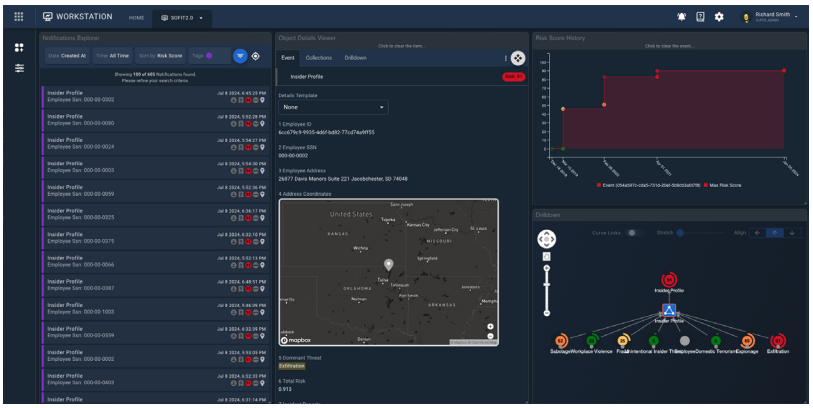
COGILITY

Cogility™ Counter-Insider Threat

Proactive, Whole-Person Insider Risk Management

Summary

Most counter-insider threat (C-InT) programs rely solely on detecting explicit security violations and anomalies. This reactive approach fails to identify high-risk individuals early enough to mitigate or preempt their actions and damage. Security staff need to detect and quickly react to violations, suspicious user behavior, and malicious actions that are identified by technical risk indicators. However, disgruntled personnel with perceived grievances, or who have been compromised and coerced, may abuse their access privileges by committing acts of data theft, espionage, 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 C-InT detection, prediction, and mitigation solution.



Cogility C-InT dashboard: case viewer, profiles, details, risk history, traceability

Challenge

The demands of insider threat management can overwhelm the operational and assessment capacity of insider threat analysts and case managers. Much time, investment, and resources are spent reacting to and gathering evidence on incidents after-the-fact. 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 threat 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.

Solution

Cogility's C-InT 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 unified real-time platform (URP), 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 C-InT programs to help organizations more efficiently respond to and prevent insider threat incidents.

Benefits

- Move from reactive to proactive, whole person insider threat management
- Monitor for explicit and predictive determination of insider threats - continuously
- Accelerate C-InT program expansion, maturity and oversight
- Extend insider threat coverage, assessment, and predictability
- 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
- Enable more efficient insider risk assessment and informed threat mitigation
- Preempt high-consequence incidents while helping personnel in need of support

Modernize Your Counter-Insider Threat Program

Cogility's whole person approach to Counter-Insider Threat management offers organizations a more efficient and effective means to manage, prevent, and mitigate insider risk. Powered by Cogynt URP for continuous intelligence, Cogility C-InT 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 C-InT 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 C-InT 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.

Get Left of Harm

Over the past 10 years, the impact of insider threats has 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, preempt, and mitigate insider risks — efficiently, effectively, and at scale.

Cogility's C-InT solution, powered by our Cogynt URP for continuous 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.

Advantages

Predictive Intelligence
Continuously monitor and assess the insider risk surface with stateful profiling, scoring, and alerting for effective threat insight, reaction, and prevention.

Whole Person Risk Management
Comprehensive technical and psychosocial behavioral intelligence to support threat analysts and case assessors to make informed decisions.

Integrated Case Management
Dashboards, workflow tracking, and collaboration help streamline workloads from monitoring and assessment to case file evidence collection and response.

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.

Foundational Threat Models
Base set of insider risk models that can be readily tuned and expanded within a self-documenting, no-code authoring environment.

Rapid Time-To-Value
Flexible data ingestion, pre-defined analytics, no-code authoring, dynamic scoring, and rich case management to expedite results.

Unified Real-Time Platform
Offering a complete URP, Cogynt integrates and augments event streaming, advanced analytics, investigation, visualization, and case workflow to deliver continuous intelligence for C-InT.

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

 08/24