CyberSecurity Journey

Information Assurance (STIG) Overview (TT8800)

Explore best practices for design, implementation, and deployment, inspired by the diverse and powerful STIGs

Course Snapshot

- **Course: Information Assurance (STIG) Overview (TT8800)**
- **Duration**: 2 days
- **Audience & Skill Level:** The content is appropriate for IT professionals, Developers, Software engineers, technical leads, Project managers, Testing/QA personnel or other key stakeholders .
- **Hands-on:** This course is lecture / demo style event. This is not a hands-on course.
- **Delivery Options**: This course is available for in-person presentation, live online / virtual presentation, or can be presented in a blended learning or short course format.
- **Public Schedule**: This course has active dates on our open enrollment **Public Schedule**.
- **Customizable**: This course agenda, topics and labs can be further adjusted to target your specific training skills objectives, tools and learning goals. Please ask for details.

Overview

The **Information Assurance (STIG) Overview** is a comprehensive two-day course that delves into the realm of Information Assurance, empowering you to enhance your cybersecurity skills, understand the essentials of STIGs, and discover cutting-edge web application security practices. This immersive experience is tailored for IT professionals, developers, project teams, technical leads, project managers, testing/QA personnel, and other key stakeholders who seek to expand their knowledge and expertise in the evolving cybersecurity landscape. The course focuses on the intricacies of best practices for design, implementation, and deployment, inspired by the diverse and powerful STIGs, ultimately helping participants become more proficient in application security.

The first half of the course covers the foundations of DISA's Security Technical Implementation Guides (STIGs) and learn the ethical approach to bug hunting, while exploring the language of cybersecurity and dissecting real-life case studies. Our expert instructors will guide you through the importance of respecting privacy, working with bug bounty programs, and avoiding common mistakes in the field.

The next half delves into the core principles of information security and application protection, as you learn how to identify and mitigate authentication failures, SQL injections, and cryptographic vulnerabilities. You'll gain experience with STIG walkthroughs and discover the crucial steps for securing web applications.

Throughout the course, you'll also explore the fundamentals of application security and development, including checklists, common practices, and secure development lifecycle (SDL) processes. You'll learn from recent incidents and acquire actionable strategies to strengthen your project teams and IT organizations. You'll also have the opportunity to explore asset analysis and design review methodologies to ensure your organization is prepared to face future cybersecurity challenges.

Note: For a deeper (or next-step) exploration of STIGs and Application Security attendees might consider the five-day course TT8815: Understanding and Verifying ASD STIGs

Learning Objectives

Working in an interactive learning environment, guided by our application security expert, you'll explore:

- the concepts and terminology behind defensive coding
- Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- the entire spectrum of threats and attacks that take place against software applications in today's world
- the role that static code reviews and dynamic application testing to uncover vulnerabilities in applications
- the vulnerabilities of programming languages as well as how to harden installations

- the basics of Cryptography and Encryption and where they fit in the overall security picture
- the requirements and best practices for program management as specified in the STIGS
- the processes and measures associated with the Secure Software Development (SSD)
- the basics of security testing and planning

Need different skills or topics? We offer additional cybersecurity, application security and other related topics that may be blended with this course for a track that best suits your needs. Our team will collaborate with you to understand your needs and will target the course to focus on your specific learning objectives and goals.

Audience

The intended audience for this comprehensive course on Information Assurance and STIGs includes professionals with roles such as:

- IT professionals - System administrators, network engineers, and security analysts who are responsible for maintaining and securing IT infrastructure and web applications.
- Developers - Software engineers and web developers who design, implement, and maintain web applications, and need to integrate security best practices throughout the development process.
- Project teams - Cross-functional teams that collaborate on application development projects, including members from development, testing, and deployment teams.
- Technical leads - Senior software engineers or architects who oversee technical aspects of projects and ensure the implementation of secure design and coding practices.
- Project managers - Professionals responsible for planning, executing, and closing projects, ensuring that security requirements are met throughout the project lifecycle.
- Testing/QA personnel - Quality assurance analysts and testers who verify the security, functionality, and performance of web applications before deployment.
- Other key stakeholders - IT managers, CISOs, and decision-makers who need to understand the importance of secure applications and the principles of Information Assurance and STIGs to make informed decisions regarding their organization's cybersecurity posture.

Pre-Requisites

While specific prerequisites may vary depending on the course provider and the targeted audience, a general set of prerequisites for attending a course on Information Assurance and STIGs could include:

- Basic understanding of information security concepts and terminology.
- Familiarity with web application architecture and development.
- Knowledge of networking and web protocols (e.g., HTTP, HTTPS, TCP/IP).
- Experience with programming languages commonly used in web application development, such as JavaScript, Python, Java, or C# would be helpful but not required, as this is not a hands-on class.
- A general understanding of operating systems, databases, and web servers.

Course Topics / Agenda

Session: STIG Foundation

Lesson: DISA's Security Technical Implementation Guides (STIGs)

- The motivations behind STIGs
- Requirements that the various software development roles must meet
- Implementing STIG requirements and guidelines
- Lab: Exploring the STIG Viewer

Lesson: Why Hunt Bugs?

- The Language of Cybersecurity
- The Changing Cybersecurity Landscape
- AppSec Dissection of SolarWinds
- The Human Perimeter
- Interpreting the 2021 Verizon Data Breach Investigation Report
- First Axiom in Web Application Security Analysis
- First Axiom in Addressing ALL Security Concerns
- Lab: Case Study in Failure

Session: Foundation for Securing Web Applications

Lesson: Identification and Authentication Failures

- Applicable STIGs
- Quality and Protection of Authentication Data
- Proper hashing of passwords
- Handling Passwords on Server Side
- Session Management
- HttpOnly and Security Headers
- Lab: STIG Walk-Throughs

Lesson: Injection

- Applicable STIGs
- Injection Flaws
- SQL Injection Attacks Evolve
- Drill Down on Stored Procedures
- Other Forms of Server-Side Injection
- Minimizing Injection Flaws
- Client-side Injection: XSS
- Persistent, Reflective, and DOM-Based XSS
- Best Practices for Untrusted Data
- Lab: STIG Walk-Throughs

Lesson: Database Security

- Design and Configuration
- Identification and Authentication
- Computing Environment
- Database Auditing
- Boundary Defenses
- Continuity of Service
- Vulnerability and Incident Management
- Lab: STIG Walk-Throughs

Session: Moving Forward

Lesson: Applications: What Next?

- Common Vulnerabilities and Exposures
- CWE/SANS Top 25 Most Dangerous SW Errors
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations

Lesson: Cryptographic Failures

- Applicable STIGs
- Identifying Protection Needs
- Evolving Privacy Considerations
- Options for Protecting Data
- Transport/Message Level Security
- Weak Cryptographic Processing
- Keys and Key Management
- Threats of Quantum Computing
- Steal Now, Crack Later Threat
- Lab: STIG Walk-Throughs

Session: Moving Forward with Application Security

Lesson: Application Security and Development Checklists

- Checklist Overview, Conventions, and Best Practices
- Leveraging Common AppSec Practices and Control
- Actionable Application Security
- Additional Tools for the Toolbox
- Strength Training: Project Teams/Developers
- Strength Training: IT Organizations
- Lab: Recent Incidents

Time Permitting

Session: Secure Development Lifecycle (SDL)

Lesson: Principles of Information Security

- Security Is a Lifecycle Issue
- Minimize Attack Surface Area
- Layers of Defense: Tenacious D
- Compartmentalize
- Consider All Application States
- Do NOT Trust the Untrusted
- Lab: Risk Escalators

For More Information

For more information about our dedicated skills-focused training services (instructor-led, self-paced or blended), collaborative coaching services, robust Learning Experience Platform (LXP) solutions, Career Experiences, public course schedule, partner programs, courseware licensing options or to see our complete list of course offerings, training solutions and special offers please visit us at **www.triveratech.com**, email **Info@triveratech.com** or call us toll free at **844-475-4559.** Our pricing and services are always satisfaction guaranteed.

TRIVERA TECHNOLOGIES • Collaborative IT Training, Coaching & Skills Development Solutions
www.triveratech.com • toll free +1-844-475-4559 • Info@triveratech.com • Twitter TriveraTech