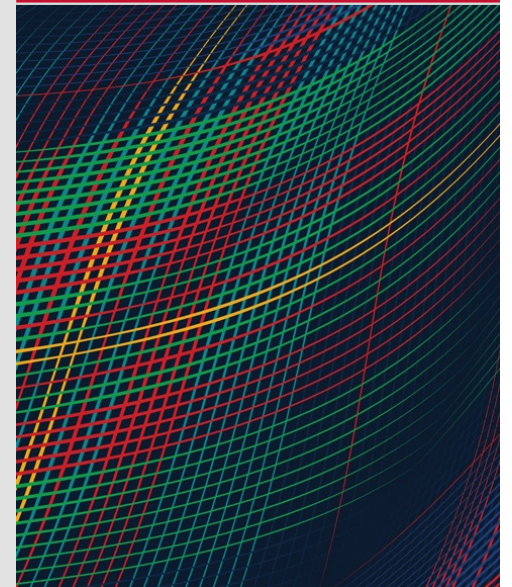


# Insider Threat Vulnerability Assessment (ITVA) Planning Briefing



# Document Markings

Copyright 2023 Carnegie Mellon University.

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

Internal use:\* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:\* 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 external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

\* These restrictions do not apply to U.S. government entities.

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

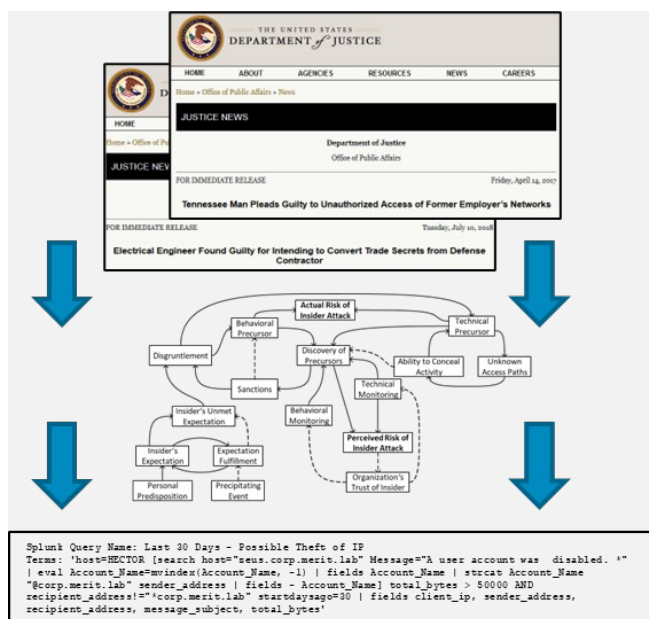
DM23-0882

# Agenda

- CMU SEI Insider Risk Overview
- ITVA Purpose and Background
- ITVA Process Overview
- ITVA Capability Review
- Next Steps / Open Discussion

# Insider Risk Research at CMU SEI

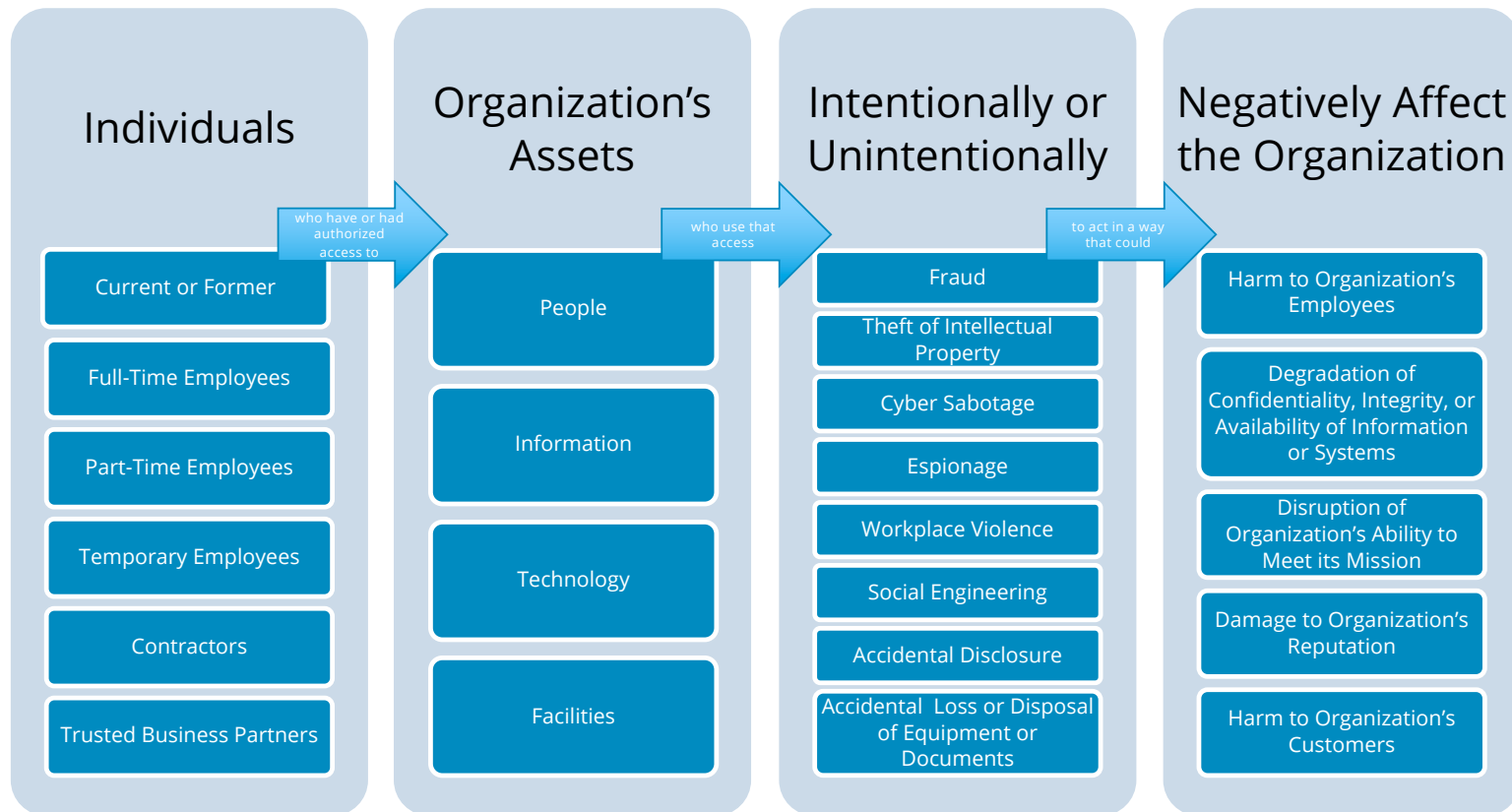
Conducting research, modeling, analysis, and outreach to develop socio-technical solutions to manage insider risk since 2001



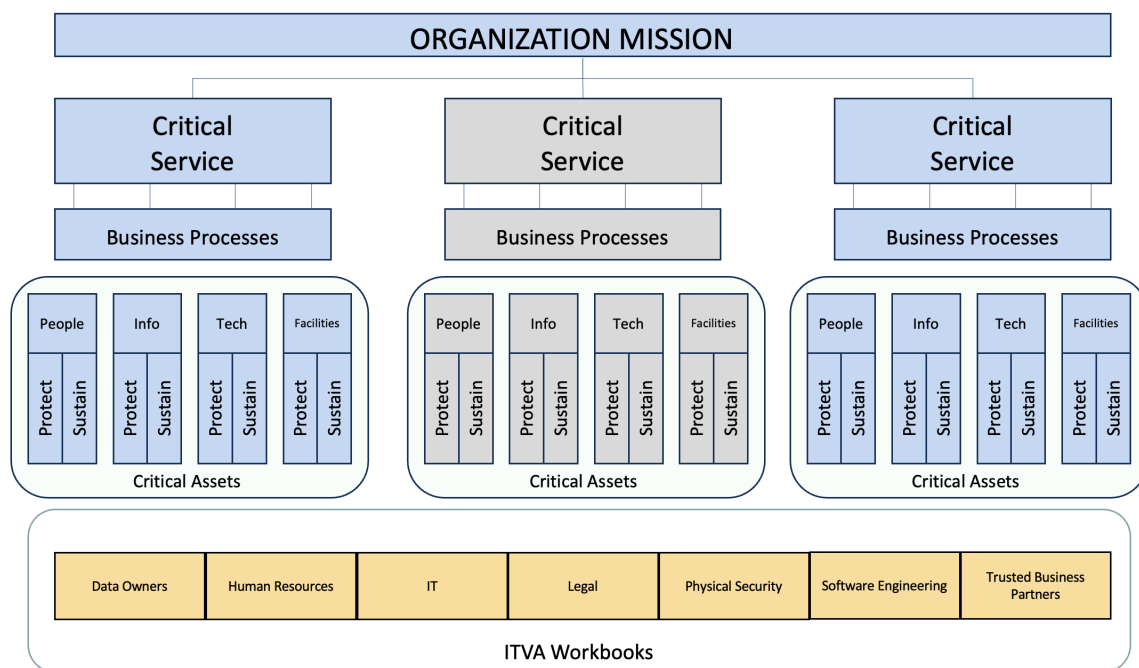
## Insider Threat Defined

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



# Insider Threat Vulnerability Assessment (ITVA) Overview



The SEI measures organizations' preparedness to prevent, detect, and respond to insider threats to critical assets using its ITVA capability

The ITVA benchmarks organizations' technical, physical, and administrative controls against the most prevalent vulnerabilities from the CERT Insider Threat Incident Corpus

The ITVA identifies key capability gaps in the protection of an organization's critical assets from authorized access misuse, and provides recommended mitigation strategies for vulnerabilities to specific assets

# Methodology – 1

Data Owners	Human Resources	Information Technology	Legal	Physical Security	Software Engineering	Trusted Business Partners
Access Control	Recruitment	Access Control	Agreements to Protect Sensitive Information	Facility Security	Technical Policies and Agreements	Screening/Hiring of Applicants
Modification of Data, Systems, or Logs	Policies and Practices	Modification of Data or Disruption of Services or Systems	Restrictions on Outside Employment	Physical Asset Security	Modification of Data or Systems	Management of Business Partners
Unauthorized Access, Download, or Transfer of Assets	Training and Education, Evaluation	Unauthorized Access, Download, or Transfer of Assets	Employee Behaviors in the Workplace		Asset Management	Asset Management
Incident Response	Policy and Practice Monitoring and Enforcement Programs	Detection and Identification	Conditions of Hire			Incident Response
Termination	Enforcement and Termination	Incident Response	Property Lending Agreements			Contractor/ Business Partner Agreements
		Termination	Contractor/ Business Partner Agreements			

The ITVA utilizes a capability-level assessment methodology, adapted from the *Standard CMMI Appraisal Method for Process Improvement (SCAMPI)*

- Goal: gain insight into an organization's **capability** by identifying strengths and weakness of current process relative to a reference model



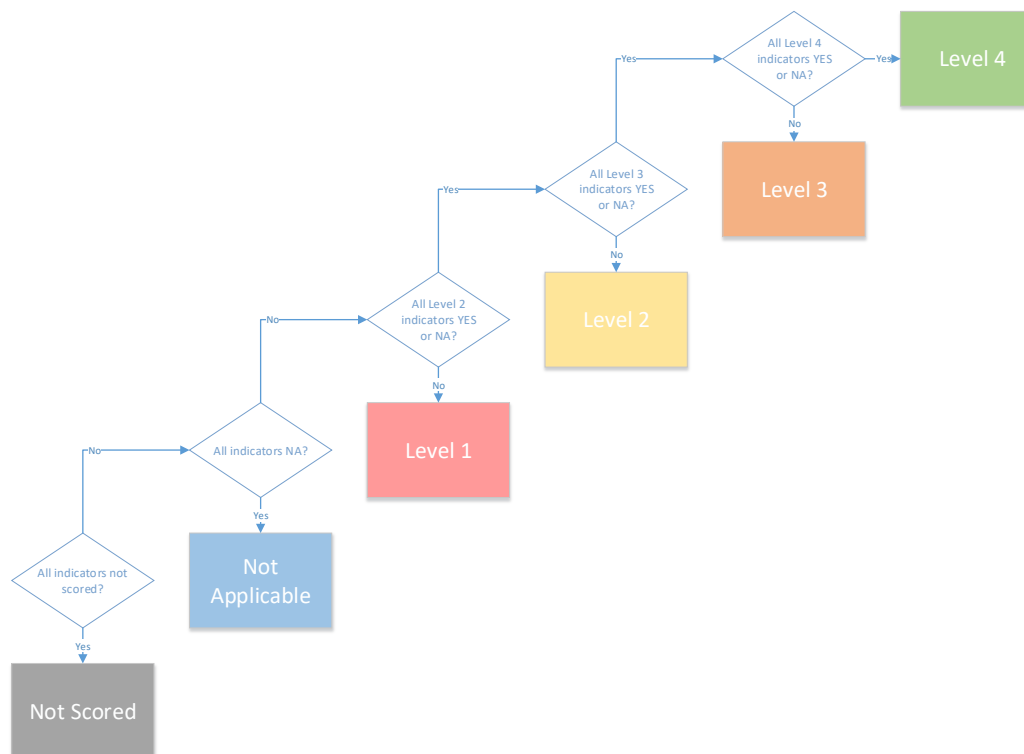
## Methodology – 2

Level	Description
1 - Not Performed	The organization does not perform the minimal recommended practices
2 - Minimal	The organization has controls and processes in place to detect, but has issues preventing or responding to the issue of concern
3 - Enhanced	The organization has controls and processes in place to detect and respond, but has issues preventing the issue of concern
4 - Robust	The organization is prepared to prevent, detect, and respond to the issue of concern

Capability level ratings are derived from **indicators** of activities

- Indicators are individual yes / no questions designed to determine if a specific policy, process, procedure, practice, or other condition or activity exists within an organization
- Each capability has one or more indicators associated with each capability level

# Capability Level Scoring Methodology



## Methodology – 3

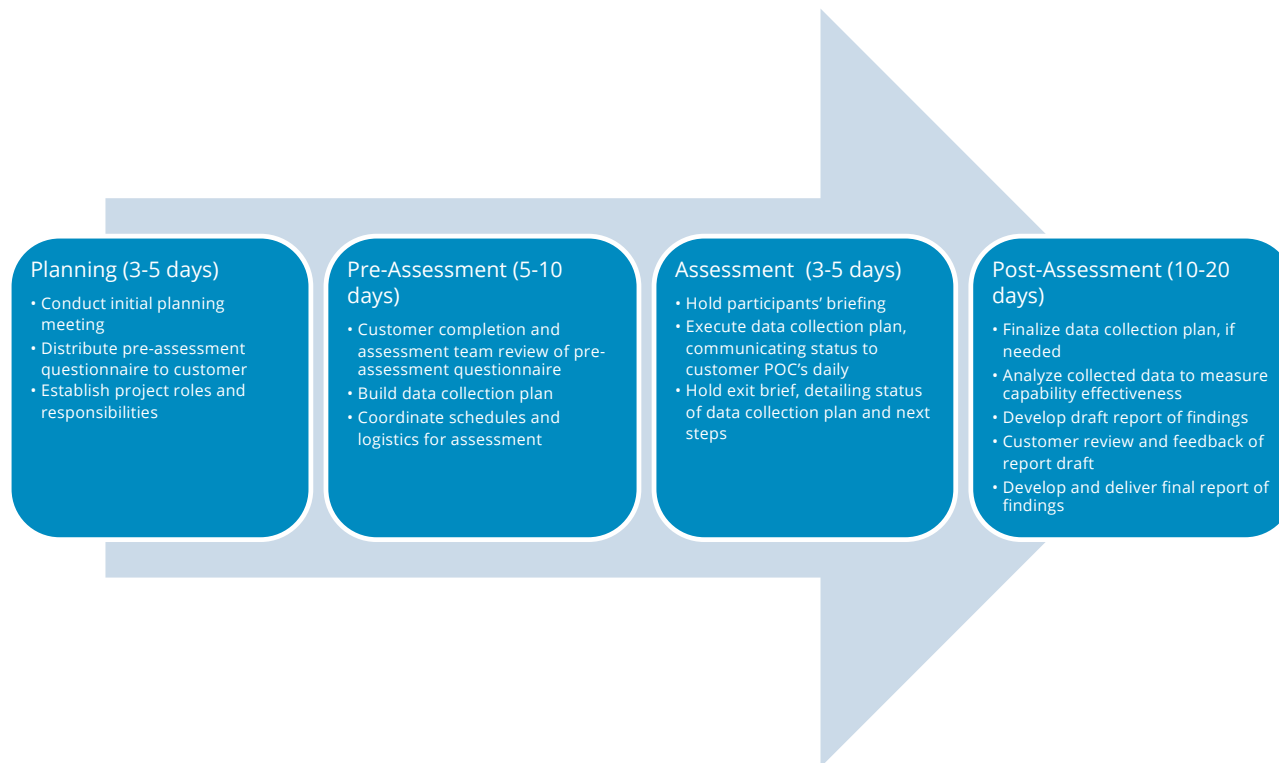
Collect and analyze **evidence** that supports the absence or presence of indicators

- Review of documents that describe existing processes and procedures
- Interviews with personnel that perform key activities
- Direct observations of capability (e.g., tool demonstrations)

Minimum standards for evidence provide confidence in the capability level scoring

- 1 document + 1 observation
- 1 document + 2 interviews
- 1 observation + 2 interviews
- 3 interviews

# ITVA Process Flow and Timeline



# ITVA Roles and Responsibilities

## Customer POC

- Ensures appropriate customer personnel are notified of and participate in the project
- Makes management decisions regarding the assessment (scope, schedule, etc.)
- Identifies a staff member to fill the role of Customer Logistics Coordinator
- Provides feedback on the draft report of findings

## Customer Logistics Coordinator

- Manages the interview and demonstration schedule
- Provides any requested documentation to the assessment team

## Customer Management and Operational Staff

- Participate in scheduled interviews or demonstrations
- Provides any additional requested documentation to assessment team via the Customer Logistics Coordinator
- Work with the Customer Logistics Coordinator to reschedule interviews or demonstrations if needed

## ITVA Team Lead

- Leads the initial planning and pre-assessment meetings
- Leads the assessment team activities
- Leads the development of the data collection plan
- Works with Customer Logistics Coordinator to schedule interviews and demonstrations
- Leads the data collection phase, to include the participants' briefing and out-brief
- Leads the data analysis and report development

## ITVA Team Members

- Participate in planning briefing as needed
- Perform pre-assessment questionnaire review
- Assist with the development of the data collection plan
- Execute data collection plan
- Perform post-assessment data analysis
- Assist with drafting the report of findings

# Questions / Discussion

