Get the training you need. And guidance when you need it.

Security Innovation's unique security education platform TEAM Academy™ combines TEAM Professor™ online training with TEAM Mentor™ secure coding knowledgebase - ensuring users learn key principles and can apply them in practice.

TEAM Academy™ has the industry's broadest and deepest coverage for application security content:

- **Various Roles & Phases**
  Architect, Developer, Tester/QA, IT, DevOps, Managers

- **Popular Languages & Technologies**
  Java, .NET, C/C++, PHP, C#, AJAX, ObjectiveC, jQuery, Scala, Ruby on Rails

- **Major Platforms**
  Web, Mobile, IoT, Database, Cloud, Windows

- **Compliance and Risk Frameworks**
  PCI-DSS, OWASP, NIST, CWE, and other best practices

- **All Skill Levels**
  Courses span foundational (100-level) to advanced topics (400-level)

Contact Us: RSAUniversity@rsa.com
While scanning tools and industry frameworks are widely adopted, they don’t provide the code-level guidance developers need, leaving them unequipped to fix security holes.

With over 2,500 guidance assets, TEAM Mentor™ provides the platform- and technology- specific remediation assistance for the task at hand, e.g., fixing a buffer overflow vulnerability for an iOS application written in Objective-C.

**EASILY SEARCH, Edit and ADD CONTENT**
Users can search by vulnerability category, guidance type, or technology. All articles are editable and extensible so you can customize to your internal coding standards and technology environment.

**LINKS TO REFRESHER COURSES IN TEAM PROFESSOR™**
As developers are accessing guidance, they have the option to take a refresher course related to specific articles. For example, a developer might be invited to participate in a SQL injection simulation exercise in TEAM Professor™ while viewing an input sanitation article in TEAM Mentor™.

**HELPS MEET COMPLIANCE AND POLICY MANDATES**
TEAM Mentor™ easily translates CWE, OWASP Top 10, PCI DSS and other popular “standards” into actionable steps for developers. It can also store and cross-references your security policies and internally approved libraries, ensuring teams are adhering to defined requirements.

**INTEGRATES WITH POPULAR SAST TOOLS**
Offered as a plug-in to HP Fortify and Checkmarx scanners, TEAM Mentor™ provides superior remediation directly within the development environment, ensuring that vulnerabilities are understood, fixed quickly, and don’t recur scan after scan.

**TEAM Mentor™ Integrated with HP Fortify**
When a vulnerability is found during a scan, detailed vulnerability descriptions, remediation checklists, and code samples are shown in the relevant programming language.
Leveraging the industry's largest application security eLearning library, TEAM Professor™ builds the awareness and technical skills needed to integrate security at every phase of development.

ACCURATE & TIMELY CONTENT
Security Innovation has an in-house pool of experts that create source content. Additionally, findings from our security testing practice are constantly restructured into appropriate course content. Updates are made on a quarterly, annual and ad-hoc basis, depending on the nature of the course.

INTERACTIVE & ENGAGING
We strive to include as many complex and real-world interactions as possible when the topic warrants it. For example, in a technical course we may include an input sanitation simulation to illustrate the impact of a SQL Injection attack, or ask a developer to debug a block of code to find the line that enables a Cross-Site Scripting vulnerability; whereas in an awareness course, we may have the student participate in a drag-and-drop game regarding the classification of sensitive data.

PROGRESSIVE & ROLE-BASED CURRICULUM
TEAM Professor features over a dozen pre-defined bundles with varying course skill levels (100-400 levels), ensuring topics previously learned are expanded upon and knowledge retention maximized. Additionally, organizations can create custom curricula for any role, technology and platform.

Sample "out of the box" bundles include:

**Java Developer**
- COD 101. Secure Development Fundamentals
- COD 153. Secure AJAX Code Fundamentals
- COD 211. Creating Secure Code - Java Foundations
- COD 252. Creating Secure AJAX Code - Java
- COD 313. Creating Secure Java Code
- COD 342. Creating Secure jQuery Code

**Architect**
- AWA 101. Application Security Fundamentals
- DES 101. Fundamentals of Secure Architecture
- DES 212. Architecture Risk Analysis
- ENG 301. Creating a Security Threat Model
- DES 311. Creating Secure Architecture
- ENG 311. Attack Surface Analysis & Reduction

**Mobile Developer**
- COD 110. Secure Mobile Development Fundamentals
- COD 217. Creating Secure Code - iPhone
- COD 218. Creating Secure Code - Android
- COD 317. Creating Secure iPhone Code in Objective-C
- COD 318. Creating Secure Android Code in Java

**Tester/QA**
- TST 201. Classes of Security Defects
- TST 211. How to Test for the OWASP Top 10
- TST 401. Advanced Software Security Testing
- TST 411. Exploiting Buffer Overflows
Integration in Action.
TEAM Professor learners can click on highlighted topics to explore code, vulnerability, and remediation examples further in TEAM Mentor.

Expert Knowledge. Real Learning
TEAM Academy content is derived from our ongoing security assessments of the world’s most dominant software applications and research conducted in our Centers of Excellence. This results in content that is timely, accurate and reflects the current threat and attack landscape.