Level 3, Unit 1 – Fundamentals of Mobile Device Security (5 credits)

1. Understand the mobile environment and tooling for security	2. Understand common mobile security threats	3. Using the OWASP Top 10 to secure your systems	4. Navigating the threat landscape for mobile
1.1 I can understand the security differences between mobile and desktop operating systems	**2.1** explain threats that effect mobile device security	**3.1** I can explain the importance of OWASP	**4.1** I can understand what is meant by SSL pinning
1.2 I can configure Linux virtual machines to prepare for a security testing environment	**2.2** explain threats that impact connected apps on mobile devices	**3.2** I can describe how to protect against the threats highlighted in the OWASP Top 10	**4.2** I can understand the importance of using secure protocols like HTTPS
1.3 I can install testing tools	**2.3** I can understand software distribution methods for mobile platforms	**3.3** I can perform a vulnerability analysis using the OWASP Top 10 on a mobile app	**4.3** I can perform traffic monitoring
1.4 I can describe sandboxing and its importance in mobile security	**2.4** I can understand injection attacks		**4.4** I can assess the impact severity level of potential threats
1.5 I can evaluate the impact of jailbreaking mobile devices.	**2.5** I can understand the high security risk of mobile devices being compromised		**4.5** I can describe how to prevent man in the middle attacks

Level 3, Unit 2 – Securing Mobile Operating Systems and Instrumentation (4 credits)

1. Understanding the principles of mobile development environments	2. Understanding how iOS handles security	3. Understanding how Android handles security	4. Instrumentation and Analysis
1.1 I can demonstrate how to setup and configure a mobile app for either iOS or Android	**2.1** I can describe how iOS handles security at an operating system level	**3.1** I can describe how Android handles security at an operating system level	**4.1** I can use Frida for iOS and Android to perform testing
1.2 I can explain the importance of Code Signing and its role in security	**2.2** I can explain the mechanisms used by Apple to enforce security	**3.2** I can explain the mechanisms used by Google to enforce security	**4.2 2** I can use Burp Suite to act as an intervention proxy
1.3 I can explain the threats posed by side loading apps and how the App Store and Google Play Store seek to avoid it for consumers	**2.3** I can explain hardware functions used by iOS for security including Secure Enclave and FaceID/TouchID	**3.3**: I can explain how Android scales across different manufacturers to allow hardware security	**4.3** I can perform a security analysis on a connected mobile application
1.4 I can use the debugging tools in Xcode or Android Studio to troubleshoot potential security issues	**2.4** I can understand the iOS runtime environment	**3.4** I can understand the Android runtime environment	**4.4** I can document the results of a vulnerability analysis
1.5 explore architecture of a modern mobile app	**2.5** I can perform a test on an iOS app	**3.5** I can perform a test on an Android app	**4.5** I can apply the OWASP principles to a vulnerability test