iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61367

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Implementing SIEM(Security Information and Environment Management) in Microsoft Azure

Rohitkumar Jha[1], Donald Laishram[2], Nishma Kamat[3], Om Panchal[4], Prof. Salabha Jacob[5]
Department of Electronics and Computer Science, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India

Abstract: ***In an increasingly interconnected and digital world, the need for robust cybersecurity measures is paramount. Cyberattacks can therefore occur upon any device at any moment of time in order to steal the sensitive information of the user or can result in identity theft and cyberbullying. There are varieties of attacks that may occur without the user being aware about the same that their computer has been attacked and the hacker has overall access of their data. Also, a user cannot sit in front of their device throughout their life to monitor and protect any type of cyberattack. Therefore, in order to solve the following problems and to enhance the overall security and accuracy of safeguarding the device and its data, we implement our project Security Information and Environment Management (SIEM) system within the Microsoft Azure cloud ecosystem. SIEM plays a critical role in monitoring, detecting, and responding to security threats, making it a crucial component of any organization's cybersecurity strategy. To view the notification of the attack for a user and all its details, we therefore connect the SIEM implementations and logs over Microsoft Azure platform, and generate the same with the help of a command-shell Windows PowerShell.***

Keywords: SIEM, Cyberattacks, Microsoft Azure, Attack, Virtual Box.

I. INTRODUCTION

A. *Introduction To SIEM*

SIEM stands for Security Information and Event Management. It is a software solution that aggregates and analyses activity from many different resources across your entire IT infrastructure. SIEM collects security data from network devices, servers, domain controllers, and more. SIEM helps organizations detect, analyse, and respond to security threats before they harm business operations. SIEM combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action. SIEM systems vary in their capabilities but generally offer these core functions: log management, event correlation, and incident monitoring and response. SIEM tools use predetermined rules to help security teams define threats and generate alerts. SIEM tools offer many benefits that can help strengthen an organization’s overall security posture, including a central view of potential threats, real-time threat identification and response, advanced threat intelligence, regulatory compliance auditing and reporting, and greater transparency monitoring users, applications, and devices.

SIEM solutions typically consist of some major components for their functioning such as:

1) Data Collection: SIEM systems gather data from a wide range of sources, such as logs, network traffic, and system events. This data is collected in a centralized repository for analysis.
2) Normalization: The collected data is normalized to ensure that it is in a consistent and standardized format, making it easier to analyze and correlate events.
3) Correlation Engine: The correlation engine identifies patterns and relationships within the data, enabling the SIEM system to detect complex security threats that might go unnoticed by individual security tools.
4) Alerting and Reporting: SIEM systems generate alerts for potential security incidents. They can also provide reporting capabilities for compliance, audit, and managerial purposes.
5) Dashboard and Visualization: SIEM solutions often offer user-friendly dashboards and visualization tools that allow security professionals to monitor the security posture of their organization in real-time.
6) Incident Response and Workflow: Many SIEM solutions integrate incident response workflows, helping organizations automate and streamline the response to security incidents.

B. Introduction To Microsoft Azure

Microsoft Azure is a cloud computing platform that provides a wide range of services and resources to help businesses meet their goals. It is similar to other cloud platforms like Google Cloud and Amazon Web Services (AWS). Azure offers virtual machines, fast data processing, analytical and monitoring tools, and more to make work simpler. It is cost-effective and offers a subscription-based model that allows users to pay only for what they use. Azure has a low operational cost because it runs on its servers whose only job is to make the cloud functional and bug-free. It is easy to implement business models in Azure with a couple of on-click activities 1. Azure also provides easy backup and recovery options, which can save time and avoid large up-front investments.

Following are some of the services Microsoft Azure offers:

1) Compute: Includes Virtual Machines, Virtual Machine Scale Sets, Functions for serverless computing, Batch for containerized batch workloads, Service Fabric for microservices and container orchestration, and Cloud Services for building cloud-based apps and APIs.
2) Networking: With Azure, you can use a variety of networking tools, like the Virtual Network, which can connect to on-premise data centers; Load Balancer; Application Gateway; VPN Gateway; Azure DNS for domain hosting, Content Delivery Network, Traffic Manager, ExpressRoute dedicated private network fiber connections; and Network Watcher monitoring and diagnostics
3) Storage: Includes Blob, Queue, File, and Disk Storage, as well as a Data Lake Store, Backup, and Site Recovery, among others.
4) Web + Mobile: Creating Web + Mobile applications is very easy as it includes several services for building and deploying applications.
5) Containers: Azure has a property that includes Container Service, which supports Kubernetes, DC/OS or Docker Swarm, and Container Registry, as well as tools for microservices.
6) Databases: Azure also included several SQL-based databases and related tools.
7) Data + Analytics: Azure has some big data tools like HDInsight for Hadoop Spark, R Server, HBase, and Storm clusters
8) AI + Cognitive Services: With Azure developing applications with artificial intelligence capabilities, like the Computer Vision API, Face API, Bing Web Search, Video Indexer, and Language Understanding Intelligent.
9) Internet of Things: Includes IoT Hub and IoT Edge services that can be combined with a variety of machine learning, analytics, and communications services.
10) Security + Identity: Includes Security Center, Azure Active Directory, Key Vault, and Multi-Factor Authentication Services.
11) Developer Tools: Includes cloud development services like Visual Studio Team Services, Azure DevTest Labs, HockeyApp mobile app deployment and monitoring, Xamarin cross-platform mobile development, and more.

C. Introduction To Windows Powershell

Windows PowerShell is a task automation and configuration management program from Microsoft. It is a modern command shell that includes the best features of other popular shells. PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. It runs on Windows, Linux, and macOS. PowerShell is designed to help you automate and quickly solve tedious administration tasks. You can use PowerShell to display all the USB devices installed on one or multiple computers in a network, or you can set a time-consuming task to run in the background while you do other work. PowerShell accepts and returns .NET objects, which makes it different from most shells that only accept and return text. PowerShell offers many advantages, including an extensible format system, built-in data formats, an extended type system, secure scripting engine, self-service development, consistent API, easy automation, and more. PowerShell is easy to install on Windows using Winget, MSI package, ZIP package, .NET Global tool, or Microsoft Store package.

II. METHODOLOGY

To implement a comprehensive security solution within Azure, several steps need to be taken, beginning with the configuration of Azure itself. This involves setting up the necessary Azure resources and services to support the security infrastructure. Once Azure is configured, the next step is to configure the required resources within the Azure environment. This includes provisioning virtual machines (VMs), storage accounts, and networking resources as needed to support the security solution.

One critical aspect of the security setup is the configuration of VMware under Azure. This entails deploying VMware virtual machines within the Azure environment and configuring them to meet the organization's security requirements. Additionally, setting up login credentials for these VMs is essential to ensure secure access and prevent unauthorized entry. This involves implementing strong password policies and multi-factor authentication where applicable.

To bolster defenses against potential threats, the project involves implementing a Brute-Force attack prevention mechanism on the VMs. This includes configuring security settings to limit login attempts and implementing measures to block or throttle repeated login attempts from suspicious sources. Furthermore, configuring Windows Powershell ISE within the VM allows for scripting and automation, enhancing security operations and response capabilities.

A crucial aspect of the project is the coding of Windows Powershell ISE scripts for generating logs of attackers' activities. These scripts are designed to capture relevant information, such as IP addresses, login attempts, and other parameters, to aid in threat detection and analysis. Additionally, disabling firewalls on the VMs allows for the logging of attacks from universal sources, providing valuable insight into potential threats.

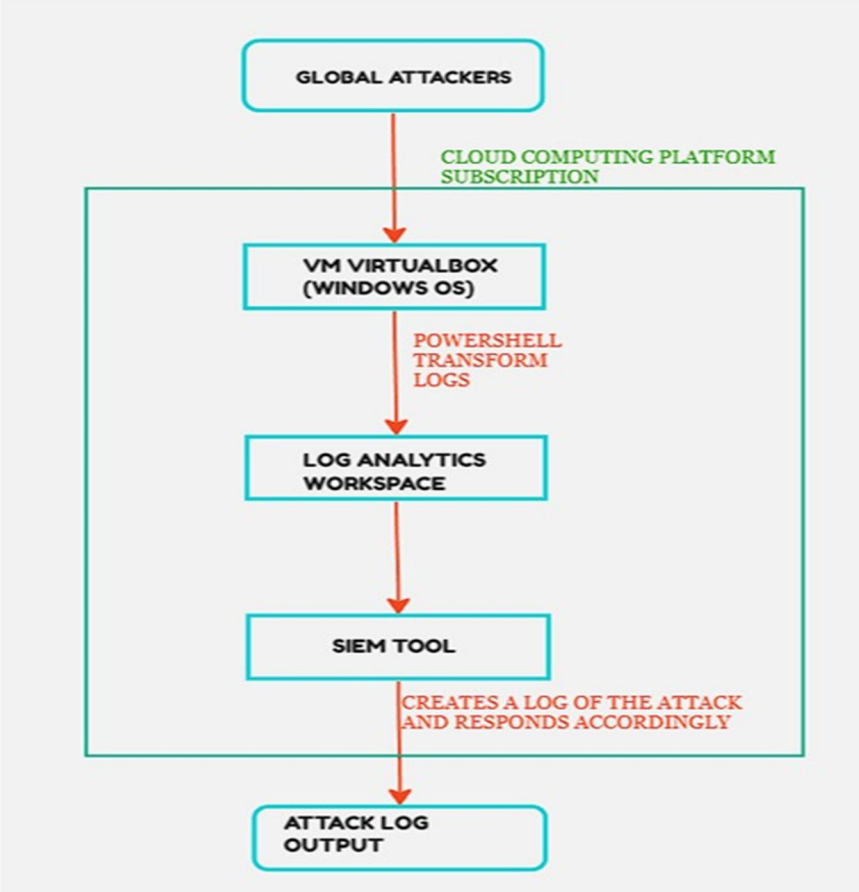
To enhance threat detection capabilities further, an API key is generated for Windows Powershell ISE, enabling the detection of attacker details and facilitating integration with other security tools and services. Additionally, the project involves coding and setting up a fake log detection mechanism to identify and eliminate false login attempts, improving the accuracy of threat detection.

In addition to traditional threat detection methods, the project includes the coding and setup of a Convolutional Neural Network (CNN) classifier to detect trojan attacks from log data. This advanced machine learning technique enhances the organization's ability to identify and mitigate sophisticated threats.

To streamline the analysis of security logs, log files are generated over the VMs and used to train a Log Analytical Workspace. This involves shaping the logs into an appropriate format using tools such as custom logs and custom fields. The Log Analytical Workspace is then connected to Microsoft Sentinel, allowing for centralized log management and analysis.

Configuration of Microsoft Sentinel includes setting up geolocation data representation for enhanced visualization of attack data. This enables security analysts to better understand the geographic origins of attacks and prioritize response efforts accordingly. Finally, public live attack detection over geolocation representation provides real-time visibility into ongoing security threats, allowing for rapid response and mitigation.

III. FLOWCHART



IV. RESULTS

The implementation of SIEM in Azure using Microsoft Azure and setting up geolocation using Microsoft Sentinel yielded significant results in bolstering the organization's cybersecurity capabilities.

Firstly, the successful deployment of Azure Sentinel within the Azure environment provided a centralized platform for collecting, analyzing, and responding to security events and alerts from various Azure services and data sources. This comprehensive security monitoring enabled proactive threat detection and response, enhancing the organization's ability to identify and mitigate security threats in real-time.

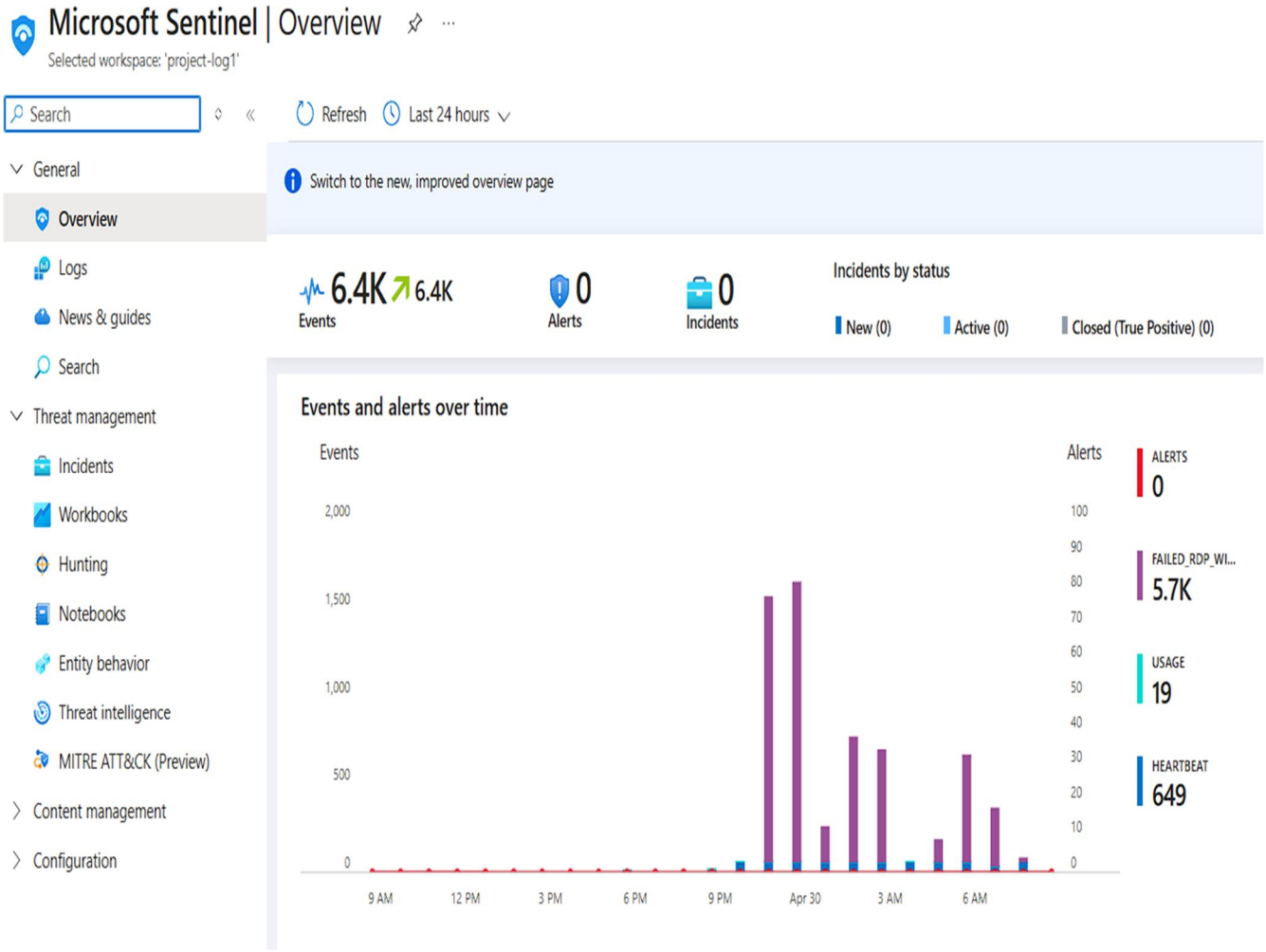
Secondly, the setup of geolocation using Microsoft Sentinel allowed for the visualization and analysis of attack data based on geographic location. This provided valuable insights into the origin of security threats, enabling targeted response strategies and prioritization of response efforts based on the geographic location of security incidents.

Additionally, the project demonstrated successful integration with the Microsoft ecosystem, including Azure services, Microsoft Threat Intelligence, and Azure Security Center. This integration enhanced the effectiveness of threat detection and response by providing access to up-to-date threat intelligence data and enabling seamless collaboration between security tools and services.

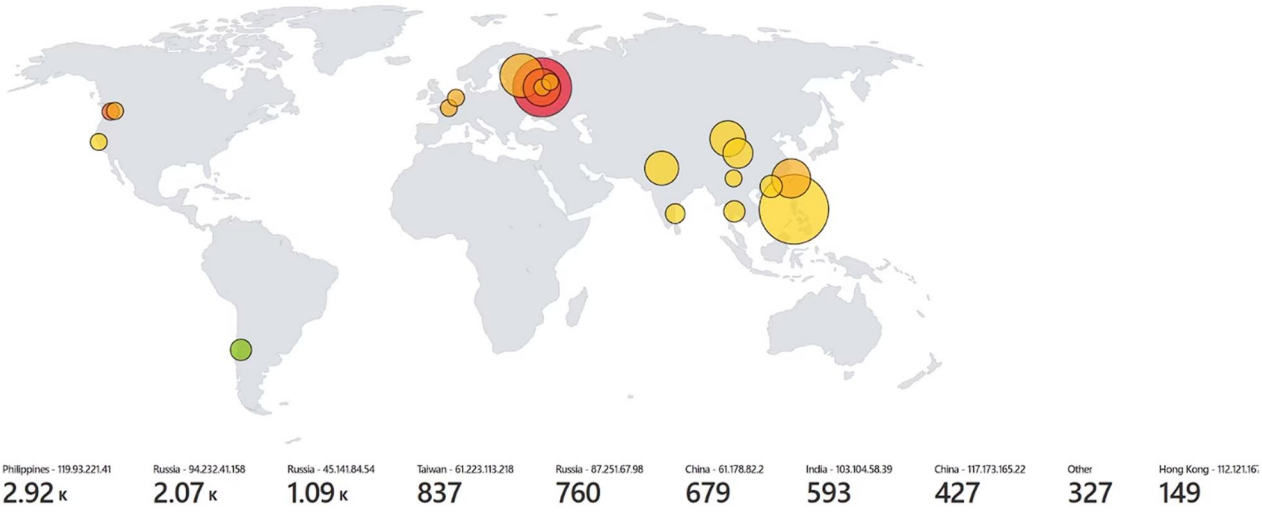
Overall, the implementation of SIEM in Azure using Microsoft Azure and setting up geolocation using Microsoft Sentinel significantly strengthened the organization's security posture in the Azure environment, ensuring the integrity and security of its Azure-based assets and services.

Here are some sample shots of the output from Microsoft Sentinel and Geolocation data from the attacker's log when we made our virtual box public over the public IP:

Connecting attack logs to Microsoft Sentinel



Making the virtual machine public for 24 hours in order for attackers to attack the system worldwide and observe if anybody could break into the system



V. ADVANTAGES

1) Comprehensive Security Monitoring: Azure Sentinel provides a centralized platform for collecting, analyzing, and responding to security events and alerts from various Azure services and data sources. This enables organizations to gain holistic visibility into their Azure environment and effectively monitor for security threats.
2) Scalability and Flexibility: Leveraging Microsoft Azure allows for scalability and flexibility in deploying and managing the SIEM solution. Organizations can easily scale resources up or down based on their evolving security needs and business requirements.
3) Integrated Threat Intelligence: Microsoft Sentinel integrates with Microsoft's extensive threat intelligence network, including Microsoft Threat Intelligence, Microsoft Defender, and Azure Security Center. This provides organizations with access to up-to-date threat intelligence data and enhances the detection and response capabilities of the SIEM solution.
4) Geolocation Data Representation: Setting up geolocation using Microsoft Sentinel enables organizations to visualize attack data based on geographic location. This enhances situational awareness and helps security analysts better understand the geographic origins of attacks, allowing for more targeted response efforts.
5) Automation and Orchestration: Azure Sentinel offers automation and orchestration capabilities, allowing organizations to automate repetitive security tasks and orchestrate security workflows. This improves operational efficiency, reduces manual intervention, and enables faster response to security incidents.

VI. DISADVANTAGES

1) Learning Curve: Implementing and configuring a SIEM solution like Azure Sentinel requires specialized knowledge and expertise in cloud security and SIEM technologies. Organizations may need to invest time and resources in training staff or hiring experienced professionals to effectively deploy and manage the solution.
2) Cost: While Azure Sentinel offers a pay-as-you-go pricing model, the costs associated with deploying and operating the SIEM solution in Azure can vary depending on factors such as data volume, retention policies, and the complexity of the environment. Organizations need to carefully consider the cost implications and budget accordingly.
3) Integration Challenges: Integrating Azure Sentinel with existing Azure services and data sources may present challenges, particularly in complex or heterogeneous environments. Ensuring seamless integration and data flow between different systems and platforms requires careful planning and coordination.
4) False Positives: Like any SIEM solution, Azure Sentinel may generate false positives, where legitimate activities are incorrectly flagged as security threats. Organizations need to fine-tune detection rules, adjust alert thresholds, and regularly review and validate alerts to minimize the impact of false positives on security operations.
5) Dependency on Microsoft Ecosystem: Organizations that choose to implement Azure Sentinel are inherently dependent on the Microsoft ecosystem, including Azure services and Microsoft's threat intelligence network. This may limit flexibility and interoperability with non-Microsoft technologies and platforms.

VII. USE CASES

Security Information and Event Management can be applied to various use cases across different industries. Here are some sectors where this model can be used:

1) Financial Services: A bank or financial institution can use this project to enhance its cybersecurity posture by implementing Azure Sentinel to monitor for suspicious activities across its Azure infrastructure. By setting up geolocation using Microsoft Sentinel, the bank can visualize and analyze attack data based on geographic location. This allows security analysts to identify and respond to potential threats targeting specific regions or branches more effectively.
2) Healthcare: A healthcare organization can leverage this project to strengthen its security monitoring capabilities in the Azure cloud environment. Azure Sentinel can be deployed to collect and analyze security logs and events from Azure services and data sources. Setting up geolocation using Microsoft Sentinel enables the healthcare organization to detect and investigate security incidents related to patient data breaches or unauthorized access attempts from different geographical locations.
3) Retail: A retail company can utilize this project to protect its e-commerce platform and customer data hosted on Azure. Azure Sentinel can help monitor for threats such as payment fraud, unauthorized access, and data exfiltration attempts. By setting up geolocation using Microsoft Sentinel, the retail company can track and analyze cyber attacks originating from different regions or countries, allowing for targeted response and mitigation efforts.
4) Manufacturing: A manufacturing company can implement Azure Sentinel to monitor its Azure-based production systems and supply chain operations for security threats. By collecting and analyzing security logs and events from IoT devices, manufacturing equipment, and other Azure resources, Azure Sentinel can help detect and respond to anomalies and potential cyber attacks. Setting up geolocation using Microsoft Sentinel enables the company to identify and mitigate threats targeting specific manufacturing facilities or regions.
5) Government: Government agencies can deploy Azure Sentinel to enhance the security of their Azure cloud environments and protect sensitive government data and systems. By leveraging Azure Sentinel's advanced threat detection capabilities, government agencies can detect and respond to cyber threats in real-time. Setting up geolocation using Microsoft Sentinel allows agencies to visualize and analyze attack data based on the geographical location of government assets and critical infrastructure.

VIII. CONCLUSION

The implementation of a Security Information and Environment Management (SIEM) system in the Microsoft Azure environment represents a significant step forward in enhancing an organization's cybersecurity posture. This project, which focused on the integration and deployment of a SIEM solution within the Azure cloud ecosystem, has provided valuable insights and practical knowledge for IT professionals and organizations seeking to bolster their security measures. In this concluding section, we recap the key takeaways and the importance of this project.

SIEM can increase its ability to identify threats by determining whether the state of the present gathered data is a threat or not employing a neural network model that generates threat classifications or normalcy by inferring patterns from long-term data collected. And using such a method will significantly improve the SIEM's long-term data collection's analysis of intelligent cyber threats.

In conclusion, integrating Security Information and Event Management with a cloud platform using PowerShell provides a powerful solution for bolstering an organization's security defenses. By harnessing the cloud's agility and PowerShell's automation capabilities, businesses can achieve the following:

1) Agile Deployment
2) Cost Efficiency
3) Compliance Management
4) Global visibility
5) Real Time monitoring
6) Automated Responses

IX. FUTURE SCOPE

The implementation of a SIEM system in Microsoft Azure is a critical step in fortifying an organization's security posture. As technology and cybersecurity landscapes evolve, the project's future scope expands to address emerging trends and challenges.

Here are some areas of potential future development and focus for organizations that have implemented or plan to implement SIEM in Microsoft Azure:

1) Advanced Threat Detection: SIEM systems should evolve to incorporate more advanced threat detection techniques, such as machine learning and behavior analytics. These technologies can help identify previously unknown threats and anomalies in Azure environments.
2) Threat Intelligence Integration: Future SIEM implementations should incorporate threat intelligence feeds and services to provide real-time information on emerging threats and vulnerabilities specific to Azure services.
3) Automated Incident Response: The automation and orchestration capabilities of SIEM systems can be further enhanced. Future development may focus on automating incident response processes to a greater extent, reducing the response time and manual intervention required.
4) User and Entity Behavior Analytics (UEBA): Incorporating UEBA features into SIEM solutions can help organizations detect insider threats and unusual user behaviors in Azure environments.
5) Customization and Extensibility: The ability to create custom dashboards, reports, and alerts should be further enhanced. Future development may focus on providing more user-friendly interfaces for customization.
6) AI-Driven Security: The integration of artificial intelligence (AI) and machine learning (ML) for predictive analysis and security decision-making will become more prevalent. SIEM solutions should leverage AI to proactively address potential threats.
7) Community and Knowledge Sharing: The SIEM community is vibrant, and knowledge sharing is crucial. Future projects could involve the development of open-source SIEM tools and the creation of platforms for sharing SIEM-related best practices and threat intelligence.

X. LITERATURE SURVEY

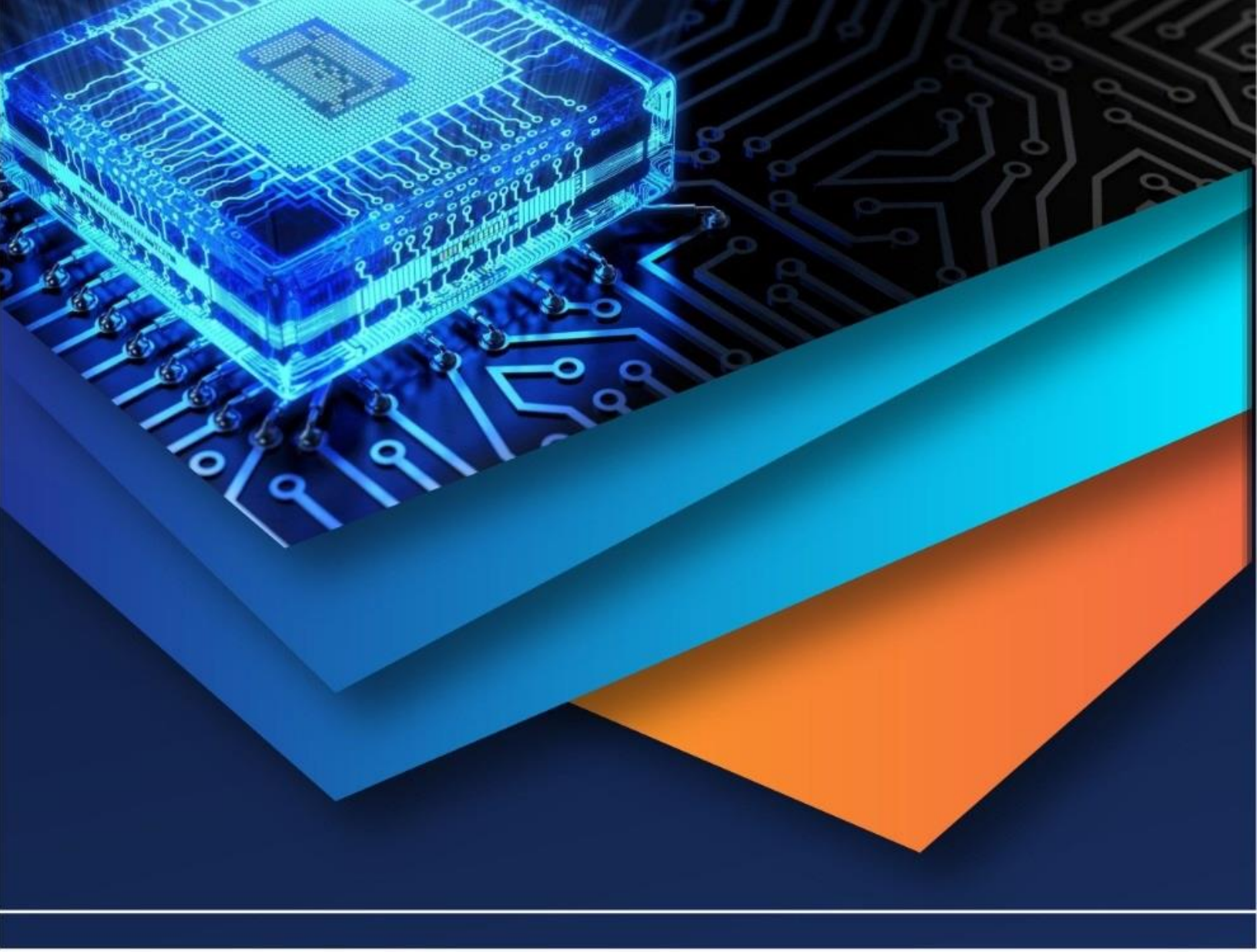
NAME OF PAPER | AUTHOR | YEAR OF PUBLISH	METHODOLOGY	CONCLUSION
Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning AUTHOR: Adabi Raihan Muhammad, Parman Sukarno, Aulia Arif Wardana YEAR OF PUBLICATION: 2022	This section investigates the difference between the proposed model and system in this research and another related research. Cakmakci et al. proposed SIEM to detect DDoS attacks on the network. This research uses ontologies methods to detect, recover, and respond to DDoS attacks. This research combines three security tools like firewalls, antivirus, and IDS/IPS to integrate with SIEM. This research used signature-based detection to detect DDoS attacks. This research is prepared to be implemented for IT organizations or industrial ready. Azodi et al. more focus on processing the log for integrate IDS and SIEM. This research also employs a signature-based method to analyze the traffic.	Based on some previous research, it states that there is no integrated SIEM and IDS with anomaly detection method in live analysis mode. Live analysis mode in anomaly detection method means that machine learning detection and network monitoring need to perform in real-time. The SIEM also gives telegram and email alerts to the IT team when cyberattack alarm detection occurs. The system in this research is also built using opensource software and suitable for industrial applications, especially for SME because opensource software is low cost.
Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures	Security Information and Event Management (SIEM) systems have been widely deployed as a powerful tool to prevent, detect, and react against cyber-attacks. SIEM solutions	Security Information and Event Management (SIEM) systems have been widely deployed as a powerful tool to prevent, detect, and react against cyber-attacks. SIEM solutions

AUTHOR: Gustavo Gonzalez Granadillo, Atos S.A., Susana González-Zarzosa, Rodrigo Diaz YEAR OF PUBLICATION: 2021	have evolved to become comprehensive systems that provide a wide visibility to identify areas of high risks and proactively focus on mitigation strategies aiming at reducing costs and time for incident response.	have evolved to become comprehensive systems that provide a wide visibility to identify areas of high risks and proactively focus on mitigation strategies aiming at reducing costs and time for incident response. Currently, SIEM systems and related solutions are slowly converging with big data analytics tools. We survey the most widely used SIEMs regarding their critical functionality and provide an analysis of external factors affecting the SIEM landscape in mid and long-term. A list of potential enhancements for the next generation of SIEMs is provided as part of the review of existing solutions as well as an analysis on their benefits and usage in critical infrastructures
SIEM (security information and event management solutions) implementations in private or public clouds AUTHOR: Vlad-Mihai Cotenescu YEAR OF PUBLICATION: 2017	The paper discusses the historical offerings of SIEM, including SEM and SIM, and how integrated SIEM platforms now provide real-time monitoring of network and security devices. It highlights the challenges faced by end users in implementing SIEM, with perceptions of complexity and slow implementation without sufficient customer value. The paper contrasts SIEM with Log Management solutions, which are perceived more positively for their ability to aggregate, parse, and index logs effectively	SIEM solutions have evolved to centralize security data management and provide real-time monitoring of security alerts. The paper discusses the challenges faced by end users in implementing SIEM, highlighting perceptions of complexity and slow implementation without sufficient customer value. Today's security threats are dynamic in nature and exploits are constantly evolving. Attackers grow more organized, precise and persistent and have access to various automated tools that can trigger very sophisticated attacks. As threats and security events evolve, SIEM vendors and the information security community must work together to build relevant and actionable model into their systems.Contrasting SIEM with Log Management solutions, the latter are perceived more positively for their effective aggregation, parsing, and indexing of logs.

REFERENCES

[1] Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., ... & Asari, V. K. (2019). A state-of-the-art survey on deep learning theory and architectures. Electronics, 8(3), 292. (For understanding deep learning architectures for threat detection, relevant to the project's CNN classifier implementation.)

[2] Microsoft. (n.d.). Azure Sentinel documentation. Retrieved from https://docs.microsoft.com/en-us/azure/sentinel/ (Official documentation for Azure Sentinel, providing technical guidance and best practices for implementing SIEM in Azure.)
[3] Gartner. (2021). Gartner Magic Quadrant for Security Information and Event Management. Retrieved from https://www.gartner.com/en/documents/3989645 (For insights into the SIEM market landscape, including evaluations of vendors such as Microsoft Azure Sentinel.)
[4] Bhat, A., & Kapoor, R. (2020). An analytical study of geolocation-based intrusion detection techniques. International Journal of Computer Applications, 175(2), 29-34. (Provides insights into geolocation-based intrusion detection techniques, relevant to the project's geolocation setup.)
[5] Microsoft. (n.d.). Azure Architecture Center - Security. Retrieved from https://docs.microsoft.com/en-us/azure/architecture/browse/?product=security (Offers architectural guidance and best practices for implementing security solutions in Azure, including SIEM deployment.)
[6] Ficco, M., Esposito, C., Palmieri, F., Castiglione, A., & Verde, N. (2016). An adaptive network-based security framework for the detection of cyber activities. IEEE Transactions on Industrial Informatics, 12(5), 1891-1900. (Discusses adaptive network-based security frameworks, relevant to the project's implementation of security monitoring.)
[7] Jones, B., & Barker, A. (2019). Learn Microsoft Azure: Build, manage, and scale cloud applications using the powerful features of Azure. Packt Publishing Ltd. (Provides comprehensive guidance on using Microsoft Azure, including topics relevant to setting up and configuring Azure services for the project.)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY