

Cisco Threat Intelligence Director configureren en oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Hoe werkt het?](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u Cisco Threat Intelligence Director (TID) moet configureren en probleemoplossing bieden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Management Center (FMC)-beheer

U moet deze voorwaarden verzekeren voordat u de functie Cisco Threat Intelligence Director configureren:

- FireSIGHT Management Center (FMC): Moet worden uitgevoerd op versie 6.2.2 (of hoger) (u kunt dit via een fysiek of virtueel VMC ontvangen). Moet worden geconfigureerd met minimaal 15 GB RAM-geheugen. Moet worden ingesteld met REST API-toegang ingeschakeld.
- De sensor moet versie 6.2.2 (of later) draaien.
- In het tabblad Geavanceerde instellingen van de optie Toegangsbeheer, moet **Threat Intelligence Director inschakelen** worden ingeschakeld.
- Voeg regels toe aan het toegangscontrolebeleid indien deze nog niet aanwezig zijn.
- Als u wilt dat SHA-256-observeermiddelen opmerkingen genereren en FireSIGHT Management Center-gebeurtenissen, een of meer **Malware Cloud**-regels maken of **Malware**-bestandsregels **blokkeren** en het bestandsbeleid koppelen aan een of meer regels in het toegangsbeheerbeleid.
- Als u wilt dat IPv4, IPv6, URL of de observaties van de Naam van het Domein om verbinding

en veiligheidsintelligentie gebeurtenissen te genereren, toelaat verbinding en veiligheidsinlichtingen in het toegangscontrolebeleid.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco Firepower Threat Defense (FTD) Virtual Edition voor 6.2.2.81
- Firepower Management Center Virtual (vFMC) die draait op 6.2.2.81

Opmerking: De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

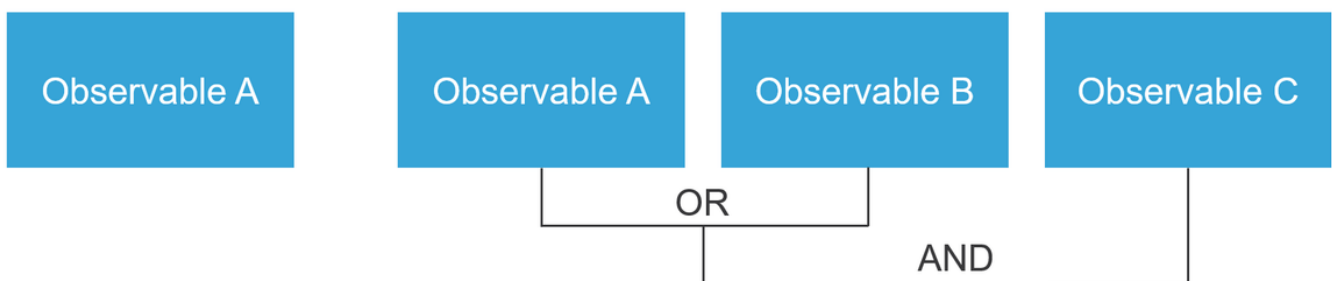
Achtergrondinformatie

Cisco Threat Intelligence Director (TID) is een systeem dat bedreigingsinformatie exploiteert. Het systeem consumeert en normaliseert heterogene derde partij cyber-dreigingsintelligentie, publiceert de intelligentie voor detectietechnologieën en correleert de waarnemingen van de detectietechnologieën.

Er zijn drie nieuwe termen: **observeert tabellen**, **indicatoren** en **incidenten**. Observable is slechts een variabele, kan bijvoorbeeld URL, domein, IP adres of SHA256 zijn. Indicatoren worden gemaakt van waarnemingen. Er zijn twee soorten indicatoren. Een simpele indicator bevat slechts één waarneembare. In het geval van complexe indicatoren zijn er twee of meer waarneembare indicatoren die met elkaar zijn verbonden met gebruikmaking van logische functies zoals AND en OR. Zodra het systeem verkeer detecteert dat blokkeert of controleert op het VMC, verschijnt het incident.

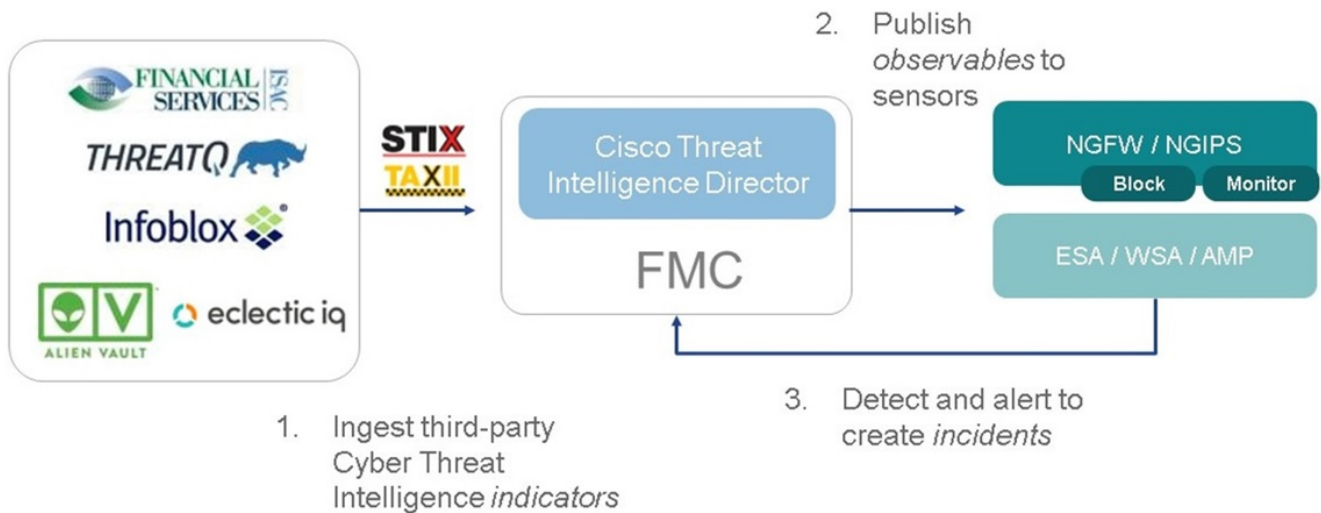
Simple Indicator

Complex indicator, two operators



Hoe werkt het?

Zoals in de afbeelding wordt getoond, dient u op het VCC bronnen te configureren van waar u bedreigingsinformatie wilt downloaden. Het FMC drukt die informatie vervolgens op sensoren. Wanneer het verkeer overeenkomt met de wachtrijen, worden de incidenten weergegeven in de gebruikersinterface van het FMC (GUI).



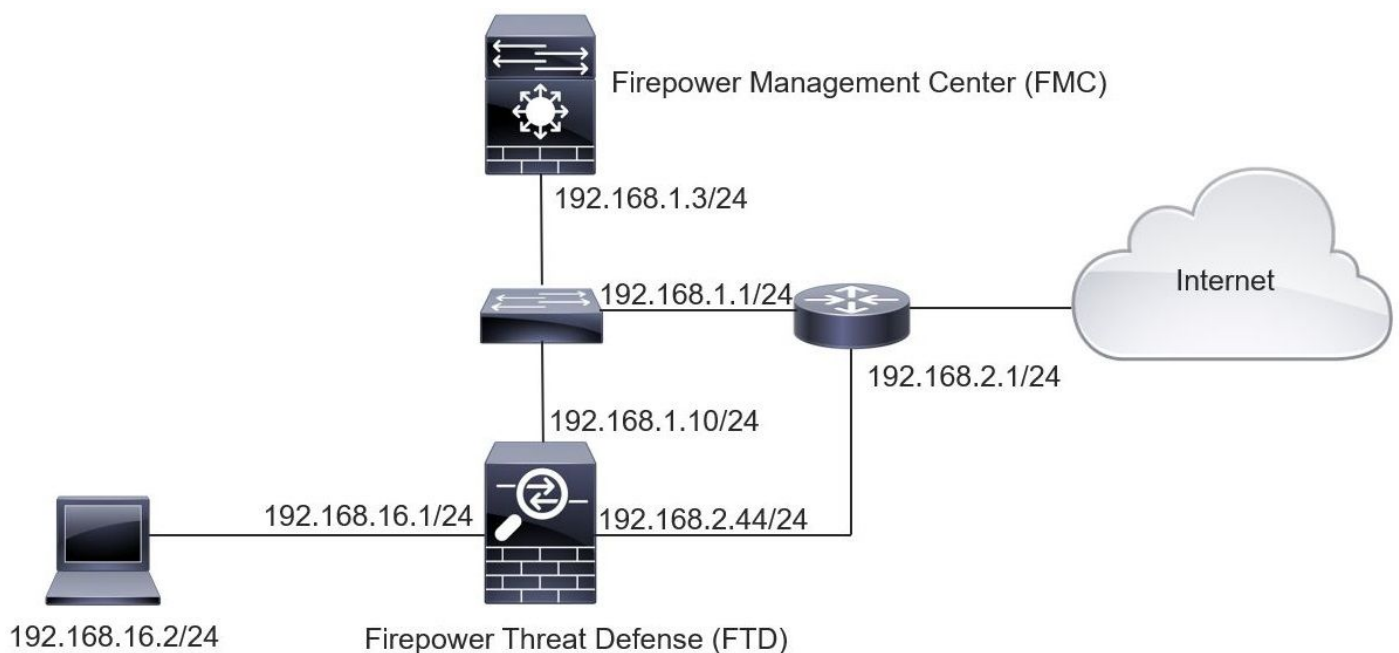
Er zijn twee nieuwe termen:

- STIX (Structured Threat Intelligence eXpression) is een norm voor het delen en gebruiken van informatie over bedreigingen. Er zijn drie essentiële functionele elementen: Indicatoren, waarnemingen en incidenten
- TAXII (Betrouwbare geautomatiseerde uitwisseling van informatie over indicatoren) is een transportmechanisme voor dreigingsinformatie

Configureren

Om de configuratie te voltooien, moet u rekening houden met deze punten:

Netwerkdigram



Configuratie

Stap 1. Om TID te configureren moet u naar het tabblad **Intelligentie** navigeren, zoals in de

afbeelding.

The screenshot shows the Cisco AMP Intelligence interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Sources' tab is active, showing a list of four sources. The table columns are Name, Type, Delivery, Action, Publish, Last Updated, and Status. The sources listed are 'guest.Abuse_ch', 'guest.CyberCrime_Tracker', 'user.AlienVault', and 'test_flat_file'. The status of 'guest.Abuse_ch' and 'user.AlienVault' is 'Completed with Errors', while 'guest.CyberCrime_Tracker' and 'test_flat_file' are 'Completed'.

| 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 |

Opmerking: Status 'Voltooid met fouten' wordt verwacht als een feed niet-ondersteunde punten bevat.

Stap 2. U moet bronnen van bedreigingen toevoegen. Er zijn drie manieren om bronnen toe te voegen:

- TAXII - Wanneer u deze optie gebruikt, kunt u een server configureren waar de bedreigingsinformatie in STIX-indeling wordt opgeslagen

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

Opmerking: De enige beschikbare Actie is Monitor. U kunt de blokactie niet in STIX-indeling configureren voor bedreigingen.

- URL - U kunt een link naar een HTTP/HTTPS lokale server configureren waar de STIX-dreiging of het platte bestand zich bevindt.

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

- Bestand - U kunt een bestand in de *.txt-indeling uploaden en u moet de inhoud van het bestand specificeren. Het bestand moet één inhoudsopgave per regel bevatten.

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

Opmerking: Standaard worden alle bronnen gepubliceerd, wat betekent dat ze naar een sensor worden geduwd. Dit proces kan tot 20 minuten of langer duren.

Stap 3. Onder het tabblad Indicator kunt u bevestigen of er indicatoren zijn gedownload van de geconfigureerde bronnen:

| Intelligence | | | | | | | Deploy | System | Help | admin |
|--------------|---|----------------|-------------|---------|--------------------------|---------------------------|-----------------------|--------|------|-------|
| 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 malicious... <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 malicious... <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 malicious... <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 malicious... <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 malicious... <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 malicious... <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 | | | |

Stap 4. Zodra u de naam van een indicatielampje hebt geselecteerd, kunt u meer informatie over dit indicatielampje zien. Daarnaast kunt u beslissen of u het naar de sensor wilt publiceren of of dat u de actie wilt wijzigen (in het geval van een eenvoudige indicator).

Zoals in de afbeelding wordt getoond, wordt een complexe indicator weergegeven met twee waarnemingen die door de OR-exploitant zijn verbonden:

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](#)

Stap 5. Navigeer naar het tabblad Observables in waar u URL's, IP-adressen, domeinen en SHA256 kunt vinden die in de indicatoren opgenomen zijn. Je kunt beslissen welke waarnemingen je naar sensoren wilt duwen en de actie voor die sensoren optioneel wijzigen. In de laatste kolom is er een whitelist-knop die gelijk is aan een publiceren-optie.

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

Stap 6. Navigeer naar het tabblad Elementen om de lijst met apparaten te controleren waar TID is ingeschakeld.

| 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 |

Stap 7 (optioneel). Blader naar het tabblad Instellingen en selecteer de knop Pauze om te stoppen met het drukken van indicatoren op sensoren. Deze bewerking kan tot 20 minuten duren.

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

Verifiëren

Methode 1. Om te verifiëren of TID een actie op het verkeer heeft uitgevoerd, moet u naar het tabblad Incidenten navigeren.

| 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. De incidenten zijn te vinden op het tabblad Security Intelligence onder een TID-label.

| 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 |

Opmerking: TID heeft een opslagcapaciteit van 1 miljoen incidenten.

Methode 3. U kunt bevestigen of er op het VCC en een sensor geconfigureerde bronnen (voedingen) aanwezig zijn. Om dat te doen, kunt u naar deze locaties op de CLI navigeren:

`/var/sf/siurl_download/`

`/var/sf/sidns_download/`

`/var/sf/ipprep_download/`

Er is een nieuwe directory aangemaakt voor 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-f6cc0e401935.1f
-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

```

Opmerking: TID is alleen beschikbaar op de Global Doiman-toets op het FMC

Opmerking: Als u TID op het actieve FireSIGHT Management Center installeert in een hoge beschikbaarheid (fysieke FMC-apparaten), synchroniseert het systeem de TID-configuraties en TID-gegevens niet naar het stand-by FireSIGHT Management Center.

Problemen oplossen

Er is een top-level proces dat **tid** wordt genoemd. Dit proces is afhankelijk van drie processen: **Mongo**, **RabbitMQ**, **hers**. Om de **status** van de processen te controleren, voert u een gereedschap uit | **grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "** opdracht.

```
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#
```

Om in real-time te verifiëren welke actie wordt ondernomen, kunt u **systeem steun firewall-motor-debug** of **systeem** spooropdracht uitvoeren.

```
> 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
```

Er zijn twee actiemogelijkheden:

- **URL SI: Aangepaste regel 19, ID 19, is lijst nummer 1074790455, actie 4** - het verkeer was geblokkeerd
- **URL SI: Volgorde 20, ID 20, is lijst nummer 1074790456, actie 6** - het verkeer werd bewaakt.