在Firepower上配置SecureX威胁响应源以阻止URL

目录

简介

本文档介绍如何从威胁响应调查期间发现的URL和IP创建威胁情报，以供Firepower使用。

背景信息

思科威胁响应是一个强大的工具，能够利用来自多个模块的信息调查整个环境中的威胁。每个模块都提供由Firepower、安全终端、Umbrella和其他第三方供应商等安全产品生成的信息。这些调查不仅有助于揭示系统中是否存在威胁，而且有助于生成重要的威胁情报，这些情报可以追溯到安全产品以增强环境中的安全性。

SecureX Threat Response使用的一些重要术语：

- **指示符**是与AND和OR运算符逻辑相关的可观察量的集合。 有结合多种可观察量的复杂指标，也有仅由一个可观察指标构成的简单指标。
- **可**观察变量可以是IP、域、URL或sha256。
- **判断**由用户创建，用于连接特定时间段内的可观察处置情况。
- **创建**源是为了将SecureX威胁响应调查生成的威胁情报与其他安全产品（如防火墙和Firepower和ESA等邮件内容过滤器）共享。

先决条件

要求

Cisco 建议您了解以下主题：

- SecureX CTR(思科威胁响应。

- Firepower TID（威胁情报导向器）。
- Firepower访问控制策略配置。

本文档使用Firepower TID实施在SecureX威胁响应上生成的威胁情报。对于FMC版本7.3，在FMC部署中使用TID的要求如下：

- 版本 6.2.2 或更高版本.
- 至少配置15 GB的内存。
- 配置为REST API访问已启用。请参阅《思科安全防火墙管理中心管理指南》中的“启用REST API访问”。
- 如果设备在版本6.2.2或更高版本上，则可以将FTD用作threat intelligence director元素。

> **注意**：此文档认为Threat Intelligence Director已在系统上处于活动状态。有关TID初始配置和故障排除的更多信息，请查看“相关信息”部分中提供的链接。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- SecureX思科威胁响应控制面板
- FMC（防火墙管理中心）版本7.3
- FTD（防火墙威胁响应）版本7.2

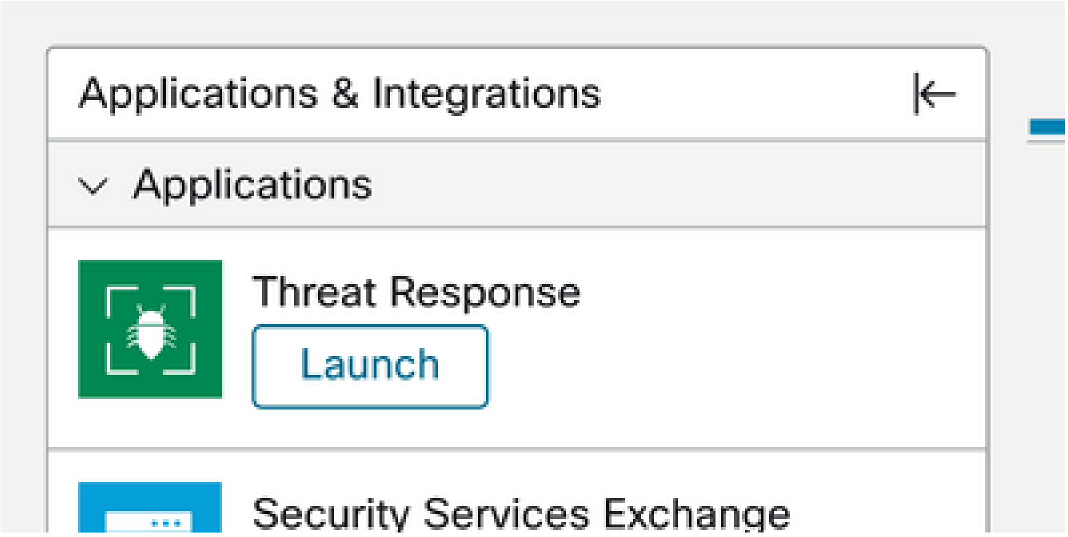
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

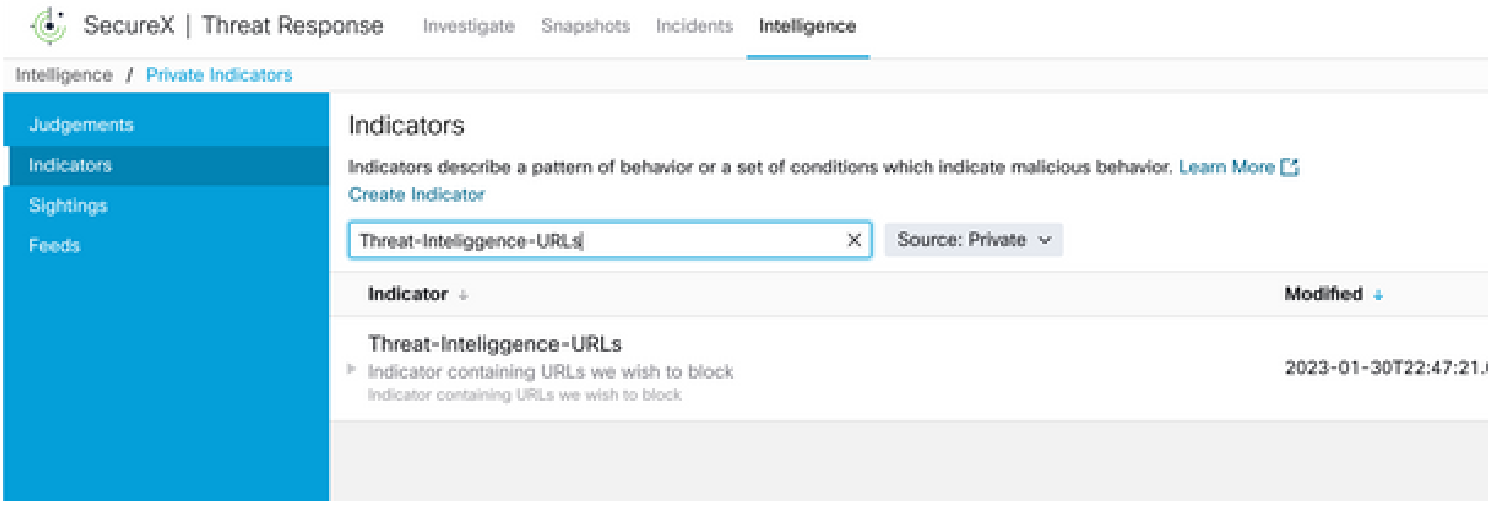
创建SecureX威胁响应源

SecureX Threat Response允许以可观察到的输入开始对环境进行调查。威胁响应引擎查询模块以搜索与可观察事件相关的任何活动。调查返回模块发现的任何匹配项，此信息可包括IP、域、Url邮件或文件。后续步骤将创建与其他安全产品一起使用信息的源。

第1步登录到SecureX控制面板，然后点击**Threat** Response Module的Launch按钮。这会在新窗口中打开“威胁响应”页面：



第2步在 Threat Response页面中点击Intelligence > Indicators，然后将Source下拉列表从Public更改为Private。这必须允许您点击Create Indicator链接。进入“指示器创建者”向导后，为您的指示器选择任何有意义的标题和说明，然后选中“URL监视列表”复选框。此时您可以保存指示器，无需其他信息，但您可以选择配置其余的可用选项。

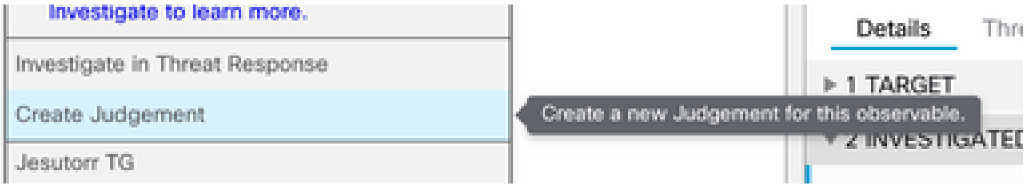


Indicators describe a pattern of behavior or a set of conditions which indicate malicious behavior. Learn More

Threat-Inteliggence-URLs

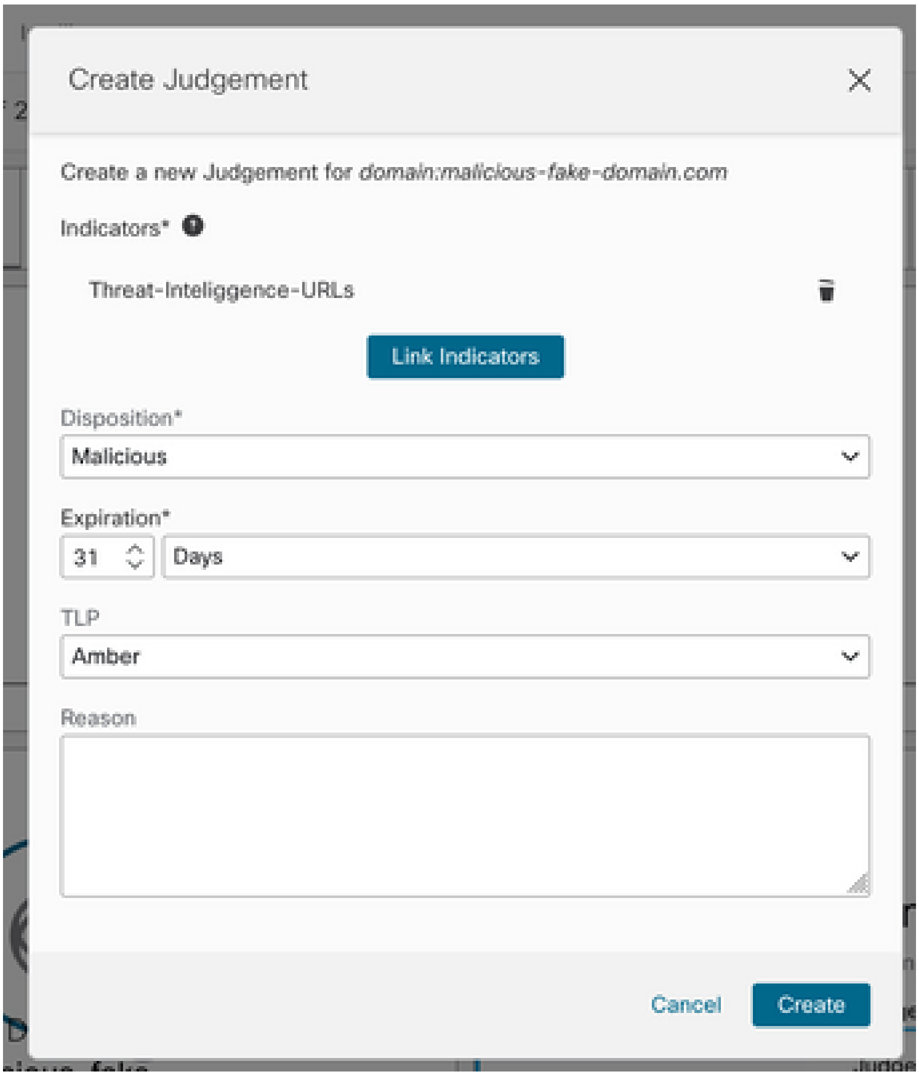
Indicator	Modified
Threat-Inteliggence-URLs Indicator containing URLs we wish to block Indicator containing URLs we wish to block	2023-01-30T22:47:21.

第3步导航到**Investigate**选项卡，并将要调查的任何可观察信息粘贴到调查框中。为了演示目的，虚假URL https://malicious-fake-domain.com 用于此配置示例。单击**Investigate**并等待调查完成。虚拟URL处置情况如预期未知。继续右键点击**下箭头**以展开上下文菜单，然后点击**创建判断**。



Create a new Judgement for this observable.

第4步点击**Link Indicators**，然后从第2步中选择指示器。选择**Malicious**性质并选择您认为适当的到期日。最后单击**Create**按钮。URL现在必须显示在**Intelligence > Indicators > View Full Indicator**下。



Create Judgement

Create a new Judgement for *domain:malicious-fake-domain.com*

Indicators*

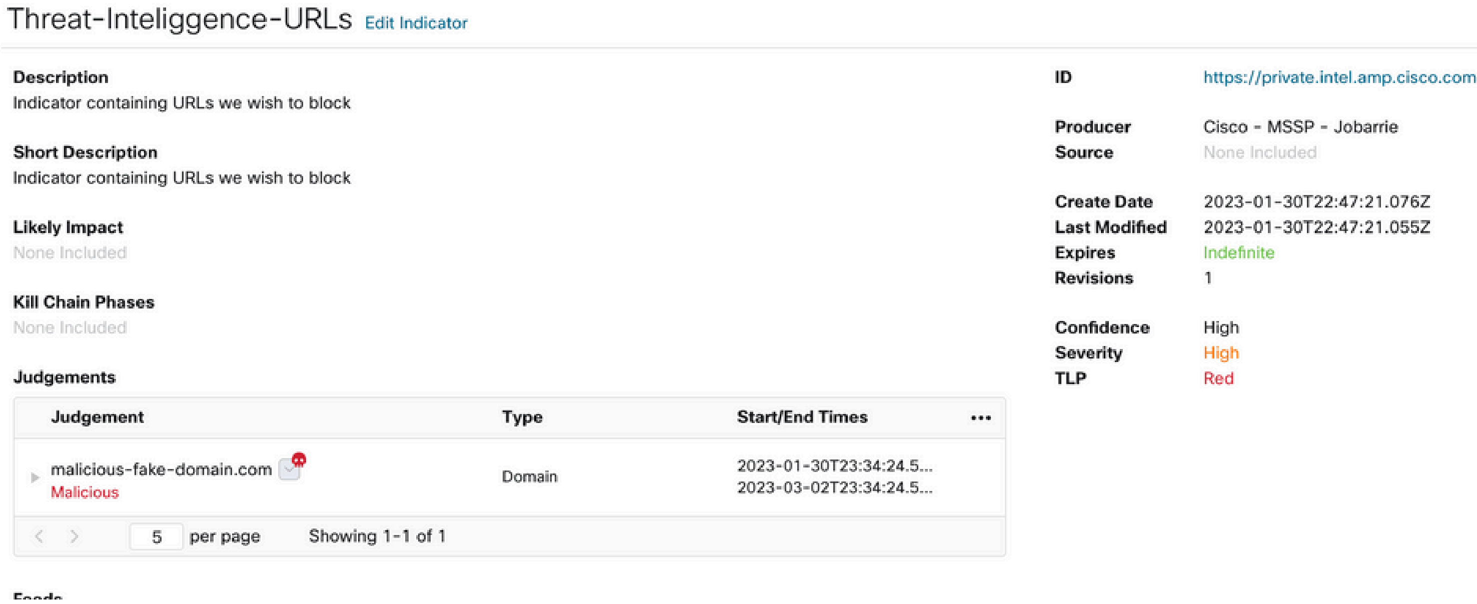
Threat-Inteliggence-URLs

Disposition*: Malicious

Expiration*: 31 Days

TLP: Amber

Reason



Threat-Inteliggence-URLs

Description
Indicator containing URLs we wish to block

Short Description
Indicator containing URLs we wish to block

Likely Impact
None Included

Kill Chain Phases
None Included

Judgements

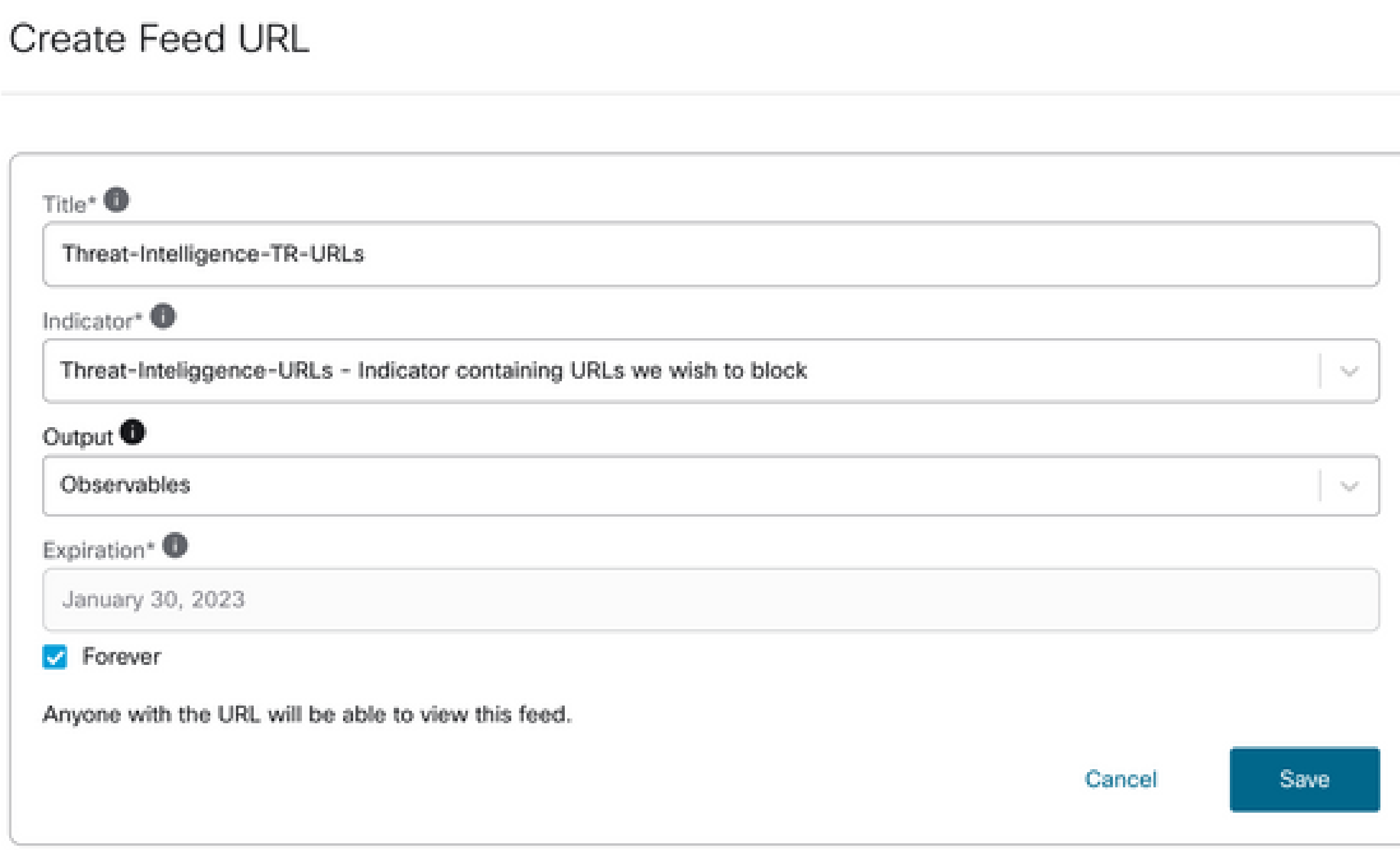
Judgement	Type	Start/End Times
malicious-fake-domain.com Malicious	Domain	2023-01-30T23:34:24.5... 2023-03-02T23:34:24.5...

5 per page Showing 1-1 of 1

Feeds

ID	https://private.intel.amp.cisco.com
Producer	Cisco - MSSP - Jobarrie
Source	None Included
Create Date	2023-01-30T22:47:21.076Z
Last Modified	2023-01-30T22:47:21.055Z
Expires	Indefinite
Revisions	1
Confidence	High
Severity	High
TLP	Red

第5步导航到**Intelligence** > **Feeds，然后单击Create Feed URL。** 填写**Title**字段，然后选择步骤2中创建的**Indicator**。确保将**Output**下拉列表保留为 **可观察**，然后单击**Save。**



Create Feed URL

Title*
Threat-Intelligence-TR-URLs

Indicator*
Threat-Inteliggence-URLs - Indicator containing URLs we wish to block

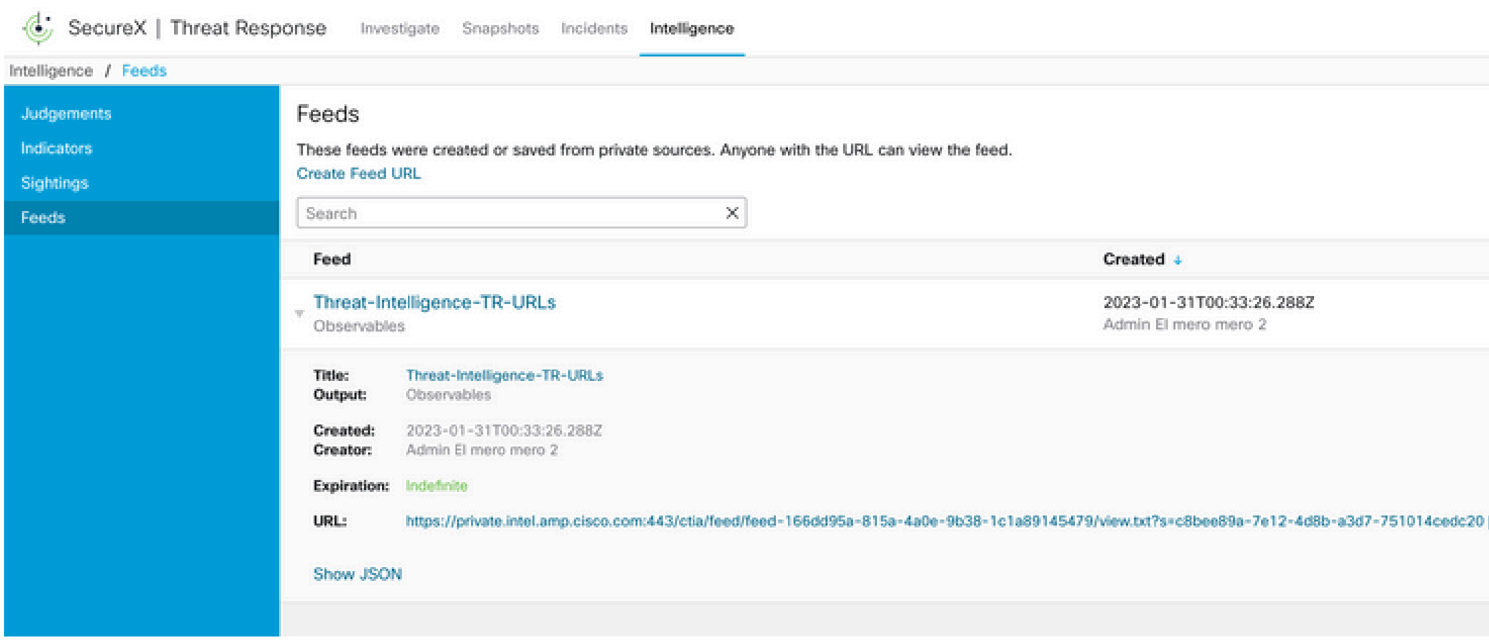
Output
Observables

Expiration*
January 30, 2023

☑ Forever

Anyone with the URL will be able to view this feed.

第6步在**Intelligence** > **Feeds**下创建Verify Feed，然后点击以展开源详细信息。单击**URL**以直观显示源中列出了预期的URL。



Feeds

These feeds were created or saved from private sources. Anyone with the URL can view the feed.
Create Feed URL

Feed	Created
Threat-Intelligence-TR-URLs Observables	2023-01-31T00:33:26.288Z Admin El mero mero 2

Title: Threat-Intelligence-TR-URLs
Output: Observables

Created: 2023-01-31T00:33:26.288Z
Creator: Admin El mero mero 2

Expiration: Indefinite

URL: https://private.intel.amp.cisco.com:443/ctia/feed/feed-166dd95a-815a-4a0e-9b38-1c1a89145479/view.txt?s=c8bee89a-7e12-4d8b-a3d7-751014cedc20

Show JSON

配置FMC Threat Intelligence Director以使用威胁响应源

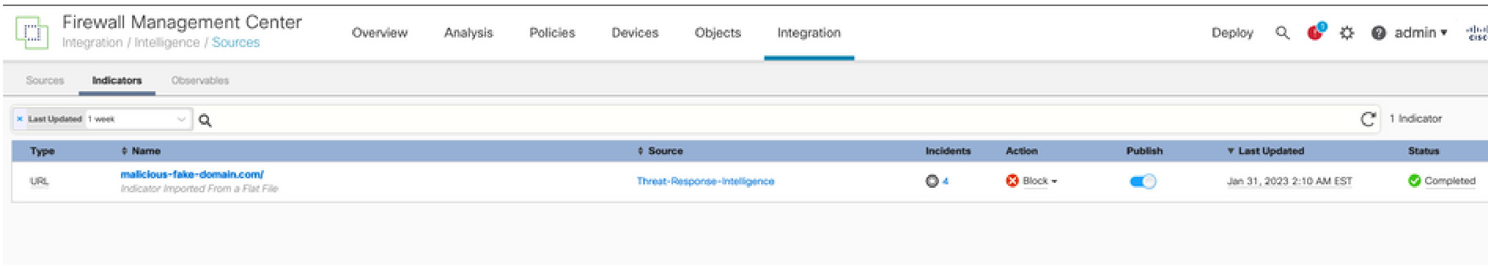
第1步登录您的FMC控制面板并导航到**Integration** > **Intelligence** > **Sources**。 单击**加号**以添加新源
。

第2步使用以下设置创建新源：

- 传送>选择URL
- “文字”>“选择平面文件”
- 内容>选择URL
- Url > Paste the URL from section "Create SecureX Threat Response Feed" step 5。
- Name >选择您认为合适的任何名称
- Action > Select Block
- Update Every > Select 30 min（用于快速更新威胁情报源）

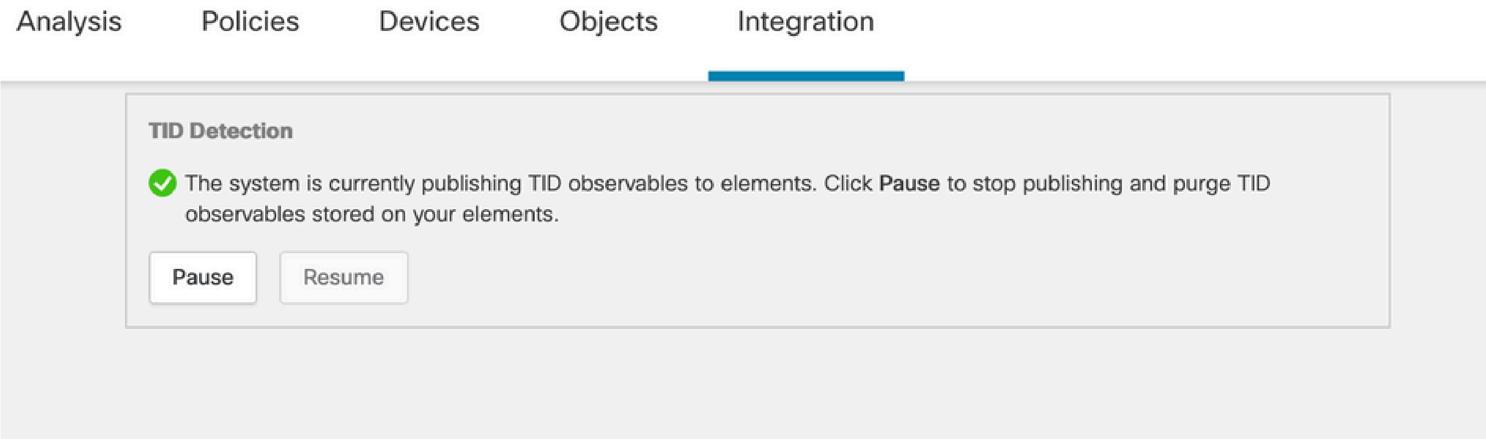
Click **Save**.

第3步在 Indicators and Substituted verify domain下列出：



Type	Name	Source	Incidents	Action	Publish	Last Updated	Status
URL	malicious-fake-domain.com/ Indicator Imported From a Flat File	Threat-Response-Intelligence	4	Block		Jan 31, 2023 2:10 AM EST	Completed

第4步确保Threat Intelligence Director处于活动状态并保持元素为最新（FTDs设备）。导航到**集成** > **智能** > **元素**:

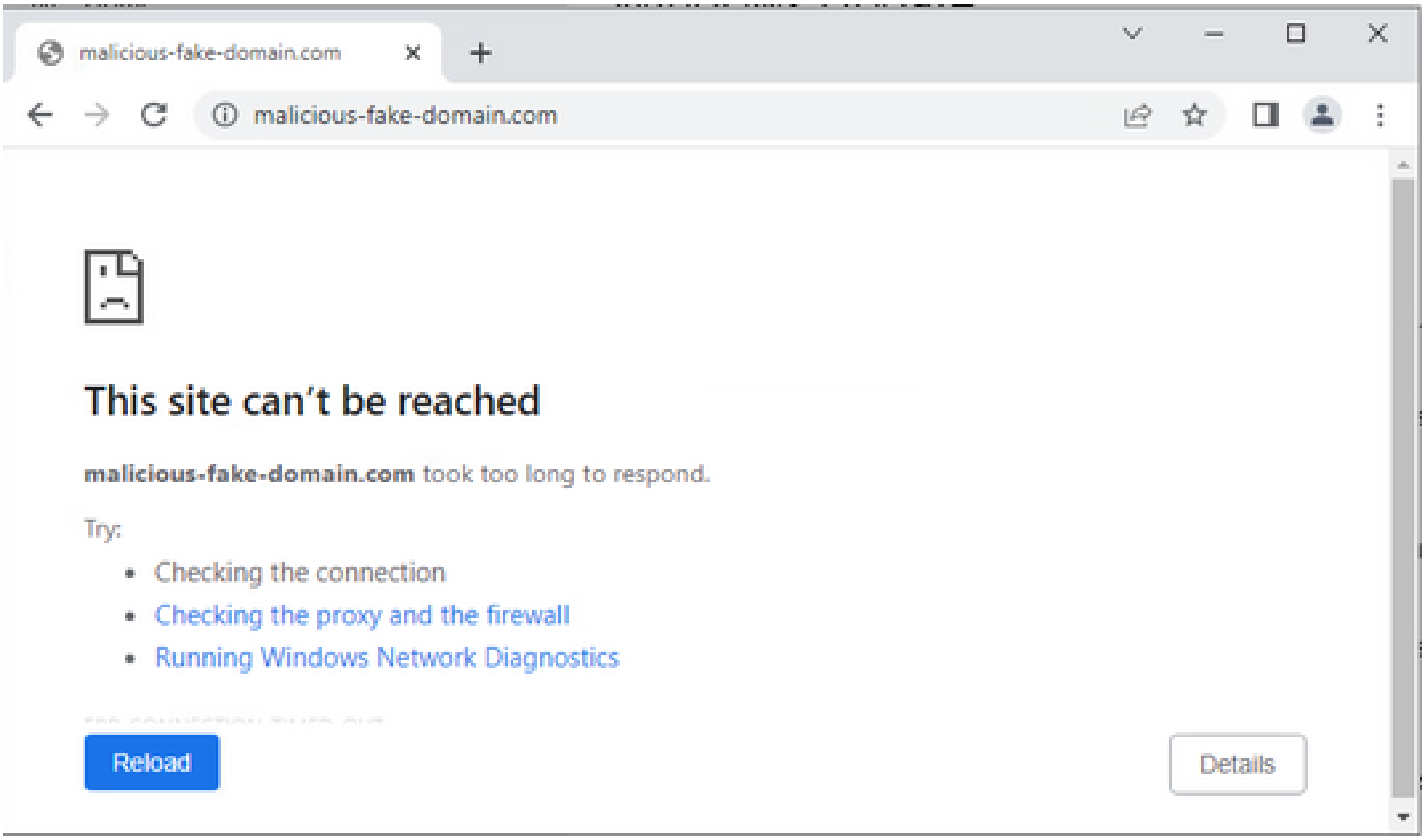


TID Detection

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

验证

配置完成后，终端尝试连接到外部区域上托管的https://malicious-fake-domain[.]com URL，但连接会按预期失败。



This site can't be reached

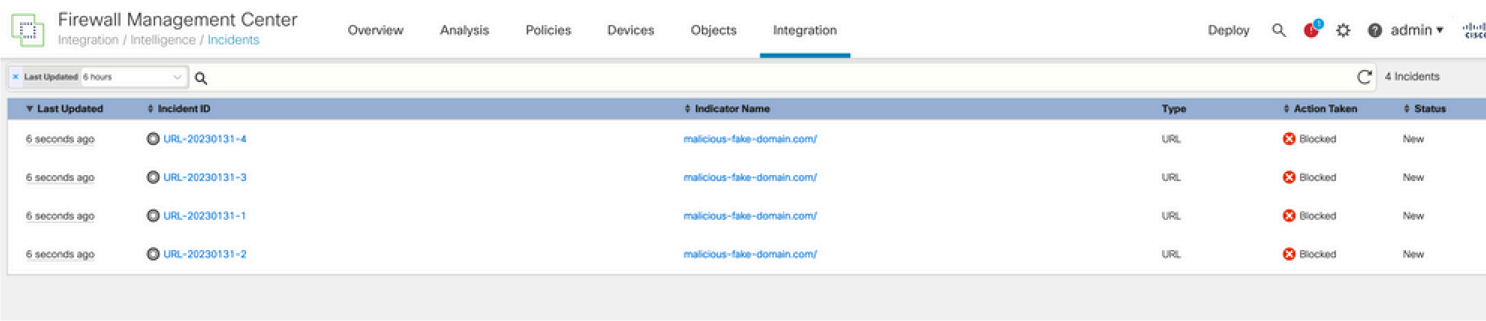
malicious-fake-domain.com took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

要验证连接失败是否是由于Threat Intelligence源，请导航到Integrations > Intelligence > Incidents。阻止的事件必须列在此页上。



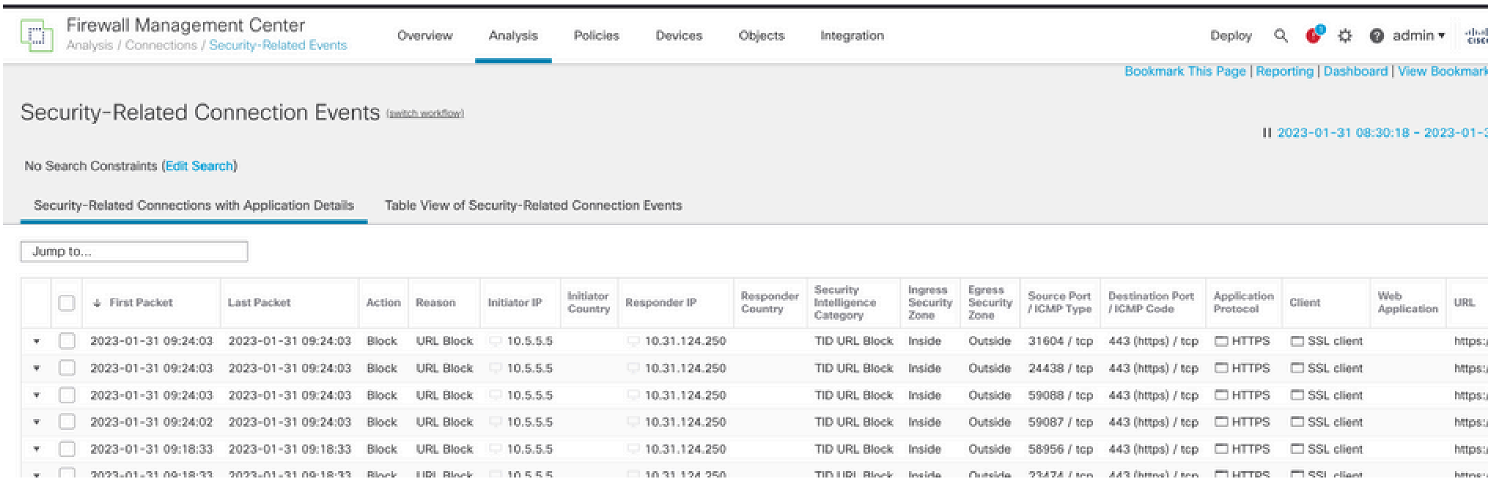
Firewall Management Center
Integration / Intelligence / Incidents
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin

Last Updated 6 hours

4 Incidents

Last Updated	Incident ID	Indicator Name	Type	Action Taken	Status
6 seconds ago	URL-20230131-4	malicious-fake-domain.com/	URL	Blocked	New
6 seconds ago	URL-20230131-3	malicious-fake-domain.com/	URL	Blocked	New
6 seconds ago	URL-20230131-1	malicious-fake-domain.com/	URL	Blocked	New
6 seconds ago	URL-20230131-2	malicious-fake-domain.com/	URL	Blocked	New

您可以在Analysis > Connections > Security-Related Events下验证这些阻止事件：



Firewall Management Center
Analysis / Connections / Security-Related Events
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
Bookmark This Page | Reporting | Dashboard | View Bookmark

Security-Related Connection Events (switch workflow)

2023-01-31 08:30:18 - 2023-01-

No Search Constraints (Edit Search)

Security-Related Connections with Application Details | Table View of Security-Related Connection Events

Jump to...

	□	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	Application Protocol	Client	Web Application	URL
▾	□	2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	31604 / tcp	443 (https) / tcp	HTTPS	SSL client		https:
▾	□	2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	24438 / tcp	443 (https) / tcp	HTTPS	SSL client		https:
▾	□	2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	59088 / tcp	443 (https) / tcp	HTTPS	SSL client		https:
▾	□	2023-01-31 09:24:02	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	59087 / tcp	443 (https) / tcp	HTTPS	SSL client		https:
▾	□	2023-01-31 09:18:33	2023-01-31 09:18:33	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	58956 / tcp	443 (https) / tcp	HTTPS	SSL client		https:
▾	□	2023-01-31 09:18:33	2023-01-31 09:18:33	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	23474 / tcp	443 (https) / tcp	HTTPS	SSL client		https:

FTD LINA捕获允许通过多次检查查看从终端到恶意URL的流量。 请注意，Snort引擎第6阶段检查会返回丢弃结果，因为威胁情报功能使用snort引擎进行高级流量检测。请注意，Snort引擎需要允

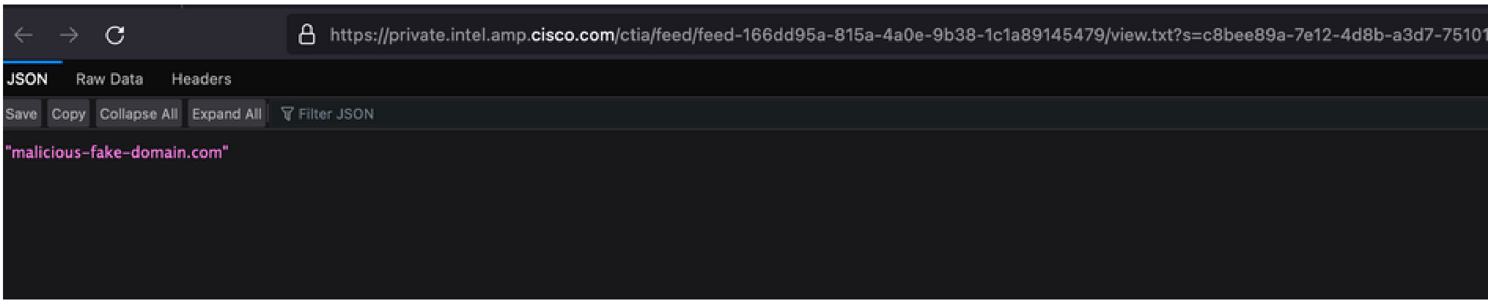
许前几个数据包，以便分析和了解连接的性质，从而正确触发检测。 有关FTD LINA捕获的更多信息，请查看Related Information部分。

```
7: 18:28:46.965449 0050.56b3.fd77 0050.56b3.de22 0x0800 Length: 571
10.5.5.5.63666 > 10.31.124.250.443: P [tcp sum ok] 2993282128:2993282645(517) ack 2622728404 win
1024 (DF) (ttl 128, id 2336)
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 1926 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x14745cf3b800, priority=13, domain=capture, deny=false
hits=553, user_data=0x14745cf4b800, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=Inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 1926 ns
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x14745c5c5c80, priority=1, domain=permit, deny=false
hits=7098895, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=Inside, output_ifc=any

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 3852 ns
Config:
Additional Information:
Found flow with id 67047, using existing flow
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
```

```
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 31244 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 655704 ns
Config:
Additional Information:
service: HTTPS(1122), client: SSL client(1296), payload: (0), misc: (0)

Phase: 6
Type: SNORT
Subtype: SI-URL
Result: DROP
Elapsed time: 119238 ns
Config:
URL list id 1074790412
Additional Information:
Matched url malicious-fake-domain.com, action Block


Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
Action: drop
Time Taken: 813890 ns
Drop-reason: (si) Blocked or blacklisted by the SI preprocessor, Drop-location: frame
0x000056171ff3c0b0 flow (NA)/NA
```

故障排除

- 要确保“威胁响应”(Threat Response)使用正确信息保持更新源，您可以在浏览器上导航至源URL，并查看共享的观察值。



https://private.intel.amp.cisco.com/ctia/feed/feed-166dd95a-815a-4a0e-9b38-1c1a89145479/view.txt?s=c8bee89a-7e12-4d8b-a3d7-75101

"malicious-fake-domain.com"

- 有关FMC Threat Intelligence Director的故障排除，请查看“相关信息”(Related Information)上的链接。

相关信息

- 配置Cisco Threat Intelligence Director并排除故障
- 在FMC 7.3上配置Secure Firewall Threat Intelligence Director
- 使用Firepower威胁防御捕获和Packet Tracer

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。