

Configurazione dei feed SecureX Threat Response per bloccare l'URL su Firepower

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Crea feed di risposta alle minacce SecureX](#)

[Configurazione del direttore dell'intelligence delle minacce del CCP per l'utilizzo dei feed di risposta alle minacce](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come creare informazioni sulle minacce da URL e IP trovati durante le indagini di risposta alle minacce per essere utilizzati da Firepower.

Premesse

Cisco Threat Response è un potente strumento in grado di indagare le minacce nell'intero ambiente grazie alle informazioni provenienti da più moduli. Ogni modulo fornisce le informazioni generate da prodotti di sicurezza quali Firepower, Secure Endpoint, Umbrella e altri fornitori di terze parti. Queste indagini possono non solo aiutare a scoprire se una minaccia esiste nel sistema, ma anche contribuire a generare importanti informazioni sulle minacce, che possono essere rinviate al prodotto di sicurezza per migliorare la sicurezza nell'ambiente.

Di seguito sono riportati alcuni termini importanti utilizzati da SecureX Threat Response:

- **Indicator** è una raccolta di elementi osservabili correlati logicamente con gli operatori AND e OR. Vi sono indicatori complessi che combinano più indicatori osservabili, inoltre vi sono anche indicatori semplici che sono costituiti da un solo indicatore osservabile.
- **Observable** è una variabile che può essere un IP, un Dominio, un URL o un sha256.
- I **giudizi** vengono creati dall'utente e utilizzati per collegare un osservabile a una disposizione per un periodo di tempo specifico.
- I **feed** vengono creati per condividere la funzionalità Threat Intelligence generata dall'indagine SecureX Threat Response con altri prodotti di sicurezza, ad esempio firewall e filtri dei contenuti e-mail, ad esempio Firepower e ESA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SecureX CTR (Cisco Threat Response)
- Firepower TID (Threat Intelligence Director).
- Configurazione dei criteri di controllo di accesso Firepower.

In questo documento viene utilizzato Firepower TID per applicare la funzionalità Threat Intelligence generata in SecureX Threat Response. I requisiti per l'utilizzo di TID nella distribuzione del CCP, come per la versione 7.3 del CCP, sono:

- Versione 6.2.2 o successiva.
- configurata con almeno 15 GB di memoria.
- configurata con l'accesso all'API REST abilitato. Vedere Enable REST API Access nel manuale Cisco Secure Firewall Management Center Administration Guide (in lingua inglese).
- È possibile utilizzare FTD come elemento threat intelligence director se il dispositivo è nella versione 6.2.2 o superiore.

Nota: in questo documento viene indicato che Threat Intelligence Director è già attivo nel sistema. Per ulteriori informazioni sulla configurazione iniziale di TID e sulla risoluzione dei problemi, consultare i link disponibili nella sezione Informazioni correlate.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

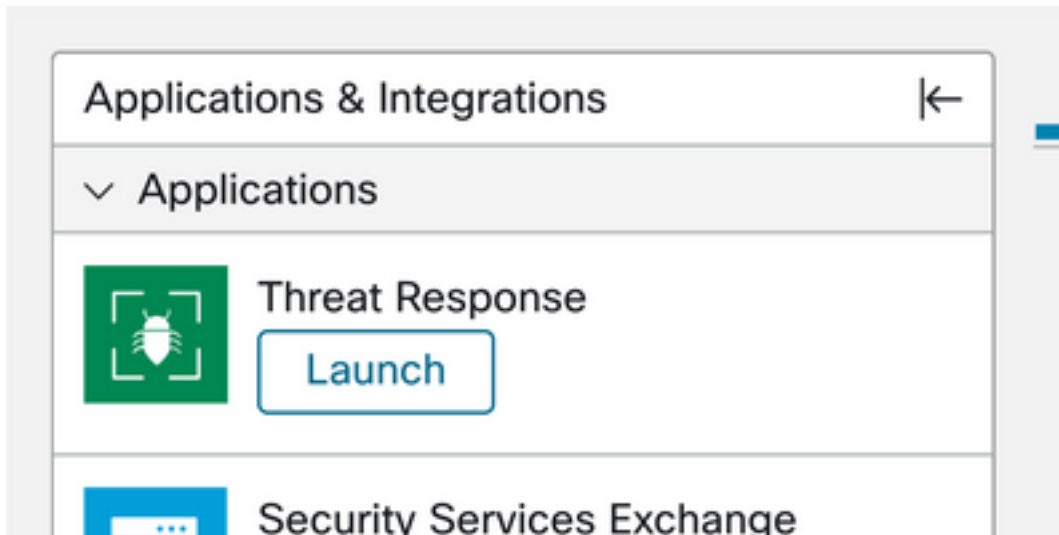
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

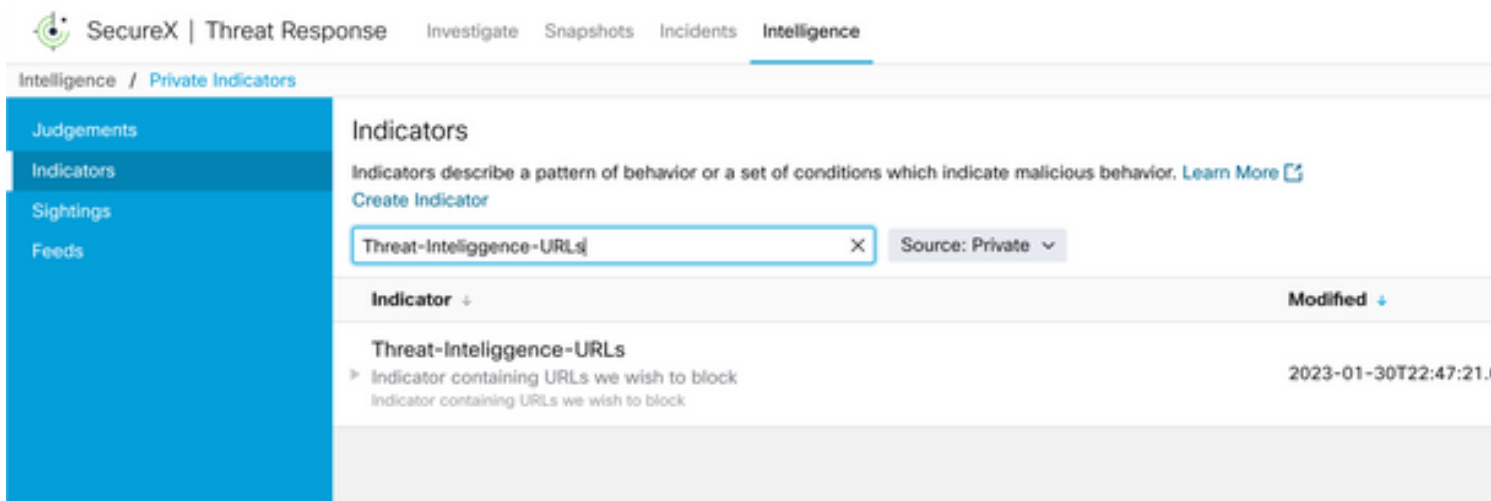
Crea feed di risposta alle minacce SecureX

SecureX Threat Response consente di avviare un'indagine sull'ambiente con un input osservabile. Il modulo di gestione delle risposte alle minacce esegue una query sui moduli per cercare qualsiasi attività correlata all'osservabile. L'indagine restituisce qualsiasi corrispondenza trovata dai moduli. Queste informazioni possono includere indirizzi IP, domini, URL e-mail o file. I passaggi successivi creano un feed per l'utilizzo di informazioni con altri prodotti di sicurezza.

1. Accedere al dashboard SecureX e fare clic sul pulsante **Avvia** per il modulo di risposta alle minacce. Verrà visualizzata la pagina Risposta di rischio in una nuova finestra:



2. Nella pagina Risposta alla minaccia, fare clic su Intelligence > Indicatori, quindi modificare l'elenco a discesa Origine da Pubblica a Privata. In questo modo è necessario fare clic sul collegamento Crea indicatore. Dopo aver aperto la procedura guidata per la creazione degli indicatori, selezionare il titolo e la descrizione dell'indicatore desiderati, quindi selezionare la casella di controllo Lista di controllo URL. Al momento è possibile salvare l'indicatore, non sono necessarie ulteriori informazioni, ma è possibile scegliere di configurare le altre opzioni disponibili.



3. Passare alla scheda **Indaga** e incollare nella casella di investigazione gli elementi osservabili che si desidera esaminare. A scopo dimostrativo il falso URL <https://malicious-fake-domain.com> utilizzato per questo esempio di configurazione. Fare clic su **Indaga** e attendere il completamento dell'indagine. Come previsto, la disposizione dell'URL fittizio è sconosciuta. Procedere a fare clic con il pulsante destro del mouse sulla freccia **Giù** per espandere il menu contestuale e fare clic su **crea giudizio**.



4. Fare clic su **Link Indicatori** e selezionare l'indicatore dal punto 2. Selezionare la disposizione come **Dannosa** e scegliere il giorno di scadenza come si ritiene appropriato. Fare infine clic sul pulsante **Crea**. L'URL deve essere ora visibile in **Intelligence > Indicatori > Visualizza indicatore completo**.

Create Judgement ✕

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

Indicators* ℹ

Threat-Intelligence-URLs 🗑

[Link Indicators](#)

Disposition*

Expiration*

TLP

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	...
<div style="display: flex; align-items: center;"> ▶ malicious-fake-domain.com Malicious 🔒 </div>	Domain	2023-01-30T23:34:24.5... 2023-03-02T23:34:24.5...	⋮

< >
 per page
 Showing 1-1 of 1

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

5. Passare a **Intelligence > Feed** e fare clic su **Crea URL feed**. Riempire il campo **Titolo**, quindi **selezionare l'indicatore** creato al punto 2. Assicuratevi di lasciare l'elenco a discesa **Output** come **osservabili** e fate clic su **Salva (Save)**.

Create Feed URL

Title* ⓘ
Threat-Intelligence-TR-URLs

Indicator* ⓘ
Threat-Intelligence-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.

Cancel Save

6. Verificare che il feed sia stato creato in **Intelligence > Feed**, quindi fare clic per espandere i dettagli del feed. Fare clic sull'**URL** per verificare che gli URL previsti siano elencati nel feed.

SecureX | Threat Response Investigate Snapshots Incidents **Intelligence**

Intelligence / Feeds

Judgements
Indicators
Sightings
Feeds

Feeds

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

Search

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

Configurazione del direttore dell'intelligence delle minacce del CCP per l'utilizzo dei feed di risposta alle minacce

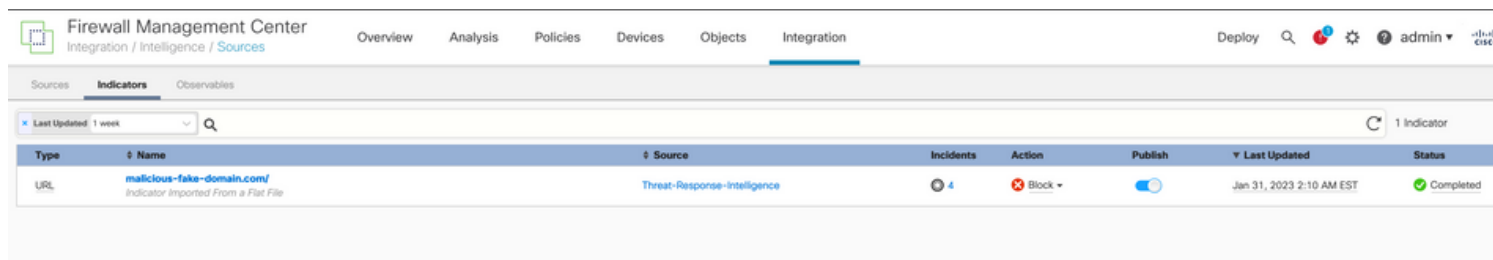
1. Accedere al dashboard di FMC e selezionare **Integrazione > Intelligence > Origini**. Fare clic sul segno **più** per aggiungere una nuova sorgente.

2. Creare la nuova origine con queste impostazioni:

- Recapito > Seleziona URL
- Testo > Seleziona file flat
- Contenuto > Seleziona URL
- Url > Incollare l'URL dalla sezione "Create SecureX Threat Response Feed" al punto 5.
- Nome > Scegliere il nome che si desidera
- Azione > Seleziona blocco
- Aggiorna ogni > Seleziona 30 minuti (per aggiornamenti rapidi del feed di Threat Intelligence)

Fare clic su **Salva**.

3. In Indicators and Observables verificare che il dominio sia elencato:

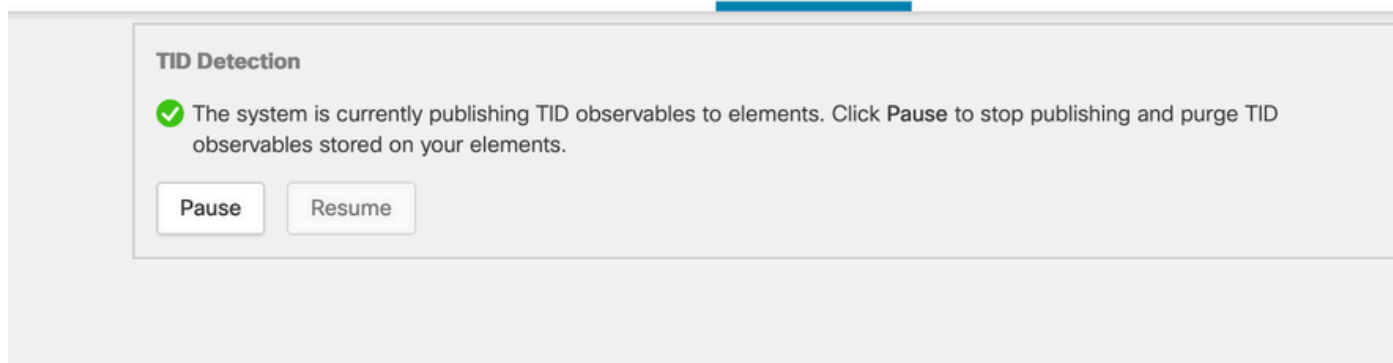


The screenshot shows the 'Indicators' tab in the Firewall Management Center. A table lists indicators with columns for Type, Name, Source, Incidents, Action, Publish, Last Updated, and Status. One indicator is visible: a URL named 'malicious-fake-domain.com/' with source 'Threat-Response-Intelligence', 4 incidents, a 'Block' action, a 'Publish' toggle, last updated on Jan 31, 2023, and a 'Completed' status.

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

4. Accertarsi che Threat Intelligence Director sia Attivo e che mantenga gli elementi aggiornati (dispositivi FTD). Passare a **Integrazioni > Intelligence > Elementi**:

Analysis Policies Devices Objects **Integration**



The screenshot shows the 'TID Detection' status panel. It features a green checkmark icon and the text: 'The system is currently publishing TID observables to elements. Click Pause to stop publishing and purge TID observables stored on your elements.' Below the text are two buttons: 'Pause' and 'Resume'.

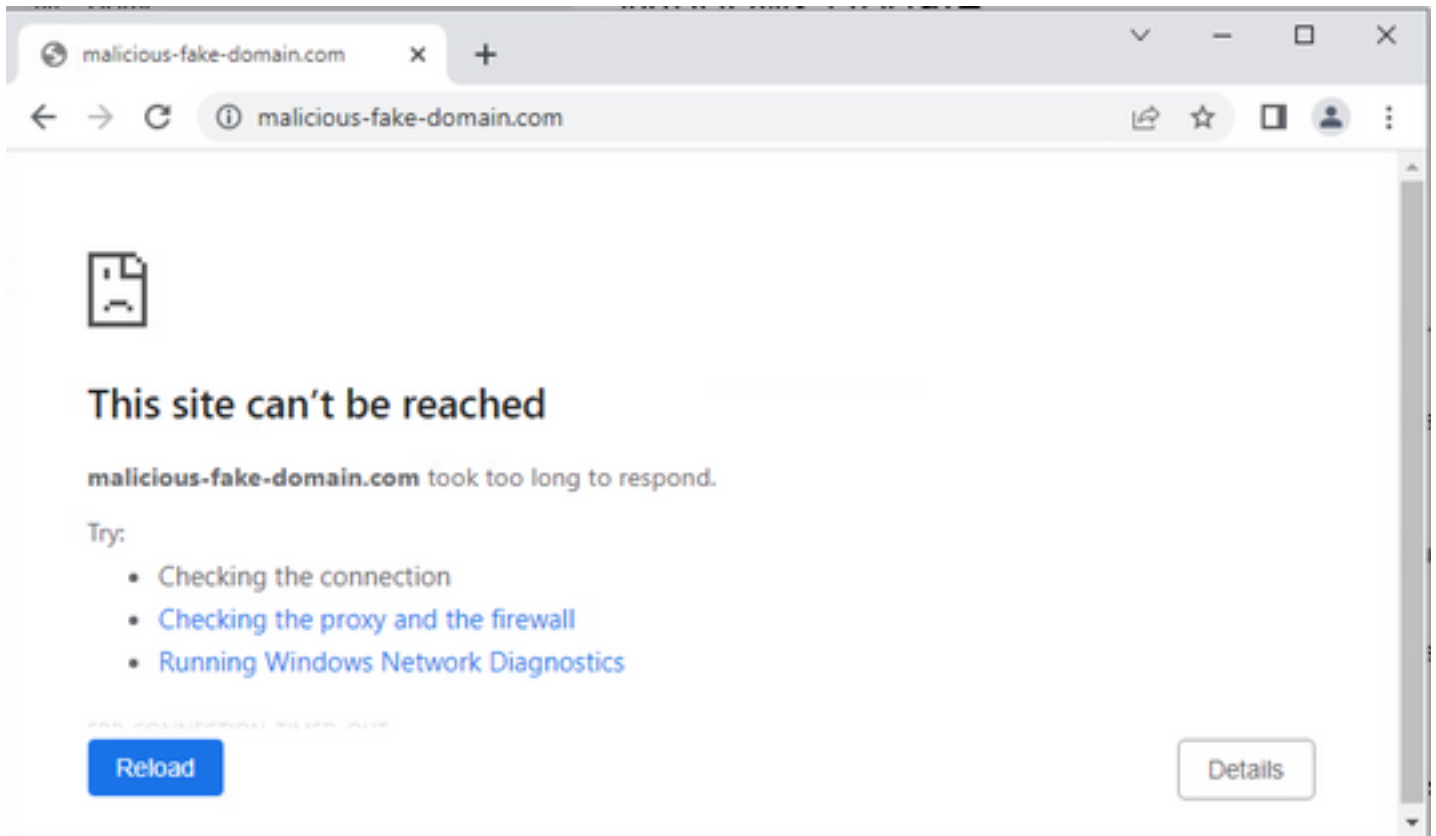
TID Detection

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

Pause Resume

Verifica

Al termine della configurazione, l'endpoint tenta di connettersi all'URL `https://malicious-fake-domain[.]com` ospitato nell'area Esterna, ma le connessioni non riescono come previsto.



Per verificare se l'errore di connessione è dovuto al feed di Threat Intelligence, passare a Integrations > Intelligence > Incident. Gli eventi bloccati devono essere elencati in questa pagina.

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

È possibile verificare questi eventi di blocco in Analisi > Connessioni > Eventi correlati alla sicurezza:

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](#)

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://

Un'acquisizione LINA FTD consente di visualizzare il traffico tra l'endpoint e l'URL dannoso

attraverso il controllo multiplo. Il controllo della fase 6 del motore di snort restituisce un risultato negativo, in quanto la funzionalità Threat Intelligence utilizza il motore di snort per il rilevamento avanzato del traffico. Tenere presente che il motore Snort deve consentire la prima coppia di pacchetti al fine di analizzare e comprendere la natura della connessione per attivare correttamente un rilevamento. Per ulteriori informazioni sulle acquisizioni LINA FTD, consultare la sezione Informazioni correlate.

```
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

Risoluzione dei problemi

- Per essere certi che Threat Response mantenga aggiornato il feed con le informazioni corrette, puoi navigare nel browser fino all'URL del feed e vedere gli oggetti osservabili condivisi.



- Per la risoluzione dei problemi relativi a FMC Threat Intelligence Director, fare clic sul collegamento Informazioni correlate.

Informazioni correlate

- [Configurazione e risoluzione dei problemi di Cisco Threat Intelligence Director](#)
- [Configurazione di Secure Firewall Threat Intelligence Director su FMC 7.3](#)
- [Uso di Firepower Threat Defense Capture e Packet Tracer](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).