Konfiguration und Fehlerbehebung mit Cisco Threat Intelligence Director

Inhalt

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 Domänennamen-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:

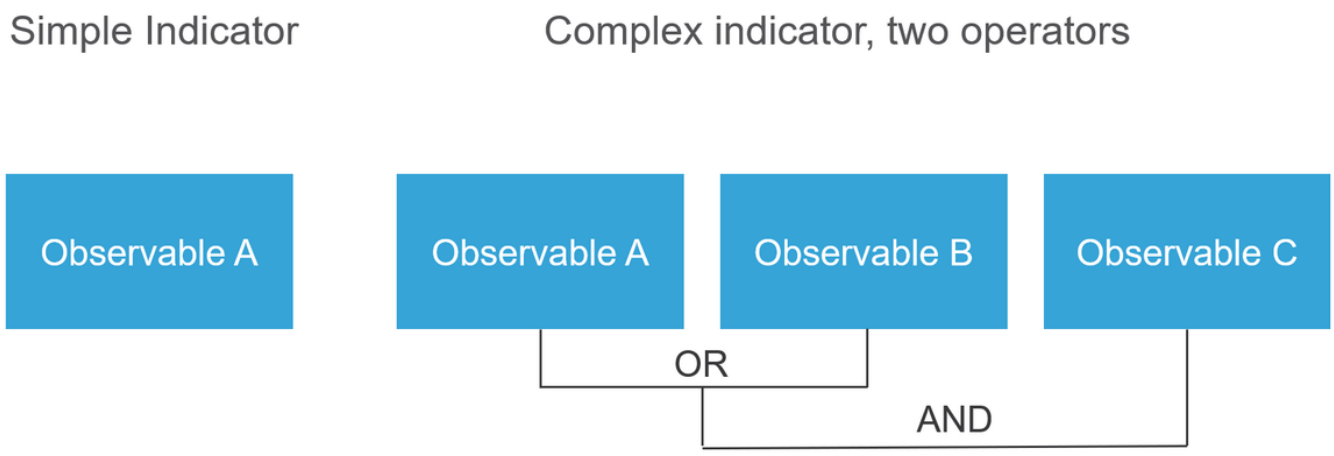
- Cisco FirePOWER Threat Defense (FTD) Virtual mit 6.2.2.81
- FirePOWER Management Center Virtual (vFMC) mit 6.2.2.81

> 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.

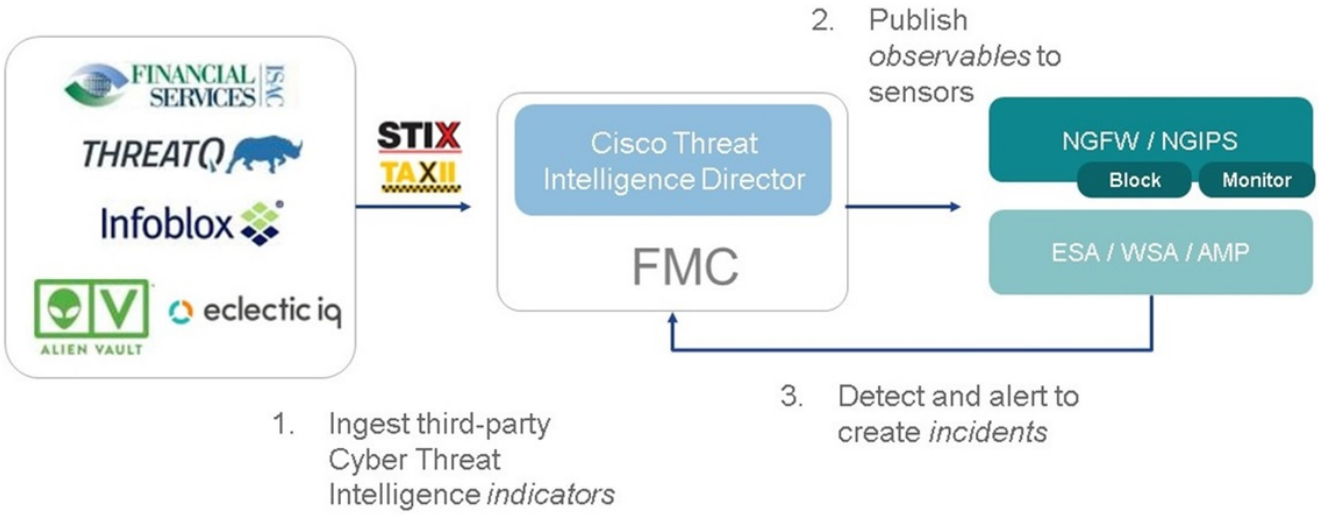
Es gibt drei neue Begriffe: **Beobachtungen**, **Indikatoren** und **Vorfälle**. Observable ist nur eine Variable, kann z. B. URL, Domäne, IP-Adresse oder SHA256. Indikatoren werden aus Beobachtungswerten erstellt. Es gibt zwei Arten von Indikatoren. Ein einfacher Indikator enthält nur einen beobachtbaren. 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.



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.



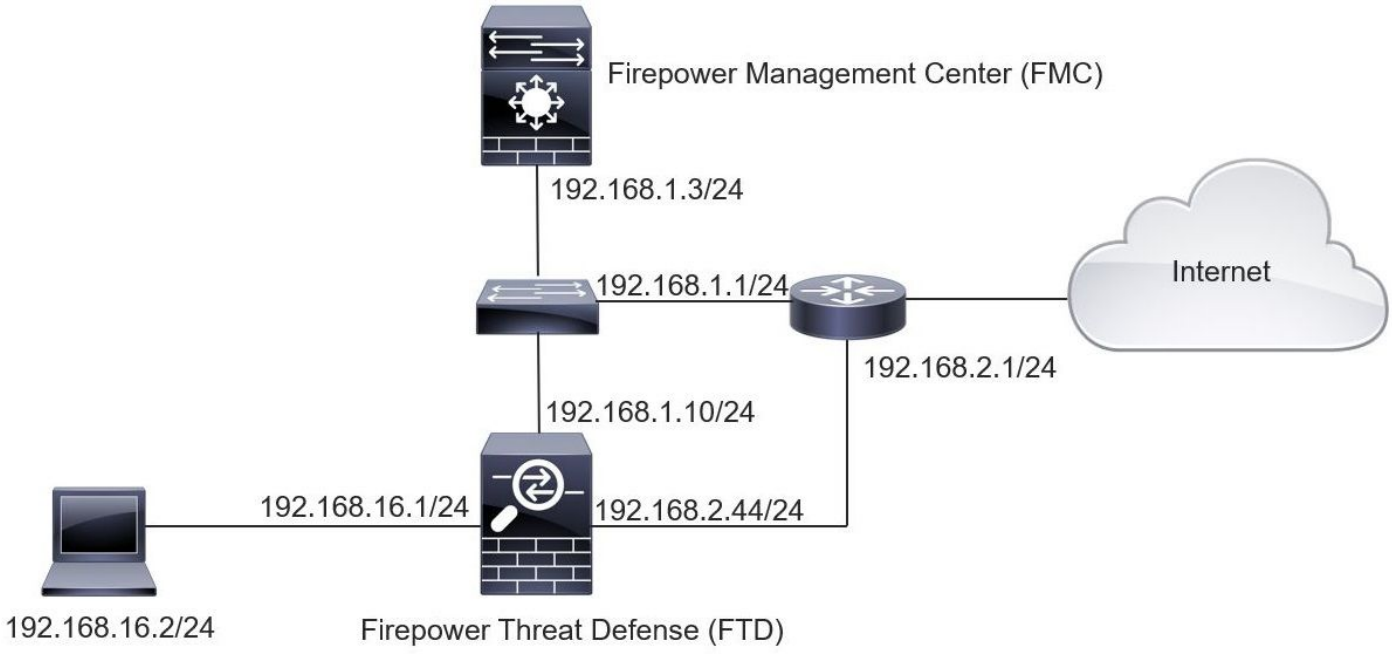
Es gibt zwei neue Begriffe:

- 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

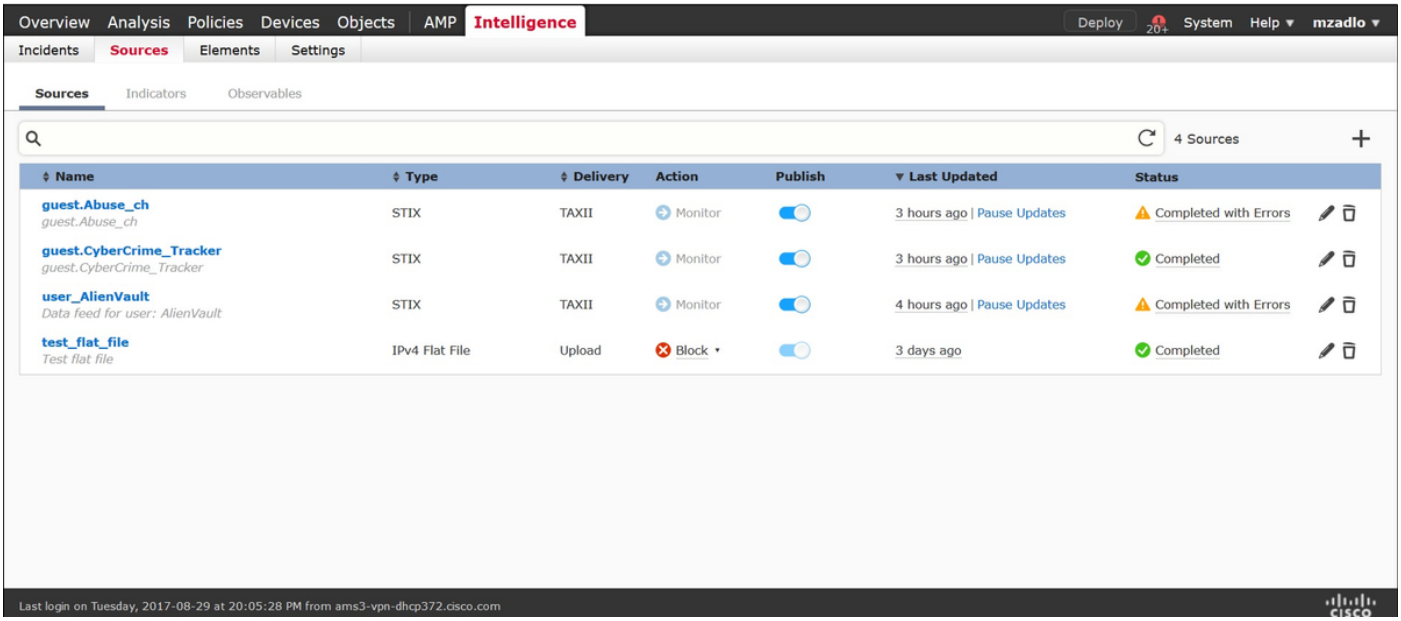
Um die Konfiguration abzuschließen, müssen folgende Abschnitte berücksichtigt werden:

Netzwerkdiagramm



Konfiguration

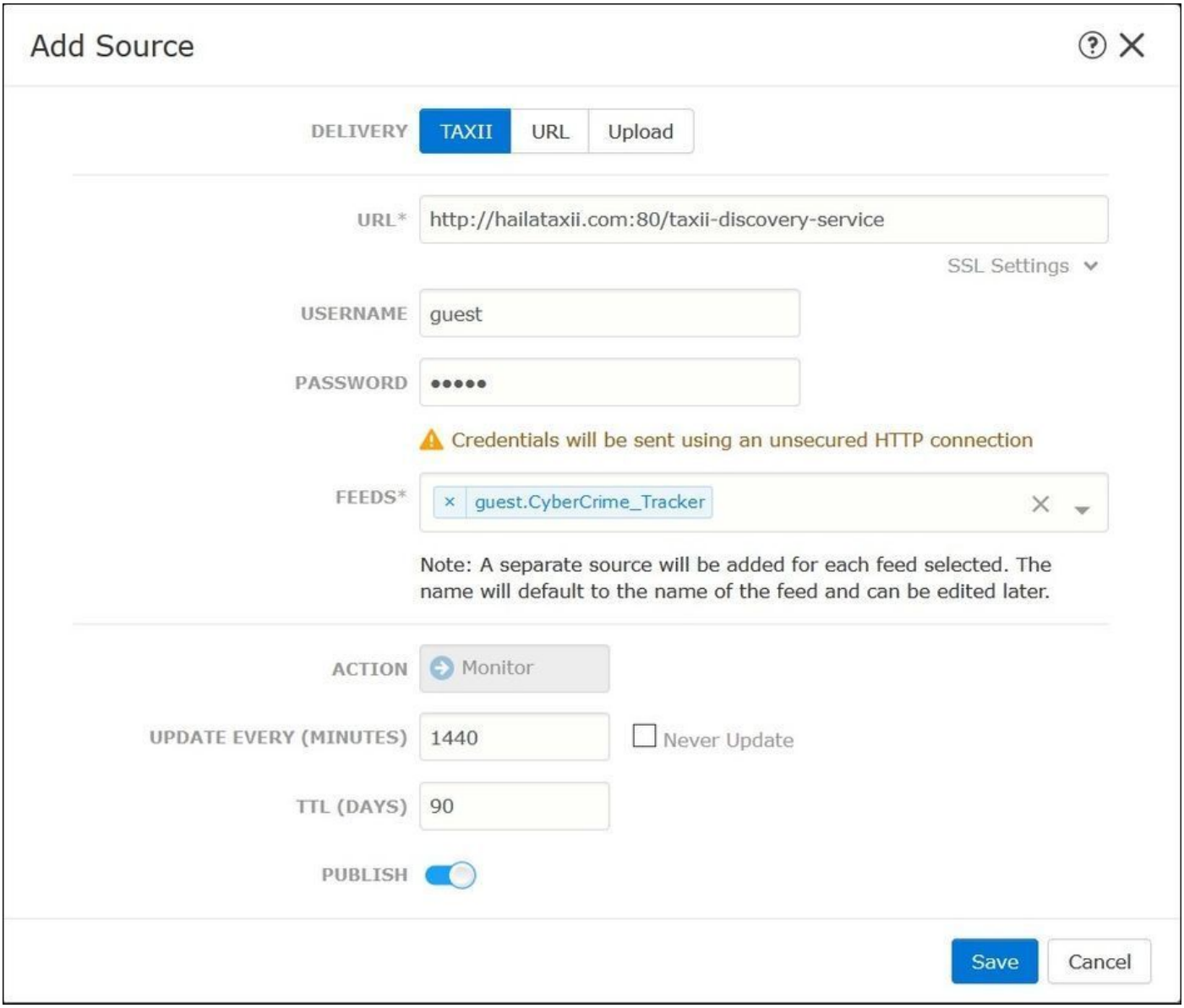
Schritt 1: Um TID zu konfigurieren, müssen Sie zur Registerkarte **Intelligence** navigieren, wie im Bild gezeigt.



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

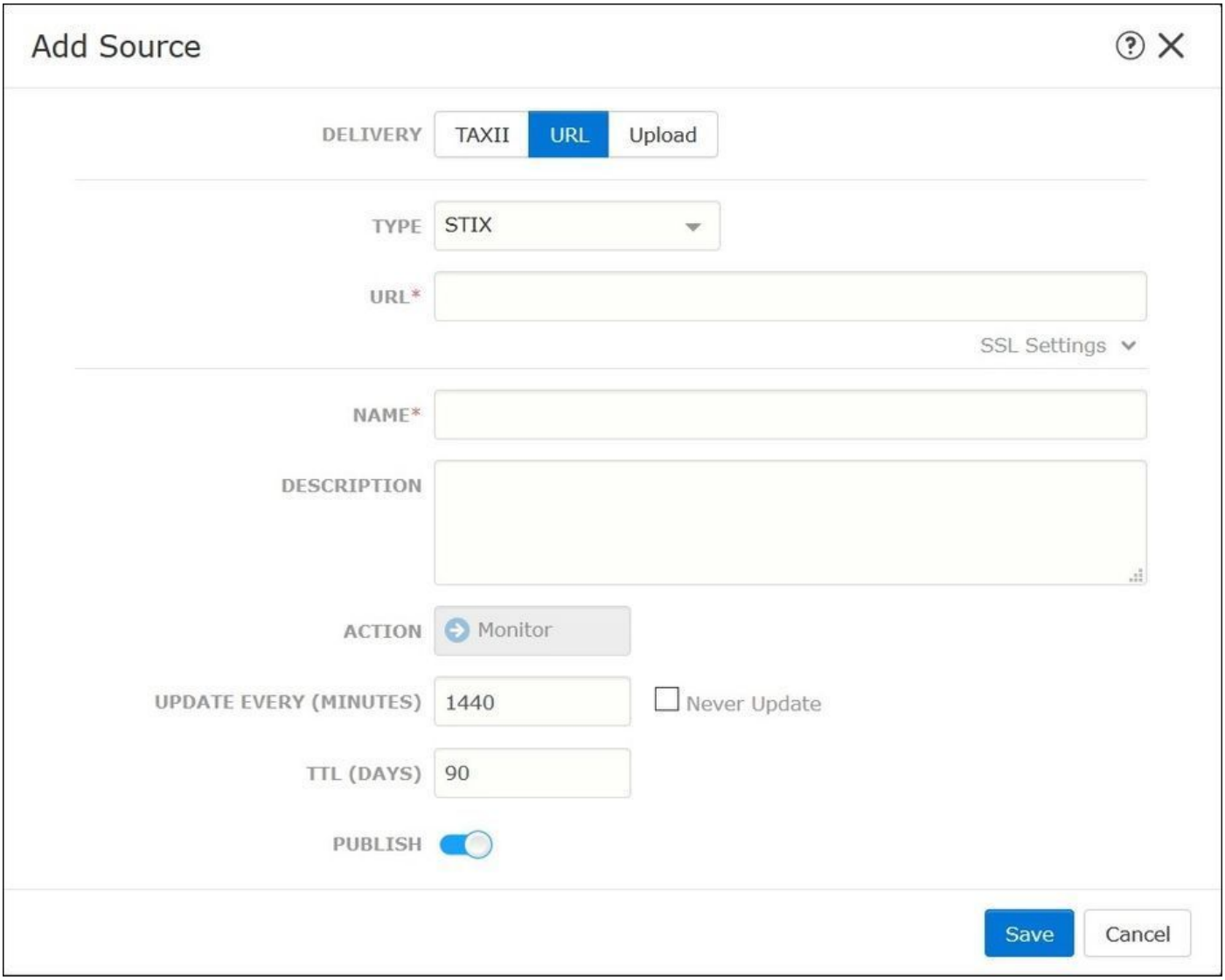
Schritt 2: Sie müssen Bedrohungsquellen hinzufügen. Es gibt drei Möglichkeiten, Quellen hinzuzufügen:

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

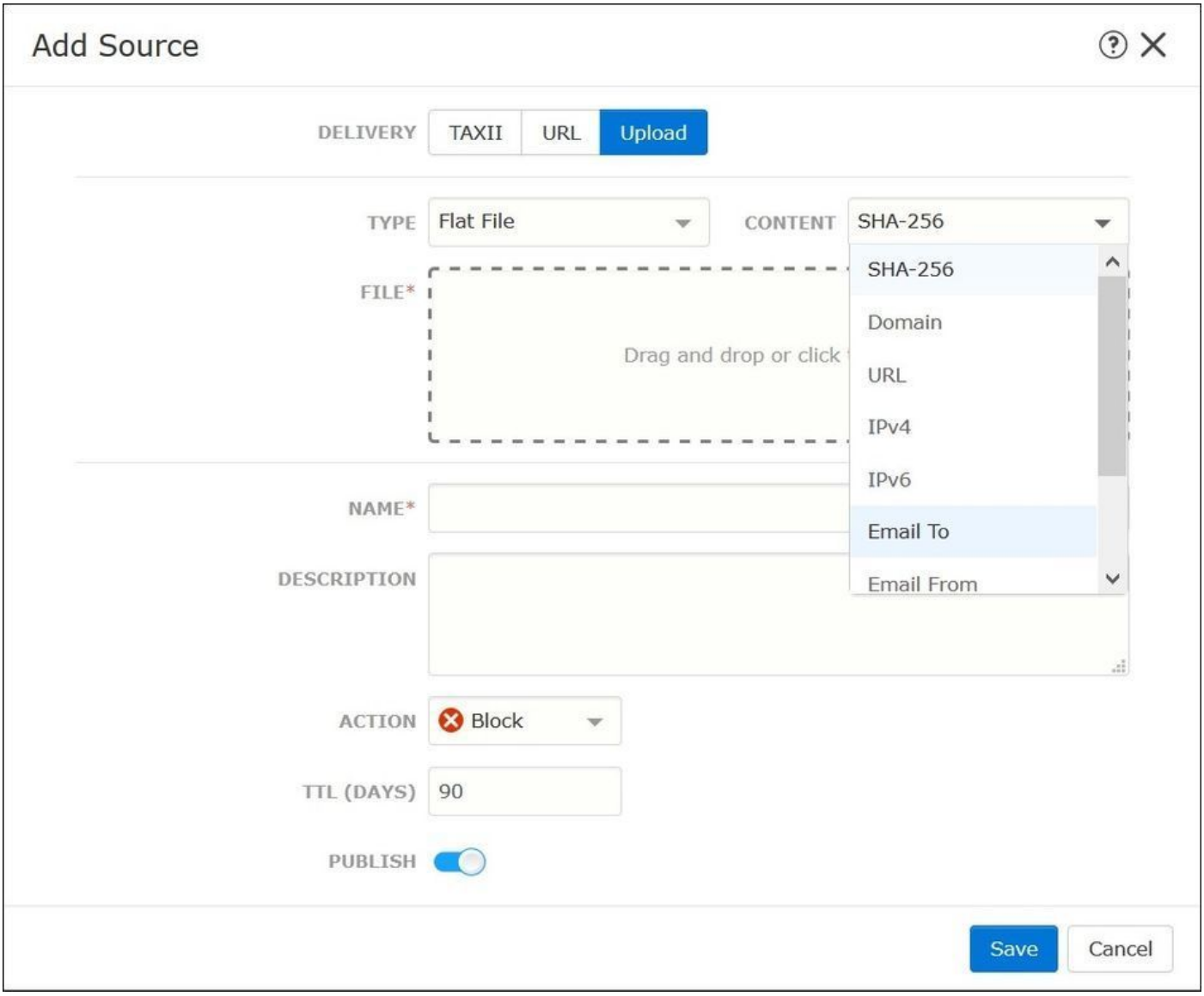


Hinweis: Die einzige Aktion, die verfügbar ist, ist Monitor. Sie können die Blockaktion nicht für Bedrohungen im STIX-Format konfigurieren.

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

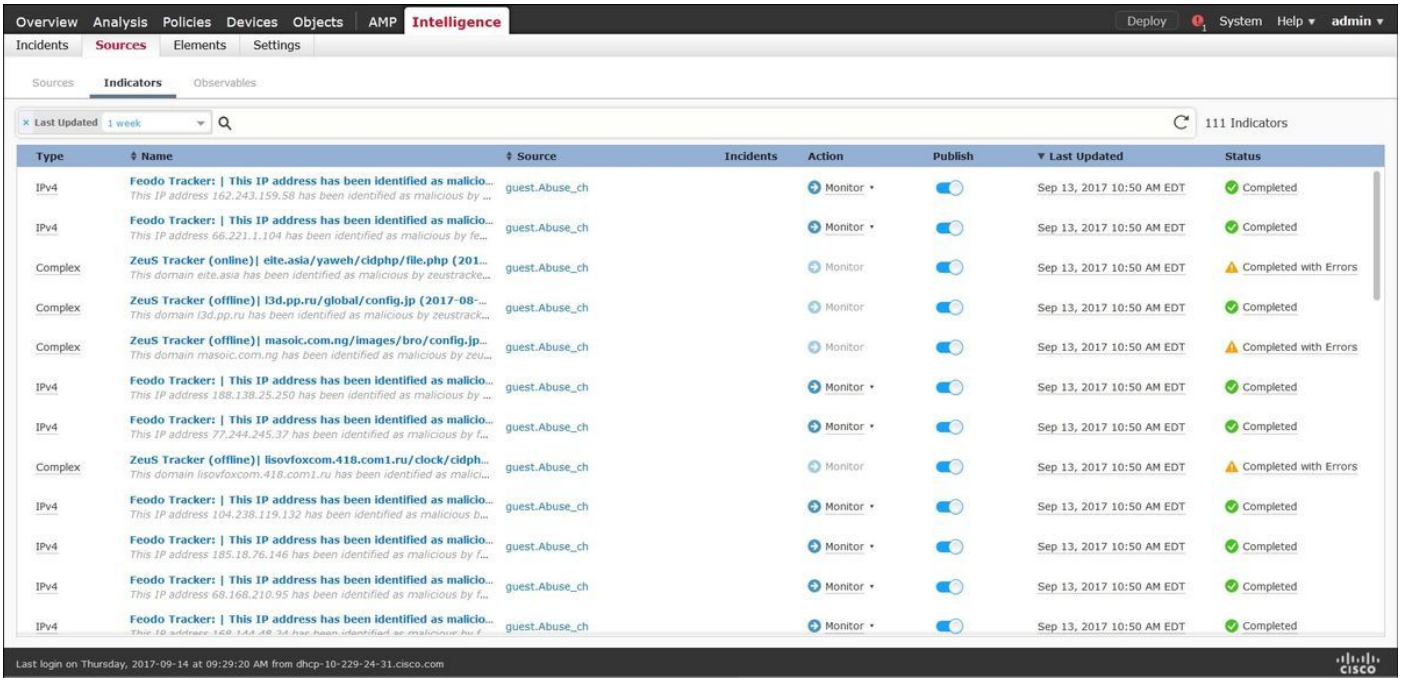


- Flachdatei: Sie können eine Datei im Format ***.txt** hochladen und müssen den Inhalt der Datei angeben. Die Datei muss pro Zeile einen Content-Eintrag enthalten.



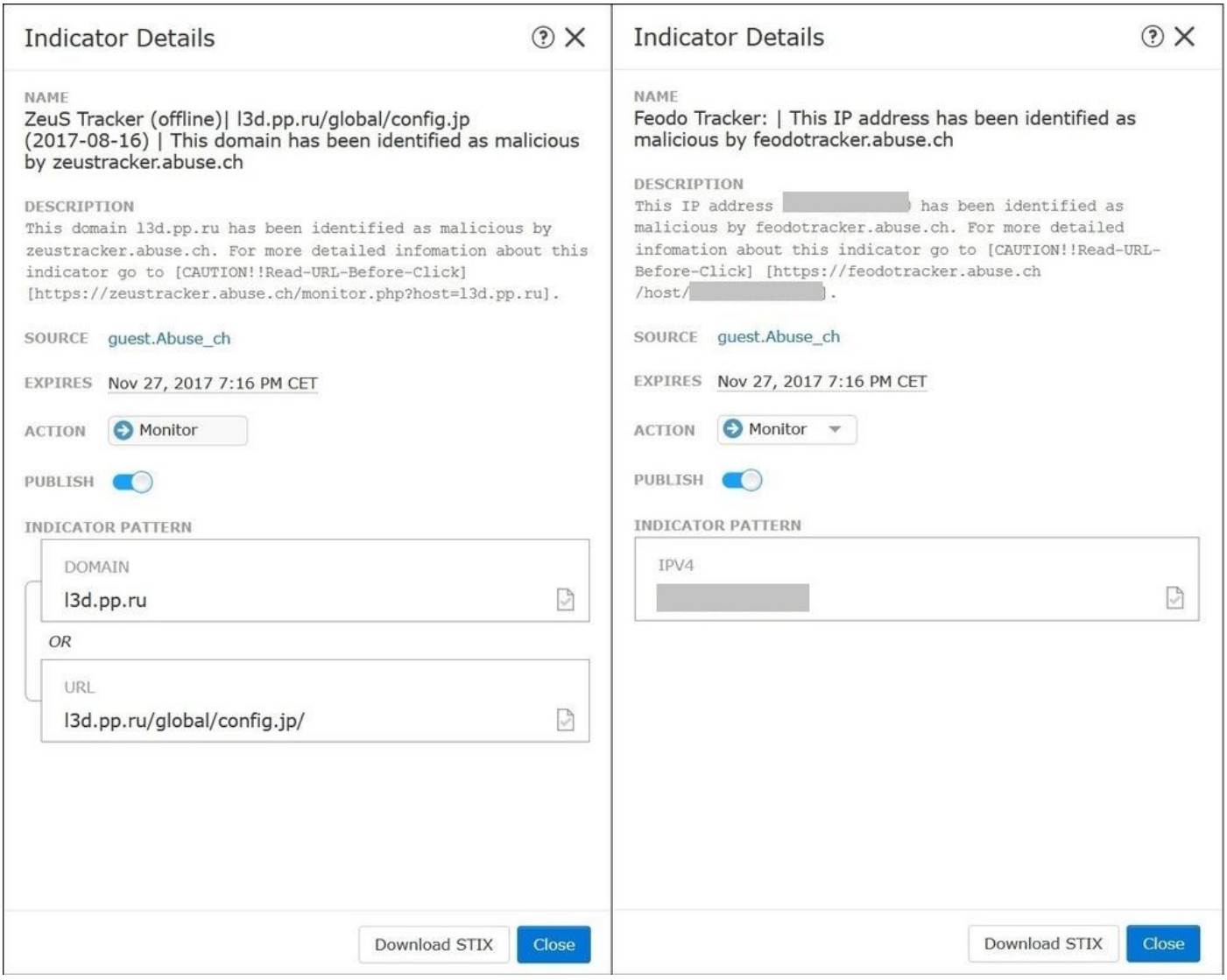
Hinweis: Standardmäßig werden alle Quellen veröffentlicht, d. h. sie werden an Sensoren übertragen. Dieser Vorgang kann bis zu 20 Minuten oder länger dauern.

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

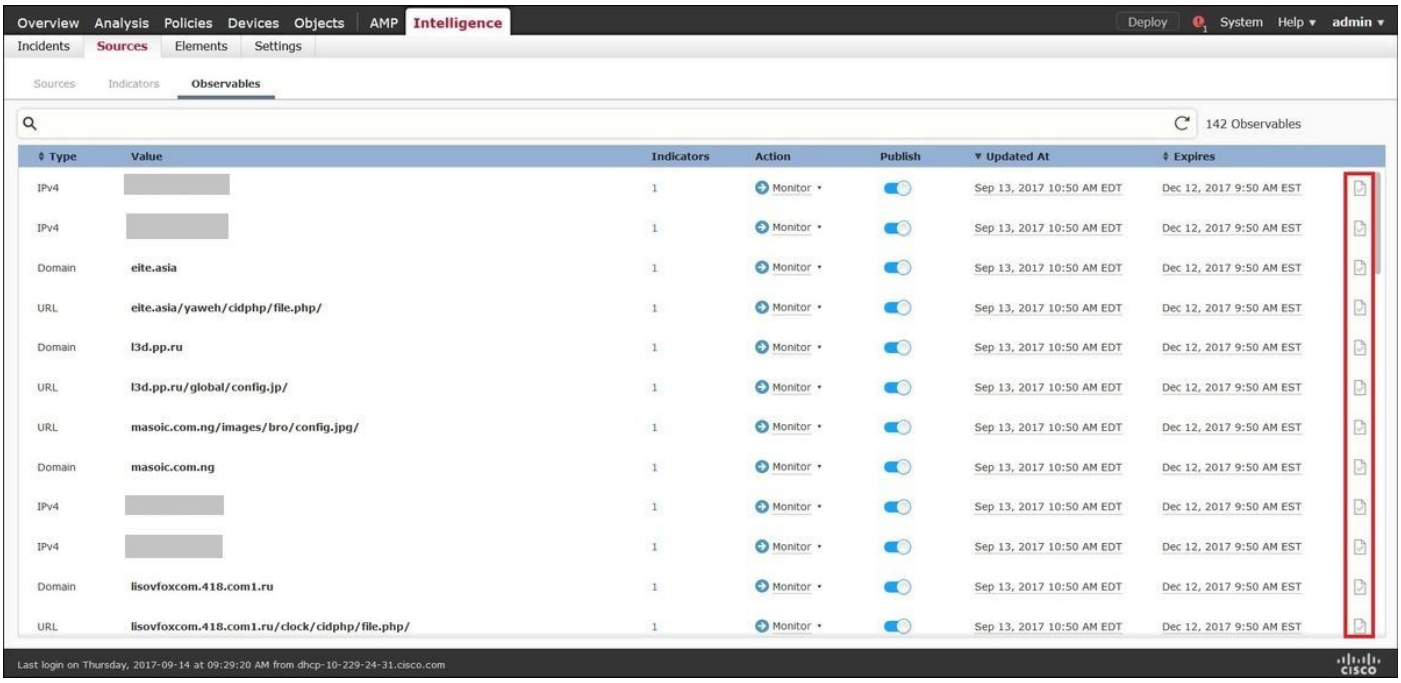


Schritt 4: Sobald Sie den Namen einer Anzeige ausgewählt haben, werden weitere Details angezeigt. Zusätzlich können Sie entscheiden, ob Sie den Sensor veröffentlichen oder die Aktion ändern möchten (bei einer einfachen Anzeige).

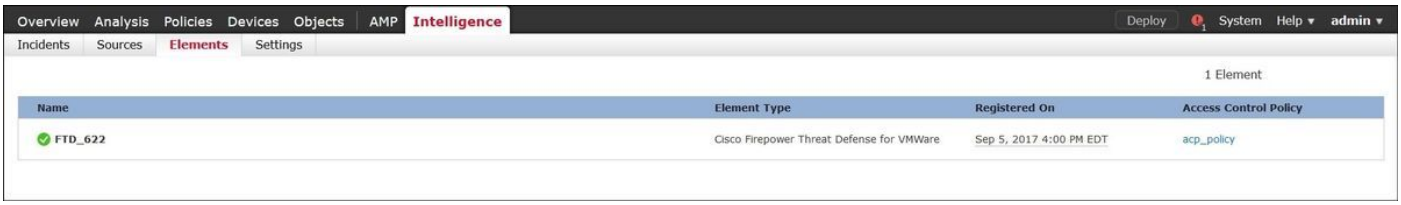
Wie im Bild gezeigt, wird ein komplexer Indikator mit zwei Sternchen aufgelistet, die durch den OR-Operator verbunden sind:



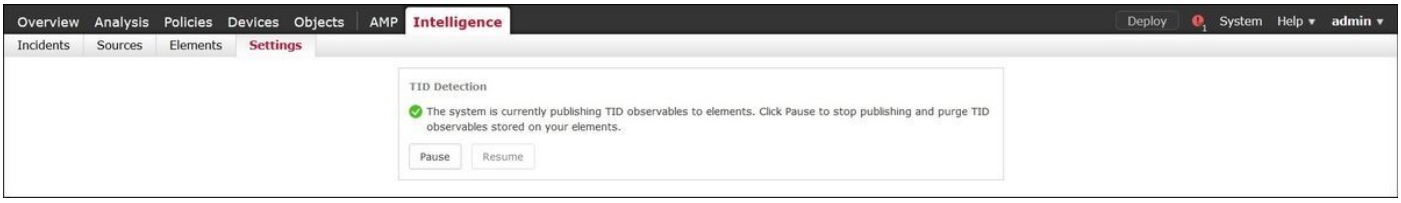
Schritt 5: Navigieren Sie zur Registerkarte Observables (Observables), auf der Sie URLs, IP-Adressen, Domänen und SHA256 finden, die in den Anzeigen enthalten sind. Sie können entscheiden, welche Beobachtungen Sie an die Sensoren senden möchten und optional die Aktion für sie ändern. In der letzten Spalte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



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

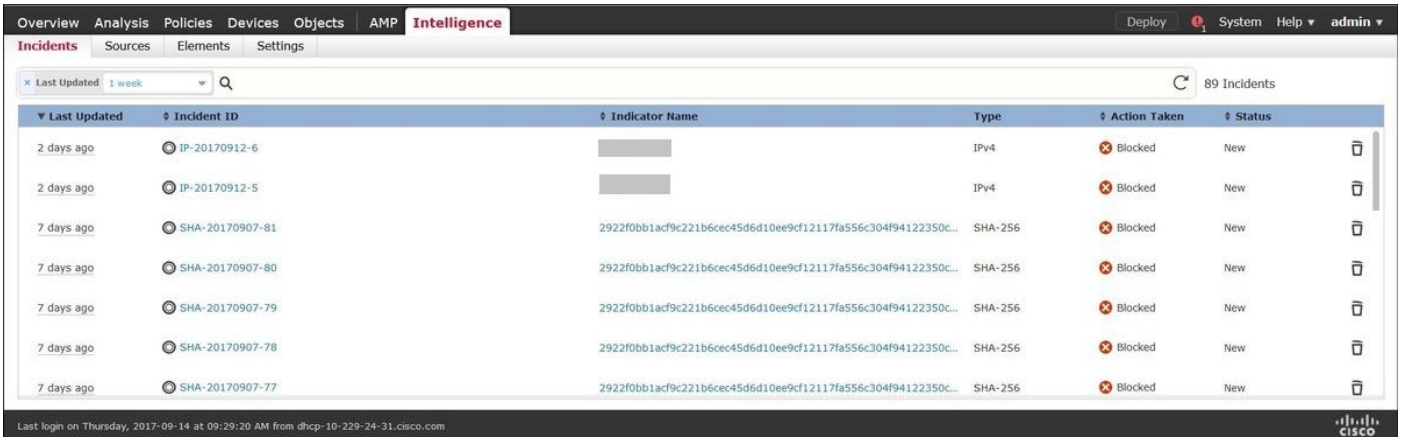


Schritt 7 (optional). Navigieren Sie zur Registerkarte Settings (Einstellungen), und wählen Sie die Schaltfläche Pause (Anhalten) aus, um zu verhindern, dass die Anzeigen auf die Sensoren gedrückt werden. Dieser Vorgang kann bis zu 20 Minuten dauern.

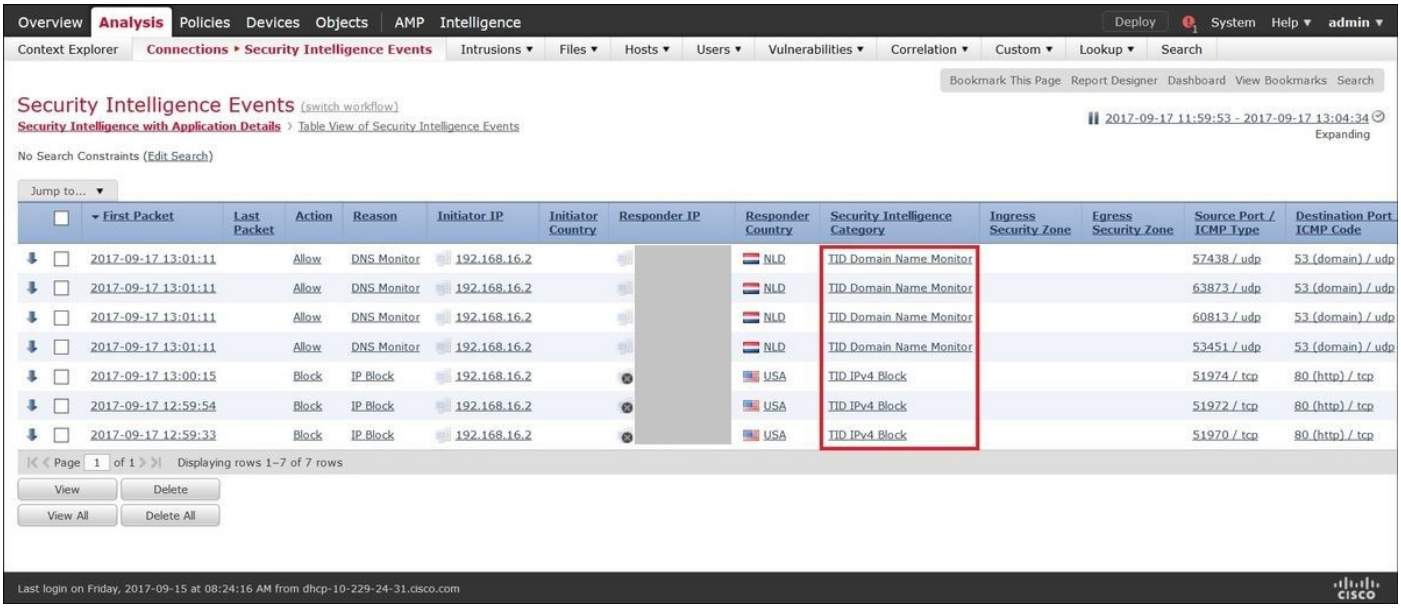


Überprüfen

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



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



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
2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c2bcbdc
```

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.