ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Detecting Insider Threats: Best Practices and Technologies

Haritha Madhava Reddy

USA

ABSTRACT

Insider threats represent a critical challenge for modern organizations as they can cause significant harm through the misuse of authorized access to sensitive systems and data. Detecting insider threats is complicated by the fact that insiders, including employees, contractors, and business partners, already possess legitimate access rights, making it difficult to distinguish between regular and malicious activities. This review paper examines insider threat detection strategies, focusing on the role of both human and technological factors. Best practices, such as establishing behavior baselines, implementing strict access controls, and conducting regular security training, are discussed alongside advanced technologies like User and Entity Behavior Analytics (UEBA), Security Information and Event Management (SIEM) systems, and Data Loss Prevention (DLP) solutions. By integrating these practices and technologies, organizations can more effectively detect, mitigate, and respond to insider threats. As insider risks grow in both frequency and sophistication, this review highlights the need for a multi-layered, adaptive approach to securing organizational assets.

***Corresponding author**

Haritha Madhava Reddy, USA.

Received: December 06, 2022; **Accepted:** December 13, 2022, **Published:** December 20, 2022

Keywords: Insider Threats, Detection Strategies, User and Entity Behavior Analytics (UEBA), Security Information and Event Management (SIEM), Data Loss Prevention (DLP), Network Traffic Analysis (NTA), Principle of Least Privilege (PoLP), Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Security Awareness Training, Audits and Assessments, Risk Assessments, Hybrid Work Environments, Employee Privacy Rights, Incident Response Procedures, Data Protection Protocols

Introduction

The digitalization of modern businesses has brought about numerous benefits but has also introduced new vulnerabilities, particularly from insider threats. Unlike external attackers, insiders have authorized access to an organization's network, systems, and data, making their actions harder to detect and more damaging when malicious [1]. Insider threats can stem from a variety of actors, including current employees, former employees, contractors, and business partners. Their motivations may range from personal gain, such as financial fraud, to grievances or industrial espionage.

The detection of insider threats is an ongoing challenge for security teams due to the difficulty of distinguishing between normal and malicious activities by trusted users. In addition, the rise of remote work, cloud computing, and increased reliance on digital infrastructure has further complicated the task of securing sensitive data against both intentional and unintentional insider breaches. This review provides an in-depth analysis of the best practices and technologies used to detect and mitigate insider threats in organizations.

Types of Insider Threats

Insider threats can be categorized into three main types, each posing distinct risks. Malicious insiders intentionally exploit their access privileges to harm the organization for personal gain or to support a third party [2]. These individuals may engage in espionage, sabotage, or data theft, driven by motives such as financial incentives, like selling trade secrets, or ideological reasons, such as aiding a competitor. Malicious insiders often take deliberate steps to cover their tracks, making early detection critical to preventing significant damage.

On the other hand, negligent and compromised insiders represent different forms of risk. Negligent insiders, while not malicious, cause harm through carelessness, such as failing to follow security protocols, accidentally sharing sensitive information, or falling victim to phishing schemes [3]. Though unintentional, their actions can still expose critical systems or sensitive data. Compromised insiders, however, occur when external attackers gain control of legitimate credentials, allowing them to operate undetected within the organization's systems [4]. Phishing, social engineering, and credential theft are common methods used by attackers to compromise insiders, making these threats particularly challenging to detect [5].

Challenges in Detecting Insider Threats

Detecting insider threats is a complex and multifaceted challenge for organizations due to the inherent nature of these threats. Unlike external attacks, insider threats stem from individuals who have legitimate access to an organization's systems, data, and networks, making it difficult to identify malicious intent behind seemingly normal actions. The subtle and covert nature of insider threats makes it especially challenging for security teams to distinguish between routine user behavior and actions that may pose a risk to the organization.

One of the primary challenges in detecting insider threats lies in recognizing the behavioral and technical indicators that could signal a potential threat [6]. Since insiders typically perform daily tasks that require access to sensitive information, their activity

may not immediately raise suspicion. However, there are several behavioral and technical signals that organizations can monitor to help detect malicious activity. For instance, an increase in unauthorized data access such as an employee accessing files outside their role or repeatedly attempting to view sensitive information can indicate malicious intent. Similarly, unusual login patterns, such as an employee logging in at irregular hours or from unfamiliar locations, could be a sign that an insider is acting with malicious intent or that their credentials have been compromised.

In addition to these behavioral indicators, technical signs such as spikes in network traffic, particularly involving sensitive data, can be a red flag for insider threat activity [7]. Data exfiltration where large volumes of information are transferred to unauthorized locations, devices, or external parties often serves as a clear technical signal of insider abuse. For example, sudden or frequent uploads to personal cloud storage accounts or external drives can signal that an insider is attempting to steal proprietary or sensitive data. Furthermore, unexplained changes to access privileges or unauthorized attempts to elevate system permissions are another strong technical indicator of potential malicious activity.

Detecting insider threats requires security teams to carefully analyze these subtle signs in combination with broader security data. Unfortunately, this is often easier said than done. Insider threats are particularly difficult to detect because malicious actions are often performed under the guise of routine operations, using the same access rights and privileges that employees, contractors, or partners are legitimately granted. As a result, insider threat detection relies heavily on organizations' ability to identify deviations from baseline user behavior and to correlate different security events into a broader picture of potentially harmful activity.

Moreover, the rise of hybrid and remote work environments further complicates insider threat detection. As more employees work from outside traditional office settings, organizations must manage a broader attack surface. Remote workers often access organizational resources through personal devices or unsecured networks, increasing the risk of credential theft or unintentional data leaks. Additionally, it becomes more challenging for security teams to establish baselines for employee behavior, as remote work can result in more variable login patterns, such as accessing systems at odd hours or from different geographic locations [8]. These challenges make it more difficult to distinguish between normal remote work habits and potential insider threats.

Remote work also increases the possibility of employees using personal cloud services, external drives, or shadow IT solutions, which operate outside the visibility of the organization's security systems. Employees may accidentally or intentionally use these unsanctioned tools to handle sensitive data, creating new opportunities for data exfiltration or loss [9]. Without robust monitoring tools, organizations may struggle to detect and prevent these actions, further complicating the challenge of insider threat detection.

As such, balancing security monitoring with employee privacy presents an additional challenge for organizations aiming to detect insider threats. While monitoring employee activity is essential for identifying suspicious behavior, overly intrusive surveillance can create tension between employees and management, potentially leading to morale issues and legal challenges. Regulations such as the General Data Protection Regulation (GDPR) in Europe and other privacy laws emphasize the need for careful handling of employee data and place restrictions on how organizations can monitor user activity [10]. These regulations require organizations to strike a delicate balance between implementing effective insider threat detection measures and respecting employee privacy rights.

Organizations must also consider the ethical implications of monitoring employees. Excessive monitoring, particularly of personal communications or private activities, can lead to distrust among the workforce. This can be counterproductive, as employees may be less likely to report potential insider threats or participate in security awareness programs if they feel that their privacy is being violated. As a result, organizations must adopt a targeted, risk based approach to insider threat detection, ensuring that monitoring efforts are focused on high risk behaviors and are conducted in compliance with applicable privacy laws.

Best Practices for Insider Threat Detection

Successfully detecting and mitigating insider threats requires organizations to adopt a multi-faceted approach that integrates a combination of technical controls, behavioral analysis, and comprehensive organizational policies. To build a robust insider threat detection program, organizations should implement best practices that focus on monitoring, controlling access, promoting security awareness, and creating a proactive insider threat program.

The cornerstone of any insider threat detection strategy is the ability to monitor user behavior and system activity continuously. To achieve this, organizations should implement a suite of monitoring tools that can collect, aggregate, and analyze data from across the organization's digital ecosystem. Solutions such as User and Entity Behavior Analytics (UEBA) and Security Information and Event Management (SIEM) systems are critical components of this strategy.

UEBA solutions use machine learning algorithms to analyze patterns in user behavior, establishing a baseline of normal activity for each individual within the organization [11]. These tools continuously monitor deviations from normal behavior, such as accessing files that are unrelated to the user's job, logging in from unusual locations, or transferring large volumes of data at irregular times. UEBA solutions can flag these anomalies for further investigation, allowing security teams to detect insider threats that would otherwise go unnoticed.

SIEM systems provide a centralized platform for collecting and correlating security event data from various sources, such as firewalls, servers, and applications. By analyzing security data in real-time, SIEM systems can generate alerts when unusual or suspicious activity is detected. These systems also provide historical data that can be used for post-incident investigations or to identify patterns of malicious behavior over time [12].

In addition to automated tools, organizations should conduct regular audits of user activity and access logs. Periodic reviews of these logs can help identify insider threats that may have slipped through automated detection systems. Audits are especially useful for uncovering long-term patterns of misuse, such as repeated unauthorized access to sensitive files or escalating privileges without proper approval.

Establishing Behavioral Baselines

To effectively detect insider threats, organizations must first establish behavioral baselines for their employees. This involves

analyzing user activity over time to determine what constitutes normal behavior for each role, department, or individual. Behavioral baselines are particularly useful for detecting deviations from expected patterns, which could indicate an insider threat [13]. For instance, an employee who usually works on customer service data but suddenly starts accessing financial records may be exhibiting suspicious behavior that warrants further investigation.

Once baselines are established, machine learning models within UEBA systems can automatically flag deviations from these norms. These deviations can range from logging in from unfamiliar IP addresses or geographic locations to transferring unusually large volumes of data. Behavioral baselines help reduce false positives by ensuring that alerts are only triggered when there is a significant deviation from normal behavior, rather than flagging routine activities that do not pose a security risk.

Another key principle of insider threat prevention is the principle of least privilege (PoLP), which ensures that employees only have access to the systems and data necessary for their specific job functions [14]. By minimizing unnecessary access privileges, organizations reduce the likelihood of accidental or intentional misuse of sensitive information. Implementing role-based access control (RBAC) and multi-factor authentication (MFA) further enhances security by adding layers of protection [15].

Regular access reviews are essential for maintaining the principle of least privilege. These reviews help ensure that employees are not granted excessive permissions and that their access rights are adjusted when they change roles or leave the organization. Organizations should also monitor for privilege escalation attempts, where users try to gain unauthorized access to higher-level systems or data. Privileged Access Management (PAM) tools can help enforce strict control over privileged accounts by monitoring administrative actions and generating detailed logs of all activities performed by privileged users [16].

Similarly, an often-overlooked aspect of insider threat detection is the role of employee training. Even the most sophisticated detection systems can be undermined by employees who are unaware of the risks posed by insider threats or who do not know how to recognize suspicious behavior. To create a security-conscious culture, organizations should conduct regular security awareness training programs that educate employees on the dangers of insider threats, how to spot potential warning signs, and the importance of following security policies [17].

Training programs should be designed to address the specific types of insider threats relevant to the organization, including negligent insider behaviors such as mishandling sensitive data or falling victim to phishing attacks. Employees should also be encouraged to report suspicious behavior through secure and confidential channels. By fostering a culture of vigilance, organizations can reduce the risk of insider threats and increase the likelihood that potential threats will be identified and reported early. As such, an effective insider threat program should integrate technical controls, organizational policies, and incident response procedures. This program should not only focus on detection but also prevention and remediation. Establishing clear policies for acceptable behavior, data access, and reporting procedures ensures that employees understand the consequences of misconduct and the importance of adhering to security protocols.

Implement Data Loss Prevention (DLP) and Network Traffic Analysis (NTA) tools

Data Loss Prevention (DLP) solutions monitor and control data transfers within the organization, preventing unauthorized access or exfiltration of sensitive information. By enforcing data-handling policies and monitoring traffic to detect abnormal movements of data, DLP solutions provide an additional layer of defense against both malicious insiders and compromised accounts attempting to steal or leak confidential information [18].

Network Traffic Analysis (NTA) tools provide deep insights into network behavior by monitoring traffic patterns to detect anomalies that may indicate insider threats. NTA solutions analyze data flows, identifying unusual spikes in traffic, unauthorized access attempts, or covert communications with external entities. For instance, if an insider attempts to transfer large amounts of data to an unfamiliar external IP address, NTA tools can flag this activity for further investigation [19].

By continuously analyzing network activity, NTA solutions offer an additional layer of protection against both insider threats and external attacks leveraging compromised credentials. These tools are particularly useful for detecting threats that bypass traditional security mechanisms, such as insiders using encrypted channels to exfiltrate data. Combined with other technologies like SIEM and DLP, NTA enhances an organization's ability to identify and respond to insider threats with precision.

Conducting Regular Audits and Assessments

Regular audits and assessments are fundamental to a robust insider threat detection strategy, offering organizations a proactive method to uncover potential risks that may evade real time monitoring tools. These periodic reviews enhance the organization's ability to detect insider threats and provide a framework for refining security policies, access controls, and incident response mechanisms. Through meticulous examination of user activity logs, system access records, and security configurations, audits can reveal unusual patterns of behavior or vulnerabilities that automated systems may overlook [20]. Furthermore, they enable the identification of systemic weaknesses in privilege management, data protection protocols, and procedural enforcement, ensuring that insider threat detection efforts remain resilient against evolving threats.

Regular risk assessments complement these audits by evaluating the organization's exposure to insider risks, allowing for continuous detection and prevention measures adaptation. As insider threat tactics evolve in sophistication driven by advanced social engineering, credential theft, or exploitation of remote access risk assessments play a critical role in updating detection frameworks. They ensure that organizations remain agile in response to new attack vectors, from compromised credentials to the exploitation of excessive access rights. Beyond detection, these assessments also provide strategic insights that influence long-term security planning, guiding investments in advanced monitoring tools, employee training, and policy refinement to mitigate insider threats effectively.

Conclusion

Detecting insider threats necessitates a multi-layered approach that integrates both advanced technologies and best practices into a comprehensive security framework. While sophisticated tools such as User and Entity Behavior Analytics (UEBA), Security Information and Event Management (SIEM), and Data Loss

Prevention (DLP) are essential for identifying anomalous activities and preventing data exfiltration, the human element remains equally important. A robust security culture, fostered by continuous employee education, vigilance, and a deep understanding of insider risks, forms the foundation of an effective defense.

As insider threats grow more sophisticated and complex, organizations must be proactive in evolving their detection strategies and technologies. Regular risk assessments, strengthened security measures, and cross-functional collaboration across IT, human resources, and legal departments are critical to building a resilient security posture. These collaborative efforts ensure that both technical and procedural safeguards are aligned to detect, mitigate, and respond to potential threats.

In conclusion, by combining advanced technological solutions with proactive security policies, organizations can significantly reduce the risks posed by insider threats, safeguarding their most valuable assets and maintaining the trust of their stakeholders. In an era where data breaches can lead to severe financial and reputational damage, the implementation of a comprehensive insider threat detection program is not just advisable but imperative for ensuring long-term organizational security and success.

References

1. Mazzarolo G, Jurcut A D (2019). Insider threats in Cyber Security: The enemy within the gates. arXiv preprint arXiv:1911.09575.
2. Prabhu S, Thompson N (2020) A unified classification model of insider threats to information security https://aisel.aisnet.org/acis2020/40/.
3. Sangster M (2020) When it comes to cyber security, ignorance isn't bliss–it's negligence. Network Security 12: 8-12.
4. Cole E, Ring S (2005) Insider threat: Protecting the enterprise from sabotage, spying, and theft. Elsevier https://shop.elsevier.com/books/insider-threat-protecting-the-enterprise-from-sabotage-spying-and-theft/cole/978-1-59749-048-1.
5. Xiangyu L, Qiuyang L, Chandel S (2017) Social engineering and insider threats. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 25-34.
6. Noonan C F (2018) Spy the lie: Detecting malicious insiders https://irp.fas.org/eprint/noonan.pdf.
7. Garza V R, Wood B P, Monaco J V, Blockmon R, Males N, et al. (2020) Machine Learning Techniques for Identifying Anomalous Network Traffic.
8. ISACA (2022) The impact of a hybrid workplace on security. ISACA Now Blog. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-impact-of-a-hybrid-workplace-on-security
9. Denison S (2015) The accessibility of insider threats on a corporate network. Utica College https://www.proquest.com/openview/6afee5200ca0b436cdc766a33544fb12/1.pdf?pq-origsite=gscholar&cbl=18750.
10. Tikkinen Piri C, Rohunen A, Markkula J (2018) EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review 34: 134-153.
11. Babu S (2020) Detecting anomalies in Users-An UEBA approach. In Proceedings of the International Conference on Industrial Engineering and Operations Management 863-876.
12. Sekharan S S, Kandasamy K (2017) Profiling SIEM tools and correlation engines for security analytics. In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) 717-721.
13. Jiang W, Tian Y, Liu W, Liu W (2018) An insider threat detection method based on user behavior analysis. In Intelligent Information Processing IX: 10th IFIP TC 12 International Conference, IIP 2018, Nanning, China, Proceedings Springer International Publishing 10: 421-429.
14. Sanders M, Yue C (2017) Automated least privileges in cloud-based web services. In Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies 1-6.
15. Fatima A, Ghazi Y, Shibli M A, Abassi A G (2016) Towards Attribute-Centric Access Control: an ABAC versus RBAC argument. Security and Communication Networks 9: 3152-3166.
16. Purba A, Soetomo M (2018) Assessing Privileged Access Management (PAM) using ISO 27001: 2013 Control. ACMIT Proceedings 5: 65-76.
17. Safa N S, Sookhak M, Von Solms R, Furnell S, Ghani N A, Herawan T (2015) Information security conscious care behaviour formation in organizations. Computers & Security 53: 65-78.
18. Securosis L L C (2010) Understanding and selecting a data loss prevention solution. Securosis, LLC http://viewer.media.bitpipe.com/985719113_684/1294934983_394/whitepaper-understanding-and-selecting-a-data-loss-prevention-solution-en.pdf.
19. Oh C, Ha J, Roh H (2021) A survey on TLS-encrypted malware network traffic analysis applicable to security operations centers. Applied Sciences 12: 155.
20. Cappelli D M, Moore A P, Trzeciak R F (2012) The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley https://insights.sei.cmu.edu/library/the-cert-guide-to-insider-threats-how-to-prevent-detect-and-respond-to-information-technology-crimes-theft-sabotage-fraud/.