MITRE | Insider Threat Framework Initiative

MITRE is creating an evolving, data-driven Insider Threat Framework that includes cyber-physical and psycho-social characteristics as common and observable indicators for insider risks.

How Will The Framework Be Created?

MITRE will create the Framework by analyzing raw insider threat case data contributed by government and industry organizations. All received sensitive data is processed and analyzed in an access-controlled, closed-network MITRE Insider Threat Lab. There, a team of behavioral scientists, insider threat subject matter experts, data scientists, and cyber security engineers continually aggregate, consistently structure, hand-code, and analyze the data.

The team will identify nation-level and sector-level patterns and trends. The framework–but not the raw or aggregated data–will be discreetly shared with vetted insider threat community leaders on a need-to-know basis (i.e., the framework will not be publicly accessible). MITRE plans to transition the findings via no-cost licensing agreements to make our nation and the world a safer place.

Are There Any Existing Insider Threat Frameworks?

No, there are currently no data-driven comprehensive threat frameworks for insider threat. While there have been some attempts to develop conceptual threat frameworks for insider threat, those efforts are generally based on assumptions, or have limited or no utility due to inadequate data quantity and quality. Most existing frameworks fail to account for both behavioral and cyber aspects of insider threat.

Can We Use Existing Threat Frameworks For External Adversaries?

Threat frameworks for external adversaries do not work for insider threat. Insider threats simply act differently than Advanced Persistent Threats (APTs). Malicious insiders know how to leverage organizational processes to meet their objectives, obfuscate malicious activities inside their legitimate work activity, and take actions that do not require them to directly interact with cyber systems or break rules. Malicious insiders engage in more than just cyber activities, and any credible, effective insider threat framework must account for the cyber, physical, organizational, and human components of insider threat.

How Do I Contribute Data?

For organizations interested in contributing data to the Insider Threat Framework Initiative, MITRE will work with you to secure approvals within your organization. We are experienced in briefing the importance of the framework initiative including data protections, return on investment, and setting clear expectations about the types of data needed for success. Our briefing also emphasizes the security of our lab to C-suite executives and governance boards who understandably must approve sharing sensitive organization data. Minimal preparation of the data is required.

Will My Data Be Secure?

We will work with you to transfer the data securely to our access-controlled, air-gapped MITRE Insider Threat Lab. The Lab is NIST SP-800-171 compliant and secured by stringent physical, personnel, contractual, and information security controls.

How Much Data Do I Need?

Any number of cases is valuable. There is no such thing as "not enough data" to contribute. For example, some organizations have sent five cases and others provided fifty or hundreds of cases. We only ask that cases be closed, rather than in-progress, to preserve the integrity of any ongoing investigation processes for your organization and your employees.

Why Do We Need A Framework?

Once completed, the MITRE Insider Threat Framework will help government and industry organizations improve their insider threat capabilities and use evidence in the following ways:

- **Data-driven design:** Design, target, and deploy deterrence, detection, and mitigation efforts based on evidence.
- **Prune your program:** Discard or modify efforts that are found to be ineffective or even counterproductive.
- **Secure support:** Use evidence to build support more effectively from key organizational stakeholders and data/resource owners (e.g., legal, human resources, security).
- **Proactive risk detection**: Identify patterns and changes in behavior to detect malicious insider risks before they become a threat.
- **Verification:** Verify deterrence, detection and mitigation processes work as expected.
- **Informed risk-taking:** Assess whether program design decisions are appropriate.
- **Focus and assess vendors:** Proactively drive the commercial vendor marketplace and better assess what you need and if a given vendor fulfils that need.

What Are The Benefits Of Contributing Data?

Your organization has the opportunity to contribute to the cutting-edge of insider threat science and practice. Sharing case data will accelerate the development of the framework and benefit your organization in the following ways:

- **Representation:** Improve the applicability of the framework structure and findings to your organization.
- **Engage expertise:** Early access to the evolving framework and the insight and experiences of MITRE's behavioral sciences and insider threat subject matter experts.
- **Community of interest:** Engage with – and learn from – Insider Risk/Threat Programs across your and other sectors.
- **Proactive responsibility:** Insider threat is not just a corporate problem – it is a national responsibility. Your organization can demonstrate leadership in this critical field.

For more information, please contact:
Dr. Deanna D. Caputo, MITRE's Chief Scientist for Insider Threat Research & Solutions
Email: dcaputo@mitre.org / Telephone: 703-983-3846