CSA(Certified SOC Analyst)安全運營中心分析師認證課程 課程大綱			
序號	**課程大綱**	**課程內容摘要**	**課時**
1	安全運營與管理	• 企業的安全管理及安全管理中涉及的安全活動 • 安全運營的不同方面及其基本概念 • 實施安全運營的不同階段 • 安全運營實施的挑戰 • 安全運營中的關鍵績效指標（KPI）和度量 • 安全運營的最佳實踐	3
2	了解網絡威脅、入侵指標及攻擊模式	• 網絡、服務器和應用層攻擊的不同類型 • 攻擊的威脅和方法 • 不同類型攻擊的特徵（IoCs） • 駭客的通用攻擊方法	3
3	安全事故、事件及日誌記錄	• 事故、事件及日誌之間的關係 • 日誌在事件檢測中的重要性 • 日誌的主要來源及常用格式 • 日誌管理的挑戰和要求 • 本地和集中式日誌概念	6
4	如何使用安全性資訊與事件管理服務檢測事件	• 安全信息和事件管理（SIEM）及其功能 • 不同類型的 SIEM 解決方案 • SIEM 架構及其組件；SIEM 部署中的挑戰；部署 SIEM 的建議 • SIEM 開發的階段和所有 SIEM 部署中常用的例子 • 不同的 SIEM 部署架構 • 處理警報分類、分析過程及其挑戰	6
5	如何利用威脅情報增強事件檢測能力	• 威脅情報的基本概念 • 獲取威脅情報的不同來源；不同的威脅情報平台（TIP） • 威脅情報驅動 SOC 的需求 • 威脅情報如何幫助 SOC • 在 SIEM 中整合威脅情報的好處 • 用於增強事件響應的威脅情報例子	3
6	網絡安全事故管理	• 事件響應及事件響應流程中的不同階段 • SOC 和事件響應團隊（IRT）在事件響應中的運作 • 如何應對網絡安全事件 • 如何應對電子郵件安全事件 • 如何應對內部人員事件 • 如何應對惡意軟件事件	3
7	認證考試	• 學員出席率達標後可參與考試，通過考試將獲發國際資格認可證書	3
		總計	**27**