MITRE | Insider Threat Research & Solutions™

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

About Us

MITRE's Insider Threat Research & Solutions has developed rigorous and data-driven frameworks, indicators, methodologies, mitigations, operational successes, and thought leadership to reduce the risk from harmful acts undertaken by trusted employees inside an organization. MITRE's subject matter expertise uniquely spans a spectrum of harmful cyber and non-cyber (behavioral) insider incidents that our sponsors face daily, including those from malicious or non-malicious employees (e.g., negligent, mistaken, or outsmarted). Our solutions are based on over 15 years of scientific research and standing up insider threat programs. We put science into the equation.

MITRE knows that insider threat requires a human solution and not just technology. We uniquely harness both behavioral sciences and cyber sciences to more effectively deter, detect, and mitigate insider threats. Our multi-disciplinary team consists of 20 researchers and practitioners who have worked in insider threat programs in government and critical infrastructure organizations, and/or have significant expertise applying the behavioral sciences, cybersecurity, data sciences, and intellectual property protection to insider risk.

Building, growing, and maturing insider threat programs for government, industry, and academia, the MITRE Insider Threat Research & Solutions team is recognized as national and international experts. Our work is sought out for consultations, partnerships, and presentations.

Capabilities

Detection and Indicators
We develop and hone a set of research methodologies to identify and evaluate potential risk indicators of insider risk and threat. We offer objective feedback on the relative cost-benefit of solutions for insider threat programs, and a thorough evaluation and comparison of third-party tools.

Deterrence and Mitigation
We are experts in producing interventions that aim to deter or mitigate insider risk within government agencies and critical infrastructure industry. We leverage cutting-edge behavioral and cyber sciences to create meaningful behavior change to protect people, information, and assets.

Program Design and Development
We review, evaluate, and make actionable recommendations for paths forward for sponsors looking to build, grow, or mature state-of-the-art insider threat programs. This includes core decision points they will reach, and how to overcome key challenges and misconceptions.

Screening and Vetting
We are conducting behavioral analysis of a large quantity of existing derogatory background investigation data to identify data-driven patterns in critical behavioral flags, develop validated novel indicators, and identify most appropriate data sources for risk decisions.

Our Research

Program Design: Reviewed all practices from 20 industry insider threat programs in detailed benchmarking report.

Indicator Design: Developed a methodology to identify novel cyber indicators that differentiate malicious from non-malicious employee-generated computer activity.

Psycho-social Characteristics: Identified a large set of psycho-social characteristics of known spies and operationalizing these into data-driven proactive indicators.

Tool Evaluation: Developed a methodology to evaluate and compare the effectiveness of data analytics tools (e.g., sentiment analysis in email, User Activity Monitoring).

Employee Reporting: Created and tested a methodology to derive insights about real employee reporting of insider risk (or lack of). Developed training and awareness guidance.

Supervisor and HR Reporting: Created low-burden tools to increase quantity and quality of insider risk reporting by supervisors and HR.

New Data Sources: Developed a methodology to generate vulnerability and threat scenarios for insider threat programs based on insights directly from benign frontline employees.

Remote Work Indicators: Identified cyber indicators, key risks, and challenges that differentiate malicious from non-malicious employee behavior specifically in remote working.

Psychological Financial Strain (not Debt): Identified, tested, and evaluated indicators of high psychological financial strain, rather than material debt which fails to consider level of worry about finances.

Protective Factors: Identified and evaluated positive factors that can be used to lower an employee risk score (e.g., signs of coping or resilience).

Post-incident: Developed an interview protocol for interviewing malicious insiders post-incident to generate new insider threat characteristics and indicators.

Critical Assets Risk Assessments: Developed a methodology to identify and prioritize the highest value insider threat human, cyber, and physical assets in organizations.

Position Risk Designation: Tailored a methodology to identify the level of risk associated with positions (not people) that could present risk to the organization, its reputation, and/or its current and future work.

COMING SOON

MITRE is a thought leader in insider threat and currently conducting applied scientific research and developing new solutions:

- **Insider Threat Framework Initiative:** Creating the first data-driven framework that includes psycho-social and cyber-physical characteristics as common and observable indicators from real government and industry insider threat investigations (Planning for over 5,000 cases).
- **Domestic Extremism:** Developing detectors of workforce domestic extremism for use by insider threat programs.
- **Workplace Violence:** Creating a methodology to research expectations and tolerance of escalating employee aggressive behaviors in the workplace, to develop recommendations to improve risk identification and reporting.
- **Deterring Malicious Elicitations:** Testing effectiveness of skills-based training to protect the workforce against foreign influence and interference.
- **Bi-Directional Loyalty (BDL)**: Refining a more suitable and practical measure of risk than organizational commitment, developing and testing measurement methods, and creating a future research plan.
- **Sector-Specific Reference Manuals:** Generating insider threat scenarios and developing bespoke insider risk programs and practices for individual critical sectors (e.g., energy, higher education, transportation).

MITRE Insider Threat Lab (InT Lab)

The InT Lab is a secure, air-gapped MITRE facility built for curating and extracting value from sensitive insider threat data shared by the insider threat community in government and critical infrastructure industry both nationally and internationally. Since 2019, our multi-disciplinary team has used the InT Lab to receive, store, process, clean, structure, analyze, collate, and interpret insider threat data from across cyber, physical, human, and organizational data sources. The InT Lab is NIST 800-171 compliant and the data within are protected by stringent physical security, information security, personnel security, and contractual safeguards.

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