BLACKBIRD FOR TRAINING

Internet of Things (IoT) Security and Management

20 – 24 December 2026
Cairo (Egypt)



Internet of Things (IoT) Security and Management

Ref: 3255298_204701 **Date:** 20 – 24 December 2026 **Location:** Cairo (Egypt) **Fees:** 4900 GBP

Introduction

The rapid expansion of the Internet of Things IoT has transformed how businesses, industries, and governments operate. Billions of connected devices now exchange data seamlessly, enabling automation, real-time insights, and improved decision-making.

However, this interconnected ecosystem also introduces significant security and management challenges, as every connected device represents a potential entry point for cyber threats.

The IoT Security and Management course provides a comprehensive framework for understanding, protecting, and managing IoT systems efficiently.

Participants will explore the key concepts of IoT architecture, common vulnerabilities, risk mitigation strategies, and governance practices essential for securing connected environments.

Course Objectives

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

- Understand the core architecture and components of IoT ecosystems.
- Identify key security challenges related to connected devices and data flow.
- Apply best practices in IoT network protection and risk management.
- Implement encryption, authentication, and access control mechanisms.
- Manage the lifecycle of IoT devices, including configuration, monitoring, and updates.
- Analyze and respond to IoT-related cyber incidents.
- Design governance frameworks and compliance strategies for IoT systems.
- Integrate IoT security principles with enterprise-level IT and operational systems.

Course Outlines

Day 1: Introduction to IoT Architecture and Ecosystems

- Overview of IoT technologies and their industrial applications.
- Understanding IoT architecture layers devices, connectivity, cloud, analytics.
- Communication protocols: MQTT, CoAP, HTTP, and others.
- Edge computing and distributed data processing.
- Interaction between IoT devices, data, and control systems.
- Hands-on exercise: mapping data flow in a connected IoT network.



Day 2: IoT Threats and Vulnerability Management

- Common security risks in IoT systems.
- Attack vectors targeting devices, sensors, and gateways.
- Case studies on IoT breaches and lessons learned.
- Fundamentals of preventive security and threat detection.
- Developing multi-layered IoT defense strategies.
- Practical session: simulating an IoT attack and analyzing vulnerabilities.

Day 3: Identity, Authentication, and Access Control

- Role of identity management in IoT ecosystems.
- Implementing authentication and device verification mechanisms.
- Encryption techniques and key management.
- Designing secure access control policies for users and devices.
- Data privacy and compliance considerations.
- Hands-on exercise: building a secure authentication system for IoT devices.

Day 4: IoT Governance and Policy Enforcement

- Establishing governance frameworks for IoT environments.
- Setting up compliance and regulatory standards.
- Centralized monitoring and device management systems.
- Risk analysis and business continuity planning.
- Key performance indicators for IoT security and management.
- Workshop: designing a governance dashboard for IoT systems.

Day 5: Incident Response and Continuous Improvement

- Developing effective incident response plans for IoT security breaches.
- Analyzing attack patterns and collecting digital evidence.
- Recovery and remediation planning after security incidents.
- Implementing continuous monitoring and improvement practices.
- Leveraging AI and analytics for predictive threat detection.
- Final simulation: end-to-end IoT incident management exercise.



Why Attend this Course: Wins & Losses!

- Gain in-depth knowledge of IoT architecture, risks, and security controls.
- Acquire hands-on experience in identifying and mitigating IoT vulnerabilities.
- Learn how to design and enforce governance frameworks for connected environments.
- Improve operational resilience through better device lifecycle management.
- Develop practical skills in encryption, authentication, and threat analysis.
- Understand how to integrate IoT security with enterprise IT infrastructure.
- Stay updated with emerging IoT standards and technologies.
- Strengthen your organization's overall cybersecurity posture.

Conclusion

As organizations increasingly adopt connected technologies, IoT Security and Management becomes a strategic necessity, not just a technical priority.

This course provides the knowledge and practical tools needed to protect and manage IoT systems effectively, ensuring both operational efficiency and data integrity.

Participants will walk away with a solid understanding of how to build resilient, secure IoT ecosystems that can withstand evolving threats while enabling innovation and growth.

In a world driven by connectivity, mastering IoT security and management is a vital step toward ensuring sustainable digital transformation.

