FirepowerでURLをブロックするための SecureX脅威応答フィードの設定

内容

概要 背景説明 前提条件 要件 使用するコンポーネント 設定 SecureX脅威応答フィードの作成 Threat Response Feedを使用するためのFMC Threat Intelligence Directorの設定 確認 トラブルシュート 関連情報

概要

このドキュメントでは、Firepowerで使用される脅威応答調査中に検出されたURLおよびIPから脅威インテリジェンスを作成する方法について説明します。

背景説明

Cisco Threat Responseは、複数のモジュールからの情報を利用して、環境全体で脅威を調査でき る強力なツールです。各モジュールは、Firepower、セキュアエンドポイント、Umbrella、その他 のサードパーティベンダーなどのセキュリティ製品によって生成された情報を提供します。これ らの調査は、システムに脅威が存在するかどうかを明らかにするだけでなく、重要な脅威インテ リジェンスを生成するのに役立ちます。脅威インテリジェンスは、セキュリティ製品に戻され、 環境内のセキュリティを強化することができます。

SecureX Threat Responseで使用される重要な用語は次のとおりです。

- Indicatorは、ANDおよびOR演算子に論理的に関連する観測可能な変数の集合です。 複数の 観測可能を組み合わせた複雑な指標があり、また一つの観測可能のみで構成された単純な指 標もあります。
- Observableは、IP、ドメイン、URL、またはsha256である変数です。
- **判定**はユーザによって作成され、特定の期間の処分に監視可能なものをリンクするために使 用されます。
- フィードは、SecureX Threat Responseの調査によって生成された脅威インテリジェンスを、ファイアウォールなどの他のセキュリティ製品や、FirepowerやESAなどの電子メールコンテンツフィルタと共有するために作成されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SecureX CTR(Cisco Threat Response)
- Firepower TID(Threat Intelligence Director)。
- Firepowerアクセスコントロールポリシーの設定。

このドキュメントでは、Firepower TIDを使用して、SecureX Threat Responseで生成される脅威 インテリジェンスを適用します。FMCバージョン7.3と同様に、FMC環境でTIDを使用するための 要件は次のとおりです。

- •バージョン 6.2.2 以降.
- •15 GB以上のメモリで構成されます。
- REST APIアクセスを有効にして設定します。『Cisco Secure Firewall Management Center Administration Guide』の「Enable REST API Access」を参照してください。
- デバイスがバージョン6.2.2以降である場合、FTDを脅威インテリジェンスディレクタ要素として使用できます。

注:このドキュメントでは、Threat Intelligence Directorがシステム上ですでにアクティブで あると見なしています。TIDの初期設定とトラブルシューティングの詳細については、「関 連情報」セクションのリンクを参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- SecureX Cisco Threat Responseダッシュボード
- FMC(Firewall Management Center)バージョン7.3
- FTD(Firewall Threat Response)バージョン7.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

設定

SecureX脅威応答フィードの作成

SecureX Threat Responseを使用すると、監視可能な情報を入力として、環境内の調査を開始で きます。Threat Response Engineは、モジュールに対してクエリを実行し、オブザーブに関連す るアクティビティを検索します。Investigationは、モジュールで検出された一致を返します。こ の情報には、IP、ドメイン、URLの電子メールまたはファイルが含まれます。次の手順では、他 のセキュリティ製品で情報を消費するフィードを作成します。

ステップ1 SecureXダッシュボードにログインし、Threat Response Moduleの[Launch] ボタンを クリックします。新しいウィンドウで[Threat Response]ページが開きます。

Applications & Integrations						
\sim Appl	ications					
	Threat Response					
	Security Services Exchange					

ステップ2 [Threat Response (脅威対応)]ページで、[Intelligence (インテリジェンス)] > [Indicators (インジケータ)]をクリックし、[Source (送信元)]ドロップダウンリストを [Public (パブリック)]から[Private (プライベート)]に変更します。これにより、[インジケータ の作成]リンクをクリックできるようになります。インジケータ作成ウィザード内で、インジケー タのタイトルと説明を選択したら、[URLウォッチリスト(URL Watchlist)]チェックボックスをオン にします。この時点でインジケータを保存できます。それ以上の情報は必要ありませんが、残り の使用可能なオプションを設定することもできます。

🔆 SecureX Threat Resp	OONSE Investigate Snapshots Incidents Intelligence	
Intelligence / Private Indicators		
Judgements	Indicators	
Indicators	Indicators describe a pattern of behavior or a set of conditions which indicate malicious behavior. Learn Mo	ore 🖸
Sightings	Create Indicator	
Feeds	Threat-Inteliggence-URLs X Source: Private ~	
	Indicator +	Modified +
	Threat-Inteliggence-URLs Indicator containing URLs we wish to block Indicator containing URLs we wish to block	2023-01-30T22:47:21.

ステップ3 [Investigate] タブに移動し、調査するオブザーブを調査ボックスに貼り付けます。デモ 目的で偽のURL https://malicious-fake-domain.com この設定例で使用されています。[Investigate] をクリ ックし、調査が終了するまで待ちます。予想通り、ダミーURLの配置は不明です。下矢印を右ク リックしてコンテキストメニューを展開し、Create Judgmentをクリックします。

Investigate to learn more.	Details Three
Investigate in Threat Response	> 1 TAPGET
Create Judgement	Create a new Judgement for this observable.
Jesutorr TG	+ 2 INVESTIGATEL

ステップ4 [Link Indicators] をクリックし、ステップ2のインジケータを選択します。 [disposition]で[Malicious] を選択し、必要に応じて[Expiration day]を選択します。最後に、 [Create] ボタンをクリックします。URLが[Intelligence] > [Indicators] > [View Full Indicator] に表 示されている必要があります。

Create Judgement	×
Create a new Judgement for domain:malicious-fake-domain.com	
Indicators*	
Threat-Inteliggence-URLs	ĩ
Link Indicators	
Disposition*	
Malicious	~
Expiration*	
31 🗘 Days	~
TLP	
Amber	~
Reason	
Cancel	Create
	During of

Threat-Inteliggence-URLs Edit Indicator

Description				ID	https://private.intel.amp.cisco.co
Short Description				Producer Source	Cisco - MSSP - Jobarrie None Included
Likely Impact None Included				Create Date Last Modified Expires Pervisions	2023-01-30T22:47:21.076Z 2023-01-30T22:47:21.055Z Indefinite
Kill Chain Phases None Included Judgements				Confidence Severity TLP	' High Red
Judgement	Туре	Start/End Times			
malicious-fake-domain.com	Domain 2023-01-30T23:34:24.5 2023-03-02T23:34:24.5				
Sper page Showing 1-1 of 1					

Foods

ステップ5 [Intelligence] > [Feeds] に移動し、[Create Feed URL] をクリックします。 **Title**フィー ルドに入力し、ステップ2で作成した**Indicator**を**選択**します。必ず[Output] ドロップダウンリスト を[observables] のままにして、[Save] をクリックします。

Threat-Intelligence-TR-URLs		
Indicator* 0		
Threat-Inteliggence-URLs - Indicator containing URLs we wish to block		~
Output 🕕		
Observables		~
Expiration* 🕕		
January 30, 2023		
V Forever		
Anyone with the URL will be able to view this feed.		
	Cancel	Save

ステップ6 [Intelligence] > [Feeds] でフィードが作成されたことを確認し、をクリックしてフィードの詳細を展開します。URLをクリックすると、フィードに予期されるURLが表示されます。

SecureX Threat Res	sponse Inves	stigate Snapshots Incidents Intelligence											
Intelligence / Feeds	_												
Judgements	Feeds												
Indicators	These feeds v	were created or saved from private sources. Anyo	one with the URL can view the feed.										
Sightings	Create Feed	Create Feed URL											
Feeds	Search	×											
	Feed		Created +										
	Threat-Int Observable	telligence-TR-URLs	2023-01-31T00:33:26.288Z Admin El mero mero 2										
	Title: Output:	Threat-Intelligence-TR-URLs Observables											
	Created: Creator:	2023-01-31T00:33:26.288Z Admin El mero mero 2											
	Expiration:	Indefinite											
	URL:	https://private.intel.amp.cisco.com:443/ctia/feed/fe	eed-166dd95a-815a-4a0e-9b38-1c1a89145479/view.txt?s=c8bee89a-7e12-4d8b-a3d7-751014cedc20										
	Show JSO	N											

Threat Response Feedを使用するためのFMC Threat Intelligence Directorの設定

ステップ1 FMCダッシュボードにログインし、[Integration] > [Intelligence] > [Sources] に移動し ます。 **プラス**ため息をクリックして、新しい送信元を追加します。 ステップ2次の設定で新しいソースを作成します。

- [Delivery] > [Select URL]
- Type > Select Flat File
- •[コンテンツ] > [URLの選択]
- [Url] > [Create SecureX Threat Response Feed]セクションのURLを貼り付けます。ステップ 5.
- [Name] > [Choose any name you see fit]
- •アクション>ブロックの選択
- [Update Every] > [Select 30 min](脅威インテリジェンスフィードのクイックアップデート用)

[Save] をクリックします。

ステップ3:[Indicators and Observables(インジケータとオブザーブ)]で、ドメインがリストされ ていることを確認します。

Firew Integrat	all Management Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 💕 🔅 🕢 admin				n • alta			
Sources Inc	ficators Observables														
× Last Updated 1 we	≪ ∨ Q												(C 1 Indica	tor
Type	¢ Name				¢ Source	•		Inc	cidents	Action	Publish	▼ Last Updated		Stat	us
URL	malicious-fake-domain.com/ Indicator Imported From a Flat File				Threat-R	esponse-Intellige	nce	0	4	😣 Block 🕶		Jan 31, 2023 2:10	AM EST	0	Completed

ステップ4 Threat Intelligence Directorがアクティブで、要素を最新の状態に保っていることを確認します(FTDsデバイス)。[Integrations] > [Intelligence] > [Elements] に移動します。

Analysis	Policies	Devices	Objects	Integration	
	TID Detection	is currently publishing	g TID observables	to elements. Click Pause to stop publishing and purge TID	
	observables Pause	s stored on your eleme	ents.		

確認

設定が完了すると、エンドポイントはOutsideゾーンでホストされているhttps://malicious-fakedomain[.]com URLへの接続を試みますが、接続は期待どおりに失敗します。



接続障害の原因が脅威インテリジェンスフィードであるかどうかを確認するには、[統合 (Integrations)] > [インテリジェンス(Intelligence)] > [インシデント(Incidents)]に移動します。ブロ ックされたイベントは、このページに表示する必要があります。

Firewall Integration /	Management Center Intelligence / Incidents	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q	¢ 😵	🕜 admin	t ¥ dia Gis
× Last Updated 6 hours	~ Q										C 4 Incident	its
▼ Last Updated	Incident ID					Indicator Na	me	Туре		Action Taken	¢ Sta	tus
6 seconds ago	O URL-20230131-4					malicious-fake-	domain.com/	URL		Blocked	New	
6 seconds ago	Q URL-20230131-3					malicious-fake-	domain.com/	URL		Blocked	New	
6 seconds ago	O URL-20230131-1					malicious-fake-	domain.com/	URL	1	8 Blocked	New	
6 seconds ago	O URL-20230131-2					malicious-fake-	domain.com/	URL		Blocked	New	

これらのブロックイベントは、[Analysis] > [Connections] > [Security-Related Events]で確認できます。

Ę	Fi An	rewall Managem alysis / Connections / S	ent Center ecurity-Related Events	0	verview	Analysis	Policies	s Devices	Objects	Integration					Deploy	२ 💕 🔅	0	admin 🔻	alta Cist
Se	Bookmark This Page Reporting Dashboard View Bookmark Security-Related Connection Events (webt workfree)																		
N	II 2023-01-31 08:30:18 - 2023-01-							-01-											
S	No Search Constraints (Lair Search) Security-Related Connections with Application Details Table View of Security-Related Connection Events																		
J	ump 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	Wet	b dication	URL
		2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	0 10.5.5.5		0.31.124.250		TID URL Block	Inside	Outside	31604 / tcp	443 (https) / tcp	HTTPS	SSL clie	int		https
		2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	0 10.5.5.5		0 10.31.124.250		TID URL Block	Inside	Outside	24438 / tcp	443 (https) / tcp	HTTPS	SSL clie	nt		https
		2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	0 10.5.5.5		0.31.124.250		TID URL Block	Inside	Outside	59088 / tcp	443 (https) / tcp	HTTPS	SSL clie	nt		https
*		2023-01-31 09:24:02	2023-01-31 09:24:03	Block	URL Block	0.5.5.5		0.31.124.250		TID URL Block	Inside	Outside	59087 / tcp	443 (https) / tcp	HTTPS	🗆 SSL clie	nt		https
		2023-01-31 09:18:33	2023-01-31 09:18:33	Block	URL Block	0 10.5.5.5		0.31.124.250		TID URL Block	Inside	Outside	58956 / tcp	443 (https) / tcp	HTTPS	SSL clie	int		https:
		2023-01-31 00-18-33	2023-01-31 00-18-33	Black	LIDI Block	10555		10 31 124 250		TID LIDI Rivek	Insida	Outsida	23474 / Ico	AA3 (https) / top	IT HTTPS	E SSI dia	est.		https

FTD LINAキャプチャを使用すると、複数のチェックでエンドポイントから悪意のあるURLへのト ラフィックを確認できます。Snortエンジンのフェーズ6チェックでは、高度なトラフィック検出 にSnortエンジンが使用されるため、ドロップ結果が返されることに注意してください。Snortエ ンジンでは、接続の性質を分析および理解して検出を正しくトリガーするために、最初のパケッ トの組み合わせを許可する必要があることに注意してください。FTD LINAキャプチャの詳細に ついては、「関連情報」セクションを参照してください。

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, 13_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

トラブルシュート

• Threat Responseが正しい情報でフィードを最新の状態に保つことを確認するには、ブラウザ でフィードURLに移動し、共有されている監視可能な項目を確認します。

$\leftarrow \ \ \rightarrow \ \ \mathbf{G}$	A https://private.intel.amp.cisco.com/ctia/feed/feed-166dd95a-815a-4a0e-9b38-1c1a89145479/view.txt?s=c8bee89a-7e12-4d8b-a3d7-75101
JSON Raw Data Headers	
Save Copy Collapse All Expand All	7 Filter JSON
"malicious-fake-domain.com"	

• FMC Threat Intelligence Directorのトラブルシューティングについては、「関連情報」のリン クを参照してください。

関連情報

- <u>Cisco Threat Intelligence Directorの設定とトラブルシューティング</u>
- FMC 7.3でのSecure Firewall Threat Intelligence Directorの設定
- <u>Firepower Threat Defense(FTD)のキャプチャとPacket Tracerの使用</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。