數字政策辦公室

資訊保安

資訊科技保安威脅管理

實務指引

第 1.1 版

2024 年 7 月

版權公告

修改記錄				
修改次數	修改詳情	經修改頁數	版本編號	日期
1	將「政府資訊科技總監辦公室」修改為「數字政策辦公室」。 在第 5.2 節更新威脅情報來源的例子。		1.1	2024 年 7 月

目錄

1 簡介

在現今互聯互通的數字化環境中，決策局／部門的資訊系統、網絡和敏感資料皆面臨日益增加的威脅。為協助決策局／部門應對複雜環境，本指引提供了全面的資訊科技保安威脅管理框架，其中包含了所需的知識和策略，以建立完善的威脅監察能力、主動檢測潛在保安漏洞，以及迅速有效地作出反應，以減少資訊科技保安威脅的影響。管理層用戶、資訊科技經理、系統管理員及其他技術與操作人員可借助該框架更了解資訊科技保安威脅管理流程，以在日益嚴峻的威脅環境中保護其數字資產。

1.1 目的

本文件展示了資訊科技保安威脅管理的總體框架，且應與其他保安文件結合使用，例如《基準資訊科技保安政策》[S17]、《資訊科技保安指引》[G3]以及相關程序（如適用）。

本實務指引旨為政府所有需要處理保安風險評估或保安審計的人員，以及為政府進行保安風險評估或保安審計的保安顧問或供應商而設。

1.2 參考標準

以下參考文件對於本文件的應用必不可少。

- 《基準資訊科技保安政策》[S17]，香港特別行政區政府
- 《資訊科技保安指引》[G3]，香港特別行政區政府
- Information technology - Security techniques - Information security management systems - Requirements (third edition), ISO/IEC 27001:2022
- Information technology - Security techniques - Code of practice for information security controls (third edition), ISO/IEC 27002:2022
- NIST SP 800-92 – Guide to Computer Security Log Management
- NIST SP 800-150 – Guide to Cyber Threat Information Sharing
- NIST SP 800-137 – Information Security Continuous Monitoring for Federal
- Information Systems and Organizations
- Guide to Cyber Threat Modelling, Cyber Security Agency of Singapore
- Cyber-threat intelligence information sharing guide, GOV.UK
- 保安風險評估及審計實務指引
- 資訊保安事故處理實務指引
- Endpoint Detection & Response: A Malware Identification Solution, IEEE Xplore. 可供查閱：https://ieeexplore.ieee.org/document/9703010

- Best endpoint detection and response solutions reviews 2024: Gartner Peer insights, Gartner. 可供查閱：https://www.gartner.com/reviews/market/endpoint-detection-and-response - solutions

1.3 定義及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用，以及以下的定義及慣用詞。

縮寫及術語	
ACL	接達控制清單
APT	進階持續性威脅
CRM	客戶關係管理
DDoS	分散式拒絕服務攻擊
DLP	資料外泄防護
DNS	域名系統
EDR	端點偵測和回應
EPP	端點保護平台
ERP	企業資源計畫
ICS	工業控制系統
IDS	入侵偵測系統
IOA	攻擊指標
IoC	入侵指標
IP	互聯網規約地址
IPS	入侵防禦系統
ITSM	資訊科技服務管理
KPI	關鍵績效指標

MTTD	平均偵測時間
MTTR	平均回應時間
NAC	網絡接達控制
NDR	網絡偵測和回應
PAM	特權接達管理
PoC	概念驗證
POS	銷售點
ROI	投資回報
SEM	保安事件管理
SIEM	保安資訊和事件管理
SIM	保安資訊管理
SOAR	保安編排、自動化和回應
SOC	保安營運中心
TCO	整體擁有成本
TIP	威脅情報平台
TTP	策略、技術和程序
UEBA	用戶和實體行為分析
URL	劃一資源定位址
VM	虛擬機器
VPN	虛擬私有網絡
WAF	網絡應用系統防火牆
XDR	擴展偵測和回應

1.4 聯絡方法

本文件由數字政策辦公室編制及備存。如有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

Lotus Notes 電郵： IT Security Team/DPO/HKSARG@DPO

CMMP 電郵： IT Security Team/DPO

2 資訊保安管理

資訊保安是關於保安控制和措施的規劃、實施和持續提升，以保護資訊資產的機密性、完整性和可用性，適用於資訊的存儲、處理或傳輸過程及其相關資訊系統中。資訊保安管理是一套有關規劃、組織、指導、控制的原則和以這些原則迅速有效地管理實體、財務、人力資源和資訊資源的應用，以確保資訊資產和資訊系統的安全。

資訊保安管理涉及一系列需要持續監測和控制的活動。這些活動包括但不限於以下的範疇：

- 保安管理框架與組織；
- 管治、風險管理和遵行要求；
- 保安操作；
- 保安事件和事故管理；
- 保安意識培訓和能力的建立；和
- 態勢感知和資訊共享。

保安管理框架與組織

決策局／部門須根據業務需要和政府保安要求，制定和實施部門資訊保安政策、標準、指引和程序。

決策局／部門亦須界定資訊保安的組織架構，並須向有關各方就保安的責任及問責提供清晰的定義和適當的分配。

管治、風險管理和遵行要求

決策局／部門須採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。

決策局／部門須定期和在必要時對資訊系統和生產應用系統進行保安風險評估，以識別與保安漏洞相關的風險和後果，並為建立具成本效益的保安計畫和實施適當的安全保護和保障措施提供依據。

決策局／部門亦須定期對資訊系統進行保安審計，以確保當前的保安措施符合部門資訊保安政策、標準和其他合約或法律上的要求。

保安操作

為保護資訊資產和資訊系統，決策局／部門應根據業務需要實施全面的保安措施，涵蓋業務上不同的技術領域，並在日常操作中採取「預防、偵測、應急和復原」原則。

- 預防措施避免或阻止不良事件的發生；
- 偵測措施識別不良事件的發生；
- 應急措施是指在發生不良事件或事故時，採取相應行動來遏制損害；和
- 復原措施是將資訊系統的機密性、完整性和可用性恢復到預期狀態。

保安事件和事故管理

在現實環境中，由於存在不可預見並致服務中斷的事件，故此保安事故仍可能會發生。若保安事件危及業務的連續性或引起資料保安風險，決策局／部門須啟動其常規保安事故管理計畫，以實時識別、管理、記錄和分析保安威脅、攻擊或事故。決策局／部門亦應準備與有關各方適當地溝通，透過分享對有關保安風險的應急以消除不信任或不必要的猜測。當制定保安事故管理計畫時，決策局／部門應規劃和準備適當的資源，並制定相關程序，以配合必要的跟進調查。

保安意識培訓和能力建立

因為資訊保安是每個人的責任，所以決策局／部門應不斷提升機構內的資訊保安意識，透過培訓及教育，確保有關各方了解保安風險，遵守保安規定和要求，並採取資訊保安的良好作業模式。

態勢感知和資訊共享

因應網絡威脅形勢不斷變化，決策局／部門亦應不斷關注由保安行業和政府電腦保安事故協調中心發佈的現時保安漏洞訊息、威脅警報和重要通知。應將即將或已經發生具威脅的保安警報傳達及分享給決策局／部門內的負責同事，以便採取及時的應對措施來緩解風險。

決策局／部門可以利用威脅情報平台接收和分享保安事務、保安漏洞和網絡威脅情報的訊息。

所有人員亦可以通過參與保安演習和參加研討會、展示會或瀏覽載有保安情報資訊和一般保安資訊（例如網絡安全資訊站、資訊安全網）的專頁來提高保安意識。

3 資訊科技保安威脅管理

3.1 資訊科技保安威脅管理簡介及其重要性

資訊科技保安威脅是指通過未經授權的接達、破壞、披露、修改資訊或拒絕服務使該組織的營運、資產、聲譽或人員有可能造成任何負面影響的情況或事件。該等威脅在數字化環境下日趨普遍，為世界各國政府和組織帶來重大風險。

為有效應變此等威脅，決策局／部門需要了解與資訊科技保安威脅管理相關的各種要素。威脅者，即構成威脅的個人或團體，在此情況下發揮著至關重要的角色。此外，決策局／部門需要獲取威脅資訊，包括指標、策略、技術和程序、保安警報、威脅情報報告和工具設定。這些資訊有助決策局／部門保護自身並檢測威脅者的活動。

在資訊科技保安方面，威脅與風險、漏洞和影響密切相關。

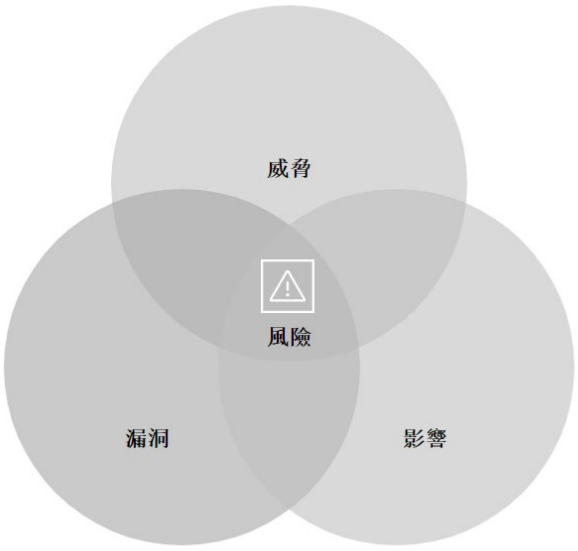

圖 3.1 風險被定義為威脅、漏洞和影響的組合

威脅者利用決策局／部門系統或網絡的漏洞，可造成各種負面後果。決策局／部門需要識別和評估威脅、漏洞和潛在影響，以有效管理和減低風險，保障其數字資產的機密性、完整性和可用性。請參閱《**資訊科技保安風險管理實務指引**》和《**保安風險評估及審計實務指引**》以了解更多詳情。

換言之，管理威脅可為管理風險奠定基礎。資訊科技保安威脅管理包括以一種全面的方式減低和應變數字化環境中的資訊科技保安威脅。通過構建穩健的資訊科技保安威脅管理能力，決策局／部門可持續監控威脅環境、迅速識別潛在攻擊、推行控制措施減少漏洞，並迅速遏制威脅。這增強了態勢感知能力、降低風險，並能夠敏捷應對潛在的資訊科技保安事故。

有效的資訊科技保安威脅管理對於建立抵禦資訊科技保安攻擊的復原能力、保護敏感資料和維護公眾信任至關重要。為了建立情報導向和風險爲本的資訊科技保安威脅管理方法，決策局／部門需充分了解其面臨的威脅。基於此理解，決策局／部門能夠評估其防禦措施的成熟程度，並判斷發生保安事故的可能性。同時使決策局／部門有效地評估風險並排列先後次序，從而分配其保安資源。

資訊科技保安威脅分析可分為三個層面：部門層面、系統層面，及設備或應用層面。每個層面都提供了關於威脅分析不同方面的見解，有助決策局／部門確定整體威脅管理方向。

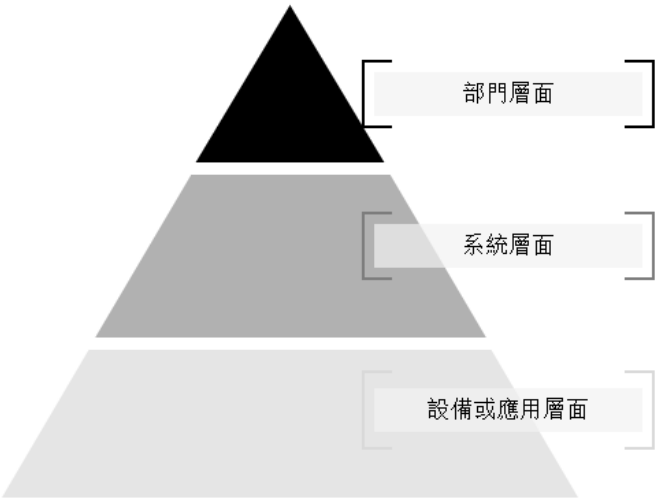

圖 3.2 威脅分析的層級

部門層面

部門層面的威脅分析涉及分析部門層面的情報來源和趨勢，重點關注於外部因素，例如地緣政治。決策局／部門會根據其入侵前後的動機和行動進行敵方剖析。這一層的分析通常從宏觀角度進行，供管理層使用。

系統層面

系統層面的威脅分析考慮系統的架構、關係和行為。這涉及對環境中的資產、數據流通和界線建立模型，以判斷與系統相關的威脅事件。有關此層面威脅分析的詳情，請參閱《**保安風險評估及審計實務指引**》。

設備或應用層面

設備或應用層面是威脅分析中最精細的層面。這涉及威脅搜尋、日誌關聯、詳細資料分類、進階分析和試探技術等活動。此層面的分析旨在識別和解決對已公佈漏洞詳細的規避和利用。

通過推行資訊科技保安威脅管理，決策局／部門能夠通過有系統的框架更了解威脅，並主動採取措施有效地預防、檢測和應變威脅。推行資訊科技保安威脅管理有數項主要優點：

- ***保護政府敏感資料。***決策局／部門通常需要處理敏感資料，包括市民記錄、財務資訊和機密文件。保護這些資訊對維持公眾的信任和信心至關重要。通過有效的威脅管理實踐，決策局／部門可建立完善的保安措施，例如接達控制、加密和保護資料存儲，以防止未經授權的接達和資料外泄。

- ***確保必要服務的連續性。***任何關鍵系統的中斷或入侵都可造成嚴重後果，阻礙其向公眾提供重要服務。決策局／部門可以通過主動管理資訊科技保安威脅，識別潛在漏洞，實施減低措施，並建立事故應變計劃，使決策局／部門迅速檢測和應對保安事故，降低對必要服務的影響並確保其服務提供不受干擾。

- ***致力於維護監管要求和國際標準。***規管框架到位以保護個人資料、確保私隱並維護資訊科技保安。遵守這些法規和標準對決策局／部門履行法律義務和維持公眾信任至關重要。通過實施資訊科技保安威脅管理措施，決策局／部門可以展示其致力於保護敏感資料、遵守相關保護資料的法例，並維持高水準的資訊科技保安。

3.2 資訊科技保安威脅管理框架

為建立一致且有效的資訊科技保安威脅管理方法，各決策局／部門應採用標準化的資訊科技保安威脅管理框架。此框架與國際良好作業模式和行業標準保持一致，為管理資訊科技保安威脅和確保全面的資訊科技保安提供有系統的方法。

採用標準化框架可為決策局／部門提供共同基礎，以就管理資訊科技保安威脅開展交流和協作，並加強決策局／部門與數字政策辦公室之間的協調和資訊共享。

資訊科技保安威脅管理分為六個主要階段（如下文概述），且每個階段的工作在相應的章節中有更詳細的描述。

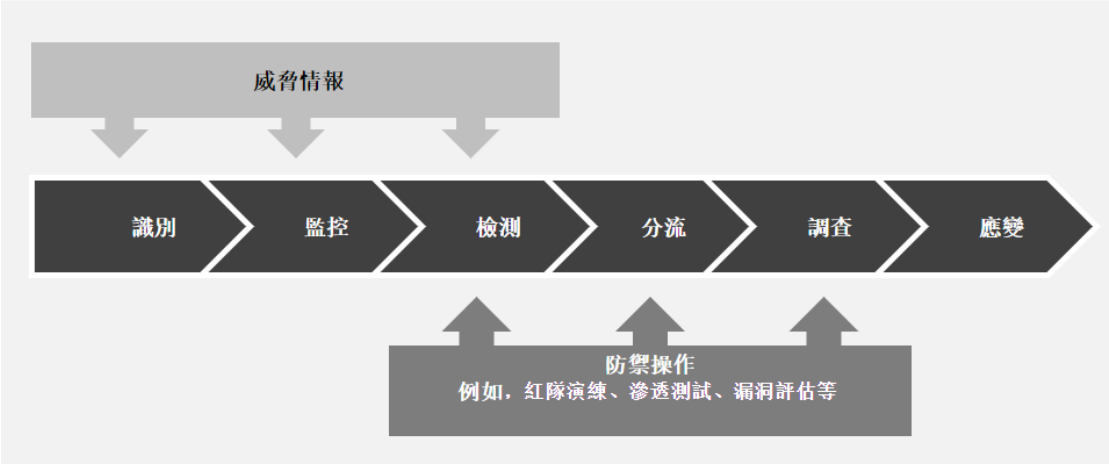

圖 3.3 資訊科技保安威脅管理框架中的主要階段

A. 識別（部門與系統層面）（第 4 節）

此階段中，決策局／部門應識別可能損害資訊系統、資料、操作或聲譽的潛在威脅。這階段涉及的主要工作如下所示：

- 識別和分類相關資訊科技保安威脅
- 使用威脅情報來源和共享平台

B. 監控（設備或應用層面）（第 5 節）

此階段中，決策局／部門應持續監察網絡流量、系統日誌和保安事件。這階段涉及的主要工作如下所示：

- 設計和實施全面監控策略

C. 檢測（設備或應用層面）（第 5 節）

此階段中，決策局／部門應分析已收集的資料，如日誌文件和網絡流量，以識別可能存在保安漏洞或惡意活動的模式或異常。這階段涉及的主要工作如下所示：

- 資料收集、日誌分析和威脅情報集成
- 行為分析、異常檢測和威脅情報應用

D. 分流（設備或應用層面）（第 6 節）

一旦檢測階段得出潛在威脅警報，決策局／部門需要根據警報的嚴重程度和潛在影響對其排序和分類。此分流流程有利於有效分配資源以迅速解決關鍵威脅。分流階段的概述如下：

- 警報收集和分析
- 警報驗證
- 嚴重程度分類
- 持續監察和重複分流

E. 調查（設備或應用層面）（第 6 節）

從分流隊列中選擇警報後，決策局／部門應進行徹底調查，以確定潛在威脅的真實性及其性質。調查階段對準確評估是否存在實際攻擊方面有至關重要的作用。這階段涉及的主要工作如下所示：

- 證據收集
- 威脅分析

F. 應變（設備或應用層面）（第 7 節）

在此階段，決策局／部門應制定和執行行動和措施以應變潛在的威脅或警報，以避免其演變成真實事故，或在調查階段確認為真實事故後造成損害。主要工作可涉及：

- 遏制
- 攔截
- 修補
- 培訓

下表列出針對不同資訊系統保安等級的資訊科技保安威脅管理機制的示例。保安要求是以**累計**橫跨不同等級的資訊系統（即所有第 1 級資訊系統規定的保安要求須擴展到第 2 級和第 3 級資訊系統）。

階段	第 3 級資訊系統	第 2 級資訊系統	第 1 級資訊系統
識別	建立機制排序和監察涵蓋所有威脅組件的威脅情報來源。 分析威脅情報以生成全面的威脅摘要報告，其中包含網絡風險詳細資訊和建議措施。 利用威脅情報為決策局／部門提供風險狀況資訊，確定緩解措	威脅情報和分析的流程分配給特定群組或個人。	制定流程監察威脅情報，以識別新興的威脅。

	施的優先次序，並更新資訊科技保安架構和配置標準。 採用多種情報來源和分析技術以預測未來攻擊及識別趨勢。		
監控	建立中央保安監察流程，包括專責的 24／7 監察團隊。 建立用於監察和分析用戶行為（如互聯網協定位址、網絡使用模式、工作時間和已知設備）並提供異常活動警報的系統。	備份審計日誌到中央日誌伺服器或媒體，以防止日誌被未經授權的更改。 使用主動監察保安日誌異常行為的工具，並提供在既定參數範圍內的警報。	定期覆檢系統日誌中是否存在異常或可疑活動。 建立通過環境監察檢測異常活動的流程。
檢測	安裝自動化工具以檢測對關鍵系統文件、防火牆、入侵防禦系統、入侵偵測系統或其他保安設備未經授權的更改。 使用實時網絡監察和檢測工具。 使用可主動關聯多個來源的事件資訊並根據既定參數發送警報的工具。	建立流程以在攻擊者遍歷系統、建立立足點、竊取資訊或對資料和系統造成損害之前發現滲透跡象。 端點行為檢測能力（如端點偵測和回應解決方案）應可用於各端點（即用戶工作站、膝上電腦和伺服器）。	建立機制（如防毒警報、日誌事件警報等）以提醒保安監察功能和管理層注意潛在的攻擊。
分流	基於嚴重程度和潛在影響對威脅進行排序。		
調查	調查威脅的特性、動機和潛在影響。		
應變	開發和執行措施應變威脅。		

表 3.1 針對不同系統關鍵程度資訊科技保安威脅管理機制的示例

在資訊科技保安威脅管理流程的不同階段，可能存在不同的輸出或交付成果，如下表 3.2 所示。

階段	輸出／交付成果示例
識別	• 提供有關新興威脅、攻擊趨勢和相關保安新聞的最新資訊的威脅情報報告。 • 威脅分類，已識別威脅的完整列表。
監控	• 威脅監察目標、工具和採用的技術。
檢測	• 基於可疑活動、異常行為或已知威脅模式生成警報和事件的既定規則和閾值。
分流	• 既定機制、分類標準、程序和工作流程。
調查	• 潛在威脅調查過程的步驟、工具和技術的記錄，包括資料收集、分析和證據保存。
應變	• 既定的行動和措施以便在威脅演變成真實事故之前作出應變。

表 3.2 資訊科技保安威脅管理框架的輸出／交付成果示例

4 部門背景建立

4.1 了解威脅環境和新興趨勢

了解威脅環境和新興趨勢對決策局／部門有效管理和降低資訊科技保安風險至關重要。以下是了解威脅環境和新興趨勢的一些工作：

- ***保持了解。***定期監察和收集來源可靠的資訊，例如來自資訊科技保安新聞網站、行業報告和政府公告。訂閱相關郵寄清單、關注保安網誌，並加入專業網絡以保持了解最新的威脅和趨勢。

- ***參與威脅情報。***利用提供有關資訊科技保安威脅、漏洞和新興趨勢實時資訊的威脅情報服務或平台。此類服務集成了來自不同來源的資料，並提供可行的見解。

- ***定期進行風險評估。***通過定期建立威脅模型和風險評估以識別潛在威脅和漏洞，包括分析網絡基礎設施、系統、應用和數據資產。

- ***參與資訊共享活動。***參與資訊共享活動和政府資助的方案。這些平台有助於各決策局／部門與數字政策辦公室交換威脅情報，並使其了解其他決策局／部門所面臨的威脅。

- ***分析事故數據。***定期覆檢和分析保安事故數據。查找模式、趨勢和常見攻擊途徑。此分析可幫助決策局／部門了解威脅者採用不斷演變的策略、技術和程序。

- ***持續學習和培訓。***決策局／部門應持續提升資訊科技保安威脅管理意識，並安排培訓和教育，以確保有關各方了解風險、遵守保安法規和要求，並符合保安良好作業模式。

鑒於資訊科技保安威脅持續演變的性質，各決策局／部門應積極參與上述活動以收集和交流見解、威脅指標和良好作業模式。這種協作方法加強了對攻擊的整體防禦能力，並能夠及時識別和應變新興威脅，包括以下優勢：

- ***共享態勢感知。***資訊共享利用共享夥伴的集體知識和經驗增強了各決策局／部門的防禦能力，從而提高了整個社區的保安。

- ***改善保安態勢。***共享威脅資訊使得決策局／部門能更了解威脅環境，促使知情的資訊科技保安實務、識別受影響的系統、實施保護措施，以及更有效的事故應對和復原能力。

- ***增強認知成熟度。***共享和分析看似無關的觀察結果可以豐富資訊、增強指標和了解威脅者的策略、技術和程序，從而提高整體理解和應對能力。

- ***提升防禦敏捷性。***共享資訊可讓決策局／部門了解不斷演變的威脅者策略、技術和程序，從而實現快速的檢測和應變。這加快了操作節奏，降低了攻擊成功的可能性，並且由於威脅者需要被迫建立新的策略、技術和程序，為其造成了成本劣勢。

決策局／部門可能面對各種嚴重影響國家安全、公共安全及政府運作的資訊科技保安威脅。以下列出多項主要類型的威脅者：

- ***網絡罪犯。***這些個體或團體進行網絡犯罪，主要為了獲取經濟利益。常見網絡犯罪包括勒索軟件攻擊和網絡釣魚詐騙，誘騙人們進行匯款或泄露信用卡資訊、登錄憑證、知識產權或其他私人或敏感資料。

- ***國家級網路攻擊者。***國家級和有關政府頻密資助威脅者竊取敏感資料、收集機密資訊或破壞另一政府的關鍵基礎設施。這些惡意活動通常包括間諜活動或網絡戰爭，並且資金充裕，使其威脅複雜且難以檢測。

- ***黑客行動主義者。***黑客行動主義者使用黑客技術宣揚政治或社會議程，例如傳播自由言論或揭露侵犯人權的行為。黑客行動主義者認為他們正在積極影響社會變革，並認為有理由針對個人、組織或決策局／部門揭發秘密或其他敏感資料。

- ***尋求刺激者。***尋求刺激者攻擊電腦和資訊系統主要為了娛樂。一些尋求刺激者想看到自己可以竊取多少敏感資料或數據；另一些則希望使用黑客技術更了解網絡和電腦系統的運作原理。儘管他們並不總是試圖造成傷害，但尋求刺激者仍然會通過干擾網絡保安，並為未來攻擊建立途徑，而造成無意的損害。

- ***內部威脅者。***內部威脅者的意圖並不總是惡意的。有些內部威脅者因人為錯誤而損害公司，如無意間安裝惡意軟件，或遺失公司發放的設備，這些設備被網絡罪犯拾得並接達公司網絡。除此之外，內部人員的惡意損害亦存在，例如心懷不滿的員工濫用接達權限竊取資料以獲取金錢利益，或損害資料或應用以報復其晉升失敗或給予其不公平對待的上級。

- ***網絡恐怖分子。***網絡恐怖分子出於其政治或意識形態的動機發起網絡攻擊，威脅或造成暴力行為。這些網絡恐怖分子可能包括國家級網路攻擊者，以及獨立行動或代表非政府組織行事的個體。

威脅者在執行攻擊時會部署多種策略，包括但不限於以下內容：

- ***進階持續性威脅。***進階持續性威脅為複雜且有針對性的保安攻擊，通常由國家資助的威脅者，或技術高超的黑客組織執行。這些威脅涉及對政府網絡的長期隱蔽滲透，以收集敏感資料、破壞營運或進行間諜活動。

- ***勒索軟件攻擊。***勒索軟件攻擊日趨普遍，對決策局／部門構成重大威脅。攻擊者對關鍵資料進行加密，並要求公司支付贖金以換取恢復接達權限。此類攻擊可能會造成政府系統癱瘓，擾亂公共服務，並洩露敏感資料。

- ***分散式拒絕服務攻擊。***分散式拒絕服務攻擊使政府網站或網絡不堪流量重負，導致用戶無法接達。該等攻擊可能會擾亂公共服務，損害市民信任，並分散對其他入侵的注意力。

- ***社交工程和網絡釣魚。***社交工程技術，例如網絡釣魚電子郵件和欺詐電話，通常用於欺騙政府僱員，以泄露敏感資料或提供未經授權的系統接達，可能導致資料外泄、未經授權的接達或安裝惡意軟件。

- ***供應鏈攻擊。***決策局／部門依賴龐大的供應商和承包商網絡使其容易受到供應鏈攻擊。惡意威脅者可能會破解這些供應商提供的軟件或硬件，從而利用惡意軟件或後門感染政府系統。

- ***關鍵基礎設施攻擊。***決策局／部門通常負責營運和監督關鍵基礎設施，例如電網、運輸系統和濾水廠。針對這些系統的資訊科技保安攻擊可能會造成嚴重後果，包括關鍵服務中斷、經濟損失甚至生命損失。

- ***零日漏洞利用。***零日漏洞利用針對尚未修補的軟件或系統中以往未知的漏洞。對於在黑市上發現或購買這些漏洞的黑客來說，決策局／部門是他們吸引的目標，因其可用於獲得未經授權的接達或開展有針對性的攻擊。

- ***資訊戰和虛假資訊。***決策局／部門也容易受到資訊戰和虛假宣傳活動的影響。這些行為包括傳播虛假資訊、操縱公眾輿論或進行資訊科技保安操作，以影響政治流程或破壞公眾信任。

4.2 範圍制定

制定範圍對各決策局／部門至關重要，可使其根據特定需要在資訊科技保安威脅管理中有效分配資源、建立監察措施，以及建立保安措施的優先次序。

在部門層面明確制定範圍，可使決策局／部門確定其需要保護的特定部門或分部（例如財務部、人力資源部或研發部）免受潛在威脅。通過制定該層面的範圍，決策局／部門可以分配資源和實施保安措施，以解決與有關部門或分部的特定漏洞和風險。

至於系統層面，範圍制定涉及識別決策局／部門需要保護的系統，例如企業資源計畫系統（ERP）、客戶關係管理系統（CRM）或內部通訊系統。通過制定系統層面的範圍，決策局／部門可以集中精力保護這些關鍵系統，並確保其能夠抵禦潛在威脅。

在設備或應用層面，範圍制定涉及識別需要保護的特定設備或應用，例如伺服器、路由器、防火牆或關鍵業務的應用。通過制定該層面的範圍，決策局／部門可以實施有針對性的保安控制措施，以保護這些關鍵組件免受潛在威脅。

此外，在制定資訊科技保安威脅管理的範圍時，必須識別依賴關係。舉例來說，各決策局／部門應考慮對供應商或服務供應商等外部利益相關者（例如第三方軟件供應商、雲端服務供應商或關鍵組件供應商）的依賴關係。通過識別依賴關係，決策局／部門可以評估相關風險，並採取適當的保安措施，以確保系統和數據的安全。

5 威脅識別和情報收集

5.1 識別和分類資訊科技保安相關威脅

威脅可分為三個主要類別：

- ***社會威脅。***直接與人為因素相關有意或無意的威脅，例如人為錯誤、遺漏或疏忽、盜竊、欺詐、誤用、損害、破壞、披露和修改資料。
- ***技術威脅。***源自技術問題，例如錯誤流程、設計缺陷、佈線等通訊路徑中斷。
- ***環境威脅。***源自火災、水災、供電、地震等環境災害。

識別和分類相關的資訊科技保安威脅有助於有效降低風險。為此，發展全面準確的威脅分類至關重要。威脅分類組織並分類不同類別的資訊科技保安威脅，以清楚了解威脅環境，使決策局／部門能夠相應地分配資源和工作。

為識別和分類資訊科技保安威脅，各決策局／部門應遵循以下建議步驟：

1. ***進行威脅評估：***全面評估決策局／部門資訊科技保安的潛在威脅，這可能涉及分析歷史資料、研究行業趨勢、諮詢保安專家，以及考慮決策局／部門資訊科技基礎設施的個別特徵。
2. ***識別威脅類別：***根據評估將威脅劃分為相關類別。可以上述三類威脅（社會威脅、技術威脅和環境威脅）為起點。確保該類別涵蓋決策局／部門特有的威脅範圍尤其重要。
3. ***制定威脅類別：***在每個類別中，制定與決策局／部門相關的特定威脅類別。例如，在社會威脅下，其可能包括惡意軟件、網絡釣魚攻擊、內部威脅、社交工程等。建議盡可能全面地擷取決策局／部門可能遇到的各種威脅。
4. ***定期更新和完善：***威脅環境為不斷變化的，新威脅和現有威脅都在不斷演變。定期覆檢和更新威脅分類以保持最新狀態至關重要。決策局／部門應保持了解新興威脅、攻擊技術、漏洞和行業良好作業模式，並將知識納入威脅分類，以確保其相關性和成效。
5. ***記錄和溝通：***決策局／部門應以清晰易讀的格式記錄威脅分類，建立數據庫或知識庫，以便相關持份者能接達和了解分類威脅，並向相關持份者傳達威脅分類，以提高風險意識並確保共同了解相關風險。

威脅分類應適應決策局／部門的需要，並隨著威脅環境的變化而發展。威脅分類屬於動態文件，需要定期更新和完善，以有效指導決策局／部門的資訊科技保安工作。另見**附件 A** 了解威脅分類的樣本和具說明作用的示例，以協助決策局／部門使用威脅分類識別特定威脅並確定其優先排序的方式。

威脅分類和保安風險評估在資訊科技保安中是相互關聯且相輔相成。威脅分類提供結構化框架，用於組織和分類不同的資訊科技保安威脅，使決策局／部門能夠了解其所面臨的威脅環境。該分類通過將威脅劃分為特定類別，為進行全面的保安風險評估奠定了基礎。

保安風險評估使用威脅分類，識別和評估每個威脅的漏洞和潛在後果。它考慮了決策局／部門的資產、價值、現有控制措施，以及漏洞利用的可能性，以確定每種威脅構成的風險水準。威脅分類為風險評估過程提供資訊和指導，確保所有相關威脅已基於其潛在影響對其進行優先排序。

相反地，風險評估結果（例如已識別的風險及其相關的可能性和嚴重程度）為完善和更新威脅分類提供了有價值的見解。此迭代運算流程可確保威脅分類保持最新狀態，並與不斷演變的風險環境保持一致。

因此，應使用威脅分類和保安風險評估以有系統地識別資訊科技保安風險、訂定風險的緩急次序和緩解相關風險。有關更多詳情，請參閱《**資訊科技保安風險管理實務指引**》和《**保安風險評估及審計實務指引**》。

5.2 使用威脅情報來源和共享平台

威脅資訊是指可說明組織保護自身或檢測威脅者活動的所有資訊，例如：

- **入侵指標（IoC）**是技術上的產物或可觀察物，表明攻擊即將發生或正在發生，或可能已經發生。這些指標可作為線索，用於檢測和防禦潛在威脅。指標示例包括單一可疑命令和控制伺服器的互聯網協定（IP）位址、可疑的域名系統（DNS）域名、標記惡意內容的劃一資源定位址（URL）、惡意可執行文件的文件哈希或惡意電子郵件主題文本。
- **策略、技術和程序（TTPs）**描述了行為者的表現。策略是對行為的高層次描述，技術是在策略條件下對行為的詳細描述，而程序是對技術較低層次、高度詳細的描述。策略、技術和程序可以描述行為者使用特定惡意軟件變體、操作順序、攻擊工具、發送機制（例如網絡釣魚或水坑攻擊）或漏洞利用的傾向。
- **保安警報**，也稱為公告和漏洞說明，是關於當前漏洞、利用和其他保安問題，通常人類可讀，簡短的技術通知。
- **威脅情報報告**通常是散文般的文件，描述策略、技術和程序、行為者、系統類型和目標資訊，以及其他為組織提供更強態勢感知能力的威脅資訊。威脅情報是經匯總、轉換、分析、解釋或擴充的威脅資訊，為決策流程提供必要的背景資訊。
- **工具配置**是設置和使用工具（機制）的建議，該工具（機制）支持自動收集、交換、處理、分析和使用威脅資訊。例如，工具配置資訊說明可能包含有關安裝和使用隱匿軟件檢測程式和軟體刪除工具，或創建和自訂入侵

偵測識別碼、路由器接達控制清單（ACLs）、防火牆規則或網絡篩檢程式設定文件。

威脅情報是指有關潛在資訊科技保安威脅的資訊和見解，包括新興的攻擊技術、漏洞和入侵指標。利用威脅情報，決策局／部門可以增強其資訊科技保安能力，並主動防禦不斷演變的威脅。

威脅情報是了解和解決資訊科技保安威脅的關鍵部分，涉及收集和分析有關潛在威脅的資訊，包括其策略、技術和指標。不同類型的威脅情報為各決策局／部門提供有價值的見解：

- ***戰略性情報。***戰略性情報側重長期趨勢、地緣政治因素以及威脅者的能力和動機，有助決策局／部門預測風險，並相應地調整保安策略。戰略情報通過提供有關業務風險易懂的報告，協助制定長期戰略。

- ***技術性情報。***技術性情報提供有關直接威脅（例如新型惡意軟件或漏洞）的具體和可執行資訊，使決策局／部門能夠迅速有效地應變該等威脅。技術性情報包括威脅者使用的策略、技術和程序，並提供可用於更新防禦系統的入侵指標。

- ***操作性情報。***操作性情報側重威脅者的策略、基礎建設和活動，提供對威脅者所使用策略和方法的見解。操作性威脅情報通常涉及針對組織的潛在且即將開展的行動詳情，可幫助決策局／部門預測和準備特定的威脅活動。

威脅情報應：

- 具有相關性（即與決策局／部門的保護相關）；
- 具有見解的（即為決策局／部門提供對威脅形勢的準確而詳細的理解）；
- 具有情境性，提供態勢感知（即根據事件發生的時間、地點、以往經驗和在類似組織盛行為資訊提供更多前因後果）；
- 具有可行性（即決策局／部門可以快速有效地就資訊採取行動）。

威脅情報提供者從各種來源搜集資訊，例如入侵指標、用戶端生成資料、深網、暗網、訊息平台、社交媒體、人力情報、惡意軟件分析、地緣政治發展、代碼倉庫和內容公開張貼網站。多樣化的來源資訊能夠提供全面的威脅洞察，包括威脅者使用的策略、技術和程序、需要修補的漏洞，以及可能的入侵或攻擊指標。有效的威脅情報提供者會驗證並匯總不同來源的資訊，以提供對威脅的全面理解。理想的多源情報報告應結合至少兩種來源的資訊。請參閱**附件 B** 以了解評估資訊科技保安威脅情報提供者的問題示例。

威脅情報透過各種方式傳遞，包括訂閱、威脅情報平台（TIP）和資料來源。訂閱提供對當前和歷史情報的接達、互動式調查功能，且能夠與現有流程整合。威脅情報平台整合並關聯不同的資料來源，允許用戶在各種威脅情報來源間切換並進行調查。資料來源提供持續更新的威脅情報，可整合到保安系統和流程中，實現實時保護。

鼓勵各決策局／部門採用威脅情報平台，以主動有效地利用威脅情報。這些平台是集中式存儲庫，用於收集、分析和傳播來自各種來源的威脅情報。決策局／部門可利用威脅情報平台簡化威脅情報的收集和分析，從而能夠識別相關威脅並及時主動採取措施來降低風險。威脅情報平台還能促進不同決策局／部門之間的合作和資訊共享，促進集體和協作的資訊科技保安方式。

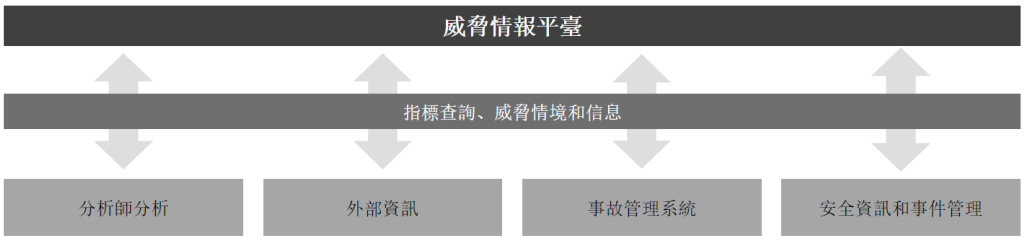

圖 5.1 威脅情報平台的使用情況

此外，決策局／部門可與可信任的資訊科技保安組織，例如行業協會、研究機構和私營資訊保安公司，建立戰略合作夥伴關係。這些合作夥伴可以為決策局／部門提供專業知識、研究發現、額外的威脅情報來源，在決策局／部門現有能力基礎上提供補助。

為有效利用威脅情報來源和共享平台，建議採取以下步驟：

1. ***建立目標：***制定決策局／部門內製造威脅情報的目的和目標，考慮到決策局／部門營運的具體需求和優先事項。

2. ***識別和選擇資訊來源：***識別和審視提供相關可靠威脅情報的內部和外部資訊來源。這些資訊來源可以是政府來源（例如政府電腦保安事故協調中心）、特定行業組織、資訊科技保安供應商以及國際資訊共享平台。這些來源提供了關於新興威脅趨勢、已知漏洞以及網絡罪犯使用的策略的及時可靠資訊。

3. ***收集資訊：***從選定的內部和外部管道收集資訊，建立一個全面的資料集用於分析。收集的資訊可能來自入侵指標、用戶端生成資料、深網、暗網、訊息平台、社交媒體、人力情報、惡意軟件分析、地緣政治發展、代碼倉庫和內容公開張貼網站。

4. ***處理和準備資訊：***對收集到的資訊進行處理，使其便於分析。此過程中可能需要翻譯、格式化或核實資料，以確保其準確性和一致性。

5. ***分析資訊：***對收集到的資訊進行徹底分析，了解其與決策局／部門的相關性和重要性。識別與威脅者策略、技術和程序（TTP）、漏洞以及入侵指標（IoC）相關的模式、趨勢和潛在風險。

6. ***溝通和共享：***與決策局／部門內相關人士和分部有效溝通和共享已分析的威脅情報。以易於理解和可行動的格式呈現資訊。

7. ***納入資訊科技保安流程：***將從各種管道收集到的威脅情報整合到決策局／部門的資訊科技保安威脅管理流程中。這可能涉及使用相關的入侵指標和策略、技術和程序來更新技術性的預防和檢測控制，例如防火牆、入侵偵測系統、反惡意軟件解決方案等。

8. ***加強資訊保安測試：***使用威脅情報作為資訊保安測試過程和技術的輸入。這有助於識別決策局／部門系統和基礎設施中的漏洞和弱點。

下文以案例形式闡述決策局／部門如何有效處理威脅情報：

決策局／部門收到了一份威脅情報報告，報告顯示行業內某類惡意軟件的使用頻率正在逐漸上升。該報告包括技術細節，例如惡意軟件可執行文件的哈希值，而文件哈希值是關鍵的入侵指標。

收到該情報後，決策局／部門立即展開行動。由決策局／部門的資訊科技保安管理組啟動流程了解威脅情境，審查與報告的惡意軟件相關的策略、技術和程序，包括感染方法（例如電子郵件附件、下載被篡改的軟件）、惡意軟件安裝後的行為（例如資料外泄、系統損壞）以及任何已知的防禦措施。

資訊科技保安管理組將了解到的資訊傳達給關鍵持份者，包括高層管理人員、部門資訊科技保安主任和相關資訊科技團隊。此確保每人都了解到威脅的性質以及減輕威脅需要採取的步驟。

然後，相關團隊使用入侵指標（惡意軟件可執行文件的哈希值）來更新防禦措施，通過配置反惡意軟件系統來識別並隔離任何具有報告哈希值的文件。同時，團隊還應調整入侵偵測系統，以尋找與惡意軟件相關的網絡流量模式。

最後，團隊應檢視威脅情報報告，尋找任何關於可能被惡意軟件利用的軟件漏洞的資訊。如果決策局／部門的系統使用了任何易受攻擊的軟件或硬件，應儘快修補軟件或硬件以進一步保護系統免受惡意軟件侵害。

6 威脅監控和檢測與威脅情報的整合與應用

6.1 制定監察目標、技術和工具

各決策局／部門應制定監察目標，包括識別需要保護的關鍵資產、系統和網絡，並了解潛在的威脅和風險。通過全面了解這些要素，決策局／部門應繼而使監察工作與總體資訊科技保安目標一致。建立目標後，決策局／部門可選擇適當的監察技術和工具。決策局／部門應評估並部署與監察目標一致的工具，確保工具的覆蓋範圍足夠，且能夠良好地與其他保安解決方案結合。

決策局／部門應根據其目標和具體要求選擇適當的保安監察工具。以下工具僅供舉例說明，在選擇工具時應考慮特定部門要求、預算和現有基礎設施：

- ***入侵防禦系統（IPS）。***入侵防禦系統理論上能夠在入侵活動到達目標前，檢測並嘗試阻止其入侵活動。

- ***網絡偵測和回應（NDR）解決方案。***網絡偵測和回應解決方案集中對網絡流量進行實時監察、分析行為，並檢測潛在威脅。這方案提供了解網絡可見性、識別異常，並有助發現隱藏威脅。

- ***端點偵測和回應（EDR）解決方案。***端點偵測和回應解決方案集中於監察和保護個別端點，並收集和分析端點資料以檢測和應變高級威脅。有關 EDR 的更多詳細資訊，請參閱附件 D。

- ***端點保護平台（EPP）。***端點保護平台集合了防病毒、防惡意軟件和主機為基礎入侵防禦功能，以保護端點免受各種威脅。

- ***威脅情報平台（TIPs）。***威脅情報平台匯總、分析並傳達各種來源的威脅情報資料，有助於識別新興威脅和入侵指標。

- ***用戶和實體行為分析（UEBA）。***用戶和實體行為分析是一種利用行為分析、機器學習演算法和自動化來識別異常和潛在危險的用戶和設備行為的保安軟件。

- ***擴展偵測和回應（XDR）解決方案。***擴展偵測和回應解決方案從組織的技術堆棧中以往分離的保安工具收集威脅資料，以便更輕鬆、更快速地調查、搜索和應變威脅。擴展偵測和回應平台可從端點、雲端工作負載、網絡電子郵件等方面收集保安遙測資料。

- ***保安資訊和事件管理（SIEM）系統。***保安資訊和事件管理系統收集並分析不同來源的保安事件日誌，將事件進行關聯並根據預先定義的規則和模式生成警報。

- ***保安編排、自動化和回應（SOAR）解決方案。***保安編排、自動化和回應解決方案平台監察威脅情報源，並觸發對保安問題的自動回應，這有助快速高效地減輕橫跨多個複雜系統的威脅。

附件 E 中的圖表說明了綜合的威脅監控架構，展示了資訊科技保安威脅監控中相互關聯的監控工具，以供參考。

在選擇適當的資訊科技保安威脅監控解決方案時，各決策局／部門應考慮以下因素：

- ***可擴展性：***確保解決方案能處理隨決策局／部門規模的擴大而不斷增加的資料。
- ***相容性：***確保解決方案應能與現有系統和技術相容。
- ***實時監控能力：***解決方案應能實時監控和檢測威脅。
- ***威脅情報匯總能力：***解決方案應能匯總各種來源的外部威脅情報。
- ***可調整性和靈活性：***解決方案應具備可調整性，以配合決策局／部門的特定需求。
- ***報告和分析能力：***具備全面報告和分析的能力。
- ***供應商聲譽和支持：***考慮供應商的聲譽和提供的支持。
- ***成本效益：***評估解決方案的成本，確保其物有所值。

此外，各決策局／部門應戰略性地在整個網絡基礎設施中部署感測器，以捕獲相關資料並檢測潛在威脅。部署決策應考慮以下要素：

- ***網絡拓撲：***考慮網絡的佈局和結構。
- ***關鍵資產：***識別並優先保護重要資產。
- ***進出點：***關注網絡流量進出區域。
- ***網絡段：***查看網絡中的不同部分或分區。
- ***網絡交匯點：***注意不同網絡段相交的點。
- ***已知攻擊途徑：***考慮攻擊者使用的常見方法。
- ***易受攻擊的服務和協定：***識別服務和協定中的弱點。
- ***歷史攻擊：***從過去的攻擊和漏洞中積累經驗。
- ***威脅情報：***了解當前和新興威脅。

採用風險為本的方法來部署感測器至關重要，優先考慮關鍵資產、高風險區域以及曾經出現漏洞的區域。應定期覆檢和評估網絡拓撲、攻擊途徑和新興威脅，以確保持續有效。

資訊科技保安威脅監控目標、技術和工具可用於及時識別和應變資訊科技保安威脅，相關示例如下。

目標	技術和工具
盡可能減少影響、檢測和應對惡意軟件感染。	實施實時掃描端點和網絡流量惡意軟件，識別並阻止惡意文件或活動。
識別並攔截未經授權的接達嘗試，以保護敏感資料和系統。	實施用戶活動監察和異常檢測，以檢測可疑登錄嘗試、權限升級或未經授權的用戶權限變更。
監控資料泄露的嘗試，防止敏感資料從決策局／部門泄露。	部署資料外泄防護（DLP）解決方案，監控並阻止通過電子郵件、網站上傳或流動裝置傳輸未經授權的敏感資料。
監控用戶行為，並檢測員工或外判人員潛在的內部威脅或惡意活動。	實施用戶行為分析，監控異常的資料接達模式、過多文件下載或未經授權對機密資訊的接達嘗試。
檢測並防止網絡入侵或未經授權的接達嘗試。	部署入侵偵測系統（IDS）或入侵防禦系統（IPS），以監控已知攻擊識別碼或可疑活動的網絡流量。
監控網絡應用程式的保安漏洞，並防範基於網絡的攻擊。	實施網絡應用程式防火牆（WAF），監控和過濾傳入的網絡流量，攔截惡意請求或對應用程式漏洞利用的嘗試。
監控雲端基礎架構和服務，以檢測並應對保安事故或配置錯誤。	利用雲端服務供應商提供的雲端特定監控工具和服務，追蹤和分析保安事件，例如未經授權的接達嘗試或可疑的應用程式介面（API）調用。

表 6.1 資訊科技保安威脅監控目標、技術和工具示例

各決策局／部門在實現有效的網絡保安監察和檢測方面可能面臨重大挑戰。這通常依賴於專業工具和技術，而這些工具和技術需要大量資金投入。然而，有限的預算可能會妨礙決策局／部門獲取和應用這些工具，使其難以充分監控系統並及時檢測潛在保安事故。

儘管如此，有限預算的決策局／部門仍然可以採取措施來增強其監控和檢測能力。採用富有策略的方法以盡可能地利用資源和替代方法至關重要。建議如下：

- ***排序監控目標和區域：***確定需要保護的最關鍵資產、系統和網絡。根據風險評估和保安事故潛在影響來分配資源。通過排序這些領域的監控工作，重點保護高價值目標和敏感資料。

- ***利用內置保安功能：***充分利用現有基礎設施和可用的系統內置保安功能。現代作業系統、網絡設備和雲端平台通常具有原生的保安監測功能，如日誌匯總、審計和基本威脅檢測。確保這些功能已啟用並適當地配置。

- ***集中端點保護：***通過在決策局／部門所有設備上實施完善的防病毒／反惡意軟件解決方案優先進行端點保護。配置這些工具以實現實時監控、威脅檢測和事故應變。定期更新防病毒或惡意軟件識別碼，以防範最新的威脅。

- ***注重用戶意識培養和培訓。***開展用戶意識培養和培訓計畫，幫助員工了解常見的保安威脅、網絡釣魚攻擊和保安計算的最佳實踐。對於用戶意識非常了解的用戶可作為保安風險的第一道防線，減少對監控工具的依賴。

- ***進行網絡分段：***利用網絡分段將關鍵系統和敏感資料與網絡的其他部分隔離。此可實現更加集中的監控工作，並減少攻擊面。通過虛擬區域網絡（VLAN）或防火牆等方式進行網絡分段無需大量的資金投入。

6.2 資料收集、日誌分析和威脅情報匯總

為有效監控和檢測資訊科技保安威脅，啟用日誌記錄和資料收集機制是必要的。保安記錄文件可能有各種來源，例如硬件設備、軟件系統和應用程式。有關保安記錄文件管理和相關保安注意事項，請參考《資訊保安記錄管理實務指引》。

集中的日誌匯總和分析解決方案（例如保安資訊和事件管理（SIEM）系統）可讓決策局／部門全面了解保安事件，並分析資訊科技基礎設施中各種來源日誌間的相關性。保安資訊和事件管理（SIEM）是一種結合了保安資訊管理（SIM）和保安事件管理（SEM）功能的保安軟件產品和服務。除了保安資訊管理和保安事件管理功能外，一些保安資訊和事件管理產品還具備實時保安警報分析、威脅驗證和事故工作流程自動化等額外功能。

保安資訊管理自動收集來自網絡和保安設備／終端（例如防火牆、代理伺服器、入侵偵測系統和防毒軟件）的事件日誌資料，並將收集的資料和威脅情報日誌進行關聯和簡化，以便長期存儲、分析和報告。

保安事件管理提供事件管理功能，可導入保安事件進行分析和視覺化呈現（以圖表和儀表板等形式）作事故應變和保安操作。保安事件管理主要進行實時監測、事件匯總、相關性分析和通報來自作業系統、防毒軟件、防火牆和入侵偵測系統的事件，以及由認證系統、伺服器和數據庫直接通報的事件。

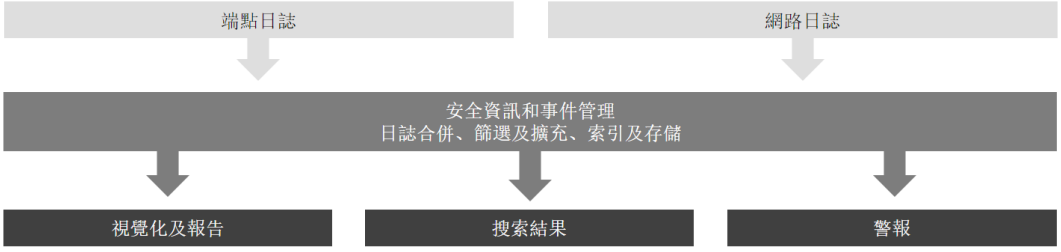

圖 6.1 保安資訊和事件管理功能

除保安資訊和事件管理外，還有一些更具成本效益的替代方案可用於日誌匯總和分析，例如主要用於從收集、存儲和分析各種來源日誌的日誌管理工具。這些工具提供集中進行日誌匯總和分析的功能，但不具備保安資訊和事件管理的進階保安功能。雖然這些替代方案可能更具成本效益，但可能不具備與完整的保安資訊和事件管理解決方案相同級別的進階保安功能和威脅檢測能力。在選擇替代方案之前，決策局／部門應仔細評估其需求和預算。

檢測階段的成功在很大程度上取決於前一階段收集到的資料的可用性。收集功能運作越高效，檢測功能效果越好。

工具的品質會影響檢測階段的成效，包括威脅狩獵能力、內外部威脅情報資訊的可用性，以及檢測工程功能的成效。

此外，為有效檢測和分析威脅，決策局／部門應將威脅情報納入監察和分析流程。威脅情報包括已知入侵指標、新興威脅、攻擊手法以及漏洞等相關資訊。

- ***利用外部威脅情報。***將威脅情報源、數據庫或平台整合至監察基礎設施，以提高識別和應變特定威脅的能力。決策局／部門可以利用威脅情報主動防禦已知威脅，應對不斷變化的攻擊技術。

- ***關聯和警報生成。***利用威脅情報整合，將傳入日誌、網絡流量和端點活動與已知威脅指標進行比較。這關聯提高了威脅檢測的準確性和成效，使系統能夠在發現潛在威脅時發出警報或通知。

威脅情報源可提供有關最新攻擊活動、惡意軟件變體、漏洞和漏洞利用技術的資料。通過仔細分析這些資訊，決策局／部門可以發現網絡犯罪活動的模式和趨勢，確定其動機，並了解所使用的工具和方法。

以下是對於資料收集、日誌分析和威脅情報整合的一些建議執行步驟：

1. ***識別日誌來源：***根據其對業務、監管和遵行要求的重要性，確定應監察的內容。這些可包括網絡交換機、路由器、防火牆、主機作業系統、保安軟件、網絡應用系統、電子郵件應用系統等。

2. ***制定日誌記錄政策：***評估各組件對業務和營運的重要性，並確定應記錄的資訊。建立日誌記錄政策指明應記錄的事件／活動。例如，決策局／部門宜記錄所有登錄嘗試、接達控制變更和關鍵系統事件。

3. ***進行負載測試：***在生產環境中實施日誌記錄政策之前，在測試環境中對日誌記錄進行負載測試。這將有助於確保計畫的日誌配置能夠處理預期負載，並且不會對系統性能產生不利影響。例如，決策局／部門可以模擬大量日誌事件，以確保配置能夠在不影響系統性能的情況下處理預期負載。

4. ***實施集中日誌匯總與分析：***考慮實施集中日誌匯總與分析解決方案，例如保安資訊和事件管理系統。保安資訊和事件管理系統可就保安事故提供全面的可見性，並對資訊科技基礎設施內各種來源的日誌進行有效分析。

5. ***評估保安資訊和事件管理功能：***根據保安資訊和事件管理產品的功能（例如保安資訊管理、保安事件管理、實時保安警報分析、威脅驗證和事故工作流程自動化）對其進行評估。選擇最符合決策局／部門需求的保安資訊和事件管理解決方案。

6. ***整合威脅情報：***將威脅情報納入監察和分析流程，例如利用外部威脅情報源、數據庫或平台來提高識別和應變特定威脅的能力。

7. ***關聯和警報生成：***利用威脅情報整合，將傳入的日誌、網絡流量和端點活動與已知威脅指標進行比較。這一關聯提高了威脅檢測的準確性和成效，使系統能夠在發現潛在威脅時發出警報或通知。

8. ***分析威脅情報：***仔細分析威脅情報資訊，以揭發網絡犯罪活動的模式和趨勢、識別動機，並了解攻擊者使用的工具和方法。這種分析有助於加強決策局／部門的防禦，並應對不斷變化的攻擊技術。

9. ***評估檢測工具：***評估可用檢測工具的品質，包括威脅狩獵能力的強度和內部及外部威脅情報資訊的可用性。確保檢測工程功能的成效。

10. ***確保資料收集的效率：***檢測功能的成效取決於資料收集階段獲得的資料的可用性。確保收集功能有效運行，收集必要資料以有效檢測威脅。

11. ***保持更新：***根據不斷變化的保安威脅和新興技術，持續監察和更新日誌記錄和威脅情報整合流程。

6.3 行為分析、異常檢測和威脅情報應用

為有效監控和檢測資訊科技保安威脅，各決策局／部門應為其網絡、系統和用戶建立基準行為模式。通過了解什麼構成環境中的正常行為，決策局／部門可識別出具潛在威脅或惡意活動的偏差或異常。在建立基準行為模式後，決策局／部門應利用行為分析技術識別異常或偏差。行為分析涉及通過監察和分析持續活動檢測出偏離既定規範的行為。此可通過利用進階的分析工具和技術，將當前行為與既定基準進行比較。

以下是一些建議執行步驟：

1. ***部署資料分析工具：***部署適當的資料分析工具或平台，例如保安資訊和事件管理系統、日誌管理解決方案或其他資料分析工具，以處理和分析歷史資料。

2. ***資料準備和分析：***分析網絡流量、系統活動和用戶行為的歷史資料，以深入了解決策局／部門基礎設施內的典型模式和活動。通過標準化格式、將時間戳記轉換為通用時區以及解決資料來源中的差異或不一致問題，使收集到的資料規範化。

3. ***識別相關資料參數：***識別與建立基準行為模式資料相關的關鍵參數或屬性，例如網絡流量、系統資源利用率、用戶登錄活動和應用系統使用情況。

4. ***統計分析和用戶／系統剖析：***應用平均值、中位數、標準差或聚類演算法等統計分析技術分析歷史資料，以確定趨勢、模式和分佈。根據歷史資料分析用戶和系統剖析，針對典型用戶行為、系統活動和網絡流量模式創建個人檔案或角色。

5. ***覆檢、更新和存檔：***建立流程持續監察運行資料，以持續更新基準行為模式，因決策局／部門基礎設施和用戶行為演化。記錄基準行為模式建立的流程，例如數據收集計畫、分析技術和識別的正常行為參數。建立文檔總結基準行為模式，並指導持續的監察和檢測工作。

在行為分析中應用威脅情報有助於決策局／部門將觀察到的異常與已知攻擊技術或指標關聯。這一關聯有助於確定和驗證潛在威脅的緩急次序、減少誤報，並將資源集中用於最重大風險。決策局／部門可通過分析威脅情報識別常見攻擊途徑，例如網絡釣魚電子郵件、社交工程技巧或惡意軟件傳播方式。這有助決策局／部門主動實施防禦措施，並教育員工有關潛在風險，從而降低被成功攻擊的可能性。

決策局／部門可參考以下步驟在監控和檢測過程中應用威脅情報源和資料：

1. ***選擇相關威脅情報來源：***決策局／部門可以從多個威脅情報來源中選擇，例如商業型供應商、開源資訊源和行業特定的資訊共享平台。這些來源提供有關新興威脅和已知攻擊技術的資訊。

2. ***制定入侵指標（IoCs）：***決策局／部門可根據已識別的威脅和攻擊途徑制定入侵指標。這些入侵指標是顯示潛在保安事故的特定資訊，例如互聯網規約地址、域名、文件哈希值或與已知威脅相關的行為模式。

3. ***收集和匯總威脅情報資料：***決策局／部門通過各來源收集威脅情報資料，並將其集中存儲。全面收集資料有助於更廣泛地了解威脅環境。

4. ***標準化和豐富威脅情報資料：***決策局／部門對收集的威脅情報資料進行規範和豐富，以確保一致性並提高分析效用。這過程包括標準化格式、添加背景資訊和關聯不同來源的資料。

5. ***將威脅情報源納入監控和檢測流程：***將威脅情報源整合至決策局／部門的監控和檢測系統。這可將觀察到的異常與已知攻擊技術或指標關聯，從而實現更快和更準確的威脅檢測。

6. ***將入侵指標與收集到的資料進行匹配和關聯：***將已制定的入侵指標與收集到的資料進行匹配和關聯，以確定並驗證潛在威脅的緩急次序。這流程有助識別和集中於最相關和最高風險的保安事故。

7. ***持續更新和刷新威脅情報資料：***威脅情報資料並非一成不變，新的威脅和漏洞會定期出現。決策局／部門需持續更新和刷新威脅情報資料，以便及時了解新興威脅，並相應調整其保安措施。

8. ***監察和評估成效：***決策局／部門對整合威脅情報源和資料於其監控和檢測過程的成效展開監察和評估。這評估有助於識別需要改進的方面，並確保威脅情報程式在加強網絡保安方面發揮作用。

7 威脅分流和調查

7.1 通過分流程序訂定威脅的緩急次序

分流指對保安警報進行初步評估和分級，以訂定其緩急次序和相應的應變。分流的目的是進行快速的修復或升級，以應對大量的保安警報。與醫院急症分流程序類似，決策局／部門的目標是根據現有資料，合理地訂定調查佇列的緩急次序。利用以往的防禦經驗，決策局／部門作出明智的決策以確保有效的資源分配。

為便於分流，以下前提條件應予滿足：

1. ***建立預先定義的準則：***決策局／部門應建立明確的準則，以指導分流期間的決策程序。圖 7.1 展示更多分流程序概覽的示例。這些準則應定期覆檢和更新，以適應威脅環境和新興技術的變化。

2. ***利用威脅框架：***決策局／部門應利用各框架（例如 Lockheed Martin Cyber Kill Chain 以及 MITRE ATT&CK）以深入了解攻擊的週期及其不同階段，以及攻擊者使用的常見技術。這些框架有助於理解和分類保安警報。

以下是分流程序的概覽：

1. ***警報收集和分析：***警報由保安分析員和自動化工具收集和分析。分析員覆檢各警報提供的詳細資訊，包括相關日誌、網絡流量數據和相關入侵指標。

2. ***警報驗證：***下一步是驗證警報以確認其準確性和相關性。這包括檢查支持證據（例如網絡日誌、系統日誌或入侵偵測系統資料），以判斷警報的保安事故是否屬實或誤報。配置錯誤、軟件故障或良性的用戶行為都可導致誤報。識別誤報後，應向檢測工程團隊回饋以完善準則。

3. ***嚴重性確認：***根據預先定義的準則，按照警報的潛在影響和迫切性對其分類，並指派其嚴重性等級。這使保安團隊可集中優先處理最嚴重的威脅。常見類別宜包括攻擊步驟／階段或技術。常見的嚴重性等級可包括高、中、低，或根據決策局／部門的需求制定類似的等級判定方案。這步驟有助於為警報訂定緩急次序作進一步調查。

4. ***持續監察和迭代分流：***在整個應變過程中進行持續的監察和進一步分流，以識別威脅環境中任何新的警報或變化，這確保及時發現和處理新出現的威脅或不斷變化的事故。

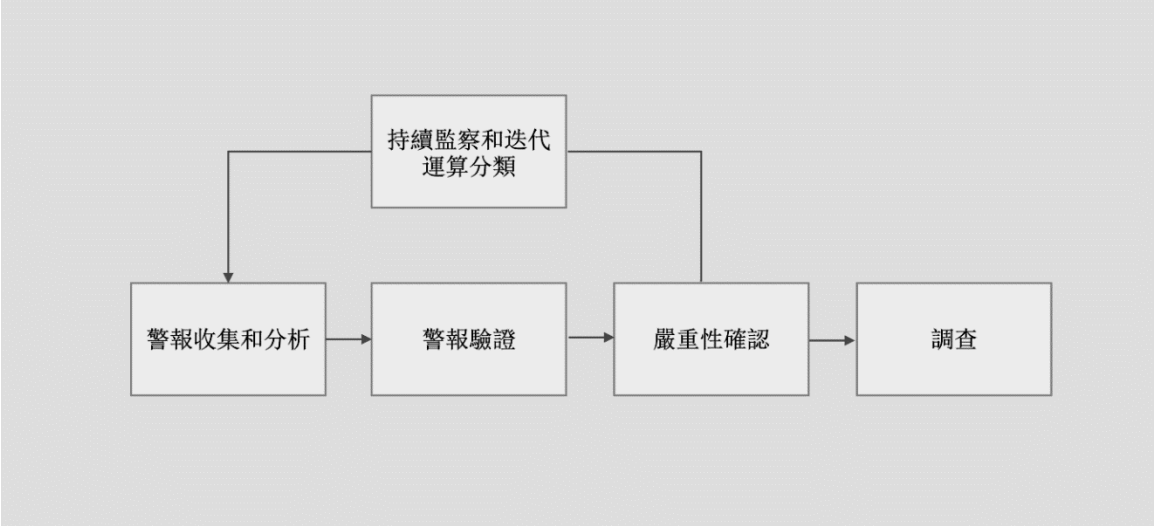

圖 7.1 分流程序概覽

分流程序的成效主要取決於決策局／部門在對警報進行分流時，保安工具和技術所提供的資訊詳細程度和額外背景。保安工具（例如事務跟蹤管理系統和安全資訊與事件管理系統）可提供功能促進決策、自動化工作流程，並提升分流程序的效率和成效。分流工具為保安團隊提供了專用平台，以快速和一致地接收、評估和管理保安事故。

值得注意的是，分流過程是動態的，並可能需要根據從威脅情報中收集的背景情況持續地重新評估。威脅情報提供有價值的背景資料，有關威脅者的性質、能力、動機和目標。這些背景資訊有助決策局／部門評估威脅對其系統、數據和業務營運的潛在影響。隨著新資訊的出現或威脅環境的變化，分流程序可能需要調整以反映不斷變化的威脅環境。

以下示例闡述了使用 MITRE ATT&CK 框架預先定義的準則進行分流。假設決策局／部門收到警報，稱內部系統與已知惡意的互聯網規約地址存在可疑的向外連接，則需根據以下準則訂定應變的緩急次序：

準則	描述	示例說明
警報的嚴重性	評估警報指派的嚴重性等級，表示着保安警報的潛在影響和迫切性。嚴重性較高的警報可能需要即時的關注和優先的緩急次序。	團隊評估警報的嚴重性程度。如果連接指出高風險事故，或與已知威脅者有關，其緩急次序應優先於嚴重性程度較低的警報。
對關鍵系統或功能的潛在影響	考慮警報對決策局／部門運行所需關鍵系統或功能的潛在影響。對於可能破壞或危及關鍵系統的警報，應給予更優先的緩急次序。	團隊考慮惡意互聯網規約地址連接對決策局／部門關鍵系統或基本功能的潛在影響。如該連接存在未獲授權接達、資料外泄或干擾關鍵

準則	描述	示例說明
		業務的風險，則予其更優先的緩急次序。
監管與遵行要求	考慮檢測到的技術可能對任何監管或遵行要求的影響。對可能違反監管或遵行要求的技術，應給予較優先的緩急次序。	團隊考慮惡意互聯網規約地址連接可能牽連的任何監管或遵行要求。如因未獲授權通訊與惡意單位連接而可引致違反監管或遵行要求，團隊給予更優先的緩急次序以確保遵行法律和行業標準。
運行中斷的可能性	評估警報對造成重大運行中斷或停機的可能性。就風險較高可中斷業務營運或服務的警報，應給予較優先的緩急次序。	團隊評估惡意互聯網規約地址連接造成運行中斷的可能性。如存在系統入侵、全網感染或服務中斷的風險，則給予更優先的緩急次序以盡量減少對業務營運的影響。
受影響系統的數量	考慮受警報影響的系統或資產數量。由於潛在的廣泛影響，對於影響大量系統的警報，可能需要即時的關注和優先的緩急次序。	團隊根據受惡意互聯網規約地址連接影響的系統數量來考慮範圍和規模。如多個系統與同一惡意互聯網規約地址通訊或涉及關鍵系統，考慮到潛在的廣泛影響和增加的風險，團隊給予較優先的緩急次序。
情況的迫切性	評估警報的迫切性和立即採取行動的必要性。如警報表明當前或正在發生的保安事故需要立即控制或補救，應給予該警報更優先緩急次序，以儘量減少進一步的損害或入侵。	團隊根據連接的性質、與惡意互聯網規約地址相關的威脅程度或即時資料外泄的可能性等因素評估其迫切性。如需迅速採取行動阻斷連接或控制威脅，團隊則相應給予其更優先的緩急次序。
技術相關性	評估檢測到的技術與決策局／部門基礎設施和系統的相關性。對於已知能有效攻擊決策局／部門環境的技術，給予更優先緩急次序。	團隊評估惡意互聯網規約地址連接的技術與決策局／部門基礎設施的相關性。團隊考慮是否曾發生類似事故或是否有類似攻擊歷史。如威脅者經常使用該技術或對決策局／部門的系統構成重大風險，則相應給予其更優先緩急次序。

策略重要性	考慮與檢測到的技術相關策略的重要性。重點關注與高優先順序策略一致的技術，例如初始接達、執行或滲透。	團隊評估與惡意互聯網規約地址連接相關策略的重要性。如果該連接是初始接達策略的一部分，或顯示曾有試圖在未獲授權的情況下接達決策局／部門的系統，團隊考慮到防止此類未獲授權接達的重要性，給予其更優先緩急次序。
持續的可能性	評估檢測到的技術在決策局／部門系統內持續存在的可能性。對於較可能允許長期接達的技術，給予其更優先緩急次序。	團隊考慮惡意互聯網規約地址連接在其系統內持續存在的可能性。如成功，是否可以讓攻擊者保持長期接達或為未來攻擊建立立足點？如該技術持續存在的可能性很高，應給予其更優先緩急次序。
利用的成熟程度	考慮與檢測到的技術相關漏洞利用的成熟程度。對已知的有效利用給予其更優先緩急次序。	團隊評估與惡意互聯網規約地址連接相關漏洞利用的成熟程度。如存在與互聯網規約地址相關已知和有效的漏洞利用，或與複雜的攻擊技術有關聯，團隊給予其更優先緩急次序以及時解決該技術。
已知攻擊者的使用情況	判斷檢測到的技術是否被已知的威脅者使用，或是否與其典型策略、技術和程序一致。對於複雜或有針對性的攻擊者使用的技術，可給予其更優先緩急次序。	團隊判斷已知的威脅者是否使用過惡意互聯網規約地址。如互聯網規約地址與進階的持續威脅或已知惡意活動有關，團隊考慮到被這些攻擊者作為目標的潛在影響，給予其更優先緩急次序以解決該技術。
橫向移動的可能性	評估檢測到的技術促使於決策局／部門網絡內橫向移動的可能性。對於使橫向移動容易的技術，應給予其更優先緩急次序。	團隊評估惡意互聯網規約地址連接在促使於其網絡內橫向移動的可能性。如成功，是否可以讓攻擊者橫向移動並接達其他系統？由於橫向移動的技術可能導致進一步的入侵和資料外泄，給予其更優先緩急次序。

可見性	考慮檢測到的技術於決策局／部門保安控制的可見性和檢測能力。對於可繞過或規避現有保安措施的技術，給予更優先緩急次序。	團隊考慮其識別和監察向外連接的可見性和檢測能力程度。如現有的保安措施能夠有效檢測惡意互聯網規約地址連接和發出警報，與其他較難檢測到的技術相比，團隊可給予其較低緩急次序。

表 7.1 使用 MITRE ATT&CK 框架進行分流的預先定義準則示例

7.2 調查可疑活動和指標

對警報進行分流後，決策局／部門應採用有系統的方法，包括進行進階分析，以調查已驗證的警報是否構成威脅或實際攻擊，例如，警報表示有更複雜的攻擊者觸發行為警報和潛在持續攻擊活動。

以下是調查過程中的關鍵步驟：

1. ***證據收集：***警報一經驗證並分流為合法的保安警報，分析員便會收集更多證據以更了解潛在威脅。這步驟包括獲取和保存相關日誌、網絡流量資料、系統快照或其他能夠反映事故性質和影響的資訊。

2. ***威脅分析：***調查分析員全面地分析威脅以確定其特徵、動機和潛在影響。這步驟可包括利用威脅情報源、分析惡意軟件樣本，或研究與事故相關的已知攻擊技術。威脅分析有助於識別攻擊者的意圖、潛在風險以及任何有助於檢測和預防的入侵指標。

以下兩個示例有助決策局／部門了解調查階段的主要工作和流程。

- 決策局／部門收到惡意互聯網規約地址連接嘗試的已分流警報。團隊收集網絡日誌、防火牆日誌或其他任何能捕獲連接嘗試的網絡資料。團隊查閱威脅情報源和數據庫以識別已知惡意互聯網規約地址、其相關活動和潛在威脅者。然後，團隊分析嘗試連接的特徵，例如來源位址、目標互聯網規約地址和埠口，以識別已知惡意活動的模式或相似性。

- 決策局／部門收到關於在用戶端系統上檢測到新管理員憑證的已分流警報。團隊收集系統事件日誌或身份驗證日誌等相關日誌，以收集有關創建新管理員帳戶的資訊。團隊查閱威脅情報源和數據庫，以識別與未獲授權的帳戶創建或權限升級相關的已知技術或入侵指標。團隊分析日誌記錄事件，包括時間戳、帳戶名稱和系統活動，以識別新管理員憑證創建過程中存在的可疑模式或異常。

為確保調查有效，決策局／部門應接受嚴格培訓進行有系統的分析，以避免認知偏差和常見錯誤。這使決策局／部門具備必要技能以進行徹底和公正的調查。

調查階段的成效取決於數項因素。有關人員的經驗和分析技術、相關資料的可用性，以及有助生成證據和展示予決策局／部門的科技和自動化工具的使用，所有這些皆有助提高調查的效率。

通過進行徹底的調查並利用人員技術、知識和可用資源，決策局／部門可準確地確定威脅的性質、範圍和根本原因。這允許實施適當的應變措施。

8 威脅應變

威脅應變是一種在網絡威脅升級為事故之前，減輕和預防網絡威脅的主動方法。這方法包括及時採取行動抵消威脅，並將其影響降至最低。有效的威脅應變有賴於準確的威脅情報和預先定義的措施，以確保採取迅速而適當的行動。準確的威脅情報可以提供有關新興威脅和漏洞的實時資訊，使決策局／部門能夠及時採取措施預防攻擊。

當保安警報被確認為威脅時，應做出適當的應變。為了將威脅的影響減至最低和保護資產、系統和數據，決策局／部門應建立可執行已經預先定義的行動及措施，以應變潛在威脅或警報。嚴重性分類為選擇適當的應變行動提供指導。對於嚴重性較高的威脅，需要採取立即和集中的控制、調查和根除等應變措施。相比之下，嚴重性較低的威脅可根據資源可用性和緩急次序採取相應進一步的控制。

以下是有效威脅應變中常見採取的關鍵行動和措施：

1.***遏制：***這包括從用戶郵箱中撤回已發送的電子郵件、將用戶添加到低權限組別、更新防火牆和網絡過濾器的攔截清單，以及實施在郵件閘道、防火牆、端點偵測和回應（EDR）、網絡閘道、活動目錄、網絡接達控制（NAC）等各種解決方案中攔截機制的措施。

2.***攔截：***採取措施攔截惡意活動或未獲授權的系統和網絡接達。

3.***修補：***應安裝必要的軟件修補程式和更新解決漏洞，並增強保安態勢。

4.***培訓：***執行培訓計畫以教育用戶和人員有關潛在威脅、良好作業模式和保安意識。

在應變威脅後，決策局／部門應從各來源收集到的威脅進行歸納和分組，並確定是否將其升級為事故。分析員應根據鑑證分析提供情境豐富的威脅視圖。這允許決策局／部門確定需要進一步調查的範圍，或觸發所需的事故應變。詳情請參閱**《資訊保安事故處理實務指引》**。

以下是威脅應變示例：

當監察工具檢測到可疑活動時，即時威脅應變行動便會啟動。分析員對警報進行分析，確定其是否會對決策局／部門的保安構成潛在威脅。根據嚴重性分類，確定可以通過預先定義的行動來緩解威脅。

受影響的系統會立即與網絡隔離，作為遏制措施防止潛在的威脅擴散。同時，分析員在不同解決方案中採用攔截機制，例如防火牆、網絡過濾器和網絡接達控制，以攔截惡意活動和未獲授權的接達。

為解決可能已被利用的漏洞，分析員確保已即時安裝必要的軟件修補程式和更新，以增強整體保安態勢。

在應變威脅後，分析員對收集的資料進行分組和分析，從而覆檢和歸納威脅情報。這分析提供情境豐富的威脅視圖。如有需要，這分析有助識別需要進一步調查的範圍或上報到事故應變小組。

為提高人員的保安意識，決策局／部門定期進行培訓計畫，以教育用戶和人員有關潛在威脅、良好作業模式和保安意識。這些培訓課程有助建立具警覺性和主動通報威脅的文化。

在這情況下，威脅應變成功緩解了潛在事故。

決策局／部門可考慮建立操作手冊，記錄已定義的行動和措施，以便在威脅演變成真實事故前作出應變。有關操作手冊示例，請參閱**附件 C** 。

9 持續改進和調整

9.1 定期監控、評估和保安態勢評估

應進行定期監控、評估和保安態勢評估，以衡量威脅監控的成效，並做出充分了解的決策，以增強整體保安態勢。

決策局／部門應建立衡量威脅監控成效的關鍵績效指標（KPI）。這些可衡量的指標提供決策局／部門在資訊科技保安工作的表現和進展的見解。在確定關鍵績效指標時，決策局／部門應考慮遇到的威脅數量和類型、事故應變時間、檢測準確度以及已實施保安控制的成效等因素。這些關鍵績效指標應與決策局／部門的目標一致，並反映其獨特的風險環境。

持續監控威脅環境對於防範新興風險和漏洞至關重要。這包括監控外部威脅情報源、保安警報和決策局／部門內部事故等。應定期評估威脅監控程序和技術的成效，以確保它們保持更新和高效。評估可包括威脅檢測系統的準確性和及時性、保安控制的成效，以及事故應變程序的回應能力。資訊科技保安威脅管理的特定關鍵績效指標示例包括：

- ***平均檢測時間（MTTD）。***這關鍵績效指標衡量發現資訊科技保安威脅或保安事故的平均時間。該指標提供決策局／部門監控效率和成效的見解。平均檢測時間越低，決策局／部門越快可應變威脅，進而將潛在的損失減到最低。

- ***平均回應時間（MTTR）。***這關鍵績效指標衡量應變並解決已發現資訊科技保安威脅或保安事故所需的平均時間。該指標反映決策局／部門的事故應變效率以及控制和減輕威脅影響的能力。平均回應時間越低，應變越快越有效。

- ***誤報率。***這關鍵績效指標衡量監控系統生成的警報中被確定為誤報（即並非實際保安威脅）的百分比。誤報率越高，說明投入非威脅事件的不必要調查或資源越多。降低誤報率有助提高威脅監控的效率，及減輕事故應變小組的負擔。

- ***檢測準確性。***這關鍵績效指標衡量監控系統成功檢測到的真實保安威脅的百分比。該指標能夠反映系統準確識別和標記真正威脅的能力。檢測準確性越高，說明監控能力越完善、越可靠。

- ***事故應變時間。***這關鍵績效指標衡量檢測到保安事故後，啟動適當應變所需的時間。這包括事故分流、評估和啟動事故應變程序所需的時間。縮短事故應變時間可更迅速地控制和緩解威脅。

- ***威脅情報使用。***這關鍵績效指標衡量決策局／部門將威脅情報有效納入其監控和應變程序的程度。該指標評估決策局／部門主動利用外部威脅情報來源識別和解決新興威脅的能力。

- ***受監控資產範圍。***這關鍵績效指標評估主動監控潛在威脅的關鍵資產或系統的百分比。這確保全面覆蓋並識別監控方面存在的缺口，使決策局／部門能夠確定資源配置的緩急次序，並提高其整體監控能力。

- ***遵行監控政策和程序。***這關鍵績效指標評估決策局／部門對既定監控政策和程序的遵行情況。該指標衡量對法規要求、內部政策和業界良好作業模式的遵行情況，確保監控活動符合既定標準。

保安態勢評估提供全面反映決策局／部門整體保安準備的情況，這包括評估保安控制的成效、識別漏洞以及評估決策局／部門偵測和應變威脅的能力。保安態勢評估的示例包括：

- ***滲透測試。***滲透測試涉及模擬真實世界的攻擊，以識別系統、網絡或應用的保安漏洞。通過進行受控和授權測試，決策局／部門可以有效評估其偵測和應變各種攻擊場景的能力。滲透測試的結果有助於確定需要立即關注的具體領域，並根據其關鍵性確定補救行動的緩急次序。

- ***漏洞評估。***漏洞評估包括掃描系統和網絡中的已知保安漏洞和不當配置。通過識別這些弱點，決策局／部門可以立即修補或緩解這些漏洞，從而降低被威脅者利用漏洞的風險。

- ***紅隊演練。***紅隊演練指通過設立專門小組模仿真實攻擊者的策略和技術測試防禦的能力。該模擬可對威脅監控控制和作業的成效進行真實評估。通過挑戰現有的保安措施，紅隊演練有助於發現潛在的漏洞，並識別需要改進的領域。

- ***紫隊演練。***紫隊演練指專家小組同時扮演紅隊和藍隊的角色，旨在通過更實質、更深入的保證活動提供更有針對性和更現實的保證。通過演練，團隊相互學習改進進攻和防禦策略，從而增強決策局／部門的整體資訊科技保安態勢。

決策局／部門應聘用合資格和信譽良好的資訊科技保安專業人員或外部服務供應商，具備必要的專業知識、工具和方法，以進行保安態勢評估。

9.2 評估和更新威脅情報

應定期覆檢和驗證威脅情報來源的相關性和準確性。決策局／部門應建立程序作持續評估，其中可包括以下因素：

- 來源相關性；
- 來源準確性；
- 及時性；
- 質量和可信度。

根據評估結果，決策局／部門應視需要更新其威脅情報來源。這過程可包括新增的威脅來源、刪除不相關或不可信的威脅來源，或根據不同威脅來源的表現和相關性調整其重要性和緩急次序。

9.3 評估和更新控制與技術

應定期評估和更新資訊科技保安控制和技術，以跟上資訊科技保安威脅迅速變化的步伐。決策局／部門在評估和更新控制和技術時應考慮以下因素：

- ***關注行業趨勢。***主動關注威脅監控和檢測方面的行業趨勢和發展。隨時了解資訊科技保安領域的最新技術、工具和方法。通過業界刊物、相關會議和研討會、參加業界論壇和工作小組，以了解最新情況。

- ***威脅監控和檢測技術。***定期評估決策局／部門內部署的威脅監控和檢測技術的成效。評估其對不斷變化的威脅（包括進階持續性威脅、零日漏洞和內部威脅）的識別和應變能力。考慮可增強威脅檢測能力的新技術可用性，例如機器學習、人工智能和行為分析。

- ***評估事故應變計畫。***評估現有事故應變計畫和程序的成效。覆檢有效處理事故的措施，包括應變時間、控制措施和恢復程序。隨時了解最新的事故應變框架和方法，確保與業界良好作業模式和不斷變化的威脅場景保持一致。

- ***合作與共享資訊。***加強與其他決策局／部門和行業合作夥伴的合作和共享資訊。參與知識交流活動，了解其他成功實施的戰略和技術。參與威脅情報共享社區等資訊共享平台，以了解新威脅和有效的緩解戰略。

決策局／部門應根據評估結果更新控制和技術，與不斷變化的威脅環境和行業發展看齊。這過程可包括實施新技術、採用更新的框架和方法，或根據經驗和新興的良好作業模式修訂事故應變計畫。

完

附件 A：威脅分類示例

編號	威脅類型	威脅	威脅詳情
1	社會威脅	欺詐行為	人為欺詐行為
2	社會威脅	盜竊（設備、儲存媒體和文件）	竊取資訊或資訊科技資產。搶劫。
3	社會威脅	資訊泄漏／共享	有意或無意的人為行為或錯誤造成的資訊泄漏／共享。
4	社會威脅	未獲授權的物理接達／未獲授權進入場地	未經批准進入場所。
5	社會威脅	恐怖襲擊	恐怖分子的威脅。
6	技術威脅	使用來源不可靠的資訊	根據不可靠的資訊來源或未獲核實的資訊做出錯誤決定。
7	技術威脅	設計和計畫不足或調整不當	不當的資訊科技資產或業務流程設計導致的威脅（資訊科技產品規格不足、可用性不足、介面不安全、政策／程序流程、設計錯誤）。
8	技術威脅	通訊鏈路（通訊網絡）故障或中斷	通訊鏈路故障或中斷的威脅。
9	技術威脅	拒絕服務	大量服務請求導致服務不可用的威脅。
10	技術威脅	惡意代碼／軟件／活動	執行惡意程式碼或軟件的威脅。
11	技術威脅	未獲授權安裝軟件	未獲授權安裝軟件的威脅。
12	環境威脅	火災	火災威脅。
13	環境威脅	雷擊	雷擊（過量電壓）對資訊科技硬件造成損壞的威脅。
14	環境威脅	水患	水患對資訊科技硬件造成損壞的威脅。
15	環境威脅	爆炸	爆炸對資訊科技硬件造成損壞的威脅。
16	環境威脅	不利的氣候條件	由於氣候條件對硬件產生不利影響而中斷資訊科技系統的工作。
17	環境威脅	野生動物	動物（小鼠、大鼠、鳥類）對資訊科技資產造成破壞的威脅。

以上示例說明了威脅分類法如何協助該決策局／部門識別具體威脅，並確定其緩急次序，使其能夠實施有針對性的保安措施，以保護納稅人資訊並維護其業務的完整性：

該決策局／部門負責執行香港的稅法，並確保稅款徵收，以支持政府運作和公共服務。作為保護納稅人資訊和維護系統完整性工作的一部分，該決策局／部門開展威脅評估，以確定針對其業務的潛在資訊科技保安威脅。

在威脅評估過程中，該決策局／部門識別可能會危及納稅人資料並破壞其業務的各種威脅。

在社會威脅類別，該決策局／部門識別到針對納稅人或決策局／部門員工的網絡釣魚攻擊風險。該等攻擊旨在誘騙人員泄露可用於欺詐的敏感資料，例如稅務編號或登錄憑證。

在技術威脅類別中，該決策局／部門確認勒索軟件攻擊加密其系統的可能性，使其在支付贖金前無法接達。該決策局／部門同時考慮未獲授權接達納稅人數據庫的風險，例如外部黑客攻擊和員工濫用接達權限的內部威脅。

在環境威脅類別中，該決策局／部門辨認到停電或其他基礎設施故障可能會破壞其資訊科技系統，並危及資料可用性。該決策局／部門還考慮到實體漏洞的風險，如未獲授權進入其數據中心或辦公室，可能導致盜竊或篡改敏感納稅人資訊。

根據這些已識別威脅，該決策局／部門建立適合其特定需求的分類。該決策局／部門在每個類別中制定特定的威脅類型，例如將有針對性的稅務網絡釣魚電子郵件定義為社會威脅，將勒索軟件攻擊定義為技術威脅，將物理破壞定義為環境威脅。

通過明確定義的威脅分類，該決策局／部門就可以實施有針對性的保安措施，保護納稅人資料並保持業務的連續性。該決策局／部門投入完善的電子郵件過濾和保安意識計畫，以教育納稅人和員工有關網絡釣魚攻擊的風險。該決策局／部門還實施進階端點保護、定期系統備份和事故應變協定，以減輕勒索軟件和未獲授權接達嘗試的影響。

此外，該決策局／部門建立嚴格的物理保安措施，包括接達控制、監視系統和人員審查，以保護其場所和防止未獲授權的接達。

定期的保安審計和滲透測試有助於識別漏洞，並確保實施保安控制的成效。該決策局／部門還與執法機構、行業協會和其他政府部門保持密切合作，共享威脅情報，協同促進網絡保安活動。

附件 B：針對資訊科技保安威脅情報供應商的問題示例清單

1. 使用的資訊來源範圍有多廣？
   按照情報週期，供應商應從廣泛的原始來源收集情報並加以融合。

2. 如何從原始來源收集情報？
   供應商應能提供足夠的詳細資訊，以確保其收集能力，且理想情況下能夠獨立收集資訊，而不必依賴第三方。

3. 情報涵蓋甚麼類型的威脅者？
   供應商應涵蓋決策局／部門所面臨的所有類型的威脅者，這通常代表需要從不同來源來收集資訊。

4. 所提供的情報是否及時？
   這應取決於所提供情報的級別，即戰略性、策略性或操作性。

5. 情報以何種格式提供？
   這將根據資料的性質和級別而有所不同。然而，分析員接達、現場簡報、定制的報告和情報報告與決策局／部門相關的可能比一般通用的威脅資料更有幫助。

6. 產品如何與現有的功能整合？
   如果決策局／部門擁有現行的供應商和基礎設施，整合能力則非常重要。

7. 產品如何為決策局／部門定制？
   量身定制的產品通常比一般通用產品更有幫助，由技術性的分析員評估的情報相比於數據對決策局／部門而言更有幫助。

8. 對產生的情報採用什麼評估流程？
   優質供應商將採用既定的方法評估情報，並確保其適用於決策局／部門。

9. 如何排除誤報？
   人工審核資料可減少誤報。

10. 團隊的背景和語言能力如何？
    多元化且經驗豐富的分析團隊往往有能力提供最優質成果，團隊成員的個人認證亦很可能是有用的指南。

11. 分析是否具有預測性和反應性？
    優質供應商應為決策局／部門提供前瞻性評估。

12. 團隊成員是否獲得了威脅情報專業人員認證？
    威脅情報實踐有專業的資格認證，例如 CREST 認證和 SANS 等其他組織的資格認證。

13. 貴公司是否被公認的權威機構認證為威脅情報供應商？
    經例如 CREST 的認證除了證明供應商能力，更顯示其具有高度的法律和道德標準。

14. 是否定期提供服務予該等受監管的框架？
    優質供應商將定期為該等框架提供支持服務。

15. 如何展示對我們（買方）行業的了解？
    供應商可能具有定制研究的經驗，並在團隊中擁有專門的主題專家。

16. 貴公司採取了甚麼保安措施確保我們威脅情報的安全？
    鑒於所提供情報的潛在敏感性，供應商應能向客戶確保其保安，例如共同使用客戶資訊保安政策。

17. 如何證明產品和服務的品質？
    供應商應能提供合作成功的參考。

附件 C：威脅應變行動手冊示例

請注意，以下行動手冊是威脅應變的示例，各決策局／部門應根據其具體需求進行調整，而非僅遵循以下步驟。

1. 威脅情報中的新漏洞

階段	簡介
識別	• 識別相關的資訊科技保安威脅並進行分類，包括威脅情報中新發現的漏洞。
監控	• 持續監控網絡流量、系統日誌和保安事故，以查找與已識別漏洞相關的任何指標。
檢測	• 分析收集的資料，例如日誌文件和網絡流量，以檢測可能顯示已識別漏洞被利用的模式或異常。
分流	• 根據可用的漏洞和資產關鍵性的資訊啟動分流。 • 通過分析入侵指標以及策略、技術和程序，檢查是否有任何跡象表明攻擊已經發生。 • 通過將資產與易受攻擊的版本／配置資訊進行匹配，驗證資產是否存在漏洞。 • 根據分流結果升級處理情況。
調查	• 進行徹底的調查，以評估漏洞的影響、識別潛在的攻擊途徑，並為未來的預防收集額外的情報。 • 覆檢防火牆規則和其他保安配置，以識別潛在的攻擊途徑。可利用自動化工具來進行此項工作。
應變	• 與保安營運中心、資訊科技保安管理組和資訊科技支援團隊討論緩解措施。 • 制定並執行行動和措施，以應對已識別的漏洞，這可能包括立即關機、應用修補程式、實施替代方案或考慮未來資產構建的預防措施。 • 重新掃描漏洞以確認完結。

2. 特權帳戶強制身份驗證

階段	簡介
識別	不適用。
監控	• 利用特權接達管理系統監控特權接達的使用情況。 • 監控並記錄來自相關端點的身份驗證活動。
檢測	• 將特權接達管理日誌與相關端點的認證日誌相關聯，以檢測未經授權的使用並識別潛在被竊取的憑證。 • 對未經相應特權接達管理批准的特權帳戶的任何登錄活動觸發警報。
分流	• 根據可用的漏洞和資產關鍵性資訊啟動分流。 • 通過分析入侵指標以及策略、技術和程序，檢查是否有任何跡象表明攻擊已經發生。 • 通過將資產與易受攻擊的版本／配置資訊進行匹配，驗證資產是否存在漏洞。 • 根據分流結果升級處理情況。
調查	• 進一步調查以確定未經授權的接達的範圍、評估潛在的保安漏洞，並為未來的預防收集額外的資訊。 • 聯繫相關系統管理員，詢問他們是否在指定的時間段內使用過該帳戶。 • 如果沒有管理員聲稱對該使用情況負責，則應將合作範圍擴展到包括相關的應用程式支援團隊。 • 如果沒有得出結論，則將其視為事故並執行事故應變。
應變	• 開展事故應變程序，以緩解成功攻擊的影響。 • 更新例外接受風險的關聯規則，以完善偵測流程和準確識別未經授權的特權接達事故。

3. 虛擬私有網絡異常

階段	簡介
識別	不適用。
監控	• 鑒於攻擊者經常利用虛擬私有網絡來保持對組織環境的持續接達，應持續監控虛擬私有網絡的異常。
檢測	• 從身份管理系統接收警報，顯示存在沒有相應帳戶創建批准記錄的虛擬私有網絡帳戶。 • 如果身份管理系統不可用，可手動或通過編譯，將導出的虛擬私有網絡帳戶列表與用戶請求事務跟蹤系統進行對照。 • 用戶報告在未經其同意和非預期的情況下，虛擬私有網絡密碼被更改或註冊的流動裝置被重置。
分流	• 驗證所涉虛擬私有網絡帳戶及其活動的合理性。 • 諮詢虛擬私有網絡管理員以確認帳戶的合理性和活動。 • 收集已識別虛擬私有網絡帳戶的接達日誌，並檢查連接的來源位址。確認他們是否與合法的虛擬私有網絡用戶一致。 • 攻擊者可能會租用決策局／部門用戶群附近的機架空間（例如，同一城市的數據中心）來繞過基於位置的篩檢，因此，在僅依賴地理互聯網規約地址資訊時需謹慎。 • 鑒於虛擬私有網絡系統可能並非攻擊者的初始入口，需根據分流結果將情況上報給相關資訊科技團隊以確定根本原因。
調查	• 進行深入的鑑證分析，以了解虛擬私有網絡異常的根本原因，並識別任何其他受損系統。
應變	• 將發現的異常情況通知虛擬私有網絡帳戶持有者，並建議更改其他系統（包括個人設備）的密碼。 • 如果檢測到未經授權的帳戶或活動，則考慮相關帳戶（甚至虛擬私有網絡系統）為已遭破壞，觸發事故應變。

4. 域名系統回調

階段	簡介
識別	不適用。
監控	• 持續監控與域名系統相關的惡意活動指標。 • 設置域名系統監控發出針對長域名查詢、已知惡意查詢（入侵指標／策略、技術和程序）以及異常域名系統流量和頻率的警報。
檢測	• 識別使用域名系統作為惡意軟件的回調機制，該機制已經發生了演變。 • 入侵防禦系統／入侵偵測系統等網絡保安設備可能會對異常的域名系統查詢發出警報。
分流	• 確認是否存在惡意域名系統活動及其範圍。 • 覆檢域名系統日誌，以確定類似域名系統查詢的開始日期，並識別其他端點的類似行為。根據域名系統伺服器配置將被拒絕的查詢納入日誌覆檢。 • 檢查端點保安事故日誌（例如擴展偵測和回應），查找相關端點上惡意軟件的跡象。 • 如有必要，對受影響的端點進行鑑證分析，以識別負責發送可疑域名系統查詢的過程。
調查	• 進行詳細的鑑證分析，以揭示域名系統回調的根本原因，並識別任何可能受損的系統。 • 分析收集的資料和證據，了解惡意軟件的入侵點。
應變	• 如果確認存在漏洞，則觸發事故應變以調查惡意軟件如何獲得接達權限。 • 在受損主機上實施適當的應變措施，這可能涉及隔離、檢疫隔離或移除惡意軟件。

附件 D：端點偵測和回應採用及架構指引

在不斷變化的網絡保安威脅環境中，端點偵測和回應解決方案已成為決策局／部門保護其數字資產的一道關鍵防線。這些指引旨在提供綜合的端點偵測和回應採用和架構指引，以協助決策局／部門有效實施這些解決方案。

D.1. 端點偵測和回應簡介

端點偵測和回應解決方案扮演了警惕的前哨，強化決策局／部門對潛伏在數字領域各種威脅的防禦。通過採用端點偵測和回應，決策局／部門可以提高其威脅檢測能力、增強事故應變程序，並加強其保安態勢。通過實時監控、行為分析和威脅情報集成，端點偵測和回應賦予決策局／部門主動識別和消除惡意軟件、勒索軟件和內部攻擊等進階威脅的能力。

D.1.1. 端點偵測和回應的核心功能

端點偵測和回應解決方案的核心功能獨具特徵，決策局／部門能因此應變複雜威脅。實時監控、行為分析、威脅情報集成、事故應變自動化和鑑證能力是制定端點偵測和回應解決方案的核心功能。下文將深入探討每個功能的重要性，重點介紹其如何有助於在決策局／部門環境中進行有效的威脅管理和事故應變。部分核心功能如下：

- ***端點可見性：***端點偵測和回應解決方案可實時查看所有端點，包括膝上電腦、桌上型電腦、流動裝置、伺服器和物聯網設備。此可見性使保安團隊可監察和分析端點活動以識別可疑行為。

- ***威脅檢測：***端點偵測和回應解決方案使用進階威脅檢測技術，例如行為分析和機器學習，來識別入侵指標和攻擊指標，亦可通過分析端點事故和遙測數據來檢測潛在威脅並發出警報。

- ***事故調查：***端點偵測和回應解決方案提供調查功能，以分析和了解保安事故。方案提供工具搜索和查詢端點資料，使保安團隊能調查事故的根本原因並收集證據進行進一步分析。

- ***威脅狩獵：***端點偵測和回應解決方案使保安團隊可在端點上搜索潛在威脅和入侵指標，從而實現主動的威脅狩獵。這功能有助於識別可能躲過傳統保安措施的隱藏或進階威脅。

- ***威脅情報集成：***端點偵測和回應解決方案整合威脅情報源，以增強威脅檢測和應變能力。通過利用最新的威脅情報，端點偵測和回應解決方案能夠識別已知的惡意活動，並提供有關攻擊的背景資訊。

- ***實時和歷史資訊可見性：***端點偵測和回應解決方案扮演端點上的數位硬碟錄影機，實時記錄和提供保安相關活動的全面可見性，包括監察網絡連接、用戶登錄、進程

執行和文件創建。歷史資訊可見性使保安團隊可分析過去的事故，並識別模式或趨勢。

- ***事故應變和修復：***端點偵測和回應解決方案通過提供實時應變功能，實現快速果斷的事故應變。這包括在不影響性能的情況下，將受破壞的端點從網絡中隔離、遏制威脅，並修復事故。

D.1.2. 端點偵測和回應與其他產品的區別

在數項關鍵方面，端點偵測和回應解決方案與傳統的端點保安產品（例如防毒軟件或入侵偵測系統）有所不同，以下是主要區別：

1. 檢測方法：

- 傳統的防毒軟件主要依賴基於識別碼的檢測，即把文件與已知惡意軟件識別碼的數據庫進行比較。這種方法對已知威脅有效，但可能難以應對新的或未知的惡意軟件。
- 端點偵測和回應方案則側重於基於行為的檢測。通過實時監控和分析端點活動，查找可能預示潛在威脅的可疑或異常行為。這種方法使端點偵測和回應能夠檢測已知和未知威脅，包括零日攻擊。

2. 可見性和應對能力：

- 防毒軟件通常提供有限的端點活動可見性，通常僅在檢測到已知威脅時發出警報，缺乏詳細了解攻擊鏈的能力，以及有效的應對能力。
- 端點偵測和回應解決方案增強了對端點的可見性和控制能力，收集並分析廣泛的端點資料，包括文件修改、程序創建、網絡連接等。這種全面的可見性使保安團隊快速識別並應對保安事故，將攻擊的影響降至最低。

3. 事故應變和威脅狩獵：

- 傳統防毒軟件主要側重於檢測和阻止惡意軟件，可能無法提供完善的事故應變能力或支援主動的威脅狩獵活動。
- 端點偵測和回應解決方案旨在支持事故應變和威脅狩獵，在同一控制台內提供集成的事故應變能力，保安分析員從而可以快速調查和應變保安事故。端點偵測和回應還提供威脅狩獵支援，使決策局／部門能夠主動搜索入侵指標，並識別可能已躲過其他保安措施的潛在威脅。

4. 自動化和補救：

- 防毒軟件通常依賴於手動干預來進行事故應變和修復。保安分析員需要手動分析和處理檢測到的威脅。
- 端點偵測和回應解決方案可自動執行某些事故應變活動，並提供多種應對選項，如隔離或清除，以解決保安事故。這種自動化簡化了事故應變流程，並降低了保安事故的影響和成本。

端點偵測和回應解決方案超越了傳統的防毒軟件，提供了基於行為的檢測、更強的可見性、事故應變能力以及主動威脅狩獵的支援。它們提供了一種更全面和主動的端點

保安方法，決策局／部門從而能夠檢測、應變和緩解各種的威脅。了解這些區別，決策局／部門可以避免混淆，並選擇提供必要的深度和廣度保護的端點偵測和回應解決方案。

D.2. 端點偵測和回應的部署和實施

部署和實施端點偵測和回應解決方案是一個多步驟的過程，涉及在決策局／部門進行謹慎的規劃、技術配置和保安基礎架構中集成。部署和實施端點偵測和回應的主要注意事項如下：

1. ***制定目標和要求：***首先制定部署端點偵測和回應解決方案的目標和要求。識別決策局／部門利用端點偵測和回應應對的保安挑戰和風險。考慮因素例如需要保護的端點數量和類型、監管合規要求，以及所需水平的可見性和威脅檢測能力。這些資訊將指導選擇適合的端點偵測和回應解決方案。

2. ***評估和選擇解決方案：***對可用的端點偵測和回應解決方案進行全面評估。考慮因素例如解決方案的功能、可擴展性、整合能力、對端點的性能影響，以及供應商的聲譽。利用行為分析、機器學習和威脅情報整合，評估解決方案檢測和應變進階威脅的能力。選擇符合決策局／部門目標、要求和預算的端點偵測和回應解決方案。

3. ***計畫部署：***制定詳細的部署計畫，概述必要的步驟、資源和時間表。考慮因素例如端點覆蓋範圍、代理部署、網絡考慮、與現有保安工具的整合，以及用戶和相關持份者的溝通等。

4. ***基礎設施的準備情況：***確保決策局／部門的基礎設施滿足端點偵測和回應解決方案的要求。驗證必要的硬件、網絡資源和存儲容量是否可用。識別現有系統或軟件的任何潛在相容性問題。

5. ***安裝和配置：***根據供應商的指引，在指定的伺服器或設備上安裝端點偵測和回應解決方案。根據決策局／部門的保安目標和操作要求，配置解決方案的設置、政策和規則。這包括制定應從端點收集的事件和資料，設置檢測規則，以及配置應變操作。

6. ***部署端點代理：***在需保護的端點上部署端點偵測和回應代理，可能涉及自動部署方法，例如軟件分發工具或群組政策，以確保在所有端點進行一致和高效的安裝。驗證代理是否已在每個端點成功安裝並運行。

7. ***與保安基礎架構整合：***將端點偵測和回應解決方案與決策局／部門環境中的其他保安工具和系統整合，可能涉及資料來源配置、與保安資訊和事件管理系統的整合，或與威脅情報平台的連接。確保正確整合以及資料在端點偵測和回應解決方案和其他保安組件之間的無縫流動。

8. ***調整和定制：***調整端點偵測和回應解決方案，使其符合決策局／部門的特定需求和環境。根據決策局／部門的風險承受能力、合規要求和操作注意事項，調整檢測規則、政策和應變措施。自訂警報和通知，以確保相關保安事件得到適當的優先處理並傳達予保安分析員。

9. ***測試和驗證：***對端點偵測和回應解決方案進行全面測試和驗證，確保其有效性和準確性。模擬各種攻擊場景，評估解決方案檢測和應變這些威脅的能力。驗證解決方案是否生成準確的警報，捕獲所需的端點遙測，並按預期執行。

10. ***監察和維護：***建立持續的監察和維護流程，確保端點偵測和回應解決方案持續有效。定期覆檢和分析端點偵測和回應警報和事件，以識別保安事故和潛在威脅。通過產品供應商提供的更新、修補程式和威脅情報源，保持解決方案的最新狀態。執行常規的維護任務，例如數據庫優化、日誌輪換和系統健康檢查。

11. ***員工培訓和意識：***提供端點偵測和回應解決方案的特點、功能和最佳實踐的培訓予保安營運團隊，確保團隊能有效地使用解決方案進行威脅偵測、調查和應變。此外，提高終端用戶對端點偵測和回應解決方案、其目的以及任何保安程序或政策變更的意識。

D.2.1. 端點偵測和回應的覆蓋範圍

為確保全面覆蓋和有效的威脅管理，端點偵測和回應解決方案必須將其保護範圍擴展到傳統端點之外。覆蓋範圍通常包括決策局／部門網絡中的各種端點設備，包括：

- ***桌上型電腦和膝上電腦：***端點偵測和回應解決方案通常涵蓋運行各種作業系統（例如 Windows、macOS 和 Linux）的桌上型電腦和膝上電腦。這些端點通常由決策局／部門的員工使用。

- ***伺服器：***端點偵測和回應解決方案通常將其覆蓋範圍擴展到對決策局／部門基礎設施至關重要的物理和虛擬伺服器，包括文件伺服器、應用伺服器、數據庫伺服器和雲端伺服器。

- ***流動裝置：***隨著流動裝置在工作場所的使用日益增多，端點偵測和回應解決方案也宜為智慧手機和平板電腦提供保護，包括運行安卓或 iOS 作業系統的設備，確保流動裝置端點免受保安威脅。

- ***虛擬機器：***大量使用虛擬化技術的決策局／部門可能需要能夠監察和保護虛擬機器（VMs）的端點偵測和回應解決方案。這些虛擬機器可以存放在例如 VMware、Hyper-V 或 KVM 等管理程式上。

- ***物聯網設備：***隨著物聯網在決策局／部門中日益普及，端點偵測和回應解決方案可能需覆蓋連接到網絡的物聯網設備，包括的設備例如互聯網規約地址攝像頭、智慧恒溫器、工業感測器和其他物聯網端點等。

- ***嵌入式系統：***部分決策局／部門可能需要對專用嵌入式系統或設備提供端點偵測和回應覆蓋，例如銷售點系統、自動櫃員機、工業控制系統或醫療設備。這些設備可能具有獨特要求和限制需要加以解決。

- ***自助服務亭：***部分決策局／部門可能需要端點偵測和回應覆蓋專用的自助服務亭。這些自助服務亭可在公共場所、零售環境或其他允許自助互動的地點中找到。端點偵測和回應解決方案可為其提供保護，確保端點免受保安威脅和漏洞。

建立強大的保安態勢需要對所有端點類型進行一致的覆蓋。決策局／部門應注意採用統一方式的端點偵測和回應的重要性。通過將桌上型電腦、工作站、伺服器、流動裝置等集成到一個集中的監察和應變系統中，決策局／部門可以有效地檢測、調查和應變威脅。應詳細說明管理各種各樣的端點環境的策略，包括策略執行和代理管理，以確保採取協調一致的防禦策略。

附件 E：威脅監控架構示意圖

下圖為全面的威脅監控架構的例子，展示了相互連接的監控工具共同監控資訊科技保安威脅。

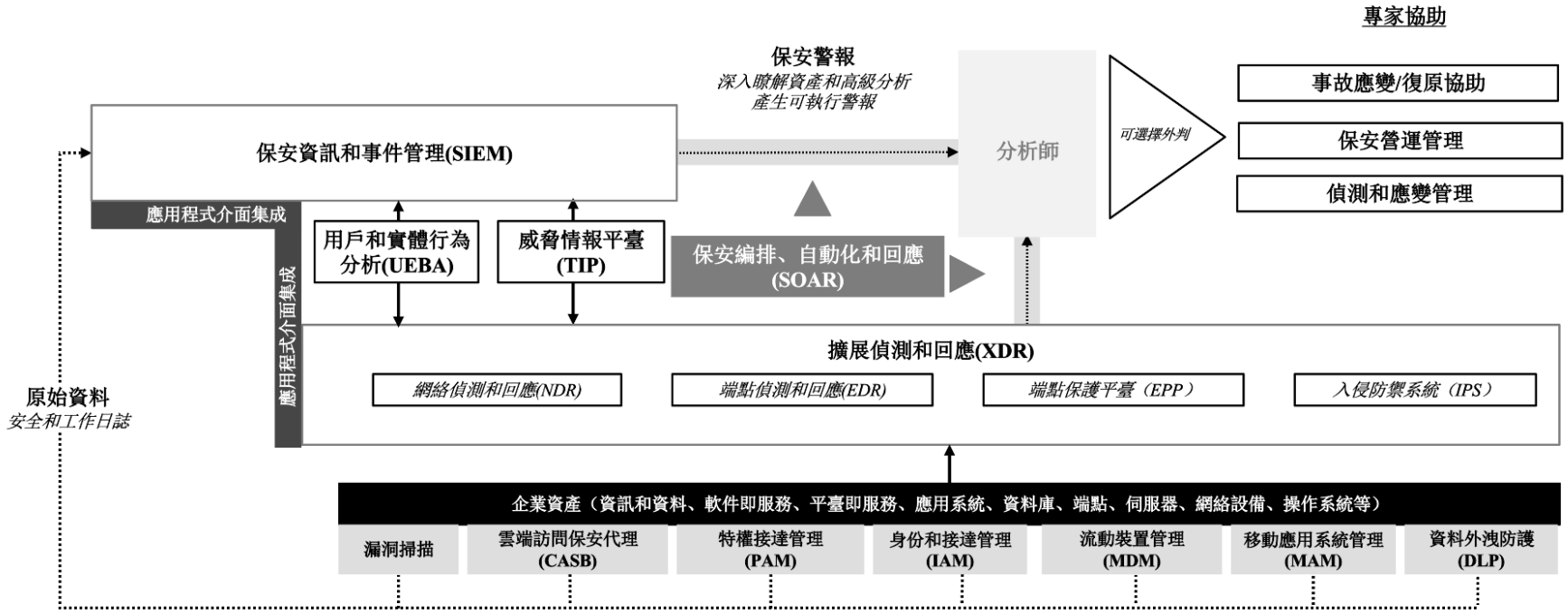

圖 E.1 威脅監控架構示意圖