iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.61375

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 V May 2024- Available at www.ijraset.com

Improving Privacy and Security: Artificial Intelligence's Ability to Detect and Stop Threats with IBM SAAS SIEM

Gurunivas Mudiraj
Malla Reddy University, India

Abstract: ***Artificial intelligence has become a vital part of cyber security because of its capacity to assess security threats instantly and respond appropriately. AI currently has a greater influence on identifying and thwarting assaults that maintain companies' technological edge. AI's function in cybersecurity focuses primarily on detection and mitigation. Artificial intelligence uses predictive algorithms and sophisticated data analysis to find trends and irregularities in transmitted data and usage that may indicate a potential cyberattack. This enables security staff to react swiftly and proactively to possible assaults. Artificial Intelligence may be employed to stop assaults by using predictive modeling. The findings suggest that further research and development on the integration of machine learning and artificial intelligence into security platforms has a lot of promise. Among the most intriguing applications found are security for networks, detection of malware, and detection of intrusions and response. The poll indicates that 35% of firms intend to implement machine learning and artificial intelligence throughout existing cyber networks, while 45% of companies have already done so.***
Keywords: Artificial Intelligence, Machine Learning, Cyber Systems, IDS, Malware Identification,Networking.

I. INTRODUCTION

This article is to provide a comprehensive summary of the most recent developments in AI including automated learning. applications for privacy. The study highlights the most potential uses of machine learning and artificial intelligence in information security, including identifying malware, detection of intrusions and response, and the protection of networks. It concentrates on latest studies and breakthroughs in the field of AI. The poll also addresses outstanding research questions and current issues in the field. In order to provide those working in the field with an outline and an overview of the latest state of the field in machine learning and artificial intelligence for information security.

More intelligent technology has effectively substituted the conventional rule-based methods thanks to AI's generalization power . Nonetheless, as the digital environment develops, malicious actors' skill is likewise rising in tandem with technological advancements. Conventionally speaking, the internet had an enormous amount of relatively simple assaults. But the advent of AI-assisted operations by cybercriminals released both known and undiscovered alterations in infection routes, ushering in a whole new age. Because AI and ML have made hacks more effective, hackers are now more powerful than ever. Evidently, several of previous high-profile instances have piqued the curiosity of cybersecurity professionals in GenAI, for both digital offensive as well as defensive purposes.

II. AI'S SIGNIFICANCE IN CYBERSECURITY

Businesses in the public and commercial sectors are currently implementing artificial intelligence (AI) systems, numerous federal agencies are additionally making use of the tech. Artificial intelligence (AI) may quickly and efficiently conserve time and money by skimming through regulated data and thoroughly examining unorganized numbers, voice patterns, and words. In actuality, AI has the potential to protect national Making AI as Cybersecurity Defense :

- Creating accurate fingerprint password-based sign in methods.
- Ensuring connection and identity through a mandate.
- Threat and inappropriate behavior detection using forecasting .
- Better comprehension and reasoning through realistic voice recognition.

More intelligent technology has effectively supplanted the conventional techniques based on rules thanks to AI's generalization ability.

Nonetheless, as the digital landscape develops, cyber threat actors' sophistication is likewise rising in conjunction with advances in technology. Conventionally speaking, internet had a high volume of relatively simple intrusion attempts. But the advent of AI-assisted operations by hackers released both known and undiscovered alterations in infection routes, ushering in a whole new age. Because AI and ML have made hacks more effective, hackers are now more powerful than ever. Evidently, several of previous high-profile instances have piqued the curiosity of cybersecurity professionals in GenAI, for both digital offensive as well as defensive purposes.

Security officers may be given the advantage they need by forecasting AI: to thwart threats earlier instead of later. The field of cybersecurity is going to have to establish formats for data and processes and strike an equilibrium of the two types of machine learning in order to enable artificial intelligence (AI) technologies to independently monitor business operations.Though the name "AI" raises some discussion, it might be the next big thing. While certain individuals applaud AI, others think it's risky to rely too much on it. Some fear that our AI overlords will bring about the extinction of humanity. However, AI's impact on medical care and the global Internet of Everything is still relatively new. Cybersecurity represents the next great technological and economic opportunity.

III. THREAT DETECTION USING ARTIFICIAL INTELLIGENCE(AI)

Regardless of whether it's privacy, information security, or safety at work. One of the most important aspects of maintaining the security of people and companies is threat detection. Artificial intelligence(AI) technology advancements have made it simpler to identify and remove risks in the moment . Alarm systems based on artificial intelligence enable safety devices to identify threats and hazards quicker, accurately, and effectively. With the use of techniques and statistical approaches, artificial intelligence (AI) threat detecting devices may identify patterns in vast amounts of data that may indicate possible threats. A variety of data sources, including social media feeds, network traffic, and CCTV footage, can be utilized to train artificial neural networks to recognize and alert security staff to possible security breaches or threats.

Massive amounts of data may be analyzed in the moment by AI, which can reliably spot anomalies and potential threats. The reason for this is that artificial intelligence (AI) can see patterns in data that humans cannot, and it can identify threats that traditional security systems would miss. Artificial intelligence (AI) can be used, for example, to analyze traffic on a network and identify odd patterns, like a high number of operations starting solely from an Internet Protocol (IP) address.

AI can assess security data to detect and neutralize potential dangers. This is because AI can learn from hazards that are already present and use that knowledge to identify risks that may not yet be known. For example, AI can be used to predict which social media channels a specific actor is a probable target.AI can detect abnormalities in conduct, helping in the identification of zero-day threats. This is because AI can learn typical behavior and identify irregularities in it. AI, for example, may be used to spot anomalous system behaviors that might point to a zero-day attack.

IV. GENAI'S IMPACT ON PRIVACY AND CYBERSECURITY

The growing capabilities of GenAI in cybercrime have shown to be a contradiction that benefits adversaries as well as attackers. Security personnel can use ChatGPT and other GenAI technologies to keep thieves off the network.These systems utilize LLM data, which has been trained on a vast amount of security-related knowledge, including attack signals, strategies, and flaws. With the use of this enormous volume of data, web defenses can enhance their ability to detect and identify new threats and make conclusions.

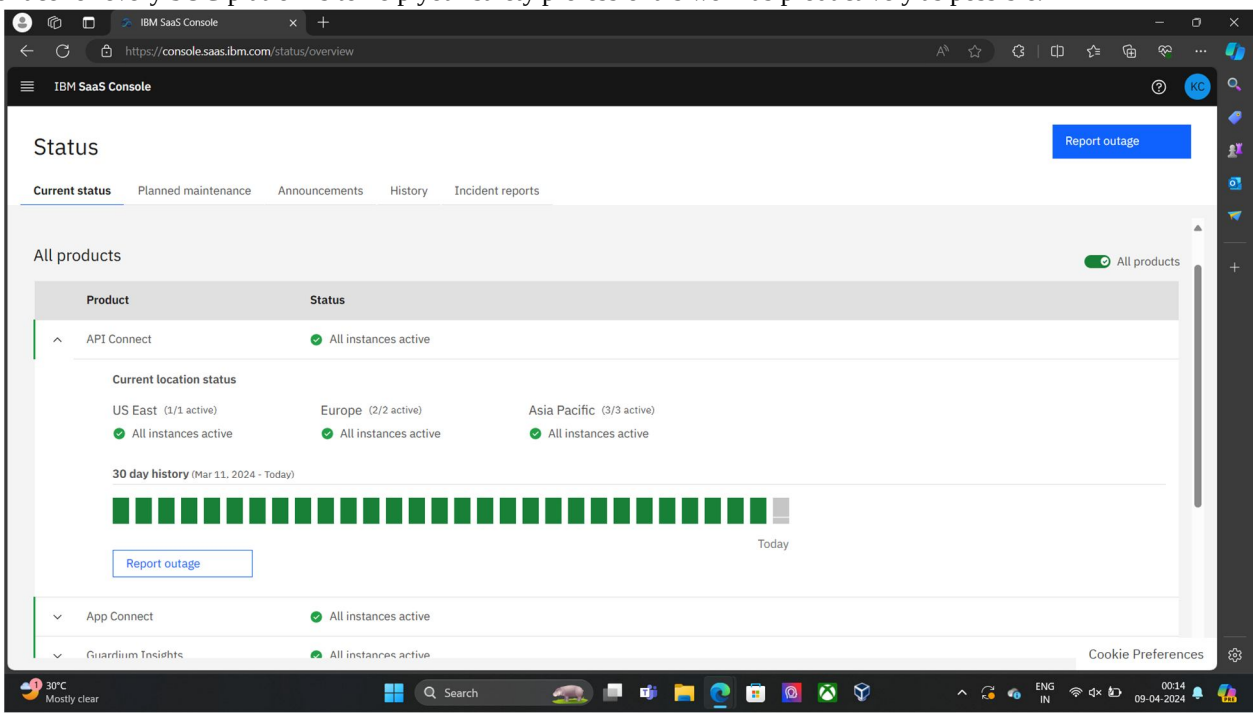
In the event of a cyber incident, the vast amount of recordings, computer results, or information related to network disturbances may be evaluated with the GenAI technologies. Defenders are able to expedite and automate the reaction to incidents as a result.

Given that everyone is now able to utilize GenAI technologies, it is evident that understanding the cybersecurity effects of GenAI models is crucial. Furthermore, ChatGPT is the primary instrument we use in this paper for understanding and evaluating the implications of GenAI on security due to its advanced capabilities and accessibility. There are a few websites on the internet that talk about the advantages and disadvantages of GenAI, however as far as we know, no official scientific article has been written that offers a comprehensive analysis of the technology's effects on cybersecurity. We think that our effort is going to improve our grasp of GenAI through the point of view of cybersecurity is helping partners to better understand the threat, building a strong defense, and advocating for a secure digital environment.

V. IBM SECURITY QRADAR SIEM PERFORMANCE TOWARDS CYBERSECURITY

Security operations center (SOC) researchers play an even greater part than ever as the price of an information theft increases and assaults grow more complex. With its sophisticated AI, potent intelligence about threats, as well as entry to the most recent discovery material, IBM Security QRadar SIEM is not only something to use for SOC analyst it is a partner.

In order to improve signal enhancement, risk scheduling, and event association, IBM Security QRadar SIEM employs different types of artificial intelligence and automating. This results in the coherent presentation of linked warnings in a single screen, which reduces pollution and preserves effort. With integrated, cutting-edge machine learning and robotics features, QRadar SIEM offers one interface for every SOC platforms to help your safety professionals work as productively as possible.



A range of alerting tools are supported by QRadar SIEM to spot alterations in activity directed at devices, computers, applications, and additional network segments. For instance, using an online service or application excessively during off-peak hours, or engaging in internet usage trends that deviate from previous patterns.

In order to accurately analyze and deliver knowledge about a company's network for regulations, danger, and basic network usage tracking, QRadar SIEM has to be able to identify apps above Tier 7. reveal improper transmissions of information by observing behavior on other networks and logging it.

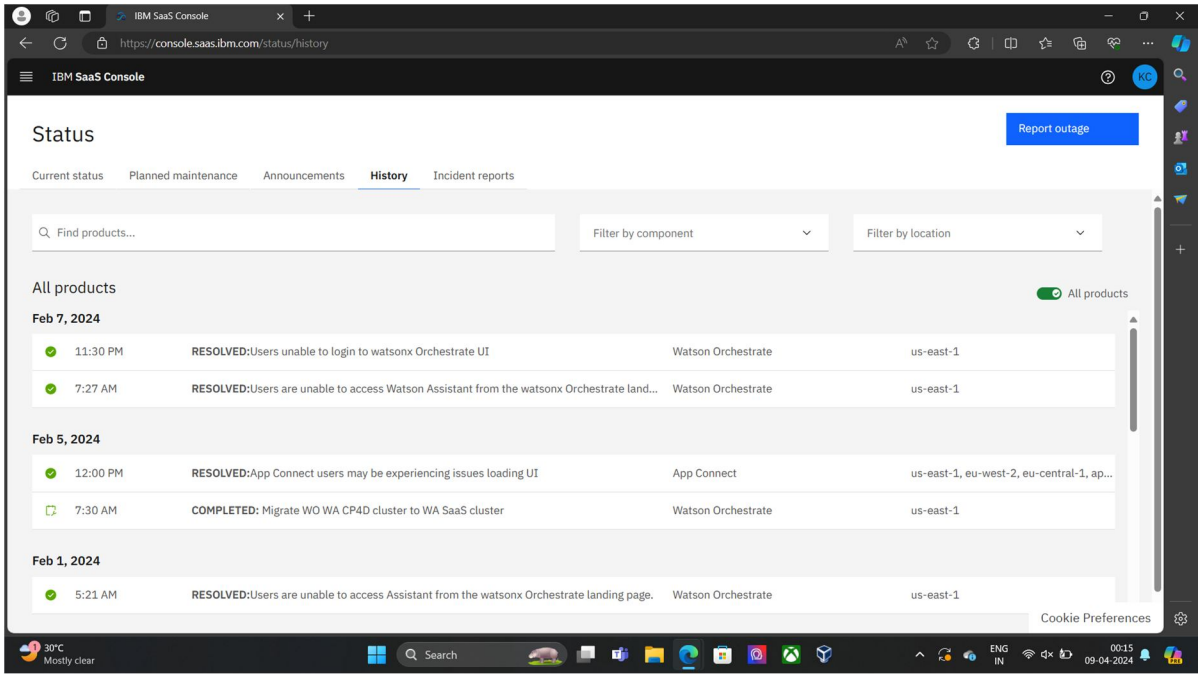
Numerous out-of-the-box abnormal and activity recognition rules are supported by QRadar SIEM. With an easy-to-use filtering feature, users may create custom views and perform detect anomalies for any period of serial data.

VI. CONCLUSION

ChatGPT, powered by GenAI, and various other Legal methods have had an enormous effect on humanity. Humans are completely accepting it and are employing them in a variety of inventive ways to compose songs, write phrases, and create artwork.

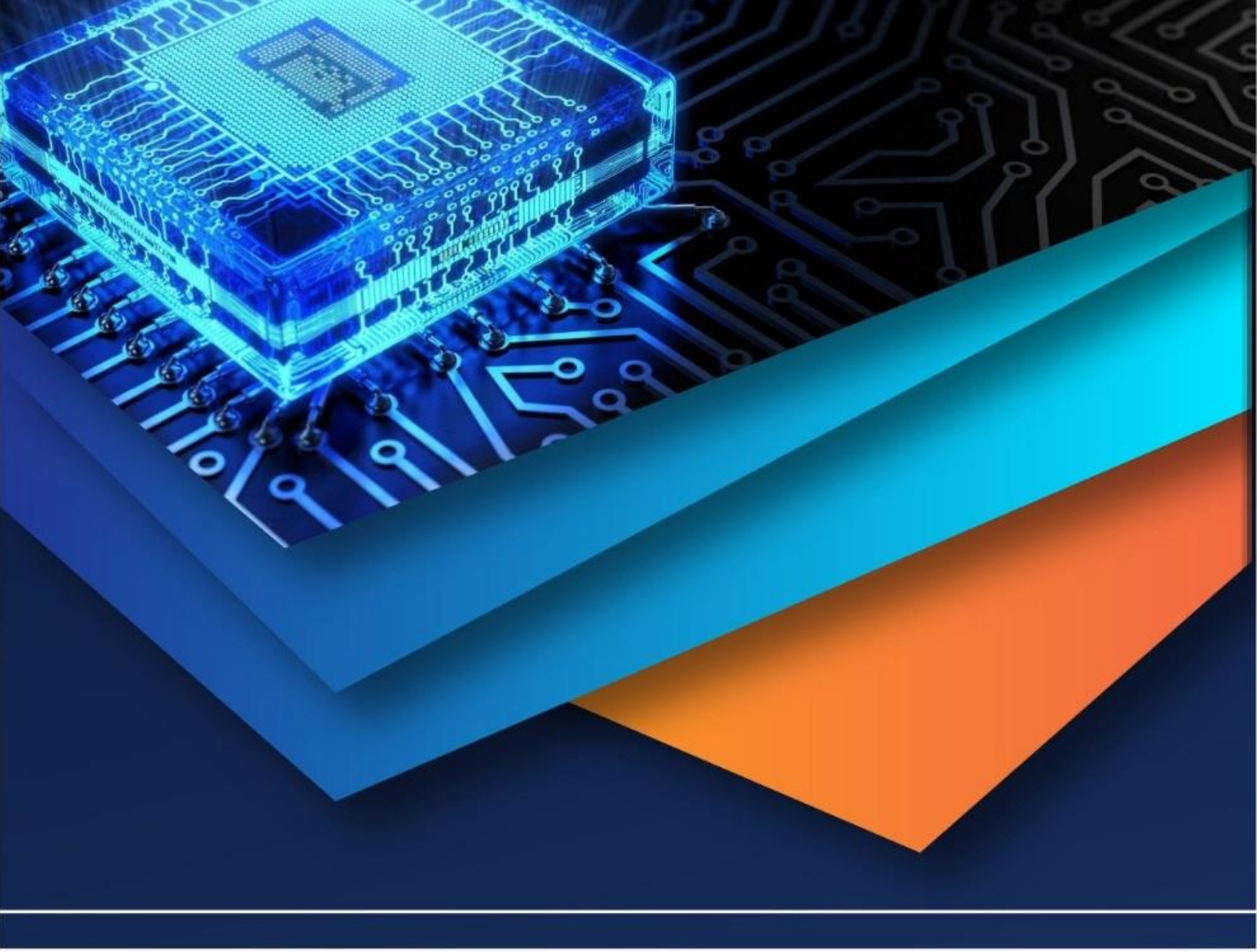
It appears that there is hardly a field in which this innovation hasn't grown and infringed on applications.It goes without saying that security is no unique, with GenAI having a major impact on how a company's safety record will change in response to the strength and danger that ChatGPT (as well as other LLM technologies) offer. This essay makes an effort to methodically examine and discuss the difficulties, restrictions, and possibilities that GenAI presents in the field of cybersecurity.

We still believe that the benefits of AI in internet safety outweigh the drawbacks, despite some drawbacks. Ultimately, human beings are incapable of processing the volume of data at the required pace to ensure the security of your system and data. AI is capable of doing this without the need for food, rest, or vacation time. All of this is not to argue that human intervention is no longer necessary in cyber security, of course. Cybersecurity still requires the human aspect.



REFERENCES

[1] G. A., S. (2022). The Review of Artificial Intelligence in Cyber Security. International Journal for Research in Applied Science and Engineering Technology, 10(1), 1461–1468.
[2] Harel, Y., Gal, I. Ben, & Elovici, Y. (2017a). Cyber security and the role of intelligent systems in addressing its challenges. ACM Transactions on Intelligent Systems and Technology,
[3] Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (2021). WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings.
[4] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. IJARCCE, 11(9).
[5] Nong Ye(2000), ”A Markov Chain Model of Temporal Behavior for Anomaly Detection”, Proceedings of the 2000 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point,pp. 171-174.
[6] Ye, Nong, et al(2001), "Probabilistic techniques for intrusion detection based on computer audit data." ,Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions, Vol.31, No.4, pp.266-274..
[7] Poulose Jacob, K., and Varghese Surekha Miriam (2007), "Anomaly Detection Using System Call Sequence Sets." , Vol.2, pp.14-21.
[8] Rahul Rastogi1, Zubair Khan2, M. H and Khan (2012), “Network Anomalies Detection Using Statistical Technique : A Chi- Square approach.”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, pp.515-522.
[9] Gyanchandani, Rana.J.L, Yadav.R.N(2012), ”Taxonomy of Anomaly Based Intrusion Detection System: A Review”, International Journal of Scientific and Research Publications, Volume:2, Issue:12,1 ISSN 2250-3153.
[10] Seongjium Shin, Seungmin Lee, Hyunwoo Kim, Sehum Kim (2013), “Advanced Probabilistic Approach For Network Intrusion Forecasting and Detection.“, Expert system with applications, Vol.40, pp. 315 – 322,.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY