



# Insider Threat Program Evaluation (ITPE) Overview

CERT<sup>®</sup> Insider Threat Center

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-0029

# Agenda

**SEI / CERT Insider Threat Center  
Overview**

**ITPE Overview**

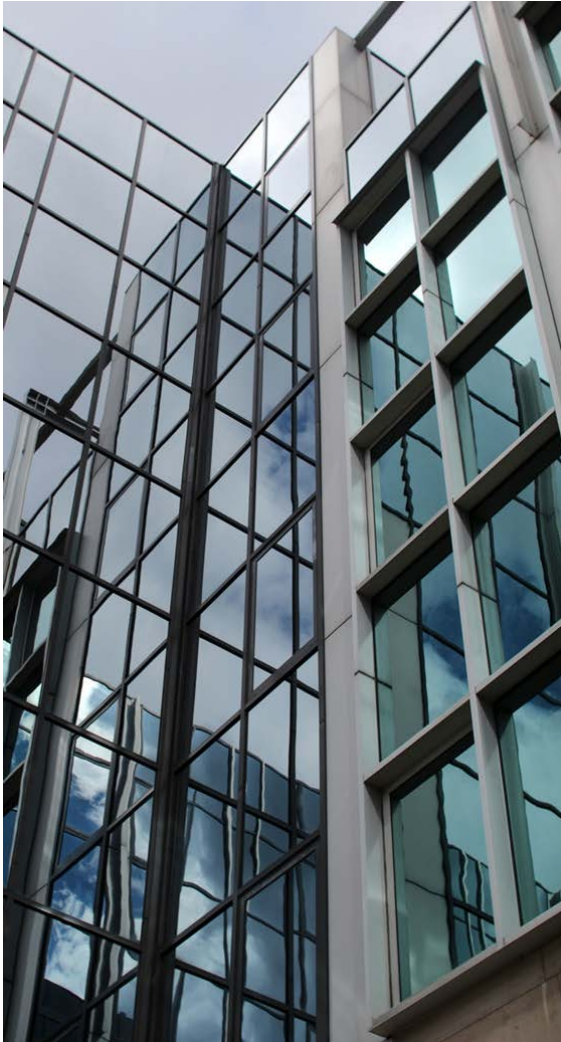
**Evaluation Team Introductions**

# SEI Overview



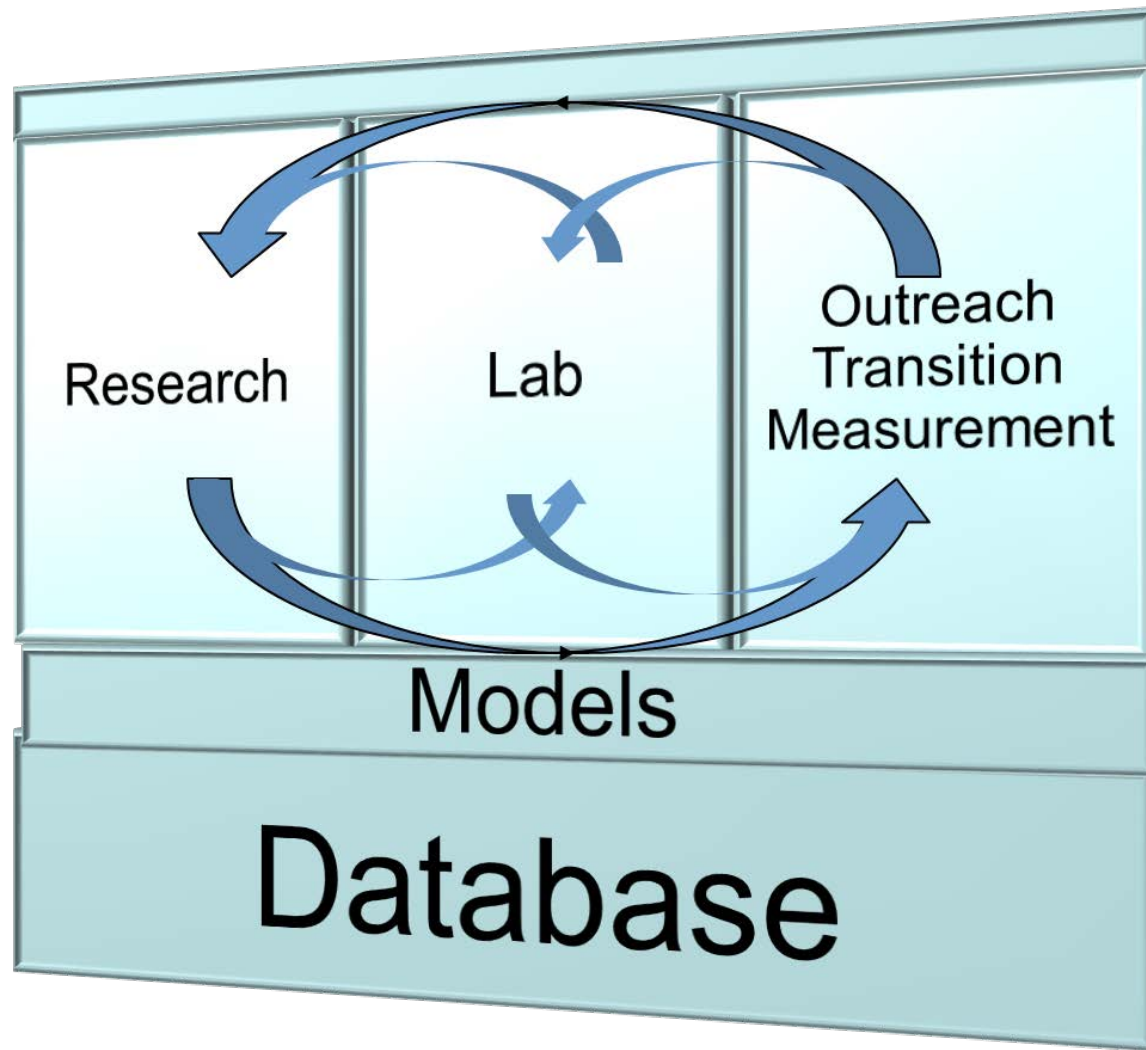
- Established as a DoD FFRDC at Carnegie Mellon University in 1984
- Only DoD R&D center focused on software and cybersecurity
- Offices in Pittsburgh, Arlington, and Los Angeles
- About 700 staff (~450 tech staff)

# 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

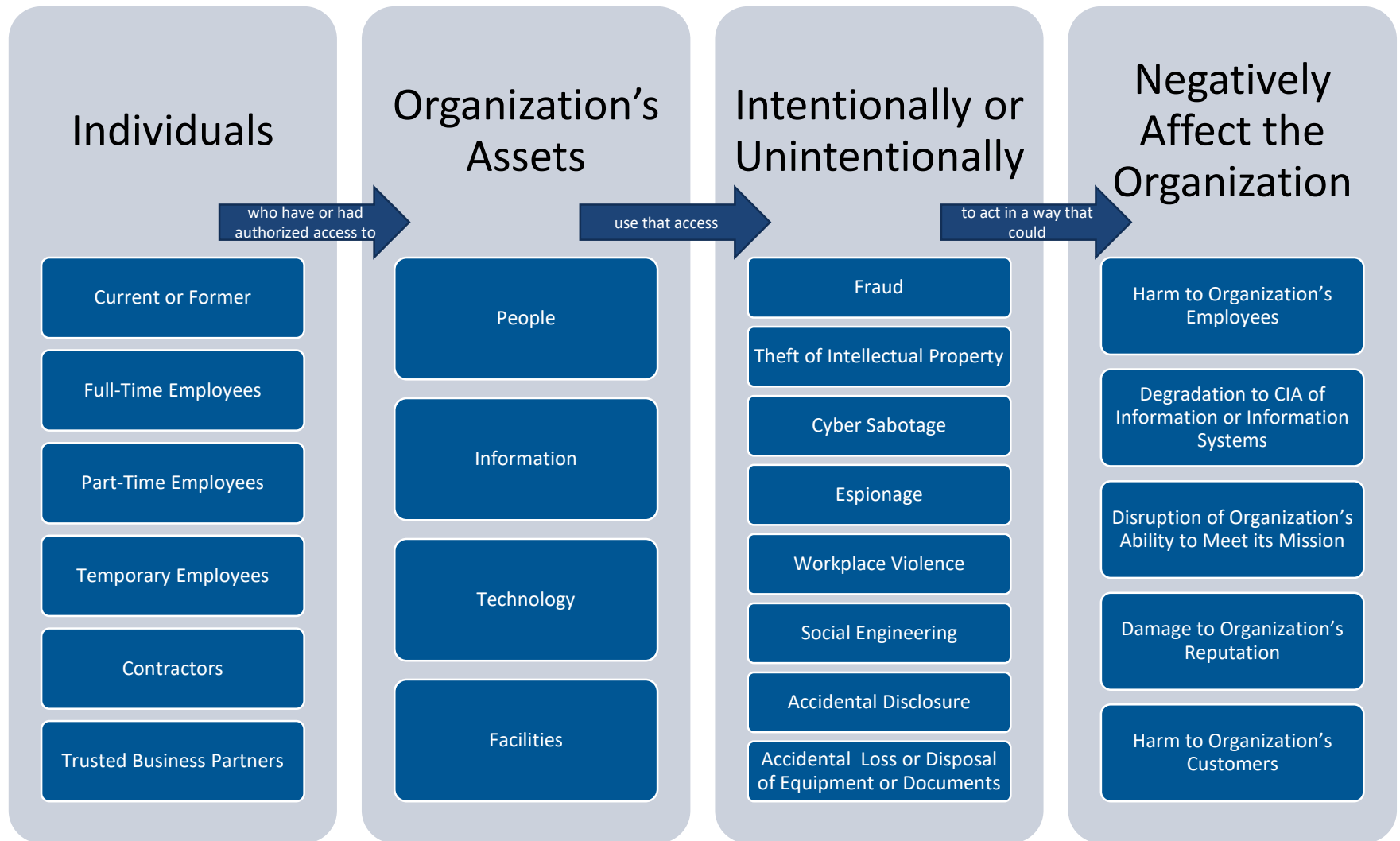
# CERT's Unique Approach to the Problem



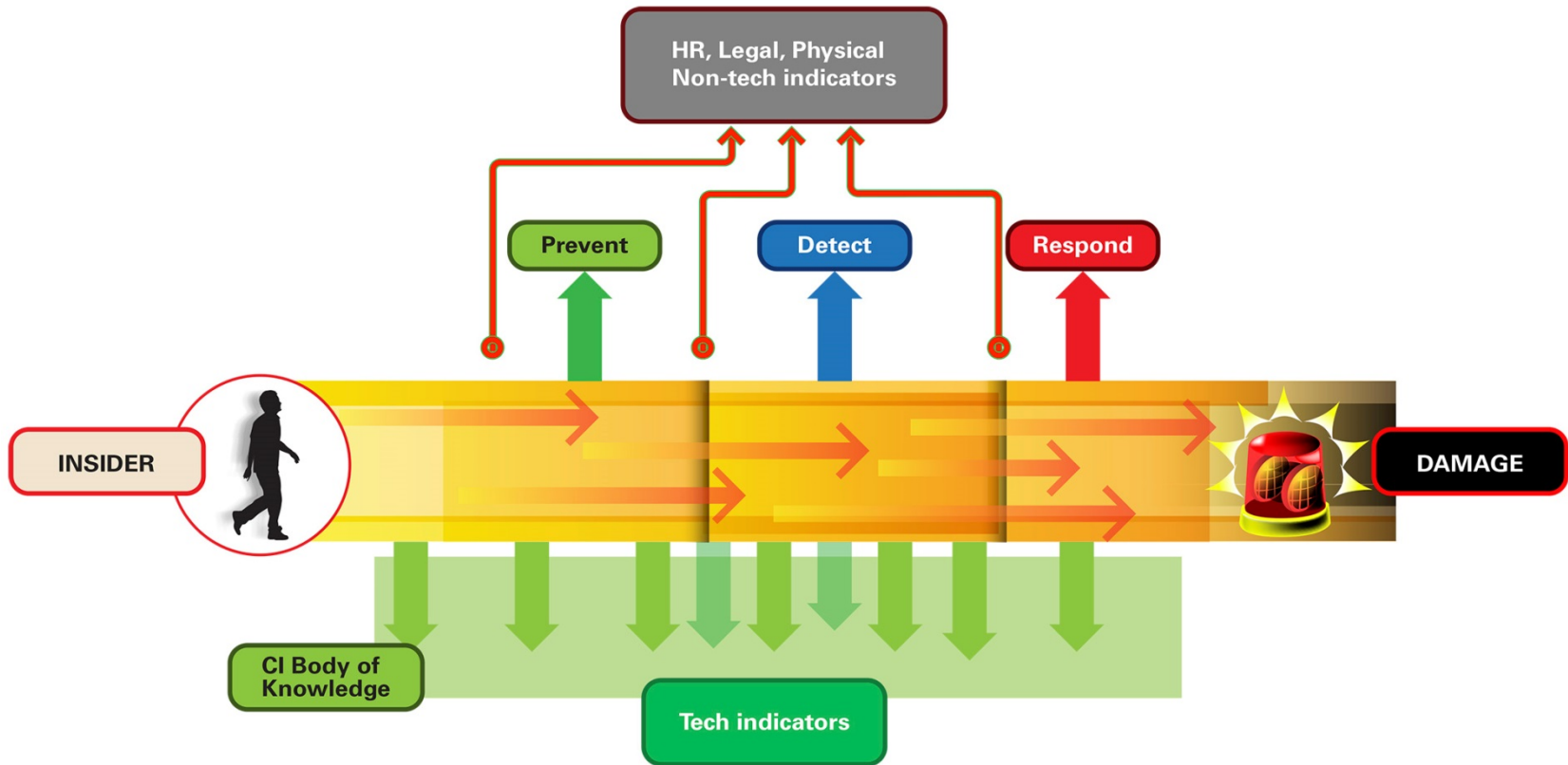
# CERT's Definition of Insider Threat

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

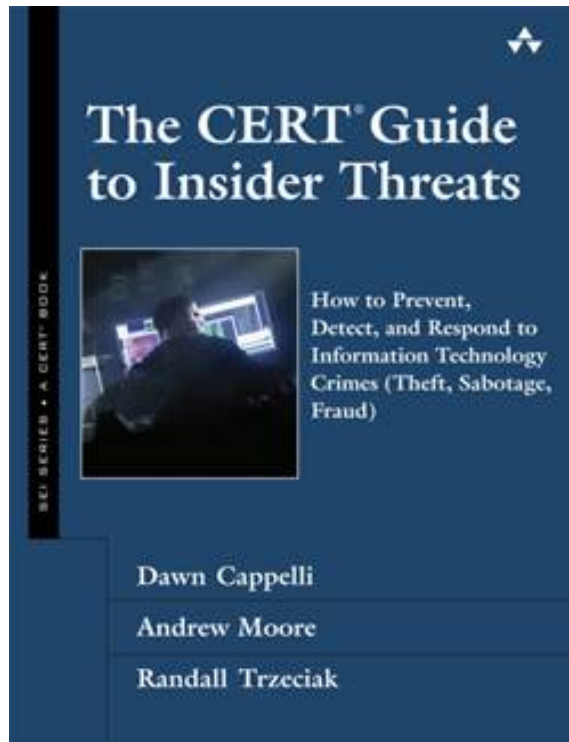


*Opportunities for prevention, detection, and response for an insider incident*

# 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](http://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

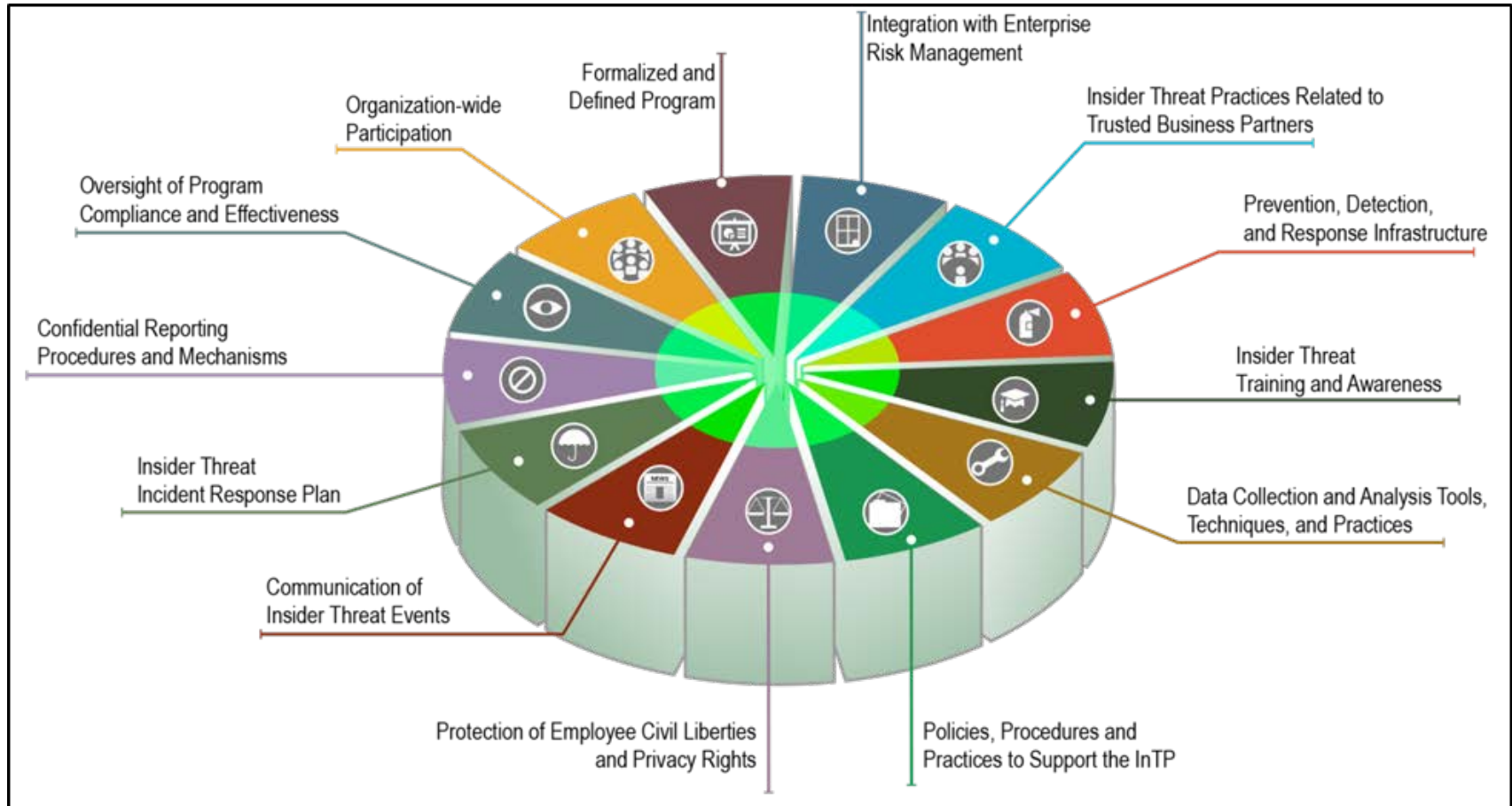
The Insider Threat Program Evaluation assesses the robustness of the organization's program to prevent, detect, and respond to insider threats and provides recommendations for enhancing the program's effectiveness.

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

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

# 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](mailto:dlcosta@sei.cmu.edu)