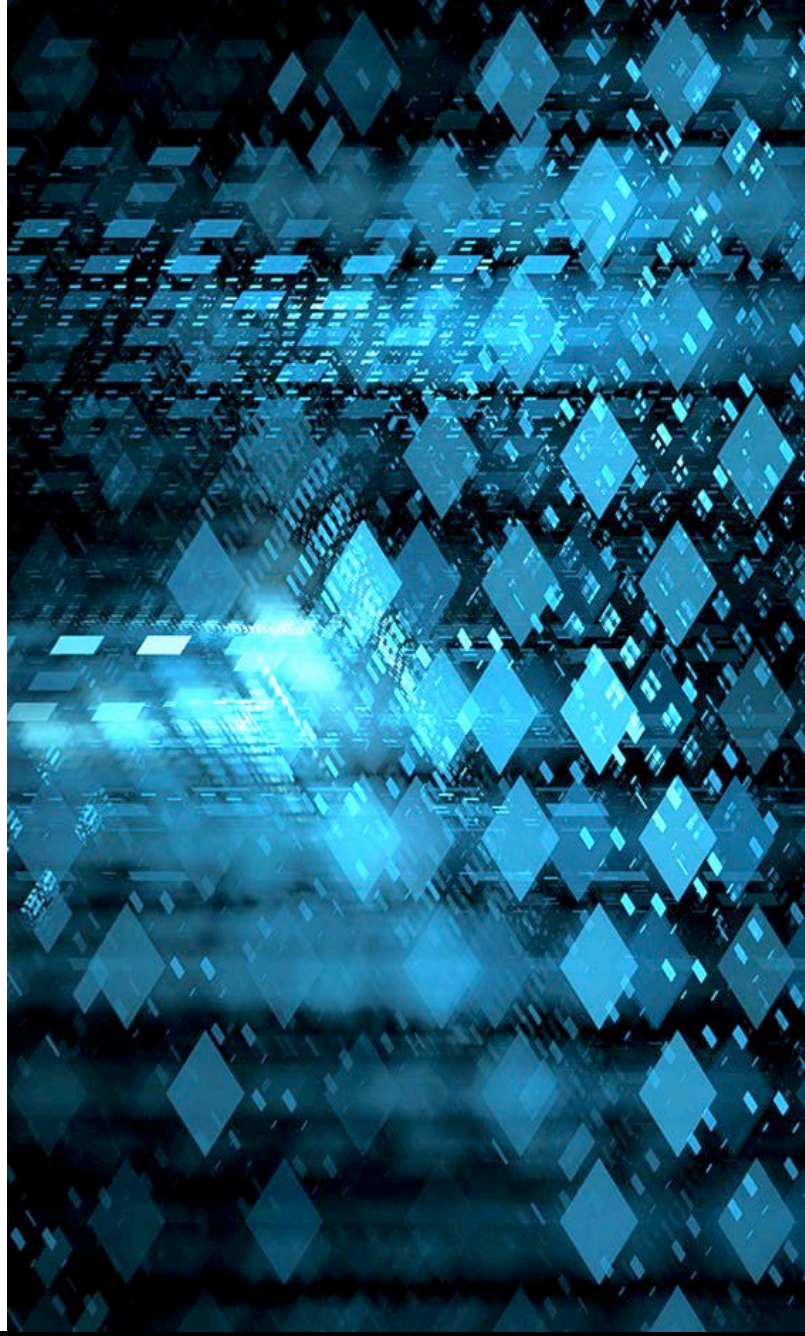
Module 1: Introduction

Insider Threat Program Evaluator Certificate

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Notices

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 is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

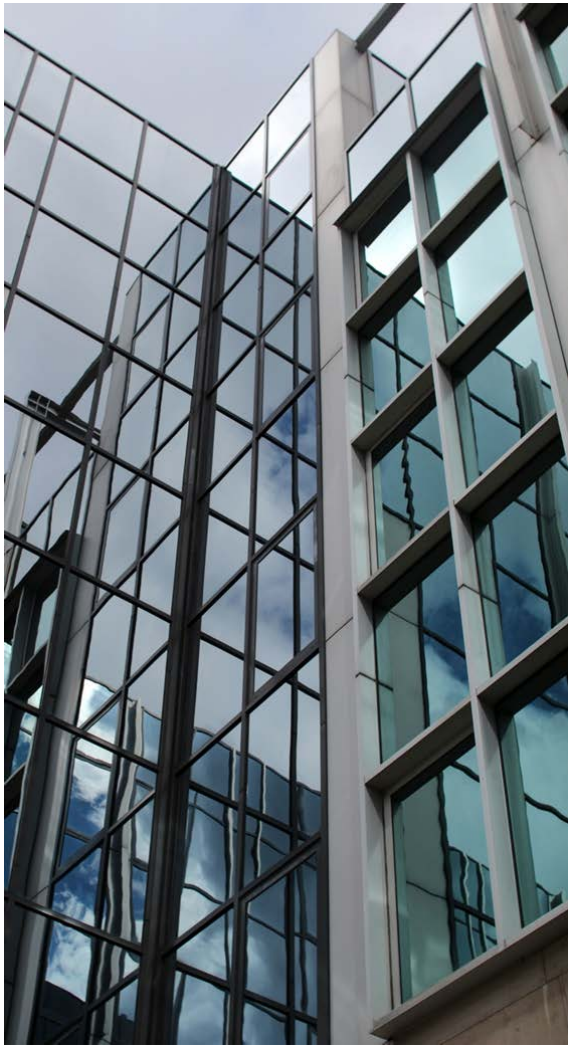
Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

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

DM18-0376

Introduction to the CERT National Insider Threat Center

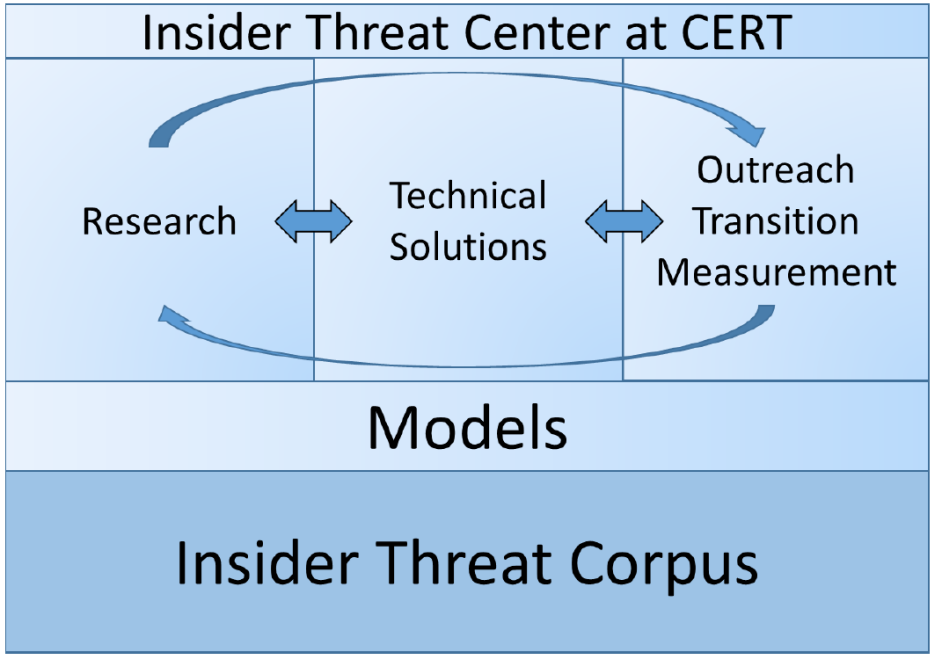
The CERT National Insider Threat Center (NITC)



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

Insider Threat Incident Corpus

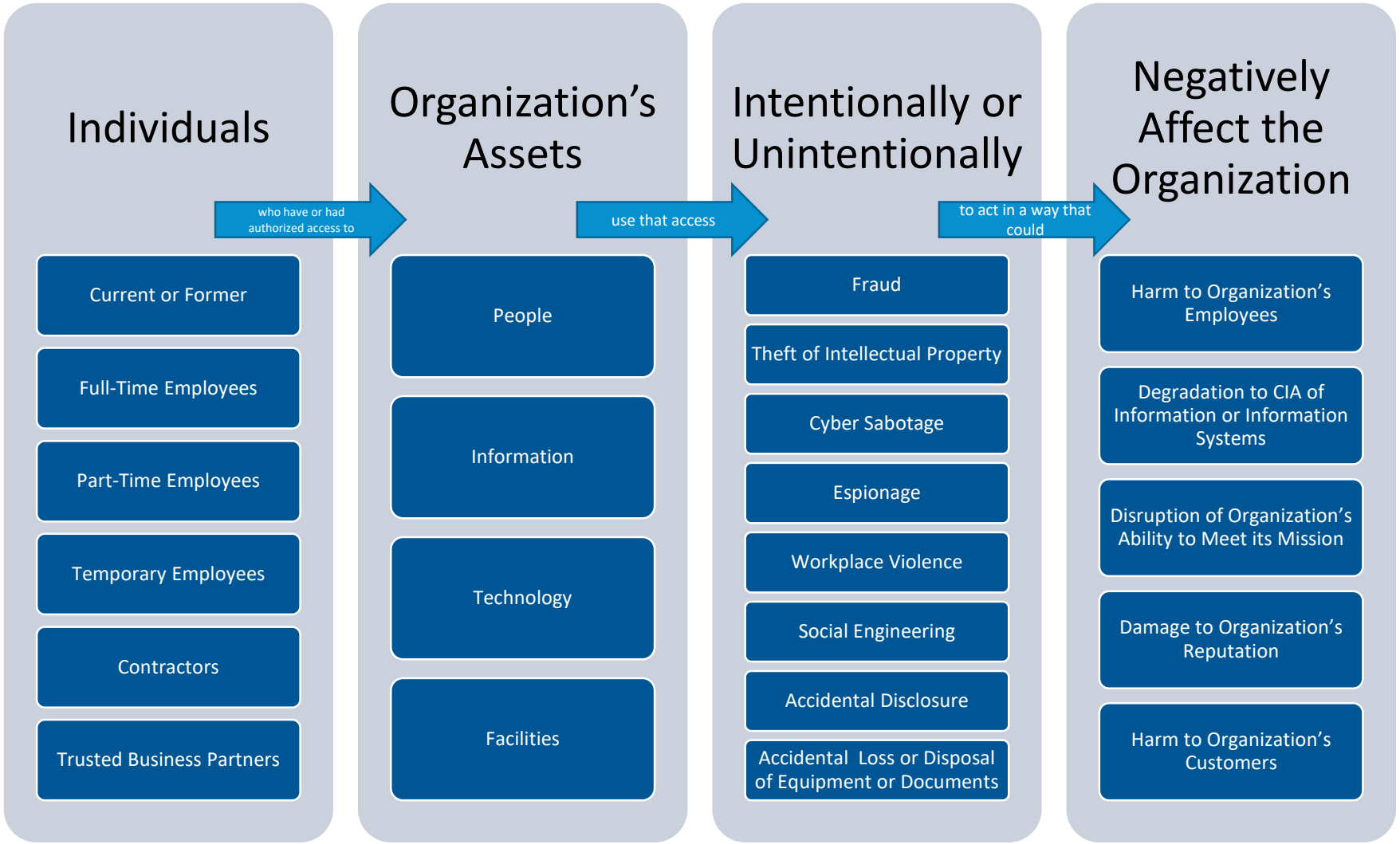
- Database of over 1600 insider threat incidents
  - Includes interviews of actual offenders
- Coded to allow analysis of technical actions & behaviors observables
- Development of technical controls to baseline and detect anomalous actions
- Research into areas of
  - Sentiment analysis
  - Workplace violence
  - Typing heuristics
  - Biometrics



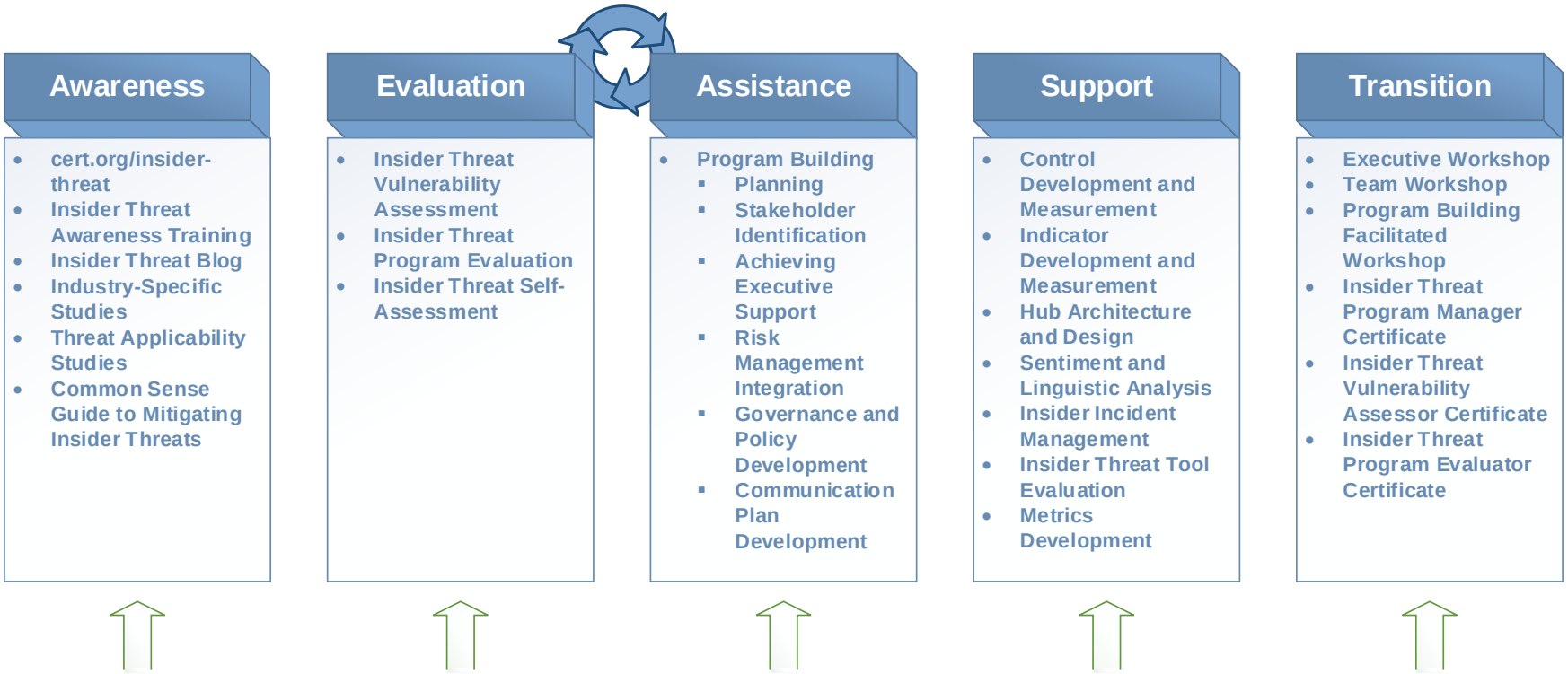
NITC's Definition of Insider Threat

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.

What / Who is an Insider Threat?



Our Insider Threat Portfolio



Overview of NITC Evaluation Instruments

A Little Bit More About Our Two Evaluations

The NITC has developed two types of Insider Threat related assessment instruments:

- The Insider Threat Program Evaluation (ITPE)
- The Insider Threat Vulnerability Assessment (ITVA)

The Evaluations Have a Different Focus and Purpose -1

The ITPE

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

The Evaluations Have a Different Focus and Purpose -2

The ITVA

- Is more narrowly focused on a particular part of the organization
- Specifically looks at critical assets and business processes that support key services related to the mission of the organization
- Looks across a broad range of potential vulnerabilities that might impact the system, asset, or process being assessed
- Is limited to only areas of concern observed in the hundreds of cases in the CERT insider threat database

An organization may have good controls and processes in place for certain assets and services but not others. This is why the ITVA is a focused assessment, not an enterprise-wide one.

Course Introduction

Purpose of This Course

Provide the basis for an organization to benchmark its insider threat program against defined criteria.

Present a methodology to assess the robustness of an organization's insider threat program.

Show one example of such a methodology: the NITC's Insider Threat Program Evaluation method.

Presents strategies for measuring and improving an operational insider threat program within an organization.

What Is the Scope of an ITPE?

The NITC ITPE

- can be applied to organizations with both unclassified and classified networks and data
- is applicable to the various types of insider threat activities:
  - IT Sabotage
  - IP Theft
  - Fraud
  - Unintentional Insider Threat
  - National Security Espionage
  - Workplace Violence

What The ITPE Is Not

The NITC ITPE is

- Not an audit
- Not a performance review
- Not a maturity model
- Not a vulnerability assessment
- Not looking for malicious insiders

The evaluation only evaluates how well the organization's insider threat program compares to the National Insider Threat Task Force (NITTF) minimum standards and NITC, government, and industry best practices.

Intended Audience -1

There are two types of audience participants who can attend this course.

Licensed Partners

- Are SEI Partners
- Will follow the NITC ITPE methodology
- Will receive NITC ITPE licensed materials
- Are interested in learning how to evaluate an insider threat program

General Assessors

- Are interested in learning a general evaluation methodology
- Will not necessarily use the CERT ITPE methodology
- Will not receive the CERT ITPE licensed materials
- Will receive an overview of the CERT ITPE methodology and materials
- Are interested in learning how to evaluate an insider threat program

Intended Audience -2

Assessors

- Those with evaluation experience
- Those wanting to expand their evaluation skills to include insider threat programs

Insider Threat Program Managers

- Those wanting to ensure their insider threat program has addressed common areas such as program management, training, infrastructure, and human resources

Insider Threat Program Staff

- Those who want to better understand insider threat program practices
- Those who may be assigned to perform evaluations

Others

- Managers or staff in other areas of an organization, who want to ensure their operations take into account insider threat program needs
- Others interested in learning what an insider threat program evaluation entails

Course Instructor Objectives

Identify types of capabilities (e.g., controls, policies, processes, and technologies) required for effective insider threat program.

Identify ways to evaluate the effectiveness of those capabilities.

Teach licensed partners how to use the CERT ITPE process and materials.

Provide a general introduction to the CERT ITPE process and materials for non-licensees (i.e., general assessors).

Participant Learning Objectives

After completing this course, participants will be able to

- Identify types of capabilities (e.g., controls, policies, processes, and technologies) required for effective insider threat program.
- Describe a basic process for performing insider threat program evaluations.
- Understand considerations in improving an insider threat program.
- List criteria for determining if program controls are in place to prevent, detect, and respond to insider threats.

Licensee Learning Objectives

After completing this course, licensed participants will also be able to

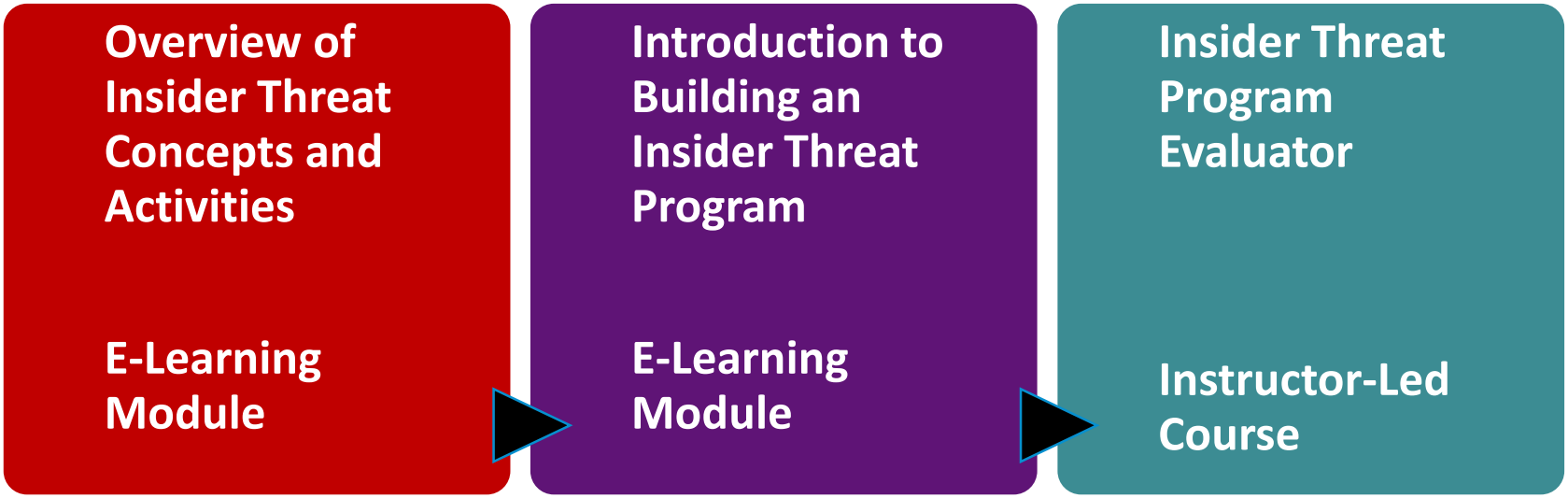
- Describe the process and components of the NITC ITPE
- Conduct a CERT ITPE, including performing
  - Planning and pre-evaluation activities
  - Data collection planning and interview scheduling
  - Documentation review, observations, and interviews
  - Indicator and capability scoring
- Complete an ITPE report including describing the process for
  - Uploading scored capabilities to the CERT Insider Threat Center for review and report development
  - Receiving a completed report from CERT
  - Handling issues and problems

Where Does This Course Fit?

This course is the last component you must complete before taking the exam for the ITPE Professional Certificate.

The other courses are e-learning modules and are prerequisites for this course.

When all three courses are completed, you can take the exam.



Course Format

.....

Course Outline -1 TBD

Module 1: Introduction

Module 2: General Insider Threat Vulnerability Assessment Components

Module 3: General Insider Threat Vulnerability Assessment Methodology

Module 4: Criteria and Capabilities for Assessment

Module 5: ITVA Essentials

Module 6: Introduction to ITVA Capabilities

Module 7: Assessment Planning

Course Outline -2 TBD

Module 8: Pre-Assessment

Module 9: Onsite Assessment

Module 10: Post Assessment

Module 11: Capability Analysis and Scoring

Module 12: Report Development

Module 13: Summary and Wrap-Up

Workshop Methodology

Sessions will contain

- Lectures
- Questions and answers
- Small and large group discussions
- Exercises

One of the primary methodologies used in this workshop is asking questions.

We will ask you lots of questions to help you think about these issues as they apply to your organizational situation.

General Workshop Materials

Contents

- PowerPoint slides

Supplemental materials

- Handouts
- Course attendance certificate
- Course evaluation online
- ITPE certificate (after passing exam)

Licensee Additional Materials

After licensees pass the exam, they will receive access to the ITPE Toolkit containing

- Four ITPE workbooks
- Briefing slides
- Templates for data collection and scheduling
- A copy of the latest Joint Assessment Tool (JAT) for scoring capabilities
- Access to the portal for submitting completed evaluations for report generation

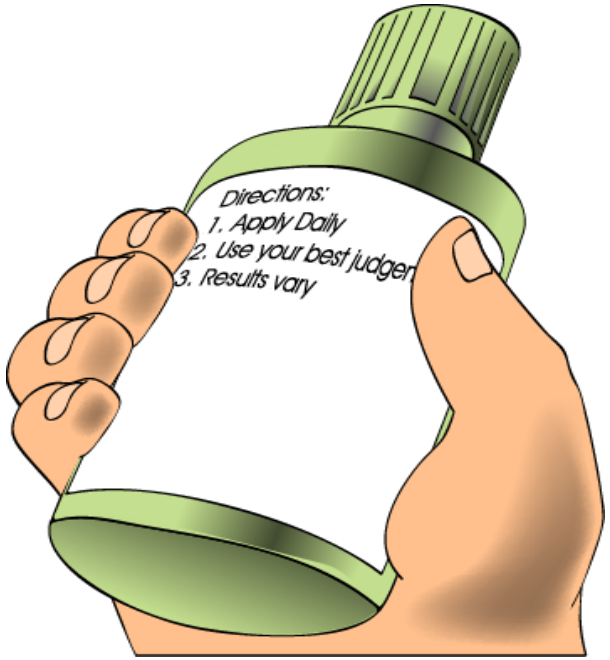
Applying this Material

Any evaluation effort must fit the organizational environment.

Take what makes sense for your situation.

- Your mileage may vary.
- Each organization may have diverse constraints, culture, and resources.

Remember that licensees have stricter requirements that must be met.



Introductions

Attendee Introductions

Please introduce yourself.

- Name and title
- Organization
- Your background and related experience in insider threat detection, prevention, and/or response
- Your evaluation experience
- The current status of the insider threat program within your organization
- Your expectations for the workshop
- Questions you would like to have answered during this workshop