代號：37420
頁次：1－1

113年公務人員高等考試三級考試試題

類　　科：資訊處理
科　　目：資通網路與安全
考試時間：2小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡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。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、惡意攻擊常態化的網路資訊環境，於資安事件發生時，可快速偵測威脅並作出應變措施。

㈠何謂端點偵測與回應（Endpoint Detection and Response, EDR），及託管偵測與回應（Managed Detection and Response, MDR）機制。（10分）

㈡請分別說明EDR及MDR在偵測方面及回應方面有那些活動。（15分）

二、防火牆用以保障內部網路避免受攻擊，目前常被應用的有 WAF（Web Application Firewall）及次世代防火牆（Next-Generation Firewall, NGFW），試問：

㈠ WAF的防禦機制為何？（10分）

㈡次世代防火牆的防禦機制為何？（10分）

㈢當內容傳遞網路CDN（Content Delivery Network）與WAF架設在一起時，其效益為何？（5分）

三、隨著網路興起及資通技術發展，資安風險評估已經是機關資安管理的重要環節，機關在事前、事中及事後等三階段可導入那些資安控制措施，才能降低風險，提升資安防護水平。（25分）

四、資通安全責任等級分級辦法中，針對各資通安全責任等級之資通系統防護基準於營運持續計畫構面包含系統備份及系統備援兩項措施，請依據系統防護需求分級要求，說明：

㈠系統備份應辦事項。（15分）

㈡系統備援應辦事項。（10分）