KOENIG
step forward

Hardening and Securing Oracle with Pete Finnigan

- Why is data insecure
    - Introduction to the example systems
    - Some realistic demonstrations to show how data can be exposed and leaked and stolen due to design decisions and weak hardening
- Data leakage
    - Data leakage due to the way Oracle works
    - Data leakage due to incomplete solutions
    - Placing data security into categories (10/30/60)
    - Looking at how data access and controls affect security
    - The task of securing all data held in Oracle
- A sample database audit
    - A walk through running a simple free audit scanner script with approximately 50 tests
    - Showing the results of the audit
- Investigation
    - A walk through of the results plus placing the possible solutions in context both in terms possibility and also cost
    - Look at the hardening issues located
    - Look at design issues located with a detailed overview of the reports tool output and showing where and what we could do to reduce the risk posed to the data to the most effect
- Solutions for the data lock down
    - The design solutions presented will be implemented as examples in our sample system

    - User privilege analysis and least privilege steps to reduce risks
    - User authentication and password lock down, protection and profiles design
    - DBA role design
    - DBA access lockdown and process
    - Third party and developer access to the database techniques, process and tools
    - Break glass access, lockdown and monitoring techniques
    - Context based security around time, location and privilege
    - Provisioning of user accounts
- Conclusions
    - What is next
    - Automated scanning
    - Lock down of all databases
    - Policy design and lock down
    - Show how our lock down efforts affect our simple database and application