WHITE PAPER

COGILITY

Migrating to Whole Person Insider Threat Management:

Quick Primer on Trends, Technology Considerations, and Whole Person Risk Assessment

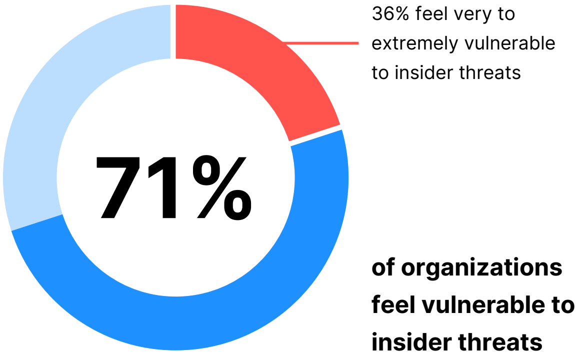
Introduction

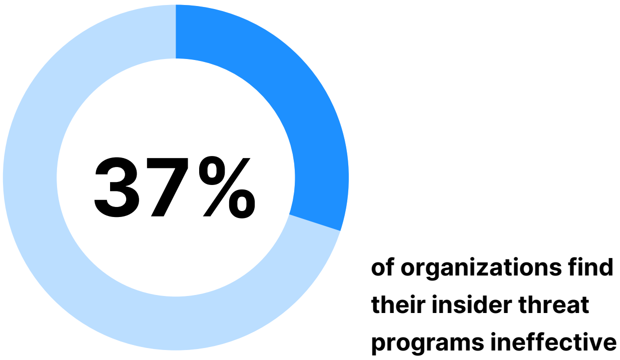
Insider threat management remains a top priority for both government and commercial sectors, especially as insider incidents increase and attract more attention. Insider threats refer to harmful actions by trusted individuals who have access to an organization's resources — ranging from sensitive data theft and data exfiltration to sabotage, espionage, fraud, and workplace violence. To address this growing concern, many organizations are enhancing their insider risk management programs by investing in new resources and technologies.

Derived from a companion webinar on the subject, this paper explores the current landscape of insider threat management. It shares industry survey insights on how organizations perceive their risks and the effectiveness of current defenses. Leveraging industry analyst insights, it examines key functionality, differentiators, and technologies that are progressing insider risk solutions. This paper also explores the advantages of whole person insider threat management to enable predictive risk assessment and proactive mitigation. Lastly, it provides expert advice towards how an organization can move to a "whole person" approach for Counter-Insider Threat (C-InT) management.

Insider Threat Landscape and Perceptions

A recent Insider Threat survey from Cybersecurity Insiders[1] of over 400 cybersecurity professions reveals insight into the current state of insider threat management as insider incidents are on the rise with many gaining public attention and countless others remaining undisclosed. According to the survey findings, 71% of organizations feel vulnerable to insider threats with a third feeling significantly at risk. Over a third of survey respondents admitted their organization's efforts are only nominally effective, showing significant room for improvement in both processes and solutions to address this cyber risk. The survey findings focus on the scope of utilizing technical security controls across identity, physical, endpoint, network, cloud and content sources to address insider threats.





[1] 2024 Insider Threat survey by Cybersecurity Insiders n=413

A whole person approach to insider threat management would extend beyond monitoring known technical security violations and user activity anomalies. The survey indicates that approximately half of organizations are also incorporating behavioral data sources, such as legal data, human resources data and social media data, into their insider threat programs. By analyzing both technical and behavioral sources, organizations can identify personnel on the path to critical insider risk[2] — allowing for preemptive action. As explored later in this paper; by integrating behavioral data sources and advanced modeling techniques, organizations can identify potential insider even before an impactful incident occurs.

Insider Threat Considerations

Thwarting insider threats is challenging. Insiders have legitimate access to sensitive data and have elevated access privileges. They have the potential to inflict severe damage before being detected and mitigated. Data privacy concerns and regulations can impede insider threat monitoring and response. In most cases, mitigation requires substantive, documented evidence to take actions such as termination and law enforcement. Given the above obstacles, security and human resource (HR) professionals need to consult with legal counsel. As such, Insider threat management programs require executive support and legal guidance in addition to establishing requisite policies, procedures, and resources. Once said requisites are in place, security tools and insider threat solutions provide the means to invoke controls, monitor threats, and facilitate action.

Challenges

- Insiders have legitimate access to sensitive data and have elevated access privileges
- Insiders have the potential to inflict severe damage before being detected and mitigated
- Data privacy concerns and legislation can impede monitoring and mitigation
- Requires substantive evidence to take actions (termination, law enforcement...)

The majority of C-InT Management solutions seek to detect insider threats by assimilating security data that identify security issues such as access and policy violations, data leakage issues, anomalous user behavior, and malicious actions. As such, insider threat detection often relies on monitoring physical, identity, endpoint, and network security controls, including communications and user activity. Insider threat solutions can correlate a broad array of security data including access attempts, downloads, file transfers, application usage and more. Modern SIEM and IAM tools are often employed to gain user and entity behavior analytics (UEBA) insight. Many organizations are beginning to incorporate publicly available information (PAI) that can trigger or fortify finding insider risks. As earlier mentioned, the application of such insider threat monitoring, without consistent policies and procedures and sans obtaining legal advice, can yield privacy and other regulatory exposures.

[2] Shaw, E. & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. Studies in Intelligence, 59 (2), 41-48

According to a recent Insider Risk Management market report by QKS-Group[3], key functionality among C-InT solutions include: user and device monitoring, EUBA, extended detection and response (XDR), security response automation, audit and reporting, analytics and dashboarding. UEBA capabilities helps analyze users, systems, apps, and suspicious activities to detect unusual behavior. They can highlight potential insider risk events, such as privilege abuse, unauthorized file access, interaction with and sharing of sensitive information, or application misuse. Analytics and dashboarding capabilities help organizations monitor users, document issues, and response to incidents. It also can facilitate risk assessment and response coordination, as well as can provide performance insights into your insider threat program.

Risk response capabilities encompass manual, semi-automated and automated means to respond to threats in real-time. Depending on the type of threat, automated responses can trigger security tools to lock accounts, block devices, block communications, and quarantine files. This can enhance the productivity and efficiency of the security team — this approach is typically reacting to security violations and anomalies. AI (artificial intelligence) and ML (machine learning) are being applied to analyze more data and data types, not only to reduce repeat alert noise, but equally to identify anomalies — deviations from policies, as well as from user norms and group norms that potentially indicate insider risks.

Solutions

- Seek to detect data leakage, fraud, disgruntled user behavior, and deviations
  - Detection is thus after the fact, reactive
- Monitor endpoint and network technical controls, communications, and user activity
  - Use an array of security data: access attempts, downloads, file transfers, and app usage
- Incorporate other publicly available data sources including HR, law, financial, and social media

The same QKS-Group report highlighted functionality and differentiators among leading C-InT solutions assessed by QKS-Group in their market analysis. Key differentiators to consider include scalability and flexibility; integration and interoperability; risk modeling and scoring; multi-layered analytics; user profiling; and whole person insider threat management. According to QKS-Group, organizations should evaluate their needs with regarding scalability, flexibility, integration and interoperability requirements. Organizations should consider the extent of data that can be collected and processed across channels in a way that avoids performance setbacks — and how that data will be utilized and managed. Beyond technical indicators such as endpoint, network, cloud and application event data, data sources may include behavioral indicators. Another key factor is the means to be able to obtain the data sources across their organization, infrastructure and applications. Once confirmed, organizations can assess how the insider threat solution will consume and process the data and how the output of that information will be used

[3] 2024 QKS-Group SPARK Matrix™: Insider Risk Management

by the organization. Further integration may also require interoperability with other IT management applications such as content management and service management systems.

According to QKS-Group, when it comes to risk modeling and scoring — here too, insider risk management tools should allow the organization to define and tune rules to identify threats that align to the organization's policies. Additionally, organizations can also leverage identity-centric risk modeling to correlate information generated from user behavioral patterns to gain deeper insights for investigations across the threat landscape. Multilayered analytics enables organizations to detect insider security scenarios, such as fraud, by leveraging a preconfigured set of rules. The ease at which to author and manage models is crucial. The more flexible, comprehensive and intuitive the modeling, the better the insider threat solution can adapt to evolving policies and new controls.

Advancements in AI and Predictive Analytics

The QKS-Group research identified key insider risk management technology trends, which included the use of artificial intelligence; machine learning; sentiment analysis; real-time processing; predictive analytics; workflow automation, and whole person insider threat management. Real-time processing is important given the types and scale of data to analyze. This incorporates technologies that allow for high-speed processing of massive volumes of data streams to determine actionable insider risk insights, including means to analyze concurrently across multiple sources and diverse data types.

According to the QKS-Group, by applying AI and machine learning, C-InT systems can detect patterns and anomalies more effectively, filtering out redundant alerts and false positives to identify insider actions with greater precision — albeit still reactionary. However, AI approaches are often black-box in that they identify active insider threats, but have gaps in explainability. Given limited training data, their ability to predict insiders can be prone to hallucination and bias. These gaps are significant considering the high-consequence decision affecting a person's livelihood and reputation.

Predictive analytics offers the means to model risk indicators and behavioral analytic logic to identify explicit threats and persons who are on the path to commit an insider threat. Organizations want more capabilities beyond receiving insider threat notifications. Workflow automation streamlines alerts, investigation analysis, documentation, and response tasks to coordinate detection and mitigation of insider threats. This enhances the productivity and efficiency of the security and insider threat response teams. There are a wide variety of technical indicators which can be monitored. However, solely using security data sources for detection often results in a more reactive insider risk management stance, as typically the impactful event has already occurred.

The Whole Person Approach: A Game Changer

Whole person insider threat management aims to collect and process behavioral data, as well as technical data, to analyze, detect and predict insider threats. As described earlier, behavioral data can be comprised of personnel vetting and performance assessment information from H.R. as well as publicly available law enforcement, financial, and social media information. This data can afford organization's a more holistic, proactive approach to insider threat management. The most compelling argument for whole person insider threat management is to get left of harm, since insiders typically exert multiple actions that lead to an impactful incident. Explained by Frank L Greitzer Ph.D.[4], chief behavioral scientist as Cogility — "traditional approaches focusing only on technical indicators will most often alert security analysts and threat responders only during or after the attack. But if organizations incorporate behavioral factors into their analysis, analysts may observe various trip wires or red flags along the critical pathway." [See Figure 1]

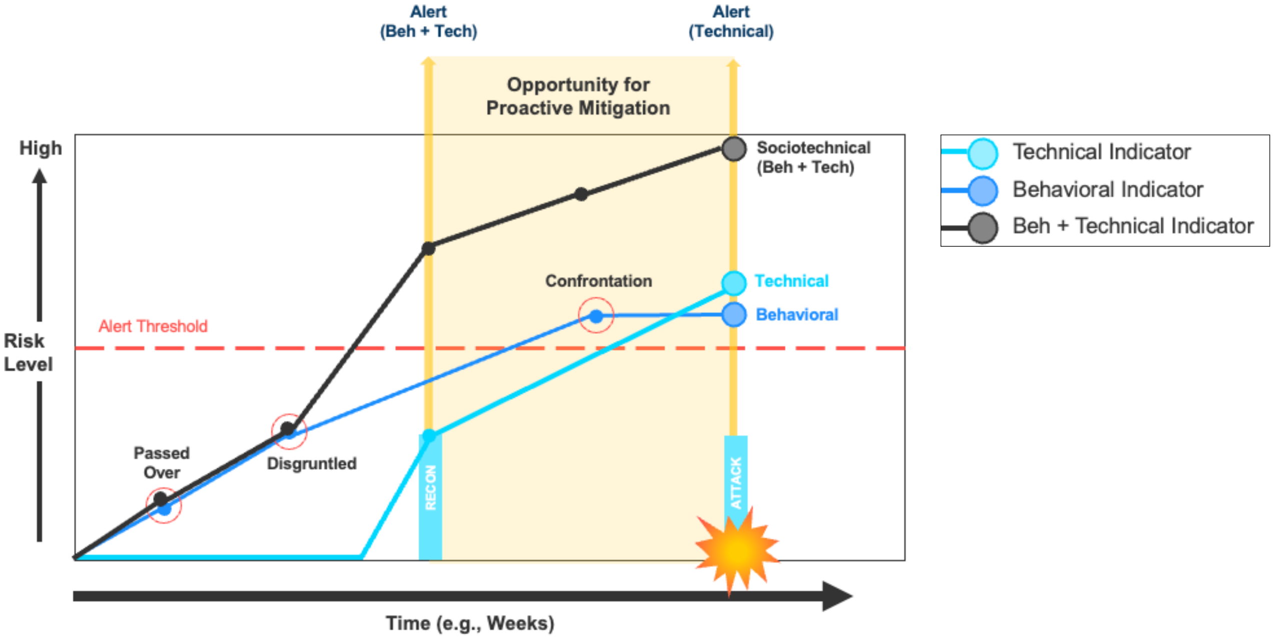


Figure 1: Whole Person C-InT advantage to get left of harm

The concept of whole person insider risk assessment as a best practice is not a new concept. Unfortunately, whole person insider risk management it is not in the mainstream of counter-insider threat programs except in more progressive commercial and government institutions. There are several reasons why programs are hesitant. Two prevailing reasons are behavioral data acquisition and management. It can be difficult to obtain behavioral data sources and there are privacy restrictions and obligations when managing this information. Technical security sources are more readily available and often already managed — and analyzed within simpler detection models. So how can organizations transition to a whole person approach to move from reactive to proactive.

[4] Adapted from: Greitzer et al. (2018). https://ieeexplore.ieee.org/document/8424651

Frank L Greitzer shares a top 10 best practices to migrate to a whole person insider threat management program:

1. Expand the breadth of stakeholders beyond insider threat security staff to include representatives from human resources, legal, behavioral experts/scientists, and employee. This provides a cross-functional team to better define C-InT risks, models, requisites, implementation needs, PKIs and program enhancements.[5]

2. Define key insider risks that are of concern to the organization and insider threat assessment processes. Define not only the most egregious violations, but also concerning events, behaviors, and characteristics that help to identify at-risk individuals, preempt impactful incidents, and provide an "offramp" from critical pathway to insider risk.

3. Identify the technical and behavioral potential risk indicators (PRIs) that could identify people who pose the greatest insider threat risks. This can process can be augmented by leveraging existing PRI taxonomies such as SOFIT — Socio-technical and Organizational Factors for Insider Threats.[6]

4. Create insider risk assessment models by mapping the sets of PRIs and possible weights (rating scales) of the respective PRIs associated with a specific insider threat behavior. Calibrate the assessment model by applying feedback from internal and expert insider threat analysts.

5. Assess and document the sources of technical and behavior data within the organization to identify owners, acquisition methods, frequency and volume, usage limitations, and protection obligations, as well as approval processes. Determine the scope, acceptable risks, and gaps to securely obtain and manage these data sources and maintain compliance.

6. Develop monitoring specifications, assessment templates, and response guidance to establish requirements and processes. Identify gaps by comparing current supporting resources, processes, and technologies.

7. Assess current insider threat program costs across staff and resources, which often are a portion of a security-centered threat detection and response team. Document the number of insider threats identified, investigated, technically resolved, and those requiring more extensive investigation, mitigation and intervention effort. Ideal to estimate any quantitative measures.

[5] Intelligence and National Security Alliance (INSA), Human Resources and Insider Threat Mitigation: A Powerful Pairing, September 2020 - INSA White Paper

[6] SOFIT; Greitzer, Pearl, Leuong, and Becker. https://ieeexplore.ieee.org/document/8424651

8. Ascertain key implementation requirements, costs, operational tradeoffs, and integration must-haves to augment existing tools, controls, and capabilities. Examine the capabilities and costs of new tools and technologies, including the use of expert systems and AI/ML for real-time threat detection and analysis, as well as case management functions that affect analyst workloads from assessment to mitigation.

9. Determine the operational, economic, and risk management improvements by augmenting the current C-InT program (underlying resources, processes, and technology) with a whole person approach. Estimate implementation scope, timing, and KPI targets.

10. Document and present key highlights and KPIs to gain stakeholder commitment and move to actionalize plans.

Modernizing Insider Threat Management

As organizations face increasing insider threats, the integration of continuous behavioral monitoring, AI-augmentation, predictive modeling, and case management will be essential to meet the processing, assessment, and mitigation needs of modern C-InT programs.

A whole person insider threat management approach helps organizations move from reactive detection to proactive risk assessment to better protect assets and personnel, manage risk, and foster a secure workplace. Now is the time to modernize your program and adopt a forward-thinking, whole person approach to counter-insider threats.

Cogility Counter-Insider Threat

Cogility Counter-Insider Threat (C-InT) empowers organizations to take a whole person approach to detect, prevent, and mitigate insider threats. Cogility continuously monitors and analyzes both technical and behavioral potential risk indicators (PRIs) at machine-speed to identify insider threats with full explainability. Cogility C-InT, powered by its patented Hierarchical Complex Event Processing, leverages a foundational insider risk model informed by SOFIT. Combined with its cloud-scalable behavioral analytics and integrated case management features, Cogility C-Int modernizes insider threat management programs to help organizations more efficiently and effectively respond to and avoid impactful incidents. For more information, visit www.cogility.com/insiderthreat/.

COGILITY

Visit **www.cogility.com/counter-insider-threat** to obtain more information and request an expert demo.

Cogility
15495 Sand Canyon Ave. #150
Irvine, CA. 92618

sales@cogility.com
+1 949.398.0015

01/25