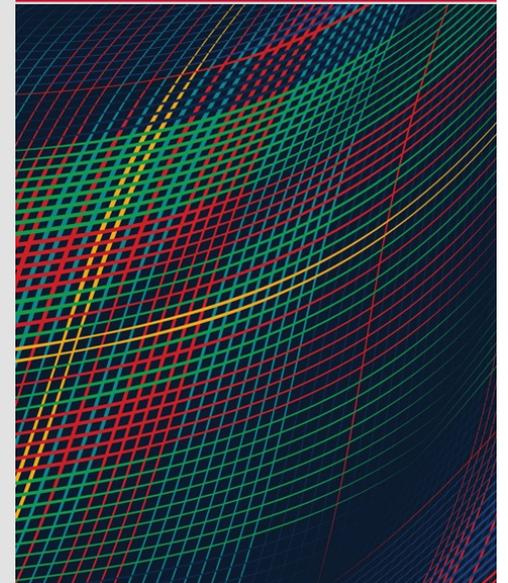


Insider Threat Vulnerability Assessment (ITVA) Exit Briefing

MONTH 00, 2023

FirstName LastName
Very Smart Researcher



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.

* 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.

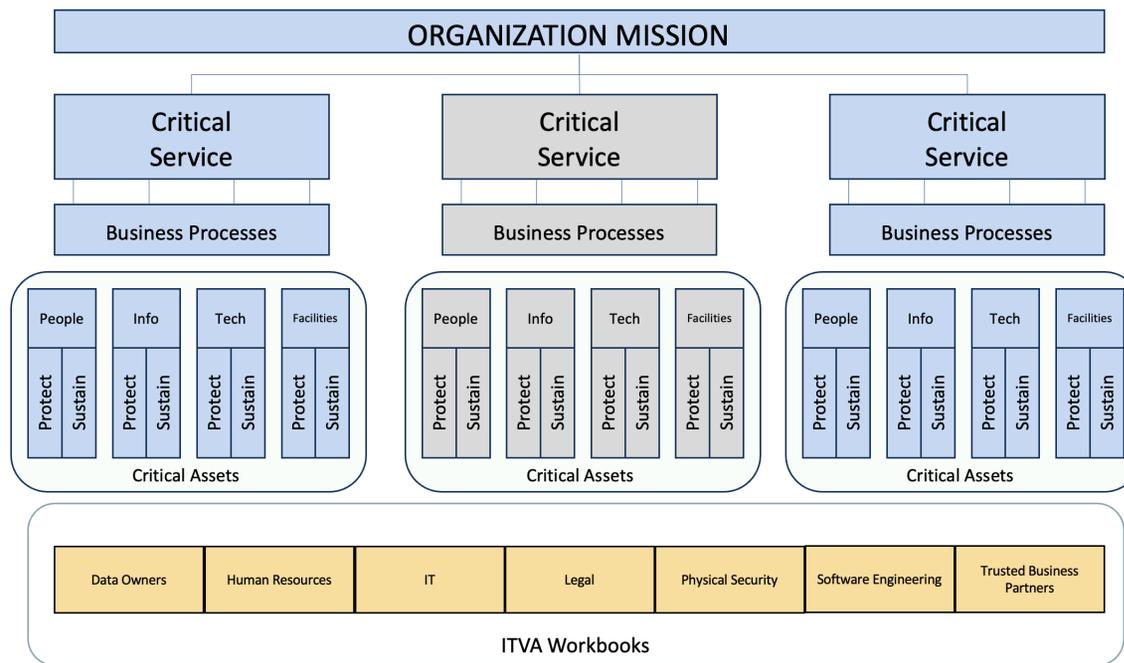
DM23-0882

SEI Insider Risk ITVA Process Review

**Carnegie
Mellon
University**
Software
Engineering
Institute

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

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

Assessment Methodology

Assess Scoped Business Processes.

- Conduct interviews with key personnel.
- Review key company artifacts.
- Review data sources used for analysis.
- Review tools.

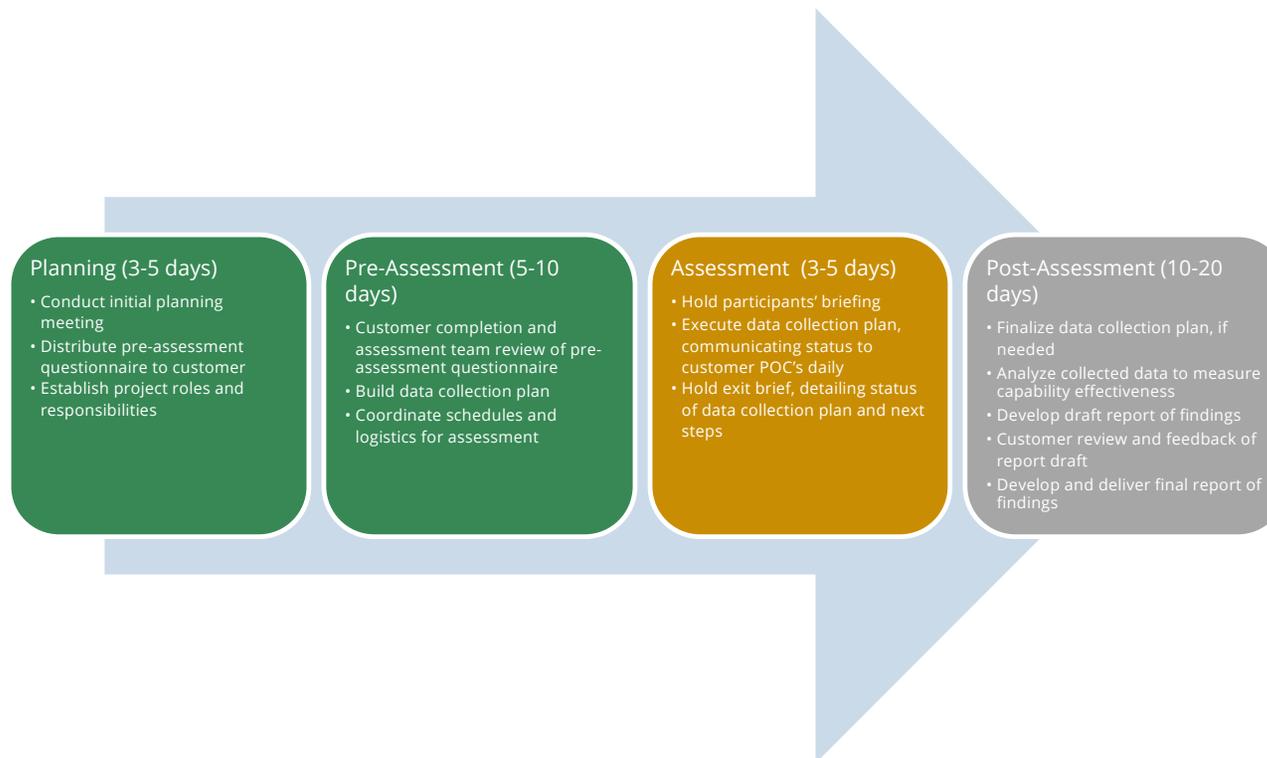
The ITVA methodology is designed to

- encompass policies, practices, and technologies
- focus on all three aspects of insider threat: prevention, detection, and response

Provide a final report that enumerates

- strengths
- gaps
- prioritized recommendations

ITVA Process Flow and Timeline



Data Collection

XX documents provided and reviewed pre-assessment
XX additional documents requested and received during on-site
XX documents total

XX total on-site interviews conducted <Dates>

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

Q&A / Open Discussion

