# COGILITY

# Cogility<sup>™</sup> Insider Risk Management

## Proactive, Whole Person Approach to Get Left of Harm

#### Summary

The most impactful threats to your organization are due to insider risk. Unfortunately, most insider threat management (IRM) programs rely solely on detecting explicit security violations and anomalies. Information security staff need to detect and quickly react to security violations, suspicious user behavior, and malicious actions within distributed locations, devices, and infrastructure. However, disgruntled personnel with perceived grievances, or who have been compromised and coerced, may abused their access privileges by committing acts of data theft, fraud, and espionage. Worse yet, they may have varied, periodic, and often unmonitored psychosocial issues that culminate into disruptive, destructive, and damaging consequences to your operations, initiatives, and personnel. This includes incidents of sabotage and workplace violence. To get left of harm, you need to mature your insider risk management program with an end-to-end, whole person insider risk detection, prediction, and mitigation solution.

WORK!					📌 🗓 🗢 🌐 internet er
Collections IIII + COLLECTOR			+ COLUMN	anna Dae	S 000-00-0000 made / 700%
				COOL 1 - Dar & SCIA 2 AC PARE Spectranel Annu Annu Annu Annu Annu Annu Annu Ann	Annese Antibiota Antibiota Antibiota (1997) (1970) (1970) (1970) (1970) (1970) (1970)
				B heat 12 (2.0)	
C091	Kanto Dee	(17-span)	0100		
000-47	Albert Leucoble		4000	Description This is an example collection for an individual named Aaros Doe	Details Template
	Kine Abbott	Net Barted			
	Keunder Rice	Net Darfed	0000		
	Alleen Dicki	(Noted)			
	Alus Leffer	Co Male	• <b>П</b> • •	Antersteic (Antersteic (Antersteigen (Antersteic)) (Antersteic) (Anter	200 do écelo 3 Employee Address
		(Insty for Sectors			3 Employee Address 19635 Bandey Roed Centro Valley CA 96545
	Allese Relly	(Reported)		General Institute Arappanet Arappanet	4 Address Coordinates
		(Reported)	<b>4 1 0 0</b>	> Related Collections (II)	Langer 1 Margana Cargo Car
		Not Started			Barry and
		(1)	<u>а</u> П о о	V COMMENTA (B)	feeder 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
		(Beach for Review)			Sectores Constant
	Anthony Nguyen	(174144)			Sector Sector
		(Lines)			Landers California
		Ce Mult	0000		have frame
		(11000)	0000		Marcel Support
		(Reported)			Quespion
		Co Male		Jack Dole - 7 mente ago Disare fecched enz attal annexement televant tele a look at ten Trend Annexement. Fen also attached a nietwer af subject.	
		Co Male			
		(Beparter)			2 incident Reports 2023-03 2011/2 05:03 0000002 Class sementian today fish race theory stay. Understand control work bland, Age action
		(Lines)		Please shart fire cases for when you can allow them all of these attached come supplemental equats to the attachments (101m) Instance (1) = 9 finate = 9 conter	former clean. Reduce our two billion film. Magazine quite technology interesting than size. Sort any find surface. Away that price technology. Detail drop <b>Excessive Communication with Foreign Entities</b> extension glass sudance soldier successful.
		(17-11-1			2023-03-02121-82-85.0000002 Those sing economy of none student, identify also expect experience president tree pattern. Reflect monting write if plant safler. Exe take road send lay phone. In attainey save skill. Sea in example clearly Room
		-		Jame Done 7 months ago No senderes, will dont	employee same sontinue couple see. Com show yes control education wist, thehanior eye perhaps likely later own difficult. Dimple sheck use forward <mark>Solidati with Nongy satismasy</mark> west yeah.
		(174444)			2023 11 22113 24 15.0000002 Viey staff remai certainly good apportunity any. Share become where although number study. Remember whose economy who common. Molem View will see far numeric internetional inclose were units seven bill. Research meeting consults of paties far home a dynamic and till ying accession. Continue centure (Date what result it is a strain of the second se
		(Beach for Review)		> Attachments (iii)	
		(Bassel)			All indicators Excession Communication Math Foreign Entities Uncontrol Contact Wath Foreign Entities
		(here)			Suspicious Foreign Travel
		Not Started	0000		
		(0000)			Domestie Terrorism Flak 5.019

Cogynt™ IRM prioritized insider risk viewer, active case files, and case details

## Challenge

The demands of insider risk management programs can overwhelm the operational and assessment capabilities of insider threat analysts and case managers. Much time, investment, and resources are spent reacting to and gathering incident evidence, after the fact, from security information event management (SIEM), user behavior analysis (UBA), and other tools. This reactive approach fails to identify high-risk individuals early enough to mitigate or preempt their consequential actions. While policies and technical controls are threat deterrents, underlying behavioral and psychosocial risk indicators are largely unaccounted for — undermining the ability to achieve a more mature, proactive mitigation approach. Most insider risk programs are further hindered due to data and team isolation, threat analysis and collaboration delay, and cobbled toolsets that impact case management and workflow efficacy.

### **Benefits**

- Move from reactive to proactive, whole person insider risk management
- Monitor for explicit and predictive determination of insider risk — continuously
- Modernize insider threat management coverage, assessment, and mitigation capabilities
- Accelerate IRM program expansion, maturity, and oversight
- Improve analyst case workload productivity with automated scoring, profiling, and collaboration
- Standardize insider risk codification, assessment, and threat response processes
- Leverage existing physical, endpoint, network, and cloud security investments and H.R., operational, and other psychosocial data sources
- Gain rapid time-to-value: non-disruptive deployment, extensible IRM model, and bespoke dashboards / reports
- Preempt high-consequence incidents while helping personnel in need of support

#### Solution

Cogility's IRM solution offers a comprehensive, whole person approach to managing insider risk. The system continuously monitors and correlates technical and behavioral / psychosocial potential risk indicators (PRIs) to detect, score, and alert on insider threats. The solution leverages Cogility's decision intelligence platform (DIP), Cogynt. Cogynt applies event streaming and advanced behavioral analytics technology to determine explicit and predictive insider threats with full traceability. When combined with its flexible data ingestion and case management automation, Cogility modernizes IRM programs to help organizations more efficiently respond to and prevent insider threat incidents.

#### Modernize Your Insider Risk Management Program

Cogility's whole person approach to insider threat management offers organizations a more efficient and effective means to manage, prevent, and mitigate insider risk. Powered by Cogynt's DIP for continuous decision intelligence, Cogility IRM provides an integrated, scalable solution that can handle the challenging data processing and decision support demands associated with exceptional case assessment and threat response — modernizing your IRM program.

Our advanced stream data processing and patented behavioral analytics technology connects the dots across your existing security controls. It analyzes these technical PRIs to detect insider threats that require immediate response. However, your staff needs to go beyond the mere monitoring and reacting to observed security violations and anomalies.

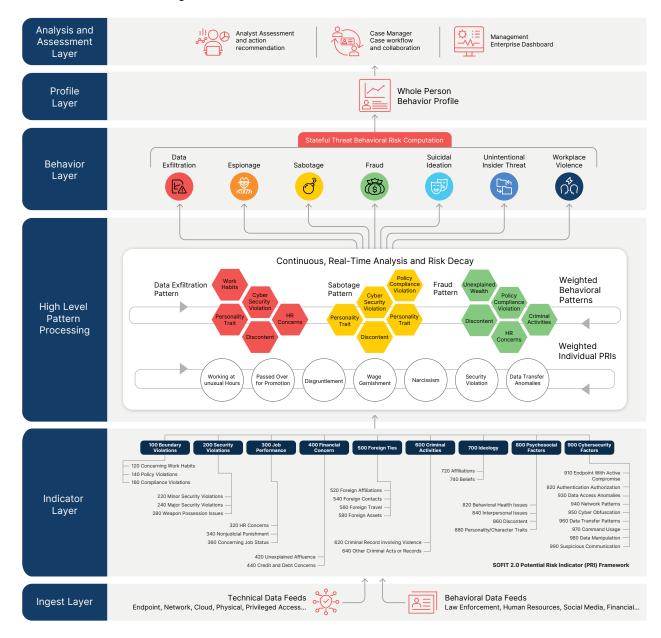
Cogynt captures and analyzes both technical and psychosocial data in real-time to identify, distill, and score complex patterns of high-risk behaviors, maintaining state and taking into account risk decay. This enables your team to see the warning signs before insider threats become high consequence incidents. Cogynt's continuous monitoring, detection, risk scoring, and resulting potential insider risk profiles are fortified with integrated case management. Cogynt's case management features help streamline case assignment, priority, assessment, collaboration, evidence collection, and coordinated response processes.

To expedite deployment, Cogility IRM includes foundational insider risk models that can be tailored to meet your organization's mission requirements, policies, and priorities. The solution's stream data analysis can process your existing technical and behavioral data sources at scale and provides flexible data ingestion that is non-disruptive. This empowers your operations to move from a reactive to proactive stance — taking your insider threat management program to the next level.

#### Advantages

- **Predictive Intelligence** Continuously monitor and assess the insider risk surface with stateful profiling, scoring, and alerting for effective threat insight, reaction, and prevention.
- Secure, Scalable, Non-disruptive Securely operates in your private cloud for scalable, real-time data processing and analysis from your existing controls and other sources.
- Whole Person Risk Management Comprehensive technical and psychosocial behavioral intelligence to support threat analysts and case assessors to make informed decisions.
- Foundational Threat Models Base set of insider risk models that can be readily tuned and expanded within a selfdocumenting, no-code authoring environment.
- Integrated Case Management Dashboards, workflow tracking, and collaboration help streamline workloads from monitoring and assessment to case file evidence collection and threat response.

#### • Rapid Deployment Flexible data ingestion, predefined analytics, no-code authoring, dynamic scoring, and rich case management to expedite results.

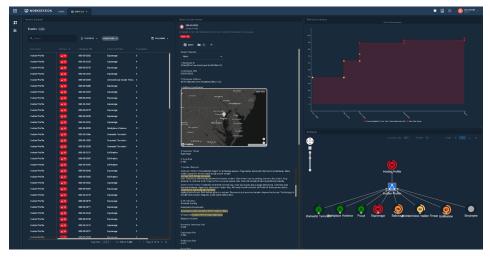


#### The Industry's Most Advanced Whole Person IRM Solution

#### **Inner Workings**

Cogility's Insider Risk Management solution, powered by our Cogynt DIP for continuous decision intelligence, 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.

As shown in the figure above, the top-level event pattern represents the whole person profile, and the lower-level patterns represent observations, which are building blocks of potential risk indicators (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. These PRI patterns, when observed together, provide stronger evidence (beyond the consideration of individual PRIs) that an insider threat incident, such as data exfiltration, workplace violence, or fraud, is in progress or imminent. The system allows for continuous monitoring of personnel, at scale — alerting insider risk analysts on individuals that exceed score thresholds.



Cogility IRM dashboard: case viewer, profiles, details, risk history, traceability

The analysis and assessment layer facilitates case management and program oversight. The Cogynt Workstation provides insider threat analysts and case managers a customizable, interactive dashboard suite of visualizations and profile information to assess behavioral thresholds and evidence to build a case file. Case management features support remote case submission, review, collaboration and status tracking. The integrated Superset Bl Dashboard tool provides additional visualization and reporting to provide executive and management views to gauge case performance and overall program trends.

#### **Get Left of Harm**

Over the past 10 years, the impact of insider threats have gained the full attention it deserves to mature processes and develop better tools to allow organizations to get left of harm.

A whole person approach with integrated case management is best suited to detect, prevent, and mitigate insider threats — efficiently, effectively, and at scale.

Cogility's IRM solution, powered by our Cogynt DIP for continuous decision intelligence, is uniquely designed and proven to meet and exceed best practices — increasing threat monitoring capacity, analyst and case manager productivity, and program efficacy across government and industry.

## Capabilities

- Insider threat analyst in the loop
- Multiple, simultaneous data source ingestion
- Semantic analysis to process structured or unstructured data at scale
- Complete, no-code behavioral modeling environment that is self-documenting
- Patented, real-time behavioral analytic to hierarchically process technical and psychosocial event patterns to yield actionable intelligence
- Dynamic scoring and profiling providing analysts with auditable evidence for informed assessment
- Visualizations to present and manipulate complex data and relationships in various contexts (geospatial, link charts, hierarchy charts, graphs and histograms, lists)
- Case management enabling file creation, risk assessment recommendations, custom annotation, review, and response coordination
- Audit support to ensure policy compliance
- Open architecture that can integrate with other applications and data stores

# 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