配置Cisco Threat Intelligence Director并排除故障

目录

简介

本文档介绍如何配置和排除思科威胁情报导向器(TID)故障。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower管理中心(FMC)管理

在配置Cisco Threat Intelligence Director功能之前，您需要确保以下条件：

- Firepower管理中心(FMC): 必须在6.2.2版（或更高版本）上运行（可托管于物理或虚拟FMC上）。必须配置至少15 GB的RAM内存。必须配置REST API访问已启用。
- 传感器必须运行6.2.2版（或更高版本）。
- 在访问控制策略选项的Advanced Settings选项卡中，**必须启用**Enable Threat Intelligence Director。
- 如果规则尚未存在，请将其添加到访问控制策略。
- 如果希望SHA-256可观察项生成观察结果和Firepower管理中心事件，请创建一个或多个**恶意软件云查找**或**阻止恶意软件**文件规则，并将文件策略与访问控制策略中的一个或多个规则相关联。
- 如果希望IPv4、IPv6、URL或域名观察生成连接和安全情报事件，请在访问控制策略中启用连接和安全情报日志记录。

使用的组件

本文档中的信息基于以下软件版本：

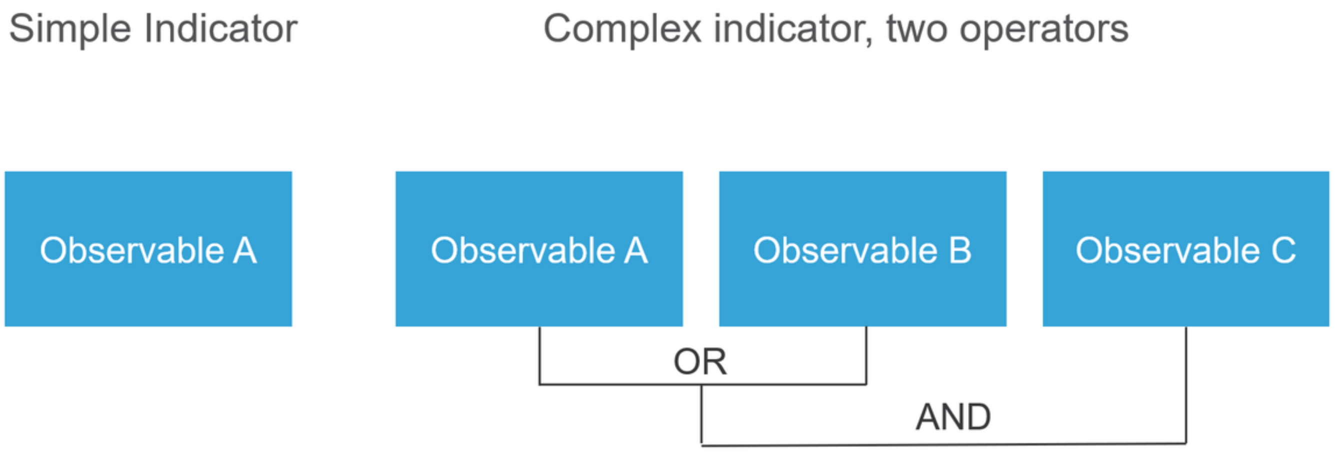
- 运行6.2.2.81的思科Firepower威胁防御(FTD)虚拟
- 运行6.2.2.81的Firepower管理中心虚拟(vFMC)

注意：本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

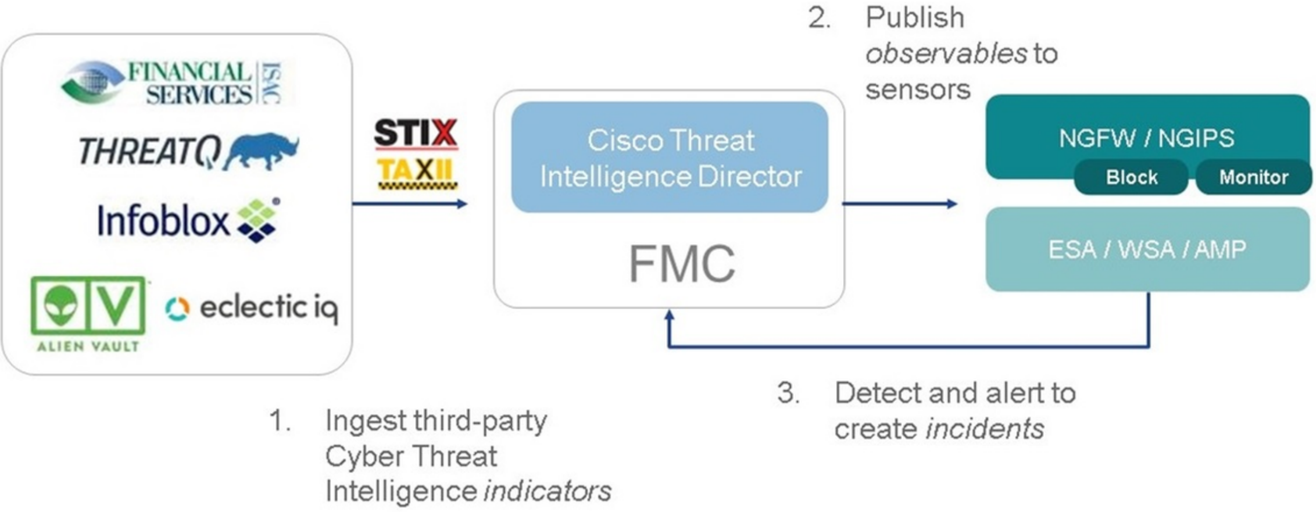
思科威胁情报导向器(TID)是可操作威胁情报信息的系统。系统消耗并规范异类第三方网络威胁情报，将情报发布到检测技术，并关联来自检测技术的观察结果。

有三个新术语：**可观察**量、**指标**和事**故**。可观察只是变量，例如URL、域、IP地址或SHA256。指示器由可观察项组成。有两种类型的指示器。简单指示器只包含一个可观察的。在复杂指示器的情况下，有两个或多个可观察的，它们使用逻辑函数（如AND和OR）彼此连接。一旦系统检测到应在FMC上阻止或监控的流量，就会出现事故。



此计划如何运作？

如图所示，在FMC上，您必须配置源，从中下载威胁情报信息。然后，FMC将该信息（可观察信息）推送到传感器。当流量与可观察项匹配时，事故将显示在FMC用户界面(GUI)中。


FINANCIAL SERVICES ISAC
THREATQ
Infoblox
ALIEN VAULT
eclectic iq
STIX
TAXII
Cisco Threat Intelligence Director
FMC
2. Publish *observables* to sensors
NGFW / NGIPS
Block
Monitor
ESA / WSA / AMP
3. Detect and alert to create *incidents*
1. Ingest third-party Cyber Threat Intelligence *indicators*

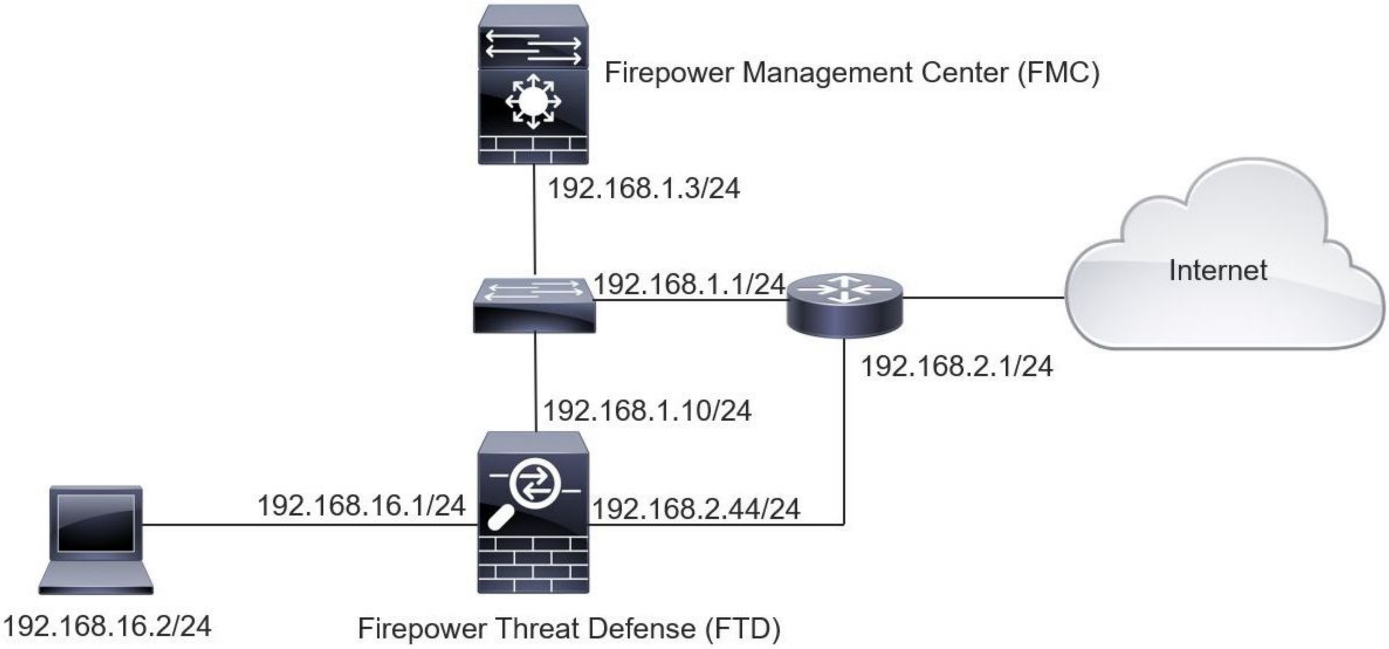
有两个新术语：

- STIX（结构化威胁情报表达式）是共享和使用威胁情报信息的标准。有三个关键功能要素：指标、可观察项和事故
- TAXII（可信自动交换指标信息）是威胁信息的传输机制

配置

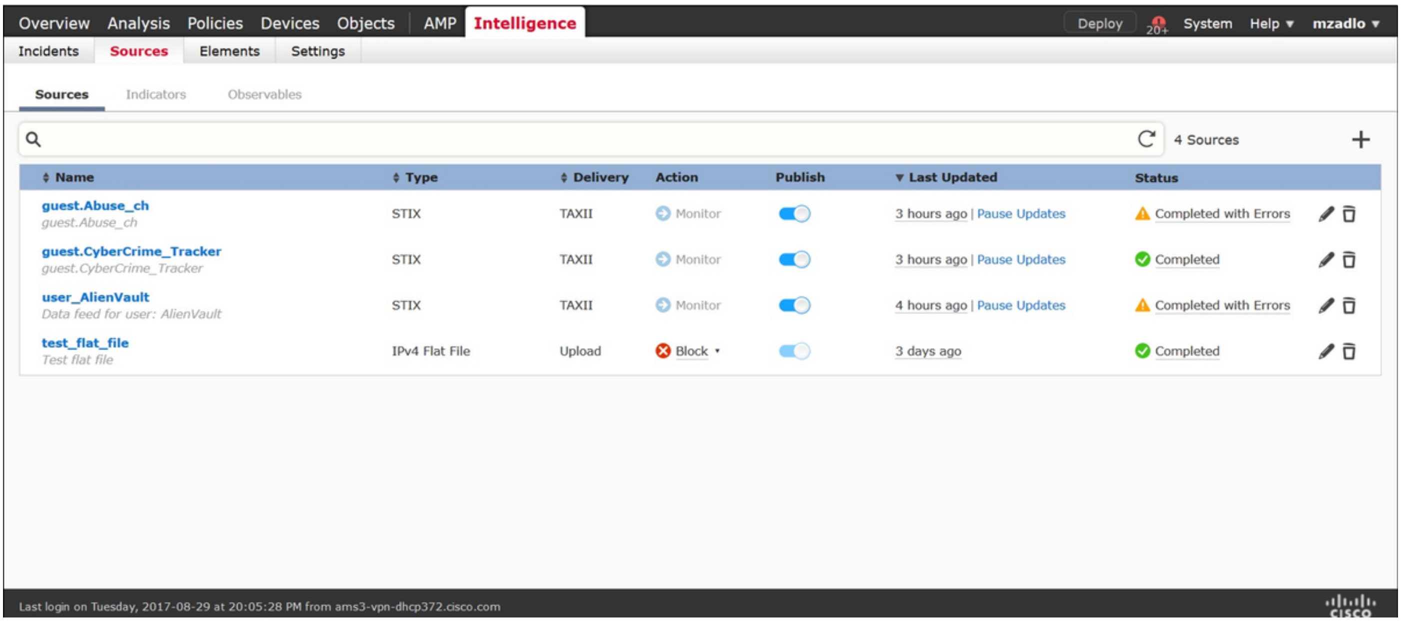
要完成配置，请考虑以下部分：

网络图



配置

步骤1.要配置TID，您必须导航至**Intelligence**选项卡，如图所示。



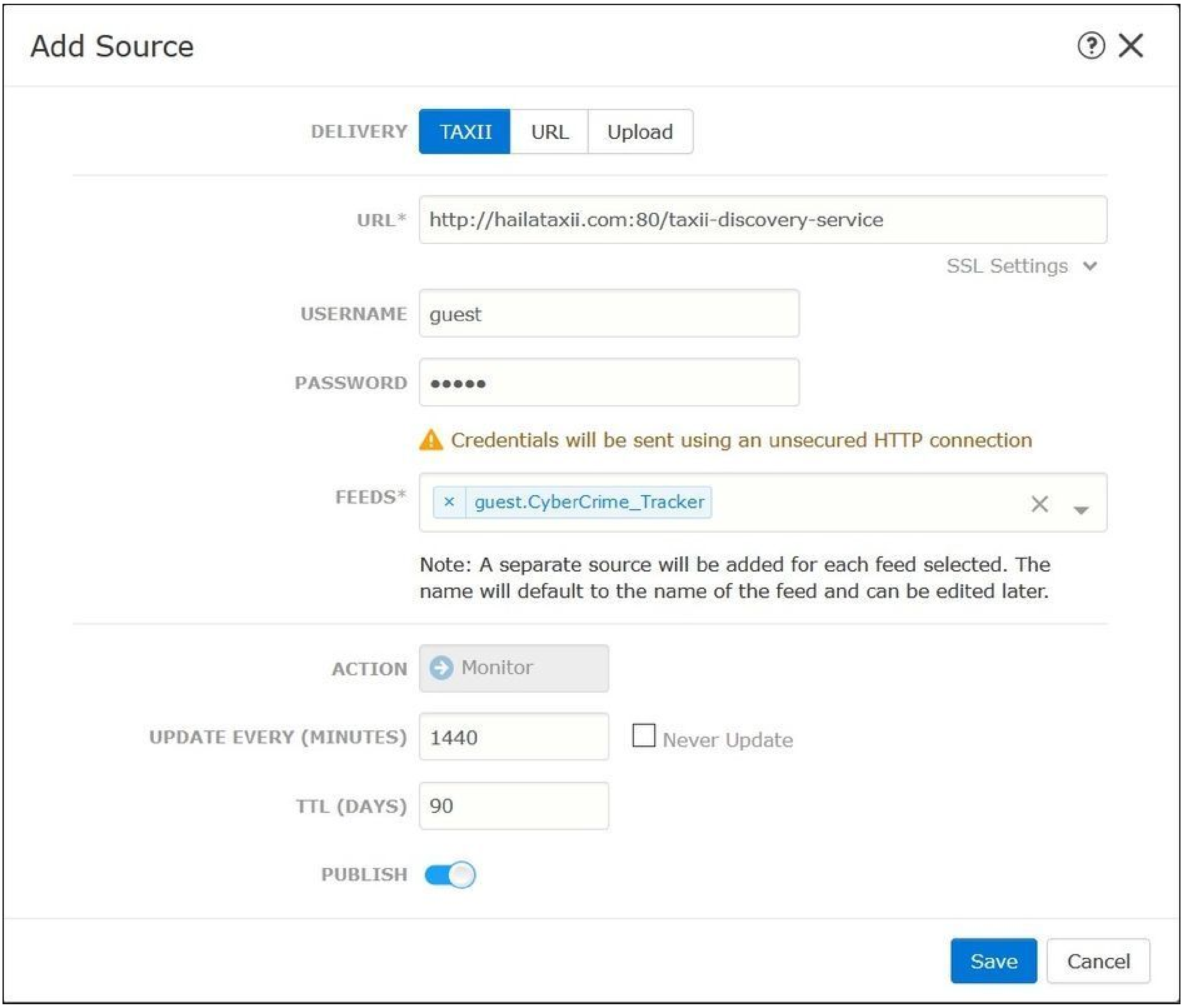
Name	Type	Delivery	Action	Publish	Last Updated	Status
guest.Abuse_ch *guest.Abuse_ch*	STIX	TAXII	Monitor	●	3 hours ago | Pause Updates	⚠ Completed with Errors
guest.CyberCrime_Tracker *guest.CyberCrime_Tracker*	STIX	TAXII	Monitor	●	3 hours ago | Pause Updates	✓ Completed
user_AlienVault *Data feed for user: AlienVault*	STIX	TAXII	Monitor	●	4 hours ago | Pause Updates	⚠ Completed with Errors
test_flat_file *Test flat file*	IPv4 Flat File	Upload	✕ Block ▾	●	3 days ago	✓ Completed

Last login on Tuesday, 2017-08-29 at 20:05:28 PM from ams3-vpn-dhcp372.cisco.com

注意：如果源包含不受支持的可观察项，则状态应为“已完成，但出现错误”。

步骤2.您必须添加威胁源。添加源有三种方法：

- TAXII — 使用此选项时，可以配置以STIX格式存储威胁信息的服务器



Add Source

DELIVERY: TAXII | URL | Upload

URL*: http://hailataxii.com:80/taxii-discovery-service

SSL Settings

USERNAME: guest

PASSWORD: •••••

⚠ Credentials will be sent using an unsecured HTTP connection

FEEDS*: × guest.CyberCrime_Tracker

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: Monitor

UPDATE EVERY (MINUTES): 1440 □ Never Update

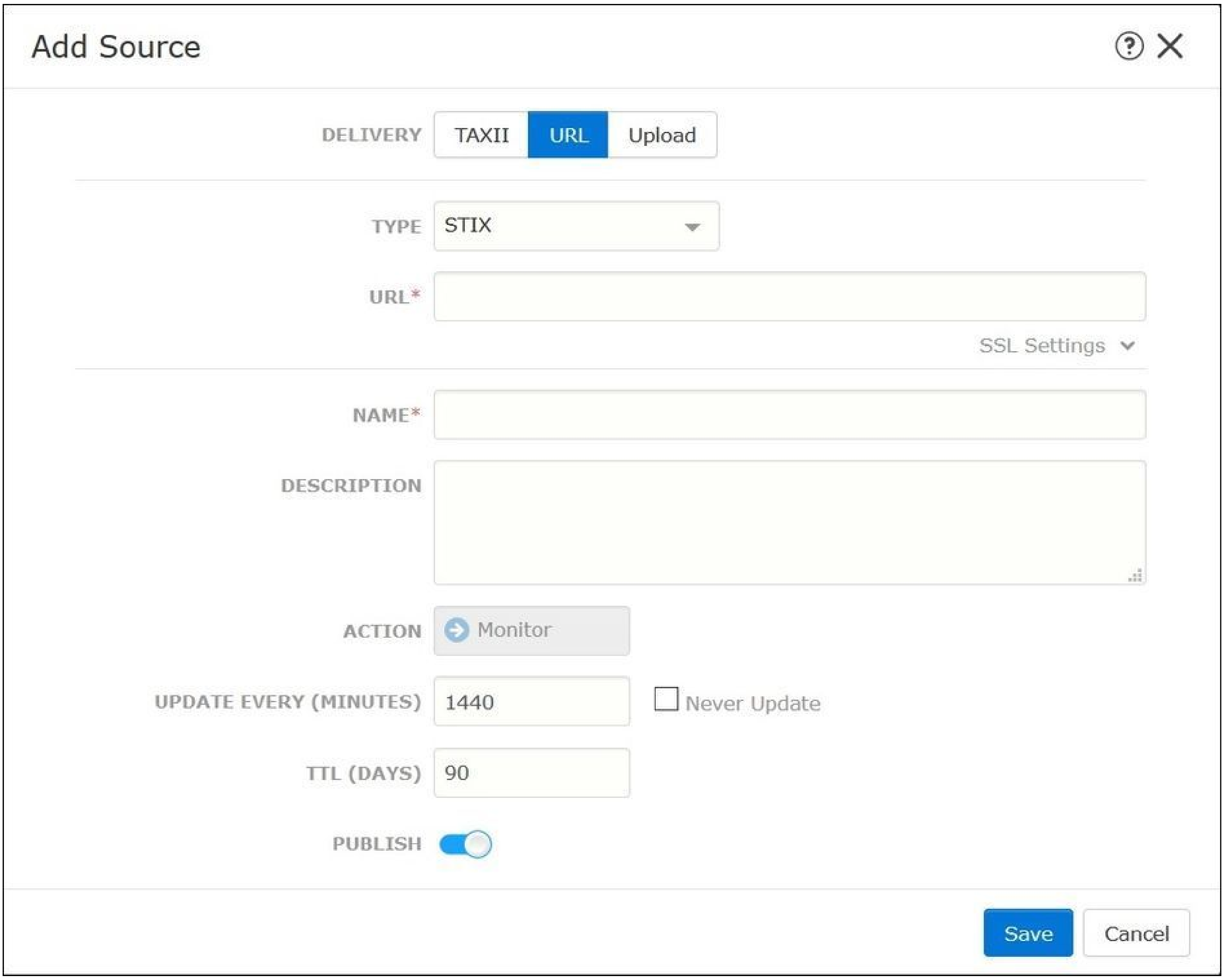
TTL (DAYS): 90

PUBLISH: ●

Save | Cancel

注意：唯一可用的操作是监控。您无法以STIX格式配置威胁的阻止操作。

- URL — 您可以配置指向STIX威胁或平面文件所在的HTTP/HTTPS本地服务器的链接。



Add Source

DELIVERY: TAXII | URL | Upload

TYPE: STIX

URL*

SSL Settings

NAME*

DESCRIPTION

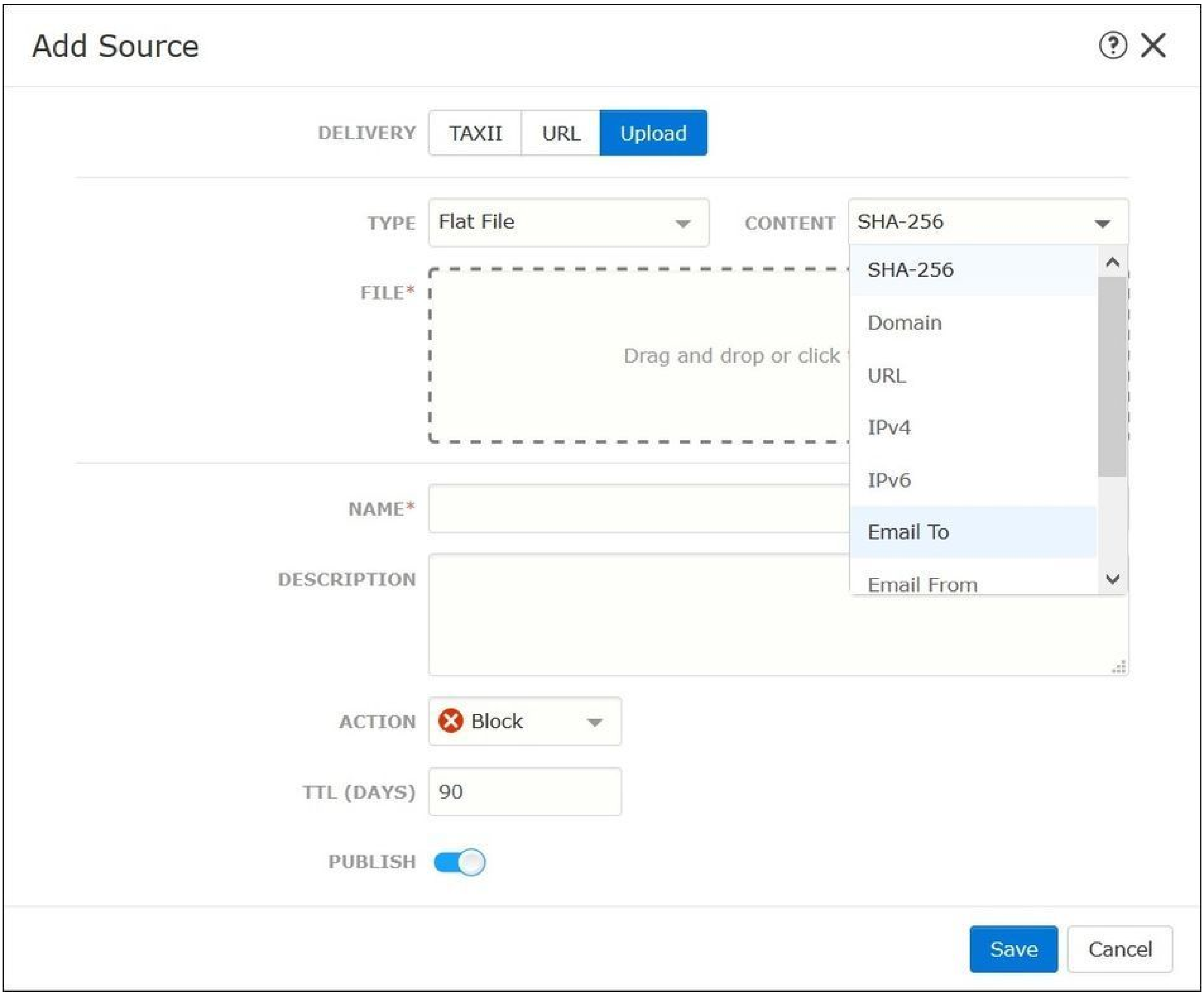
ACTION: Monitor

UPDATE EVERY (MINUTES): 1440 □ Never Update

TTL (DAYS): 90

PUBLISH

- 平面文件 — 可以上传*.txt格**式的文**件，并且必须指定文件的内容。文件每行必须包含一个内容条目。



Add Source

DELIVERY: TAXII | URL | Upload

TYPE: Flat File

CONTENT: SHA-256

FILE*: Drag and drop or click

NAME*:

DESCRIPTION:

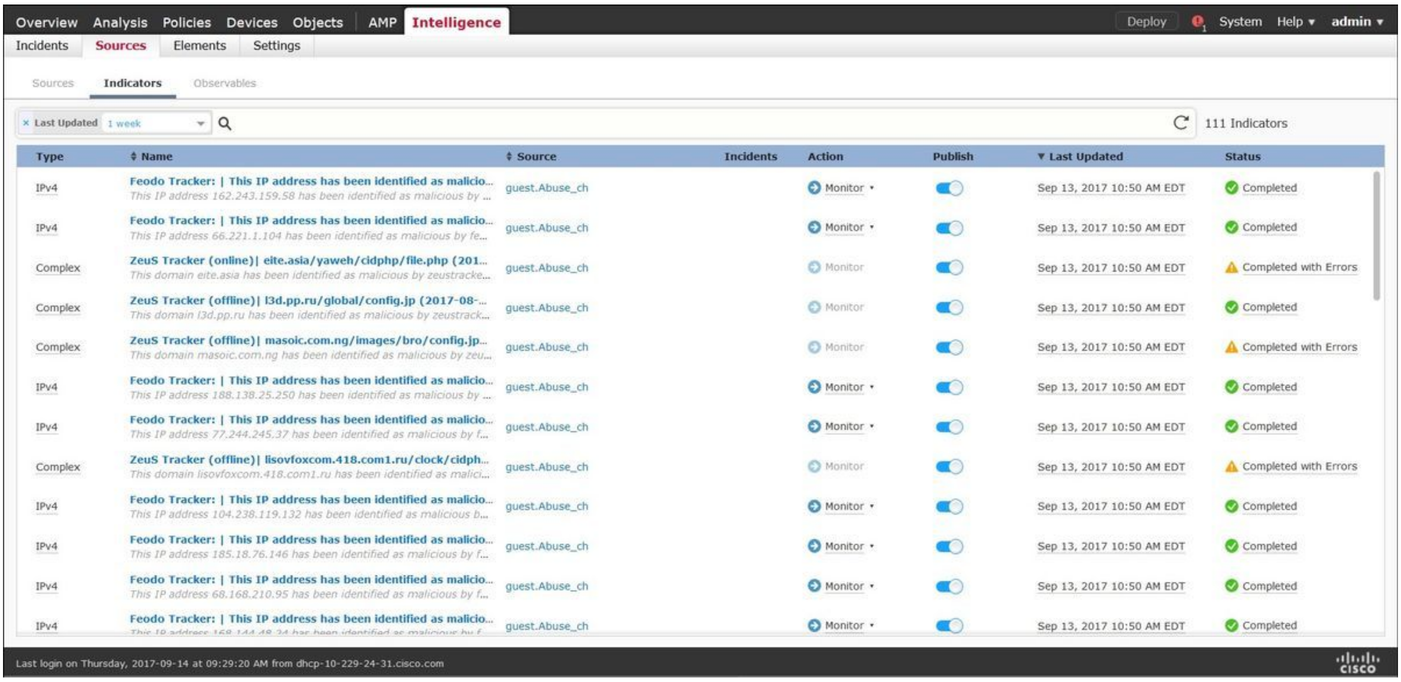
ACTION: Block

TTL (DAYS): 90

PUBLISH

注意：默认情况下，所有源都会发布，这意味着它们会被推送到传感器。此过程可能需要20分钟或更长时间。

步骤3.在Indicator选项卡下，您可以确认是否从已配置的源下载了指示符属性：



× Last Updated 1 week

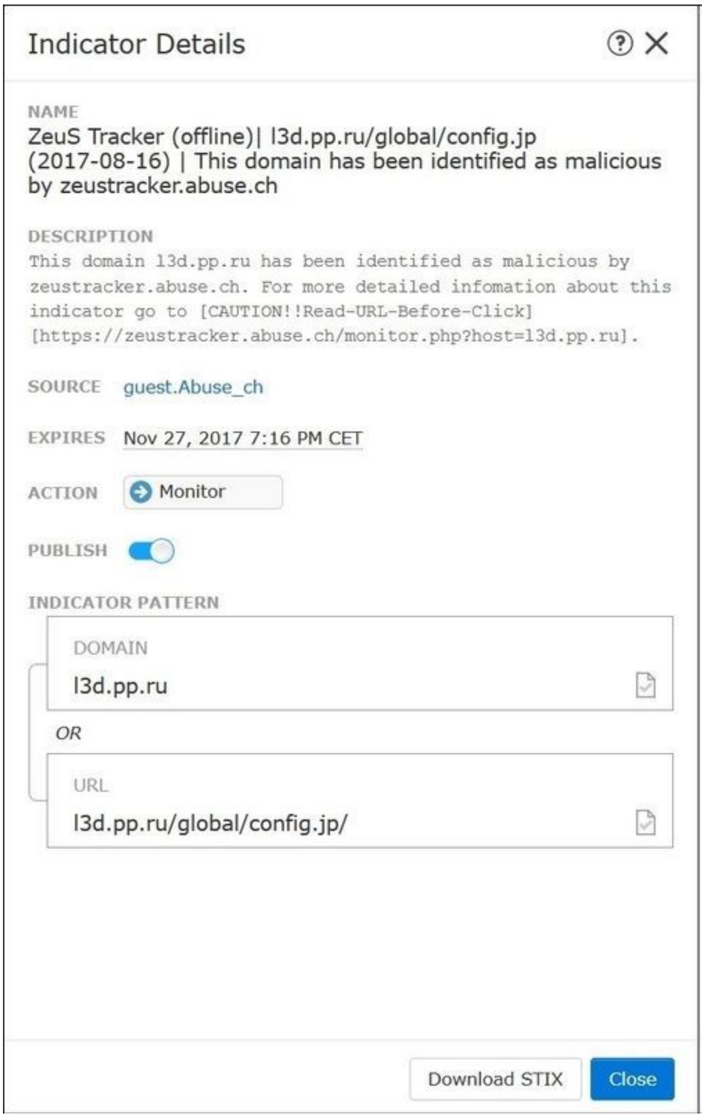
111 Indicators

Type	Name	Source	Incidents	Action	Publish	▼ Last Updated	Status
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 162.243.159.58 has been identified as malicious by ...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 66.221.1.104 has been identified as malicious by fe...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
Complex	ZeuS Tracker (online)| eite.asia/yaweh/cidphp/file.php (201... This domain eite.asia has been identified as malicious by zeustracke...	guest.Abuse_ch		Monitor	●	Sep 13, 2017 10:50 AM EDT	⚠ Completed with Errors
Complex	ZeuS Tracker (offline)| l3d.pp.ru/global/config.jp (2017-08-... This domain l3d.pp.ru has been identified as malicious by zeustrack...	guest.Abuse_ch		Monitor	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
Complex	ZeuS Tracker (offline)| masoic.com.ng/images/bro/config.jp... This domain masoic.com.ng has been identified as malicious by zeu...	guest.Abuse_ch		Monitor	●	Sep 13, 2017 10:50 AM EDT	⚠ Completed with Errors
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 188.138.25.250 has been identified as malicious by ...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 77.244.245.37 has been identified as malicious by f...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
Complex	ZeuS Tracker (offline)| lisovfoxcom.418.com1.ru/clock/cidph... This domain lisovfoxcom.418.com1.ru has been identified as malici...	guest.Abuse_ch		Monitor	●	Sep 13, 2017 10:50 AM EDT	⚠ Completed with Errors
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 104.238.119.132 has been identified as malicious b...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 185.18.76.146 has been identified as malicious by f...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 68.168.210.95 has been identified as malicious by f...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed
IPv4	Feodo Tracker: | This IP address has been identified as malicio... This IP address 168.144.48.24 has been identified as malicious by f...	guest.Abuse_ch		Monitor ▾	●	Sep 13, 2017 10:50 AM EDT	✓ Completed

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

步骤4.选择指示器的名称后，您可以看到有关该指示器的更多详细信息。此外，您还可以决定是否要将其发布到传感器，还是要更改操作（如果显示简单指示器）。

如图所示，复杂指示器列有两个由OR运算符连接的可观察项：



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 infomation 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

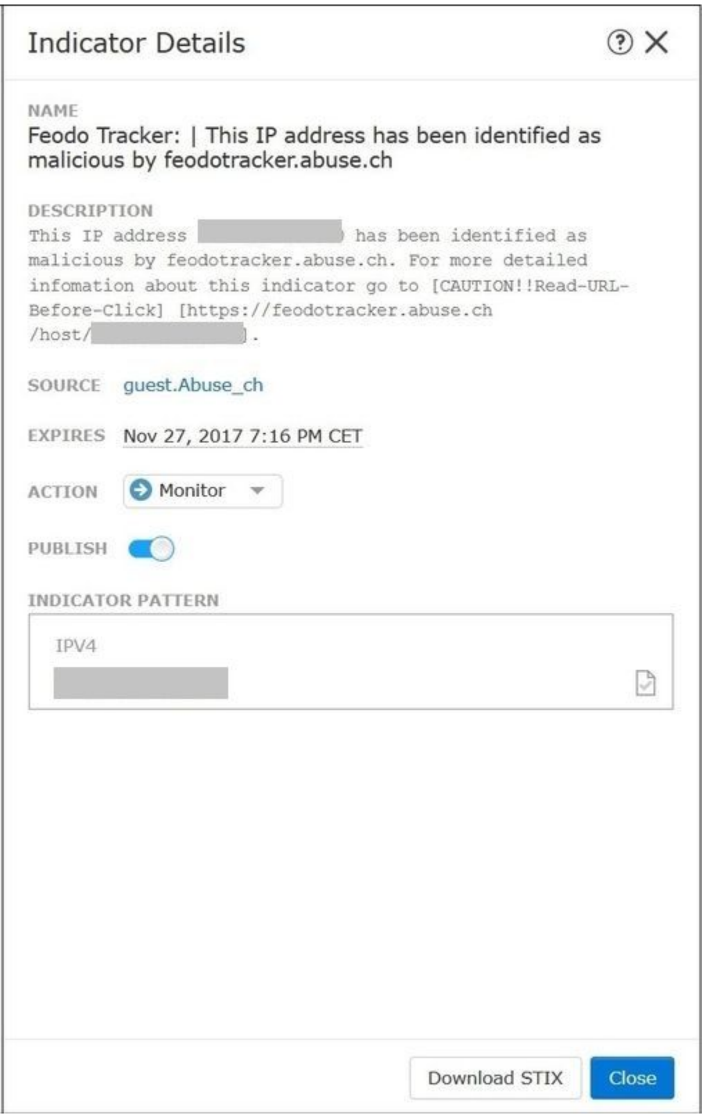
PUBLISH ●

INDICATOR PATTERN

DOMAIN
l3d.pp.ru

OR

URL
l3d.pp.ru/global/config.jp/



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 infomation 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

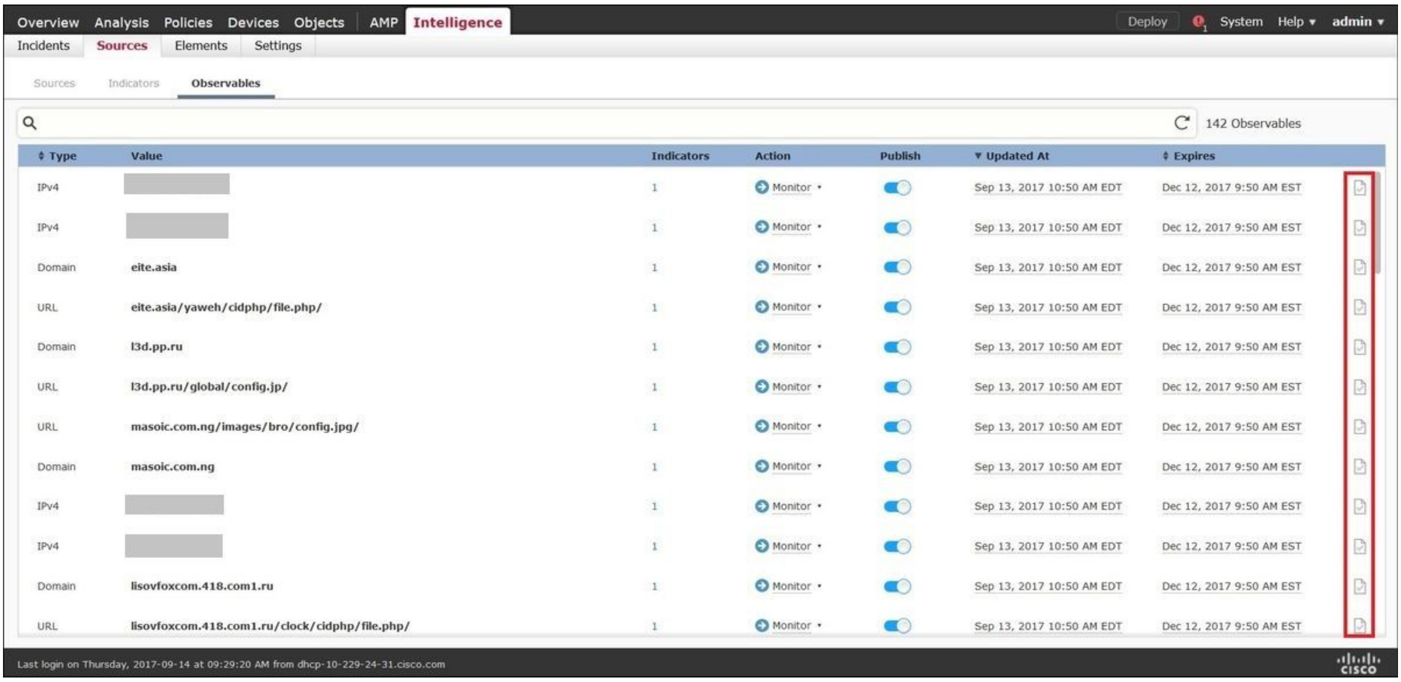
ACTION Monitor ▾

PUBLISH ●

INDICATOR PATTERN

IPV4
[redacted]

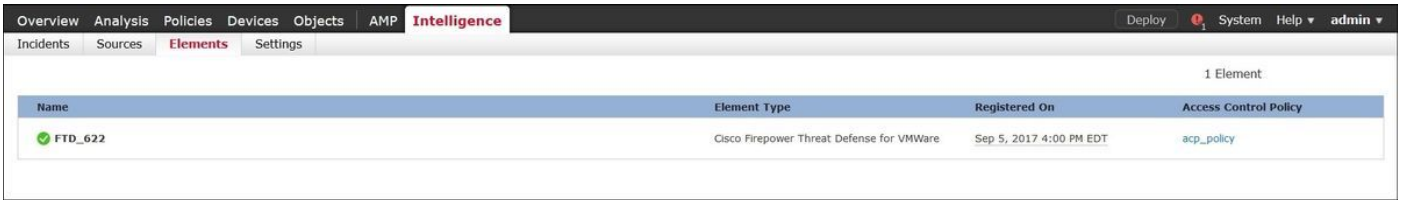
步骤5.导航至“可观察”选项卡，在该选项卡中可以找到指示器中包含的URL、IP地址、域和SHA256。您可以确定要推送到传感器的可观察项，并可以选择更改它们的操作。在最后一列中，有一个白名单按钮，相当于发布/不发布选项。



Type	Value	Indicators	Action	Publish	Updated At	Expires
IPv4	[redacted]	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
IPv4	[redacted]	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
Domain	eite.asia	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
URL	eite.asia/yaweh/cidphp/file.php/	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
Domain	l3d.pp.ru	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
URL	l3d.pp.ru/global/config.jp/	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
URL	masoic.com.ng/images/bro/config.jpg/	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
Domain	masoic.com.ng	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
IPv4	[redacted]	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
IPv4	[redacted]	1	Monitor	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
Domain	lisovfoxcom.418.com1.ru	1	Monitor	●	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	●	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST

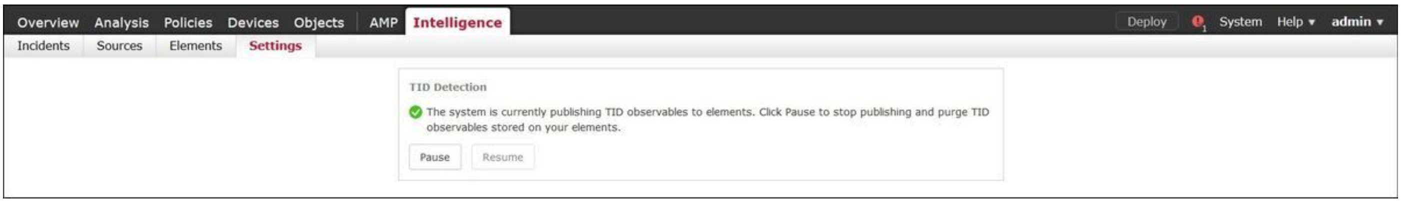
Last login on Thursday, 2017-09-14 at 09:29:20 AM from dhcp-10-229-24-31.cisco.com

步骤6.导航至Elements选项卡以验证启用TID的设备列表。



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

步骤 7（可选）。 导航至“设置”选项卡，然后选择“暂停”按钮，以停止向传感器推送指示器。此操作最多可能需要20分钟。

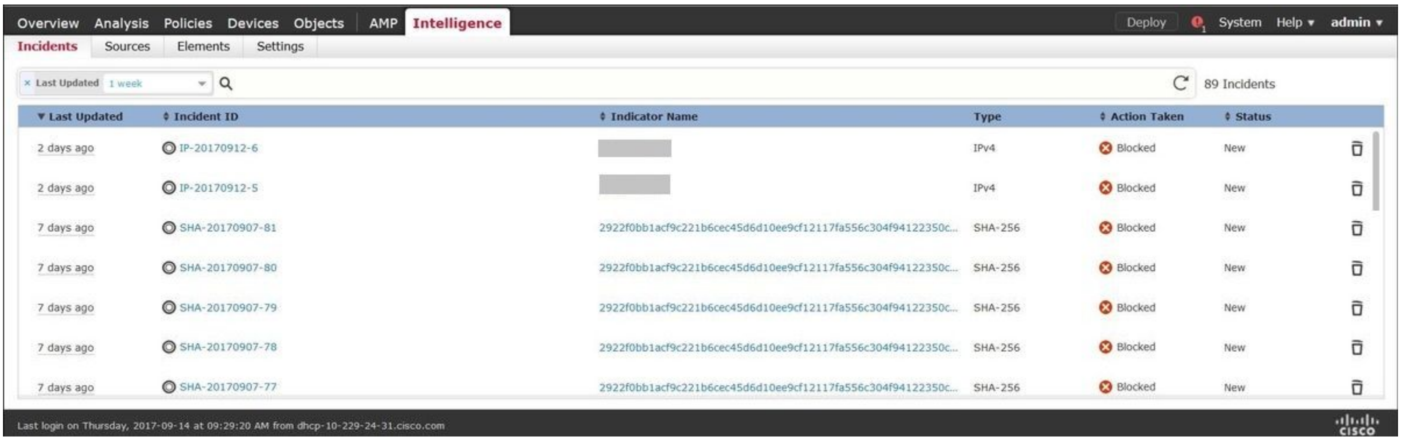


TID Detection

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

验证

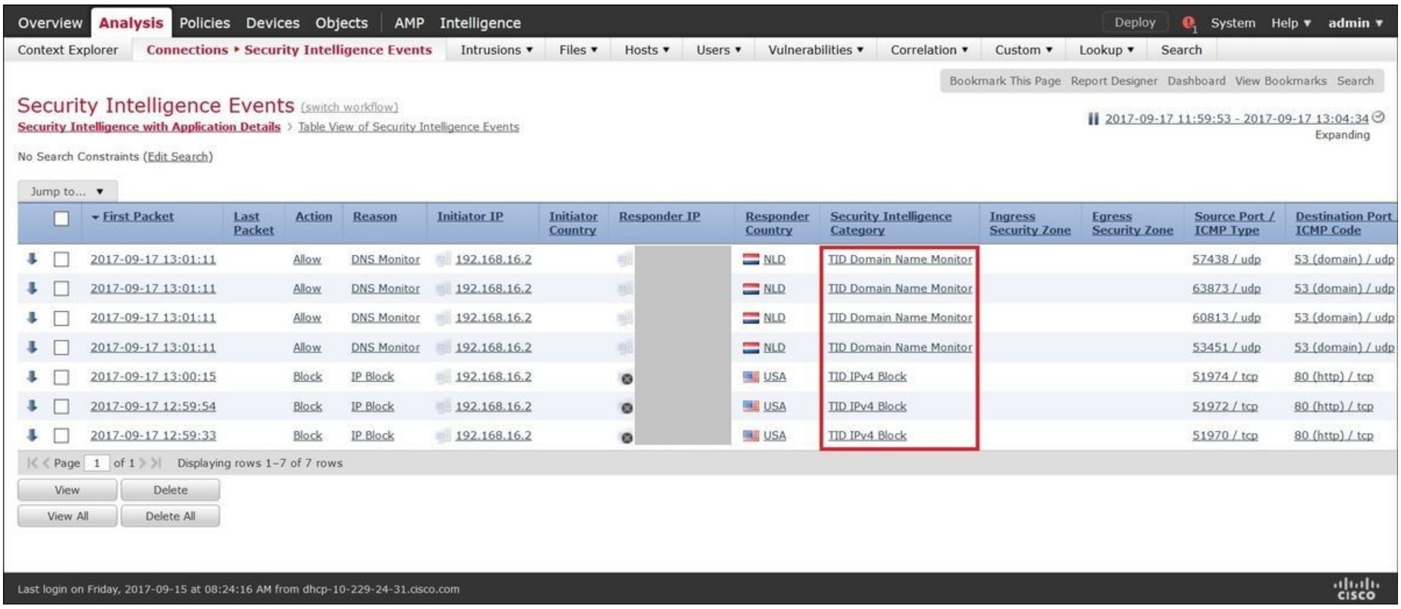
方法1.要验证TID是否对流量执行了操作，您需要导航至Incidents选项卡。



▼ 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

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

方法2.在TID标记下的Security Intelligence Events选项卡下可以找到事故。



Security Intelligence Events (switch workflow)

Security Intelligence with Application Details > Table View of Security Intelligence Events

2017-09-17 11:59:53 - 2017-09-17 13:04:34
Expanding

No Search Constraints (Edit Search)

	☐	▾ 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		[redacted]	NLD	TID Domain Name Monitor			57438 / udp	53 (domain) / udp
⬇	☐	2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2		[redacted]	NLD	TID Domain Name Monitor			63873 / udp	53 (domain) / udp
⬇	☐	2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2		[redacted]	NLD	TID Domain Name Monitor			60813 / udp	53 (domain) / udp
⬇	☐	2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2		[redacted]	NLD	TID Domain Name Monitor			53451 / udp	53 (domain) / udp
⬇	☐	2017-09-17 13:00:15		Block	IP Block	192.168.16.2		[redacted]	USA	TID IPv4 Block			51974 / tcp	80 (http) / tcp
⬇	☐	2017-09-17 12:59:54		Block	IP Block	192.168.16.2		[redacted]	USA	TID IPv4 Block			51972 / tcp	80 (http) / tcp
⬇	☐	2017-09-17 12:59:33		Block	IP Block	192.168.16.2		[redacted]	USA	TID IPv4 Block			51970 / tcp	80 (http) / tcp

Page 1 of 1 Displaying rows 1–7 of 7 rows

Last login on Friday, 2017-09-15 at 08:24:16 AM from dhcp-10-229-24-31.cisco.com

注意：TID的存储容量为100万次。

方法3.您可以确认FMC和传感器上是否存在已配置的源（源）。为此，您可以在CLI上导航到以下位置：

/var/sf/siurl_download/

/var/sf/sidns_download/

/var/sf/iprep_download/

为SHA256源创建了新目录：/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
```

> **注意：**TID仅在FMC的全局Doiman上启用

> **注意：**如果在活动Firepower管理中心上以高可用性配置（物理FMC设备）托管TID，则系统不会将TID配置和TID数据同步到备用Firepower管理中心。

故障排除

有一个称为tid的顶级进程。此过程取决于三个过程：**蒙哥**,**RabbitMQ**，红**皮**。要验证进程是否运行pmtool**状态 | grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "命**令。

```
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#
```

为了实时验证所执行的操作，您可以执行system support firewall-engine-debug**或system support trace命**令。

```
> 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
```

在行动方面有两种可能：

- **URL SI:匹配的规则顺序19、ID 19、ID 1074790455、操作4** — 流量被阻止
- **URL SI:匹配规则顺序20、ID 20、si列表ID 1074790456、操作6** — 流量受监控。