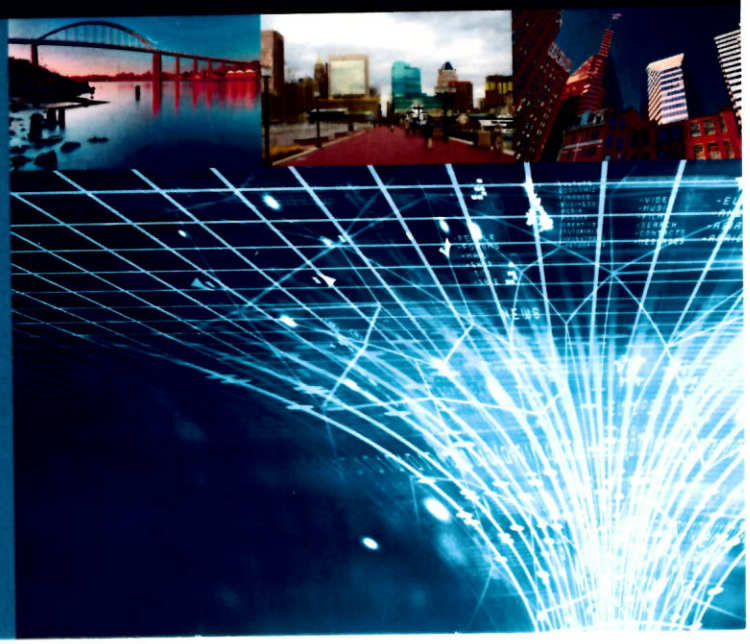
Software Engineering Institute | Carnegie Mellon University

SATURN 2015

11th Software Engineering Institute Architecture Technology User Network Conference

April 27 – April 30, 2015
Baltimore, Maryland



The SATURN software architecture conference returns in April 2015 with an exciting lineup of speakers and events

Each year the Software Engineering Institute (SEI) Architecture Technology User Network (SATURN) Conference attracts an international audience of practicing software architects, industry thought leaders, developers, technical managers, and researchers to share ideas, insights, and experience about effective architecture-centric practices for developing and maintaining software-intensive systems.

The 11th SATURN Conference will be at the Lord Baltimore Hotel in Baltimore, Maryland, April 27-30, 2015.

This year's technical program will cover a variety of subjects within three broad themes: (1) technology, (2) methods and tools, and (3) leadership and business. The conference fee pays for three full days of presentations and interactive events. The SEI also offers one-day courses on Big Data, DevOps, and Technical Debt.

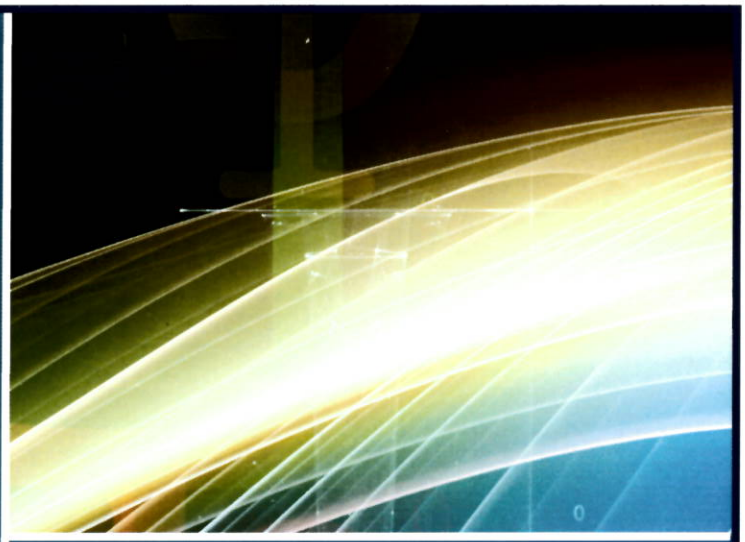
Whether you're just starting out in architecture or have many years of experience, SATURN 2015 offers something for everyone. You will leave with dozens of new ideas and solutions to implement in your organization.

Discounts from $300-$600 on conference registration are available now to the first 75 people who register for the conference at **http://www.sei.cmu.edu/saturn/2015**.

Visit the SATURN 2015 website to register or for more information.

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

Content



CERT Insider Threat Center

The CERT Division

Software Engineering Institute
Carnegie Mellon University

Anticipating and Solving the Nation's Cybersecurity Challenges

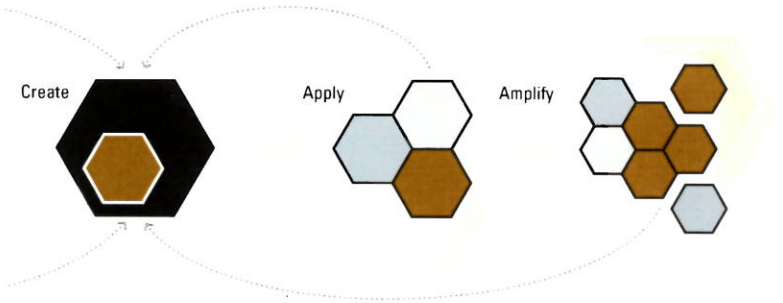
Software Engineering Institute

Solid Reputation

Since 1984, the Software Engineering Institute (SEI) has served the nation as a federally funded research and development center (FFRDC) based at Carnegie Mellon University, a global research university recognized worldwide for its highly rated programs in computer science and engineering. As part of Carnegie Mellon, the SEI operates at the leading edge of technical innovation. The SEI staff has advanced software engineering principles and practices and has served as a national resource in software engineering, computer security, and process improvement.

Unique Strategy

The SEI achieves its goals through technology innovation and transition. The SEI creates usable technologies by motivating and conducting research, applies them to real problems by partnering with government and industry, and amplifies their impact by accelerating broad adoption through direct engagement with the community and through partners.



The CERT® Division

Begun with a simple handshake and a fundamental mission, the CERT Division has evolved dramatically since it was created in 1988 as the CERT Coordination Center in response to the Morris worm incident. The small organization established to coordinate response to internet security incidents now has more than 150 cybersecurity professionals working on projects that take a proactive approach to securing systems.

Recognized as a trusted, authoritative organization dedicated to improving the security and resilience of computer systems and networks, the CERT Division is a national asset in the field of cybersecurity. We regularly partner with government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats.

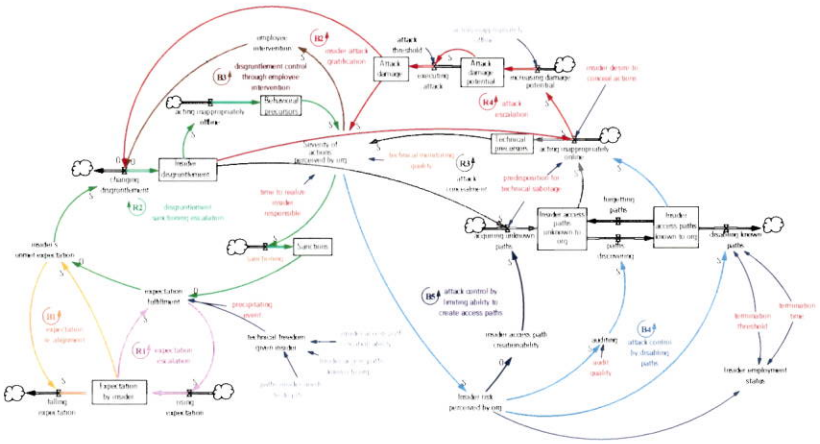
For more than 25 years, the CERT Division has been a leader in cybersecurity. Originally focused on incident response, we have expanded into areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threat, digital investigations and intelligence, and workforce development.

CERT Insider Threat Center

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 conducts empirical research and analysis to develop and transition sociotechnical solutions to combat insider cyber threats. We have been doing research on this problem 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.

The foundation of our work is our database of more than 800 insider threat cases. 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. The CERT insider threat lab provides a foundation to identify, tune, and package technical controls as an extension of our modeling efforts. We have developed an assessment framework based on fraud, theft of intellectual property, and IT sabotage incidents to help organizations identify their technical and nontechnical vulnerabilities to insider threats as well as executable countermeasures.



Simulation Model of Insider IT Sabotage

As part of an FFRDC, the CERT Insider Threat Center is uniquely positioned, and has been serving as a trusted broker to assist the community in the short term and through our ongoing research for more than a decade. Learn more by visiting www.cert.org/insider-threat, or by contacting us at insiderthreat-feedback@cert.org.

Key Capabilities

We create technical controls and indicators.

Using our wealth of socio-technical information on insider activity, our CERT insider threat lab creates controls and indicators for preventing, detecting, and responding to insider incidents.

We conduct case analyses and develop best practices.

In 2002, we collected approximately 150 insider threat cases in the U.S. critical infrastructure sectors and examined them from technical and behavioral perspectives. The scope and body of our case analyses continue today, which allows us to publish best practices for the mitigation of insider threats.

We model and simulate insider threat.

Our MERIT project combines empirical data and system dynamics modeling and simulation to illustrate the big picture and complexity of the insider threat problem. We also collaborate with the U.S. Department of Defense on espionage research.

Insider Threat Best Practices

Products and Services

We assess your gaps.

A confidential Insider Threat Vulnerability Assessment helps you understand your exposure to insider threat along multiple vectors and delivers a single actionable framework to manage these issues and associated risks.

We evaluate your program.

A confidential Insider Threat Program Evaluation helps you to reduce risk to critical assets by determining the efficacy of the organization's insider threat program.

We help you build a program.

A customized Insider Threat Program Development Workshop assists executives to develop a strategic plan and to create a program that specifically suits their needs.

Insider threats are influenced by a combination of technical, behavioral, and organizational issues and must be addressed by policies, procedures, and technologies. Accordingly, best practices to mitigate insider threats involve an organization's staff in management, human resources (HR), legal counsel, physical security, information technology (IT), and information assurance (IA), as well as data owners and software engineers. Decision makers across the enterprise should understand the overall scope of the insider threat problem and communicate it to all the organization's employees.

Our current analysis recognizes the following unique patterns of insider threat behavior: intellectual property (IP) theft, IT sabotage, fraud, espionage, and unintentional insider incidents.

The CERT Division has created the following best practices for mitigating IP theft, IT sabotage, and fraud:

1. Consider threats from insiders and business partners in enterprise-wide risk assessments.
2. Clearly document and consistently enforce policies and controls.
3. Incorporate insider threat awareness into periodic security training for all employees.
4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5. Anticipate and manage negative issues in the work environment.
6. Know your assets.
7. Implement strict password and account management policies and practices.
8. Enforce separation of duties and least privilege.
9. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
10. Institute stringent access controls and monitoring policies on privileged users.
11. Institutionalize system change controls.
12. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
13. Monitor and control remote access from all end points, including mobile devices.
14. Develop a comprehensive employee termination procedure.
15. Implement secure backup and recovery processes.
16. Develop a formalized insider threat program.
17. Establish a baseline of normal network device behavior.
18. Be especially vigilant regarding social media.
19. Close the doors to unauthorized data exfiltration

These best practices appear in the *Common Sense Guide to Mitigating Insider Threats, 4th Edition.*

Insider Threat Vulnerability Assessment

The Insider Threat Vulnerability Assessment enables organizations to gain a better understanding of insider threat and an enhanced ability to assess and manage associated risks. The assessment instrument, which is based on more than 800 insider threat cases in our database, encompasses information technology, human resources, physical security, legal, trusted business partners, business processes, management, and organizational issues. It merges technical, behavioral, process, and policy issues into a single, actionable framework.

Our research has proven that the insider threat problem is quite complex, and organizations need an instrument that has the following characteristics:

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

The CERT insider threat vulnerability assessment, which is based on psychological expertise as well as technical expertise, will help you to better safeguard your critical assets. The purpose of the assessment is to

- enable you to gain a better understanding of your vulnerability to insider threat and an enhanced ability to assess and manage associated risks
- include technical, organizational, personnel, and business security and process issues from all of our past research in a single, actionable framework
- benefit all individuals involved in the insider threat vulnerability assessment process: information technology, human resources, physical security, general counsel, data and business process "owners," trusted business partners, and all levels of organizational management
- provide a measure of an organization's preparedness to prevent, detect, and respond to the threats posed by insiders

Assessment Process

For the assessment, members of the Insider Threat Center staff will spend three to five days at your organization. During that time, we will review documents, interview key personnel in your organization, and observe key processes and security issues. We will sign non-disclosure agreements, and all collaborations will remain confidential.

After the onsite visit, we will provide you with a confidential report that contains the findings of the assessment and considerations for potential mitigation strategies. Organizations have used this report to

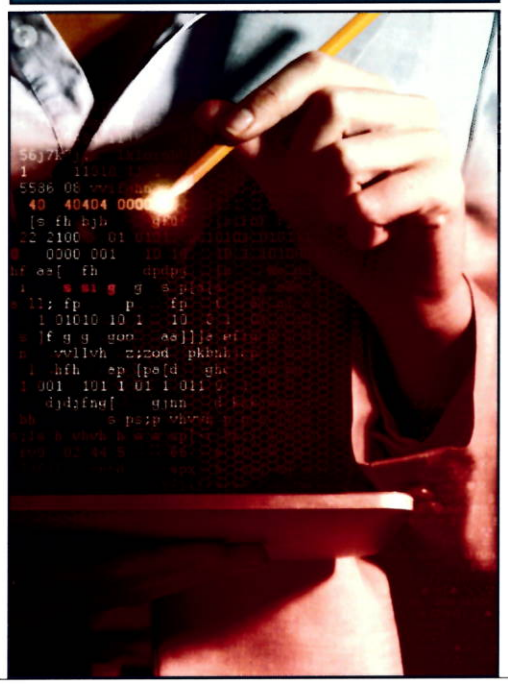
- identify and implement short-term tactical countermeasures
- help guide their ongoing risk management process for implementing long-term, strategic countermeasures
- justify follow-up actions to key decision makers

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

Identify Vulnerabilities and Issues of Concern

To defend against the insider threat, you must understand your organization's susceptibility to it.

Our assessment explores the entire organization, including technical vulnerabilities, business process gaps, management issues, and the ability to deal effectively with behavioral issues.



Insider Threat Program Evaluation

The Insider Threat Program Evaluation enables organizations to determine the efficacy of their existing insider threat program mitigation strategies. To reduce organizational risk to critical assets, the evaluation methodology reviews 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
- Ensuring the organization is protecting the privacy and civil liberties of its employees

Evaluation Scope and Process

For the evaluation, members of the Insider Threat Center staff will spend three to five days at your organization. During that time, we will review documents, interview key personnel in your organization, and observe key processes and security controls in operation. We will sign non-disclosure agreements, and all collaborations will remain confidential. The purpose of the evaluation is to

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

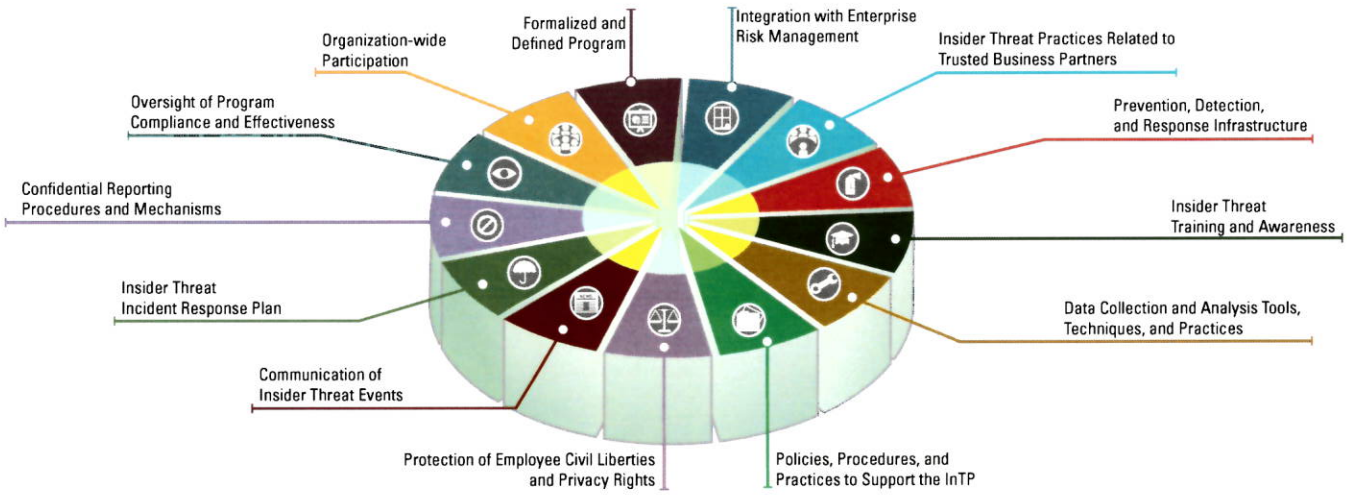
An evaluation report containing analysis and review of the effectiveness of the organization's Insider Threat program is developed, plus CERT experts discuss how the program compares to other programs based on *CERT's Common Sense Guide to Mitigating Insider Threat*.

For more information, visit http://www.sei.cmu.edu/training/P76.cfm.

Mitigate High-Risk Areas of Concern

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

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



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