International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Enhancing threat detection in Identity and Access Management (IAM) systems

Nikhil Ghadge *

Software Architect Okta.Inc, Software Engineering, Dublin, CA, USA.

International Journal of Science and Research Archive, 2024, 11(02), 2050–2057

Publication history: Received on 16 March 2024; revised on 27 April 2024; accepted on 29 April 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.2.0761

Abstract

Identity and Access Management (IAM) systems play a pivotal role in safeguarding organizational resources by controlling access to sensitive information. However, these systems face evolving threats that can compromise security and privacy. This paper proposes a comprehensive approach to enhance threat detection within IAM systems. By integrating advanced techniques such as anomaly detection, machine learning, and behavior analysis, organizations can better identify and respond to suspicious activities. This paper discusses the challenges associated with threat detection in IAM systems and presents practical solutions to mitigate these risks. Furthermore, the paper highlights the importance of continuous monitoring and adaptation effectively combat emerging threats.

Keywords: Identity and Access Management; Security; Threat detection; Identity theft; Artificial Intelligence; Machine Learning

1. Introduction

In this comprehensive paper, our goal is to provide a thorough understanding of the effective use of automated reasoning techniques for threat detection in identity and access management systems. The following sections of this introduction will provide a detailed background on the security contexts and motivations behind the development and implementation of these systems, as well as an exploration of their defining characteristics and the numerous threats they face.

Threat detection is performed to determine if an action has the potential to negatively impact the future state of a resource, leading to a violation of the access control policy in place. It is important to note that any action that changes the state of a resource is essentially a formal request for a specific operation or access related to a particular identity. Therefore, the determination of whether an action poses a threat can be successfully achieved through a careful comparison of that action against the access control policy. It is widely recognized that the use of automated reasoning greatly optimizes this process of threat determination. Automated reasoning has the potential to bridge the gap between the capabilities of machine learning and statistical analysis techniques in security data and the ultimate goal of achieving high-level threat detection through comprehensive analysis of metadata and policy-informed examination of activities. The purpose of implementing threat detection mechanisms goes beyond exposing and apprehending wrongdoers during a breach. It also involves providing the necessary capabilities and resources to counter ongoing security violations or take appropriate action after a security violation has occurred. It is worth mentioning that the field of intrusion detection has primarily focused on detecting misuse, which refers to unauthorized attempts to perform actions. However, with the introduction of Identity and Access Management (IAM) systems, it is now possible to accurately determine whether an action poses a potential threat by considering the actor's identity and the established access control policy. This is facilitated by the fact that these systems inherently incorporate a security policy that grants access to various resources based on different identities. This policy is often represented through Role-Based Access Control (RBAC) at the enterprise level and further refined through Task-Based Access Control (TBAC) mechanisms, which correspond to

* Corresponding author: Nikhil Ghadge

specific user tasks. Implementing strong protection measures, along with careful management of role and task information, serves as an important form of security-related metadata. Threat detection plays a crucial role in security monitoring, as it is the fundamental process through which we determine whether an activity is considered a potential threat [1][2].

Traditionally, threat detection has focused on identifying misuse, which involves detecting deliberate attempts to violate computer security policies. In this paper, we define a threat as an intentional violation of a computer security policy. It is important to emphasize that the detection of deterioration, which refers to identifying breaches of established policies and the affected resources, is a cornerstone of comprehensive threat detection in identity and access management systems. Unfortunately, this aspect of threat detection has received limited attention in the research community. The ever-evolving and increasingly sophisticated security threats in the digital landscape are alarming. Networks are constantly targeted by hackers, criminals, and even insiders who exploit vulnerabilities for personal gain, sabotage, or espionage. These persistent and complex security attacks have the potential to disrupt our global information infrastructure. Therefore, identity and access management systems serve as the first line of defense in providing secure access to networked resources. This paper focuses specifically on threat detection in the complex landscape of identity and access management systems, which requires careful attention and continuous innovation.

2. Current Challenges in Threat Detection

Traditional network security solutions create perimeters with firewalls and intrusion detection systems. These solutions are designed to prevent attacks from reaching a protected system and, if one does get through, detect the attack as it traverses the network and prevent it from causing damage. Unfortunately, many identity systems are housed on Internet-facing systems, and the nature of the systems requires a level of access from various locations and systems. This results in the equivalent of Swiss cheese in the network perimeter and makes it quite difficult to distinguish legitimate access from an attack. Once inside the network, the attack has free rein with little chance of detection. Attacks generally occur throughout every phase of an identity lifecycle, and an attack against an identity store, a privacy invasion, or a denial of service can target any one of the 'verbs' of an identity and severely affect the business processes that the identity supports. Traditional network security solutions cannot adequately detect and prevent these attacks, and existing identity management provisioning and access controls can exacerbate certain conditions and make the systems more susceptible to attacks. Therefore, it is crucial for organizations to adopt comprehensive security measures that go beyond traditional perimeter defenses. In order to address this challenge, organizations need to implement a multi-layered security approach that combines advanced threat detection and prevention technologies with robust identity and access management systems. By doing so, they can create a more resilient security posture that is capable of detecting and thwarting attacks at multiple stages of the identity lifecycle. Additionally, organizations should leverage advanced analytics and machine learning algorithms to continuously monitor and analyze network traffic, identifying anomalies and suspicious patterns that may indicate the presence of an ongoing attack. Furthermore, organizations should prioritize the implementation of security measures that focus on proactive threat hunting and intelligence gathering. This involves actively searching for potential threats within the network and leveraging threat intelligence sources to stay ahead of emerging attack techniques. By staying proactive and vigilant, organizations can significantly reduce the risk of successful attacks and minimize the potential damage that can be caused by such incidents. To enhance security, organizations should also promote a culture of security awareness among employees and stakeholders. This can be achieved through comprehensive training programs that educate individuals on best practices for protecting sensitive information, recognizing phishing attempts, and maintaining strong password hygiene. By empowering individuals to become the first line of defense against cyber threats, organizations can create an environment where security is everyone's responsibility. In summary, traditional network security solutions are no longer sufficient to protect against the evolving threat landscape. Organizations must embrace a holistic approach to security that encompasses advanced threat detection, robust identity and access management, proactive threat hunting, and security awareness training. By implementing these measures, organizations can better safeguard their critical assets and ensure the continuity of their business operations in the face of increasingly sophisticated cyber attacks.

3. Overview of IAM Systems

Access management is the intricate and crucial process of identifying, meticulously tracking, effectively controlling, and appropriately limiting the access to a specific object by a designated subject. It encompasses a comprehensive range of activities that enable the smooth functioning of access control systems, dictating and regulating the permissions for allowable and restricted access. The concepts and terminologies of identity, access, and objects play a pivotal role in the meticulous execution of access management [3]. Access, in its essence, denotes the inherent capability and authoritatively conferred power possessed by a subject to perform actions or carry out operations on an object. When a

subject initiates an attempt to access an object, it undergoes the scrutiny and evaluation of the access management system, eventually leading to either the approval or denial of the access attempt. The object, on the other hand, signifies any tangible or intangible resource that is susceptible to the application of access control measures. Examples of such objects include files, computing services, databases, and physical locations. Crucially, every object is attributed with an owner who possesses the requisite authority and control to regulate and administer access to the object. In the vast landscape of cyberspace, digital identity emerges as a multifaceted and encompassing entity. It represents the online presence of an individual or organization, encapsulating the exhaustive assortment of information that has been placed or encountered within the virtual realm. Such information serves as distinctive markers that aid in the identification of the entity. The domain of digital identity encompasses both actively generated data, originating from deliberate actions, as well as passively gathered information, obtained from various sources. Additionally, the identity comprises data that is established or defined by the entity itself, by other entities, and even by the underlying computing infrastructure. An identity, within the context of an information system, represents an entity or subject that is acknowledged and manifested. It serves as a tangible portrayal or depiction of a user or any other relevant subject, be it human or computer-based. The identity offers a unique means of distinguishing and discerning one entity or subject from another. Importantly, it is plausible for certain subjects to possess multiple identities, each designed to suit and fulfill different contextual requirements. For instance, an individual may possess one identity that pertains to an employee role, another for a customer role, and yet another identity that specifically caters to an administrator role.

4. Importance of Threat Detection in IAM Systems

Regular monitoring and reactive methods alone cannot provide this level of security, and the difference is ultimately a matter of finding the proverbial needle in the haystack. An example from the realm of traditional IT security is antivirus software. The disparity between detecting viruses solely through signature files and employing heuristics is essentially the distinction between mere monitoring and true detection. By leveraging heuristics, analysts are able to identify previously unknown malware based on behavior patterns, rather than relying solely on pre-existing signatures. In a similar vein, should a user account become compromised – perhaps through a phishing attack – the attacker's behavior will inevitably deviate from the norm, thus presenting detectable anomalies. For instance, the attacker might log in from an unusual location, attempt to escalate privileges, or access data beyond the boundaries of standard protocols. By detecting such irregularities and promptly suspending the compromised account, the risk of damage to data and system resources can be greatly mitigated. In essence, in both cases, the threat is promptly identified, allowing for immediate action to prevent any harm or disruption to the system. A key differentiating factor between regular monitoring and true threat detection lies in the proactive nature of the latter. Attack patterns tend to follow a distinct lifecycle, and if their activities can be discerned at an early stage – such as during the reconnaissance or exploitation phases – swift action can be taken to neutralize the threat before it has the chance to wreak havoc. For instance, consider the detection of an SQL injection attack designed to gain elevated privileges within an application. If such malicious activity could be promptly identified within the database framework and effectively prevented from proceeding, the attacker would be thwarted in their attempts to infiltrate the system and potentially cause substantial harm to both the application and the underlying data infrastructure. Furthermore, comprehensive security measures encompass not only the detection of threats but also the prevention of unauthorized access and the safeguarding of sensitive data. It is crucial to implement robust authentication mechanisms, such as multi-factor authentication, to ensure that only legitimate users can gain access to the system. Additionally, strict access controls and permissions should be enforced to limit the actions that users can perform within the system. By implementing these measures, the risk of unauthorized access and data breaches can be significantly reduced. Moreover, the importance of regular security audits and vulnerability assessments cannot be overstated. These proactive measures help identify potential weaknesses and vulnerabilities in the system before they can be exploited by malicious actors. By conducting frequent audits, organizations can stay one step ahead of attackers and ensure that their systems are adequately protected. In conclusion, true threat detection and comprehensive security measures are essential in safeguarding against increasingly sophisticated cyber threats. By leveraging proactive techniques, such as behavior-based analysis and prompt response protocols, organizations can effectively mitigate risks and protect their data and system resources. It is imperative for organizations to stay vigilant and continuously adapt their security strategies to counter evolving threats in today's digital landscape.

5. Common Threats in IAM Systems

An illustration-based approach has been demonstrated by JC Mitchell in the field of Identity and Access Management (IAM). Therefore, we also have a strong inclination towards approaching policies as comprehensive sets of permissions that accurately map roles to extensive sets of authorized operations within an IAM system. In this particular context, a threat is precisely defined as any unauthorized or illicit attempt to perform an operation that should not be granted to the specific identity carrying it out. To further enhance the clarity of this concept, Mitchell constructs a highly intricate

state machine that effectively represents the entire system's functionality and subsequently develops a state-based model for an authentication protocol. Through this meticulous process, he is able to visually illustrate a threat as a tangible instance of a protocol run that shockingly permits an unauthorized operation to transpire [4][5]. Although the concept is seemingly straightforward, it is essential to acknowledge the immense power embedded within this model and recognize the multitude of activities that can be undertaken to successfully detect and prevent threats within IAM systems. For instance, one highly effective approach involves drafting a rigorous specification that explicitly declares, at all times, the absolute prohibition of an identity, possessing a particular role, from performing certain operations that are deemed highly sensitive or restricted. This specification serves as an invaluable instrument for system administrators, as it sets a concrete standard of compliance that must be maintained. To support this compliance verification process, the utilization of a cutting-edge model checker is strongly recommended due to its remarkable capabilities in automatically validating whether the existing IAM system accurately adheres to the established specification. If, during the verification process, the system is found to be non-compliant, the model checker swiftly generates a comprehensive counterexample trace that meticulously outlines the exact sequence of events that would hypothetically grant access to the unauthorized operation. This trace essentially shines a spotlight on the precise areas where the IAM system exhibits shortcomings and illuminates the key areas where critical modifications and adjustments desperately need to be implemented in order to fortify the overall security posture [6].

6. Enhancing Threat Detection Capabilities

Several features have been suggested to enhance the threat detection capabilities of an Identity Management System. Again, separating these into policy, association, and authentication level threats, these features include the ability to build role hierarchies from direct user assignments, to increase the quality and ease of building policies. This would automatically build the appropriate and transparent set of access policies and enable root cause analysis as to why a particular access was or was not allowed. The methodology would only be focused on association and policy level threats.

Another suggested feature is to automatically identify any inconsistency that a policy change may have with previous policies. This could be called a policy violation. It is stated that changes in company access policies are an everyday occurrence, but it is not always clear what effect that has on the current and outstanding access for an individual.

A comparison of a before and after state can determine any possibly damaging effect the change would have, and the automatic reports provided explain the effect to the users and suggest remedial actions. This provides a way to proactively stabilize access control on an ongoing basis. The final methodology scales down all arising problems to a binary classification where a classifier would be trained to identify previous similar incidents and suggest future remedial action. Considering that many access failures are low risk and that there are multiple methods in rectifying a problem, this would make more efficient use of the remediation phase of access control [7].

7. Machine Learning Techniques for Threat Detection

Real-world systems employ a clustering algorithm to classify usage data into sets of regular and abnormal behavior, which enables effective identification of insider abuse in the form of excessive utilization of privileges. Recent research has also utilized association rule mining techniques to identify alterations in user access patterns and applied sequence matching techniques to detect attacks related to identity theft through analysis of path deviation. Despite their favorable outcomes, these approaches are frequently burdensome in terms of computational resources and pose challenges when it comes to implementation in large-scale systems. More recent work has seen the use of association rule mining techniques to detect changes in user access behaviors and path deviation analysis using sequence matching techniques to detect identity theft-related attacks. While all these methods have shown positive results, they are often computationally expensive and difficult to scale to large systems.

The complexity of the issue and change in attack strategies has prompted many individuals and organizations to turn towards artificially intelligent (AI) approaches to assist in addressing the problem of insider abuse and identity theft-related attacks. The utilization of pattern-based anomaly detection engines has emerged as one of the most successful approaches in combating these issues by identifying inappropriate or unusual access to information. Anomaly detection entails the process of identifying patterns in data that do not adhere to established normal behaviors. Due to the targeted nature of attack patterns in relation to identity theft and insider abuse, it is often feasible to create a set of rules that accurately describe unauthorized access to information. Regrettably, traditional rule-based systems necessitate predefined knowledge and frequently prove ineffective in detecting newly emerging forms of attack. However, an exciting and promising area of research involves the implementation of unsupervised machine learning techniques to directly generate these rule sets from system audit data. By leveraging unsupervised machine learning, it becomes

possible to develop more dynamic and adaptive rule sets that can successfully identify and detect novel forms of attack [8]. This approach overcomes the limitations of rule-based systems by allowing the AI algorithms to autonomously analyze and learn from vast amounts of system audit data, seeking patterns that may not be evident to human analysts. This ability to continually adapt and evolve the rule sets is crucial in staying one step ahead of the ever-evolving landscape of insider abuse and identity theft. The potential applications and implications of utilizing unsupervised machine learning in this context are substantial. As the capabilities of AI continue to advance, so too does the effectiveness and reliability of anomaly detection engines. With ongoing research and development, it is conceivable that these AI-driven systems will become increasingly adept at detecting and preventing insider abuse and identity theft-related attacks. In conclusion, the utilization of artificially intelligent approaches, specifically unsupervised machine learning techniques, holds great promise in addressing the complexity of insider abuse and identity theft-related attacks. By leveraging the power of AI, organizations can enhance their ability to detect and mitigate these threats, thus safeguarding sensitive information and valuable assets. Continued research and development in this field are essential to stay ahead of the ever-evolving landscape of malicious activities, ensuring a secure and resilient future for individuals and organizations alike [9][10].

The rapid increase in adoption of IAM systems has made managing large user populations from different environments a challenging task. A poorly managed system would not only be ineffective in providing a basis for provisioning and access control, but have given rise to several new issues such as reduced security, excessive administration costs or even complete system failure. Many previous studies have shown that the linkage between identity management and access control has been recognized as the primary dimension in which information system security is centered around, and violations of security policies often originate from excessive access rights due to the lack of control in user provisioning into the system.

8. Behavioral Analytics for Threat Detection

The initial step in the process of effectively utilizing behavioral analytics for Information Technology Management (ITM) is to comprehensively prepare the system for monitoring purposes. This integral step entails defining and clearly establishing the organizational objectives that the system will assess and evaluate. By doing so, a solid foundation for gauging and evaluating normal system behavior can be established. To ensure a seamless process, the ITM system and data administrators play a crucial role by providing invaluable insights into the data that is being stored and how it is utilized within the system. Moreover, they can offer specific examples of activities that are considered both normal and abnormal, thereby aiding the system in the later stages of analysis and monitoring. Moreover, in the realm of user-based ITM, such as a role-based access control system or RBAC, it becomes integral to monitor users within the context of the business processes they engage in. For this purpose, it becomes imperative to define rules that dictate and govern the access to certain resources, ensuring that they are being accessed in a legitimate and authorized manner. This not only ensures the security of the system but also provides a comprehensive understanding of user behavior within the ITM framework. Once the system possesses a clear comprehension of what it needs to monitor, it can seamlessly commence assessing the current activities in relation to the established baseline. This evaluation helps in identifying any deviations or anomalies that might require further investigation or analysis. By comparing the ongoing system behavior to the baseline data, the ITM system can effectively detect the slightest irregularities and potential threats, enabling prompt and decisive action to safeguard the system's integrity and functionality.

9. Real-time Monitoring and Alerting

Real-time monitoring and alerting from IAM frameworks should be both undertakings: from one viewpoint, to interpret and follow up on any suspicious conduct from clients that might be in fact approved yet taking part in unseemly action, and on the other to recognize and square unauthorized clients that are endeavoring to amplify past their given benefits by getting substantial credentials under a false personality. With regards to the former, IAM frameworks ought to receive a two-levelled way to deal with the intruder. For those that are as a matter of first importance clients with substantial credentials yet have connected with coming about suspicious action, the IAM framework ought to depend upon its identity governance and administration (IGA) arrangement to convey the client under the watchful eye of an advisory group that will figure out whether the user's identity ought to be verified or punished by minimization of benefits. This direction will likely include an adjustment in client roles and thusly, there ought to be an office accessible to generate an account of the activity of both the client being referred to and the council individuals. This is a potential state of integration with present activity checking arrangements.

While for quite a while, access control applications, for example, firewalls and IDS/IPS frameworks have had the capacity to caution when an unauthorized client endeavors to get to touchy resources, IAM frameworks still generally miss the

mark in their detection about suspicious and potentially hazardous conduct. For instance, it isn't remarkable in numerous endeavor IT frameworks where an assailant can acquire substantial credentials and login as a genuine client, yet from a suspicious area (for example, an alternate nation than the client's recorded address) without raising any notice from the IAM framework since it can't distinguish when a genuine client accomplishes something that is out of the standard. Progressively, some IGA arrangements are beginning to highlight this capacity, and given the attention on attaching IAM frameworks to the general IT hazard arrangement process, it is sensible to expect that additions here will increment in both the pace of improvement and measure of change.

10. Integration with Security Information and Event Management (SIEM) Systems

SIEM systems provide real-time event collection, alerting, and after-the-fact analysis for IT security purposes. SIEM is the product of the real-time Security Event Management (SEM) and the security information management (SIM). SIM is the aggregation of data for analysis. The data is gathered from security software and devices and identify patterns, track activity, and identify trends. This is also viewed as the process of event data collection. This data is normalized so that events can be correlated and analyzed. In the context of SIEM, 'normalization' is the process of taking data from different sources and changing it so that it "conforms" to some defined standard. This includes the correlation of security events from disparate systems—from firewalls, to intrusion detection systems (IDS) and many others. The correlation of security events plays a crucial role in SIEM systems. By harmonizing data from various sources and adhering to a predetermined structure, SIEM ensures effective analysis and threat identification. This intricate process involves capturing data from diverse security software and devices, including firewalls, intrusion detection systems (IDS), and other components of the security infrastructure. Through normalization, the collected data undergoes a transformation to meet a standardized format. This standardized data allows for seamless correlation and comprehensive analysis, facilitating the detection of patterns and trends. The normalization process aims to bring consistency and uniformity to the data, enabling efficient event correlation across different systems. In essence, SIEM combines the power of SEM and SIM to deliver unparalleled IT security capabilities. By leveraging real-time event collection, alerting, and post-analysis, SIEM empowers organizations to proactively defend against cyber threats, identify potential vulnerabilities, and respond swiftly to security incidents. With its ability to gather, normalize, and correlate data from disparate sources, SIEM emerges as an indispensable tool in today's complex and evolving digital landscape.

11. User Behavior Analysis for Threat Identification

Once a normal profile of a user's interaction with the system has been established, deviations from that profile may be indicators of possible security threats. Incorporating threat assessment strategies and policies, we can construct a taxonomy of potential threat behaviors. High level threats such as identity theft and impersonation will typify certain forms of user behavior when attempting to breach the system. Differences between normal and ruse actions can be hard to detect, for example an attacker who has obtained a stolen password may still use the normal authentication procedures but with anomalous pre or post activities. Insider threats will be defined by changes in the level and content of access on the part of the user. Elevation of privilege and information theft often entails disguising as another user or gaining administrative privileges. Anomalous behavior based detections will often consist of comparing the action with a predefined security policy created using deontic logic. Although it is highly context dependent, considering an action as an actual or possible change to the system state, user U doing an operation O will be a function to a specific access level. Identified threats and policy violations can sometimes merely be revealed by presenting the evidence to an administrator. For each type of threat behavior outlined above, corresponding data can be collected from an IAM system.

Static techniques such as audit and Java byte-code analysis will collect a snapshot of data in the form of log files, however interpreting these logs to detect threats will essentially require a form of dynamic analysis. In contrast to the automatic log analysis methods described which merely look for errors or vulnerabilities, dynamic analysis focuses on using and observing the system in an automated fashion to determine if actions are safe and/or if specific threats can be detected. Considering the principle that user behavior is a sequence of events E in response to a perceived state S trying to achieve a goal G, behavior based detection will create a state transition model to map user types and define the boundaries between acceptable and threatening behavior. State transition models are regularly used to identify and monitor system resources relevant to users and were used by the prototype system described in which aimed to prevent insider threats from administrators or IT staff, who would often damage or misappropriate organizational resources. The most effective data collection for user behavior analysis is likely to come from contemporary machine learning methods using input data to classify or make decisions. Building an intelligent agent to represent user behavior and train a classifier to distinguish agent actions in normal and threat scenarios has been suggested as a long-term goal in identifying and preventing all types of threat from specific user types. Terminology and framework classifiers will apply the classification of data into threat and non-threat categories at specific user types to real user data and inform trusting

decisions on probable user actions. Two known and widely applicable probabilistic models that could make use of such data are the Bayesian network and Hidden Markov Model, facilitating reasoning and prediction of complex user actions and making inferences on evidence to identify specific threats and policies.

12. Access Control Policies and Threat Detection

An access control policy (ACP) is a crucial aspect of system security that either grants or denies requests for accessing system objects or utilizing system resources. The implications of this policy are significant, as it can either lead to the exposure of vulnerabilities and subsequent notification or create a potential pathway for malicious attacks. In instances where access is denied, users may resort to modifying replicated versions of the information or data, thereby circumventing security measures and posing a risk to system integrity. The decision rendered by the access control policy serves as a valuable source of data for intrusion and misuse detection. Obtaining this data is instrumental for system administrators and security officers in evaluating the suitability of the existing access control policy in relation to the desired level of security within the system. A comparative analysis between the ACP and the system's security requirements leads to a greater understanding of any disparities or room for improvement. By conducting attack simulations and utilizing event data to trace the attack's progression, it becomes possible to identify weaknesses within the access control policy that allowed for the success of the attack. This practice is indispensable when establishing a foundation of system and ACP state information, serving as a baseline for detection algorithms to identify deviations from normal or anomalous behavior. The event data, and its significance with regard to access control policies, aids in facilitating automatic recovery or adaptation of access control policies to proactively prevent similar attacks from occurring in the future [11].

13. Role of Artificial Intelligence in Threat Detection

Artificial Intelligence (AI) has emerged as an incredibly powerful tool in the field of cybersecurity, offering advanced capabilities for threat detection, mitigation, and response. With the help of AI technologies like machine learning, natural language processing, and anomaly detection, the world of cybersecurity is experiencing a significant transformation. These AI-based technologies play a crucial role in identifying and mitigating security threats across various domains, paving the way for enhanced protection. Among the various applications of AI in cybersecurity, threat detection systems stand out as particularly noteworthy. By leveraging the power of AI, threat detection systems can greatly improve the accuracy and efficiency of identity and access management (IAM) systems. IAM systems, in turn, play a vital role in protecting organizations from unauthorized access and malicious activities. With the support of AI technologies, IAM systems are able to analyze massive amounts of data in real-time, allowing them to detect abnormal patterns or behaviors that may indicate a potential security threat. This proactive approach to threat detection provides organizations with the ability to swiftly respond to security incidents and prevent potential breaches before they occur. By harnessing the capabilities of AI-powered IAM systems, organizations are empowered to stay one step ahead of cyber threats. These AI-powered systems continuously learn from new data and adapt their threat detection algorithms to keep up with the ever-evolving landscape of cybersecurity. This adaptability is crucial in maintaining effective threat detection capabilities, as cyber threats continue to grow in sophistication [12]. In conclusion, the incorporation of AI technologies in cybersecurity, specifically in threat detection systems and IAM systems, has revolutionized the way organizations protect themselves against security breaches. The ability of AI-powered IAM systems to continuously learn and adapt is paramount in the face of constantly evolving cyber threats. By embracing the potential of AI in cybersecurity, organizations can significantly enhance their defense mechanisms and safeguard their digital assets with greater efficiency and precision.

14. Continuous Improvement and Adaptation of Threat Detection Systems

The baseline of security can be considered as the current state of threat detection features provided for system and security administrators. The detection of threats is largely based on the logs and audit information obtained from the IT systems. Then patterns of behavior and typical usage by users and administrators are learned and changes/deviations from these patterns are considered as suspicious behavior. A simple example would be an administrator who usually logs into a server from 9am to 6pm suddenly starts logging in at 2am. This could indicate that the administrator's account is being used by someone else, i.e. an imposter. The change in login time is a weak indication and unsatisfying answer can only be reported as a shortfall in the threshold of known error. A good detection system should be able to pick this up and give an accurate analysis and clear information. This would require continuous testing and monitoring of the current detection methods and features.

The area of enhancing threat detection in IAM system plays an important role in the world of internet and computer security. It is widely accepted that today's security systems still have weaknesses and can be exploited by attackers if it is known. The principle of continuous improvement and adaptation is an approach that can be effectively used to bring the security system to a better state. It is based on the assumption that the current security system provides a baseline of security and what is required is to refine the ability to detect threats, actual attacks from vulnerable conditions and weaknesses, known and new types of attacks.

15. Conclusion and Future Directions

When studying threats and their attributes, the goals and motivations of the attacker may be useful to determine the possible impact of the threat. High-impact threats pose a risk to the availability, integrity, and confidentiality of information and resources. Detecting and preventing these threats is an important function of a security system. This research could be followed up with a study into threat prevention through control modification and the automatic repair of security holes in an IAM system. This could provide a cost-effective simplification for administrators in the hardening of an IAM system. Automatic repair methods would have some level of autonomous control. This can make the system more vulnerable to intelligent threats, so it is essential to test the efficiency and the side effects of these methods on threat prevention. The identity management process is complex and involves many different stages. This study only addressed one segment of the provisioning process. There are many events that can happen to an identity and its privileges after they have been provisioned. The monitoring of identity and access data over time is important for anomaly detection. Anomalies in a system are not always a security threat. Incident and event information can be used to attribute detected anomalies to the root cause, which can be an error or the presence of a business.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] K. Huang, G. Huang, Y.Duan, and J. Hyun, “Utilizing Prompt Engineering to operationalize Cybersecurity” in Generative AI Security: Theories and Practices, Springer, 2024.

[2] S. Aboukadri, A. Ouaddah, and A. Mezrioui, "Machine Learning in Identity and Access Management Systems: Survey and Deep Dive," Computers & Security, 2024.

[3] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, "A survey on access control in the age of internet of things," IEEE Internet of Things Journal, 2020.

[4] C. Singh, R. Thakkar, and J. Warraich, "IAM Identity Access Management— importance in maintaining security systems within organizations," European Journal of Engineering and Technology Research, 2023.

[5] M. J. Haber and D. Rolls, "Identity Threat Detection and Response (ITDR)," in Identity Attack Vectors: Strategically Designing and Implementing Identity Security, Springer 2024

[6] J. J. Ang'udi, "Security challenges in cloud computing: A comprehensive analysis," World Journal of Advanced Engineering Technology, 2023

[7] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," The journal of supercomputing, 2020.

[8] M. Ahsan, K. E. Nygard, R. Gomes et al., "Cybersecurity threats and their mitigation approaches using Machine Learning—A Review," Journal of Cybersecurity and Privacy, vol. 2022, mdpi.com, 2022..

[9] F. R. Alzaabi and A. Mehmood, "A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods," IEEE Access, 2024.

[10] S. Mittal, "A review of machine learning techniques in cybersecurity and research opportunities," Machine Learning for Cyber Security, 2022.

[11] AAN Patwary, A Fu, RK Naha, SK Battula, "Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review," arXiv preprint arXiv, 2020

[12] V. Adenola, "Artificial intelligence based access management system," 2023.