瞭解適用於自訂整合的Umbrella執行API

目錄

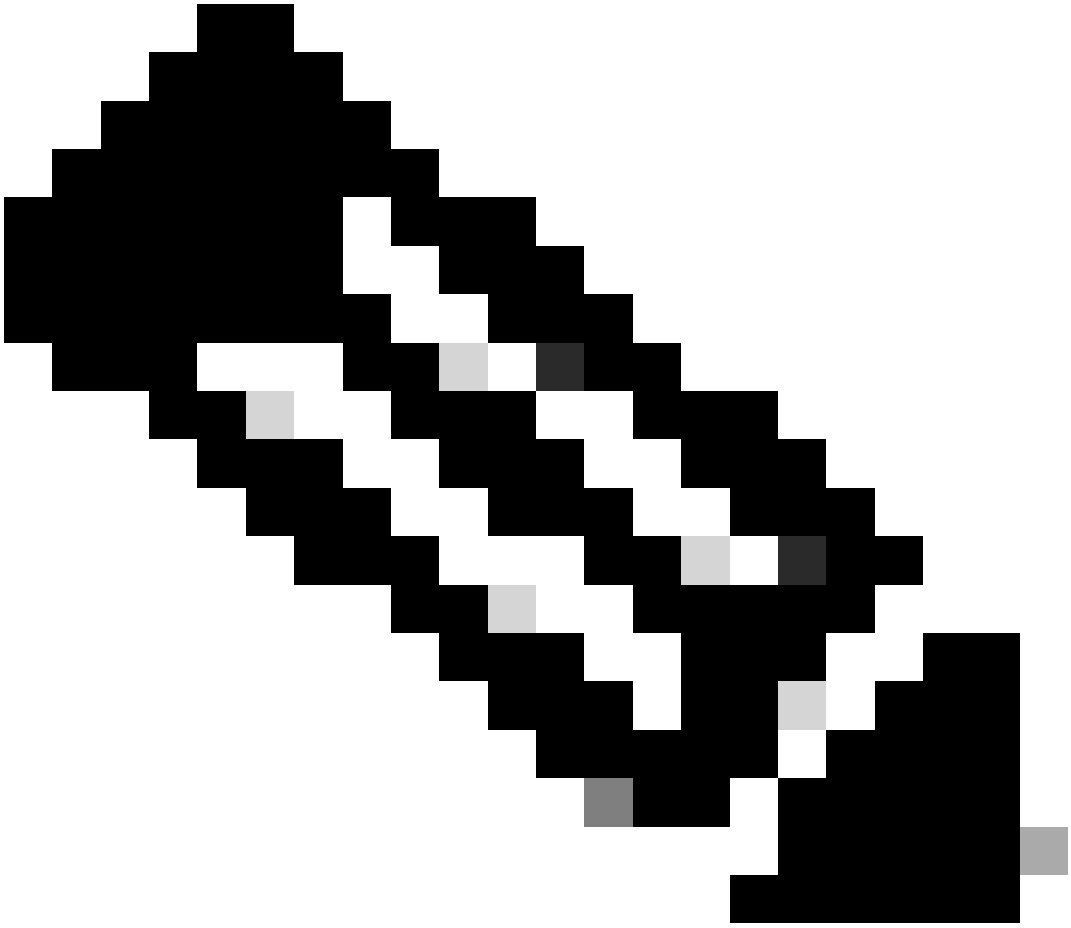
簡介

本檔案介紹用於自訂整合的Umbrella Enforcement API。

什麼是Umbrella Enforcement API?

Umbrella Enforcement API允許合作夥伴和擁有自己自主開發的SIEM/威脅情報平台(TIP)環境的客戶將事件和/或威脅情報注入其Umbrella環境中。然後，這些事件會立即轉換為可視性和強制性，其範圍可以超出邊界，從而超出可能生成這些事件或威脅情報的系統的範圍。

實施API可以採用此API文檔中所述的通用事件格式接收事件，並且可以支援ADD、DELETE或LIST函式。



附註：如果您的Umbrella控制面板中沒有用於自定義整合的Umbrella Enforcement API，並且希望擁有訪問許可權，請與您的Cisco Umbrella代表聯絡。

我為什麼要用它？

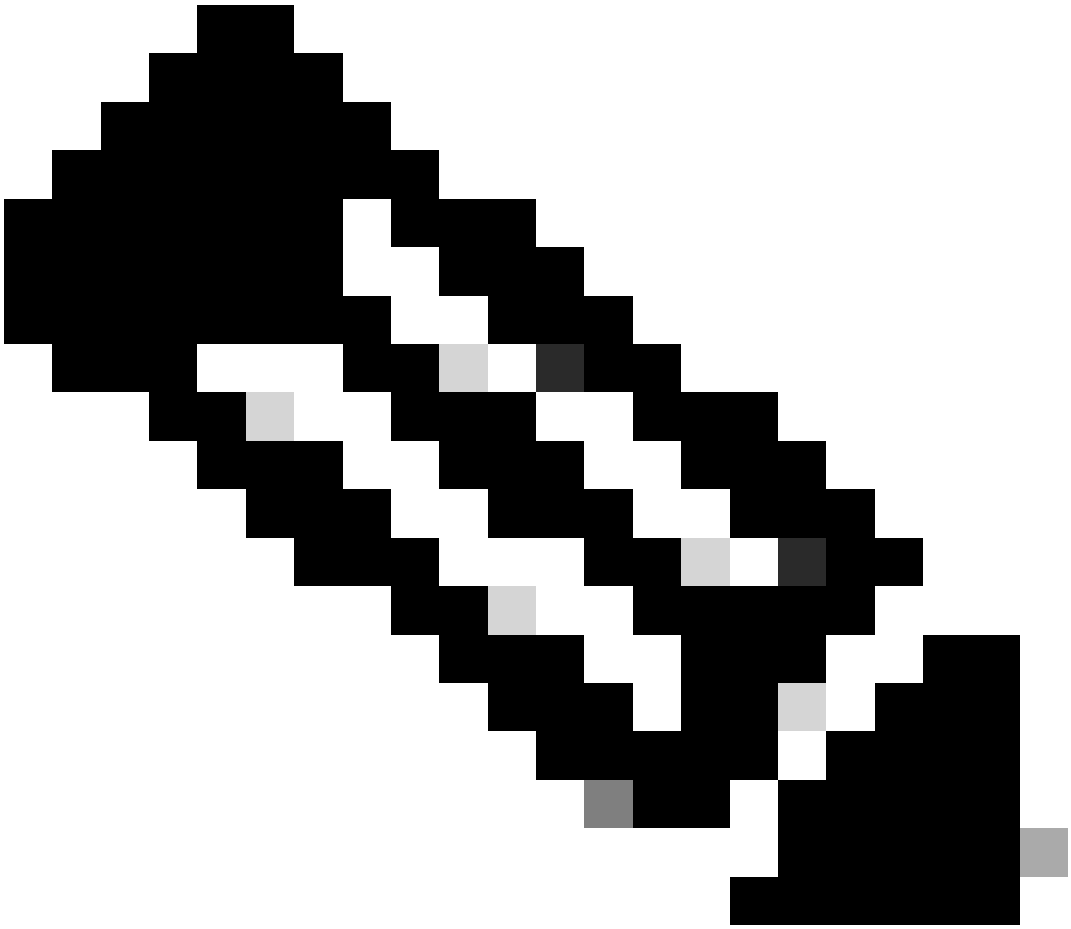
您可能已經處理、管理和建立自己的威脅情報系統和流程，從而產生對識別為惡意或可疑的域採取措施的願望。在這種情況下，一旦決定需要對事件執行操作（例如，將其轉換為保護），而不是出於實施目的手動向Umbrella新增保護，您就可以使用實施API來自動化此過程，並根據與事件關聯的域即時實施保護。

這樣，您的安全團隊就可以將時間和精力集中到調查上，而不是持續配置Umbrella。它使您的安全團隊能夠繼續使用他們的工具和流程，而不必跳到Umbrella控制面板來更新目標清單。實質上，您可以通過API直接管理的外部源在Umbrella中建立目標清單，然後選擇在Umbrella中阻止這些目標的身份標識。

我該如何使用它？

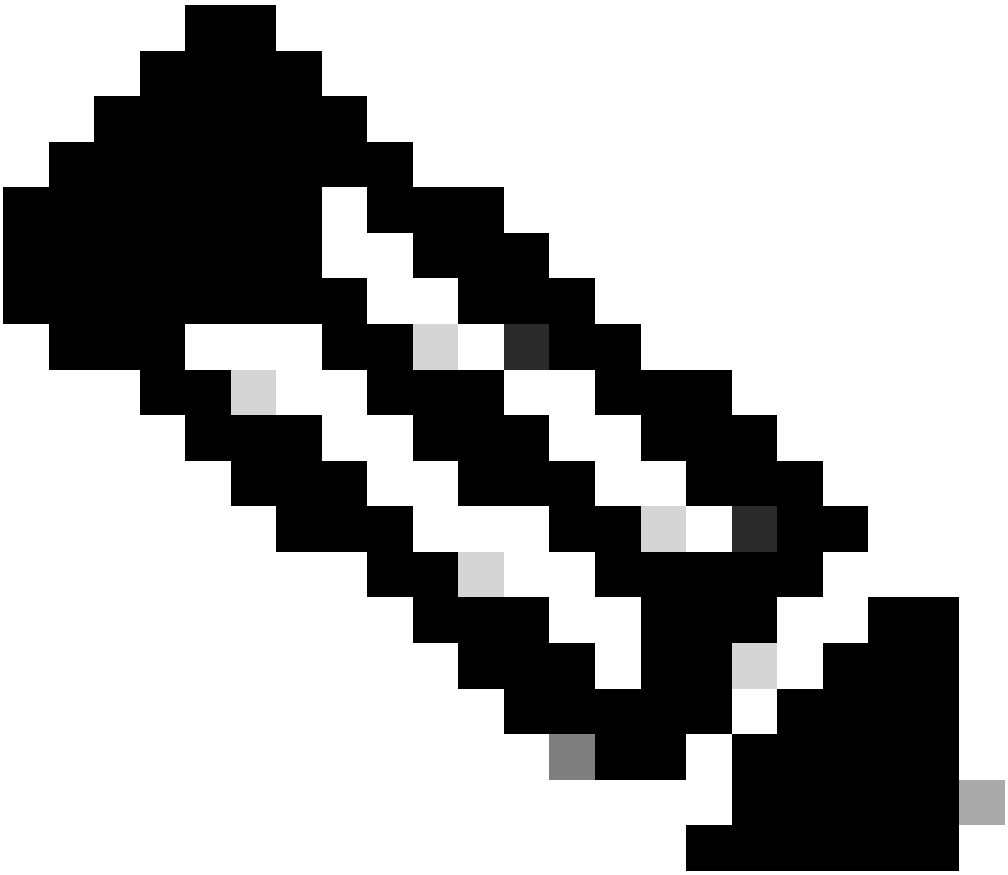
將事件新增到實施API

新增事件後，Enforcement會嘗試從事件中提取域。



附註：未來會新增對於IP位址和URL的支援。

- 事件可以包含任何您想要的原始事件詳細資訊，但是必須符合在API文檔中說明的規範。



附註：以後可能會在Umbrella控制面板中新增對表面事件詳細資訊的支援。

- 如果提取了域，則由Cisco Umbrella安全圖形驗證該域，以確保它不是已知正常的域，該域可能會導致誤報或已被思科Umbrella安全圖形視為惡意域。
- 如果它通過驗證（例如，它處於未知狀態並且可被安全阻止），則會將其新增到與該自定義整合關聯的目標清單中，並作為一個自定義安全類別顯示在Umbrella控制面板中。
- 可以基於每個策略阻止或允許自定義安全類別，以允許對可疑請求進行主動實施或被動的「稽核」。

列出實施API清單的域

- 如果工作流包括取消阻止由於以前注入的事件而被阻止的域，則LIST請求會提供當前包括在與該整合關聯的目標清單中的所有域。

從實施API清單中刪除域

- 如果工作流包括取消阻止由於以前注入的事件而被阻止的域，則DELETE請求允許您從與該整

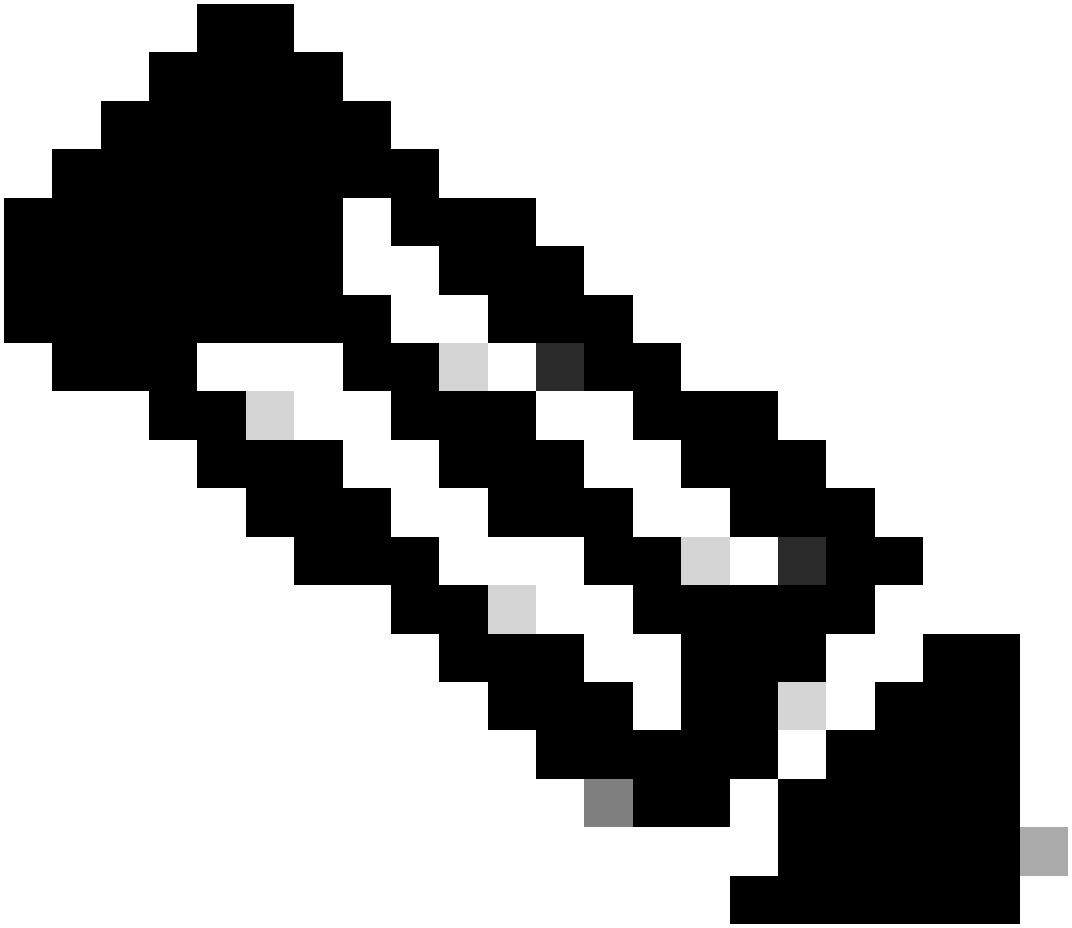
合關聯的目標清單中刪除域。

- 如果來自某個Umbrella標識的傳入DNS請求發往自定義整合目標清單中的域，則根據與觸發該請求的策略關聯的自定義整合安全設定來阻止或允許該請求。
- 結果會隨所有其他Umbrella事件一起記錄，可通過活動搜尋或使用S3整合通過Amazon S3訪問。因此，與自定義整合關聯的流量可以選擇性地收回到SIEM/TIP中，並關閉反饋迴路。

使用實施API的演練

步驟 1:建立自定義整合

一次最多可以進行10個自定義整合。



附註：如果組織是Umbrella MSP、MSSP或MOC的子組織，則在子組織級別建立整合之前，將顯示從控制檯級別共用的自定義整合。

---

1. 在Umbrella中，導航到Policies > Policy Components > Integrations，然後點選Add。
2. 為自定義整合新增名稱，然後按一下Create。
3. 展開新的自定義整合，選中Enable，複製整合URL，然後按一下Save。

步驟 2:建立自定義指令碼。

1. 請參閱本文檔附錄中的generate_event和delete_domain示例指令碼，或使用API文檔建立自己的指令碼，為生成事件、刪除域或列出域生成格式正確的請求。接下來您需要在這些指令碼中使用自定義整合URL。

步驟 3:注入示例事件

1. 使用您建立的指令碼將事件插入到您的自定義整合中。在我們的示例中，我們注入了一個包含域「creditcards.com」的事件。

步驟 4:在Umbrella控制面板中檢查目標清單

1. 返回Settings > Integrations，並在表中展開自定義整合。
2. 按一下See Domains。此時將顯示一個可搜尋的已新增域清單，並且您在第4步中的示例事件現在位於清單中。

步驟 5:檢查管理員稽核日誌。

1. 另一種驗證與自定義整合關聯的活動的方法是檢視管理員稽核日誌。
2. 導航到Reporting > Admin Audit Log。
3. 在「篩選器」下，在按標識和設定篩選中輸入自定義整合的名稱，然後按一下運行篩選器。

展開條目時，現在會看到導致將示例事件(creditcards.com)新增到自定義整合中的事件。

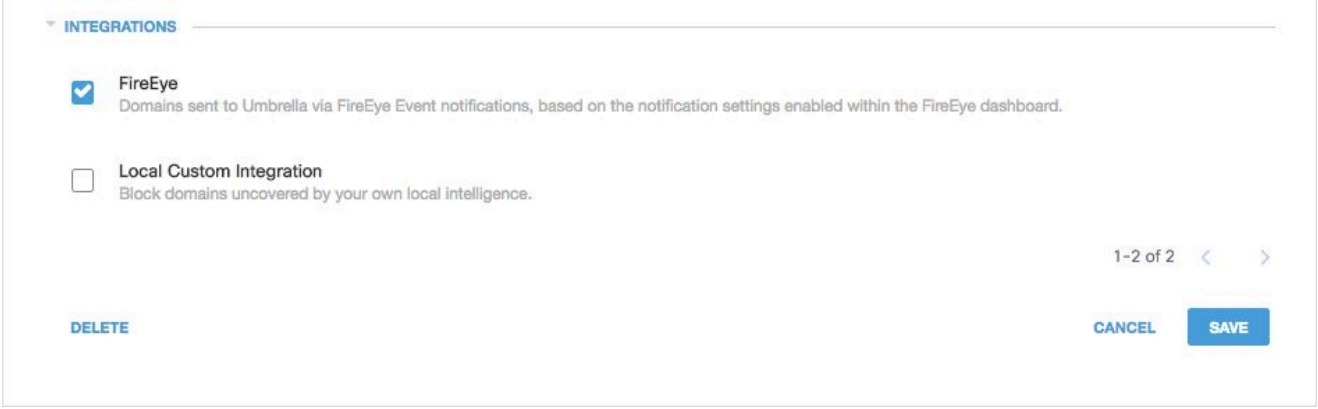
可選步驟：列出或刪除域

您可能還希望進行測試以確保在自定義整合中列出域，並在您不想對該域強制實施或不再將其包含在整合中時刪除域。使用API文檔中概述的步驟來列出和刪除域。

配置安全設定

現在，您已驗證可以插入事件（並可選擇列出和刪除域），您可以從您的身份中配置要傳送到自定義整合安全類別中的域的DNS請求要執行的操作。

1. 導覽至Policies > Security Settings，然後在Integrations下檢查啟用的整合（在本例中為FireEye），然後按一下Save。

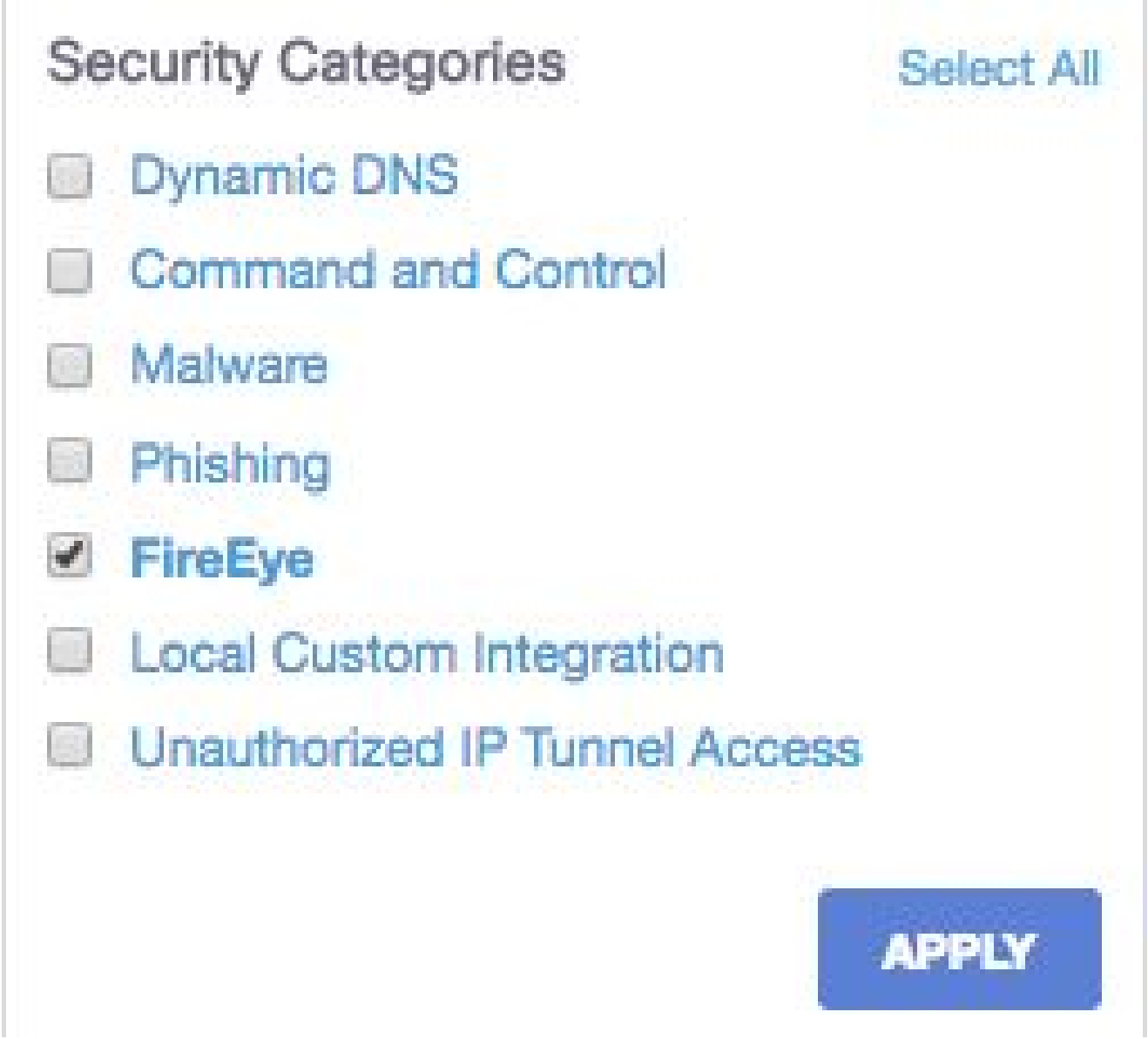


115014145103

檢視自定義整合的報告

從您的某個身份（例如，網路或漫遊電腦）生成發往自定義整合中的域（在我們的示例中為「creditcards.com」）的DNS請求。 從客戶端的角度來看，您現在會看到相應的塊或允許結果，具體取決於您如何配置安全設定。

1. 導覽至Reporting > Activity Search，然後在Security Categories下選擇自定義整合（在此示例中為FireEye），以篩選報表，使其僅顯示FireEye的安全類別。

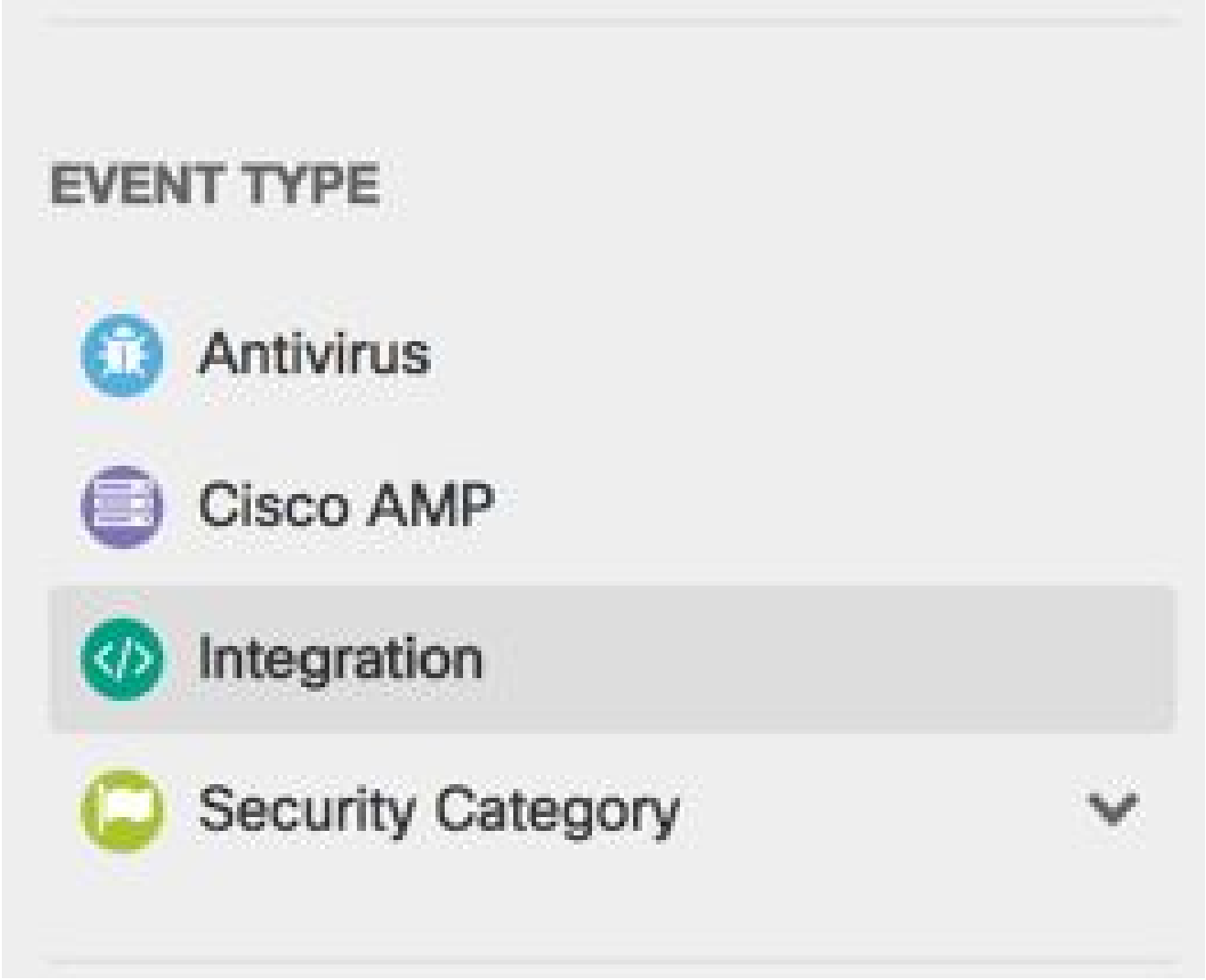


115013981706

2. 按一下Apply以檢視報告中選定時間段的活動。

您還可以檢視「活動卷」報告以檢視快照或隨時間變化的趨勢計數報告，包括自定義整合。

1. 導航到報告>安全活動卷。
2. 在Event Type下，選擇Integration。



115013982286

為日誌儲存和消耗配置S3整合（可選）

如果您想將包含您環境的所有請求的Umbrella日誌反饋到SIEM/TIP環境中，可以使用我們的S3整合來完成此操作，這樣您就可以將DNS活動事件流式處理回來。

附錄:示例指令碼

這些perl指令碼提供有關如何為自定義整合生成事件的指導。請在兩個指令碼中替換整合的customerKey值。請注意，這些指令碼作為示例提供，可能需要自定義或更新。

generate_event.pl:

```
#!/usr/bin/perl -w

# Custom integration - ADD EVENT URL
```

```
my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl:

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

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）。