

Configuración y resolución de problemas de Cisco Threat Intelligence Director

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[¿Cómo funciona?](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar y resolver problemas de Cisco Threat Intelligence Director (TID).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de Firepower Management Center (FMC)

Debe garantizar estas condiciones antes de configurar la función Cisco Threat Intelligence Director:

- Firepower Management Center (FMC): Debe ejecutarse en la versión 6.2.2 (o posterior) (puede alojarse en FMC físico o virtual). Debe configurarse con un mínimo de 15 GB de memoria RAM. Debe configurarse con acceso API REST habilitado.
- El sensor debe ejecutar la versión 6.2.2 (o posterior).
- En la ficha Advanced Settings (Parámetros avanzados) de la opción access control policy (Política de control de acceso), debe habilitarse **Enable Threat Intelligence Director**.
- Agregue reglas a la política de control de acceso si aún no están presentes.
- Si desea que los observables SHA-256 generen observaciones y eventos de Firepower Management Center, cree una o más reglas de archivo **Malware Cloud Lookup** o **Block Malware** y asocie la política de archivos con una o más reglas de la política de control de acceso.
- Si desea que las observaciones de IPv4, IPv6, URL o Nombre de dominio generen eventos

de inteligencia de seguridad y conexión, habilite el registro de la inteligencia de seguridad y conexión en la política de control de acceso.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Threat Defense (FTD) Virtual que ejecuta 6.2.2.81
- Firepower Management Center Virtual (vFMC), que ejecuta 6.2.2.81

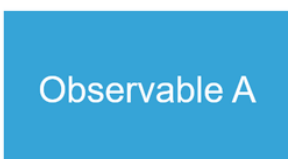
Nota: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

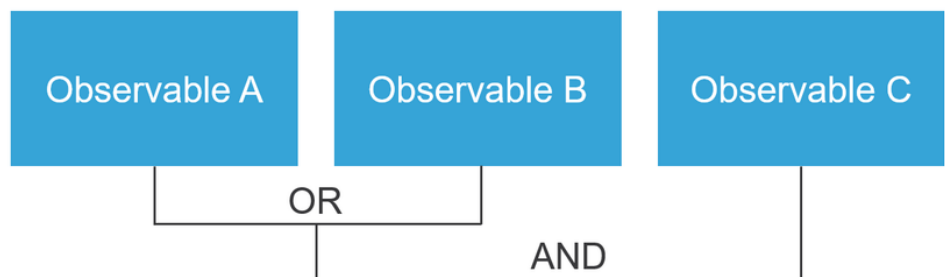
Cisco Threat Intelligence Director (TID) es un sistema que pone en funcionamiento la información de inteligencia de amenazas. El sistema consume y normaliza la inteligencia de ciberamenazas heterogénea de terceros, publica la inteligencia para las tecnologías de detección y correlaciona las observaciones de las tecnologías de detección.

Hay tres nuevos términos: **observables**, **indicadores** e **incidentes**. Observable es sólo una variable, puede ser por ejemplo URL, dominio, dirección IP o SHA256. Los indicadores se elaboran a partir de observables. Hay dos tipos de indicadores. Un indicador simple sólo contiene uno observable. En el caso de indicadores complejos, hay dos o más observables que se conectan entre sí usando funciones lógicas como AND y OR. Una vez que el sistema detecta el tráfico que debe bloquearse o monitorearse en el FMC, aparece el incidente.

Simple Indicator

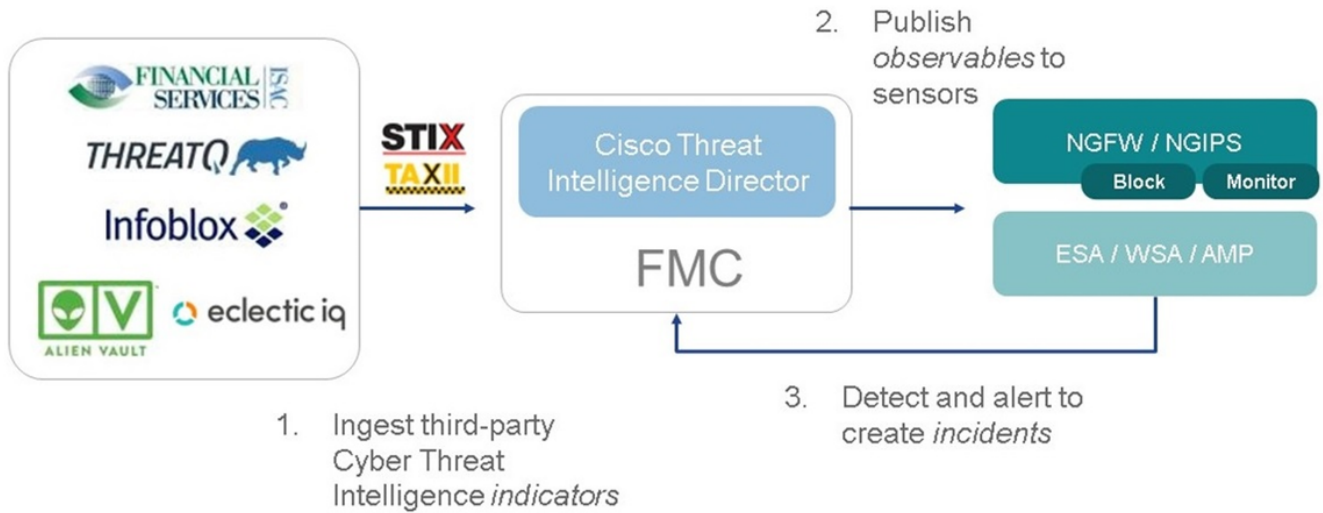


Complex indicator, two operators



¿Cómo funciona?

Como se muestra en la imagen, en el FMC debe configurar los orígenes desde los que desea descargar información de inteligencia de amenazas. Luego, el FMC envía esa información (observables) a los sensores. Cuando el tráfico coincide con los observables, los incidentes aparecen en la interfaz de usuario (GUI) de FMC.



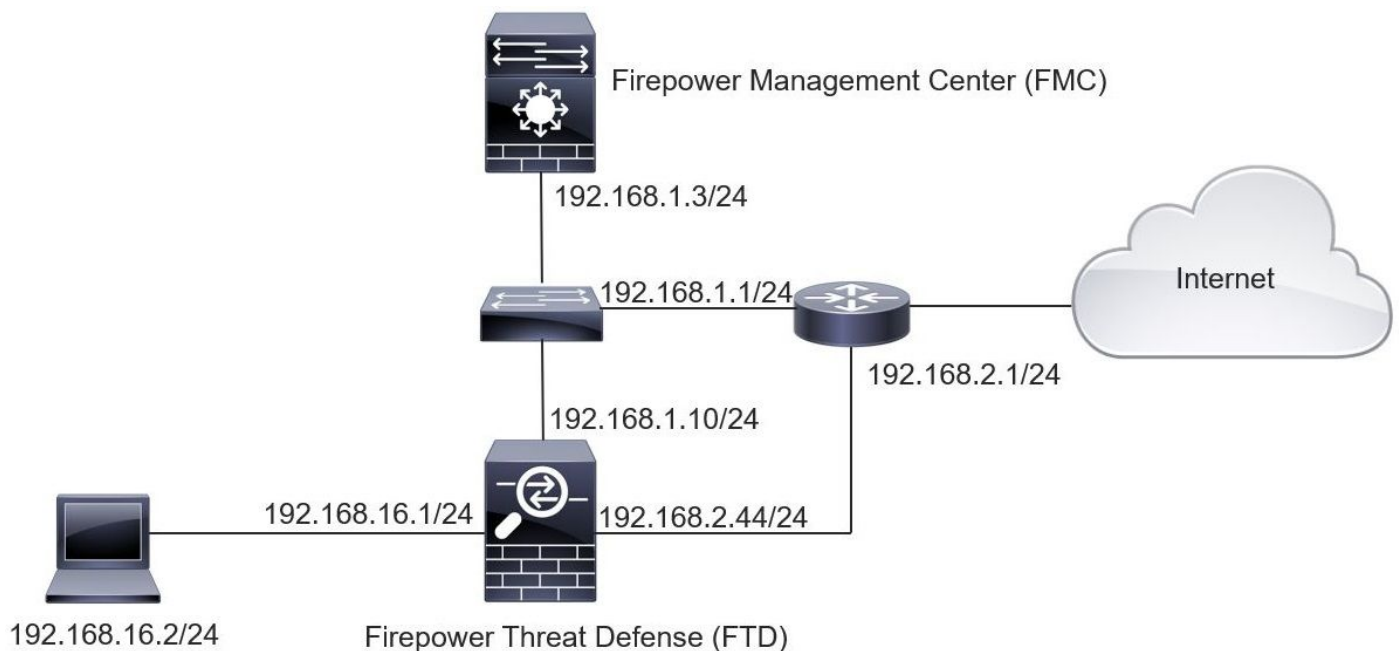
Hay dos nuevos términos:

- STIX (Intelligent Threat Intelligence eXpression estructurado) es un estándar para compartir y utilizar información de inteligencia de amenazas. Hay tres elementos funcionales clave: Indicadores, observables e incidentes
- TAXII (Trusted Automated eXchange of Indicator Information) es un mecanismo de transporte para la información sobre amenazas

Configurar

Para completar la configuración, tenga en cuenta estas secciones:

Diagrama de la red



Configuración

Paso 1. Para configurar TID, debe navegar a la pestaña **Intelligence**, como se muestra en la

imagen.

The screenshot shows the Cisco AMP Intelligence interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Intelligence' section is active, and the 'Sources' tab is selected. Below the navigation, there are tabs for 'Sources', 'Indicators', and 'Observables'. A search bar is present with a refresh icon and '4 Sources' displayed. The main content area is a table with the following columns: Name, Type, Delivery, Action, Publish, Last Updated, and Status. The table lists four sources: 'guest.Abuse_ch' (STIX, TAXII, Monitor, 3 hours ago, Completed with Errors), 'guest.CyberCrime_Tracker' (STIX, TAXII, Monitor, 3 hours ago, Completed), 'user.AlienVault' (STIX, TAXII, Monitor, 4 hours ago, Completed with Errors), and 'test_flat_file' (IPv4 Flat File, Upload, Block, 3 days ago, Completed). The footer shows the last login information and the Cisco logo.

Name	Type	Delivery	Action	Publish	Last Updated	Status
guest.Abuse_ch <small>guest.Abuse_ch</small>	STIX	TAXII	Monitor	On	3 hours ago Pause Updates	Completed with Errors
guest.CyberCrime_Tracker <small>guest.CyberCrime_Tracker</small>	STIX	TAXII	Monitor	On	3 hours ago Pause Updates	Completed
user.AlienVault <small>Data Feed for user: AlienVault</small>	STIX	TAXII	Monitor	On	4 hours ago Pause Updates	Completed with Errors
test_flat_file <small>Test flat file</small>	IPv4 Flat File	Upload	Block	On	3 days ago	Completed

Nota: Se espera el estado "Completado con errores" en caso de que una fuente contenga una tabla de observación no admitida.

Paso 2. Debe agregar fuentes de amenazas. Existen tres formas de agregar orígenes:

- TAXII - Cuando utiliza esta opción, puede configurar un servidor donde la información sobre amenazas se almacena en formato STIX

Add Source ? ×

DELIVERY **TAXII** URL Upload

URL* SSL Settings ▾

USERNAME

PASSWORD

⚠ Credentials will be sent using an unsecured HTTP connection

FEEDS* × ▾

Note: A separate source will be added for each feed selected. The name will default to the name of the feed and can be edited later.

ACTION

UPDATE EVERY (MINUTES) Never Update

TTL (DAYS)

PUBLISH

Nota: La única acción disponible es Monitor. No puede configurar la acción de bloqueo para las amenazas en formato STIX.

- URL: puede configurar un enlace a un servidor local HTTP/HTTPS donde se encuentra la amenaza STIX o el archivo plano.

Add Source



DELIVERY TAXII **URL** Upload

TYPE STIX

URL*

SSL Settings

NAME*

DESCRIPTION

ACTION Monitor

UPDATE EVERY (MINUTES)

1440

Never Update

TTL (DAYS)

90

PUBLISH



Save

Cancel

- Archivo plano: puede cargar un archivo en formato *.txt y debe especificar el contenido del archivo. El archivo debe contener una entrada de contenido por línea.

Add Source ? X

DELIVERY

TYPE CONTENT

FILE*

Drag and drop or click

NAME*

DESCRIPTION

ACTION

TTL (DAYS)

PUBLISH

Nota: De forma predeterminada, se publican todas las fuentes, lo que significa que se las envía a los sensores. Este proceso puede tardar hasta 20 minutos o más.

Paso 3. En la ficha Indicador, puede confirmar si los indicadores se descargaron desde los orígenes configurados:

Intelligence							Deploy	System	Help	admin
Sources		Elements	Settings							
Sources		Indicators	Observables							
Type	Name	Source	Incidents	Action	Publish	Last Updated	Status			
IPv4	Feodo Tracker: This IP address has been identified as malicious... <small>This IP address 162.243.159.58 has been identified as malicious by ...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
IPv4	Feodo Tracker: This IP address has been identified as malicious... <small>This IP address 66.221.1.104 has been identified as malicious by fe...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
Complex	Zeus Tracker (online) elite.asia/yaweh/cidphp/file.php (201... <small>This domain elite.asia has been identified as malicious by zeustrack...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed with Errors			
Complex	Zeus Tracker (offline) l3d.pp.ru/global/config.jp (2017-08-... <small>This domain l3d.pp.ru has been identified as malicious by zeustrack...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
Complex	Zeus Tracker (offline) masoic.com.ng/images/bro/config.jp-... <small>This domain masoic.com.ng has been identified as malicious by zeu...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed with Errors			
IPv4	Feodo Tracker: This IP address has been identified as malicio... <small>This IP address 188.138.25.250 has been identified as malicious by ...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
IPv4	Feodo Tracker: This IP address has been identified as malicio... <small>This IP address 77.244.245.37 has been identified as malicious by f...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
Complex	Zeus Tracker (offline) lisovfoxcom.418.com1.ru/clock/cidph... <small>This domain lisovfoxcom.418.com1.ru has been identified as malici...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed with Errors			
IPv4	Feodo Tracker: This IP address has been identified as malicio... <small>This IP address 104.238.119.132 has been identified as malicious b...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
IPv4	Feodo Tracker: This IP address has been identified as malicio... <small>This IP address 185.18.76.146 has been identified as malicious by f...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
IPv4	Feodo Tracker: This IP address has been identified as malicio... <small>This IP address 68.168.210.95 has been identified as malicious by f...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			
IPv4	Feodo Tracker: This IP address has been identified as malicio... <small>This IP address 169.144.48.34 has been identified as malicious by f...</small>	guest.Abuse_ch		Monitor	<input type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed			

Paso 4. Una vez seleccionado el nombre de un indicador, podrá ver más detalles al respecto. Además, puede decidir si desea publicarlo en el sensor o si desea cambiar la acción (en el caso de un indicador simple).

Como se muestra en la imagen, un indicador complejo se enumera con dos observables conectados por el operador OR:

Indicator Details

NAME
Zeus Tracker (offline) | l3d.pp.ru/global/config.jp (2017-08-16) | This domain has been identified as malicious by zeustracker.abuse.ch

DESCRIPTION
This domain l3d.pp.ru has been identified as malicious by zeustracker.abuse.ch. For more detailed information about this indicator go to [CAUTION!!Read-URL-Before-Click] [https://zeustracker.abuse.ch/monitor.php?host=l3d.pp.ru].

SOURCE [guest.Abuse_ch](#)

EXPIRES Nov 27, 2017 7:16 PM CET

ACTION [Monitor](#)

PUBLISH

INDICATOR PATTERN

DOMAIN

`l3d.pp.ru`

OR

URL

`l3d.pp.ru/global/config.jp/`

[Download STIX](#) [Close](#)

Indicator Details

NAME
Feodo Tracker: | This IP address has been identified as malicious by feodotracker.abuse.ch

DESCRIPTION
This IP address [REDACTED] has been identified as malicious by feodotracker.abuse.ch. For more detailed information about this indicator go to [CAUTION!!Read-URL-Before-Click] [https://feodotracker.abuse.ch/host/[REDACTED]].

SOURCE [guest.Abuse_ch](#)

EXPIRES Nov 27, 2017 7:16 PM CET

ACTION [Monitor](#)

PUBLISH

INDICATOR PATTERN

IPV4

[REDACTED]

[Download STIX](#) [Close](#)

Paso 5. Vaya a la pestaña Observables en la que puede encontrar las URL, direcciones IP, dominios y SHA256 que se incluyen en los indicadores. Puede decidir qué elementos observables desea presionar a los sensores y, opcionalmente, cambiar la acción por ellos. En la última columna, hay un botón de lista blanca equivalente a una opción de publicación/no publicación.

Overview Analysis Policies Devices Objects AMP **Intelligence** Deploy System Help admin

Incidents Sources Elements Settings

Sources Indicators **Observables**

142 Observables

Type	Value	Indicators	Action	Publish	Updated At	Expires	
IPV4	[REDACTED]	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
IPV4	[REDACTED]	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	eite.asia	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
URL	eite.asia/yaweh/cidphp/file.php/	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	l3d.pp.ru	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
URL	l3d.pp.ru/global/config.jp/	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
URL	masoic.com.ng/images/bro/config.jpg/	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	masoic.com.ng	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
IPV4	[REDACTED]	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
IPV4	[REDACTED]	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	lisovfoxcom.418.com1.ru	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
URL	lisovfoxcom.418.com1.ru/clock/cidphp/file.php/	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	

Last login on Thursday, 2017-09-14 at 09:29:20 AM from dhcp-10-229-24-31.cisco.com

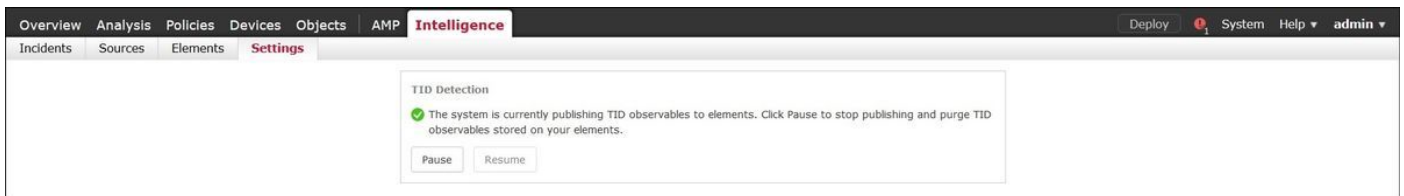
CISCO

Paso 6. Navegue a la pestaña Elementos para verificar la lista de dispositivos donde TID está habilitado.



Name	Element Type	Registered On	Access Control Policy
FTD_622	Cisco Firepower Threat Defense for VMWare	Sep 5, 2017 4:00 PM EDT	acp_policy

Paso 7 (opcional). Navegue hasta la ficha Settings (Parámetros) y seleccione el botón Pause (Pausa) para dejar de enviar indicadores a los sensores. Esta operación puede tardar hasta 20 minutos.

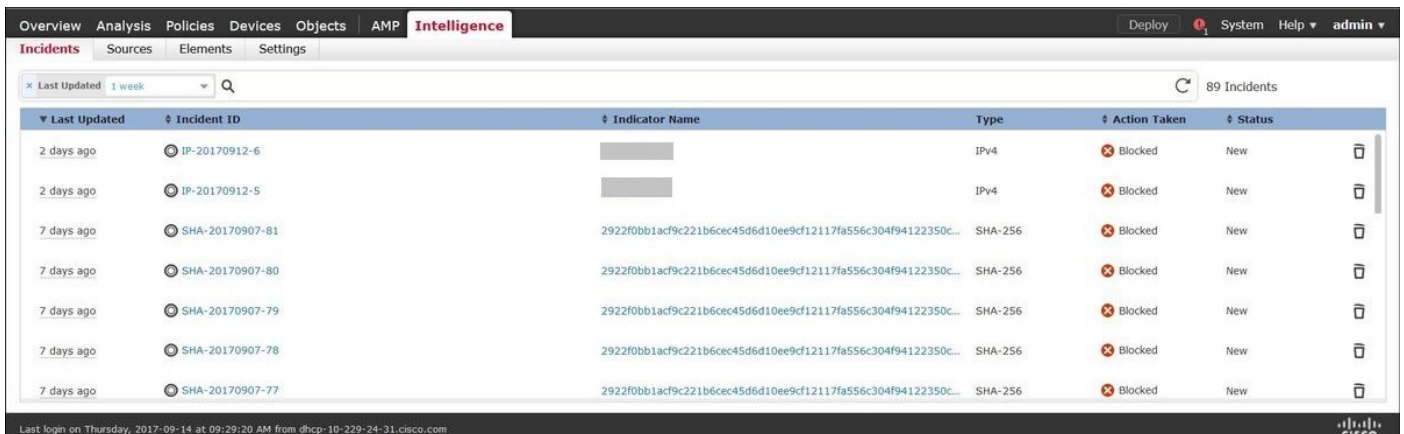


TID Detection

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

Verificación

Método 1. Para verificar si TID realizó una acción en el tráfico, debe navegar a la pestaña Incidentes.



Last Updated	Incident ID	Indicator Name	Type	Action Taken	Status
2 days ago	IP-20170912-6	[REDACTED]	IPv4	Blocked	New
2 days ago	IP-20170912-5	[REDACTED]	IPv4	Blocked	New
7 days ago	SHA-20170907-81	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-80	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-79	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-78	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-77	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New

Método 2. Los incidentes se pueden encontrar en la ficha Eventos de inteligencia de seguridad bajo una etiqueta TID.

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			57438 / udp	53 (domain) / udp
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			63873 / udp	53 (domain) / udp
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			60813 / udp	53 (domain) / udp
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			53451 / udp	53 (domain) / udp
2017-09-17 13:00:15		Block	IP Block	192.168.16.2	USA		USA	TID IPv4 Block			51974 / tcp	80 (http) / tcp
2017-09-17 12:59:54		Block	IP Block	192.168.16.2	USA		USA	TID IPv4 Block			51972 / tcp	80 (http) / tcp
2017-09-17 12:59:33		Block	IP Block	192.168.16.2	USA		USA	TID IPv4 Block			51970 / tcp	80 (http) / tcp

Nota: TID tiene una capacidad de almacenamiento de 1 millón de incidentes.

Método 3. Puede confirmar si hay fuentes configuradas (fuentes) en el FMC y un sensor. Para ello, puede navegar a estas ubicaciones en la CLI:

`/var/sf/siurl_download/`

`/var/sf/sidns_download/`

`/var/sf/iprep_download/`

Hay un nuevo directorio creado para las fuentes SHA256: `/var/sf/sifile_download/`.

```

root@ftd622:/var/sf/sifile_download# ls -l
total 32
-rw-r--r-- 1 root root 166 Sep 14 07:13 8ba2b2c4-9275-11e7-8368-f6cc0e401935.1f
-rw-r--r-- 1 root root 38 Sep 14 07:13 8ba40804-9275-11e7-8368-f6cc0e401935.1f
-rw-r--r-- 1 root root 16 Sep 14 07:13 IPRVersion.dat
-rw-rw-r-- 1 root root 1970 Sep 14 07:13 dm_file1.acl
-rw-rw-r-- 1 www www 167 Sep 14 07:13 file.rules
drwxr-xr-x 2 www www 4096 Sep 4 16:13 health
drwxr-xr-x 2 www www 4096 Sep 7 22:06 peers
drwxr-xr-x 2 www www 4096 Sep 14 07:13 tmp
root@ftd622:/var/sf/sifile_download# cat 8ba2b2c4-9275-11e7-8368-f6cc0e401935.1f
#Cisco TID feed:TID SHA-256 Block:1
7a00ef4b801b2b2acd09b5fc72d7c79d20094ded6360fb936bf2c65a1ff16907
2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c2bcdbdc

```

Nota: TID se habilita solamente en el Doiman global en el FMC

Nota: Si aloja TID en el Firepower Management Center activo en una configuración de alta disponibilidad (dispositivos físicos FMC), el sistema no sincroniza las configuraciones TID y los datos TID con el Firepower Management Center en espera.

Troubleshoot

Hay un proceso de nivel superior que se llama **tid**. Este proceso depende de tres procesos: **mongo**, **RabbitMQ**, **redis**. Para verificar los procesos ejecute **pmtool status | grep 'RabbitMQ|mongo|redis|tid' | grep " - "** comando.

```
root@fmc622:/Volume/home/admin# pmtool status | grep 'RabbitMQ|mongo|redis|tid' | grep " - "  
RabbitMQ (normal) - Running 4221  
mongo (system) - Running 4364  
redis (system) - Running 4365  
tid (normal) - Running 5128  
root@fmc622:/Volume/home/admin#
```

Para verificar en tiempo real qué acción se realiza, puede ejecutar el comando **system support firewall-engine-debug** o el comando **system support trace**.

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:  
Please specify a client IP address: 192.168.16.2  
Please specify a client port:  
Please specify a server IP address:  
Please specify a server port:  
Monitoring firewall engine debug messages  
...  
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1 URL SI: ShmDBLookupURL("http://www.example.com/")  
returned 1  
...  
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1 URL SI: Matched rule order 19, Id 19, si list id  
1074790455, action 4  
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1 deny action
```

Hay dos posibilidades de acción:

- **URL SI: Orden de regla coincidente 19, Id 19, id de lista si 1074790455, acción 4:** tráfico bloqueado
- **URL SI: Orden de regla coincidente 20, Id 20, ID de lista de si 1074790456, acción 6** - tráfico monitoreado.