



## TT8820: Database Security (STIG)

**According to research by the National Institute of Standards, 92% of all security vulnerabilities are now considered application vulnerabilities and not network vulnerabilities**

Trivera Technologies' *Best Defense™ Security Training Series* is a suite of frontline-oriented security courses that provide complete and current coverage of *DISA's Security Technical Implementation Guides (STIGS)* and associated checklists. STIGS are an integral part of the required configuration standards for DoD Information Assurance measures. These measures are focused on preventing cyber espionage and crime as well as denial-of-service attacks. Our comprehensive set of classes address each of the critical issues head-on, as our courses, seminars and workshops explicitly:

- Teach developers, DBAs, and stakeholders what the vulnerabilities are
- Demonstrate, in real terms, the potential impact of each of these vulnerabilities
- Provide experience in how to recognize and properly address these vulnerabilities
- Teach stakeholders how to defend against the potential consequences of security breaches
- Illustrate the value and the process of integrating security into the entire lifecycle of applications, products, and devices

### COURSE SNAPSHOT

**Course:** TT8820: Database Security (STIG)

**Duration:** 3 days

**Skill Level:** Intermediate and beyond

**Format:** Extensive hands-on programming labs, expert lecture combined with open discussions and high-level demonstrations and dynamic group exercises.

**Language / Tools:** Specific databases that are currently covered are Microsoft SQL Server, IBM's DB2, and Oracle.

**Delivery Format:** Available for onsite private classroom presentation, or live online / virtual presentation

**Audience:** DBAs, developers, and other enterprise team members

**Customizable:** Yes

*DISA's Database STIG*, in conjunction with both generic and product-specific checklists, provides a comprehensive listing of requirements and needs for improving and maintaining the security of Database Management Systems within the Department of Defense. This course fills in the context, background, and best practices for fulfilling those requirements and needs. As with all of our courses, we maintain tight synchronization between the latest DISA releases and our materials. The close ties between this STIG and the *Applications Security and Development STIG* are reflected in the coverage of application issues within the context of this course.

*Database Security* is an intense database security training course essential for DBAs, QA, Testing, and other personnel who need to deliver secure database applications and manage secure databases within the DoD. In addition to teaching basic skills, this course digs deep into sound processes and practices that apply to the entire software development lifecycle. Perhaps just as significantly, students learn about current, real examples that illustrate the potential consequences of not following these best practices.

Data, databases, and related resources are at the heart of the DoD's IT infrastructures. They must be protected accordingly. In this course, students repeatedly attack and then defend various assets associated with a fully-functional database. This approach illustrates the mechanics of how to secure databases in the most practical of terms.

Security experts agree that the least effective approach to security is "penetrate and patch". It is far more effective to "bake" security into an application throughout its lifecycle. After spending significant time trying to defend a poorly designed and configured (from a security perspective) database application, students are ready to learn how to build secure their databases and applications starting at project inception. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

A key component to our coverage of *DISA's Security Technical Implementation Guides (STIGS)*, this course is a companion course with several developer-oriented courses and seminars.

### ► Course Objectives: What You'll Learn

Students who attend **Database Security (STIG)** will leave the course armed with the skills required to recognize actual and potential database vulnerabilities, implement defenses for those vulnerabilities, and test those defenses for sufficiency.

This course quickly introduces students to the most common security vulnerabilities faced by databases today. Each vulnerability is examined from a database perspective through a process of describing the threat and attack mechanisms, recognizing associated vulnerabilities, and, finally, designing, implementing, and testing effective defenses. Multiple practical demonstrations reinforce these concepts with real vulnerabilities and attacks. Students are then challenged to design and implement the layered defenses they will need in defending their own databases.

Working in a dynamic learning environment attendees will learn to:

- Understand the consequences for not properly handling untrusted data such as denial of service, cross-site scripting, and injections
- Be able to review and test databases to determine the existence of and effectiveness of layered defenses and required checks
- Prevent and defend the many potential vulnerabilities associated with untrusted data
- Understand the concepts and terminology behind supporting, designing, and deploying secure databases
- Appreciate the magnitude of the problems associated with data security and the potential risks associated with those problems
- Understand the currently accepted best practices for supporting the many security needs of databases.
- Understand the vulnerabilities associated with authentication and authorization within the context of databases and database applications
- Understand the dangers and mechanisms behind Cross-Site Scripting (XSS) and Injection attacks
- Perform both static reviews and dynamic database testing to uncover vulnerabilities
- Design and develop strong, robust authentication and authorization implementations
- Understand the fundamentals of Encryption as well as how it can be used as part of the defensive infrastructure for data

This class is “technology-centric”, designed to train attendees in essential secure database skills, coupling the most current, effective techniques with the soundest industry practices.

The course provides a solid foundation in basic terminology and concepts, extended and built upon throughout the engagement. Students will examine various recognized attacks against data and databases. Processes and best practices are discussed and illustrated through both discussions and group activities.

### ► Audience & Pre-requisites: Who Should Attend

This is an **intermediate-level** database course, designed for those who wish to get up and running on developing well defended database applications. This course may be customized to suit your team’s unique objectives.

Familiarity with databases is required and real world experience is highly recommended. Ideally, students should have approximately 6 months to a year of database working knowledge.

### ► Related Courses – Suggested Learning Path

**Take Instead:** We offer other courses that provide different levels of knowledge or focus:

- For a high level view of the STIGS and related issues, consider **TT8800 Information Assurance (STIG) Overview**
- For an application orientation, consider: **TT8810 Application Security and Development (STIG)**
- For a high level view of web application security and related issues, consider **TT8020 Understanding Web Application Security**
- For in-depth developer training for web applications with the lifecycle aspect, consider: **TT8325 Securing Web Applications**
- For in-depth developer training with less web application orientation, consider: **TT8200-J Secure Java Coding** (also offered for .net or other languages)

**Take After:** We offer a variety of introductory through advanced security, development, project management, engineering, architecture and design courses. Students may want to consider the following topics as follow-on to this course.

- **TT8150 Mastering Secure SOA**
- **TT8600 Secure Software Design**
- Additional advanced Security or Secure Programming topics
- Service-Oriented Analysis and Design
- Web Services – Intro through Advanced
- Software Engineering, Design or Project Management tracks

Please note all development courses may also be offered in other programming languages or tailored to suit your unique requirements. Please contact us for details. Please contact us for recommended next steps tailored to your longer-term education, project or development objectives.

### ► Delivery Environment: Tools to Use

Although this training is skills-centric, this course can be delivered one of a variety of database products. Please inquire for details and options.

### ► Student Materials: What You'll Receive

Our robust course materials include much more than a simple

slideshow presentation handout. Student materials include a comprehensive hard-copy course manual, complete with detailed course notes, code samples, diagrams and current reference materials, all directly related to the course at hand, indexed for ease of use. Step-by-step lab instructions and project descriptions are clearly illustrated and commented for maximum learning.

In addition to everything students need for the course, the course includes workshop demonstrations; non-restricted workshop software, APIs, documentation, technical education papers, and specifications and tutorials pertinent to the training course. Our course kits are designed to serve as an excellent and useful reference set, long after we leave your classroom.

► **Optional Pre / Post-Testing & Skills Assessment**

We work with you to ensure that your resources are well spent. Through our basic course pre-testing and/or post-course assessments, we ensure your team is up to the challenges that this course offers. Our goal is to structure the best solution to ensure your needs are met, whether we customize the material, or devise a different educational path to prepare for this course.

Please contact us for details about our online pre and post test

assessment services, custom managed training plans for one student or your entire organization, or our custom online training program management system for monitoring the courses or progress while skilling your students of all experience levels.

► **Bridging the Gap: Collaborative Mentoring Services**

Our team of technical experts is also available for various project assistance services to help your team apply their newly-learned classroom skills to their real-world project in a meaningful, practical way, right after the training ends.

Our custom **collaborative mentoring programs** integrate with or extend your team’s classroom training experience, to help bring these skills into existing (or inherited) legacy projects, into new projects, or to simply keep your students sharp them in between projects. Our programs can be highly involved and closely integrated with your project timelines or group development efforts, or can be less involved, serving simply as an overarching educational framework or ‘spot check’ to keep your group skills moving forward in between projects or waiting for projects to begin. Please contact us for details about this exciting custom service.

---

**Workshop Topics Covered**

---

**Session: Foundation**

- Misconceptions
  - Thriving Industry of Identify Theft
  - Dishonor Roll of Data Breaches
  - TJX: Anatomy of a Disaster
  - Heartland: What? Again?
- Security Concepts
  - Terminology and Players
  - Assets, Threats, and Attacks
  - OWASP
  - CWE/SANS Top 25 Programming Errors
- DISA’s Security Technical Implementation Guides (STIGS)
  - Purpose
  - Process
  - Areas Covered
  - Checklists
  - Scripts (SRRs)
  - Resources
- Security Concerns Common to all DBMSs
  - Authentication
  - Authorization
  - Confidentiality
  - Integrity
  - Auditing
  - Replication, Federation, and Clustering
  - Backup and Recovery

- OS, Application, and Network Components
- Defensive Principles
  - Security Is A Lifecycle Issue
  - Minimize Attack Surface
  - Manage Resources
  - Application States
  - Compartmentalize
  - Defense In Depth - Layered Defense
  - Consider All Application States
  - Not Trusting The Untrusted
  - Security Defect Mitigation
  - Leverage Experience
- Reality
  - Recent, Relevant Incidents
  - Find Security Defects In DBMSs

**Session: Top Database Security Vulnerabilities**

- Unvalidated Input
  - Sources of Untrusted Input
  - Trust Boundaries
  - Designing and Implementing Defenses
- Broken Authentication
  - Quality of Passwords
  - Protection of Passwords
  - Hashing Passwords
  - Protecting Authentication Assets
  - System Account Management

- User Account Management
- Broken Access Control
  - Gaining Elevated Privileges
  - Compartmentalization Based on Level of Privilege
  - Special Privileges Provided by Database and Systems
  - Protecting Special Roles
- Cross Site Scripting (XSS/CSRF) Flaws
  - What and How
  - Role of Databases in Enabling XSS
  - Designing and Implementing Defenses
- Injection Flaws
  - What and How
  - SQL, PL/SQL, XML, and Others
  - Stored Procedures
  - Buffer Overflows
  - Designing and Implementing Defenses
- Error Handling and Information Leakage
  - What and How
  - Four Dimensions of Error Response
  - Proper Error Handling Design
- Insecure Handling
  - Data at Rest
  - Data in Motion
  - Encryption

- Compartmentalization Based on Level of Privilege
- Backups and Archives
- Connection Strings and High Value Server-Side Credentials
- Designing and Implementing Defenses
- Insecure Management of Configuration
  - Initial Installation
  - Patch Management
  - Server Hardening
  - Operating System Hardening
  - Connection Hardening
  - Replication Hardening
  - Best Practices
- Direct Object Access
  - What and How
  - Role of Databases in Enabling Access
  - High Risk Practices to Avoid

- Practices
- Enclave Boundary Defenses
  - Continuity of Service
    - Defending Backup/Restoration Assets
    - Data and Software Backups
    - Trusted Recovery
  - Vulnerability and Incident Management

- Best Practices
- Generic Database Checks and Procedures
  - SQL Server Checks and Procedures (Optional)
    - Installation Checks
    - Database Checks
  - Oracle Checks and Procedures (Optional)
    - Database Automated Checks
    - Database Interview Checks
    - Database Manual Checks
    - Database Verify Checks
    - Home Automated Checks
    - Home Interview Checks
    - Home Manual Checks
    - Home Verify Checks
  - Practical Application of the Checklists

#### Session: Secure Software Development (SSD)

- SSD Process Overview
- Asset, Boundary, and Vulnerability Identification
- Process, Design, and Code Reviews
- Applying Processes and Practices
- Configuration Specification and Compliance
- Software and Data Baselines
- Testing as Lifecycle Process
- Testing Planning and Documentation
- Testing Tools And Processes
  - Principles
  - Reviews
  - Testing
  - Tools
- Static and Dynamic Analysis
- Testing Practices
  - Authentication Testing
  - Data Validation Testing
  - Denial Of Service Testing

#### Session: Database Checklists

- Checklist Overview, Conventions, and

#### Session: STIG Database Security Requirements

- Identification and Authentication
  - Group and Individual
  - Key Management Practices
  - Token and Certificates Practices
- Enclave/Computing Environment
  - Auditing Mechanics and Best Practices
  - Data Changes and Controls
  - Encryption
  - Privilege Management
  - Additional Controls and

**Need more details?** Please note that a more detailed outline of the course table of contents, lists of lab exercises and project descriptions is available. Please contact us at [Training@triveratech.com](mailto:Training@triveratech.com) for info.

**Need courseware?** This course is fully customizable, and also available for license with complete support for qualified organizations. Please contact [Courseware@triveratech.com](mailto:Courseware@triveratech.com) for details.

#### ► Why Work With Trivera Technologies?

Whether you are a project leader choosing a training provider or course to bring to your team, or an organization or an instructor looking to potentially license or use course materials to train your own team, or a student looking for an exciting, targeted training class to attend or to recommend to your colleagues - **Our single focus is to make YOUR training event or experience a success.** Here's why choosing Trivera Technologies as your IT security education resource takes the risk right out of your decision making process...

- **We provide a solid secure, design, coding and implementation foundation.** Students will learn how to code, use (and reuse!) essential secure Java programming and design skills and concepts properly, using best coding practices, grounding them for advanced curriculum, and will be prepared for designing and implementing solutions. **Students will learn the importance of developing well-defended applications.**
- **Our courses are focused - no "fluff" included.** We offer more than a "laundry list" approach to teaching. All lessons have clear objectives, are fundamental to core secure application development and design practices, and are reinforced by hands-on labs and solid practical examples. Each lesson has performance driven objectives that ensure students will learn technologies and skills core to fundamental server-side application design – nothing more, nothing less.
- **Our materials are comprehensive, and current.** Our comprehensive manuals include not only a hard copy of the course presentation, but also detailed reference notes, pertinent diagrams and charts, current lists of suggested online resources and articles, and often technical tutorials or white papers geared to the topics at hand. Our dedicated course development team keeps everything as current as possible with both industry trends and software editions to ensure your team is getting the most current information available.
- **We foster "Learning by Doing".** Progressive labs are designed in such a way that students get a firm grasp on fundamental skills while they work toward designing a complete application. All labs are take-home, and all solution code is presented in an easy to use self-study format

for future use and review.

- **We set you up!** Hands-on courses also include our unique materials for each student, complete with our **LoadNGo Instant Classroom** course set up DVD, software, and a multitude of learning resources that complement the course. Run the course right off the DVD – minimal set up for your company – maximum results for your students.
- **We have to adhere to higher standards.** As a courseware provider to other organizations, training firms and/or independent instructors, our content and hands-on lab materials are licensed internationally by dozens of firms, and are therefore subject to very stringent quality requirements. Not only will your organization benefit from our own technical team’s technical expertise, but also benefit from the feedback of hundreds of students and trainers using these materials, worldwide, on a regular basis. This unique fact guarantees that our materials are not only robust and interesting, but also technically correct, current and of the highest quality and usability.
- **We bring years of practical, current experience into the classroom and content.** Our instructors and course authors are also skilled mentors, Java, JEE/JavaEE, J2EE, .Net, Agile, SOA, and web services developers, architects and security-oriented professionals. We believe that learning, using and maintaining solid software execution and delivery methods are as important as gaining sharp coding skills. Best Practices for software development and execution, beyond technical coding skills, are enforced throughout all of our courses and discussions. Our team brings this extensive experience into every classroom and engagement. Our team has trained thousands of students.
- **We're skills-centric.** Although our team has extensive experience using a variety of tools and solutions, our core content is “technology-centric”. Our aim is to teach you the best skills and solutions out there – not to sell you software from any particular vendor.
- **We're Java & JEE / J2EE authors and industry speakers.** Our team was selected to write the online *J2EE, EJB, EJB CMP-CMR and Web Services Tutorial Series for IBM developerWorks®* ([www.ibm.com](http://www.ibm.com)) These are the same instructors who train our classes and author the courseware. Most of our trainers/consultants have also authored additional articles on web services, EJB, Struts, J2EE / JEE and advanced Java topics, and are recognized speakers and presenters on the industry technical seminar circuit. Our team is comprised on several successful published authors. Members of our team have written or contributed to: *Eclipse Kick Start, Mastering Eclipse; Professional Jakarta Struts; Using Java Tools for Extreme Programming; Mastering Resin; Mastering TomCat and others.*
- **Our services are guaranteed.** Whether you’re a stakeholder organizing your firm’s educational services, a student in our live or virtual classroom or a trainer using our materials to educate your own client or team – **Our core mission is to make YOU a success in the classroom.**

#### ► For Additional Information

**Need dedicated training?** All courses can be brought onsite or run virtually for a **private presentation, anywhere around the world**, customized to suit your unique requirements or goals.

Please contact [Training@triveratech.com](mailto:Training@triveratech.com) for course details, Public Schedule dates and locations, and Special Discount Offers.



Trivera Technologies is a 100%  
Female-Owned Small Business Concern  
GSA Schedule # GS-35F-0188T  
Please contact us for details & pricing.

**Need courseware?** **Let us take the risk out of your classroom delivery!** All materials are also available on a worldwide basis for corporate license with complete instructor support and free corporate branding. Our LoadNGo Set up is available to partners as well! We guarantee our pricing and service. Samples of our course materials, as well as live client references for all of our services are available upon request. Please contact [Courseware@triveratech.com](mailto:Courseware@triveratech.com) for details.

**For more information** about our training, mentoring or courseware development or licensing options, or to see our complete list of course offerings and services, please visit us at [www.triveratech.com](http://www.triveratech.com), email [Training@triveratech.com](mailto:Training@triveratech.com) or call 609.953.1515.