Carnegie Mellon University
Software Engineering Institute

CERT Insider Threat Center

The CERT Division

What You Should Know About Insider Threats

Did you know that cyberattacks from employees and other insiders is a common problem that you should be planning for and preventing? Insiders pose a substantial threat to your organization because they have the knowledge and access to proprietary systems that allow them to bypass security measures through legitimate means.

At the CERT Insider Threat Center at Carnegie Mellon's Software Engineering Institute (SEI), we are devoted to combatting cybersecurity issues. Our research has uncovered information that can help you identify potential and realized insider threats in your organization, institute ways to prevent them, and establish processes to deal with them if they do happen.

Besides our research, you can also benefit from the assessments, courses, and certificates we offer. You can ask us to assess your organization to find out how likely it is to be a victim of insider threats or how well your insider threat program is working. Our courses help you understand the nature of insider threats and what to do about them. Our certificates enable you to become an expert in the field of insider threat.

The nature of insider threats is different from other cybersecurity challenges; these threats require a different strategy for preventing and addressing them. In this booklet, we explain what insider threats are and show you how you can form a strategy to best help your organization tackle them.

Who We Are

Carnegie Mellon University—a global research university—is recognized worldwide for its highly rated programs in computer science and engineering. Carnegie Mellon is home to the SEI, which was created in 1984 as a federally funded research and development center (FFRDC). The SEI has advanced software engineering principles and practices and has served as a national resource in software engineering, computer security, and process improvement. The CERT Division of the SEI was created in 1988 in response to the Morris worm incident. Today it is a team of more than 150 cybersecurity professionals who proactively work to help you and others secure their systems. The CERT Insider Threat Center is the part of the CERT Division that researches insider threats.

Contents

About the Insider Threat Center

At the CERT Insider Threat Center, we conduct empirical research and analysis to develop solutions that combat insider threats. Our database of more than 1000 insider threat cases contains information we've used to learn about and analyze insider threats. 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.

In the CERT insider threat lab, we identify, tune, and package technical controls as an extension of the work we do on modeling. We developed an assessment method to help you identify your technical and nontechnical vulnerabilities to insider threats. We've also developed countermeasures you can use to combat insider threats.

Our Research

Some of our research includes

- Creating controls that can be used for preventing, detecting, and responding to insider incidents
- Identifying unique patterns of insider threat behavior, including intellectual property (IP) theft, IT sabotage, fraud, espionage, and unintentional insider incidents
- Collecting insider threat cases (now numbering over 1000) and examining them from technical and behavioral perspectives
- Formulating and publishing best practices for mitigating insider threats
- Combining empirical data and system dynamics modeling and simulation to illustrate the big picture and complexity of the insider threat problem
- Collaborating with the U.S. Department of Defense on espionage research.

Read more about our research at cert.org/insider-threat/research.

Our Products and Services

Our confidential Insider Threat Vulnerability Assessment (see page 6) helps you understand your exposure to insider threat along multiple vectors and delivers a single, actionable framework so that you can manage these issues and associated risks.

Our confidential Insider Threat Program Evaluation (see page 7) helps you reduce risk to critical assets by determining the efficacy of your insider threat program.

If you are an executive, our customized Insider Threat Program Development Workshop (see page 8) helps you develop a strategic plan and create a program that specifically suits your needs.

Our insider threat courses help you understand the nature of insider threats and what to do about them. Visit cert.org/training for details.

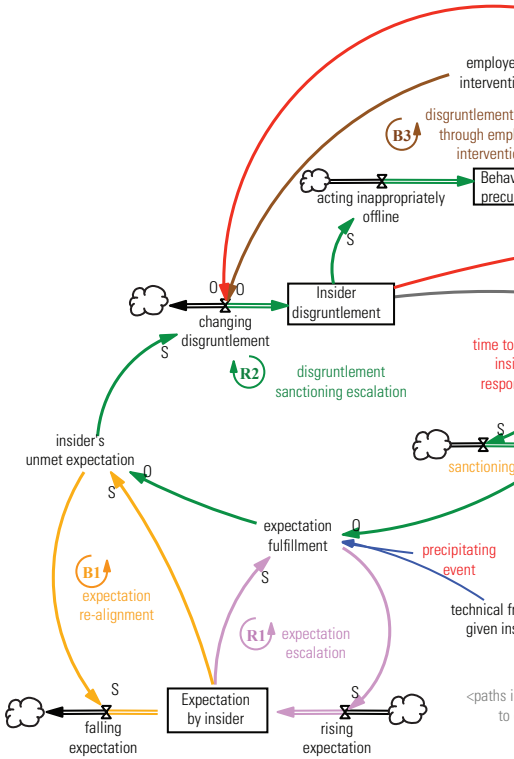
Our insider threat certificates (pages 12–14) enable you to become an expert in the field of insider threat.

Our Best Practices

Insider threats are influenced by technical, behavioral, and organizational issues and must be addressed by policies, procedures, and technologies, so best practices should involve your entire staff. Decision makers across your organization must understand the overall scope of the insider threat problem and communicate it to everyone.

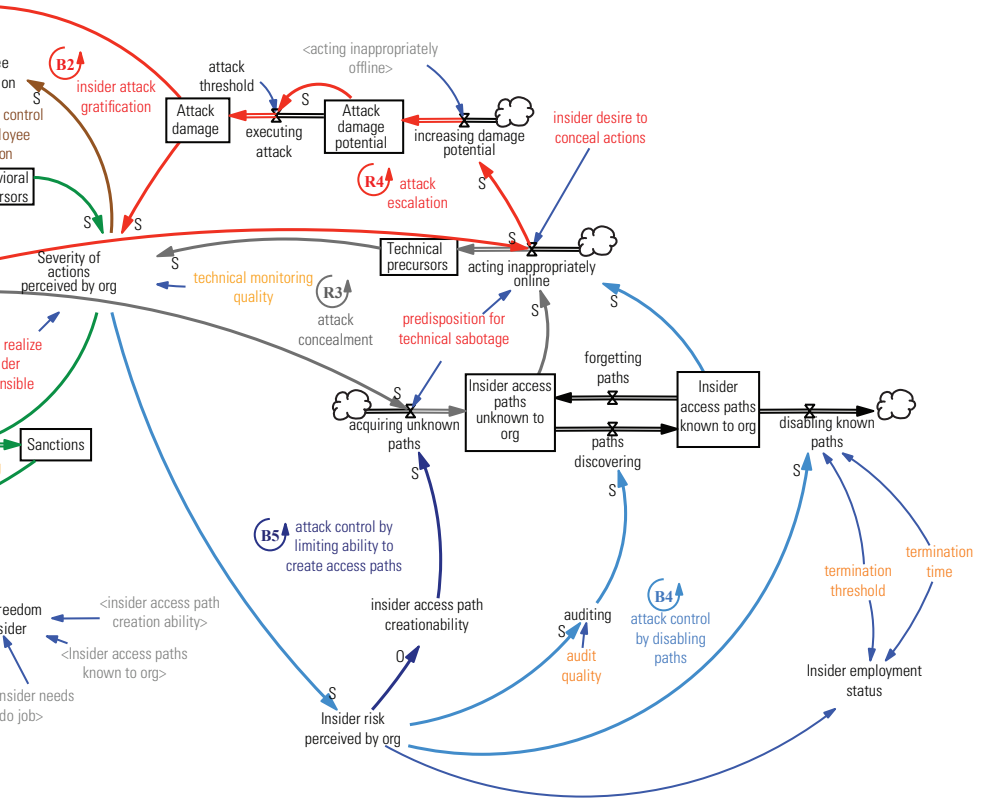
To help guide you through this process, we created best practices that mitigate IP theft, IT sabotage, and fraud. For example, your organization should implement strict password and account management policies and practices, enforce separation of duties and least privilege, define explicit security agreements for any cloud services, and institutionalize system change controls. Read about our best practices in the *CERT Common Sense Guide to Mitigating Insider Threats, 4th Edition*.

Learn more about our work by visiting cert.org/insider-threat or by contacting us at cert.org/insider-threat/contact.cfm.



What Is an 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).



Our Research Partners

We have been researching insider threats since 2001 in partnership with the Department of Defense, the Department of Homeland Security, the U.S. Secret Service, other federal agencies, the intelligence community, private industry, academia, and the vendor community.

CERT Insider Threat Center's Key Components of an Insider Threat Program

Before establishing an insider threat program in your organization, you must first understand the required components of such a program. We in the CERT Insider Threat Center identified the following key components that we believe are necessary to produce a fully functioning insider threat program.


Oversight of Program Compliance and Effectiveness
Protection of Employee Civil Liberties and Privacy Rights
Insider Threat Incidence Response Plan
Confidential Reporting Procedures and Mechanisms
Organization-Wide Participation
Communication of Insider Threat Events
Policies, Procedures, and Practices to Support the Insider Threat Program
Data Collection and Analysis Tools, Techniques, and Practices
Insider Threat Training and Awareness
Prevention, Detection, and Response Infrastructure
Insider Threat Practices Related to Trusted Business Partners
Integration with Enterprise Risk Management
Formalized and Defined Program

Insider Threat Vulnerability Assessment

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

Our research has proven that the insider threat problem is complex; therefore, you 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 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.

Insider Threat Program Evaluation

Our Insider Threat Program Evaluation (ITPE) enables you to determine the efficacy of your existing insider threat program mitigation strategies. To reduce organizational risk to critical assets, we use an evaluation methodology to review the following program elements:

- mitigation strategies
- tactical execution as noted in associated processes and procedures
- insider threat data collection and analysis tools
- insider threat control measures
- planned employee awareness and education activities
- protection of employee privacy and civil liberties

Evaluation Scope and Process

For the evaluation, 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 controls in operation. We sign non-disclosure agreements, and all collaborations remain confidential. The purpose of the evaluation is to

- review key artifacts including insider threat program procedures, information technology procedures, standard business operating procedures, and data collection procedures
- observe data sources used for analysis
- analyze program controls including security, tool access, personnel assignments, and audits

An evaluation report containing analysis and review of the effectiveness of your Insider Threat program is developed, plus CERT experts discuss how your program compares to other programs based on the CERT Common Sense Guide to Mitigating Insider Threat.

For more information about the ITPE, visit cert.org/insider-threat/products-services/program-evaluations.cfm.

Mitigate High-Risk Areas of Concern

Does your insider threat program have all the necessary components to be effective?

Our evaluation reviews your key artifacts, processes, and controls to ensure that your organization is well protected against potential threats from the actions of insiders.

Insider Threat Program Development Custom Workshops

We tailor confidential onsite workshops to your organizations needs and use actual malicious insider incidents that occurred in your organization. To prepare for the customized workshop, you provide us with a number of insider cases so that we can understand your organization's threat landscape. For three days prior to the workshop, members of the Insider Threat Center are onsite at your organization, interviewing staff members who are familiar with the insider cases provided. We treat all customer data as confidential and do not publicly distribute it.

The workshop spans two days. The first day consists of presentations and interactive exercises that help you assess your organization's vulnerability to insider threats. On the second day, we provide you with actionable steps to better manage your risk of insider threats. 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, and considers your organization's unique corporate culture.

The target audience for the workshop includes 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 about these custom workshops, visit cert.org/insider-threat/products-services/workshops.cfm.

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 the organization's needs.

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.

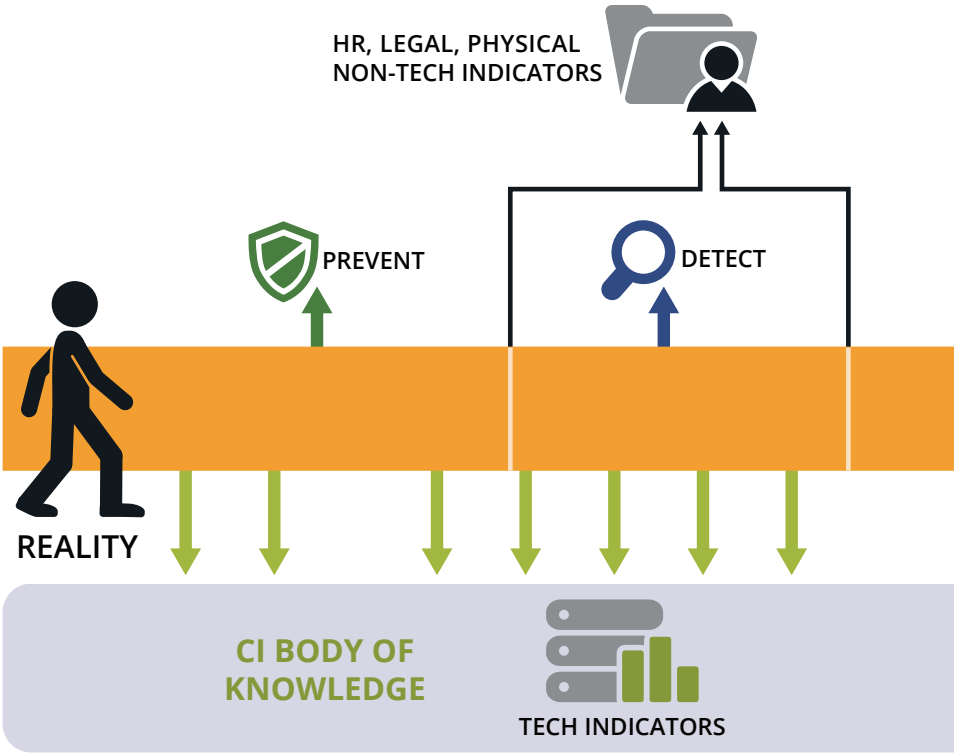
In addition, proposed changes to the National Industrial Security Program Operating Manual (NISPOM) will require contractors that engage with federal agencies that operate or access classified computer networks to also implement an insider threat program in accordance with EO 13587.

…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, our solutions share our important research to enable others to also provide this critical support.

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

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



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

Insider Threat Program Manager Certificate (ITPM)

(Now Available)

The ITPM program helps insider threat program managers develop a formal insider threat program.

Insider Threat Vulnerability Assessor Certificate (ITVA)

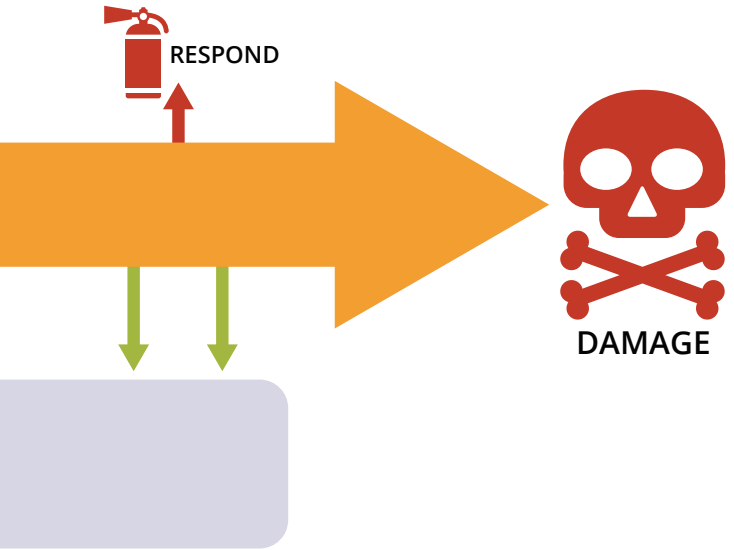
(Now Available)

The ITVA program enables authorized assessors to help organizations gain a better understanding of their insider threat risk and be better able to identify and manage associated risks.

Insider Threat Program Evaluator Certificate (ITPE)

(Available Fall 2017)

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



Insider Threat Program Manager (ITPM) Certificate

The ITPM certificate program assists insider threat program managers who are developing a formal insider threat program. The certificate covers 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 a program within an organization.

Components

COURSE	DELIVERY	AUDIENCE	COMPLETION
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	Available
Building an Insider Threat Program This 7-hour course provides a thorough understanding of the organizational models for an insider threat program, the necessary components to have in 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-day course helps you 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

Extensive research, comprehensive solutions, and technical expertise have make 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.

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

Insider Threat Vulnerability Assessor (ITVA) Certificate

Our ITVA program enables assessors to help organizations gain a better understanding of their insider threat risk and improve their ability to identify and manage associated risks. Our assessment methodology assists your organization by measuring how prepared you are to prevent, detect, and respond to the insider threats. Your organization will be able to license the CERT Insider Threat Vulnerability Assessment tool for internal use or to assess others for potential vulnerabilities.

Components

COURSE	DELIVERY	AUDIENCE	COMPLETION
Insider Threat Overview: Preventing, Detecting, and Responding to Insider Threats This 5-hour course provides a deep 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 provides a thorough understanding of the organizational models for an insider threat program, the necessary components to have in 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 3-day course helps you develop the skills and competencies necessary to perform an insider threat vulnerability assessment of an organization.	Classroom	Candidate Assessors	Available
Insider Threat Vulnerability Assessor Certificate Exam Candidate assessors must successfully complete this exam to obtain the certificate.	Online Exam	Candidate Assessors	Available

Extensive research, comprehensive solutions, and technical expertise make 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.

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

Insider Threat Program Evaluator (ITPE) Certificate

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

Components

COURSE	DELIVERY	AUDIENCE	COMPLETION
Insider Threat Overview: Preventing, Detecting, and Responding to Insider Threats This 5-hour course provides a deep 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 provides a thorough understanding of the organizational models for an insider threat program, the necessary components to have in 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 3-day course helps you develop the skills and competencies necessary to perform an insider threat program evaluation of an organization or organizational component.	Classroom	Candidate Evaluators	Available Spring 2018
Insider Threat Program Evaluator Certificate Exam Candidate evaluators must successfully complete this exam to obtain the certificate.	Online Exam	Candidate Evaluators	Available Spring 2018

Extensive research, comprehensive solutions, and technical expertise make 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.

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

Engage with Us

Engaging with us is easy. Attend one of our training courses, request a security-related assessment, collaborate with us on our research projects, and more.

Learn from Our Training

Available online and in person, our cybersecurity courses help you tackle the cybersecurity challenges you face in areas such as insider threats, DevOps, and software assurance, to name a few. Get certified by taking multiple related courses in our insider threat and secure coding certificate programs.

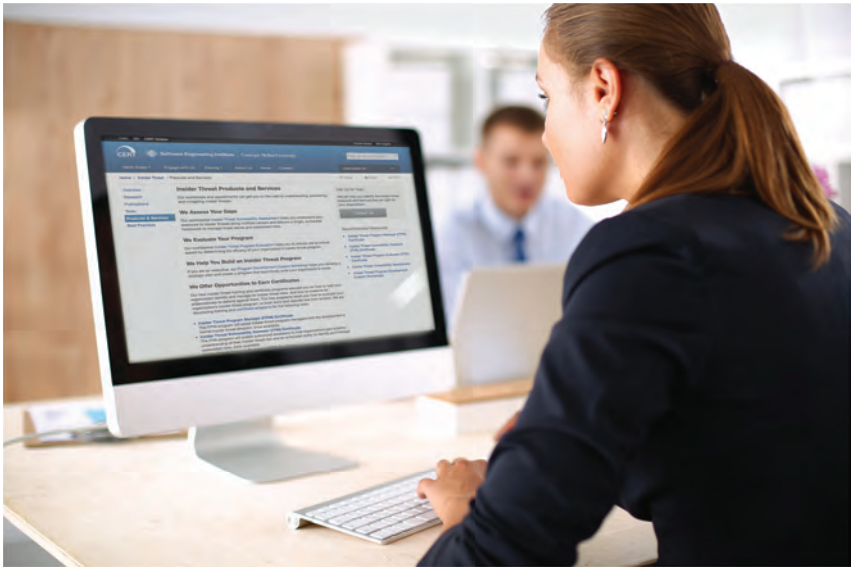
For information about these programs, see cert.org/insiderthreat and cert.org/go/secure-coding. Explore the complete range of our cybersecurity training opportunities at cert.org/training.

Report a Vulnerability

You can report security vulnerabilities to us when vendors have not responded to your direct contact with them. We then work with affected vendors to resolve reported vulnerabilities. Learn more at cert.org/vulnerability-analysis.

Use Our Tools

Use our tools and methods when you conduct your forensic examinations, analyze vulnerabilities, monitor large-scale networks using flow data, and more. See our full array of tools at cert.org/engage/tools.cfm.



Attend an Event

We sponsor many conferences and meetings, including

- Insider Threat Symposium (cert.org/go/insider-threat-symposium), an annual event that brings together those mitigating insider threats to share their successes and challenges
- CYBURGH, PA (bit.ly/cyburghPA), an annual event for local Pittsburgh organizations to share information about cybersecurity challenges and solutions
- FloCon (cert.org/flocon), an annual network security conference where you learn more about the next generation of flow-based analysis techniques

Request an Assessment

Do you want to know how effective your organization's security-related practices are? Our experts offer assessments that include

- Insider Threat Vulnerability Assessments that help you understand your exposure to potential insider threats (cert.org/insider-threat/products-services/vulnerability-assessments.cfm)
- CERT-RMM Capability Appraisals that evaluate your organization's operational resilience using the CERT-RMM (cert.org/resilience/products-services/cert-rmm/cert-rmm-appraisals.cfm)
- SCALe Conformance Analyses that evaluate the C code in your software to help you improve it before you release it to your customers (cert.org/secure-coding/products-services/scale.cfm)

Read Our Blogs

Check out the latest insights from our researchers.

- Our Insider Threat bloggers advise you and offer best practices to help you deter, detect, and respond to insider threats.
- Our CERT/CC bloggers share advice on timely issues related to vulnerabilities, network situational awareness, and security research.
- Our DevOps bloggers offer technical guidance to help you achieve successful DevOps.

Access all of our blogs at insights.sei.cmu.edu.

Stay Informed with Our Podcast Series

If you are leading an enterprise-wide security effort, make sure your security programs are as good as they can be by listening to our podcasts at cert.org/podcasts.

Join the Secure Coding Wiki

Read and contribute to our secure coding wiki, where you and your peers can work with us to develop new coding standards. Learn to develop secure code using our coding standards for C, C++, Java, and Perl. We also have programming standards for the Android platform. Join the wiki at securecoding.cert.org/.

Participate in Our Webinars

We offer a vast collection of webinars at sei.cmu.edu/webinars covering topics such as DevOps, insider threats, malware analysis, secure coding, and more.

Learn About Our Research

We focus our research on cybersecurity challenges in national security, homeland security, and critical infrastructure protection. Our research produces new approaches, analysis tools, and training options to improve the practice of cybersecurity in private and public sector organizations.

Conduct Research with Us

Watch some of our researchers describe their work on cert.org/research. They discuss projects such as behavior-based analysis and detection of mobile devices, malware distribution networks, and analyzing Internet and online social network concerns.

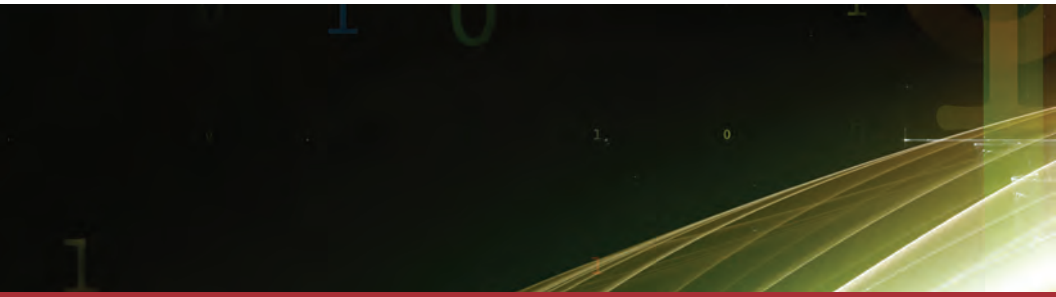
We invite you to engage with us on these and other research projects on our website at cert.org. Contact us at cert.org/contact to discuss the work and the collaboration opportunities we offer.

Sponsor Our Research

In our sponsored research and development, we study and solve problems that have widespread implications for cybersecurity. We have worked with many organizations on a variety of research projects. For example, the U.S. Department of Homeland Security and the Department of Energy have sponsored some of our research in software assurance and resilience management. Reach out to us at cert.org/contact if you are interested in exploring sponsorship opportunities.

Collaborate with Us

Are we working on the same cybersecurity problems? Let's talk about how we can collaborate to find or develop solutions. Reach us at cert.org/contact.



About Us

For nearly 30 years, the CERT Division of the Software Engineering Institute (SEI) at 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 investigations and intelligence, workforce development, DevOps, forensics, software assurance, vulnerability discovery and analysis, and risk management. To learn more, visit our website at www.cert.org or send us an email at cert@cert.org.

Contact Us

SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE
PITTSBURGH, PA 15213-2612

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