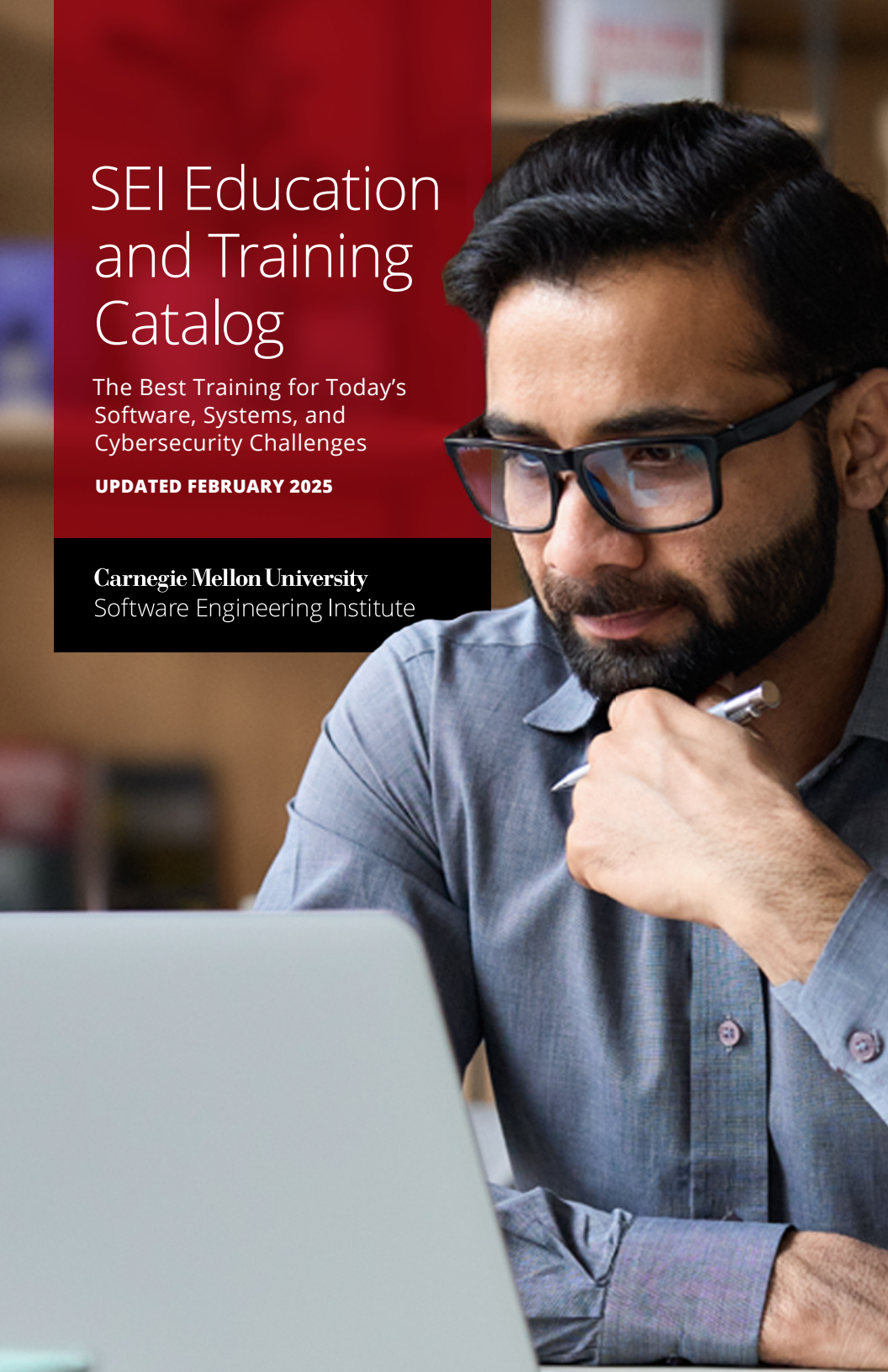


SEI Education and Training Catalog

The Best Training for Today's Software, Systems, and Cybersecurity Challenges

UPDATED FEBRUARY 2025

Carnegie Mellon University
Software Engineering Institute

Get the Edge You Need

By completing our training courses at the Carnegie Mellon University Software Engineering Institute (CMU SEI), you learn to acquire, develop, operate, and sustain software systems. Our many learning options are sure to meet your learning goals.

Our software and cybersecurity experts, recognized for their contributions to field-based research, have practical experience that enables them to develop and teach our courses. Acquire critical skills through hands-on tasks and real-world scenarios. Immerse yourself in current and practical courses that challenge your assumptions and help you explore new and unexpected ideas.

Contents

Flexible Course Delivery Options

Our course delivery options help you follow the best training approach given your schedule and preferred learning style. All training is presented by our expert instructors and includes one or more of the following: lectures, exercises, and discussions where you also learn from fellow professionals.

Classroom training is public training that is available at an SEI facility.

Live-Online training offers synchronous learning where you and your instructor can interact during classes.

Online learning is eLearning (self-paced online training).

On-Site training is classroom training that is taught on site at your facility.

How to Register

Individuals

Register for most courses and credentials on the SEI website (**sei.cmu.edu/education-outreach**).

Groups

Schedule private, on-site classroom training, or take advantage of group discounts for online training. Contact us (**course-info@sei.cmu.edu**) for more information.

Recognize Your Educational Accomplishments

An SEI professional certificate acknowledges your professional accomplishments in a technical curriculum. Each certificate requires that you work through a carefully designed set of courses. Requirements differ among technical areas and programs. As an SEI professional certificate holder, you receive an official certificate from the SEI and the option of having your name and accomplishment published on the SEI website.

Certificate courses fulfill the requirements for one or more professional certificate programs.

More Information

Find more information about SEI education and training on the SEI website:

sei.cmu.edu/education-outreach

We offer public domain continuing educational units (CEUs) for most of our training courses. We calculate CEUs based on your total class hours using the ANSI/IACET standard, which awards one CEU for every 10 hours of instruction.

Training courses provided by the SEI are not academic courses for academic credit toward a degree. Any certificates provided are evidence of the completion of the courses and are not official academic credentials.

Software Architecture

Software Architecture: Principles and Practices

Two-Day Course • Classroom • Live-Online • Online • On-Site

insights.sei.cmu.edu/training/software-architecture-principles-practices/

In this course, you learn the essential concepts of software architecture and the importance of the business (or mission) context for system design. The course introduces software architectures in a real-world setting and uses "industrial-strength" case studies that cover key technical and organizational issues.

Who should attend? those who design, develop, or manage the construction of software-reliant systems

Topics covered include what a software architecture is and why it's important, the architecture influence cycle, the relationships among system qualities and software architectures, architectural patterns and tactics and their relationship to system qualities, and more.

NOTE: This Live-Online offering consists of four consecutive half-day sessions.

Documenting Software Architectures

Two-Day Course • Classroom • Live-Online • Online • On-Site

insights.sei.cmu.edu/training/documenting-software-architectures

In this course, you learn effective software architecture documentation practices that meet the needs of the stakeholder community in the context of prevailing prescriptive models, including the Rational Unified Process (RUP), the Siemens Four Views software approach, the ISO/IEC 42010 standard, and the Unified Modeling Language (UML).

Who should attend? software architects and lead designers, and software technical managers and engineers who may be expected to use architecture documentation

Topics covered include the basic principles of sound technical documentation, a stakeholder- and view-based approach to documenting software architectures, views available for documenting an architecture, and more.

NOTE: This Live-Online offering consists of four consecutive half-day sessions.

Software Architecture Design and Analysis

Two-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/software-architecture-design-and-analysis

In this course, you learn concepts for effectively designing and analyzing a software architecture. You apply the SEI Attribute-Driven Design (ADD) software architecture design method and are introduced to the SEI Quality Attribute Workshop (QAW), the SEI Architecture Tradeoff Analysis Method (ATAM), and several lightweight evaluation techniques.

Who should attend? practicing software architects, and designers and developers of software-reliant systems

Topics covered include the essential considerations in any architectural design process, how to elicit critical quality attributes, the ADD method for designing an architecture, the role of architecture evaluation, and how to use these methods in a software development lifecycle.

NOTE: This Live-Online offering consists of four consecutive half-day sessions.

Designing Modern Service-Based Systems

One-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/designing-modern-service-based-systems

In this course, you learn the main types of service-oriented architecture (SOA) design elements and technologies. You study comparisons of microservices, the monolithic deployment model, security, transaction management, and service deployment.

Who should attend? software and application architects, developers who use service technologies in their solutions, and project managers and IT personnel responsible for SOA implementations

Topics covered include basic concepts related to SOA and service-based solutions; what is necessary to be successful with SOA; and the main types of components found in service-based solutions, including REST services, platform-specific services, message brokers, and API gateways.

Design Guidelines and Patterns for Microservices

Two-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/design-guidelines-and-patterns-for-microservices

In this course, you gain the essential knowledge needed to understand the microservices landscape, including the seven guidelines for service-oriented designs. You study strategies that help you realize each design guideline. In the design lab, you evaluate designs based on guidelines and create new designs using different patterns and other design strategies.

Who should attend? software and application architects and developers who use service and microservice technologies in their solutions

Topics covered include microservices and microservice architecture styles; design guidelines for successful service-based solutions; and strategies, including several design patterns that can be used to realize service-orientation guidelines.

NOTE: This Live-Online offering consists of four consecutive half-day sessions.

Managing Technical Debt of Software

One-Day Course • Classroom • On-Site

insights.sei.cmu.edu/training/managing-technical-debt-of-software

In this course, you learn about the concept of technical debt—when a design or construction approach is expedient in the short term but increases complexity and cost in the long term. You study how technical debt manifests, accumulates, and affects the enterprise. You also learn to assess, measure, and manage the technical debt landscape.

Who should attend? software professionals who design, develop, or manage the construction of software-reliant systems and who need insights into how to successfully manage technical debt

Topics covered include learning the technical debt definition framework, making technical debt visible, understanding when it accumulates, paying it back, and living with it.

Modeling System Architectures Using the Architecture Analysis and Design Language (AADL)

Five-Day Course • Online • On-Site

insights.sei.cmu.edu/training/modeling-system-architectures-using-aadl-elearning/

In this course, you learn the fundamental model-based concepts for engineering real-time, embedded software systems by defining and documenting software and system architectures and validating system quality attributes. This course builds on the SAE Architecture Analysis and Design Language (AADL) standard for engineering real-time, embedded software systems.

Who should attend? software developers; those tasked with validating embedded, real-time system performance; technical managers; managers; and software/system architects

Topics covered include the value of model-based engineering, choices for system representation and modeling, core elements of the AADL, quantitative validation of quality attributes through the analysis of system architecture, and more.

AADL in Practice Workshop

Five-Day Course and Two-Day Workshop • On-Site

insights.sei.cmu.edu/training/aadl-in-practice-workshop

In this course and follow-up workshop, you learn and apply the modeling techniques necessary to adopt the Architecture Analysis and Design Language (AADL). You are introduced to model-based engineering (MBE) methods and AADL tools in the course. You then put those skills to use in a realistic modeling and analysis scenario in the workshop with expert SEI guidance.

Who should attend? those who design and develop software; those tasked with validating embedded, real-time system performance; technical managers, managers, and software/system architects looking for a solid overview of system and software modeling; and those who make decisions about developing or acquiring real-time, embedded systems

Topics covered include reviewing the existing example problem, defining modeling and analysis objectives, discussing practical modeling approaches, creating and analyzing models, and reviewing/critiquing the work produced.

Understanding Software Architecture, Quality, and Security Through Code Analysis

3.5-Hour Course • Online

insights.sei.cmu.edu/training/understanding-software-architecture-quality-and-security-through-code-analysis

In this course, you learn what distinguishes high-quality code and how to achieve it using static and dynamic analysis, coding standards, metrics, and more. While primarily technical, this course also shows you how code analysis basics contribute to acquisition success and reveal the overall health of software, helping you ensure that quality is built into code.

Who should attend? program office or contractor personnel responsible for developing, testing, project management, and acquisition of software-intensive systems

Topics covered include quality attributes, static code analysis, static analysis tools, code metrics, discerning architecture from code, common code quality issues, dynamic code analysis, testing criteria and coverage, security analyses, and acquisition considerations.

Cyber Intelligence

Cyber Intelligence for Decision Makers

Two-Hour Course • Online

insights.sei.cmu.edu/training/cyber-intelligence-for-decision-makers

In this course, you learn a non-technical approach to cyber intelligence, how important it is to understand cyber intelligence in the context of your organization, and how to use cyber intelligence to improve the way you make decisions. You study a structured approach you can use to understand, evaluate, and assess cyber intelligence vulnerabilities.

Who should attend? executives, managers, and team leaders

Topics covered include the role of cyber intelligence in your organization, your organization's cyber-threat environment, potential risk factors and preventive measures, core competencies and skills recommended for an intelligence team, and more.

Incident Handling

Creating a Computer Security Incident Response Team (CSIRT)

One-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/creating-a-computer-security-incident-response-team

This course is designed for managers and project leaders who have been tasked with implementing a computer security incident response team (CSIRT) or similar capability. This course provides a high-level overview of the key issues and decisions that must be addressed in establishing an incident management capability. The course can also be used as an introduction to incident management and CSIRT activities, responsibilities, and services for incident handlers and for those who work with incident handlers. As part of the course, attendees will develop an action plan that can be used as a starting point in planning and implementing their specific capability.

Who should attend? current and prospective CSIRT managers; C-level managers such as CIOs, CSOs, CROs; and project leaders interested in establishing, starting, or understanding a CSIRT, other staff who interact with CSIRTs, incident management capabilities, or incident handlers who would like to gain a deeper understanding of how each operates

Topics covered include types of CSIRTs and incident management capabilities or security teams; incident management and the relationship to CSIRTs, Security Operations Centers (SOCs), Product Security Incident Response Teams (PSIRTs) and Information Sharing and Analysis Centers (ISACs); prerequisites to planning an incident management capability; creating and institutionalizing a vision for the capability; developing appropriate mission, objectives, and level of authority; organizational issues, dependencies, needed integration, interfaces, and models; range and levels of provided services; funding issues; hiring and training initial and additional staff and subject matter experts (SMEs); implementing relevant and supporting policies and procedures; requirements for an incident handling infrastructure; implementation and operational issues and strategies; and collaboration and communication issues.

Managing Computer Security Incident Response Teams (CSIRTs)

Three-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/managing-computer-security-incident-response-teams

This course provides current and future managers of computer security incident response teams (CSIRTs) with a pragmatic view of the issues that they will face in operating an effective team.

Who should attend? managers who are interested in implementing or are required to implement a CSIRT or incident management capability; managers who have responsibility or must work with those who do have responsibility for incident management activities; managers who have experience in incident handling and want to learn more about operating effective incident management capabilities; and other staff who interact with incident management capabilities and would like to gain a deeper understanding of how they operate, potential services to provide, needed infrastructure for support and incident management processes to establish

Topics covered include incident management process; hiring and mentoring incident handling staff developing supporting policies and procedures; requirements for developing services; handling media issues; building and managing the incident management infrastructure; coordinating response; handling major or crisis events and incidents; working with law enforcement; evaluating CSIRT operations; integration with insider risk processes or capabilities; incident management capability metrics; and exercises in triage, coordinating response and an incident handling scenario.

Foundations of Incident Management

Four-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/foundations-of-incident-management

This course provides foundational knowledge for those in security-related roles who need to understand the functions of an incident management capability and how best to perform those functions. It is recommended for those new to incident handling or security operations work. This course was recently updated including a new ransomware exercise.

Who should attend? new incident handlers, investigators, and security operations center (SOC) analysts (one to three months of experience) who will be performing various incident management or security operations activities; staff performing work roles in the NICE Computer Network Defense Analysis and Incident Response specialty areas; experienced staff who would like to benchmark their processes and skill sets against incident management and security operations best practices; and anyone who would like to learn about basic incident handling functions and activities

Topics covered include basic incident management processes and services based on the FIRST CSIRT Services Framework; new technology or mitigation strategies that incident handlers should know about, such as blockchain, zero-trust, etc.; the current threat environment; team code of conduct; security tools and technologies used by incident handlers; effective gathering of critical information; detecting and analyzing incidents; performing triage; identifying the basic steps in response; using the Domain Name System for handling information security incidents (newly expanded and updated module); finding contact information; coordinating response and disseminating information; handling phishing, email, ransomware, and other malicious code attacks; working with law enforcement; overview of insider threat or risk; exercises: critical information, triage, coordinating response; and analyzing and responding to ransomware.

Advanced Topics in Incident Handling

Four-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/advanced-topics-in-incident-handling

This course, designed for cybersecurity incident management and security operations center (SOC) technical personnel with several months of incident handling experience, addresses techniques for detecting and responding to current and emerging cybersecurity threats and attacks. You work on a team throughout the course to handle a series of escalating incidents that are presented as part of an ongoing scenario. Work includes team analysis of information and presentation of findings and response strategies. You also review more advanced types of activities related to incident handling such as threat hunting; artifact and malware analysis; vulnerability handling; major or crisis events; and publishing and communicating information.

Who should attend? current cybersecurity incident management capability and security operations center (SOC) technical staff with six or more months of incident handling experience

Topics covered include incident handling lifecycle and critical information review, new technologies and impacts on incident handling and mitigation, discussion of blockchain for incident, discussion of advanced persistent threats, artifact and malware analysis categories and techniques overview, threat hunting processes and critical thinking, fundamental causes of vulnerabilities, vulnerability handling overview including vulnerability disclosure, analyzing and coordinating response to major cybersecurity events and incidents, and developing and delivering effective communications.

Introduction to Computer Forensics

Two-Hour Course • Online

insights.sei.cmu.edu/training/cert-certificate-digital-forensics

In this course, you learn about the tasks, processes, and technologies used to identify, collect, preserve, and analyze data so that it can be used in a judiciary setting. You also learn to apply sound forensic practices and understand how routine actions can affect the forensic value of data.

Who should attend? those involved in collecting, storing, and analyzing computer systems and network data, including digital forensics, systems security analysis, and incident response

Topics covered include developing a process for a digital forensic investigation; methods of focusing investigations; preparing for incident response, including network reconnaissance and network traffic analysis; and more.

This course is a component of the **CERT Certificate in Digital Forensics**.
For additional details, see Training Certificates section.

Advanced Digital Forensics

Ten-Hour Course • Online

insights.sei.cmu.edu/training/cert-certificate-digital-forensics/

In this course, you learn the details of the entire investigative process and how to determine “who did it.” You improve your ability to piece together the components of a digital investigation. Using a simulated lab environment, you refine your investigative skills by responding to a realistic scenario.

Who should attend? those involved in collecting, storing, and analyzing computer systems and network data, including digital forensics, systems security analysis, and incident response

Topics covered include preparing for and responding to incidents on victim and suspect systems, conducting network reconnaissance, analyzing network traffic, identifying sources of evidentiary value in various evidence sources, and more.

This course is a component of the **CERT Certificate in Digital Forensics**.
For additional details, see Training Certificates section.

Overview of Creating and Managing Computer Security Incident Response Teams (CSIRTs)—eLearning

Three-Hour Course • Online

insights.sei.cmu.edu/training/overview-of-creating-and-managing-csirts-elearning

In this course, you learn about planning, implementing, operating, and evaluating a computer security incident response team (CSIRT). You benefit from a consolidated view of information from two other CERT courses: *Creating a Computer Security Incident Response Team (CSIRT)* and *Managing Computer Security Incident Response Teams (CSIRTs).* Much of the course is also applicable to incident management in other types of security operation teams, such as security operation centers (SOCs).

Who should attend? CSIRT and C-level managers, project leaders, CSIRT team members, system and network administrators, security staff, human resources staff, media or public relations staff, law enforcement, and legal counsel

Topics covered include best practices for CSIRTs; creating an effective CSIRT; CSIRT components, operational management issues; incident management processes, and more.

Developing a National or Government CSIRT

Two-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/developing-a-national-or-government-csirt

This course focuses on the key decisions and considerations encountered when developing a national or government CSIRT. It discusses the basic components of CSIRTs in general and highlights the characteristics that make national or government versions of CSIRTs unique. Topics covered include capabilities and functions of each entity type, working with stakeholders, planning activities, implementation strategies, enablers, and supporting resources. The course presents definitions for both types of incident management capabilities and examples of existing national or government CSIRTs.

Who should attend? the intended audience includes those charged with developing CSIRTs in general but specifically focuses on those in national or government organizations. Other audience members include: current and prospective CSIRT managers, C-level managers, such as chief information officers (CIOs), chief security officers (CSOs), and chief risk officers (CROs), project leaders interested in establishing or starting a national or government CSIRT, and other organizations that interact with national or government CSIRTs and would like to gain a deeper understanding of how they operate and how to engage with them

Topics covered include Introduction to Developing a National/Government CSIRT, National Incident Management Ecosystem, Defining Incident Management and CSIRTs, the Evolving Nature of Incident Management Capabilities, Uniqueness of a National or Government CSIRT, National CSIRT Principles, Connection with Critical Infrastructures, Planning a National or Government CSIRT, and Implementing Your National or Government CSIRT

Network & Software Security

DevSecOps Process and Implementation

Three-Day Course • On-Site

insights.sei.cmu.edu/training/devsecops-process-and-implementation

In this course, you learn DevOps, a set of software development principles that emphasize collaboration, communication, and automation among all stakeholders. You study how to design and build a secure development pipeline from project planning through deployment. You learn about reference architectures and use cases for architectural design principles, including technical demonstrations and practical scenarios.

Who should attend? anyone working in software development, including technical managers, technical leads, developers, security staff, quality assurance engineers, release/deployment engineers, and operational staff who want to bring DevOps to their organization; those who want to improve their existing DevOps strategy to include security; those looking for solutions to managing evolving software development needs; those challenged by slow deployment cycles; those who see a disconnect among business needs, development, and operational teams; and those looking for strategies to convince their organization of the benefits of DevOps

Topics covered include an explanation of DevOps, organizational needs and linking business into DevOps, communication and collaboration, infrastructure as code, continuous integration and testing, continuous delivery/deployment, process monitoring and measurement, secure DevOps, and hands-on exercises.

Software Assurance Methods in Support of Cybersecurity Engineering

4.5-Hour Course • Online

insights.sei.cmu.edu/training/cert-cybersecurity-engineering-software-assurance-professional-certificate

In this course, you study four critical software assurance areas: security requirements, software supply chain assurance, mission thread analysis, and measurement. You are exposed to concepts and resources for addressing software security assurance across the acquisition and development lifecycles.

Who should attend? software managers, technical leads, software and lead engineers, software and system acquisition experts, and program/project managers

Topics covered include the challenges of software assurance; key concepts and methods for security risk analysis and measurement, including security requirements elicitation, mission thread analysis, and supply chain risk analysis; best practices for software assurance; and more.

This course is a component of the **CERT Cybersecurity Engineering and Software Assurance Professional Certificate**. For additional details, see Training Certificates section.

SQUARE Workshop

Nine-Hour Workshop • Online

insights.sei.cmu.edu/training/cert-cybersecurity-engineering-software-assurance-professional-certificate

In this workshop, you learn popular techniques for identifying security requirements and the Security Quality Requirements Engineering (SQUARE) Method. You apply the SQUARE method's nine steps through a series of guided exercises. You study five hours in class and spend five additional hours on assigned exercises.

Who should attend? software acquirers and developers, software and system assurance managers, systems engineers, and software engineers

Topics covered include the challenges of security requirements engineering; how identifying functional requirements may not work for security requirements; and methods used for security risk analysis, security requirements elicitation, and security requirements identification.

This course is a component of the **CERT Cybersecurity Engineering and Software Assurance Professional Certificate**. For additional details, see Training Certificates section.

Security Engineering Risk Analysis (SERA) Tutorial

Two-Hour Tutorial • Online

insights.sei.cmu.edu/training/cert-cybersecurity-engineering-software-assurance-professional-certificate

In this tutorial, you learn the Security Engineering Risk Analysis (SERA) method, a systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain. You apply the steps of the SERA method to a realistic system acquisition scenario.

Who should attend? software acquirers and developers, software and system assurance managers, systems engineers, and software engineers

Topics covered include risk management concepts as applied to software and systems engineering, details of the SERA method, and how to identify and address cybersecurity weaknesses in the design phase of the development lifecycle.

This course is a component of the **CERT Cybersecurity Engineering and Software Assurance Professional Certificate**. For additional details, see Training Certificates section.

Supply Chain Risk Management

1.5-Hour Course • Online

insights.sei.cmu.edu/training/cert-cybersecurity-engineering-software-assurance-professional-certificate

In this course, you learn about the complex, multi-layered information and communication technologies related to supply chains. You study how to address supply chain cybersecurity by developing an acquisition strategy that defines supply-chain-related actions.

Who should attend? software acquirers and developers, software and system assurance managers, systems engineers, and software engineers

Topics covered include identifying gaps in supply chain risk management, exploring different types of supply chain relationships, and developing an acquisition strategy to drive supply chain structure.

This course is a component of the **CERT Cybersecurity Engineering and Software Assurance Professional Certificate**. For additional details, see Training Certificates section.

Advanced Threat Modeling

2.5-Hour Course • Online

insights.sei.cmu.edu/training/cert-cybersecurity-engineering-software-assurance-professional-certificate

In this course, you learn threat modeling techniques, including an expanded STRIDE (Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service, and Elevation of privileges) methodology and three additional threat modeling techniques. You study the most recently developed threat modeling methods and how they are used in different scenarios.

Who should attend? software acquirers and developers, software and system assurance managers, systems engineers, and software engineers

Topics covered include the role of threat modeling in the security development lifecycle, how to apply threat models to a system, how to assess new threat modeling methods, and how they apply in a system environment.

This course is a component of the **CERT Cybersecurity Engineering and Software Assurance Professional Certificate**. For additional details, see Training Certificates section.

Secure Software Concepts

Two-Hour Course • Online

insights.sei.cmu.edu/training/cert-secure-coding-professional-certificate/

In this course, you learn basic security concepts and how security design principles protect your organization. To prepare for a deep study of secure coding, you learn about risk assessment and management, regulatory requirements, and software design in the context of an organization's acquisition and development lifecycles.

Who should attend? software developers in government and industry organizations who want to increase the security of their code and reduce its vulnerability to attack and IT professionals who want to gain a working knowledge of common programming errors that lead to software vulnerabilities, how these errors can be exploited, and effective mitigation strategies for preventing the introduction of these errors

Topics covered include software design in the context of acquisition and development, preventing vulnerabilities that can lead to cybersecurity attacks, security design principles and their impact, and what secure coding really means.

This course is a component of the **CERT Secure Coding in C and C++ Professional Certificate** and **CERT Secure Coding in Java Professional Certificate**.
For additional details, see Training Certificates section.

Secure Coding in C and C++

Online

insights.sei.cmu.edu/training/cert-secure-coding-in-c-and-c-professional-certificate

In this course, you learn common programming errors in C and C++ and how these errors can lead to code that is vulnerable to exploitation. You study security issues intrinsic to the C and C++ programming languages and their associated libraries.

Who should attend? C and C++ developers

Topics covered include how coding errors can be exploited, effective mitigation strategies, how to thwart buffer overflows and stack-smashing attacks, how to eliminate integer-related problems, how to avoid I/O vulnerabilities, and more.

This course is a component of the **CERT Secure Coding in C and C++ Professional Certificate**. For additional details, see Training Certificates section.

Secure Coding in Java

Online

insights.sei.cmu.edu/training/cert-secure-coding-in-java-professional-certificate

In this course, you learn about common programming errors in Java and how they can lead to code that is vulnerable to exploitation. You study security issues intrinsic to Java programming languages and their associated libraries.

Who should attend? Java developers

Topics covered include how coding errors can be exploited, effective mitigation strategies, how to avoid injection attacks, how to prevent race conditions while avoiding deadlock, how to throw and catch exceptions at the right time, and more.

This course is a component of the **CERT Secure Coding in Java Professional Certificate**. For additional details, see Training Certificates section.

Secure DevOps Process and Implementation

Five-Hour Course • Online

insights.sei.cmu.edu/training/secure-devops-process-and-implementation

In this course, you learn DevOps principles, processes, and techniques for project planning, development, and deployment. You are exposed to reference architectures and use cases on continuous integration tools and practices, including technical demonstrations and practical scenarios.

Who should attend? software development technical managers, technical leads, developers, quality assurance engineers, release engineers, and operational support staff

Topics covered include the common pitfalls and missteps of DevOps; adapting DevOps theories, practices, and tools to meet your particular business needs; and providing measurable value to your organization.

Risk Assessment & Insider Threat

Overview of Insider Threat Concepts and Activities

Three-Hour Course • Online

insights.sei.cmu.edu/training/overview-of-insider-threat-concepts-and-activities

In this course, you learn the latest insider threat terminology, how to identify the different types of insider threats, how to recognize technical and behavioral indicators, and mitigation strategies.

Who should attend? Executive leadership, current or potential insider threat program team members and program managers, non-executive employees that have access to classified information, and employees who interact with and support insider threat program team members

Topics covered include insider threat definitions, issues, and types; severity and impact of insider threat activity; sabotage, fraud, and theft of intellectual property; unintentional insider threat; and insider threat prevention, detection, and mitigation strategies.

Building an Insider Threat Program

Seven-Hour Course • Online

insights.sei.cmu.edu/training/building-an-insider-threat-program

In this course, you learn about the organizational models and necessary components of an insider threat program. You learn how to identify the key stakeholders to involve, create, and roll out an implementation plan and identify needed policies and procedures.

Who should attend? insider threat program team members and program managers

Topics covered include identifying the staff and skills needed for an insider threat program operational team, identifying the type of governance and management support needed to sustain the formal program, and more.

Insider Risk Management: Measures of Effectiveness

Three-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/insider-risk-management-measures-of-effectiveness

In this course, you develop the skills and competencies needed to assess an organization's insider threat prevention, detection, and response capabilities; evaluate the effectiveness of formal insider threat and insider risk management programs; identify the maturity of an organization's insider risk management processes and practices; and develop tailored metrics for various aspects of insider threat and insider risk management program operation.

Who should attend? insider threat program practitioners (managers, analysts, etc.) looking for ways to measure the effectiveness of their insider threat and insider risk management capabilities; security auditors looking for ways to extend or adapt their current auditing capabilities to comprehensively cover insider threats

Topics covered include ITVA, ITPE, and IRMPE assessment methodology lifecycles; ITVA, ITPE, and IRMPE components; ITVA, ITPE, and IRMPE question sets; assessor knowledge, skills, and abilities; assessment planning, preparation, and execution; and applying the GQIM process to insider threat and insider risk management program activities.

Insider Threat Program Manager: Implementation and Operation

Three-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/insider-threat-program-manager-implementation-and-operation

In this course, you learn a process roadmap you can use to build an insider threat program. You study techniques and methods for developing, implementing, and operating program components. You learn how to establish insider threat detection and prevention programs to satisfy government mandates and guidance.

Who should attend? insider threat program team members and managers

Topics covered include identifying critical assets and protection schemes, identifying data sources and priorities for data collection, improving security awareness, identifying competencies for insider threat team staff, and more.

Insider Threat Analyst

Three-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/insider-threat-analyst

In this course, you learn strategies for collecting and analyzing data to prevent, detect, and respond to insider activity. You study techniques and methods for designing, implementing, and measuring the effectiveness of various components of an insider threat data collection and analysis capability. Applying what you've learned, you will be able to navigate the insider threat tool landscape.

Who should attend? insider threat program team members and managers

Topics covered include strategies for identifying risks to assets from insiders, data collection and analysis for technical and behavioral data, data sources for insider threat analysis, prioritizing data sources, developing insider threat indicators from raw data, advanced analytics for insider threat mitigation, and more.

Insider Threat Awareness Training

One-Hour Course • Online

insights.sei.cmu.edu/training/insider-threat-awareness-training/

In this course, you learn about insider threats and how to protect your organization's critical assets. You also learn how insider threats can affect your work.

Who should attend? all employees (especially those with a security clearance), senior executives, insider threat program team members, insider threat program managers, contractors and subcontractors, and suppliers and business partners

Topics covered include the common motivations of malicious insiders, different types of insider threats, the impacts of insider threats, how you can be targeted by malicious individuals and external adversaries, and more.

Assessing Information Security Risk Using the OCTAVE Approach—eLearning

Three-Day Course • Classroom • Live-Online • Online • On-Site

insights.sei.cmu.edu/training/assessing-information-security-risk-using-octave-elearning/

In this course, you learn to perform information security risk assessments using the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach. You study OCTAVE's prescribed activities for risk identification, analysis, and response.

Who should attend? security professionals, business continuity planners, compliance personnel, risk managers, and others who must satisfy security standard requirements

Topics covered include the connection between information security, business continuity, IT operations, and operational risk management; tailoring OCTAVE to meet unique organizational needs; and more.

Risk Program Development—Governance and Appetite Workshop

Two-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/risk-program-development-governance-and-appetite-workshop

In this course, you learn the latest model in the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)—the Facilitated process for managing Operational Risks Tailored for the Enterprise (FORTE). OCTAVE FORTE helps your organization assess its technical risks and build an enterprise risk management (ERM) program using a process that spans the entire risk management lifecycle from identification through closure.

Who should attend? executives, managers, and technical staff who play a decision-making role in the organization, including members of the following functions: security, information security, information systems, strategy, risk management, and operation

Topics covered include the fundamental principles of risk management, risk frameworks and standards, establishing risk governance and appetite, managing critical services and assets, gathering resilience requirements, risk analysis, response planning, and measuring risk program effectiveness.

Introduction to the CERT Resilience Management Model

Two-Day Course • Classroom • Live-Online • On-Site

insights.sei.cmu.edu/training/introduction-to-the-cert-resilience-management-model

In this course, you learn how to manage operational resilience using the CERT Resilience Management Model (CERT-RMM). You also learn how to evaluate your current security, business continuity, and IT operations practices and determine which ones are working and which ones to replace.

Who should attend? security and business continuity professionals; process improvement professionals, particularly those focusing on operations processes; enterprise and operational risk management professionals; and anyone interested in applying a maturity model approach to managing operational resilience

Topics covered include CERT-RMM process areas, how CERT-RMM is used to appraise an organization's capability for managing operational resilience, and how to plan process improvement in your organization.

Acquisition Support

Agile Virtual Schoolhouse

Live-Online

insights.sei.cmu.edu/training/agile-virtual-schoolhouse

This collection of customized, online learning sessions—called Agile Virtual Schoolhouse—introduces you to Agile-related topics. Each package includes a self-study assignment and a live lecture/discussion session to help build a shared understanding of Agile across your organization. You are introduced to the Agile/Lean principles that inform organizational change, and you explore how to implement Agile principles in software-intensive programs.

Who should attend? leaders and staff of software-intensive, government programs who want to learn more about how Agile principles can be applied in a highly regulated government setting.

Topics covered include one or more of the following: Agile in the DoD landscape; Agile/Lean principles deep dive; oversight vs. insight in Agile, government settings; Agile and requirements; Agile and testing; Agile and system engineering; Kanban in the program office; and DevSecOps for the program office.

Leading SAFe/Agile in Government

Three-Day Course • On-Site

insights.sei.cmu.edu/training/leading-safeagile-in-government

In this course, you are introduced to the interactions that government program offices have with developers who are using Agile team methods and the Scaled Agile Framework (SAFe) approach to develop government systems. You also learn about the Agile and Lean concepts that software developers use and how those concepts impact government program office activities.

Who should attend? government staff who (1) interact with contractor SAFe/Agile teams, (2) are considering adopting SAFe/Agile methods, or (3) will be interacting in an Agile enterprise; development contractors interested in understanding how government organizations expect to interact with them in Agile development settings

Topics covered include SAFe principles and application; Agile basics (e.g., lifecycles, the Agile Manifesto, methods, and practices); the new product-owner role of government; Agile insight and oversight; SAFe portfolio management; Agile in the larger ecosystem; and enabling an Agile culture.

Agile Adoption Readiness and Fit Workshop

Two-Day Workshop • Live-Online • On-Site

insights.sei.cmu.edu/training/agile-adoption-readiness-and-fit-workshop

In this workshop, you learn how to identify the adoption risks related to an Agile governance or acquisition approach. You study your current program environment to determine which areas are ready to adopt Agile methods, identify the relevant adoption risks, and develop mitigation strategies.

Who should attend? teams considering or currently engaged in an Agile adoption project

Topics covered include the Readiness and Fit Analysis (RFA) technique, how to create a profile of the assumptions inherent in new Agile practices, and how to map those assumptions to the cultural and social realities of the organization.

Agile in Government: Concepts for Senior Executives

Half-Day Tutorial • Live-Online • On-Site

insights.sei.cmu.edu/training/agile-in-government-concepts-for-senior-executives

In this tutorial, you participate in a small group of senior executives who are contemplating or are already in the process of adopting Agile approaches in their organizations. You learn the major tenets and principles of the Agile Manifesto and why Agile is not a "silver bullet" for government acquisition.

Who should attend? government decision makers in programs already within an Agile enterprise of interacting with contractor Agile teams

Topics covered include Agile basics (e.g., lifecycles, principles, methods, and practices); the government's role as a product owner; Agile insight and oversight (e.g., technical reviews, requirements management); Agile in the larger ecosystem (e.g., systems engineering, OSD policy); and enabling an Agile culture.

Agile in Government: Practical Considerations

Two-Day Tutorial • Live-Online • On-Site

insights.sei.cmu.edu/training/agile-in-government-practical-considerations

In this tutorial, you learn basic Agile concepts, but you focus on the interactions that government program offices can and should have with Agile developers building government systems. You study several areas of acquisition that are affected by the use of Agile methods and practices.

Who should attend? government staff who (1) interact with contractor Agile teams, (2) are considering adopting Agile methods for their own work, or (3) were told they will be interacting in an Agile enterprise, and development contractor staff who are interested in understanding how the government expects to interact in Agile development settings

Topics covered include Agile basics (e.g., lifecycles, principles, methods, and practices); the government's role as a product owner; Agile insight and oversight (e.g., technical reviews, requirements management); Agile in the larger ecosystem (e.g., systems engineering and OSD policy); and enabling an Agile culture.

Agile Requirements Elicitation Workshop

Onsite

insights.sei.cmu.edu/training/agile-requirements-elicitation-workshop

The purpose of this two-day workshop is to capitalize on pre-existing work on requirements for the system in question; bringing information into a consistent, actionable form; filling gaps in requirements when uncovered; and paying attention to non-functional architectural drivers.

Who should attend? participants who represent a broad spectrum of stakeholders in the desired system. Participants should also expect that the system will be developed according to Agile principles.

Topics covered include beginning with level setting on terminology and understanding of existing artifacts and then leads through a series of exercises designed to elicit: expected roles, operational value streams/use cases, mission threads supporting the value streams, functional requirements on the systems to support the mission threads, and non-functional requirements to be used as architectural drivers.

Agile Requirements Prioritization Workshop

Onsite

insights.sei.cmu.edu/training/agile-requirements-prioritization-workshop

The purpose of this one-day workshop is to teach members of an organization how to prioritize requirements using their own requirements for a development effort. Subsequently, the organization can use the same techniques to reprioritize requirements as needed.

Who should attend? participants who represent a broad spectrum of stakeholders in the desired system. Participants should also expect that the system will be developed according to Agile principles.

Topics covered include beginning with a short tutorial on requirements prioritization (and the need for periodic review of the priorities) and then participants will select techniques appropriate to the current needs. The selection will be based on factors such as: the number of requirements, the number of participants, and environmental factors.

AI Engineering and Machine Learning

CERT Artificial Intelligence (AI) for Cybersecurity

Online

insights.sei.cmu.edu/training/cert-ai-cybersecurity-professional-certificate

Over the past decade, artificial intelligence (AI) has made remarkable strides. From deep neural networks that can identify and label objects in images, to AI systems that outperform humans in complex games like chess, to the emergence of large language models like ChatGPT that can respond to a wide range of queries, we have entered a new era of AI.

These AI advancements are transforming many fields, including cybersecurity. AI technologies can streamline existing cybersecurity processes and enable entirely new approaches. However, these technologies also introduce new potential attack vectors for adversaries.

Who should attend? cybersecurity professionals who operate in technical roles

Topics covered include constructing machine learning (ML) models, applying deep neural networks (DNNs), interacting with large language models (LLMs), analyzing text data, creating automated planners, selecting and implementing appropriate AI tools for various cybersecurity challenges.

Introduction to Artificial Intelligence (AI) Engineering—eLearning

Online

insights.sei.cmu.edu/training/introduction-to-ai-engineering-elearning

Introduction to Artificial Intelligence (AI) Engineering is an introductory eLearning course designed to help you develop a foundational understanding of the process, requirements, resources, and constraints involved in engineering AI-enabled systems. By the end of this course, you will have a better understanding of how you can use AI technologies to solve real-world problems and how you can use the AI engineering process to build human centered, scalable, robust, and secure AI Systems.

Who should attend? design researchers, usability experts, AI ethicists, risk and compliance officers, program managers, product managers, executives, data scientists, software engineers, machine learning (ML) engineers, data engineers, and solution architects

Topics covered include an overview of the discipline of AI engineering, planning an AI solution, architecting an AI system, building AI systems with multidisciplinary teams, and AI risk management

Fundamentals of Statistics Applied to Cybersecurity

Online

insights.sei.cmu.edu/training/fundamentals-of-statistics-applied-to-cybersecurity

Through the fundamentals of statistics related to cybersecurity, aspiring data scientists can

- gain knowledge of common problems that a data scientist encounters
- become fluent in statistics with the help of a scripting language
- increase predictive power and reduce risk within a model
- better estimate parameters for a dataset
- investigate and solve problems in the cybersecurity realm

Who should attend? those with a particular interest in data science and cybersecurity, but limited experience with both concepts

Topics covered include fundamentals of probability, including basic properties of probability, common distributions of data, visualizing data, maximum likelihood estimation, hypothesis testing, parametric and nonparametric tests, supervised and unsupervised learning methods, the bias-variance tradeoff, training and validating a model, and regularization techniques for creating more generalizable models.

Advanced Analytics: Netflow

Online

insights.sei.cmu.edu/training/advanced-analytics-netflow

After learning about NetFlow related to cybersecurity, aspiring data scientists can

- gain knowledge of common problems that a data scientist encounters
- become fluent in NetFlow with the help of a scripting language
- understand NetFlow architecture
- identify types of attacks with network flow data
- gain experience with different types of attacks
- investigate and solve problems in the cybersecurity realm

Who should attend? Those with a particular interest in data science and cybersecurity, but limited experience with both concepts.

Topics covered include Bayes' Rule and Error Rate, common metrics in machine learning, common machine learning algorithms, network flow architecture, flowmeters and records, brute force attacks with network flow data, DRDoS attacks with network flow data, and network beacons with network flow data.

Advanced Analytics: Malware

Online

insights.sei.cmu.edu/training/advanced-analytics-malware

After learning about malware related to cybersecurity, aspiring data scientists can

- gain knowledge of common problems that a data scientist encounters
- become fluent in malware with the help of a scripting language
- understand principles of investigating and analyzing properties of malware captured at run time
- understand how to detect several suspicious behaviors
- gain experience with hands-on feature engineering and building end-to-end data pipelines
- gain experience with deep neural networks and train one to identify malicious processes
- investigate and solve problems in the cybersecurity realm

Who should attend? Those with a particular interest in data science and cybersecurity, but limited experience with both concepts.

Topics covered include fundamentals of malware, self-replication, behavior detectors and PID statistics, suspicious requests and process ancestry, fundamentals of neural networks and deep learning, regularization with deep learning, the bias-variance tradeoff, and training deep neural networks/identifying malicious processes.

Advanced Analytics: Digital Forensics

Online

insights.sei.cmu.edu/training/advanced-analytics-digital-forensics

After learning about digital forensics related to cybersecurity, aspiring data scientists can

- gain a fundamental understanding of forensic based data science problems
- become fluent in natural language processing techniques for insider threat analysis with the help of a scripting language
- better understand the procedure for a digital investigation
- investigate and solve problems in the cybersecurity realm utilizing data science techniques

Who should attend? Those with a particular interest in data science and cybersecurity, but limited experience with both concepts.

Topics covered include fundamentals of digital forensics, crimes with digital assets, PRAVARA and a digital investigation, deepfakes, neural networks and natural language processing techniques related to insider threat analysis through email.

Training Certificates

CERT Artificial Intelligence (AI) for Cybersecurity Professional Certificate

One course and an Exam

insights.sei.cmu.edu/credentials/cert-artificial-intelligence-ai-cybersecurity-professional-certificate

The CERT Artificial Intelligence (AI) for Cybersecurity Professional Certificate introduces technical professionals to the application and implications of AI on cybersecurity. SEI cybersecurity experts focus their instruction on the strengths, limitations, and appropriate use cases for AI technology in cybersecurity and how AI tools can be selected and realistically applied. The curriculum concludes with a comprehensive examination on the material taught.

Who should attend? Cybersecurity professional operating in technical roles

CERT Applied Data Science for Cybersecurity Certificate Package

Four Courses and an Exam

insights.sei.cmu.edu/training/cert-applied-data-science-for-cybersecurity-certificate-package

Through this Professional Certificate program, the CERT machine learning research scientists and cybersecurity experts at the Software Engineering Institute (SEI) share their expertise in a suite of courses teaching ML and AI techniques and best practices for the analysis of cybersecurity data using the tools of data science.

Who should attend? analysts with a particular interest in data science and cybersecurity, but limited experience with both concepts

CERT Certificate in Digital Forensics

Two Courses

insights.sei.cmu.edu/training/cert-certificate-in-digital-forensics

By earning this certificate, you—as a system and network administrator—build on your existing skills by learning the essential elements of digital forensics. You study how to approach both routine and unusual events in a systematic, forensic manner. Ultimately, you will understand the fundamentals of computer forensics, including how to apply good forensic practices to routine administrative procedures and alert verification, and how routine actions can adversely affect the forensic value of data.

Who should attend? experienced system and network computer professionals who collect, store, and analyze computer systems and network data; and those who conduct digital forensics, systems security analysis, or incident response activities

CERT Cybersecurity Engineering and Software Assurance Professional Certificate

Five Courses and an Exam

insights.sei.cmu.edu/credentials/cert-cybersecurity-engineering-and-software-assurance-professional-certificate/

By earning this certificate, you become aware of cybersecurity and learn approaches that are helpful in establishing cybersecurity engineering practices. Its courses introduce you to areas critical to software assurance, including security requirements, risk analysis, software supply chain assurance, and mission thread analysis. You study the SQUARE (Security Quality Requirements Engineering) Method, SERA (a risk analysis method), supply chain risk analysis, and advanced threat modeling.

Who should attend? software acquirers and developers, software and system assurance managers, systems engineers, and software engineers

CERT Incident Response Process Professional Certificate

Two Courses

insights.sei.cmu.edu/credentials/cert-incident-response-process-professional-certificate/

Earning this certificate prepares you to be a member of a computer security incident response team (CSIRT). You study incident handling and common and emerging attacks that target a variety of operating systems and architectures. You gain insight into the work of a CSIRT member and other topics related to incident handling, including intruder threats, the nature of incident response activities, and how incident handlers can respond to system compromises.

Who should attend? CSIRT technical personnel; systems and network administrators responsible for identifying and responding to security incidents

CERT Insider Risk Management Measures of Effectiveness Certificate

Three courses and an Exam

insights.sei.cmu.edu/credentials/cert-insider-risk-management-measures-of-effectiveness-certificate/

Earning this certificate helps practitioners acquire the knowledge, skills, and abilities they need to develop metrics that align with their organizations' insider risk management goals.

Who should attend? insider threat program practitioners (managers, analysts, etc.) looking for ways to measure the effectiveness of their insider threat and insider risk management capabilities; security auditors looking for ways to extend or adapt their current auditing capabilities to comprehensively cover insider threats.

CERT Insider Threat Program Manager (ITPM) Certificate

Three Courses and an Exam

insights.sei.cmu.edu/credentials/cert-insider-threat-program-manager-certificate/

By earning this certificate, you learn how to develop a formal insider threat program in your organization. You study 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.

Who should attend? insider threat program managers and team members

CERT Secure Coding in C and C++ Professional Certificate

Two Courses and an Exam

insights.sei.cmu.edu/credentials/cert-secure-coding-in-c-and-c-professional-certificate/

Earning this certificate helps you increase the security of your software and reduce vulnerabilities in the programs you develop using C and C++. You learn to recognize common programming errors that lead to software vulnerabilities, thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic, avoid the incorrect use of dynamic memory management functions, eliminate integer-related problems, and avoid I/O vulnerabilities, including race conditions.

Who should attend? C and C++ software developers

CERT Secure Coding in Java Professional Certificate

Two Courses and an Exam

insights.sei.cmu.edu/credentials/cert-secure-coding-in-java-professional-certificate/

Earning this certificate helps you increase the security of your software and reduce vulnerabilities in the programs you develop using Java. You learn to recognize common programming errors that lead to software vulnerabilities, avoid injection attacks, understand Java's memory model, recognize when to throw and catch exceptions, understand how common errors can be exploited, employ mitigation strategies to prevent introducing common errors, and avoid I/O vulnerabilities.

Who should attend? Java software developers

CISO-Executive Certificate Program

16 Modules

heinz.cmu.edu/programs/executive-education/chief-information-security-officer-certificate

Earning this certificate enables you to develop and manage information security (IS) resources and design and implement organizational IS policies. You study everything from security metrics to enterprise security governance to crisis communication to information security law. You learn to address the issues that chief information security officers (CISOs) face and have an opportunity to interact with peer CISOs.

Who should attend? CISOs or those in equivalent positions

CRO Certificate Program

14 Modules

heinz.cmu.edu/programs/executive-education/chief-risk-officer-certificate

Earning this certificate provides domain leaders with the latest skills and best practices in risk management. You focus on what chief risk officers (CROs) need to be successful and develop your risk management skills. You learn strategies for communicating risks to executive leadership and learn about tools you can use to analyze and address enterprise risks.

Who should attend? CROs or those in equivalent positions

National Association of Corporate Directors (NACD) Cyber-Risk Oversight Program

16 hours/Seven Modules

nacdonline.org/events/detail.cfm?itemnumber=37092

Enhance your cyberliteracy. Understand your board's responsibilities for overseeing cyber-risk preparedness. Earn the CERT Certificate in Cybersecurity Oversight by completing this self-paced, online course developed by NACD, Ridge Global LLC and the CMU SEI CERT Division. The course consists of seven modules, including a cyber-crisis simulation exercise and series of exams. The course takes approximately 16 hours to complete, and participants complete the course at their own pace. Exams must be completed within one year of registration.

Who should attend? Corporate board members and directors or those in equivalent positions

SEI Service-Based Architecture Professional Certificate

Three Courses and an Exam

insights.sei.cmu.edu/credentials/sei-service-based-architecture-professional-certificate/

Earning this certificate provides you with the software architecture and service-oriented architecture (SOA) concepts and practices that you need to successfully architect service-based systems. The courses that support this certificate apply to service-based systems in general and do not favor specific platforms, tools, or products.

Who should attend? software professionals responsible for designing, developing, or deploying service-based systems; technical and project managers responsible for migrating legacy systems or managing SOA or microservice implementations

SEI Software Architecture Professional Certificate

Three Courses and an Exam

insights.sei.cmu.edu/credentials/sei-software-architecture-professional-certificate/

Earning this certificate provides you with the breadth and depth of knowledge you need to understand software architecture concepts and practices. Beginning with software architecture fundamentals, you gain experience in effective architecture documentation, design, and analysis techniques, and then learn how these techniques can be used in adopting a product line approach to software.

Who should attend? designers and developers of software-reliant systems

Course Credit

Training courses provided by the SEI are not academic courses for academic credit toward a degree. Any certificates provided are evidence of the completion of the courses and are not official academic credentials.

Copyrights

Copyright 2025 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

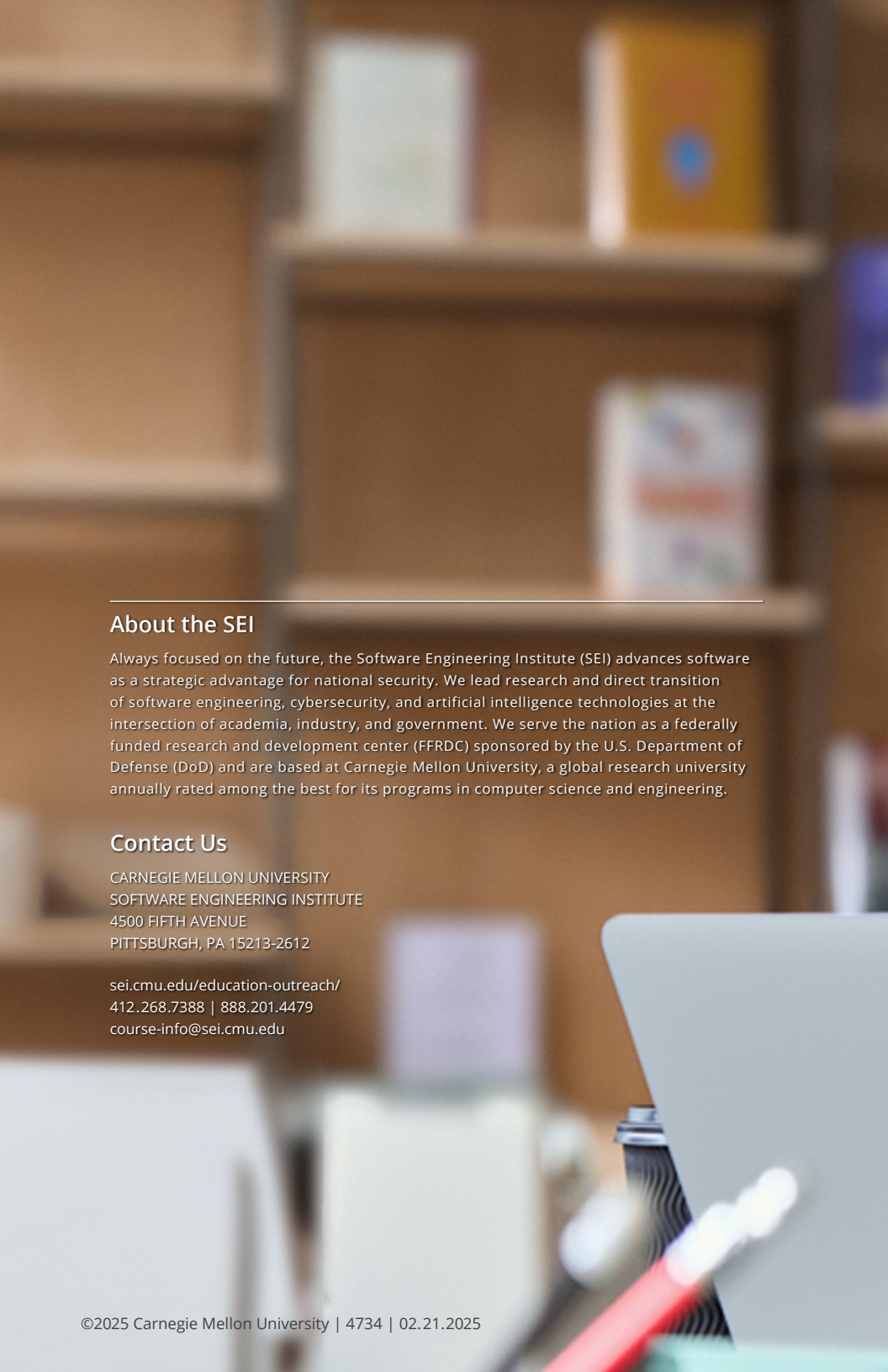
NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. Requests for permission for non-licensed uses should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT®, ATAM®, Carnegie Mellon®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM25-0263



About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

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

sei.cmu.edu/education-outreach/
412.268.7388 | 888.201.4479
course-info@sei.cmu.edu

©2025 Carnegie Mellon University | 4734 | 02.21.2025