# 《資通安全防護技術》

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）

| | |
|---|---|
| **試題評析** | 主要是描述對於資安事件的處理流程演變，此類考題容易回答，但是不易辨別出各類型的不同，因此如何掌握為何要改變成新一代的資安事件處理額外重要，與其死背概念，可以試著從歷史的角度，從以前到現在產品的變化，隨著時代如何推陳出新，方能了解三者之中有何差異。 |
| **考點命中** | 1.《高點・高上資通安全講義》第二回，金乃傑編撰，第三章第三節，頁47。<br>2.《高點・高上資通安全講義》第二回，金乃傑編撰，第四章第五節，頁109。 |

**答**：

駭客攻擊手法已經超出傳統防護模式，如：防火牆+防毒軟體，大約於2008年，光纖網路到家將網路速度提高一個層次，APT進階持續威脅式攻擊因應而生，服務型態也從個人硬碟到雲端網路運作與儲存。

因此，企業必須能夠同時從多方位、多維度分析，萃取出威脅情資，並且即時反應處理。以近年來的例子來說，WannaCry蠕蟲勒索軟體造成巨大災情，就是透過目標魚叉或是APT結合，長期摸索內部網路，導致勒索病毒造成全球等級規模災情，主要就是感染途徑不再是不點擊就不會中毒，而是可以主動感染有SMB漏洞的電腦。

(一)SIEM：安全性資訊與事件管理，是一種軟體系統，從各種不同對內外基礎設施、網路連線，收集和分析資料，並提供視覺化圖像管理，一目了然目前所發生的事件。

1.優點：威脅偵測、記錄管理、事件分析以及法規和標準的合規性，偵測過程中的潛在威脅，和提供簡單的事件回應處理。

2.缺點：隨著威脅增加，使用者面臨成本增加、過多的虛假警報、有限的偵測攻擊類型。

(二)SOAR：安全性協調流程、自動化和回應的縮寫，是一套可自動預防和回應網路攻擊的整合性流程系統服務。為了完成自動化流程，必須將組織的作業流程統一整合與定義，進而產生回應。

1.優點：透過協同合作、自動化流程處理和事件回應三大模組，將收集的日誌與警報更有效率地處理，降低成本(包含軟體與人工處理)、增加可處理攻擊類型範圍並即時處理。

2.缺點：於雲端基礎建設與新型的網路通訊來源，攻擊可能是彈性、廣泛，而非皆可以自動化處理與執行。

小結：SIEM收集log並分析結論，而SOAR會根據此結論來自動化流程運作，即時回應事件與減少人力負擔成本。

舉例：每當某個外部IP連線後，網路壅塞，SIEM會根據事實記錄log，哪個IP來源，使用哪些服務，假如對方是合法白名單IP，但是負載過重偶爾會造成server當機，因此當server沒有回應時，SOAR便會自動重啟該server。

隨著網路服務增加，各種xaas as service出現，XDR因應而生。

(三)XDR：延伸式偵測及回應，可蒐集並自動交叉關聯涵蓋多個防護層的資料，包括：電子郵件、伺服器、雲端工作負載以及網路通訊，藉由「多維度」的整合各種資安工具，自動化的資料分析，提供更快的威脅偵測、與事件回應時間。

1.優點：多維度的整合交叉分析資料，提供更準確、更全面的防護效果。

2.缺點：費用昂貴，技術門檻高，且須分析的資料多，耗費更多頻寬與資源，過於複雜防護邏輯技術，可能影響原有系統的效能。



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）

| | |
|---|---|
| **試題評析** | IPS與IDS為傳統考題，基本上有準備的考生都可以回答出來它們之間的差異，然而若能舉出實例，說明IDS與IPS應用時機，則是可以獲得高分的關鍵。 |
| **考點命中** | 《高點・高上資通安全講義》第二回，金乃傑編撰，第三章第三節，頁38。 |

**答**：

(一)IDS：入侵偵測系統，用於監控網路並檢查是否有可疑活動或是異常事件，有違反既定的組織作業政策，向網路管理者回報潛在威脅警示。

IDS有分主機型與網路型，主機型可以檢查至內部應用程式活動，然而同時也占用主機運作資源；網路型快速，部署於閘道，多台主機只要部署一套即可，然而對於有加密的封包無法檢測。

IDS步驟為：事件產生→事件分析→透過儲存發生過的事件資料庫進行比對，發出警報通知SOC或是直接採取簡單處理措施，如：封鎖IP→事件處理與日後稽核。

(二)IPS：即時防禦系統，由IDS演化而來，採取更多資源於即時回應自動化阻斷的議題上，同時管控網路存取、監控與掃描可能入侵資料、並防止攻擊的形成。

實例：某政府單位遭受勒索軟體攻擊，IDS記錄內部目前哪些主機被感染、哪些目標受到感染、進行了哪些操作，來源IP為何，目前被攻破的網段為哪些，作為事後手法研究與復原的依據；IPS則是在邊界將惡意的IP即時擋下，假如已經有主機被感染，則隔離該台主機，並切斷電源，避免災情擴大。

小結：IDS重視內部監控，提供可能的攻擊並詳細記錄，作為事後分析與預防、稽核使用；IPS注重來源端至目的端的路徑，通常部署於邊界，重視於事件即時反應。

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）

| | |
|---|---|
| **試題評析** | 零信任架構從去年到今年在國家考試已經連續兩年出現，現行資安狀況為何不滿足與零信任架構希望達到的效益為何，構成核心為何，乃是答題重點。 |
| **考點命中** | 《高點・高上資通安全講義》第二回，金乃傑編撰，第三章第一節，頁6～8。 |

**答**：

根據國家資通研究院與台灣資安大會說明，零信任架構主要是APT攻擊多元、存取設備行動化、雲端趨勢與網路購物盛行，個資、商業機密與網路密切結合，因此對於組織的攻擊不再區分內網與外網，將邊界模糊化，但每個功能領域都應該要有自己的邊界，ZTA的精神是把邊界切得更細。

外部網路來源阻擋太多，影響系統效率，內部網路不必然一定安全，可能有潛在的攻擊者，因此微核心邊界興起，不再完全依賴傳統防火牆，而是個別網路封包、資料庫和應用程式都應該要有自己的驗證安全與個資保護機制，與傳統資訊安全混用並行，達到整合協同的防禦機制。

決策引擎的核心有「身分鑑別」、「設備鑑別」及「信任推斷」三大關鍵技術：

(一)身分鑑別：多因子身分鑑別與鑑別聲明。

1.多因子身分鑑別：使用傳統密碼外，可以搭配持有卡片、OTP(one time password)簡訊動態一次性驗證碼方式驗證身分。

2.鑑別聲明：出示由CA曾簽署過的數位簽章或出示員工證件，表示與所聲稱的身份相符。

(二)設備鑑別：設備鑑別與設備健康管理

1.設備鑑別：基於公開金鑰演算法，任何設備皆須向CA單位註冊與核發的憑證，未來CA認為此設備有問題，則註銷憑證。

2.設備健康管理：目前設備的狀態，任何電子設備皆有年限問題，因此作業系統是否有更新、防毒軟體是否有更新、網域是否有納入管理與保護，或是基礎硬體設施是否健康，皆作為評估關鍵，代表企業產品：Google Kubernetes Engine。

(三)信任推斷：使用者情境信任推斷機制。

1.依使用情境計算每次存取之信任分數作為判斷依據。

2.依登入時間、是否為新的行動設備或是網段，推斷是否為攻擊，若為高風險登入，則傳送OTP動態簡訊至行動設備進行驗證。



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）

| | |
|---|---|
| **試題評析** | 這些名詞相當混淆，若是一味死記通常拿不到高分，而且若答案模擬兩可，無法有效區分差異，會影響到第二小題的作答，無法從第一小題中的分類加強敘述論點；弱點掃描、滲透測試、源碼檢測皆為測試項目的工作之一，而從白箱與黑箱的區別先分類，再加以論述個別測試之中該項工作有何特色，為取分之關鍵，若能帶入系統分析與設計概念更具有鑑別度。 |

**考點命中**　《高點・高上資通安全講義》第二回，金乃傑編撰，第四章第四節，頁93～95。

**答**：

(一)1.源碼檢測：屬於白箱測試的一種，須要「握有原始碼」才能進行的檢測，通常原始碼只會在開發軟體商手上，購買的客戶端不能擁有其原始碼，只有購買年限使用權，除非雙方有訂定特別條款。源碼檢測分析應在軟體開發生命週期各階段皆須檢測，並且持續用於應用程式生命週期中，實踐SSDLC開發精神。可以檢測到各種類型的漏洞，包括：SQL注入、跨站腳本攻擊，或是程式碼非預期的例外未處理和安全版本漏洞。代表工具為： Fortify Static Code Analyzer。

2.滲透測試：屬於黑箱測試的一種，從未擁有原始程式碼的角度下進行作業。滲透測試通常是透過「雇用專業熟悉電腦的白帽專家」，而非「工具」所進行一連串的攻防測試，在有限的時間內模擬「惡意駭客」可能攻擊的方式，從各個服務端點執行攻擊，確認系統與組織是否可以有效防禦應對的指標，找出最有可能被攻擊風險路徑、遇到災害時如何應對與事後復原。

3.弱點掃描：屬於黑箱測試的一種，主要是透過「自動化流程的工具」偵測應用程式與作業系統的潛在弱點，這些弱點比較容易被發掘，例如：不當的程式設計(像是：未過濾特殊字元、if沒有搭配else、switch沒有break、未定義的變數)、已過時不支援的SDK、不當的防火牆網路規劃(如：port設定)、密碼強度不足等問題。知名軟體有：Nessus、資策會OKWASP弱點掃描平台。

(二)1.主機弱掃：主要是針對內網服務主機的弱點掃描，掃描評估是否存在漏洞與風險等級嚴重程度，並提出相關建議。主要弱點有：太久未更新作業系統、是否存在已發現的CVE並且未修補、使用程式語言是否過期，導致原有架構有溢位攻擊可能、開啟過多不需要開啟的port、權限控管問題。

2.網頁弱掃：常見的有OWASP排名第三的注入式攻擊(SQL、XSS)、管理者權限控管問題、傳輸過程中的機密性與完整性評估、語法與邏輯錯誤、未定義變數、OWASP排名第六危險與過舊元件安全性問題。