EVENT ANALYSIS USING QRADAR SIEM

[1]A.Varsha, [2]M.Subashini, [3] J.Cirani Joshiya, [4] M.Sathish Kumar

[1]UG Student, ECE, National Engineering College, Kovilpatti, Tamilnadu, India
[2]UG Student, ECE, National Engineering College, Kovilpatti, Tamilnadu, India
[3]UG Student, ECE, National Engineering College, Kovilpatti, Tamilnadu, India
[4]Assistant Professor, ECE, National Engineering College, Kovilpatti, Tamilnadu, India

Email: [1]1911022@nec.edu.in, [2]1911046@nec.edu.in,
[3]1911120@nec.edu.in, [4]mskece@nec.edu.in

Abstract:. The importance of security information in a number of fields, such as banking, healthcare, information technology, and education, is evident in daily life.Security Information and Event Management, or SIEM, is able to continuously monitor the network in real-time for signs of any security issues and to send out alerts when it does.SIEM, short for Security Information and Event Management, has the capacity to continually scan the network in real-time for hints of any security problems and to deliver warning signs when it detects any. While earlier SIEM technologies analysed less data and had trouble handling big quantities.The IBM QRadar SIEM is a component of the IBM QRadar Security Intelligence Platform, which also provides modules for risk management, vulnerability management, forensics investigation, and incident response.It is used to examine network traffic and log data in real-time in order to promptly spot and restrict undesired activities. The primary objective of event data and flow data analysis performed using the QRadar SIEM technology is to evade or reduce harm to the host enterprise. For the purpose of identifying anomalous behaviour in your network, custom rules test events, flows, and offences. Anomaly detection rules run checks on the outcomes of stored flow or event searches to find instances of strange network traffic patterns.

Index terms: Event Analysis, SIEM, Qradar Console, Magistrate Core

I. INTRODUCTION

SIEM, or Security Information and Event Management, is a tool that enables enterprises to pinpoint, assess, and respond to security threats before they cause an adverse effect on their daily affairs.It tracks log data from an organization's network devices, host assets and operating systems, applications, vulnerabilities, and user actions and behaviours.It conducts real-time analysis of the network traffic and log data for the sake of detecting malicious behaviour,. Malicious behaviours can be immediately prevented, limiting or entirely avoiding harm to the enterprise. Information security can be described as the processes and methodologies which are designed and implemented to protect confidential, sensitive , electronic, or any other form of information or data via unauthorised activities including disclosure, destruction, modification, or disruption.For systems connected to the internet, including their data, software, and other components, cybersecurity is the fundamental line of defence against cyberthreats. People as well as enterprises both employ this technique to prevent unauthorized access to servers and other computerized systems. Protecting computer networks from unauthorised access, abuse, modification, or denial-of-service assault is the norm of network security. It describes a wide variety of tools, guidelines, and practises intended to ensure the privacy and reliability of data communicated across a network. Access Control, Firewall, Intrusion Detection and Prevention, Encryption, Virtual Private Networks, and Network Segmentation are some of the essential elements of Network Security.

II. RELATED WORKS

On a short, medium, and long term basis, it has been explored how key SIEM characteristics and outside forces would affect the SIEM landscape. A list of potential upgrades for the following generation of SIEMs was published together with an analysis of their benefits and use in important infrastructures. Nearly all of the options are approachable. When processing a high volume of gathered events, graphic user interfaces, visualisation, and response capabilities are limited. It highlights the value of developing visualisation and analytical extensions that give users a thorough grasp of the problem and enhanced capability for decision-making and response. Due to hardware availability, the solution under consideration has a limited amount of storage space, necessitating the purchase of more items at a greater price. This issue has been examined in more detail in[1].For analysis, logs were sent to SIEM as input. the extent to which a SIEM can identify insider risks by analysing user behaviour and unidentified threats. The mean temporal resolution value and false positive rate were both kept as low as possible, and there was no

limit on the number of events per second. The current SIEM challenges include data storage in the cloud, improper account security configurations on premises, excessive alerts degrading system performance, log correlation issues, low coverage of all devices in the network leading to undiscovered devices, and deployment of SIEM as a time-consuming process requiring first completing prerequisites and then adjusting to network architecture.By utilising the most recent SOAR and UEBA research, the study will reduce workloads and accelerate time to action at System Operations Centre (SOC). By automatically reducing response times with a SOC analyst, it lowers the percentage of workload related to handling threats. It decreases the time of detection, the typical duration between detection and resolution of an attack, the proportion of threats that automatically responded to but turned out to be false positives, and other factors that were looked at in[2].The idea was to put up a controller application on a host machine to collect the log files from ransomware and good software. The sequential pattern mining approaches was adopted to promptly detect the ransomware families by implementing machine learning classification methods within malware and authentic software samples. The most frequent patterns with various malware families are also found using this technique. The speed and accuracy with which system logs can be mined to look for anomalies and halt the occurrence is what determines how soon and correctly ransomware may be discovered. When identifying ransomware sample families to gather information about threat actors and threat profiles of a target, it can be helpful to look for distinguishing recurring patterns associated with various ransomware families. The use of sequence pattern mining to identify the common traits of ransomware programmes and create vector datasets of ransomware logs has theoretical ramifications. The practical consequences of using reported features for separating ransomware and benign applications for ransomware threat hunting, while reported features for ransomware family categorization are ideal for generating intelligence about threat profiles relevant to the given target. Additionally, methods for stream data mining that were used to speed up the detection of ransomware were explored in [3].A comparative examination of a few chosen products was carried out after defining the comparison criteria. This investigation had established the fundamental capabilities of the SIEM solutions. The solutions offered by IBM and Splunk are described together with a list of their core capabilities and a mapping to their respective architectures. In order to identify, categorise, prioritise, and mitigate cyberattacks at the beginning of the cyber death chain, SIEM handles log and event data from heterogeneous data space sources. The needs for the SIEM's functionality, including Data Collection and Aggregation from Different Sources and Applications, Storage, Retention, and Visualisation for Real-Time and Historical Data, and Functionality for Ensuring Compliance with Regulations and Standards, were discussed in [4].It was found that this effort's goal is to provide a standard method for acquiring and analysing event logs from Windows-based sources. The authors extract data from logs using event-forwarding technology. Events are used by event management and security data to pinpoint occurrences. The authors examine existing techniques for transmitting event log data from sources that are Windows-based.The method for establishing a connection between Windows-based event sources and the event collector without a domain controller is discussed in extensively in this article. Using credentials that the event collector creates, event sources are verified. The author set forth a method for fusing security data and event administration with the event collector.To be deployed with event forwarding technology, security data and event management must adhere to strict standards. There was technological exploration.[5].It has been suggested that the data, logs, and other output from IT operations in corporations are significant events. The management of a sizable amount of data in today's IT world is a challenging task, and network administrators are in charge of sending and storing the data securely. Any data that is compromised or manipulated by a hacker, whether locally or remotely, can have very negative effects. Solutions for firewalls and intrusion prevention systems (IPS) are used to validate each packet passed over the network in order to prevent this, which were covered in[6].

III. PROPOSED WORK

The proposed job involves investigating the warnings produced in accordance with the rules specified in the IBM QRADAR SIEM tool and analysing the event data using demo log sources.

Event Analysis:

The investigation of offences will be done with the aid of the IBM Qradar SIEM solution after event data analysis using demo log sources.

Planned analysis of events:

EventID:4624 - Account successfully logged in to

EventID:4625 - Account unable to log on.

IV. ARCHITECTURE-IBM Qradar SIEM

Data Collection:

The initial layer of data processing involves gathering data from your network, such as events or flows. Either deploy the All-in-One appliance to extract data directly from your network or accumulate event or flow data via collectors like Qradar Event Collectors or Qradar Flow Collectors.. Prior to being sent to

the processing layer, the data is normalised and parsed. When the raw data is parsed, it is normalised to make it available in a format that is structured and practical. The primary functions of Qradar SIEM are the gathering of event data and the gathering of flow data.

Data Processing:

After data collection, the Custom Rules Engine (CRE), which creates offences and alerts, is used to process event data and flow data before the data is written to storage. An All-in-One components can deal with event and flow data, without the insertion of additional event or flow processors.If the all-in-one appliance's processing capacity exceeds its limits, it may be required to add event processors, flow processors, or additional processing appliances to handle the rising demands.Storage requires data nodes. Network infrastructure configuration is gathered by Qradar Risk Manager, which also offers a topological map of your network. By simulating different network scenarios by changing configurations and establishing rules in the network, data can be used to control risk.

Data Searches:

Users can search, analyze, report, receive alerts, and investigate offences using the data that QRadar has collected and processed in the third or top layer. From the QRadar Console user interface, users may search for and handle the security admin tasks for their network.

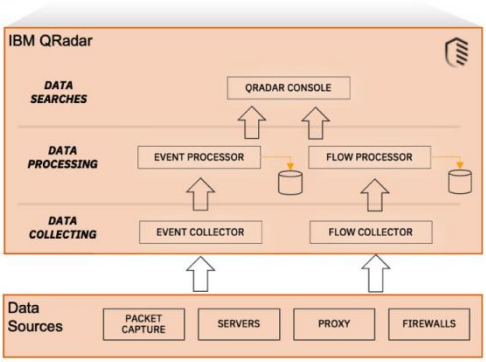

Figure 1: Architecture of Qradar SIEM

V. RESULTS

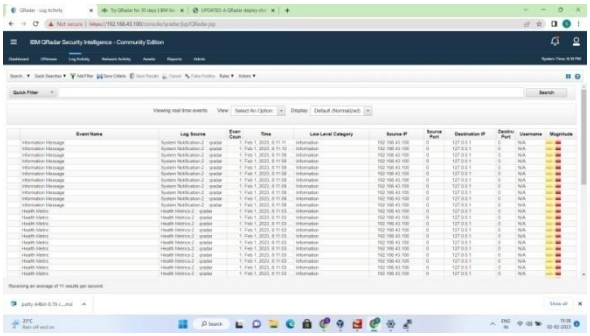

Figure 2: Log Activity Tab

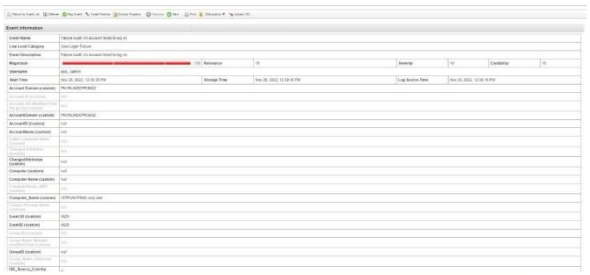

Figure 3:Offense Triggered For Login Failure

Figure 4: Description of the Offense(Login Failure)

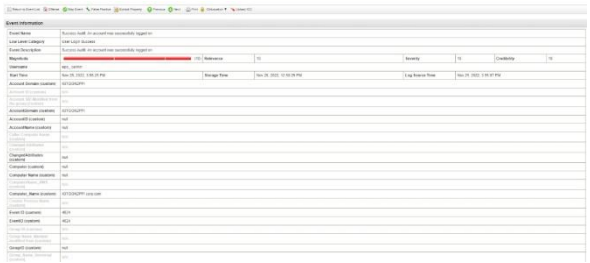

Figure 5: Offense Triggered For Login Success

Figure 6: Description of the Offense(Login Success)

CONCLUSION

A technique known as security information and event management enables threat identification, complaint handling, and security incident management through the gathering and examination of security events. It enables organisations to quickly gather and organise all of their digital assets' log data in one location.This section presents a study of a few window events. Similarly flow data can also be analysed.

REFERENCES

[1]. González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in CriticalInfrastructures. Sensors 2021, 21, 4759. https://doi.org/10.3390/s21144759

[2]. MukeshYadav, Dhirendra S Mishra, "Study of challenges faced by Enterprises using Security Information and Event Management (SIEM)"*Journal of University of Shanghai for Science and Technology*, 2021, Vol 23(08), pp. 511-522

[3]. SajadHomayoun,AliDehghantanha, MarziehAhmadzadeh, SattarHashemi, RaoufKhayami, "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence" *IEEE Transactions on Emerging Topics in Computing*2020, pp. 341-351, vol. 8

[4]. Giorgi Sharia, "Comparative Analysis Of Enterprise Security Information And Event Management(Siem) Solutions, Case Of Cybers" Thesis report, *InfotehnoloogiaTeaduskond*, 2020.

[5]. A.D. Moskvichev, M.V. Dolgachev, "System of Collection and Analysis Event Log from Sources under Control of Windows Operating System" *International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*,2020

[6]. On SivaramanEswaran, Aruna Srinivasan, Prasad Honnavalli, "A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise"*PES University, Bangalore*,3 Nov 2021.

★★★