Insider Threat Vulnerability Assessment

The Situation

To effectively mitigate the threats posed by trusted insiders, you must understand your organisation's susceptibility to internal threats.

CommsNet Group **Insider Threat Vulnerability Assessment** which is based upon CERT Carnegie Mellon University methodology helps you determine how well prepared you are to prevent, detect, and respond to insider threats, should they appear in your organisation.

The assessment takes a holistic approach to identifying threats by identifying your business vulnerabilities, business process gaps, management issues and your ability to effectively integrate behavioural analytics into your threat assessment process.

Insider threat problem is complex and therefore, organisations need an approach that

- Encompasses policies, practices, and technologies
- Is empirically based, yet adaptable to current trends and technologies
- Focuses on prevention, detection, and response strategies

Vulnerability Examples

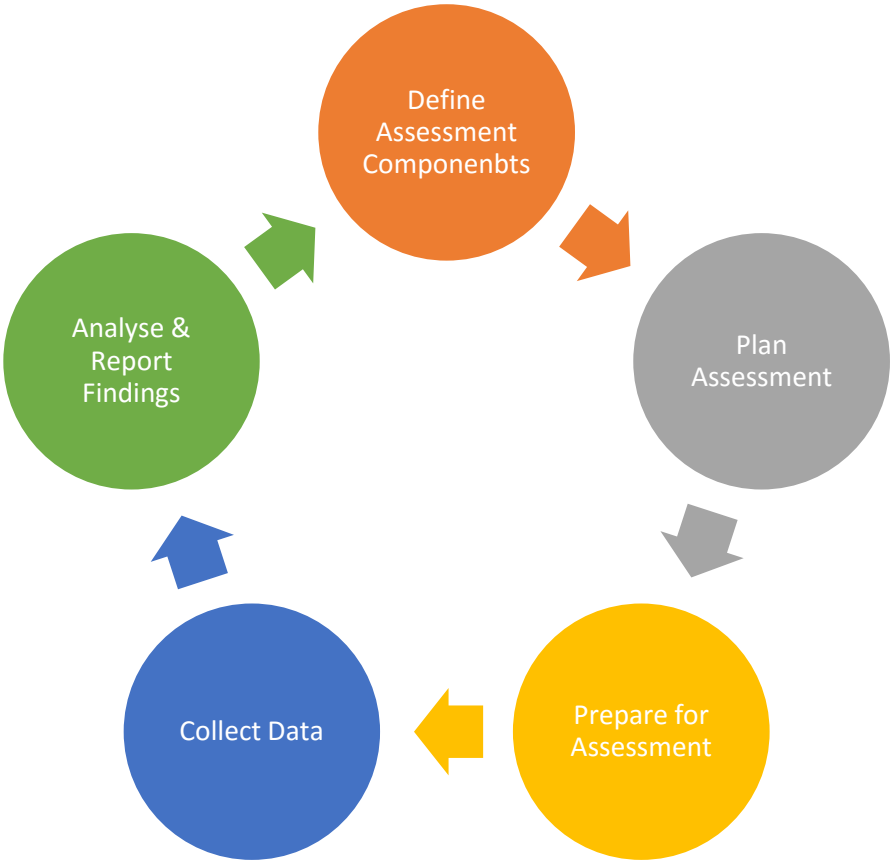
Technical	No method for detecting ex-filtrated intellectual property
Organisation	HR does not share information with IT on employees to be terminated
Process	No background checking of candidates for hire is performed
Security	There are no physical controls preventing access to critical data servers.

The **Insider Threat Vulnerability Assessment** enables your organisation to gain a better understanding of insider threat and an enhanced ability to assess and manage associated risks. The assessment toolset methodology, which is based on CERT's more than 1000 insider threat incidents in the key corpus, encompasses information technology, human resources, physical security, business processes, legal, management, contracting, and organizational issues. It merges technical, behavioural, process, and policy issues into a single, actionable framework.

By asking us to perform an assessment on your organisation, you take the first step in safeguarding your critical assets, gaining a better understanding of your vulnerability to insider threats, and managing the risks associated with them. The assessment results benefit everyone involved in the vulnerability assessment process and provides a measure of your organisation's preparedness to prevent, detect, and respond to the threats posed by insiders

Assessment Methodology

The Insider Threat Vulnerability Assessment program is based on the following methodology



Define Assessment

The criticality of this phase is to identify the following:

- The organisation structure and authority of the program. Whom within the organisation will drive this assessment? Which people will be involved?
- The scope of the program. What area within the organisation will this assessment cover?
- How will data be collected, stored and protected? Who will have access to it?
- What policies must we follow?
- What scoring mechanisms should we use?

Plan Assessment

Planning includes but is not limited to the following

- Scheduling the timeframe for the assessment
- Identifying all point of contacts
- Performing the coordination and scheduling activities

Prepare for Assessment

A key part of this phase, is to understand the organisation and its operations, infrastructure and culture. We will collect and review information ahead of time related to the following:

- Critical assets
- Network topology
- Corporate boundary defences (physical, wireless, removable, mobile)
- Existing policies and procedures
- Staff roles and responsibilities (type of people to interview or observe)

Collecting Data

Based on the criteria that we set in (Define Assessment), we collect data to be able to observe metrics. It can be collected in various manner:

- Interviews
- Documentation / Policy review
- Observations
- Shadowing
- Survey
- Exercises

Analyse & Report Findings

The analysis is looking at each criteria and scoring.

- Based on evidence, is the criteria met?

We then develop a report. In the report, it will include

- Overview of assessment
- Scores
- Highlights of strength & weaknesses
- Highlights of significant gap areas
- Specific vulnerabilities to be addressed immediately
- Recommendation for improvements

- Opportunity for feedback & review from organisation before a final report is produced

Once completed, we destroy all notes and material at the end of the ITVA.

The Insider Threat Vulnerability Assessment is not an audit nor an enterprise-wide risk assessment, but a focused vulnerability assessment on your key business systems

Deliverable & Completion Time

For the assessment, members of our insider threat staff spend five to ten days at your organisation.

During that time, we review documents, interview key personnel in your organisation, and observe key processes and security issues. We sign a non-disclosure agreement to ensure that all collaborations remain confidential.

After the onsite visit, we analyse the data and then provide you with a confidential report that contains the findings of the assessment to help you understand your exposure to insider threats along multiple vectors (technical, behavioural, process, and policy) and deliver a single actionable framework to manage these issues and associated risks. This could take anywhere between five to 10 days.

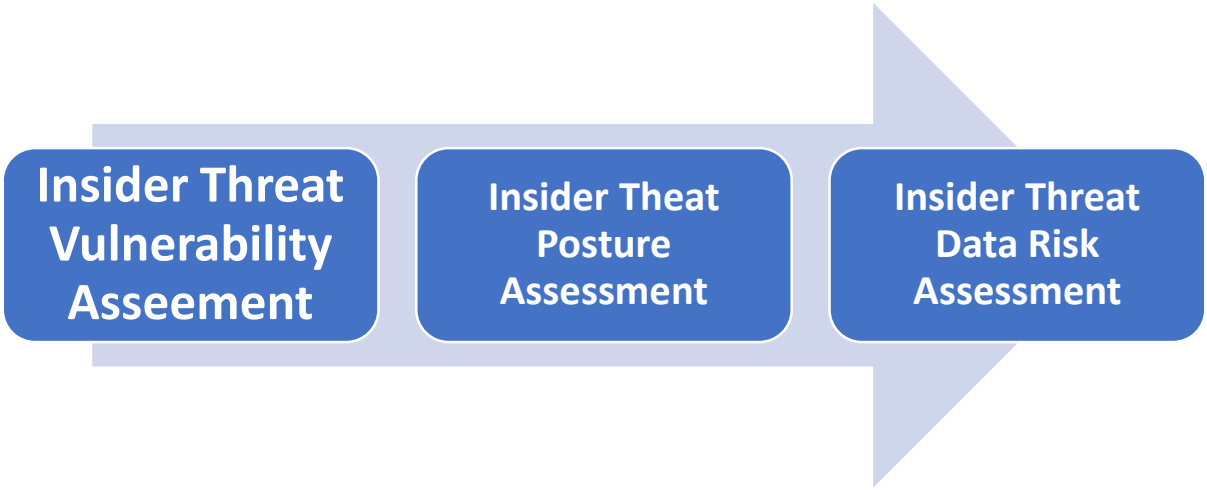
Benefits

Other organizations have used their reports to

- Understand how well their organisation is able to respond and prevent insiders exploiting vulnerabilities to cause damage, disruptions and loss
- Immediately identify specific vulnerabilities to be addressed
- Identify and implement short-term tactical countermeasures. That is address and improve on gaps and weaknesses
- Guide their ongoing risk management process for implementing long-term, strategic countermeasures for building insider threat best practices.
- Justify follow-up actions to key decision makers

IDENTITY Service Process

Where Does **Insider Threat Vulnerability Assessment Sit** as Part Of CommsNet Group IDNETITY Services?



Question: What are the differences between the services?

- Insider Threat Vulnerability Assessment focuses on your business risk
- Insider Threat Posture Assessment focuses on your technical risks
- Insider Threat Data Risk Assessment focuses only on your data risks

Key Takeaway

The Insider Threat Vulnerability Assessment (ITVA) is more narrowly focused on a particular part of the organisation. It specifically looks at critical assets and business processes that support key services related to the mission of the organisation.

It looks across broad range of potential business vulnerabilities that might impact the system, asset or processes being assessed.

The CommsNet Group Advantage

CommsNet Group is the first company to partner with the Carnegie Mellon University Software Engineering Institute (SEI) in the Asia/Pacific region for Insider Threat and licensed to provide official SEI services in Insider Threat Vulnerability appraisals.

Carnegie Mellon University works with the U.S. Computer Emergency Response Team (CERT) to analyse known insider threat cases in an effort to draw attention and understanding of motivation and opportunity and to help communicate important risk factors.

This unique partnership enables CommsNet Group to provide a unique combination of services and solutions:

- An assessment of an organization’s capabilities to prevent, detect and respond to insider threats
- Solutions to fill the gaps identified during the assessment
- Expertise to assist them in building a program to tie everything together