Trusted AI Decision Intelligence Support for Nuclear Material Accountability and Control

Frank L. Greitzer, Cogility Software
fgreitzer@cogility.com

COGILITY
www.cogility.com
Related materials are available on the website.

Abstract: Despite significant investment in technical safeguards, the nuclear industry faces challenges detecting human-centric threats to nuclear material control and accountability (MC&A), including information theft, sabotage, nuclear material diversion, and unintentional errors. The high safety, regulatory, and geopolitical demands of the nuclear domain require more mature, human-centric risk models that exceed compliance-focused controls. Traditional perimeter defenses and cybersecurity tools often fail to identify early behavioral risk indicators, leaving analysts in a reactive posture. Effective solutions require proactive strategies that provide timely, reliable, and explainable analytic assessments. This highlights the need for a behavioral-science-driven approach that identifies behavioral indicators of stress, complacency, poor security culture, or malicious intent when assessing anomalies in user behavior, access patterns, and material handling.

The Human-Centric Challenge

Despite major investments in technical safeguards, nuclear MC&A programs remain vulnerable to human-centric risks that evade early detection.

Information Theft
Unauthorized access to sensitive nuclear data

Material Diversion
Theft or misrouting of nuclear materials

Sabotage
Deliberate damage to systems or processes

Unintentional Errors
Human mistakes with safety consequences

Barriers to a Whole-Person Insider Risk Approach

- Fragmented data and organizational silos
- Governance and ownership gaps
- Privacy, trust, and acceptability concerns
- Reactive operating models
- Resource and tooling constraints

Decision Intelligence and Expert AI Analytics

Fusing behavioral science, cyber-physical signals, and organizational context into explainable, auditable decision support.

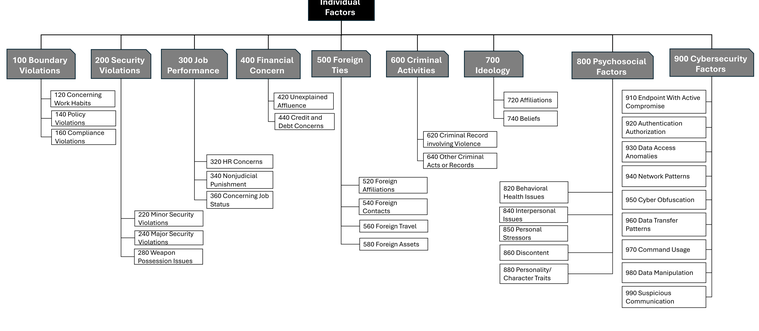
Comparing Threat Assessment Approaches

Expert AI Analytics with hierarchical pattern-based structured reasoning and human oversight excels in modeling expert judgment with a scalable solution that is explainable by design.

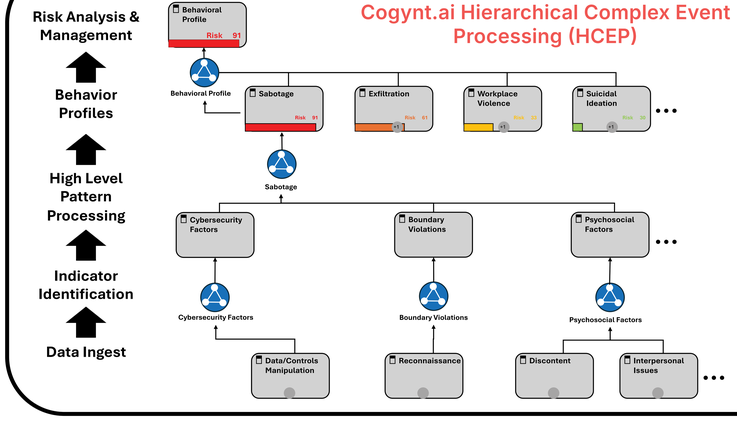
	Expert Model	Transparency	Scalability
Qualitative Models • Analyst Judgment • "Counting" Models	●	◒	●
Quantitative Models • Probabilistic (e.g., Bayesian)	◒	●	◒
Machine Learning (ML)	◒	●	○
Expert AI Behavioral Analytics Integrating AI and Quantitative Modeling	●	●	●

SOFIT

Structured knowledge base of behavioral/ psychosocial, organizational, and technical/ cybersecurity contributors to insider risk



Cognyt.ai Expert AI Analytics



Conclusions

Effective insider risk mitigation requires the ability to recognize early risk patterns across human behavior, operational context, and cyber-physical activity.

Benefits

- Early Detection
- Reduced False Positives
- Strengthened Security Culture
- Cross-Functional Collaboration
- Regulatory Alignment

The Cognyt.ai expert AI decision intelligence platform provides a scalable, explainable behavioral analytic solution to support whole-person risk assessment. With appropriate governance, privacy safeguards, and human oversight, this capability can elevate nuclear security from reactive to proactive, more proportionate, and more resilient insider risk management.