# 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

曹勝老師

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）

*1.*《考題難易》：★★★☆☆ **(最難 5 顆星)**
*2.*《解題關鍵》：**本題為資安防禦應用題，掌握偵測與回應相關技術概念始可作答。**
*3.*《命中特區》：

【擬答】：

這兩種偵測與回應機制在現代企業中都扮演著重要角色，幫助企業迅速響應和處理安全事件，保護其資訊系統和資料的安全。

㈠端點偵測與回應（Endpoint Detection and Response, EDR）以及託管偵測與回應（Managed Detection and Response, MDR）是兩種常見的資訊安全機制，用於快速偵測和應對資安威脅。以下是它們的定義和主要特點：

*1.*端點偵測與回應（EDR）

端點（Endpoint） 指的是連接至企業網路的裝置，如桌面電腦、筆記型電腦、手機等。偵測與回應（Detection and Response） 是指在端點上實施的技術，用於即時偵測並回應潛在的安全事件和威脅。EDR 特點：

⑴即時監控：持續監控端點設備的活動和事件。
⑵威脅偵測：使用行為分析、機器學習和規則引擎等技術來偵測異常行為和已知的攻擊模式。
⑶事件回應：在偵測到威脅後，迅速針對端點執行應變措施，如隔離感染的設備、刪除惡意軟件等。
⑷調查和分析：提供詳細的事件日誌和報告，支援安全專家進行事件調查和根本原因分析。

*2.*託管偵測與回應（MDR）

託管（Managed）指的是由專門的資安服務提供商來執行偵測和應對。偵測與回應（Detection and Response） 與 EDR 相似，但 MDR 將偵測和應對能力外包給第三方服務提供商。MDR 特點：

⑴全面監控：不僅限於端點，還包括網絡、日誌和雲端等多個範疇的監控。
⑵專業知識：提供由專家團隊操作的服務，具備更深入的安全知識和技術專長。
⑶迅速應變：提供 24/7 的監控和應急響應服務，以迅速回應和處理安全事件。

*3.*報告和優化：提供定期的安全狀態報告和建議，幫助企業優化安全策略和措施。

*4.*比較

⑴ EDR 更加侷限於端點設備，企業需要自行管理和操作。
⑵ MDR 提供全面的監控和專業的安全操作，適合企業希望外包安全監控和響應功能的需求。

㈡偵測方面及回應方面活動

*1.*端點偵測與回應（EDR）偵測方面的活動：

⑴行為分析：監控端點設備的使用模式和活動，檢測異常行為，如非授權的系統訪問或檔案操作。
⑵機器學習：利用機器學習算法分析端點上的活動，以檢測新型攻擊模式和未知的威脅。

⑶威脅情報整合：與外部威脅情報平台整合，及時更新和應用最新的安全威脅資訊。

2.端點偵測與回應（EDR）回應方面的活動：

⑴即時響應：一旦偵測到威脅，立即採取行動，如阻止攻擊進一步擴散、切斷訪問權限等。

⑵隔離感染設備：將受感染的端點設備隔離，防止威脅擴散到整個網路。

⑶檔案修復或刪除：移除或修復受感染的檔案，以消除潛在的威脅和後續風險。

3.託管偵測與回應（MDR）偵測方面的活動：

⑴全面監控：不僅限於端點，還包括網絡流量、雲端平台、日誌等多個範疇的持續監控。

⑵威脅檢測與分析：透過安全操作中心（SOC）的專家團隊，分析多源頭的威脅情報，以及內部和外部的安全事件。

⑶實時警報：及時識別和回報安全事件，並啟動適當的應變程序。

4.託管偵測與回應（MDR）回應方面的活動：

⑴ 24/7 的監控和支援：提供全天候的安全監控和支援服務，以應對即時的安全威脅。

⑵應急響應：在檢測到威脅後，立即採取行動，如隔離受感染的設備、阻斷攻擊來源等。

⑶安全事件調查：進行深入的事件調查和分析，以確定攻擊的來源、影響範圍和後續防範措施。

5.兩者比較

⑴ EDR 主要專注於端點設備上的威脅偵測和即時回應，企業需自行管理和操作。

⑵ MDR 提供全面的安全監控和專業的安全操作服務，外包給專門的安全服務提供商管理，通常包括 24/7 的支援和更深入的安全分析能力。

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（WebApplication 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）

**1.《考題難易》：★★★☆☆ (最難 5 顆星)**

**2.《解題關鍵》：本題為防火牆整合應用題，掌握 CDN 與各種防火牆相關技術概念始可作答。**

**3.《命中特區》：**

【擬答】：

㈠Web 應用程式防火牆（Web Application Firewall, WAF）是一種專門用於保護網路應用程式安全的防禦工具，透過深入監控和分析網路應用程式的流量和行為，採取多層次的防禦機制來保護應用程式不受各種常見的攻擊和威脅的影響。其主要防禦機制包括以下幾個方面：

1.應用程式層面的攻擊防禦：

⑴ SQL 注入防禦：檢測並阻止攻擊者嘗試通過應用程式界面對資料庫進行 SQL 注入攻擊。

⑵跨站腳本（XSS）防禦：檢測並阻止攻擊者試圖將惡意腳本注入到網頁中，從而攻擊用戶端的瀏覽器。

⑶跨站請求偽造（CSRF）防禦：確保只有來自預期的用戶端發送的請求才能成功處理，防止 CSRF 攻擊。

2.協議層面的安全檢測：

完成 HTTP/HTTPS 請求和回應檢測，透過監控和篩選來自用戶端和伺服器的 HTTP 和 HTTPS 流量，防止不合法的請求和應答。

3.威脅情報檢測：

⑴黑名單和白名單控制：基於已知的攻擊模式和 IP 地址黑名單，防止攻擊者利用已知的漏洞進行攻擊。

⑵異常行為檢測：分析和監控用戶端和伺服器之間的通訊模式，檢測並阻止不正常的行為

模式，如大量的請求或不尋常的資料傳輸量。

4. 即時監控和報警：

進行事件記錄和報警，透過記錄所有攻擊嘗試和安全事件，並發出警報以通知安全操作人員進行即時響應和調查。

㈡次世代防火牆（Next-Generation Firewall, NGFW）整合了傳統防火牆的基本功能，同時加入了更先進的安全功能和技術，以應對現代和未來的複雜安全威脅，同時提供更靈活和精確的安全管理和控制能力。其主要防禦機制包括以下幾個方面：

1. 應用程式識別與控制：

NGFW 能夠深度分析和識別不同應用程式的流量，包括通常運行在標準端口以外的應用程式。這使得管理者可以更精確地控制哪些應用程式可以訪問網路，並對其進行限速或阻止。

2. 用戶與設備識別：

NGFW 可以識別和控制連接至網路的用戶和設備，基於用戶身份或設備特徵，允許或限制其訪問特定的應用程式和資源。

3. 內容過濾與深度封包檢測：

NGFW 能夠進行深度封包檢測，分析網路流量中的每個封包內容，以識別潛在的威脅和攻擊。這包括檢測並阻止傳統防火牆可能會錯過的高級威脅，如進階持續性威脅（APT）和未知的零日漏洞攻擊。

4. 威脅智能防禦：

NGFW 整合了實時威脅情報和智能分析能力，用於即時檢測和防禦新興和已知的安全威脅。這包括使用威脅情報訂閱服務來更新和應用最新的威脅簽名和行為模式。

5. 安全性政策和運營洞察：

NGFW 提供強大的安全性政策管理功能，使管理者能夠制定和執行細緻的安全性策略，包括基於應用程式、用戶、設備和內容的細緻控制。同時，NGFW 也能提供全面的運營洞察，通過分析網路流量和事件記錄，來優化安全性策略和警報。

6. SSL/ TLS 解密：

NGFW 具有能力解密和檢查加密的 SSL/TLS 流量，這使得它能夠分析和檢測潛藏在加密流量中的威脅和攻擊。

㈢當內容傳遞網路（CDN）與 Web 應用程式防火牆（WAF）結合在一起時，僅提升網站性能和安全性，還能降低運營成本，並提高網站的可用性和可靠性，這對於需要提供快速、安全且可靠的網站服務的企業和組織來說是一個非常有效的解決方案。可以帶來以下主要效益：

1. 提升網站性能與加速頁面載入速度：

CDN 通常會將網站的靜態資源（如圖片、CSS、JavaScript 文件）分發到全球各地的節點上。這樣一來，當用戶訪問網站時，他們可以從最接近他們位置的節點快速載入這些靜態資源，大大減少了網頁載入的時間。同時，CDN 的高效傳輸和壓縮技術也有助於提升整體網站的性能和用戶體驗。

2. 增強網站安全性：

WAF 用於保護網站免受各種攻擊，如 SQL 注入、跨站腳本攻擊（XSS）、跨站請求偽造（CSRF）等。當 WAF 與 CDN 結合時，CDN 可以作為第一道防禦線，將大部分惡意流量擋在網站之外，減輕 WAF 的負擔，同時 CDN 還能夠過濾掉一些常見的簡單攻擊，這樣可以有效減少 WAF 需要處理的請求數量，提高 WAF 的效率。

3. 降低網站運營成本：

CDN 可以減少原始伺服器的負載和流量，這樣一來，您可以使用較少的伺服器來處理相同或更多的訪問量。同時，由於 CDN 節點散佈在全球各地，可以有效減少全球用戶訪問您網站時的延遲，提升用戶體驗，進而增加用戶黏性和轉換率，從而間接降低營運成本。

4. 提高服務的高可用性和可靠性：

CDN 的多節點部署和自動故障轉移功能，使得即使某些節點或伺服器出現問題，仍能保證用戶能夠訪問到網站的內容。這種高可用性和可靠性可以有效降低因服務中斷而造成的損失和用戶流失。

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)

**1.《考題難易》：★★☆☆☆ (最難 5 顆星)**
**2.《解題關鍵》：本題為資安管理基本題，掌握資安風險控制措施即可作答。**
**3.《命中特區》：**

【擬答】：

機關在進行資安風險評估和管理時，可以採取以下資安控制措施，以降低風險並提升資安防護水平，分別涵蓋事前、事中和事後三個階段：

㈠事前階段（防範措施）：

1. 風險評估和管理計畫：制定和實施系統化的風險評估計畫，定期評估機關面臨的各種資安風險，並確定應對策略和控制措施。
2. 資安政策與程序：制定全面的資安政策和相應的程序，包括存取控制、密碼管理、資料分類和保護等，以確保整體資安控制框架的有效實施。
3. 安全意識與培訓：進行定期的資安意識培訓，提高機關內部人員對於資安風險的認識和應對能力，並推動資安文化的建立和強化。
4. 技術防禦措施：部署先進的技術防禦措施，如防火牆、入侵檢測系統（IDS）、入侵防禦系統（IPS）等，以及安全設計和網絡架構設計，有效防止外部攻擊和內部威脅。

㈡事中階段（偵測與應對措施）：

1. 威脅偵測和事件監控：建立和運營威脅偵測系統（例如 SIEM 系統），持續監控網路、系統和應用程式的活動，及時發現和回應潛在的安全事件。
2. 即時響應與事件處理：建立和實施即時響應計畫，包括建立應急響應小組、制定事件處理程序和應急響應計畫，以迅速應對資安事件和減少損失。
3. 漏洞管理：定期進行系統和應用程式的漏洞掃描和評估，及時修補已知漏洞，並監控漏洞修補的有效性。

㈢事後階段（恢復與改進措施）：

1. 資料備份與恢復：實施完整的資料備份和恢復策略，包括定期備份和測試恢復流程，以確保在資安事件發生後能夠快速恢復資料和服務。
2. 安全審查與改進：定期進行資安審查和漏洞分析，評估資安事件的影響和應對效果，並不斷改進資安策略和控制措施。

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)

*1.*《考題難易》：★★☆☆☆ **(最難 5 顆星)**

*2.*《解題關鍵》：**本題為資安系統防護法規題，掌握資通系統防護基準即可作答。**

*3.*《命中特區》：

【擬答】：

根據資通安全責任等級分級辦法，系統防護基準在營運持續計畫構面中包含系統備份和系統備援兩項重要措施。這些措施根據不同的資通安全責任等級需求，有以下要求：

㈠系統備份應辦事項

*1.* 定期備份計畫：

制定定期的備份計畫，確保系統資料能夠定期進行完整和增量備份。根據系統的敏感性和重要性，確定備份頻率，通常包括每日、每週或每月的備份週期。

*2.* 資料完整性驗證：

建立資料備份後的驗證機制，確保備份數據的完整性和可恢復性。可以通過定期的驗證和測試來確保備份數據的有效性，並且在備份後立即進行校驗。

*3.* 安全存儲和存取控制：

確保備份數據的安全存儲，採用加密和存取控制措施，避免未經授權的存取或篡改。存儲備份的位置應遠離主系統位置，以防止同時遭受物理或數字攻擊。

*4.* 災害恢復計畫整合：

將備份策略整合到災害恢復計畫中，確保在發生災害或系統故障時能夠快速恢復。包括確定恢復點目標（RPO）和恢復時間目標（RTO），並確保備份策略能夠達到這些目標。

㈡系統備援應辦事項

*1.* 熱備援或冷備援選擇：

根據系統可用性需求，選擇合適的備援策略。熱備援通常保持系統的即時複製，能夠迅速切換以提供服務。冷備援則更為成本效益，但在恢復時間上可能較長。

*2.* 故障轉移測試：

定期進行備援系統的故障轉移測試，確保備援系統的正確性和可用性。測試應覆蓋從主系統到備援系統的轉換過程，並驗證所有系統功能和數據的完整性。

*3.* 即時監控和自動切換：

配置監控系統，實時監控主系統和備援系統的狀態。當主系統發生故障時，能夠自動切換到備援系統，減少服務中斷時間和影響。

*4.* 跨地理區域備援：

對於高度可用性要求的系統，考慮跨地理區域的備援部署，以防止單一地點的自然災害或人為事故對系統造成的影響。