Cisco Threat Intelligence Director 구성 및 문제 해결

목차

소개

이 문서에서는 Cisco TID(Threat Intelligence Director)를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(Firepower Management Center) 관리

Cisco Threat Intelligence Director 기능을 구성하기 전에 다음 조건을 확인해야 합니다.

- FMC(Firepower Management Center): 6.2.2 이상 버전에서 실행해야 합니다(물리적 또는 가상 FMC에서 호스팅할 수 있음).최소 15GB의 RAM 메모리를 사용하여 구성해야 합니다.REST API 액세스를 사용하도록 설정해야 합니다.
- 센서는 6.2.2 버전 이상을 실행해야 합니다.
- 액세스 제어 정책 옵션의 Advanced Settings(고급 설정) 탭에서 **Enable Threat Intelligence Director**를 활성화해야 합니다.
- 규칙이 아직 없는 경우 액세스 제어 정책에 규칙을 추가합니다.
- SHA-256 관찰자가 관찰 및 Firepower Management Center 이벤트를 생성하도록 하려면 하나 이상의 **Malware Cloud Lookup** 또는 **Block Malware** 파일 규칙을 만들고 파일 정책을 액세스 제어 정책의 하나 이상의 규칙과 연결합니다.
- IPv4, IPv6, URL 또는 도메인 이름 관측에서 연결 및 보안 인텔리전스 이벤트를 생성하도록 하려면 액세스 제어 정책에서 연결 및 보안 인텔리전스 로깅을 활성화합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

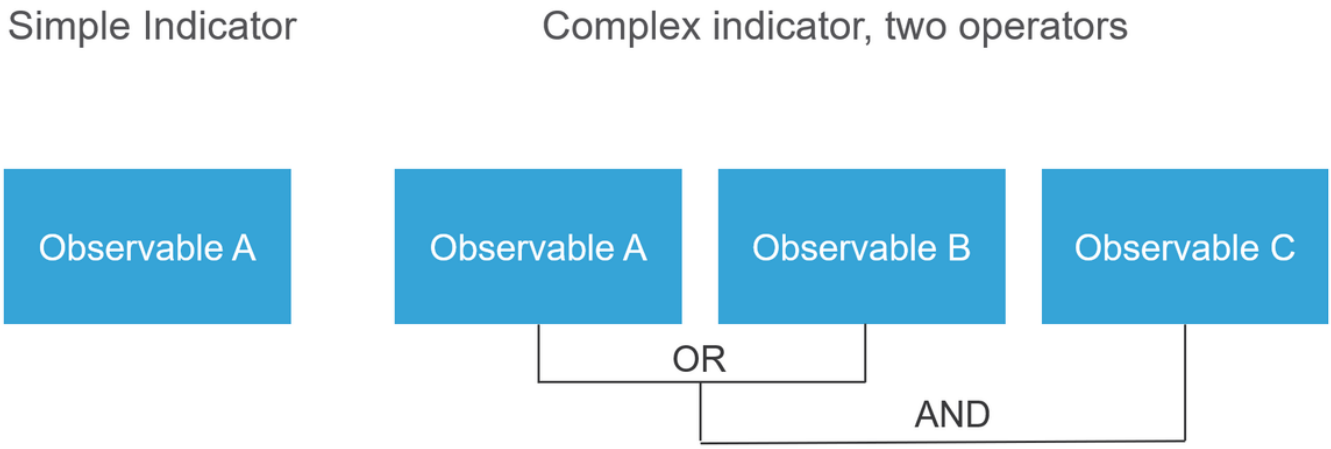
- Cisco FTD(Firepower Threat Defense) Virtual은 6.2.2.81
- 6.2.2.81을 실행하는 vFMC(Firepower Management Center Virtual)

참고:이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

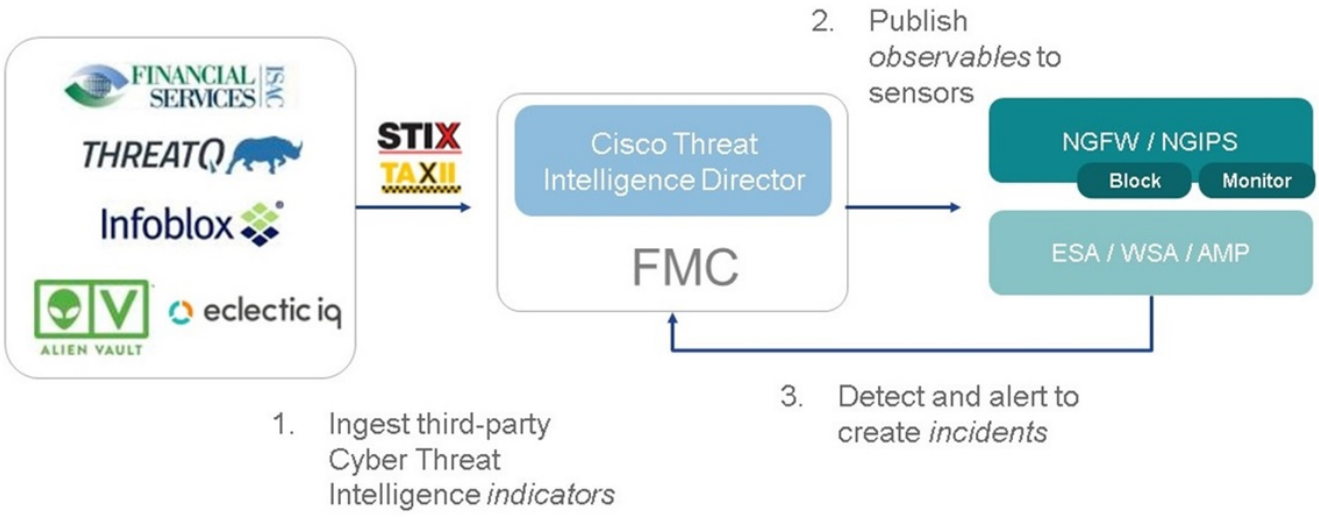
Cisco TID(Threat Intelligence Director)는 위협 인텔리전스 정보를 운영하는 시스템입니다.이 시스템은 이기종 타사 사이버 위협 인텔리전스를 사용 및 표준화하고, 인텔리전스를 탐지 기술에 게시하며, 탐지 기술로부터 관찰의 상관성을 분석합니다.

세 가지 새로운 용어가 있습니다.**관찰 가능**, **지표** 및 **사고**.관찰 가능 한 변수는 URL, 도메인, IP 주소 또는 SHA256과 같은 변수입니다. 지표들은 관찰 가능 요소로 이루어집니다.두 가지 유형의 지표가 있습니다.단순 표시기는 관찰이 가능한 항목을 하나만 포함합니다.복합 표시기의 경우, AND 및 OR와 같은 논리적 함수를 사용하여 서로 연결되는 관찰이 가능한 두 개 이상의 항목이 있습니다.시스템이 FMC에서 차단하거나 모니터링해야 하는 트래픽을 탐지하면 인시던트가 나타납니다.



작동 방식

이미지에 표시된 대로 FMC에서 위협 인텔리전스 정보를 다운로드할 소스를 구성해야 합니다.그런 다음 FMC는 해당 정보(관찰 가능 항목)를 센서에 푸시합니다.트래픽이 관찰 가능 요소와 일치하면 FMC GUI(사용자 인터페이스)에 인시던트가 나타납니다.



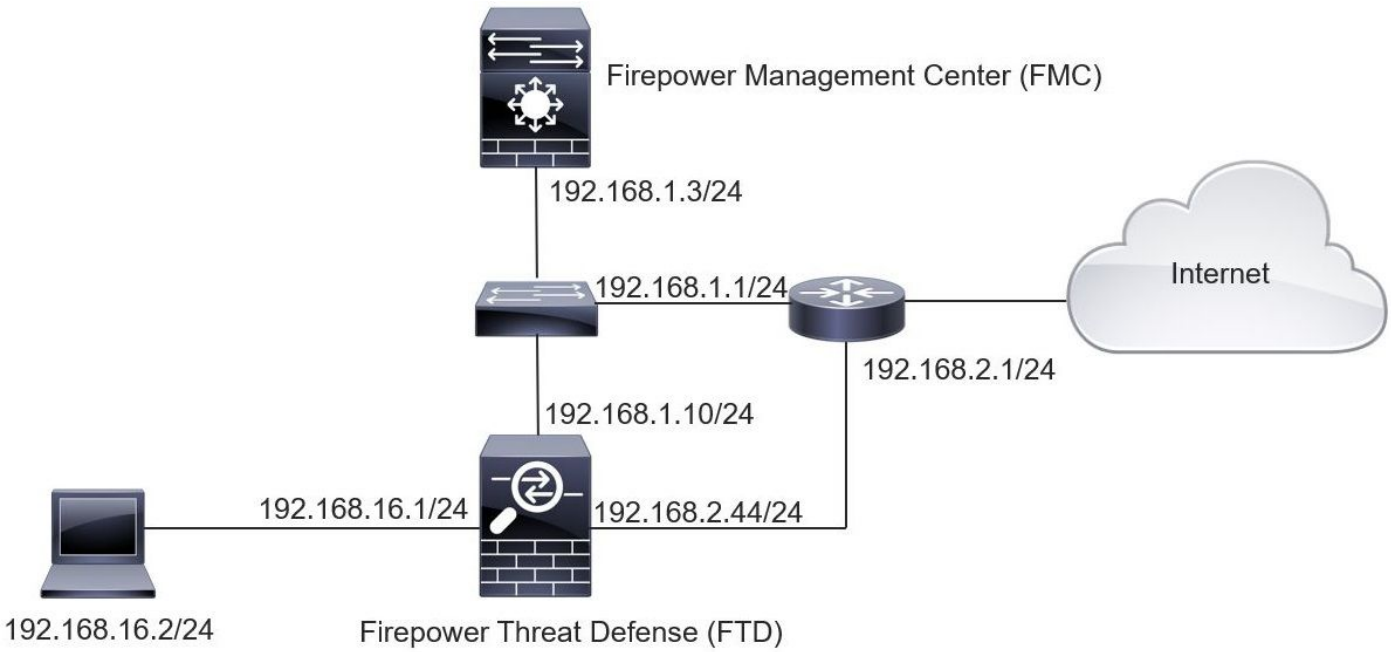
두 가지 새로운 용어가 있습니다.

- STIX(Structured Threat Intelligence eXpression)는 위협 인텔리전스 정보를 공유하고 사용하는 표준입니다.세 가지 주요 기능 요소가 있습니다.지표, 관찰 가능 항목 및 사고
- TAXII(Trusted Automated EXchange of Indicator Information)는 위협 정보에 대한 전송 메커니즘입니다.

구성

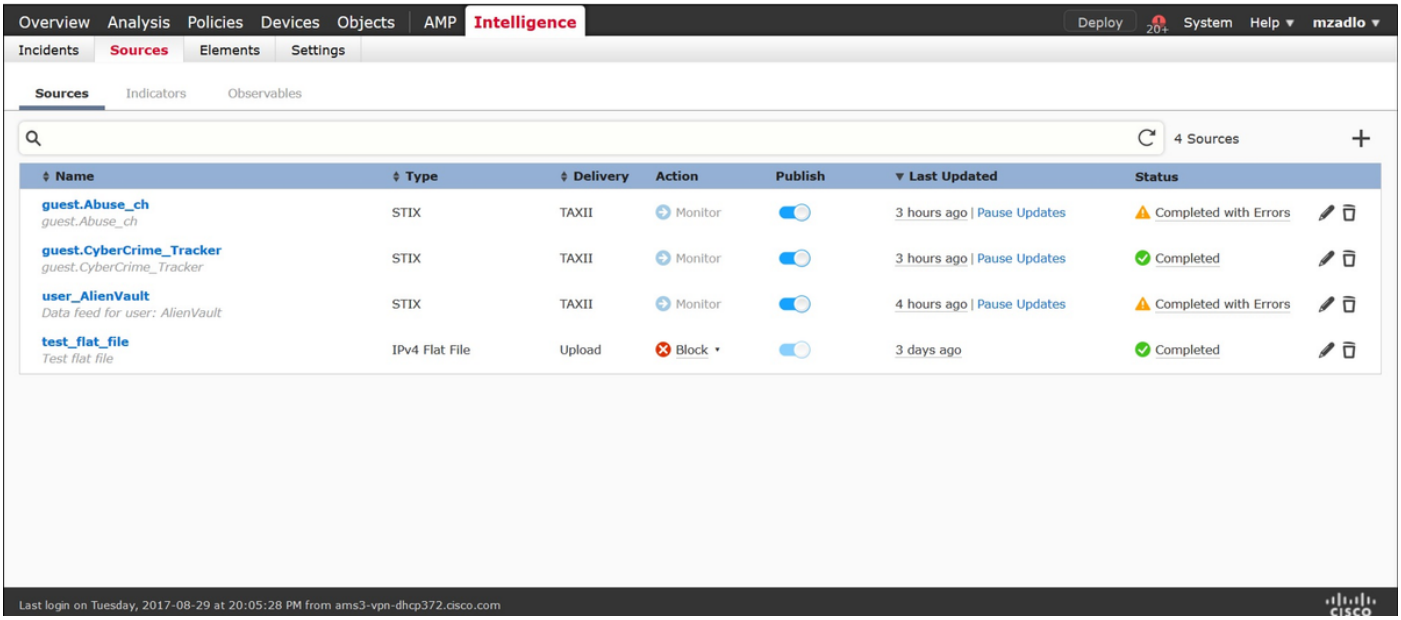
구성을 완료하려면 다음 섹션을 고려하십시오.

네트워크 다이어그램



구성

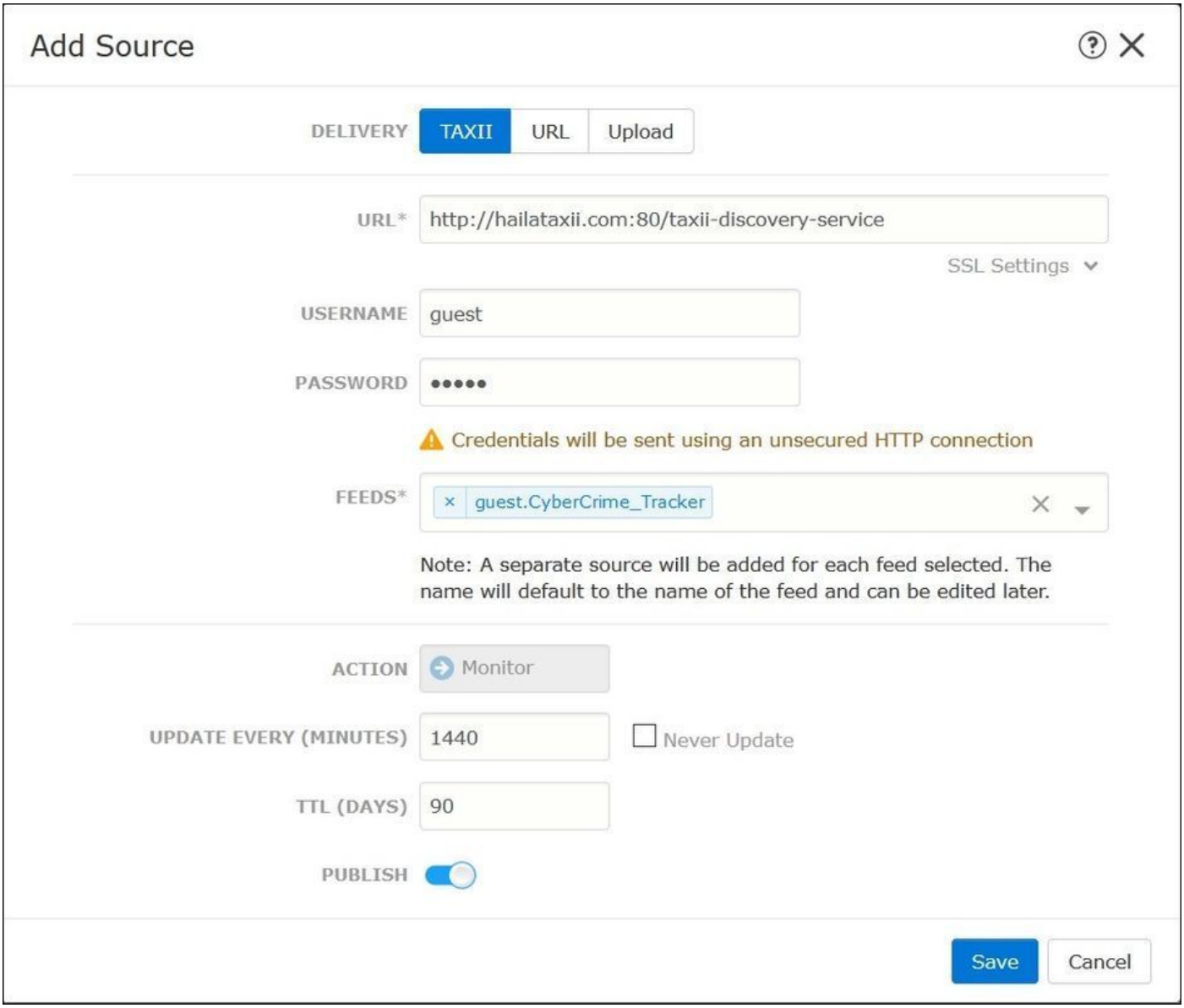
1단계. TID를 구성하려면 이미지에 표시된 대로 **Intelligence** 탭으로 이동해야 합니다.



참고:피드에 지원되지 않는 관찰 항목이 포함되어 있는 경우 'Completed with Errors' 상태가 필요합니다.

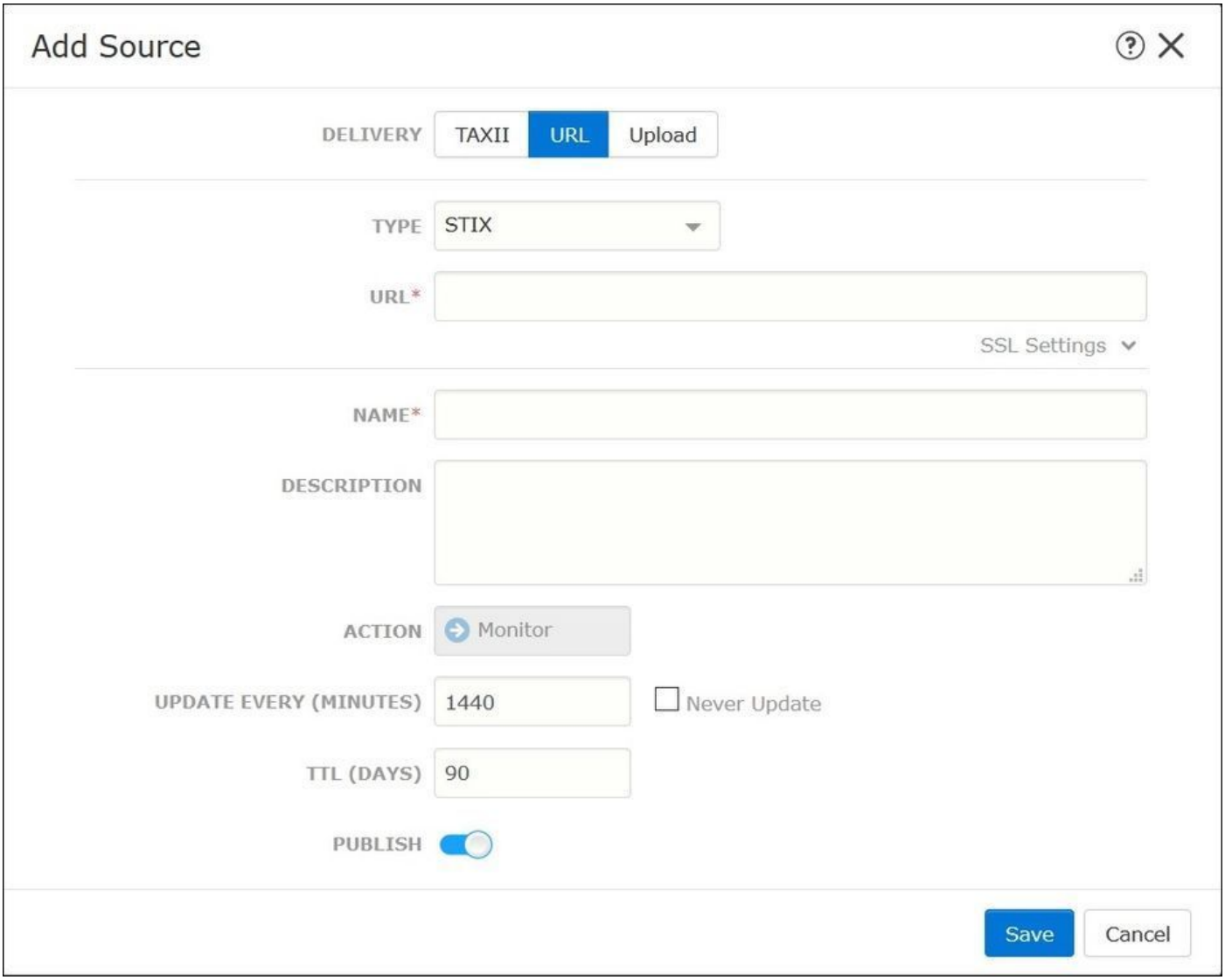
2단계. 위협의 소스를 추가해야 합니다.소스를 추가하는 방법은 세 가지가 있습니다.

- TAXII - 이 옵션을 사용하면 위협 정보가 STIX 형식으로 저장되는 서버를 구성할 수 있습니다

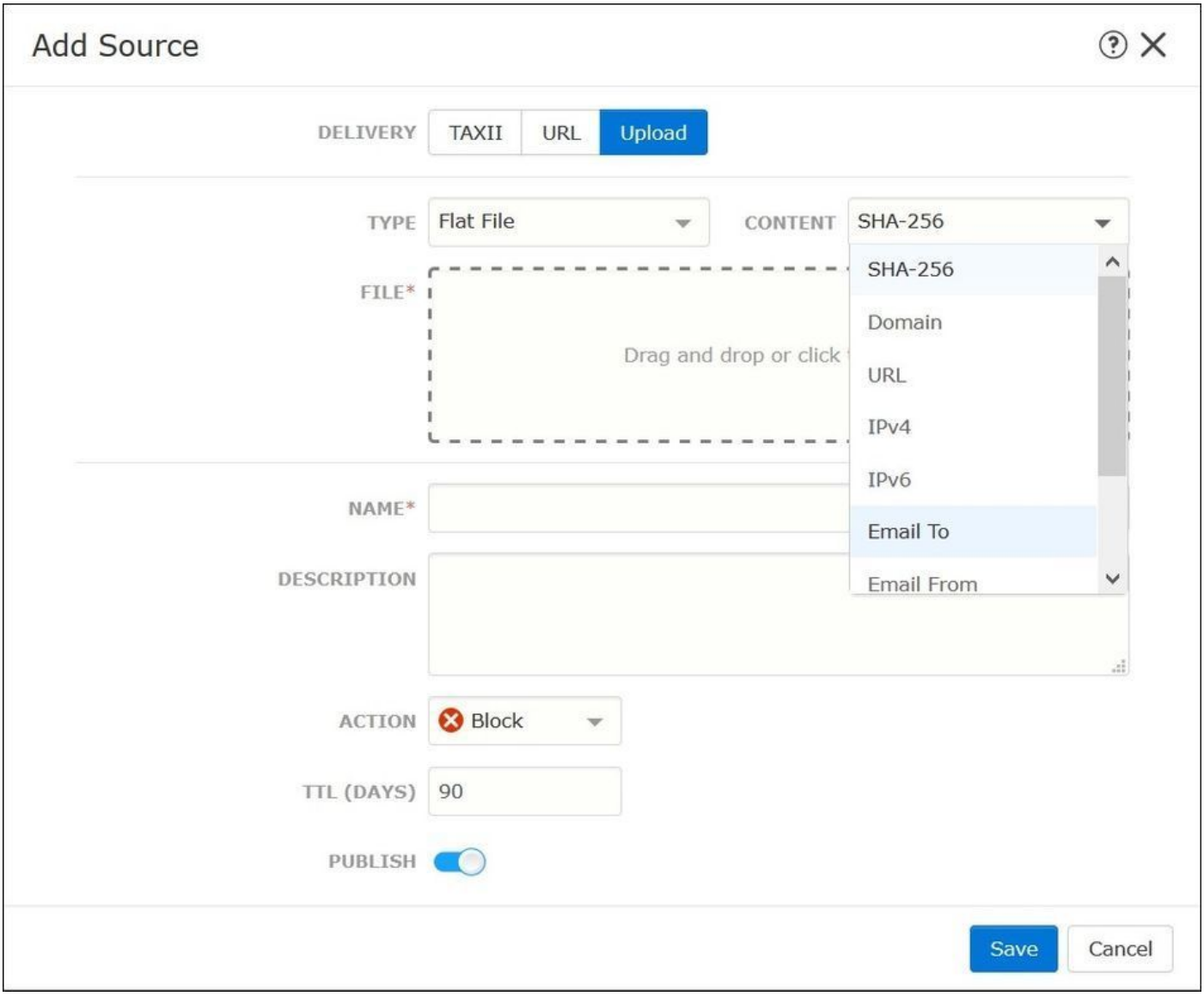


참고:사용 가능한 유일한 작업은 모니터입니다.STIX 형식의 위협에 대한 차단 작업은 구성할 수 없습니다.

- URL - STIX 위협 또는 플랫 파일이 있는 HTTP/HTTPS 로컬 서버에 대한 링크를 구성할 수 있습니다.

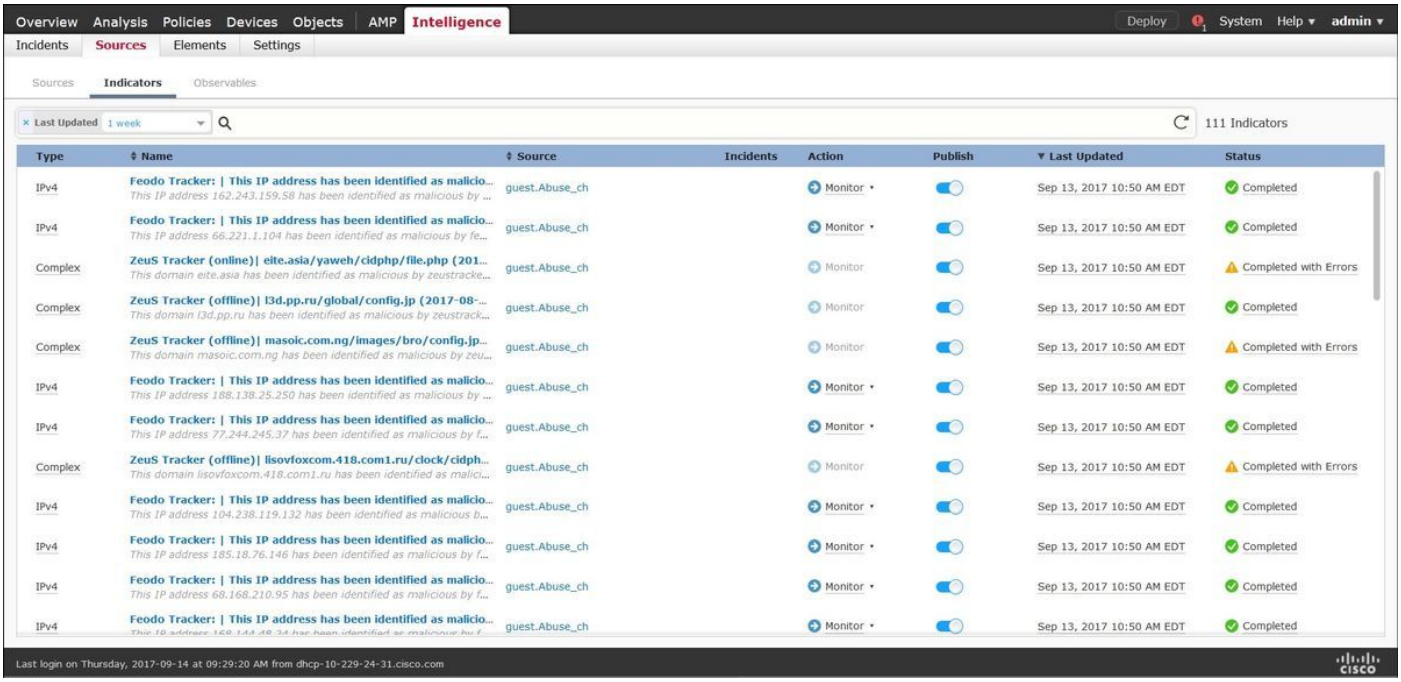


- 플랫 파일 - 파일을 ***.txt** 형식으로 업로드할 수 있으며 파일의 내용을 지정해야 합니다.파일에는 한 줄에 하나의 콘텐츠 항목이 포함되어야 합니다.



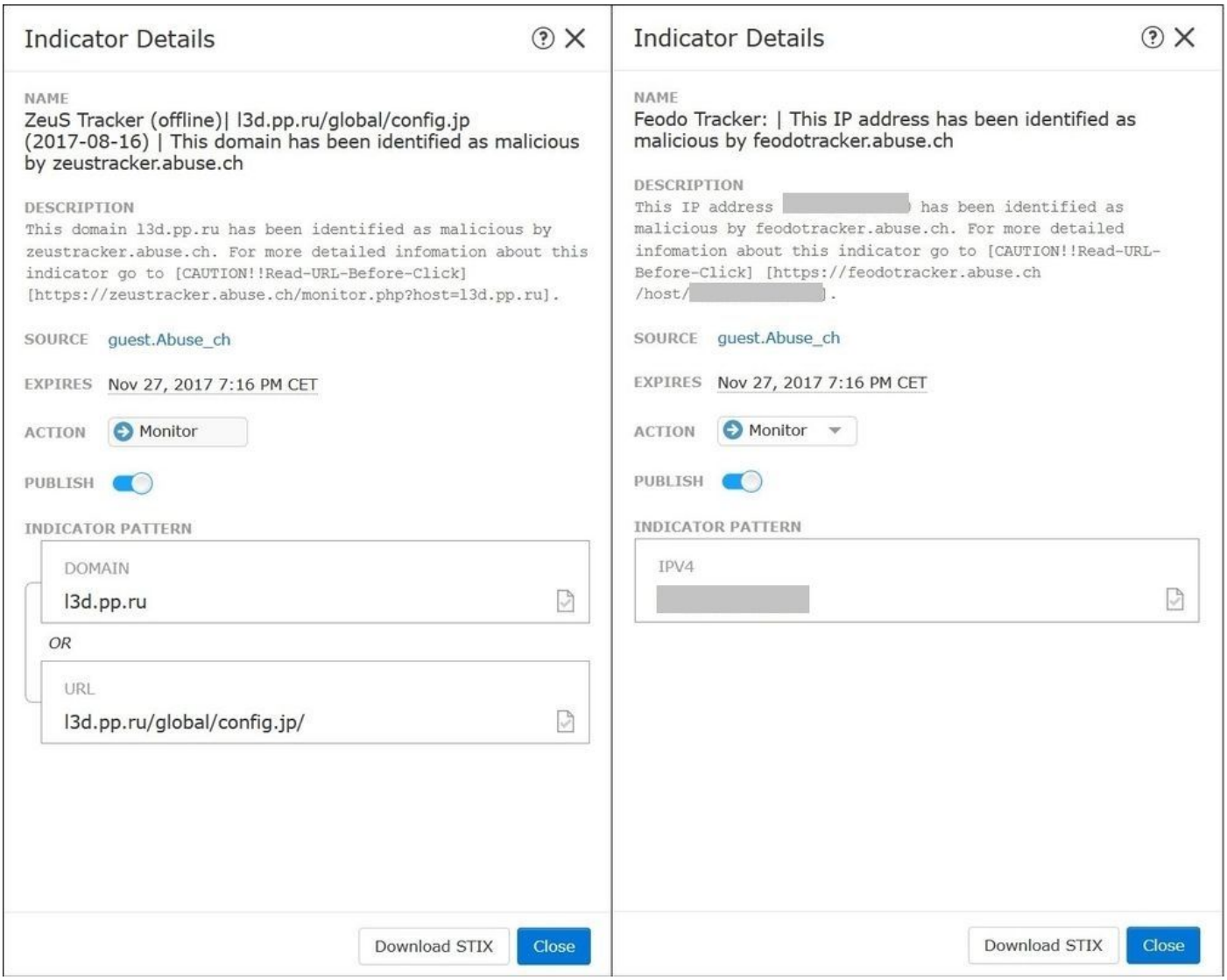
참고:기본적으로 모든 소스가 게시됩니다. 즉 센서에 푸시됩니다.이 프로세스는 최대 20분 이상 걸릴 수 있습니다.

3단계. Indicator(지표) 탭에서 구성된 소스에서 지표가 다운로드되었는지 확인할 수 있습니다.

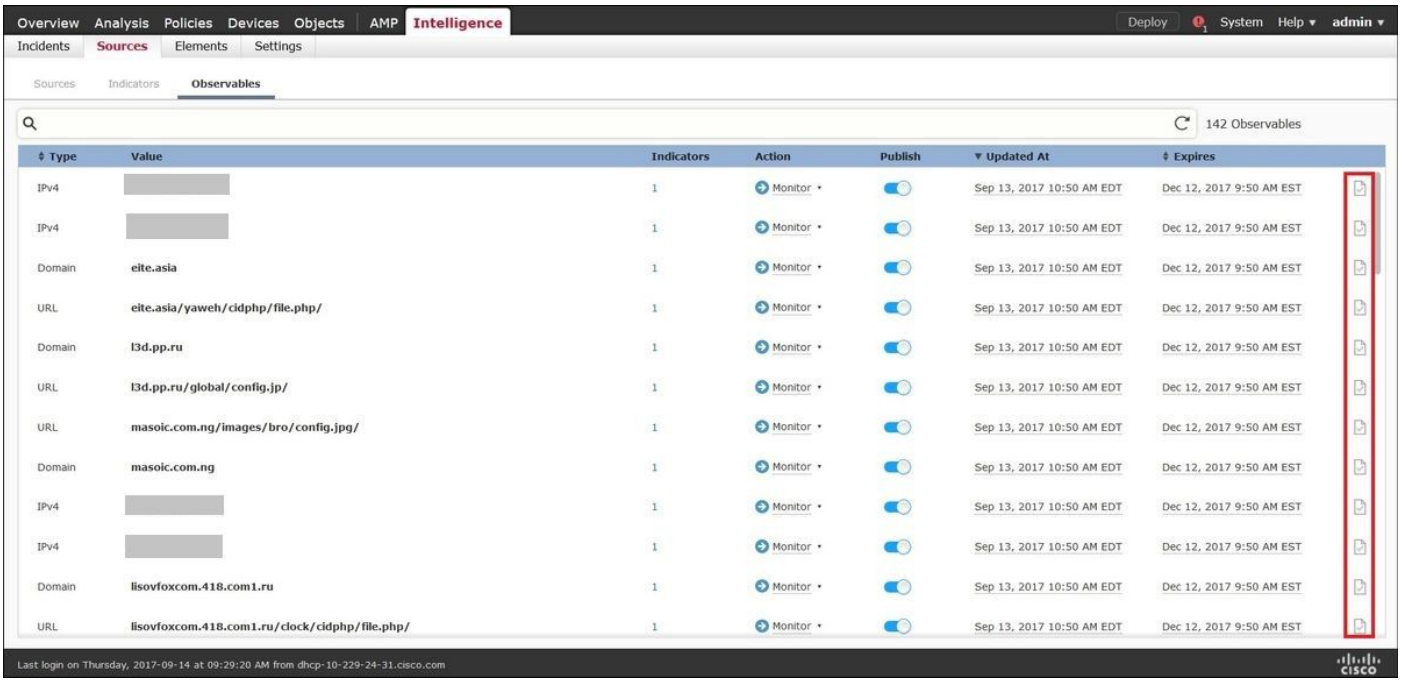


4단계. 표시기의 이름을 선택하면 자세한 정보를 볼 수 있습니다.또한 센서에 게시할 것인지 또는 동작을 변경할 것인지(단순 표시기의 경우) 결정할 수 있습니다.

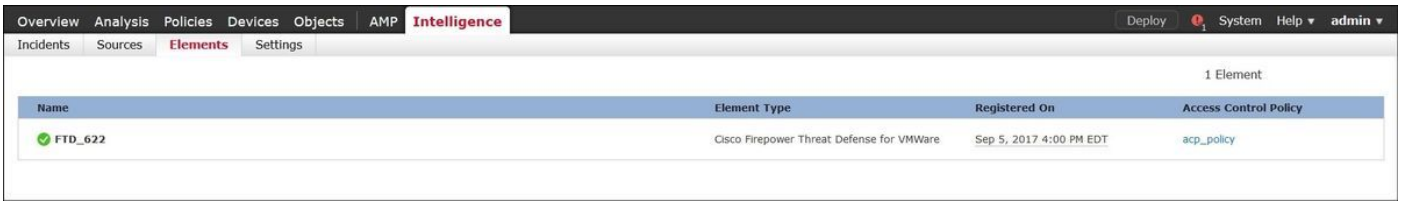
이미지에 표시된 대로 복합 표시기는 OR 연산자로 연결된 두 개의 관찰 가능 요소로 나열됩니다.



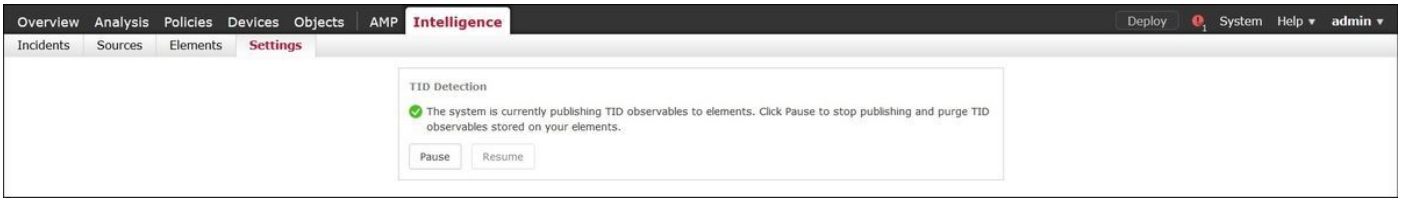
5단계. 지표에 포함된 URL, IP 주소, 도메인 및 SHA256을 찾을 수 있는 Observables 탭으로 이동합니다.센서에 푸시할 관찰 가능 장치를 결정하고 선택적으로 센서에 대한 작업을 변경할 수 있습니다.마지막 열에는 게시/게시 안 함 옵션과 같은 화이트리스트 단추가 있습니다.



6단계. Elements(요소) 탭으로 이동하여 TID가 활성화된 디바이스 목록을 확인합니다.

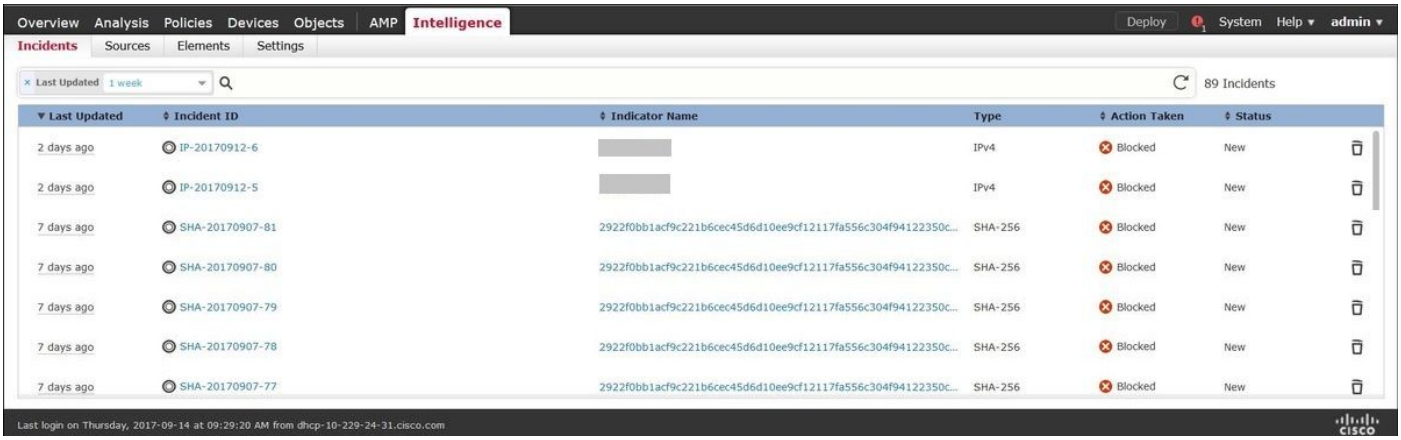


7단계(선택 사항). 센서를 센서로 푸시하지 않으려면 Settings(설정) 탭으로 이동하고 Pause(일시 중지) 버튼을 선택합니다.이 작업은 최대 20분 정도 걸릴 수 있습니다.

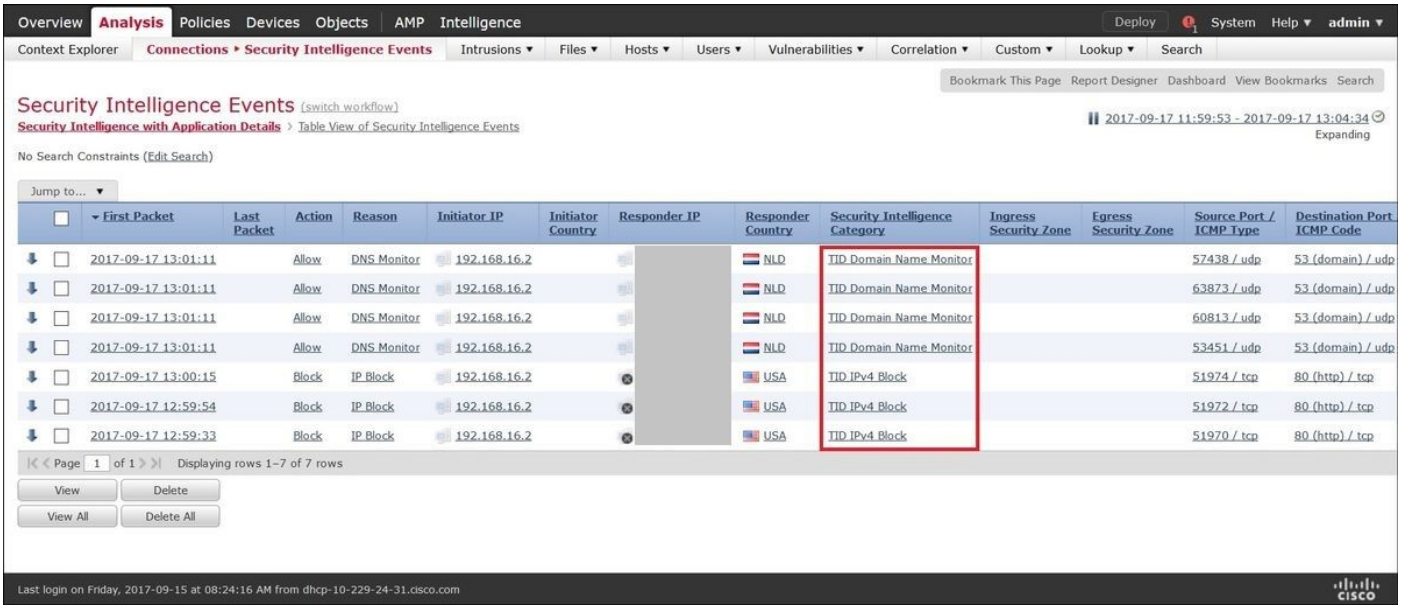


다음을 확인합니다.

방법 1. TID에서 트래픽에 대한 작업을 수행했는지 확인하려면 Incidents(인시던트) 탭으로 이동해야 합니다.



방법 2. 인시던트는 Security Intelligence Events(보안 인텔리전스 이벤트) 탭의 TID 태그 아래에서 찾을 수 있습니다.



참고:TID는 100만 개의 인시던트를 저장할 수 있습니다.

방법 3. 구성된 소스(피드)가 FMC 및 센서에 있는지 확인할 수 있습니다.이를 위해 CLI에서 다음 위치로 이동할 수 있습니다.

/var/sf/siurl_download/

/var/sf/sidns_download/

/var/sf/iprep_download/

SHA256 피드에 대해 생성된 새 디렉토리가 있습니다./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
```

참고:TID는 FMC의 전역 도메인에서만 활성화됩니다.

참고:고가용성 컨피그레이션(물리적 FMC 어플라이언스)에서 활성 Firepower Management Center에서 TID를 호스트하는 경우, 시스템은 TID 컨피그레이션 및 TID 데이터를 대기 Firepower Management Center에 동기화하지 않습니다.

문제 해결

tid라는 최상위 프로세스가 있습니다.이 프로세스는 다음 세 가지 프로세스에 따라 달라집니다.**몬고** , **RabbitMQ**, **Redis**.프로세스 실행 pmtool **상태**를 확인하기 위해 **| grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "** 명령

```
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#
```

어떤 작업이 수행되는지 실시간으로 확인하기 위해 **system support firewall-engine-debug** 또는 **system support trace** 명령**을** 실행할 수 있습니다.

```
> 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
```

실행 측면에는 두 가지 가능성이 있습니다.

- **URL SI:일치하는 규칙 순서 19, ID 19, si list id 1074790455, 작업 4** - 트래픽이 차단됨
- **URL SI:일치하는 규칙 순서 20, Id 20, si list id 1074790456, action 6** - 트래픽이 모니터링되었습니다.