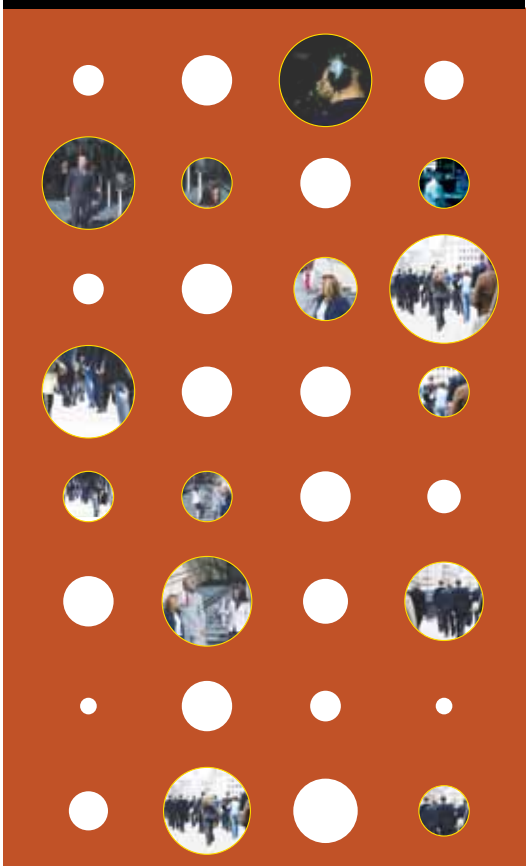
CERT

Software Engineering Institute

Carnegie Mellon

Creating a Customized Insider Threat Program

A single insider threat strategy may not be appropriate for all organizations. The purpose of this workshop is to work with executives in an organization to design an insider threat program. Using actual data from the organization, we are able to help the executives tailor a program that specifically suits their needs.



Customized Insider Threat Executive Workshop

Offering Our Expertise

For the past decade, members of the CERT® Insider Threat Center have been researching insider threat, conducting assessments of organizations, and presenting workshops. We also have a database of more than 550 actual insider threat cases, from which we have extracted a list of technical and non-technical methods used by malicious insiders, including current and former employees, contractors, and business partners.

The Customized Insider Threat Executive Workshop is based on the standard Insider Threat Workshop, and it focuses explicitly on an organization's specific needs and objectives. The workshop leverages our expertise in the field of insider threat to assess an organization's own experiences with malicious insider activity, existing security controls, business processes, and unique organizational culture. The end result is a strategic action plan, developed with our guidance and created and endorsed by senior leadership. The organization can immediately implement this plan after the workshop to address and mitigate the risk of insider threat.

The Workshop Consists of Two Phases

This workshop differs from the public workshop because the course material is tailored to use actual malicious insider incidents that occurred in the organization. To prepare for the customized workshop, the organization provides us with a number of insider cases so that we can understand the organization's threat landscape. For three days prior to the workshop, members of the Insider Threat Center will be onsite at the organization, interviewing staff members who are familiar with the set of insider cases. We treat all customer data as confidential and do not publicly distribute it.

The actual workshop spans two days. The first day consists of presentations and interactive exercises, which help participants assess their organization's vulnerability to insider threat. The second day focuses on providing participants with actionable steps to better manage the risk of insider threat. On the second day, we help participants develop a strategic action plan to address the risk of insider threat in their organization. This action plan is useful because it is created and endorsed by senior leadership, addresses the particular problems faced by the organization, and considers the organization's unique corporate culture.

Software Engineering Institute

Carnegie Mellon

For more information about our research, visit the CERT® website:

www.cert.org/insider_threat

For more information about this workshop, email Insider Threat Center staff:

insider-threat-feedback@cert.org

Customized Insider Threat Executive Workshop (continued)

Multiple Departments Must Be Involved

The target audience for the workshop is senior executives and decision makers within an organization. However, the complex nature of the insider threat problem requires a holistic approach. Multiple departments must be involved in the overall strategy. These departments include, but are not limited to, human resources, information technology, legal and contracting, physical security, and software engineering. This inter-departmental cooperation is the key to creating an effective strategy against insider threat.