However, we aim to detect the failed ones. As per the Anomalous activity timeline 4625 – log off events takes place with the highest number of entries anomaly score is around 176.55.



Investigation: An incident is completely based on an analytics rule created in the workspace for a specific investigationpace. Sentinel helps to detect the behavior and threats that can investigate

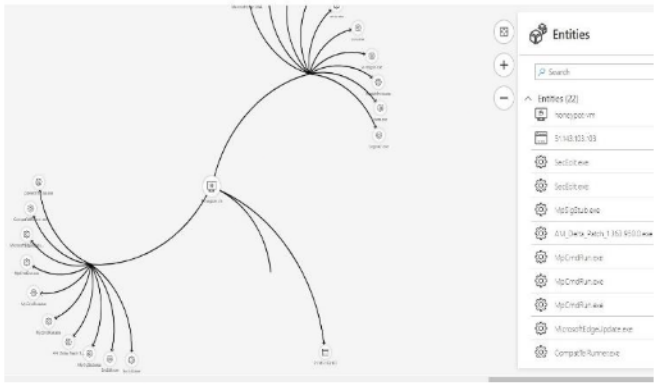


Figure 10 :Investigation procedure.

As per the method entity graph of investigation, several entities take place, such as host (51.143.103.103) and process execution events tracer. Let's discuss tracelog.exe (trace logs). These logs produce an event; each contains trace messages during the sessions. Overall, the investigation graph helps to understand the scope of the threat and the cause by correlating the relevant data with any other involved entities.

Security Events & Alerts: The captured security events are around 145.1k in 24 hours of live events. The figure describes respective time events with alert.

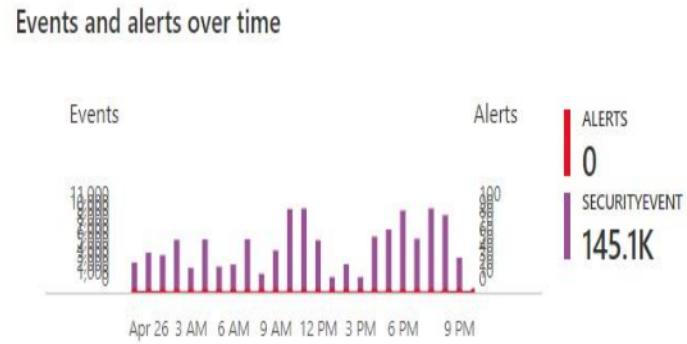


Figure 11 :Overall events and alerts

Alert description: Although none of them succeeded, some of them used accounts recognized by the host. it resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords to find valid credentials to access the host. it indicates that some of your host account names might exist in a well-known account name dictionary.

Prediction: Generally, classification plays a key role in retrieved data. The most commonly used classifications are KNN (k-nearest neighbors), (Naïve Bayes), NB, SVM (Support vector machine), etc. above all, KNN is one of the best and most effective classification algorithms in the vector space model.

KNN: :

KNN model classification report before scalling data:-

	precision	recall	f1-score	support
0	0.98	1.00	0.99	288
1	0.00	0.00	0.00	6
accuracy			0.98	294
macro avg	0.49	0.50	0.49	294
weighted avg	0.96	0.98	0.97	294

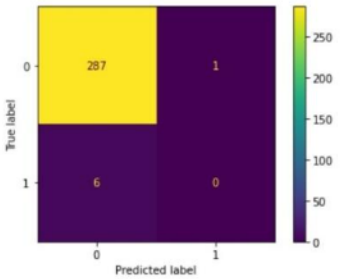


Figure 12 :KNN accuracy test

The scaling data report's classification visualizes the display of the model's precision, recall, F-1, and support scoresof . The overall accuracy 98 of the KNN model prediction was correct between a true label and a predicted label. Support is said to be an actual number of occurrences in the specific dataset; it just diagnoses the evaluation process.

Comparing Existing Work: From above case study discussed small and large business and organizations' considerations of SIEM. For example, suppose a company denies on firewall facing the internet on sentinel. In that case, adversaries launch an unknown attack against the organization . as a result of an unexpectedly huge amount of log events occurred .in that case, our project aims to defend the companies that cause log ingestion, and by geolocation, hunting, Entity behavior, and prediction analysis we are preventing from the future pre-attacks.

So based on the critical internal or external threats, vulnerabilities, and attacks, I have created a testbed as a suspicious one tried to keep my foothold inside an organization. Moreover, after many failed logon attempts, I have used some techniques such as Mapping, Hunting, Entities behavior, prediction analysis, and investigations, which help detect and find the adversaries from any place around the world, protecting the business organizations from future attacks with the low-cost budget.

V. Conclusion

This research paper has discussed an overview of capturing the live attacks, log ingestion, and its solution in the SIEM tool by some additional investigation and prediction analysis. The complete process discusses internal and external threats(attackers) for organizations to get inside of it to access or steal valuable data.

A summary, we have tried all the possibilities of detecting the adversary's geolocation and their sort of attacks, analyzing and investigating these brute force RDP attacks to protect the companies from future pre-attacks. However, it is also crucial to remind that log events are employed in various settings. Their incident response is technically high; well, most log usage occurs more often. So, for innovation and uniqueness of the project, I have made a testbed that truly acts as an attacker. I have taken the initiative and create a honeypot (Virtual machine) and try to log in with a fake credential. Once the event occurred and recorded in an event viewer, can ingest it to the analytics workspace. After ingesting the raw data, it can be extracted to the sentinel and captures all the live attacks or threats to the organization. After collecting and calculating all the failed events, which is "4625-failed log on, "has collected numerous hosts from different countries, which decides the majority of the attackers rather than genuine users. I have made my samples into three different sections to predict and protect from bad resources by analyzing all the situations.

Firstly, I decided to detect the suspicious attacker's geolocation to check whether it is an insider or external threat. Considering my testbed, which comes under insider, means through from inside user of an organization need to access the sensitive information of a particular company. Secondly, I swapped my place from the hacker to the defender, to protect against all the threats and vulnerabilities. Took part started all the investigation like a hunter with hunting the initial access, after running the query tactics justifies those adversaries are tried to foothold within a network. Moreover, Accounts and Host are the entities involved in our investigation; T1078 is the technique for valid accounts used by attackers to mitigate the threats, enforce to use the of strong passwords, and do not re-use them across multiple resources and services.

As per our comparative prediction analysis, I tried Naïve Bayes, SVM (Support Vector Machine), and KNN (K-nearest neighbor's). From all the above, KNN is considered the best method for precision. Hence it gives an accuracy of 98 percent. However, Naïve Bayes is 94, as well as SVM, is 96 percent. Overall, by train and test and testbed results, the final mark considered as 21 might be attackers out of 900 users. On the other hand, in 21, I'm one of the suspected attackers who tried to step inside the organization.

In short, some active security recommendations prevent future attacks. Firstly, the machines should encrypt temp disks, caches, and data between storage resources and computing. Secondly, should restrict all the network ports to a specific network security group. Lastly, all the internal machines should have a vulnerability assessment solution.

Extended investigation: This investigation has chances of extending for more clearance of work. Many business organizations use the (TIP) Threat Intelligence platform solutions . are used to accumulate the threat and vulnerability feeds from different sources within the sentinel platform. one of the best security solutions is EDR (End point Detection and Response)/XDR (Extended Detection and Response). XDR uses high-end security techniques that it collects and correlates the data from servers, endpoints, cloud workloads, and logs. Moreover, XDR enhances with SecOps efficiency, improving detection, etc. [15] Sentinel ones is an XDR AI platform that benefits from a single solution with single code based and deployment model.[16]

REFERENCES:

[1] . https://www.ibm.com/topics/siem.

[2].https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7412083

[3]. The History of Cybersecurity | Avast

[4]. M. Cinque, D. Cotroneo, and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," 2018, pp. 95–99, doi: 10.1109/ISSREW.2018.00-24.

[5].https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/2021/BlueVoyant_CloseUp_Whitepaper_Microsoft_Azure_Sentinel_Deployment_Q3_2021.pdf

[6]. What to Log in a SIEM? Security Logging Best Practices Explained | AT&T Cybersecurity

[7]. https://www.managedsentinel.com/edos-attack-azure-sentinel

[8] .P. Kaushik, A. M. Rao, D. P. Singh, S. Vashisht, and S. Gupta, "Cloud Computing and Comparison based on Service and Performance between Amazon AWS, Microsoft Azure, and Google Cloud," 2021, pp. 268–273, doi: 10.1109/ICTAI53825.2021.9673425.

[9]N. Naik, P. Jenkins, R. Cooke, and L. Yang, "Honeypots That Bite Back: A Fuzzy Technique for Identifying and Inhibiting Fingerprinting Attacks on Low Interaction Honeypots," 2018, pp. 1–8, doi: 10.1109/FUZZ-IEEE.2018.8491456.

[10]. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

[11].https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial

[12]. USB Artifact Analysis Using Windows Event Viewer, Registry and File System Logs Ashar Neyaz †,‡ and Narasimha Shashidhar *,‡ Department of Computer Science, Sam Houston State University, Huntsville, TX 77341, USA; ashar.neyaz@shsu.edu * Correspondence: karpoor@shsu.edu; Tel.: +1 (936)-294-1591 † Current address: 1900 Avenue I, Suite 214, Academic Bldg One, Huntsville, TX 77341, USA ‡ These authors contributed equally to this work. Received: 30 September 2019; Accepted: 7 November 2019; Published: 9 November 2019.

[13]. https://www.javatpoint.com/windows-powershell-ise

[14].https://docs.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-tip

[15] P. R. Brandao and J. Nunes, "Extended Detection and Response."

[16].https://www.sentinelone.com/cybersecurity-101/extended-detection-response-xdr/