WHITE PAPER

COGILITY

Cogynt Behavioral Analytic Platform ROI Projection

By Frank L. Greitzer, PhD

Chief Behavioral Scientist

Executive Summary

This paper develops a business case for Cogynt™, a high-fidelity/high-automation Behavioral Analytic Platform, contrasting it with traditional, low-fidelity/low-automation approaches for Insider Risk Management (IRM). The analysis focuses on projecting the Return on Investment (ROI) and risk reduction benefits to inform prospective adopters of this technology.

Background

Insider threat is a persistent and growing risk, evidenced by high-profile cases and industry statistics. A 2024 Insider Threat Report found that a staggering 83% of organizations experienced at least one insider incident in 2024, and the average annual cost of dealing with insider risk has risen to over $17 million USD.

Organizations are advised to adopt mature IRM programs with risk modeling approaches that incorporate behavioral data in addition to technical risk indicators such as User Activity Monitoring (UAM) of cybersecurity data. This more advanced Whole-Person approach seeks to proactively identify at-risk individuals before they cause harm. Behavioral data sources include financial credit bureaus, law enforcement, counterintelligence, personnel security, and human resources. This requires continuous monitoring and assessment. A major challenge is the sheer volume of alerts and the time it takes to manage them. Cogility's Cogynt decision intelligence platform supports this critical Whole-Person requirement.

The number of UAM alerts alone can exceed thousands per day, leading to 40% or more of all alerts going uninvestigated. Furthermore, it takes an average of 81 days to detect and contain an insider threat incident, allowing threats to linger and cause significant damage.

These challenges underscore the need for effective automated decision support tools. Cogynt — a behavioral analytic decision intelligence platform designed to improve the accuracy and efficiency of IRM programs — offers distinct advantages through:

- **Continuous risk assessment** that explicitly models the expert decision process
- **Integrated AI capabilities** with its patented HCEP (Hierarchical Complex Event Processing) expert AI behavioral analytic and generative AI/LLM support to enhance analyst understanding
- **Explainability** supported by causal event analysis for full traceability
- **Scalability** to support high data volumes and concurrent users
- **Configurability** that accommodates a wide range of intelligence and decision support missions with diverse data requirements
- **Digital Twin** functionality to maintain history and integrate asynchronous data over long periods

Summary of Findings

The benefits of Cogynt are characterized by its impact on the timing and quality of actionable intelligence, its proactive risk assessment capabilities, and its ability to reduce risk. While precise quantitative ROI calculations require proprietary or sensitive data that are only available to the organization of concern, it is possible to make general comparisons and projections for a hypothetical organization by adopting conservative estimates and assumptions.

We estimated resource requirements by examining the following major risk categories for a hypothetical organization with 100,000 personnel: UAM/IT risks, mental illness,disgruntlement/disengagement, and financial stress. For these general risk types, we used open source population statistics to estimate the frequency of insider risk indicator alerts. For the unaided Low-Fidelity/Low-Automation use case, there are an estimated 60,893 alerts per month that require a total of 274 Full-Time-Equivalent (FTE) resource requirements. In contrast, the Cogynt High-Fidelity/High-Automation solution provides triage and case management support that “shrinks the haystack” to below 3,500 indicator alerts per month, significantly reducing the analysis workload to 11 FTE: yielding a 26:1 benefit in analyst resources.

The associated cost advantage is most compelling. For an organization with 100,000 personnel, the cost comparison is:

- **Low-Fidelity/Low-Automation System (Staff Cost Alone):** $45.7M.
- **High-Fidelity/High-Automation System (Staff + System Cost):** $4.62M.

This yields an overall annual cost/benefit ratio of 11:1 in favor of the Cogynt solution.

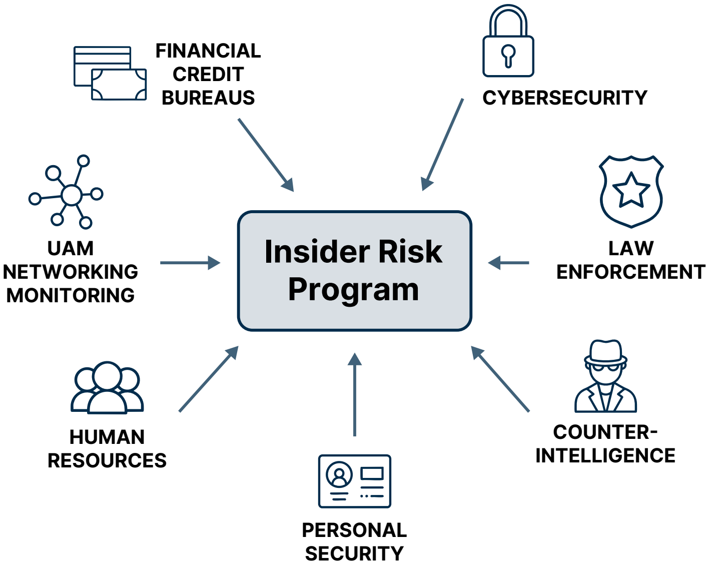
Conclusion

Deployment of a behavioral analytic platform like Cogynt is mission-critical and cost-effective for modern Insider Risk Management. The quantitative analysis, using conservative estimates, compellingly demonstrates that the Cogynt High-Fidelity/High-Automation solution yields substantial advantages over traditional programs. The platform achieves dramatic improvements with an overall cost reduction of 11:1 for an organization with 100,000 personnel by enabling continuous coverage while significantly reducing risk and FTE requirements. Beyond these quantifiable metrics, the advanced behavioral analytic platform provides substantial intangible benefits that are critical to mission success, including enhanced insight and proactive opportunities for incidence avoidance: If deploying the more effective Cogynt solution leads to the avoidance of a single insider incident per year that the baseline solution would miss, the resulting cost avoidance would largely justify the investment.

1. Introduction

Insider Threat is a persistent and growing risk. Over the past 10 years, there have been several high-profile cases such as Edward Snowden, Chelsea Manning and Nidal Malik Hasan[1] that caused great harm to the US government and national security at-large. More generally, industry surveys such as the *2024 Insider Threat Report* by Cybersecurity Insiders found that a staggering 83% of organizations experienced at least one insider incident in 2024, and nearly half of the organizations polled reported that insider attacks had become more frequent in the past year.[2] The Poneman *Insider Risk Global Report*[3] notes that the average annual cost of dealing with insider risk has risen to over $17M USD. Most assessments of insider risk stress the importance of the human element: For example, the 2024 Verizon Data Breach Investigations Report found that more than two-thirds of all data breaches reflect misuse/abuse of privilege, social engineering compromises, and human errors.[4] Thus, it is imperative that organizations planning to set up or improve existing Insider Risk Management (IRM) programs incorporate behavioral factors as well as more traditional technical risk indicators into their risk assessment processes.[5] While the likelihood of any one individual at any given time being a high security risk is quite small, the security and financial consequences of just a single serious incident can be enormous. Therefore, the challenge is to proactively identify those individuals who exhibit behavioral risk factors in their personal or professional lives that pose a potential risk to the organization.

Organizations are advised to adopt mature Insider Risk Management programs with risk modeling approaches that incorporate behavioral data in addition technical risk indicators such as User Activity Monitoring (UAM) of cybersecurity data. This more advanced Whole-Person approach seeks to proactively identify at-risk individuals before they cause harm. This Whole-Person approach uses social, behavioral and technological indicators to identify problematic employees *before they*



[1] *CCDCOE NATO Cooperative Cyber Defence Centre of Excellence Tallinn Estonia; Insider Threat Detection Study*

[2] Cybersecurity Insiders. (2024). *2024 Insider Threat Report: Trends, challenges, and solutions.* https://go1.gurucul.com/2024-insider-threat-report

[3] Poneman Institute. 2025. *Cost of Insider Risks Global Report 2025*. Poneman / DTEX. https://www2.dtexsystems.com/l/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf

[4] Verizon. 2024. 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/Tb2/infographics/2024-dbir-finance-snapshot.pdf

[5] F.L. Greitzer, J. Purl, Y. M. Leong, and P. J. Sticha. 2019. Positioning your organization to respond to insider threats. IEEE Engineering Management Review, 47(2), 75-83. https://ieeexplore.ieee.org/document/8704879

do something harmful.[6, 7] Behavioral data sources include financial credit bureaus, law enforcement, counterintelligence, personnel security, and human.

This requires continuous monitoring and assessment. A major challenge is the sheer volume of alerts and the time it takes to manage them. Cogility's Cogynt decision intelligence platform supports this critical Whole-Person requirement. This proactive approach is also essential to help the IRM team identify unknown insider risks, which, by definition, may lack a pre-identified threat vector or target but where identification of relevant PRIs can still inform appropriate mitigation strategies.

The above cases and statistics underscore the urgent need for enhancing IRM programs throughout the US government and across all business sectors. As stipulated in *Executive Order 13587*, all US government agencies and departments — and especially those that deal with classified information such as the DoD — are required to continuously monitor, identify and mitigate insider threat risks. Within the DoD, all DoD components have set up IRM Hubs whose responsibilities are to implement the associated DoD IRM policies, including DoD Instruction *5205.83, DoD Insider Threat Management Analysis Center, 30 March 2017*. Typically, IRM Hubs address five functional categories as shown in Figure 1.

Network Audit	Information Sharing	Security	Training/Awareness	Insider Threat Reporting/ Response
Establish a capability to monitor & audit users across all domains	*Facilitate the sharing of CI, Security, cyber, LE, HR, and other related information (medical)*	*Evaluate security controls in place to protect assets (information, people, equipment)*	*Provide workforce with training on insider threat awareness & reporting responsibilities*	*Establish an integrated reporting and response capability*

Figure 1. Typical IRM Hub Focus Areas

Critical to insider threat analysis and risk reduction is detecting, avoiding or mitigating a threat by tracking risk indicators over a period of time. Gartner[8] states that over 70% of the breaches that begin with an abuse of access are not found for months or years for medium size enterprises. For large enterprises, this is an even greater challenge. Figure 2 provides a timeline graphic that depicts both technical and non-technical risk indicators that, over time, can lead to incidents.

[6] D. Cappelli, A. Moore and R. Trzeciak. 2012. *The CERT Guide to Insider Threats*. New York: Addison-Wesley.

[7] F. L. Greitzer. 2019. Insider Threat: It's the HUMAN, Stupid! In *Proceedings of the Northwest Cybersecurity Symposium*, April 8-10, 2019. Article No. 4, pgs 1-8. ACM ISBN 978-1-4503-6614-4/19/04. https://doi.org/10.1145/3332448.3332458

[8] *Strategies for Midsize Enterprises to Mitigate the Insider Threat; 17 January 2020, Paul Furtado, Gartner Sr. Director Analyst.*

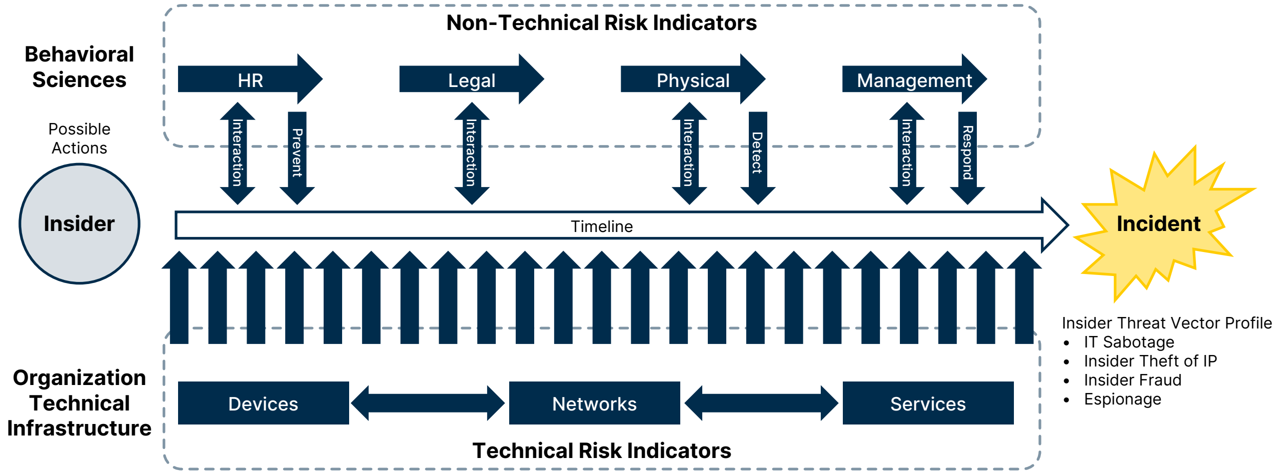


Figure 2. Insider Threat Timeline (Ref: Insider Threat Detection Study)[9]

Monitoring, tracking and assessing risk of even a modest number of potential insider threat cases is an exceedingly difficult job that requires broad expertise and collaboration across multiple perspectives including cybersecurity, security, human behavioral/psychological, legal, etc. Performing this cognitively demanding risk assessment task consistently and effectively is a challenge for any organization, but the demands are multiplied manyfold for very large organizations whose IRM Hub may be overwhelmed with the task of tracking risk indicators of hundreds of individuals to determine if they fit various Insider Threat profiles.

The sheer number of insider incidents can overwhelm a security team. Indeed, the 2024 Cybersecurity Insiders survey[10] found that 38% of security professionals indicate that they lack effective means of detecting insider attacks, which means that a large number of incidents may go completely unnoticed. Further, the Poneman *Insider Risk Global Report* indicates that it takes an average of 81 days to detect and contain an insider threat incident, and only 12% are contained within 31 days.[11] Thus, threats can linger and cause damage long before they are properly assessed, if indeed they are ever identified.

These statistics show that all organizations, regardless of their size, require effective automated decision support tools to improve the efficiency and effectiveness of their insider risk programs. Cogynt is a behavioral analytic decision intelligence platform that can detect patterns of behavioral risk indicators that evolve over time and generate alerts to notify analysts when a case merits further analysis. New data sources can be easily integrated into Cogynt as they become available, using off the shelf connectors

[9] *CCDCOE NATO Cooperative Cyber Defence Centre of Excellence Tallinn Estonia; Insider Threat Detection Study*

[10] Cybersecurity Insiders. (2024). *2024 Insider Threat Report: Trends, challenges, and solutions*. https://go1.gurucul.com/2024-insider-threat-report

[11] Poneman Institute. 2025. *Cost of Insider Risks Global Report 2025*. Poneman / DTEX. https://www2.dtexsystems.com/l/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf

Cogynt uniquely ingests all of the required data sources to conduct a proper Whole-Person IRM analysis of the entire employee-base

including Apache Kafka, which is an open source streaming storage solution that provides specialized connectors for most data sources. Cogynt also offers a declarative zero-coding authoring environment that uses graphical notation and can be easily learned by analysts with no programming background. Further, Cogynt provides advanced workflow features and visualizations, allowing analysts to examine behavioral patterns from the lowest to highest levels of detail. These features in combination enable analysts to be more effective in their analysis, freeing them from more repetitive, mechanical tasks and allowing them to spend more time doing what they do best — critical thinking.

The purpose of this paper is to develop a general business case for Cogynt's high-fidelity/high-automation solution that contrasts with traditional low-fidelity/low-automation programs. We shall provide a general overview of program benefits and apply rules of thumb on Return on Investment (ROI) to help prospective adopters of this technology assess possible benefits.

2. Insider Risk Population Statistics

The process starts with people and data. Everyone within the organization creates a personalized digital signature simply by doing what she or he normally does every day. For example, most individuals use an electronic ID card to enter a building, log into a computer, check email, write and send emails with attachments, access websites (both government and non-government), download files, and many other routine activities related to the performance of their daily functions. Much is of this information is available. User Activity Monitoring (UAM) is one of the largest data sources; other types of available data include financial credit bureaus, cybersecurity, law enforcement, counterintelligence, personnel security, and human resources. Cogynt uniquely ingests all of the required data sources to conduct a proper Whole-Person IRM analysis of the entire employee-base. The following analysis, summarized in Table 1, provides rough estimates of the processing demands for a typical IRM Hub in an organization with 100,000 personnel. As shown, the estimated number of reported "stress events" of concern per month for this size of an organization is 60,893.

Concerning behaviors that may be represented in these cases might be manifested in maladaptive actions (e.g., substandard work performance) or any of a varied collection of insider threat incidents such as data exfiltration, fraud, sabotage, espionage, workplace violence, or suicidal ideation.

Table 1. Estimated Baseline Non-Automated FTE Risk Assessment Requirements Based on 100,000 Personnel

Risk Category	Percentage of Occurrence	Average Number Per Year	Average Per Month	Stress Events	Risk Population Events/Month
UAM/IT Risks	10% per day	3,600,000	300,000	20%	60,000
Mental Illness	5.6% per year	5,600	467	20%	93
Disgruntlement	18% per year	18,000	1,500	10%	150
Financial Stress	78%	78,000	6,500	10%	650
				TOTAL	**60,893**

UAM Statistics

The volume of UAM alerts handled by Security Operations Center (SOC) teams is highly variable and depends on the size and nature of the organization. The number of alerts generally exceeds thousands per day. Further, surveys indicate that 40-50% or more of these alerts go uninvestigated: A survey of nearly 300 security leaders by Prophet Security, published in 2025 and cited by *SecurityInfoWatch*[12], found that, on the average, organizations handle 960 alerts per day and enterprises with over 20,000 employees receive an average of 3,181 security alerts per day. With this high volume, they report that nearly 40% of these alerts go uninvestigated. Similarly, an IBM survey[13] found that only 49% of alerts are investigated in a typical workday, leaving more than half uninvestigated. A Forrester report published in 2020, reported by IONIX,[14] states that security teams face an average of 11,000 alerts per day. On a per capita basis, these figures yield a wide range of estimates for the percentage of daily alerts occurring per employee count, ranging from as low as 5% to 100% or more. We shall assume a conservative figure of 10% in our calculations: In other words, for a large company with 100,000 staff members (accounts), there would be 10,000 UAM alerts per day or 300,000 per month. Not all of these alerts are actionable for an IRM analyst: Indeed, an IBM survey observed that, on average, SOC team members spend one-third (32%) of their typical workday investigating and validating incidents that are not real threats.[13] We shall make a conservative assumption that 20% will be relevant "stress alerts" for insider risk assessment, which yields a queue of 60,000 UAM alerts to be examined. In the Baseline non-automated use case, this will still create a huge, unanswerable demand produced by the large number of UAM alerts that must be examined by analysts.

[12] R. Bosch. Prophet security report highlights urgent need for AI in SOCs. *SecurityInfoWatch.com*, Sept 10, 2025. https://www.securityinfowatch.com/ai/article/55315748/prophet-security-report-highlights-urgent-need-for-ai-in-socs

[13] IBM. Global Security Operations Center Study Results. March 2023. https://www.ibm.com/downloads/documents/us-en/10c31775a05401a5

[14] O. Shushan. Security alert overload: Causes, costs, & solutions. *IONIX blog*, November 3, 2024. https://www.ionix.io/blog/security-alert-overload-causes-costs-solutions/

Mental Illness Statistics

The National Alliance on Mental Illness posts annual prevalence of mental illness figures for U.S. adults.[15] For 2024, this reflects a total of 23.4% of U.S. adults experiencing mental illness. Combined figures for schizophrenia, borderline personality disorder, and major depressive disorder produces a total percentage of about 17.9%. Perhaps most importantly, in 2024 a total of 5.6% of U.S. adults experienced serious mental illness that severely disrupts daily functioning; similar results apply in 2025.[16]

For an organization with 100,000 personnel, we expect 5.6% or 5,600 staff members to have serious mental illness issues in any given year, which averages 467 individuals per month. Assuming that 20% of these individuals will present behaviors of some concern to the organization, this yields an average of 93 concerning “stress events” per month that must be addressed by analysts in the IRM Hub.

Employee Disgruntlement/Disengagement Statistics

The Society for Human Resource Management (SHRM) reports that in a Gallup poll of 67,000 full- and part-time employees, only 32% were “actively engaged” in their work; and 18% were actively disengaged, while 50% were neither engaged nor actively disengaged.[17] Engaged employees are involved and enthusiastic about their work. Actively disengaged employees are “disgruntled and disloyal” because “most of their workplace needs are unmet.” Of great concern is the finding that the percentage of active disengagement has risen each year since 2020. For an organization with 100,000 personnel, the disengagement statistics suggest that at least 18% of the workforce is actively disengaged/disgruntled in any given year, which averages 1,500 individuals per month. If 10% of these individuals will present behaviors of some concern to the organization, this yields an average of 150 “stress events” per month that must be addressed by analysts in the IRM Hub.

Financial Stress Statistics

The severity of financial stress varies widely, with the most significant impacts reflected in bankruptcy. According to various published statistics (e.g., Motley Fool Money website[18]), there were 494,201 bankruptcy filings in the U.S. in 2024. This represents about 0.2% of the adult population of 267 million in that year. For an organization with 100,000 personnel,

[15] National Alliance on Mental Illness (NAMI). Mental health by the numbers. https://www.nami.org/about-mental-illness/mental-health-by-the-numbers/

[16] The Global Statistics. Mental health in the U.S. 2025: Key Facts. https://www.theglobalstatistics.com/united-states-mental-health-statistics/

[17] Society for Human Resource Management (SHRM). Gallup: Employee disengagement hits 9-year high. January 25, 2023. https://www.shrm.org/topics-tools/news/inclusion-diversity/gallup-employee-disengagement-hits-9-year-high#:~:text=January%2025%2C%202023,the%20COVID%2D19%20pandemic%20were:

[18] J. Caporal. Personal bankruptcy statistics: Chapter 7 and Chapter 13. *Motley Fool Money*, May 16, 2023. https://www.fool.com/the-ascent/research/personal-bankruptcy-statistics/

we expect this annual rate of bankruptcies (0.2%) to yield 200 bankruptcies, or 17 per month. More generally, according to Forbes, 78% of workers live paycheck to paycheck and suffer general financial woes.[19] For an organization with 100,000 personnel, we expect this annual rate of general financial difficulties of any type to represent 78,000 individuals, or 6,500 per month. If we assume that 10% of these individuals experiencing financial difficulties will present behaviors of some concern to the organization, this yields an average of 650 stress events per month that may come to the attention of the IRM Hub.

3. Estimating Resource Requirements for Insider Risk Assessment

In this section, we take the statistics estimated in Section 2 to generate resource (manpower or FTE) estimates required to conduct the IRM duties. Following the estimates applied in Section 2, we have adopted a conservative approach to estimate the manpower required to assess risk for each of the concerning behaviors that contribute to insider risks and require IRM processing. In each analysis that follows, we derive and compare FTE estimates for an organization with 100,000 personnel, based on two options: Low-Fidelity/Low-Automation (representing current baseline typical IRM Hub operations) versus High-Fidelity/High-Automation (based on Cogynt).

To support this analysis, we compare the labor hours required to triage and process cases. The triage activity takes the risk population events occurring per month (derived in the previous section) and determines which of these are of sufficient concern to be taken forward for risk assessment processing. In the Low-Fidelity/Low-Automation use case, this must be performed unaided by analysts. For the High-Fidelity/High-Automation use case (based on Cogynt), this triage activity is performed by Cogynt to substantially “shrink the haystack” and reduce the number of cases required (and therefore the time required) to assess. The following rationale supports conservative estimates of the benefits of High-Fidelity/High-Automation:

- **UAM Risk Assessment.** For processing cases that reflect mainly UAM data, there is a huge benefit in automating the triage process that eliminates a large proportion (95%) of cases that would otherwise consume valuable analyst time.
- **Mental Health, Disgruntlement, and Financial Stress Risk Assessments.** In each of these categories of risk, we assume that there is a significant benefit in automating the triage process that eliminates 50% of cases that would otherwise consume valuable analyst time. This estimate is supported by recent research[20] that compared Cogynt’s triage output with expert judgments, revealing that Cogynt correctly

[19] Z. Friedman. 78% of workers live paycheck to paycheck. Forbes, Jan 11, 2019. https://www.forbes.com/sites/zackfriedman/2019/01/11/live-paycheck-to-paycheck-government-shutdown/#58be09db4f10

[20] F. L. Greitzer. Manuscript submitted for publication. From patterns to predictions: Insider risk modeling with a pattern-based behavioral analytic model

identified essentially all cases deemed by experts to be of sufficient concern to justify detailed analysis versus those cases that were not considered worthy of further referral/study. Taking this finding at face value would even justify the assumption that the automated solution could eliminate nearly all but the most severe cases — i.e., 80-90% rather than 50%. We therefore consider the 50% triage benefit to be a conservative estimate. Regarding the risk assessment of the referred cases, the automated use case is assumed to provide a 2:1 increase in analysis/assessment efficiency due to Cogynt's HCEP and case management features.

3.1 UAM – Resource Requirements to Assess Malicious Insider Computer Use

The hypothetical company used in this ROI analysis has 100,000 personnel, an existing UAM investment and 8 data analysts already employed to process the UAM alerts. UAM activity represents the largest driver in terms of potential risk and volume of data to be processed and in this case 300,000 total UAM alerts produce 60,000 alerts that require further effort. As noted in the previous section and Table 1, given the large volume of alerts per month, we used a conservative estimate of the risk pool by assuming that 60,000 of an assumed 300,000 UAM alerts per month (for an organization with 100,000 personnel) require detailed evaluation by IRM analysts; we also used conservative estimates for associated manpower.

Low-Fidelity/Low-Automation Case. For the non-automated/manual effort, estimates of time required to assess the risk for a given alert range widely; the Prophet Security report estimates that an average of 70 minutes (1.17 hrs) is required to manually investigate an alert.[21] We reduce this assumption to 45 minutes (0.75 hrs) to take into consideration productivity boosts from readily available tools such as AI , which produces a requirement for 0.75 hrs x 60,000 alerts = 45,000 hours/month (260 FTE). Our hypothetical IRM Hub, with eight analysts, has an existing capacity of 8 FTE; thus the additional required capacity is 252 FTE. Of course, this unmet capacity leads to large UAM alert backlogs that have been widely observed.

High-Fidelity/High-Automation. For the automated option using Cogynt, we assess that this solution will provide triage support that will significantly reduce the number of alerts that must be examined by IRM analysts — we assume that the Cogynt triage support will "shrink the haystack" by 95%. Therefore, the number of alerts that must be processed (those that exceed a threshold) will be greatly reduced (from 60,000 for the manual option to 3,000 for the automated option). While it is likely that Cogynt would also decrease the risk assessment time per alert, we shall conservatively assume that the same 0.75 hours is required to address alerts. Thus, the analyst processing time is reduced to 2,250 hours/month and the total FTE monthly requirement is reduced from 260 to 13 FTE, which is five more analysts than the hypothetical organization's current team.

[21] Prophet Security. The alert problem: By the numbers. https://www.linkedin.com/posts/prophetsecurity_the-average-security-alert-sits-in-the-queue-activity-7373354955807780864-ShXX/

To summarize, for an organization that has 8 analysts in its IRM Hub, the baseline *Low-Fidelity/Low-Automation* solution would require the addition of 252 analysts in order to eliminate the UAM backlog. in contrast, with the *High-Fidelity/High-Automation* solution, this IRM Hub would need to add only five analysts to completely remove the backlog. The automated high-fidelity (Cogynt) option produces a substantial reduction in manpower requirements with a ratio of 20:1.

Table 2. Comparing Estimated Additional FTE Requirements for Non-Automated Versus Automated Support for UAM Related Risk Assessment Based on 100,000 Personnel for IRM Hub With 8 Analysts

Solution	Risk Population Alerts/Month (From Table 1)	"Shrinking the Haystack": % of Alerts passed forward to analyst due to Automated Triage Support	No. Alerts/ Month for Analysis	Analyst Task Time (hrs)	Total Time (hours)	Additional FTE to Clear Alert Backlog
Low-Fidelity/Low-Automation	60,000	--	60,000	0.75	45,000	252
High-Fidelity/High-Automation	60,000	5%	3,000	0.75	2,250	5
					Ratio automated vs manual process	**20:1**

3.2 Mental Health – Resource Requirements to Insider Risk Due to Mental Health Factors

We have adopted informed, reasonable assumptions to derive estimates for assessing insider risk based on mental health factors. For each detected risk threshold, an analyst must perform research and determine the severity of the risk — not only for mental illness but for other factors that contribute to the Whole-Person picture.

Low-Fidelity/Low-Automation Case. Based on the general analysis described in the previous section and listed in Table 1, we expect approximately 93 mental health related events per month to be recorded through various information sources for a hypothetical organization with 100,000 personnel. For the unaided Low-Fidelity/Low-Automation use case, the IRM analysts must examine all these events. Some analyses may be done more quickly, and others may take more than a day, based on the complexity of the case and risk severity. What is typical for the analyst is that regardless of the PRI event, they must develop context before they can make any kind of risk judgment. This takes time and in the low-fidelity and low-automation case, we estimate the average time required for this assessment is 8 hours. The 93 events per month will require 747 hours/month or 4.3 FTE/year to assess.

High-Fidelity/High-Automation. For the High-Fidelity/High-Automation use case, we adopt a conservative estimate that triage performed by the advanced behavioral analytic platform will "shrink the haystack" of events by 50%, resulting in a smaller set of 47 mental health related events per month for analysts to examine in more detail. This advantage derives from Cogynt's unique continuous risk assessment features. Given that the context is already provided, Cogynt supports a quicker and more accurate informed judgment about risk severity: We assume that four hours are required for this assessment in this computer-aided use case (i.e., the unaided use case requires four times as long to assess than the High-Fidelity/High-Automation use case). As shown in Table 3, this results in a substantial savings in analyst time (requiring 187 hours per month versus 747 hours for the unaided use case), which yields an efficiency/manpower benefit of 4:1.

Table 3. Comparing Estimated FTE Requirement For Non-Automated Versus Automated Support for Mental Health Related Risk Assessment Based on 100,000 Personnel

Solution	Risk Population Events/Month (From Table 1)	"Shrinking the Haystack": % of events passed forward to analyst due to Automated Triage Support	No. Events/ Month for Analysis	Analyst Task Time (hrs)	Total Time (hours)	FTE Required
Low-Fidelity/Low-Automation	93	--	93	8	747	4.3
High-Fidelity/High-Automation	93	50%	46	4	187	1.1
					Ratio automated vs manual process	**4:1**

3.3 Disgruntlement – Resource Requirements to Insider Risk Due to Disgruntlement/Disengagement Factors

The Disgruntlement/Disengagement risk assessment has a similar rationale to the mental health assessment.

Low-Fidelity/Low-Automation Case. The manual option requires that IRM analysts must examine all the events that are reported (no shrinkage of the haystack), which yields a requirement to examine 150 events per month. We have made a conservative assumption that this assessment requires 4 hours per event, which yields a total time estimate of 600 hours/month (about 3.5 FTE).

High-Fidelity/High-Automation. The advantages of the automated/Cogynt use case are that (a) the triage process eliminates an assumed 50% of events that are deemed not of sufficient concern (shrinking the haystack) and (b) the information collected, HCEP analysis, and case management support facilitates more efficient risk assessment by the analyst (2 hours versus 4 hours). This produces a 4:1 reduction in the FTE resources required for the automated support solution as shown in Table 4.

Table 4. Comparing Estimated FTE Requirement For Non-Automated Versus Automated Support for Disgruntlement Related Risk Assessment Based on 100,000 Personnel

Solution	Risk Population Events/Month (From Table 1)	"Shrinking the Haystack": % of events passed forward to analyst due to Automated Triage Support	No. Events/ Month for Analysis	Analyst Task Time (hrs)	Total Time (hours)	FTE Required
Low-Fidelity/Low-Automation	150	--	150	4	600	3.5
High-Fidelity/High-Automation	150	50%	75	2	150	0.9
					Ratio automated vs manual process	**4:1**

3.4 Financial Stress – Resource Requirements to Insider Risk Due to Financial Stress

For financial stress, the assumptions for determining the risk pool are similar to the other categories. As shown in Table 1 above, the estimated financial risk indicator events per month is 650 for an organization with 100,000 personnel being monitored.

Low-Fidelity/Low-Automation Case. As in the other use cases, we assume that in the manual use case, the analyst must review all the financial-risk related events that come into the IRM hub without the benefit of triage filtering. This produces a processing load of 650 events per month. The Low-Fidelity/Low-Automation system requires significantly more analyst time to assemble the contextual information and to monitor financial risk. We assume that the average unaided time required per event is 4 hours.

High-Fidelity/High-Automation. We assume that the automated support provided for triage helps to reduce the size of the haystack by 50% from 650 events to 325. Further, the Cogynt High-Fidelity/High-Automation solution — through its HCEP analysis and case management support — will have all essential contextual information available for review and will enable the analysis to be conducted far more quickly and efficiently: the time required for the analyst to assess risk in this case is reduced to 2 hours. This produces a 4:1 reduction in the FTE resources required for the automated support solution, as shown in Table 5.

Table 5. Comparing Estimated FTE Requirement For Non-Automated Versus Automated Support for Financial Stress Related Risk Assessment Based on 100,000 Personnel

Solution	Risk Population Events/Month (From Table 1)	"Shrinking the Haystack": % of events passed forward to analyst due to Automated Triage Support	No. Events/ Month for Analysis	Analyst Task Time (hrs)	Total Time (hours)	FTE Required
Low-Fidelity/Low-Automation	650	--	650	4	2,600	15
High-Fidelity/High-Automation	650	50%	325	2	650	3.8
					Ratio automated vs manual process	**4:1**

4. Comparing Automated Versus Non-Automated Insider Risk Assessment Options

4.1 Accuracy and Efficiency Benefits

The previous section itemized four risk areas as a basis for comparison, using available information and conservative percentages of the total population and numbers of potential risk indicators. We argued that regardless of the organization's size, an effective IRM solution requires a high-performance behavioral analytic platform such as Cogynt to manage scope, provide the analytic fidelity for detecting and evaluating risk indicator patterns and risk thresholds, and to deliver workflow automation while remaining agile to accommodate new and changing requirements and capabilities. These represent several of many qualitative benefits afforded by the Cogynt High-Fidelity/High-Automation solution.

We now aggregate the likely risk pools and total man hours and FTEs to compare the two solutions. Tables 6 and 7 (respectively for non-automated and automated solutions) pull together the results from Section 3 showing the monthly totals for number of risk indicator events, total time for each of the four risk categories examined, and the corresponding FTE values.

High-Automation/High-Fidelity — Cogynt Solution Deployment Addresses the Backlog

Consider our hypothetical organization with 100,000 personnel. The analysis presented here shows that the organization's IRM program needs over 280 analysts to process all alerts and eliminate the backlog: It is not surprising to find that typical IRM backlogs average 40-50%.

Realistically, it is not feasible to hire so many people. Our calculations reveal that the High-Fidelity/High-Automation/Cogynt use case requires only 19 FTE to completely eliminate the backlog. (cf. Tables 6 and 7).

The total number of risk indicator alerts per month in the non-automated case is 60,893 (per 100,000 personnel), while the total alerts per month for the automated case is 3,447. This reflects advantage of the automated support solution that has the effect of "shrinking the haystack" — yielding a benefit ratio of 18:1 as shown in the second column of Table 8. For the non-automated solution, the total additional analyst FTE requirement (in an organization with 100,000 personnel and an IRM Hub with 8 analysts) is 274, compared to 11 required additional FTE for the automated support solution, yielding an efficiency benefit ratio of 26:1 for automated support.

Table 6. Non-Automated FTE Requirements For Insider Risk Assessment Based on 100,000 Personnel

Risk Category	No. Alerts/Month	Total Time (hours)	Additional FTE/Month
UAM/IT Risks	60,000	45,000	252
Mental Illness	93	747	4.3
Disgruntlement/Disengagement	150	600	3.5
Financial Stress	650	2,600	15.0
Total	**60,893**	**48,947**	**274**

Table 7. Automated Support FTE Requirements For Insider Risk Assessment Based on 100,000 Personnel

Risk Category	No. Events/Month	Total Time (hours)	Additional FTE/Month
UAM/IT Risks	3,000	2,250	5
Mental Illness	47	186.7	1.08
Disgruntlement/Disengagement	75	150	0.87
Financial Stress	325.0	650	3.75
Total	**3,447**	**3,237**	**11**

Table 8. Comparing Benefit Ratios for Non-Automated Versus Automated Support for Insider Risk Assessment Based on 100,000 Personnel

Solution Option	No. Alerts/Month	Additional FTE/Month
Low-Fidelity/Low-Automation	60,893	274
High-Fidelity/High-Automation	3,447	11
RATIO	**18:1**	**26:1**

4.2 Examining Cost Models

Estimating cost benefits is much more speculative than comparing efficiencies of insider risk assessment functions using High-Fidelity/High-Automation software (Cogynt platform) versus the Low-Fidelity/Low-Automation software option associated with a traditional, less mature, baseline IRM program. This is because other benefits (including less tangible ones) derive from more mature IRM programs that use High-Fidelity/High-Automation support such as that provided by the Cogynt decision intelligence platform. Perhaps the most significant benefit derives from the greater accuracy and efficiency afforded by the more proactive, behavioral analytic approach used in the Cogynt solution: This improvement in program effectiveness has the net effect of helping to avoid insider threat incidents. The associated cost avoidance advantage is substantial, given the extremely high (and increasing) cost of remediating insider threat incidents — recall that the average annual variable costs of running an Insider Risk Department (including incident response) has risen to over $17M USD according to the Poneman *Insider Risk Global Report*.[22]

[22] Poneman Institute. 2025. *Cost of Insider Risks Global Report 2025*. Poneman / DTEX. https://www2.dtexsystems.com/l/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf

The high-fidelity and high-automation software costs are included in this solution estimate, while the Low-Fidelity/Low-Automation software costs are not. We assume that the Low-Fidelity/Low-Automation software costs will not be a significant factor in the overall cost profile. Other costs such as facilities and infrastructure costs are not considered in this analysis because they will mostly cancel each other out in a comparative analysis.

Low-Fidelity/Low-Automation Cost Model. Table 9 summarizes the FTE requirements for the hypothetical case examined here for an organization with 100,000 personnel and an IRM Hub with 8 analysts.

Table 9 Low-Fidelity/Low-Automation Baseline FTE Summary

Number of Personnel in Organization	No. Alerts/Month	Total Man Hours/Month	Additional FTE/Month
100,000	60,893	48,947	274

Table 10 translates the information in Table 9, row 2 (100,000 personnel) to IRM Hub personnel cost estimates. We assume that the IRM team includes a mixture of threat analysts, data scientists, and management as shown.

Table 10 Low-Fidelity/Low-Automation Baseline Cost Model – 100,000 Personnel

Analyst Type	Rate	Required FTE/Year	Annual Cost
Threat Analyst	70	225	$32,759,328
Data Scientist	125	36	$9,274,200
Management	130	14	$3,709,680
	Total	**274**	**$45,743,208**

High-Fidelity/High-Automation Cost Model. Table 11 summarizes the FTE requirements for the hypothetical case examined here for an organization with 100,000 personnel and an existing IRM Hub with 8 analysts.

Table 11 High-Fidelity/High-Automation FTE Summary (Cogynt)

Number of Personnel in Organization	No. Events/Month	Total Man Hours/Month	Additional FTE/Month
100,000	3,447	3,236.7	11

Table 12 translates the information in Table 11, row 2 (100,000 personnel) to IRM Hub personnel cost estimates. We assume that the IRM team includes a mixture of threat analysts, data scientists, and management as shown.

Table 12 High-Fidelity/High-Automation Cost Model (Cogynt) – 100,000 Personnel

Analyst Type	Rate	Required FTE/Year	Annual Cost
Threat Analyst	70	9	$1,274,280
Data Scientist	125	1	$360,750
Management	130	1	$144,300
	Total:	**11**	**$1,779,330**

4.3 Cost Summary

Table 13 reflects the costs associated with conducting the advanced analytics for the hypothetical organization with 100,000 personnel, maintaining the data on each person (digital twin) that yields the high-fidelity analytic results, and the essential automation needs for the IRM Hub. This is priced on a per entity basis (per person) for the monthly subscription, which also includes a separate support cost (also priced on a per entity basis).

Table 13 Cogynt – High-Fidelity/High-Automation Cost Model for (100,000 Personnel)

Software Platform	Entities	Cost per Entity/mo.	Cost per Month
Cogynt	100,000	$1.80	$180,000
Enterprise Support	100,000	$0.25	$25,000
		Total per month:	$205,000
		Total Cost (Software and Support) per Year:	$2,460,000
		Total Staffing Cost/Year (from Table 12):	$1,779,330
		TOTAL COST:	$4,239,330

Table 14 shows a consolidated view of the estimated risk reduction projections between Cogynt and the Low-Fidelity/Low-Automation solutions for an organization with 100,000 personnel. The Table compares the Low- versus High-Automation solutions based on several evaluation criteria: Accuracy of analysis, Efficiency (FTE Staffing Levels), and Cost. The ratios show the forecasted benefit of investing in a Cogynt type system given the scale of the insider threat challenge.

The analysis in this paper identifies three essential metrics: Accuracy (PRI event detection per month), Analyst Efficiency /Staffing levels in terms of FTEs (needed to perform the analysis) and Total cost. This analysis confirms that from a coverage capability, timing, proactive capability and overall risk reduction posture, the deployment of a behavioral analytic is mission critical as well as being cost effective.

Table 14 Risk Reduction Summary – 100,000 Personnel

Information System Capabilities	Accuracy (Risk Indicator Events/ Month) – Shrinking the Haystack	Efficiency (Analyst Hours/Month) — Reducing FTE Requirements	Total Annual Cost Estimate
Low-Fidelity/Low-Automation system solution [Staff Cost Alone]	60,894	274	$45,743,208
High-Fidelity/High-Automation system solution [Staff + System Cost]	3,447	11	$4,239,330
Projected Risk Reduction Ratio (High-Fidelity/High-Automation versus Low-Fidelity/Low-Automation) options	**18:1**	**26:1**	**11:1**

With a moderate size organization comprising 100,000 personnel, the expected IRM program cost comparison, with versus without the benefit of an advanced High-Fidelity/High-Automation system (Cogynt) solution, yields a 11:1 overall annual cost ratio.

5. Conclusions

This brief report provided a general business case for Cogynt's high-fidelity/high-automation solution for IRM that contrasts with traditional low-fidelity/low-automation programs. We provided a general overview of program benefits and applied rules of thumb on Return on Investment (ROI) to help prospective adopters of this technology assess possible benefits. We concluded that for a modest sized organization with 100,000 personnel, there is a 11:1 cost benefit in adopting the Cogynt high-fidelity/high-automation IRM solution.

The baseline non-automated approach reflects multiple disparate unintegrated data sources, while the more advanced automated support approach emphasizes the role of the behavioral analytic as an integrated function. Further, the advanced behavioral analytic incorporates risk indicator models and weighting factors that are not implemented in the baseline approach. This distinction alone makes a stronger case for accuracy of detection than a manual assessment approach. The advanced analytic approach collects threshold detections and presents results to the user in context, while the baseline model requires the user to collect the information manually from multiple data sources. The High-Fidelity/High-Automation model will deliver more effective analytics (higher accuracy) and enhance insider risk assessment performance compared to the lower accuracy product of the Low-Fidelity/Low-Automation Baseline.

We showed that for a moderate size organization comprising 100,000 personnel, the advanced High-Fidelity/High-Automation system (Cogynt) yields a 11:1 overall annual cost efficiency ratio compared to the baseline IRM program. Beyond this general ROI advantage, we note that with most organizations experiencing high IRM backlogs of 40-50% that can potentially be eliminated through deployment of the more effective Cogynt solution, there is potential for significant additional cost avoidance if the more effective solution proactively identifies, mitigates or prevents incidents — which lead to remediation costs exceeding $700K each — that would have been missed by the Low-Fidelity/Low-Automation approach. This additional increase in the value of investment provides further incentives for IRM programs to adopt the advanced Cogynt technology.

COGILITY

Visit **www.cogility.com/insider-risk-management** 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

11/25