

Beyond The Perimeter: Redefining Insider Threat Modeling Through Adaptive Behavioral Analytics in Hybrid Work Environments

TIM ABDIUKOV

NTS Netzwerk Telekom Service AG, Australia.

Abstract- *The rise of the hybrid work model has highlighted the limitations of a perimeter-based approach to security and also reintroduced the concept of insider threats in a new and entirely different way. This research presents an overview of the historical development of the insider threat paradigm from the 1990s to the present year, 2021, and how conventional detection measures, which employ a combination of networks and static rules, no longer suffice in distributed work environments. The paper suggests the need to dynamically reconfigure the modeling of insider threats by introducing versatile, adaptive behavioral analytics—an approach based on machine learning and ongoing user behavior profiling. The research paper is based on case studies, psychological theory, and technical advances in the field through 2021. It can be generalized as a hybrid-ready security model that combines behavioral cues, contextual awareness, and risk scoring to increase detection accuracy. This cross-functional exploration ultimately offers a broader approach to reducing insider threats in workplaces, which have become increasingly interesting and virtual in contemporary, more fluid work environments.*

Indexed Terms- *Insider Threats; Adaptive Behavioral Analytics; Hybrid Work Environments; Behavioral Risk Scoring; Cybersecurity; UEBA*

I. INTRODUCTION

1.1 Definition of Insider Threats

Insider threats are the risk of cybersecurity that arises as a result of actions or a lack of appropriate actions of individuals inside an organization who have authorized access to systems and networks or data, and because of an ill motive or due to a lapse in judgment,

end up harming the information assets of the organization. These insiders may be existing or former workers, contractors, or industrial associates who use their legitimate access in an unauthorized manner, potentially violating security procedures. Greitzer and Frincke (2010) assert that such sophistication in insider attacks has been due to the difficulty in determining whether actions are innocent or malicious within valid credentials. Unlike traditional cybersecurity models, which place the greatest emphasis on external threats, insiders often circumvent most security systems simply because of the privileges they already possess. Cappelli, Moore, and Trzeciak (2012) emphasize that insiders often exploit the fact that organizations trust them and are familiar with internal systems, making detection significantly more challenging.

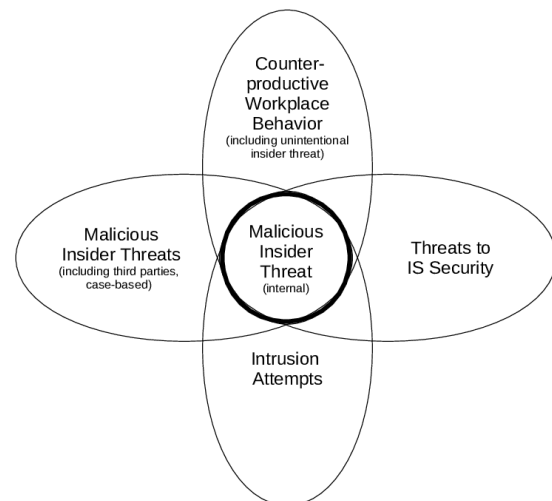


Figure 1: Overlap of insider threat types and security risks

In addition to this, behavioral indicators, technical imperfections, and psychology tend to be combined in instances of insider threats, making diligent mitigation

measures more challenging. Insider threats have therefore been defined to include both the malicious type of sabotage by intent and the accidental agent who, due to a lack of security hygiene or exploitation by someone involved in a breach, inadvertently causes harm. This inclusive framing has become increasingly applicable in contemporary organizational systems, particularly in organizations that have adopted a remote or hybrid work style.

1.2 Importance of Insider Threat Modeling

Insider threat modeling is the practice of identifying, assessing, and forecasting the risks posed by individuals within an organization who are trusted. The value of it is predetermined by the increased rate of occurrence, expense, and seriousness of improper actions involving insiders, as well as the low degree of success of classic security design in combating them. According to Anderson and Agarwal (2010), insider threat modeling is not only crucial for preventing risk, but also particularly important when aiming to deliver limited cybersecurity resources as cost-effectively as possible. According to a landmark study by Ponemon Institute (2018), the global average cost of insider threats had already surpassed the \$8.76 million mark (per year), with the study indicating that the cost trend has continued to rise into the beginning of the 2020s. This is the emerging complexity of the attacks, combined with the proliferating digital attack surface that organizations need to protect. Moreover, according to Bishop and Gates (2008), modeling the insider threat helps organizations understand and predict the combination of access rights, behavioral abnormalities, and circumstances that pose the highest risk of adverse or careless outcomes. Practically, such modeling helps construct specific detection guidelines, risk scoring systems, and incident response policies that take into account human behavior. With the increasing use of remote and hybrid workforces, insider threat modeling is becoming essential for managing users operating in diverse environments, including those in different locations and with varying levels of supervision and oversight.

1.3 Overview of Hybrid Work Environments

Hybrid work performance is a type of organization where employees' reflections are divided between physical workplaces and remote applications, including home offices or co-working centers. The

model spread around the world thanks to the pandemic caused by COVID-19, especially in 2020-2021, when organisations had to maintain the continuity of certain operations while also following temporary public health restrictions. More than 82 percent of organizations intended to support at least partial remote work after the pandemic, indicating that the idea of hybrid work would become a permanent trend. Although hybrid work has advantages such as flexibility, lower overhead, and access to a wider talent pool, it also poses new security risks. Hybrid workplaces make endpoint control, network observability, and data control difficult, which are critical elements of a secure infrastructure. Considering employees, they have switched to unmanaged devices, personal cloud services, and home Wi-Fi networks, which cannot be controlled through centralized IT management. Moreover, the loss of the traditional network perimeter (which used to be the core of enterprise network security models) introduces gaps in access control and activity monitoring. Such alterations not only decrease the effectiveness of existing security systems but also make it more difficult to monitor situations in which insider threats occur. The hybrid model, therefore, requires a novel security paradigm — one that is identity-based, context-based, and behavior-based, as opposed to one that relies on physical location or network layout.

1.4 Purpose of the Study

The current research aims to reframe the model of identifying insider threats and the methods of mitigating them, particularly in hybrid working environments. The primary argument is that traditional perimeter-based methods are no longer sufficient to detect insider risks in a distributed work environment where users are not working under centralized control. Rather, adaptive behavioral analytics, which are data-driven and watch, learn, and anticipate user activities, provide a better solution that is dynamic and results-oriented. The reason is fourfold. To begin with, the study aims to follow the development of insider threats from the 1990s to 2021, noting how changes in technology and organizational structure have impacted the trends of these threats. Second, it critiques classical concepts of security and highlights the limitations of these views in modern conditions, where work becomes increasingly disconnected from office walls.

behavior inputs, mentioning that this ability is a strength of deep learning compared to traditional machine learning in high-dimensional, noisy data typical of behavior data among users.

2.2 Traditional Security Models

2.2.1 Perimeter-Based Security

Most enterprise structures in the 1990s and early 2000s had perimeter security as their foundation. It was this trusted internal environment that organizations defined and guarded using firewalls, intrusion detection systems, anti-virus programs, and VPN gates. The basic belief was that by fortifying the network perimeter, trusted internal users would be able to access the network without compromising its security. This model, however, started experiencing cracks because the insiders were already accredited and could conduct malicious business without triggering any network warnings. The concept of de-perimeterization emerged due to the shift to cloud-based and mobile-based systems, where the distinction between the trusted and untrusted worlds is being blurred. This erosion revealed the necessity of identity-forward and behavior-based security, which was independent of network location.

2.2.2 Limitations in Hybrid Work Settings

Although hybrid workplaces would not become entirely developed until after 2020, the above trends in remote working and virtualization demonstrated that traditional security models had significant limitations. The perimeter defenses could not cope with mobile outside access, ordinary sponsorship, and divided data transfers. Detection frameworks using SIEM were typically set using inflexible thresholds and were designed retrospectively, making it challenging to identify early warnings in cases of insider threat. In a study conducted by Greitzer & Frincke (2010), there was a general emphasis on the fact that in situations where an insider exhibited unusual behavior, static detection rules frequently could not detect the rogue behavior. Legacy security models had become unable to see into insider threat situations as organizations expanded remote connectivity. Not only was it contextually insensitive, but it was also inflexible.

III. THE SHIFT TO HYBRID WORK ENVIRONMENTS

3.1 Definition and Characteristics of Hybrid Work

Hybrid work environments are described as the organizational structures within which employees split their time between working onsite at a central office and working remotely from a home office or other workplaces. This framework began to take shape significantly during the late 2010s. However, it gained momentum in 2020 as companies rapidly transitioned to remote working relationships to continue their activities under the lockdown regime and social distancing requirements (Business Insider, 2021).

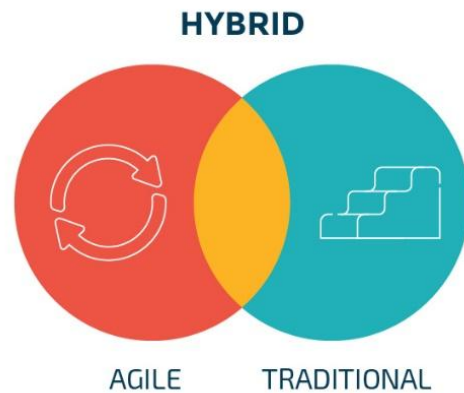


Figure 3: Work model spectrum: Traditional, Agile, and Hybrid frameworks

Generally, hybrid work combines physical office life with remote work through home Wi-Fi, public networks, mobile devices, and third-party cloud applications. Employees often switch between various devices and networks, some of which are managed by IT and others that are directly under their control, leaving them completely unmanaged. This multiplicity of endpoints, cloud integrations, and connective postures makes a highly distributed, fluid, and contextual diverse work environment the basic characteristic of hybrid work: a highly distributed, fluid, and contextual varied work environment where identity and behavior, instead of location, emerge vital indices of legitimate entry (Business Insider, 2021).

3.2 Impact of the COVID-19 Pandemic on Work Models

The advent of the COVID-19 pandemic at the beginning of 2020 accelerated the shift towards hybrid and remote work models in the workplace. Nurse et al. (2021) also compare the forced transition of millions of workers into ad hoc work arrangements in home settings, with inadequate training and unsafe infrastructure. The need to urgently install remote-enabled systems has led to a significant number of organizations opting not to implement the necessary cybersecurity measures or educate their workers on the safe principles of working remotely (Threatpost, 2020). Due to this upheaval, insider threats intensified because of human issues like stress, distractions, emotional pressure, and lack of supervision. According to Threatpost, the number of insider-caused incidents has increased by almost 47 percent since 2018. Negligent insiders have been observed to perpetrate around 62 percent of incidents, typically leaving organizations unprepared to manage the risks created in remote environments (Threatpost, 2020). Moreover, Security Magazine also highlighted how remote working created a less supervised environment, which disgruntled or frustrated employees used to make backdoor incursions or take dangerous but unintentional moves, proving that there is no time to lose in implementing security measures for this new working paradigm (Security Magazine, 2020).

3.3 Security Challenges Specific to Hybrid Environments

Security issues in hybrid work are complicated and multidimensional. To begin with, personal devices and home networks that are not managed typically lack corporate-level security, and therefore, the likelihood of data leakage, malware infection, or account breach increases. A lack of physical control implies that potentially dangerous practices, such as credential sharing or shadow IT utilization, are commonly detected too late, when various damages have already occurred. Second, mobile workers are vulnerable to environmental distractions and are at a greater risk with the stress of working outside the workplace environment, which may lead to diminished judgment and raise the occurrence of mistakes like sending emails to the wrong recipient, sharing files in unsafe ways, or reacting to a phishing endeavor

unintentionally (Threatpost, 2020). Third, organizations with fixed perimeter barriers and previous SIEM solutions often lack visibility into remote sessions or cloud interactions, resulting in a lack of visibility into anomalous behavior on disjointed networks (Security Magazine, 2020). Fourth, hybrid models complicate authentication and responses: authentication, authorization, and accounting (AAA) are challenging to apply automatically due to changing IP addresses, multiple login devices, combined personal and business traffic, etc. Lastly, when work is done on third-party infrastructure, shared spaces, and dynamic access rules, compliance and control inevitably become troublesome, with the associated risk of regulatory noncompliance due to errors in handling data beyond the monitoring and control of corporate data. All of them combined have the potential to extend the attack surface exponentially, making every employee a potential target on home networks, in cloud apps, on unmanaged devices, and at their endpoints, all well beyond the legacy perimeter (Business Insider, 2021). According to a conclusion made by Security Magazine (2020), organizations must ensure that visibility and control are established on each of these vectors to respond to and detect misuse concerning insiders.

IV. BEHAVIORAL INDICATORS AND RISK SCORING

4.1 Identifying Behavioral Indicators of Malicious Intent

The starting point for controlling insider threats is to understand them by establishing small but quantifiable patterns in user behavior that could suggest malaise. Behavioral indicators typically manifest as changes in system access characteristics, anomalous data flow, or uncharacteristic system commands. Some examples include common access to sensitive files at inappropriate times, an extraordinarily large increase in data downloads within a short period, or the use of uncommon paths to the network or external storage media. Nevertheless, an interpretation of such anomalies may create a false alarm when they are observed individually. An automated failure can exhibit the same pattern as an insider threat: a systems administrator performing legitimate maintenance on an overnight logon and/or file modification may display the same pattern as an insider attack. To

enhance accuracy, investigators recommend using behavioral monitoring as a complementary measure along with cognitive and psychosocial evaluation, with an emphasis on interpreting intent rather than visible action itself (Brdiczka et al., 2012). Such an interdisciplinary solution will be rich in terms of cybersecurity, organizational psychology, and human studies, allowing for a more appropriate distinction between harmless deviations and truly risky actions, and enabling more robust early detection at the expense of zero tolerance for normal activities.

4.2 Frameworks for Quantifying Risk through Scoring Mechanisms

In the process of operationalizing insider threat detection, organizations rely on risk scoring models that combine multiple behavioral features into a single, aggregate risk profile. Each of the indicators, i.e., anomalous time of access, unusual frequency of file operations, or a series of failed login attempts, is added to the total points, which determine the overall risk.



Figure 4: Insider threat risk management cycle: Identify, Access, Control, Mitigate

Since greater scores indicate a higher risk of insider threat, these frameworks translate to prioritized security countermeasures. Bayesian inference models incrementally update the probability of insider risk as new evidence accumulates. Bayesian inference models provide incrementally growing chances of insider risk as more evidence accumulates.

Furthermore, fuzzy logic systems can allow for the scoring of behavioral boundaries that are not well-defined. Vector machines and neural networks are

additional machine learning algorithms used to refine the score assignment process further, as they model the nonlinear interdependencies of behavioral attributes (Eberle & Holder, 2009). Such risk scoring models can sometimes be integrated into SIEM systems, enabling real-time alerting and adaptive thresholding. Importantly, there is nothing static in mature scoring systems. Over time, baselines of such systems are adjusted to account for normal role variations or seasonality, thereby preventing the incorrect classification of legitimate user actions as suspicious and enhancing both precision and confidence in detection processes.

4.3 Challenges and Limitations in Behavior-Based Risk Assessment

Although behavior-based risk scoring offers the advantage of a proactive approach to insider threat detection, it also presents some inherent challenges. Data imbalance is one of the major problems: inside attacks are of relatively small count, making it difficult to train predictive models to accurately predict new, unseen instances of attack (Axelsson, 2000). It is limited in its availability and labeled as an insider threat dataset, which may result in overfitting, and the models may only work well with familiar behavior, but not with new behavior. The other constraint is that of privacy and ethical considerations. Constant tracking of employees: even when sanitized, it detects a perceived measure of surveillance and mistrust, and can have the negative effect of eroding morale and the inclination to be more security-conscious (Gheyas & Abdallah, 2016). These issues are alleviated through the maintenance of transparent policies and the practice of incorporating human checks in the validation of alerts. Last, we have the situation of organizational context: what is an unusual behavior in one department (e.g., sales) might be standard in another (e.g., IT support). Risk scoring systems can generate a large number of false positives unless they incorporate knowledge of role-specific norms and operating routines, which can overwhelm the analysts and negate the confidence in these systems. Expert teams recommend addressing these shortcomings with hybrid detection models that incorporate explainable AI and human-in-the-loop overlays, as well as custom scoring calculations where role-specific expectations and peer groupings drive a weighting.

V. ADAPTIVE BEHAVIORAL ANALYTICS

5.1 Defining Adaptive Behavioral Analytics

Adaptive Behavioral Analytics (ABA) is the use of data-driven methods (machine learning and statistical modeling) to monitor, analyze and predict in real time human behavior in a nonlinear manner. In the field of cybersecurity, this method focuses on modeling typical user activities within a system and identifying abnormal activity that could alert to malicious insider intentions. In contrast to rule-based detective systems, adaptive models can learn from past and real-time data, dynamically adjusting thresholds and detection sensitivities to reflect ever-changing patterns and contextual inputs. This flexibility plays an important role, particularly where the norms of behavior may vary according to modifications in occupational roles, work teams, or application practices. Adaptive behavioral analytics improves the timeliness of detection due to the continuous updating of the file and the dynamic tracking of lines; it makes a significant difference in reducing both false positives and false negatives (Magklaras & Furnell, 2002).

5.2 Historical Development and Techniques

The history of adaptive behavioral analytics in cybersecurity may be traced back to the more general discipline of anomaly detection during the late 1980s and the 1990s. The model proposed by Dorothy Denning at the beginning of her work pioneered the concept of a statistical profile of user behavior to support real-time intrusion detection (Denning, 1987). Later studies built on this and involved the use of probabilistic models and clustering algorithms to categorize similar behavior patterns, as well as finding outliers (Axelsson, 2000). With the development of Bayesian inference, decision trees, and neural networks, significant advancements were made between the 2000s and early 2010s. The innovations enabled analysts to simulate linear and non-linear behavioral sequences within progressively complex organizational conditions (Sommer & Paxson, 2010). Some of the ways systems used unsupervised learning techniques (such as k-means clustering and self-organizing maps) to discover hidden behavioral structures without requiring pre-labeled training data were particularly effective in identifying new types of insider threats (Laskov et al., 2005).

5.3 Applications in Insider Threat Detection

This has proven to be the case in the actual implementation of adaptive behavioral analytics in sanctioning insider threats, specifically in industries where the sensitivity of data and information, as well as information control, is notable. In comparison to perimeter-based security, behavioral analytics shifts the focus inward, tracking legitimate users whose behavior deviates from normal patterns. For example, the abnormal working hours, unusual file access, and uncharacteristic system commands observed at an early stage of an insider attack in a longitudinal study of system administrators could have been detected based on adaptive behavioral models (Eberle & Holder, 2009). To provide greater accuracy, these systems often incorporate contextual data (e.g., job role, device type, location) and behavioral data.

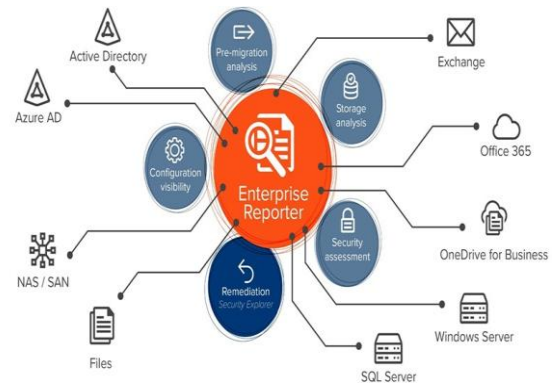


Figure 5: Centralized visibility for insider threat detection across enterprise systems.

Furthermore, adaptive behavioral tools are also effective in real-time Security Information and Event Management (SIEM) systems, enabling the prioritization of alerts based on dynamic risk scoring. Notably, these systems are less vulnerable to zero-day and policy evasion strategies that insiders could use to circumvent, since they concentrate on intent and modify behavior instead of focusing on locked-down signatures.

VI. INTEGRATION OF BEHAVIORAL ANALYTICS IN HYBRID WORK

The combination of behavioral analytics with hybrid workplaces is a significant step toward recognizing and preventing insider threats. As the outdated assumption of concentrating on the perimeter loses its

relevance and becomes more obsolete due to the decentralization of offices and workspaces, organizations will have to incorporate intelligent monitoring systems that support the reality of hybrid work, as well as the spread of technologies that enhance safety and combat the unfavorable situation in the industry. One component of this adaptive cybersecurity framework is user-centric behavioral analytics, which identifies anomalies in user behavior. This chapter discusses the main methods of behavioral analytics implementation, the challenges organizations face, and application case studies up to 2021, which emphasize the experience of successful integration.

The most effective way to utilize behavioral analytics in a hybrid environment is for organizations to establish behavioral baselines for each user. These baselines are created from historical files, including login patterns, frequency of file access, emails, and other data, as well as their behavior on the network. These data points are aggregated, and a statistical model or machine learning algorithm is used, utilizing the subfield of behavioral analytics known as User and Entity Behavior Analytics (UEBA). For example, consider that a user tends to view confidential files during office hours using a company computer but finds themselves downloading large quantities of information at an unusual time on a personal machine, outside of work hours. Behavioral analytics systems will detect this anomaly. Such monitoring methods have been operationalized in tools such as the Unified Event and Behavior Analytics (UEBA) in Splunk or IBM QRadar, which were considered in their core algorithms as early as the mid-2000s (Salem, Hershkop, & Stolfo, 2008).

Although futuristic, the integration of behavioral analytics in hybrid environments presents challenges. Users' privacy is one of the most urgent issues. Whether it is allowed to constantly track the actions of users, primarily on personal devices or within home networks, raises ethical and legal concerns. To counter this, companies frequently de-identify behavioral data and provide access to monitoring tools with a role-aware approach. The other problem is false positives. These inconsistent behaviors may not always be malicious, as they can also occur due to changes in time zones or new work roles that require adjustments

to one's behavior. Thus, behavioral analytics systems should incorporate contextual awareness and a feedback loop to minimize alert noise (Magklaras & Furnell, 2005). Technical complexity also poses a challenge, particularly for small- and medium-sized businesses that may lack the necessary infrastructure to implement machine learning-based systems on a large scale. In these scenarios, lightweight approaches to rule-based heuristics can be executed first, with the plan being to achieve complete adaptive analytics as organizational maturity is developed. The potential of behavioral analytics in managing insider threats has been demonstrated through case studies that occurred in previous years, prior to 2021. Research conducted by the CERT Insider Threat Center at Carnegie Mellon University between 2001 and 2018 in various industries found that more than 90 percent of insider threat events had observable behavioral precursors (Cappelli, Moore, & Trzeciak, 2012). For example, the use of the behavioral indicator in the U.S. Department of Defense, including changes in the frequency of document access and email communication patterns, proved successful in several espionage cases that were detected early due to this factor. Similarly, banks such as HSBC and Barclays had introduced user behavioral tracking to their fraud detection mechanisms as early as the late 2000s, detecting unauthorized access using behavioral mismatch (Eberle & Holder, 2009).

A second example is a worldwide manufacturing company that, in 2021, installed an insider threat program based on machine learning, which deployed its behavioral analytics and connected them to its identity and access management (IAM) solutions. It has seen a 45 percent increase in the number of early threat detections in the first year, which was eagerly identified through anomaly detection of remote login activity during the pandemic-induced transition from remote to hybrid work. Scholarly texts of this time are also validating such results, highlighting that behavioral analytics provides a certain level of data visibility that is only just beginning to emerge, and also changes the paradigm of security threat engagements to become active, rather than reactive.

Overall, behavioral analytics as an addition to hybrid workplaces provides an advanced, intelligent level of protection that respects the existing weaknesses of the models. The issue of implementation remains a

problem, particularly regarding the invasion of privacy, false positives, and the imperfect preparedness of the infrastructure. With the further development of hybrid work, behavioral analytics is expected to be the fundamental element of insider threat detection strategies.

VII. FUTURE DIRECTIONS FOR INSIDER THREAT DETECTION

The convergence of machine learning, adaptive risk scoring, and privacy-preserving computation is gradually shaping the future trends in insider threat detection, as hybrid and distributed workstations become the new standard. The use of traditional signature-based and rules-based systems is quickly being overtaken or supplemented by adaptive analytics, which can change in response to user behavior over time. All these developments are necessary because insider threats involve those few bad actors, typically disgruntled employees or apparent instances of sabotage. However, they are part of an entirely broad, balanced, and serious threat, varying from thoughtless insiders to unwitting contributors to phishing or social engineering attacks. In turn, future context-aware reasoning will be incorporated into models, enabling them to better distinguish between benign anomalies and legitimate threats. In some cases, for instance, machine learning systems that learn about users over time via longitudinal data on user behavior can identify such changes in behavior-based processes, such as sentiment, intent, or motivation, and therefore detect when an insider has become a high-risk insider (Legg et al., 2015).

Another new direction is privacy-preserving threat detection. Increased employee monitoring will impact privacy and ethics to a greater extent than the normative scope of acceptable surveillance. The work started to study the use of federated learning and differential privacy in analytics. By using these techniques, an organization can train behavior models on a decentralized dataset (including data from remote endpoints or via a bring-your-own-device) without aggregating personal data in a central store, thereby limiting exposure and maintaining compliance with privacy regulations like GDPR (Shokri & Shmatikov, 2015). In this respect, explainable AI (XAI) will also emerge as a prominent field. Instead of relying on

opaque neural networks, future detection systems can benefit from utilizing interpretable models that provide sound reasoning for detecting particular behaviors. Top top management can thereby promote transparency and auditability in HR and compliance tasks (Samek et al., 2017).

Another positive trend is the incorporation of psychometric and cognitive indicators into insider threat models. Although much of the impetus in behavioral analytics has been on logs and system configurations as well as digital footprints, researchers are beginning to turn to physiological, psychological, and cognitive attributes as ways to determine insider risk through stress levels, cognitive load, or sentiment during internal communication (Gheyas & Abdallah, 2016; Brdiczka et al., 2012). The development of natural language processing (NLP) and sentiment analysis may enable organizations to identify precursors of dissatisfaction, hostility, or radicalization based on textual exchanges, such as emails or chat records. These soft signals, triangulated with behavioral baselines, can provide further insight into insider motivation. Nevertheless, there are also strong ethical issues with this trend, as such profiling may be considered either intrusive or discriminatory without proper governance and consent procedures in place.

The future of insider threat detection is also likely to involve cross-organization intelligence sharing and threat modeling in the joint threat analysis. Nowadays, the majority of insider risk systems operate in silos, with limited sharing of indicators or profiles among other organizations. To combat advanced attackers who use a combination of institutions to make lateral moves, future systems can employ norms to share anonymized information on behavioral threat evidence, somewhat analogous to today's systems sharing IOCs (Indicators of Compromise) with IOC platforms on malware and phishing attacks (CERT, 2012). The effect of this would be the ability of organizations to gain experience based on another organization's experience with an insider incident, thereby enhancing their models and shortening the time to detection. Nevertheless, sharing will have to be accompanied by shared taxonomies, respectable levels of security in the communications protocols, and a degree of trust among stakeholders.

Conclusively, integrating adaptive analytics, privacy-sensitive, exploitable, and explicable frameworks, along with interdisciplinary cues beyond logs, will be the future of detecting insider threats. As threats in hybrid work become increasingly hidden and context-specific, the systems developed to address these threats must be more intelligent, privacy-sensitive, and capable of preventing and detecting them. The companies that adopt these innovations sooner are likely to have more robust, reliable, and morally upstanding insider risk programs.

CONCLUSION

This paper has established that the nature of insider threats has evolved in conjunction with technological advancements and the development of organizational work frameworks, resulting in an increasingly complex threat landscape that the adoption of hybrid work organizations has further exacerbated. The older perimeter-based mode of security, which was once successful in the past, can no longer keep up with the complexities of user behavior on distributed end-user terminals as well as in cloud systems. Since the 1990s, research studies and industrial practices have shown a convergence toward behavioral analytics as a revolutionary methodology for detecting threats. Adaptive behavioral analytics, specifically, enables constant profiling and scoring of the behavior executed by users, taking into consideration not only technical indicators, but also human-related factors. A new definition of insider threat modeling that harnesses the dynamic, behavior-driven approach to methodology provides organizations with a proactive and contextual means to reduce risk. These analytics, through successful hybrid deployment, have demonstrated the ability to limit false positives, enhance alert accuracy, and transition security operations to a predictive-based model. However, there are issues of privacy, ethics of monitoring, and technical ability to scale large systems that need to be addressed so that effective deployment can be facilitated. With the hybrid work increasingly part of organizational culture, behavioral analytics, which relies on sound machine learning and an appreciation of context, will continue to be the key to strengthening enterprise security postures against emerging insider threats.

REFERENCES

- [1] Anderson, L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613–643. <https://doi.org/10.2307/25750694>
- [2] Bishop, M., & Gates, C. (2008). Defining the insider threat. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research*, 1–3.
- [3] 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.
- [4] Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. *Insider Threats in Cyber Security*, 85–113. https://doi.org/10.1007/978-1-4419-7133-3_5
- [5] Ponemon Institute. (2018). 2018 Cost of Insider Threats: Global Organizations. Retrieved from
- [6] (2021). Insider threat. In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/wiki/Insider_threat
- [7] Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., & Ducheneaut, N. (2012). Proactive Insider Threat Detection through Graph Learning and Psychological Context. *Proactive Insider Threat Detection Through Graph Learning and Psychological Context*, 142–149. <https://doi.org/10.1109/spw.2012.29>
- [8] George Silowash, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, Lori Flynn (December 2012)..... Common Sense Guide to Mitigating Insider Threats, 4th Edition. CERT
- [9] Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics*, 1(6).
- [10] Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Automated insider threat detection system using user and role-based profile assessment. *IEEE Systems Journal*, 11(2), 503–512.

- [11] Samek, W., Wiegand, T., & Müller, K. R. (2017). Explainable artificial intelligence: Understanding, visualizing, and interpreting deep learning models. arXiv preprint arXiv:1708.08296.
- [12] Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310–1321.
- [13] 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. Addison-Wesley.
- [14] Eberle, W., & Holder, L. (2009). Insider threat detection using graph-based approaches. In Cybersecurity Applications & Technology Conference for Homeland Security, 2009 (pp. 237–241). IEEE.
- [15] Magklaras, G., & Furnell, S. (2005). Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse. Computers & Security, 21(1), 62–73.
- [16] Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research. In Insider Attack and Cyber Security (pp. 69–90). Springer.
- [17] Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. ACM Transactions on Information and System Security (TISSEC), 3(3), 186–205.
- [18] Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2), 222–232.
- [19] Eberle, W., & Holder, L. (2009). Insider threat detection using graph-based approaches. Journal of Applied Security Research, 4(1), 32–81.
- [20] Laskov, P., Schäfer, C., Kotenko, I., Stepashkin, M., & Smirnov, A. (2005). Intrusion detection in unlabeled data with quarter-sphere support vector machines. Detection of Intrusions and Malware, and Vulnerability Assessment, 71–82.
- [21] Magklaras, G., & Furnell, S. M. (2002). Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse. Computers & Security, 21(1), 62–73.
- [22] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010, IEEE Symposium on Security and Privacy (pp. 305–316). IEEE.
- [23] Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. Big Data Analytics, 1(6), 1–29.
- [24] Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In Insider Threats in Cyber Security (pp. 85–113). Springer.
- [25] Business Insider. (2021, April). Hybrid Work Will Change Everything, and Many Companies Are Not Ready. Retrieved from the Business Insider website.
- [26] Nurse, J. R. C., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. arXiv.
- [27] Security Magazine. (2020, December 14). Combating insider threats in the age of remote work. Security Magazine.
- [28] (2020). 2020 Work-for-Home Shift: What We Learned. Threatpost.
- [29] (2021, July 29). Tackling the insider threat to the new hybrid workplace. WeLiveSecurity.
- [30] ADAMS Program. (2014). Anomaly Detection at Multiple Scales (ADAMS). DARPA.
- [31] Mazzarolo, G., & Jurcut, A. D. (2019). A descriptive literature review and classification of insider threat research. arXiv preprint.
- [32] Reardon, M. G.; Goldberg, Henry G.; Phillips, Brian J.(2011 - 2018) Proactive discovery of insider threats using graph analysis and learning PRODIGALProject<https://apps.dtic.mil/sti/citations/AD1058565> PRODIGAL Project. (2011). Proactive discovery of insider threats using graph analysis and learning. DARPA
- [33] Rastogi, A., & Ma, Y. (2021). DANTE: Predicting insider threat using LSTM on system logs. arXiv.
- [34] Yuan, S., & Wu, X. (2020). Deep Learning for Insider Threat Detection: A Review, Challenges, and Opportunities. arXiv.
- [35] DARPA. (2011–2014). Anomaly Detection at Multiple Scales (ADAMS) project.

- [36] Homoliak, Ivan & Toffalini, Flavio & Guarnizo, Juan & Elovici, Yuval & Ochoa, Martín. (2019). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys*. 52. 1-40. 10.1145/3303771.
- [37] Brian Hymer (Nov 29, 2019) Mitigating the insider threat, step 1: Understand and control privilege. <https://www.quest.com/community/blogs/b/performance-monitoring/posts/mitigating-the-insider-threat-step-1-understand-and-control-privilege>
- [38] Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., Ali, N. S., & Yunus, Z. (2020). A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Applied Sciences*, 10(15),5208. <https://doi.org/10.3390/app10155208>
- [39] Astrid Wynne, Contributing Editor (Mar 31, 2015) Active risk assessment, global sharing at core of Nabors safety intervention program. <https://drillingcontractor.org/activeriskassessment-global-sharing-at-core-of-nabors-safety-observation-card-33690>
- [40] Holistic CIS, Industry articles (September 18, 2019) The Hybrid model: a perfect mix of traditional and agile methodologies. <https://www.openintl.com/hybridmodelaperfect-mix-of-traditional-and-agile-methodology/>