

Firepower에서 URL을 차단하도록 SecureX 위협 응답 피드 구성

목차

[소개](#)

[배경 정보](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[SecureX 위협 응답 피드 생성](#)

[위협 대응 피드를 사용하도록 FMC Threat Intelligence Director 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Firepower에서 사용할 위협 대응 조사 중에 발견된 URL 및 IP로부터 위협 인텔리전스를 생성하는 방법에 대해 설명합니다.

배경 정보

Cisco Threat Response는 여러 모듈의 정보를 통해 전체 환경의 위협을 조사할 수 있는 강력한 툴입니다. 각 모듈은 Firepower, Secure Endpoint, Umbrella 및 기타 서드파티 벤더와 같은 보안 제품에서 생성된 정보를 제공합니다. 이러한 조사를 통해 시스템에 위협이 존재하는지 확인할 수 있을 뿐만 아니라 중요한 위협 인텔리전스를 생성하는 데 도움이 될 수 있습니다. 이를 보안 제품에 다시 소싱하여 환경의 보안을 강화할 수 있습니다.

SecureX Threat Response에서 사용하는 몇 가지 중요한 용어:

- **지표**는 AND 및 OR 연산자와 논리적으로 관련된 관찰 가능 항목의 컬렉션입니다. 여러 개의 관찰 가능한 요소를 결합하는 복잡한 표시기가 있으며, 하나의 관찰 가능한 요소로만 구성된 간단한 표시기도 있습니다.
- **Observable**은 IP, Domain, URL 또는 sha256일 수 있는 변수입니다.
- **판단**은 사용자에게 의해 생성되고, 관찰 가능을 특정 기간 동안의 성향과 연결하는 데 사용됩니다.
- **피드**는 SecureX Threat Response 조사에서 생성된 위협 인텔리전스를 방화벽, 이메일 콘텐츠 필터(Firepower, ESA) 등의 다른 보안 제품과 공유하기 위해 생성됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SecureX CTR(Cisco 위협 대응
- Firepower TID(Threat Intelligence Director).
- Firepower 액세스 제어 정책 컨피그레이션입니다.

이 문서에서는 Firepower TID를 사용하여 SecureX Threat Response에서 생성된 위협 인텔리전스를 적용합니다. FMC 버전 7.3에 대해 FMC 구축에서 TID를 사용하려면 다음과 같은 요구 사항이 있어야 합니다.

- 버전 6.2.2 이상
- 최소 15GB의 메모리로 구성됩니다.
- REST API 액세스가 활성화된 상태로 구성됩니다. Cisco Secure Firewall Management Center Administration Guide의 Enable REST API Access를 참조하십시오.
- 디바이스가 버전 6.2.2 이상에 있는 경우 FTD를 위협 인텔리전스 디렉터 요소로 사용할 수 있습니다.

참고: 이 문서에서는 Threat Intelligence Director가 시스템에서 이미 활성화되어 있는 것으로 간주합니다. TID 초기 컨피그레이션 및 문제 해결에 대한 자세한 내용은 Related Information(관련 정보) 섹션에서 사용 가능한 링크를 확인하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SecureX Cisco 위협 대응 대시보드
- FMC(Firewall Management Center) 버전 7.3
- FTD(Firewall Threat Response) 버전 7.2

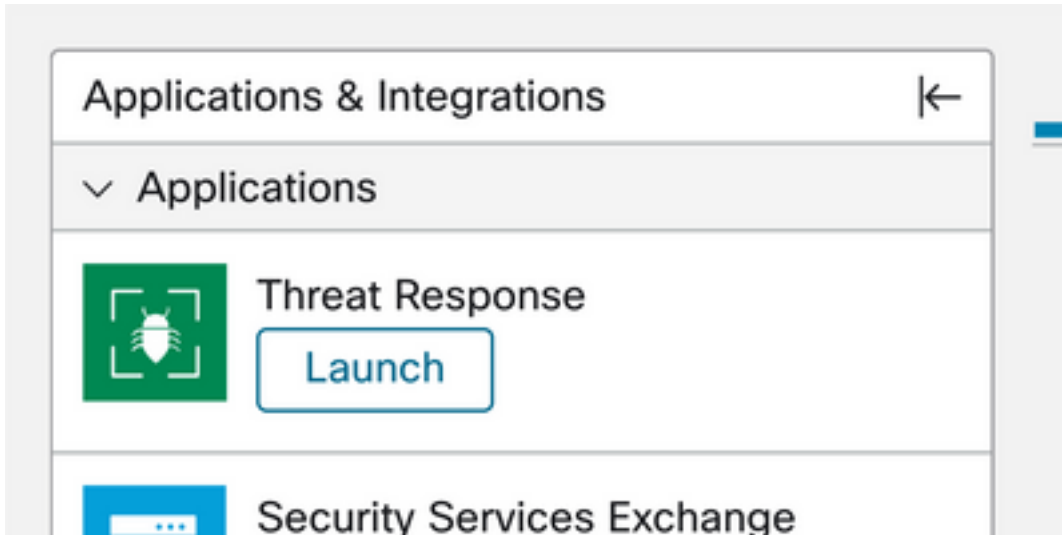
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

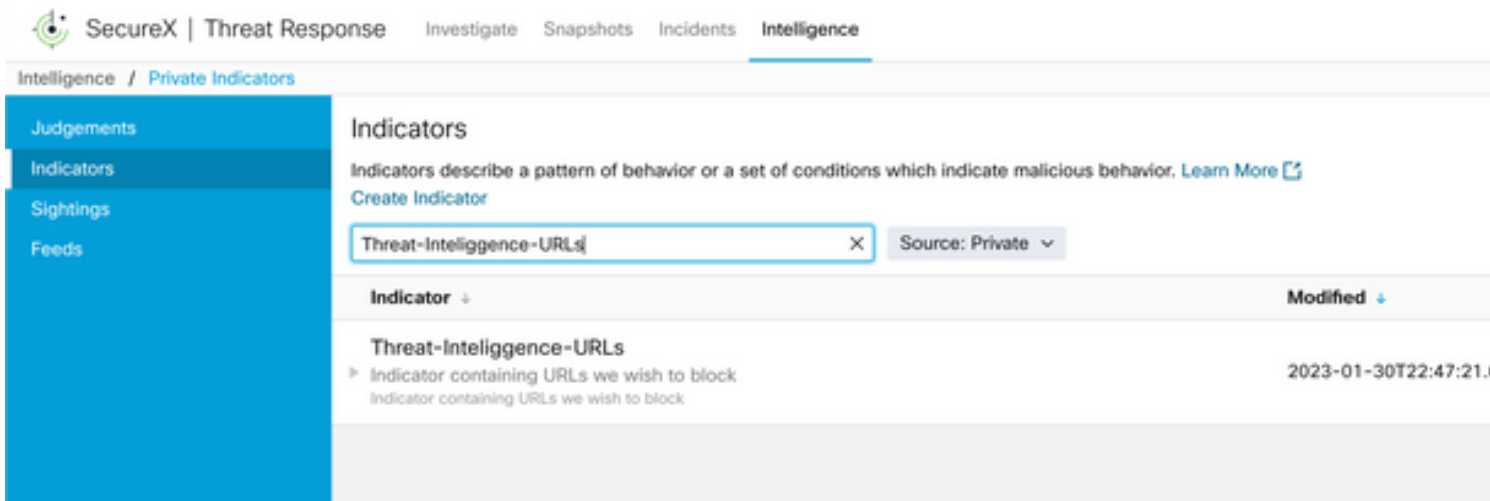
SecureX 위협 응답 피드 생성

SecureX Threat Response를 사용하면 관찰 가능한 as 입력을 사용하여 환경에 대한 조사를 시작할 수 있습니다. 위협 응답 엔진은 모듈을 쿼리하여 관측 가능한 것과 관련된 활동을 검색합니다. Investigation은 모듈에서 찾은 일치를 반환합니다. 이 정보에는 IP, 도메인, Url 이메일 또는 파일이 포함될 수 있습니다. 다음 단계에서는 다른 보안 제품과 함께 정보를 사용할 피드를 생성합니다.

1단계 SecureX 대시보드에 로그인하고 Threat Response **Module**의 Launch(실행) 버튼을 클릭합니다. 그러면 새 창에서 Threat Response(위협 대응) 페이지가 열립니다.



2단계 Threat Response(위협 대응) 페이지에서 Intelligence(인텔리전스) > Indicators(표시기)를 클릭한 다음 Source(소스) 드롭다운 목록을 Public(공개)에서 Private(비공개)로 변경합니다. 이렇게 하려면 Create Indicator(표시기 생성) 링크를 클릭해야 합니다. 표시기 작성기 마법사 내부에서 표시기에 대한 의미 있는 제목과 설명을 선택한 다음 URL 감시 목록 확인란을 선택합니다. 이 시점에서 표시기를 저장할 수 있지만 추가 정보는 필요하지 않습니다. 그러나 사용 가능한 나머지 옵션을 구성하도록 선택할 수 있습니다.



3단계 Investigate(조사) 탭으로 이동하여 조사하려는 관찰 가능 항목을 조사 상자에 붙여넣습니다. 데모용으로 위조 URL <https://malicious-fake-domain.com> 이(가) 이 컨피그레이션 예시에 사용되었습니다. Investigate를 클릭하고 조사가 완료될 때까지 기다립니다. 예상대로 더미 URL 속성을 알 수 없습니다. 아래쪽 측면 화살표를 마우스 오른쪽 버튼으로 클릭하여 상황에 맞는 메뉴를 확장하고 Create Judgement(판단 생성)를 클릭합니다.



4단계 Link Indicators(표시기 링크)를 클릭하고 2단계에서 표시기를 선택합니다. Disposition(처리)을 Malicious(악의적)로 선택하고 Expiration day(만료일)를 적절히 선택합니다. 마지막으로 Create(생성) 버튼을 클릭합니다. URL은 Intelligence(인텔리전스) > Indicators(표시기) > View Full Indicator(전체 표시기 보기) 아래에서 볼 수 있어야 합니다.

Create Judgement ✕

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

Indicators* ℹ

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 Malicious 🚫	Domain	2023-01-30T23:34:24.5... 2023-03-02T23:34:24.5...	

<
>
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

5단계 Intelligence(인텔리전스) > Feeds(피드)로 이동하고 Create Feed URL(피드 URL 생성)을 클릭합니다. 제목 필드를 채운 다음 2단계에서 만든 표시기를 선택합니다. 출력 드롭 다운 목록을 관찰 가능한 상태로 남겨두고 저장을 클릭 합니다.

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

6단계 Intelligence(인텔리전스) > Feeds(피드)에서 피드가 생성되었는지 확인한 다음 클릭하여 피드 세부사항을 확장합니다. URL을 클릭하여 예상 URL이 피드에 나열됨을 시각화합니다.

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

위협 대응 피드를 사용하도록 FMC Threat Intelligence Director 구성

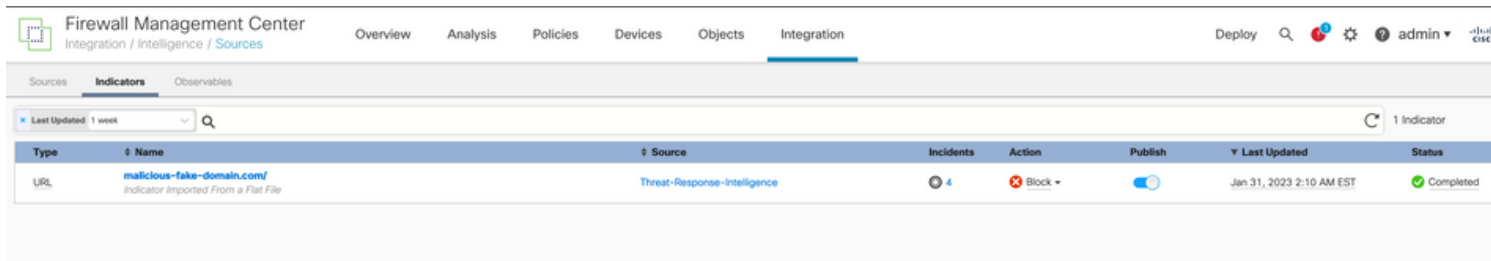
1단계 FMC 대시보드에 로그인하고 Integration(통합) > Intelligence(인텔리전스) > Sources(소스)로 이동합니다. 새 소스를 추가하려면 더하기 쉬운 숨을 클릭합니다.

2단계 다음 설정으로 새 소스를 만듭니다.

- 전달 > URL 선택
- 문자 > 플랫폼 파일 선택
- 내용 > URL 선택
- Url > 5단계 "Create SecureX Threat Response Feed(SecureX 위협 응답 피드 생성)" 섹션의 URL을 붙여넣습니다.
- Name(이름) > 맞는 이름을 선택합니다.
- Action(작업) > Select Block(차단 선택)
- Update Every(업데이트 간격) > Select 30 min(Threat Intelligence 피드의 빠른 업데이트)

저장을 클릭합니다.

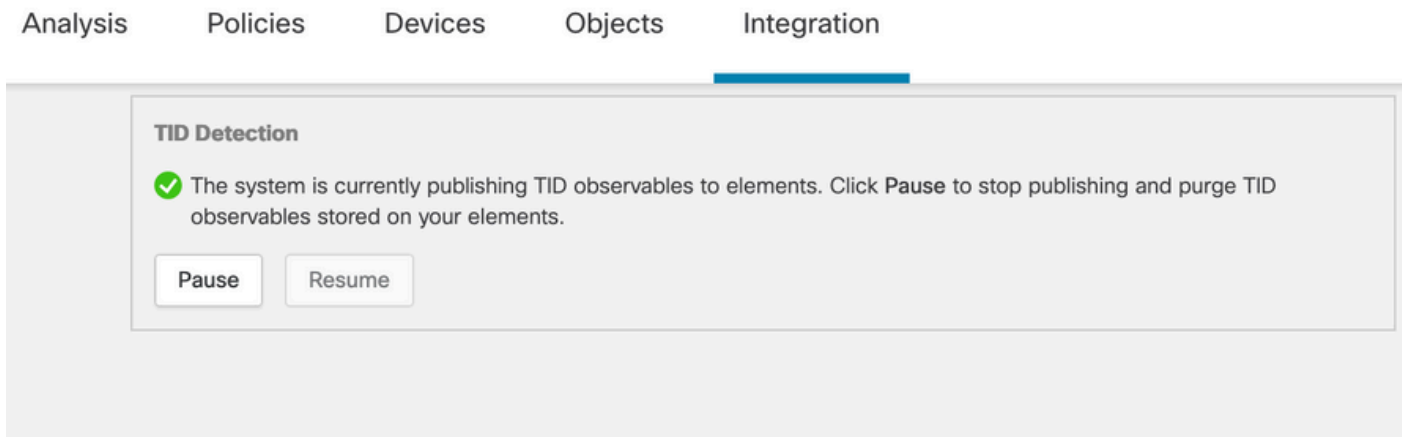
3단계 Indicators and Observables verify domain(지표 및 관찰 가능 항목 확인) 아래에 다음 항목이 표시됩니다.



The screenshot shows the 'Indicators' tab in the Firewall Management Center. A table lists one indicator with the following details:

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

4단계 Threat Intelligence Director가 활성 상태인지 확인하고 요소를 최신 상태로 유지합니다(FTD 디바이스). Integrations > Intelligence > Elements로 이동합니다.



The screenshot shows the 'TID Detection' status in the 'Intelligence' section. It indicates that the system is currently publishing TID observables to elements. There are 'Pause' and 'Resume' buttons available.

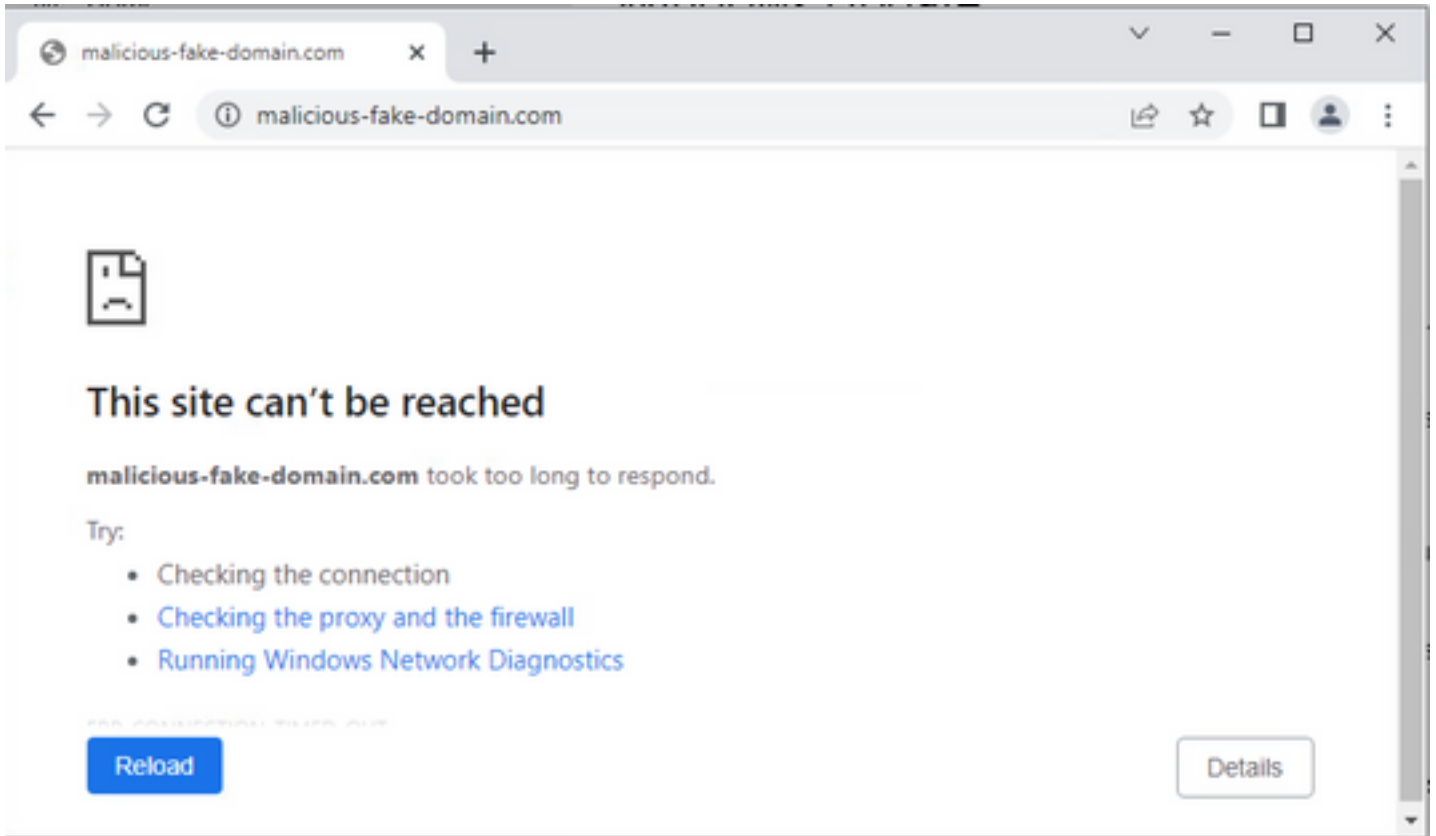
TID Detection

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

Pause Resume

다음을 확인합니다.

컨피그레이션이 완료되면 엔드포인트는 외부 영역에서 호스팅되는 https://malicious-fake-domain[.]com URL에 연결을 시도하지만 연결이 예상대로 실패합니다.



연결 실패가 위협 인텔리전스 피드로 인한 것인지 확인하려면 Integrations(통합) > Intelligence(인텔리전스) > Incidents(인시던트)로 이동합니다. 차단된 이벤트는 이 페이지에 나열되어야 합니다.

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

Analysis(분석) > Connections(연결) > Security-Related Events(보안 관련 이벤트)에서 다음 차단 이벤트를 확인할 수 있습니다.

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://

FTD LINA 캡처를 사용하면 엔드포인트에서 악성 URL로의 트래픽을 다중 검사를 통해 확인할 수

있습니다. Threat Intelligence 기능은 고급 트래픽 탐지를 위해 snort 엔진을 사용하므로 Snort Engine Phase 6 확인은 삭제 결과를 제공합니다. Snort 엔진이 탐지를 올바르게 트리거하려면 연결의 특성을 분석하고 파악하기 위해 첫 번째 패킷 쌍을 허용해야 합니다. FTD LINA 캡처에 대한 자세한 내용은 Related Information 섹션을 참조하십시오.

```
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=0x14745c5c80, 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'
```

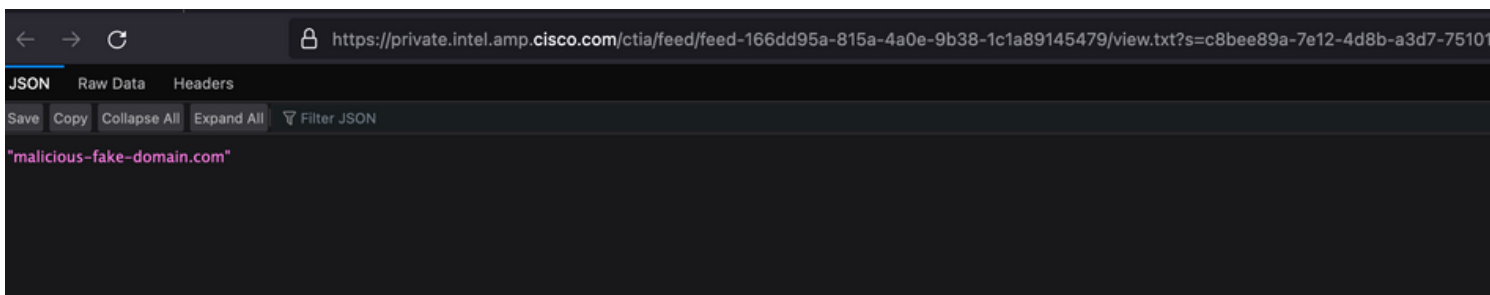
```
Phase: 5
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 655704 ns
Config:
Additional Information:
service: HTTPS(1122), client: SSL client(1296), payload: (0), misc: (0)
```

```
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
```

문제 해결

- 위협 대응이 올바른 정보로 피드를 최신 상태로 유지하도록 하려면 브라우저에서 피드 URL로 이동하여 공유 관찰 가능 항목을 볼 수 있습니다.



- FMC Threat Intelligence Director의 문제를 해결하려면 관련 정보의 링크를 확인하십시오.

관련 정보

- [Cisco Threat Intelligence Director 구성 및 문제 해결](#)
- [FMC 7.3에서 Secure Firewall Threat Intelligence Director 구성](#)
- [Firepower Threat Defense 캡처 및 패킷 추적기 사용](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.