



## Table of Contents

Preface / Why this book is being written

What we plan to accomplish and in what order

Security Begins at the data layer

1. Environment Configuration
  - Database Servers
  - SAN/Storage
  - Operating Systems
  - Network Infrastructure
  - Installed Software
2. Oracle Database Server Preparation
3. Oracle Database Vault
  - Configuring Oracle Database Vault
4. Oracle Audit Vault & Database Firewall
  - Configuring Oracle Audit Vault
  - Installing OAV Agents and HOSTMON
  - Configuring Oracle Database Firewall
5. Monitoring Servers with Oracle Audit Vault
  - Operating System Monitoring
  - Monitoring Oracle
  - Monitoring MySQL
  - Monitoring IBM DB2
  - Monitoring SQL Server
  - Monitoring PostgreSQL
6. IBM Guardium
7. SQL Firewalls
8. Identity & Access Management
9. Application Security
  - Userid & Passwords



IP Whitelisting

Application Whitelisting

Blacklisting

Biometric Security

Active Directory/LDAP

## 10. Blockchain Technology

## 11. Forensic Collection & Data Use

Collected Data Storage & Reporting

Big Data

Data Collection Format(s)

Splunk

Advanced Threat Detection

Insider Threat

Incident Investigation, Forensics, and Response

SOC Automation

Compliance

Fraud Detection

Security Monitoring

Splunk Add-on Applications

Elasticsearch

Monitoring Password File

Examining System Logfiles

CPU & Memory Analysis

Monitoring Network Traffic

Collecting Shell Histories

Gathering Filesystem Information

Amazon S3 Monitoring Tools


## 12. Email Servers

Email Phishing Attacks

MALWARE Scanning

## 13. Penetration Testing

Information Gathering



Vulnerability Analysis

Wireless Attacks

Web Applications

Exploitation Tools

Stress Testing

Forensics Tools

Sniffing & Spoofing

Password Attacks

Maintaining Access

Reverse Engineering

Hardware Hacking

Reporting Tools

14. Web Proxy Servers

15. VPN Appliance

16. Best Practices

17. Advanced Security Technology Adopters

18. Managing the System Retrofit

Application Software

Application Servers

Multi-Factor Authentication

HTTP Web Servers

Microsoft IIS

Apache

Nginx

Google

HTTP Server Attacks

Encryption Appliances

Oracle Database Encryption

Blockchain

IBM DB2 Database and file Encryption

IBM Multi-Cloud Data Encryption

HP-UX Data Security Offerings



Splunk Encryption

Elastic Encryption

MySQL Encryption

SQL Server Encryption

Sybase Encryption

SAP HANA Encryption

AWS Encryption

MariaDB Encryption

Teradata (FDE) Encryption

Apache Spark Encryption

Informix Encryption

Filesystem Encryption

Hardware Encryption Modules

Network Traffic Encryption

## 19. Performance Testing (Encrypted vs. Non-Encrypted )

Performance Testing Expectations

## 20. Relational Databases

IBM DB2

Microsoft SQL Server

MySQL

Oracle

PostgreSQL

Database Migration

Reporting

High Availability

Database Replication

## 21. Migration Strategies

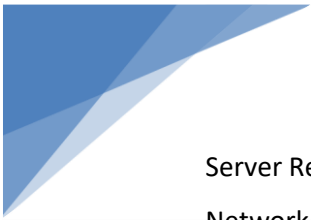
NoSQL Databases

Containers

Kubernetes (Google platform)

Docker

Vendor Support



Server Replication

Network Infrastructure

Wireless Networks

Wired Networks

Operating Systems

Hardware / Server

Password Complexity

Platform Change

IPMI Vulnerability

Virtualization

Oracle Virtualization

IBM Virtualization

Hewlett Packard (HP) Virtualization

Microsoft Server Virtualization

Intel Virtualization Technology (Intel VT)

AMD-V (Advanced Micro Devices Virtualization)

X86 Virtualization Products

Migration to the CLOUD

22. Vulnerability Assessment

23. Machine Learning

24. Orderly Shutdown