

# Konfigurieren von SecureX Threat Response-Feeds zum Sperren von URLs in FirePOWER

## Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[SecureX Threat Response-Feed erstellen](#)

[Konfigurieren von FMC Threat Intelligence Director zur Nutzung des Threat Response-Feeds](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie Bedrohungsinformationen aus URLs und IPs erstellen, die bei Untersuchungen zur Reaktion auf Bedrohungen gefunden und von FirePOWER verwendet werden.

## Hintergrundinformationen

Cisco Threat Response ist ein leistungsstarkes Tool, mit dem Bedrohungen in der gesamten Umgebung mithilfe von Informationen aus mehreren Modulen untersucht werden können. Jedes Modul liefert die Informationen, die von Sicherheitsprodukten wie Firepower, Secure Endpoint, Umbrella und anderen Drittanbietern generiert werden. Diese Untersuchungen können nicht nur Aufschluss darüber geben, ob eine Bedrohung im System vorhanden ist, sondern auch wichtige Informationen zu Bedrohungen generieren, die an das Sicherheitsprodukt zurückgegeben werden können, um die Sicherheit in der Umgebung zu erhöhen.

Einige wichtige Begriffe, die von SecureX Threat Response verwendet werden:

- **Der Indikator** ist eine Sammlung von Observablen, die logisch mit UND- und ODER-Operatoren verknüpft sind. Es gibt komplexe Indikatoren, die mehrere Observables kombinieren, außerdem gibt es auch einfache Indikatoren, die aus nur einem Observable bestehen.
- **Observable** ist eine Variable, die eine IP, Domain, URL oder ein sha256 sein kann.
- **Urteile** werden vom Benutzer erstellt und verwendet, um eine beobachtbare mit einer Disposition für einen bestimmten Zeitraum zu verknüpfen.
- **Feeds** werden erstellt, um die von der SecureX Threat Response-Untersuchung generierten Bedrohungsinformationen mit anderen Sicherheitsprodukten wie Firewalls und E-Mail-Content-Filtern wie Firepower und ESA zu teilen.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SecureX CTR ( Cisco Threat Response )
- FirePOWER TID ( Threat Intelligence Director ).
- Konfiguration der FirePOWER-Zugriffskontrollrichtlinien.

In diesem Dokument wird die FirePOWER-TID verwendet, um die bei SecureX Threat Response generierten Bedrohungsinformationen durchzusetzen. Die Anforderungen für die Verwendung von TID in Ihrem FMC-System sind wie für FMC Version 7.3:

- Version 6.2.2 oder höher
- mindestens 15 GB Arbeitsspeicher zur Verfügung.
- konfiguriert und der Zugriff auf die REST-API aktiviert. Siehe "Enable REST API Access" im Cisco Secure Firewall Management Center Administration Guide .
- Sie können FTD als Threat Intelligence Director-Element verwenden, wenn das Gerät Version 6.2.2 oder höher verwendet.

**Hinweis:** In diesem Dokument wird berücksichtigt, dass Threat Intelligence Director bereits auf dem System aktiv ist. Weitere Informationen zur Erstkonfiguration von TID und zur Fehlerbehebung finden Sie unter den im Abschnitt "Related Information" (Verwandte Informationen) verfügbaren Links.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Threat Response-Dashboard mit SecureX
- FMC (Firewall Management Center) Version 7.3
- FTD (Firewall Threat Response) Version 7.2

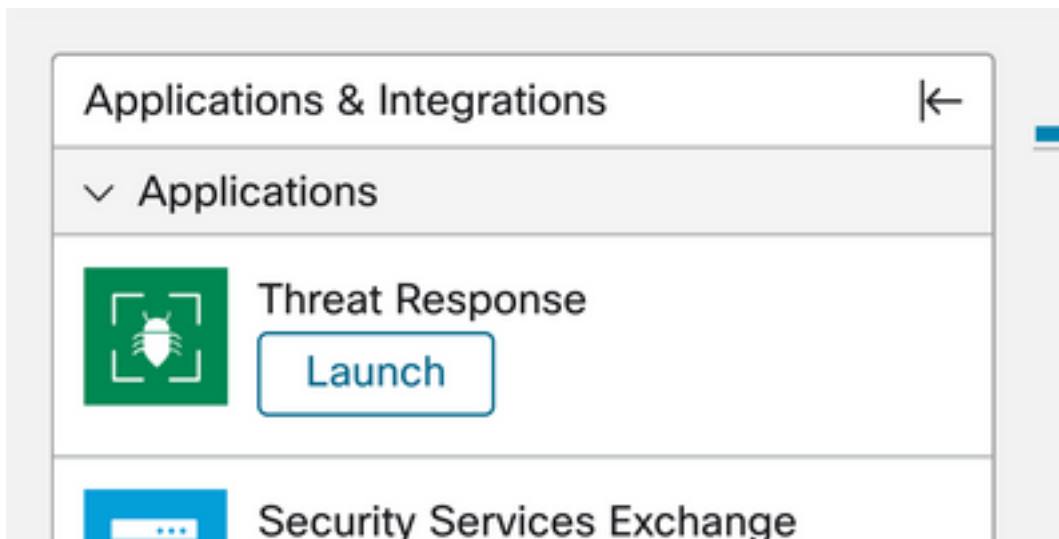
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Konfigurieren

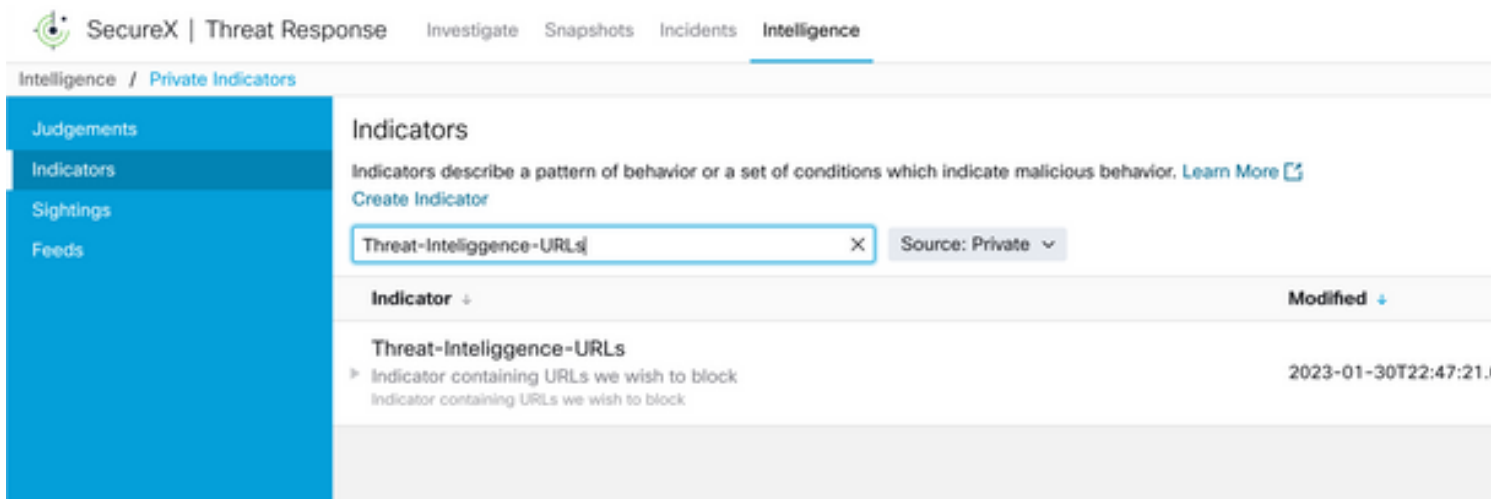
### SecureX Threat Response-Feed erstellen

Mit SecureX Threat Response kann eine Umgebungsuntersuchung mit einem beobachtbaren Input gestartet werden. Die Threat Response-Engine fragt die Module ab, um nach Aktivitäten zu suchen, die sich auf das Beobachtbare beziehen. Bei der Untersuchung werden alle von den Modulen gefundenen Übereinstimmungen zurückgegeben. Diese Informationen können IPs, Domänen, URLs, E-Mails oder Dateien umfassen. Mit den nächsten Schritten erstellen Sie einen Feed, um Informationen mit anderen Sicherheitsprodukten zu nutzen.

**Schritt 1** Melden Sie sich bei Ihrem SecureX Dashboard an, und klicken Sie für das Threat Response-Modul auf die Schaltfläche **Starten**. Daraufhin wird die Seite "Reaktion auf Bedrohungen" in einem neuen Fenster geöffnet:



**Schritt 2** Klicken Sie auf der Seite "Threat Response" auf Intelligence > Indicators, und ändern Sie dann die Dropdown-Liste "Source" (Quelle) von Public zu Private. Klicken Sie auf den Link Create Indicator (Indikator erstellen). Sobald Sie sich im Indikator-Erstellungs-Assistenten befinden, wählen Sie einen aussagekräftigen Titel und eine Beschreibung für Ihren Indikator aus. Aktivieren Sie anschließend das Kontrollkästchen URL-Watchlist. In diesem Moment können Sie die Anzeige speichern, es sind keine weiteren Informationen erforderlich, Sie können jedoch den Rest der verfügbaren Optionen konfigurieren.



**Schritt 3** Navigieren Sie zur Registerkarte **Investigate** (Nachforschen), und fügen Sie alle sichtbaren Informationen, die Sie untersuchen möchten, in das Nachforschungs-Feld ein. Zu Demonstrationszwecken dient die gefälschte URL `https://malicious-fake-domain.com` wurde für dieses Konfigurationsbeispiel verwendet. Klicken Sie auf **Investigate** (Ermitteln), und warten Sie, bis die Untersuchung abgeschlossen ist. Die Dummy-URL-Einstufung ist erwartungsgemäß unbekannt. Klicken Sie mit der rechten Maustaste auf den Pfeil **Unten**, um das Kontextmenü zu erweitern, und klicken Sie auf **Urteilsvermögen erstellen**.



**Schritt 4** Klicken Sie auf **Verknüpfungsindikatoren**, und wählen Sie die Anzeige aus Schritt 2 aus. Wählen Sie die Einstufung als **schädlich** und den Tag des Ablaufs aus, den Sie für angemessen halten. Klicken Sie abschließend auf die Schaltfläche **Erstellen**. Die URL muss nun unter **Intelligence > Indicators > View Full Indicator (Intelligenz > Indikatoren > Vollständigen Indikator anzeigen)** sichtbar sein.

Create Judgement

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

Indicators\* ⓘ

Threat-Intelligence-URLs

Link Indicators

Disposition\*

Malicious

Expiration\*

31 Days

TLP

Amber

Reason

Cancel Create

## Threat-Intelligence-URLs [Edit Indicator](#)

### 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 <br>Malicious | Domain | 2023-01-30T23:34:24.5...<br>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


**Schritt 5** Navigieren Sie zu **Intelligence > Feeds**, und klicken Sie auf **Feed URL erstellen**. Füllen Sie das Feld **Titel** aus, und **wählen Sie** dann den in Schritt 2 erstellten **Indikator** aus. Vergewissern Sie sich, dass Sie die **Ausgabe**-Dropdown-Liste als **Observables** belassen und auf **Speichern** klicken.

## Create Feed URL

Title\* 

Indicator\* 

Output 

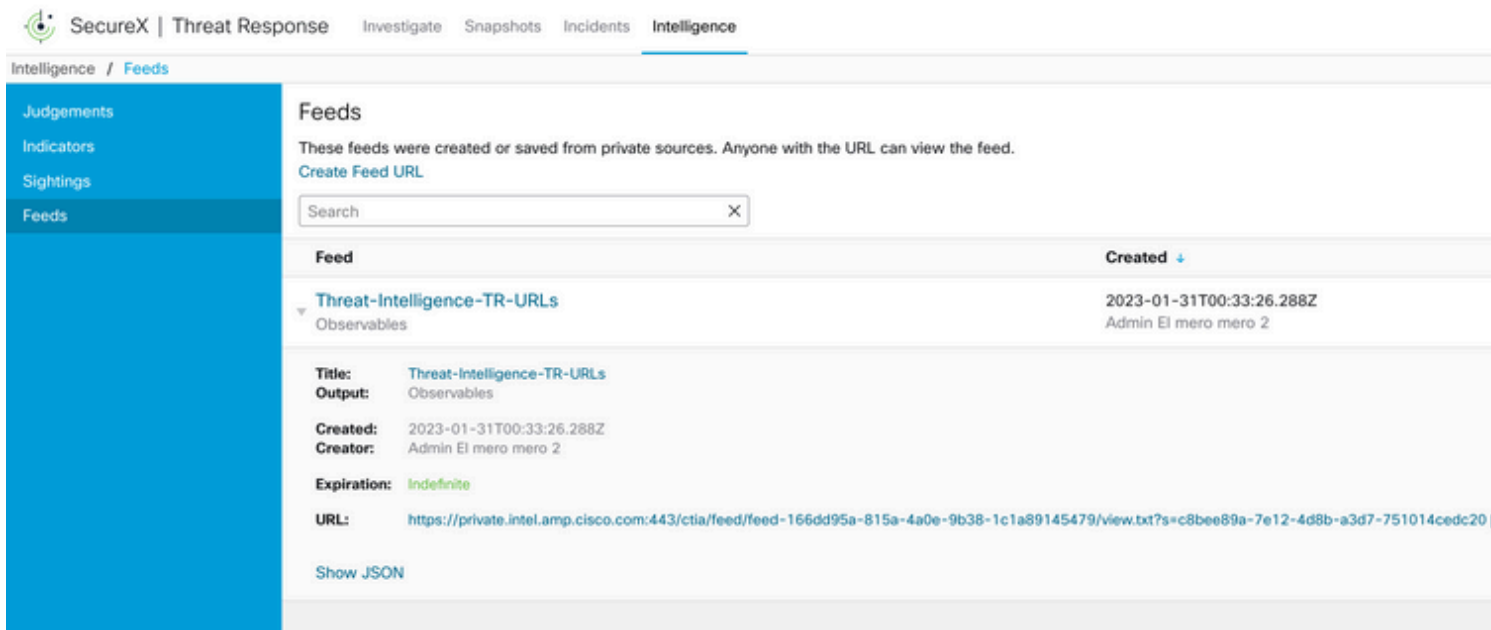
Expiration\* 

Forever

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

[Cancel](#) [Save](#)

**Schritt 6** Überprüfen Sie, ob Feed unter **Intelligence > Feeds** erstellt wurde, und klicken Sie dann auf, um die Feed-Details zu erweitern. Klicken Sie auf die **URL**, um zu sehen, dass die erwarteten URLs im Feed aufgeführt sind.



## Konfigurieren von FMC Threat Intelligence Director zur Nutzung des Threat Response-Feeds

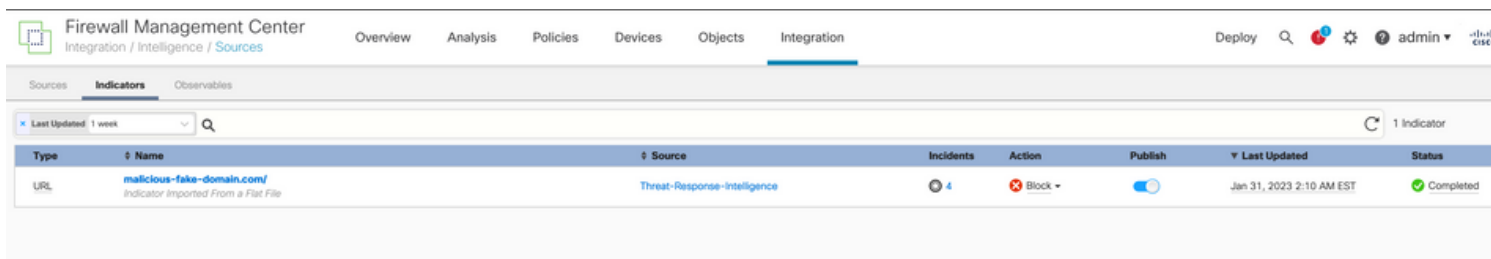
**Schritt 1** Melden Sie sich bei Ihrem FMC-Dashboard an, und navigieren Sie zu **Integration > Intelligence > Sources**. Klicken Sie auf den **Pluszeichen**, um eine neue Quelle hinzuzufügen.

**Schritt 2** Erstellen Sie die neue Quelle mit den folgenden Einstellungen:

- Zustellung > URL auswählen
- Typ > Flat File auswählen
- Inhalt > URL auswählen
- URL > Fügen Sie die URL aus dem Abschnitt "Create SecureX Threat Response Feed" Schritt 5.
- Name > Wählen Sie einen Namen aus, den Sie passend finden
- Aktion > Block auswählen
- Alle aktualisieren > 30 Minuten auswählen (für schnelle Updates für Threat Intelligence-Feed)

Klicken Sie auf **Speichern**.

**Schritt 3** Überprüfen Sie unter Indikatoren und Beobachtungswerte, ob die Domäne aufgeführt ist:



**Schritt 4** Stellen Sie sicher, dass Threat Intelligence Director aktiv ist und die Elemente auf dem neuesten Stand hält (FTD-Geräte). Navigieren Sie zu **Integrations > Intelligence > Elements**:

**TID Detection**

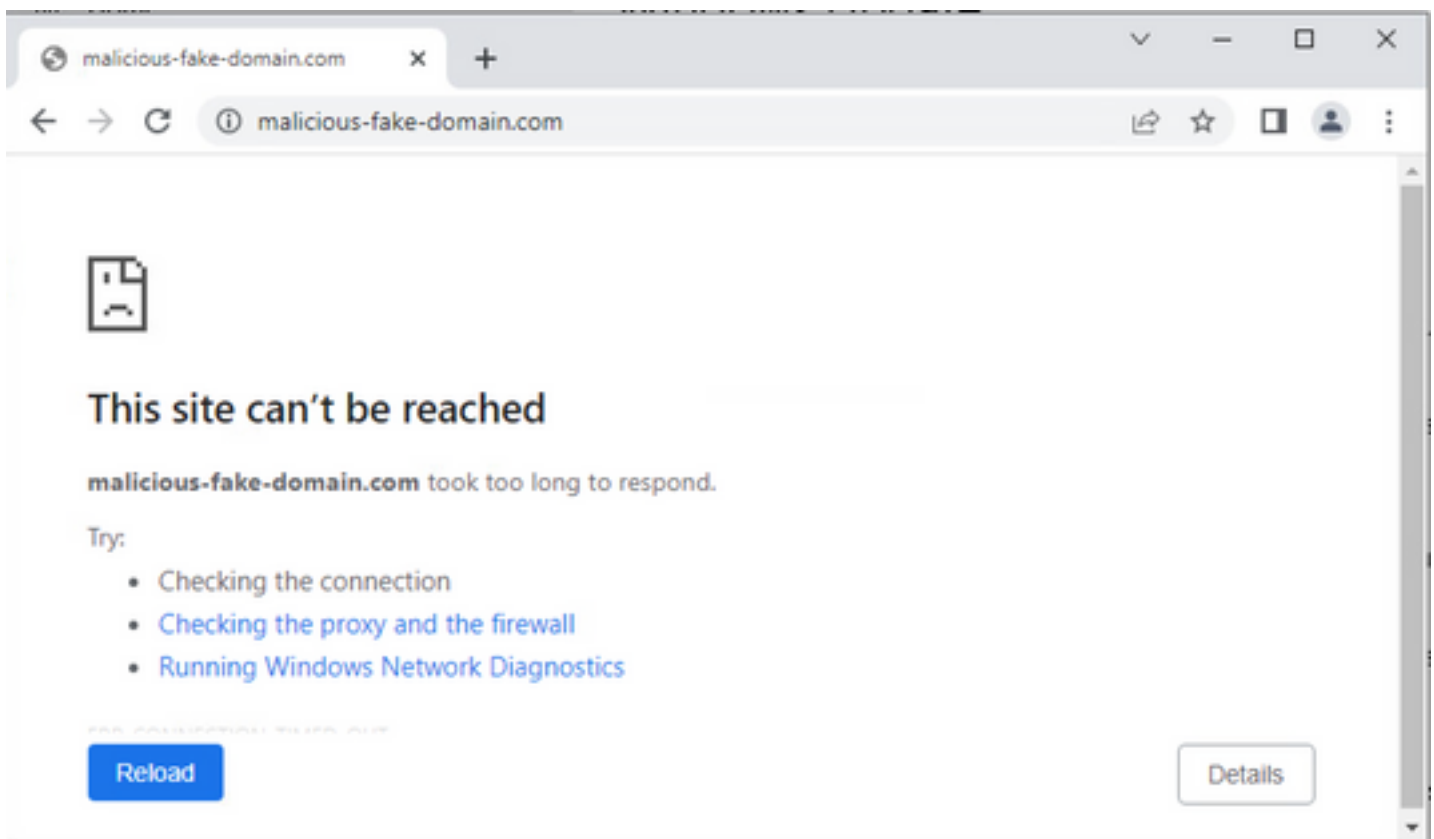
✓ The system is currently publishing TID observables to elements. Click **Pause** to stop publishing and purge TID observables stored on your elements.

Pause

Resume

## Überprüfung

Nach Abschluss der Konfiguration versucht der Endpunkt, eine Verbindung zur `https://malicious-fake-domain[.]com`-URL herzustellen, die in der Zone "Outside" gehostet wird, die Verbindungen schlagen jedoch erwartungsgemäß fehl.



Um zu überprüfen, ob der Verbindungsausfall auf dem Threat-Intelligence-Feed beruht, navigieren Sie zu Integrations > Intelligence > Incidents. Blockierte Ereignisse müssen auf dieser Seite aufgelistet werden.

| 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    |

Sie können diese Blockierungsereignisse unter Analyse > Verbindungen > Sicherheitsrelevante Ereignisse überprüfen:

| 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:// |

Eine FTD LINA-Erfassung ermöglicht es, den Datenverkehr vom Endpunkt zur schädlichen URL über die Mehrfachprüfung zu sehen. Beachten Sie, dass die Prüfung der Snort Engine Phase 6 ein Löschergebnis zurückgibt, da die Threat Intelligence-Funktion die Snort Engine für die erweiterte Verkehrserkennung verwendet. Beachten Sie, dass die Snort-Engine die ersten Pakete zulassen muss, um die Art der Verbindung zu analysieren und zu verstehen und so eine korrekte Erkennung auszulösen. Weitere Informationen zu FTD LINA-Aufnahmen finden Sie im Abschnitt "Verwandte Informationen".

```

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

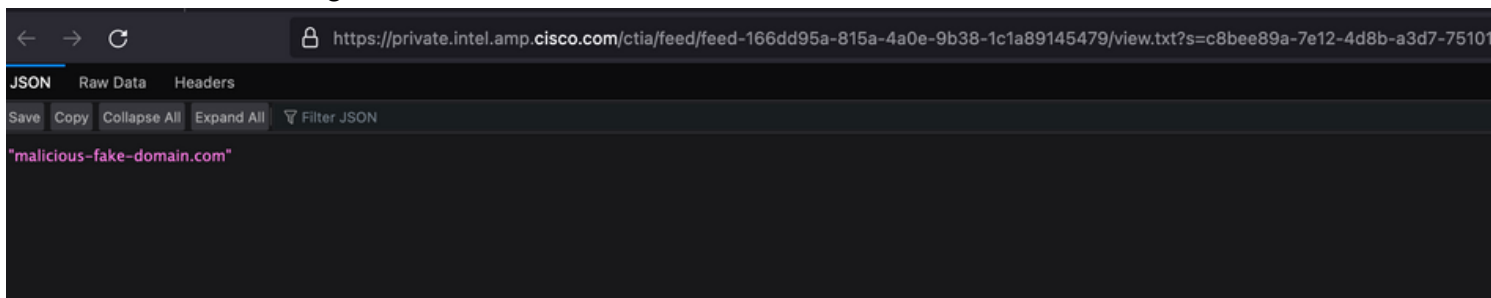
Time Taken: 813890 ns

Drop-reason: (si) Blocked or blacklisted by the SI preprocessor, Drop-location: frame

0x000056171ff3c0b0 flow (NA)/NA

## Fehlerbehebung

- Um sicherzustellen, dass Threat Response den Feed mit den richtigen Informationen aktualisiert, können Sie in Ihrem Browser zur Feed-URL navigieren und die freigegebenen Observables anzeigen.



- Um eine Fehlerbehebung für FMC Threat Intelligence Director durchzuführen, klicken Sie auf den Link "Zugehörige Informationen".

## Zugehörige Informationen

- [Cisco Threat Intelligence Director konfigurieren und Fehlerbehebung dafür durchführen](#)
- [Konfigurieren von Secure Firewall Threat Intelligence Director auf FMC 7.3](#)
- [Verwenden von FirePOWER Threat Defense-Erfassungen und Packet Tracer](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.