Carnegie Mellon University
Software Engineering Institute

# INSIDER THREAT VULNERABILITY ASSESSMENT (ITVA) – OVERVIEW



## Introduction

Since 2001, the CERT Division of the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) at Carnegie Mellon University (CMU), has conducted research and gathered data about actual malicious insider acts including IT sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to our Nation's critical infrastructures.

This research and work has been done by the CERT Insider Threat Center. To date this center has collected, coded, and analyzed more than 1600 cases of malicious insider attacks against organizations.

## What is a malicious insider?

Current or former employee, contractor, or other business partner who

- has or had authorized access to an organization's network, system, or data and
- intentionally exceeded or misused that access in a manner that
- negatively affected the confidentiality, integrity, or availability of the organization's information or information systems or harm the organizations assets or reputation [1]

## What is the ITVA?

The ITVA is an assessment that helps identify potential vulnerabilities in unclassified systems, data, and processes that can be exploited by malicious insiders. It is based on actual methods (vulnerabilities) used by real insiders. It is based on the empirical data collected in the 1000+ insider threat cases coded by the CERT Insider Threat Center.

The objective of the ITVA is to assist organizations in reducing exposure to damage from potential insider threats. Given the variety of attack vectors

[1] A more detailed description of various definitions related to insider threat and malicious actions that can result in harm to an organization can be found at https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

available to malicious insiders, determining how vulnerable an organization is to insider threat can be difficult. The scope of an ITVA is limited to organization-defined critical services, and the assessment focuses on the people, technology, information, business processes, and facilities that support those services. There are five activities that comprise the ITVA Process:

1. Assessment Planning
2. Pre-Assessment
3. Assessment
4. Post-Assessment

The ITVA team performs interviews, observations of work activity, and document reviews to collect relevant data for the assessment.

**Why is my organization participating?**

Your organization has requested that the SEI conduct an assessment of the organization's preparedness to prevent, detect, and respond to insider threats.

**Why am I involved?**

Because your roles and/or responsibilities involve some aspect of activities related to prevention, detection, and response to malicious or unintentional insider behavior or actions, your management has selected you to participate.

**What am I expected to do?**

You do not need to prepare in advance. The ITVA team will lead you through the relevant questions about capabilities that relate to your organization. You may be asked to participate in an interview or to perform an activity for observation by the ITVA team. If so, we ask that you

- cooperate with the interviewers or observers
- be available to participate when asked or scheduled
- be prepared to discuss your work activities, roles, and responsibilities
- provide copies of documents and work products as appropriate
- demonstrate specific activities or tools as part of an observation if asked

**How will the information be used?**

The information obtained, collected, and reviewed during this assessment is considered sensitive. Your responses are confidential. Information that you provide will not, in any way, be attributed to you.

The analysis of consolidated document reviews, interviews, and observations are used to arrive at a set of results for this assessment. A final report is presented to designated organizational stakeholders.

**Is this an official audit or certification?**

No, it is not an audit or certification of any organizational functions, nor is it a compliance assessment.

**Will our organization be scored on this assessment?**

The ITVA methodology uses seven workbooks. Each workbook has a set of capabilities related to the workbook topic. Each capability has a set of indicators used to determine if the capability is being met and if met, at what level of robustness. An indicator is marked as being met or not. Based on the indicators met, a preparedness "level" score is provided. The level definitions are seen below.

| Preparedness Level | Description |
|---|---|
| 4 | The organization has exceptional controls and policies in place. The organization is prepared to Prevent / Detect / Respond to the issue of concern. |
| 3 | The organization has adequate controls and processes in place. The organization is partially prepared to Detect and Respond, but has issues Preventing the issue of concern. |
| 2 | The organization has minimal controls and processes in place. The organization is prepared to Detect), but has issues Preventing or Responding to the issue of concern. |
| 1 | There is a failure in an organization's ability to meet the capability. The organization is not prepared to perform this capability. |

Results from the ITVA can provide the organization with business justification for implementing improvements and revising resources. The scores can be used by an organization to identify gaps in practice. The information can also be leveraged by the organization to help prioritize which improvements should be done first (e.g., which are the most critical or have the highest priority).

## Legal 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.



DM23-0882

## Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

**Phone**: 412/268.5800 | 888.201.4479
**Web**: www.sei.cmu.edu
**Email**: info@sei.cmu.edu