

如何應用『行動應用 APP安全開發指引』

趨勢科技股份有限公司

技術經理：莊卓浩

指引使用建議表

表1 指引使用建議表

章節 角色	SSDLC	Ch. 1	Ch. 2	Ch.3				Ch. 4	Ch. 5	Ch.6
				3.1	3.2	3.3	3.4			
PM	全程	V	V	V	V	V	V	V		V
SA	需求	V	V	V	V	V	V			V
SD	設計	V	V	V	V	V	V	V	V	V
Android PG	開發實作	V	V	V	V		V	V		V
iOS PG	開發實作	V	V	V		V	V	V		V
TEST/QA	測試	V		V	V	V		V	V	V
MIS	部署維運	V					V	V		V
IS	全程	V	V	V	V	V	V	V	V	V

資料來源：本計畫整理

P.14

RD / QA 重點章節

- Junior App Developer / QA
 - Ch2: 行動應用 App 安全開發基本概論
 - Ch3: 行動應用 App 安全開發最佳實務
 - Ch4: 行動應用 App 安全開發生命週期 (SSDLC)
 - Ch5: 行動應用 App 資安檢測實務
- Senior App Developer / QA
 - Ch3: 行動應用 App 安全開發最佳實務
 - Ch4: 行動應用 App 安全開發生命週期 (SSDLC)
 - Ch5: 行動應用 App 資安檢測實務
- Staff App Developer / QA
 - Ch3: 行動應用 App 安全開發最佳實務
 - Ch5: 行動應用 App 資安檢測實務



核心章節!

安全分類

- 第一類
 - 定義：純功能性
 - 安全等級：初級
- 第二類
 - 定義：具認證功能與連網行為
 - 安全等級：中級
- 第三類
 - 具交易功能(包括認證功能及連網行為)
 - 安全等級：高級

依安全分類參考開發實務準則

- 開發實務準則（CH3）為本指引之核心，所有App 開發應以本章節為基礎
- 本章節條文眾多，但可以安全分類來擇定需參考之準則
- 依安全分類可於表15 – 17中對照出應遵循之準則

依安全分類參考資安檢測實務

- 資安檢測實務（CH4）亦為本指引之核心，所有App 檢測應以本章節為基礎
- 本章節條文眾多，但可以安全分類來擇定檢測基準
- 依安全分類可於表 12 及表 18中對照出應遵循之準則



Thank You !