Mobile Device Security and Enterprise Mobility Management Training Course



19 - 23 Oct 2026

Boston

7500 € (Per Person)

Ref: #CYB4163_89302

Course Introduction / Overview:

In today's hyper-connected business environment, mobile devices are no longer peripheral but central to corporate productivity and data access. This paradigm shift introduces significant security vulnerabilities, making a robust mobile security strategy non-negotiable for any modern enterprise. This comprehensive training course is meticulously designed to transform participants into proficient architects of secure mobile ecosystems. We will journey from the foundational principles of Mobile Device Management (MDM) to the sophisticated frameworks of Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM). The curriculum delves into the intricate mobile threat landscape, exploring real-world attack vectors and defensive strategies. Drawing on insights from experts like Dr. Kevin Curran, a leading academic in cybersecurity, we will dissect the core components of a successful mobility program. The course also references key concepts discussed in seminal texts such as "Enterprise Mobility Management: Everything You Need to Know About MDM, MAM, and BYOD," providing a solid theoretical and practical grounding. At BIG BEN Training Center, we are committed to equipping professionals with the skills to design, implement, and manage secure, flexible, and compliant mobility solutions that protect corporate assets while empowering the workforce.

Target Audience / This training course is suitable for:

- IT Security Managers and Administrators.
- Network and Systems Engineers.
- Cybersecurity Analysts and Consultants.
- IT Directors and Chief Information Security Officers (CISOs).
- Compliance and Risk Management Officers.
- Mobile Application Developers with a focus on security.
- IT Operations and Help Desk Team Leads.
- Anyone responsible for implementing or managing a mobile device policy.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Government and Public Sector Agencies.
- Telecommunications and Technology.
- Retail and E-commerce.
- Legal and Professional Services.
- Education and Research Institutions.
- Energy and Utilities.

Target Organizations Departments:

- Information Technology (IT) and Information Security (InfoSec).
- Cybersecurity Operations Center (CSOC).
- Risk Management and Compliance.
- Legal and Human Resources (HR).
- Internal Audit and Governance.
- Software Development and Engineering.
- Operations and Field Services.
- Procurement and Asset Management.

Course Offerings:

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

- Develop a comprehensive enterprise mobility security strategy.
- Differentiate between MDM, EMM, and UEM solutions and select the appropriate one.
- Create and enforce effective Bring Your Own Device (BYOD) and Corporate-Owned policies.
- Secure both iOS and Android platforms using native controls and third-party tools.
- Implement robust mobile application management (MAM) and mobile content management (MCM) policies.
- Deploy advanced mobile threat defense (MTD) mechanisms to counter malware and phishing.
- Integrate mobile devices into an existing Identity and Access Management (IAM) framework.

- Configure secure mobile connectivity using VPNs and containerization technologies.
- Conduct mobile security risk assessments and audits.
- Develop and execute a mobile security incident response plan.
- Ensure compliance with regulations like GDPR and HIPAA in a mobile context.
- Manage the complete lifecycle of mobile devices from provisioning to decommissioning.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants not only learn the theory but can also apply it effectively in their professional roles. This course employs a blended learning approach that combines expert-led presentations with hands-on (simulated) lab exercises, allowing participants to configure policies and respond to security scenarios in a controlled environment. A significant portion of the training is dedicated to analyzing real-world case studies of mobile security breaches, deconstructing the attack chain and evaluating the response. Participants will engage in collaborative group workshops to design mobile security policies for hypothetical organizations, fostering teamwork and critical thinking. Interactive Q&A sessions, peer-to-peer knowledge sharing, and facilitated discussions are integrated throughout the five days to address specific challenges and contexts. Our instructors provide continuous feedback and guidance, ensuring a deep understanding of complex topics like mobile threat defense and Zero Trust architecture. The focus is on building practical, transferable skills that provide immediate value to the participant's organization, moving beyond vendor-specific training to instill universal best practices in mobile security and management.

Course Agenda (Course Units):

Unit One: Foundations of Enterprise Mobility and Security

- The Evolution from MDM to EMM and UEM.
- Understanding the Modern Mobile Threat Landscape.
- Key Components of a Mobility Strategy: MDM, MAM, and MCM.
- Assessing Mobile Security Risks and Vulnerabilities.
- Introduction to Mobile Operating System Architectures (iOS and Android).
- The Business Case for a Robust Mobile Security Program.
- Legal, Privacy, and Compliance Considerations in Mobility.

Unit Two: Developing Mobile Security Policies and Strategies

- Crafting an Effective Mobile Security Policy.
- Comparing Device Ownership Models: BYOD, COPE, CYOD, and COBO.
- Establishing Acceptable Use Policies (AUP) for Mobile Devices.
- Defining Data Classification and Handling Standards for Mobile.
- Integrating Mobile Policy with Overall Corporate Security Governance.
- User Enrollment and Onboarding Strategies.
- Communicating Security Policies to End-Users Effectively.

Unit Three: Securing and Managing Mobile Platforms

- Deep Dive into iOS Security Architecture and Management Features.
- Deep Dive into Android Enterprise Security and Management Frameworks.
- Mobile Device Hardening and Configuration Best Practices.
- Implementing Secure Containerization for Corporate Data.
- Managing Corporate App Stores and Application Vetting.
- Application Whitelisting, Blacklisting, and Required Apps.
- Patch Management and Over-the-Air (OTA) Update Strategies.

Unit Four: Advanced Mobile Security Controls and Technologies

- Implementing Mobile Threat Defense (MTD) Solutions.
- Mobile Identity and Access Management (IAM) and Single Sign-On (SSO).
- Multi-Factor Authentication (MFA) for Mobile Access.
- Securing Data-in-Transit with Mobile VPN and Per-App VPN.
- Implementing Data Loss Prevention (DLP) on Mobile Endpoints.
- Principles of Zero Trust Architecture for Mobile Security.
- Geofencing, Geolocation, and Context-Aware Security Policies.

Unit Five: Mobile Security Operations and Incident Response

- The Mobile Device Lifecycle: Provisioning, Management, and Decommissioning.
- Monitoring, Logging, and Auditing Mobile Device Activity.
- Developing a Mobile Security Incident Response Plan.
- Responding to Common Incidents: Lost/Stolen Devices, Malware, and Data Leakage.
- Mobile Device Forensics and Evidence Collection.
- Generating Reports for Compliance and Management Review.
- Future Trends in Mobile and Endpoint Security.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As the lines between personal and corporate devices continue to blur, how can an organization balance robust security enforcement with employee privacy and user experience, and what role does a Zero Trust architecture play in this new paradigm?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic, strategy-first approach to mobile security, moving beyond the technical specifics of any single EMM vendor. While many courses focus narrowly on tool configuration, our curriculum emphasizes the foundational pillars of policy development, risk management, and legal compliance, ensuring participants can build a sustainable and defensible mobility program from the ground up. We dedicate significant time to the strategic comparison of ownership models like BYOD and COPE, enabling leaders to make informed decisions that align with their organization's culture and risk appetite. The content is uniquely structured to bridge the gap between high-level governance and on-the-ground technical implementation, covering both iOS and Android Enterprise with equal depth. Furthermore, the course integrates advanced, forward-looking concepts such as Mobile Threat Defense (MTD) and the application of Zero Trust principles to mobile endpoints, preparing participants for the next generation of security challenges. By focusing on transferable skills and critical thinking through real-world case studies and policy-building workshops, this training equips professionals not just to manage devices, but to lead their organization's entire enterprise mobility security posture with confidence and foresight.