將ZeroFOX與Umbrella整合

目錄

簡介

本文檔介紹如何將ZeroFOX Enterprise與Umbrella整合，以便可以將安全事件應用於受Umbrella保護的客戶端。

ZeroFOX企業版和思科Umbrella整合概述

通過將ZeroFOX Enterprise與Cisco Umbrella整合，安全人員和管理員可以擴展針對漫遊的筆記型電腦、平板電腦或電話的當今基於社群媒體的威脅的防護，同時為分散式企業網路提供另一層強制措施。

Cisco Umbrella和ZeroFox整合：如何運作？

ZeroFOX Enterprise將其發現的任何威脅（例如基於社群媒體的網路威脅，包括目標惡意軟體、網路釣魚、社交工程、模擬和其他欺詐或惡意活動）推送至思科保護傘，以便在全球範圍內實施。

然後，Umbrella驗證威脅以確保將其新增到策略中。如果確認來自ZeroFOX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ZeroFOX目標清單。該策略會立即應用於從分配給該策略的裝置發出的任何請求。

接下來，Cisco Umbrella會自動解析ZeroFOX警報並將惡意站點新增到ZeroFOX目標清單，從而將

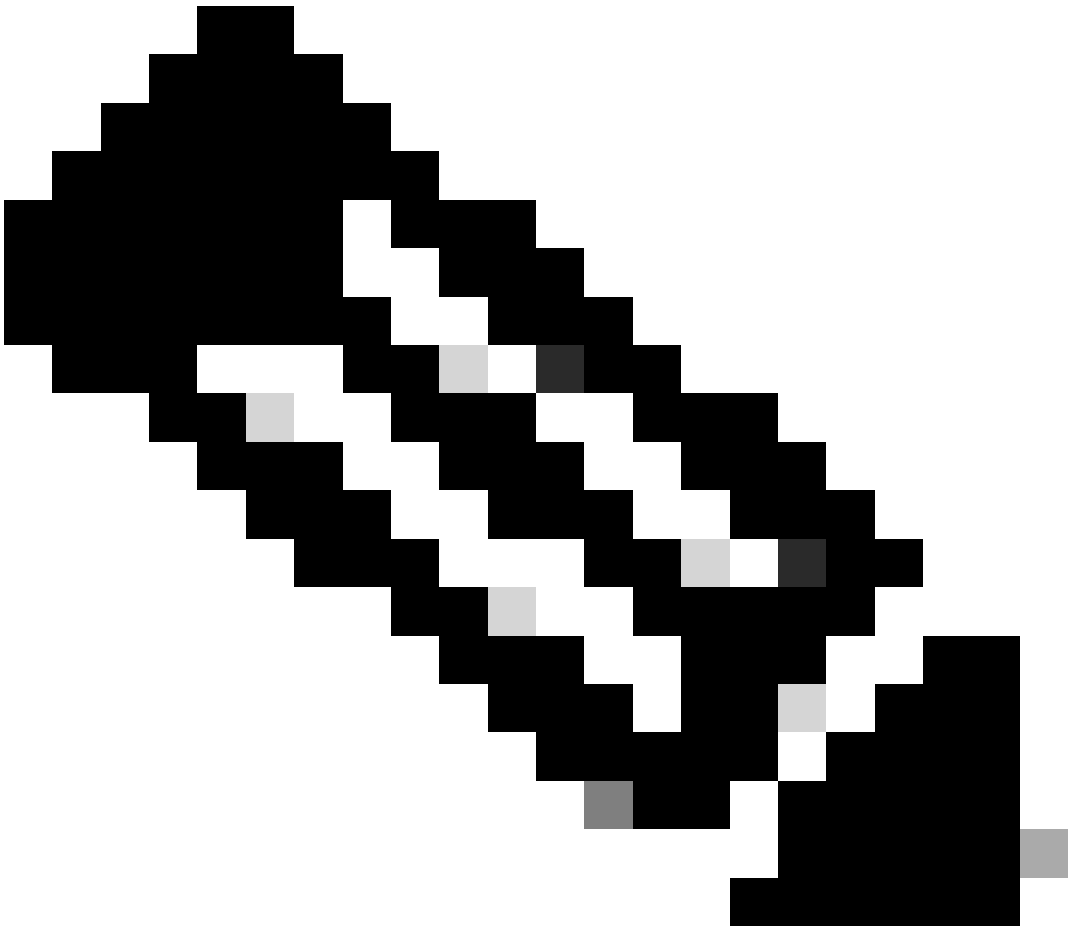
ZeroFOX智慧擴展到所有遠端使用者和裝置，並為您的公司網路提供另一層實施功能。

這通過以下簡單的設定步驟實現：

1. 啟用Umbrella中的整合以生成API令牌。
2. 將該API令牌貼上到您的ZeroFOX帳戶中。
3. 將ZeroFOX設定為在所需策略的安全設定下阻止

必要條件

- ZeroFOX Enterprise管理許可權
- Umbrella儀表板管理許可權
- Umbrella儀表板必須啟用ZeroFOX整合



附註：ZeroFOX整合僅包含在Umbrella Platform軟體包中。如果您沒有平台軟體包並希望整合ZeroFOX，請聯絡您的Cisco Umbrella代表。如果您有平台軟體包，但是沒有將ZeroFOX視為控制面板的整合，請與Umbrella支援聯絡。

重要事項：雖然Umbrella會嘗試盡最大努力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，我們建議根據您的策略，將您不希望阻止的任何域新增到Global Allow List或其他目標清單中。

示例包括：

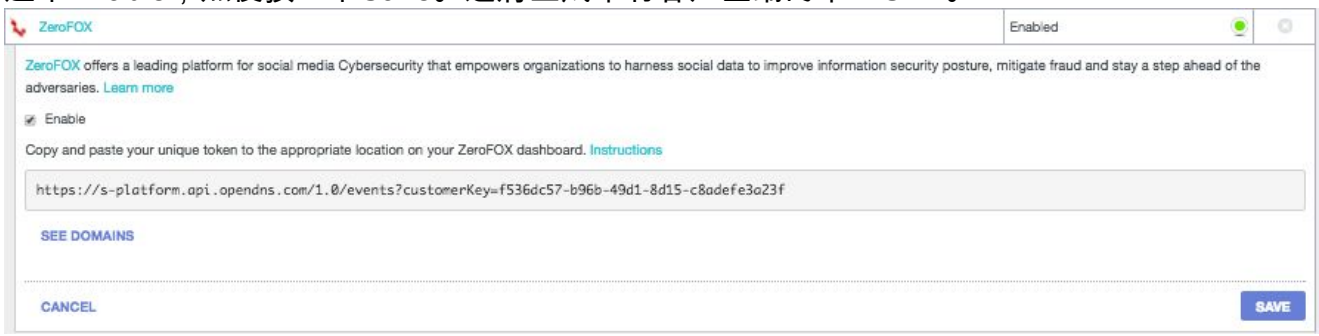
- 您組織的首頁。例如，mydomain.com。
- 表示您提供的服務的域，可以同時具有內部和外部記錄。例如，mail.myservicedomain.com和portal.myotherservicedomain.com。
- 您嚴重依賴的不太知名的雲應用程式無法識別Umbrella，也無法將其包括在其自動域驗證中。例如，localcloudservice.com。

全域性允許清單位於Umbrella中的Policies > Destination Lists。如需詳細資訊，請參閱我們的檔案：管理目的地清單

步驟 1:Umbrella指令碼和API令牌生成

首先在Umbrella中查詢您的唯一URL，以便與ThreatQ裝置通訊。

1. 以Admin身份登入到Umbrella控制面板，導航到Settings > Integrations，然後按一下表格中的「ZeroFOX」將其展開。
2. 選中Enable，然後按一下Save。這將生成帶有客戶金鑰的唯一URL。

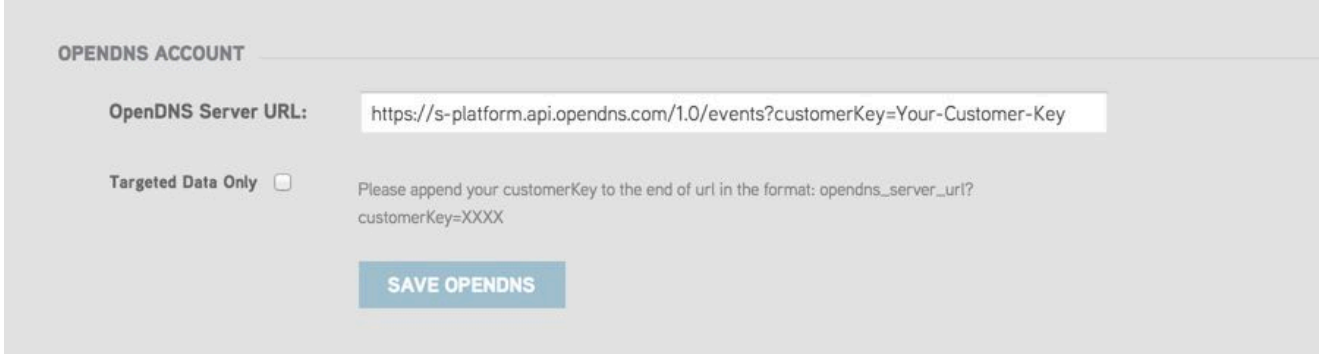


以後配置ZeroFOX時需要URL，因此請複製該URL並轉到ThreatQ儀表板。

步驟 2:設定ZeroFOX企業儀表板以向Umbrella傳送資訊

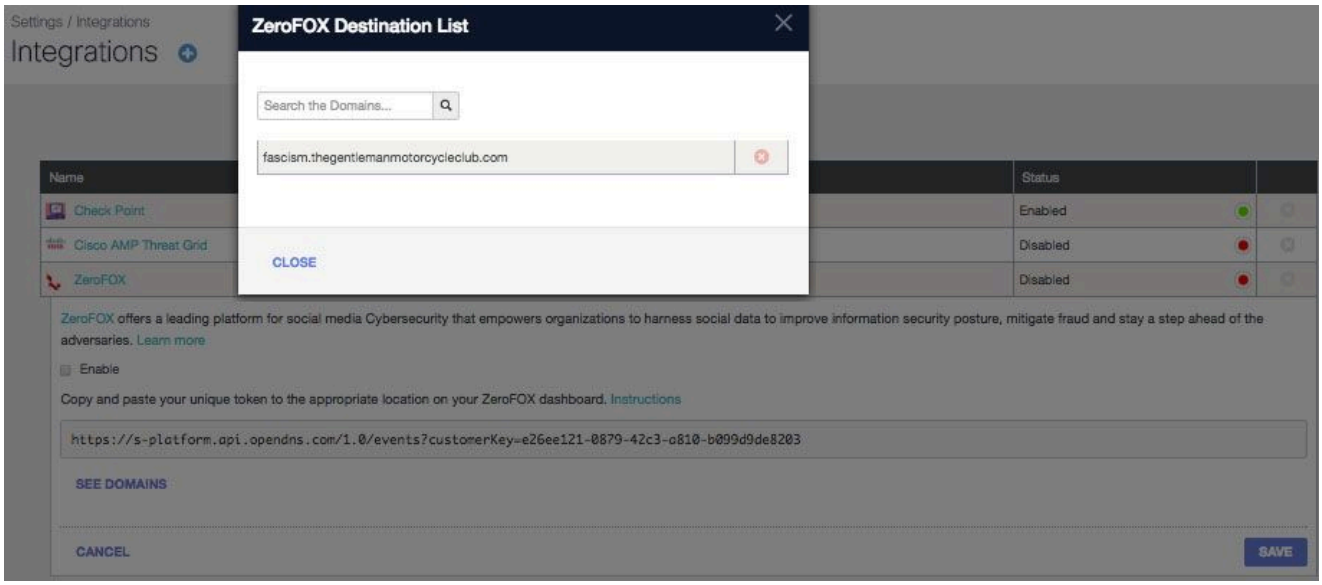
下一步是將您在步驟1中複製的URL新增到ZeroFOX儀表板中。

1. 按一下Zerofox控制面板中的齒輪圖示，然後選擇Account Settings。
2. 向下滾動整合清單，直到您看到OpenDNS帳戶資訊，然後將Umbrella中的URL貼上到OpenDNS伺服器URL欄位。
3. 在首次啟用整合後，我們建議您選中Targets Only。



步驟 3:設定要在Umbrella中阻止的ZeroFOX事件

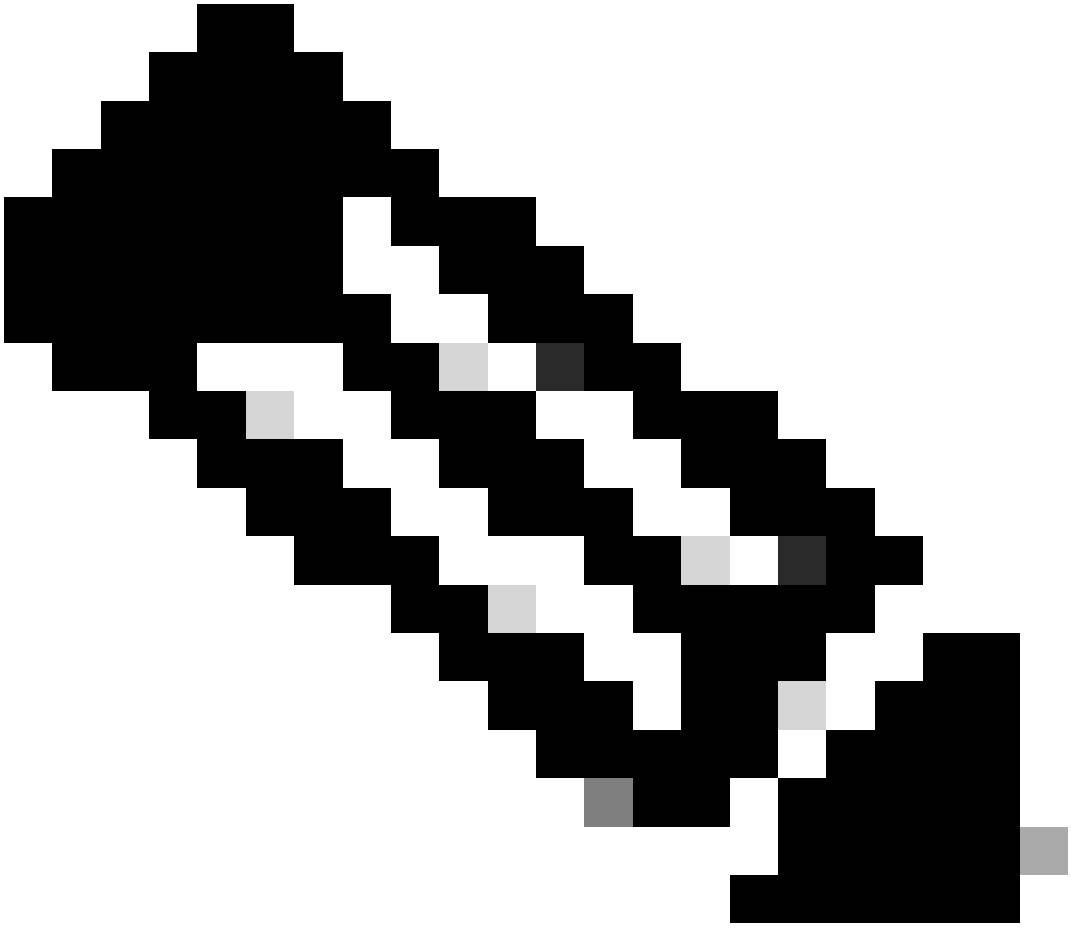
1. 以管理員身份重新登入到Umbrella控制面板。
2. 導航到設定>整合，然後按一下表格中的「ZeroFOX」將其展開。
3. 按一下See Domains。
   這將展開一個域清單，其中包括來自您的ZeroFOX帳戶的最後幾個小時事件。從那時起，一個可搜尋的清單開始被填充和增長。



下一步是觀察和稽核新增到您的新ZeroFOX安全類別的事件。

觀察在審計模式下新增到ZeroFOX安全類別的事件

ZeroFOX Enterprise中的事件開始填充一個特定目標清單，該清單可以作為ZeroFOX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審計模式，不應用於任何策略，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

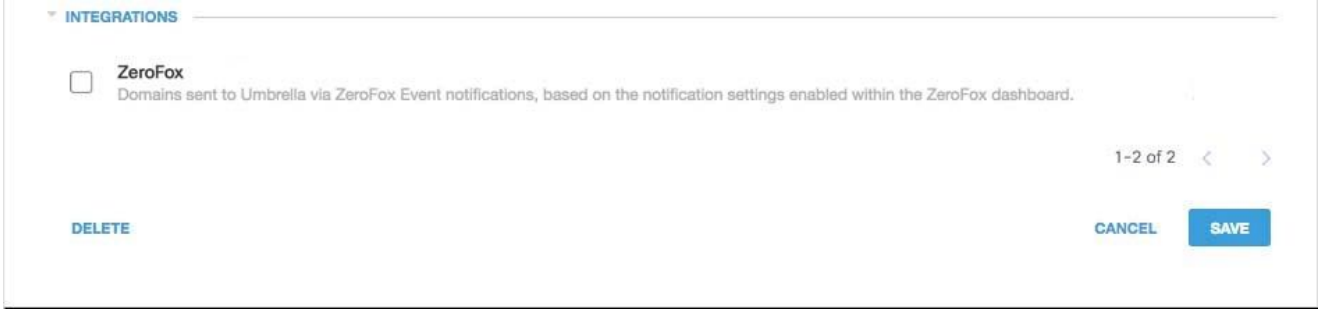
您可以隨時檢視ZeroFox目標清單。

1. 導覽至Settings > Integrations。
2. 展開表中的「ZeroFOX」，然後按一下「查看域」。

檢視策略的安全設定

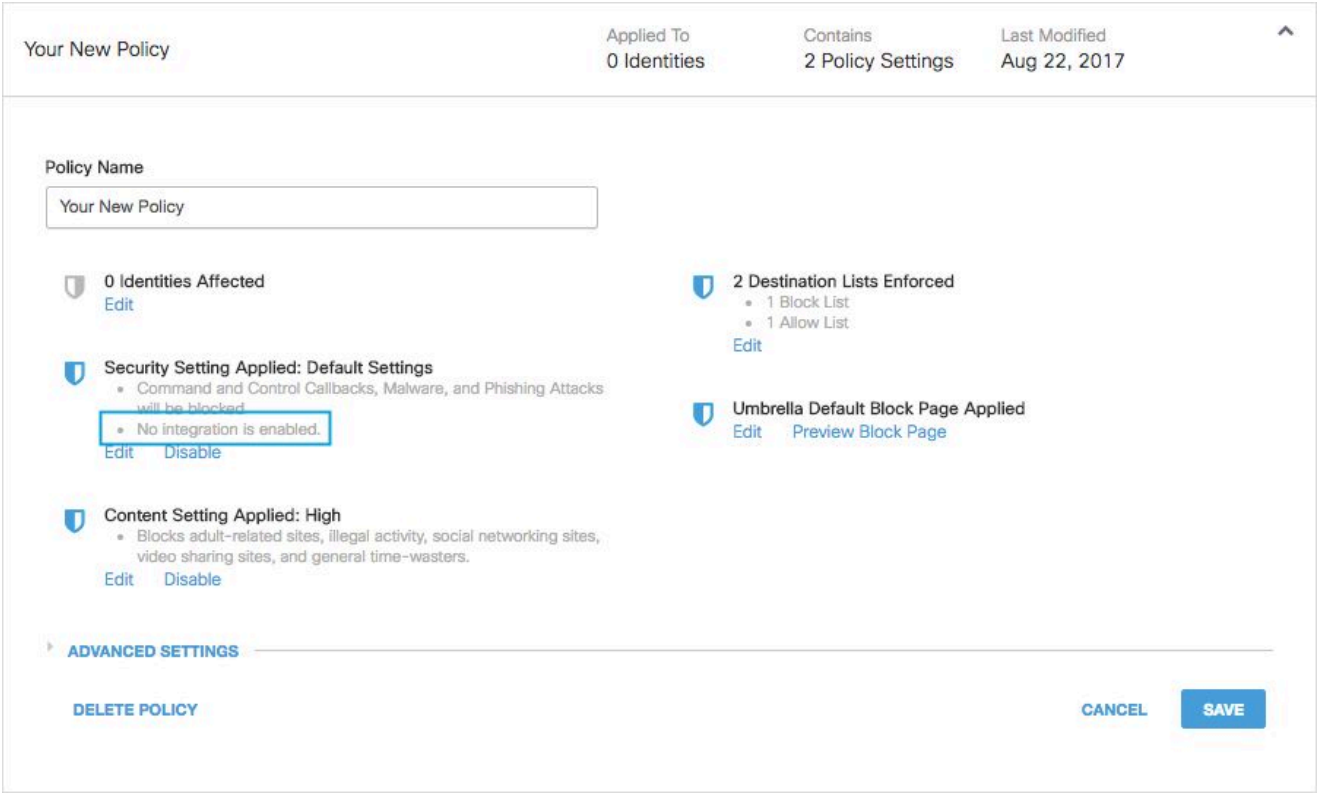
您可以隨時檢視可以為策略啟用的安全設定。

1. 導航到Policies > Security Settings。
2. 按一下表中的安全設定將其展開，然後滾動到Integrations以查詢ZeroFOX設定。



115014041606

您還可以通過「安全設定摘要」頁檢視整合資訊。

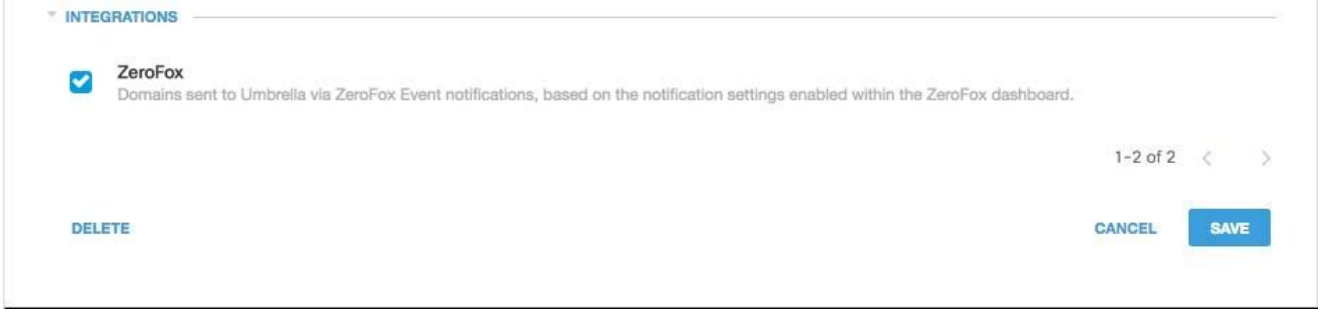


25464154913556

在塊模式下將ZeroFOX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，或建立一個高於預設策略的新策略，以確保首先實施該策略。

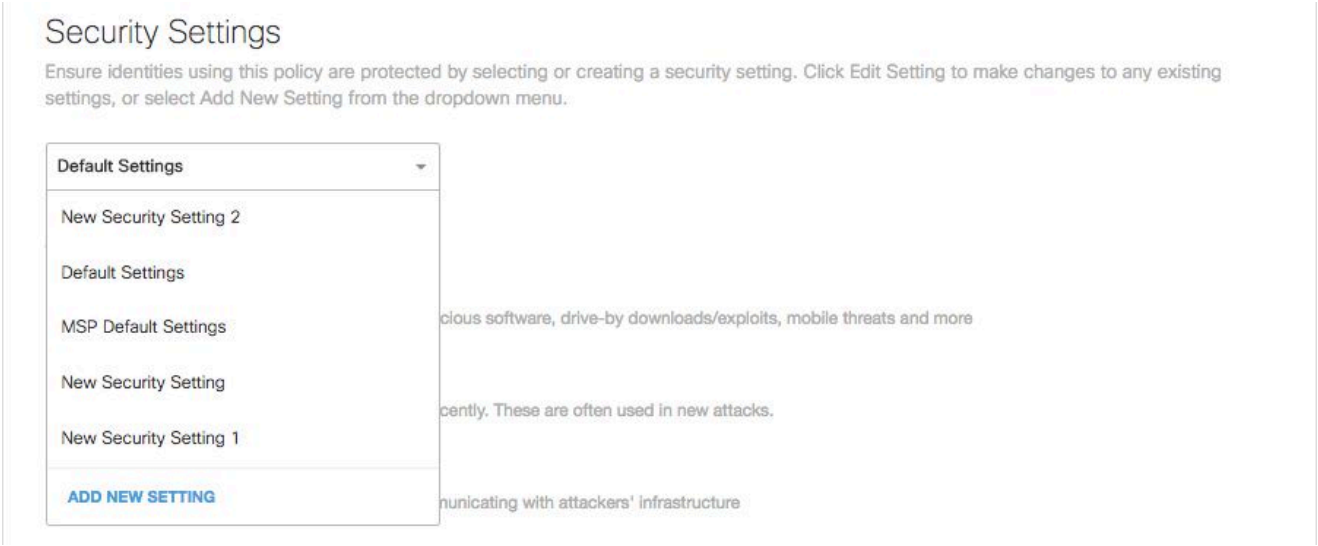
1. 導覽至Policies > Security Settings，然後在Integrations下選中ZeroFOX，然後按一下Save。



115014042806

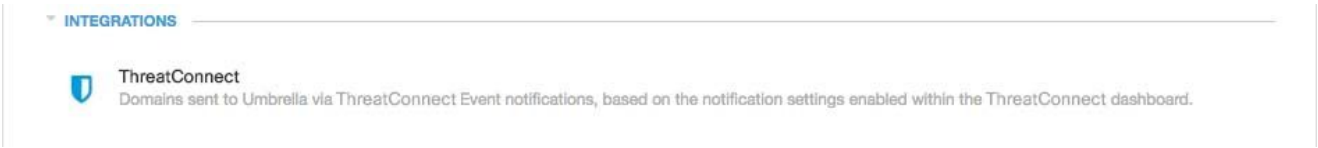
接下來，在「策略」嚮導中，將安全設定新增到正在編輯的策略中：

1. 導航到Policies > Policy List。
2. 展開策略並按一下Security Setting Applied下的Edit。
3. 在「Security Settings」下拉選單中，選擇包含ThreatConnect設定的安全設定。



25464147943700

Integrations下的遮蔽圖示將更新為藍色。



25464147957652

4. 按一下「Set & Return」。

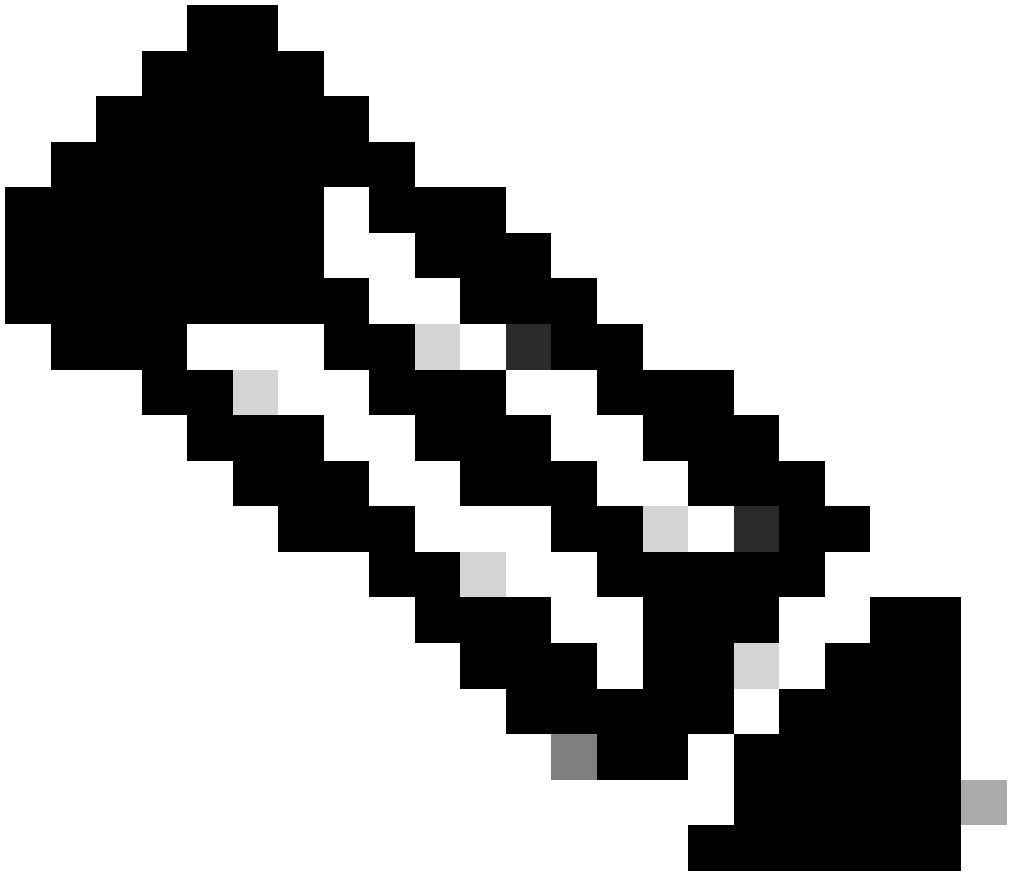
ZeroFOX的安全設定中包含的ZeroFOX域對於使用該策略的那些標識被阻止。

在Umbrella for ZeroFOX事件中報告

報告ZeroFOX安全事件

ZeroFOX 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，以便只顯示ZeroFOX相關的活動。

1. 導航到Reporting > Activity Search，然後在Security Categories下選擇ZeroFOX以篩選報告，以便僅顯示ZeroFOX的安全類別。



附註：如果禁用ZeroFOX整合，則不會顯示在「安全類別」篩選器中。

115014043046

2. 按一下「Apply」。

報告將域新增到ZeroFOX目標清單的時間

Umbrella Admin Audit（Umbrella管理稽核）日誌包含來自您ZeroFOX帳戶的事件，因為它將域新增到目標清單。

Umbrella Admin Audit日誌位於Reporting > Admin Audit Log。為了報告何時新增域，請將過濾器應用於ZeroFox目標清單的標識與設定，篩選為僅包含ZeroFOX更改。

運行報告後，您會看到從整合新增ZeroFOX目標清單時所進行的更改的清單。

處理不需要的檢測或誤報

管理用於不需要的檢測的允許清單

雖然不太可能，但是ZeroFOX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，我們建議將網域新增到允許清單，此清單優先於所有其他型別的封鎖清單（包括安全設定）。當兩個域中都存在域時，允許清單優先於阻止清單。

這一方法更可取有兩個原因。首先，如果ZeroFOX裝置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。

如果塊模式中的ZeroFOX安全設定僅應用於受管Umbrella標識的子集（例如，它僅應用於漫遊電腦和流動裝置），則可以為這些標識或策略建立特定允許清單。

要建立允許清單，請執行以下操作：

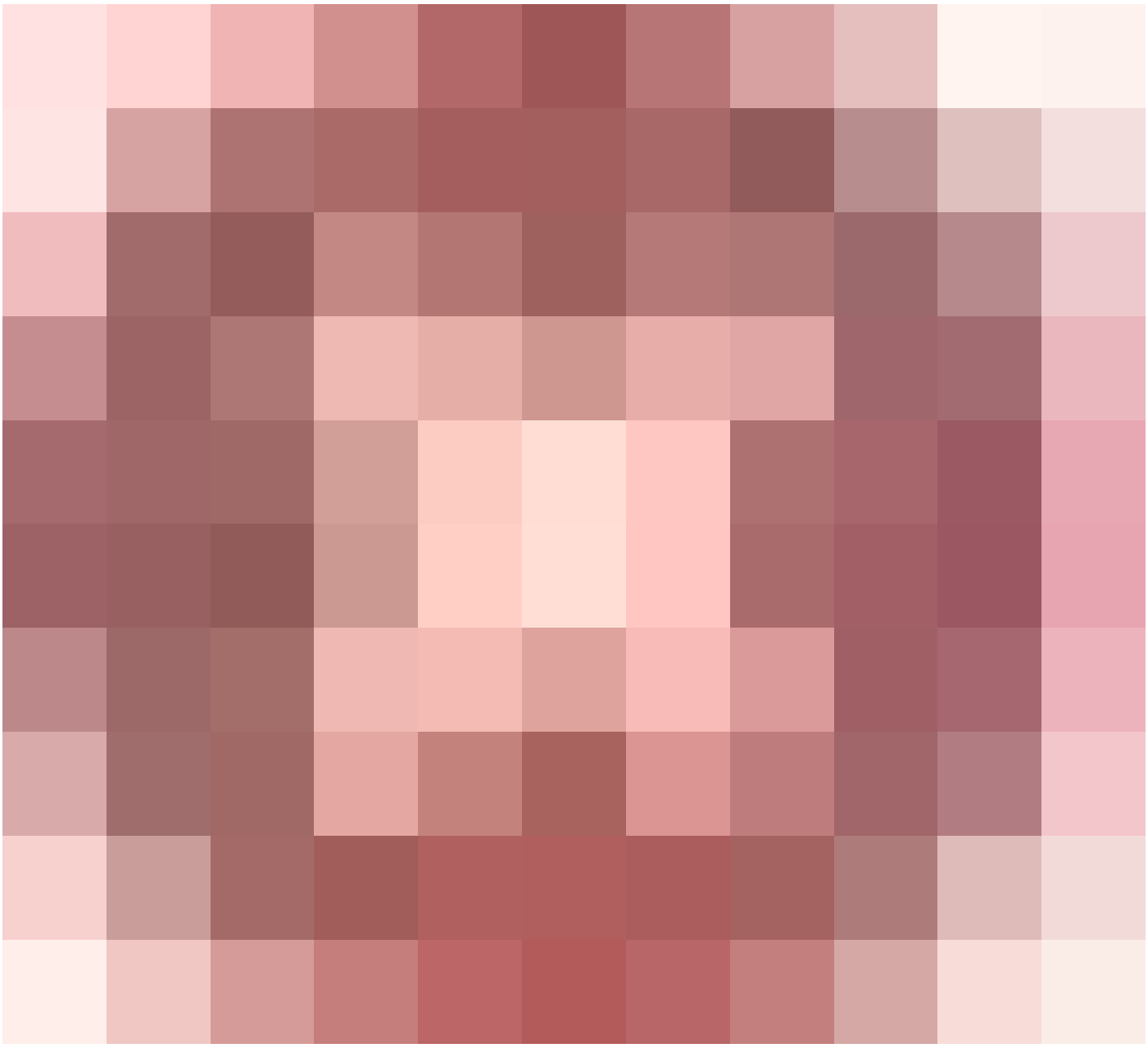
1. 導航到Policies > Destination Lists，點選 

「新增」圖示。
2. 選擇Allow，然後將您的域新增到清單中。
3. 按一下「Save」。

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ZeroFOX目標清單中刪除域

有一個



「ZeroFOX目標清單」中每個域名旁邊的(刪除)圖示。通過刪除域，可以在出現不需要的檢測時清除ZeroFOX目標清單。

但是，如果ZeroFOX將域重新傳送到Umbrella，則刪除操作不是永久性的。

刪除域：

1. 導航到設定>整合，然後按一下「ZeroFOX」將其展開。
2. 按一下See Domains。
3. 搜尋要刪除的域名。
4. 按一下Delete圖示。

5. 按一下「Close」。
6. 按一下「Save」。

如果出現不需要的檢測或誤報，我們建議立即在Umbrella中建立允許清單，然後在ZeroFOX中修正誤報。稍後，您可以從ZeroFOX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）。