ADVANCED CYBER SECURITY CENTER

Insider Risk Programs: MITRE Research and Resources

Cyber Risk Governance Executive Practice Guide Addendum

June 2024

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

ADVANCED CYBER SECURITY CENTER

MITRE's Anonymized Database: Tracking Insider Risk Detection Collaboratively

Suneel Sundar, head of public sector and non-profit R&D at MITRE's CTID (Center for Threat-Informed Defense) previewed an anonymized, real world database organized with a working group of large businesses and organizations. The goal is to capture and analyze the human behaviors and technical issues that drive insider threats. Sponsors include CrowdStrike, Microsoft, HCA, and JP Morgan Chase.

- Teams have documented technical issues and observable human indicators (OHI)
- OHIs are divided into two categories:
  - Binary indicators are flags like telework status or elevated privilege
  - Quantitative indicators include evolving metrics like length of service
- This helps shrink the universe and focuses resources around three screens:
  a. Start with everything that insiders could potentially do
  b. Narrow to everything an average insider would do
  c. End with documented insider incidents that did occur

Current data allow organizations to focus limited resources on the most probable threats, bringing together human- and tech- focused defenses most effectively.

MITRE Resources

MITRE's Insider Threat Research & Solutions website

MITRE's Guiding Principles for Insider Threat

MITRE's Key Terminology for Insider Threat

Suneel Sundar's Presentation Slides

Contact Us
(617) 485-1112
wguenther@acscenter.org

ADVANCED CYBER SECURITY CENTER

Early Takeaways from the Data

A Sub-set of Familiar Tactics

Research identified 47 TTPs and 29 sub-techniques from the MITRE framework

Most Frequent Targets

The most common targets are:

- Information repositories
- Payments systems
- User credential

Unevenly Distributed Frequency

The knowledge base tracks frequency of threats, from most to least frequent.

Most Effective Mitigations

The database highlights 36 mitigations most effective against the 47 identified TTPs.

Not many surprises in the top five:

1. User Activity Monitoring
2. Privileged Account Management
3. Multifactor Authentication
4. IT Audits
5. Feature disable/remove

About the ACSC

The Boston-based ACSC advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent. This Executive Practice Guide reflects key takeaways, with proprietary information redacted, from this NDA-covered session.

Contact Us

(617) 485-1112

wguenther@acscenter.org