COHESITY

Cyberworld

如何部署 Cohesity Clean Room 解決方案

快速指南

Cohesity Clean Room 解決方案提供了一個可信環境，可提升資安事件應變速度，支援SecOps調查，同時最大限度地降低被二次攻擊的風險。

由於採用了模組化設計，Cohesity可以快速建立一個隔離環境，支援應變與復原流程，讓團隊更快地減輕威脅。

五個階段

1. **準備** — 做好應對網路攻擊的準備
2. **啟動** — 最低可行應變能力 (MVRC)
3. **調查** — 確定攻擊的範圍與原因
4. **緩解** — 修復、修補、強化、測試
5. **復原** — 驗證、可信的生產復原

階段 1

準備

準備階段著重於採取主動措施，以減輕攻擊的影響，確保企業在需要時能夠使用可信賴的資源。

COHESITY

Cyberworld

1

3-2-1 備份原則

至少製作 3 份數據副本。

2 份副本存放在本地的不同媒體上，1 份副本存放在異地。

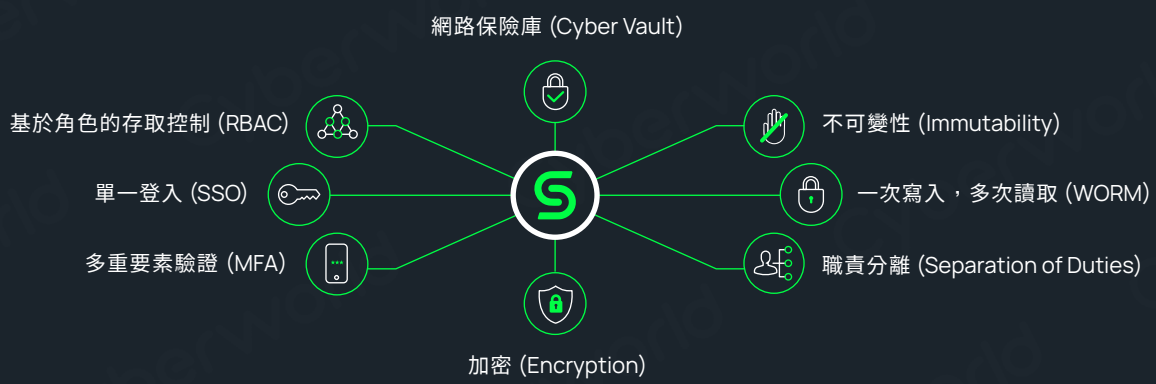
部署拓撲

		備份	複製	雙複製 (Dual-Replication)	存檔	雙存檔 (Dual-Archive)
基本 2 份或更少副本	拓撲 1	✓	-	-	-	-
	拓撲 2	✓	✓	-	-	-
	拓撲 3	✓	-	-	✓	-
增强 3 份副本	拓撲 1	✓	✓	-	✓	-
	拓撲 2	✓	-	✓	-	-
關鍵任務 4 份或更多副本	拓撲 1	✓	-	✓	✓	-
	拓撲 2	✓	✓	-	-	✓
	拓撲 3	✓	-	✓	-	✓

2

强化您的 Cohesity 平台

透過實施主動措施來提高數據的安全性，減少漏洞並緩解潛在風險。



COHESITY

Cyberworld

3

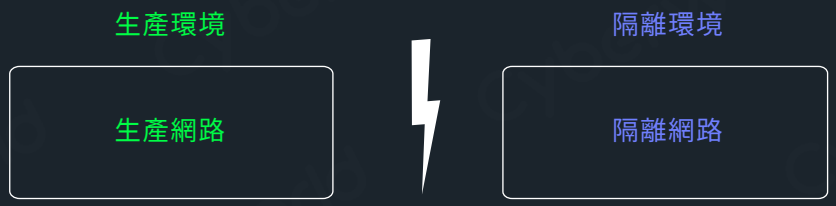
準備好您的數位應急包 (digital jump bag™)

在 Cohesity SmartFiles View 上準備一個軟體儲存庫，用於存放關鍵工作負載的黃金映像(golden image)，包括 ISO、軟體、設定檔、檔案、範本等，這些都是建立隔離環境所需的。

4

隔離您的網路

規劃網路分段，確保隔離環境與生產網路完全斷開連線，可以使用專用網路交換器或虛擬區域網路 (VLAN) 來實現。



5

建立通訊協定

清晰的通訊協定可確保有效的協調，減少混亂，並最大限度地減少停機時間。

流程	目的
角色與責任	確保問責制。您可以將具體任務分配給團隊成員（事件協調員、IT 應變人員、法律顧問、高階主管），由他們負責決策。
通訊管道與工具	安全且集中化的通訊。建立專用管道，例如內部通訊使用 Slack 或 Microsoft Teams（啟用 VPN），安全的外部通訊則使用 ProtonMail 。
通訊計劃	有效協調。使用 Confluence 或 Google Docs 等工具建立結構化計劃，詳細說明在復原階段中由誰負責通訊、傳達什麼內容、以及何時進行。
定期更新	即時更新。使用 ServiceNow 或 PagerDuty 中的儀表板，通知所有利害關係人進度與後續步驟。

階段 2

啟動

啟動階段涉及建立最低可行應變能力 (Minimum Viable Response Capability, MVRC)，包括控制資安漏洞、復原基本操作、最大限度地減少停機時間所需的關鍵工具與流程，以幫助確保網路攻擊期間的營運連續性。

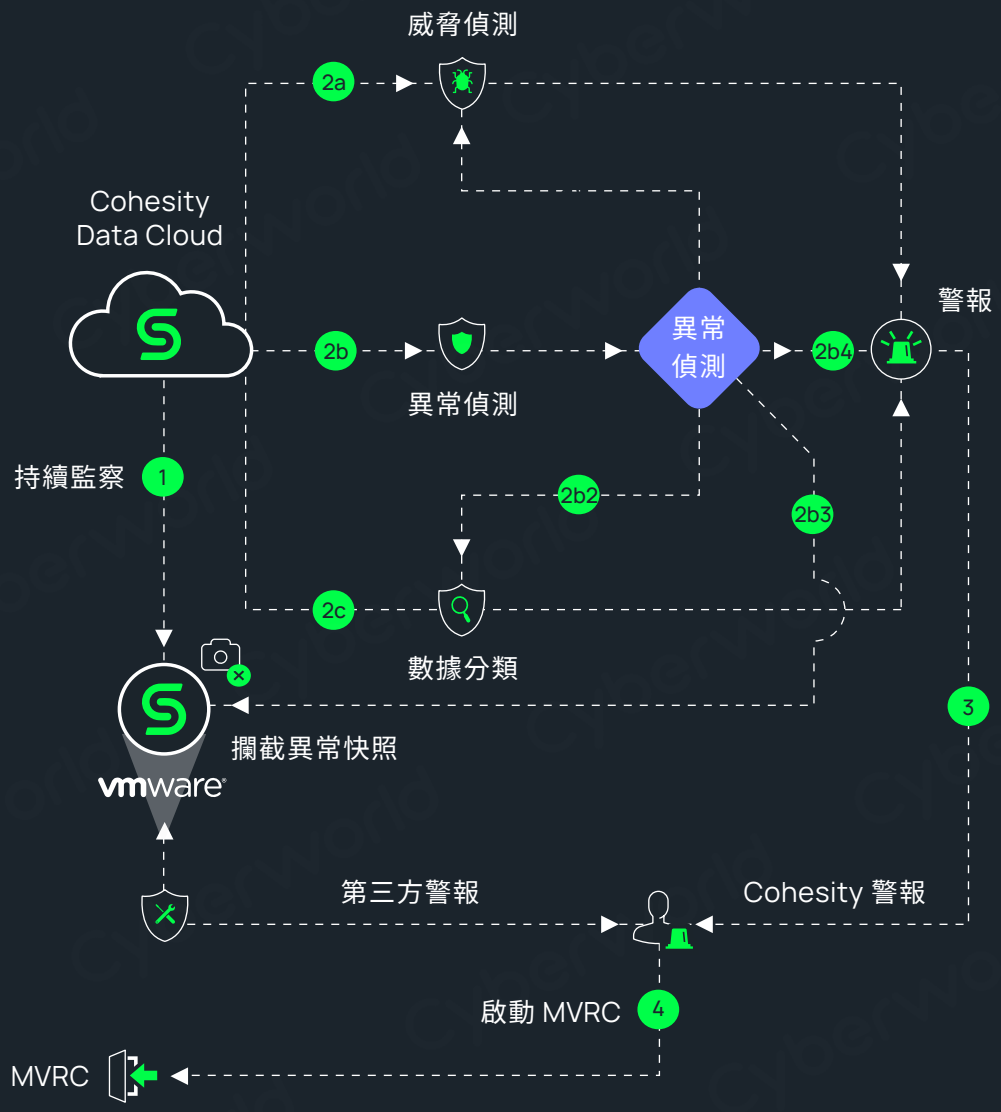
1

偵測網路攻擊

網路攻擊可以由 Cohesity 的異常與威脅偵測功能自動偵測，或由客戶使用其他資安工具來偵測。一旦偵測到網路攻擊，啟動階段就開始了。

COHESITY

Cyberworld



2

識別 Cohesity Source Cluster（來源叢集）

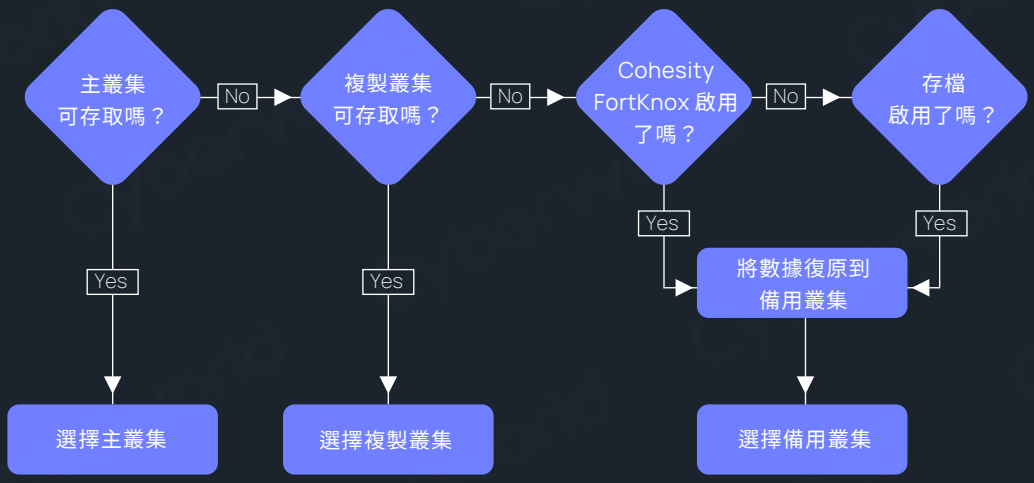
要確定從哪個 Cohesity Source Cluster 中檢索數據或快照，以便用於在 Clean Room 進行取證分析。
從 Cohesity Source Cluster 中選擇要用於取證分析的數據或快照。

位置	形式
客戶自己管理的 本地數據中心	· 主叢集 (Primary Cluster) · 複製叢集 (Replication Cluster) · 虛擬隔離 (Virtual air-gapped) 複製叢集 · NAS 存檔
雲端	· FortKnox（虛擬隔離網路保險庫） · 雲端存檔 (AWS / Azure / GCP)

COHESITY

Cyberworld

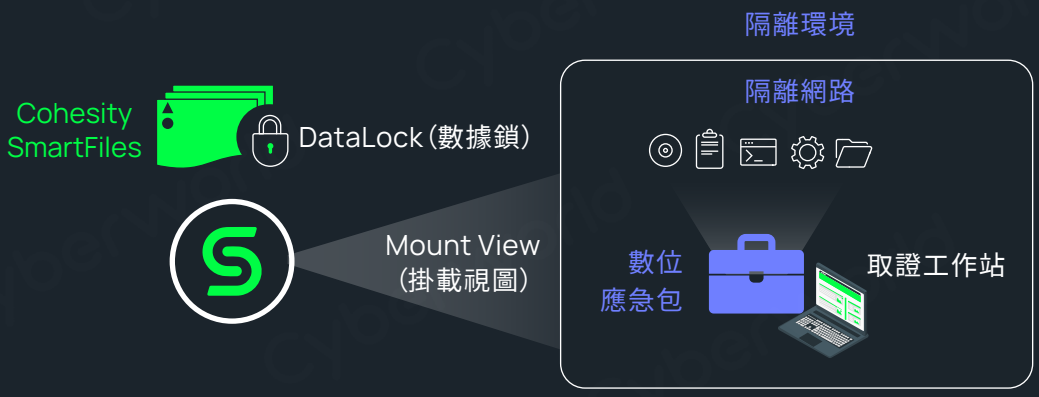
Cohesity 可以從上述任何形式中復原數據。



3

檢索您的數位應急包

將數位應急包掛載到 Clean Room 的主機上。
如準備階段所述，數位應急包位於 Cohesity SmartFiles View 上。



數位應急包檢索策略

位置	描述	用例
主叢集	數據中心或生產位置的 Cohesity Cluster	· 當您的生產環境受到信任時 · 用於資安演練
隔離開的複製叢集	災難復原 (DR) 站點上的 Cohesity Cluster 有複製副本	· 當主叢集發生故障時 · 在 DR 站點檢索數位應急包
FortKnox	Cohesity 安全保險庫解決方案	· 當主叢集與複製叢集都無法存取時

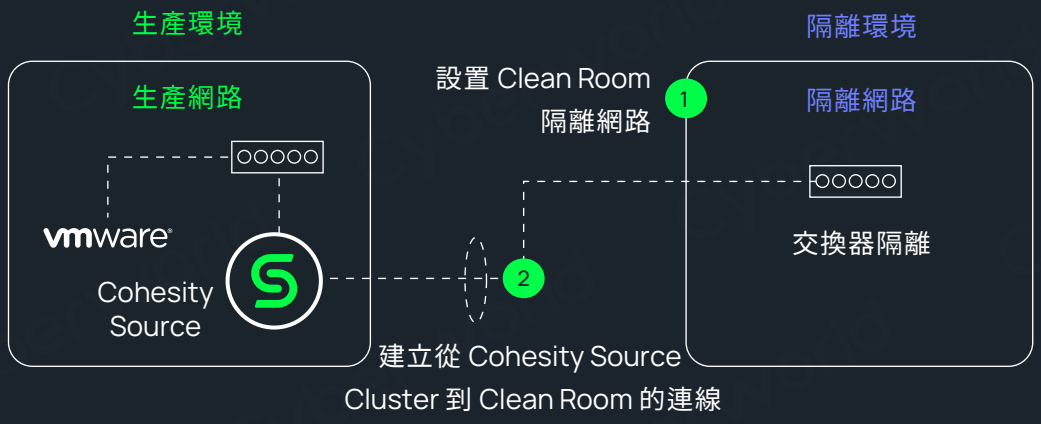
COHESITY

Cyberworld

4

設置隔離的 Clean Room 網路

如準備階段所述，在 Clean Room 中設置一個隔離網路，
並建立 Clean Room 與您的 Cohesity Source（在上一步中選擇）之間的連線。

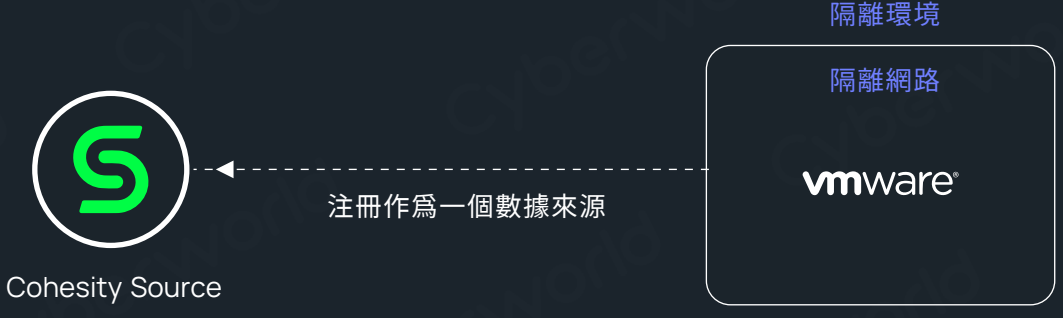


5

設置您的 Clean Room 基礎設施

利用數位應急包組件建立您的 Clean Room 基礎設施。使用數位應急包在 Clean Room 中設定網路組件、虛擬環境、撥號音應用程式 (Dial Tone Applications)。

在 Clean Room 中安裝的虛擬環境，必須在 Cohesity Source Cluster（生產或複製）上注冊，作爲一個數據來源，以便您從中將快照復原到 Clean Room 進行調查。



* 撥號音應用程式 (Dial Tone Applications) 是指一些基本的業務工具及系統，例如電話系統、身分識別與存取管理 (IAM)、電子郵件、DNS、資安工具等。

COHESITY

Cyberworld

階段 3

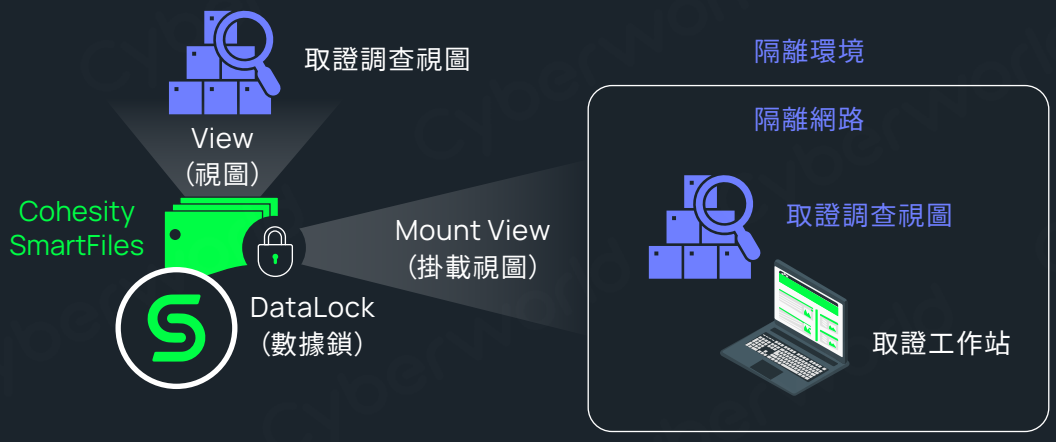
調查

調查階段著重於了解網路攻擊的範圍與影響，確定攻擊原因，
評估其對系統的影響程度，並保留證據以供進一步調查。

1

建立取證調查視圖

在 Cohesity SmartFiles View 上準備取證儲存庫，用於收集證據。然後，將這個取證調查視圖掛載到 Clean Room 中的取證工作站上。



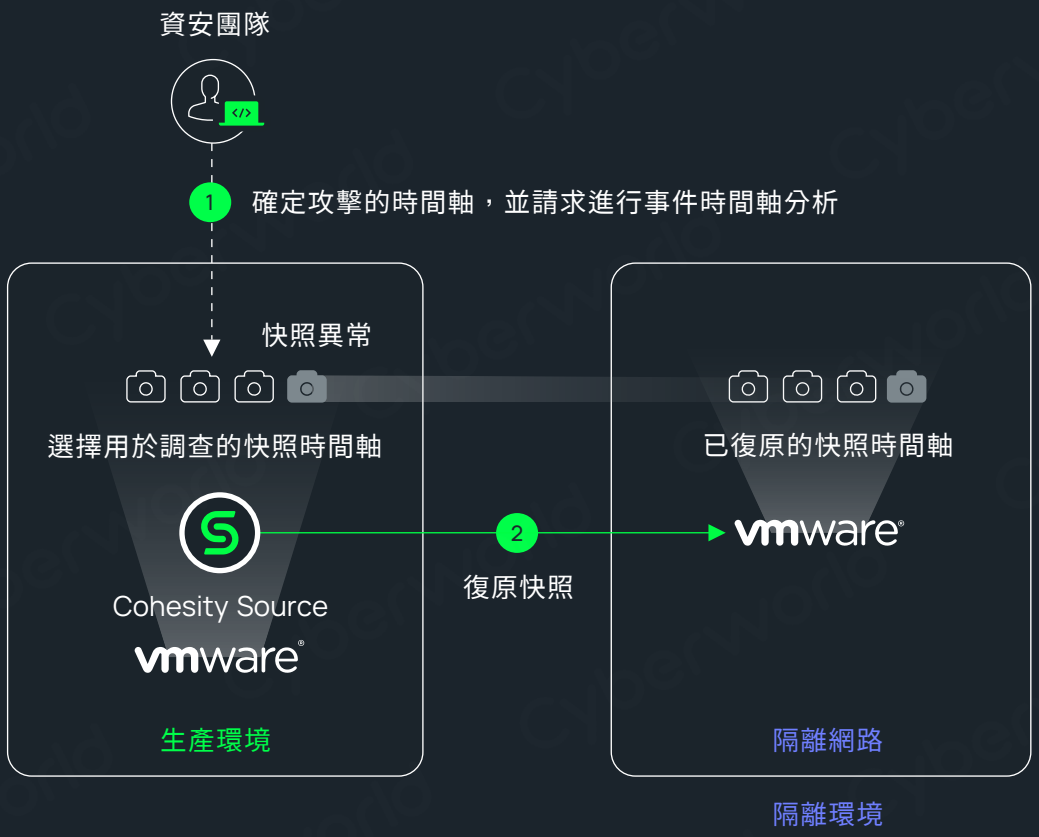
2

復原用於調查的系統與數據

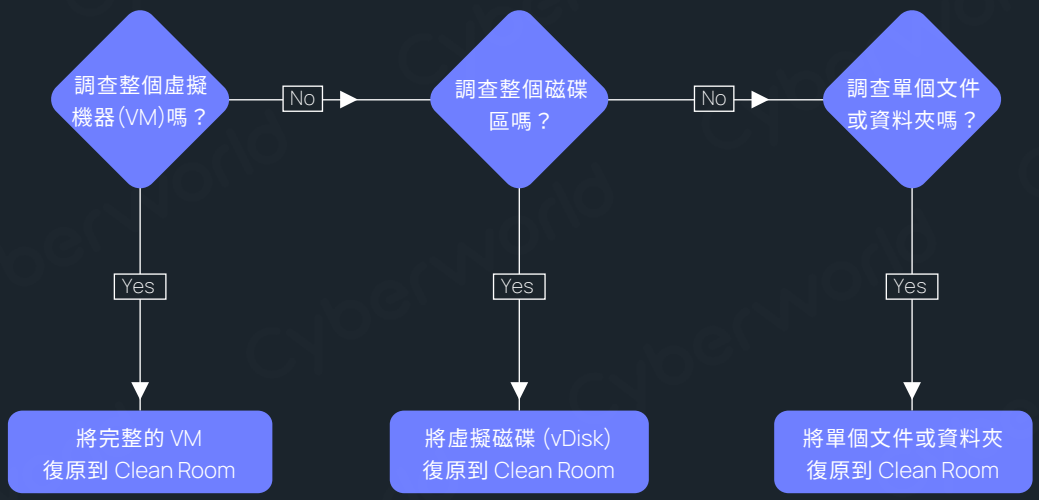
將您需要的系統、磁碟區、文件及資料夾，連同其他收集的證據一起復原到 Clean Room 中。
確定事件的時間軸，並關聯攻擊的細節，以用於緩解措施。

COHESITY

Cyberworld



選擇復原方法



* 根據您的 SecOps 決策，選擇是否復原整個磁碟區、單個資料夾或文件。

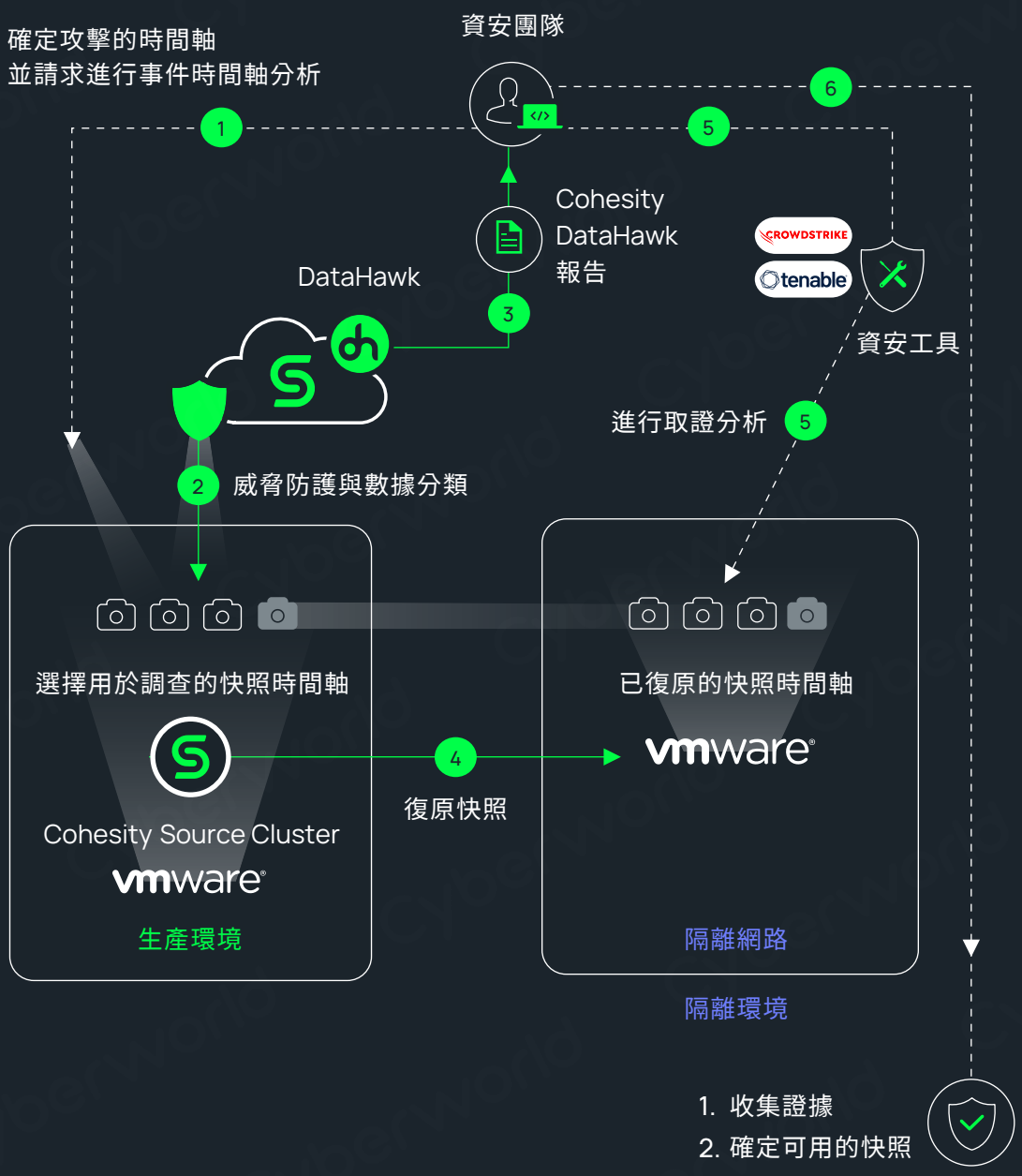
3

進行取證調查

使用資安工具及 Cohesity DataHawk 報告，在 Clean Room 中對已復原的快照進行取證檢查。

COHESITY

Cyberworld



- 在取證調查期間，動員您的資安事件應變處理團隊。
- 比較 Active Directory (AD) 的變更，以確保使用者帳戶、權限及設定的完整性。

建議

使用 Cohesity DataProtect 保護您的 AD，並輕鬆比較您的 AD 快照。

[1] 在您選擇的時間內，對所需範圍的快照執行 DataHawk 操作。

[2] 所需範圍的快照會被復原到 Clean Room，並對其進行調查。

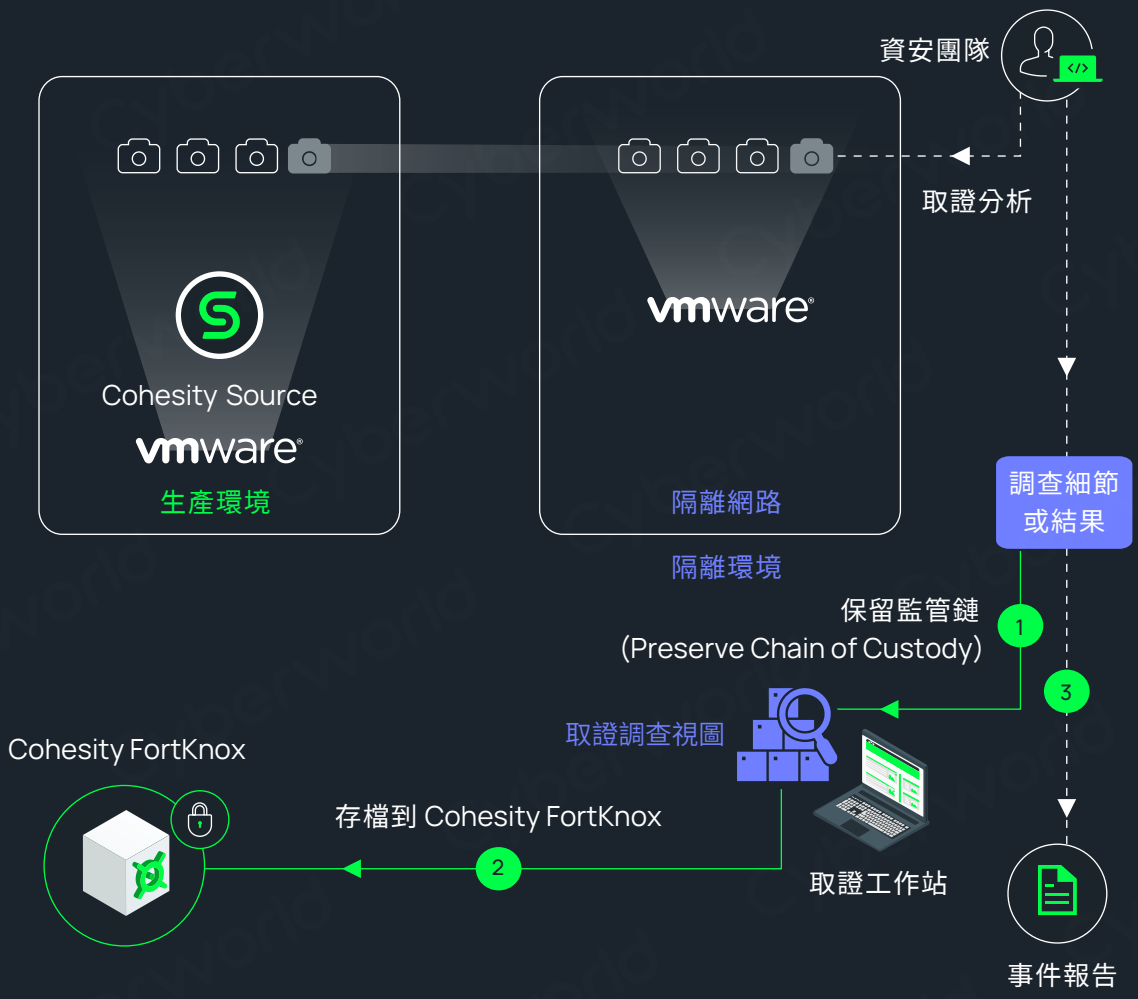
COHESITY

Cyberworld

4

保存證據

收集所有取證調查的細節及結果，將其保存在步驟 1 建立的取證調查視圖中。



調查階段的成果

- 建立可用的快照，用於緩解措施。
- 建立事件報告，詳細說明修復及消除步驟。

階段 4

緩解

緩解階段著重於採取措施限制損害程度，在暫存環境中復原及測試受影響的系統，從網路中刪除惡意軟體，並防止進一步感染。

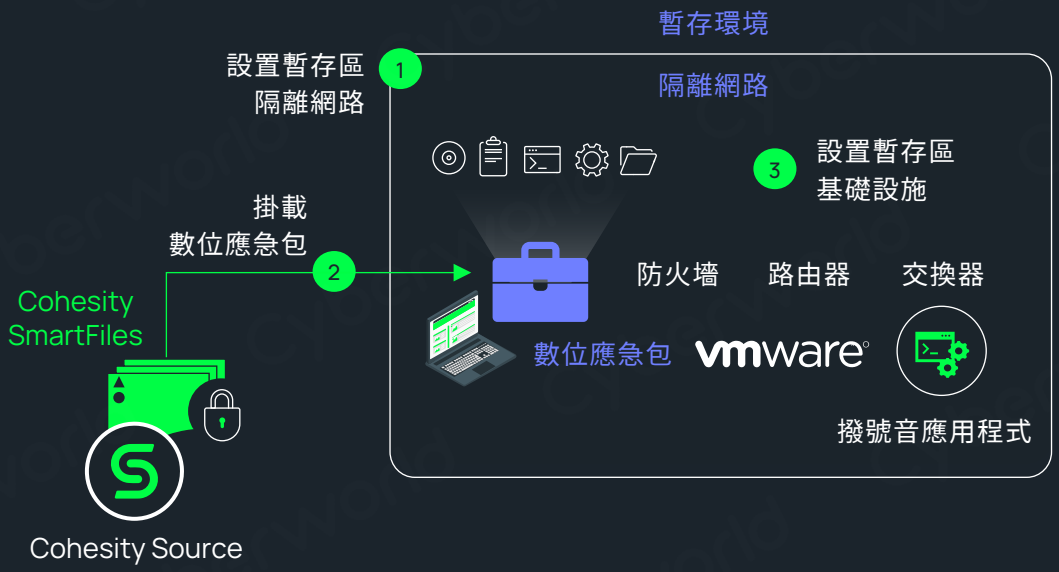
COHESITY

Cyberworld

1 設置暫存區 (Staging Room)

暫存區是一個隔離且受控的環境，類似於 Clean Room。在暫存區，數據與系統會進行全面的修復及驗證，以確保它們不會受到威脅或損壞。

按照準備 Clean Room 的相同步驟來準備暫存區。詳情請參閱「啟動階段」。



---

2 復原系統與數據

將系統與數據復原到暫存區進行修復。

決定是否復原或重建系統與數據

1. 從 Cohesity 備份中將系統與數據復原到暫存區，並進行修復。
2. 用黃金映像在暫存區中重建系統。從 Cohesity 備份中復原數據到暫存區進行修復。

COHESITY

Cyberworld

3

修復

使用調查階段的事件報告來修復受影響的工作負載。

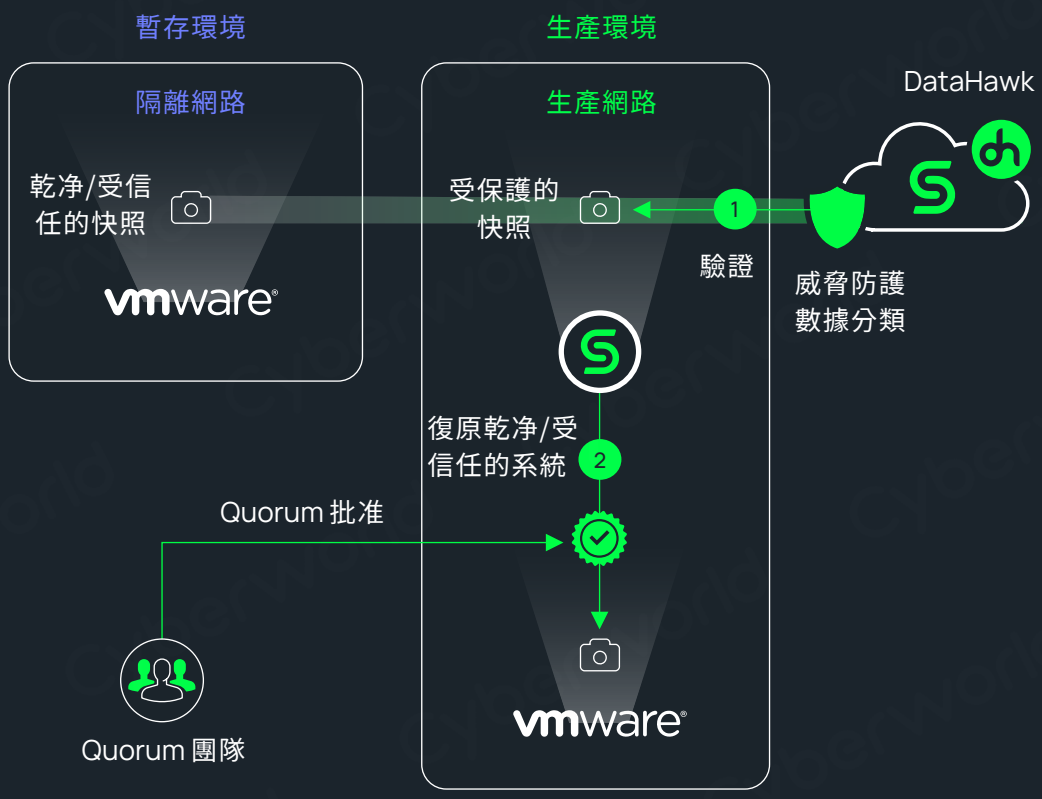
修復步驟

步驟	目的	責任方
修補	解決已知問題或更新軟體系統，以防止威脅利用漏洞。	IT 團隊
漏洞修復	解決系統中的安全弱點與漏洞，以防止漏洞及攻擊，包括修補系統。	IT 團隊
系統强化	透過減少攻擊面與應用安全控制來增強系統的安全性，以防範威脅及未授權的存取。	IT 或資安團隊
整合測試	確保不同的組件與系統能夠無縫協作，在部署到生產環境之前，識別並解決任何問題。	IT 或資安團隊

階段 5

復原

復原階段著重於最終驗證以及將乾淨的系統安全復原到生產環境。同時，IT 與資安團隊需要實施長期的改進或調整，避免未來再次發生類似的攻擊。



Cyberworld
台灣科明大同科技有限公司

COHESITY
AUTHORIZED DISTRIBUTOR

大中華區總代理
網址 www.cyberworld.com.tw
電話 +886-2-7724-8320
電郵 info@cyberworld.com.tw