將SecureX威脅響應源配置為阻止Firepower上的URL

目錄

簡介

本文檔介紹如何根據在威脅響應調查期間發現的URL和IP建立威脅情報，以供Firepower使用。

背景資訊

思科威脅響應是一個強大的工具，能夠利用來自多個模組的資訊調查整個環境中的威脅。每個模組都提供由Firepower、安全終端、Umbrella和其他第三方供應商等安全產品生成的資訊。這些調查不僅有助於揭示系統中是否存在威脅，而且有助於生成重要的威脅情報，這些情報可以源回安全產品以增強環境中的安全性。

SecureX Threat Response使用的一些重要術語：

- **Indicator**是與AND和OR運算子邏輯相關的可觀察量的集合。 有結合多種可觀察量的複雜指標，也有僅由一種可觀察量構成的簡單指標。
- **可**觀察是一個變數，可以是IP、域、URL或sha256。
- **判斷**由使用者建立，並用於將可觀察資料與特定時間段內的處置聯絡起來。
- **建立**源是為了將SecureX威脅響應調查生成的威脅情報與其他安全產品（如防火牆和電子郵件內容過濾器，如Firepower和ESA）共用。

必要條件

需求

思科建議您瞭解以下主題：

- SecureX CTR(思科威脅響應。

- Firepower TID(Threat Intelligence Director)。
- Firepower訪問控制策略配置。

本文檔使用Firepower TID強制實施在SecureX威脅響應上生成的威脅情報。對於FMC 7.3版，在FMC部署中使用TID的要求如下：

- 版本6.2.2或更高版本。
- 配置至少15 GB的記憶體。
- 已配置啟用REST API訪問。請參閱《Cisco Secure Firewall Management Center管理指南》中的「啟用REST API訪問」。
- 如果裝置在6.2.2版或更高版本上，則可以使用FTD作為threat intelligence director元素。

注意：本文檔認為Threat Intelligence Director已在系統上處於活動狀態。有關TID初始配置和故障排除的更多資訊，請檢查「相關資訊」部分中提供的連結。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- SecureX思科威脅響應控制面板
- FMC（防火牆管理中心）版本7.3
- FTD（防火牆威脅回應）版本7.2

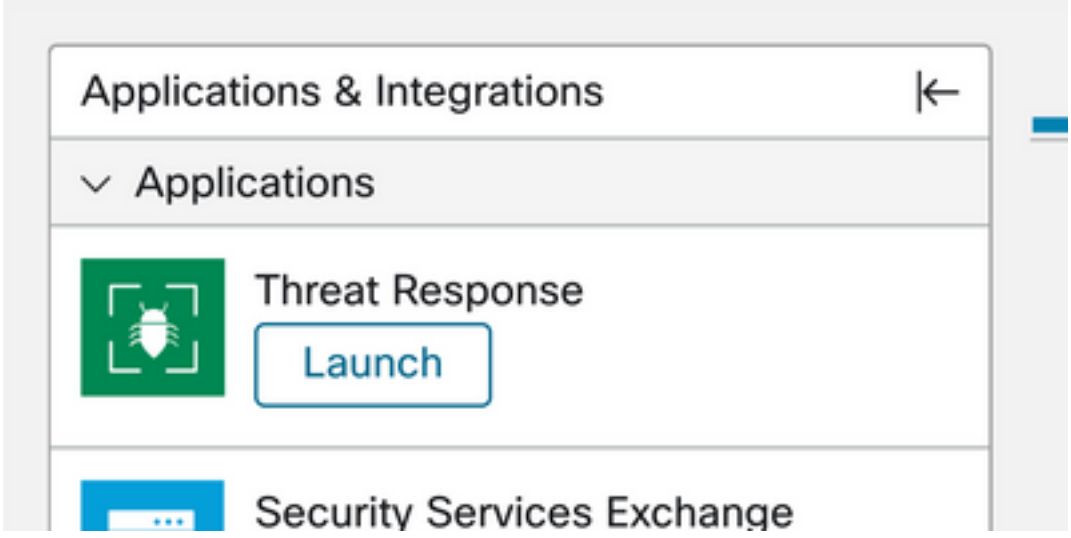
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

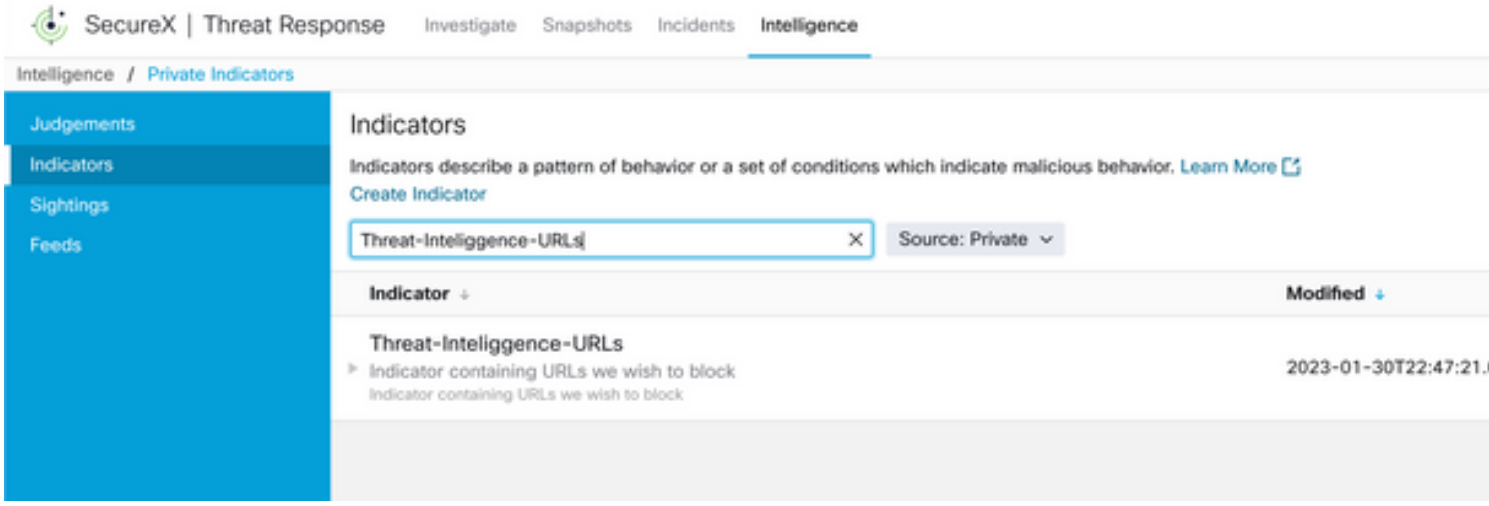
建立SecureX威脅響應源

SecureX Threat Response允許以可觀察到的輸入內容開始對環境進行調查。威脅響應引擎查詢模組以搜尋與可觀察對象相關的任何活動。調查將返回模組發現的任何匹配項，此資訊可能包括IP、域、Url電子郵件或檔案。接下來的步驟是建立源，以使用其他安全產品來使用資訊。

步驟1登入到SecureX控制面板，然後點選**Threat** Response Module的Launch按鈕。這將在新視窗中開啟「威脅響應」頁面：

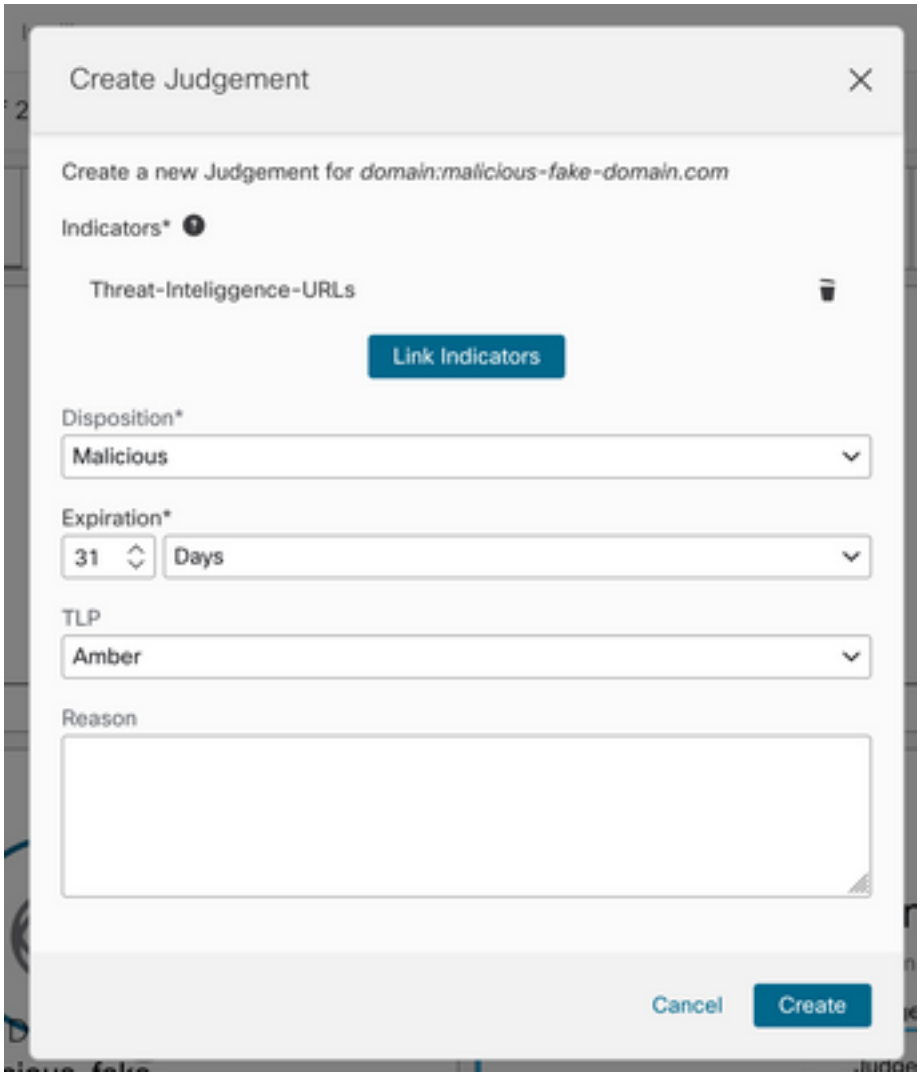


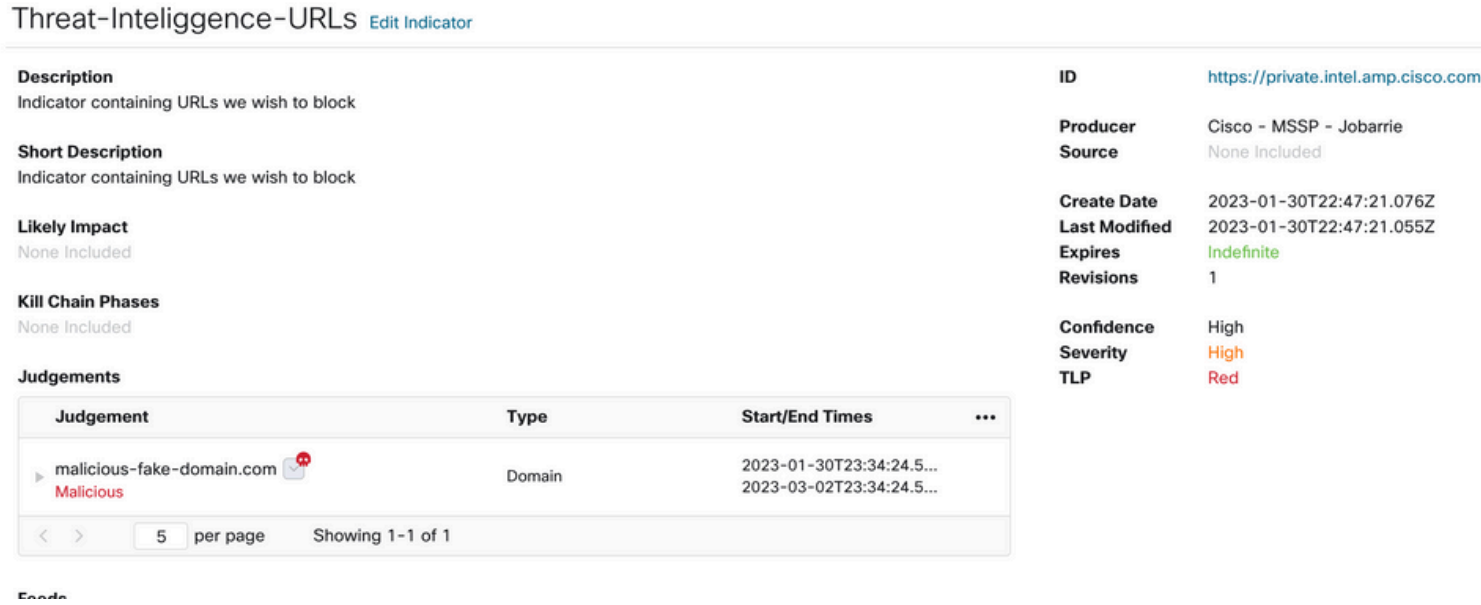
第2步在Threat Response頁面中，按一下Intelligence > Indicators，然後將Source下拉選單從Public更改為Private。這必須允許您按一下「建立指示器」連結。進入「指示器建立者」嚮導後，為您的指示器選擇任何有意義的標題和說明，然後選中「URL監視清單」覈取方塊。此時您可以儲存指示器，無需其他資訊，但是您可以選擇配置其餘的可用選項。



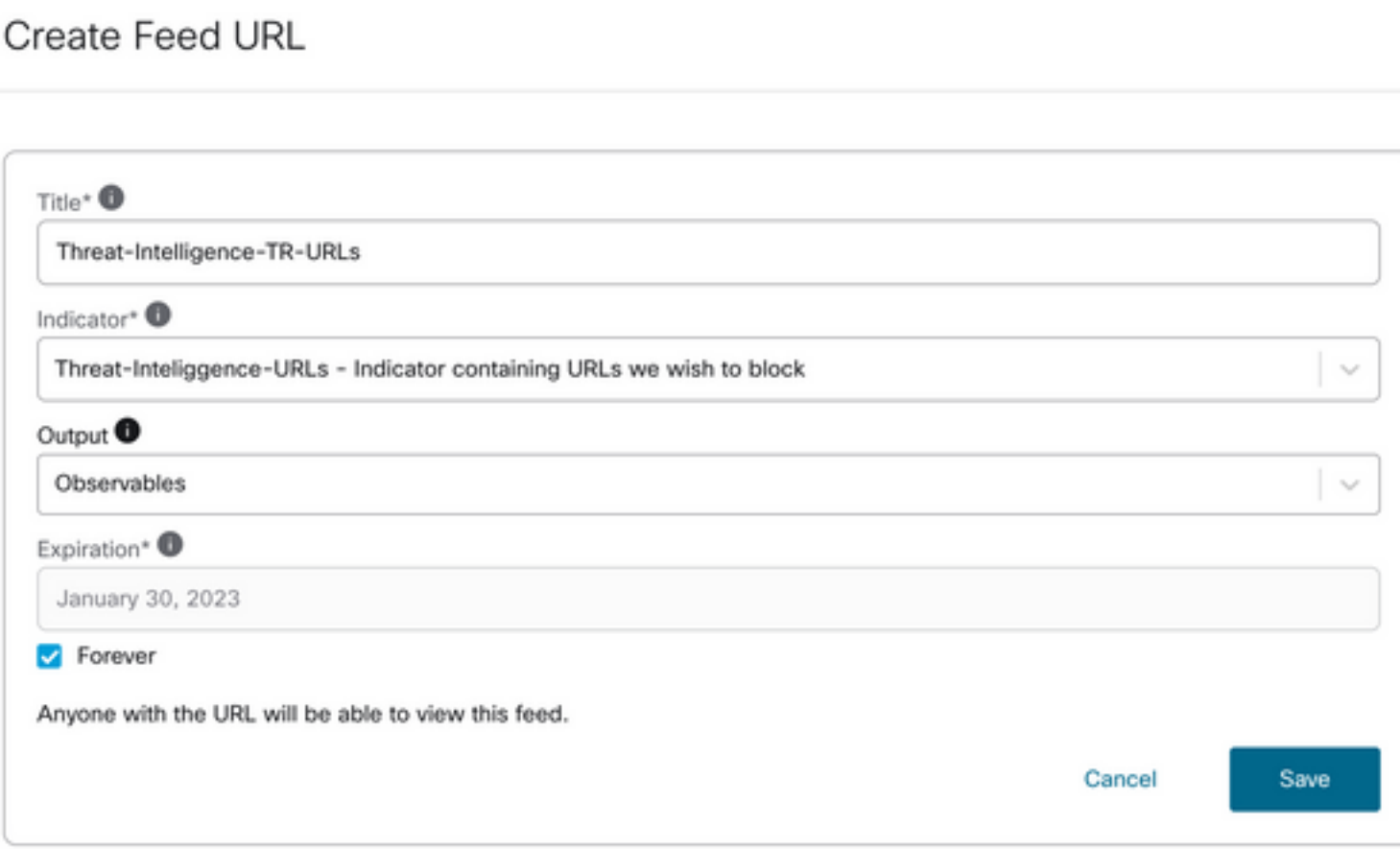
步驟3導覽至**Investigate**索引標籤，並將您要調查的任何可觀察專案貼到調查方塊中。為了說明目的，虛假URL https://malicious-fake-domain.com 用於此配置示例。按一下**Investigate**並等待調查完成。如預期的那樣，虛擬URL處置未知。繼續右鍵點選**下箭頭**以展開上下文選單，然後點選**建立判斷**。

步驟4按一下**Link Indicators**，然後從步驟2中選擇指標。將處置選擇為**Malicious**，然後根據您的認為適當選擇「到期日」。最後按一下**Create**按鈕。現在，URL必須在**Intelligence > Indicators > View Full Indicator**下可見。

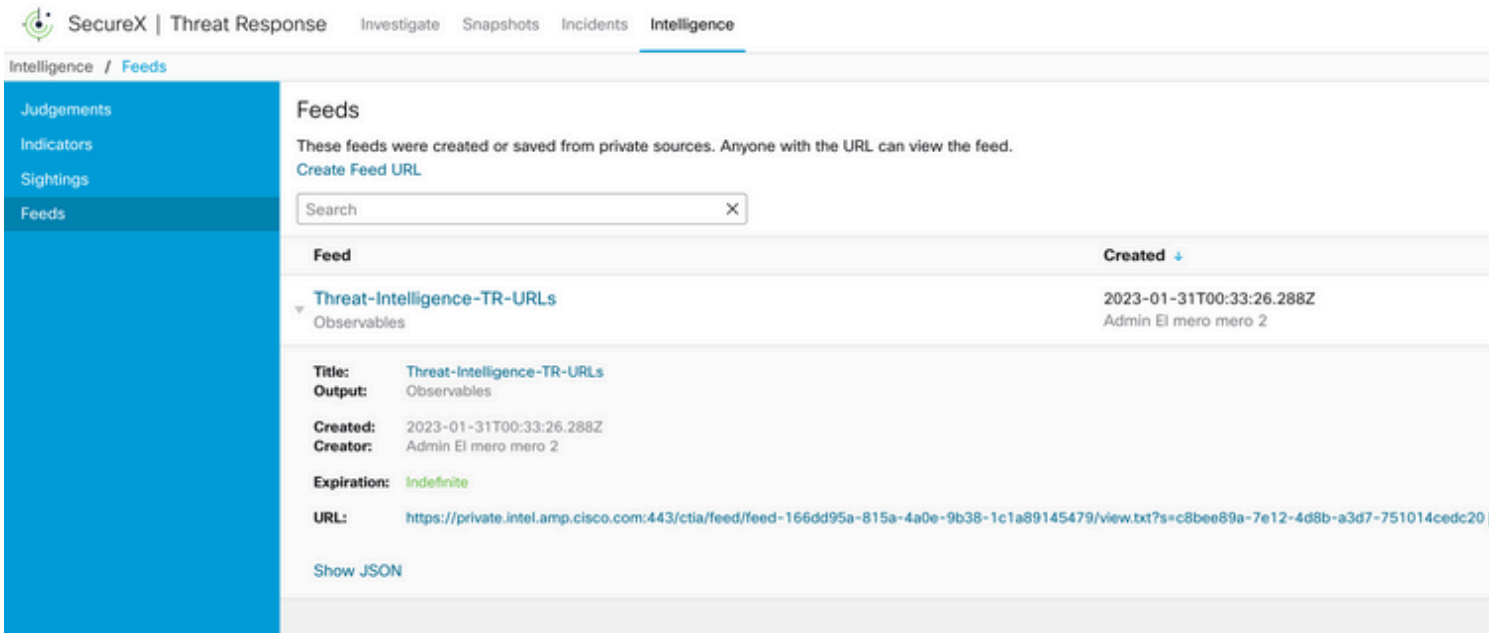




步驟5導覽至**Intelligence > Feeds，然後按一下Create Feed URL。** 填寫**Title**欄位，然後選擇步驟2中建立的**Indicator**。確保將「輸出」(**Output**)下拉選單保留為**觀察值**，然後按一下「儲存」(**Save**)。



第6步驗證在**Intelligence > Feeds**下建立了源，然後按一下**展開源詳細資訊。**按一下**URL**可直觀顯示源中列出了預期的URL。



配置FMC Threat Intelligence Director使用威脅響應源

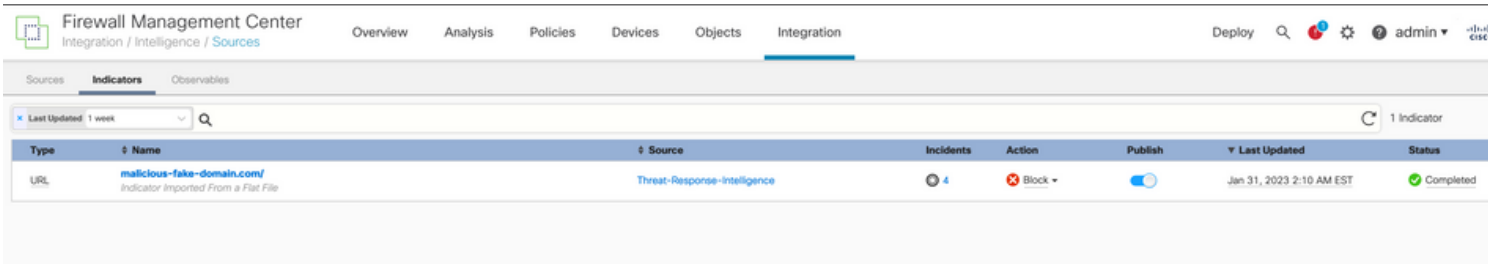
第1步登入您的FMC控制面板並導航至**Integration > Intelligence > Sources。** **單擊plus歎號新增新源。**

步驟2使用以下設定建立新來源：

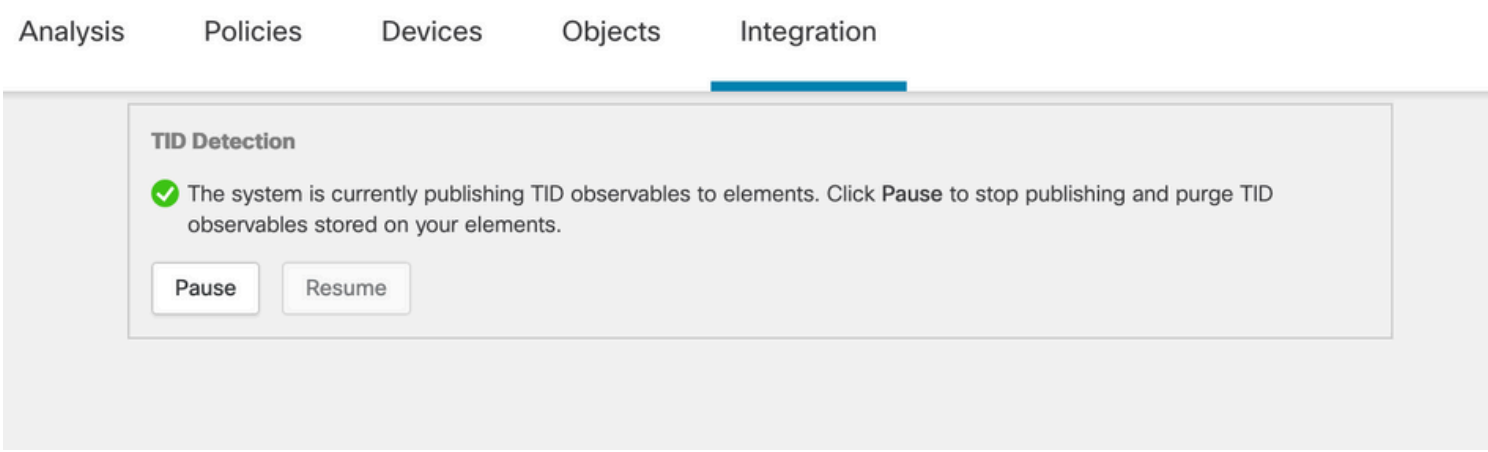
- 交付>選擇URL
- 「文字」(Type)>「選取平面檔案」(Select Flat File)
- 內容>選擇URL
- Url >貼上「Create SecureX Threat Response Feed」部分的URL步驟5。
- 「名稱」(Name)>選擇您認為合適的任何名稱
- Action > Select Block
- 更新間隔>選擇30分鐘（用於威脅情報源的快速更新）

按一下「**Save**」。

步驟3在Indicators and Substitutes verify domain下列出：

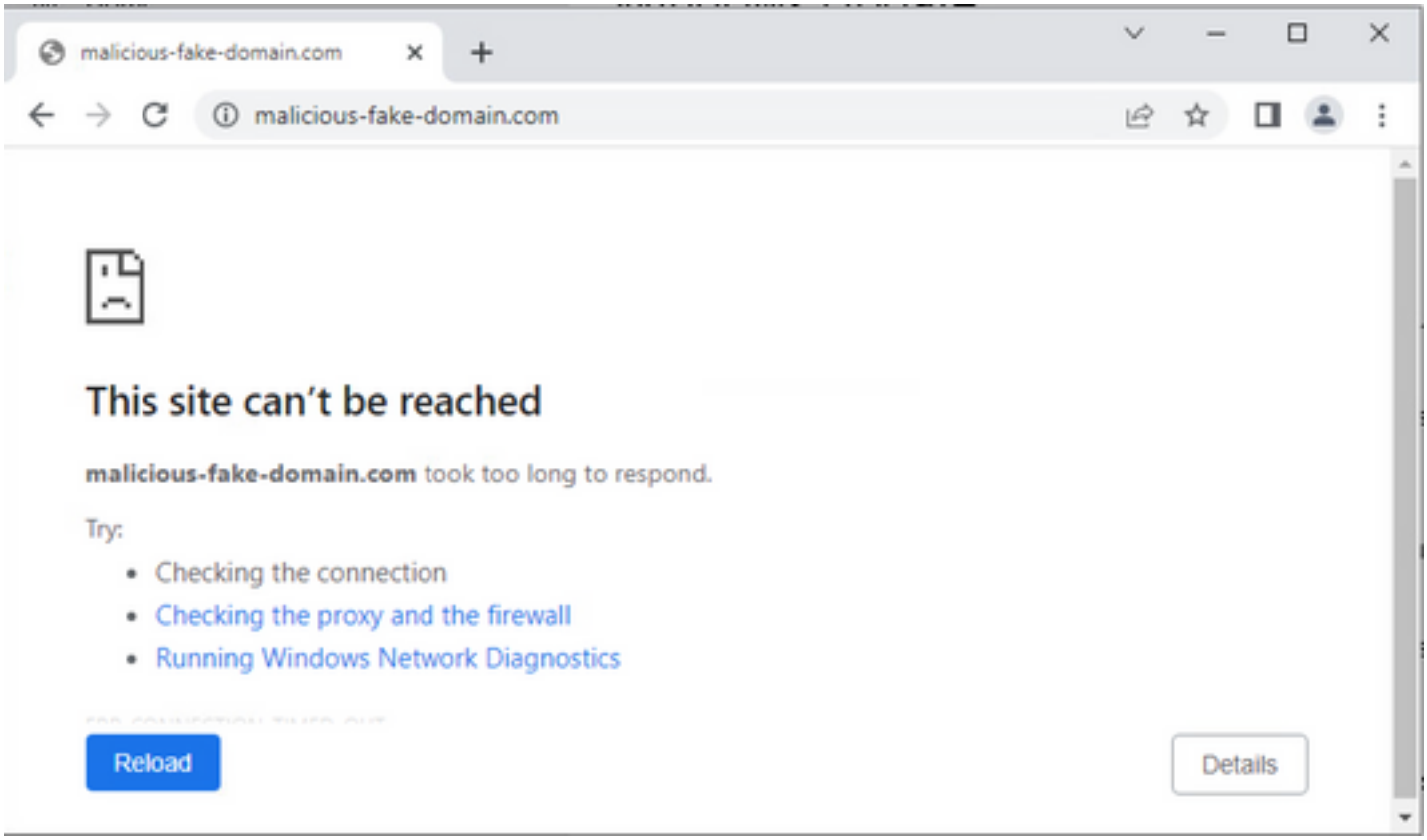


步驟4確保Threat Intelligence Director處於活動狀態並保持元素處於最新狀態（FTDs裝置）。導覽至**Integrations > Intelligence > Elements**:

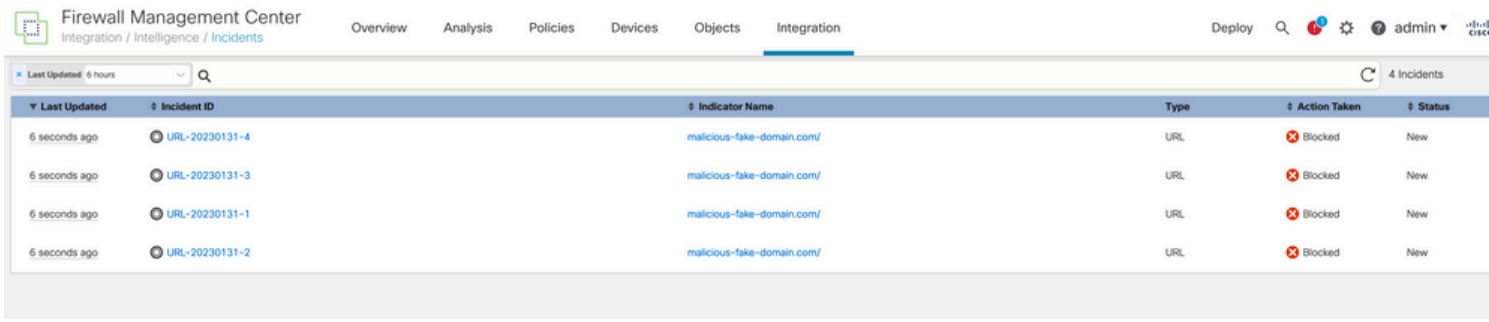


驗證

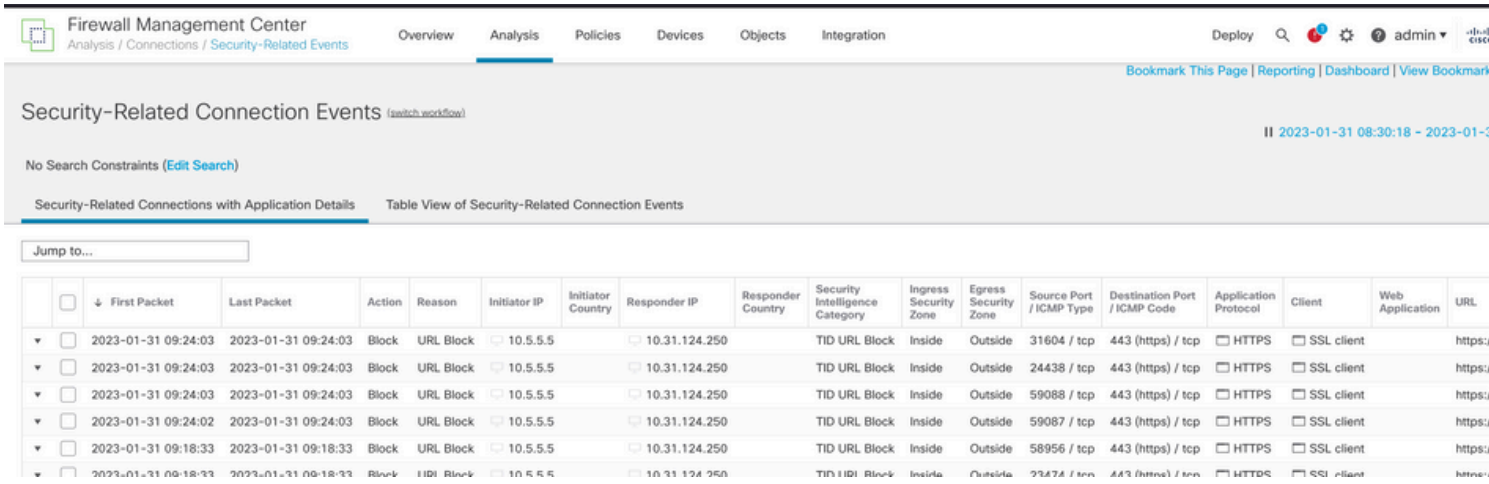
配置完成後，終結點嘗試連線到外部區域上託管的https://malicious-fake-domain[.]com URL，但連線會按預期失敗。



要驗證連線失敗是否是由於Threat Intelligence源，請導航到Integrations > Intelligence > Incidents。被阻止的事件必須列在此頁面上。



您可以在Analysis > Connections > Security-Related Events下驗證這些塊事件：



FTD LINA擷取允許透過多重檢查檢視從端點到惡意URL的流量。 請注意，由於Threat Intelligence功能使用Snort引擎進行高級流量檢測，因此Snort引擎第6階段檢查將返回丟棄結果。請

注意，Snort引擎需要允許第一組資料包，以便分析和瞭解連線的性質，從而正確觸發檢測。 檢查相關資訊區段，瞭解有關FTD LINA擷取的詳細資訊。

```
7: 18:28:46.965449 0050.56b3.fd77 0050.56b3.de22 0x0800 Length: 571
10.5.5.5.63666 > 10.31.124.250.443: P [tcp sum ok] 2993282128:2993282645(517) ack 2622728404 win
1024 (DF) (ttl 128, id 2336)
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 1926 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x14745cf3b800, priority=13, domain=capture, deny=false
hits=553, user_data=0x14745cf4b800, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=Inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 1926 ns
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x14745c5c5c80, priority=1, domain=permit, deny=false
hits=7098895, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=Inside, output_ifc=any

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 3852 ns
Config:
Additional Information:
Found flow with id 67047, using existing flow
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
```

```
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 31244 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 655704 ns
Config:
Additional Information:
service: HTTPS(1122), client: SSL client(1296), payload: (0), misc: (0)

Phase: 6
Type: SNORT
Subtype: SI-URL
Result: DROP
Elapsed time: 119238 ns
Config:
URL list id 1074790412
Additional Information:
Matched url malicious-fake-domain.com, action Block


Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
Action: drop
Time Taken: 813890 ns
Drop-reason: (si) Blocked or blacklisted by the SI preprocessor, Drop-location: frame
0x000056171ff3c0b0 flow (NA)/NA
```

疑難排解

- 要確保「威脅響應」使用正確資訊使訂閱源保持最新，您可以在瀏覽器上導航到訂閱源URL並檢視共用的可觀察量。

- 要排除FMC Threat Intelligence Director故障，請檢視「相關資訊」上的連結。

相關資訊

- 配置Cisco Threat Intelligence Director並排除故障
- 在FMC 7.3上配置安全防火牆威脅情報導向器
- 使用Firepower威脅防禦捕獲和Packet Tracer

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）。