Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 11 Issue 5, May - 2024

Security Auditors' Perspective in Tackling Cyber-Threats

Oluwatosin Amodu
Department of Information Security,
University of The Cumberlands, Kentucky, USA oamodu23777@ucumberlands.edu

***Abstract*—The persistent rise in cyber threats necessitates an evolving and proactive stance in cybersecurity. This study explores the perspectives of security auditors on effectively tackling these cyber threats. By analyzing the methodologies, tools, and strategies auditors employ, the research identifies critical components for enhancing organizational defenses. Security auditors emphasize the importance of comprehensive risk assessments, continuous monitoring, and adaptive security frameworks. They advocate for a synergistic approach, integrating advanced technologies such as artificial intelligence and machine learning with traditional security measures. Additionally, the auditors highlight the need for robust incident response plans and ongoing staff training to mitigate human error. This study underscores the pivotal role of security auditors in fortifying cybersecurity postures and provides actionable insights for organizations aiming to bolster their resilience against cyber-attacks [1].**

Keywords—Cybersecurity, Security auditors, Cyber threats, Risk assessments, Continuous monitoring, Adaptive security frameworks, Artificial intelligence, Machine learning, Incident response plans, Organizational defenses, Proactive stance, and Advanced Technologies

1. Introduction to Security Auditing

Vulnerability disclosure is not a dichotomy of open versus closed but a spectrum of approaches. Traditionally, vulnerabilities, once discovered, were disclosed discreetly. This practice changed in the 1980s, resulting in most software vendors recognizing the need to establish a dedicated security team, such as an incident response team or similar role, to manage the coordination of vulnerability handling [2]. More recent decades have seen an increased push towards responsible disclosure, coordinated disclosure, and bug bounty programs, all designed to promote a more coordinated approach to disclosing accurate and proportionately informative information about vulnerabilities and maintaining vigilance in maintaining the privacy and secrecy of the same. Often, security auditors and compliance bodies or professional bodies might have different normalization techniques of quantitative and or qualitative approaches to security compliance, and hence, the guidelines of disclosure should be properly followed. It is often seen that auditors indulge in scorched-earth disclosures that neither benefit the user nor the acquirer of the technology.

Security auditing is the practice of reviewing an organization's security policies and infrastructure to uncover security weaknesses [3]. Security auditing is a fundamental part of information security, ensuring that an organization’s security posture meets the organization's policy and procedural requirements. Security errors are the leading cause of security breaches. Failures can be attributed to errors in software development, system integration, component selection, parameter settings, and lack of procedures and policy enforcement. Security auditors follow a large number of guidelines or checklists to audit the security of an organization [4]. A lot of tools and automated techniques are available for auditing the security policies, local security and remote security of a network.

1.1. Definition and Purpose

Initial security audit preparation notices the need to inspect organizational policies, security protocols, client records, risk management practices, details of IT infrastructure, business processes, evidence of previous security audit results within the organization, plans for tech updating, etc. The output of this step helps security auditors shape the security audit strategy and audit inception. The inception phase lays the foundation for security auditors in a manner that understands the business requirements and objective within the given assessment period Grounding in information security controls, readiness assessment, and risk management (ITcRA) defensible security coursework are essentially performed to administer the breadth and depth of the upcoming security audit.

Not all risks can be identified with absolute certainty, no matter how methodically the security process has been designed. Primarily, a security audit operates on the assumption that any security breach can occur due to unpredictability. Security Auditors are mainly responsible for conducting the security audit with the help of different skills acquired from diverse, often legislative, and technological backgrounds. Generally, security auditors possess a critical skill set like analytical skills, technical skills, communication skills, problem-solving abilities,

computer forensics skills, Knowledge of regulations and laws, etc. At the same time, data security knowledge, information technology skills, management skills, business awareness skills, etc.

Security auditing is an essential aspect of organizational management that seeks to identify the formidable and inherent cyber risks within an entity's system by assessing the strength of the security protocols, awareness/training, and policies of an organization. Security auditors are cybersecurity professionals or teams that specialize in system verification, analyzing networks, ensuring data protection and encryption, safeguarding information through backups, and detecting security defects [5]. The main aim of a security audit is to protect valuable resources, break down the security burdens, and prevent the risk of privacy breaches, security breaches, cyber-attacks, or unauthorized access within the organization. A security audit holds the intrinsic asset to mitigate potential information security incidents by mitigating the risk of unauthorized access into the company's computer network, which limits and ultimately reduces the damage of security breaches and compliance-related violations.

1.2. Role of Security Auditors

Our results provide empirical evidence for the need for the inclusion of RBAC-related standards within enterprise frameworks for IS. The conceptual framework proposed serves as a guide for IS professionals in using RBAC to make IS audits more effective. Evidence for the consideration of legislation to make the integration of RBAC with IS audits more uniform is provided as well. Finally, the study demonstrates that ISAs play a critical role in enterprise IS governance and that not only does strategic importance exist for IS audits, but they are important for tactical and operational concerns as well [6].

Security auditors are valuable in determining whether security practices are being updated regularly, and if they provide value with regards to minimizing the risk of security breaches. They also help in understanding why security practices remain as-is or provide insights into providing value to upgrading certain devices [2]. Thus, the role held by security auditors is crucial, especially in a digital world where time is of the essence and flexibility is vital when responding to daily cyber threats. The purpose of our work is to understand the multifaceted roles that Information Security Auditors (ISAs) perform, using Role-Based Access Control (RBAC) as the principal interview guide. We participated in one-on-one interviews with seven ISAs, to discuss their nuanced roles as well as how they use RBAC in implementing Information Security (IS) audits. In utilizing the data collected, we theorize that ISAs play a pivotal role in ensuring that IS controls and protections are not just fully implemented, but enforced across the enterprise, across silos or business units.

Security auditors are responsible for performing thorough cybersecurity checks and are critical when it comes to ensuring security controls and protections are fully implemented and enforced **[7].**

2. UNDERSTANDING CYBER-THREATS

The continuous progression of virtualization and client-server architecture technology lies at the root of fulfilling computing needs at the time of the advent of the internet. Then the client-server computing model caught industry, academician, researcher, and layman's interest like wildfire; most of the computation was carried out on the server side. Building or constructing the main purpose of virtualization was to run multiple Virtual machines (VMs) at the same time independent of each other. The server side having high processing and memory resources became a playground to host multiple virtual machines (VMs) concurrently.

Fog computing, a distributed computing model that provides edge computing, is well-suited as an effective platform to enhance security features. This article illustrates the security mechanisms and algorithms and performs comprehensive training, testing, and deployment through real-world implementations [8]. In the upcoming era, fog computing is a solution for cyber threat treatments and incident handling. It focuses on network communication, DNS security, firewall network, and testing, adding security layers to the embedded devices spanning the network by which instant decisions could be made over the security attacks and incidents without any dependence on the cloud. This exploit-based approach, which is considered practical and efficiently works, is in common use by all penetration testers, cybersecurity researchers, and ethical hackers alike [9].

Introduction From a general perspective, cyber threats evolve in many dimensions and impose severe challenges for cybersecurity defenses. The Article classifies the cyber threats and models the security through two frameworks, the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevating of privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability). Therefore, a complete security model is established; many defense mechanisms and countermeasures should be in place to resist or prevent cyber-attacks or security threats [10].

2.1. Types of Cyber-Threats

It is also mentioned that various studies released different categorizations of threats due to which, the international standard organizations Organization for Economic Co-operation and Development (OECD) and Information Technology Study Group (ITSG) have classified internet cyber threats into three categories such as threats to confidentiality, threats to integrity, and threats to system availability, which have helped to classify and discuss cyber threats [11].

However, different entities have defined types of cyber threats in different ways. To clarify misinterpret being conducted in the classification of cyber threats, there is a scientific and systematic process. Though cyber-attacks have been classified differently according to certain situations from the perspectives of different authors, considering the implementation of cyber-attacks, cyber threats have been divided into different categories. There are mainly four categories into which cyber-threats have been divided namely, WEB-ORIENTED THREATS, CLIENTORIENTED THREATS, BOTNET THREATS, and NETWORK SERVICE THREATS. This has implemented innovation in the classification of cyber threats on valuable resources.

The network-based cyber-attacks can be conducted using a wide range of attack tools, techniques, or methodologies to compromise information-based assets such as hardware, software, and corporate networks as well as to seek unauthorized access to sensitive information and services. Each attack is also focused primarily on an organization, affecting its specific security view, and these are normally well-armed to tackle any form of cyber threat. Moreover, every threat increases the fear of everyday attacks as per the rise of new technologies and management practices, which must be protected against the same. Nevertheless, in terms of categories of cyber-threats, security incidents are classified into many types like malware, phishing attacks, system failure, password attacks, and breaking of configurations [12].

2.2. Common Attack Vectors

Firstly, let us discuss several common attack vectors that are frequently used by attackers, supported by real-world examples. Attack vectors are different ways through which networks and systems can be attacked. “Vulnerabilities in software” remains the most popular attack vector and is the bread and butter for cyber attackers. Attackers use available tools/exploits to gain access and install backdoors, keyloggers, or other malware [4].

Social Engineering and Phishing target human emotions and is a common tactic used by adversaries to manipulate, deceive, or browbeat individuals into giving them confidential information and/or access to an otherwise secure system. It is the easiest, cheapest, and fastest way to achieve the same objective. Anti-analysis refers to a group of tactics used to deter security analysts from reverse engineering or otherwise analyzing the malware or attack. These methods are used to evade inquiry/discovery and have two primary goals, first, critical computation and anti-analysis techniques verify if they are being executed inside a sandbox. If any such mechanism detects that a sandbox is being used, the stage does not perform any function critical to the surrounding malware, second, verify if a dynamic analysis is used to monitor the behavioral characteristics of the stage. By successfully passing checks meant to detect analysis, the stage can manage to chain artefacts without interference [8].

During September and October 2021, a Zero-Day RCE exploit for Apache C* that affected both the Community and Enterprise Editions of Apache Cassandra was identified. This Zero Day allowed any user with the ability to execute arbitrary CQL commands to execute OS-level commands on any node in the cluster. This Zero-Day is rated CVSS 9.8 and affects Apache Cassandra versions 3.0.24 and 3.11.12. Users must upgrade to the below versions as soon as possible to patch their clusters from this Zero-Day and protect their datacenter or cloud environments. In addition to the Zero-Day RCE, these versions also contain multiple non-security-related bug fixes that make them a recommended upgrade for users of affected versions [13].

3. SECURITY AUDIT METHODOLOGIES

One concluding approach to security audit, predominantly applicable to binary systems such as e.g., peer computers, is the model checking both the explicit and the stochastic properties of computational algorithms. Such methods, such as those in probabilistic model checking, represent a topic of valuable, albeit not overly extensive research including its decentralized networked execution in interdependent application contexts as well as in hardware control systems such are health devices. Cyber security threat detection systems have introduced material quality-oriented adversarial classification. There are vast grounds for cyber security conflicts compared with failures, back doors in embedding algorithmic equilibrium and obfuscated logic of evaluation leading to network attack or exploitation.

In network security, the list of vulnerabilities discovered in automated systems is constantly maintained and updated. Tools for network logging and visualization as well as deep packet inspection can assist in the extraction and analysis of network attacks in feature extraction, and reporting. They have

been associated with a variety of IDS enhancement initiatives. Their objective could be to inspect and detect common albeit different novel signatures by suggesting from the familiar variability of cyber threats including those in the context of IoT settings [8]. Cyber systems are continually subjected to unsophisticated risk, albeit not only vulnerable. Some start on attempt attribute in recognizing the possibility of with exploit, equivocation and c principles in decreasing threat of straightforward to you.

Security audit methodologies encompass an array of approaches, which include cyber risk management, cybersecurity assessment, cyber security compliance, cyber penetrative testing, cyber intrusion simulation and cyber emulation simulation. Some of these endure; for example, a considerable amount of literature is published on the development of vulnerability analysis directed towards reverse engineering methodologies, as well as red teaming and penetration testing automation [14]. Vulnerabilities might be limited solely to the application objective of performing root analysis, which is essential for verifying secure system partitioning and testing vulnerability severity or for a tool for an assessment, such as an application vulnerability identifier (acronyms and little words: AVI or AVID). Analysis of known vulnerabilities could additionally be used to evaluate the overall security of the system.

3.1. Pre-Audit Preparation

Pre-audit preparation is a necessary step after the organization expresses their intent to get audited. It is natural to think of pre-audit preparation only in terms of making the security controls ready to be audited. However, auditors understand that security is only partial to what organizations do. All IT security measures are part of a larger system designed to protect valuable assets within the organization. Equally important are the people and processes following the security policies in a cyclical manner known as the PDCA (plan, do, check, & act) cycle. Therefore, the more security control is on paper spread across different departments, the longer lead time is necessary to merge these plans on audit day to demonstrate the controls in the field. In the past, some of the security auditors delayed the audit, recommending that the organization do this merger exercise in the form of ad hoc beta audits. However, security controls having a great area are difficult both in terms of time and resource hiring to be justified as a beta audit. Moreover, many organizations use security controls of high probability and high severity due to the visibility normally seen in the beta audit. Therefore, it is important to address the different aspects of security controls starting from management is materialized in the case of Security 1, Security 2, and non-specialty security. Preparedness for an audit of the same security control differs considerably from the extent of their materialization.

Security Auditors assess the reality of the organization's security posture from the perspective of the organization's stakeholders [4]. As practitioners, they understand that security controls are beneficial but not fail-safe, and therefore also consider the organization's ability to manage the risk posed by threats [3]. In this scenario, assessors do not require specific domain knowledge, or they should acquire it incrementally through a background study or interview by the stakeholders concerned, to assess the security controls. Each threat will have several remedies, encompassing both security controls and the ability to manage the risk posed by the threat. A security auditor with a diverse skill set will be able to quantify the impact of the threats of attackers, their likelihood of success, the extent to which they can be detected in the event of success, the technical measures available for organizations to manage the risks the threat represents, the additional capabilities the organization has to enhance its risk management and expand its operational slot, the additional considerations required for legal and liability reasons, and so on. Increasingly, auditors' considerations are being systematized, particularly regarding security controls and threat management, in threat and control libraries [6]. While such systematizations do give more auditors a head start and allow audits to scale in difficulty, they also require the auditor to be attentive to changes in the organization and threat model to be effective.

3.2. Audit Execution and Reporting

The execution process in phase two is efficient, with practically almost no time being squandered by the time all necessary documents are on hand. However, it is suggested to rely on a risk-based strategy and less on workout compliance-based audits. In using the former strategy, managers first focus on areas or systems likely to have weaknesses – especially those that could potentially facilitate cybercrime – or vulnerabilities due to threats that are not mitigated well [8]. Once they are audited, the firm undertakes to examine those areas or those systems that are less likely to have flaws or be attacked. Lastly, the auditor will climb to very compliant baselines and quality systems that stand between the system/workflow and real-world threats. The final reporting phase represents the most difficult section of the audit item When presenting the management team, the auditor is tasked with persuading them to support the proposals and entice them to allocate the necessary financial and human capital for their implementation.

Security auditors represent a critical line of defense in tackling cyber threats. They undertake the execution of security audits for their clients while

striving to keep abreast of the most recent security vulnerabilities. Security auditor firms may undertake the audit process using different individual approaches and specializing in varied audited information systems [3]. However, they do share several best practices, providing a unique as well as a standardized perspective that is worth understanding and emulating. Regardless of the clientele, demographics, or worldwide locations, a series of documented standard operating procedures (SOPs) significantly demonstrate their constant auditing approach over the years. This is important for the deletion of any hindrances that may obstruct the organization from executing the audit across multiple countries with different regulatory requirements [14]. Shared below are the standard steps for undertaking a standard security audit on any company's environment. Although security auditors prioritize formulation with management to reach a common understanding and establish objectives, obtaining a briefing on the audit to develop a focused scope and audit plan session is indispensable.

4. Tools and Technologies in Security Auditing

Some tools simply rely on generating a flood of events in a system without even knowing the actual state of the system. The number of these tools is countless and many of them are freely available. Many of the security solutions offered by Microsoft are susceptible to flooding attacks and without referring to Open Source applicable for different operating system environments, there are Linux-compatible security tools that generate flooding attacks. The reverse flooding tools are also explored to a very large extent and are freely available. The majority of the systems, be it Unix or Linux systems there are many reverse flooding tools available which allow the computer systems to put up a fight against the attack and avoid the denial of service (DoS) attack, the way flooding is rendered futile by taking extra measures. The message digest is different from conventional encryption. Hash values are encrypted and are not usually decrypted. MD5 is no longer suitable for encryption. The message digest algorithm gets a particular segment of data as an input and generates a fixed-size output.

Security audit in the digital world is the process of evaluating the mechanism of an organization" 's information systems and resources using automated or manual tools, for the identification of their vulnerabilities in all aspects. The tools used in security audits are used for internal as well as external audits and are also known as audit tools. The tools include commercial, shareware and open-source tools [15]. These tools include software for vulnerability scanning, password cracking, network discovery, sniffing, and automated and manual scanning tools. Certain proprietary agents are installed on the systems to which the audit is to be made, sending the collected data to a central server, where it is analyzed using vulnerability management tools. In general, the tools that are used in security auditing can be categorized as logical testing tools, penetration testing tools, network security audit tools, vulnerability assessment tools, and web applications security tools.

4.1. Vulnerability Assessment Tools

To launch and test their attacks, Pentest operates in conformance with the Open Web Application Security Project (OWASP) guide. There is a community collecting, producing as well as distributing principles and methods to deal with internet application security. The altered hacking or assaulting mode against a computer network framework leads to a lower assault range on a real-time basis. An internet security testing method helps the students as well as the corporate campus to understand the protection of web-based applications as well as to improve their theoretical as well as practical knowledge based on security vulnerabilities. It refers to the knowledge of how information leakage results in web application mistakes so that an organization devises an appropriate configuration to shield itself. If an architect or a web developer has adequate information regarding the mentioned issues, it is straightforward for him to utilize permitted deviations as well as lawful proposals to improve the safety prevention criteria that involve InfoSec as well as CyberSec threats and hazards. As a defense against real-time internet assaults, firewalls are of utmost priority in a computer network grid after VPN because such a strategy should be put into place to make sure that continually requested data either by trainees or by associates is permitted based on the regulations of the company.

To defend themselves against novel cyber threats affecting information systems, organizations should conduct routine network penetration testing and security audits, using well-known tools, practices, and standards like OWASP guide and CIS top 20 standards for identifying vulnerabilities that might open doors to potential attackers [16]. Security audits, including internal and external penetration testing and security scanning, ensure that networks remain protected. These security tests must be conducted regularly to match an ever-changing threat environment. Every outward-facing IT system is considered to be at risk and a potential door through which an attacker might enter [9].

4.2. Intrusion Detection Systems

Intrusion detection systems (IDS) are software or hardware-implemented detection systems capable of detecting and following signs of malicious activity as it occurs. They can alarm system users upon detection of signs of malicious activity like in Advanced Intrusion Detection Environment (AIDE),

and OSSEC. Host-based Intrusion Detection System (HIDS) inspects the incoming traffic for each system while Network-based Intrusion Detection System (NIDS) inspects traffic externally on an entire network. There are two methods of detection in IDS: Signature-based detection (Misuse Detection): In this method, preconfigured signatures can consist of variables that help in capturing specific traits of attack into a database and the system inspects the traffic present on the network and compares it to these signatures. Anomaly-based detection (Behavioral Detection): In this method, the system decides traffic as anomalous according to the difference between preserved regular patterns and the traffic examined in the network.

An intrusion detection system (IDS) is a software or hardware tool installed on servers or boundary computers that raises an alert when it detects an activity that may indicate an attempt to breach security policies [17]. It can be detected in two ways, including pattern matching and traffic flow-based detection. Intrusion detection systems have become a vital part of network security as they help to prevent a wide range of attacks [18]. It can be classified into host-based intrusion detection systems (HIDS) and Network-based intrusion detection systems (NIDS) depending on the information source. Although both forms have their advantages and disadvantages, NIDS is based on perimeter networks and sensing traffic so many researchers tend to consider traffic flow-based detection in the prevention of sophisticated cyber threats [19].

5. BEST PRACTICES IN SECURITY AUDITING

Security audits give the organization the authority to identify vulnerabilities in the security system and conclude how the company's data is at risk. By identifying the immediate and future risks, the company can provide the extent and the kind of security it needs. The company will then have a clear idea about which type of security it needs to invest in, to avoid future data thefts. In conclusion, security auditing can be very helpful. The company will have a streamlined idea of what its security requirements are and what security infrastructure it needs to invest in.

It should be kept in mind that all users, including business owners and employees, are potential targets for cyber-attacks and the thing which the entrepreneur should realize that within a matter of days, hours or even in some cases minutes the way an attackers can penetrate the security system. The hackers who have stolen a person's identity can even detect when there are plans, meetings, or conversations with important information which could be useful for authorized access [20].

There are some important precautions every business should take if it comes to crucial data-protecting, network stability and productivity: • All IT systems should be encrypted; • Firewalls should be installed by default on all network-connected devices; • Passwords should change at least every month; • Cybersecurity training should be provided to all members of the enterprise to tell them what should be done in case unauthorized physical or virtual access is detected [4].

Security auditing that is thoroughly conducted and closely observed by the IT team, or the passion and intelligence of a leader's skills to catch some visual and unobvious signs, can save from more than failure in work or damaged productivity. Usually, it is helpful but not obligatory, which means that there is still a possibility to recover from a collision, theft, or an inside breach and reestablish a productive workflow [8].

5.1. Continuous Monitoring and Improvement

In computing resources and cybersecurity risk management are managed by possessing cyber threat intelligence, defining and conforming to prescribed rules, implementing preventative measures and facilitating post-incident recovery. Effective RNSS norm enforcements will necessarily encompass the installation and running of antivirus software and the continuous upgrading and patching of operating systems and applications as well as the configuration and carrying out of security firewalls for recurrent threats. In compliance with insider threats, access management, network segregation, intense checking of the log, etc. offer methods for the avoidance of unambiguous cyber-threats. Access rights to personal data must strictly adhere to established protocols and procedures to reduce and contain the risk of data loss or infringement. Inspections of the configuration of the organization's information system and surveillance of network traffic are crucial. All incidents, including cyber-attacks, must be logged to resolve and record the weighable proof of breaches in information security protocols [21].

Monitoring and measurement functions in a quality management system are an intrinsic part of an organization's effectual operation [22]. Food Standard Agency's research [23] stipulates that "effective measurements are critical to continuous improvement strategy" and the British Heart Foundation advises that the "only way organizations can learn, grow, and have a competitive edge is by assiduously measuring and then improving". It is pertinently apparent that legislation calls for the maintenance of a functioning control panel and, it is surmised, particularly whether the protection concerned is a healthcare institution, a food business, or network security compliance [10].

5.2. Incident Response Planning

Business IT infrastructure, no matter its size, is endangered, and so, sooner or later, every

organization will experience a security incident. Thus, every system and every organization should prepare an incident response plan for major and minor incidents. Every organization defines the division of responsibility into maintenance, the IT department overall management and predefined incident response employees involved in helping the existing standard should be followed by incident response staff in case of accidental perusal, testing or transference within the workplace. Severe security incidents are to be neutralized by the organization according to a predefined scheme; all incidents need to be recorded by the SOC in the organization's information systems. Any information stored and processed during the neutralization process can serve as an important base for analyzing security breaches.

The organization must ensure that the incident response staff is adequately trained in the roles and responsibilities assigned to them. Staff should be trained and ready to respond well in a timely and coordinated manner. After the occurrence of an incident, the organization should iron out both a preliminary approach designed to prevent further harm as soon as possible and a plan for a further investigation of the system's operators. The organization should impose clearly defined guidance for immediate investigation of suspected incidents and authorize operators to follow this guidance.

Well-prepared and quickly prevented incidents are a guarantee of avoiding unnecessary harm to organizations, as security incidents are almost unstoppable. An incident response plan must be a part of the overall business continuity plan. The organizations should ensure that the incident response plan is updated regularly and includes key steps and an action plan managed by the security operation center (SOC). This includes handling classified information produced, processed, preserved, approved, and received by the organization and the SOC, and other categories of organizational information as classified by the organization [24]. The incident response plan should be risk-driven, and its objective should be to significantly reduce the information system-related risks like detection time, response time, recovery uptime and availability [4].

CONCLUSION

The knowledge gained from security auditors emphasizes how urgently a dynamic and comprehensive strategy to counter cyber threats is needed. More than only technical fixes are required for effective cybersecurity; a whole approach is needed, including detailed risk assessments, ongoing monitoring, and flexible security frameworks. Improving detection and reaction capabilities mostly depends on integrating cutting-edge technology like machine learning and artificial intelligence. Moreover, robust event response plans and continuous staff training are necessary to reduce human mistakes and raise organizational readiness. Proactive and cooperative security auditors recommend fusing cutting-edge technology with conventional security protocols to provide a substantial barrier against changing cyber threats. Organizations can significantly improve their cybersecurity posture and guarantee better defense against possible assaults while preserving the integrity of their information systems by implementing these tactics [25].

REFERENCES

[1] Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974.

[2] Larios-Vargas, E., Elazhary, O., Yousefi, S., Lowlind, D., Vliek, M. L. W., & Storey, M. A. (2023). DASP: A Framework for Driving the Adoption of Software Security Practices. *IEEE Transactions on Software Engineering*, *49*(4), 2892–2919.

[3] de Oliveira Albuquerque, R., Villalba, L., Orozco, A., Buiati, F., & Kim, T. H. (2014). A Layered Trust Information Security Architecture. *Sensors*, *14*(12), 22754–22772.

[4] Chaudhary, P.K (2024).AI, ML, and Large Language Models in Cybersecurity. *International Research Journal of Modernization in Engineering Technology and Science*.

[5] Mazzarolo, G. & Delia Jurcut, A. (2019). Insider threats in Cyber Security: The enemy within the gates.

[6] Eiroa, E. F., & Sendra, C. M. (2018). Shadow cast by rotating braneworld black holes with a cosmological constant. *The European Physical Journal C*, *78*(2).

[7] Carboni, A., Russo, D., Moroni, D., & Barsocchi, P. (2023). Privacy by design in systems for assisted living, personalised care, and wellbeing: A stakeholder analysis. *Frontiers in Digital Health*, *4*.

[8] Simeoni, E., Gaeta, E., García-Betances, R. I., Raggett, D., Medrano-Gil, A. M., Carvajal-Flores, D. F., Fico, G., Cabrera-Umpiérrez, M. F., & Arredondo Waldmeyer, M. T. (2021). A Secure and Scalable Smart Home Gateway to Bridge Technology Fragmentation. *Sensors*, *21*(11), 3587.

[9] Tudosi, A. D., Graur, A., Balan, D. G., & Potorac, A. D. (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. *Sensors*, *23*(5), 2683.

[10] Ghanem, M. C., Chen, T. M., Ferrag, M. A., & Kettouche, M. E. (2023). ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance. *IEEE Access*, *11*, 129840–129853.

[11] Paredes, J. N., Simari, G. I., Martinez, M. V., & Falappa, M. A. (2021). Detecting malicious behavior in social platforms via hybrid knowledge- and data-driven systems. *Future Generation Computer Systems*, *125*, 232–246. https://doi.org/10.1016/j.future.2021.06.033

[12] Gavilanez, O., Gavilanez, F., & Rodriguez, G. (2017). Audit Analysis Models, Security Frameworks and Their Relevance for VoIP.

[13] Hussien, O., Butt, U., & Bin Sulaiman, R. (2023). Critical Analysis and Countermeasures Tactics, Techniques and Procedures (TTPs) that target civilians: A case study On Pegasus.

[14] Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Perez-Meana, H., Olivares-Mercado, J., Portillo-Portillo, J., Benitez-Garcia, G., Sandoval Orozco, A. L., & García Villalba, L. J. (2023,). ReinforSec: An Automatic Generator of Synthetic Malware Samples and Denial-of-Service Attacks through Reinforcement Learning. *Sensors*, *23*(3), 1231.

[15] Alwaheidi, M. K. S., & Islam, S. (2022). Data-Driven Threat Analysis for Ensuring Security in Cloud-Enabled Systems. *Sensors*, *22*(15), 5726.

[16] Armando, Y., & Rosalina, R. (2023). Penetration Testing Tangerang City Web Application With Implementing OWASP Top 10 Web Security Risks Framework. *JISA(Jurnal Informatika Dan Sains)*, *6*(2), 105–109.

[17] Rodríguez, M., Alesanco, L., Mehavilla, L., & García, J. (2022). Evaluation of Machine Learning Techniques for Traffic Flow-Based Intrusion Detection. *Sensors*, *22*(23), 9326.

[18] Hua Yeo, L., Che, X., & Lakkaraju, S. (2017). Understanding Modern Intrusion Detection Systems: A Survey. [PDF]

[19] Abdi, N., Albaseer, A., & Abdallah, M. (2024). The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: A Survey. *IEEE Internet of Things Journal*, *11*(9), 16398–16421.

[20] Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), 8663.

[21] Awodiji, Ayoola, Owoyemi, & Tosin-Amos. (2023). STOP CYBER ATTACKS BEFORE THEY HAPPEN: HARNESSING THE POWER OF PREDICTIVE ANALYTICS IN CYBERSECURITY. Journal of Multidisciplinary Engineering Science and Technology (JMEST), 10(4).

[22] Sanyal, S., Shelat, A., & Gupta, A. (2010). New Frontiers of Network Security: The Threat Within. [PDF]

[23] Alahmari, S., Renaud, K., & Omoronyia, I. (2022). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and E-Business Management*, *21*(1), 123–158.

[24] Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology*, *8*.

[25] Alahmadi, A. N., Rehman, S. U., Alhazmi, H. S., Glynn, D. G., Shoaib, H., & Solé, P. (2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors*, *22*(9), 3520.