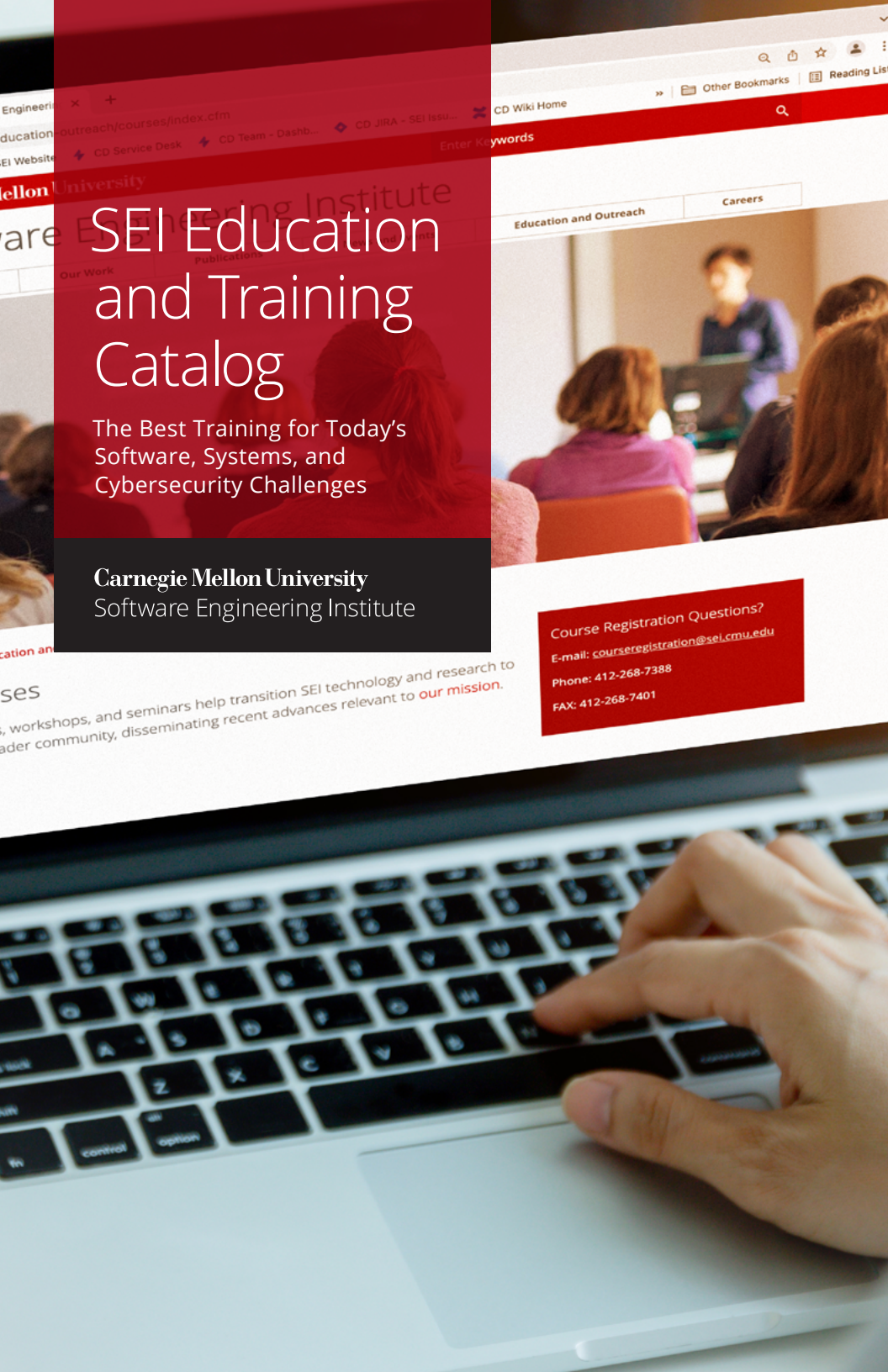

SEI Education and Training Catalog

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

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

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 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

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.

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

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.

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

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, 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

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 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 • 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.

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

Five-Day Course • Online • On-Site

sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=V40
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 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

sei.cmu.edu/training/v48.cfm

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

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 • Live-Online • 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 and effective team, using organizational models for a new CSIRT, and more.

Managing Computer Security Incident Response Teams (CSIRTs)

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

sei.cmu.edu/training/P139.cfm

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. This course is recommended for those new to incident handling or security operations work.

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 the current threat environment; the incident management team code of conduct; security tools and technologies used by incident handlers; and basic incident management process, including gathering critical information, detecting and analyzing incidents, performing triage, 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, and working with law enforcement.

Advanced Topics of Incident Handling

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

sei.cmu.edu/training/P23B.cfm

In this course, you learn techniques for detecting and responding to current and emerging computer security threats and attacks. You work on a team throughout the course to handle a series of escalating incidents as part of an ongoing scenario. Your team analyzes information and presents findings and response strategies.

Who should attend? computer security incident response team (CSIRT), security operations center (SOC), and other security operations technical staff with six or more months of incident handling experience

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

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)—eLearning

Three-Hour Course • Online

sei.cmu.edu/training/v49.cfm

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.

Network & Software Security

DevSecOps Process and Implementation

Three-Day Course • On-Site

sei.cmu.edu/training/P141.cfm

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

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

SQUARE Workshop

Nine-Hour Workshop • Online

sei.cmu.edu/training/V46.cfm

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.

Security Engineering Risk Analysis (SERA) Tutorial

Two-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

2.5-Hour Course • Online

sei.cmu.edu/training/V46.cfm

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.

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++

Online

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

Online

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, 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

sei.cmu.edu/training/V26.cfm

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

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 • Live-Online • 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 • Live-Online • 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, and 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 • Live-Online • 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 • Live-Online • 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 • Live-Online • 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 • Live-Online • On-Site

sei.cmu.edu/training/P136.cfm

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.

System Assessment and Authorization Process

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

sei.cmu.edu/training/P137.cfm

In this course, you are introduced to the NIST Risk Management Framework (RMF) process for system assessment and authorization, a 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 non-government organizations. The course includes lectures, class exercises, and discussions.

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 a high-level knowledge of RMF and NIST security controls

Topics covered include fundamental concepts of the RMF, how RMF fits within the broader context of cyber risk management and resilience, RMF process steps, cybersecurity frameworks and standards, privacy and security, NIST RMF roles and responsibilities, implementing a disciplined and effective RMF process, and improving the implementation of RMF in your organization.

Measuring What Matters: Security Metrics Workshop

Workshop • Classroom • Live-Online • 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, measurable, 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 • Live-Online • 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 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

sei.cmu.edu/training/p145.cfm

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

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 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

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

Half-Day Tutorial • Live-Online • 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 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

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, (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.

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 how to use the *Standard Driver Workbook* to assess a program's success.

Training Certificates

CERT Certificate in Digital Forensics

Two Courses

sei.cmu.edu/go/forensics-credentials

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

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 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 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; systems and network administrators responsible for identifying and responding to security incidents

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

https://www.nacdonline.org/events/detail.cfm?itemnumber=37092

Enhance your cyberliteracy. Understand your board's responsibilities for overseeing cyber-risk preparedness. Developed by NACD, Ridge Global LLC, and the CMU SEI CERT Division, earn the CERT Certificate in Cybersecurity Oversight by completing this self-paced, online course. 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

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 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

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

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, artificial intelligence, and emerging 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