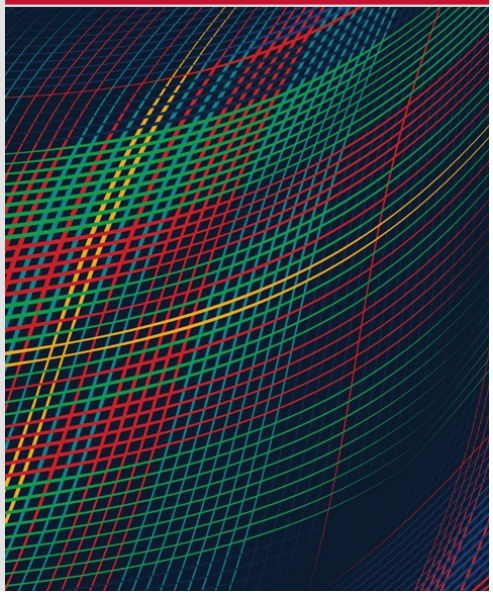
Insider Threat Program Evaluation (ITPE)
Participants Briefing

Carnegie Mellon University
Software Engineering Institute



Document Markings

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.

DM23-0883

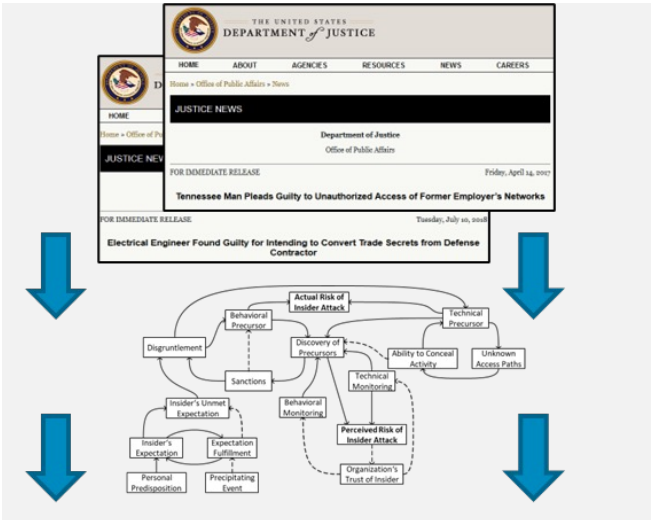
Agenda

Carnegie Mellon University Software Engineering Institute

- CMU SEI Insider Risk Overview
- ITPE Purpose and Background
- ITPE Process Overview
- Next Steps / Open Discussion

Insider Risk Research at CMU SEI

Carnegie Mellon University Software Engineering Institute




```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="seus.corp.merit.lab" Message="A user account was  disabled. *"
| eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND
recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address,
recipient_address, message_subject, total_bytes'
```

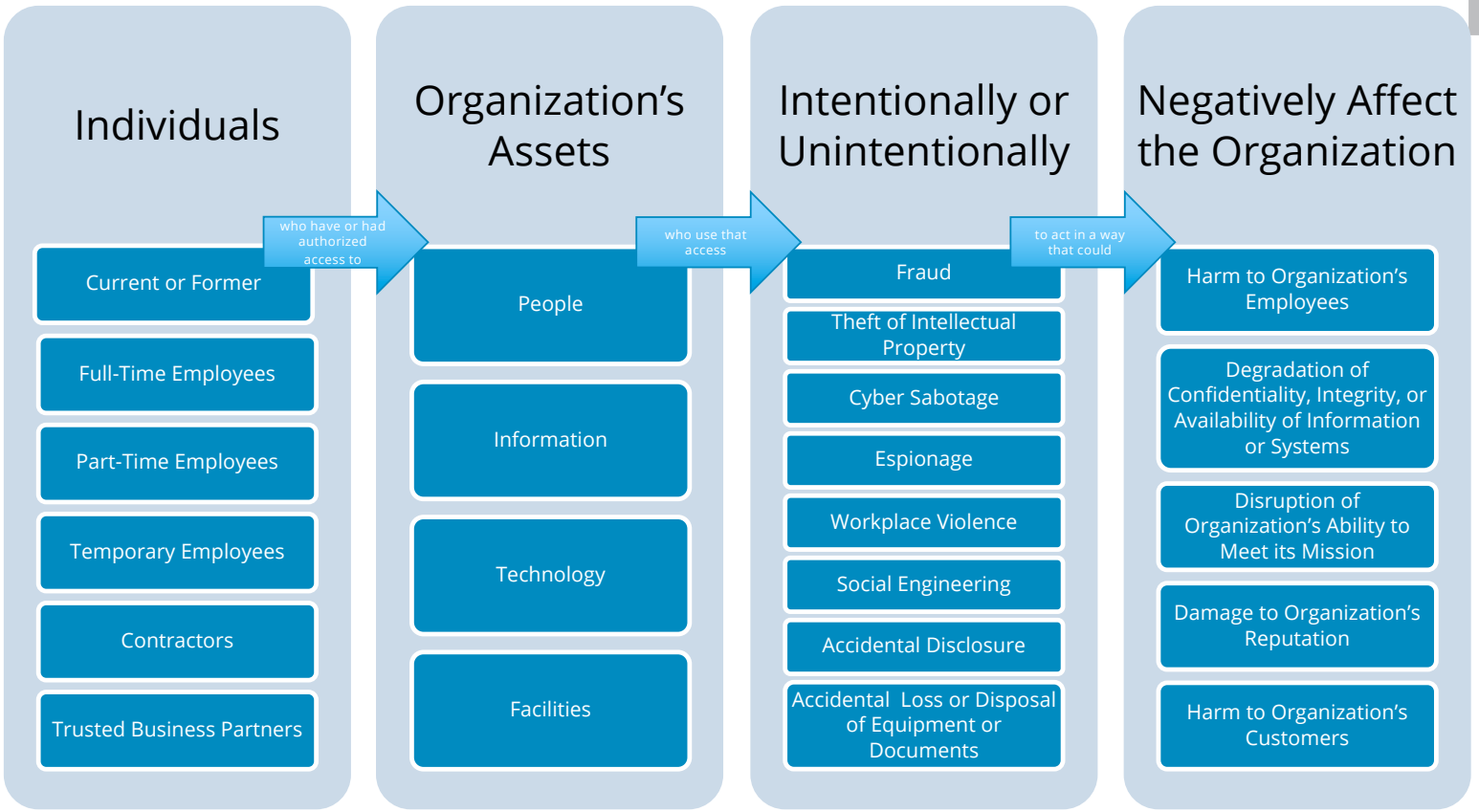
Conducting research, modeling, analysis, and outreach to develop socio-technical solutions to manage insider risk since 2001

Insider Threat Defined

Carnegie Mellon University Software Engineering Institute

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



Scale of the Insider Threat

Carnegie Mellon University Software Engineering Institute

1 in 3 cyber crimes are perpetrated by insiders

Insider incidents have increased by 47% since 2018 (Source: Ponemon 2022 Cost of Insider Threat Global Report)

1 in 4 insider incidents are perpetrated by trusted external entities

1 in 3 insider incidents are committed with malicious intent

Insider Threat Program Evaluation (ITPE) Overview

Carnegie Mellon University Software Engineering Institute

- The ITPE **benchmarks** organizations against a set of recommended best practices derived from the **National Insider Threat Policy and Minimum Standards**, and the SEI's extensive research background in insider risk mitigation
- The findings of the ITPE provide a **roadmap** that can be used to establish and maintain a mature and effective insider threat program

ITPE Myth-Busting

Carnegie Mellon University Software Engineering Institute

The ITPE IS NOT:

- An audit
- An inspection
- A compliance certification
- An attempt to investigate potential insider incidents
- A direct response to an insider incident

The ITPE IS:

- A proactive attempt to understand an organization's current ability to prevent, detect, and respond to insider threat and holistically manage insider risk to acceptable levels.
- A reference model that can be used to plan for future improvements to an organization's security posture.

Methodology – 1

Carnegie Mellon University Software Engineering Institute

Program Management	Personnel and Training	Data Collection and Analysis
Formalized Program	Organization-Wide Participation	Executing Response
InTP Policy	InTP Team Composition	Information Access Management
Insider Threat Response Plan	Insider Threat Awareness Training for Organization	InTP Access to Technical Information
InTP Communication Plan	InTP Team Training	InTP Access to HR Information
ERM Integration	Role-Based Training for Organization	InTP Access to Counterintelligence and Security Information
Critical Asset Identification	Manager and Supervisor Training	User Activity Monitoring
InTP Governance	Employee Onboarding Process	Integrated Data Analytical Capability
Quality, Effectiveness, and Performance of the InTP		InTP Access to HR Information
Employee Investigations		Employee Behavior
Employee Support Programs		Employee Separation

The ITPE 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

Carnegie Mellon University Software Engineering Institute

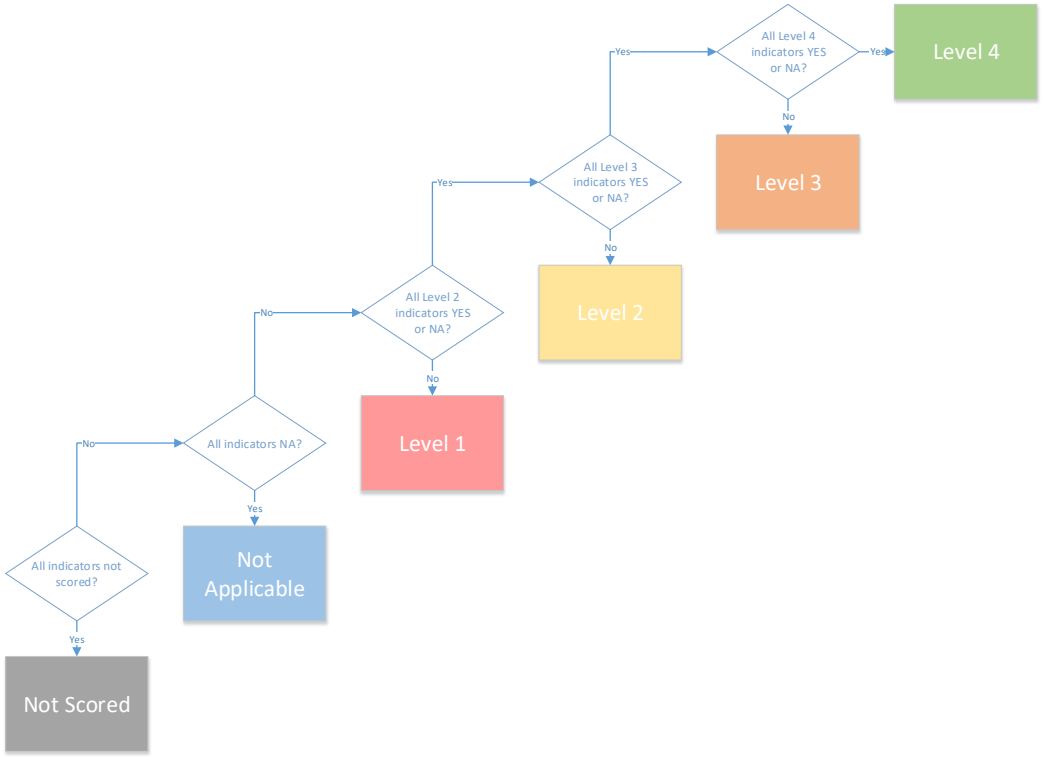
Level	Description
1 - Not Performed	The organization does not perform the minimal recommended practices
2 - Minimal	The organization performs a minimal set of practices, as designated by the National Insider Threat Policy and Minimum Standards (where applicable) and SEI recommended best practices
3 - Enhanced	The organization has additional practices in place that exceed the minimal capability
4 - Robust	The organization has extensive practices in place that provide effective, efficient, and sustained capability

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

Carnegie Mellon University Software Engineering Institute



Methodology – 3

Carnegie Mellon University Software Engineering Institute

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

Data Handling

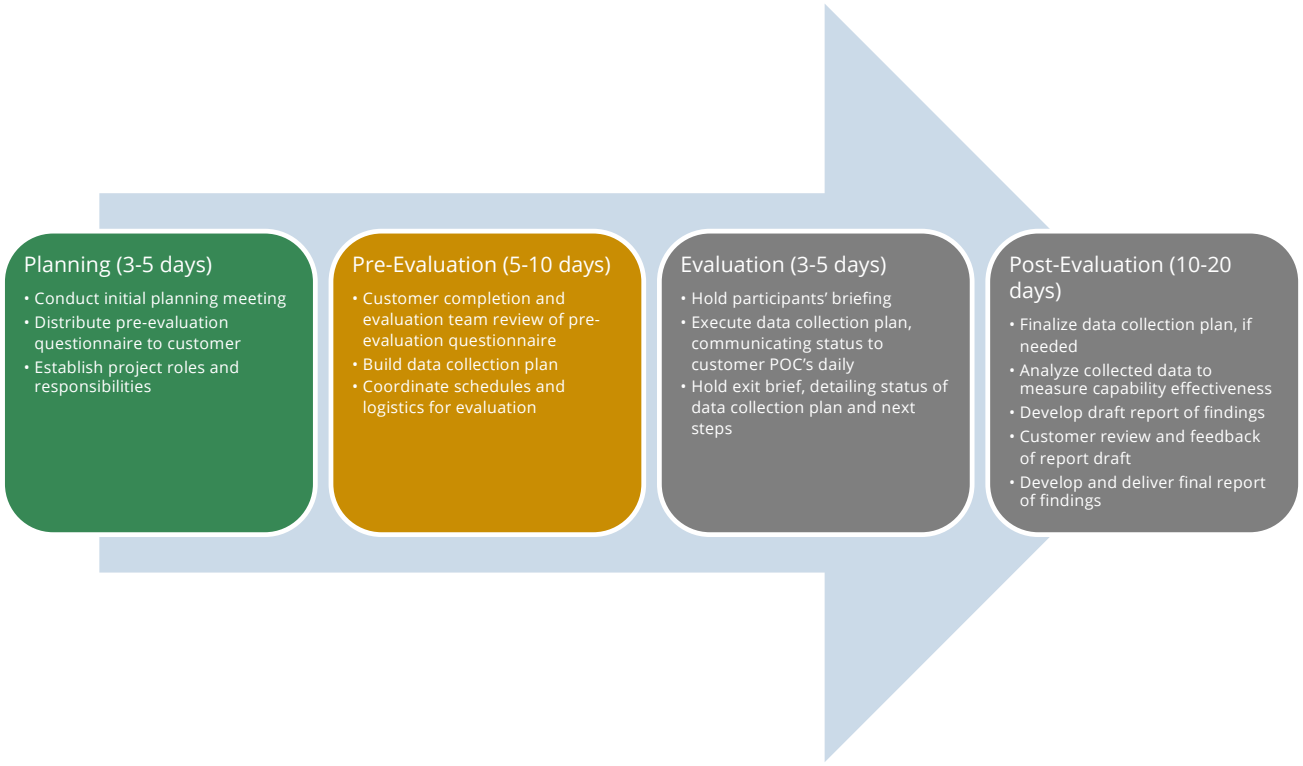
Carnegie Mellon University Software Engineering Institute

We take the protection of all data collected during this engagement seriously.

- All collected data is encrypted at-rest and in-transit, and access controlled to only those with a valid need-to-know.
- Pseudonyms are used to reference interview subjects in assessment team's notes.
- There is no attribution of any data collected.
- All project artifacts are securely destroyed at the completion of the effort.

ITPE Process Flow and Timeline

Carnegie Mellon University Software Engineering Institute



ITPE Roles and Responsibilities

Carnegie Mellon University Software Engineering Institute

Customer POC

- Ensures appropriate customer personnel are notified of and participate in the project
- Makes management decisions regarding the evaluation (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 evaluation team

Customer Management and Operational Staff

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

ITPE Team Lead

- Leads the initial planning and pre-evaluation meetings
- Leads the evaluation 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

ITPE Team Members

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

Questions / Discussion

Carnegie Mellon University Software Engineering Institute

For More Information

Carnegie Mellon University Software Engineering Institute

- The Common Sense Guide to Mitigating Insider Threats, Seventh Edition
- Balancing Organizational Incentives to Counter Insider Threat
- Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump-Start an Insider Threat Program
- Insider Threats Across Industry Sectors
- Insider Threats in the Software Development Life Cycle
- Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls
- Analytic Approaches to Detect Insider Threats
- Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments
- Workplace Violence & IT Sabotage: Two Sides of the Same Coin?
- An Insider Threat Indicator Ontology