Does your job include:

Managing Mobile Device Deployment?

Developing Enterprise Applications?

Researching or Writing Mobile Policy?

Conducting Mobile Device User Training?

Certified Mobile Device Security Professional™

- Applications
- Connectivity
- Device File Structure
- Enterprise Integration
- Vulnerabilities
- Penetration Testing

We are committed to making mobile computing more secure. Smartphones and tablets are increasingly becoming the means for the population to handle critical personal as well as business information and data. The Certified Mobile Security Device Professional (CMDSP) certification promotes knowledge of mobile devices and the environments they work within. A CMDSP certification shows that the holder is knowledgeable with the operating environments of mobile devices, and how those environments affect security.

The CMDSP certification shows employers that the individual can manage the mobile devices for a workforce within an enterprise in a secure manner, keeping institutional data, information, and knowledge secure even while the devices are mobile.

www.cmdsp.org info@cmdsp.org 240.233.4303

5523 Research Park Drive, Suite 325, Catonsville MD 21228

Applications

The Applications domain covers the steps required to take an application from concept to market, including aspects of application design, development and deployment. This topic area focuses on the following:

- Development of applications – the differences/similarities between Software Development Kits (SDK), which kits are appropriate for which operating system
- Review of applications – Services, processes
- Data access/permissions – Sandboxing
- Publishing requirements – Device requirements, certificate requirements
- Using simulators/emulator (what can/can't they do)
- Secure coding practices

Enterprise Integration

Some companies issue employees a company phone, and some have a "bring your own device" (BYOD) policy. Regardless of the source of the device, management of those devices within the enterprise is important. This section requires knowledge of how to securely manage the devices within the enterprise. This topic area focuses on the following:

- BYOD policies including Acceptable Use Policies, and technical and legal issues.
- Mixed networks – How to manage/secure multiple mobile operating systems within a network.
- Management Schemes
- Mobile vs. in-house management policies
- Personal versus enterprise/professional apps

Connectivity

The Connectivity domain covers the ways that mobile devices communicate with other mobile devices, computers, and the wider internet. This topic area also covers data connections with cloud environments, such as iCloud and Google's cloud. This topic area includes:

- Cellular/Wifi
- Computer-Device Connection
- Cloud connection (iCloud, Google)
- Bluetooth
- Network tools
- Denial of access
- Secure remote access solutions: Architecture and operations for mobile environments

Vulnerabilities

This topic area is a "red team" focused area, where the candidate is expected to know what types of vulnerabilities exist within the mobile device. These vulnerabilities could be within the operating system, an application, file structure, or within the user base (e.g. social engineering). This topic area looks at specific known vulnerable areas, and where future exploits could be located. This topic area focuses on the following:

- Operating System
- Application
- Users
- Computer based connections
- Cloud based connections

Device File Structures

Understanding how the devices store and retrieve data from within their own device, and on associated software (e.g.: iTunes). This topic area also covers where and how backups are managed, and the tools required to manage these files. This topic area includes:

- Database types and locations
- Database and XML schemas
- XML usage on device
- Access
- Backup
- Tools

Penetration Testing

This topic area is an extension of the Vulnerability topic area. Candidates should have an understanding of the tools used to find, exploit, and mitigate vulnerabilities.

- Tools
- Usage (targets, situations when to use)
- Targets

CMDSP™

www.cmdsp.org info@cmdsp.org 240.233.4303

5523 Research Park Drive, Suite 325, Catonsville MD 21228