Module 1: Introduction

Insider Threat Vulnerability Assessor Training

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.

DM20-1068

Course Introduction

Purpose of This Course

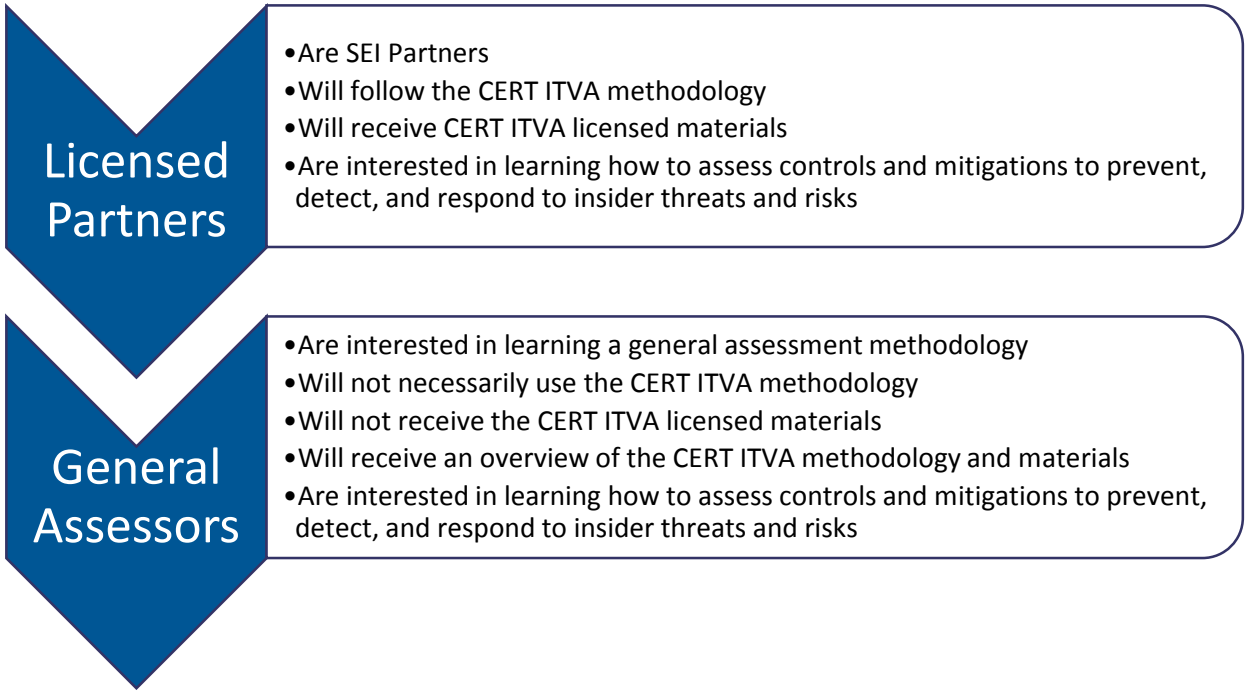
Provide the foundation for an organization to implement its own insider threat vulnerability assessment program.

Present a generic methodology to assess an organization's preparedness to prevent, detect, and respond to insider threats.

Show one example of such a methodology: the CERT Insider Threat Center's Insider Threat Vulnerability Assessment (ITVA) method.

Intended Audience -1

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



Intended Audience -2

Assessors

- Those with assessment experience
- Those wanting to expand their assessment skills to include insider threat risks, controls, and mitigations

Insider Threat Program Managers

- Those wanting to ensure their organization has addressed common organizational and technical vulnerabilities that might be exploited purposefully or accidentally by insiders

Insider Threat Program Staff

- Those who want to better understand controls and mitigations for insider threat risks
- Those who may be assigned to perform assessments

Others

- Managers or staff in other areas of an organization, who want to ensure their operations take into account insider threat risks and mitigations
- Others interested in learning what an insider threat vulnerability assessment entails

Participant Learning Objectives

After completing this course, participants will be able to

- Describe a basic process for performing insider threat vulnerability assessments
- Explain the significance of identifying critical assets and how it impacts any assessment
- Propose options for implementing an insider threat vulnerability assessment program
- Plan the steps to build, implement, and operate their assessment program
- Understand considerations in developing an insider threat vulnerability assessment program or process
- List criteria for assessing if controls and mitigations are in place to prevent, detect, and respond to insider threats related to fraud, IP theft, and IT sabotage

Licensee Learning Objectives

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

- Describe the process and components of the CERT Insider Threat Vulnerability Assessment (ITVA)
- Conduct a CERT ITVA, including performing
  - Scoping activities
  - Planning and pre-assessment activities
  - Data collection planning and interview scheduling
  - Documentation review, observations, and interviews
  - Indicator and capability scoring
- Complete an ITVA report including describing the process for
  - Uploading scored capabilities to the CERT Insider Threat Center for review and report development
  - Receiving an initial report from CERT; adding in customizations
  - Handling issues and problems

Where Does This Course Fit?

This course is the last component you must complete before taking the exam for the CERT Insider Threat Vulnerability Assessment (ITVA) Assessor 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 Outline

Module 1: Introduction

Module 2: ITVA Components

Module 3: ITVA Essentials

Module 4: ITVA Capability Overview

Module 5: ITVA Planning

Module 6: ITVA Pre-Evaluation

Module 7: ITVA On-site

Module 8: ITVA Post-Evaluation

Module 9: ITVA Scoring and Analysis

Module 10: ITVA Report Development

Module 11: Summary and Wrap-up

Workshop Methodology

Sessions will contain

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

Course Materials

There are three main documents you will be working with in the course besides your copies of the presentation slides

- Student Activity Guide
- Scenario Evaluation Instrument
- Scenario Evidence Collection

Other resources

- Licensee Brochure
- additional reading materials
- specific module document examples

Activity Guide

The student activity guide contains information and resources that are needed to complete the course exercises.

This includes the exercise scenarios and worksheets that will be used in the breakout rooms and in-class discussions.

Evaluation Instrument

The scenario evaluation instrument will be used as a resource and reference for many of the

- course exercises
- class examples and walkthroughs
- in-class discussions

The instrument is based on a small set of capabilities extracted from the CERT ITVA.

Evidence Collection

The Scenario Evidence Collection document will be used for a few exercises on the last day of class.

It will contain evidence collected from the scenario assessment that you will use to analyze and score capabilities reviewed.

Additional Reading Material

Additional Reading Material icon indicates that there are documents providing supplemental information beyond the module slides.

This additional information may be found in the file repository or the appendix of the Student Activity Guide.

These supplements are for the participants to read on their own in their own time.

Licensee Brochure

The Licensee Brochure contains information that explains ITVA processes and materials for participants who license the evaluation.

The brochure will contain additional details about what materials and resources are provided to licensees once they complete the course and the exam successfully.

This icon will appear whenever there are templates or other materials that the licensee receives with their ITVA files.

Applying this Material

Any assessment program 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.

Overview of CERT NITC Evaluation Instruments

More About Our Evaluations

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

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

Each Instrument Has a Different Focus and Purpose -1

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.

Each Instrument Has a Different Focus and Purpose -2

ITVA

- Is more narrowly focused on a particular part of the organization
- Looks specifically 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 NITC insider threat case corpus

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.

What Do We Mean By *Vulnerability Assessment*?

We define an insider threat *vulnerability assessment* as an evaluation of the type of vulnerabilities an organization may be susceptible to.

Such an assessment is focused on identifying insider threat vulnerabilities—organizational, behavioral, or technical vulnerabilities that a malicious insider could take advantage of to do harm to a company or institution and its critical assets.

What Is the Scope of a Vulnerability Assessment?

A vulnerability assessment can be applied to both unclassified and classified systems.

Vulnerabilities can be both **Technical** and **Behavioral** in nature, including but not limited to

- Psychological
- Process based
- Policy based
- Control based

What a Vulnerability Assessment Is Not

For our definition, a vulnerability assessment is

- Not an audit
- Not a compliance exercise or performance review
- Not a maturity model
- Not an evaluation of an Insider Threat Program
- Not looking for malicious insiders

The assessment only evaluates how well an organization would do against vulnerabilities exploited by real malicious insiders or other potential vulnerabilities.

Introductions

Attendee Introductions

Please introduce yourself.

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