Course Description

This course is a one day class run on your site or at a public venue or can be arranged on-line that teaches the delegates about the issues related to designing, enabling and configuring practical and simple audit trails in your databases.

The focus is on free and practical. The class is structured to take the delegate from first principals, what is available with the database and what is easy and simple to implement and manage and report on BUT most importantly what can be done with the free solutions available with the database. Most people are not utilising the free facilities to gain a better understanding of how their databases may be abused both by staff and also potential attackers.

The course also includes a demonstration at the end of a simple practical audit design that works. We include the free tools and scripts written in PL/SQL and SQL so that you can go away and implement something useful in your own database.

Course Goals

The aim of the course is for the students to get an appreciation of how to use the core audit features to best effect in their own database using simple but structured ideas.

Course Duration

The class is One Day 9am to 5pm and is instructor lead with demonstrations

Course Location

The course can be held at your site or students can attend a public class. No public classes are scheduled at present. Details of on-site requirements are provided during the booking process

Course Pre-Requisites

The delegates must have a good working knowledge of PL/SQL and SQL ideally as a Developer or DBA to appreciate the content.

The class is intended for DBA's and developers who can write PL/SQL and is of an intermediate level but students can benefit from the overall message of the class and use the free scripts even if they are not experts themselves

Course Material

The student will receive a URL to download a zip file that includes:

- The course notes as PDF files
- Free PL/SQL tools and scripts
- All of the examples used as SQL and PL/SQL scripts

Course Outline

The course outline is as follows

- Introduction
  - What do we want to achieve, audit goals
  - Reactive audit, proactive audit
- Design process
  - Based on “I want to know”
  - Regulatory reasons to include audit data
  - Local audit, remote storage
  - Technical solutions, Core audit, triggers, functions and Correlation
  - Layered audit, Alerts and escalation
  - Sizing, performance and storage
- What to audit
  - DBA activities and Third party activities, Breakglass, End users
  - Schema and application maintenance
  - Escalation of privilege and audit of data access
- Audit security
  - Protect the audit trails
  - Local, database, file based, remote, syslog
  - Centralising logging and audit
- Auditing audit
  - Protect the audit trails
  - Verify audit and check summing
- Reporting
  - Develop reporting plan and create simple reports with SQL
- Management
  - Purge and archive and manage size and users
- Simple firewalls
  - Implement a simple firewall using triggers and other functions
  - Intrusion detection
  - Intrusion prevention
  - DAM and activity monitoring
- Implementation
  - Sample implementation
- Conclusions
  - Focus on fast and simple and free

This course is fast paced and very interesting and is delivered by one of the most well known experts in database security. Pete Finnigan created the SANS Oracle security step-by-step guide and the CIS Oracle benchmark used by NIST, USA DoD and more is a reference to secure Oracle databases. Pete worked out the mechanisms that Oracle used to protect PL/SQL and showed how they can be easily defeated at the Black Hat conference in Las Vegas in 2006. Pete has published multiple books on databases security and speaks and publishes papers regularly. His company also produces the tool PFCLObfuscate used to protect IPR in PL/SQL.

