Carnegie Mellon University
Software Engineering Institute

SEI Education and Training Catalog

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

Get the Edge You Need

By completing our training courses at the Software Engineering Institute (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.


Online learning includes 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 the total class hours using the ANSI/IACET standard, which awards one CEU for 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 • Online • On-Site

sei.cmu.edu/training/V07.cfm

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 to 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.

Documenting Software Architectures

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

sei.cmu.edu/training/V18.cfm

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 IEEE 1471-2000 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.

Software Architecture Design and Analysis

Two-Day Course • Classroom • On-Site

sei.cmu.edu/training/p34.cfm

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.

Designing Modern Service-Based Systems

One-Day Course • Classroom • On-Site

sei.cmu.edu/training/p124.cfm

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, and learn about 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 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 • On-Site

sei.cmu.edu/training/p125.cfm

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 style; design guidelines for successful service-based solutions; and strategies, including several design patterns that can be used to realize service-orientation guidelines.

Managing Technical Debt of Software

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

sei.cmu.edu/training/V37.cfm

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.

Advanced Software Architecture Workshop

Two-Day Workshop • On-Site

sei.cmu.edu/training/p102.cfm

In this workshop, you are introduced to an architecture that has undergone evaluation through the SEI Architecture Tradeoff Analysis Method (ATAM). You learn to select a problematic scenario for a system, examine weak points of its software architecture, decide appropriate mitigations, review proposed changes in groups, and revise the architecture as required.

Who should attend? software architects and software lead designers who want to practice what they've learned in the SEI software architecture curriculum or want to prepare for a project that requires major architecture improvements

Topics covered include improving architecture through a defined process, analyzing and planning architecture tasks, improving an existing architecture design, conducting a scenario-based peer review, and preparing documentation to support conformance of the implementation.

Architecture Tradeoff Analysis Method (ATAM) Evaluator Training

Two-Day Course • Classroom • On-Site

sei.cmu.edu/training/p31.cfm

In this course, you learn to conduct a software architecture evaluation using the ATAM, including how to apply it to software architectures. You perform an ATAM evaluation exercise with guidance from your instructors to systematically evaluate software architectures for fitness of purpose and to expose architectural risks.

Who should attend? those responsible for or involved in the evaluation of software architectures, such as software architects, system architects, software designers, system designers, and those who want to participate in SEI-authorized ATAM evaluations

Topics covered include quality attributes and their role in software architectures, quality attribute tradeoffs, and why architecture analysis is important.

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

Five-Day Course • On-Site

sei.cmu.edu/training/p72.cfm

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

sei.cmu.edu/training/p128.cfm

In this course and follow-up workshop, you learn and apply the modeling techniques necessary to adopt 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.

Software Product Lines

11-Hour Course • Online

sei.cmu.edu/training/V08.cfm

In this course, you learn the basic concepts of software product lines and the essential technical and management practices needed to succeed with them. Using case studies, you learn how to apply product line techniques and determine whether a product line approach is right for your organization.

Who should attend? software engineers and technical managers interested in effective reuse strategies or who are adopting or using a software product line approach

Topics covered include the essential activities involved in fielding software product lines, product line practice patterns that aid in product line adoption, a product line diagnostic method, and more.

Cyber Intelligence

Cyber Intelligence for Decision Makers

Two-Hour Course • Online

sei.cmu.edu/training/V33.cfm

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 • On-Site

sei.cmu.edu/training/p25.cfm

In this course, you learn the issues and decisions you need to address when establishing a CSIRT. You develop an action plan for implementing a CSIRT in your organization. You study organizational models for CSIRTs, the services that a CSIRT can provide, and the resources and infrastructure needed to support one.

Who should attend? current and prospective CSIRT managers, C-level managers interested in establishing a CSIRT, and other staff who interact with CSIRTs

Topics covered include developing and implementing a new CSIRT; addressing issues related to assembling a responsive, effective team; using organizational models for a new CSIRT; and more.

Managing Computer Security Incident Response Teams (CSIRTs)

Three-Day Course • Classroom • On-Site

sei.cmu.edu/training/p28.cfm

In this course, you develop a pragmatic view of the issues you face when operating an effective CSIRT. You gain insight into the work that CSIRT staff may be expected to handle as well as the basics of the incident-handling process and the types of tools and infrastructure it needs to be effective.

Who should attend? CSIRT managers and other staff who interact with CSIRTs and want to learn more about how they operate

Topics covered include the policies and procedures needed to establish a CSIRT; processes for detecting, analyzing, and responding to computer-security events and incidents; key components for sustaining CSIRT operations; and more.

Foundations of Incident Management

Four-Day Course • Classroom • On-Site

sei.cmu.edu/training/P139.cfm

This four-day 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.

Who should attend? new incident handlers, investigators, and 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 NICE1 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 the current threat environment and basic incident management processes, team code of conduct, gathering critical information, data sources for incident investigation, detecting and analyzing incidents, performing triage, analyzing log files, identifying the basic steps in response, using the domain name system, finding contact information, coordinating response and disseminating information, handling email and malicious code attacks, understanding insider threats, and working with law enforcement.

Advanced Topics of Incident Handling

Four-Day Course • Classroom • On-Site

sei.cmu.edu/training/P23B.cfm

This four-day course, designed for computer security incident response team (CSIRT) and security operations center (SOC) technical personnel, addresses techniques for detecting and responding to current and emerging computer security threats and attacks. Participants work as 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. Participants also review more advanced types of activities related to incident handling, such as threat hunting, artifact and malware analysis, vulnerability handling, and publishing and communicating information.

Who should attend? current CSIRT, SOC, and other security operations technical staff with six or more months incident handling experience

Topics covered include incident handling lifecycle review, data loss prevention techniques, advanced persistent threats, artifact and malware analysis categories and techniques overview, fundamental causes of vulnerabilities, vulnerability handling overview, analyzing and coordinating response to major computer security events and incidents and developing and delivering effective communications.

Thinking like an Analyst

One-Day Course • On-Site

sei.cmu.edu/training/P143.cfm

This tutorial introduces the basic skills necessary to be an effective cyber analyst. The central focus is analytical acumen, or "how to think."

Practical application of portions of the analytic process will be interspersed throughout the presentation, building around a scenario of a company at risk while conducting IT business processes.

Who should attend? staff new to incident handling processes and related technology and staff with limited incident handling experience who are seeking formal training to improve their skills or benchmark their existing operations who are in other parts of an enterprise and want a basic understanding of incident handling

Topics covered include framing the analysis context, logical fallacies, data gathering, microanalysis, macroanalysis, awareness of assumptions, the various forms of bias, and reporting.

Effective Security Operations

Two-Day Course • On-Site

sei.cmu.edu/training/P140.cfm

This two-day course takes a more detailed look at security operations (including SOC operations) and what it means to be effective. The course includes lectures, discussions, and group exercises regarding practices to improve security operations and functions. The course also introduces new trends and functions for moving security operations forward and provides information to help an organization identify a strategy for security operations transformation and enhancement. The course presents methods for structured analysis and allows attendees to test their understanding by applying the analysis techniques via tabletop exercises.

Who should attend? individuals performing security operations roles and activities, individuals coordinating with or interfacing with a security operations team or SOC, individuals reporting incidents to a SOC, and individuals managing security operations functions.

Topics covered include effective security operations, organizational issues for effectiveness, situational awareness, structured analysis techniques and comparisons, and strategies for transformation and future growth.

Introduction to Computer Forensics

Two-Hour Course • Online

sei.cmu.edu/training/V34.cfm

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.

Advanced Digital Forensics

Ten-Hour Course • Online

sei.cmu.edu/training/V34.cfm

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.

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

One-Day Course • On-Site

sei.cmu.edu/training/p68.cfm

In this course, 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).* You learn best practices in planning, implementing, operating, and evaluating a CSIRT.

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 differentiating between incident management and incident response activities, identifying the type of work that CSIRT managers and staff may be expected to handle, and more.

Network & Software Security

Enterprise Information Security for Technical Staff

Four-Day Course • Classroom • On-Site

sei.cmu.edu/training/P138.cfm

This four-day course is designed to provide participants with practical techniques for protecting the security of an organization's information assets and resources, beginning with concepts and proceeding to technical implementations.

The course provides a technical foundation for working with TCP/IP security and cryptography. The course focuses on concepts such as host hardening, network hardening, and network monitoring, and it helps participants learn to design a secure network architecture managing host systems, securing network services and infrastructure, working with firewalls, and understanding ways of monitoring and defending against cyber intrusions.

Who should attend? technical staff members who manage or support networked information systems and have

- two years of practical experience with networked systems or equivalent training/education
- some degree of familiarity with the ISO/OSI 7-layered reference model as well as TCP/IP, and major network operating systems, such as Windows and Linux

Topics covered include the challenge of survivability; cryptography and its application; tcp/ip security; secure network design; intrusion detection, prevention, and access controls; network monitoring; logging principles and best practices; securing host systems; host and application security; and common cyber attacks and preventive measures.

Hands-On Threat Detection and Hunt

Four-Day Course • Classroom • On-Site

sei.cmu.edu/training/P142.cfm

This four-day hands-on course is designed to increase the knowledge and skills of technical staff charged with administering and securing information systems and networks. Cybersecurity topics such as network monitoring, intrusion detection and response, digital forensics, and threat hunting will offer a comprehensive defense-in-depth experience. Each participant will have direct administrative access to a wide variety of networked systems, which will be leveraged throughout the course. Instruction will consist of cybersecurity tool demonstrations, individual labs, and team-based exercises modeled from real-world threat scenarios.

Who should attend? technical staff members who manage or support networked information systems and have

- two years of practical experience with networked systems or equivalent training/education
- some degree of familiarity with the ISO/OSI 7-layered reference model as well as TCP/IP and major network operating systems such as Windows and Linux

Topics covered include network and system monitoring; event collection, analysis, and correlation; incident detection and response; digital investigation (aka forensics) best practices; volatile and persistent system data analysis; common cyber attacks and preventive measures; threat hunting; and remote live forensics.

DevSecOps Process and Implementation

Three Day Course • On-Site

sei.cmu.edu/training/P141.cfm

DevOps is a set of software development principles that emphasize collaboration, communication, and automation among all stakeholders, including IT operations, testers, developers, customers, and security personnel at the inception of a project. This tutorial is designed for managers, developers, security, and operational teams, and it covers DevOps principles and processes for designing and building a secure development pipeline for project planning, gathering and meeting cybersecurity requirements, secure development, security testing, and deployment from start to finish. You will learn about reference architectures and use cases for architectural design principles on continuous integration (CI), continuous delivery/deployment (CD), and continuous authorization (CA) tools and practices, including technical demonstrations and practical scenarios.

Who should attend? anyone working in software development, including technical managers, technical leads, developers, QA engineers, release/deployment engineers, and operational support staff who want to bring DevOps to their organization; want to improve their existing DevOps strategy to include security; are looking for solutions to manage evolving software development needs; are challenged by slow deployment cycles; see a disconnect between business needs, development and operational teams; or are looking for strategies to convince their business 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 exercise.

Software Assurance Methods in Support of Cybersecurity Engineering

4.5-Hour Course • Online • On-Site

sei.cmu.edu/training/V46.cfm

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, security requirements elicitation, mission thread analysis, and supply chain risk analysis; best practices for software assurance; and more.

Security Requirements Engineering Using the SQUARE Method

One-Day Course • On-Site

sei.cmu.edu/training/p104.cfm

In this course, you learn about security requirements engineering and the SQUARE method. You learn the steps of the method in detail. For each step, you participate in a team case study and discuss follow-up research and transition activities. You learn how SQUARE helps organizations build security into the early stages of the production lifecycle.

Who should attend? software managers, technical leads, software engineers, requirements engineers, and security specialists

Topics covered include the importance of developing security requirements when you develop functional requirements, why methods to identify functional requirements may not work directly for security requirements, methods for security risk analysis, and more.

SQUARE Workshop

Nine-Hour Workshop • Online • On-Site

sei.cmu.edu/training/V46.cfm

In this workshop, you learn popular techniques for identifying security requirements and the Security Quality Requirements (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.

Security Engineering Risk Analysis (SERA) Tutorial

Four-Hour Tutorial • Online

sei.cmu.edu/training/V46.cfm

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.

Supply Chain Risk Management

1.5-Hour Course • Online

sei.cmu.edu/training/V46.cfm

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.

Advanced Threat Modeling

4.5-Hour Course • Online

sei.cmu.edu/training/V46.cfm

In this course, you learn threat modeling techniques, including an expanded STRIDE 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, and how to assess new threat modeling methods and how they apply in a system environment.

Secure Software Concepts

Two-Hour Course • Online

C and C++: sei.cmu.edu/training/V35.cfm

Java: sei.cmu.edu/training/V36.cfm

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.

Secure Coding in C and C++

Four-Day Course • Online • On-Site

sei.cmu.edu/training/V35.cfm

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.

Secure Coding in Java

Four-Day Course • Online • On-Site

sei.cmu.edu/training/V36.cfm

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.

Secure DevOps Process and Implementation

Five-Hour Course • Online

sei.cmu.edu/training/V38.cfm

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, QA 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.

Vulnerability Response Capability Development

One-Day Course • On-Site

sei.cmu.edu/training/p123.cfm

In this course, you learn the key issues, processes, and decisions that must be made to enable your organization to respond to vulnerabilities reported in its products. You develop an action plan to use as a starting point for planning and implementing your vulnerability response capability.

Who should attend? managers and project leaders, current and prospective product security managers, and project leaders interested in establishing or starting a vulnerability response capability

Topics covered include requirements, policies, and procedures for establishing a vulnerability response capability, various organizational models used, and the types of resources and infrastructures needed to support a team.

Risk Assessment & Insider Threat

Insider Threat Overview: Preventing, Detecting, and Responding to Insider Threats

Five-Hour Course • Online

sei.cmu.edu/training/V26.cfm

In this course, you learn the different types of insider threats, the threats they pose to critical assets, how to recognize technical and behavioral indicators, and various insider threat mitigation strategies.

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

Topics covered include the prevalence of insider threat activity and the damage it can cause, how to recognize and avoid unintentional insider threats, the best practices for insider threat mitigation, and more.

Building an Insider Threat Program

Seven-Hour Course • Online

sei.cmu.edu/training/V27.cfm

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 Threat Program Manager: Implementation and Operation

Three-Day Course • Classroom • On-Site

sei.cmu.edu/training/p110.cfm

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 Program Evaluator Training

Three-Day Course • Classroom • On-Site

sei.cmu.edu/training/p133.cfm

In this course, you learn strategies for measuring and evaluating an operational insider threat program in an organization. Using scenario-based exercises, you study how to conduct an insider threat program evaluation, including designing an evaluation plan, building an evaluation team, and scoring capabilities based on evidence.

Who should attend? insider threat program managers, evaluators, team members, those interested in licensing the CERT methodology and tools to perform insider threat program evaluations, and those working in auditing and risk management

Topics covered include techniques and templates for performing evaluation preparation and execution tasks and processes for engagement, planning, data collection, scoring, and report development.

Insider Threat Vulnerability Assessor Training

Three-Day Course • Classroom • On-Site

sei.cmu.edu/training/p112.cfm

In this course, you develop the skills and competencies needed to perform an insider threat vulnerability assessment. You learn how to plan and conduct an assessment to identify issues, design tactical countermeasures, and formulate a strategic action plan for long-term risk mitigation.

Who should attend? those interested in performing an insider threat vulnerability assessment

Topics covered include developing a data collection plan, interviewing staff to corroborate indicators, entering evidence into the Joint Assessment Tool (JAT), scoring capabilities, defending assessment results, and more.

Insider Threat Analyst

Three-Day Course • Classroom • On-Site

sei.cmu.edu/training/p132.cfm

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

sei.cmu.edu/training/V29.cfm

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

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

sei.cmu.edu/training/V22.cfm

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.

OCTAVE FORTE: Connecting the Board Room to Cyber Risk

Two-Day Course • Classroom • On-Site

sei.cmu.edu/training/P136.cfm

Organizations need an adaptable and agile process that allows executives to have a real-time view of cyber risks. To address this challenge, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) process has been helping organizations assess their technical risks for the better part of two decades, and the SEI has recently worked to update the process model to manage cyber risks in a manner that is consistent across an entire enterprise. The Facilitated process for managing Operational Risks Tailored for the Enterprise (FORTE) focuses upon building an enterprise risk management (ERM) program for organizations with nascent risk management programs or improving on existing programs to drive risk management with a process that spans the entire risk management lifecycle from identification through closure.

Who should attend? This course is targeted to executives, managers, and technical staff who play a decision making role in the enterprise. This may include members of the following functions: security, information security, information systems, strategy, risk management, operation.

Topics covered include fundamental principles of risk management, 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.

System Assessment and Authorization Process

Two-Day Course • Classroom • On-Site

sei.cmu.edu/training/P137.cfm

This two-day course introduces the NIST Risk Management Framework (RMF) process for system assessment and authorization. The RMF is the cybersecurity framework mandated for federal government departments and agencies, including the U.S. Department of Defense (DoD). Like other NIST guidance, the RMF is also used by organizations outside of the federal government to ensure a comprehensive and effective system assessment and authorization process.

This course places the RMF process within a broader cyber risk management and resilience context and provides guidance on implementing a disciplined and effective RMF process. The course includes lectures and class exercises with opportunity for discussions and participant questions. After attending the course, participants will understand the fundamental concepts underpinning the RMF, have a working knowledge of RMF process steps, and be able to improve the implementation of RMF in their organizations.

Who should attend? Leaders, managers, and technical staff members with oversight and/or management responsibility for information systems, and those wishing to gain implementation knowledge as well as high-level knowledge of RMF and NIST Security Controls, will find value in attending.

Topics covered include risk management and resilience, cybersecurity frameworks and standards, privacy and security, NIST, and RMF roles and responsibilities.

Measuring What Matters: Security Metrics Workshop

Workshop • Classroom • On-Site

sei.cmu.edu/training/p117.cfm

In this workshop, you develop specific business goals and learn about the questions, indicators, and actionable metrics that you can implement in your organization to improve how you manage operational risks, particularly cybersecurity risks.

Who should attend? directors and managers of operational risk management, information technology (IT), cybersecurity/information security, IT and cybersecurity compliance, and IT and cybersecurity auditors

Topics covered include refining strategic or business objectives to meet specific, measureable, achievable, relevant, time-bound, evaluated, and reviewed (SMARTER) criteria and initiate the Goals, Questions, Indicators, Metrics (GQIM) process; identifying a set of goals based on your business objectives; and more.

Introduction to the CERT Resilience Management Model

Two-Day Course • Classroom • On-Site

sei.cmu.edu/training/p66.cfm

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 looking to 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

Leading SAFe/Agile in Government

Three-Day Course • On-Site

sei.cmu.edu/training/p126.cfm

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.

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 • On-Site

sei.cmu.edu/training/p130.cfm

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

0.5-Day Tutorial • On-Site

sei.cmu.edu/training/p131.cfm

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 interacting with contractor Agile teams or within an Agile enterprise

Topics covered include Agile basics, including 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 eco-system (e.g., systems engineering, OSD policy); and enabling an Agile culture.

Agile in Government: Practical Considerations

Two-Day Tutorial • On-Site

sei.cmu.edu/training/p129.cfm

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, or (2) are considering adopting Agile methods for their own work, or (3) were told they will be interacting in an Agile enterprise, and (4) development contractor staff who are interested in understanding how the government expects to interact in Agile development settings

Topics covered include Agile basics, including 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.

Acquisition Essentials for Software-Reliant Systems

One-Hour Course • Online

sei.cmu.edu/training/V23.cfm

In this course, you learn three fundamental software acquisition topics: software requirements, software architecture, and software testing. You study stories from real acquisition programs that show the significance of these three topics.

Who should attend? acquisition program leaders and staff

Topics covered include the unique challenges of software-reliant systems and the knowledge needed to manage software-reliant acquisition programs and keep them on track by proactively recognizing symptoms and implementing recovery strategies.

Twenty Questions to Assess Your Program's Chances of Success

One-Hour Course • Online

sei.cmu.edu/training/V24.cfm

In this course, you learn risk management concepts and the 20 key drivers that comprise the SEI risk-based method for assessing complex projects: the Mission Diagnostic Protocol. You study these drivers and how the assessment of a program using these drivers creates a profile of a program's chances of success.

Who should attend? managers and program staff interested in project and program management as well as those interested in learning how to assess and manage risk in developmental and operational settings

Topics covered include risk management concepts and terminology, the key drivers of program success, how drivers can be used when assessing a program's systemic risk, and using the *Standard Driver Workbook* to assess a program's success.

Practical Risk Management: Principles and Methods

Two-Day Course • On-Site

sei.cmu.edu/training/p78.cfm

In this course, you learn practical methods for managing risk across the lifecycle and supply chain. You learn a practical approach to risk management, and you examine several ways to implement this approach.

Who should attend? project managers; lead engineers; software engineers; risk managers and others performing risk management activities; EPG and SEPG members; change or technology transition agents; and those from related disciplines, such as quality assurance, acquisition, security, and IT

Topics covered include tailoring the Mosaic risk management methodology to your needs and constraints, applying Mosaic risk management methods to evaluate an existing risk management practice for completeness and effectiveness, and more.

Training Certificates

CERT Certificate in Digital Forensics

Two Courses

sei.cmu.edu/go/forensics-credentials

As a system and network administrator, you must understand the fundamentals of computer forensics. You must also apply good forensic practices to routine administrative procedures and alert verification, and know how routine actions can adversely affect the forensic value of data. This certificate builds on your existing skills by teaching you the essential elements of digital forensics. You study how to approach both routine and unusual events in a systematic, forensic manner.

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

sei.cmu.edu/go/assurance-credentials

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) 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 Insider Threat Program Manager (ITPM) Certificate

Three Courses and an Exam

sei.cmu.edu/go/itpm-credentials

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 Insider Threat Program Evaluator (ITPE) Certificate

Three Courses and an Exam

sei.cmu.edu/go/itpe-credentials

Earning this certificate enables insider threat program team members to help organizations understand the effectiveness of their insider threat programs. You study the concepts and practices necessary for measuring and managing an organization's insider threat risk.

Who should attend? technical staff members who manage or support networked information systems

CERT Insider Threat Vulnerability Assessor (ITVA) Certificate

Three Courses and an Exam

sei.cmu.edu/go/itva-credentials

Earning this certificate enables you to help organizations gain a better understanding of their insider threat risk and identify and manage that risk. You study an assessment methodology that measures how prepared organizations are to prevent, detect, and respond to insider threats.

Who should attend? insider threat program managers and candidate assessors

CERT Incident Response Process Professional Certificate

Two Courses

sei.cmu.edu/go/response-credentials

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

CERT Information Security Professional Certificate

Two Courses

sei.cmu.edu/go/infosecurity-credentials

Earning this certificate provides you with practical techniques for protecting the security of your organization's information assets and resources, and it increases your ability to administer and secure information systems and networks. You study security issues, technologies, and recommended practices at increasing layers of complexity, beginning with concepts and proceeding to technical implementations.

Who should attend? technical staff members who manage or support networked information systems

CISO-Executive Certificate Program

Fourteen Courses

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

Ten Courses

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

CERT Secure Coding in C and C++ Professional Certificate

Two Courses and an Exam

sei.cmu.edu/go/securec-credentials

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

sei.cmu.edu/go/securejava-credentials

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

SEI Software Architecture Professional Certificate

Three Courses and an Exam

sei.cmu.edu/go/architecture-credentials

Earning this certificate provides you with the breadth and depth 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

SEI Architecture Tradeoff Analysis Method (ATAM) Evaluator Certificate

Two Courses and an Exam

sei.cmu.edu/go/atam-credentials

Earning this certificate prepares you to perform SEI-authorized ATAM architecture evaluations. You study the essential concepts of software architecture and the ATAM, an effective method for systematically evaluating software architectures for fitness of purpose.

Who should attend? software professionals responsible for or involved in the evaluation of software architectures

SEI Service-Based Architecture Professional Certificate

Three Courses and an Exam

sei.cmu.edu/go/servicearch-credentials

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

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.

About the SEI

For more than three decades, the Software Engineering Institute (SEI) has been helping government and industry organizations acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy. 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