

113年公務人員高等考試三級考試試題

類 科：資通安全

科 目：資通安全防護技術

考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

一、請分別說明 SIEM、XDR 與 SOAR 三種資通安全防護機制的功能。(30 分)

二、請分別說明資通網路中 IPS 與 IDS 的功能各為何？並說明其差異性。
(20 分)

三、請條列說明零信任架構的決策引擎之功能及其所包含的組件與組件功能各為何？(25 分)

四、請分別說明弱點掃描、滲透測試、源碼檢測的主要工作；並分別條列主機弱掃常見的弱點與網頁弱掃常見的弱點。(25 分)