Insider Threat Program Development Workshop

The Customized Insider Threat Program Development Workshop is designed to focus explicitly on an organization's specific needs and objectives as it builds an insider threat program. The workshop leverages our expertise in the field of insider threat to assess an organization's own experiences with insider activity. The CERT Insider Threat Center's experts help the organization develop and implement security controls and business processes that address the insider threat and are customized to the organization's 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.

This service is different from the Insider Threat Vulnerability Assessment. The Insider Threat Program Development Workshop helps an organization build a formal insider threat program rather than measure an organization's preparedness to prevent or detect specific technical and behavioral vulnerabilities. The workshop's intended audience is organizations who are considering building an insider threat program or are in the early stages of program development.

Workshop Approach

This workshop begins by tailoring the CERT Insider Threat Workshop to use actual insider incidents that occurred in the participating organization. To prepare for the customized workshop, the organization provides the CERT Insider Threat Center with a few insider incidents so that we can understand the organization's threat and vulnerability landscape. For three days prior to the delivery of the customized workshop, members of the CERT Insider Threat Center will be onsite at the organization, interviewing staff members who are familiar with the set of insider incidents as well as organizational units and key personnel who will be involved in the development and implementation of the insider threat program.

The workshop spans two days. The first day consists of presentations and interactive exercises that help you assess your organization's vulnerability to insider threat. The second day focuses on developing actionable steps to better manage the organization's risk of insider threat. We help you to develop a strategic action plan to address the risk of insider threat in your organization. This action plan is created and endorsed by senior leadership, addresses the particular problems faced by your organization, considers the minimum standards required for insider threat programs, and tailors the program to fit your organization's unique corporate culture.

The target audience for the workshop consists of senior executives and decision makers. 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. Inter-departmental cooperation is the key to creating an effective strategy against insider threat.

For more information, read our brochure at http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=51652.

Develop a Customized Insider Threat Program

A single insider threat strategy may not be appropriate for all organizations. The purpose of the facilitated 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.

New CERT Insider Threat Solutions

A CALL FOR ACTION....

On October 7, 2011, President Obama signed Executive Order 13587 (EO) – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information – which states that federal agencies that operate or access classified computer networks must implement an insider threat detection and prevention program.

In addition, proposed changes to the National Industrial Security Program Operating Manual (NISPOM) will require contractors that engage with federal agencies that operate or access classified computer networks to also implement an insider threat program in accordance with EO 13587.

.... TO PREVENT, DETECT, AND RESPOND TO INSIDER THREATS.

As a trusted third party between government, industry, and academia, the CERT Insider Threat Center is in a unique position to help organizations with their insider threat challenges. However, the need for qualified experts to support organizations in the development and operation of insider threat programs is now greater than ever. To meet this growing demand, we are developing new solutions to transition our important research to enable others to also provide this critical support.

Our new insider threat training and certificate programs will educate professionals on how to help organizations identify and manage their insider threat risks, and how to measure their preparedness to defend against them. The new programs will also teach how to evaluate an organization's insider threat program, or even build and operate one from scratch.

To assist organizations, the CERT Insider Threat Center is developing training and certificate programs for the following roles:

Insider Threat Program Manager Certificate (ITPM-C)

The ITPM program will assist insider threat program managers with the development a formal insider threat program.

Now Available

Insider Threat Vulnerability Assessor Certificate (ITA-C)

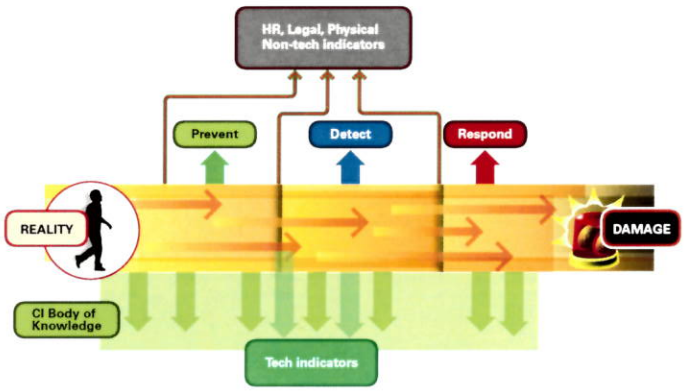
The ITA program will enable authorized assessors to help organizations gain a better understanding of their insider threat risk and an enhanced ability to identify and manage associated risks.

Expected Program Launch – Fall 2014

Insider Threat Program Evaluator Certificate (ITPE-C)

The ITPE program will enable evaluators to help organizations gain a better understanding of the effectiveness of their established insider threat programs.

Expected Program Launch – Winter 2014



Opportunities to Prevent, Detect, and Respond to an Insider Incident

Insider Threat Program Manager (ITPM) Certificate

The ITPM certificate program will assist insider threat program managers developing a formal insider threat program. The certificate will cover areas such as insider threat planning, identification of internal and external stakeholders, components of an insider threat program, insider threat team development, strategies for effective communication of the program, and how to effectively implement and operate the program within the organization.

Components

COURSE	DELIVERY	AUDIENCE	COMPLETION DATE
Insider Threat Overview: Preventing, Detecting, and Responding to Insider Threats This 5-hour course provides a deep er understanding of insider threat terminology, identifies the different types of insider threats, teaches how to recognize both technical and behavioral indicators, and outlines mitigation strategies.	E-learning	Team Members Program Managers	Available
Building an Insider Threat Program This 7-hour course is to provide a thorough understanding of the organizational models for an insider threat program, the necessary components to have an effective program, the key stakeholders who need to be involved in the process, and basic education on the implementation and guidance of the program.	E-learning	Team Members Program Managers	Available
Insider Threat Program Implementation and Operation This 3.5-day course is to develop the skills and competencies necessary to oversee the development, implementation, and operation of an effective insider threat program.	Classroom	Program Managers	Available
Insider Threat Program Manager Certificate Exam Candidate managers must successfully complete this exam to obtain the certificate.	Online Exam	Program Managers	Available

To sign up for program updates, go to cert.org/insiderthreat

Extensive research, comprehensive solutions, and technical expertise have made the CERT Division a sought-after leader in the prevention, detection, and mitigation of insider threats. Now it's your turn to act, with support from the CERT Insider Threat Center.

Insider Threat Vulnerability Assessor (ITA) Certificate

The ITA program enables assessors to help organizations gain a better understanding of their insider threat risk and an enhanced ability to identify and manage associated risks. The assessment methodology assists organizations by measuring how prepared they are to prevent, detect, and respond to the insider threat. Organizations will have the ability to license the CERT Insider Threat Vulnerability Assessment tool for internal use or to assess others for potential vulnerabilities.

Components

COURSE	DELIVERY	AUDIENCE	COMPLETION DATE
Insider Threat Overview: Preventing, Detecting, and Responding to Insider Threats This 5-hour course provides a deeper understanding of insider threat terminology, identifies the different types of insider threats, teaches how to recognize both technical and behavioral indicators, and outlines mitigation strategies.	E-learning	Team Members Program Managers Candidate Assessors	Available
Building an Insider Threat Program This 7-hour course is to provide a thorough understanding of the organizational models for an insider threat program, the necessary components to have an effective program, the key stakeholders who need to be involved in the process, and basic education on the implementation and guidance of the program.	E-learning	Team Members Program Managers Candidate Assessors	Available
Insider Threat Vulnerability Assessor Training This 4-day course develops the skills and competencies necessary to perform an insider threat vulnerability assessment of an organization.	Classroom	Candidate Assessors	Fall 2014
Insider Threat Vulnerability Assessor Certificate Exam Candidate assessors must successfully complete this exam to obtain the certificate.	Online Exam	Candidate Assessors	Fall 2014

To sign up for program updates, go to cert.org/insiderthreat

Extensive research, comprehensive solutions, and technical expertise have made the CERT Division a sought-after leader in the prevention, detection, and mitigation of insider threats. Now it's your turn to act, with support from the CERT Insider Threat Center.

Insider Threat Program Evaluator (ITPE) Certificate

The ITPE program enables evaluators to help organizations gain a better understanding of the effectiveness of their established insider threat programs. Organizations will have the ability to license the CERT Insider Threat Program Evaluation methodology for internal use or to evaluate the effectiveness of other programs.

Components

COURSE	DELIVERY	AUDIENCE	COMPLETION DATE
Insider Threat Overview: Preventing, Detecting, and Responding to Insider Threats This 5-hour course provides a deeper understanding of insider threat terminology, identifies the different types of insider threats, teaches how to recognize both technical and behavioral indicators, and outlines mitigation strategies.	E-learning	Team Members Program Managers Candidate Evaluators	Available
Building an Insider Threat Program This 7-hour course is to provide a thorough understanding of the organizational models for an insider threat program, the necessary components to have an effective program, the key stakeholders who need to be involved in the process, and basic education on the implementation and guidance of the program.	E-learning	Team Members Program Managers Candidate Evaluators	Available
Insider Threat Program Evaluator Training This 4-day course is to develop the skills and competencies necessary to perform an insider threat program evaluation of an organization or organizational component.	Classroom	Candidate Evaluators	Winter 2014/2015
Insider Threat Program Evaluator Certificate Exam Candidate evaluators must successfully complete this exam to obtain the certificate.	Online Exam	Candidate Evaluators	Winter 2014/2015

To sign up for program updates, go to cert.org/insiderthreat

Extensive research, comprehensive solutions, and technical expertise have made the CERT Division a sought-after leader in the prevention, detection, and mitigation of insider threats. Now it's your turn to act, with support from the CERT Insider Threat Center.

Engage with Us

As a trusted, authoritative, and neutral third party, we regularly partner with government, industry, law enforcement, and academia to develop advanced methods and technologies that counter large-scale, sophisticated cyber threats. The CERT Division has a long history of involving individuals and agencies from outside our organization.

We have assisted and collaborated with

- government agencies, including the U.S. Department of Defense, the Department of Homeland Security, law enforcement, the intelligence community, other U.S. federal agencies, state and local governments, and other operators of infrastructures critical to the national defense, cybersecurity, and the national economy
- industry organizations
- end users worldwide who benefit from our work that exposes vulnerabilities and makes systems safer

Benefit from Our Experiences by Using Our Tools

We offer a range of tools and methods to help you conduct forensic examinations, analyze vulnerabilities, monitor large-scale networks using flow data, and more.

Attend Training or Learn Online

The CERT Division offers courses both in person and online, and we have repositories of training materials:

- Explore our in-person training courses or bring training to your organization.
- View online learning options in CERT STEPfwd.
- Explore our Software Assurance Curriculum repository.

Collaborate with Us

Are we working on the same problems? Let's talk about how we can collaborate to find solutions. Contact us today.

Request an Assessment

Do you want to know how your organization's security-related practices compare to best practices? Do you need to understand your team's security capabilities? Our experts offer assessments to provide support.

Explore Our Digital Library

Our digital library offers an extensive collection of publications, including technical reports and papers, podcasts, webinars, news stories, presentations, and articles.

Engage with Us

Report a Vulnerability

We accept reports of security vulnerabilities and serve as a coordinating body that works with affected vendors to resolve vulnerabilities. If you believe you have found a security vulnerability that has not been resolved, please report it to us.

Sponsor Research and Development

We perform sponsored research and development. Sponsored research and development projects typically involve studying or solving a particular problem that has widespread implications. If your organization would like to sponsor research and development work at the CERT Division, contact us.

Attend an Event

The CERT Division hosts or contributes to many webinars, conferences, and meetings throughout the year.

Stay Connected

Keep up with current CERT Division work and learn about upcoming opportunities with these resources:

- CERT/CC Blog http://www.cert.org/blogs/certcc/
- Insider Threat Blog http://www.cert.org/blogs/insider-threat/
- CERT Podcast Series http://www.cert.org/podcasts/
- RSS Feed https://www.cert.org/rss/
- Connect with us on LinkedIn https://www.linkedin.com/company/cert

For more than 25 years, the CERT Division has been a leader in cybersecurity. Originally focused primarily on incident response, we have expanded into areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threat, digital investigations and intelligence, and workforce development. To learn more, visit our website at www.cert.org or send us an email at cert@cert.org.

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
Phone: +1 412-268-5800

Toll free: +1-888-201-4479
Fax: +1 412-268-5758
www.sei.cmu.edu
www.cert.org
info@sei.cmu.edu

SEI Washington, DC
NRECA Building
Suite 200
4301 Wilson Boulevard
Arlington, VA 22203

Phone: +1 703-247-1300
Fax: +1 703-908-9317

SEI Los Angeles, CA
2401 East El Segundo Boulevard
El Segundo, CA 90245

Phone: +1 310-725-9000
Fax: +1 310-725-9014

Software Engineering Institute
Carnegie Mellon University