## D7-002 結果 2022 年 12 月 3 日

### 問題一

tb787631.CISSPPT3E.c07.044

以下哪一項是計算機安全事件的示例？（選擇所有符合條件的。）

A. 備份未能正確完成

B. 系統訪問記錄在日誌中

C. 文件服務器未授權漏洞掃描

D. 反病毒簽名的更新

你回答正確！

安全事件會對信息或資產的機密性、完整性或可用性產生負面影響和/或

違反安全策略。服務器未經授權的漏洞掃描確實違反了安全策略並且可能

對該系統的安全性產生負面影響，因此它符合安全事件的條件。備份未能

正確完成會危及可用性，因此也是安全事件。系統訪問的日誌記錄和防病

毒簽名的更新都是常規操作，不違反策略或危害安全，因此它們都是事件

而不是事件。

### 問題 2

tb787631.CISSPPT3E.c07.065

請參考以下場景：

- Ann 是一家中型企業的安全專家，通常為她的組織處理日誌分析和安全監控任務。她的職責之一是監控來自組織的入侵檢測系統的警報。該系統通常每天會生成幾十條警報，經過她的調查，其中許多警報都是誤報。
- 今天早上，入侵檢測系統發出警報，因為網絡開始接收異常大量的入站流量。Ann 收到此警報並開始調查流量的來源。

當 Ann 進一步分析流量時，她意識到流量來自許多不同的來源並且已經使網絡不堪重負，從而阻止了合法使用。入站數據包是對她在出站流量中看不到的查詢的響應。對於它們的類型，響應異常大。安應該懷疑哪種類型的攻擊？

A. 認可

B、惡意代碼

C. 系統滲透

D. 拒絕服務

你回答正確！

此場景中描述的攻擊具有拒絕服務攻擊的所有特徵。更具體地說，Ann 的組織可能正在經歷 DNS 放大攻擊，攻擊者使用屬於目標系統的偽造源 IP 地址向第三方 DNS 服務器發送虛假請求。因為攻擊使用 UDP 請求，

所以沒有三向握手。攻擊數據包經過精心設計，可以從簡短的查詢中引出

冗長的響應。這些查詢的目的是生成前往目標系統的響應，這些響應足夠

大且數量足以壓倒目標網絡或系統。

**問題三**

tb787631.CISSPPT3E.c07.028

弗蘭克正在考慮在即將發生的刑事案件中使用不同類型的證據。以下哪一項不是法庭採納證據的必要條件？

A. 證據必須是相關的。

B. 證據必須是實質性的。

C. 證據必須是有形的。

D. 證據必須是有能力獲得的。

您回答錯誤。

法庭上提供的證據必須與確定相關事實相關，對手頭的案件具有重要意義，

並且是合法獲得的。證據不需要是有形的。證人證詞是可以在法庭上提供

的無形證據的一個例子。

**問題四**

tb787631.CISSPPT3E.c07.011

請參考以下場景：

- Gary 最近被當地政府機構聘為首位首席信息安全官 (CISO)。該機構最近遭遇安全漏洞，正試圖建立一個新的信息安全計劃。Gary 希望在設計此程序時應用一些安全操作的最佳實踐。

當 Gary 決定他應該授予每個用戶什麼訪問權限時，什麼原則應該指導他關於默認權限的決定？

A. 職責分離

B. 最小權限

C、聚合

D. 特權分離

你回答正確！

Gary 應該遵循最小權限原則，只為用戶分配他們履行工作職責所需的權限。聚合是一個術語，用於描述特權隨時間的無意累積，也稱為特權蔓延。

職責分離和特權分離是用於保護敏感進程的原則。

**問題 5**

tb787631.CISSPPT3E.c07.092

Jerome 正在進行取證調查並審查數據庫服務器日誌以調查查詢內容以尋找 SQL 注入攻擊的證據。他在進行什麼類型的分析？

A. 硬件分析

B、軟件分析

C. 網絡分析

D. 媒體分析

您回答錯誤。

應用日誌的分析是軟件分析的核心任務之一。這是正確的答案，因為

SQL 注入攻擊是應用程序攻擊。

**問題 6**

tb787631.CISSPPT3E.c07.017

Tonya 正在從涉及網絡安全事件的一系列系統中收集證據。一位同事建議她在收集過程中使用取證磁盤控制器。這個裝置的功能是什麼？

A. 存儲設備上報的屏蔽錯誤情況

B. 向存儲設備發送寫命令

C.攔截修改或丟棄發送到存儲設備的命令

D. 防止發送到設備的讀操作返回數據

你回答正確！

取證磁盤控制器執行四個功能。其中之一，寫阻塞，攔截發送到設備的寫

命令並阻止它們修改設備上的數據。其他三個功能包括返回讀取操作請求

的數據、從設備返回訪問重要信息以及從設備向取證主機報告錯誤。

**問題 7**

tb787631.CISSPPT3E.c07.013

請參考以下場景：

- Gary 最近被當地政府機構聘為首位首席信息安全官 (CISO)。該機構最近遭遇安全漏洞，正試圖建立一個新的信息安全計劃。Gary 希望在設計此程序時應用一些安全操作的最佳實踐。

Gary 正準備為新用戶創建帳戶並為 HR 數據庫分配權限。在授予此訪問權限之前，Gary 必須驗證哪兩個信息要素？

A. 證書和需要知道的

B. 許可和需要知道的

C. 密碼與權限

D. 密碼和生物識別掃描

您回答錯誤。

在授予訪問權限之前，Gary 應該驗證用戶是否具有有效的安全許可，並且企業需要了解這些信息。Gary 正在執行授權任務，因此他不需要驗證用戶的憑據，例如密碼或生物識別掃描。

**問題 8**

tb787631.CISSPPT3E.c07.059

Melanie 懷疑有人正在使用惡意軟件竊取她公司的計算週期。以下哪一種安全工具最適合檢測此類事件？

A. NIDS
B、防火牆
C、HIDS
D、DLP

您回答錯誤。

基於主機的入侵檢測系統 (HIDS) 可能能夠檢測系統上運行的未經授權的進程。提到的其他控制，網絡入侵檢測系統 (NIDS)、防火牆和 DLP 系統，都是基於網絡的，可能不會注意到流氓進程。

**問題 9**

tb787631.CISSPPT3E.c07.083

應用程序開發人員可以使用什麼技術在隔離的虛擬化環境中測試應用程序，然後再允許它們進入生產網絡？

A. 滲透測試
B. 沙盒
C. 白盒測試
D. 黑盒測試

你回答正確！

沙盒是一種技術，應用程序開發人員（或不受信任的應用程序的接收者）

可以在與生產系統隔離的虛擬化環境中測試代碼。白盒測試、黑盒測試和

滲透測試都是常見的軟件測試技術，但不需要使用隔離系統。

**問題 10**

tb787631.CISSPPT3E.c07.031

Sam 負責備份公司的主文件服務器。他配置了一個備份計劃，每週一晚上 9 點執行完整備份，並在一周的其他日子的同一時間執行差異備份。文件根據下圖所示的信息變化。星期三的備份將復制多少文件？

- 文件修改
- 星期一上午 8 點 - 創建文件 1

- 星期一上午 10 點 - 創建文件 2
- 星期一上午 11 點 - 創建文件 3
- 星期一下午 4 點 - 文件 1 已修改
- 星期一下午 5 點 - 創建文件 4
- 星期二上午 8 點 - 文件 1 已修改
- 星期二上午 9 點 - 文件 2 已修改
- 星期二上午 10 點 - 創建文件 5
- 星期三上午 8 點 - 文件 3 已修改
- 星期三上午 9 點 - 創建文件 6

A2
B.3
C.5
D.6

您回答錯誤。

在這種情況下，服務器上的所有文件將在星期一晚上在完整備份期間進行

備份。週三的差異備份將復制自上次完整備份以來修改過的所有文件。其

中包括文件 1、2、3、5 和 6：總共五個文件。

- 文件修改

- 星期一早上 8 點。- 創建文件 1

- 星期一上午 10 點。- 創建文件 2

- 星期一上午 11 點 - 創建文件 3

- 星期一下午 4 點 - 文件 1 已修改

- 星期一下午 5 點 - 創建文件 4

- 星期二上午 8 點 - 文件 1 已修改

- 星期二上午 9 點 - 文件 2 已修改

- 星期二上午 10 點 - 創建文件 5

- 星期三上午 8 點 - 文件 3 已修改

•星期三上午 9 點 - 創建文件 6

**問題 11**

tb787631.CISSPPT3E.c07.027

Helen 正在實施一種新的安全機制，以授予員工在會計系統中的管理權限。她設計了流程，以便員工的經理和會計經理都必須在授予訪問權限之前批准該請求。Helen 執行的信息安全原則是什麼？

A. 最小權限

B、兩人控制

C. 崗位輪換

D. 職責分離

你回答正確！

在這種情況下，Helen 設計了一個流程，需要兩個人同意才能執行敏感操作。這是一個兩人控制的例子。這與職責分離不同，在職責分離中，一個人可能沒有兩個單獨的權限，當合併時，可能會允許不需要的操作。適用於這種情況的職責分離可能意味著同一個人可能無法同時擁有發起請求和批准請求的能力。最小特權表示個人應該只擁有執行其工作職能所需的

必要權限。工作輪換是一種讓用戶定期轉換工作職能以檢測瀆職行為的方案。

## 問題 12

tb787631.CISSPPT3E.c07.055

Veronica 正在考慮實施顧問推薦的數據庫恢復機制。在推薦的方法中，自動化過程每晚將數據庫備份從主要設施移動到異地位置。顧問描述的是哪種類型的數據庫恢復技術？

A. 遠程日誌
B、遠程鏡像
C. 電子拱頂
D. 事務日誌

您回答錯誤。

在電子存儲方法中，自動化技術按計劃（通常是每天）將數據庫備份從主數據庫服務器移動到遠程站點。事務日誌記錄不僅僅是一種恢復技術；它是生成遠程日誌中使用的日誌的過程。遠程日誌記錄將事務日誌傳輸到遠程站點的頻率比電子存儲更頻繁，通常是每小時一次。遠程鏡像在備份站

點維護一個實時數據庫服務器，並將主站點的所有事務鏡像到備份站點的

服務器上。

**問題 13**

tb787631.CISSPPT3E.c07.051

在事件調查期間，調查人員會見可能了解事件相關信息但不是嫌疑人的系統管理員。在這次會議期間正在進行什麼類型的對話？

A.面試

B. 訊問

C. 面談和審訊

D.既不是面談也不是審問

你回答正確！

當調查人員會見可能擁有與他們的調查相關的信息但不是嫌疑人的個人時，

就會進行面談。如果個人是嫌疑人，那麼會面就是審訊。

**問題 14**

tb787631.CISSPPT3E.c07.032

以下哪一個安全工具不能對安全事件產生主動響應？

A.IPS

B、防火牆

C、入侵檢測系統

D、殺毒軟件

您回答錯誤。

入侵檢測系統 (IDS) 僅提供被動響應，例如提醒管理員注意可疑攻擊。

另一方面，入侵防禦系統和防火牆可能會採取措施阻止攻擊企圖。防病毒

軟件還可以通過隔離可疑文件來進行主動響應。

**問題 15**

tb787631.CISSPPT3E.c07.042

以下哪一項不是您可以採取的基本預防措施來保護您的系統和應用程序免受攻擊？

A. 實施入侵檢測和預防系統。

B. 維護所有操作系統和應用程序的當前補丁級別。

C. 刪除不必要的帳戶和服務。

D. 對所有系統進行取證成像。

你回答正確！

沒有必要進行法醫成像作為預防措施。相反，應該在事件響應過程中使用

取證成像。維護補丁級別、實施入侵檢測/預防以及刪除不必要的服務和

帳戶都是基本的預防措施。

**問題 16**

tb787631.CISSPPT3E.c07.078

Kevin 正在為他的組織製定持續的安全監控策略。在確定評估和監測頻率時，通常不使用以下哪一項？

A. 威脅情報
B. 系統分類/影響級別
C. 安全控制操作負擔
D. 組織風險承受能力

您回答錯誤。

根據 NIST SP 800-137，組織應使用以下因素來確定評估和監控頻率：

安全控制波動性、系統分類/影響級別、安全控製或提供關鍵功能的特定

評估對象、已識別弱點的安全控制、組織風險承受能力、威脅信息、漏洞

信息、風險評估結果、監控策略審查的輸出和報告要求。

## 問題 17

tb787631.CISSPPT3E.c07.096

Pauline 正在審查她所在組織的應急管理計劃。在製定這些計劃時，什麼應該是最優先考慮的？

A. 保護關鍵任務數據
B. 操作系統的保存
C. 證據收集
D. 維護安全

你回答正確！

在製定應急管理計劃時，所有這些考慮因素都很重要。然而，人的生命安全應始終是壓倒一切的優先事項，高於所有其他考慮因素。

## 問題 18

tb787631.CISSPPT3E.c07.018

Lydia 正在為她的組織處理訪問控制請求。她遇到一個請求，其中用戶確實具有所需的安全許可，但沒有訪問的業務理由。莉迪亞拒絕了這個請求。她遵循什麼安全原則？

A、需要知道
B. 最小權限
C. 職責分離
D.兩人控制

您回答錯誤。

莉迪亞遵循需要知道的原則。雖然用戶可能具有適當的安全許可來訪問此

信息，但沒有提供商業理由，因此她不知道用戶有適當的需要了解該信息 。

**問題 19**

tb787631.CISSPPT3E.c07.094

Carolyn 擔心她網絡上的用戶可能會在沒有適當授權或安全控制的情況下將敏感信息（例如社會安全號碼）存儲在他們的硬盤上。她可以實施哪種第三方安全服務來最好地檢測此活動？

艾滋病

B、IPS

C、DLP

D、TLS

你回答正確！

數據丟失防護 (DLP) 系統可以識別存儲在端點系統上或通過網絡傳輸的

敏感信息。這是他們的主要目的。DLP 系統通常作為第三方託管服務產

品提供。入侵檢測和預防系統 (IDS/IPS) 可用於使用為此目的構建的簽

名來識別一些敏感信息，但這不是這些工具的主要作用，並且它們在執行

此任務時不如 DLP 系統有效。TLS 是一種網絡加密協議，可用於保護敏

感信息，但它不具有任何識別敏感信息的能力。

**問題 20**

tb787631.CISSPPT3E.c07.073

Allie 負責審查其組織網絡上的身份驗證日誌。她沒有時間查看所有日誌，因此她決定只選擇有四次或更多次無效身份驗證嘗試的記錄。Allie 使用什麼技術來減小池的大小？

A、抽樣

B. 隨機選擇

C、裁剪

D. 統計分析

你回答正確！

從大型池中選擇記錄以進行進一步分析的兩種主要方法是抽樣和裁剪。抽

樣使用統計技術來選擇代表整個池的樣本，而裁剪使用閾值來選擇那些超

過預定義閾值的記錄，因為它們可能是分析師最感興趣的。

## 問題 21

tb787631.CISSPPT3E.c07.036

作為一家大型組織的 CIO，Clara 希望採用標準流程來管理 IT 活動。以下哪個框架側重於 IT 服務管理並包括變更管理、配置管理和服務級別協議等主題？

A. ITIL
B、PMBOK
C. PCI DSS
D.TOGAF

你回答正確！

IT 基礎架構庫 (ITIL) 框架側重於 IT 服務管理。項目管理知識體系 (PMBOK) 提供了項目管理專業知識的共同核心。支付卡行業數據安全標準 (PCI DSS) 包含信用卡安全法規。Open Group Architecture Framework (TOGAF) 專注於 IT 架構問題。

## 問題 22

tb787631.CISSPPT3E.c07.071

以下哪些事件會構成安全事件？（選擇所有符合條件的。）

A. 網絡入侵未遂
B. 一次成功的數據庫入侵
C. 惡意軟件感染

D. 訪問文件的成功嘗試

E. 違反保密政策

F. 從安全區域移除信息的不成功嘗試

您回答錯誤。

任何破壞組織安全或違反安全策略的企圖都是安全事件。所有描述的事件都符合這個定義，應該被視為一個事件，只有一個例外。成功訪問文件的嘗試當然是安全事件，但除非確定訪問文件的個人未獲得授權，否則這不是安全事件。

## 問題 23

tb787631.CISSPPT3E.c07.072

Amanda 正在配置她所在組織的防火牆以實施出口過濾。她的組織的出口過濾策略應該阻止以下哪一種流量類型？（選擇所有符合條件的。）

A. 流量在端口 22 上快速掃描許多 IP 地址

B. 帶有廣播目的地的流量

C. 具有來自外部網絡的源地址的流量

D. 目標地址在外部網絡上的流量

您回答錯誤。

出口過濾掃描出站流量以查找潛在的安全策略違規行為。這包括可能是惡

意的流量，例如端口 22 上的出站 SSH 掃描。它還包括看似屬於攻擊或

錯誤配置的流量，例如將流量發送到廣播目標地址。最後，它包括內部系

統生成的欺騙流量，這些流量可能帶有來自外部網絡的源地址。防火牆應

該期望看到的正常流量是在外部網絡上承載目標地址的流量。

**問題 24**

tb787631.CISSPPT3E.c07.043

蒂姆是一名法醫分析師，他正試圖從硬盤中檢索信息。用戶似乎試圖刪除數據，而 Tim 正試圖重建數據。Tim 正在執行哪種類型的取證分析？

A、軟件分析

B. 媒體分析

C. 嵌入式設備分析

D. 網絡分析

你回答正確！

出於取證目的對硬盤驅動器的審查是媒體分析的一個例子。嵌入式設備分

析著眼於其他大型系統（例如汽車或安全系統）中包含的計算機。軟件分

析分析應用程序及其日誌。網絡分析著眼於網絡流量和日誌。

**問題 25**

tb787631.CISSPPT3E.c07.074

您正在對您網絡上的潛在機器人感染進行調查，並希望對您網絡上的不同系統與 Internet 上的系統之間傳遞的信息進行取證分析。您認為該信息可能已加密。您在活動結束後開始調查。獲取此信息來源的最佳和最簡單方法是什麼？

A. 抓包

B. NetFlow 數據

C. 入侵檢測系統日誌

D. 集中認證記錄

您回答錯誤。

NetFlow 數據包含有關所有網絡通信的來源、目的地和大小的信息，並

作為正常活動的一部分定期保存。數據包捕獲數據將提供相關信息，但它

必須在可疑活動期間捕獲，並且不能在事後重新創建，除非組織已經進行

了 100% 的數據包捕獲，這種情況很少見。此外，加密的使用限制了數

據包捕獲的有效性。入侵檢測系統日誌不太可能包含相關信息，因為加密

流量可能與入侵簽名不匹配。集中式身份驗證記錄不會包含有關網絡流量

的信息。

**問題 26**

tb787631.CISSPPT3E.c07.067

弗蘭克試圖在法庭上出示一名黑客的筆記本電腦作為對黑客不利的證據。筆記本電腦確實包含表明黑客實施犯罪的日誌，但法院裁定警察搜查公寓後發現筆記本電腦是違憲的。什麼可接受性標準阻止 Frank 將筆記本電腦作為證據？

A. 重要性
B. 相關性
C. 道聽途說
D. 能力

你回答正確！

要被採納，證據必須是相關的、重要的和有說服力的。本案中的筆記本電

腦顯然具有重要意義，因為它包含與所涉犯罪相關的日誌。它也很重要，

因為它提供了將黑客與犯罪聯繫起來的證據。它沒有資格，因為證據不是

合法獲得的。

**問題 27**

tb787631.CISSPPT3E.c07.088

Candace 正在為其組織的文件服務器設計備份策略。她想在每個工作日執行一次備份，以盡可能減少存儲佔用空間。她應該執行哪種類型的備份？

A.增量備份

B、完整備份

C、差異備份

D.事務日誌備份

您回答錯誤。

增量備份提供了包含最少數據量的選項。在這種情況下，那將只是自最近

的增量備份以來修改的數據。差異備份將備份自上次完整備份以來修改的

所有數據，這將是一個很大的數量。完整備份將包括服務器上的所有信息 。

事務日誌備份專門用於支持數據庫服務器，在文件服務器上無效。

**問題 28**

tb787631.CISSPPT3E.c07.080

Bruce 在他的網絡上發現了相當多的可疑活動。在查閱他的 SIEM 中的記錄後，似乎有一個外部實體正在嘗試使用端口 22 上的 TCP 連接來連接到他的所有系統。外部人員可能正在進行哪種類型的掃描？

A. FTP 掃描

B. Telnet 掃描

C、SSH 掃描

D. HTTP 掃描

你回答正確！

SSH 使用 TCP 端口 22，因此這種攻擊很可能是為了掃描開放或安全性較弱的 SSH 服務器。FTP 使用端口 20 和 21。Telnet 使用端口 23，HTTP 使用端口 80。

**問題 29**

tb787631.CISSPPT3E.c07.084

Gina 是一家小型企業的防火牆管理員，她最近安裝了一個新的防火牆。在看到網絡流量異常大的跡像後，她檢查了入侵檢測系統，該系統報告說正在進行 SYN 泛洪攻擊。Gina 可以更改哪些防火牆配置以最有效地防止此攻擊？

A. 阻止來自已知 IP 的 SYN。

B. 阻止來自未知 IP 的 SYN。

C. 在防火牆上啟用 SYN-ACK 欺騙。

D. 禁用 TCP。

你回答正確！

雖然這似乎不是顯而易見的答案，但許多防火牆都具有內置的反 SYN 泛洪防禦功能，可以代表受保護系統響應 SYN。一旦遠程系統通過繼續三向握手證明是合法連接，TCP 會話的其餘部分就會通過。如果連接被證明是攻擊，防火牆會使用適當的緩解技術來處理額外的負載。阻止來自已知或未知 IP 地址的 SYN 可能會導致本應能夠連接的系統出現問題，而關閉 TCP 將破壞大多數現代網絡服務！

**問題 30**

tb787631.CISSPPT3E.c07.056

在設計訪問控制方案時，Hilda 設置了角色，使同一個人無法提供新用戶帳戶並向帳戶分配超級用戶權限。希爾達遵循什麼信息安全原則？

A. 最小權限
B. 職責分離
C. 崗位輪換
D. 默默無聞的安全

您回答錯誤。

Hilda 的設計遵循職責分離的原則。賦予一個用戶創建新帳戶和授予管理

權限的能力結合了兩個操作，這兩個操作會導致重大的安全更改，應該在

兩個用戶之間分配。

**問題 31**

tb787631.CISSPPT3E.c07.060

Brandon 觀察到他網絡上某個系統的授權用戶最近濫用他的帳戶來利用針對共享服務器的系統漏洞，從而使他能夠獲得對該服務器的 root 訪問權限。發生了什麼類型的攻擊？

A. 拒絕服務
B. 提權
C. 認可
D、蠻力

你回答正確！

該場景描述了一種特權升級攻擊，其中具有系統授權訪問權限的惡意內部

人員濫用該訪問權限來獲取特權憑據。

## 第 32 題

tb787631.CISSPPT3E.c07.050

Grant 收集記錄是為可能的訴訟做準備的一部分，他擔心他的團隊可能會花太多時間收集可能不相關的信息。聯邦民事訴訟規則 (FCRP) 中的什麼概念有助於確保在收益不超過成本時，作為電子發現的一部分不會產生額外的時間和費用？

A. 工具輔助審查

二、合作

C. 腐敗

D. 相稱性

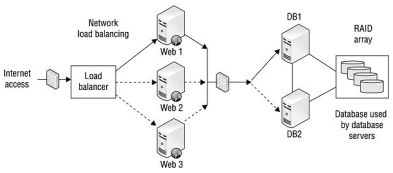
您回答錯誤。

額外發現的好處必須與其所需的額外成本成正比。這可以防止額外的發現請求變得異常昂貴，並且請求者通常必須向主持案件的法官證明這些請求是合理的。

## 問題 33

tb787631.CISSPPT3E.c07.001

Mary 正在審查此處顯示的系統架構的可用性控制。展示了哪些技術可以為數據庫服務器提供容錯能力？




A.故障轉移集群

B、UPS

C、磁帶備份

D、冷場

你回答正確！

The illustration shows an example of a failover cluster, where DB1 and DB2 are both configured as database servers. At any given time, only one will function as the active database server, while the other remains ready to assume responsibility if the first one fails. While the environment may use UPS, tape backup, and cold sites as disaster recovery and business continuity controls, they are not shown in the diagram.

## Question 34

tb787631.CISSPPT3E.c07.016

Which one of the following terms is often used to describe a collection of unrelated patches released in a large collection?

A. Hotfix

B. Update

C. Security fix

D. Service pack

You Answered Correctly!

修補程序、更新和安全修復都是旨在糾正單個問題的單個補丁的同義詞 。

Service Pack 是許多不同更新的集合，可作為操作系統或應用程序的主要更新。

**問題 35**

tb787631.CISSPPT3E.c07.005

約旦正準備在網絡安全事件調查後向法庭提供證據。他負責準備物理工件，包括受影響的服務器和移動設備。什麼類型的證據完全由可以帶入法庭的有形物品組成？

A. 書面證據

B.口頭證據

C. 證明證據

D. 真實證據

您回答錯誤。

真正的證據包括實際上可能作為證據帶入法庭的事物。例如，真正的證據

包括硬盤、武器和帶有指紋的物品。書面證據包括可能有形或無形的書面

項目。證言證據是證人提供有關信息的口頭證詞。口頭證據規則規定，當

協議以書面形式出現時，書面文件被假定為包含協議的所有條款。

## 問題 36

tb787631.CISSPPT3E.c07.057

Patrick 負責為他的組織實施威脅追踪計劃。以下哪一項是他在計劃工作時應該使用的威脅搜尋程序的基本假設？

答：安全控制是使用縱深防禦策略設計的。

B. 審計可能會發現控制缺陷。

C. 網絡上可能已經存在攻擊者。

D. 防禦機制可能包含未修補的漏洞。

你回答正確！

雖然所有這些假設都是帕特里克可能參與演習的有效前提，但威脅搜尋演

習的基本假設是所謂的妥協假設。這意味著帕特里克應該假設攻擊者已經

獲得了對他系統的訪問權限，然後尋找他們存在的跡象。

## 問題 37

tb787631.CISSPPT3E.c07.023

Ricky 正在尋找應用程序、設備和操作系統中的信息安全漏洞列表。以下哪一項威脅情報來源對他最有用？

A.OWASP

B. Bugtraq

C. 微軟安全公告

D、CVE

您回答錯誤。

Common Vulnerability and Exposures (CVE) 詞典包含有關許多不同安全問題的標準化信息。開放 Web 應用程序安全項目 (OWASP) 包含有關 Web 應用程序安全問題的一般指南，但不跟踪特定漏洞或超越 Web 應用程序。Bugtraq 郵件列表和 Microsoft 安全公告是漏洞信息的良好來源，但不是已知問題的綜合數據庫。

## 問題 38

tb787631.CISSPPT3E.c07.010

Jim 想要識別他網絡上可能參與殭屍網絡的受損系統。他計劃通過監視與已知命令和控制服務器的連接來做到這一點。如果 Jim 可以訪問已知服務器列表，以下哪一項技術最有可能提供此信息？

A. NetFlow 記錄

B、IDS 日誌

C. 認證日誌

D. RFC 日誌

您回答錯誤。

NetFlow 記錄包含網絡上發生的每個網絡通信會話的條目，並且可以與已知惡意主機列表進行比較。IDS 日誌可能包含相關記錄，但這種可能性較小，因為它們只會在流量觸發 IDS 時創建日誌條目，而不是包含所有通信的 NetFlow 記錄。身份驗證日誌和 RFC 日誌不會有任何網絡流量的記錄。

**第 39 題**

tb787631.CISSPPT3E.c07.085

Nancy 正在努力實現其組織的反惡意軟件保護現代化，並希望添加端點檢測和響應 (EDR) 功能。EDR 系統通常支持以下哪些操作？（選擇所有符合條件的。）

A. 分析端點內存、文件系統和網絡活動以尋找惡意活動的跡象

B. 自動隔離可能的惡意活動以遏制潛在的損害

C. 進行模擬網絡釣魚活動

D. 與威脅情報來源的整合

你回答正確！

EDR 平台不進行模擬網絡釣魚活動。EDR 系統最常見的功能是分析端點內存、文件系統和網絡活動以尋找惡意活動的跡象；隔離可能的惡意活動以遏制潛在的損害；與威脅情報來源整合；並與其他事件響應機制相結合。

## 問題 40

tb787631.CISSPPT3E.c07.068

戈登怀疑黑客侵入了他公司的系統。該系統不包含任何受監管的信息，Gordon 想代表他的公司進行調查。他已獲得主管的許可進行調查。下面哪個描述是正確的？

答：法律要求 Gordon 在開始調查之前聯繫執法部門。

B. Gordon 可能不會進行自己的調查。

C. Gordon 的調查可能包括檢查硬盤內容、網絡流量以及屬於公司的任何其他系統或信息。

D. 戈登可能會在確定肇事者後合乎道德地進行“黑客攻擊”活動。

您回答錯誤。

Gordon 可以按照自己的意願進行調查，並使用他可以合法獲得的任何信息，包括屬於他雇主的信息和系統。沒有義務聯繫執法部門。但是，Gordon 不得進行“黑客攻擊”活動，因為這些活動可能違反法律和/或 (ISC) 2 道德規範。

**問題 41**

tb787631.CISSPPT3E.c07.041

Javier 正在驗證只有 IT 系統管理員才能登錄到用於管理目的的服務器。他執行的信息安全原則是什麼？

A、需要知道
B. 最小權限
C.兩人控制
D. 傳遞信任

您回答錯誤。

最小特權原則表明，個人應該只擁有完成其工作職能所必需的特權。刪除

非管理用戶的管理權限是最小權限的一個例子。

## 問題 42

tb787631.CISSPPT3E.c07.075

以下哪一個工具通過為操作系統和應用程序提供標準、安全的配置設置模板來幫助系統管理員？

A. 安全準則
B. 安全政策
C. 基線配置
D. 運行配置

你回答正確！

基線配置作為配置安全系統和應用程序的起點。它們包含遵守組織安全策

略所必需的安全設置，然後可以進行定制以滿足實施的特定需要。雖然安

全策略和指南可能包含保護系統所需的信息，但它們不包含可應用於系統

的一組配置設置。系統的運行配置是一組當前應用的設置，可能安全也可

能不安全。在這種情況下，Allie 只選擇超過無效登錄閾值的記錄，這就

是一個裁剪示例。她沒有使用統計技術來選擇記錄子集，因此這不是抽樣

示例。

**問題 43**

tb787631.CISSPPT3E.c07.086

艾倫正在評估在他的網絡安全計劃中使用機器學習和人工智能的潛力。以下哪項活動最有可能從這項技術中受益？

A. 入侵檢測
B. 賬戶配置
C. 防火牆規則修改
D. 媒體消毒

您回答錯誤。

雖然任何網絡安全活動都有可能受益於機器學習和人工智能功能，但這項

技術在用於模式檢測和異常檢測問題時確實大放異彩。這是入侵檢測系統

執行的活動類型，因此，該系統將從 ML/AI 技術的使用中受益最多。

**問題 44**

tb787631.CISSPPT3E.c07.058

Brian 正在為其組織的災難恢復計劃制定培訓計劃，並希望確保參與者了解災難活動何時結束。以下哪個事件標誌著災難恢復過程的完成？

A. 保障財產和生命安全

B. 在替代設施中恢復運行

C. 恢復主要設施的運作

D. 撤下急救人員

你回答正確！

災難恢復過程的最終目標是恢復主要設施的正常業務運營。列出的所有其

他操作都可能在災難恢復過程中發生，但直到組織在其主要設施中再次正

常運行後，該過程才算完成。

**問題 45**

tb787631.CISSPPT3E.c07.053

作為業務連續性計劃 (BCP) 工作的一部分，您正在努力評估某個地區的洪水風險。您查閱了聯邦緊急事務管理局 (FEMA) 的洪水地圖。根據這些地圖，該地區位於 200 年一遇的洪氾區內。該地區洪水的年化發生率 (ARO) 是多少？

答：200

B、0.01

C.0.02

D、0.005

你回答正確！

年化發生率 (ARO) 是事件每年發生的預期次數。對於 200 年一遇的洪氾

區，規劃者應該預計每 200 年發生一次洪水。這相當於任何給定年份發

生洪水的可能性為 1/200，或每年發生 0.005 次洪水。

**問題 46**

tb787631.CISSPPT3E.c07.015

Gary 和他的團隊應該多久檢查一次用戶對敏感系統的特權訪問權限？（選擇所有符合條件的。）

A. 定期

B. 當用戶離開組織時

C. 當用戶改變角色時

D、每天

你回答正確！

特權訪問審查是組織安全計劃中最關鍵的組成部分之一，因為它們確保只

有授權用戶才能訪問以執行最敏感的操作。它們應該在具有特權訪問權限

的用戶離開組織或更改角色時以及定期、重複發生時發生。但是，期望每

天進行這些耗時的審查是不合理的。

## 問題 47

tb787631.CISSPPT3E.c07.082

Roger 最近在一家公司接受了一個安全專家的新職位，該公司在 IaaS 環境中運行其整個 IT 基礎設施。以下哪一項最有可能是羅傑公司的責任？

A.配置網絡防火牆

B. 應用管理程序更新

C. 修補操作系統

D. 處理前擦拭驅動器

您回答錯誤。

在基礎架構即服務環境中，供應商負責與硬件和網絡相關的職責。其中包括配置網絡防火牆、維護管理程序和管理物理設備。客戶保留在其虛擬機實例上修補操作系統的責任。

## 問題 48

tb787631.CISSPPT3E.c07.093

Quigley Computing 定期將全國各地的備份數據磁帶運送到二級設施。這些磁帶包含機密信息。Quigley 可以用來保護這些磁帶的最重要的安全控制是什麼？

A. 上鎖的集裝箱

B. 私人快遞員

C、數據加密

D. 媒體輪換

你回答正確！

Quigley 可能會選擇使用這些安全控制中的任何一個或全部，但數據加密是迄今為止最重要的控制。它保護存儲在磁帶上的數據的機密性，這些數據在兩個安全位置之間傳輸時最容易被盜。

## 問題 49

tb787631.CISSPPT3E.c07.054

在大多數防禦嚴密的組織中，以下哪一個人對安全構成最大風險？

A. 政治活動家
B. 惡意內幕
C. 腳本小子
D. 刺激攻擊者

您回答錯誤。

雖然所有懷有惡意的黑客都會對組織構成風險，但惡意內部人員對安全構成的風險最大，因為他們可能擁有對敏感系統的合法訪問權限，這些系統可能被用作攻擊的啟動點。其他攻擊者並沒有從這個優勢開始。

## 第 50 題

tb787631.CISSPPT3E.c07.079

Hunter 正在審查其組織的監控策略並確定他們可能部署的新技術。他的評估表明，該公司在監控端點設備上的員工活動方面做得不夠。以下哪一項技術最能滿足他的需求？

A、EDR

B、IPS

C、入侵檢測系統

D、UEBA

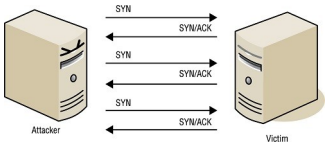
你回答正確！

所有這些技術都有可能監控端點設備上的用戶行為。正確回答這個問題的關鍵是意識到對用戶的重視。入侵檢測和防禦系統 (IDS/IPS) 專注於網絡和主機行為。端點檢測和響應 (EDR) 系統專注於端點設備。用戶和實體行為分析 (UEBA) 解決方案以用戶為中心，因此是滿足 Hunter 要求的最佳方式。

## 問題 51

tb787631.CISSPPT3E.c07.047

Evan 檢測到對其組織中服務器的攻擊，並檢查了一系列數據包上的 TCP 標誌，如下圖所示。最有可能發生什麼類型的攻擊？




A. SYN 泛洪

B. 平洪水

C.藍精靈

D. 碎片

你回答正確！

在 SYN Flood 攻擊中，攻擊者向系統發送大量 SYN 數據包，但不響應 SYN/ACK 數據包，試圖用半開連接淹沒被攻擊系統的連接狀態表。

**問題 52**

tb787631.CISSPPT3E.c07.070

Fran 正在考慮為她的銀行製定新的人力資源政策，以防止欺詐。她計劃實施強制休假政策。通常認為強制休假的最短有效長度是多少？

A、兩天

B、四天

C、一周

D、一個月

你回答正確！

大多數安全專家建議至少休假一周，最好是兩週，以防止欺詐。這個想法是，在員工離開並且沒有永久掩蓋所需的訪問權限期間，將發現欺詐計劃。

**問題 53**

tb787631.CISSPPT3E.c07.004

當愛麗絲公司的一名員工尋求支持時，她使用了公司同意在員工被迫執行某項操作時使用的代碼字。這個場景叫什麼？

A. 社會工程學
B. 脅迫
C、不可抗力
D、斯德哥爾摩綜合症

您回答錯誤。

脅迫，或受到暴力或其他限制的威脅，是銀行、珠寶店或攻擊者可能試圖強迫員工執行操作的其他組織等組織關注的問題。預計會發生這種情況的組織通常會使用脅迫密碼，讓其他人知道他們正在執行受到威脅的行動。

**問題 54**

tb787631.CISSPPT3E.c07.019

海倫的任務是在她的組織中實施安全控制，這些安全控制可能被用來阻止欺詐性的內部人員活動。以下哪一項機制對她的工作最無用？

A. 崗位輪換

B. 強制休假

C. 事件響應

D.兩人控制

你回答正確！

工作輪換和強制休假通過增加被發現的可能性來阻止欺詐。兩人控制通過要求兩名員工之間的勾結來阻止欺詐。事件響應通常不作為威懾機制。

**問題 55**

tb787631.CISSPPT3E.c07.064

請參考以下場景：

- Ann 是一家中型企業的安全專家，通常為她的組織處理日誌分析和安全監控任務。她的職責之一是監控來自組織的入侵檢測系統的警報。該系統通常每天會生成幾十條警報，經過她的調查，其中許多警報都是誤報。
- 今天早上，入侵檢測系統發出警報，因為網絡開始接收異常大量的入站流量。Ann 收到此警報並開始調查流量的來源。

Ann 繼續調查並意識到生成警報的流量是端口 53 上異常大量的入站 UDP 流量。什麼服務通常使用此端口？

A、DNS

B、SSH/SCP

C、SSL/TLS

D、HTTP

你回答正確！

DNS 流量通常使用端口 53 進行 TCP 和 UDP 通信。SSH 和 SCP 使用

TCP 端口 22。SSL 和 TLS 沒有分配給它們的端口，但通常用於端口

443 上的 HTTPS 流量。通過 HTTP 的未加密 Web 流量通常使用端口

80。

## 問題 56

tb787631.CISSPPT3E.c07.089

達西是一名計算機安全專家，正在協助起訴一名黑客。檢察官要求達西在法庭上就她認為案件中的日誌和其他記錄是否表明存在黑客企圖提供證詞。達西被要求提供什麼類型的證據？

A. 專家意見

B. 直接證據

C. 真實證據

D. 書面證據

您回答錯誤。

專家意見證據允許個人根據證據中的事實和他們的個人知識提出意見。僅

當法院接受證人為特定領域的專家時，才可提供專家意見證據。直接證據

是指證人就他們的直接觀察作證。真實證據包括作為證據帶入法庭的有形

物品。書面證據包括在法庭上用作證據的書面記錄。

## 問題 57

tb787631.CISSPPT3E.c07.081

Dylan 認為他環境中的數據庫服務器受到了 SQL 注入攻擊的破壞。在攻擊的補救階段，迪倫最有可能採取以下哪一項行動？

A. 從備份重建數據庫

B. 向 Web 應用程序添加輸入驗證

C. 查看防火牆日誌

D. 查看數據庫日誌

您回答錯誤。

補救活動旨在解決導致事件的問題。在這種情況下，這是一個對 SQL 注

入攻擊開放的 Web 應用程序。添加輸入驗證旨在修復此漏洞。重建數據

庫是一種恢復操作，而查看日誌是檢測和響應工作的一部分。

## 問題 58

tb787631.CISSPPT3E.c07.095

Gavin 是他所在組織的災難恢復團隊負責人，該組織目前正處於對客戶造成嚴重影響的事件的響應階段。加文剛剛接到記者打來的電話，詢問有關根本原因的詳細信息和估計的恢復時間。Gavin 隨時掌握這些信息。他應該怎麼做？

A. 向報告者提供信息。

B. 要求幾分鐘來收集信息並回電。

C. 將此事提交給公共關係部門。

D. 拒絕提供任何信息。

你回答正確！

災難恢復團隊應始終將媒體查詢轉給公共關係團隊，以確保協調一致的響應。他們不應試圖自己回答問題。

## 問題 59

tb787631.CISSPPT3E.c07.034

什麼術語用於描述創建新帳戶時分配給用戶的默認權限集？

A.聚合

B.傳遞性

C. 基線

D. 權利

你回答正確！

權利是指首次提供帳戶時授予用戶的特權。

**問題 60**

tb787631.CISSPPT3E.c07.062

在事件響應過程的哪個階段，管理員會採取行動來限制事件的影響或範圍？

A、檢測

B. 回應

C. 緩解

D. 恢復

你回答正確！

事件響應的緩解階段側重於可以遏制事件期間造成的損害的行動。這包括

限制事件的範圍和/或有效性。檢測階段識別事件正在發生。響應階段包

括為組建團隊和對事件進行分類而採取的步驟。恢復階段恢復正常操作。

**問題 61**

tb787631.CISSPPT3E.c07.090

以下哪一項技術不常用於從磁帶中刪除不需要的殘留數據？

A. 物理破壞

B、消磁

C.覆蓋

D. 重新格式化

您回答錯誤。

根據 NIST 媒體消毒指南，清除磁帶的標準方法是用非敏感數據覆蓋磁帶、消磁以及通過切碎或焚燒進行物理銷毀。重新格式化磁帶不會刪除殘留數據。

## 第 62 題

tb787631.CISSPPT3E.c07.030

Beth 正在創建一個新的網絡安全事件響應團隊 (CSIRT)，並希望確定合適的團隊成員。她通常會包括以下哪些群體？（選擇所有符合條件的。）

一、信息安全

B. 執法

C、高級管理人員

D. 公共事務

你回答正確！

CSIRT 代表通常至少包括高級管理人員、信息安全專業人員、法定代表 、

公共事務人員和工程/技術人員的代表。執法人員不會被包括在這樣一個

團隊中，只有在必要時才會被徵求意見。

**問題 63**

tb787631.CISSPPT3E.c07.006

Lauren 希望確保她的用戶只運行她的組織批准的軟件。她應該部署什麼技術？

A. 黑名單

B、配置管理

C. 白名單

D. 灰名單

你回答正確！

允許的應用程序白名單將確保 Lauren 的用戶只能運行她預先批准的應用

程序。黑名單將要求她維護一份她不想允許的每個應用程序的列表，這幾

乎是一項不可能完成的任務。灰名單不是一種技術選項，配置管理可用於

確保正確的應用程序在 PC 上，但通常不能直接阻止用戶運行不需要的

應用程序或程序。

## 第 64 題

tb787631.CISSPPT3E.c07.052

下圖中使用了什麼技術來保護知識產權？


A.隱寫術

B、裁剪

C、抽樣

D. 水印

你回答正確！

該圖像清楚地包含美國地質調查局 (USGS) 的水印，確保任何看到該圖

像的人都知道它的來源。無法通過查看圖像來判斷是否使用了隱寫術。採

樣和裁剪是數據分析技術，不用於保護圖像。

## 問題 65

tb787631.CISSPPT3E.c07.091

Sally 正在構建一個新服務器以用於她的環境，併計劃實施 RAID 級別 1 作為存儲可用性控制。實施此方法她需要的最少物理硬盤數量是多少？

A、一個

B、兩個

C、三

D、五

你回答正確！

RAID 級別 1，也稱為磁盤鏡像，使用包含相同信息的兩個磁盤。如果一個磁盤發生故障，另一個包含系統繼續運行所需的數據。

**第 66 題**

tb787631.CISSPPT3E.c07.003

Tim 正在為其組織配置特權帳戶管理解決方案。以下哪一項不是應該自動發送到超級用戶操作日誌的特權管理活動？

A. 清除日誌條目

B. 從備份中恢復系統

C. 登錄工作站

D. 管理用戶賬戶

您回答錯誤。

雖然大多數組織都希望記錄登錄到工作站的嘗試，但這不被視為特權管理

活動，並且會通過正常的日誌記錄過程。

## 問題 67

tb787631.CISSPPT3E.c07.046

Connor 的公司最近遭受了一次拒絕服務攻擊，Connor 認為該攻擊來自內部來源。如果屬實，公司經歷過什麼類型的事件？

A. 間諜活動
B. 違反保密規定
C. 破壞
D. 違反誠信

您回答錯誤。

由內部人員（例如員工）對組織實施的攻擊稱為破壞活動。間諜和機密洩

露涉及竊取敏感信息，據稱在本案中並未發生此類事件。完整性破壞涉及

未經授權的信息修改，本場景中未對此進行描述。

## 第 68 題

tb787631.CISSPPT3E.c07.097

Barry 是一家組織的首席信息官，該組織最近遇到了嚴重的運營問題，需要啟動災難恢復計劃。他想召開一次吸取教訓的會議來回顧這一事件。誰將是本次會議的最佳主持人？

A. Barry，擔任首席信息官

B、首席信息安全官

C. 災備組組長

D. 外部顧問

您回答錯誤。

Barry 應該招募一名獨立的主持人來促進會議。有一個沒有直接參與工作的版主鼓勵誠實和開放的反饋。雖然沒有必要使用外部顧問，但他們可以輕鬆擔任此角色。雖然也可以找到合格的內部員工來填補這個職位，但不應是參與事件響應工作或在計劃中有主要利益的人，例如 Barry、CISO 或 DR 團隊負責人.

**第 69 題**

tb787631.CISSPPT3E.c07.069

以下哪一種工具為組織提供了最高級別的保護，以防止軟件供應商倒閉？

A. 服務水平協議

B. 託管協議

C. 互助協議

D. PCI DSS 合規協議

你回答正確！

軟件託管協議將軟件包的源代碼副本交到獨立的第三方手中，如果供應商

停止業務運營，第三方會將代碼移交給客戶。如果供應商倒閉，服務水平

協議、互助協議和合規協議都會失去部分或全部效力。

**第 70 題**

tb787631.CISSPPT3E.c07.066

既然 Ann 知道發生了違反其組織安全策略的攻擊，那麼哪個術語最能描述 Ann 組織中發生的情況？

A. 安全事件

B. 安全事件

C. 安全事件

D. 安全入侵

你回答正確！

現在 Ann 懷疑她的組織受到攻擊，她有足夠的證據來宣布安全事件。正

在進行的攻擊似乎破壞了她網絡的可用性，符合安全事件的標準之一。這

是一個超越安全事件的升級，但沒有達到入侵的級別，因為沒有證據表明

攻擊者甚至試圖訪問 Ann 網絡上的系統。安全事件不是事件處理中常用

的術語。

## 第 71 題

tb787631.CISSPPT3E.c07.033

Scott 負責處理從他公司的 SAN 中取出的報廢磁盤驅動器。如果 SAN 上的數據被他的組織認為是高度敏感的，他應該避免以下哪個選項？

A. 從物理上摧毀它們。

B. 與需要適當處置並提供認證流程的 SAN 供應商簽訂合同。

C. 在離開組織之前重新格式化每個驅動器。

D. 使用像 DBAN 這樣的安全擦除工具。

您回答錯誤。

物理銷毀、適當的認證合同和安全擦除都是合理的選擇。在每種情況下，

都應進行仔細的盤點和檢查，以確保正確處理每個驅動器。重新格式化驅

動器可能會留下殘留數據，對於包含敏感數據的驅動器來說，這成為一個

糟糕的數據生命週期選擇。

## 第 72 題

tb787631.CISSPPT3E.c07.007

Colin 負責管理其組織對網絡安全欺騙技術的使用。他應該在蜜罐系統上使用以下哪一項來消耗攻擊者的時間，同時提醒管理員？

A.蜜網

B. 偽法律

C. 警告橫幅

D.暗網

你回答正確！

偽缺陷是系統中可能會分散攻擊者註意力的虛假漏洞。蜜網是一個由多個

蜜罐組成的網絡，它為入侵者創造了一個更複雜的環境來探索，而不是科

林可以在蜜罐上使用的功能。暗網是一段未使用的網絡地址空間，應該

沒有網絡活動，因此可以很容易地用於監視非法活動。警告標語是一種合

法工具，用於通知入侵者他們無權訪問系統。

## 第 73 題

tb787631.CISSPPT3E.c07.076

什麼類型的災難恢復測試激活備用處理設施並使用它來進行交易，但保持主站點正常運行？

A. 全中斷測試

B、平行測試

C. 清單審查

D. 桌面練習

你回答正確！

在並行測試期間，團隊實際上激活了災難恢復站點以進行測試，但主站點仍保持運行。在全面中斷測試期間，團隊會關閉主站點並確認災難恢復站點能夠處理常規操作。完全中斷測試是最徹底的測試，但也是最具破壞性的。清單審查是破壞性最小的災難恢復測試類型。在清單審查期間，團隊成員各自審查他們自己的災難恢復清單的內容並提出任何必要的更改。在桌面練習中，團隊成員聚集在一起，在不對信息系統進行任何更改的情況下演練一個場景。

**第 74 題**

tb787631.CISSPPT3E.c07.029

Harold 最近完成了對安全事件的事後審查。接下來他應該準備什麼文件？

A. 經驗教訓文件

B. 風險評估

C. 補救清單

D. 緩解清單

你回答正確！

在事後回顧後，通常會創建一份經驗教訓文件並將其分發給相關方，以確

保參與事件的人員和可能從知識中受益的其他人知道他們可以做些什麼來

防止未來出現問題並改進響應發生的事件。

**第 75 題**

tb787631.CISSPPT3E.c07.049

以下哪項通常被歸類為零日攻擊？（選擇所有符合條件的。）

A. 剛接觸黑客世界的攻擊者

B. 在數據表中放置日期 00/00/0000 的數據庫攻擊，試圖利用業務邏輯中的缺陷

C. 安全社區以前不知道的攻擊

D. 將操作系統日期和時間設置為 00/00/0000 和 00:00:00 的攻擊

你回答正確！

零日攻擊是安全社區以前不知道的攻擊，因此沒有可用的補丁。這些是特別危險的攻擊，因為在解決方案可用之前它們可能非常有效。此處描述的其他攻擊都是已知的攻擊，不會被歸類為零日事件。

## 第 76 題

tb787631.CISSPPT3E.c07.045

Roland 是一個組織的物理安全專家，該組織擁有大量昂貴的實驗室設備，這些設備經常在設施中移動。以下哪一項技術能夠以經濟有效的方式提供最自動化的庫存控制流程？

A.IPS

B、WiFi

C、射頻識別

D、以太網

你回答正確！

射頻識別 (RFID) 技術是跟踪設施周圍物品的一種經濟高效的方法。雖然 WiFi 可用於相同的目的，但實施起來要昂貴得多。

## 第 77 題

tb787631.CISSPPT3E.c07.022

Susan 公司的員工經常出差到世界各地，工作時需要連接到公司係統。蘇珊認為，由於她的公司正在開發的技術，這些用戶可能成為企業間諜活動的目標，並希望在向國際旅行者提供的安全培訓中包含建議。蘇珊應該建議他們在旅行時採用什麼做法來連接網絡？

A. 只連接到公共 WiFi。

B. 對所有連接使用 VPN。

C. 只使用支持 TLS 的網站。

D. 旅行時不要連接網絡。

你回答正確！

雖然告訴她的員工不要連接到任何網絡可能很誘人，但 Susan 知道他們需要連接才能完成工作。使用 VPN 將他們的筆記本電腦和移動設備連接到受信任的網絡並確保所有流量都通過 VPN 傳輸是她保護互聯網使用的最佳選擇。Susan 可能還想確保他們帶走不包含敏感信息或文件的“乾淨”筆記本電腦和設備，並確保這些系統在他們返回時被完全擦除和審查。

**第 78 題**

tb787631.CISSPPT3E.c07.063

請參考以下場景：

- Ann 是一家中型企業的安全專家，通常為她的組織處理日誌分析和安全監控任務。她的職責之一是監控來自組織的入侵檢測系統的警報。該系統通常每天會生成幾十條警報，經過她的調查，其中許多警報都是誤報。

- 今天早上，入侵檢測系統發出警報，因為網絡開始接收異常大量的入站流量。Ann 收到此警報並開始調查流量的來源。

在事件響應過程的這一點上，哪個術語最能描述 Ann 的組織中發生的情況？

A. 安全事件

B. 安全事件

C. 安全事件

D. 安全入侵

你回答正確！

在此過程中，Ann 沒有理由相信發生了任何實際的安全危害或策略違規，因此這種情況不符合安全事件或入侵的標準。相反，入侵檢測系統生成的警報只是一個需要進一步調查的安全事件。安全事件不是事件處理中常用的術語。

**第 79 題**

tb787631.CISSPPT3E.c07.037

Richard 在其組織的網絡上遇到網絡服務質量問題。主要症狀是數據包從源到目的地的傳輸時間總是太長。什麼術語描述了 Richard 面臨的問題？

A.抖動

B、丟包

C、干擾

D. 延遲

你回答正確！

延遲是數據包從源到目的地的傳輸延遲。抖動是不同數據包延遲的變化。

數據包丟失是指數據包在傳輸過程中丟失，需要重新傳輸。干擾是破壞數

據包內容的電噪聲或其他干擾。

**問題 80**

tb787631.CISSPPT3E.c07.077

在事件響應過程的哪個階段，分析師會收到入侵檢測系統警報並驗證其準確性？

一個回應

B. 緩解

C、檢測

D. 報告

您回答錯誤。

警報的接收及其準確性的驗證都發生在事件響應過程的檢測階段。

**問題 81**

tb787631.CISSPPT3E.c07.025

Glenda 想要進行災難恢復測試，並且正在尋求一種測試，該測試將允許在不中斷正常信息系統活動的情況下審查計劃，並儘可能減少承諾的時間。她應該選擇什麼類型的測試？

A. 桌面練習

B、平行測試

C. 全中斷測試

D. 清單審查

你回答正確！

清單審查是破壞性最小的災難恢復測試類型。在清單審查期間，團隊成員

各自審查他們自己的災難恢復清單的內容並提出任何必要的更改。在桌面

練習中，團隊成員聚集在一起，在不對信息系統進行任何更改的情況下演

練一個場景。在並行測試期間，團隊實際上激活了災難恢復站點以進行測

試，但主站點仍保持運行。在全面中斷測試期間，團隊會關閉主站點並確

認災難恢復站點能夠處理常規操作。完全中斷測試是最徹底的測試，但也

是最具破壞性的。

**問題 82**

tb787631.CISSPPT3E.c07.061

Carla 在她的公司工作了 15 年，擔任過各種不同的職位。每次她更換職位時，她都會獲得與該職位相關的新特權，但從未剝奪過任何特權。什麼概念描述了她積累的特權集？

A. 權利

B、聚合

C.傳遞性

D. 隔離

你回答正確！

Carla 的帳戶經歷了聚合，其中特權隨著時間的推移而累積。這種情況也

稱為特權蔓延，可能違反了最小特權原則。

**問題 83**

tb787631.CISSPPT3E.c07.040

Anne 希望收集有關安全設置的信息，並通過收集有關遍布其公司的一組 Windows 10 工作站的數據來構建其組織資產的總體視圖。哪種 Windows 工具最適合此類配置管理任務？

A.SCCM

B. 組策略

C、SCOM

D. 自定義 PowerShell 腳本

你回答正確！

System Center Configuration Manager (SCCM) 提供此功能，旨在讓管理員評估 Windows 工作站和服務器的配置狀態，並提供資產管理數據。

SCOM 主要用於監控健康和性能，組策略可用於各種任務，包括部署設置和軟件，自定義 PowerShell 腳本可以執行此操作，但配置檢查不需要。

**問題 84**

tb787631.CISSPPT3E.c07.021

Tom 正在響應最近的安全事件，並正在尋找有關最近修改系統安全設置的審批流程的信息。他最有可能在哪裡找到這些信息？

A.變更日誌

B、系統日誌

C. 安全日誌

D. 申請日誌

您回答錯誤。

變更日誌包含有關批准的變更和變更管理流程的信息。雖然其他日誌可能

包含有關變更影響的詳細信息，但變更管理的審計跟踪可以在變更日誌中

找到。

**問題 85**

tb787631.CISSPPT3E.c07.009

John 通過他的雲基礎架構作為服務提供商，使用世界各地的負載均衡器將他的網站部署到多個區域。他使用的可用性概念是什麼？

A. 多個加工點

B. 熱點站點

C. 寒冷地區

D、蜜網

你回答正確！

John 的設計提供了多個處理站點，將負載分配到多個區域。這不僅提供

了業務連續性和災難恢復功能，而且還意味著他的設計將更能抵禦拒絕服

務攻擊。

## 問題 86

tb787631.CISSPPT3E.c07.098

布倫特正在審查在持續斷電的情況下保護他的組織的控制措施。以下哪一種解決方案最能滿足他的需求？

A. 冗餘服務器

B、不間斷電源（UPS）

C、發電機

D、RAID

你回答正確！

發電機能夠在斷電的情況下持續提供備用電源，但需要時間才能啟動。不間斷電源 (UPS) 可在短時間內提供即時的電池驅動電源，以彌補瞬時斷電，但無法彌補持續斷電。RAID 和冗餘服務器是高可用性控制，但不涵蓋斷電情況。

## 問題 87

tb787631.CISSPPT3E.c07.002

Joe 是 ERP 系統的安全管理員。他正準備為幾個新員工創建帳戶。他在創建帳戶時應該為所有新員工提供哪些默認訪問權限？

A、只讀

B、編輯器

C、管理員

D、無法訪問

你回答正確！

在這種情況下，最小特權原則應該指導 Joe。他應該默認不應用任何訪問權限，然後為每個用戶提供必要的權限以履行其工作職責。這些用戶中的一個或多個可能需要只讀、編輯和管理員權限，但這些權限應根據業務需要分配，而不是默認分配。

**問題 88**

tb787631.CISSPPT3E.c07.026

以下哪一項不是備份磁帶循環方案的示例？

A. 祖父/父親/兒子

B、在中間相遇

C.河內塔

D. 每週六彈

你回答正確！

祖父/父/子、河內塔和每週六盒計劃都是不同的輪換備份介質的方法，可

以平衡介質的重用和數據保留問題。中間相遇是一種針對 2DES 加密的

密碼攻擊。

**問題 89**

tb787631.CISSPPT3E.c07.020

Matt 希望確保來自整個公司係統的關鍵網絡流量優先於該公司的 Web 瀏覽和社交媒體使用。他可以使用什麼技術來做到這一點？

A. VLAN
B、QoS
C、VPN
D、ISDN

你回答正確！

服務質量是路由器和其他網絡設備上的一項功能，可以確定特定網絡流量

的優先級。QoS 策略定義優先處理哪些流量，然後根據策略處理流量。

**問題 90**

tb787631.CISSPPT3E.c07.014

Gary 正準備圍繞對根加密密鑰的訪問制定控制措施，並希望應用專為非常敏感的操作設計的安全原則。他應該應用哪個原則？

A. 最小權限

B.縱深防禦

C. 默默無聞的安全

D.兩人控制

您回答錯誤。

Gary 應該遵循兩人控制的原則，要求兩個獨立的授權個人同時採取行動來訪問加密密鑰。他還應該應用最小特權和縱深防禦原則，但這些原則適用於所有操作，並不特定於敏感操作。Gary 應該避免通過模糊原則實現安全，即依賴安全機制的保密性為系統或進程提供安全。

**問題 91**

tb787631.CISSPPT3E.c07.039

以下哪一項是非自然災害的例子？

颶風

B. 洪水

C、泥石流

D、變壓器爆炸

你回答正確！

變壓器爆炸是人為電氣元件的故障。洪水、泥石流和颶風都是自然災害的例子。

## 問題 92

tb787631.CISSPPT3E.c07.048

Florian 正在為他的組織製定災難恢復計劃，他想確定特定 IT 服務在不對業務運營造成嚴重損害的情況下可能停機的時間量。Florian 在計算什麼變量？

A. 反收購行動
B、MTD
C、RPO
D、服務水平協議

您回答錯誤。

最長可容忍停機時間 (MTD) 是 IT 服務或組件可能不可用而不會對組織造成嚴重損害的最長時間。恢復時間目標 (RTO) 是指 IT 服務或組件在發生故障後恢復運行所需的時間。恢復點目標 (RPO) 確定在恢復工作期間可能丟失的最大數據量（按時間衡量）。服務級別協議 (SLA) 是記錄服務期望的書面合同。

## 問題 93

tb787631.CISSPPT3E.c07.008

Toni 響應報告系統活動緩慢的用戶的桌面。檢查來自該系統的出站網絡連接後，Toni 注意到來自該系統的大量社交媒體流量。用戶不使用社交媒體，當 Toni 檢查有問題的帳戶時，它們包含看似加密的奇怪消息。此流量最可能的原因是什麼？

A. 其他用戶正在通過用戶的計算機轉發社交媒體請求。

B. 用戶的計算機是殭屍網絡的一部分。

C. 用戶在使用社交媒體時撒謊。

D. 當她不在時，其他人正在使用用戶的計算機。

您回答錯誤。

社交媒體通常用作殭屍網絡活動的命令和控制系統。這裡最有可能的情況是用戶的計算機感染了惡意軟件並加入了殭屍網絡。這說明了異常的社交媒體流量和緩慢的系統活動。

## 問題 94

tb787631.CISSPPT3E.c07.038

喬想測試一個他懷疑可能包含惡意軟件的程序。他可以使用什麼技術在程序運行時將其隔離？

A、ASLR

B. 沙盒

C、裁剪

D、進程隔離

你回答正確！

在沙盒中運行該程序可提供安全隔離，從而防止惡意軟件影響其他應用程序或系統。如果 Joe 使用適當的儀器，他可以觀察程序做了什麼，它做了什麼改變，以及它可能嘗試的任何通信。ASLR 是一種內存位置隨機化技術，進程隔離可防止進程相互影響，但沙箱通常在這種情況下提供更大的實用性，因為它可以以更好地支持調查的方式進行檢測和管理，並且裁剪是一個經常使用的術語用於信號處理。

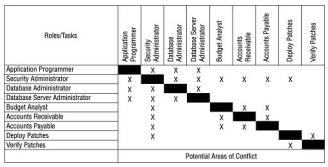
**問題 95**

tb787631.CISSPPT3E.c07.012

請參考以下場景：

- Gary 最近被當地政府機構聘為首位首席信息安全官 (CISO)。該機構最近遭遇安全漏洞，正試圖建立一個新的信息安全計劃。Gary 希望在設計此程序時應用一些安全操作的最佳實踐。

在 Gary 設計程序時，他使用此處顯示的矩陣。該矩陣最直接地幫助執行什麼信息安全原則？




A. 職責分離

B、聚合

C.兩人控制

D、縱深防禦

你回答正確！

圖中所示的矩陣稱為職責分離矩陣。它用於確保一個人不會獲得可能造成潛在衝突的兩個特權。聚合是一個術語，用於描述特權隨時間的無意累積，也稱為特權蔓延。當兩個人必須一起工作來執行一個敏感的動作時，使用兩人控制。縱深防禦是一種通用安全原則，用於描述重疊安全控制的理念。

## 問題 96

tb787631.CISSPPT3E.c07.035

以下哪種類型的協議是最正式的文件，其中包含服務提供商與客戶之間對可用性和其他性能參數的期望？

A. 服務水平協議 (SLA)

B. 業務級協議（OLA）

C. 諒解備忘錄（MOU）

D. 工作說明書 (SOW)

您回答錯誤。

服務級別協議 (SLA) 是服務提供商和客戶之間的協議，以正式的方式記

錄對可用性、性能和其他參數的期望。諒解備忘錄可能涵蓋相同的項目，

但不是正式文件。OLA 在內部服務組織之間，不涉及客戶。SOW 是描

述要執行的工作的合同的附錄。

**問題 97**

tb787631.CISSPPT3E.c07.024

在執行災難恢復計劃時，以下哪項通常被視為災難示例？（選擇所有符合條件的。）

A. 黑客事件

B. 洪水

C、火災

D. 恐怖主義

你回答正確！

災難是任何可能破壞正常 IT 操作的事件，可以是自然的也可以是人為的。

黑客攻擊和恐怖主義是人為災難的例子，而洪水和火災是自然災害的例子。

**問題 98**

tb787631.CISSPPT3E.c07.087

Timber Industries 最近與客戶發生糾紛。在與他的客戶代表會面時，客戶站起來宣稱：“沒有其他解決方案。我們將不得不把這件事告上法庭。” 然後他離開了房間。Timber Industries 何時有義務開始保存證據？

A、立即

B. 收到對方律師的訴訟通知後

C. 收到傳票後

D. 收到法院命令後

你回答正確！

只要公司認為訴訟威脅迫在眉睫，公司就有義務保存證據。該客戶的聲明“我們必須將此事告上法庭”是明顯的訴訟威脅，應觸發對任何相關文件和記錄的保存。