

UEBA

DLP

NTA

Final Executive Report

Insider Risk Mitigation Technology Study

IAM

SIEM

EPP

Darian Scherbluk

Norman Paterson School of International Affairs

December 2022

DL

DAM

Contents

- Introduction
- Identity and Access Management
- Security Information and Event Management
- Database Activity Monitoring
- Network Traffic Analysis
- Data Loss Prevention
- Endpoint Protection Platforms
- Deep Learning
- User and Entity Behavior Analytics



Introduction


The goal of this project was to conduct a technology tracking study with secondary sources to scan existing and emerging technological tools related to insider risk mitigation and management. **The major research question that this initiative was developed around asked which technologies are currently—and could be—utilized in the near future as sufficient tools for insider risk mitigation controls?** The results of this study may help organizations refine their assumptions around how and which technologies can influence an insider risk strategy and program.

After completing an initial scan of the environment, it was determined that the project would focus on different categories of tools as opposed to specific vendors. These tools were selected based on their relevance to insider risk mitigation practices, their recognized abilities in the field of cybersecurity and the amount of researchable data that was available on each given tool.



Executive Summary

- IAM tools involve a complex set of processes that require significant training to ensure that IAM tools are functioning properly and aligned with organizational policies, as well as limit errors in automation processes that could inadvertently systematically expand the potential insider threat attack surface.
- There are concerns that SIEM tools generate large amounts of false positive security alerts as they rely on the coded rules and use cases based on past compromises.
- There could be negative consequences to activity monitoring of employees as it can potentially lead to perceptions of privacy intrusion and create higher levels of stress in the workplace and mistrust of upper management.
- Organizations will have increased costs and complexities of running NTA solutions as they will require the purchase of additional storage and load balancers to integrate with NTA tools.
- Next generation integrated DLP products will have the ability to seamlessly connect with intelligent human behavioral analytics, and better monitor employee activities in organizations.
- Endpoint security tools should be considered as another component of a comprehensive risk mitigation strategy against insider threats as opposed to a sole solution.
- Deep learning solutions may be more difficult to initially employ but once properly optimized can generate results instantaneously and will continue to improve an organization's security detection mechanisms over time
- The sophistication of UEBA tools allow for it to effectively adapt to an organization's complex and evolving needs but can be overwhelming and too costly for small to medium-sized businesses to address security threat detection.



IAM has existed since the 1960s in the form of general usernames and passwords to secure computer files. It had existed mostly unchanged until the shift to present day cloud-centric virtual work environments (Williams, 2009). With significant advancements in biometrics and increased adoption of multi-factor identification, the IAM landscape has completely evolved to make simple use of usernames and passwords obsolete forms of verification.

Identity and Access Management

IAM




Overview and Development

- Identity and access management (IAM) tools are used for defining, managing and ensuring individuals have appropriate access to systems and data. IAM tools provide ongoing identity verification to reduce the likelihood of insider threats successfully exploiting access. IAM can be a significant component of an organization's corporate security strategy and critical for defending against data loss.
- There have been recent significant developments in IAM with the creation of fast identity online mechanisms. These mechanisms provide security solutions that can entirely eliminate passwords and instead rely on various biometric methods, personal smartphone device profiles, and hardware security keys that can continually assure one's identity. As an example, IAM biometric tools can include recognition of kinesthetics body movements, vocal patterns, physiological features, and device-based gestures to define and differentiate specific individuals against irregular behaviors. IAM has also evolved to identify non-human software and hardware such as IOT devices. Additional non-human entity verification includes application programming interfaces and keys that can also be authenticated to prevent potential data breaches. IAM tools can be effectively utilized within a variety of cloud and on-premise networks (Indu & Bhaskar. 2018).

Benefits and Drawbacks

- A key feature of IAM technology is its single sign-on functionality that lets individuals access all permitted applications and services within an organization by only using one set of login credentials. This control can strengthen an organization's security by removing vulnerable password management practices, minimize attack surfaces and streamline IT operations by centralizing administrative security functions (Haber & Rolls 2020). All of these practices can help reduce a company's vulnerabilities to insider threats. Most IAM tools now provide adaptive multi-factor authentication abilities to protect against insider threats, requiring users to provide multiple forms of verification to gain access to a system such as a fingerprint, voice recognition, iris scan, etc. (Devlekar, & Ramteke, 2021). This adaptive feature also uses contextual information such as time of day, device type, IP address and organizational policies to determine which different authentication factors to apply to a particular individual in a specific situation. Many IAM solutions also have automated user provisioning and life cycle management features that provide an organization with tools for onboarding and managing a person's access privileges throughout the progression of their employment. These features ensure that employees are provided fewer opportunities to maliciously exploit their corporate access, leading to potential insider threat incidents.
- There are potential drawbacks to consider including significant inefficiencies and vulnerabilities in IAM solutions if an organization has not automated repetitive processes such as offboarding (Froehlich, 2021). A lack of automation could lead to an insider threat in instances of employees who leave a company but have not had their authentication and access automatically revoked. **IAM tools involve a complex set of processes that require significant training to ensure that IAM tools are functioning properly and aligned with organizational policies, as well as limit errors in automation processes that could inadvertently systematically expand the potential insider threat attack surface.**



SIEM tools were first introduced in the early 2000s as either basic Security Information Management or Security Event Management tools used for basic log aggregation across different systems that had various limitations. Today these two types of tools have been combined into one that may utilize advanced behavioral analytics, evolving from a rules-based approach to utilizing advanced forms of artificial intelligence.

Security Incident and Event Management

SIEM




Overview and Development

- Security information and event management (SIEM) is a technological tool that can analyze events and enable a more respond quickly to potential insider threat incidents as well as effective tracking and logging of event security data. SIEM products have evolved in recent years from basic log management into a mechanism that now offers advanced artificial intelligence driven automation (González & Diaz, 2021). The main features of SIEM include log management, event correlation and analytics, incident monitoring and security alerts. SIEM tools are pre-built and pre-packaged software that can be tailored to generate automatic reports designed to meet an organization's specific security needs.
- Artificial intelligence will become increasingly important in the development and performance of SIEM tools. Enhanced artificial intelligence will expand the cognitive capabilities of SIEM technology and enable it to adapt to a larger scale of audit logs from endpoints to be consumed from cloud-based and mobile networks (Corcoran, 2018). Future iterations of SIEM tools with more highly advanced artificial intelligence will have the potential to support almost all data types and continue to self-evolve and anticipate changes in the evolving threat landscape.

Benefits and Drawbacks

- SIEM is a highly efficient system that replaces the manual processes involved in insider threat detection and incident responses by automating behavioral anomaly analysis. Mature SIEM tools integrate Security, Orchestration, Automation and Response (SOAR) capabilities which have the potential to automate an organization's information and insider threat security systems. As a result of highly intricate machine learning, SIEM tools can adapt to analyzing complex network behaviors through threat identification and independently follow a company's incident protocols for managing potential insider threat incidents (Caldeira, 2021).
- By utilizing integrated threat intelligence feeds and artificial intelligence technology, organizations can rely on SIEM tools to detect known—and provide indications on suspected—security threats, by continuously adapting to a changing attack surface (Radoglou-Grammatikis, et al., 2021). SIEM solutions can also support digital forensic investigations after an insider threat activity has occurred. SIEM tools can effectively track, collect and analyze log data from different sources in an organization in one centralized location.
- **There are concerns that SIEM tools generate large amounts of false positive security alerts as they rely on the coded rules and use cases based on past compromises.** As a result, a misconfigured SIEM system can generate thousands of false positive alerts (Villanueva, 2021). This can make it extremely difficult for a company to identify actual security threats from log data and could result in the failure to respond to a security breach. It can be quite cost-prohibitive for an organization to set up an effective SIEM system.



This technology has been around since the beginning of the 2000s starting off as a system to record every time an administrator logs into a database (Mogull, 2020). Many different versions of DAM tools have now become fully automated, providing instantaneous analysis of activity and alerts of specific undesirable actions within a database.

Database Activity Monitoring

DAM




Overview and Development

- Database activity monitoring (DAM) is a set of technological tools that have the ability to detect suspicious behavior internally. Through the implementation of standalone computer configurations or cross platform software modules loaded onto database servers, DAM utilizes real time security monitoring and analyses technologies to provide an accurate picture of all user activities that can be used for insider threat monitoring (Information Technology Newsweekly, 2009). This is done by DAM's automated processing of network sniffing, memory scraping and audit logs. In turn, the owners of the DAM tools can improve the visibility of their data and decrease the likelihood of an insider threat incident from occurring.
- DAM technologies are continually increasing in sophistication beyond a basic analysis of an individual's activities in a database (Grushka-Cohen et al., 2020). Some emerging features that distinguish the latest DAM technologies include the ability to continuously monitor and audit database activities including administrators and other privileged users without negatively impacting a system's operations or performance. In addition, DAM tools can securely store a given database's activity externally for data protection and recovery purposes and support high data integrity requirements by preventing the manipulation or tampering of recorded activities. This technology can also aggregate and correlate database activity from various different operating systems for rapid analysis and alerts on policy violations.

Benefits and Drawbacks

- DAM tools are powerful, flexible, and scalable, and are often deployed as an effective information centric security option and can be an effective insider risk mitigation mechanism. These technological tools are specifically helpful in preventing and detecting data breaches and protect a company's sensitive internal database from exposure due prohibited user activities (Kim et al., 2013). It can also help ensure employee compliance with a company's insider risk and security compliance practices by monitoring employees' activities as aligned to organizational policy and cyber security hygiene best practices.
- DAM technologies can offer an additional avenue to enhance detection of unintentional or malicious insider threats. It is one of the few technologies that can immediately improve security against insider risks and reduce the manual oversight of a company's insider risk compliance (Technology Business Journal, 2019). There are also future projections that DAM can provide unique insights into an organization's most information sensitive databases and provide a proactive security defense against insider risk activities that could occur on a company's network.
- It is important to note that DAM is still an emerging technology. **It should be considered that there could be negative consequences to activity monitoring of employees as it can potentially lead to perceptions of privacy intrusion and create higher levels of stress in the workplace and mistrust of upper management.**



NTA technologies were first developed in the late 1980s with first generation models conducting simple network management protocols to collect and manage basic information about a limited number of devices remotely. Since then, NTA's have evolved to analyze all network traffic information from any Internet source, provide live alerts on suspicious activity, and automating processes to locate patterns in large amounts of data (Araujo, 2022).

Network Traffic Analysis

NTA




Overview and Development

- Network traffic analysis (NTA) can be used to identify and respond to insider threats by intercepting, recording and analyzing network traffic communication patterns. NTA allows organizations the ability to obtain rapid threat visibility that could impact their organization (Information Technology Newsweekly, 2019). Implementing NTA technology can enable an organization to enhance its security against insider threats, by minimizing the attack surface area. The significant increase in network traffic due to the remote work posture that increased during the global pandemic along with the creation of additional global data centers and data network infrastructure is raising the need for increased NTA tools. An increasing demand for cloud computing systems will continue to drive the demand for NTA (Grand View Research, 2021). Further advances in communications and networking technology is also expected to improve the capabilities of NTA tools in the next five years.

Benefits and Drawbacks

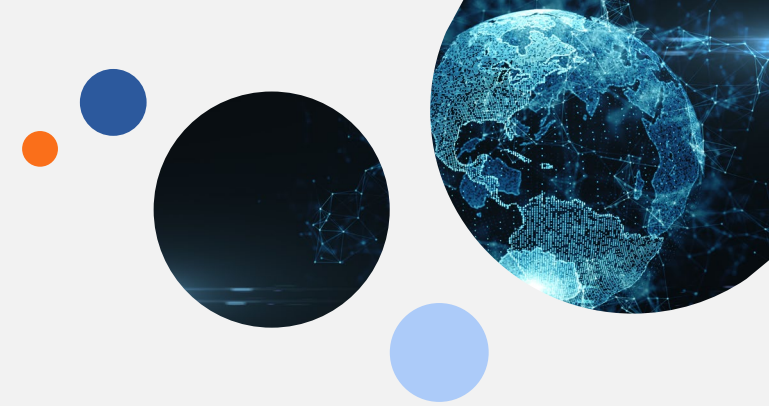
- Once NTA tools have been able to determine a baseline on normal activity on a given network, it can effectively alert an organization of suspicious activity early on to mitigate potential negative impacts (CISCO, 2022). NTA tools can attribute malicious insider threat indicators to a specific IP address, determine how a threat has moved within a given organization, and uncover what other organizational or employee devices may have been compromised, which can enable an organization to have a more rapid response time.
- NTA technology is used for collecting continuous real time network activity for archiving for further analysis to identify suspicious behavior (Miao et al., 2018). It can be an effective mitigation as almost all actions an employee takes in an organization entails interaction with the organization's network; therefore, the visibility on potential insider threats extends as far as any network access point. Whether an individual is on an organization's computers, in the cloud, or a combination of both, NTA technology can provide an organization the visibility and background context needed to fully understand what is occurring on the network at any given time.
- For NTA tools to be effective, they require large sets of historical, archived data to provide trained, time series models to highlight unfamiliar activities within a given network. NTA tools often have limited storage space and are only able to store the most recent data. As a result, NTA algorithms have the potential to be poorly trained if older archival data is not available due to storage limitations (Bais, 2022). **Organizations will have increased costs and complexities of running NTA solutions as they will require the purchase of additional storage and load balancers to integrate with NTA tools.**



Is one of the oldest types of methods involving various technologies that can be used for insider threat mitigation. DLP was first created in the early 1990s to provide encrypted email security (Brooks, 2020). Over time, various iterations of DLP methods have evolved adapting to the expanding threat surface, including the addition of information rights management tools, ability to categorize data and apply protection mechanisms—such as role-based access—appropriate to specific categorizations.

Data Loss Prevention

DLP




Overview and Development

- Data loss prevention (DLP) is a set of processes and technological tools that protect and detect against data breaches, exfiltration and the unauthorized destruction of sensitive data that can occur from insider threat attacks.
- DLP software organizes data into different categories of security access and can identify violations of data management defined by a given entity or within a predefined policy outline (Sousa, & Shahzad, 2021). Once a violation is detected, DLP tools can respond by providing management instantaneous security alerts, block user access with encryption tactics along with other protective measures to prevent from unintentional or malicious insiders from sharing or deleting data that could negatively impact an organization.
- The main objectives of DLP tools are to help organizations protect intellectual property, personal information and improve data visibility, which in turn can decrease the likelihood of insider risk incidents from occurring and make it more difficult for malicious insider threat activity to be successful.
- Ultimately, DLP solutions are not a new practice used by organizations, and has evolved to include cloud server functionality, advanced management service and threat protection (Technology Business Journal, 2022). With the increasing trend of large data breaches and the technological progression of DLP tools, more companies are implementing DLP solutions to protect sensitive data from external cyber attacks and internal insider threats. Advances in communications and networking technology are expected to open new growth opportunities for the market.

Benefits and Drawbacks

- A major component of a DLP solution is its ability to protect moving data and secure endpoints on an organization's network by analyzing traffic to detect if sensitive data is being moved in violation of security policies while also being able to control information transfers by blocking real time communications and providing user feedback (Hart & Johnson, 2011).
- These capabilities can prevent malicious or unintentional insider threats from exposing secure company information. DLP tools protect data-at-rest by implementing detailed access controls, technologically advanced encryption and can align with an organization's data retention policies to protect sensitive archived information.
- DLP technology can also secure data-in-transit through monitoring and alert on unauthorized user activities that could potentially harm an organization and provide indicators of malicious or unintentional activities (Lynch, 2022). Finally, DLP tools can automate data identification to determine the level of categorization of new organizational data.
- A considerable drawback is the time and expertise required to implement a comprehensive data protection policy that is necessary for a DLP to work effectively (Caldwell, 2011).
- A less mature data protection policy will cause significant issues when integrating DLP tools into an organization's cybersecurity system.
- In terms of insider threat detection, DLP cannot distinguish an individual's intent or analyze human nuances. As a result, DLP tools often need to be paired with behavioral analytics tools to maximize insider risk mitigation. However, products that integrate human focused threat detection benefits (i.e., user and entity behavioral analytics) are only currently being developed and beginning to appear on the market. **These next generation integrated DLP products will have the ability to seamlessly connect with intelligent human behavioral analytics, and better monitor employee activities in organizations.**



EPPs were first developed in the 1980s by physically installing basic antivirus signatures on a computer and required manually updates on a continuous basis (Obbayi, 2018). A great deal has changed since the first generation of these tools, with the emergence of next generation antivirus capabilities where updates on endpoint software may occur automatically through machine learning and artificial intelligence. During the 2010s, endpoint detection and response software was developed that could be utilized to detect, monitor and lead to the initiation of investigations to review suspicious activities occurring at organizational endpoints.

Endpoint Protection Platforms

EPP->EDR




Overview and Development

- Endpoint security involves protecting data associated with employee devices such as desktops, laptops and mobile devices that connect to an organization's network (Waseemullah et al., 2021). Endpoint protection platform (EPP) technology can detect, analyze, prohibit and contain security events that are in progress on an organization's network or cloud. Organizations of all sizes are vulnerable to cyber attacks along with malicious and unintentional insider threats in which EPPs can provide cyber security defense controls to protect organizational data (Oevering, 2020). EPPs examine files as they ingress or egress an organization's network to scan for potential threats. They provide security visibility of all connected endpoints from a single centralized location. In addition, EPPs now utilize cloud computing, enabling scalable storage of threat information that is captured.
- A recent progression in endpoint security has led to the development of proactive endpoint detection and response (EDR) tools. EDR technology is designed to move forward past the detection-based, reactive control foundation of EPP tools. EDRs provide proactive security tools such as more contextualized threat hunting. Further, EDR tools improve threat visibility by performing continuous analysis of data to produce rapid response investigations by automating data processing and incident management activities based on predetermined procedures and thresholds (Kaur & Tiwari, 2021). These capabilities enable EDR tools to remediate potential threat incidents and can reduce the workload of an organization's security analysts.

Benefits and Drawbacks

- EDR technology acts as a second layer of security allowing a company's security team to conduct threat hunting and focus on other more subtle threats that may reside on endpoints (Symphony Technology Group, 2022). This system complements existing EPP foundational tools that act as a first layer of defense and filters out potential threats. In the future, a strong endpoint security system will require a solution that integrates both EPP and EDR tools. The next steps of progression with EDR and EPP technology will involve the enhancement of threat intelligence capabilities by leveraging artificial intelligence and machine learning to further automate steps in threat intelligence and investigative processes.
- The biggest limitation to EPP and EDR tools is that they solely analyze and protect a company's traditional endpoints leaving other critical security gaps that insider threats can exploit. In an increased remote working environment, the prevalent use of bring your own devices (BYOD), allows areas in the potential attack surface where insider threats can potentially remain hidden from EPP and EDR capabilities as some Internet of Things (IoT) devices are designed with minimum regard for cybersecurity and can evade a company's security measures (Emmanouilidis, Mehen & Roy, 2019). IOT can ultimately create gaps in an organization's cybersecurity posture exposing parts of their network that are not related to known corporate endpoints. **Endpoint security tools such as EPPs and EDRs should be considered as another component of a comprehensive risk mitigation strategy against insider threats as opposed to a sole solution.**

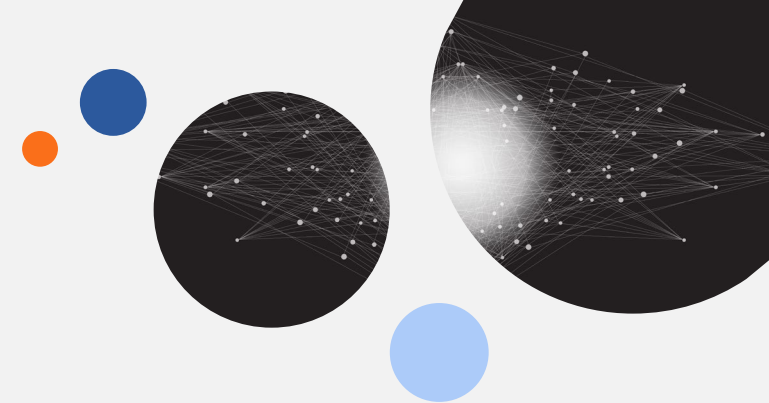


The creation of deep learning dates back to 1943 when Walter Pitts and Warren McCulloch created a computer model based on the neural networks of the human brain (Foote, 2022). Since then, deep learning has slowly evolved, with recent significant advances being enabled by increases speed and capabilities of computer processing units and cloud storage solutions.

Deep Learning

subset of machine learning and artificial intelligence

Deep Learning




Overview and Development

- Deep learning tools are a branch of machine learning classified under the category of artificial intelligence that can learn and make rational decisions on its own, attempting to imitate the way humans acquire knowledge. Deep learning utilizes artificial neural networks (ANNs) that are created with the purpose of mimicking the functionality of human brain neurons to continually analyze data to draw conclusions. As a result of the ANN structure, deep learning can effectively identify emerging patterns in unstructured data sets including sounds, images, video, and text to identify insider threat activities (Afzal, et al, 2021) . More specifically deep learning has named-entity recognition abilities that can classify specific sets of text, take large quantities of text data and create concise information out of it, and image processing powers that can filter through images and videos to analyze different pre-identified elements. Circumstances where deep learning tools would be the most relevant to use are for organizations that have large amounts of data to analyze and complex user behavior that needs to be analyzed to pinpoint individuals who could potentially be an insider threat.
- As an extremely new emerging technology, deep learning solutions have the capability of identifying more advanced insider threats for a given organization (Yuan, & Wu, 2021). In preliminary tests, deep learning ANNs are illustrating promising results in terms of analyzing HTTP network traffic to identify malicious behavior including insider threats. Companies are beginning to test deep learning technologies within their security strategies and run deep learning trial programs.

Benefits and Drawbacks

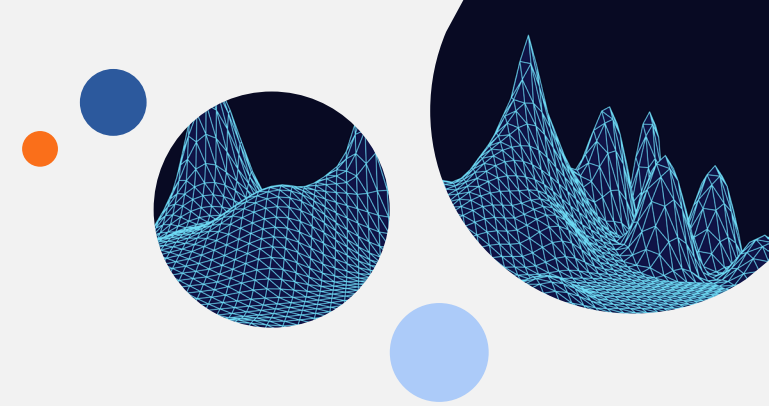
- Deep learning tools can be used as a method to automate proactive security analytics to highlight potential insider threats. These types of tools are also not necessarily reliant on commonly scripted security threat patterns and can recognize suspicious activity based on how a network system would be expected to operate at a baseline level. Deep learning solutions can also be applied to create more efficient intrusion detection and prevention systems. It more accurately analyzes network traffic, reducing the number of false positive security threats and more effectively differentiates suspicious network activities that could be indicative of insider threat activities in comparison to other machine learning systems. Deep learning ultimately takes the extra step of continuously self-evolving its decision making over time toward a more proactive risk mitigation posture (Alshehri, 2022).
- The most significant drawback of deep learning tools is its sole ability to provide organizational security through observational learning. As a result, if an entity has a minimal amount of data or if the data originates from one specific source that is not representative of the domain population, the deep learning systems will not learn and adapt in a way that is not generalizable to a given security environment. Moreover, biases can be a major concern for deep learning systems if they train on data that have biases as the model will reproduce them in its thinking and decision making (DeBrusk, 2020).
- The computer hardware requirements to run deep learning systems can be a major limitation. Deep learning systems can require advanced multicore high-performing graphics processing units, and large amounts of random access memory (RAM) to function effectively, which are extremely expensive and use large amounts of energy. **Deep learning solutions may be more difficult to initially employ but once properly optimized can generate results instantaneously and will continue to improve an organization's security detection mechanisms over time** (Shi et al., 2020).



UEBA tools represent the most recently developed insider risk mitigation tools, being introduced commercially in 2015. These tools can analyze user behavior (Kaspersky IT Encyclopedia, 2022). They can allow for more efficient threat hunting and response time to potential insider threats.

User and Entity Behavioral Analytics

UEBA




Overview and Development

- User and Entity Behavior Analytics (UEBA) is a technology that gathers insights on network events and user activities which is used to identify potential malicious user behaviors indicating potential insider threats. UEBA solutions focus on user activity rather than pre-determined fixed indicators found in use cases generated after known compromises (Beltrán, Fernández-Isabel & Diego, 2021). These tools can enable proactive risk mitigation of data breaches, sabotage, privilege abuse, and policy violations. UEBA tools are designed to expose stealthy malicious insider threats by establishing baseline user behavior patterns to distinguish what is normal behavior and what could be evidence of anomalous behavior.
- The development and rise in use of UEBA systems were influenced by traditional security tools like firewalls, private encrypted VPNs, gateways and other similar products being no longer able to sufficiently protect an organization against internal (and external) security threats (Slipenchuk & Epishkina, 2019). While it has become easier to bypass security measures like password authentication, mimicking employees' routine behavior once inside a network is more difficult. As a result, threat detection tools such as UEBA have become progressively more important as organizations use them to gather and analyze data to quickly detect threats. With the expanding IoT and additional devices being connected to cloud-based networks, UEBA solutions provide a substantial enhancement to overall IT infrastructure security from insider threats for organizations attempting to managing increasingly complex cyber security vulnerabilities.

Benefits and Drawbacks

- A major benefit of UEBA tools is that it can leverage machine learning and artificial intelligence software that can replace some of the time and effort required by IT analysts who would otherwise be manually performing similar tasks using past insider threat use cases. A UEBA system that has been properly configured can enable an organization to divert IT analyst resources to other high value projects. UEBA solutions can lower the inherent risks of insider threats. UEBA products can be used for threat detection on any device connected to an organization's network. (Martín et al., 2022).
- UEBA tools are not meant to replace early-warning security monitoring systems and are not meant as a standalone cyber security solution (Stolte, 2018). UEBA technology should be utilized to complement an organization's existing security infrastructure and improve an organization's overall security posture by enabling a proactive approach based on gaining insight into users' behaviors. UEBA solutions are often paired with existing security information and event management (SIEM) systems, and form part of a multilayer security defense in-depth solution. A significant drawback is the price and expertise required to purchase and implement a UEBA system (Petters, 2020). **The sophistication of UEBA tools allow for it to effectively adapt to an organization's complex and evolving needs but can be overwhelming and too costly for small to medium-sized businesses to address security threat detection.**



Overall, this project provides a glimpse into the present and near future landscape of technological security tools that can be used to mitigate insider threats.

It is also important to note that this project did not have in scope how the utilization of emerging technologies corresponds to Canadian privacy and security laws. This issue needs to be considered when applying the technologies discussed in this report to an organization's insider risk program.

There is also great potential for the research and findings detailed in this report to be expanded upon in future projects and partnership with Canadian organizations.

Conclusion





A major theme identified throughout this research process is that the landscape of insider risk technology mitigation tools are constantly evolving and has extremely complex nuances that need to be better understood.

It is not realistic to expect technological solutions to completely eliminate the risks posed by insider threats; however, they can sufficiently reduce the probability and negative organizational impacts from insider threats.

As a result, it is essential for academia and organizations to continue prioritizing research into the development of insider risk programs that emphasize the use of technological solutions for insider risk mitigation. It is also important to note that no individual tool can ensure sufficient insider risk mitigation—rather, a combination of different sets of tools based on an organization's unique needs and presently evaluated gaps is highly recommended.

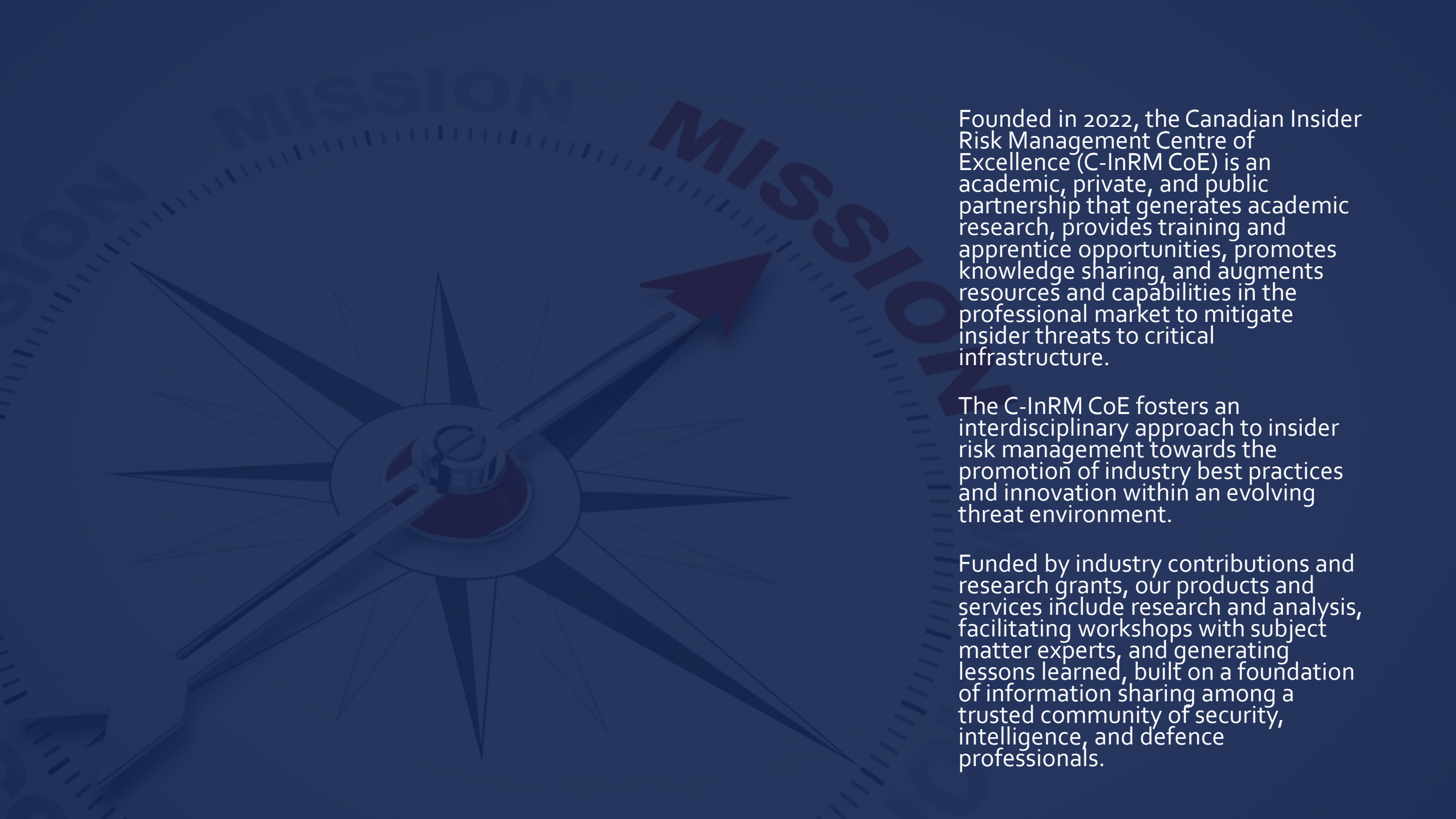
A combination of developing organizational awareness of security needs, emerging technologies and effective cybersecurity hygiene is necessary for an effective insider risk strategy.

Conclusion



References

- Alshehri, A. (2022). Relational Deep Learning Detection with Multi-Sequence Representation for Insider Threats. *International Journal of Advanced Computer Science & Applications*, 13(5).
- Araujo, R. (2022). Advanced Network Traffic Analysis & Why it Matters. *Arista*, 1.
- Awake Security Named in Gartner's First Market Guide for Network Traffic Analysis NTA. (2019). In *Information Technology Newsweekly* (p. 154-). NewsRX LLC.
- Bais, G. (2022). What is Network Traffic Analysis? *Traceable App & API Security*, 1.
- Beltrán, M., Fernández-Isabel, A., & Martín de Diego, I. (2021). An approach to detect user behaviour anomalies within identity federations. *Computers & Security*, 108, 102356.
- Brooks, L. (2020). A Brief History of Data Loss Prevention Solutions. *Tessian*, 1.
- Caldeira. (2021). *Security Information and Event Management (SIEM) Implementation Recommendations to Enhance Network Security*. ProQuest Dissertations Publishing.
- Caldwell, T. (2011). Data loss prevention – not yet a cure. *Computer Fraud & Security*, 2011(9), 5–9.
- CISCO. (2022). What Is Network Traffic Analysis? *Cisco Systems Inc*, 1.
- Corcoran. (2018). *Security Information & Event Management (SIEM)*. ProQuest Dissertations Publishing.
- Effectively Validating Dynamic Database Queries Through Database Activity Monitoring” in Patent Application Approval Process (USPTO 20190354712). (2019). In *Technology Business Journal* (p. 1086). NewsRX LLC.
- DeBrusk, C. (2020). The Risk of Machine-Learning Bias (And How To Prevent It). MIT Sloan Management Review. <https://doi.org/1>.
- Devlekar, & Ramteke, V. (2021). Identity and Access Management: High-level Conceptual Framework. *Revista GEINTEC*, 11(4), 4885–4897.
- Footo, K. (2022). A Brief History of Deep Learning. *Dataversity*, 1.
- Froehlich, A. (2021). The top 7 identity and access management risks. *West Gate Networks*, 1.
- González-Granadillo, González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors (Basel, Switzerland)*, 21(14), 4759.
- Grand View Research. (2021). Network Traffic Analysis Market Size, Share & Trends Analysis Report By Component (Software, Service), By Deployment (On-premise, Cloud), By Organization, By Vertical, By Region, And Segment Forecasts, 2021 - 2028. *GVR-4-68038-305-8*, 1–140.
- Grushka-Cohen, H., Biller, O., Sofer, O., Rokach, L., Shapira, B. (2020). Using Bandits for Effective Database Activity Monitoring. *Lecture Notes in Computer Science*(), vol 12085. *Springer, Cham*.
- Haber, & Rolls, D. (2020). *Identity Attack Vectors Implementing an Effective Identity and Access Management Solution* (1st ed. 2020.). Apress.
- Hart, Manadhata, P., & Johnson, R. (2011). Text Classification for Data Loss Prevention. In *Privacy Enhancing Technologies* (pp. 18–37). Springer Berlin Heidelberg.
- Hyder, Waseemullah, , Farooq, M. U., Ahmed, U., & Raza, W. (2021). Towards Enhancing the Endpoint Security using Moving Target Defense (Shuffle-based Approach) in Software Defined Networking. *Engineering, Technology & Applied Science Research*, 11(4), 7483–7488.
- Indu, Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, 21(4), 574–588.
- Kaspersky IT Encyclopedia. (2022). UEBA (User and Entity Behavior Analytics). *Kaspersky IT Encyclopedia*, 1.
- Logsign. (2018). Evolution of SIEM Over the Years. *Logsign*, 1.
- Kaur, & Tiwari, R. (2021). Endpoint detection and response using machine learning. *Journal of Physics. Conference Series*, 2062(1), 12013.
- Kim, S., Cho, N. W., Lee, Y. J., Kang, S.-H., Kim, T., Hwang, H., & Mun, D. (2013). Application of density-based outlier detection to database activity monitoring. *Information Systems Frontiers*, 15(1), 55–65.
- Lynch, B. (2022). Data Loss Prevention (DLP). *Imperva*, 1.
- Machado de Sousa, & Shahzad, A. (2021). Data Loss Prevention from a Malicious Insider. *The Journal of Computer Information Systems, ahead-of-print*(ahead-of-print), 1–11.
- Martin de Diego, I., Fernández-Isabel, A., Beltrán, M., & Fernández, R. R. (2022). Combining user behavioural information at the feature level to enhance continuous authentication systems. *Knowledge-Based Systems*, 244, 1.
- Miao, Y., Ruan, Z., Pan, L., Zhang, J., & Xiang, Y. (2018). Comprehensive analysis of network traffic data. *Concurrency and Computation: Practice and Experience*, 30(5).
- Mogull, R. (2020). Understanding and Selecting a Database Activity Monitoring Solution- Whitepaper. *SANS Institute*, 1–23.
- Nasir, Afzal, M., Latif, R., & Iqbal, W. (2021). Behavioral Based Insider Threat Detection Using Deep Learning. *IEEE Access*, 9, 143266–143274.
- National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *United States Government*, 1, 1–55.
- NitroSecurity Evaluated in Leading Analyst Firm's Database Activity Monitoring Market Overview. (2009). In *Information Technology Newsweekly* (p. 149-). NewsRX LLC.
- Obbayi, L. (2018). The Evolution of Endpoint Security – Changing with the Currents. *InfoSec Institute*, 1.
- Oevering. (2020). *Endpoint Security in Higher Education*. ProQuest Dissertations Publishing.
- Patent Issued for Data loss prevention techniques (USPTO 11323479). (2022). In *Technology Business Journal* (p. 2296). NewsRX LLC.
- Petters, J. (2020). What is UEBA? Complete Guide to User and Entity Behavior Analytics. *Varonis*, 1.
- Radoglou-Grammatikis, Sarigiannidis, P., Iturbe, E., Rios, E., Martínez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulis, A., Angelopoulos, M., & Ramos, F. (2021). SPEAR SIEM: A Security Information and Event Management system for the Smart Grid. *Computer Networks*, 193, 108008.
- Schrimpf, Drechsler, A., & Dagianis, K. (2021). Assessing Identity and Access Management Process Maturity: First Insights from the German Financial Sector. *Information Systems Management*, 38(2), 94–115.
- Shahraki, Taherkordi, A., & Haugen, Ø. (2021). TONTA: Trend-based Online Network Traffic Analysis in ad-hoc IoT networks. *Computer Networks*, 194, 108125.
- Slipenchuk, & Epishkina, A. (2019). Practical User and Entity Behavior Analytics Methods for Fraud Detection Systems in Online Banking: A Survey. In *Biologically Inspired Cognitive Architectures 2019* (pp. 83–93). Springer International Publishing.
- Stolte, R. (2018). The missing act for user and entity behavior analytics. *CSO (Online)*.
- Symphony Technology Group. (2022). What Is Endpoint Detection and Response (EDR)? *Trellix*, 1.
- Tedeschi, Emmanouilidis, C., Mehnen, J., & Roy, R. (2019). A Design Approach to IoT Endpoint Security for Production Machinery Monitoring. *Sensors (Basel, Switzerland)*, 19(10), 2355
- Tian, Shi, W., Tan, Z., Qiu, J., Sun, Y., Jiang, F., & Liu, Y. (2020). Deep Learning and Dempster-Shafer Theory Based Insider Threat Detection. *Mobile Networks and Applications*.
- Villanueva, M. (2021). Pros and Cons of Implementing SIEM. *Intelligent Technical Solutions*, 1.
- Williams. (2009). Eduserv Symposium 2009: Evolution or Revolution: The Future of Identity and Access Management for Research. *Ariadne (Bath, England)*, 60.
- Yuan, & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security*, 104, 102221.



Founded in 2022, the Canadian Insider Risk Management Centre of Excellence (C-InRM CoE) is an academic, private, and public partnership that generates academic research, provides training and apprentice opportunities, promotes knowledge sharing, and augments resources and capabilities in the professional market to mitigate insider threats to critical infrastructure.

The C-InRM CoE fosters an interdisciplinary approach to insider risk management towards the promotion of industry best practices and innovation within an evolving threat environment.

Funded by industry contributions and research grants, our products and services include research and analysis, facilitating workshops with subject matter experts, and generating lessons learned, built on a foundation of information sharing among a trusted community of security, intelligence, and defence professionals.