CERT | Software Engineering Institute
Carnegie Mellon University

Vulnerability Assessment

CERT Insider Threat Center

To effectively mitigate the threats posed by trusted insiders, you must understand your organization's susceptibility to threats. The CERT Insider Threat Vulnerability Assessment helps you determine how prepared you are to prevent, detect, and respond to insider threats, should they appear in your organization. The assessment takes a holistic approach to identifying threats by identifying your technical vulnerabilities, business process gaps, management issues, and your ability to effectively integrate behavioral analytics into your threat assessment process.

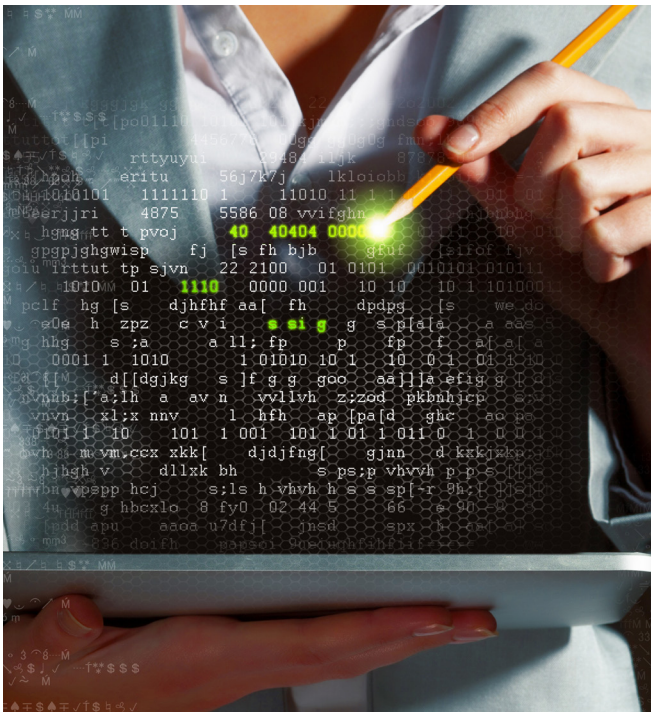
Our research has proven that the insider threat problem is complex; therefore, organizations need an approach that

- encompasses policies, practices, and technologies
- is empirically based, yet adaptable to current trends and technologies
- focuses on prevention, detection, and response strategies

Our assessment enables your organization 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 more than 1000 insider threat incidents in our corpus, encompasses information technology, human resources, physical security, business processes, legal, management, contracting, and organizational issues. It merges technical, behavioral, process, and policy issues into a single, actionable framework.

Using the insider threat incident repository, we examine the problem from technical, behavioral, process, and policy perspectives to form an approach to help you develop strategies that prevent, detect, and respond to insider threats.

By asking us to perform an assessment on your organization, 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 provide a measure of your organization's preparedness to prevent, detect, and respond to the threats posed by insiders.

Assessment Process

For the assessment, members of our insider threat center staff spend three to five days at your organization. During that time, we review documents, interview key personnel in your organization, 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 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, behavioral, process, and policy) and deliver a single actionable framework to manage these issues and associated risks.

Other organizations have used their reports to

- identify and implement short-term tactical countermeasures
- guide their ongoing risk management process for implementing long-term, strategic countermeasures
- justify follow-up actions to key decision makers

For more information, visit
cert.org/insider-threat/products-services/vulnerability-assessments.cfm

What Is Insider Threat?

A malicious insider threat to an organization is a 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. In addition, insider threats can also be unintentional (non-malicious).

The CERT Insider Threat Center

At the CERT Insider Threat Center, we conduct empirical research and analysis to develop and transition sociotechnical solutions to combat insider cyber threats. We have been researching this problem since 2001 in partnership with the Department of Defense, the Department of Homeland Security, the U.S. Secret Service, Federal Bureau of Investigation, other federal agencies, the intelligence community, private industry, academia, and the vendor community.

The foundation of our work is our database of more than 1300 insider threat incidents. We use system dynamics modeling to characterize the nature of the insider threat problem, explore dynamic indicators of insider threat risk, and identify and experiment with administrative and technical controls for insider threat mitigation.

Housed within the Insider Threat Center is an insider threat lab that provides a foundation to identify, tune, and package technical controls as an extension of our modeling efforts. We developed the assessment framework based on fraud, theft of intellectual property, IT sabotage, and unintentional insider incidents to help you identify your technical and nontechnical vulnerabilities to insider threats as well as executable countermeasures.

As part of a Federally Funded Research and Development Center (FFRDC), the CERT Insider Threat Center is uniquely positioned and has been serving as a trusted broker to assist the community through its ongoing research for more than a decade.

About

For nearly 30 years, the CERT Division of the Software Engineering Institute (SEI) of Carnegie Mellon University has been a leader in cybersecurity. Originally focused on incident response, we have expanded into cybersecurity areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threats, digital intelligence and investigation, workforce development, devops, forensics, software assurance, vulnerability discovery and analysis, and risk management.

Contact Us

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

Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu