第8章

弱點評估與管理

威脅弱點

零時差攻擊

惡意程式種類

電腦病毒種類/躲避監視種類

早期電腦病毒

惡意程式的種類

混和攻擊

攻擊工具(特權提升)

網際攻擊狙殺鏈

資訊安全防禦機制

惡意程式事件處理程序

加密勒索軟體攻擊

加密勒索攻擊

勒索軟體感染方式

勒索軟體及服務

感染勒索後的應變措施

駭客攻防

分類

階段過程

隊伍介紹

資訊安全備份管理

生命週期

備援及層次應用

備份策略

備份計畫內容

資料區分

方式與媒體

位置模式

差異比較

平率與保留週期

工具

備份回復測試

日誌管理

資訊安全監控維運中心

主要功能

八大習慣

事件管理

異常行為

資訊安全監控中心主要功能