International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 5 ||Issue|| 5 ||Pages 108-111 ||2023||

Sentinel AI: An Investigation into Robust Threat Mitigation Strategies for Artificial Intelligence

Alex Mathew
Department of Cybersecurity, Bethany College, USA

ABSTRACT : Sentinel AI is a significant transformation in the technology field, which faces multiple cyberattack threats. By incorporating cloud-based software, sentinel AI can provide the needed security and allow systems to respond to potential attacks swiftly. Sentinel AI provides security protection by detecting unusual observations and signaling alerts. It is essential to use signature-based detectors as this enables easier identification of all attacks and protects systems against damage. Sentinel systems should be capable of monitoring, visualization, and optimizing operations to facilitate inspection, analysis, and response to threats. The SIEM is an essential component that should be included in the sentinel system to help gather data from diverse sources such as servers, network devices, endpoints, and applications for maximum performance. The SIEM can facilitate correlation and analysis to distinguish the different data formats, making it easier to identify anomalies.

.

KEYWORDS - sentinel AI, artificial intelligence, cloud-based software, SIEM

I. INTRODUCTION

Artificial intelligence (AI) provides a significant opportunity to use computerized machines to simulate the intelligence of human beings successfully. Indeed, skills in computer datasets and science insights are vital and useful when designing AI systems. Notably, such skills make it possible for people to solve problems they experience in their daily lives. The advancement of technology poses a considerable challenge to traditional production models through increasing performance scale and range of activities to be accomplished within a stipulated time. Generally, by improving technology automation, even in the cybersecurity sector, AI has benefits but can also experience malware attack challenges. The increased technology vulnerabilities highlight the need to develop mitigation approaches that safeguard AI systems (Dilmaghani et al., 2019). Sentinel AI can provide security solutions by detecting unusual observations and signaling alerts of potential threats. It is essential to understand that sentinel AI uses a deep learning algorithm to prevent threats that might attack and prevent the efficiency of technological devices and systems.

II. PROPOSED METHODOLOGY BLOCK DIAGRAM

The block diagram displays important components in the systems that improve the efficiency of the sentinel system to prevent any malicious attacks. The “defender for cloud” will be a vital component that helps safeguard the cloud resources. Mainly, this section identifies any system vulnerability by monitoring any issue that can interfere with the AI functionality. Also, the “defender for the cloud” ensures that all systems supporting AI’s function are securely configured. Log Analytics, on the other hand, is concerned with collecting and analyzing data from various system applications. Once this information is collected, the system can evaluate performance and security concerns. In case of any security threat, the log analytics can raise the alarm according to how it has been customized. According to Jhaveri and Parmar (2023), log analytics shows a system’s performance history, proving useful when identifying failures and other security breaches that negatively impact a company’s progress. Generally, these components act as security operation systems that help reduce cyber-risk exposure and allow organizations to mitigate risks if they occur quickly. For instance, during a malicious incident, the log analysis allows analysts to scrutinize the system servers to determine the damage’s anomalies or extent.

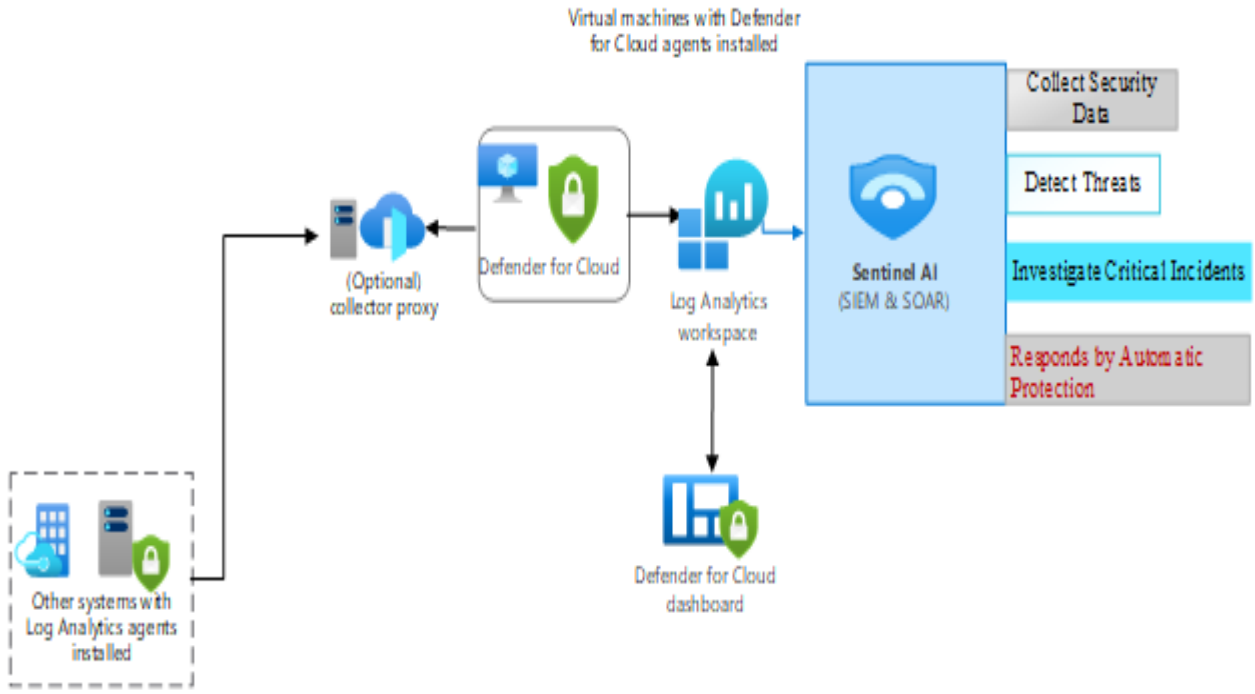


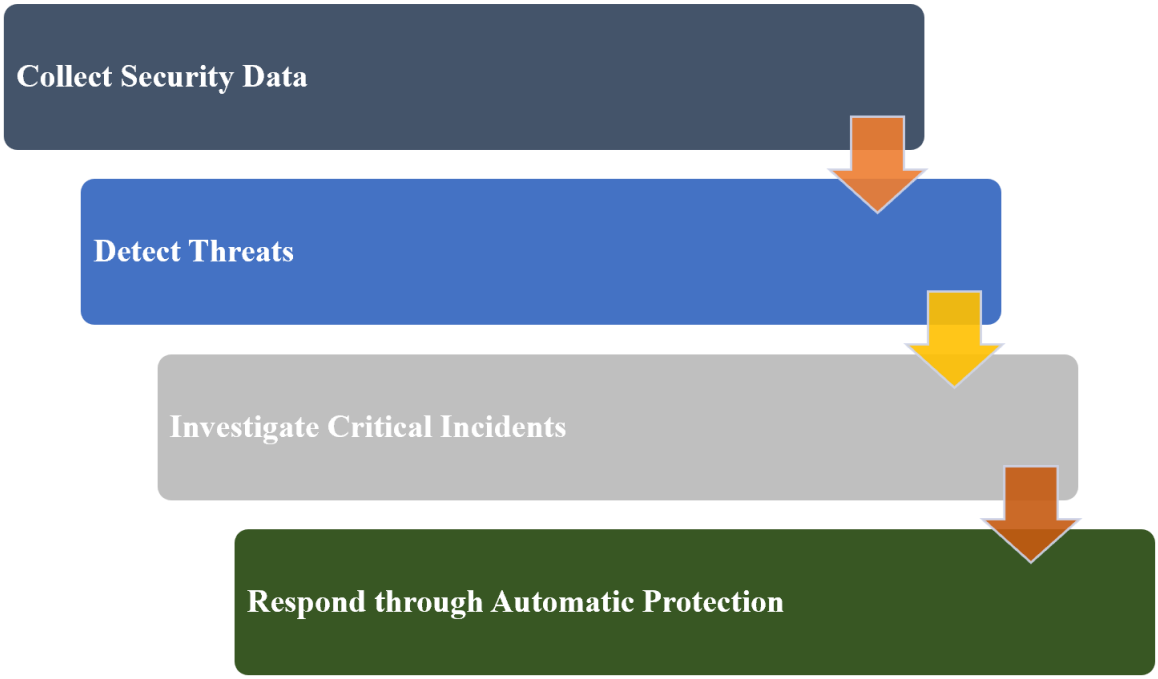
Fig. 1: Block Diagram Showing Components of Sentinel AI

III. ALGORITHM

The sentinel AI comprises several procedures that enable the system to function appropriately. The first procedure is the collection of security information using a security hub. Notably, this security hub primarily collects and combines data findings. An excellent example of a security hub is the AWS Security Hub, which the Amazon Inspector uses to detect intrusion and conduct vulnerability scans (George & Sagayarajan, 2023). Apart from collecting the data, the AWS Security Hub also consolidates security solutions that help improve operation efficiency (Penwell, 2023). More importantly, consolidating the security solutions increases the detection rate and maintains standard control of all the systems. The collection system uses real-time data to identify malicious attacks, providing analysts ample time to correct the system anomalies. A performance management system can be implemented in the sentinel AI to detect data that would cause failure. The system's security should be a top priority, and a desirable feature should be incorporated to combat attack malware. An example of a performance management system is the Google GCP command center, which performs security checks such as threat detection and identifies misconfigurations. According to Wong et al. (2023), the security commands identify threats and provide. Notably, using the GCP enables Google to mitigate misconfiguration and promptly respond to security concerns.

Electronic sentinels use high intelligence systems to detect unusual events that threaten the effective use of AI. Approaches that utilize signature-based detectors can have a profound impact when identifying all manner of attacks and protecting against damage to AI systems. Research supports using a digital signature algorithm (DSA) because it provides needed security to systems by limiting intrusion (Muhammad et al., 2023). The signature-based detection works by collecting the data and matching it with a provided database to determine if it has a comparison with any recorded information that previously posed a risk to the system. However, for this signature-based detection to work perfectly, a few critical components must be included, which include unique code and known malware signatures. Notably, during scanning, the similarity of the signatures within the database triggers an alarm of potential threats. The automatic rapid response is the procedure that makes sentinel AI protect the system from malicious attacks (Giannaros et al., 2023).

IV. FLOW CHART



V. RESULT ANALYSIS

Smartphone manufacturing companies use complex systems to protect the phones against malicious attacks. For instance, the Android version uses Linux-OS (operating system) that is securely enhanced by rules, kernel-level applications, and Linux policies. The security-enhanced Linux (SE-Linux) provides Android smartphones with security measures preventing malware attacks (Rehman et al., 2022). Google also greatly contributes to making smartphones more secure through its services, such as safety checks, security alerts and updates, and Play Protect. Another essential security measure for the Android smartphone is protection through the original equipment manufacturer (OEM). The OEM is an important security component in a smartphone because it offers antivirus applications, secure vaults, update management, and systems to track anomalies (Elahi et al., 2020). The Google Play Store is a secure platform where an Android smartphone user can download books and various apps supporting games and movies. Since the Play Store is highly accessible by the majority of people across the world, Google company ensures that the clients are protected by enhancing the security measures (Alanzi, 2021).

Another area where the concept of sentinel AI is widely utilized is in the healthcare sector. Antivirus software is used in fighting antibodies to protect the immune system from malicious software that can cause harm to the human body (Alrubayyi et al., 2021). The system is designed to predict, detect, and prevent an individual from cyber threats that target biological systems (George et al., 2023). Another important role of the digital defense system is protecting personal data from landing on an unauthorized hand, as some people can use such information to cause damage. Notably, the digital immune system is designed to use advanced encryption to protect personal data, thus making it inaccessible to unauthorized groups.

Microsoft company also uses sentinel AI in its Microsoft Azure to provide threat awareness, alert detection, and response (Karantzas & Patsakis, 2021). The Microsoft sentinel is a security solution that Microsoft provides to provide the system with the appropriate threat intelligence (Jhaveri et al., 2023). Mainly, the Microsoft sentinel gathers data from diverse sources within its system, correlates, and processes them in a visualization dashboard to determine if there are any anomalies. The system has a high functionality framework as it integrates detection, visibility, and response mechanisms by rapidly deploying dashboard panels, pre-configured ports, and other security features. The SIEM (Security Information and Event Management) provides the most advanced cloud-based software technology to enhance security monitoring and defense (González-Granadillo et al., 2021). The SIEM gathers data from diverse sources such as servers, network devices, endpoints, and applications for maximum performance. Again, it facilitates correlation and analysis to help distinguish the different data

formats, making it easier to identify anomalies. During data analysis, the SIEM enables the Microsoft sentinel to identify the presence of security breaches by examining normalized data (Younus & Alanezi, 2023). On the other hand, the correlation enables the system to compare collected data and determine the attack patterns. Generally, with this information, the system then appropriately responds to the threat to prevent damage and enhance the efficiency of the process.

CONCLUSION

Generally, sentinel AI is important for people and organizations to prevent malicious attacks that can hamper their systems or affect their health. With the advancement of technology, embracing mitigation strategies that can prevent AI from such attacks is recommended. A good sentinel system should be capable of monitoring, visualization, and optimizing operations to provide the needed standard of inspection, analysis, and response to threats. More importantly, SIEM is a system that many organizations should embrace due to its significant role in identifying and neutralizing security threats. However, more advanced sentinel AI systems are needed as the future of technology gets more sophisticated every day to protect systems from malicious attacks.

REFERENCES

[1] Alanzi, T. (2021). A review of mobile applications available in the app and google play stores used during the COVID-19 outbreak. Journal of multidisciplinary healthcare, 45-57.

[2] Alrubayyi, H., Goteng, G., Jaber, M., & Kelly, J. (2021). Challenges of malware detection in the IoT and a review of artificial immune system approaches. Journal of Sensor and Actuator Networks, 10(4), 1-20.

[3] Dilmaghani, S., Brust, M. R., Danoy, G., Cassagnes, N., Pecero, J., & Bouvry, P. (2019, December). Privacy and security of big data in AI systems: A research and standards perspective. In 2019 IEEE International Conference on Big Data (Big Data), 5737-5743.

[4] Elahi, H., Wang, G., & Chen, J. (2020). Pleasure or pain? An evaluation of the costs and utilities of bloatware applications in android smartphones. Journal of Network and Computer Applications, 102578. doi:10.1016/j.jnca.2020.102578

[5] George, A. S., & Sagayarajan, S. (2023). Securing cloud application infrastructure: Understanding the penetration testing challenges of IaaS, PaaS, and SaaS Environments. Partners Universal International Research Journal, 2(1), 24-34.

[6] George, A. S., George, A. H., & Baskar, T. (2023). Digitally immune systems: Building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 1(4), 155-172.

[7] Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), 493-543.

[8] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 1-28.

[9] Jhaveri, M., & Parmar, V. (2023). Cloud security information & event management. GIS Science Journal, 10(3), 1-11.

[10] Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), 387-421.

[11] Muhammad, Z., Anwar, Z., Javed, A. R., Saleem, B., Abbas, S., & Gadekallu, T. R. (2023). Smartphone security and privacy: a survey on apts, sensor-based attacks, side-channel attacks, google play attacks, and defenses. Technologies, 11(3), 1-50.

[12] Penwell, T. (2023). Security is not built in a day. In Beginning AWS Security: Build Secure, Effective, and Efficient AWS Architecture, 95-117.

[13] Rehman, S. R., Waheed, M., & Masood, A. (2022). Security-enhanced Android for an enterprise. International Journal of Security and Networks, 17(2), 92-106.

[14] Wong, A. Y., Chekole, E. G., Ochoa, M., & Zhou, J. (2023). On the security of containers: Threat modeling, attack analysis, and mitigation strategies. Computers & Security, 128, 103140.

[15] Younus, Z. S., & Alanezi, M. (2023). A Survey on network security monitoring: tools and functionalities. Mustansiriyah Journal of Pure and Applied Sciences, 1(2), 55-86.