MITRE | Insider Threat Research & Solutions™

https://insiderthreat.mitre.org

Managing insider threat risk using the behavioral, data, and cyber sciences to understand cyber-physical and psycho-social aspects of people, programs, indicators, analysis, and data

About Us

MITRE's Insider Threat Research & Solutions helps sponsors manage insider risk through rigorous, evidence-based approaches grounded in behavioral science, data science, and cyber science.

Our solutions are based on 20 years of applied research and practice through standing up, working in, and working with insider threat and risk programs across government, industry, and research security in the US and Five Eyes community.

Our Approach and Experience

We develop frameworks, indicators, methodologies, mitigations, and analytic approaches to enable organizations to better interpret and reduce the risk of harmful acts by trusted insiders. Our work spans both malicious and non-malicious insider risks including espionage, intellectual property theft, unauthorized disclosure, sabotage, fraud, workplace violence, negligence, mistakes, and employees outmaneuvered by adversaries.

Insider threat requires a human solution, not just a technical one. We bring a uniquely multidisciplinary approach to insider threat, combining science, applied research, operational program experience, and deep engagement with the insider threat community. We put science into the equation to help organizations deter, detect, and mitigate insider risks more effectively. We develop our data-driven solutions through research methods including applied behavioral experiments, structured interviews, systematic questionnaires, benchmarking, tool evaluation, and secure quantitative and qualitative analysis of real-world insider risk and personnel vetting data.

Our team has experience working with insider risk programs across government agencies and critical infrastructure sectors, including finance, energy, healthcare and biopharma, retail, transportation, communications, technology, research security and higher education, and the defense industrial base.

Core Capabilities

Detection & Indicators

Develop and evaluate data-driven indicators and analytic methods to help distinguish higher-risk behaviors, cases, and patterns from benign activity. Assess the effectiveness, rigor, and operational value of existing detection approaches and tools.

Deterrence & Mitigation

Design interventions to reduce insider risk by influencing attitudes, intentions, decisions, and behaviors. Our work applies behavioral science to improve workforce awareness, reporting, resilience, and protection of people, information, and assets.

Program Design & Development

Help sponsors build, grow, and mature insider threat/risk programs through reviews, assessments, roadmaps, and practical recommendations. Support decision-making on governance, scope, data sources, stakeholders, use cases, and program priorities.

Personnel Vetting

Apply behavioral analysis and data sciences to vetting and background investigation data to identify patterns, flags, and indicators that improve risk-informed personnel and entity security decisions.

Data & Analysis

Lead insider threat community in deriving operational value from sensitive insider threat data across human, organizational, cyber, and physical sensors, using structured analytic methods and secure handling practices for employee-generated data (including human employees and AI employees).

MITRE

Highest Demand Research, Methods, and Solutions

MITRE Behavioral Risk Framework for Analysts
Living, evidence-based analytic thinking tool for analysts to operationalize key insider risk concepts, consider overlooked indicators, and maintain a whole-person perspective during inquiries and reviews.

UAM Potential Risk Indicators and Models
Proactive models of cyber activities for User Activity Monitoring (UAM of elevated insider risk: malicious employee information search and collection; harm to institutional safety and integrity; sexual assault and harassment; suicide risk; and remote workers.

Program Roadmaps and Reference Manuals
Tailored, sector- and organization-specific implementation plans and recommendations for building, growing, and maturing insider risk programs over time.

Critical Assets Risk Assessment for Insider Threat
Methodology to identify/prioritize organization's highest-value human, cyber, and physical assets for insider risk.

Position Risk Designation Methodology
Tailored methodology to identify the risk level for positions and roles (not people), that could present risk to the organization, its reputation, and its current or future work.

Insider Risk Tool Requirements and Test & Evaluation
Rigorous methodologies to set comprehensive requirements and evaluate/ compare analytic tools (UAM, sentiment analysis, and credibility assessment).

Industry Threat Scenario Development: Methodology to generate sector and organization-specific vulnerability and threat scenarios for insider risk programs based on insights directly from benign frontline employees.

Known Unauthorized Disclosures Database
Curated dataset and analysis of known espionage and leak cases to identify recurring characteristics, patterns, and lessons relevant to insider threat and risk programs.

Personnel Vetting Behavioral Analysis Dataset
Structured BABI dataset and analysis of 45,000 background investigation cases to identify behavioral patterns, flags, and indicators to support more informed personnel vetting.

Cyber Evasion and Exfiltration Techniques Catalog
Empirically-based catalog of malicious insider exfiltration and evasion techniques by real employees on live network.

Employee, Supervisor, and Research Security Reporting
Evidence-based methods, tools, and guidance to improve quantity/quality of insider risk recognition and reporting by employees, supervisors, and partners—including foreign recruitment and malicious elicitation in email and online.

Psychological Financial Strain (not Debt)
Identification, testing, and evaluation of indicators of high psychological financial strain rather than material debt alone, which fails to capture level of worry about finances.

Bi-Directional Loyalty (BDL)
Concepts and measures assessing mutual loyalty between employees and organization to help identify at-risk groups.

Operationalizing and Validating Observable Psycho-social Detectors and Deterrence for Human Sensors
Common characteristics of known spies (Project Slammer); research on positive factors to lower employee risk scores; employee tolerance of workplace aggression/violence findings; and remote-worker risk deterrence.

Coming Soon! —*As insider threat thought leaders, we continue to conduct applied research and develop new solutions.*

- ❑ **MITRE Insider Threat Framework Initiative:** Data-driven insider threat framework using real industry case data with psycho-social and cyber-physical characteristics to improve operational detection, analysis, and mitigation.
- ❑ **Defensible Thresholds for Insider Risk and Personnel Vetting:** Systematic, evidence-based guidance for setting thresholds for concerning activities and events in insider risk, personnel vetting, and continuous vetting to help reduce false positives, improve consistency, and support defensible risk decisions.
- ❑ **Insider Risk Masterclass:** In-person training for leaders implementing insider risk programs, covering essentials of insider risk management, program governance, managing stakeholders, tackling misconceptions, triaging alerts, conducting evidence-based analyses, assessing program impact, and leveraging external relationships.
- ❑ **AI and Insider Threat Nexus:** How can malicious insiders use AI to evade current/future PRIs or exfiltration detectors? How can AI advance insider risk program PRI and detection capabilities? How can insider risk programs effectively monitor and detect "AI Employees"? How can AI improve personnel vetting?

MITRE Insider Threat Lab (InT Lab)

The MITRE Insider Threat Lab is a secure, air-gapped facility built to curate and extract value from sensitive insider threat and personnel vetting data shared by government and critical infrastructure partners. Since 2019, MITRE's multidisciplinary team has used the lab to receive, store, process, clean, structure, analyze, collate, and interpret insider threat data across cyber, physical, human, and organizational sources. The facility is NIST 800-171, CMMC, and GDPR compliant with data protected through physical, information, personnel, and contractual safeguards.

Point of Contact: Dr. Deanna D. Caputo, MITRE Chief Scientist for Insider Threat Research & Solutions
Phone: 703-983-3846 | Email: dcaputo@mitre.org | Website: https://insiderthreat.mitre.org