

Konfiguration und Fehlerbehebung mit Cisco Threat Intelligence Director

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Wie funktioniert es?](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von Cisco Threat Intelligence Director (TID).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FirePOWER Management Center (FMC)-Administration

Sie müssen diese Bedingungen sicherstellen, bevor Sie die Funktion Cisco Threat Intelligence Director konfigurieren:

- FirePOWER Management Center (FMC): Muss auf Version 6.2.2 (oder höher) ausgeführt werden (kann auf einem physischen oder virtuellen FMC gehostet werden). Muss mit mindestens 15 GB RAM konfiguriert werden. Muss mit aktiviertem REST-API-Zugriff konfiguriert werden.
- Der Sensor muss die 6.2.2-Version (oder höher) ausführen.
- Auf der Registerkarte "Erweiterte Einstellungen" der Zugriffskontrollrichtlinie muss **Enable Threat Intelligence Director** aktiviert sein.
- Fügen Sie der Zugriffskontrollrichtlinie Regeln hinzu, wenn diese noch nicht vorhanden sind.
- Wenn SHA-256-Beobachtungen Beobachtungen und FirePOWER Management Center-Ereignisse generieren sollen, erstellen Sie eine oder mehrere **Malware Cloud Lookup** oder **Blockieren von Malware**-Dateiregeln und ordnen die Dateirichtlinie einer oder mehreren Regeln in der Zugriffskontrollrichtlinie zu.

- Wenn Sie IPv4-, IPv6-, URL- oder Domännennamen-Beobachtungen zum Generieren von Verbindungs- und Sicherheitsinformationen verwenden möchten, aktivieren Sie die Protokollierung von Verbindungs- und Sicherheitsinformationen in der Zugriffskontrollrichtlinie.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco FirePOWER Threat Defense (FTD) Virtual mit 6.2.2.81
- FirePOWER Management Center Virtual (vFMC) mit 6.2.2.81

Hinweis: Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

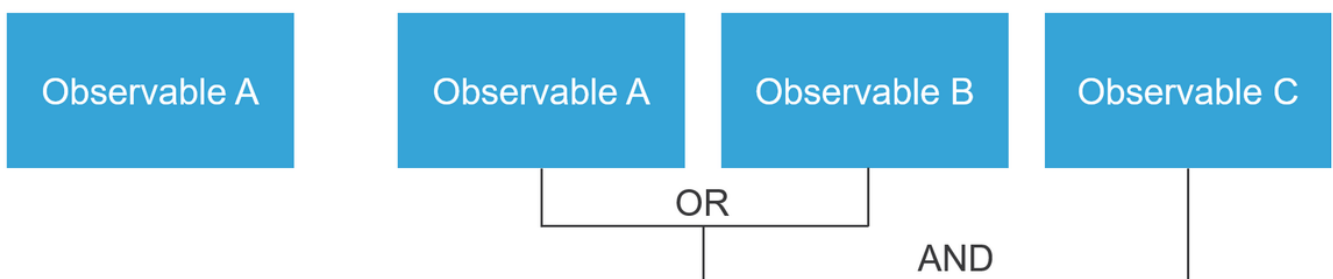
Hintergrundinformationen

Cisco Threat Intelligence Director (TID) ist ein System, das Bedrohungsinformationen operationalisiert. Das System nutzt und normalisiert heterogene Cyber-Threat-Intelligence von Drittanbietern, veröffentlicht diese Informationen für Erkennungstechnologien und korreliert die Beobachtungen aus den Erkennungstechnologien.

Es gibt drei neue Begriffe: **Beobachtungen**, **Indikatoren** und **Vorfälle**. Observable ist nur eine Variable, kann z. B. URL, Domäne, IP-Adresse oder SHA256. Indikatoren werden aus Beobachtungswerten erstellt. Es gibt zwei Arten von Indikatoren. Ein einfacher Indikator enthält nur einen beobachtbaren. Bei komplexen Indikatoren gibt es zwei oder mehr beobachtbare Indikatoren, die miteinander über logische Funktionen wie AND und OR verbunden sind. Sobald das System Datenverkehr erkennt, der im FMC blockiert oder überwacht werden soll, wird der Vorfall angezeigt.

Simple Indicator

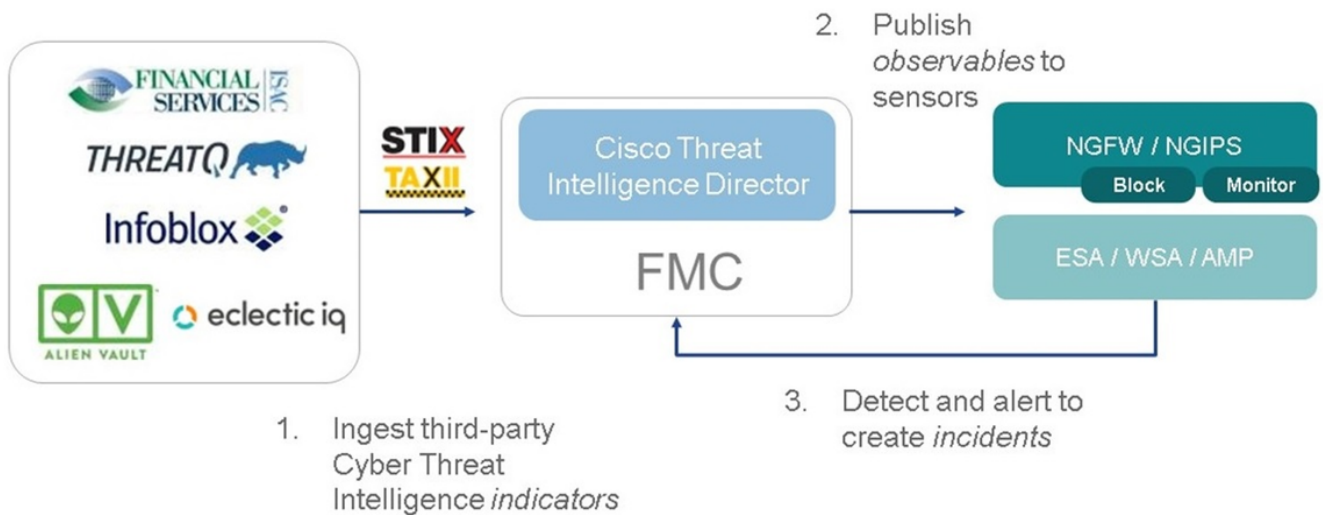
Complex indicator, two operators



Wie funktioniert es?

Wie im Bild gezeigt, müssen Sie auf dem FMC Quellen konfigurieren, von denen Sie Bedrohungsinformationen herunterladen möchten. Das FMC leitet diese Informationen

(Observables) dann an Sensoren weiter. Wenn der Datenverkehr mit den Observables übereinstimmt, werden die Incidents in der FMC-Benutzeroberfläche (GUI) angezeigt.



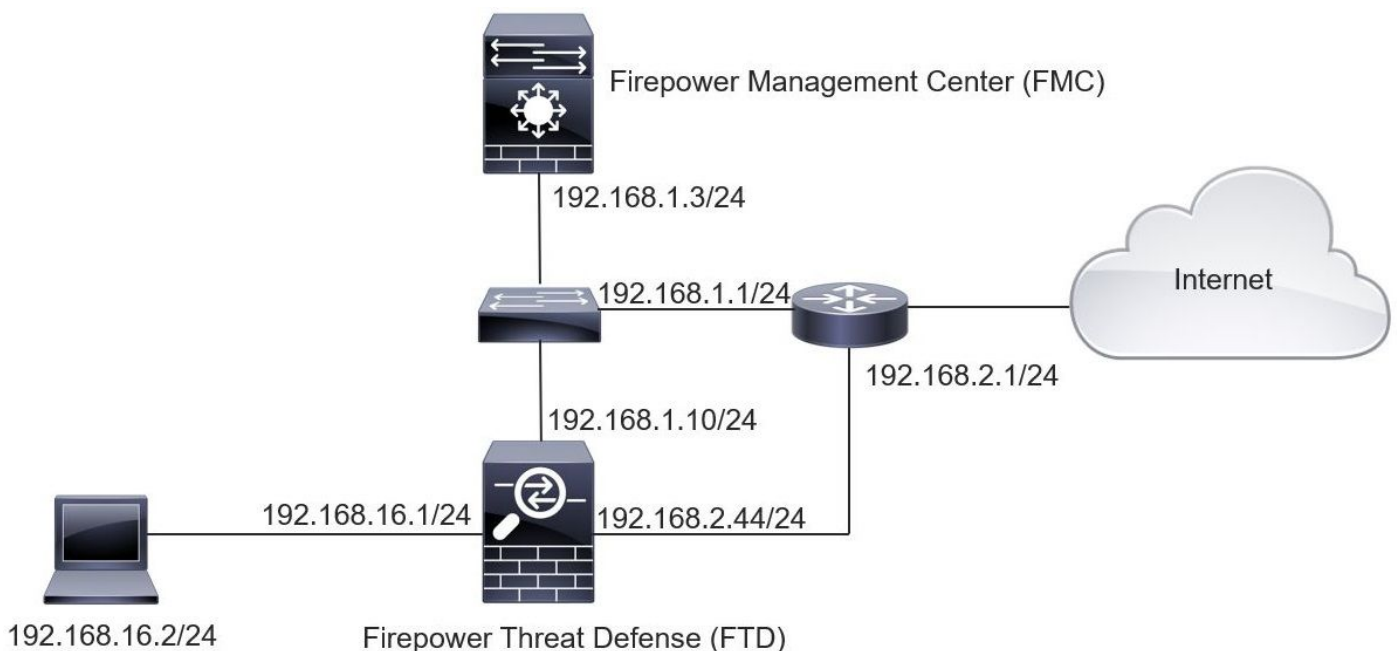
Es gibt zwei neue Begriffe:

- STIX (Structured Threat Intelligence eXpression) ist ein Standard für den Austausch und die Nutzung von Bedrohungsinformationen. Es gibt drei wichtige funktionale Elemente: Indikatoren, Observables und Incidents
- TAXII (Trusted Automated eXchange of Indicator Information) ist ein Übertragungsmechanismus für Bedrohungsinformationen

Konfigurieren

Um die Konfiguration abzuschließen, müssen folgende Abschnitte berücksichtigt werden:

Netzwerkdiagramm



Konfiguration

Schritt 1: Um TID zu konfigurieren, müssen Sie zur Registerkarte **Intelligence** navigieren, wie im Bild gezeigt.

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

Hinweis: Der Status 'Completed with Errors' (Wird mit Fehlern abgeschlossen) wird erwartet, wenn ein Feed nicht unterstützte Observables enthält.

Schritt 2: Sie müssen Bedrohungsquellen hinzufügen. Es gibt drei Möglichkeiten, Quellen hinzuzufügen:

- TAXII - Wenn Sie diese Option verwenden, können Sie einen Server konfigurieren, auf dem Bedrohungsinformationen im STIX-Format gespeichert sind.

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

Hinweis: Die einzige Aktion, die verfügbar ist, ist Monitor. Sie können die Blockaktion nicht für Bedrohungen im STIX-Format konfigurieren.

- URL: Sie können einen Link zu einem lokalen HTTP/HTTPS-Server konfigurieren, auf dem sich die STIX-Bedrohung oder eine Flatdatei befindet.

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

- Flachdatei: Sie können eine Datei im Format ***.txt** hochladen und müssen den Inhalt der Datei angeben. Die Datei muss pro Zeile einen Content-Eintrag enthalten.

Add Source ? X

DELIVERY TAXII URL Upload

TYPE Flat File ▼ CONTENT SHA-256 ▼

FILE* Drag and drop or click

NAME*

DESCRIPTION

ACTION ⊗ Block ▼

TTL (DAYS)

PUBLISH

Save Cancel

Hinweis: Standardmäßig werden alle Quellen veröffentlicht, d. h. sie werden an Sensoren übertragen. Dieser Vorgang kann bis zu 20 Minuten oder länger dauern.

Schritt 3: Auf der Registerkarte Indikator können Sie überprüfen, ob Indikatoren von den konfigurierten Quellen heruntergeladen wurden:

Intelligence								Deploy	System	Help	admin
Sources											
Indicators											
Last Updated: 1 week											
Type	Name	Source	Incidents	Action	Publish	Last Updated	Status				
IPv4	Feodo Tracker: This IP address has been identified as malicious by ... <small>This IP address 162.243.159.58 has been identified as malicious by ...</small>	guest.Abuse_ch	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				
IPv4	Feodo Tracker: This IP address has been identified as malicious by fe... <small>This IP address 66.221.1.104 has been identified as malicious by fe...</small>	guest.Abuse_ch	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed with Errors				
IPv4	Feodo Tracker: This IP address has been identified as malicious by ... <small>This IP address 188.138.25.250 has been identified as malicious by ...</small>	guest.Abuse_ch	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" 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	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				

Schritt 4: Sobald Sie den Namen einer Anzeige ausgewählt haben, werden weitere Details angezeigt. Zusätzlich können Sie entscheiden, ob Sie den Sensor veröffentlichen oder die Aktion ändern möchten (bei einer einfachen Anzeige).

Wie im Bild gezeigt, wird ein komplexer Indikator mit zwei Sternchen aufgelistet, die durch den OR-Operator verbunden sind:

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](#)

Schritt 5: Navigieren Sie zur Registerkarte Observables (Observables), auf der Sie URLs, IP-Adressen, Domänen und SHA256 finden, die in den Anzeigen enthalten sind. Sie können entscheiden, welche Beobachtungen Sie an die Sensoren senden möchten und optional die Aktion für sie ändern. In der letzten Spalte befindet sich eine Whitelist-Schaltfläche, die einer Veröffentlichungs-/Nicht-Veröffentlichungsoption entspricht.

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

Incidents Sources Elements Settings

Sources Indicators **Observables**

Q 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	<input type="checkbox"/>
IPv4	[REDACTED]	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	<input type="checkbox"/>
Domain	eite.asia	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	<input type="checkbox"/>
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	<input type="checkbox"/>
Domain	l3d.pp.ru	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	<input type="checkbox"/>
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	<input type="checkbox"/>
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	<input type="checkbox"/>
Domain	masoic.com.ng	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	<input type="checkbox"/>
IPv4	[REDACTED]	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	<input type="checkbox"/>
IPv4	[REDACTED]	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	<input type="checkbox"/>
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	<input type="checkbox"/>
URL	lisovfoxcom.418.com1.ru/dock/cidphp/file.php/	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	<input type="checkbox"/>

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

CISCO

Schritt 6: Navigieren Sie zur Registerkarte Elemente, um die Liste der Geräte zu überprüfen, auf denen TID aktiviert ist.

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

Schritt 7 (optional). Navigieren Sie zur Registerkarte Settings (Einstellungen), und wählen Sie die Schaltfläche Pause (Anhalten) aus, um zu verhindern, dass die Anzeigen auf die Sensoren gedrückt werden. Dieser Vorgang kann bis zu 20 Minuten dauern.

TID Detection

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

Überprüfen

Methode 1. Um zu überprüfen, ob TID eine Aktion für den Datenverkehr ausgeführt hat, müssen Sie zur Registerkarte "Vorfälle" navigieren.

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

Methode 2. Die Incidents sind unter dem TID-Tag auf der Registerkarte Security Intelligence Events (Sicherheitsinformationsereignisse) zu finden.

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

Hinweis: TID verfügt über eine Speicherkapazität von 1 Million Incidents.

Methode 3: Sie können überprüfen, ob konfigurierte Quellen (Feeds) auf dem FMC und einem Sensor vorhanden sind. Um dies zu tun, können Sie über die CLI zu folgenden Speicherorten navigieren:

`/var/sf/siurl_download/`

`/var/sf/sidns_download/`

`/var/sf/iprep_download/`

Es gibt ein neues Verzeichnis für SHA256-Feeds: `/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.lf
-rw-r--r-- 1 root root 38 Sep 14 07:13 8ba40804-9275-11e7-8368-f6cc0e401935.lf
-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.lf
#Cisco TID feed:TID SHA-256 Block:1
7a00ef4b801b2b2acd09b5fc72d7c79d20094ded6360fb936bf2c65a1ff16907
2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c2bcdbc
```

Hinweis: TID ist nur auf dem Global Doiman im FMC aktiviert.

Hinweis: Wenn Sie TID im aktiven FirePOWER Management Center in einer Hochverfügbarkeitskonfiguration (physische FMC-Appliances) hosten, synchronisiert das System keine TID-Konfigurationen und TID-Daten mit dem Standby FirePOWER Management Center.

Fehlerbehebung

Es gibt einen Prozess der obersten Ebene, der **tid** genannt wird. Dieser Prozess ist von drei Prozessen abhängig: **Mongo, RabbitMQ, Reds**. So überprüfen Sie den **Status** des **pmtool** auf Prozessen | **grep 'RabbitMQ\|mongo\|redis\|tid'** Befehl | **grep " - "**.

```
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#
```

Um in Echtzeit zu überprüfen, welche Aktionen ausgeführt werden, können Sie den Befehl **Firewall-Engine-debug** oder **Trace-Systemunterstützung** ausführen.

```
> 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
```

Es gibt zwei Handlungsmöglichkeiten:

- **URL SI: Übereinstimmende Regelreihenfolge 19, ID 19, si list-ID 1074790455, Aktion 4** - Datenverkehr wurde blockiert
- **URL SI: Übereinstimmende Regelreihenfolge 20, ID 20, si list-ID 1074790456, Aktion 6** - Datenverkehr wurde überwacht.