SOLUTION BRIEF

COGILITY

How Cogynt URP Delivers Continuous Intelligence for Whole Person Counter-Insider Threat Management

Introduction

The demands of Counter-Insider Threat (C-InT) assessment to fully address the insider threat analysis problem exceeds currently fielded solutions and overwhelm the cognitive limitations of C-InT professionals. In contrast to current practice that is largely reactive, a continuous intelligence approach with an advanced behavioral analytic is needed to achieve a comprehensive, proactive C-InT program that can handle the data analysis demands and decision support for C-InT professionals. Analysis of behavioral and technical data leveraging predictive, unified real-time platform (URP) technology will deliver a whole person C-InT program that monitors and detects potential insider risks so that threat mitigation efforts can be applied to help detect or avoid incidents.

Cogynt Whole Person C-Int Capabilities

1. Human in the loop
2. Multiple, simultaneous data source ingestion
3. Semantic analysis to process structured or unstructured data at scale
4. Complete, no-code behavioral modeling environment with a self-documenting model that may be reviewed and validated by third-party experts
5. Patented, real-time behavioral analytic to hierarchically process technical and psychosocial event patterns to yield actionable intelligence
6. Real-time continuous risk assessment to assess behavioral patterns
7. Visualizations to present and allow manipulation of complex data and relationships in various contexts (geospatial, link charts, hierarchy charts, graphs and histograms, lists, etc.)
8. Case file management to support risk assessment recommendations, custom annotation, review, and response coordination workflow
9. Audit support, with full traceability, to ensure compliance with organizational policies
10. Integrated business intelligence, including dashboards and reports, to readily review and share executive and operational insights, such as risk hotspots, case management performance, program trends
11. Open architecture that can be easily integrated with other applications and data stores
12. Scalable to the needs of the enterprise and big data to be processed
13. Fully integrated COTS solution, leveraging URP technology, that is easy to install and manage

Background

Insider threats are actions by trusted individuals with access to organizational assets that may harm the organization or its assets — these acts include insider data theft/exfiltration, sabotage, espionage, fraud, maladaptive behavior, workplace violence, and unintentional insider threats.[1] With potentially catastrophic consequences, these incidents often are perpetrated by individuals with 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.[2]

Figure 1 is a notional plot of insider threat risk that distinguishes between contributions of technical indicators, such as endpoint, network, cloud, and physical security violations and anomalies, versus psychosocial/behavioral indicators, demonstrating how the combination of both data sources in a comprehensive C-InT approach can provide early warning, and greater opportunity for proactive mitigation that gets "left of boom."[3]

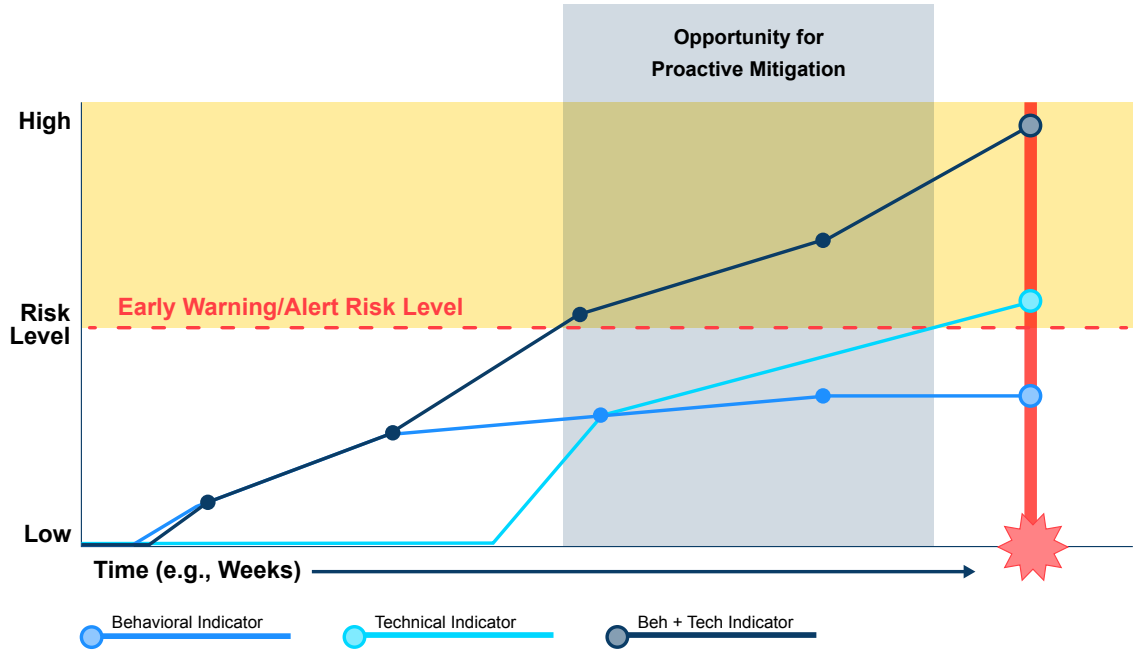

Figure 1. Sociotechnical (behavioral) data enables proactive mitigation to get "left of boom.

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

3 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.

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.[4,5,6]

The Federal Insider Threat Program was established in 2012 by Presidential Executive Order (EO) 13587.[7] Following this, the Federal agencies derived 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-InTP.

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[8] that was developed under a contract with the Intelligence Advanced Research Projects Activity (IARPA). Various government and commercial projects continue to advance this PRI knowledge base by 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.[9] These resources represent valuable guidance to understand and define insider threat behaviors and the basis for these behaviors.

4 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

5 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.

6 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

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

8 Greitzer, Purl, Leong, Becker (2018)

9 Shaw and Sellers (2015)

Cogynt Continuous Intelligence Platform with an Advanced Behavioral Analytic

Cogility offers a unified real-time platform that delivers continuous intelligence called Cogynt. Cogynt provides an advanced, big data and highly scalable behavioral analytic engine that can continuously monitor the behavior of many thousands or millions of entities and assess risk over extended periods of time. The ability to conduct this level of analysis, assuming the data and sufficiently detailed behavioral patterns are defined, allows for organizations and enterprises to conduct insider threat assessments of their employees and alerts C-InT analysts about concerning behavioral trends/potential risks so mitigating actions can be taken prior to a serious incident.

A readily configurable and adaptable continuous intelligence platform, Cogynt offers all the essential capabilities needed to augment and support a highly mature and effective Whole Person C-InT program that meets or exceeds best practices.[10] A logical depiction of the Cogynt URP architecture is shown in Figure 2.

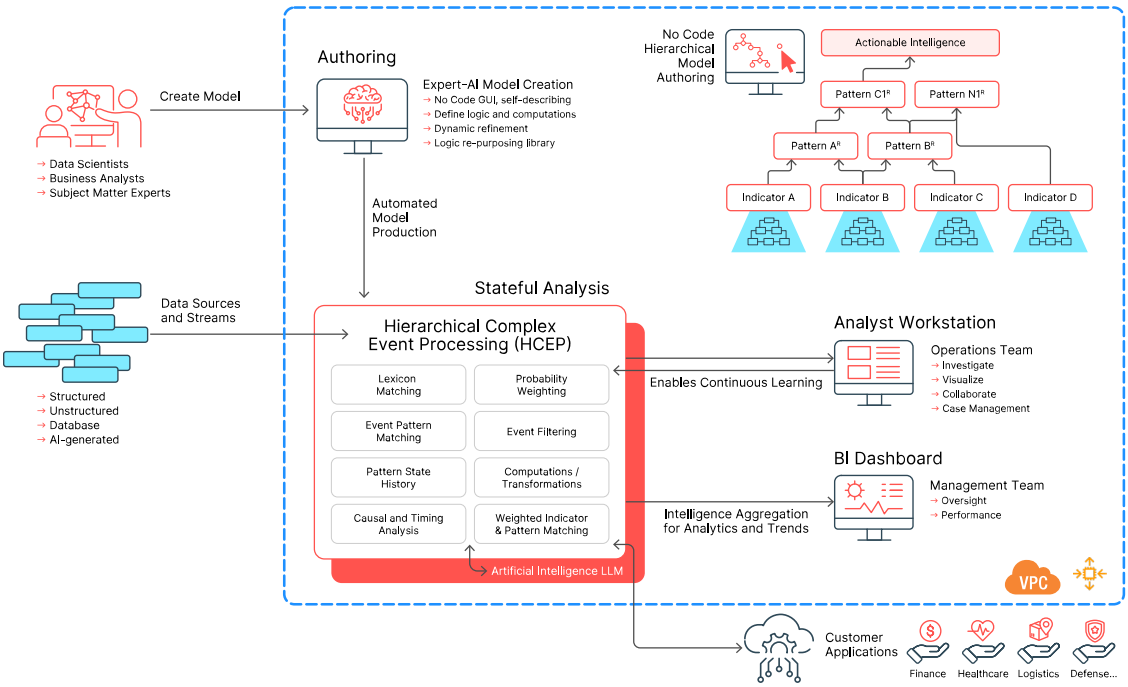

Figure 2. Cogynt URP architecture

10 Henderson, J., & Cavalancia, N. (2019). 2019 Insider Threat Program Maturity Model Report. https://cdn2. hubspot.net/hubfs/5260286/PDFs/Whitepapers/insider-threat-maturity-report-2019.pdf

The Cogynt URP components and their role within the architecture are:

- **Data Sources:** Streaming or batched data, including structured, unstructured, database and AI-generated data, are ingested via Apache Kafka connectors.
- **Cogynt Authoring Tool:** Used by the analyst to define/ manipulate lexicon, event patterns, computation logic, and risk models that comprise the Expert AI modeling created within a no-code GUI. Developed models are automatically produced for use in the HCEP engine.
- **Cogynt HCEP Analytic Engine:** Models are automatically configured within HCEP to produce analytic results that are streamed from Apache Flink to Apache Kafka and Apache Pinot for analytics and visualization. Results are displayed in the Workstation and Superset tools.
- **Analyst Workstation:** A dynamic and interactive user interface enabling the analyst to view insights, examine with widget apps, and trace predictive findings. Workstation enables the analyst to assess and add notation, as well as invoke extensive case management workflow features.
- **Artificial Intelligence LLM:** Forthcoming AI LLM will further enhance analyst experiences.
- **Business Intelligence (BI) Dashboard:** Provides overall performance and program oversight within a BI dashboard and enables access to any other preferred dashboards through Cogynt's open system architecture.
- **Applications:** As an open system, Cogynt insights can be shared with any event driven system or application.

Cogynt Behavioral Analytics and HCEP

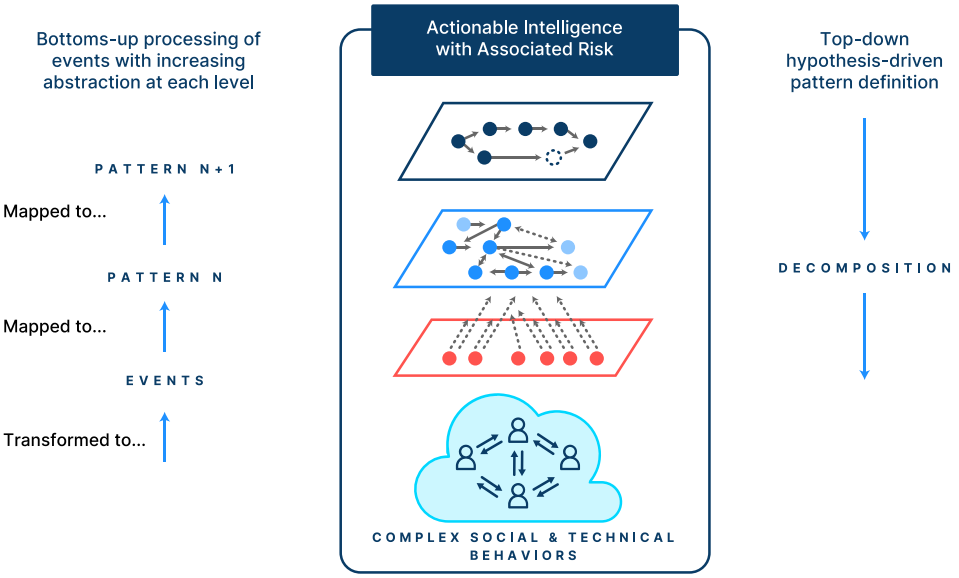

Figure 3. Hierarchical Complex Event Processing (HCEP)

The heart of Cogynt contains a patented behavioral analytic called Hierarchical Complex Event Processing (HCEP). The principles of HCEP are rooted in system theory[11] and CEP.[12] For insider threat, the solution models a whole person insider threat profile by defining all the relevant behavioral types that make up an insider threat profile. Within HCEP, the organic component of a behavior is an event pattern, and an event pattern follows the principles of CEP, where an event pattern, if fully matched, creates a new complex event that can trigger a higher-level event pattern. This process continues until it satisfies the full behavioral profile — hence the reference to Hierarchical in HCEP. In addition, HCEP allows for partial event pattern matches, which represents an indicator (or a collection of indicators) representing a behavior, but not a complete pattern of a definitive target threat behavior. Cogynt maintains the state of the event patterns over time, which allows analysts to look for trends and changes in behavior.

The general HCEP concept is represented in Figure 3. The top-level event pattern represents the whole person profile, and the lower-level patterns represent indicators (which are basically the "building blocks" of behavior patterns). The lowest level represents interpreted data, or observations, which are building blocks of indicators. Data or events are

11 https://en.wikipedia.org/wiki/Systems_theory#:~:text=Systems%20theory%20is%20the%20interdisciplinary,and%20expressed%20through%20its%20functioning.

12 https://en.wikipedia.org/wiki/Complex_event_processing

processed from the bottom up to infer observations from the real world consisting of people exhibiting sociotechnical behaviors. Initial pattern processing matches these observed events to potential risk indicators (PRIs); at a higher level of abstraction, collections of PRIs that comprise a case are interpreted and matched to behavioral patterns. These patterns are ultimately mapped to behavioral profiles for various insider threat types of concern. The ability to continuously assess a person's behavioral profile state and changes in the profile are key to predicting insider threats — and a critical facet of Cogynt HCEP.

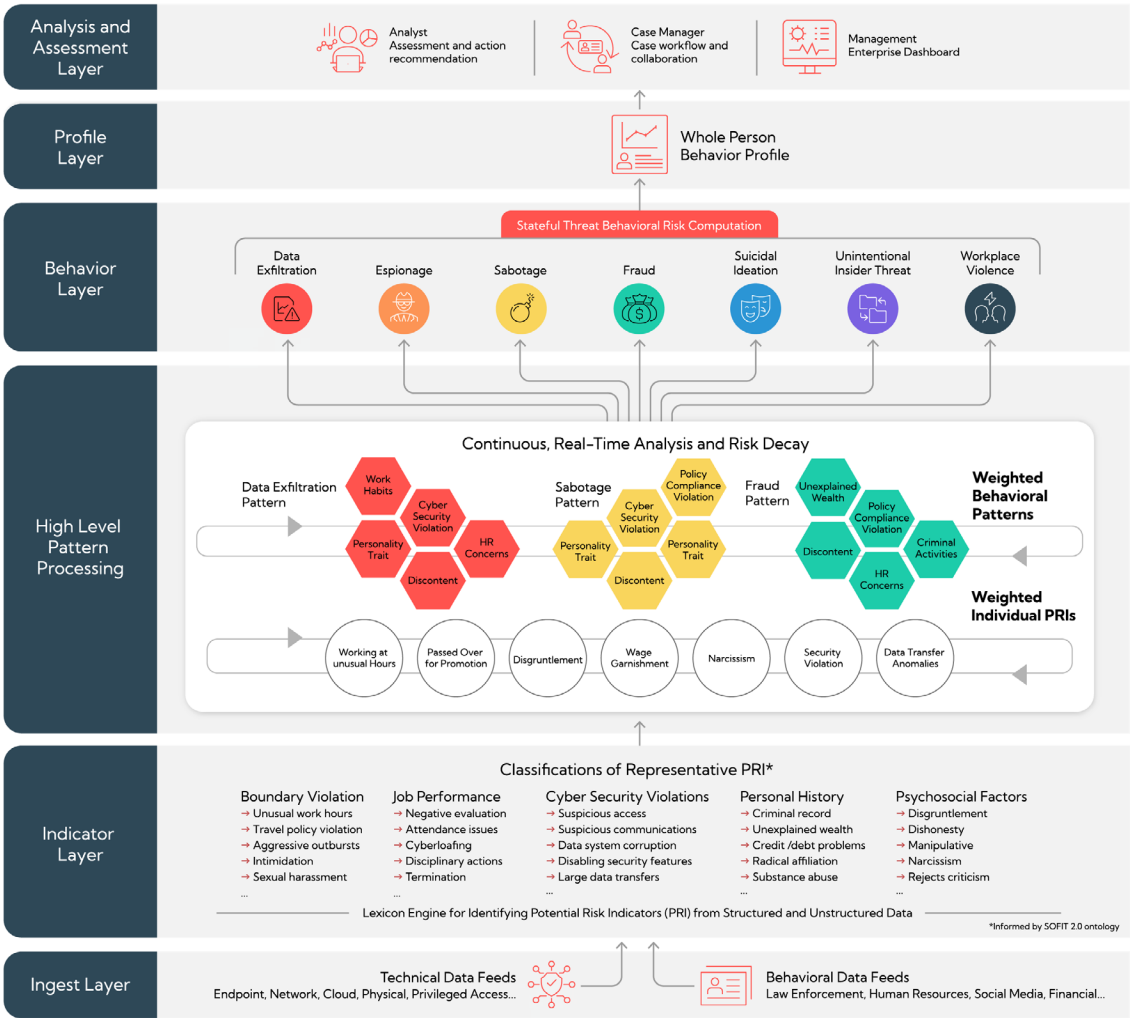

Figure 4. Cogynt C-InT Behavior and Risk Assessment in processing composite behaviors

Figure 4 represents layers of Cogynt behavioral analysis to achieve whole person C-Int management. Cogynt HCEP process as applied to insider threat. The figure depicts the matching process and continuous risk assessment where multiple threat-behavior types contribute to an individual's behavioral risk assessment, which is assessed and scored on a continuous basis. The mapping proceeds from PRIs to threat behavior types, with varying strengths of association between weighted individuals PRIs, weighted behavior patterns,

and insider risk behavior types. The mapping proceeds from lower level events are mapped to PRIs to higher level abstractions of patterns that reflect threat behavior types. These higher-level patterns represent collections of PRIs that, when observed together, provide stronger evidence (beyond the consideration of individual PRIs) that an insider threat incident is imminent or in progress.

In addition to HCEP analytics applied to compute risk based on individual PRIs, this enhanced analytic approach will identify the presence of higher-level patterns that further inform the calculation of risk. In summary, the relationships between PRIs and behaviors are dynamic — research suggests that there are complex, dynamic relationships among PRIs that produce different risk assessments when combined into various patterns.[13]

The powerful hierarchical complex event processing capabilities of Cogynt provide a unique approach to assessing insider threat risk in this complex environment. Cogility C-InT includes a foundation of PRIs, PRI patterns, and insider risk behavior models that can be customized, tuned, and expanded. Cogynt's complete no-code authoring environment allows for various logic and statistical weighting, including the use of statistical weighting computations. Furthermore, the modeling capabilities in Cogynt allow it to capture other dynamic qualities of PRIs, such as decreases in risk over time (risk decay).

Data or events are ingested and filtered using lexicons that define a PRI that is associated with a behavior (e.g., Workplace Violence) with an estimated risk weighting reflecting the extent to which the PRI is indicative of the behavior. The accumulation of risk is computed for every person/entity within the organization, and over time, these accumulated risk scores may be compared across the organization to identify individuals who are of greatest concern.

This concept of risk decay, which is currently under study in the insider threat research community, suggests that different types of PRIs may be subject to different decay parameters (e.g., those that relate to personality traits may be expected to be stable over time, while others that relate to more transient events such as network activity, may be subjected to more rapid decay in associated risk).[13]

13 Greitzer & Purl (2022)

Cogynt Analyst Support

HCEP is the workhorse that processes vast amounts of data and matches it with event patterns over time, notifying the analyst when a predefined behavioral threshold has been reached. Insider Threat scores associated per individual is continuously updated, which may be use to trigger actions. The Cogynt Analyst Workstation (Workstation) — shown in Figure 5 — allows the analyst to review this output, determine its accuracy, and instigate a workflow with other analysts or subject-matter experts — such as a psychologist or law enforcement professionals — to review the event and reach an informed decision.

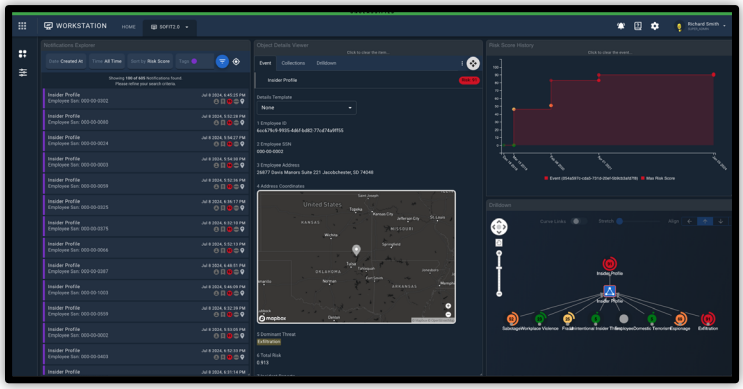

Figure 5. Cogynt Analyst Workstation

The Workstation provides a suite of flexibly configurable, interoperable tools or widgets that supports an intuitive and seamless analyst workflow to assess behavioral thresholds and build a case file. The analyst can upload files to support case management and export case file data to support external collaboration and communications. Extensive case management functions that boost analyst productivity include workflow customization, case assignment, delegation, assessment, annotation, collaboration, and reporting. The Workstation provides an assortment of visualizations such as link charts, maps, event drill down charts (event tree), and line charts for risk history that may be combined based on the user's preference.

Figure 6. Cogynt Superset for BI Insight Visualization

The Superset Tool (Figure 6) is another view — particularly of interest to stakeholders who need to see the big picture of data in the aggregate, or enterprise view. The Superset Tool provides a BI dashboard that allows users to interact with the data — i.e., the user can inspect an area such as a spike in risk or number of incidents and examine the source of incidents, such as based on the organization or geography. This can facilitate executive and management views to gauge case performance and overall program trends.

Conclusion

Insider Threat is a low probability, high consequence risk that organizations face daily. Over the past 10 years, this threat has gained the full attention it deserves to develop better tools for mitigating insider threat risk. A Whole Person C-InT program requires policies, instructions, and procedures on how to manage insider threat risk. A continuous intelligence platform with advanced behavioral analytic is needed to automate monitoring, identifying and predicting insider threats, supporting analyst assessment, and facilitating coordinated action — efficiently, effectively, and at-scale.

Cogility's Counter-Insider Threat solution, powered by its Cogynt URP, 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.

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