Configuration et dépannage de Cisco Threat Intelligence Director

Contenu

Introduction

Ce document décrit comment configurer et dépanner Cisco Threat Intelligence Director (TID).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de Firepower Management Center (FMC)

Vous devez vous assurer de ces conditions avant de configurer la fonction Cisco Threat Intelligence Director :

- Firepower Management Center (FMC) : Doit être exécuté sur la version 6.2.2 (ou ultérieure) (peut être hébergé sur une FMC physique ou virtuelle).Doit être configuré avec un minimum de 15 Go de mémoire RAM.Doit être configuré avec l'accès à l'API REST activé.
- Le capteur doit exécuter la version 6.2.2 (ou ultérieure).
- Dans l'onglet Advanced Settings de l'option de stratégie de contrôle d'accès, l'option **Enable Threat Intelligence Director** doit être activée.
- Ajoutez des règles à la stratégie de contrôle d'accès si elles ne sont pas déjà présentes.
- Si vous souhaitez que les observables SHA-256 génèrent des observations et des événements Firepower Management Center, créez une ou plusieurs règles de fichier **Malware Cloud Lookup** ou **Block Malware Malware** et associez la stratégie de fichier à une ou plusieurs règles dans la stratégie de contrôle d'accès.
- Si vous souhaitez que les observations IPv4, IPv6, URL ou Nom de domaine génèrent des événements de connexion et d'intelligence de sécurité, activez la journalisation des

informations de connexion et de sécurité dans la stratégie de contrôle d'accès.

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

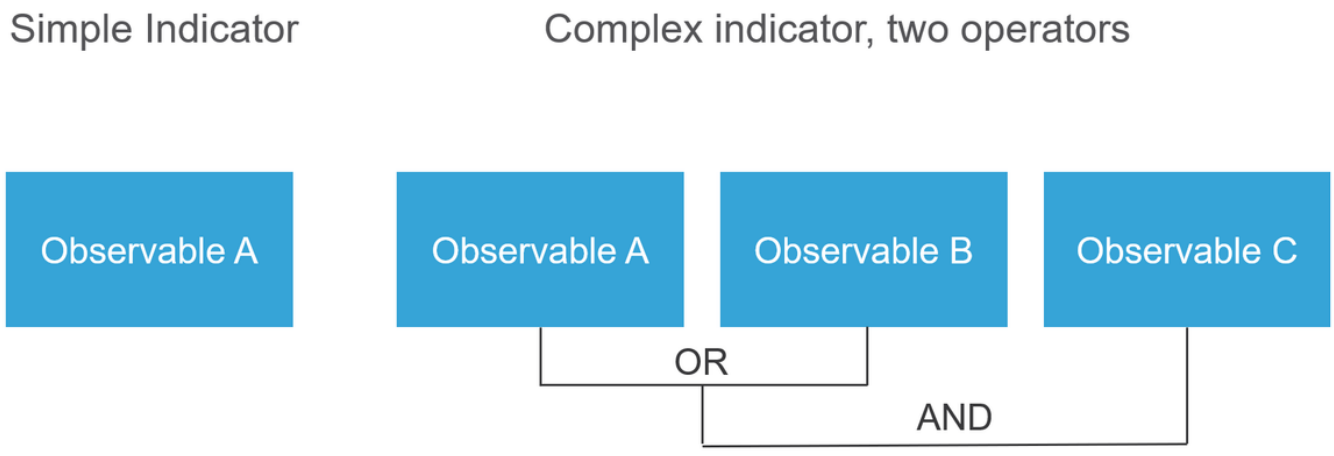
- Cisco Firepower Threat Defense (FTD) Virtual qui exécute 6.2.2.81
- Firepower Management Center Virtual (vFMC) qui exécute 6.2.2.81

Note: 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

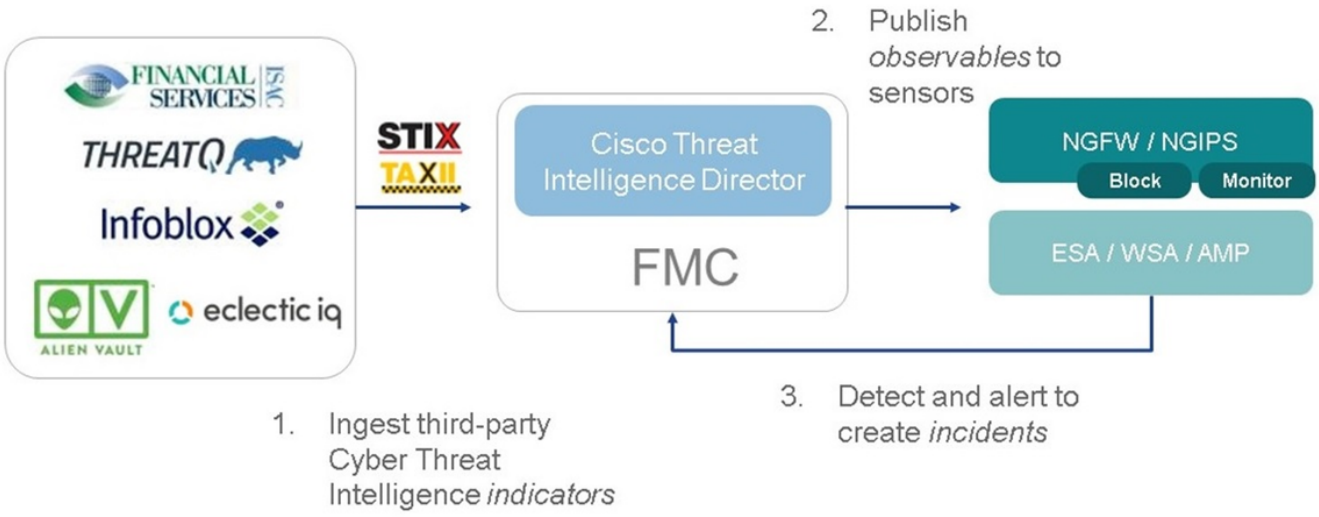
Cisco Threat Intelligence Director (TID) est un système qui rend opérationnelles les informations sur les menaces. Le système consomme et normalise des informations hétérogènes sur les cybermenaces tierces, publie ces informations sur les technologies de détection et met en corrélation les observations des technologies de détection.

Il existe trois nouveaux termes : **observables**, **indicateurs** et **incidents**. Observable n'est qu'une variable, peut être par exemple URL, domaine, adresse IP ou SHA256. Les indicateurs sont faits à partir d'observables. Il existe deux types d'indicateurs. Un indicateur simple ne contient qu'un seul indicateur observable. Dans le cas d'indicateurs complexes, il y a deux ou plusieurs indicateurs observables qui sont connectés l'un à l'autre à l'aide de fonctions logiques comme AND et OR. Une fois que le système a détecté le trafic qui doit être bloqué ou surveillé sur le FMC, l'incident apparaît.



Comment cela fonctionne-t-il?

Comme le montre l'image, sur le FMC, vous devez configurer les sources à partir desquelles vous souhaitez télécharger des informations sur les menaces. Le FMC transmet ensuite ces informations (observables) aux capteurs. Lorsque le trafic correspond aux observables, les incidents apparaissent dans l'interface utilisateur FMC (GUI).



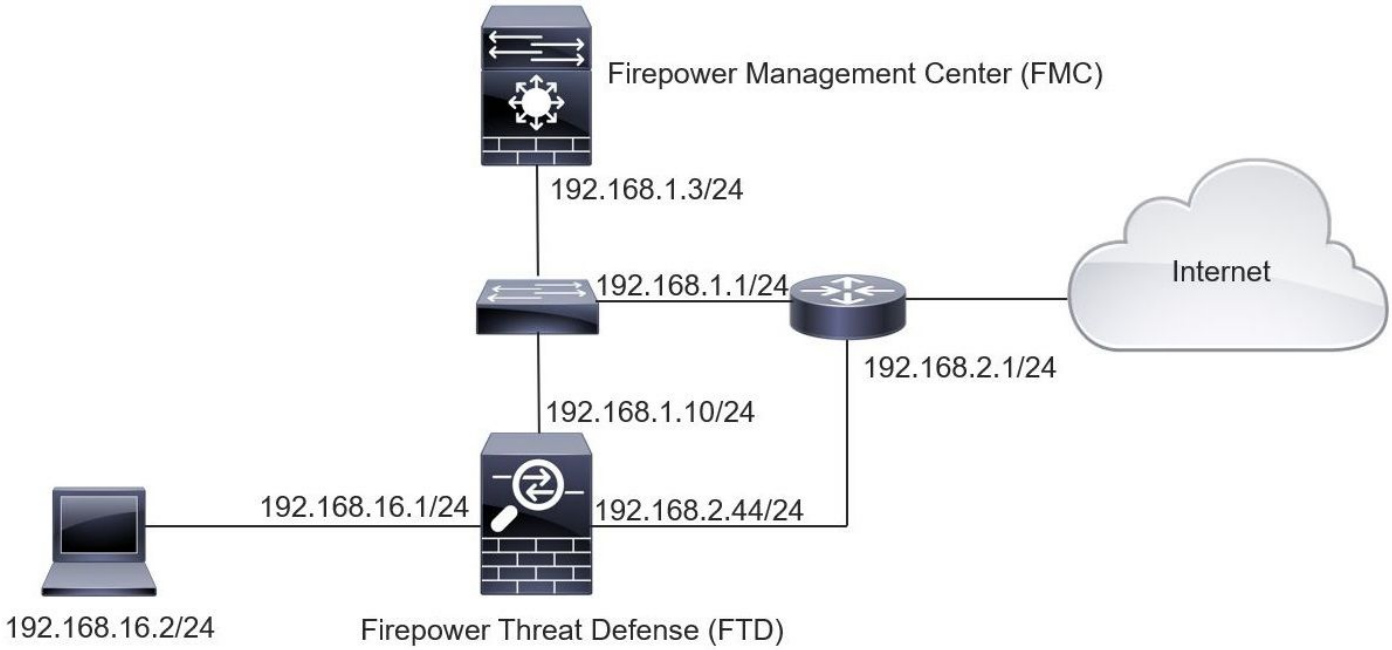
Il existe deux nouveaux termes :

- STIX (Structured Threat Intelligence eXpression) est une norme de partage et d'utilisation des informations sur les menaces. Il y a trois éléments fonctionnels clés : Indicateurs, observables et incidents
- TAXII (Trusted Automated eXchange of Indicator Information) est un mécanisme de transport des informations sur les menaces

Configuration

Pour terminer la configuration, tenez compte des sections suivantes :

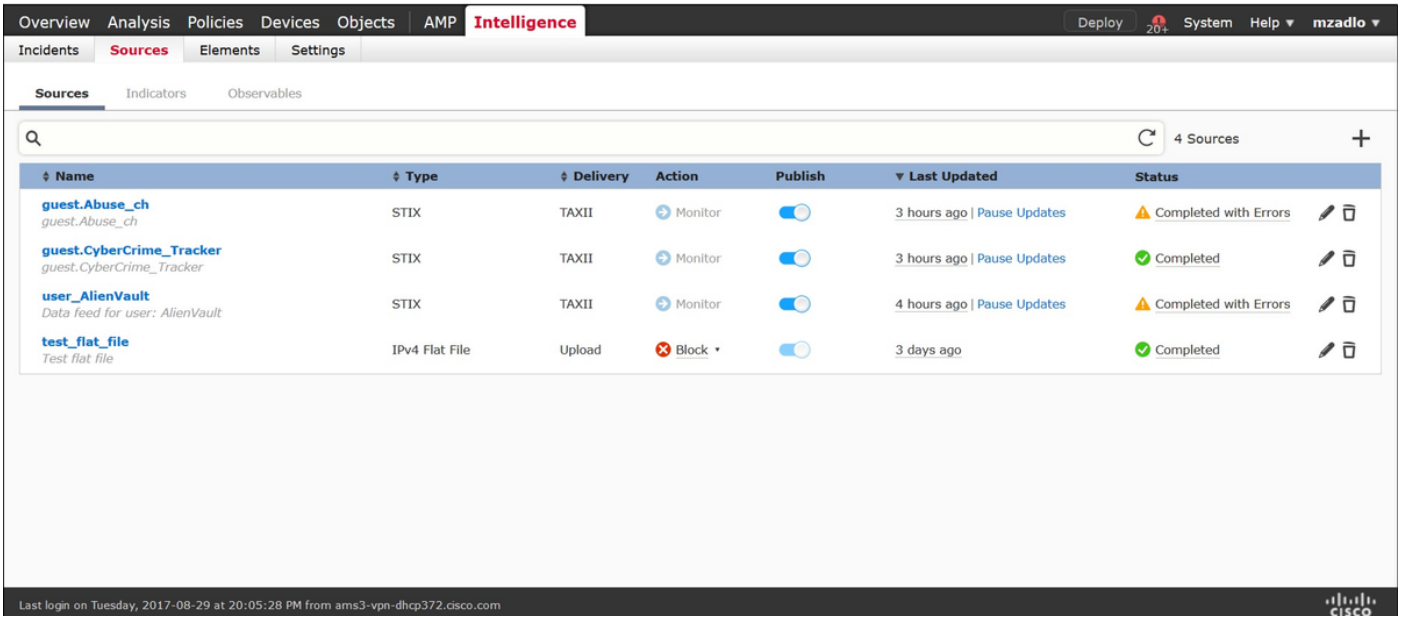
Diagramme du réseau



Configuration

Étape 1. Pour configurer TID, vous devez naviguer jusqu'à l'onglet **Intelligence**, comme indiqué

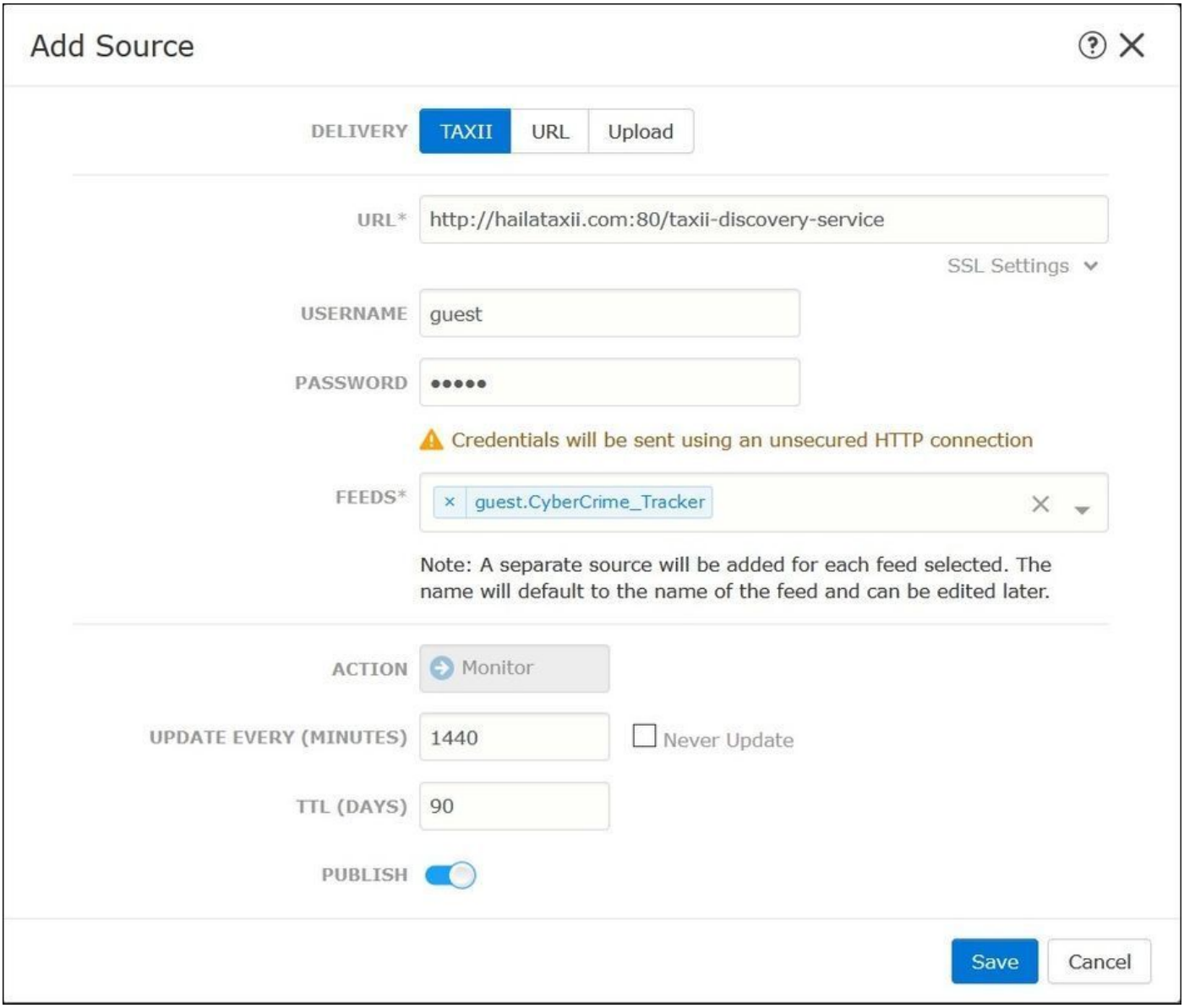
dans l'image.



> Note: L'état 'Terminé avec des erreurs' est attendu si un flux contient des observables non pris en charge.

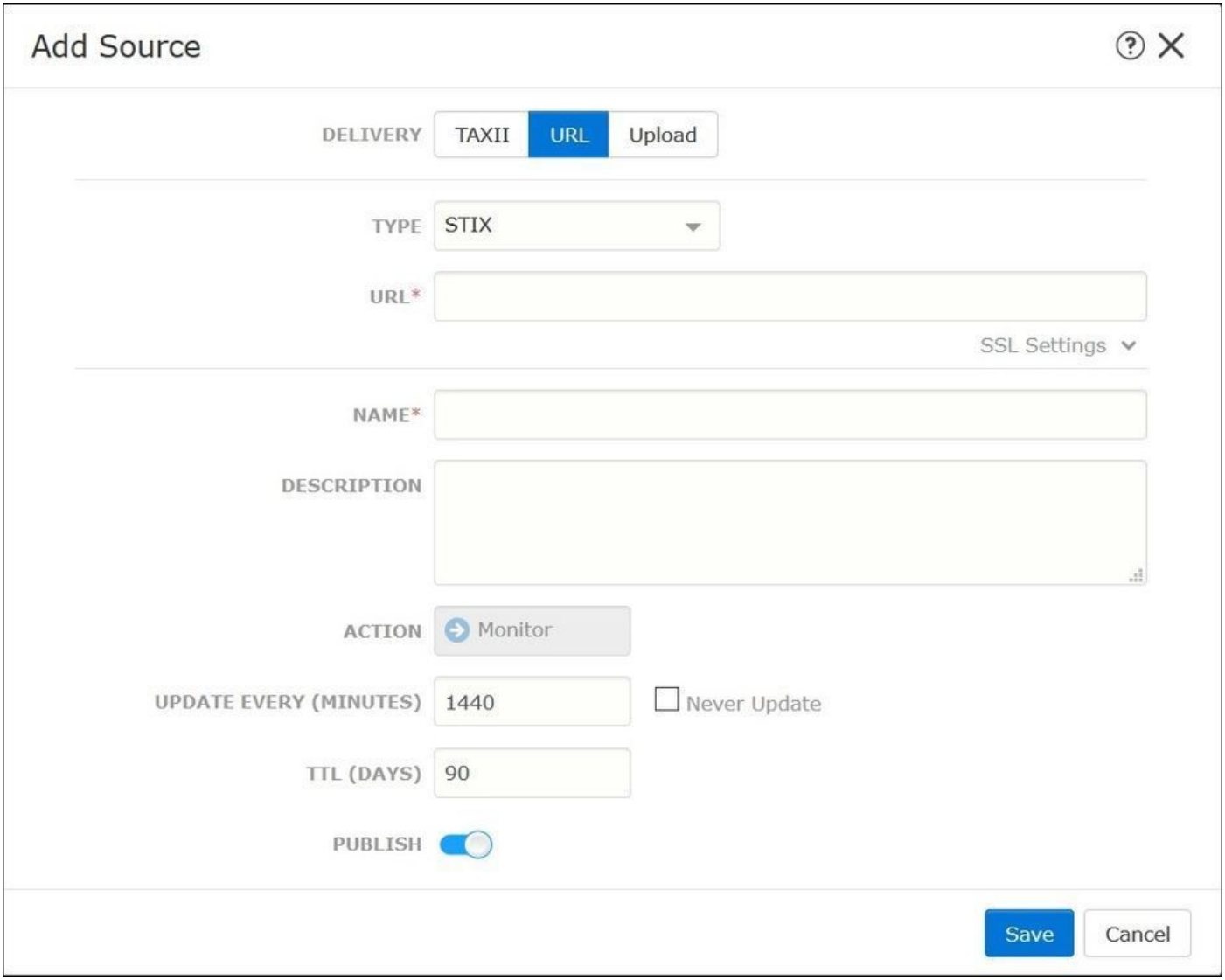
Étape 2. Vous devez ajouter des sources de menaces. Il existe trois façons d'ajouter des sources :

- TAXII - Lorsque vous utilisez cette option, vous pouvez configurer un serveur où les informations sur les menaces sont stockées au format STIX

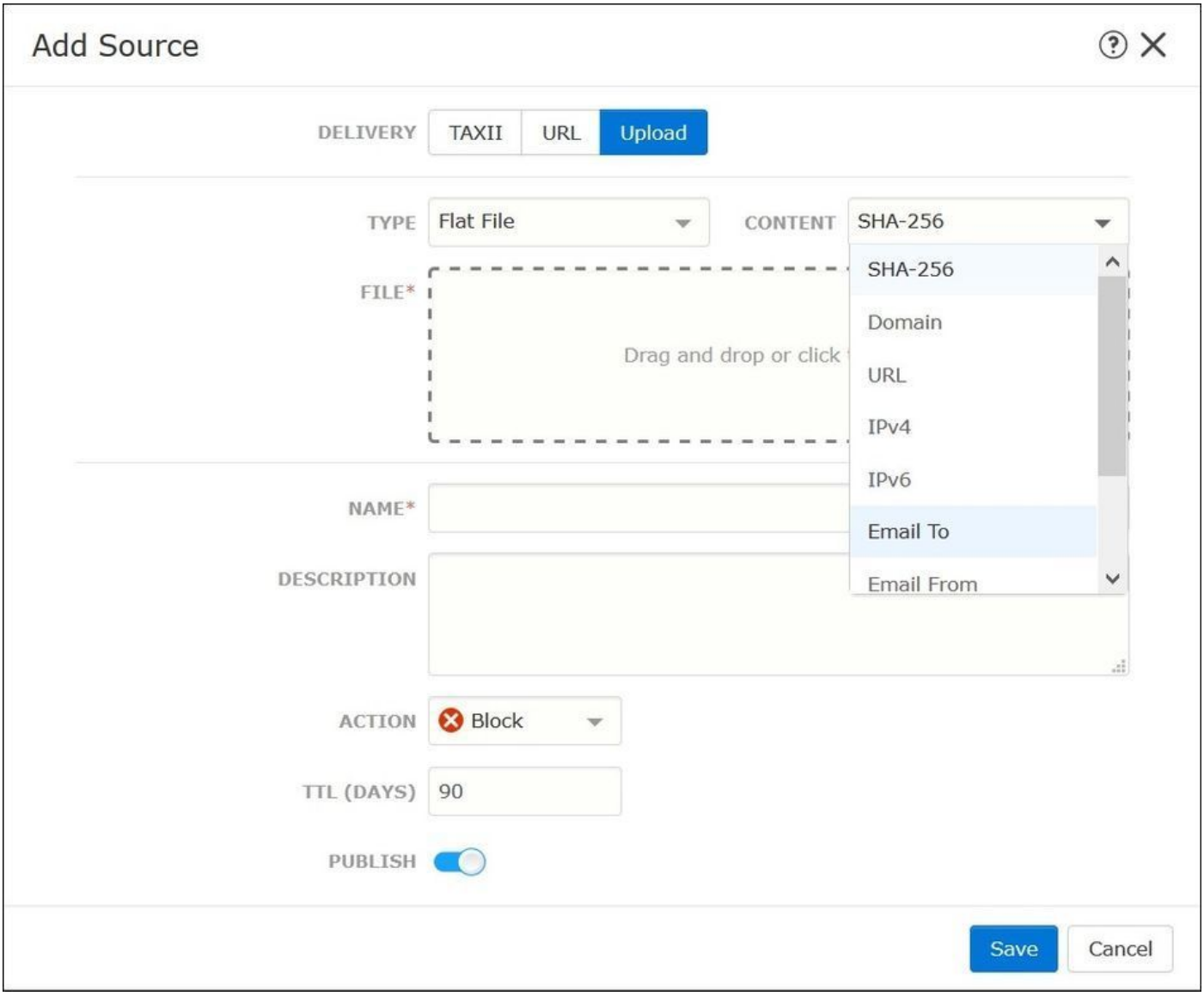


Note: La seule action disponible est Monitor. Vous ne pouvez pas configurer l'action de blocage pour les menaces au format STIX.

- URL : vous pouvez configurer un lien vers un serveur local HTTP/HTTPS où se trouve la menace STIX ou le fichier plat.

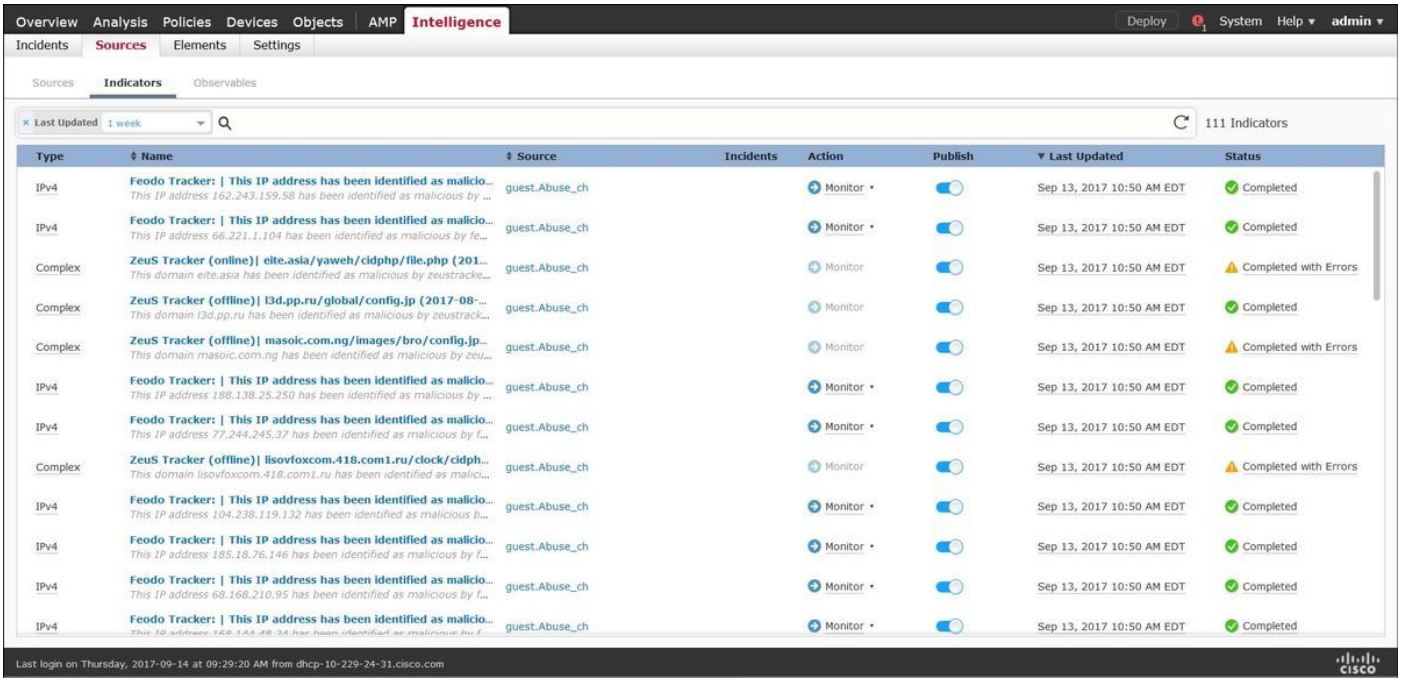


- Fichier plat - Vous pouvez télécharger un fichier au format ***.txt** et vous devez spécifier le contenu du fichier. Le fichier doit contenir une entrée de contenu par ligne.



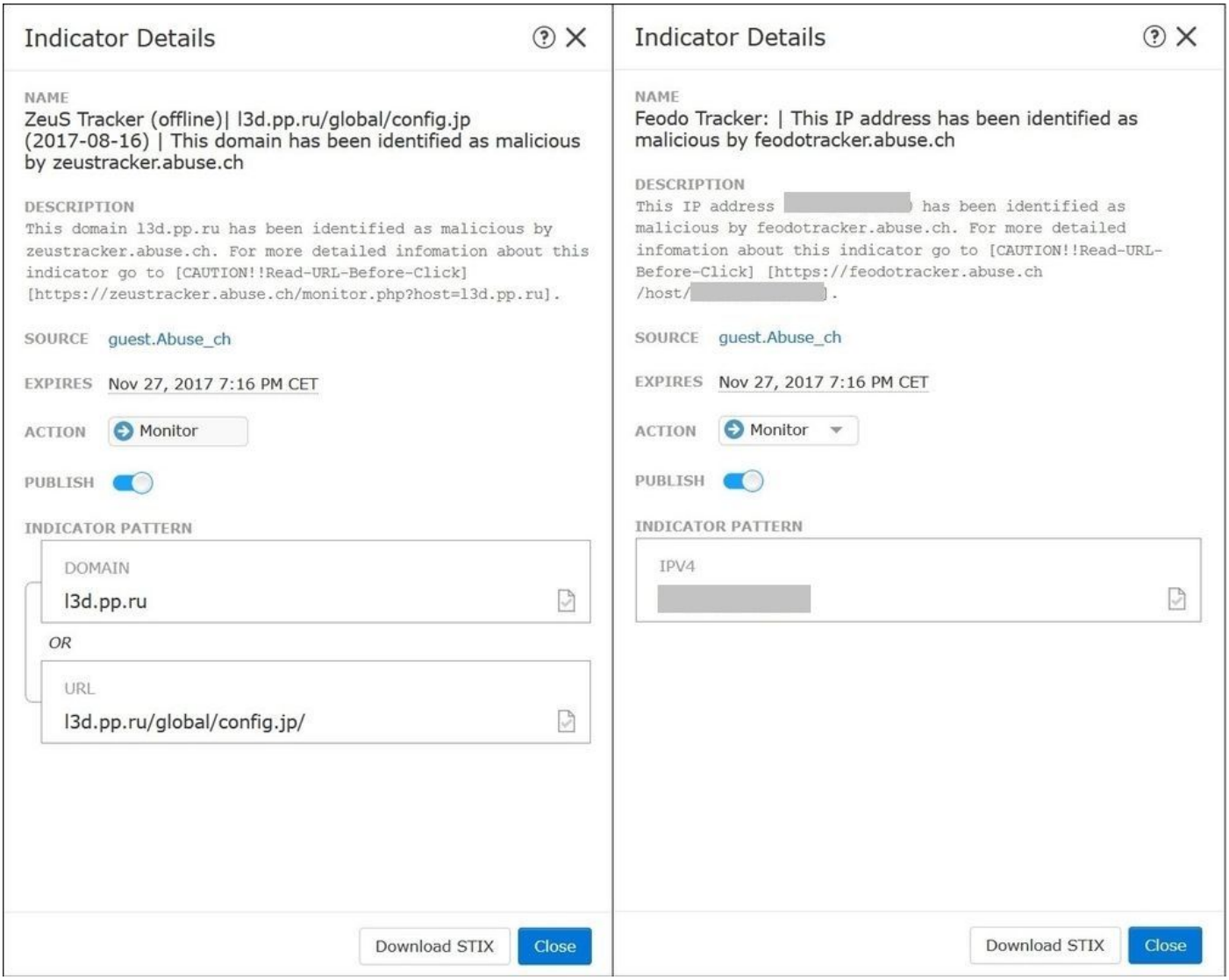
Note: Par défaut, toutes les sources sont publiées, ce qui signifie qu'elles sont transmises aux capteurs. Ce processus peut prendre jusqu'à 20 minutes ou plus.

Étape 3. Sous l'onglet Indicateur, vous pouvez confirmer si les indicateurs ont été téléchargés à partir des sources configurées :

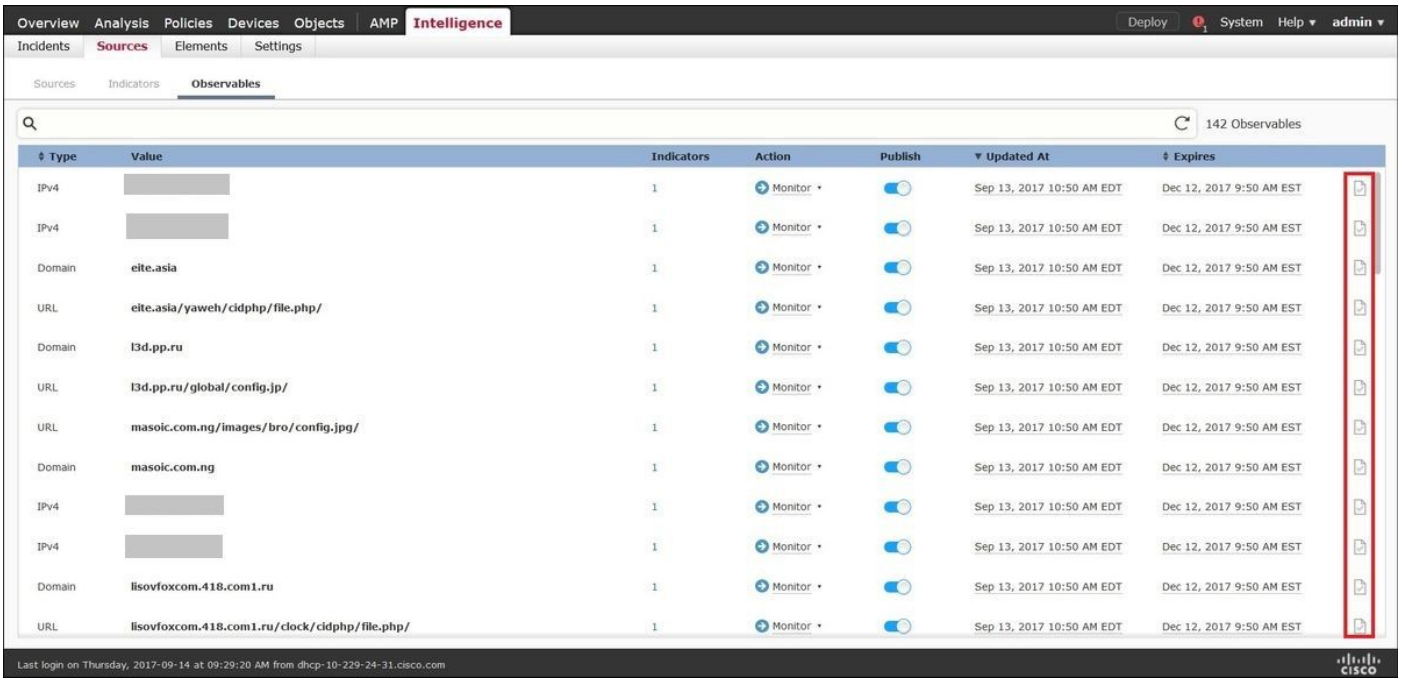


Étape 4. Une fois que vous avez sélectionné le nom d'un indicateur, vous pouvez en voir plus. En outre, vous pouvez décider si vous voulez le publier sur le capteur ou si vous voulez modifier l'action (en cas d'indicateur simple).

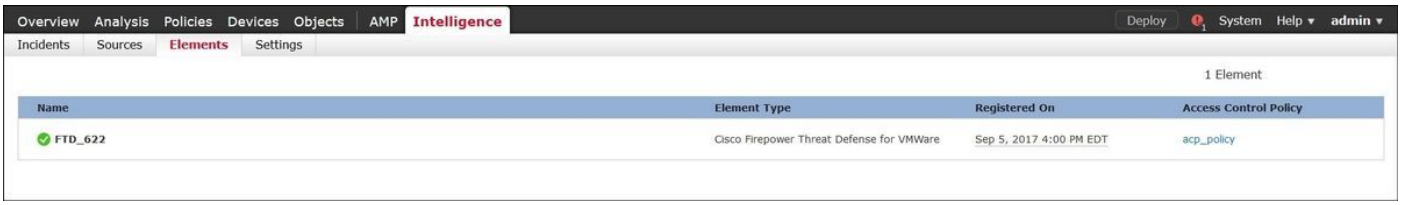
Comme l'illustre l'image, un indicateur complexe est répertorié avec deux observables connectés par l'opérateur OR :



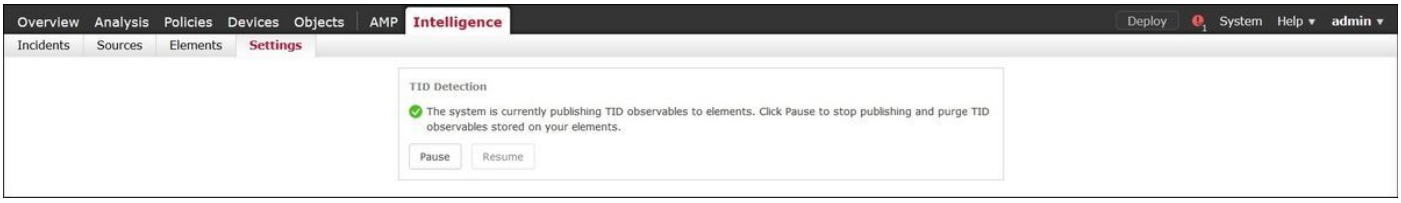
Étape 5. Accédez à l'onglet Observables dans lequel vous trouverez les URL, les adresses IP, les domaines et SHA256 inclus dans les indicateurs. Vous pouvez choisir les observables que vous souhaitez transmettre aux capteurs et éventuellement modifier l'action pour eux. Dans la dernière colonne, un bouton de liste blanche équivaut à une option de publication/non publication.



Étape 6. Accédez à l'onglet Éléments afin de vérifier la liste des périphériques sur lesquels TID est activé.

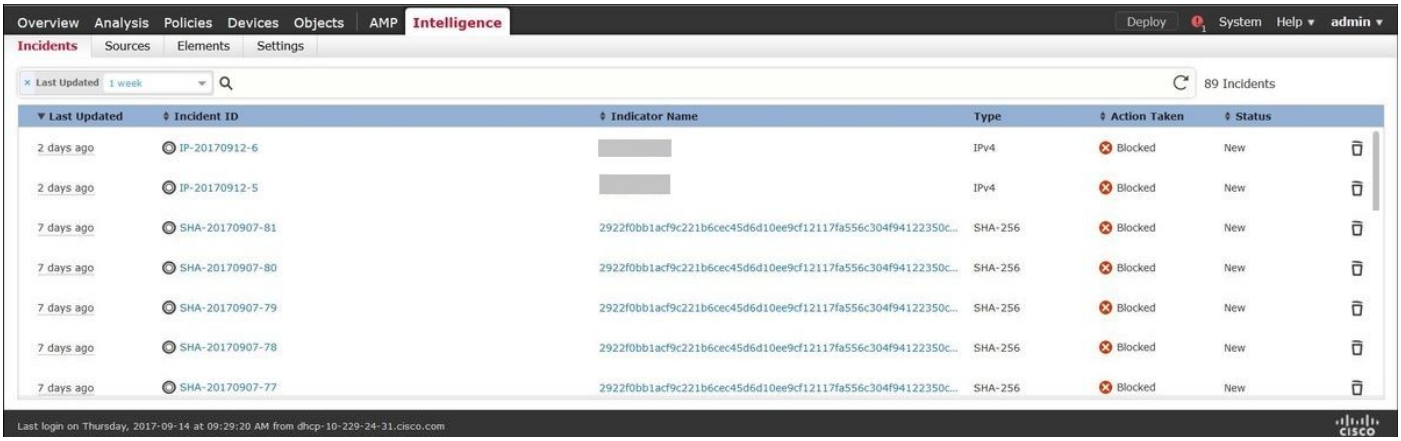


Étape 7 (Facultatif) Accédez à l'onglet Paramètres et sélectionnez le bouton Suspendre afin d'arrêter de pousser les indicateurs vers les capteurs. Cette opération peut prendre jusqu'à 20 minutes.

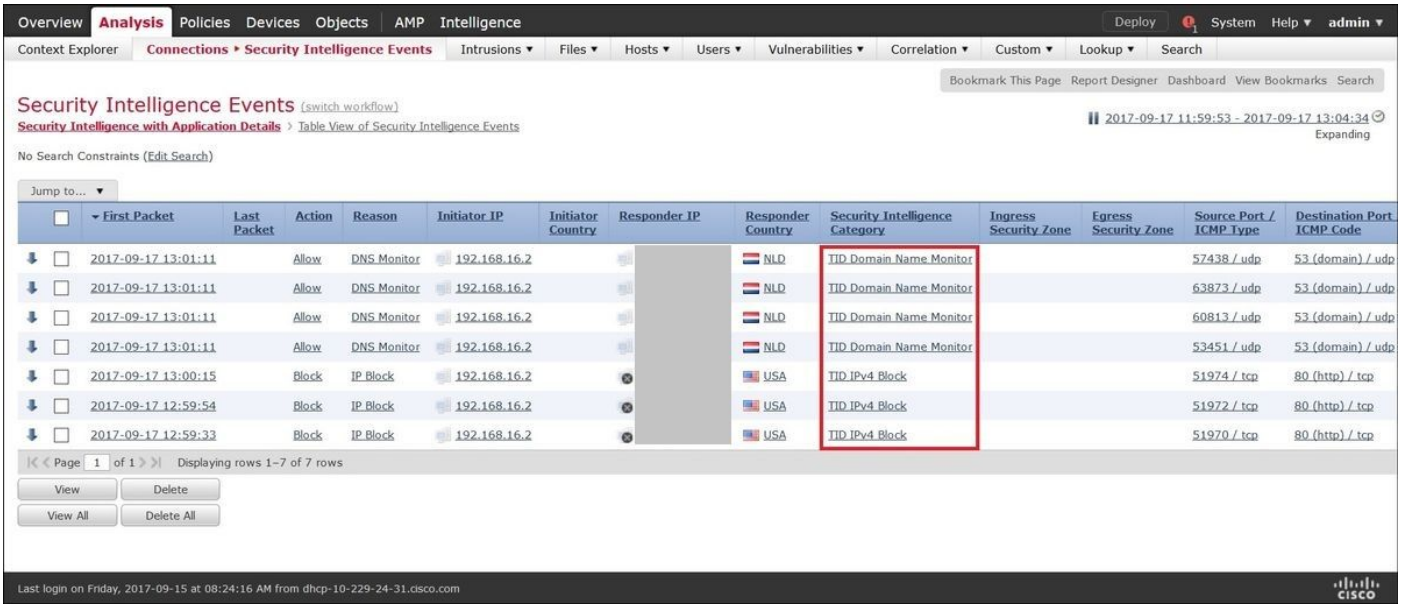


Vérification

Méthode 1. Afin de vérifier si TID a effectué une action sur le trafic, vous devez accéder à l'onglet Incidents.



Méthode 2. Les incidents se trouvent sous l'onglet Security Intelligence Events sous une balise TID.



Note: TID a une capacité de stockage de 1 million d'incidents.

Méthode 3. Vous pouvez confirmer si des sources (flux) configurées sont présentes sur le FMC et un capteur. Pour ce faire, vous pouvez accéder à ces emplacements sur l'interface de ligne de commande :

/var/sf/siurl_download/

/var/sf/sidns_download/

/var/sf/iprep_download/

Un nouveau répertoire a été créé pour les flux 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.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
```

Note: TID est activé uniquement sur le canal global sur le FMC

Note: Si vous hébergez TID sur le Firepower Management Center actif dans une configuration à haute disponibilité (appliances FMC physiques), le système ne synchronise pas les configurations TID et les données TID vers le Firepower Management Center de secours.

Dépannage

Il y a un processus de haut niveau qui s'appelle **tid**. Ce processus dépend de trois processus : **mongo**, **RabbitMQ**, **redis**. Afin de vérifier les processus exécuter **pmtool status | grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "** commande.

```
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#
```

Afin de vérifier en temps réel quelle action est effectuée, vous pouvez exécuter la commande **support du système firewall-engine-debug** ou **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
```

Il existe deux possibilités en termes d'action :

- **URL SI : Ordre de règle correspondant 19, Id 19, si id de liste 1074790455, action 4** - le trafic a été bloqué
- **URL SI : Ordre de règle correspondant 20, Id 20, si id de liste 1074790456, action 6** - le trafic a été surveillé.