將ThreatConnect與Umbrella整合

目錄

簡介

本檔案介紹如何將ThreatConnect與Cisco Umbrella相整合。

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ThreatConnect控制面板
- Umbrella儀表板管理許可權
- Umbrella儀表板必須啟用ThreatConnect整合。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

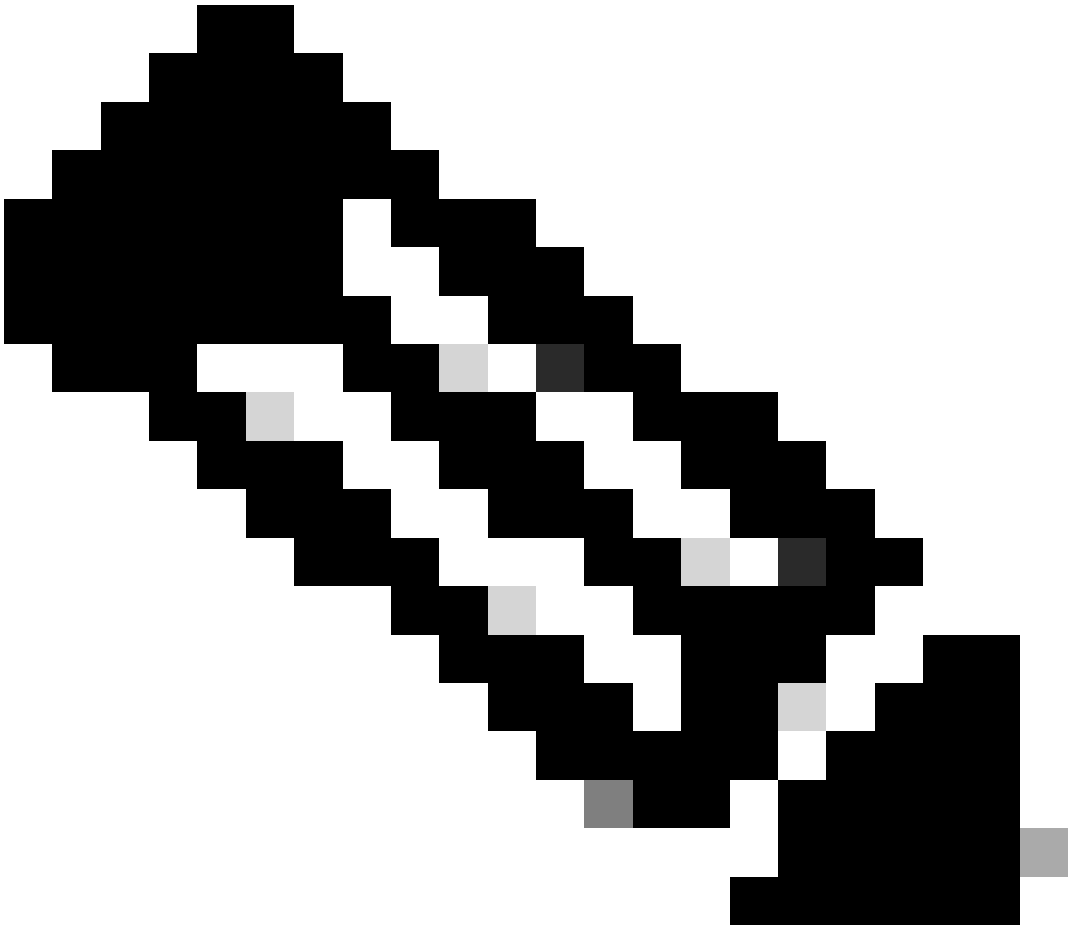
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）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。

ThreatConnect和思科Umbrella整合概述

通過將ThreatConnect與Cisco Umbrella整合，安全人員和管理員現在可以針對漫遊筆記型電腦、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ThreatConnect以與Umbrella通訊，以便將ThreatConnect TIP的安全事件整合到策略中，這些策略可應用於受思科Umbrella保護的客戶端。

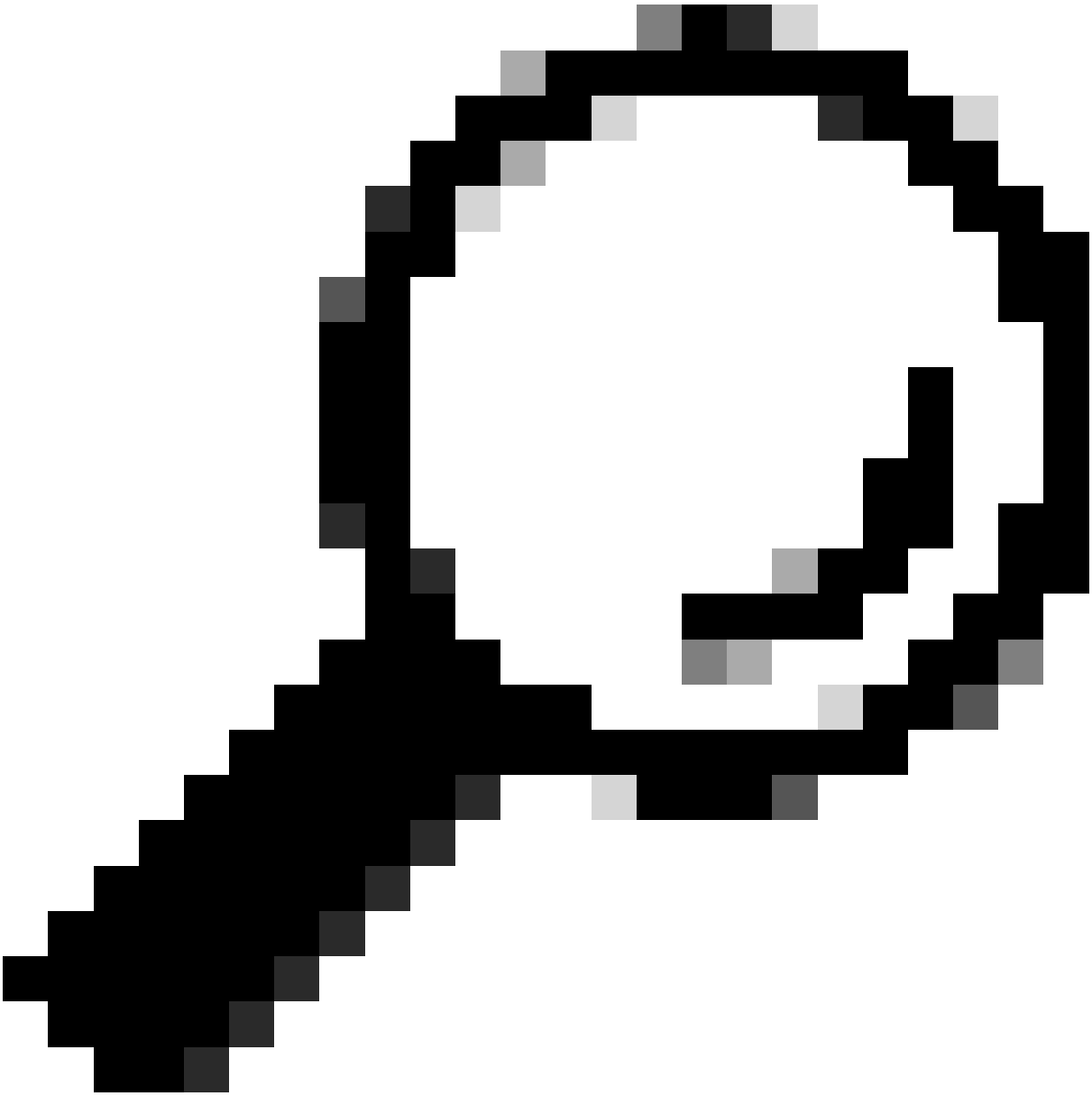


附註：ThreatConnect整合僅包含在特定思科Umbrella軟體包中。如果您沒有包含此整合的包，請聯絡您的Cisco Umbrella代表獲取該包。如果您有正確的軟體包，但是沒有將ThreatConnect視為控制面板的整合，請與Cisco Umbrella支援聯絡。

ThreatConnect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ThreatConnect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ThreatConnect目標清單。該策略會立即應用於使用帶有ThreatConnect目標清單的策略從裝置發出的任何請求。

今後，Umbrella將自動分析ThreatConnect警報並將惡意站點新增到ThreatConnect目標清單，將ThreatConnect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措施。



提示：雖然Umbrella會儘量驗證和允許已知安全域（例如Google和Salesforce），以避免任何不需要的中斷，但是Umbrella建議根據您的策略將您不希望被阻止的任何域新增到Global Allow List或其他目標清單。示例包括：

- 您組織的首頁。例如，mydomain.com。
- 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。
- 您嚴重依賴的鮮為人知的雲應用，但Umbrella不知道或在其自動域驗證中包括這些應

用。例如，localcloudservice.com。

在Umbrella中的Policies > Destination Lists中找到Global Allow List。如需詳細資訊，請參閱檔案：管理目的地清單

配置Umbrella控制面板以從ThreatConnect接收事件

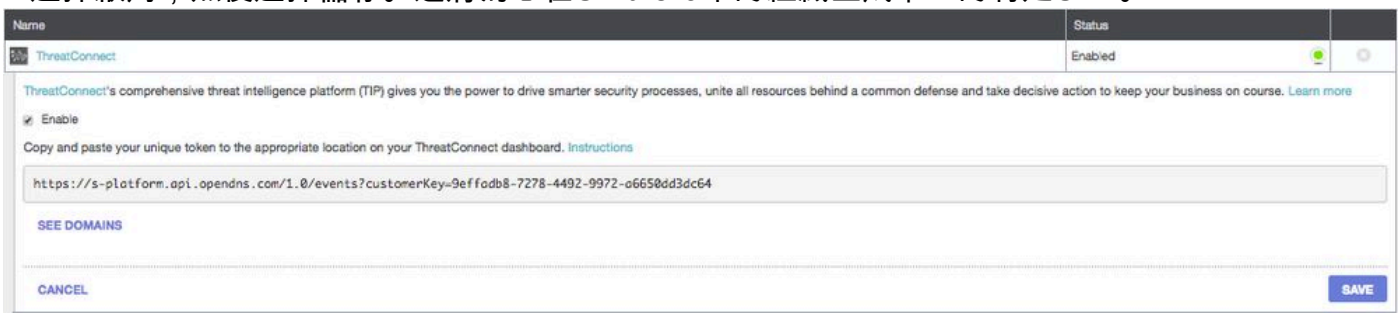
首先在Umbrella中查詢您唯一的URL，以便ThreatQ裝置與以下裝置通訊：

1.登入您的Umbrella控制面板。

2.定位至策略>整合。

3.在表中，選擇ThreatConnect將其展開。

4.選擇啟用，然後選擇儲存。這將為您在Umbrella中的組織生成唯一的特定URL。



當您將ThreatConnect配置為將資料傳送到Umbrella時，需要本文後面的URL。

配置ThreatConnect與Umbrella通訊

為了開始將流量從ThreatConnect傳送到Umbrella，您需要使用本文第一部分中生成的URL資訊配置ThreatConnect:

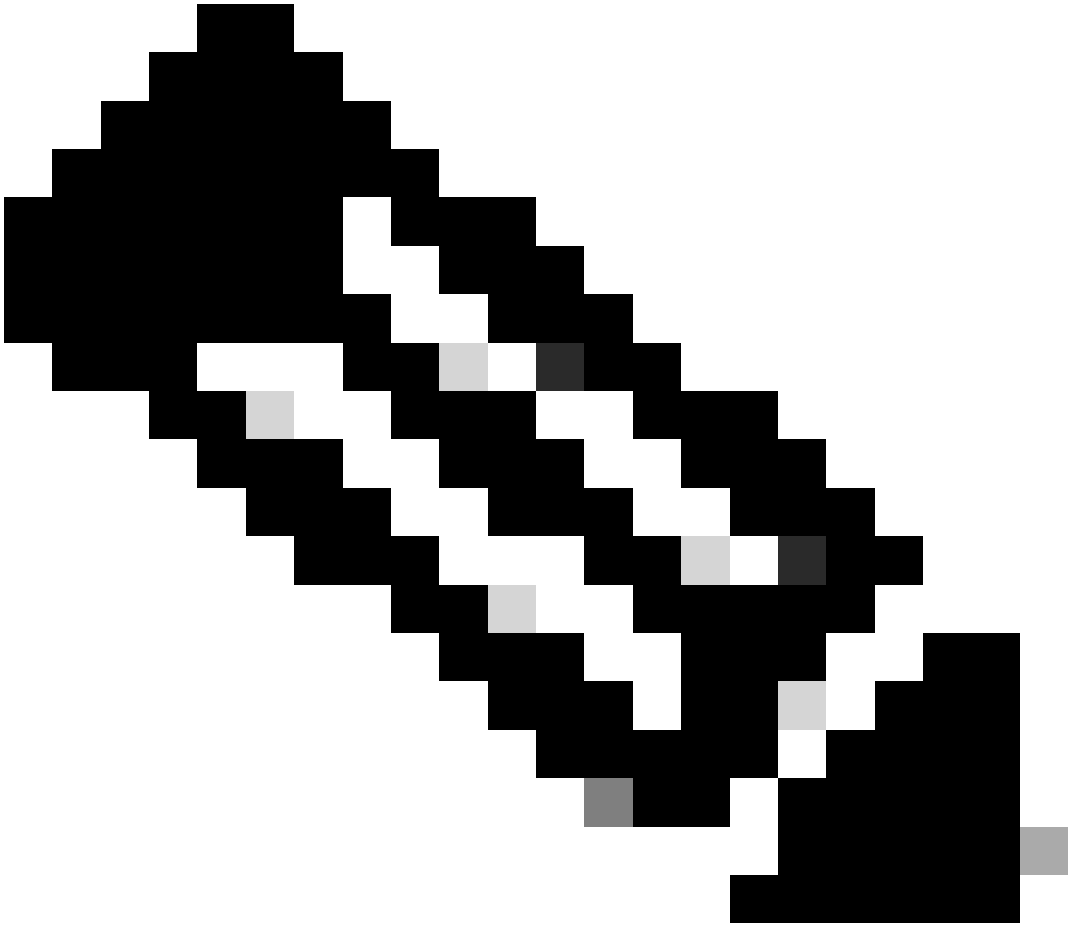
1.登入到ThreatConnect控制面板。

2.在相應區域新增URL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ThreatConnect中配置API整合，Umbrella建議聯絡ThreatConnect支援。

在稽核模式下觀察新增到ThreatConnect安全類別的事件

隨著時間的推移，ThreatConnect控制面板中的事件可以開始填充一個特定目標清單，該清單可以作為ThreatConnect安全類別應用到策略。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策略，並且不會導致對現有Umbrella策略進行任何更改。



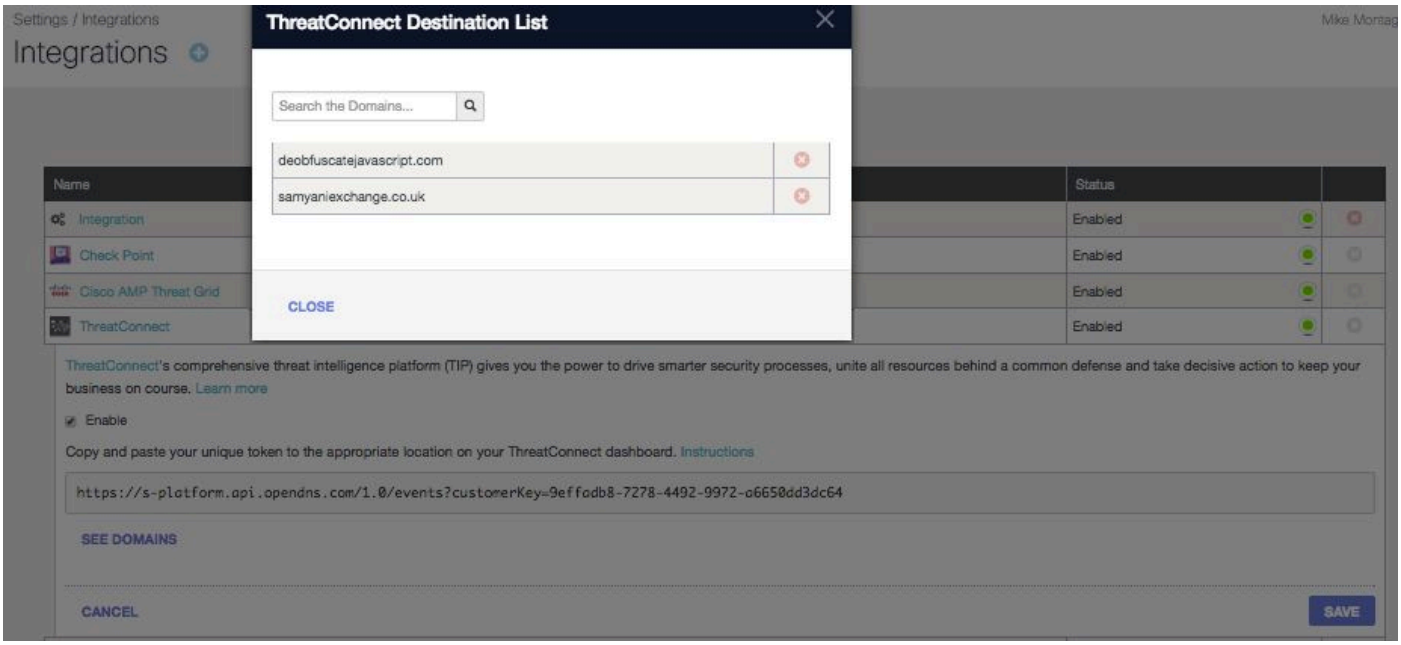
附註：可以啟用稽核模式，但根據您的部署配置檔案和網路配置，稽核模式需要很長時間。

檢視目標清單

您可以隨時檢視Umbrella中的ThreatConnect目標清單：

1.在Umbrella控制面板中，導航至Policies > Integrations。

2.在表中，展開ThreatConnect並選擇See Domains。



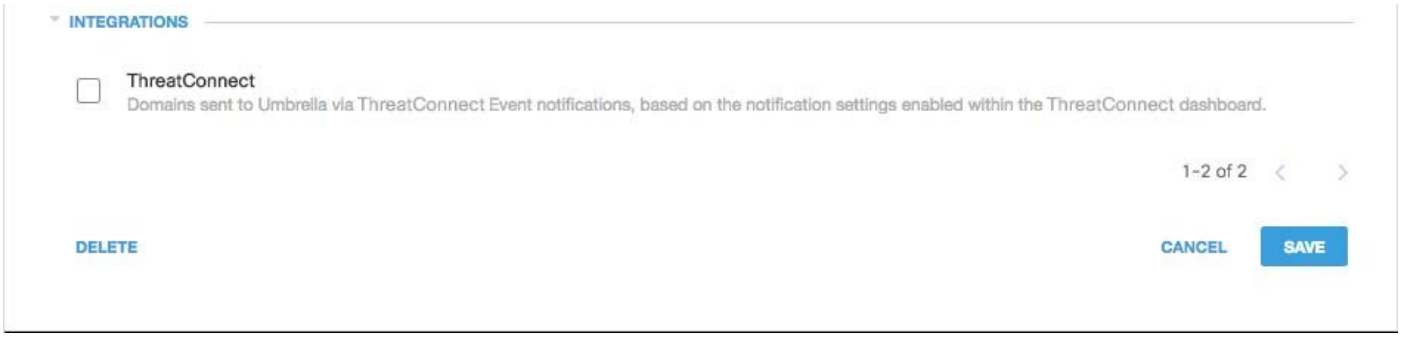
檢視策略的安全設定

您可以檢視可在任何時間為策略啟用的安全設定：

1.在Umbrella控制面板中，導航至Policies > Security Settings。

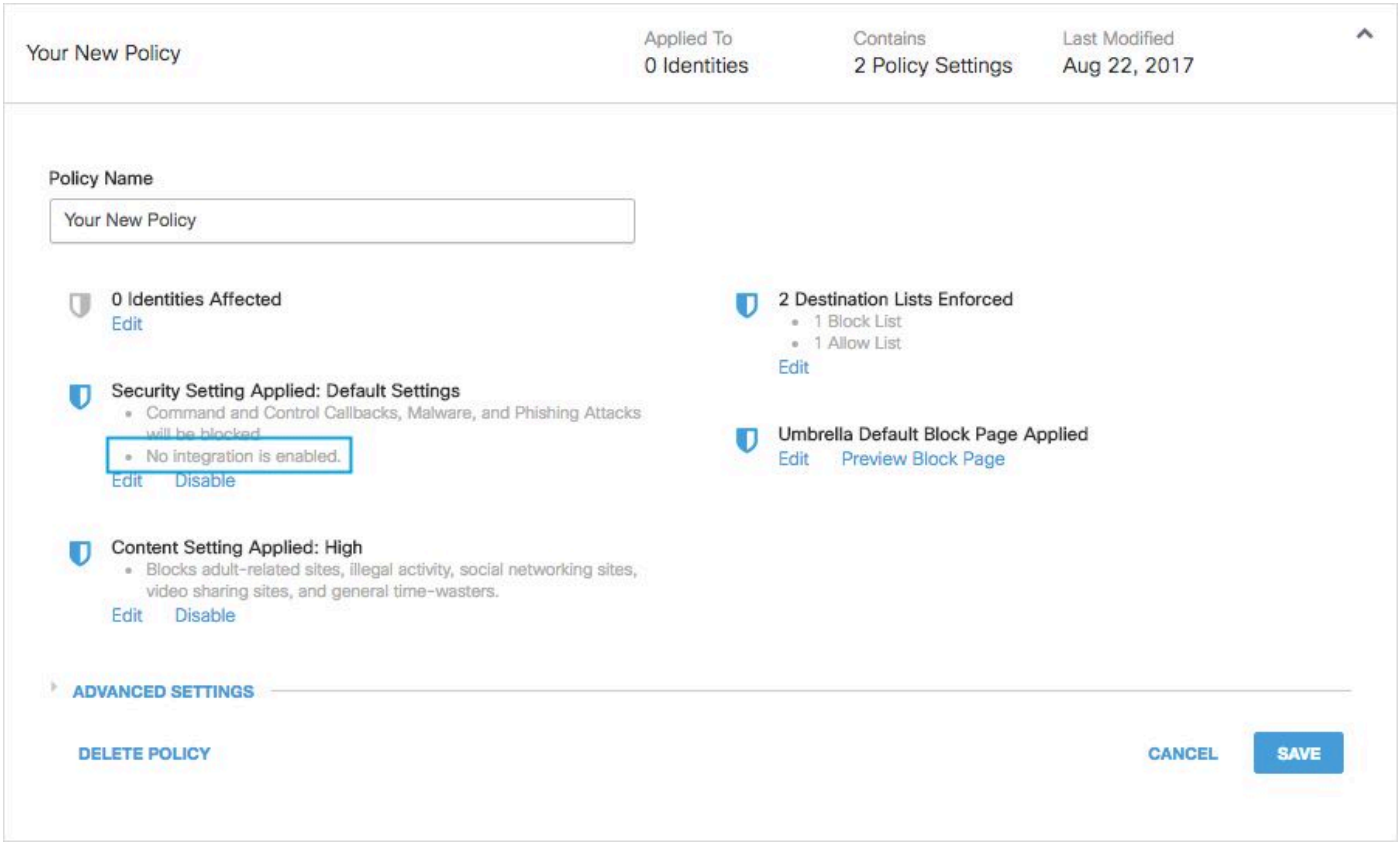
2.選擇表中的安全性設定將其展開。

3.滾動到Integrations以查詢ThreatConnect設定。



115014036566

4.您還可以通過「安全性設定彙總」頁檢視整合資訊。



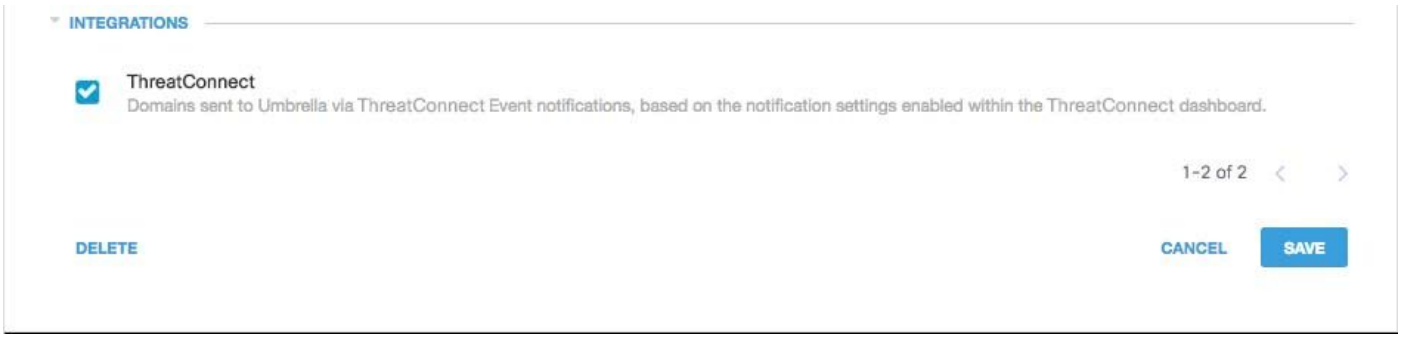
25464103885972

在阻止模式下將ThreatConnect安全設定應用於託管客戶端的策略

一旦準備好由由Umbrella管理的客戶端實施這些附加安全威脅，只需更改現有策略的安全設定，或建立位於預設策略上方的新策略以確保首先實施該策略：

1.定位至策略>安全設定。

2.在Integrations下，選擇ThreatConnect，然後選擇Save。



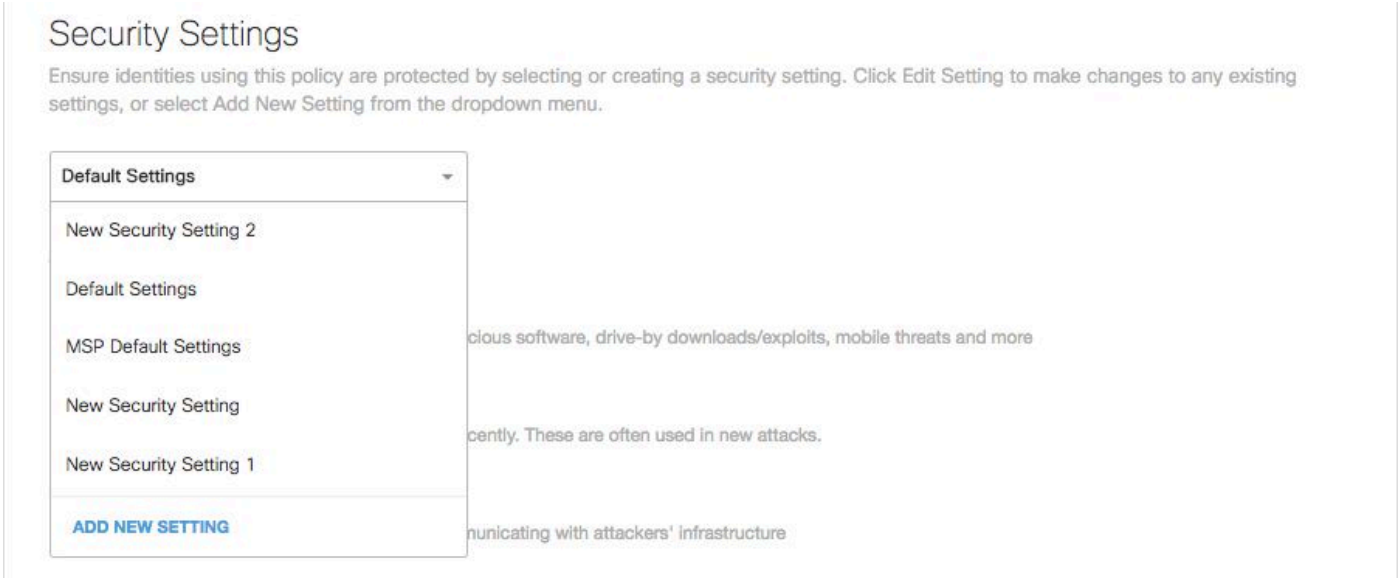
115014203703

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。

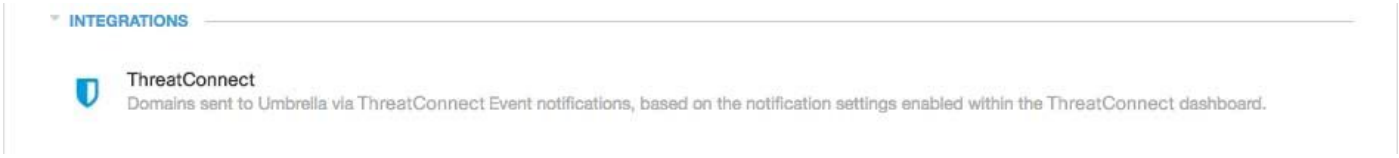
2.展開策略。在應用的安全設定下，選擇編輯。

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



25464103908884

Integrations下的遮蔽圖示將更新為藍色。



115014037666

4.選擇「Set & Return」。

然後，ThreatConnect的安全設定中包含的ThreatConnect域將使用此策略為身份進行阻止。

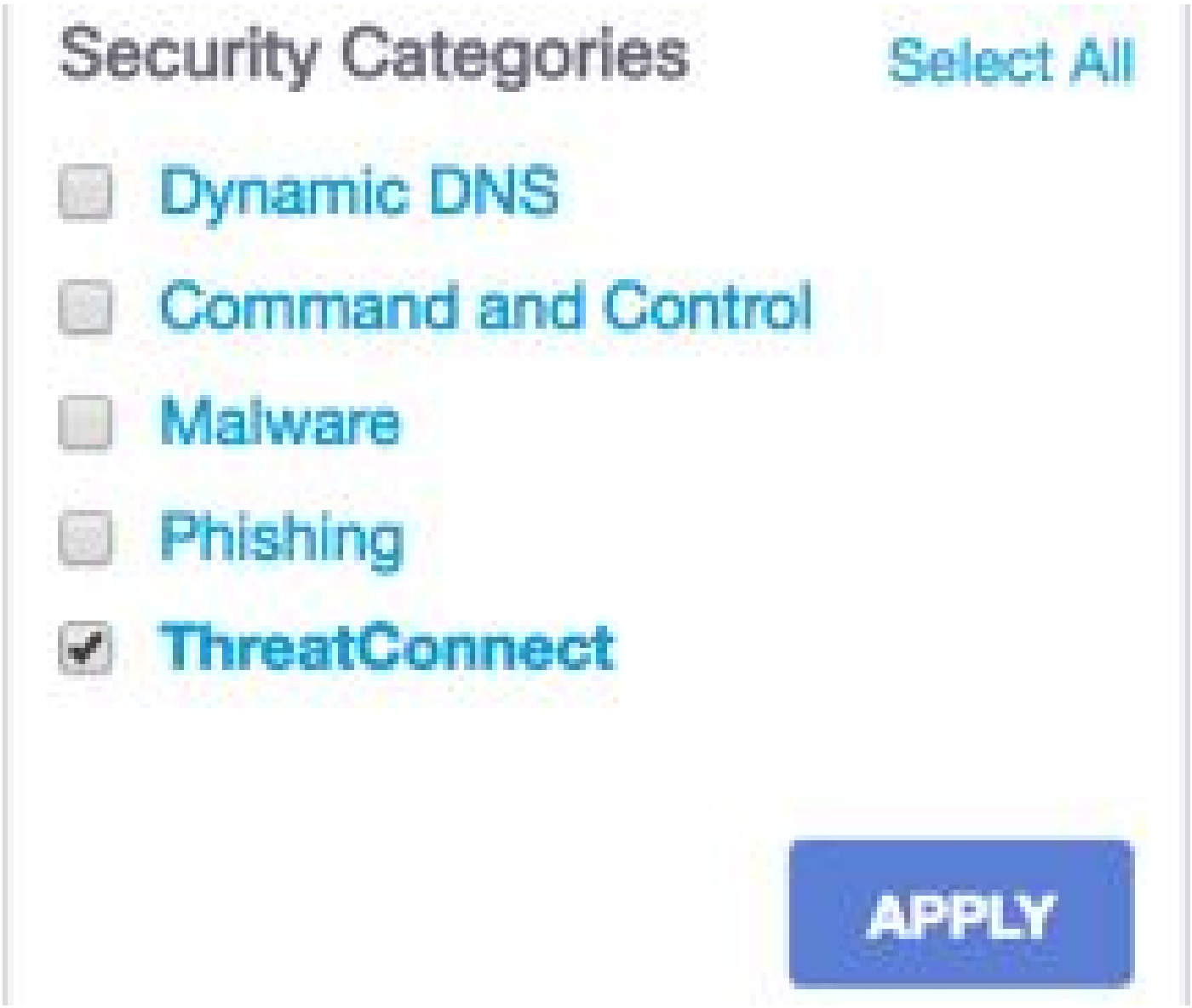
在Umbrella中報告ThreatConnect事件

報告ThreatConnect安全事件

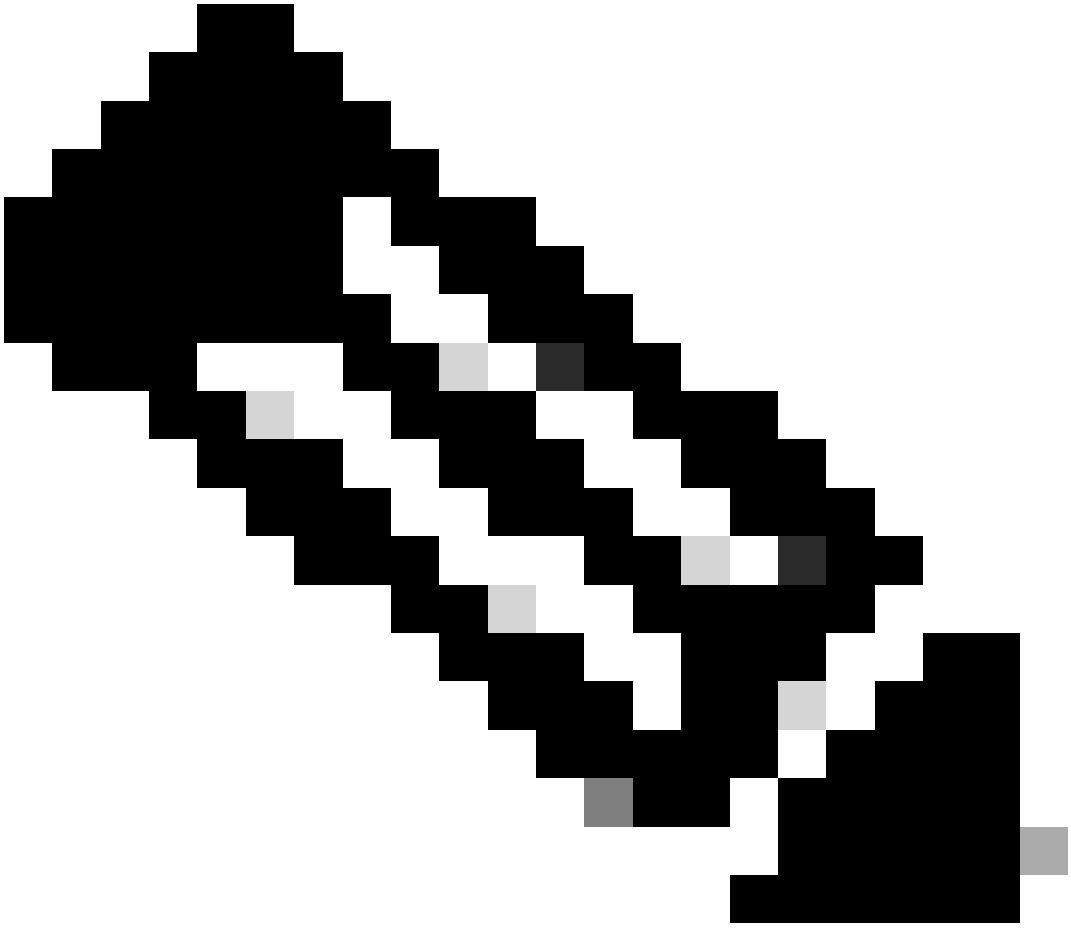
ThreatConnect Destination List是可以報告的安全類別清單之一。大多數或所有報表都使用安全類別作為篩選器。例如，您可以篩選安全類別，以便僅顯示與ThreatConnect相關的活動：

1.定位至報告>活動搜尋。

2.在Security Categories下，選擇ThreatConnect以篩選報告，以僅顯示ThreatConnect的安全類別。



115014206603



附註：如果已禁用ThreatConnect整合，則它不會顯示在「安全類別」篩選器中。

3.選擇Apply。

報告將域新增到ThreatConnect目標清單的時間

管理員稽核日誌包括ThreatConnect控制面板中向目標清單新增域的事件。名為「ThreatConnect帳戶」（也帶有ThreatConnect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。

通過為「ThreatConnect帳戶」使用者應用篩選器，您可以進行篩選以僅包括ThreatConnect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ThreatConnect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）。

這一方針更加可取，原因有二：

- 首先，如果ThreatConnect控制面板在域被刪除後重新新增域，則允許清單可防止出現進一步的問題。
- 此外，允許清單還顯示問題域的歷史記錄，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ThreatConnect安全設定僅應用於受管Umbrella身份的子集（例如，它僅應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Policies > Destination Lists，然後選擇Add(+)圖示。

2.選擇Allow並將您的域新增到清單中。

3.選擇儲存。

一旦儲存了目標清單，您就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ThreatConnect目標清單中刪除域

ThreatConnect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ThreatConnect目標清單。但是，如果ThreatConnect控制面板將域重新傳送到Umbrella，則刪除操作不是永久性的。

刪除域：

1.定位至「策略」>「整合」。

2.選擇ThreatConnect將其展開。

3.選擇檢視域。

4.搜尋要刪除的域名。

5.選擇刪除圖示。

6.選擇關閉，然後選擇儲存。

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

ThreatConnect控制面板中修正誤報。稍後，您可以從ThreatConnect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）。