將ThreatQ與Umbrella整合

目錄

簡介

本檔案介紹如何將ThreatQ與Cisco Umbrella整合。

必要條件

需求

思科建議您瞭解以下主題：

- 具有更新URL以進行整合訪問許可權的ThreatQ控制面板
- Umbrella儀表板管理許可權
- Umbrella儀表板必須啟用ThreatQ整合。

採用元件

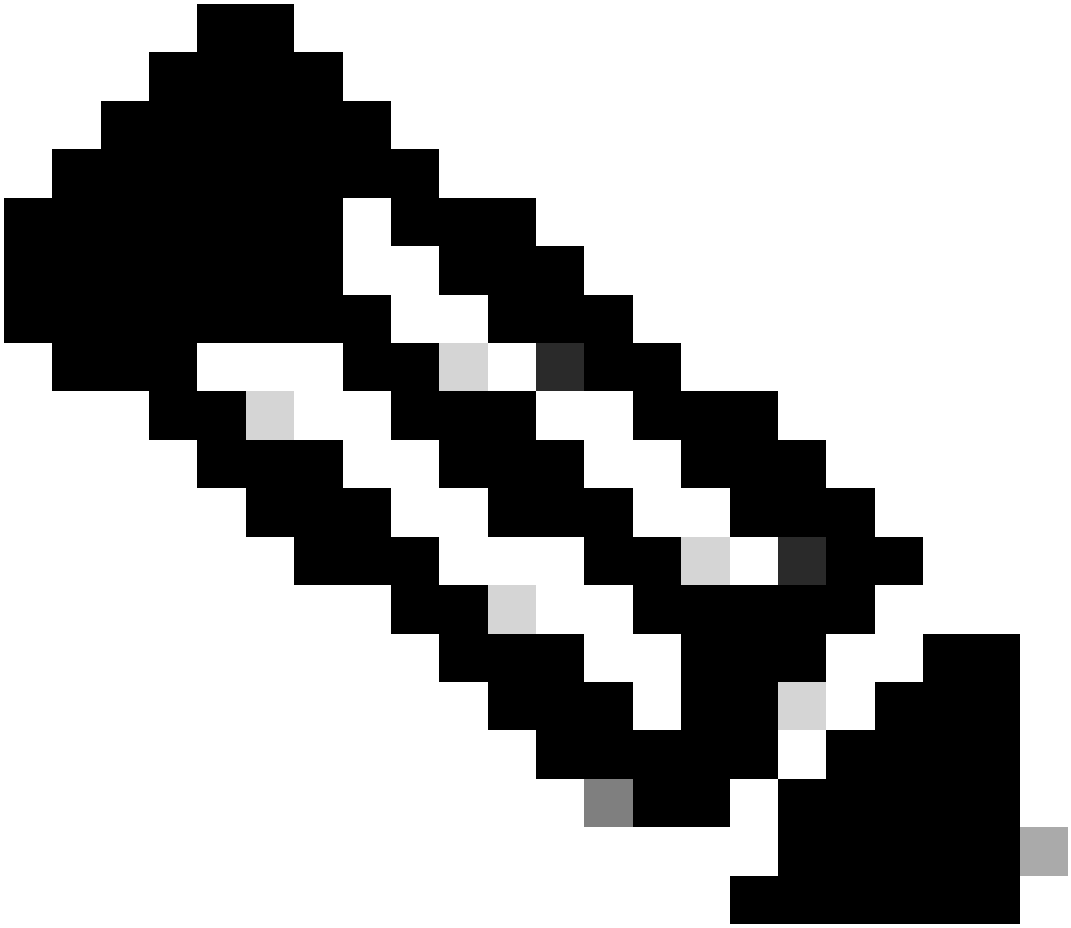
本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

ThreatQ和思科Umbrella整合概述

通過將ThreatQ與Cisco Umbrella整合，安全人員和管理員現在可以針對漫遊的筆記型電腦、平板電腦或電話的高級威脅擴展防護，同時為分散式企業網路提供另一層實施措施。

本指南概述如何配置ThreatQ以與Umbrella通訊，以便將ThreatQ TIP中的安全事件整合到策略中，這些策略可以應用於受Cisco Umbrella保護的客戶端。



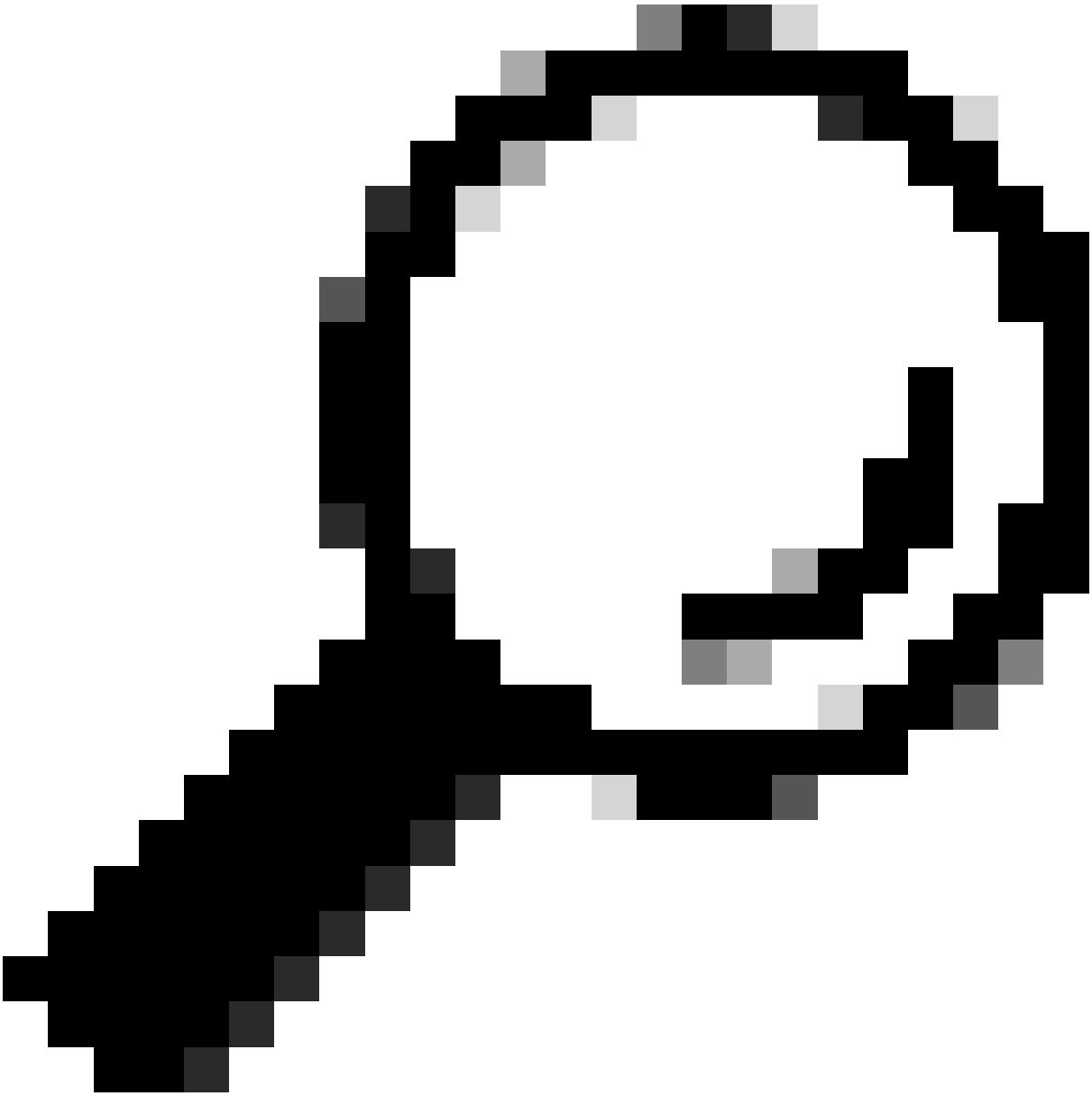
附註：ThreatQ整合僅包含在某些Cisco Umbrella軟體包中。如果您沒有所需的軟體包並且希望整合ThreatQ，請聯絡您的Cisco Umbrella代表。如果您有正確的Cisco Umbrella軟體包，但是未將ThreatQ視為控制面板的整合，請與Cisco Umbrella支援聯絡。

整合功能

ThreatQ平台首先將其找到的網路威脅情報（例如託管惡意軟體的域、殭屍網路或網路釣魚站點的命令和控制）傳送到Umbrella。

然後，Umbrella驗證威脅以確保將其新增到策略中。如果確認來自ThreatQ的資訊是威脅，則域地址會作為可應用於任何Umbrella策略的安全設定的一部分新增到ThreatQ目標清單。該策略會立即應用於使用帶有ThreatQ目標清單的策略從裝置發出的任何請求。

接下來，Umbrella會自動分析ThreatQ警報並將惡意站點新增到ThreatQ目標清單。這會將ThreatQ保護擴展到所有遠端使用者和裝置，並為您的公司網路提供另一層實施功能。



提示：雖然Cisco Umbrella會儘量驗證和允許已知安全域（例如Google和Salesforce），以避免不需要的中斷，我們建議您根據您的策略將您從未希望阻止的域新增到Global Allow List或其他目標清單。示例包括：

- 您組織的首頁

- 表示您提供的服務的域，可以同時具有內部和外部記錄。例如，「mail.myservicedomain.com」和「portal.myotherservicedomain.com」。
- 您依賴於Cisco Umbrella的不太知名的基於雲的應用程式不包括在自動域驗證中。例如，「localcloudservice.com」。

這些網域可新增到Cisco Umbrella中Policies > Destination Lists下的Global Allow List。

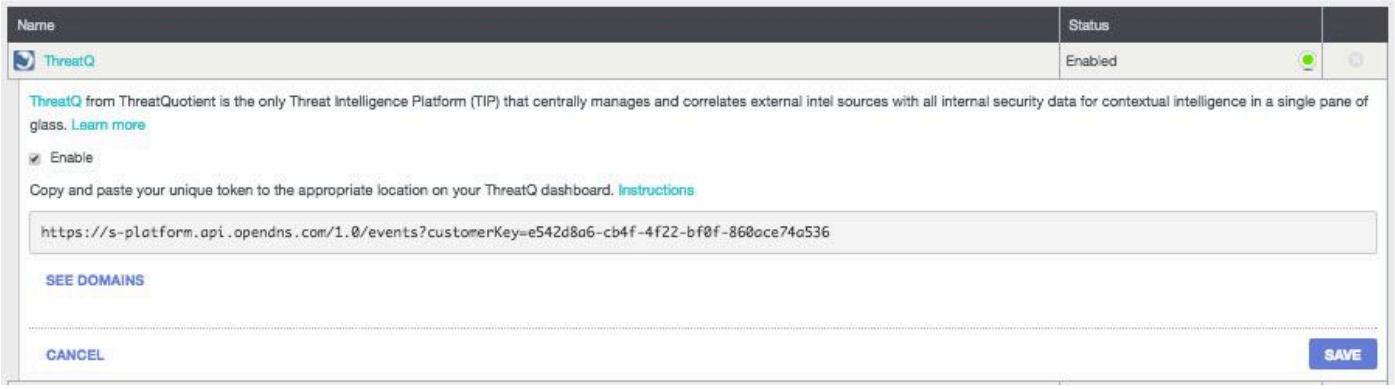
Umbrella指令碼和API令牌生成

首先在Umbrella中查詢您唯一的URL，以便ThreatQ裝置與以下裝置通訊：

1.登入您的Umbrella控制面板。

2.定位至設定>整合，然後在表中選擇ThreatQ以展開它。

3.選擇Enable，然後選擇Save。這將為您在Umbrella中的組織生成唯一的特定URL。



稍後配置ThreatQ以向Umbrella傳送資料時，您需要該URL，因此請複製該URL並轉到ThreatQ控制面板。

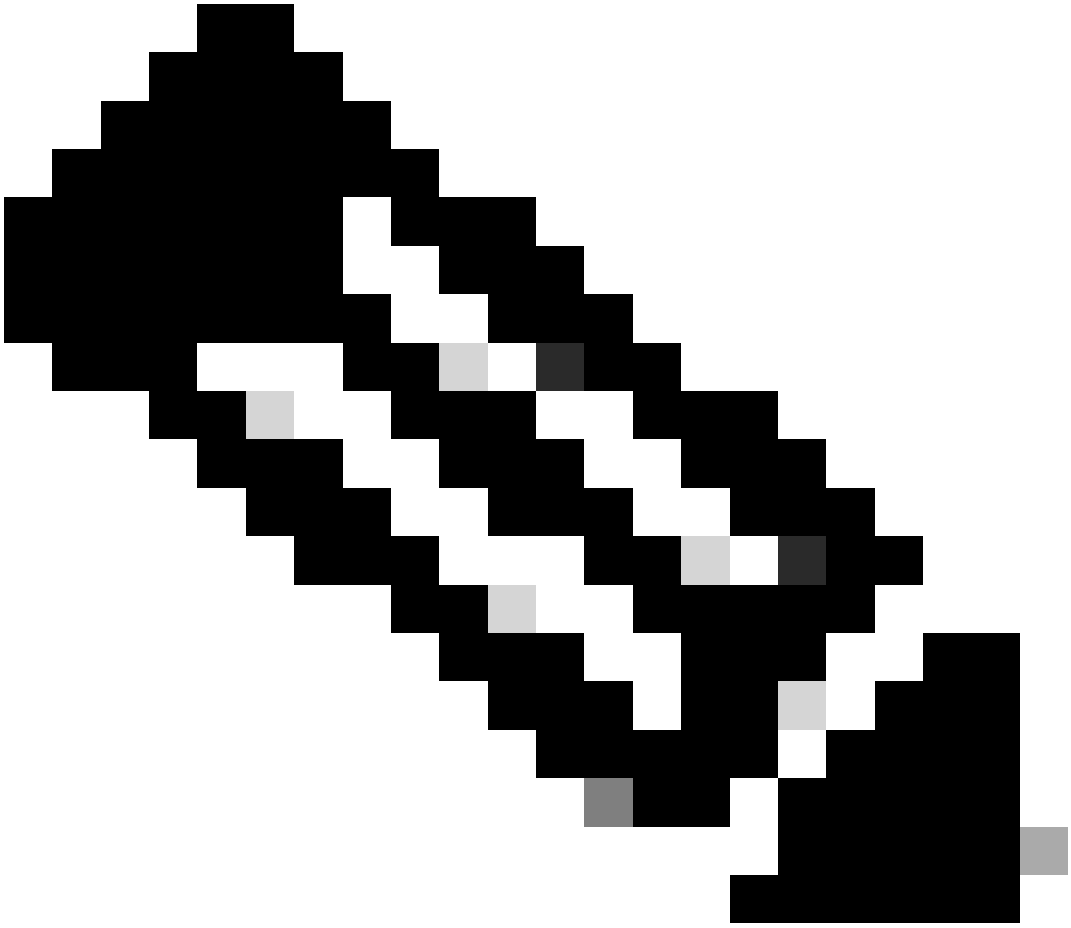
如何配置ThreatQ與Umbrella通訊

登入您的ThreatQ控制面板，將URL新增到適當的區域以與Umbrella連線。

具體說明各不相同，如果您不確定如何或何處在ThreatQ中配置API整合，Umbrella建議聯絡ThreatQ支援。

在稽核模式下觀察新增到ThreatQ安全類別的事件

隨著時間的推移，ThreatQ控制面板中的事件開始填充一個特定目標清單，該清單可以作為ThreatQ安全類別應用於策略。預設情況下，目標清單和安全類別處於稽核模式，這意味著它們不應用於任何策略，並且不能導致對現有Umbrella策略進行任何更改。



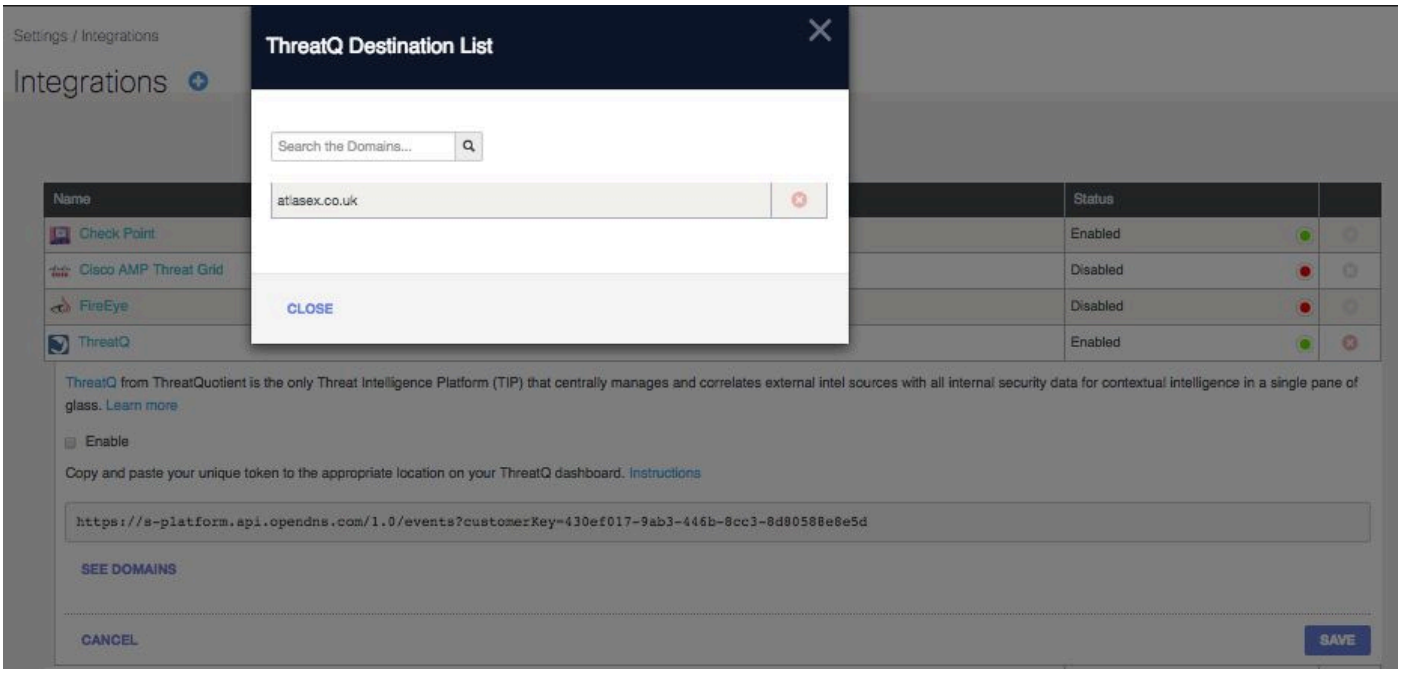
附註：可以啟用稽核模式，但根據您的部署配置檔案和網路配置，稽核模式需要很長時間。

檢視目標清單

您可以隨時檢視Umbrella中的ThreatQ目標清單：

1.定位至「設定」>「整合」。

2.展開表中的ThreatQ，然後選擇See Domains(檢視域)。



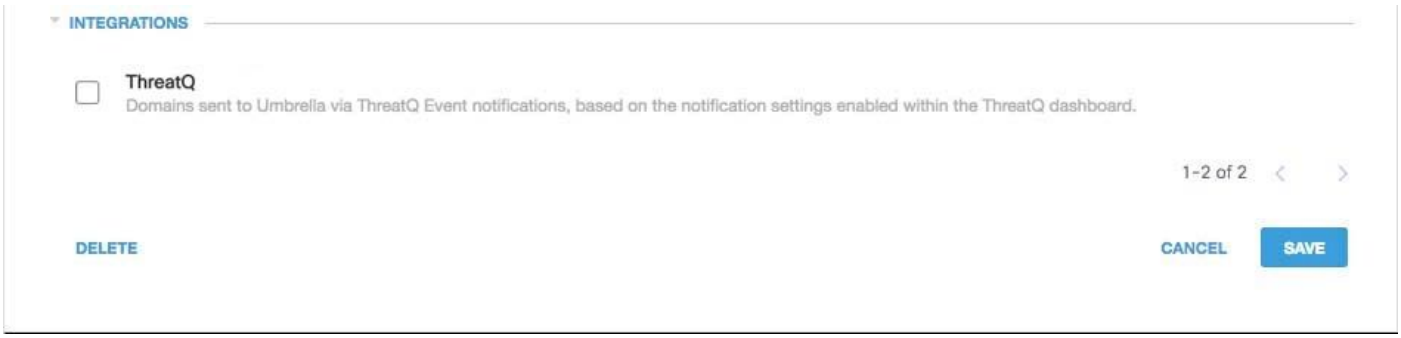
檢視策略的安全設定

您可以隨時檢視可在Umbrella中為策略啟用的安全設定：

1.定位至策略>安全設定。

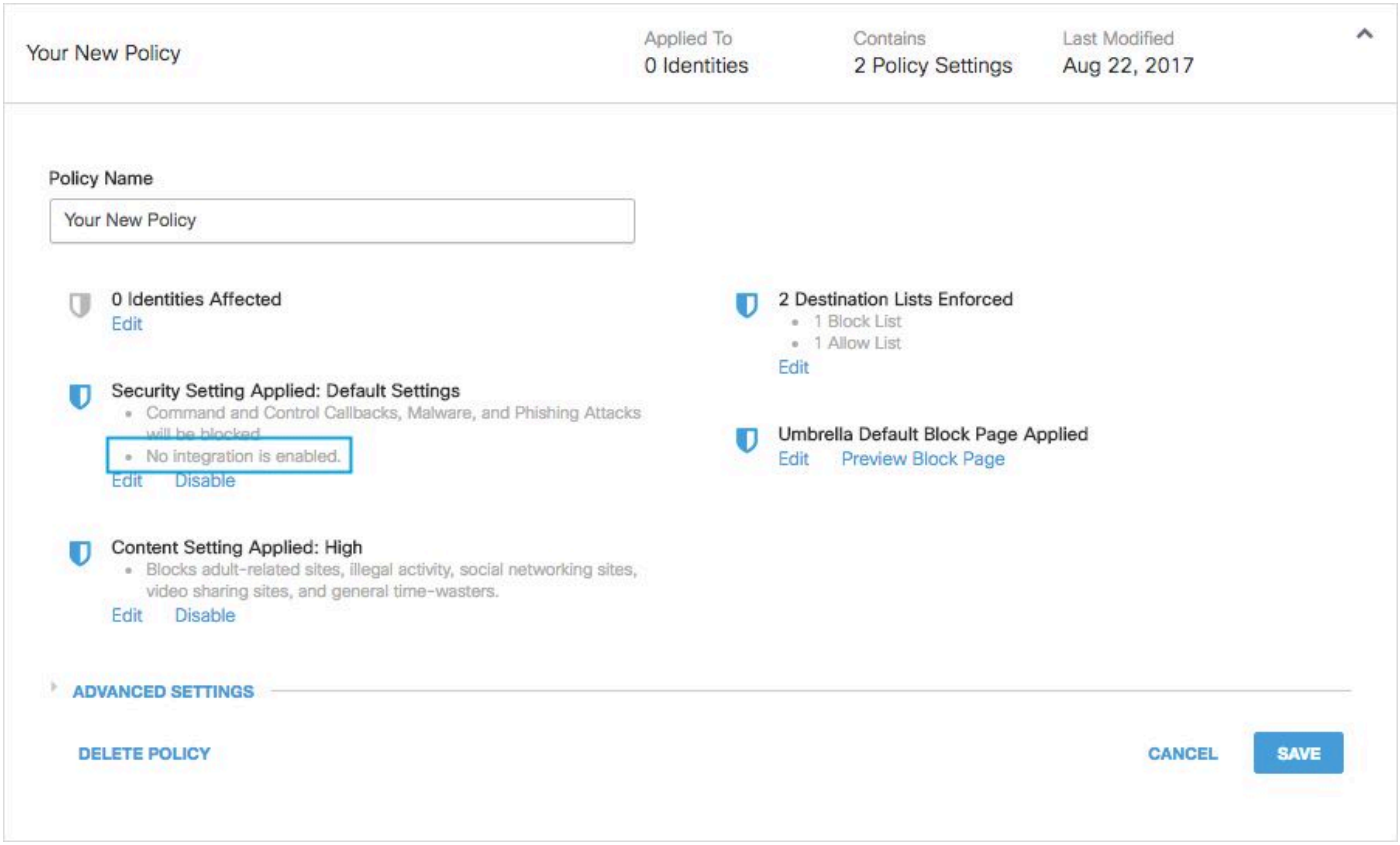
2.選擇表中的安全性設定將其展開。

3.滾動到Integrations以查詢ThreatQ設定。



115014040286

您還可以通過「安全設定摘要」頁檢視整合資訊。



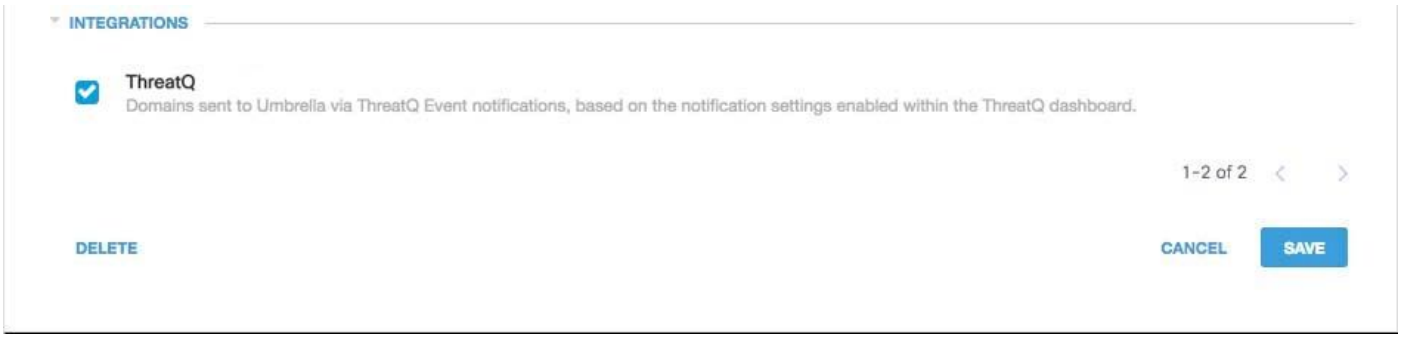
25464141748116

在塊模式下將ThreatQ安全設定應用到託管客戶端的策略

一旦準備好由由Umbrella管理的客戶端實施這些附加安全威脅，您可以更改現有策略的安全設定，或建立一個高於預設策略的新策略，以確保首先實施該策略：

1.導航到Policies > Security Settings。

2.在「整合」下，選擇ThreatQ，然後選擇Save。



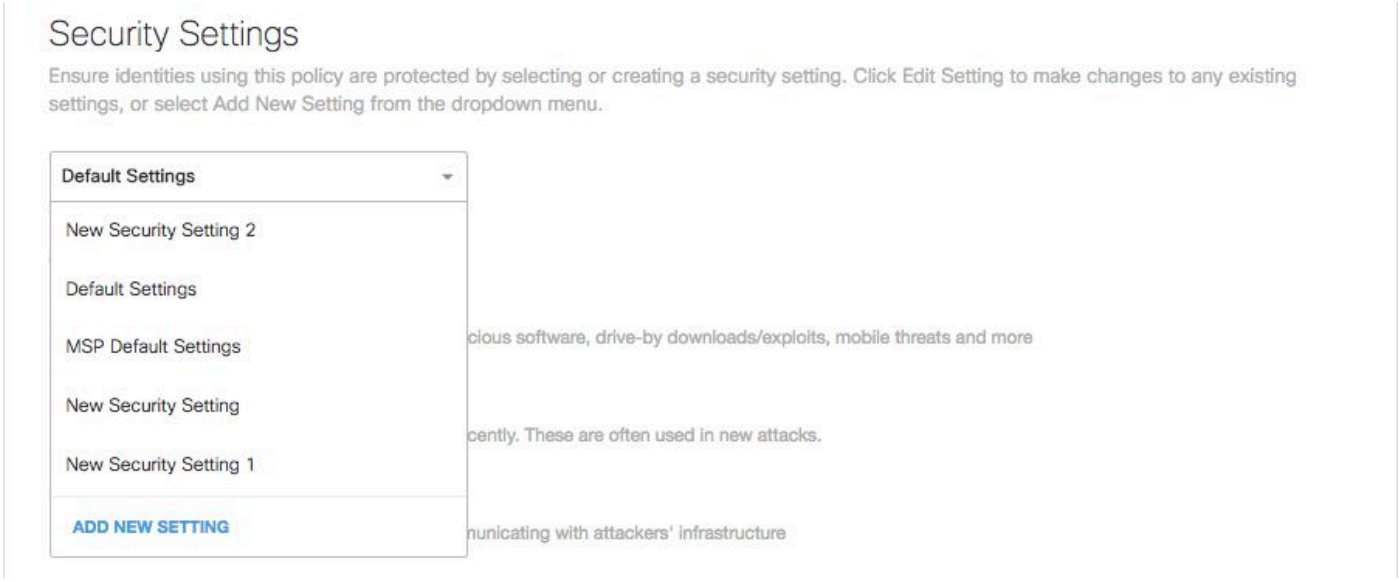
115014207403

接下來，在「策略」嚮導中，將安全設定新增到正在編輯的策略中：

1.定位至Policies > Policy List。

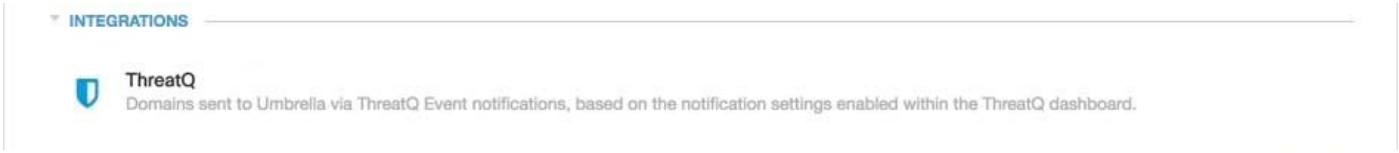
2.展開策略並選擇應用的安全設定下的編輯。

3.在「Security Settings」下拉選單中，選擇包含ThreatQ設定的安全設定。



25464141787668

「整合」(Integrations)下的遮蔽圖示將更新為藍色。



115014040506

4.選擇「Set & Return」。

現在，ThreatQ的安全設定中包含的ThreatQ域已被阻止，用於使用該策略的身份。

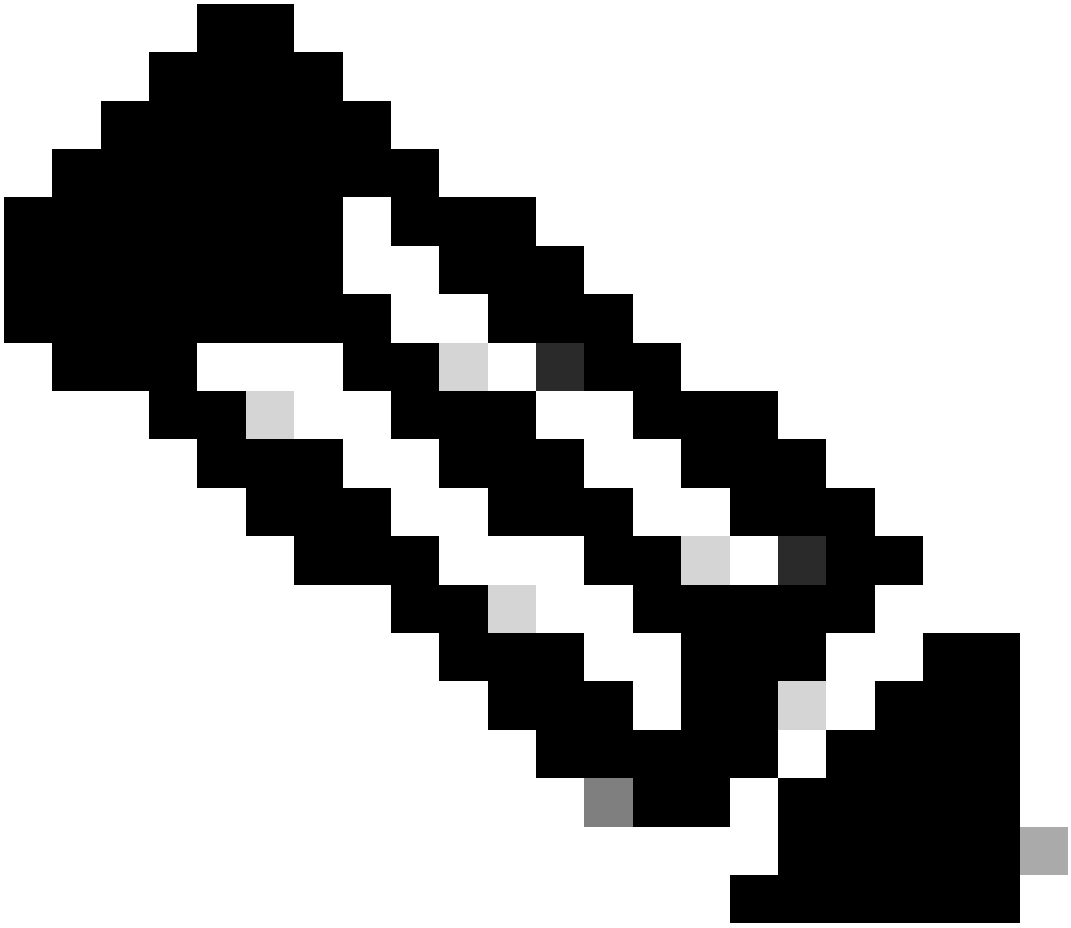
在Umbrella中報告ThreatQ事件

報告ThreatQ安全事件

ThreatQ Destination List是可以報告的安全類別清單之一。大多數或所有報表都使用安全類別作為篩選器。例如，您可以篩選安全類別，以便僅顯示與ThreatQ相關的活動。

1.定位至報告>活動搜尋。

2.在Security Categories下，選擇ThreatQ以篩選報告，以便僅顯示ThreatQ的安全類別。



附註：如果已禁用ThreatQ整合，則它不會顯示在「安全類別」篩選器中。

115014207603

3.選擇Apply。

報告何時將域新增到ThreatQ目標清單

Umbrella Admin Audit日誌包含ThreatQ控制面板中的事件，因為它將域新增到目標清單。名為「ThreatQ Account」（也帶有ThreatQ徽標）的使用者生成事件。這些事件包括所新增的域和新增該域的時間。在Reporting > Admin Audit Log中可找到Umbrella Admin Audit日誌。

通過為ThreatQ帳戶使用者應用篩選器，您可以進行篩選以僅包含ThreatQ更改。

處理不需要的檢測或誤報

允許清單

儘管可能性不大，但ThreatQ自動新增的域可能會觸發不需要的阻止，阻止使用者訪問特定網站。在這種情況下，Umbrella建議將網域新增到允許清單中，此清單優先於所有其他型別的封鎖清單（包括安全設定）。

這種方式更為可取，其原因有兩點：

- 首先，如果ThreatQ控制面板在刪除域後再次重新新增域，則允許清單可防止出現進一步的問題。
- 其次，允許清單顯示了問題域的歷史記錄，這些域可用於調查分析或審計報告。

預設情況下，全域性允許清單應用於所有策略。將域新增到全域性允許清單會導致在所有策略中允許該域。

如果阻止模式中的ThreatQ安全設定僅應用於受管Umbrella身份的子集（例如，它僅適用於漫遊電腦和流動裝置），則可以為這些身份或策略建立特定的允許清單。

要建立允許清單，請執行以下操作：

1.定位至策略>目標清單，然後選擇新增圖示。

2.選擇Allow，然後將您的域新增到清單中。

3.選擇儲存。

儲存目標清單後，可以將其新增到覆蓋那些受不需要的阻止影響的客戶端的現有策略中。

從ThreatQ目標清單中刪除域

ThreatQ目標清單中的每個域名旁邊都有一個Delete圖示。刪除域可讓您在出現不需要的檢測時清除ThreatQ目標清單。但是，如果ThreatQ控制面板將域重新傳送到Cisco Umbrella，則刪除操作不是永久性的。

刪除域：

1.定位至「設置」>「整合」，然後選擇「ThreatQ」將其展開。

2.選擇檢視域。

3.搜尋要刪除的域名。

4.選擇刪除圖示。

5.選擇關閉。

6.選擇儲存。

在出現不需要的檢測或誤報時，Umbrella建議立即在Umbrella中建立允許清單，然後在ThreatQ控

制面板中修正誤報。稍後，您可以從ThreatQ目標清單中刪除該域。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。