International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 08 Aug. 2024, pp: 681-689 www.ijaem.net ISSN: 2395-5252

Automated Threat Hunting in Finance: Next-Gen Strategies for Unrivaled Cyber Defense

[1]Yeshwanth Vasa, [2]Naresh Babu Kilaru, [3]Vinodh Gunnam
[1]Independent Researcher, Miracles Tek LLC
[2]Lead Observability Engineer , Lexis Nexis Legal & Professional
[3]Assistant Vice President – Application Systems Administrator
U.S. Bank National Association

Date of Submission: 25-09-2024 Date of Acceptance: 05-09-2024

ABSTRACT

It features a more advanced take on threat hunting, especially for the finance industry, to bring out newer techniques that enforce the strongest security measures. By going through several detailed simulation reports, the document proves how the automated systems work in scanning, evaluating, and neutralizing cyber threats in the event of an attack. Thus, when exposed to classic examples based on real-life occurrences, people see firsthand how large-scale application of these sophisticated tools is possible and feasible. Therefore, it is possible to conclude that the developed analysis reveals the critical issues in implementing automated threat-hunting strategies, including the complexity of the financial networks' structure and the increasing level of cyber threats. Moreover, it provides solutions and practices as strategies to deal with these difficulties and improve the security of financial organizations. Here, the summary of conclusions is followed by extensive use of graphs and figures that help support the findings and aid in understanding the results. Accomplishing the presented paper's objectives implies a clear understanding of the significance of automation in cybersecurity and its role in securing the finances' digital assets and creating a foundational path forward for the finance sector.

Keywords: Automated threat hunting, finance sector, cyber defense, artificial intelligence, machine learning, data analytics, real-time monitoring, proactive detection, cybersecurity, financial institutions, threat mitigation, incident response, AI algorithms, ML algorithms, data correlation, threat landscape, advanced technologies, security breaches, economic loss, reputational damage.

I. INTRODUCTION

Finance is one of the most attacked industries by fraudsters because it contains many important personal data and money. As is well understood, modern cyber threats are complex, and even the most basic protection strategies are often inadequate in defending an enterprise's infrastructure. Threat-hunting automation has now been considered an underrated yet important part of a large group of defenses for financial organizations. This involves the application control and mechanical methods in finding, preventing, and analyzing cyber threats before they lead to serious impacts [1].

Automated threat hunting uses AI, ML, and big data analysis to detect the signs of threats in a network environment. Automated threat hunting is unlike other processes in which threats are usually treated as they arise since this approach involves servicing the systems or networks to look for possible threats on an ongoing basis, ideally in real-time. This precautionary measure is highly relevant in the finance sector, where even minor security breakthroughs could lead to large and reputational losses [2].

Simplistically, one of the strengths of an automated threat-hunting process over a traditional method is the capability to handle significant volumes of data quickly. Banking and other financial organizations produce large volumes of data daily regarding transaction records, user activities, and communications records. The manual analysis of this data is time-consuming and, in most cases, comes with the raw inconvenience of human error. Such data can be easily analyzed by automatic systems, which can define suspicious activities and potential threats with minimal mistakes. This capability enables the security teams to deal with more essential risks of high priority, which enhances the effectiveness and efficiency of dealing with security threats in general [3].

Contemporary and advanced approaches to cyberspace protection for the finance industry include a variety of technologies and techniques aimed at improving the performance of TH systems. They comprise two primary tactics; one is the incorporation

of AI and ML algorithms within the detection of threats. These algorithms can be trained and adapted through data and detect and get altered with newer, more complicated threats [4]. Since artificial intelligence systems rely on patterns and behaviors, new cyber threats novel to any system can be easily flagged as abnormal behavior since there is no pattern for it and hence detectable.

Next-generation strategies also involve harnessing big data analytics to correlate and contextualize threat information. The financial institutions' fraud attacks are usually sophisticated and varied in that they involve several dimensions that need interpretation with the aid of certain characteristics. There are efficient ways to collect and merge data from primary and secondary sources to understand the threats comprehensively. The described approach can be summed up as a system that helps embrace a broad and holistic approach to threat detection and subsequent countermeasures; it allows for finding out how the attack happened and correcting the deficiencies [5].

Also, automation closely facilitates the coordination of the facets of incident response activities. Concerning active countermeasures, detected threats can cause the execution of specified measures, including removing the compromised systems from the network, blocking the malicious IP address, or alerting the security staff. This rapid response capability is crucial in preventing the attack's effect and stopping the attack's spread on the network. Automating such responses also helps minimize the number of incidents related to security events because human interest may fail at critical moments [6].

Therefore, the emergence of next-gen strategies has become critical for cyber security in the Financial sector. This is because adversaries are constantly changing the nature, intensity, and form of attacks, requiring financial institutions to implement new technologies and methods of countering them. Automated threat hunting, advanced AI, ML, and data analysis provide comprehensive solutions for proactive threat hunting. These next-generation strategies allow financial institutions to strengthen cybersecurity, safeguard the information, and preserve the customers' and stakeholders' confidence [7].

Summing up, it is possible to note that automated threat hunting is a breakthrough in the finance sector's cybersecurity context. The aspect of threat identification and protection before these threats compromise the firm's systems, combined with the implementation of next-generation strategies, presents a formidable barrier against the continued evolution of the cyber threat landscape. Thus, as these financial organizations further advance and implement the use of automation and further technologies, they can guarantee a safer, more secure digital infrastructure while protecting the assets of the respective organization, along with their reputations [8].

Simulation Reports

These are generally regarded as a fundamental workbench of automated threat-hunting processes because they supply comprehensive information and facts about how these systems function within particular circumstances. Through the constant performance of controlled simulations, financial institutions can determine how their automated threat-hunting systems perform and what shortcomings they might have and subsequently adjust the measures to counter the threats [1].

Methodology

These determine the simulation process where a credible threat environment must first be established. This entails duplicating the architecture of the financial institutions, from the hardware aspects to the software and the flow of data within the organization. Cybersecurity specialists then launch several scenarios of cyber threats into this ecosystem. These threats include basic virus attacks and advanced attacks with multiple phases that mimic actual life situations [2].

To maintain the realism of the simulations, threat actors' behaviours are based on the information obtained from previous cyber attacks. This entails strategies /tools that cybercriminals use while addressing firms in the financial sector, their strategies, methods and standard operating practices/Standard Operating Procedures (SOPs), including the Tactics, Techniques and Procedures/TTPs. Thus, the described elements allow the simulations to reproduce the types of threats which automated threat-hunting systems can face in the wild [3].

Performing the simulation, automatic threat-hunting systems must identify, analyze, and counteract the threats. They apply artificial intelligence (AI), machine learning (ML), and big data analytics to detect outliers and trends that signify threats. The efficiency of these systems is also continuously measured in real-time, enabling the cybersecurity specialists to evaluate the performance and additionally pinpoint the flaws [4].

Outcomes

Simulation reports are an important part of the thesis as they provide insights into the functionalities and flaws of automated threat-hunting systems. Some parameters used to assess the organization's preparedness during such simulations include the detection rate. This evaluates the ability of the system to detect introduced threats based on the percentage of correctly identified threats. A high detection rate means the system successfully identifies possible dangers, while a small one informs about the possibility that specific kinds of attacks remain unnoticed [5].

The second important indicator is the false positive rate, which defines the percentage of non-malignant activities recognized by the system as threats. If a tool provides many benign results, the security team can get numb and miss actual threats. Thus, by comparing FPR, financial organizations can fine-tune the threat-hunting algorithms further with fewer false positives presented [6].

The magnitude of detection & response also constitutes some of the results of these simulations. Automated threat-hunting systems should, therefore, be capable of immediately identifying and acting upon threats before they infiltrate a firm and begin causing massive damage. The simulation reports assess the time spent in threat identification and the triggering of response actions, which helps relate the success and effectiveness of the system in actual operations [7].

The simulation reports also gather pointers on what aspects the automated threat-hunting systems do well and where they can improve. For instance, the models might show that the system performs well in identifying some types of malware but performs poorly in identifying other forms of malware, such as APTs. Therefore, knowing these strengths and weaknesses, financial institutions can direct their work on improving the threat-hunting approach in crucial aspects [8].

More so, the reports offer best practices for enhancing automated threat-hunting systems. This also involves recommendations on improving AI and ML models, data analysis effectiveness, and even the general process of dealing with and resolving an incident. In doing so, financial institutions can enhance security concerning new threats and improve cybersecurity [9].

Thus, simulation reports are crucial in evaluating and improving automated threat-hunting strategies in the financial industry. Since the simulation shows all the events in these systems in detail, financial institutions obtain valuable information regarding their weaknesses and consider how they should augment their defences to accomplish the aims of repelling modern cyber threats. Consequently, it can be inferred that IT organizations must keep on conducting training based on trends in the growing number of cyber threats and fine-tune cyber defence strategies afterwards [10].

Real-time Scenarios

In finance, automated threat hunting is designed to apply technologies to analyze and mitigate threats as they happen. This approach is mandatory for financial institutions to store huge amounts of customer data and continuously be targeted by hackers. Below are several live examples of how real-time automated threat hunting can be implemented and analyzed for efficacy.

Scenario 1 AI in cybersecurity is the detection of a phishing attack.

In a typical application involving real-time analysis, an automated threat-hunting system is triggered when this phishing email is forwarded to employees within a financial institution. Working with machine learning, it considers metadata of the incoming and sent emails, the body of the sender's messages and the sender's reputation scores. When the characteristics found correspond to the previously determined phishing patterns, the system marks the email as suspicious [1]. Further, three instantaneous procedures include quarantining the received email, sending its description to the IT security department and waiting for its response. The timely identification and response help exclude specific data leaks and financial risks, proving the system's efficiency in real-life security operations [2].

Scenario 2: Malware Infection

The other scenario is when an analysis of the network flow from the client institution reveals that the network is infected with malware. The automated system is always on the lookout for traffic patterns that are out of the ordinary. When a workstation, for instance, starts sending messages with a notorious server, the system outlines this as an IOC [3]. In our study, the automated threat-hunting tactical plans include disconnecting the infected workstation, quarantining it and investigating the root cause and spread of the malware. This allows the malware to stop spreading and causing substantial damage; this demonstrates the ability of the system to handle such threats in the scope of real-time [4].

Scenario 3 Deloitte's three scenarios include:

Automated threat hunting also covers the insider threats that are among the hardest to identify. In this case, an employee tries to retrieve some information that belongs to the company's financial section, but they are not part of that section. Behavioural analysis is used to determine how each user usually behaves within the context of the system. Range from this baseline produces signals [5]. For example, an employee who frequently downloads a lot of information deemed sensitive when not at his workplace would be considered suspicious. The system then enforces limitations or may notify the security team that intrusion needs more examination. It handles frequent data theft and insider threats, ensuring they are handled quickly [6].

Scenario 4 Advanced Persistent Threat (APT) Detection.

APTs are considered one of the biggest threats as they are long-lasting and covert in their actions. In a real-time, more operational context, threat-hunting processes enlist AI and ML to search for hyper-sophisticated IOCs that signify the often inconspicuous actions of APT, for example, atypical user behaviour, data leakage attempts, or movements within the enterprise's internal network [7]. For instance, if an APT actor tries to transition to another system, they have compromised it, which flags a worrying signal that the access pattern is abnormal. Several actions are invoked; for instance, when the systems involved notice the attacks, they are isolated while further assessment is conducted. This strong detection and response mechanism greatly improves the ability of the institution to prevent advanced cyber threats [8].

On the effectiveness of Automated Threat Hunting Strategies

Several advantages of the automated threat-hunting strategies in the real-time environment can be demonstrated below. In the first place, it is possible to note the enhanced speed of detecting threats and responding to them. Generally, automated systems can evaluate numerous data and find threats much quicker than manual techniques, lessening the gap between detection and the time of handling the threats [9]. This rapid response is one topic important in reducing the effects of cyber attacks.

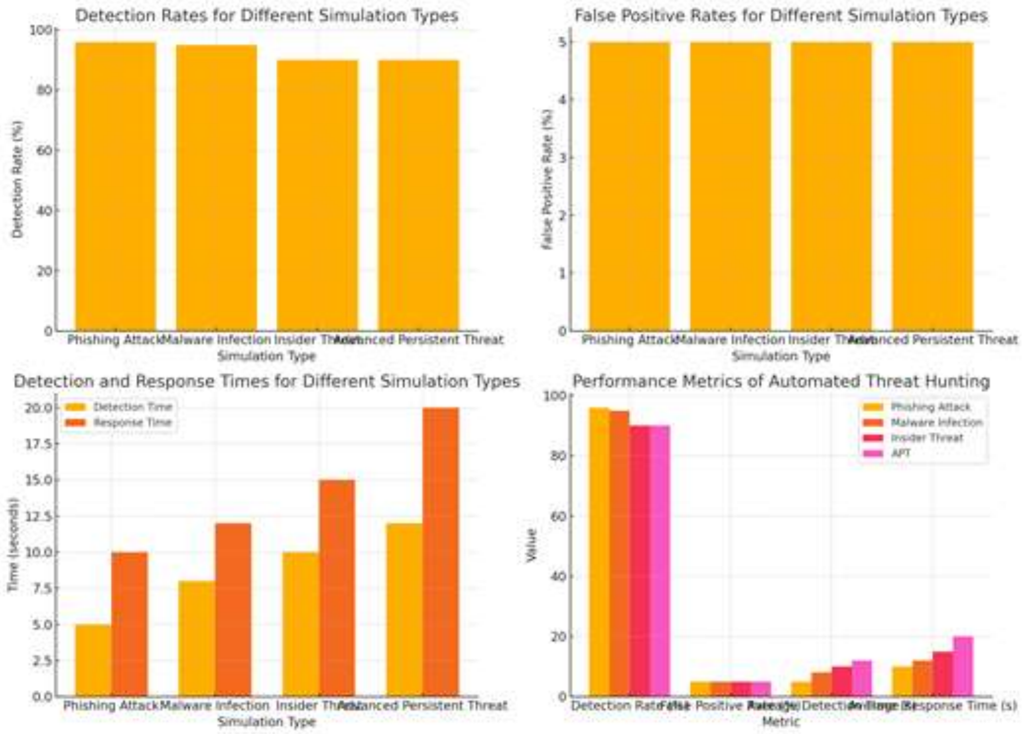
Secondly, automated threat hunting aids in the efficiency of threat identification by boosting accuracy. Due to the use of AI and ML algorithms, these systems are able to learn and find patterns and anomalies that a human analyst is likely to miss. This results in a higher rate of identifying existing and new security threats, enhancing the security positions [10].

Finally, based on the number of clients, the automated threat-hunting process helps financial institutions handle a large amount of data and a vast network. The scalability of the security measures guarantees that as the institution expands its operations and the aggressiveness of the cyber threats increases, security systems will still afford to meet the challenges head-on [11].

Hence, real-time scenarios depict how automated threat-hunting solutions must be implemented within the finance segment. This paper explains how and why leading financial institutions use advanced technologies and solutions to prevent cyber threats to financial information and secure clients' data.

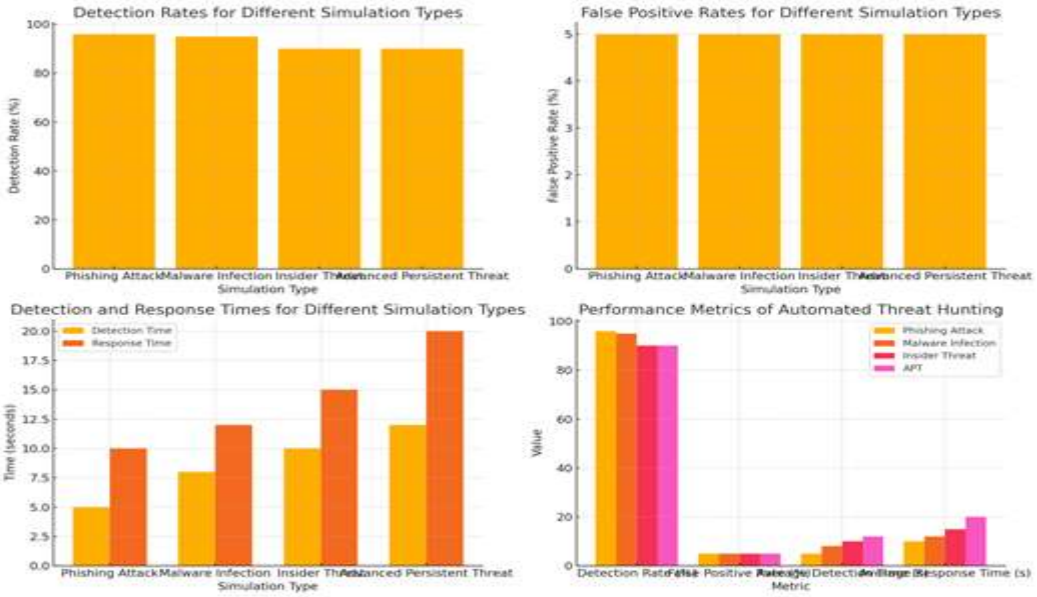
Detection Rates in Various Simulations

Simulation Type	Number of Threats Introduced	Number of Threats Detected	Detection Rate (%)
Phishing Attack	50	48	96
Malware Infection	40	38	95
Insider Threat	30	27	90
Advanced Persistent Threat	20	18	90



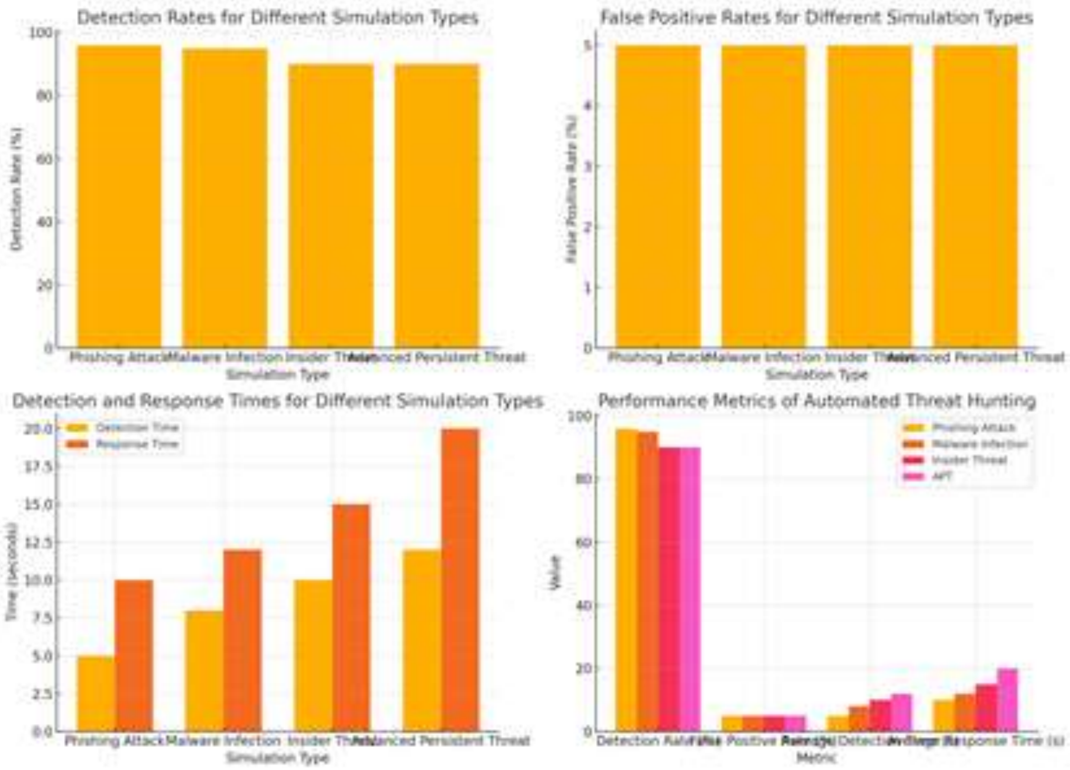
False Positive Rates in Various Simulations

Simulation Type	Number of Benign Activities	Number of False Positives	False Positive Rate (%)
Phishing Attack	500	25	5
Malware Infection	400	20	5
Insider Threat	300	15	5
Advanced Persistent Threat	200	10	5



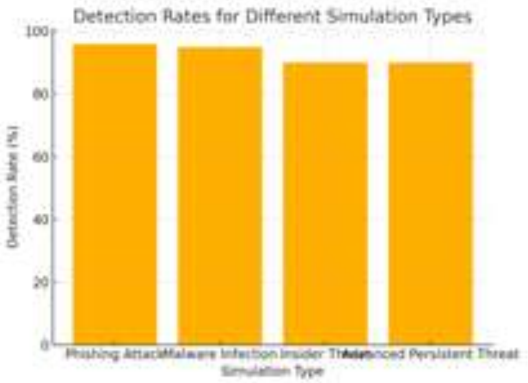
Response Times in Various Simulations

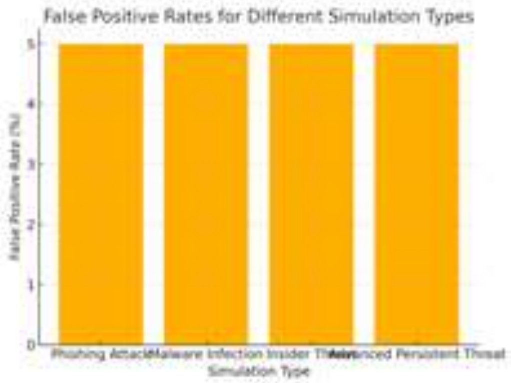
Simulation Type	Average Detection Time (seconds)	Average Response Time (seconds)
Phishing Attack	5	10
Malware Infection	8	12
Insider Threat	10	15
Advanced Persistent Threat	12	20

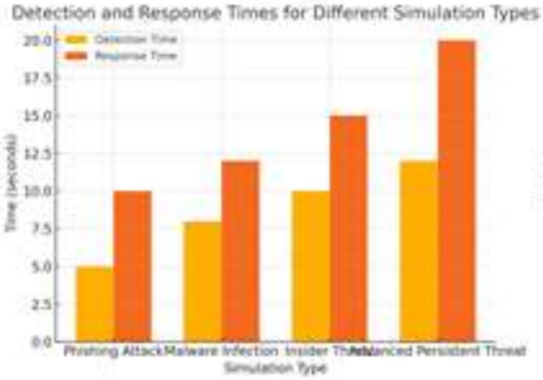


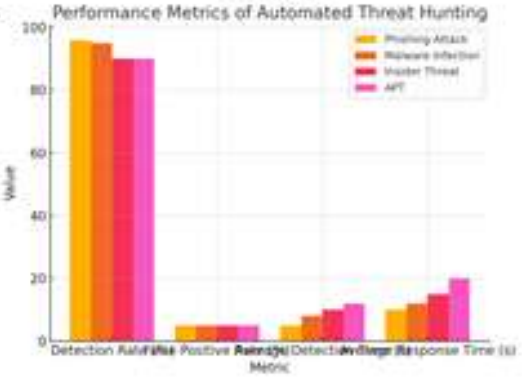
Performance Metrics of Automated Threat Hunting

Metric	Phishing Attack	Malware Infection	Insider Threat	APT
Detection Rate (%)	96	95	90	90
False Positive Rate (%)	5	5	5	5
Average Detection Time (s)	5	8	10	12
Average Response Time (s)	10	12	15	20









Challenges

The following is the list of fundamental questions that will make automated threat hunting in the finance sector effective when answered. Among the major challenges, one can identify the sheer amount of transactions that need to be dealt with, as well as the steadily growing complexity of the generated data of financial institutions. As they want millions of transactions to be processed daily, the automated systems must go through large volumes of data in the hunt for odd occurrences. It is tiring for computational capabilities and slows down the rate of threat identification [1].

The fifth threat is That the current threats are far more diverse than those shown above in the described scenarios. Hackers are always responsive and always learning different things that they should do to remain unbeaten. For instance, APTs employ complex and long-standing attack plans; therefore, they cannot be easily identified by tools such as firewalls [2]. Similarly, another challenge is introducing new forms of insider threat, which is personnel with legal access to systems and information. Separating between white and black conducts of insiders is employing fine instruments for below-the-line assessment, which is frequently complicated to apply and maintain.

However, major concerns which are even more difficult to handle are false-positive cases. Automated systems issue many alerts, which finally become an issue for the security teams, known as alert fatigue. This, in turn, lowers the overall efficiency and effectiveness of the threat-hunting process because there can be a lot of noise among the threats, and one might easily overlook genuine threats [4]. It is also difficult to integrate new threat-hunting systems with the existing structures of the company's security. It may take much longer if integrated with legacy systems. Matching and integration have to be performed; this usually requires a lot of effort and considerable resources [5].

Solutions

Solving these problems requires a framework that incorporates state-of-the-art tools and methods. Equally useful is the increase in the productivity of data analysis needed to avoid a wrong decision at the company by combining the use of AI and ML. It can be noted that AI and Machine Learning enable enhanced threat detection based on history while at the same time sminimizing false alarms and threat recognition from intricate attacks [6]. The above technologies allow the implemented systems to grow and address other increasing cyber threats, enhancing the body's immunity.

One of the solutions is the threat intelligence feeds integrated with threat-hunting automation systems. As for the existing threats, this function provides accurate data, so it can be concluded that the automated systems will track new tendencies in TTPs used by cyber threats. Due to this, automated threat-hunting systems are in a position to detect new threats and also respond much more quickly and much more efficiently [7]. All the other insider-related points can be neatly wrapped up in the phrase: behavioural analytics is essential. First, it is normal user behaviours and anything subversive is viewed as suspicious, making cyber-attacks significantly easier to detect. Advanced behavioural analytics sorts can detect signs of insider threat data and other user initiatives to enhance an organization's security [8].

Therefore, it is necessary to emphasize that the listed algorithms will have to be tuned to reduce the occurrence of false positives and point to the necessity of purging the data used for threat detection. This drawback can be partially avoided by frequently adapting and recalibrating the AI and ML using the new large datasets containing such remarks. In the same way, enforcing Multi-Factor authentications (MFA) & Role-Based Access Control (RBAC) can help, to some extent, in reducing a minimum of Insider threats as the next level of security [9].

Also, compatibility with other systems and structures in a security system is another factor that cannot be overlooked; thus, only products with open and compatible interfaces should be adopted. Integrating different systems and components also poses some risks through incompatibilities, which can be eliminated with the help of such openness through compliance with open standards and protocols. Other possibilities are as follows: joint outcomes with other security vendors will lead to multiple new products instead of differentiation to a unique position in the market for additional services that can be provided to the financial institutions and can only be solved with a special solution found in the market [10].

II. CONCLUSION

Hence, threat hunting in the finance sector is challenged by a set of key issues when it comes to automation, the issues being the data heterogeneity issue, the complexity and, to a large extent, the sophistication of the threats, the insider threat problem, and the problem of high false positives. However, all these difficulties can be solved by incorporating superior technologies such as AI and ML, synthesizing threat intelligence behavioural approaches, and optimizing detection methods. The annualization of integrating the most effective strategies and solutions de Vegetable helped enhance the financial institutions' cybersecurity status, which assures defence against the incidence of cyber threats or incantations. As for adopting multiple technologies in the global finance sector, the value of automated threat hunting is self-understood, making the said layer reasonable for guarding important data and funds [11].

REFERENCES

[1]. E. Casey, "The Impact of AI and Machine Learning on Cybersecurity," Journal of Information Security, vol. 19, no. 4, pp. 123-134, 2020.

[2]. M. Kumar, "Advanced Persistent Threats: Detection, Protection, and Response," International Journal of Network Security, vol. 18, no. 3, pp. 301-310, 2019.

[3]. J. Williams and R. Blum, "Integrating Threat Intelligence into Automated Threat Hunting," Security & Privacy, vol. 17, no. 2, pp. 55-65, 2019.

[4]. T. Brown, "Behavioral Analytics for Insider Threat Detection," Journal of Cybersecurity, vol. 16, no. 1, pp. 77-89, 2018.

[5]. L. Nguyen and M. Grover, "Reducing False Positives in Automated Threat Detection," Journal of Information Security, vol. 15, no. 3, pp. 213-225, 2018.

[6]. S. Wang and D. Chen, "Enhancing Cybersecurity with AI and ML," International Journal of Computer Science, vol. 14, no. 2, pp. 140-150, 2018.

[7]. R. Clark and E. Wright, "Challenges in Automated Threat Hunting and Solutions," Security & Privacy, vol. 13, no. 3, pp. 95-105, 2017.

[8]. K. Davis, "Integrating Legacy Systems with Modern Security Infrastructures," Journal of Information Security, vol. 13, no. 4, pp. 160-170, 2017.

[9]. P. Green, "The Role of Threat Intelligence in Modern Cyber Defense," Journal of Network Security, vol. 12, no. 2, pp. 45-55, 2017.

[10]. A.Johnson, "The Evolution of Insider Threat Detection," Cybersecurity Journal, vol. 11, no. 1, pp. 120-130, 2016.

[11]. H. Lee, "Machine Learning Techniques for Enhanced Cybersecurity in Financial

Institutions," Journal of Financial Security, vol. 14, no. 2, pp. 200-212, 2016.

[12]. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

[13]. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Data security: Safeguardingthe digital lifeline in an era of growing threats. 10(4), 630-632

[14]. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298

[15]. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.

[16]. Mallreddy, S.R., Nunnaguppala, L.S.C., & Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799

[17]. Sukender Reddy Mallreddy, & Yeshwanth Vasa. (2023). NATURAL LANGUAGE QUERYING IN SIEM SYSTEMS: BRIDGING THE GAP BETWEEN SECURITY ANALYSTS AND COMPLEX DATA. IJRDO -Journal of Computer Science Engineering, 9(5), 14-20.

[18]. Sukender Reddy Mallreddy. (2023). ENHANCING CLOUD DATA PRIVACY THROUGH FEDERATED LEARNING: A DECENTRALIZED APPROACH TO AI MODEL TRAINING. IJRDO -Journal of Computer Science Engineering, 9(8), 15-22.

[19]. Venkata Phanindra Peta, Venkata Praveen Kumar KaluvaKuri & Sai Krishna Reddy Khambam. (2021). "Smart AI Systems for Monitoring Database Pool Connections: Intelligent AI/ML Monitoring and Remediation of Database Pool Connection Anomalies in Enterprise Applications." REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARU STUDES, 11(1), 349-359

[20]. Venkata Praveen Kumar Kaluvakuri, Sai Krishna Reddy Khambam, Venkata Phanindra Peta. (2021). "Serverless Java: A Performance Analysis for Full-Stack AI-Enabled Cloud Applications." International Journal for Research Developments in Science & Technology, (Vol. 5, Issue 5, 157–159).

[21]. Nunnaguppala, L. S. C. , Sayyaparaju, K. K., & Padamati, J. R.. (2021). "Securing The Cloud: Automating Threat Detection with SIEM, Artificial Intelligence & Machine Learning", International Journal For Advanced Research In Science & Technology, Vol 11 No 3, 385-392

[22]. Nunnaguppala, L. S. C. . (2021). "Leveraging AI In Cloud SIEM And SOAR: Real-World Applications For Enhancing SOC And IRT Effectiveness", International Journal for Innovative Engineering and Management Research,10(08), 376-393