Mastering Data Security for Developers

20 – 24 June 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Mastering Data Security for Developers

Ref: 36333_96057 **Date:** 20 – 24 June 2027 **Location:** Nairobi **Fees:** 4500 Euro

Course Overview:

The course is a complete course that equips developers with the essential knowledge and skills to safeguard data in today's digital landscape. The course covers data security best practices, information security risk management, threat management techniques, privacy breach prevention, and regulatory compliance. It provides hands-on training to address malware threats, phishing attacks, and incident response, preparing participants to manage data security with a strategic, multi-layered approach.

Target Audience:

- Software Developers
- Security Engineers
- IT Managers
- Systems Administrators
- Network Security Analysts
- Cybersecurity Specialists

Targeted Organizational Departments:

- IT and Cybersecurity
- Risk Management
- Legal and Compliance
- Software Development
- Network Infrastructure

Targeted Industries:

- Financial Services
- Healthcare
- Telecommunications
- E-commerce
- Government

Course Offerings:

By the end of this course, participants will be able to:

- Implement data security best practices in development workflows
- Understand and apply integrated threat management and security management systems
- Develop risk management strategies tailored for information security
- Apply access control techniques and manage authentication tokens
- Protect enterprises using quasi-intelligence resources and prioritize security programs
- Address malware threats, such as rootkits, and apply cryptography for large-scale deployments
- Design and maintain secure architectures for both physical and digital environments
- Develop strategies for compliance with information law and manage enterprise incident response

Training Methodology:

The course uses an interactive approach to maximize learning. It includes real-world case studies, simulations, and role-playing exercises to simulate privacy breach prevention and incident response scenarios. Participants will engage with concepts such as cryptography, access control techniques, and compliance management. The course emphasizes problem-solving and explores the use of quasi-intelligence resources to protect organizations against modern threats.

Course Toolbox:

- ebooks
- Access to online resources focused on information security risk management and cryptography
- Case studies on quasi-intelligence resources and incident response management
- Templates for risk diagnosis and treatment in IT security
- Checklists for implementing access control techniques and physical security measures

Course Agenda:

Day 1: Information Security and Risk Management

- **Topic 1:** Integrated Threat Management GEORGE G. McBRIDE
- **Topic 2:** Understanding Information Security Management Systems TOM CARLSON
- **Topic 3:** Planning for a Privacy Breach REBECCA HEROLD
- **Topic 4:** Using Quasi-Intelligence Resources to Protect the Enterprise CRAIG A. SCHILLER
- **Topic 5:** Information Risk Management: A Process Approach to Risk Diagnosis and Treatment NICK HALVORSON
- **Topic 6:** Department-Level Transformation R. SCOTT McCOY
- **Reflection & Review:** Discussion on key takeaways from the day's focus on risk management, privacy breaches, and organizational security transformations.

AGILE LEADERS
Training Center

Day 2: Access Control and Methods of Attack

- **Topic 1:** Authentication Tokens PAUL A. HENRY
- **Topic 2:** Authentication and the Role of Tokens JEFF DAVIS
- **Topic 3:** Accountability in Access Control Administration DEAN R. BUSHMILLER
- **Topic 4:** Rootkits: The Ultimate Malware Threat E. EUGENE SCHULTZ & EDWARD RAY
- **Topic 5:** Setting Priorities in Your Security Program DEREK SCHATZ
- **Topic 6:** Why and How Assessment of Organization Culture Shapes Security Strategies DON SARACCO
- **Reflection & Review:** Reflect on key concepts of access control, malware threats, and how organizational culture impacts security strategies.

Day 3: Cryptography, Physical Security, and Network Security

- **Topic 1:** Encryption Key Management in Large-Scale Network Deployments FRANJO MAJSTOR & GUY VANCOLLIE
- **Topic 2:** Mantraps and Turnstiles: Elements of Physical Security R. SCOTT McCOY
- **Topic 3:** Service-Oriented Architecture and Web Services Security GLENN J. CATER
- **Topic 4:** Analysis of Covert Channels RALPH SPENCER POORE
- **Topic 5:** ISO Standards for Data Security SCOTT ERKONEN
- **Topic 6:** Security Frameworks: Concepts and Application ROBERT M. SLADE
- **Reflection & Review:** Discussion on how cryptography, physical security, and architecture frameworks combine to protect data in enterprise environments.

Day 4: Telecommunications, Network Security, and Application Security

- **Topic 1:** Facsimile Security BEN ROTHKE
- **Topic 2:** Network Content Filtering and Leak Prevention GEORGE J. JAHCHAN
- **Topic 3:** The Ocean Is Full of Phish: Network Attacks and Countermeasures TODD FITZGERALD
- **Topic 4:** Neural Networks and Information Assurance Uses SEAN M. PRICE
- **Topic 5:** Information Technology Infrastructure Library ITIL and Security Management Overview DAVID McPHEE
- **Topic 6:** Adaptation: A Concept for Next-Generation Security Application Development ROBBY S. FUSSELL
- **Reflection & Review:** Recap of network security threats, phishing attacks, and advancements in application security development.

AGILE LEADERS
Training Center

Day 5: Legal, Regulatory Compliance, and Incident Response

- **Topic 1:** Compliance Assurance: Taming the Beast TODD FITZGERALD
- **Topic 2:** Enterprise Incident Response and Digital Evidence Management MARCUS K. ROGERS
- **Topic 3:** Security Information Management Myths and Facts SASAN HAMIDI
- **Topic 4:** Quantum Computing: Implications for Security ROBERT M. SLADE
- **Topic 5:** Enterprise-Level Security Strategy for Future-Proofing SAMANTHA THOMAS
- **Topic 6:** A Look Ahead: Emerging Threats and Future Challenges in Data Security SAMANTHA THOMAS
- **Reflection & Review:** Final reflection on the importance of regulatory compliance, incident handling, and preparing for future security challenges.

How This Course is Different from Other Data Security Courses:

This course sets itself apart with a hands-on approach, integrating theoretical and applied knowledge in data security. It covers cryptography, access control, incident response, and compliance in information law. The course also addresses emerging trends such as quantum computing and neural networks. Focusing on advanced security architectures, it offers cutting-edge strategies and a dynamic learning experience through real-world case studies and simulations.