

Configuración de fuentes de respuesta ante amenazas SecureX para bloquear URL en Firepower

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Crear fuente de respuesta a amenazas de SecureX](#)

[Configurar FMC Threat Intelligence Director para que consuma la fuente de respuesta ante amenazas](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo crear inteligencia de amenazas a partir de URL e IP encontradas durante las investigaciones de Threat Response que serán consumidas por Firepower.

Antecedentes

Cisco Threat Response es una potente herramienta capaz de investigar amenazas en todo el entorno gracias a la información de varios módulos. Cada módulo proporciona la información generada por los productos de seguridad, como Firepower, Secure Endpoint, Umbrella y otros proveedores externos. Estas investigaciones no solo pueden ayudar a revelar si existe una amenaza en el sistema, sino que también ayudan a generar una importante inteligencia de amenazas, que se puede obtener del producto de seguridad para mejorar la seguridad en el entorno.

Algunos términos importantes que utiliza SecureX Threat Response:

- **Indicador** es una colección de observables que están lógicamente relacionados con los operadores AND y OR. Hay indicadores complejos que combinan múltiples observables, además hay indicadores simples que están hechos de un solo observable.
- **Observable** es una variable que puede ser una IP, un dominio, una URL o un sha256.
- **Los juicios** son creados por el usuario y utilizados para vincular un objeto observable con una disposición durante un período de tiempo específico.
- Las **fuentes** se crean para compartir la inteligencia de amenazas generada por la investigación de respuesta ante amenazas de SecureX con otros productos de seguridad,

como firewalls y filtros de contenido de correo electrónico, como Firepower y ESA.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SecureX CTR (Cisco Threat Response .
- TID de Firepower (Threat Intelligence Director).
- Configuración de políticas de control de acceso de Firepower.

Este documento utiliza Firepower TID para aplicar la inteligencia de amenazas generada en SecureX Threat Response. Los requisitos para utilizar TID en la implementación de FMC como para FMC versión 7.3 son:

- Versión 6.2.2 o posterior.
- configurado con un mínimo de 15 GB de memoria.
- configurado con el acceso API REST habilitado. Consulte Enable REST API Access en la Guía de administración de Cisco Secure Firewall Management Center .
- Puede utilizar FTD como elemento de director de inteligencia de amenazas si el dispositivo está en la versión 6.2.2 o superior.

Nota: en este documento se considera que Threat Intelligence Director ya está activo en el sistema. Para obtener más información sobre la configuración inicial de TID y la resolución de problemas, consulte los enlaces disponibles en la sección Información relacionada.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Panel de Cisco Threat Response de SecureX
- FMC (Firewall Management Center) versión 7.3
- FTD (Firewall Threat Response) versión 7.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

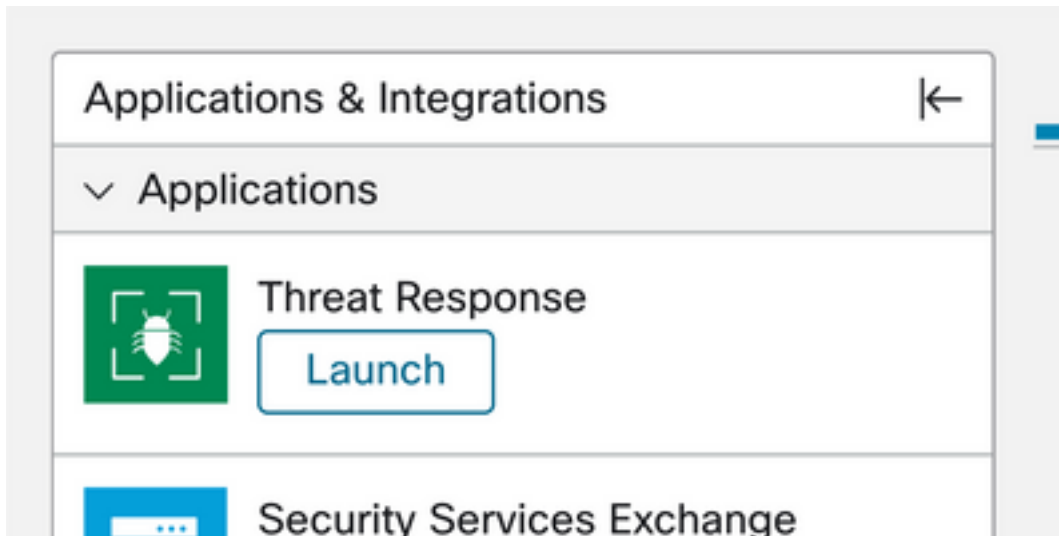
Configurar

Crear fuente de respuesta a amenazas de SecureX

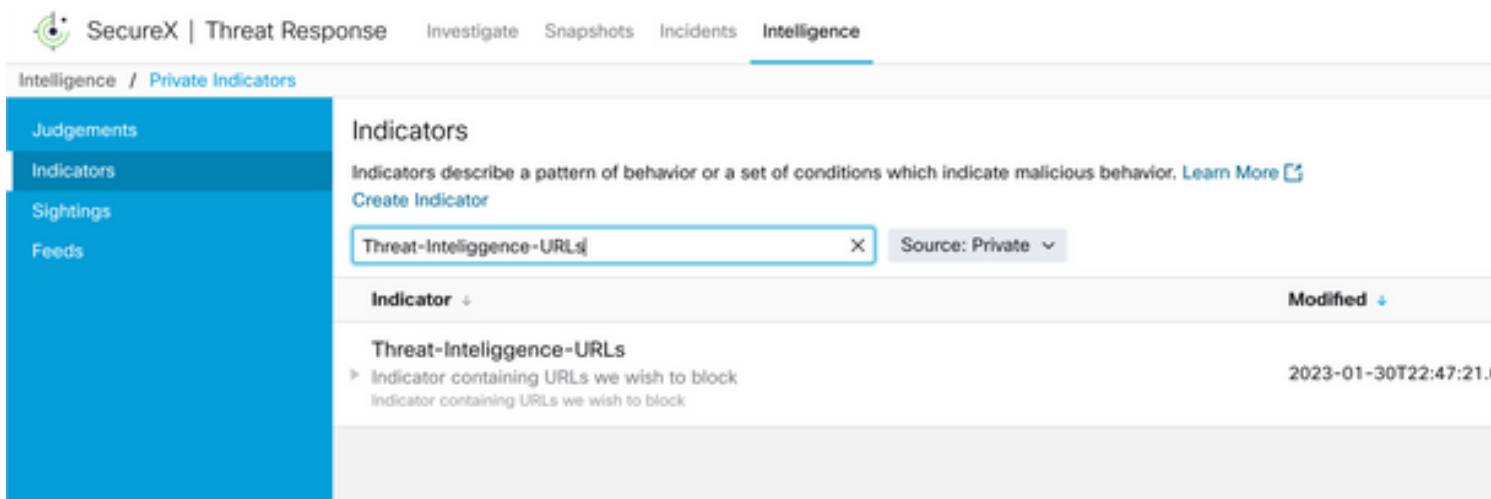
SecureX Threat Response permite iniciar una investigación sobre el entorno con un elemento observable como entrada. El motor de respuesta ante amenazas consulta los módulos para buscar cualquier actividad relacionada con lo observable. La investigación devuelve cualquier coincidencia encontrada por los módulos; esta información puede incluir direcciones IP, dominios, direcciones URL, correos electrónicos o archivos. En los siguientes pasos se crea una fuente para

consumir información con otros productos de seguridad.

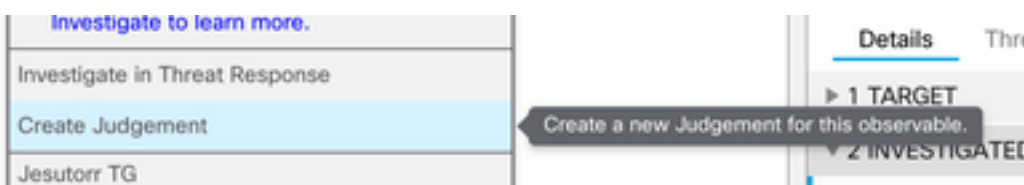
Paso 1 Inicie sesión en su panel de SecureX y haga clic en el botón **Iniciar** de Threat Response Module. Se abre la página Threat Response en una ventana nueva:



Paso 2 En la página Threat Response haga clic en Inteligencia > Indicadores y, a continuación, cambie la Lista desplegable Origen de Público a Privado. Debe permitirle hacer clic en el enlace Crear indicador. Una vez dentro del asistente de creación de indicadores elija cualquier título y descripción significativos para su indicador, después de eso marque la lista de seguimiento de URL casilla de verificación. En este momento puede guardar el indicador, no se necesita más información, sin embargo, puede optar por configurar el resto de las opciones disponibles.



Paso 3 Navegue hasta la pestaña **Investigar** y pegue cualquier elemento observable que desee investigar en el cuadro de investigación. Con fines demostrativos, la URL falsa <https://malicious-fake-domain.com> se utilizó para este ejemplo de configuración. Haga clic en **Investigar** y espere a que finalice la investigación. Como era de esperar, se desconoce la disposición de URL ficticia. Proceda a hacer clic con el botón derecho en la flecha **hacia abajo** para expandir el menú contextual y haga clic en **crear juicio**.



Paso 4 Haga clic en **Link Indicators** y seleccione el indicador del paso 2. Seleccione la disposición como **maliciosa** y elija el día de vencimiento que considere apropiado. Por último, haga clic en el botón **Create**. La URL debe estar ahora visible en **Inteligencia > Indicators > View Full Indicator**.

Create Judgement

Create a new Judgement for domain: *malicious-fake-domain.com*

Indicators*

Threat-Intelligence-URLs

[Link Indicators](#)

Disposition*

Expiration*

TLP

Reason

[Cancel](#) [Create](#)

Threat-Intelligence-URLs [Edit Indicator](#)

Description
Indicator containing URLs we wish to block

Short Description
Indicator containing URLs we wish to block

Likely Impact
None Included

Kill Chain Phases
None Included

Judgements

| Judgement | Type | Start/End Times | ... |
|--|--------|--|-----|
| malicious-fake-domain.com Malicious | Domain | 2023-01-30T23:34:24.5... 2023-03-02T23:34:24.5... | |

< > 5 per page Showing 1-1 of 1

ID <https://private.intel.amp.cisco.com>

Producer Source Cisco - MSSP - Jobarrie
None Included

Create Date 2023-01-30T22:47:21.076Z

Last Modified 2023-01-30T22:47:21.055Z

Expires Indefinite

Revisions 1

Confidence High

Severity High

TLP Red

Paso 5 Navegue hasta **Inteligencia > Fuentes** y haga clic en **Crear URL de fuente**. Rellene el campo **Título** y, a continuación, **seleccione** el **Indicador** creado en el paso 2. Asegúrese de dejar la lista desplegable **Salida** como **observables** y haga clic en **Guardar**.

Create Feed URL

Title* ⓘ
Threat-Intelligence-TR-URLs

Indicator* ⓘ
Threat-Intelligence-URLs - Indicator containing URLs we wish to block

Output ⓘ
Observables

Expiration* ⓘ
January 30, 2023

Forever

Anyone with the URL will be able to view this feed.

Cancel Save

Paso 6 Verifique que la fuente se haya creado en **Intelligence > Feeds** y, a continuación, haga clic para ampliar los detalles de la fuente. Haga clic en la **URL** para visualizar que las URL esperadas aparecen en la fuente.

SecureX | Threat Response Investigate Snapshots Incidents **Intelligence**

Intelligence / Feeds

Judgements
Indicators
Sightings
Feeds

Feeds

These feeds were created or saved from private sources. Anyone with the URL can view the feed.
Create Feed URL

Search

| Feed | Created |
|--|--|
| Threat-Intelligence-TR-URLs Observables | 2023-01-31T00:33:26.288Z Admin El mero mero 2 |

Title: Threat-Intelligence-TR-URLs
Output: Observables
Created: 2023-01-31T00:33:26.288Z
Creator: Admin El mero mero 2
Expiration: Indefinite
URL: <https://private.intel.amp.cisco.com:443/ctia/feed/feed-166dd95a-815a-4a0e-9b38-1c1a89145479/view.txt?s=c8bee89a-7e12-4d8b-a3d7-751014cedc20>

Show JSON

Configurar FMC Threat Intelligence Director para que consuma la fuente de respuesta ante amenazas

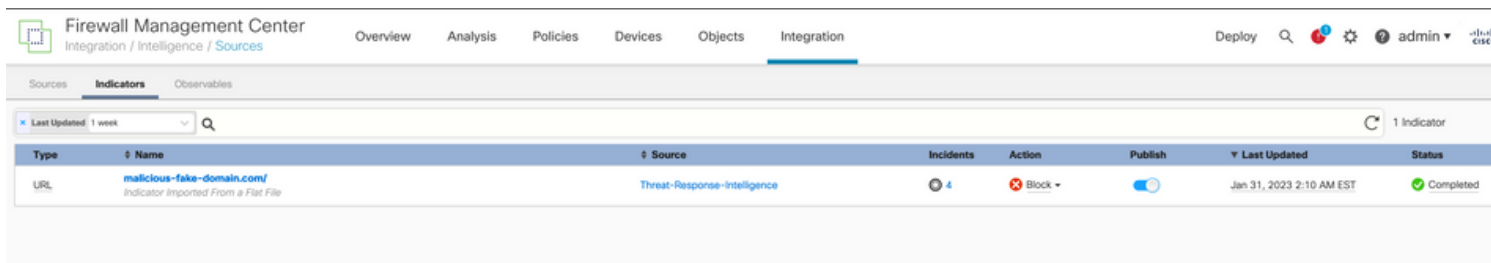
Paso 1 Inicie sesión en el panel de control de FMC y navegue hasta **Integración > Inteligencia > Fuentes**. Haga clic en el símbolo **más** para agregar un nuevo origen.

Paso 2 Cree el nuevo origen con esta configuración:

- Entrega > Seleccionar URL
- Texto > Seleccionar archivo sin formato
- Contenido > Seleccionar URL
- Url > Pegue la URL de la sección "Creación de una fuente de respuesta a amenazas SecureX", paso 5.
- Nombre > Elija el nombre que desee
- Acción > Seleccionar bloque
- Actualizar cada > Seleccionar 30 minutos (para actualizaciones rápidas de la fuente de inteligencia de amenazas)

Click **Save**.

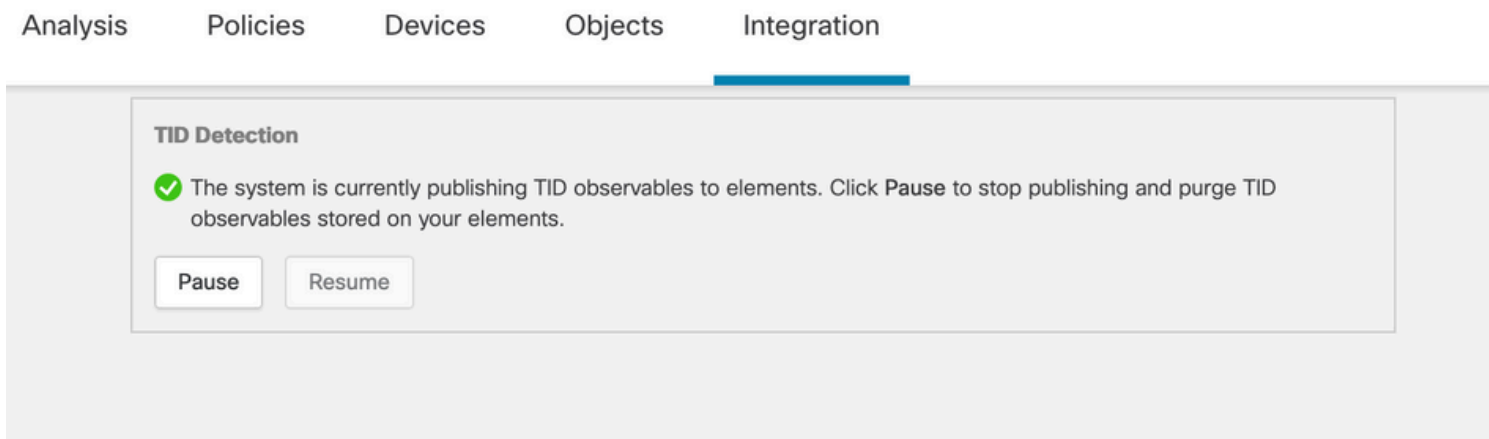
Paso 3 En Indicadores y Observables, verifique si el dominio se enumera:



The screenshot shows the 'Indicators' tab in the Firewall Management Center. A table lists one indicator with the following details:

| Type | Name | Source | Incidents | Action | Publish | Last Updated | Status |
|------|---|------------------------------|-----------|--------|-------------------------------------|--------------------------|-----------|
| URL | malicious-fake-domain.com <small>Indicator Imported From a Flat File</small> | Threat-Response-Intelligence | 4 | Block | <input checked="" type="checkbox"/> | Jan 31, 2023 2:10 AM EST | Completed |

Paso 4 Asegúrese de que Threat Intelligence Director está activo y mantiene los elementos actualizados (dispositivos FTD). Navegue hasta **Integraciones > Inteligencia > Elementos**:



The screenshot shows the 'TID Detection' status panel. It indicates that the system is currently publishing TID observables to elements. Below the status message are two buttons: 'Pause' and 'Resume'.

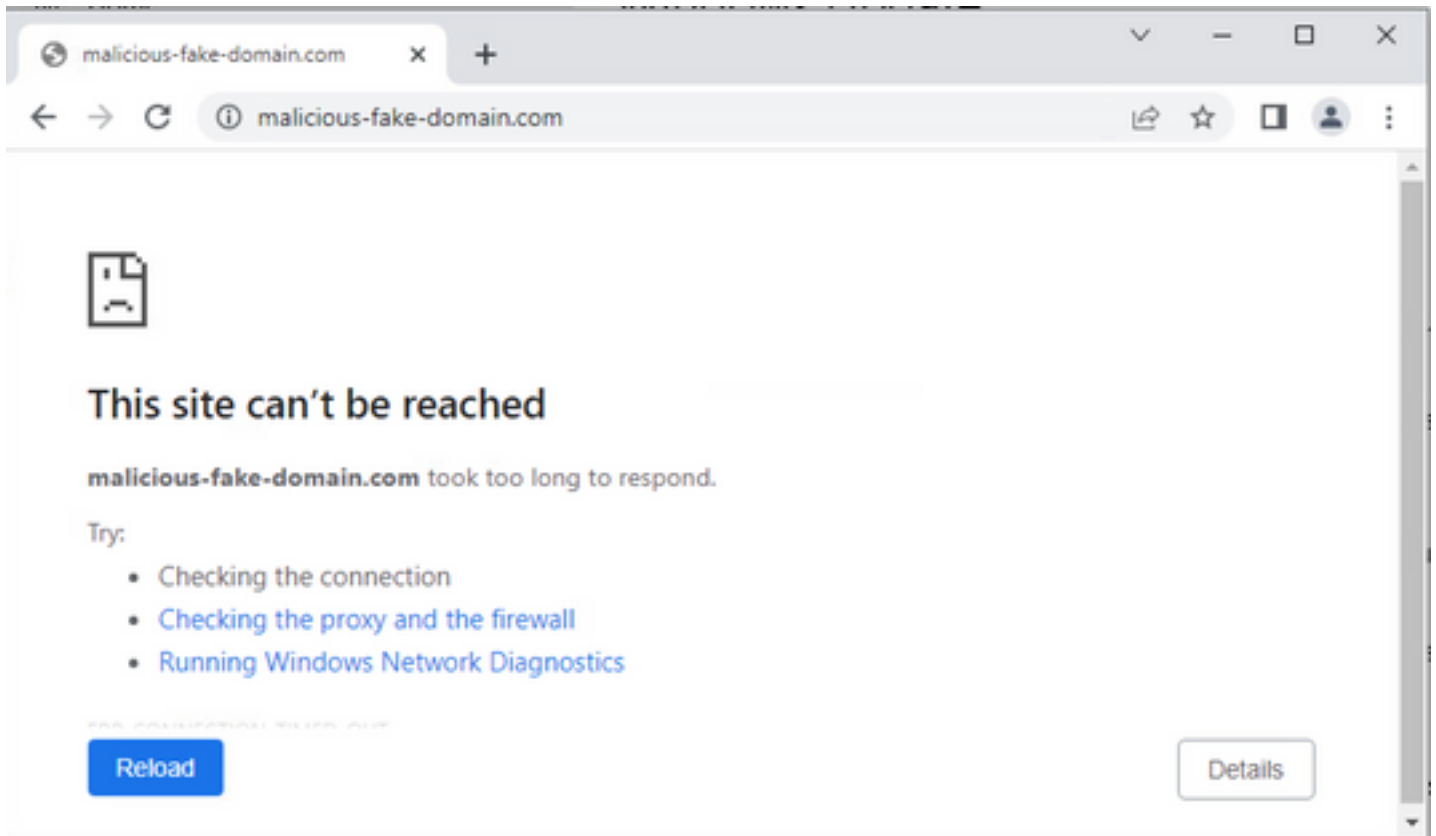
TID Detection

✓ The system is currently publishing TID observables to elements. Click Pause to stop publishing and purge TID observables stored on your elements.

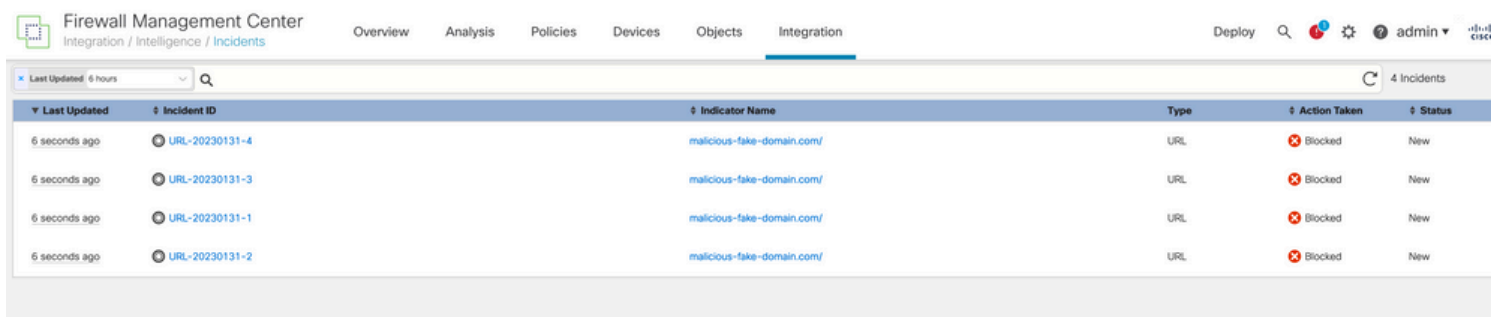
Pause Resume

Verificación

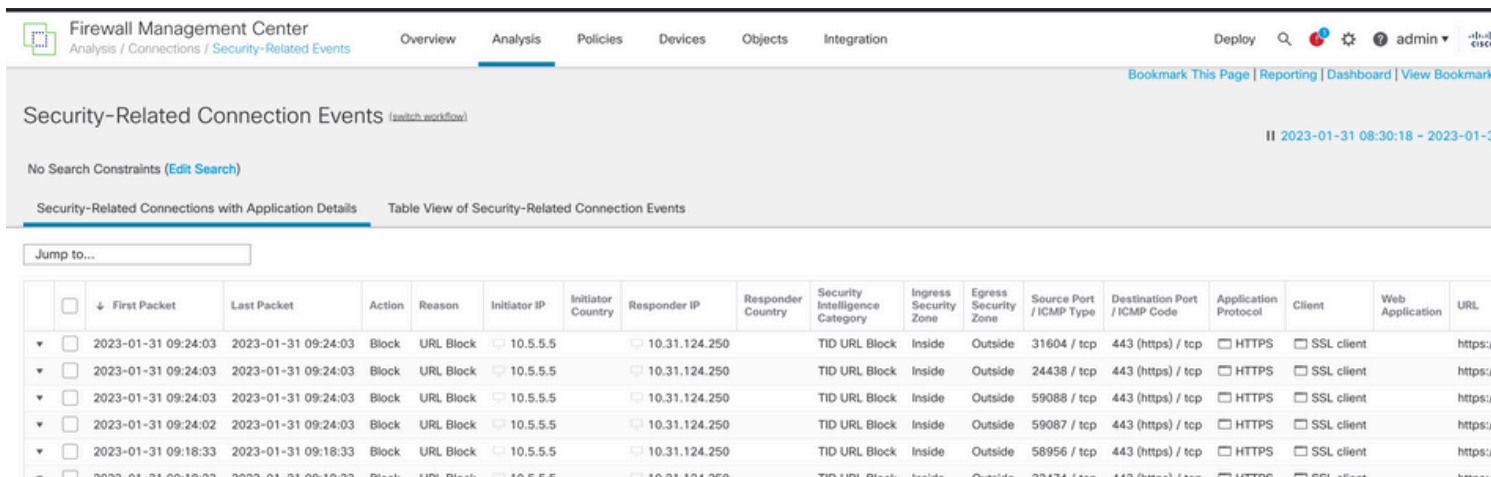
Una vez finalizada la configuración, el terminal intenta conectarse a la URL [https://malicious-fake-domain\[.\]com](https://malicious-fake-domain[.]com) alojada en la zona externa, pero las conexiones fallan según lo esperado.



Para comprobar si la falla de conexión se debe a la fuente de inteligencia de amenazas, navegue hasta Integraciones > Inteligencia > Incidentes. Los eventos bloqueados deben aparecer en esta página.



Puede verificar estos eventos de bloqueo en Análisis > Conexiones > Eventos relacionados con la seguridad:



Una captura LINA de FTD permite ver el tráfico desde el terminal a la URL maliciosa a través de varias comprobaciones. Tenga en cuenta que la comprobación de la fase 6 de Snort Engine devuelve un resultado de caída, ya que la función de inteligencia de amenazas utiliza el motor de Snort para la detección de tráfico avanzada. Tenga en cuenta que el motor Snort debe permitir que el primer par de paquetes para analizar y comprender la naturaleza de la conexión active correctamente una detección. Consulte la sección Información Relacionada para obtener más información sobre las capturas LINA de FTD.

```
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

Troubleshoot

- Para asegurarse de que Threat Response mantiene la fuente actualizada con la información correcta, puede navegar en su navegador a la URL de la fuente y ver los observables compartidos.



- Para solucionar problemas de FMC Threat Intelligence Director, consulte el enlace de Información relacionada.

Información Relacionada

- [Configuración y solución de problemas de Cisco Threat Intelligence Director](#)
- [Configuración de Secure Firewall Threat Intelligence Director en FMC 7.3](#)
- [Utilice capturas de Firepower Threat Defence y Packet Tracer](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).