Database Defense Mastery: Securing Your Most Valuable Assets

Duration: *2 Day(s)*

Course Overview

In today's environment, databases are prime targets. With threats from cybercriminals and data breaches on the rise, mastering database security is crucial. Our course delves into the most prevalent vulnerabilities and teaches the techniques needed to both attack and defend them, focusing on practical, actionable responses. Participants will gain the expertise required to secure their databases against real-world threats and design layered defenses tailored to their organization's needs.

Review this course online at https://www.alta3.com/courses/A3-8700

Objectives

- Identify and mitigate database vulnerabilities.
- Implement robust security strategies and controls.
- Analyze and reinforce authentication processes.
- Utilize encryption for data protection.

Who Should Attend

- Database administrators (DBAs)
- System administrators
- Software developers
- Enterprise IT professionals

Prerequisites

- 6-12 months database experience

Course Outline

Foundations of Securing Databases

1. Cybersecurity Language and Trends
2. SolarWinds Case Study
3. Human Factors in Security
4. Understanding Breach Reports
5. Security Analysis First Principles

Techniques for Database Discovery

6. Identifying Databases and Infrastructures
7. Scanning for Database Vulnerabilities

8. Application Security Testing

Core Information Security Principles

9. Security Across the Lifecycle
10. Defense-in-Depth Strategies
11. Managing Trust and Application States
12. Verkada Incident Analysis

Addressing Security Vulnerabilities

13. Data Protection Techniques
14. Managing Privileges and Boundaries
15. Ensuring Service Continuity and Recovery

Common Database Vulnerabilities

16. Input Validation and SQL Injection
17. Authentication Data Protection
18. System Hardening and Best Practices
19. Risks of Internet and Cloud Resources

Building a Secure Database Environment

20. Design, Configuration, and Auditing
21. Managing Access and Identifications

Advancing Database Security Practices

22. Identifying and Addressing Common Exposures
23. Training for Project Teams and IT

Incorporating Secure Development Lifecycle (SDL)

24. Understanding Offensive and Defensive Phases
25. Implementing Secure Development Processes

Taking Immediate Security Actions

26. Analyzing and Classifying Database Assets
27. Practical Application Security Strategies

Bonus: Introduction to Cryptography

28. Implementing Strong Encryption Practices
29. Key Management and NIST Standards