WHITE PAPER

COGILITY

Whole-Person C-InT Approach to Get Left of Harm

By Frank L. Greitzer, PhD
Chief Behavioral Scientist

Introduction

Insider threats are actions by individuals who abuse their access privileges by committing acts of data theft, espionage, sabotage, fraud, or workplace violence.[1] According to the 2023 Ponemon Institute's 2023 *Cost of Insider Risks Global Report*[2], 309 organizations across various industries reported 7,343 incidents, costing an average of $16.2 million each. Malicious insider threats account for about 25% of all reported incidents in 2023 and were by far the most expensive, costing on average $701,500 per incident to contain and remediate the damage. With potentially catastrophic consequences, these incidents are often perpetrated by individuals with perceived grievances, exacerbated by personal predispositions (psychological factors such as depression or personality traits such as narcissism or anti-social personality disorder) that lead them to react or act-out in response to work- or life-stressors.[3]

Getting Left of Harm

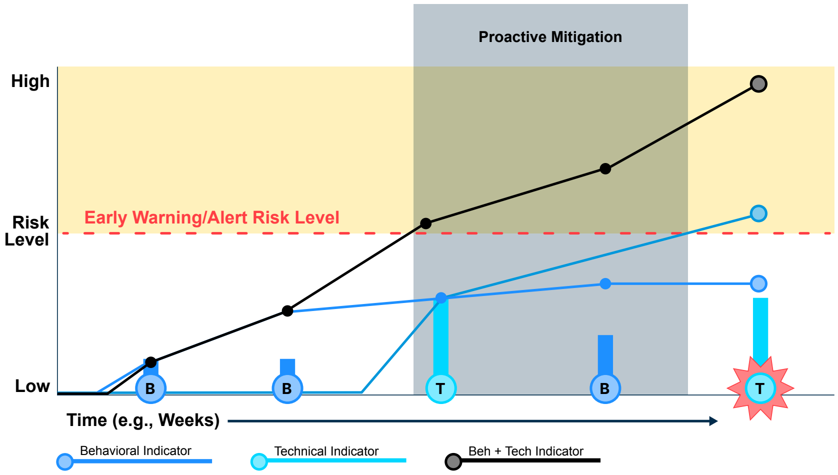

Figure 1. Sociotechnical (behavioral) data enables proactive mitigation to get "left of harm."

Early work in countering insider threats was greatly influenced by cybersecurity defenses against external attacks, which focus on detecting technical violations identified by monitoring audit data from host/network cyber activities. However, noted thought leaders have advised that a comprehensive solution is needed to effectively counter insider risk. Studies by Eric Shaw and colleagues[3] and reports by the CERT Division of Carnegie Mellon's Software Engineering Institute1 are among the best examples of these important contributions to the field. As Greitzer et al argued in a 2018 paper[4], the incorporation of behavioral factors provides an

[1] Cappelli, DN, Moore, AP, & Trzeciak RF. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Addison-Wesley.

[2] Ponemon Institute and DTEX. (2024). *Cost of Insider Risks Global Report*. Ponemon Cost of Insider Risks Global Report - DTEX Systems Inc

[3] Shaw, ED & Sellers, L. (2015). Application of the Critical-Path Method to Evaluate Insider Risks, *Studies in Intelligence* 59(2) (Extracts, June 2015)

[4] Greitzer, FL, Purl, J, Leong, YM, and Becker DE. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. *IEEE Symposium on Security and Privacy Workshops*, 197-206.

opportunity to recognize at-risk individuals early — i.e., "left of harm" — before they would otherwise be identified by methods that only examine technical indicators (see Fig. 1). Here we distinguish between contributions of technical indicators (online behavior) versus psychosocial/behavioral indicators, demonstrating how the combination of both data sources in a comprehensive Counter-Insider Threat (C-InT) approach can provide early warning and greater opportunity for proactive mitigation.

The Streetlight Effect

Unfortunately, many insider risk programs are still reluctant to adopt a more holistic, "whole person" approach. This decision bias was depicted 100 years ago in a *Mutt & Jeff* comic strip[5] and referred to as the "streetlight effect," which describes how people tend to search for a solution in the *easiest* places, rather than seeking information that is *most relevant* or likely to yield results (see Fig. 2).

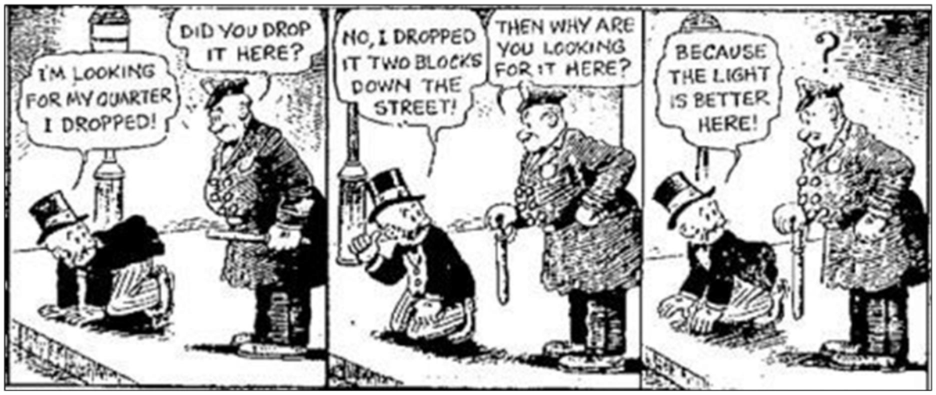
I'M LOOKING FOR MY QUARTER I DROPPED!
DID YOU DROP IT HERE?
NO, I DROPPED IT TWO BLOCKS DOWN THE STREET!
THEN WHY ARE YOU LOOKING FOR IT HERE?
BECAUSE THE LIGHT IS BETTER HERE!
?

Figure 2. The Streetlight Effect

By focusing merely on host/network audit data that is most readily obtained, insider threat programs most often miss the human side of the problem. Compared with typical reactive programs that limit analysis to technical data, programs that incorporate behavioral data monitoring and analytics (deriving from Human Resources, Security, Performance Reviews, Financial, Criminal, etc.) can gain insight about personal predispositions, precipitating events (stressors), or concerning behaviors that reveal higher-risk individuals who show behavioral signs weeks or months prior to the incident.[6,7,8]

[5] The Streetlight Effect [Mutt & Jeff comic strip, *Boston Herald*, May 24, 1924, Whiting's Column: "Tammany Has Learned That This Is No Time for Political Bosses," Page 2, Column 1, Boston, Massachusetts]

[6] Shaw ED, Fischer L. Ten tales of betrayal: an analysis of attacks on corporate infrastructure by information technology insiders, Vol. 1. Monterey, CA: Defense Personnel Security Research and Education Center. 2005

[7] Greitzer, FL, Purl, J, Leong, YM, and Becker DE. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. *IEEE Symposium on Security and Privacy Workshops*, 197-206.

[8] Greitzer, FL. (2019). Insider Threats: It's the *HUMAN, Stupid! Proceedings of the Northwest Cybersecurity Symposium*, April 8-10, 2019. Article No. 4, pp. 1-8. ACM ISBN 978-1-4503-6614-4/19/04

As the Poneman Global Report notes, “The good news is that change is on the way. Organizations are increasingly acknowledging the need to home in on the human element to shift the needle to where it needs to be, from reactive to proactive.”

Establishing an Effective C-InT Program

The Federal Insider Threat Program was established in 2012 by Presidential Executive Order (EO) 13587.[9] The National Insider Threat Task Force (NITTF) was also established to provide guidance and promote best practices. Federal agencies documented their own policies and instructions that define authorities, responsibilities, and relevant constructs — including threat behaviors of concern and definitions of contributing factors or indicators associated with these threats. All entities benefit from such standardization, but each organization may apply its own criteria or priorities, informed by its mission and culture, to implement its C-InT Program.

If you do not already have a C-InT program, you ought to establish one. If you have a program in place, you should examine its features to identify any possible improvements. Among the most important qualities of an effective program is the establishment of a whole-person approach to insider threat assessment. In reviewing the strengths and limitations of your current program, consider the following ingredients of an effective C-InT program:

- Your program should comprise a team with broad knowledge of your organization’s operations, mission, and vulnerabilities. This requires representatives from security, IT, human resources, legal, and C-suite executives. This ensures that your program has buy-in from critical stakeholders and that it operates in concert with organizational goals, policies, and legal/regulatory guidelines.
- A major requirement in establishing an effective C-InT program is to identify the organization’s critical assets. This not only includes physical assets, but also virtual assets like intellectual property and sensitive product information, as well as human assets — protecting employees, employee data, and safeguarding personally identifiable information. Having a cross-section of C-InT members from across the organization’s business units will ensure that the team is able to accurately identify and prioritize all critical assets.
- The team should perform an audit of all systems and protective strategies that guard against insider threats from authorized users. This initial risk and vulnerability assessment provides a foundation for building a robust framework of insider threat indicators and fills gaps that are identified in the audit. The specification or fine-tuning of insider risk indicators and their associations with threat types is an ongoing process. Specification of data sources is a necessary part of this process of establishing a knowledge base of insider risk indicators tailored to the organization.

[9] https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

- Technology and robust technical solutions must be implemented to provide real-time monitoring and analysis of streaming data. To achieve a level of performance that meets or exceeds best practices, the approach should evaluate behavioral as well as technical indicators. The interdisciplinary make-up of the C-InT team is crucial to overcoming resistance by important stakeholders, such as Human Resources or Security departments, to make the non-technical data sources available. Comprehensive data monitoring and analysis, including the application of evidence-based behavioral science findings, is a necessary condition for achieving a mature, highly effective C-InT program that defines and adopts whole-person, positive/supportive mitigation strategies to get "left of harm."

Defining Insider Risk Indicators

A knowledge base of Potential Risk Indicators (PRIs) has been defined by the U.S. Government. This hierarchy of PRIs compares with other knowledge bases that have been developed, such as the *Sociotechnical and Organizational Factors for Insider Threat (SOFIT) ontology*[10] (comprising more than 300 PRIs) that was developed under a contract with the Intelligence Advanced Research Projects Activity (a portion of the SOFIT taxonomy is shown in Fig. 3). SOFIT is uniquely positioned to support more proactive, whole-person approaches to insider risk mitigation through its specification of psychosocial factors that may contribute to insider threats. Thus, in addition to listing hundreds of technical (cybersecurity) violations, the SOFIT knowledge base describes various types of behavioral and psychological factors. As shown, these are organized

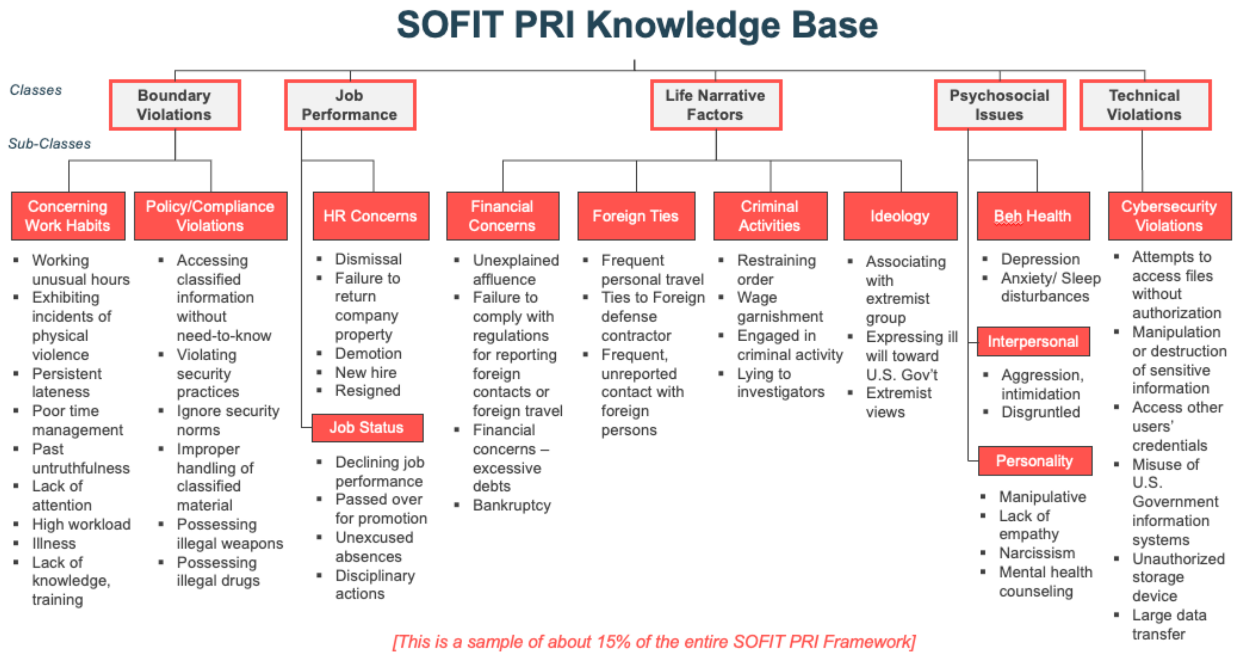
SOFIT PRI Knowledge Base
Classes
Sub-Classes
Boundary Violations
Job Performance
Life Narrative Factors
Psychosocial Issues
Technical Violations
Concerning Work Habits
Working unusual hours
Exhibiting incidents of physical violence
Persistent lateness
Poor time management
Past untruthfulness
Lack of attention
High workload
Illness
Lack of knowledge, training
Policy/Compliance Violations
Accessing classified information without need-to-know
Violating security practices
Ignore security norms
Improper handling of classified material
Possessing illegal weapons
Possessing illegal drugs
HR Concerns
Dismissal
Failure to return company property
Demotion
New hire
Resigned
Job Status
Declining job performance
Passed over for promotion
Unexcused absences
Disciplinary actions
Financial Concerns
Unexplained affluence
Failure to comply with regulations for reporting foreign contacts or foreign travel
Financial concerns – excessive debts
Bankruptcy
Foreign Ties
Frequent personal travel
Ties to Foreign defense contractor
Frequent, unreported contact with foreign persons
Criminal Activities
Restraining order
Wage garnishment
Engaged in criminal activity
Lying to investigators
Ideology
Associating with extremist group
Expressing ill will toward U.S. Gov't
Extremist views
Beh Health
Depression
Anxiety/ Sleep disturbances
Interpersonal
Aggression, intimidation
Disgruntled
Personality
Manipulative
Lack of empathy
Narcissism
Mental health counseling
Cybersecurity Violations
Attempts to access files without authorization
Manipulation or destruction of sensitive information
Access other users' credentials
Misuse of U.S. Government information systems
Unauthorized storage device
Large data transfer
[This is a sample of about 15% of the entire SOFIT PRI Framework]

Figure 3. SOFIT Taxonomy Snapshot

[10] Greitzer, Purl, Leong, Becker (2018)

into classes (Boundary Violations, Job Performance, Life Narrative Factors, Psychosocial Issues, and Technical Violations). These are further divided into sub-classes, which comprise the individual risk indicators that are defined. The entire hierarchy includes more than 300 PRIs (only a small fraction of these are shown in the figure).

Characteristics of a Highly Effective Whole-Person C-InT Program

Security is a fundamental component of organizational health: it should not be treated as an incident-driven, reactive process but rather should inform a proactive approach to establish and maintain organizational well-being. Insider Threat programs increasingly acknowledge the need to address the human element. To achieve a more proactive, positive insider risk program, management must foster a change in organizational culture that promotes sharing of information across stakeholder departments (HR, Security) and adoption of supportive rather than punitive methods to proactively mitigate insider risk. Important ingredients of effective C-InT programs that meet or exceed best practices are summarized below:

The most effective, mature C-InT programs:

1. ***Discourage Silos and Encourage Participation of All Stakeholders in C-InT Program.*** Adopt an insider threat program that comprises a diverse group of all relevant stakeholders (HR, IT, Security, Finance, Legal & Compliance, etc.). It is vital to share viewpoints through regular communication among a cross-cutting C-InT team.

2. ***Seek a More Positive Security Culture.*** Work to change mindsets across all levels of the organization by instilling a security culture that acknowledges everyone's role in maintaining an effective security climate. It's important that management fully endorses the C-InT mission and policies; but it is equally critical that it is accepted by all staff members and mid-level supervisors who must be vigilant in recognizing and reporting possible risks without fear of retribution. Regular training and awareness activities are needed to build acceptance of the idea that an effective, supportive security program benefits the entire organization by protecting intellectual and human assets while respecting individual privacy.

3. ***Adopt a Supportive, Not Punitive Approach to Insider Threat Mitigation.*** Ensure that all workers understand and "buy-into" a positive deterrence philosophy that places a priority on identifying at-risk individuals so that, wherever possible, steps can be taken to reduce the risk by helping troubled individuals find "offramps" from the critical pathway leading to insider incidents.

4. ***Embrace a Whole-Person C-InT Approach.*** Adopt a holistic approach to insider threat assessment by overcoming barriers to sharing of behavioral data (HR, Security, other sources of public information) in addition to the more traditional monitoring of technical indicators. Technical indicators are important for identifying abnormal or unauthorized behavior, but incorporation of other, human factors data helps to build a more comprehensive, proactive program by applying evidence-based, behavioral science research and practice to anticipate and mitigate risks.

Cogility Software can work with your organization's C-InT program leaders and analysts to exploit the highly flexible, scalable insider threat assessment and case management capabilities of its Cogynt continuous intelligence platform and meet or exceed best practices in achieving a proactive, whole-person, comprehensive, integrated behavioral analytic C-InT capability.

Cogynt C-InT Continuous Intelligence Platform

Cogility Software, in its efforts working with clients, is integrating existing research and operational information sources to produce the most comprehensive knowledge base of insider threat indicators available today. We are incorporating concepts described in the SOFIT ontology as well as other frameworks for understanding insider threats — particularly the Critical Pathway to Insider Risk (CPIR) model developed to better understand the role of contributing factors.[11]

Cogility's Counter-Insider Threat solution, powered by our Cogynt continuous intelligence platform, is uniquely designed and proven to meet the immense and dynamic information-processing, complex analytic, and workflow challenges faced by insider threat analysts across government and industry. Cogynt applies patented Hierarchical Complex Event Processing (HCEP) to ingest and analyze massive, diverse volumes of technical and behavioral data streams in real-time to monitor, score, and determine explicit and predicted insider risk.

Discriminating Features of Cogility Cogynt C-InT Solution

- **Cogynt builds on the SOFIT Knowledge Base.** SOFIT PRI ontology provides a solid framework for characterizing and cataloguing risk indicators and contributing factors for insider threat
- **Cogynt Model Accounts for Varying Threat Types.** PRIs vary in their degree of association with different insider threat behavior types
- **Cogynt Supports PRI "Decay" Concept.** PRIs vary in their spans of influence on risk judgments — models may apply different "rates of decay"
- **Cogynt's HCEP Approach Captures Interactions Among PRIs.** Most predictive models assume that PRIs contribute independently to risk—limiting their effectiveness. Cogynt's pattern processing captures these complex relationships.
- **Cogynt's Pattern Based Approach Reflects the Way Experts See the Problem.** The pattern-based Cogynt model provides a more robust threat assessment paradigm that reflects the complex hierarchical structure used by expert analysts when solving this problem

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

As shown in Fig. 4, the top-level event pattern represents the whole person profile, and the lower-level patterns represent observations, which are building blocks of PRIs. Different combinations of PRIs reflect different behavioral insider threat patterns. Unstructured and structured data are processed from the bottom up and mapped to PRIs with estimated risk weights and decay characteristics. The HCEP process proceeds upwards from PRIs to threat behavior types, with varying strengths of association between PRIs and behavior patterns, and higher-level patterns that represent collections of PRIs.

Counter-Insider Threat – Whole Person Behavioral Analysis

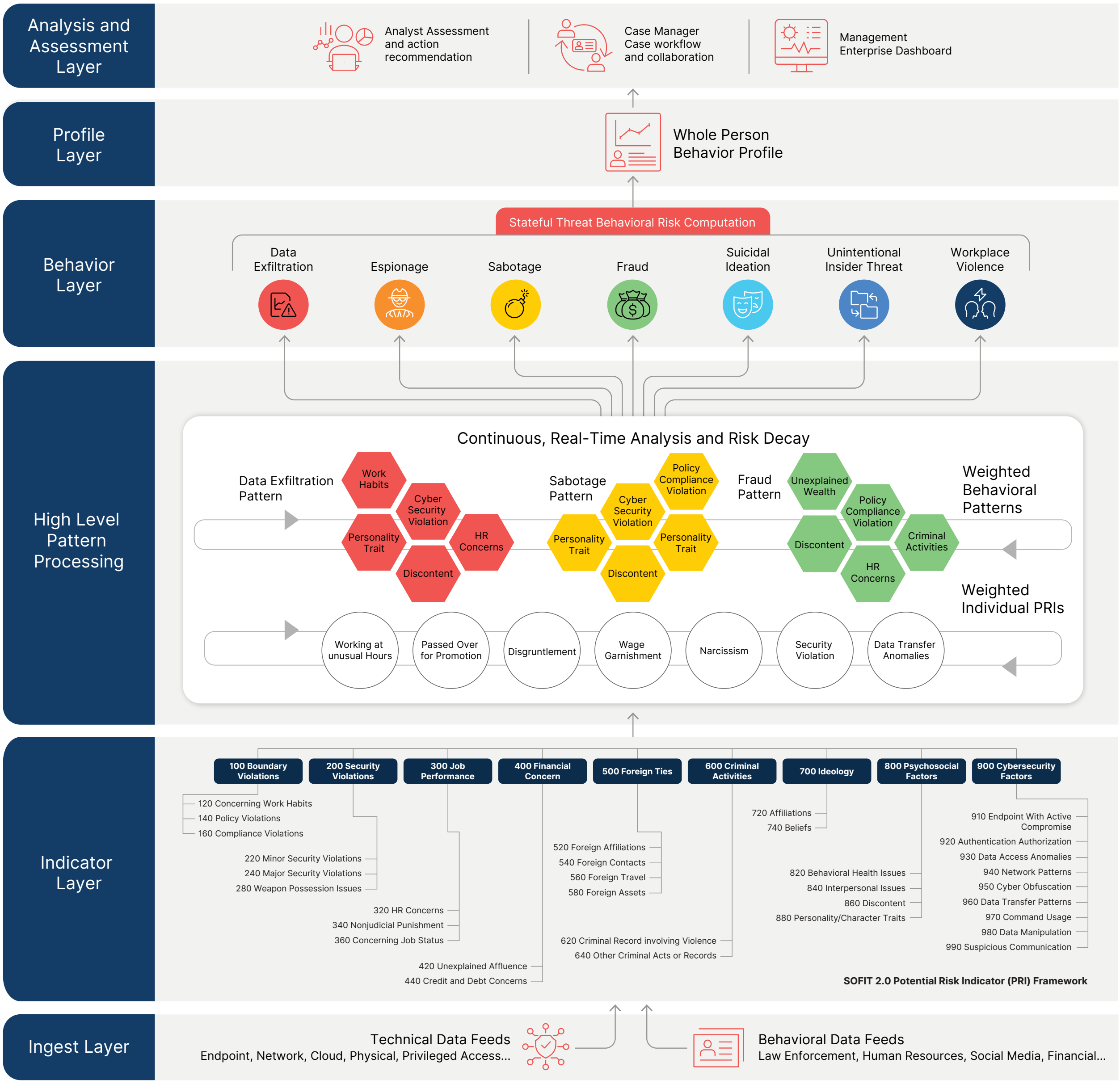
Analysis and Assessment Layer
Analyst Assessment and action recommendation
Case Manager Case workflow and collaboration
Management Enterprise Dashboard
Profile Layer
Whole Person Behavior Profile
Behavior Layer
Stateful Threat Behavioral Risk Computation
Data Exfiltration
Espionage
Sabotage
Fraud
Suicidal Ideation
Unintentional Insider Threat
Workplace Violence
High Level Pattern Processing
Continuous, Real-Time Analysis and Risk Decay
Data Exfiltration Pattern
Work Habits
Cyber Security Violation
Personality Trait
HR Concerns
Discontent
Sabotage Pattern
Policy Compliance Violation
Cyber Security Violation
Personality Trait
Personality Trait
Discontent
Fraud Pattern
Unexplained Wealth
Policy Compliance Violation
Discontent
Criminal Activities
HR Concerns
Weighted Behavioral Patterns
Weighted Individual PRIs
Working at unusual Hours
Passed Over for Promotion
Disgruntlement
Wage Garnishment
Narcissism
Security Violation
Data Transfer Anomalies
Indicator Layer
100 Boundary Violations
200 Security Violations
300 Job Performance
400 Financial Concern
500 Foreign Ties
600 Criminal Activities
700 Ideology
800 Psychosocial Factors
900 Cybersecurity Factors
120 Concerning Work Habits
140 Policy Violations
160 Compliance Violations
220 Minor Security Violations
240 Major Security Violations
280 Weapon Possession Issues
320 HR Concerns
340 Nonjudicial Punishment
360 Concerning Job Status
420 Unexplained Affluence
440 Credit and Debt Concerns
520 Foreign Affiliations
540 Foreign Contacts
560 Foreign Travel
580 Foreign Assets
620 Criminal Record involving Violence
640 Other Criminal Acts or Records
720 Affiliations
740 Beliefs
820 Behavioral Health Issues
840 Interpersonal Issues
860 Discontent
880 Personality/Character Traits
910 Endpoint With Active Compromise
920 Authentication Authorization
930 Data Access Anomalies
940 Network Patterns
950 Cyber Obfuscation
960 Data Transfer Patterns
970 Command Usage
980 Data Manipulation
990 Suspicious Communication
SOFIT 2.0 Potential Risk Indicator (PRI) Framework
Ingest Layer
Technical Data Feeds
Endpoint, Network, Cloud, Physical, Privileged Access...
Behavioral Data Feeds
Law Enforcement, Human Resources, Social Media, Financial...

Figure 4. Cogynt C-inT Hierarchical Processing

Cogynt's HCEP behavioral analytic performs pattern processing at varying levels of abstraction. At the lowest level, patterns of ingested data are recognized to identify PRIs. The mappings of PRIs to threat behaviors inform the risk calculation, but the identification of patterns at higher levels of abstraction further adjusts the risk assessment. Certain PRI patterns — collections of PRIs — provide stronger evidence (beyond the consideration of individual PRIs) that an insider threat incident is in progress or imminent. For example, if a case comprises PRIs for disciplinary action, disgruntlement, aggression, and mental health concerns, the combination of all these PRIs provides much stronger indication of potential for workplace violence, compared to the independent accounting of the separate PRIs.

Research has shown[12] that PRIs do not exert independent influence on judgments of insider risk — in other words, "the whole is not equal to the sum of its parts." Cogynt takes this dynamic feature of PRI interactions into account in its hierarchical computation of insider risk. This pattern processing concept is illustrated in Fig. 5, which shows how the computation of Workplace Violence risk not only depends on the independent contribution of observed PRIs to the risk of a case, but also receives an incremental adjustment if a certain higher level pattern is detected that reflects a key combination of PRI subclasses.

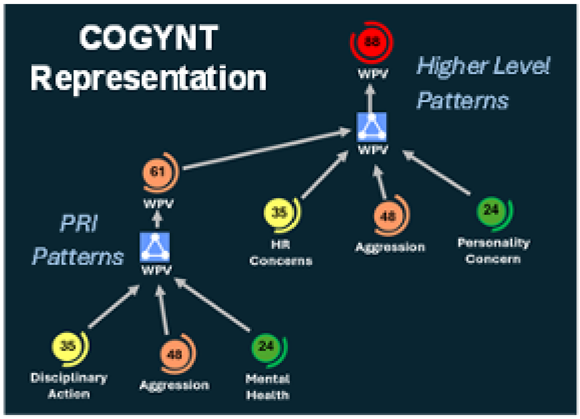

Figure 5. Risk calculation takes higher levels of abstraction into account.

[12] Greitzer, FL, & J Purl. (2022). The dynamic nature of insider threat indicators. *Springer Nature Computer Science*, 3(102). https://doi.org/10.1007/s42979-021-00990-1.

Conclusions

Cogility's C-InT solution empowers organizations to take a whole person approach to detect, prevent, and mitigate insider threats. Cogynt continuously monitors and analyzes both technical and behavioral potential risk indicators, leveraging advanced stream data analytics and Expert AI technology to dynamically map, analyze and prioritize risk with full traceability. Cogility modernizes C-InT programs to help organizations more efficiently respond to and avoid insider threat incidents. This exceptional level of analysis and case management support positions Cogility as a market leader for security and risk management solutions.

> *"Cogility C-InT stands apart owing to its "whole person" approach that continuously analyzes both technical activity and behavioral indicators.... The solution goes beyond mere detection of security violations and anomalies but provides advanced PRI pattern analytics inclusive of psychosocial behavior. [This] positions the Cogility C-InT solution as a valuable tool for proactive insider threat management – and as a market leader."*
>
> **- Quadrant Knowledge Solutions (2024)[13]**

[13] Quadrant Knowledge Solutions (2024). *Security and Risk Management SPARK MatrixTM: Insider Risk Management Q3, 2024 Market Insights, Competitive Evaluation, and Vendor Rankings*, July, 2024.

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

02/25