上的網路威脅情報共用 AWS

AWS 方案指引

AWS 方案指引: 上的網路威脅情報共用 AWS

Table of Contents

簡介 1
CTI 共用模型 3
雲端本身的安全 3
雲端內部的安全 3
CTI 架構 4
部署威脅情報平台 5
擷取 CTI 6
自動化安全控制 6
Amazon GuardDuty 8
Amazon Route 53 Resolver DNS 防火牆 9
AWS Network Firewall 11
取得可見性 12
記錄網路流量 12
在 中集中化安全調查結果 AWS 12
將 AWS 安全資料與其他企業資料整合 14
共用 CTI 15
後續步驟 17
AWS 資源 17
AWS 服務 文件 17
STIX 資源 17
威脅情報平台 18
貢獻者 19
編寫 19
檢閱 19
技術寫入 19
文件歷史紀錄 20
..... xxi

上的網路威脅情報共用 AWS

Amazon Web Services （貢獻者）

2024 年 12 月 (文件歷史記錄)

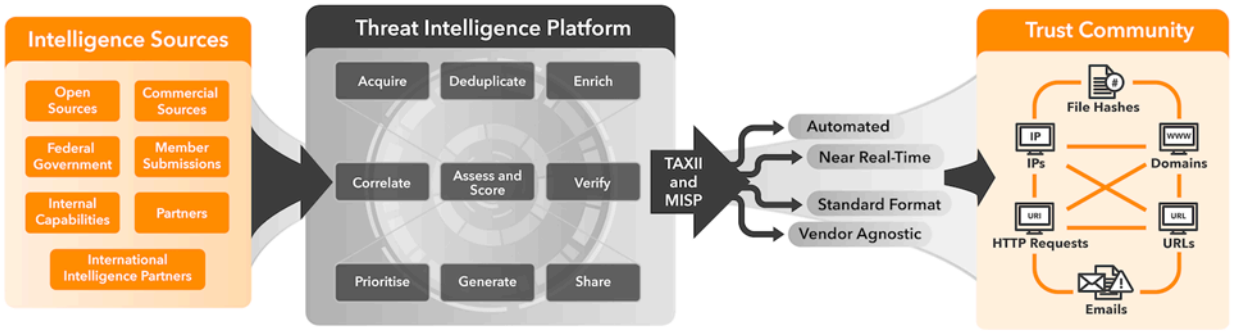
隨著新風險的出現，保護關鍵雲端工作負載的最佳實務會持續演進。隨著需要保護的網際網路連線資產數量增加，與威脅執行者相關聯的安全事件風險也會增加。網路威脅情報 (CTI) 是資料的收集和分析，指出威脅行為者的意圖、機會和能力。它以證據為基礎且可採取行動，並通知網路防禦活動。它通常包含有關演員歸因、策略技術和程序、動機或目標的資訊。

CTI 可以在組織內、信任社群中的組織之間、與資訊共用和分析中心 (ISACs) 共用，或與其他實體共用，例如政府機構。政府機構的範例包括澳洲網路安全中心 (ACSC) 和美國網路安全與基礎設施安全局 (CISA)。

如同所有形式的情報，威脅內容至關重要。CTI 共用會通知動態網路安全風險管理。這對於及時的網路安全防禦、回應和復原至關重要。這可提高網路安全功能的效率和有效性。威脅內容對於區分與不同目標相關的 CTI 功能需求也至關重要。例如，複雜的演員可能會以特定企業或政府為目標，而商品演員則使用隨時可用的工具和技術來廣泛攻擊個人和組織。

安全規劃、可觀測性、威脅情報分析、安全控制自動化和信任社群內的共享是威脅情報生命週期的關鍵部分。 AWS 可協助您自動化手動安全任務，以偵測準確性更高的威脅、更快回應，並產生您可以共享的高品質威脅情報。您可以探索新的網路攻擊、分析它、產生 CTI、共用並套用它，所有速度都旨在防止第二次攻擊發生。

本指南說明如何在 上部署威脅情報平台 AWS。信任社群提供 CTI，平台會擷取 CTI 以識別可行的智慧，並自動化 AWS 環境中的保護和偵測控制。下圖顯示威脅情報生命週期。CTI 從來源抵達，然後威脅情報平台會處理它。透過使用受信任的自動資訊交換 (TAXII) 通訊協定或惡意軟體資訊共用平台 (MISP)，CTI 會與信任社群共用以進行動作。



威脅情報平台會使用 CTI 在您的 AWS 環境中自動實作安全控制，或在需要手動動作時通知您的安全團隊。預防性控制是一種安全控制，旨在防止事件發生。範例包括使用網路防火牆、DNS 解析程式和其他入侵預防系統 (IPSs)，以自動化封鎖已知不良 IP 地址或網域名稱的清單。偵測性控制是一種安全控制，旨在於事件發生後偵測、記錄和提醒。範例包括持續監控惡意活動，以及搜尋日誌以取得問題或事件的證據。

您可以在集中式安全可觀測性工具中彙總任何問題清單，例如 AWS Security Hub CSPM。然後，您可以與信任社群共用調查結果，以協作方式建立全面的威脅情況。

CTI 共享的共同責任模型

AWS 共同責任模型定義了您如何與 共同 AWS 承擔雲端中安全和合規的責任。 AWS 保護執行 中所有服務的基礎設施 AWS 雲端，稱為雲端安全性。您有責任保護對這些服務的使用，例如您的資料和應用程式。這在雲端稱為安全性。

雲端本身的安全

安全性是 的首要任務 AWS。我們努力協助防止安全問題對您的組織造成中斷。當我們努力保護基礎設施和您的資料時，我們會使用全球規模的洞見，以大規模且即時的方式收集大量安全智慧，以協助自動保護您。可能的話， AWS 及其安全系統會中斷該動作最具影響力的威脅。通常，這項工作發生在幕後。

每一天，在 AWS 雲端 基礎設施中，我們都會偵測並成功阻止數百個網路攻擊，否則可能會造成破壞且代價高昂。這些重要但主要看不見的勝利是透過全球感應器網路和相關聯的一組中斷工具來實現的。使用這些功能，我們會讓網路攻擊對我們的網路和基礎設施進行更困難且更昂貴。

AWS 擁有任何雲端供應商的最大公有網路足跡。這可讓您 AWS 即時深入了解網際網路上的特定活動。MadPot 是全球分佈的威脅感應器網路 （ 稱為 Honeypots)。MadPot 可協助 AWS 安全團隊了解攻擊者的策略和技術。只要攻擊者嘗試以其中一個威脅感應器為目標， 就會 AWS 收集和分析資料。

Sonaris 是另一個內部工具， AWS 用於分析網路流量。它會識別並停止未經授權存取大量帳戶和資源的嘗試。在 2023 年 5 月到 2024 年 4 月期間，Sonaris 拒絕了超過 240 億次嘗試掃描存放在 Amazon Simple Storage Service (Amazon S3) 中的客戶資料。它也防止近 2.6 兆次嘗試探索在 Amazon Elastic Compute Cloud (Amazon EC2) 上執行的易受攻擊工作負載。

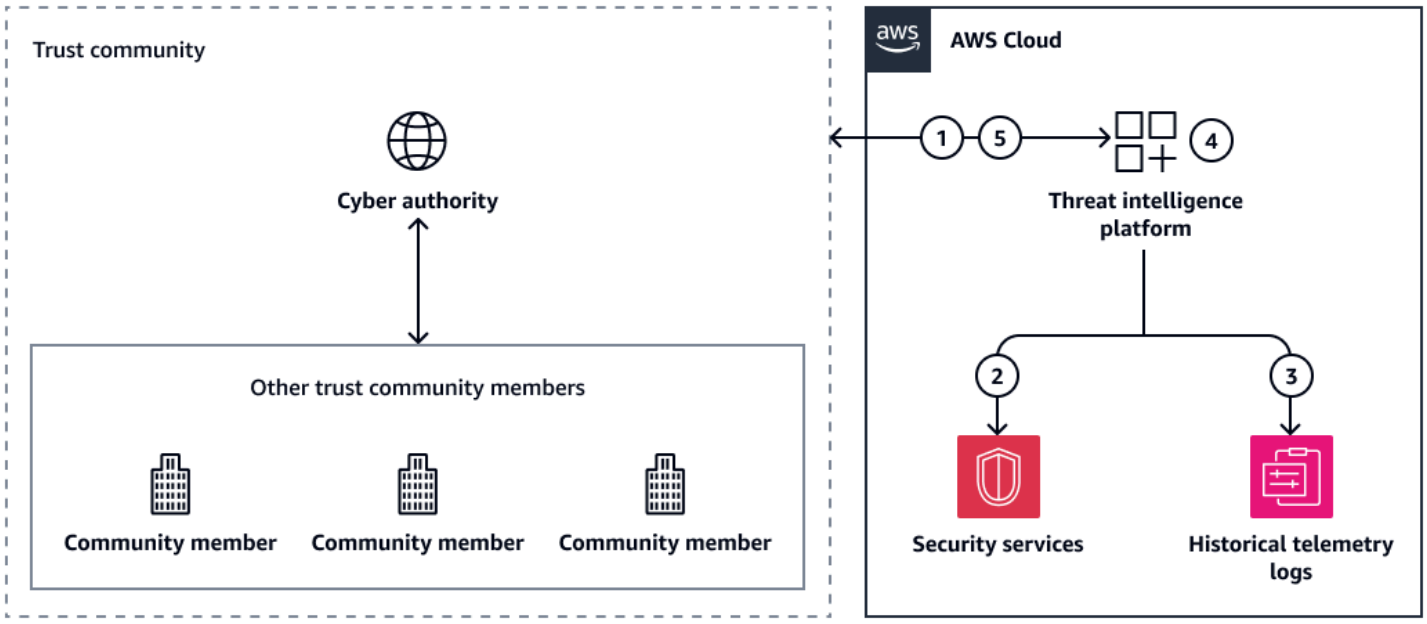
雲端內部的安全

本指南著重於 中的網路威脅情報 (CTI) 最佳實務 AWS 雲端。您負責產生當地語系化和情境化 CTI。您可以控制資料的存放位置、如何保護資料，以及誰可以存取資料。 AWS 無法查看記錄、監控和稽核資料，這對於雲端中的 CTI 型安全至關重要。

結構化威脅資訊表達式 (STIX) 是一種開放原始碼語言和序列化格式，用於交換 CTI。檔案雜湊、網域、URLs、HTTP 請求和 IP 地址等指標是用於威脅封鎖的重要輸出。不過，有效的動作依賴於其他智慧，例如確定性評分和入侵集相互關聯。STIX 2.1 定義 18 個 STIX 網域物件，包括攻擊模式、動作、威脅行為者、地理位置和惡意軟體資訊。它還引入了概念，例如可信度評分和關係，以協助實體判斷威脅情報平台收集的大量資料中來自雜訊的訊號。您可以偵測、分析和分享有關環境中 AWS 威脅的詳細程度。如需詳細資訊，請參閱本指南中的 自動化預防性和偵測性安全控制。

上的網路威脅情報架構 AWS

下圖說明使用威脅饋送將網路威脅情報 (CTI) 整合到您的 AWS 環境的廣義架構。CTI 會在 中的威脅情報平台 AWS 雲端、選取的網路授權機構和其他信任社群成員之間共用。



它顯示下列工作流程：

1. 威脅情報平台會從網路授權單位或其他信任社群成員收到可採取動作的 CTI。
2. 威脅情報平台會任務 AWS 安全服務來偵測和防止事件。
3. 威脅情報平台會從 接收威脅情報 AWS 服務。
4. 如果發生事件，威脅情報平台會策劃新的 CTI。
5. 威脅情報平台會與網路授權機構共用新的 CTI。它也可以與其他信任社群成員共用 CTI。

有許多網路授權機構提供 CTI 饋送。範例包括澳洲網路安全中心 (ACSC)、英國國家網路安全中心提供的 Connect Inform Share Protect (CISP) 計劃，以及紐西蘭政府通訊安全局提供的惡意軟體免費網路 (MFN) 計劃。許多 AWS 合作夥伴也提供 CTI 共用摘要。

若要開始使用 CTI 共用，建議您執行下列動作：

1. 部署威脅情報平台 – 部署可從多個來源以不同格式擷取、彙總和組織威脅情報資料的平台。

2. 擷取網路威脅情報 – 整合您的威脅情報平台與一或多個威脅饋送提供者。當您收到威脅摘要時，請使用您的威脅情報平台來處理新的 CTI，並識別與您環境中安全操作相關的可行情報。盡可能自動化，但有些情況需要human-in-the-loop。
3. 自動化預防性和偵測性安全控制 – 將 CTI 部署到架構中的安全服務，以提供預防性和偵測性控制。這些服務通常稱為入侵預防系統 (IPS)。在 上 AWS，您可以使用服務 APIs來設定封鎖清單，拒絕從威脅饋送中提供的 IP 地址和網域名稱存取。
4. 透過可觀測性機制獲得可見性 – 雖然安全操作在您的環境中進行，但您正在收集新的 CTI。例如，您可能會觀察到威脅包含在威脅饋送中，或者您可能會觀察到與入侵相關的入侵指標 （例如零時差入侵）。集中威脅情報可提高整個環境的情境感知，讓您可以在一個系統中檢閱現有的 CTI 和新發現的 CTI。
5. 與您的信任社群共用 CTI – 若要完成 CTI 共用生命週期，請產生您自己的 CTI，並將其共用到您的信任社群。

以下影片 Scaling 網路威脅情報與 AUS 網路安全中心共用，會更詳細地討論這些步驟。雖然此影片討論澳洲網路安全中心的 CTI 共用功能，但無論您選擇的威脅饋送或您的位置，步驟都相同。

部署威脅情報平台

威脅情報平台會從多個來源以不同的格式擷取、彙總和組織威脅情報資料。它可讓分析師檢視、排定優先順序，並對從信任社群收到的網路威脅情報 (CTI) 採取行動。

OpenCTI 和 MISP 是常見的開放原始碼威脅情報平台。上的 AWS 合作夥伴也提供解決方案AWS Marketplace。選擇威脅情報平台時，您應該考慮安全團隊的技能水準。MISP 可能功能強大但複雜，OpenCTI 具有更直覺的使用者介面。

選擇威脅情報平台時，請考慮下列事項：

- 功能 – 平台是否提供即時監控、威脅偵測和分析等功能？
- 資料來源 – 平台是否使用各種來源，包括威脅摘要、深色 Web 情報、社交媒體和開放原始碼情報？
- 資料品質 – 平台是否有程序來確保資訊準確可靠？
- 可擴展性 – 平台可以適應組織不斷變化的需求，例如成長和不斷變化的威脅嗎？
- 整合 – 平台是否可以與您現有的安全工具和基礎設施整合？
- 使用者體驗 – 平台是否易於導覽和使用？
- 自訂 – 平台是否可以自訂以符合組織的特定需求？

- 成本 – 平台是否具有成本效益，包括授權成本和維護需求？

您可以在虛擬私有雲端 (VPC) 中部署威脅情報平台。您可以直接在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或使用容器技術進行部署，例如 Amazon Elastic Container Service (Amazon ECS) 或 AWS Fargate。如需為您的現代應用程式開發選擇適當 AWS 容器服務的詳細資訊，請參閱選擇 AWS 容器服務。

擷取網路威脅情報

擷取程序的第一步是將威脅饋送的網路威脅情報 (CTI) 資料轉換為威脅情報平台可以擷取的格式。這稱為 CTI 轉換。威脅饋送資料可能有多種格式，例如結構化威脅資訊表達式 (STIX)。您必須將傳入的資料重組為可預測且易於使用的格式，適用於您在 AWS 環境中使用的安全產品。

為了獲得最大的相容性，建議您將資料轉換為 JSON 格式。例如， AWS Step Functions可以使用 JSON 格式的資料，而自動化工作流程可以更輕鬆且一致地使用這種格式。有關建置自動化工作流程的詳細資訊，請參閱下一節：自動化預防性和偵測性安全控制。

若要加速擷取 CTI 資料，您可以自動化資料轉換。資料會在擷取時轉換，然後直接傳遞至威脅情報平台。您可以使用 AWS Lambda 函數來完成轉換，也可以透過 AWS 服務 AWS Step Functions 或 Amazon EventBridge 來協調程序。

擷取 CTI 時，您可以選擇要擷取和保留的屬性。所需的確切詳細資訊量可能會因您的業務需求而有所不同。不過，若要更新防火牆和其他安全服務，建議您使用下列最低屬性：

- IP 地址和網域
- 威脅
- 從內部威脅清單中新增或移除

擷取您要使用的屬性，然後將其格式化為結構化 JSON 範本。

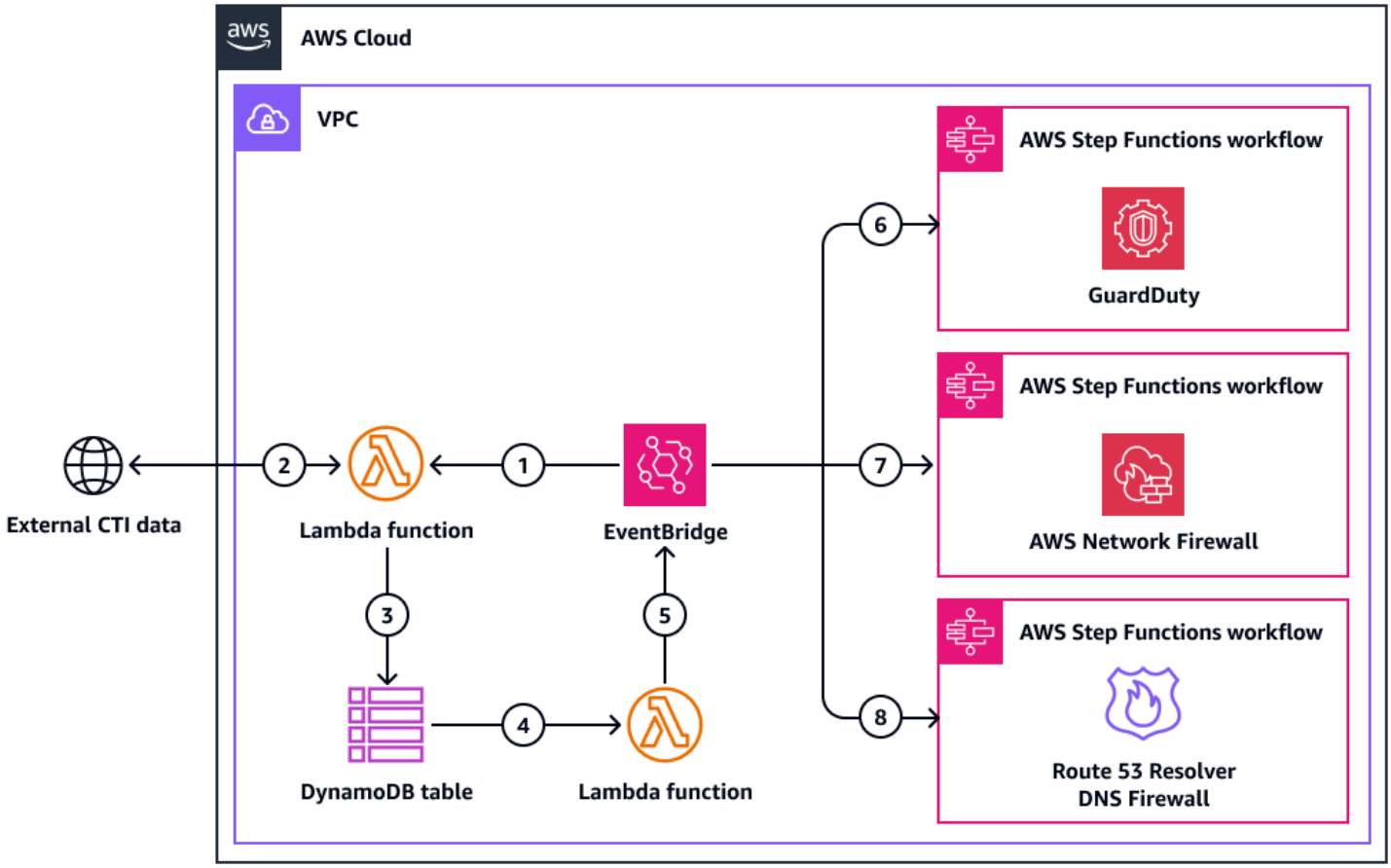
自動化預防性和偵測性安全控制

在網路威脅情報 (CTI) 擷取至威脅情報平台後，您可以自動化組態變更的程序，以回應資料。威脅情報平台可協助您管理網路威脅情報並觀察您的環境。它們提供建構、存放、組織和視覺化有關網路威脅的技術和非技術資訊的能力。它們可協助您建立威脅狀況，並結合各種情報來源來分析和追蹤威脅，例如進階持久性威脅 APTs)。

自動化可以縮短接收威脅情報和在環境中實作組態變更之間的時間。並非所有 CTI 回應都可以自動化。不過，盡可能將回應自動化，有助於您的安全團隊以更及時的方式排定優先順序並評估剩餘的 CTI。每個組織都必須判斷哪些類型的 CTI 回應可以自動化，以及哪些類型需要手動分析。根據組織內容做出此決策，例如風險、資產和資源。例如，某些組織可能會選擇自動化已知不良網域或 IP 地址的區塊，但可能需要分析師調查才能封鎖內部 IP 地址。

本節提供如何在 Amazon GuardDuty、 AWS Network Firewall和 Amazon Route 53 Resolver DNS 防火牆中設定自動 CTI 回應的範例。您可以獨立實作這些範例。讓您的組織的安全需求和需求引導您的決策。您可以透過 AWS Step Functions工作流程 AWS 服務 （ 也稱為狀態機器) 自動化 的組態變更。當AWS Lambda函數完成將 CTI 轉換為 JSON 格式時，會觸發啟動 Step Functions 工作流程的 Amazon EventBridge 事件。

下圖顯示範例架構。Step Functions 工作流程會自動更新 GuardDuty 中的威脅清單、Route 53 Resolver DNS Firewall 中的網域清單，以及 Network Firewall 中的規則群組。



下圖顯示下列工作流程：

1. EventBridge 事件會定期啟動。此事件會啟動 AWS Lambda 函數。

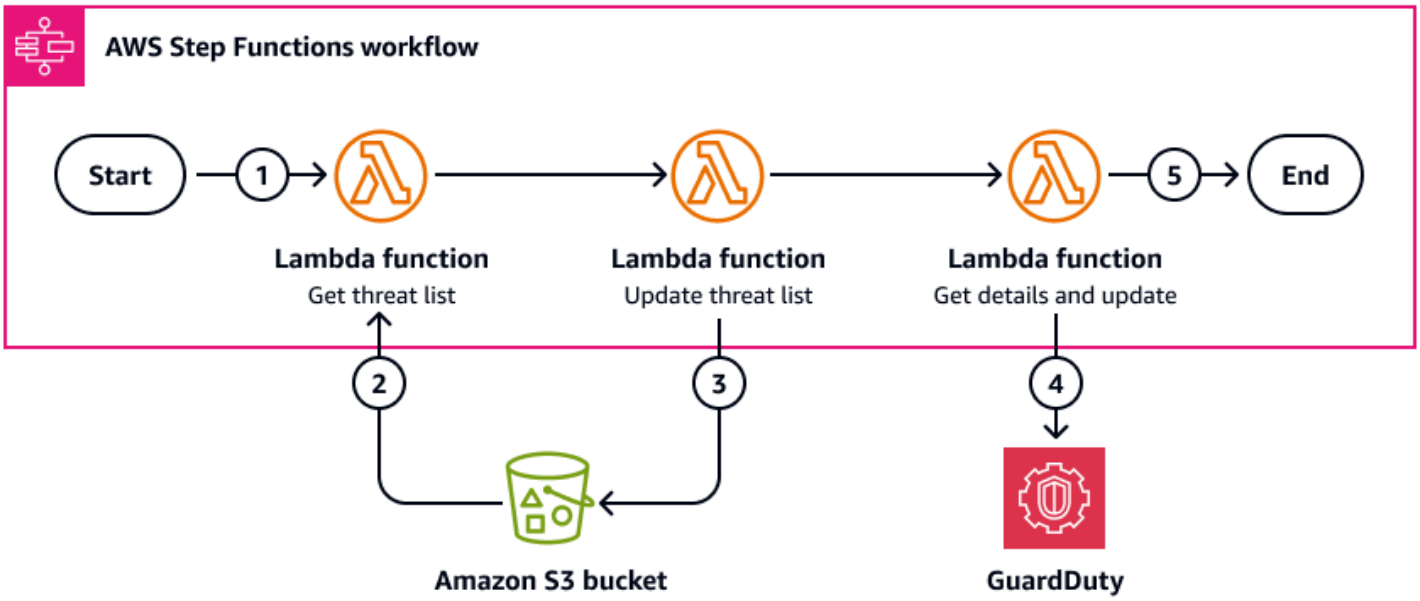
2. Lambda 函數會從外部威脅饋送擷取 CTI 資料。
3. Lambda 函數會將擷取的 CTI 資料寫入 Amazon DynamoDB 資料表。
4. 將資料寫入 DynamoDB 資料表會啟動啟動 Lambda 函數的變更資料擷取串流事件。
5. 如果發生變更，Lambda 函數會在 EventBridge 中啟動新事件。如果沒有發生變更，則工作流程會完成。
6. 如果 CTI 與 IP 地址記錄相關，則 EventBridge 會啟動 Step Functions 工作流程，自動更新 Amazon GuardDuty 中的威脅清單。如需詳細資訊，請參閱本節中的 Amazon GuardDuty。
7. 如果 CTI 與 IP 地址或網域記錄相關，則 EventBridge 會啟動 Step Functions 工作流程，自動更新其中的規則群組 AWS Network Firewall。如需詳細資訊，請參閱本節AWS Network Firewall中的 。
8. 如果 CTI 與網域記錄相關，則 EventBridge 會啟動 Step Functions 工作流程，自動更新 Amazon Route 53 Resolver DNS 防火牆中的網域清單。如需詳細資訊，請參閱本節中的 Amazon Route 53 Resolver DNS 防火牆。

Amazon GuardDuty

Amazon GuardDuty 是一種威脅偵測服務，可持續監控您的 AWS 帳戶 和工作負載是否有未經授權的活動，並提供詳細的安全調查結果，以實現可見性和修復。透過從 CTI 饋送自動更新 GuardDuty 威脅清單，您可以深入了解可能正在存取工作負載的威脅。GuardDuty 可改善您的偵測控制功能。

> **Tip**
>
> GuardDuty 原生與 整合AWS Security Hub CSPM。Security Hub CSPM 提供 中安全狀態的全方位檢視， AWS 可協助您根據安全產業標準和最佳實務檢查環境。當您將 GuardDuty 與 Security Hub CSPM 整合時，GuardDuty 問題清單會自動傳送至 Security Hub CSPM。然後，Security Hub CSPM 可以在分析您的安全狀態時包含這些調查結果。如需詳細資訊，請參閱 GuardDuty 文件中的整合 與 AWS Security Hub CSPM 。在 Security Hub CSPM 中，您可以使用自動化來改善偵測和回應式安全控制功能。

下圖顯示 Step Functions 工作流程如何使用威脅饋送中的 CTI 來更新 GuardDuty 中的威脅清單。當 Lambda 函數完成將 CTI 轉換為 JSON 格式時，會觸發啟動工作流程的 EventBridge 事件。



圖表顯示下列步驟：

1. 如果 CTI 與 IP 地址記錄相關，則 EventBridge 會啟動 Step Functions 工作流程。
2. Lambda 函數會擷取威脅清單，該清單會以物件形式存放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中。
3. Lambda 函數會使用 CTI 中的 IP 地址變更來更新威脅清單。它會將威脅清單儲存為原始 Amazon S3 儲存貯體中物件的新版本。物件名稱保持不變。
4. Lambda 函數使用 API 呼叫來擷取 GuardDuty 偵測器 ID 和威脅 intel 集合 ID。它使用這些 IDs 來更新 GuardDuty，以參考威脅清單的新版本。

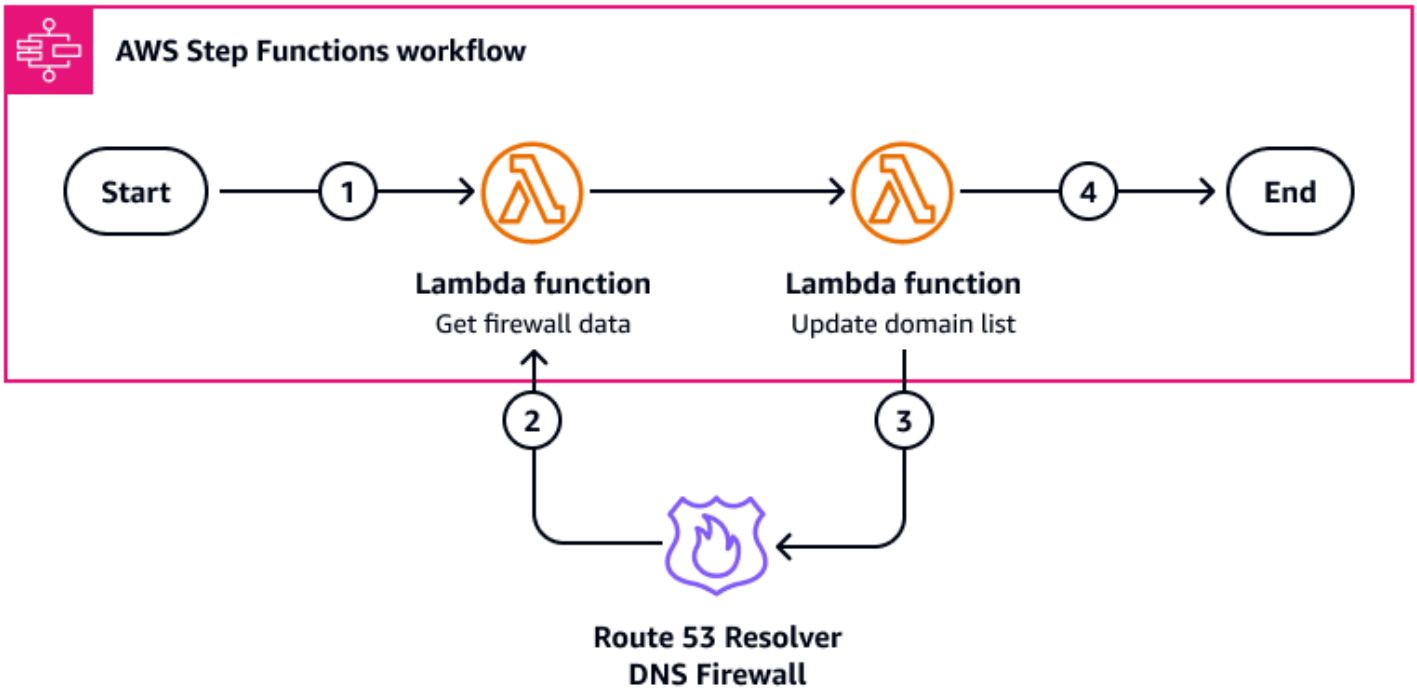
> **Note**
>
> 您無法擷取特定的 GuardDuty 偵測器和 IP 地址清單，因為它們是以陣列的形式擷取。因此，我們建議您在目標中各只有一個 AWS 帳戶。如果您不只如此，則需要確保在此工作流程的最終 Lambda 函數中擷取正確的資料。

5. Step Functions 工作流程結束。

Amazon Route 53 Resolver DNS 防火牆

Amazon Route 53 Resolver DNS 防火牆可協助您篩選和規範虛擬私有雲端 (VPC) 的傳出 DNS 流量。在 DNS 防火牆中，您可以建立規則群組，封鎖由 CTI 饋送識別的網域地址。您可以設定 Step Functions 工作流程，以自動從此規則群組新增和移除網域。

下圖顯示 Step Functions 工作流程如何從威脅饋送使用 CTI 來更新 Amazon Route 53 Resolver DNS 防火牆中的網域清單。當 Lambda 函數完成將 CTI 轉換為 JSON 格式時，會觸發啟動工作流程的 EventBridge 事件。



圖表顯示下列步驟：

1. 如果 CTI 與網域記錄相關，則 EventBridge 會啟動 Step Functions 工作流程。
2. Lambda 函數會擷取防火牆的網域清單資料。如需建立此 Lambda 函數的詳細資訊，請參閱 適用於 Python (Boto3) 的 AWS SDK 文件中的 get_firewall_domain_list。
3. Lambda 函數使用 CTI 和擷取的資料來更新網域清單。如需建立此 Lambda 函數的詳細資訊，請參閱 Boto3 文件中的 update_firewall_domains。Lambda 函數可以新增、移除或取代網域。
4. Step Functions 工作流程結束。

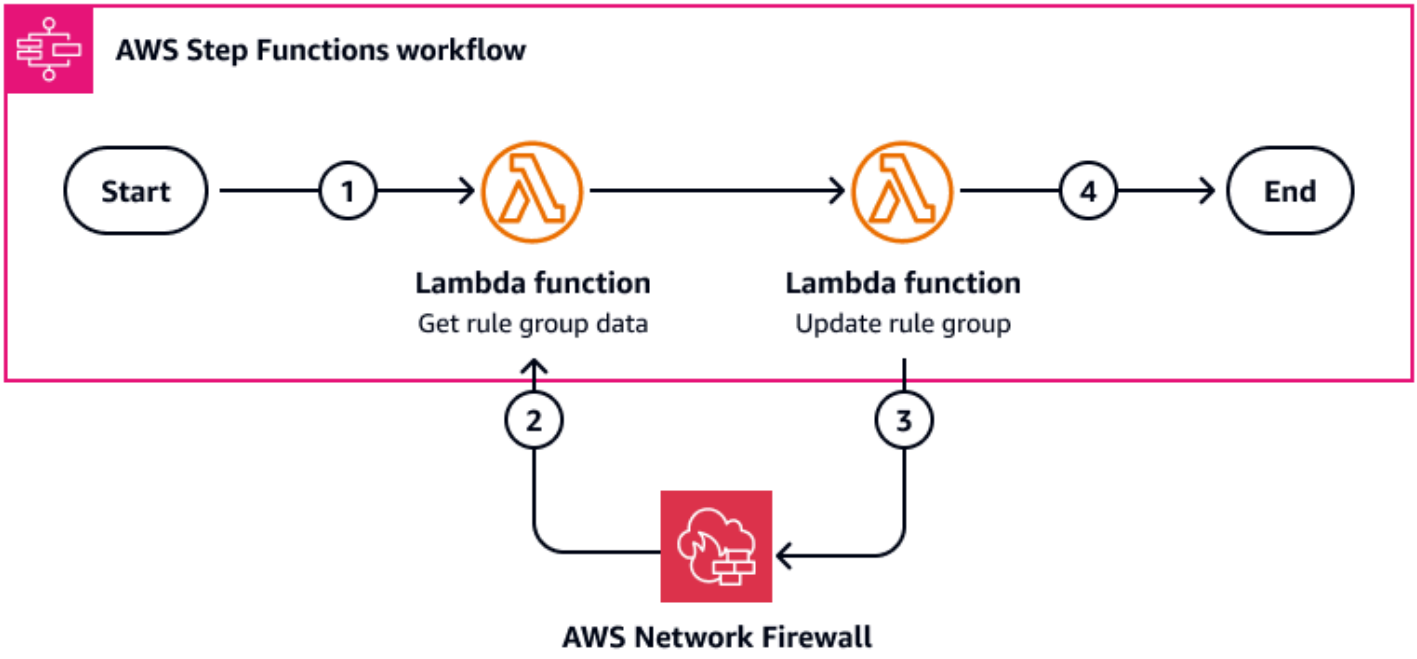
建議遵循下列最佳實務：

- 建議您同時使用 Route 53 Resolver DNS Firewall 和 AWS Network Firewall。DNS 防火牆會篩選 DNS 流量，而 Network Firewall 會篩選所有其他流量。
- 建議您啟用 DNS 防火牆的記錄。您可以建立偵測性控制項來監控日誌資料，並在受限制的網域嘗試透過防火牆傳送流量時提醒您。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控 Route 53 Resolver DNS 防火牆規則群組。

AWS Network Firewall

AWS Network Firewall 是一種具狀態、受管的網路防火牆和入侵偵測和預防服務，適用於 中的 VPCs AWS 雲端。它會篩選 VPC 周邊的流量，協助您封鎖威脅。使用威脅情報摘要自動更新 Network Firewall 規則群組，有助於保護組織的雲端工作負載和資料免於惡意人士攻擊。

下圖顯示 Step Functions 工作流程如何從威脅饋送使用 CTI 來更新 Network Firewall 中的一或多個規則群組。當 Lambda 函數完成將 CTI 轉換為 JSON 格式時，會觸發啟動工作流程的 EventBridge 事件。



圖表顯示下列步驟：

1. 如果 CTI 與 IP 地址或網域記錄相關，則 EventBridge 會啟動 Step Functions 工作流程，自動更新 Network Firewall 中的規則群組。
2. Lambda 函數會從 Network Firewall 擷取規則群組資料。
3. Lambda 函數使用 CTI 更新規則群組。它會新增或移除 IP 地址或網域。
4. Step Functions 工作流程結束。

建議遵循下列最佳實務：

- Network Firewall 可以有多個規則群組。為網域和 IP 地址建立單獨的規則群組。

- 建議您啟用 Network Firewall 的記錄。您可以建立偵測性控制項來監控日誌資料，並在受限制的網域或 IP 地址嘗試透過防火牆傳送流量時提醒您。如需詳細資訊，請參閱從 記錄網路流量 AWS Network Firewall。
- 建議您同時使用 Route 53 Resolver DNS Firewall 和 AWS Network Firewall。DNS 防火牆會篩選 DNS 流量，而 Network Firewall 會篩選所有其他流量。

透過可觀測性機制獲得可見性

檢視已發生之安全事件的功能與建立適當的安全控制同樣重要。在 AWS Well-Architected Framework 的安全支柱中，偵測最佳實務包括設定服務和應用程式記錄，以及在標準化位置擷取日誌、問題清單和指標。若要實作這些最佳實務，您必須記錄可協助您識別事件的資訊，然後以人類取用的格式處理該資訊，最好是在集中位置。

本指南建議您使用 Amazon Simple Storage Service (Amazon S3) 來集中日誌資料。Amazon S3 支援 AWS Network Firewall 和 Amazon Route 53 Resolver DNS 防火牆的日誌儲存。然後，您可以使用 AWS Security Hub CSPM和 Amazon Security Lake 將 Amazon GuardDuty 調查結果和其他安全調查結果集中到單一位置。

記錄網路流量

本指南的自動化預防性和偵測性安全控制章節說明使用 AWS Network Firewall 和 Amazon Route 53 Resolver DNS 防火牆自動回應網路威脅情報 (CTI)。建議您為這兩種服務設定記錄。您可以建立偵測性控制項來監控日誌資料，並在受限制的網域或 IP 地址嘗試透過防火牆傳送流量時提醒您。

設定這些資源時，請考慮您的個別記錄需求。例如，Network Firewall 的記錄僅適用於您轉送到具狀態規則引擎的流量。我們建議您遵循零信任模型，並將所有流量轉送至具狀態規則引擎。不過，如果您想要降低成本，您可以排除組織信任的流量。

Network Firewall 和 DNS Firewall 都支援記錄到 Amazon S3。如需設定這些服務記錄的詳細資訊，請參閱從 記錄網路流量 AWS Network Firewall和設定 DNS 防火牆的記錄。對於這兩種服務，您可以透過 設定 Amazon S3 儲存貯體的記錄 AWS 管理主控台。

在 中集中化安全調查結果 AWS

AWS Security Hub CSPM 提供 中安全狀態的完整檢視， AWS 並協助您根據安全產業標準和最佳實務來評估您的 AWS 環境。Security Hub CSPM 可以產生與您的安全控制相關聯的問題清單。它也可以接收其他 的問題清單 AWS 服務，例如 Amazon GuardDuty。您可以使用 Security Hub CSPM 集中

來自 AWS 帳戶 AWS 服務、 和支援的第三方產品的調查結果和資料。如需整合的詳細資訊，請參閱 Security Hub CSPM 文件中的了解 Security Hub CSPM 中的整合。

Security Hub CSPM 也包含自動化功能，可協助您分類和修復安全問題。例如，您可以使用自動化規則，在安全檢查失敗時自動更新關鍵問題清單。您也可以使用與 Amazon EventBridge 的整合來啟動對特定問題清單的自動回應。如需詳細資訊，請參閱 Security Hub CSPM 文件中的自動修改 Security Hub CSPM 調查結果並對其採取行動。

如果您使用 Amazon GuardDuty，我們建議您設定 GuardDuty 將其調查結果傳送至 Security Hub CSPM。然後，Security Hub CSPM 可以在分析您的安全狀態時包含這些調查結果。如需詳細資訊，請參閱 GuardDuty 文件中的與 整合 AWS Security Hub CSPM。

對於 Network Firewall 和 Route 53 Resolver DNS Firewall，您可以從您正在記錄的網路流量建立自訂問題清單。Amazon Athena 是一種互動式查詢服務，可協助您使用標準 SQL 直接在 Amazon S3 中分析資料。您可以在 Athena 中建構查詢，以掃描 Amazon S3 中的日誌並擷取相關資料。如需說明，請參閱 Athena 文件中的入門。然後，您可以使用 AWS Lambda 函數將相關日誌資料轉換為AWS 安全調查結果格式 (ASFF)，並將調查結果傳送至 Security Hub CSPM。以下是將日誌資料從 Network Firewall 轉換為 Security Hub CSPM 調查結果的範例 Lambda 函數：

```
Import { SecurityHubClient, BatchImportFindingsCommand, GetFindingsCommand } from
 "@aws-sdk/client-securityhub";

Export const handler = async(event) => {
   const date = new Date().toISOString();

   const config = {
      Region: REGION
   };

   const input = {
      Findings: [
         {
            SchemaVersion: '2018-10-08',
            Id: ALERTLOGS3BUCKETID,
            ProductArn: FIREWALLMANAGERARN,
            GeneratorId: 'alertlogs-to-findings',
            AwsAccountId: ACCOUNTID,
            Types: 'Unusual Behaviours/Network Flow/Alert',
            CreatedAt: date,
            UpdatedAt: date,
            Severity: {
               Normalized: 80,
```

```
                Product: 8
            },
            Confidence: 100,
            Title: 'Alert Log to Findings',
            Description: 'Network Firewall Alert Log into Finding - add
               top level dynamic detail',
            Resources: [
               {
                  /*these are custom resources. Contain deeper details of your event
 here*/
                  firewallName: 'Example Name',
                  event: 'Example details here'
               }
            ]
         }
      ]
   };

   const client = new SecurityHubClient(config);
   const command = new BatchImportFindingsCommand(input);
   const response = await client.send(command);
   return { statusCode: 200, response };
};
```

您擷取資訊並將其傳送至 Security Hub CSPM 的模式取決於您的個人業務需求。如果您需要定期傳送資料，您可以使用 EventBridge 來啟動程序。如果您想要在新增資訊時收到提醒，您可以使用 Amazon Simple Notification Service (Amazon SNS)。處理此架構的方法有很多，因此正確規劃以滿足您的業務需求非常重要。

將 AWS 安全資料與其他企業資料整合

Amazon Security Lake 可以自動從整合和第三方服務收集與安全相關的日誌 AWS 服務 和事件資料。它還可協助您使用可自訂的保留和複寫設定來管理資料的生命週期。Security Lake 會將擷取的資料轉換為 Apache Parquet 格式，以及稱為開放式網路安全結構描述架構 (OCSF) 的標準開放原始碼結構描述。透過 OCSF 支援，Security Lake 會標準化和合併來自 AWS 和各種企業安全資料來源的安全資料。其他 AWS 服務 和第三方服務可以訂閱存放在 Security Lake 中的資料，以進行事件回應和安全資料分析。

您可以設定 Security Lake 接收來自 Security Hub CSPM 的問題清單。若要啟用此整合，您必須啟用這兩個服務，並將 Security Hub CSPM 新增為 Security Lake 中的來源。完成這些步驟後，Security Hub CSPM 會開始將所有調查結果傳送至 Security Lake。Security Lake 會自動標準化 Security

Hub CSPM 調查結果並將其轉換為 OCSF。在 Security Lake 中，您可以新增一或多個訂閱者來取用 Security Hub CSPM 調查結果。如需詳細資訊，請參閱 Security Lake 文件中的與 整合 AWS Security Hub CSPM。

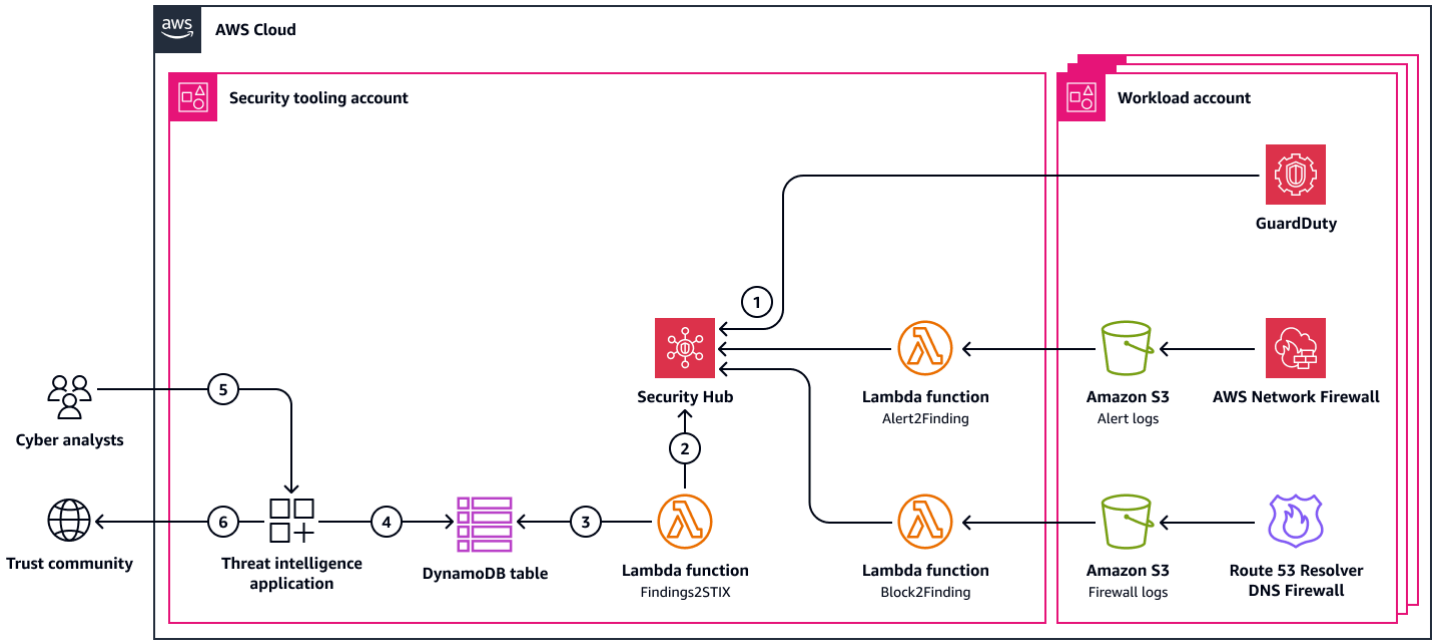
下列影片 AWS re：Inforce 2024 - 網路威脅情報共用， AWS討論如何使用 Security Hub CSPM 和 Security Lake 整合來共用 CTI。

與您的信任社群共用 CTI

您傳送網路威脅情報 (CTI) 的 社群通常與您接收 CTI 的社群相同。不過，您可以選擇與更多 共用。例如，您可以選擇與您信任的政府或法規組織共用，例如您的國家網路安全中心或資訊共用和分析中心 (ISACs)。目標是透過匯集多個組織的調查結果，快速傳播和實作 CTI。您的威脅情報平台會管理 API 整合，以便與多個摘要共用。

傳送 CTI 到信任社群與實作預防性和偵測性控制同時發生。您可以使用日誌來協助識別安全事件。然後，您可以集中事件和調查結果，以便快速了解 的安全狀態概觀 AWS 帳戶。然後，您的安全團隊，例如您的網路分析師，可以識別任何可能有價值的資訊。由於您已經在 中有調查結果 AWS Security Hub CSPM，您可以將這些調查結果轉換為威脅饋送所使用的格式，例如 JSON 或 STIX。然後，您將 CTI 傳送至饋送提供者。他們的威脅情報平台會擷取、匿名化和驗證您提供的 CTI。然後，您的 CTI 會與更廣泛的社群共用。

下圖顯示如何使用 AWS 服務 產生 CTI，然後與您的信任社群共用，包括網路授權機構和其他社群成員。



此圖表顯示下列工作流程：

1. 問題清單會在 中建立 AWS Security Hub CSPM。
2. AWS Lambda 函數會從 Security Hub CSPM 擷取問題清單，並將其轉換為可分割格式，例如 JSON 或 STIX。
3. Lambda 函數會將問題清單存放在 Amazon DynamoDB 資料表中。
4. 在 Amazon Elastic Compute Cloud (Amazon EC2) 或 Amazon Elastic Container Service (Amazon ECS) 上執行的第三方威脅情報平台，會從 DynamoDB 資料表擷取問題清單。
5. 網路分析師會檢閱威脅情報平台中的 CTI。
6. 威脅情報平台會將 CTI 發佈至信任社群，該社群由其他 CTI 生產者和消費者組成。

後續步驟和資源

考慮您組織的資產、產業和威脅環境。這些因素應該通知信任社群您選擇加入以進行網路威脅情報分享。全球許多網路授權機構都提供威脅情報摘要。考慮提供哪些服務，並選擇最適合您組織的使用案例。使用本指南做為模組化方法，並針對您的組織進行相應調整。

我們建議您檢閱下列其他資源。這些資源可協助您在 AWS 環境中建置或部署威脅情報平台，並協助您設定網路威脅情報共用。

AWS 資源

- AWS 架構中心
- AWS re：Inforce 2024 - 上的網路威脅情報共用 AWS （影片）
- AWS Summit ANZ 2023：擴展與 AUS 網路安全中心的網路威脅情報共用 （影片）

AWS 服務 文件

- Amazon DynamoDB 文件
- Amazon EventBridge 文件
- Amazon GuardDuty 文件
- AWS Lambda 文件
- AWS Network Firewall 文件
- Amazon Route 53 Resolver DNS 防火牆文件
- AWS Security Hub CSPM 文件
- Amazon Security Lake 文件
- Amazon Simple Storage Service (Amazon S3) 文件
- AWS Step Functions 文件

STIX 資源

- STIX 2.1 範例
- 惡意 URL 的指標

威脅情報平台

- OpenCTI
- MISP

貢獻者

下列個人對本指南有所貢獻。

編寫

- Jess Modini，資深技術專家， AWS
- Alexa Donovan，副解決方案架構師， AWS
- Steven Ryan，合作夥伴解決方案架構師 AWS
- Byron Pogson，安全解決方案架構師 AWS

檢閱

- Brian Farnhill，資深軟體開發工程師， AWS
- Marc Luescher，資深解決方案架構師 AWS
- Stefan Mijic，安全保證專家， AWS
- Timothy Woodill，公有產業解決方案架構師， AWS

技術寫入

- 資深技術作者，Lilly AbouHarb AWS

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	—	2024 年 12 月 12 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。