COURSE SYLLABUS

Software Supply Chain Security: SSDF, Attestations and SBOMs Course (Self-Paced)

Understand the SSDF, software producer self-attestation, and SBOMs so you can evaluate vendor submissions with confidence.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/software-supply-chain-security-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Why Software Supply Chain Security Became a Federal Priority

- Lessons:
  - What a Software Supply Chain Actually Includes
  - How a Compromise Upstream Becomes an Agency's Problem
  - Executive Order 14028 and the Federal Response
- Applied activity: Learners review a short, described scenario in which a widely used software update is later found to contain malicious code and trace which of the agency's own systems would be affected and why.

Module 2: The Secure Software Development Framework (SSDF)

- Lessons:
  - What the SSDF Is and Who It Is For
  - The Four SSDF Practice Groups
  - How the SSDF Differs From a Compliance Checklist
  - Reading an SSDF Practice: An Example Walkthrough
- Applied activity: Learners review a short, described SSDF practice statement and identify what a software producer would need to do, and what evidence they might produce, to demonstrate they follow it.

Module 3: Self-Attestation: What Agencies Require From Software Producers

- Lessons:
  - The Self-Attestation Requirement, and What It Actually Asks For
  - Who Signs an Attestation, and What They Are Certifying
  - What an Agency Does With an Attestation Once Received
  - When an Attestation Is Not Enough: Artifacts and Extensions

- Applied activity: Learners review a short, described attestation submission and identify whether it meets the basic requirements, then decide what an agency's next step should be if it does not.

Module 4: Software Bills of Materials (SBOMs): What They Are and How Agencies Use Them

- Lessons:
  - What an SBOM Actually Contains
  - Reading a Simple SBOM Example
  - Why Agencies Ask for SBOMs
  - Common SBOM Formats and Limitations
- Applied activity: Learners review a simplified, described SBOM listing several components and identify which one would need immediate attention if a newly disclosed vulnerability affected a specific component and version.