Insider Threat Program Evaluation (ITPE) Overview

CERT® Insider Threat Center

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0029

Agenda

SEI / CERT Insider Threat Center Overview

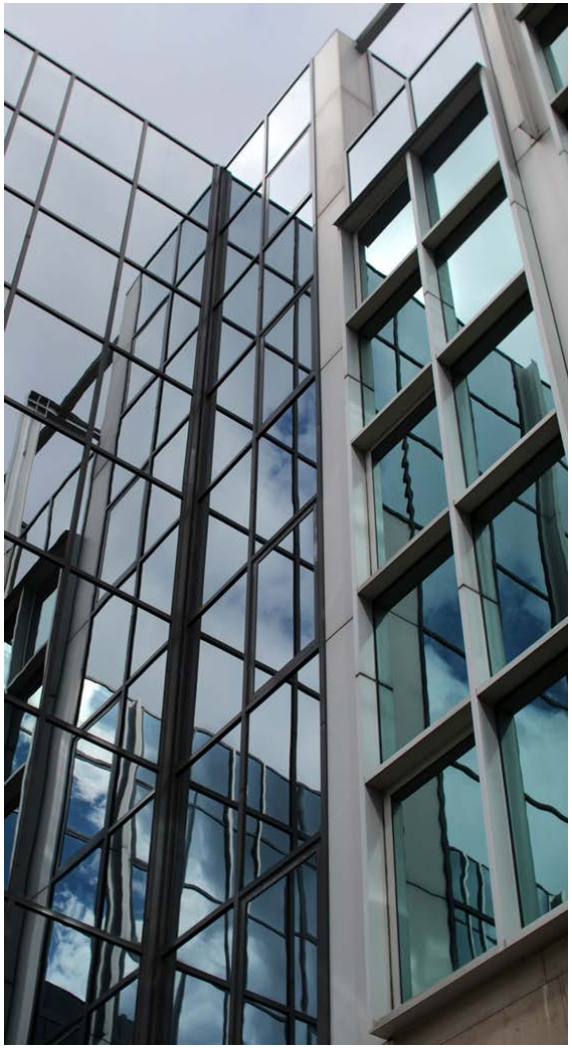
ITPE Overview

Evaluation Team Introductions

SEI Overview

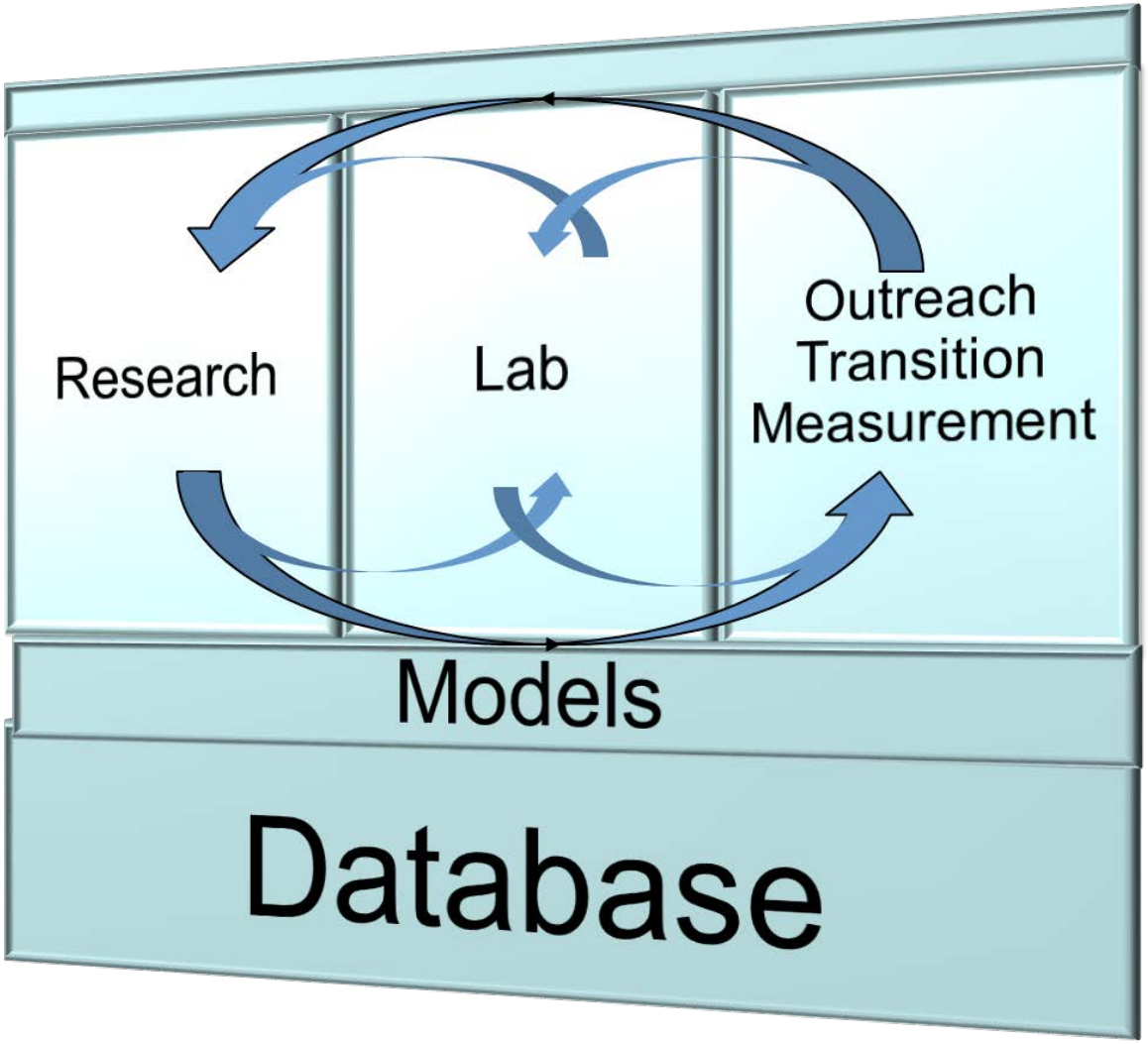
- Established as a DoD FFRDC at Carnegie Mellon University in 1984
- Only DoD R&D center focused on software and cybersecurity
- Offices in Pittsburgh, Arlington, and Los Angeles
- About 700 staff (~450 tech staff)

The CERT Insider Threat Center



- Center of insider threat expertise
- Began working in this area in 2001
- Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber threats
- Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

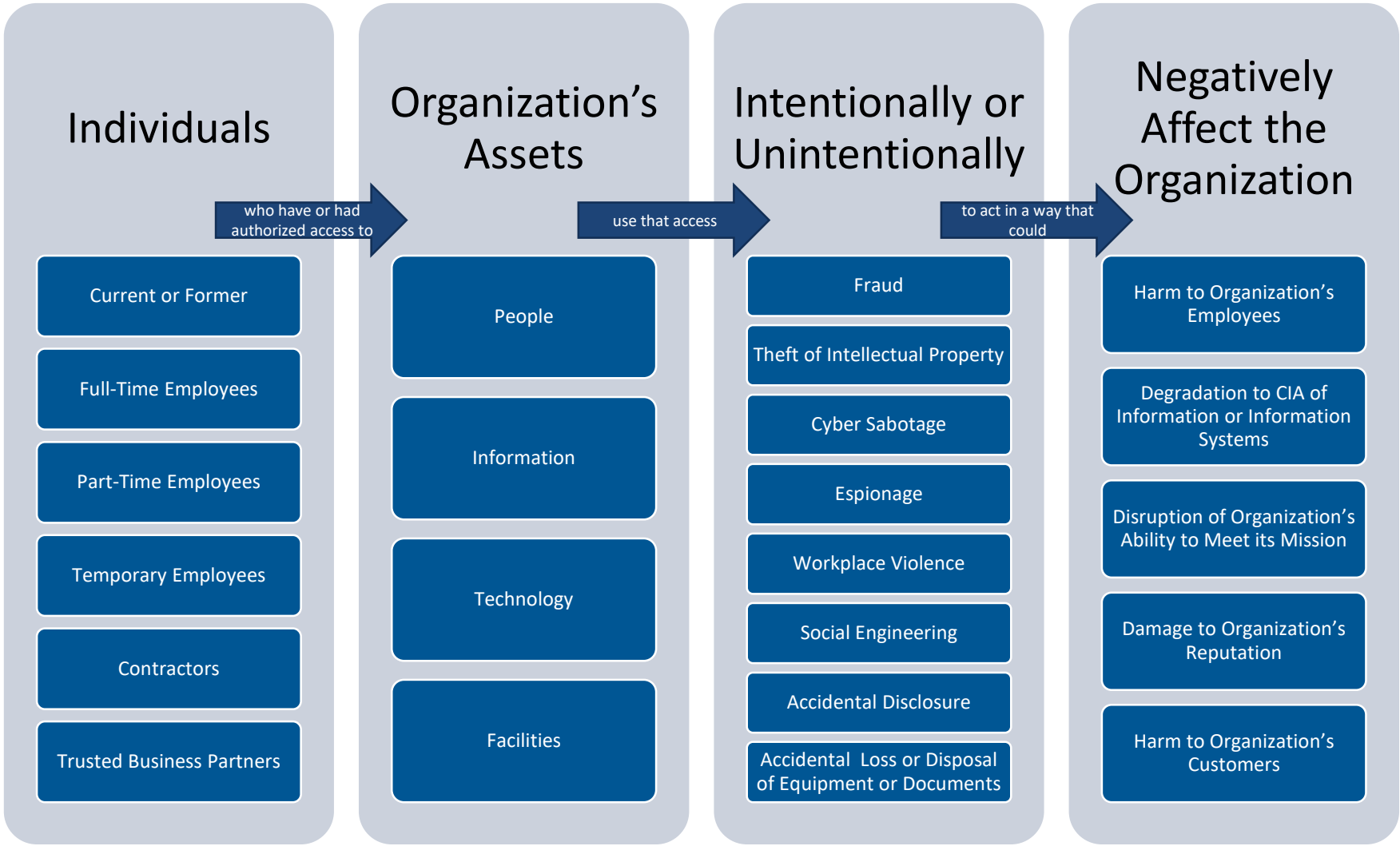
CERT's Unique Approach to the Problem



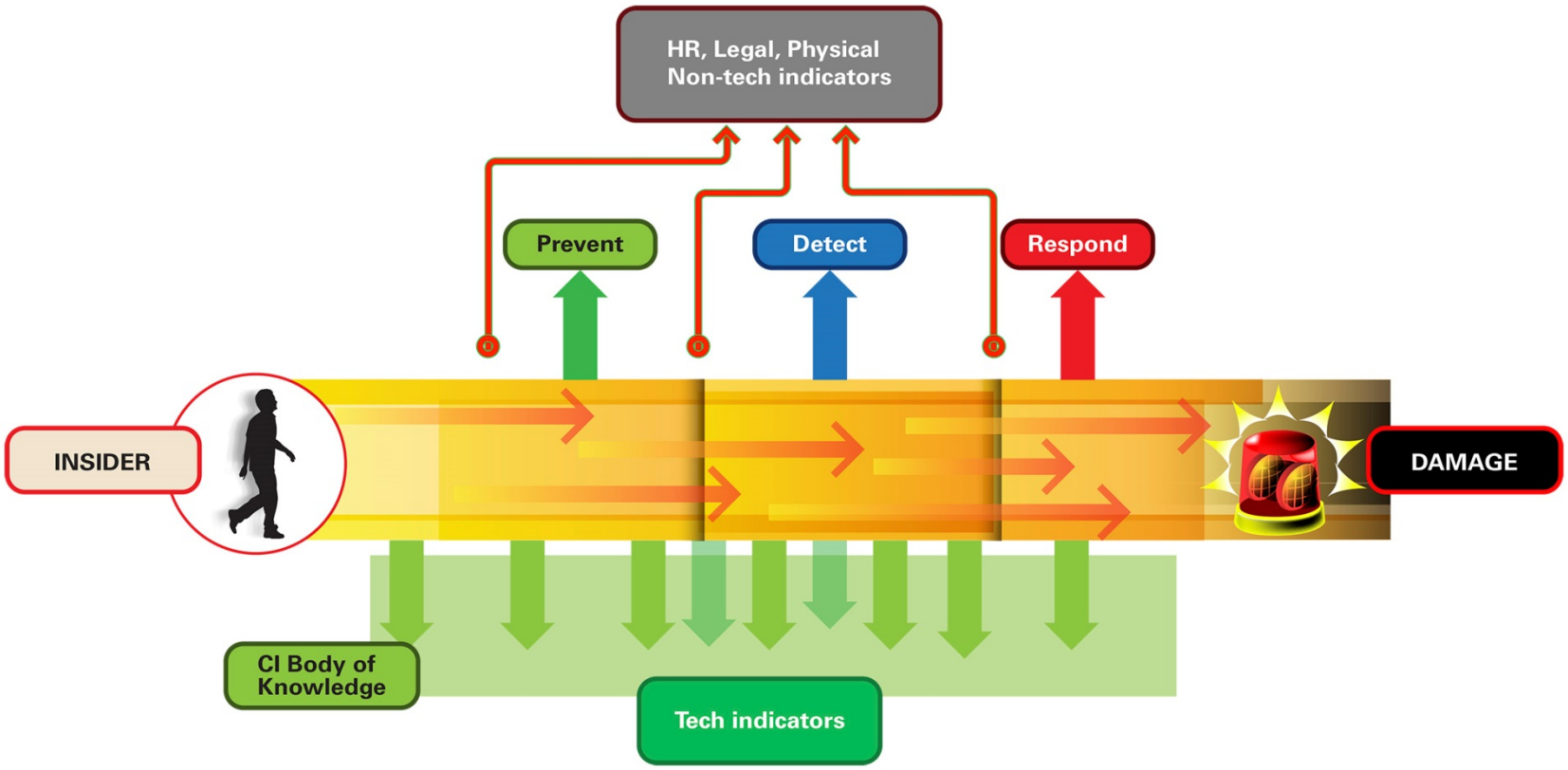
CERT's Definition of Insider Threat

The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Scope of the Insider Threat

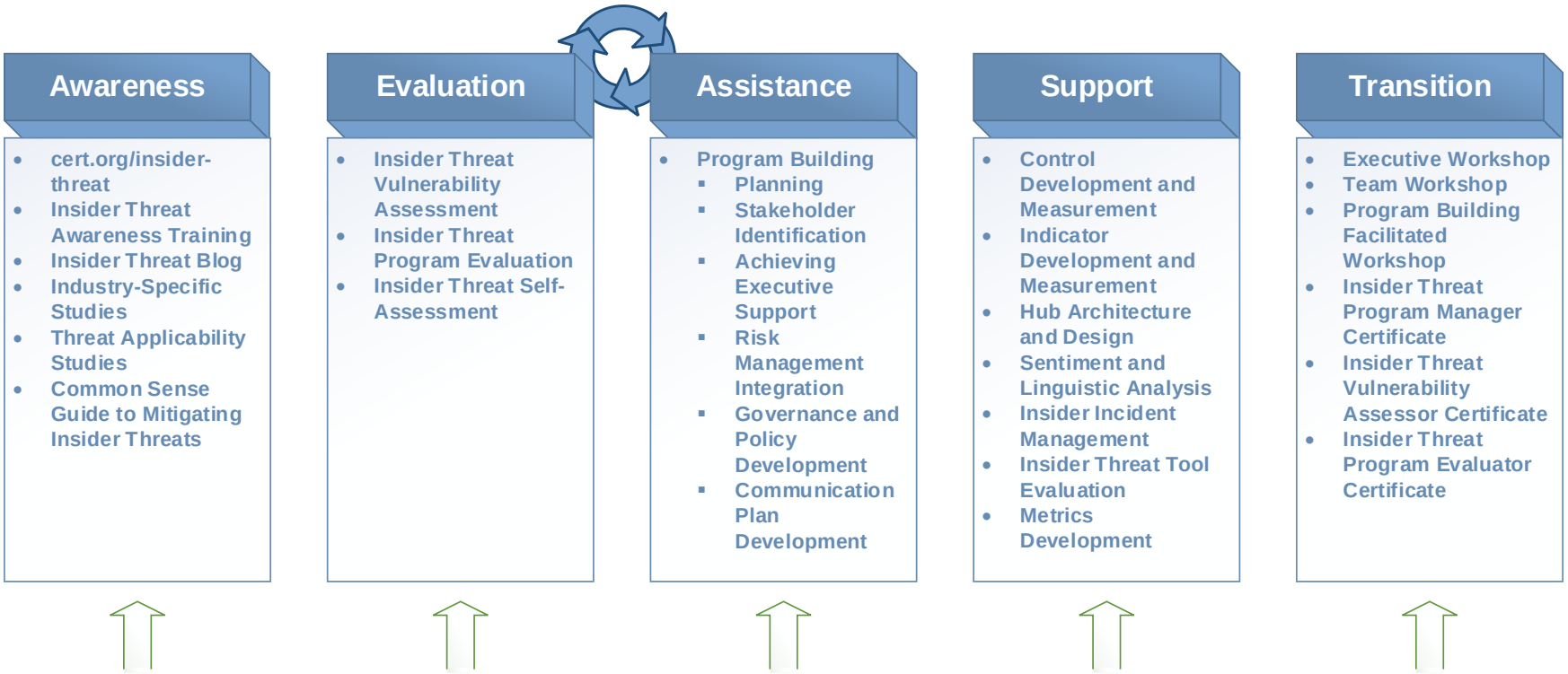


Goal for an Insider Threat Program

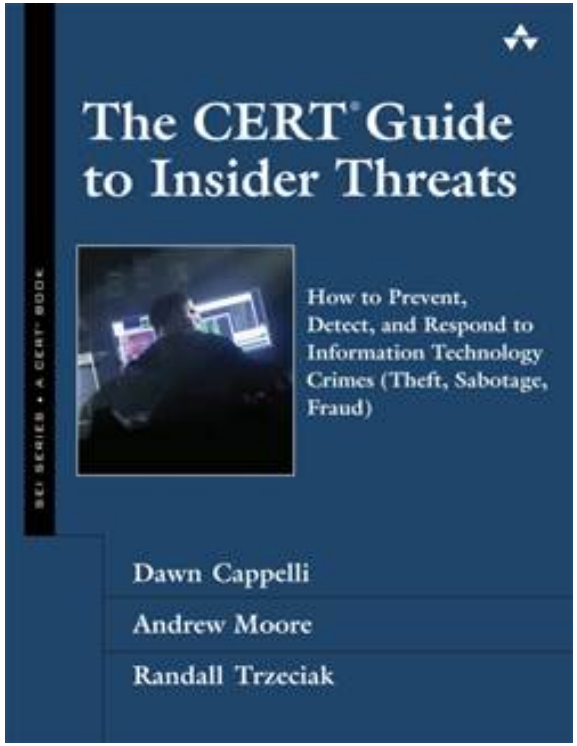


Opportunities for prevention, detection, and response for an insider incident

CERT Insider Threat Center Offerings



CERT Insider Threat Reports and Controls



- Technical Reports
  - CERT Common Sense Guide to Mitigating Insider Threats
  - Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector
  - Unintentional Insider Threats: A Foundational Study
  - An Insider Threat Indicator Ontology
  - The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures
  - Over 100 reports available at www.cert.org/insider-threat/publications
- Technical Controls
  - Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time
  - Using a SIEM signature to detect potential precursors to IT Sabotage
  - Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources

ITPE Overview

ITPE Purpose and Benefit

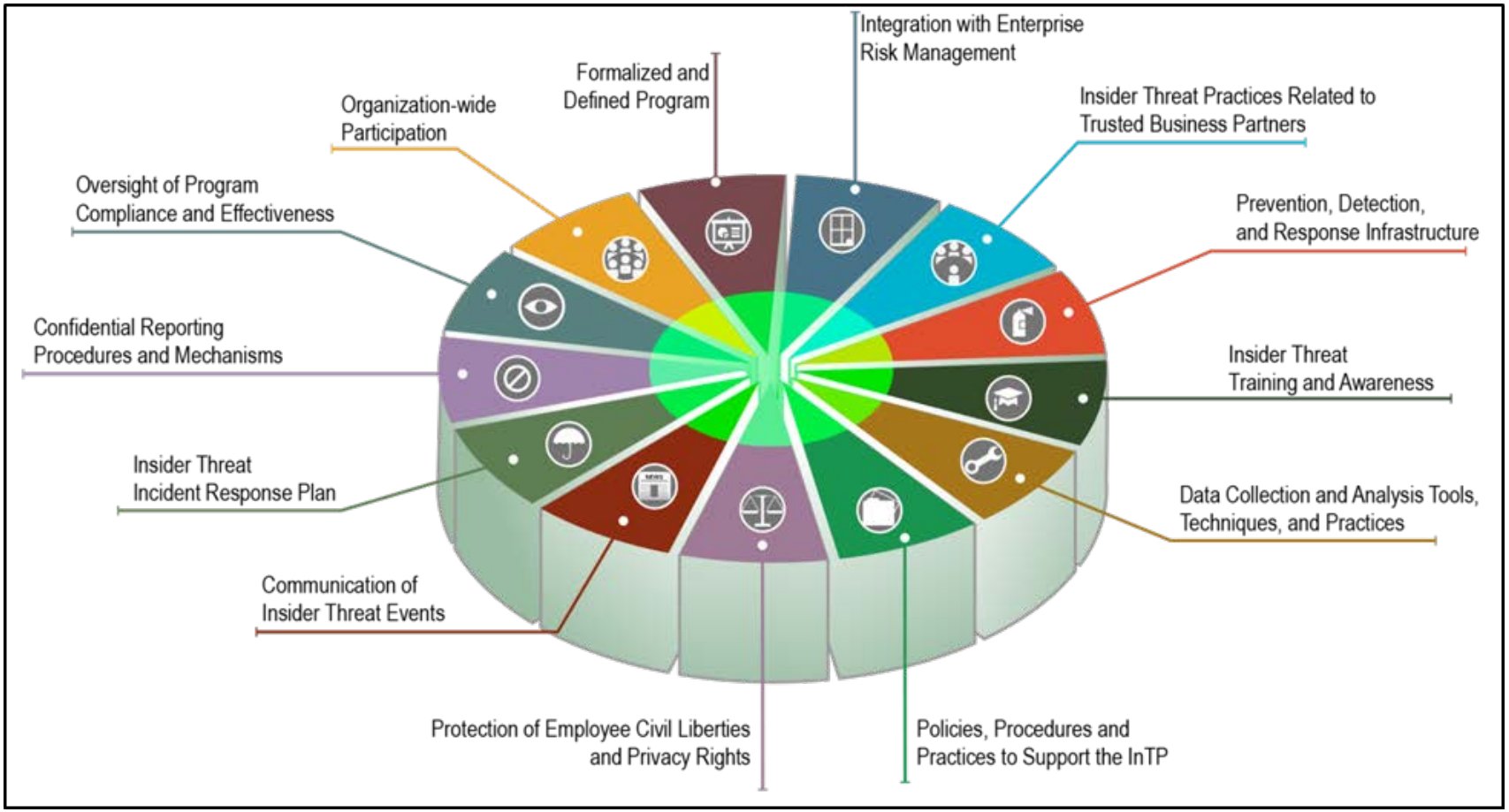
The Insider Threat Program Evaluation assesses the robustness of the organization's program to prevent, detect, and respond to insider threats and provides recommendations for enhancing the program's effectiveness.

The long-term benefit is to assist organizations in reducing exposure to damage from potential insider threats.

The ITPE

- Benchmarks an insider threat program against our criteria built on the National Insider Threat Task Force (NITTF) minimum standards and CERT Insider Threat Center, government, and industry best practices
- Looks at the organization's program via an enterprise perspective

Key Components of an Insider Threat Program



ITPE Capabilities

Program Management	Personnel and Training	Collection and Analysis	Personnel and Training Human Resources and Legal
Formalized Program	Organization-wide Training	Access Control	Employee Lifecycle: Hiring, Onboarding, and Separation
InTP Policy	InTP Team Composition	Modification of Data or Disruption of Services or Systems	Employee Investigations
Insider Threat Response Plan	Insider Threat Awareness Training for Organization	Unauthorized Access, Download, or Transfer of Assets	Confidential Reporting
Insider Threat Program Communication Plan	InTP Team Training	Detection and Identification	Identifying At-Risk Employees
ERM Integration	Role-based Training for Organization	Incident Response	Intellectual Property
Critical Asset Identification	Manager and Supervisor Training	Termination	Employee Support Programs
InTP Governance			InTP Access to HR Information
Quality, Effectiveness, and Performance of the InTP			User Monitoring Policy
			Physical and Personnel Security

ITPE Process Overview

Evaluation Phases:

- Planning – establish evaluation team, customer POC's, deliver process documentation, coordinate logistics
- Pre-evaluation – develop data collection plan, review documentation (10-20 days)
- On-site – conduct interviews with subject matter experts, on-site document reviews, direct observations of capabilities (3-5 days)
- Post-evaluation – analyze collected data, develop report, incorporate customer feedback of draft report into final deliverable (10-20 days)

Evaluation Team

Dan Costa

- Technical Solutions Team Lead, CERT Insider Threat Center
- Expertise: tools and techniques for insider threat data collection and analysis
- CISSP, PSEM, Adjunct Faculty at CMU

Tracy Cassidy

- Insider Threat Researcher, CERT Insider Threat Center
- Expertise: behavioral aspects of insider threats, workplace violence, threat assessment
- Former psychotherapist

Jean Marie Handy

- Senior Researcher, CERT Insider Threat Center
- Expertise: Insider Threat Research, Computer Forensics, Digital Crimes and Brand Reputation (Public and Private Sector)
- CISSP

Contact Information

Evaluation Lead

Dan Costa

Technical Solutions Team Lead,
CERT Insider Threat Center

Telephone: +1 412.268.8006

Email: dlcosta@sei.cmu.edu