

IBM Consulting



G-Cloud 15 IBM – IBM Mobile Security and Privacy Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

Contents

Service Overview.....	3
Addressing Business Needs	4
Service Definition	5
IBM Approach	6
Mobile Security for a Mobile World.....	8

IBM Mobile Security and Privacy

Service Overview

Features

- Provides a focused security and privacy assessment on a single mobile app or your entire mobile application portfolio.
- Physical Penetration testing on both mobile application and supporting back end services.
- Mobile Security assessment with a summary and clear recommendations.
- The assessment can also cover physical security of the device, IT control policies, device management, application distribution and best practices for applications stored on the device.

Benefits

- Secure DevOps architecture strengthened by automated scanning and AI-assisted remediation guidance
- Defined and proven Mobile Security Test Methodology.
- Clear guidance based on mobile application assessment.
- Security accredited professionals.

Key Differentiators

- End-to-end Software development lifecycle expertise
- Deep knowledge of public sector organizations
- Key strengths in the full breadth of architecture areas including delivery architecture, application architecture, security architecture and integration architecture
- Core value in the blending of COTS, bespoke software solutions, and AI-enhanced automation

IBM Mobile Security and Privacy

Addressing Business Needs

A larger remote population does not have to mean a greater security or privacy risk to your business.

1 in 4 mobile apps contain a high-risk security flaw

35% of data transmitted by mobile devices is unencrypted



Mobile services are facing increasing strain as a result of the demand for greater remote working. Security and privacy for mobile applications do not always follow the same enterprise standards introducing unseen risks and vulnerabilities that could be exploited with devastating effects. It is estimated that 1 in 4 mobile apps have some form of security vulnerability, and 35% of data through mobile apps is transmitted un-encrypted. This service proactively assesses and identifies vulnerabilities before they present an issue and then solves that issue as part of a services engagement.

This service is broken down into three stages dependant on need and identified issues / risk:

Initial Stage – This engagement provides an automated security assessment of your mobile app, identifying concerns with code, data at rest and in transit issues, core functional issues etc, which are then clearly reported back in a security assessment. AI-assisted reporting for clarity and prioritisation.

Secondary Stage – This engagement includes a full application penetration test and engagement with the IBM IX Mobile & XR teams to implement any fixes found during the initial security assessment and penetration test.

Tertiary Stage – This engagement follows on from previous stages and encompasses all your mobile apps both publically available and enterprise apps and provides a full security advisory with ongoing assistance to improve security and privacy best practice.

IBM Mobile Security and Privacy

Service Definition

We will perform an assessment of the practices, technologies, and infrastructure to holistically support and enforce security from front-end client through to mobile backend.

Activity: Security Assessment

Mobile Security is more than just proper coding practices or the right version of Encryption. Part of an applications security falls under device security. How do we protect an application from the user's device? What do we do with corporate data if a device is lost or stolen? This assessment looks at several dynamics around physical security, IT Control Policies for the device, device management, application distribution, and best practices for applications stored on the device.

Front-End Security testing areas:

- Data at rest and motion analysis.
- Application cache analysis
- Hardcoded credential and key analysis
- Obfuscation, repackaging application
- Anti-tampering
- Insecure API and crypto analysis

Back-End Security testing areas:

- REST API Authentication and Token design checking
- Horizontal/Vertical privilege escalation attack
- Parameter manipulation attack.
- Session Hijacking.
- Security http header checking for ex:- X- Content-Type-Options: , X-Frame-Options:
- Back-end vulnerability management

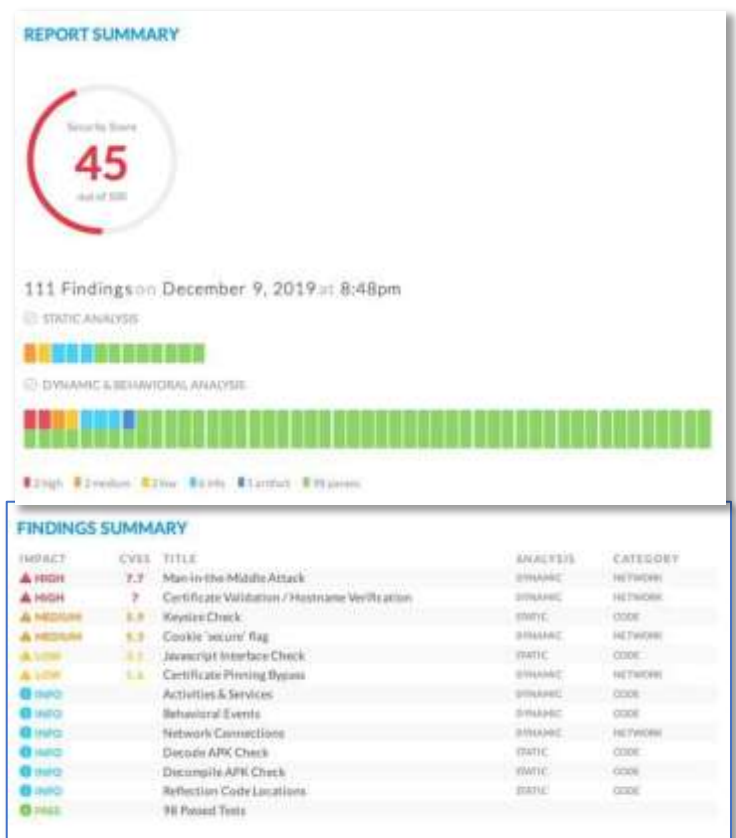


Figure 1.1: Initial App Stage Sample Report output

IBM Mobile Security and Privacy

IBM Approach

We bring the benefit to you of having worked with the world's largest organisations, transforming complex, critical services. Our approach is based on robust methods, processes, and personalised engagement.

Any application found to have a security issue that requires development in order to rectify the issue can be dealt with in the secondary stage via the IBM Mobile Garage.

We bring the benefit to you of having worked with the world's largest organisations, transforming complex, critical services. Our approach is based on robust methods, processes, and personalised engagement.

We focus on your business needs and developing trusted long-term relationships, underpinned by industry-leading experience and capabilities. We want you to get the best out of every engagement and to deliver outcomes that matter for your organisation.

Our approach is tailored to your needs and flexible to support all delivery models. We offer established programme and portfolio capabilities that can be aligned with your internal governance and methods, linking to industry recognised standards such as PRINCE2 and PMI.



We bring specific skills and attitudes including:

Proven delivery track record working in complex environments

- Access to specialists who understand the lessons and risks for transformation
- Being able to advise, support and transfer knowledge with your teams
- Implementing strong governance, defined collaboratively within the context of robust methods and processes
- Bringing an integrated and controlled planning approach



- Proactive identification and management of risks and issues based on experience
- Working across complex existing and new platforms
- Experience with the latest technologies, tools and delivery methods

We work to manage the complexity of key business projects, programmes and portfolios, communicating with clarity and helping you make informed decisions.

IBM Mobile Security and Privacy

Mobile Security for a Mobile World

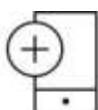
Today's workplace is anywhere. CIOs and CISOs and their teams need a secure mobile workforce, and enterprise mobile security solutions that enable flexible delivery of apps, content and resources across devices. Whether supporting bring-your-own-device (BYOD), choose-your-own- device (CYOD) or a corporate-liable environment, they need strategic options for mobile security threats and prevention, such as risk insights and behavioral analysis, security policy and containerization of mission-critical resources.

Benefits



Perform real-time AI-driven risk assessments

With Watson®, IBM Security™ MaaS360® Advisor delivers insights into the risks that may impact your enrolled devices and users. MaaS360 User Risk Management takes these insights one step further by developing a continuously updated risk score for each enrolled user.



Protect critical apps and data with container policy

Containment has been a cornerstone of mobile security since the early days of mobile device management (MDM), and is still going strong today to achieve a balance between user productivity and corporate data protection. Whether it is used for data loss prevention (DLP) or setting up authentication for an enterprise application, MaaS360 has the right container app for the job.



Take direct action with mobile threat defense

IBM Security™ MaaS360 Mobile Threat Management (MTM) can detect and remediate malware born from suspicious apps before they cause a headache. Through partnership with mobile threat defense (MTD) provider Wandera, these capabilities are deepened by defending against phishing, man-in-the-middle, cryptojacking and other device, network, app and content-based threats.



Mobile device management (MOM)

The basis of any UEM deployment is MDM. While UEM solutions deliver a rich set of security and productivity tools for any device, none of those matter if devices themselves are not enrolled and managed at a basic level. MDM solutions provide the API-based policy, same-day support for all popular operating systems, compliance rules, and app distribution that make up the backbone of any MOM platform.

Enterprise mobility management (EMM)

EMM solutions represent an evolution from MDM, a midway point to full UEM with a focus on the user experience and data security. Within MaaS360, EMM features include the secure container - an encrypted sandbox installed on user devices equipped with workplace applications-as well as identity tools and mobile app management (MAM) policies for corporate apps.

Bring your own device (BYOD)

BYOD is a corporate policy that empowers employees to be more mobile - to make their world their office. Put simply, BYOD encourages use of personal devices (smartphones, tablets, laptops and wearables) to access enterprise data from anywhere. From native containers to developer features such as User Enrollment and Android Enterprise, MaaS360 supports all flavors of BYOD deployment.

Unified endpoint management (UEM)

UEM offers a simplified and consolidated device management approach. It is a culmination of the device policy available in MOM and the data security and identity features provided through EMM deployment. UEM adds to those capabilities, layering threat defense, AI analytics and the management of any device - whether smartphone, tablet, laptop, desktop or IoT, using any of the most commonly used mobile operating systems.

Secure mobile app development

Build smarter mobile services and applications using IBM Cloud. Quickly architect, prototype and bring apps to market. Generative AI assistance for code analysis and test creation.

