《資通網路與安全》

試題評析	**資安！資安！資安！**很重要所以要說三遍。本份試題95%屬資訊安全範疇，故資訊安全相關法規、資安控制措施，以及風險管理需多加涉獵。

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。

(一)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）

(二)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）

試題評析	係屬資安防禦範疇。
考點命中	《高點・高上資通安全講義》第二回，頁46範例11。

答：

(一)1.端點偵測及回應(Endpoint Detection and Response, EDR)：又稱端點偵測及應變，對主機或端點提供防毒軟體的掃描功能，自動阻擋已知的風險，並即時通知資安人員處理。也提供資安事件記錄與管理平台，讓組織可以隨時查詢和了解環境中的資安事件。EDR為主動監測並記錄端點發生異常行為與可疑程式的技術，通常由組織自行部署於端點。一旦發現潛在威脅，即會阻斷異常行為與可疑程式的運作，並自動通報資安人員。

2.威脅偵測及回應(Managed Detection and Response, MDR)：又稱威脅偵測與應變、託管式偵測及回應，通常由資訊安全管理服務供應商(Managed Security Service Provider, MSSP)提供。MDR是由資安廠商提供的威脅偵測應變服務，亦即組織將資安防護委外由廠商專業資安人員協助進行網路監控、事件管理，以及即時回應及處理所遭遇的資安威脅。

(二)1.EDR偵測包含：記錄、分析文件讀寫、網路連接、Process執行等活動。一旦偵測到異常行為或威脅時，採取回應如：中斷活動、封鎖網路、隔離受感染的端點，並提示資安團隊進行進一步的調查和處理。

2.MDR則是提供整個網路環境7×24的即時安全監控，且會將監控資料集中傳送到SOC(Security Operation Center)進行審查和分析。其利用多種資安技術如：入侵偵測系統(Intrusion Detection System, IDS)、漏洞掃描等，並整合多種安全資訊來源，偵測異常行為和資安威脅。當發現資安威脅時可提供專業分析和應對建議，以迅速回應並協助組織快速恢復正常營運。

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：

(一) WAF的防禦機制為何？（10分）

(二) 次世代防火牆的防禦機制為何？（10分）

(三) 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）

試題評析	屬近年熱門之防火牆考題。
考點命中	《高點・高上資通安全講義》第二回，頁20，「WAF、NGFW」。

答：

(一)WAF主要檢視OSI應用層之流量，其部署於Web應用程式前端並過濾、監視、分析和阻斷網路雙向的OSI應用層流量，以檢測和阻止惡意內容。因此，WAF可防治利用網頁應用程式已知漏洞的攻擊。例如：SQL Injection、跨網站指令碼(Cross-Site Scripting, XSS)，以及不正確的系統組態等。

(二)有別於傳統使用網路流量規則與定義來允許或拒絕流量通過的傳統防火牆，次世代防火牆可檢查並獲取更多網路流量之特徵，故可實現進階的網路流量管理，識別及防止更多型態的網路攻擊行為。此外，次世代防火牆亦可提供如：統一威脅管理(Unified Threat Management, UTM)、內容過濾(Content Filtering)、入侵偵

測系統、入侵防禦系統(Intrusion Prevention System, IPS)等資訊安全服務。

(三)WAF可過濾惡意流量，CDN則可快速分散流量至網路的不同節點，故兩者架設在一起時，可避免遭遇大量分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)攻擊時，單台WAF過載造成服務中斷。

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）

試題評析	風險管理為近年來資安命題熱區。
考點命中	《高點・高上資通安全講義》第二回，頁69～71，「資安風險管理」。

答：

(一)事前：事前組織需全面盤點軟體、硬體、資料等資訊資產，分析面臨的內外部威脅及識別資安風險。導入的資安控制措施為事前預防及防護，技術方面如：透過源碼掃描、弱點掃描，以及滲透測試等找出組織的資安弱點，另適度導入資安防護機制如：政府組態基準(Government Configuration Baseline, GCB)、多因子認證等。此外，可透過舉辦資安教育訓練、社交工程演練、資安稽核等來提升人員的資安認知。

(二)事中：事中的資安控制措施為偵測與回應，如：建立NGFW、EDR、MDR、IDS、IPS等偵測異常行為與資安威脅的資安技術，並利用人工智慧(Artificial Intelligence, AI)、機器學習(Machine Learning)來阻擋、防範惡意攻擊。

(三)事後：事後的資安控制措施為復原與演練，復原係指以備份資料為基礎，恢復系統確保營運不中斷。演練則是以實際情境來驗證復原計畫的有效性，例如：營運持續計畫(Business Continuity Planning, BCP)。

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：

(一)系統備份應辦事項。（15分）

(二)系統備援應辦事項。（10分）

試題評析	屬於近年資訊安全稽核之熱門考題。
考點命中	《高點・高上資通安全講義》第二回，頁87～88，「四、資安法規：防護基準、稽核與檢測」。

答：

資通系統依防護需求分級可為高、中、普，其資通系統防護基準於營運持續計畫構面之系統備份、系統備援措施內容如下表所示：

表1 資通系統防護基準修正規定

構面	措施內容	高	中	普
營運持續計畫	系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
	系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。		無要求。

資料來源：行政院數位發展部（2021）