Cisco Secure Firewall Management Center バージョン 7.4.0 によって収集される Cisco Success Network テレメトリデータ

初版：2023 年 9 月 11 日

最終更新：2023 年 9 月 7 日

Cisco Secure Firewall Management Center によって収集される Cisco Success Network テレメトリデータ

Cisco Success Network では、登録済み Management Center はリアルタイムの設定と動作の状態に関する情報を Cisco Success Network Cloud に継続的にストリーミングすることができます。このドキュメントでは、収集およびモニターされるデータのリストを示します。

登録済みデバイス データ

Cisco Success Network に Management Center を登録したら、登録済みの Management Center デバイスに関する選択したテレメトリデータが Cisco Cloud へストリーミングされます。次の表に、登録済みのデバイスに関して収集し、監視しているデータを示します。このデータには、侵入ポリシー（システムが提供するポリシーとカスタムポリシーの両方）および登録済みの Management Center のマルウェア検出に関する機能に固有の情報が含まれます。

表 *1*：登録済みデバイスのテレメトリ データ

データ ポイント	値の例
デバイス名（Device Name）	Management Center East
デバイス UUID	24fd0ccf-1464- 491f-a503- d241317bb327
デバイス モデル	Cisco Secure Firewall Management Center for VMWare
シリアル番号（Serial Number）	9AMDESQP6UN
システム稼動時間（System Uptime）	99700000
製品 ID（Product Identifier）	FS-VMW-SW-K9
スマート ライセンス PIID	24fd0ccf-1464- 491f-a503- d241317bb327

データ ポイント	値の例
仮想アカウント識別子	CiscoSVStemp
スマートライセンスバーチャルアカウント名	FTD-ENG-SJC
有効な SSO の数。	1
SSO ユーザーの数。	2
SSO アイデンティティ プロバイダー。	okta
Management Center の SecureX 機能が有効かどうか。	1

ソフトウェア バージョン データ

Cisco Success Network は、ソフトウェアのバージョン、ルールの更新バージョン、地理位置情報データベースのバージョン、脆弱性データベースのバージョン情報など、登録済みの Management Center デバイスに関連するソフトウェア情報を収集します。次の表に、登録済みのデバイスに関して収集し、監視しているソフトウェア情報を示します。

表 *2:* ソフトウェア バージョンのテレメトリ データ

データ ポイント	値の例
Management Center ソフトウェアバージョン	{ type: "SOFTWARE", version: "x.x.x.x" }
ルールの更新バージョン	{version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }
脆弱性データベース（VDB）のバージョン	{version: "271", lastUpdated: 1468606837000 }
地理的位置情報データベースのバージョン	{version: "850" }

管理対象デバイス データ

Cisco Success Network は、登録済み Management Center に関連付けられているすべての管理対象デバイスに関する情報を収集します。次の表に、管理対象デバイスに関して収集し、監視している情報を示します。これには、管理対象デバイスの URL フィルタリング、侵略防御、およびマルウェア 検出など、機能に固有のポリシーおよびライセンス情報が含まれます。

表 *3:* 管理対象デバイスのテレメトリ データ

データ ポイント	値の例
管理対象デバイス名。	firepower
管理対象デバイスバージョン。	6.2.3-10616

データ ポイント	値の例
管理対象デバイスマネージャ。	Management Center
管理対象デバイスモデル。	Cisco Firepower 2130 NGFW アプライアンス Cisco Threat Defense VMware
管理対象デバイスのシリアル番号。	9AMDESQP6UN
管理対象デバイスの PID。	FPR2130-NGFW-K9 NGFWv
Snort エンジン。	SNORT3
データの取得に失敗した場合の localUrlCount プラグインのエラー。	"errors": ["Ping DB trial no. 1 ", "SF::SFDBI::ping", "Ping returned 1", "Can't call method \"getPayload\" on an undefined value at /usr/local/sf/lib/perl/5.10.1/SF/CSMAgent.pm line 1906.", "", "Printing stack trace:", " called from /usr/local/sf/lib/perl/5.10.1/SF/CSMAgent. pm (1906)", " called from /usr/local/sf/lib/perl/5.10.1/SF/SSE/devices _plug.pm (409)", " called from /usr/local/sf/bin/devices_plug.pl (76)", " called from /usr/local/sf/bin/devices_plug.pl (93)"]
デバイスがマネージャに接続されているかどうか。	はい（True）
コンテナのステータス（Standalone、Cluster、または HA）。	"Cluster"
デバイスのオンボーディング方式	USING_SERIAL_NUMBER_VIA_CDO

データ ポイント	値の例
デバイスにURLフィルタリング ライセンスを使用しているか	True
デバイスごとにURLフィルタリングを使用する AC ルール。	10
URL フィルタリングライセンスを使用する URL フィルタリングでの AC ルールの数。	3
脅威ライセンスを使用するURLフィルタリングでの AC ルールの数。	3
デバイスに脅威ライセンスを使用しているか	True
AC ポリシーに侵略ルールを追加しているか	True
侵入ポリシーを使用する AC ルールの数。	10
デバイスにマルウェア ライセンスを使用しているか	True
マルウェアポリシーを使用する AC ルールの数。	10
マルウェアライセンスを使用するマルウェアポリシーでの AC ルールの数。	5
デバイスに Threat Intelligence Director (TID) を使用しているか	True
静的ルートの数。	4
VRF 数。	0
デバイスでの HA のリモート展開が試行されているかどうか。	いいえ（False）
デバイス証明書が表示されるかどうか。	いいえ（False）
管理対象デバイスに nsz 値が設定されているかどうか。	いいえ（False）
管理対象デバイスに ogs 値が設定されているかどうか。	いいえ（False）
NS ネットワーク数。	2

データ ポイント	値の例
ローカル URL 項目の数。	{"url": "/api/local/fmc_config/v1/domain/{domainUUID}/object/networks", "count": 10}, {"url": "/api/local/fmc_platform/v1/info/serverversion", "count": 2}

次の表に、ポートスキャン設定に関するすべての情報を示します。

データ ポイント	値の例
トラフィックの検出	"Allowed"
ICMP ホスト	50
ICMP ホストスイープが有効かどうか。	TRUE
ICMP 間隔	50
インスペクションモード	"Detection"
IP ホスト	50
IP 間隔	50
IP プロトコル	50
IP プロトコルスキャンが有効かどうか。	TRUE
IP プロトコルスイープが有効かどうか。	TRUE
重要度タイプ	"Custom"
排除期間	50
TCP 間隔	100
TCP ポート（TCP port）	72
TCP ポートホスト	59
TCP ポートスキャンが有効かどうか。	TRUE
TCP ポートスイープが有効かどうか。	TRUE
UDP ホスト	50
UDP 間隔	50
UDP ポート（UDP port）	50
UDP ポートスキャンが有効かどうか。	TRUE

データ ポイント	値の例
UDP ポートスイープが有効かどうか。	TRUE

Cisco Success Network は、ある Threat Defense モデルから同等以上の容量のモデルへの設定の移行に関する情報を収集します。次の表に、Threat Defense モデル移行に関して収集される情報を示します。

データ ポイント	値の例
経過時間	6366
エラー	0 以上の整数値
モデル移行が完了しているかどうか。	はい（True）
デバイスがリセットされているかどうか。	いいえ（False）
インターフェイスの数	0 以上の整数値
送信元デバイスのコンテナのステータス（Standalone、Cluster、または HA）	"Standalone"
送信元デバイスのモデル	"Cisco Firepower 2130 Threat Defense"
送信元デバイスの UUID	"a8eee3f4-aa19-11ed-bda9-857788e8d45a"
IP プロトコルスキャンが有効かどうか。	TRUE
送信元デバイスの Threat Defense バージョン	"7.2.0"
ターゲットデバイスコンテナのステータス（Standalone、Cluster、または HA）	"Standalone"
ターゲットデバイスのモデル	"Cisco Secure Firewall 3105 Threat Defense"
ターゲットデバイスの Threat Defense バージョン	"7.3.0"

次の表に、ポリシーレベルごとのすべての情報を示します。

データ ポイント	値の例
Snort2 に割り当てられたアクセスポリシーデバイスの数	1
Snort3 に割り当てられたアクセスポリシーデバイスの数	0
アクセスポリシーのカスタム IPS ポリシーの数	1

データ ポイント	値の例
アクセスポリシーのカスタムNAPポリシーの数	1
IPS syslog が有効かどうか。	いいえ（False）
syslog の接続先がオーバーライドされるかどうか。	いいえ（False）
親ポリシー UUID	4294967319
ポリシー UUID	4294977323
アクセスポリシーのシステム IPS ポリシーの数	0
アクセスポリシーのシステムNAPポリシーの数	0
移行された Snort3 侵入ポリシーの数	1
失敗したポリシーの数	0
ポリシーが失敗した理由の数	該当なし
部分的に失敗したポリシーの数	0
ポリシーの部分的な失敗の理由の数	該当なし
成功したポリシーの数	1
Snort2 IPS に割り当てられたデバイスの数	0
有効なカスタムルールの数	0
設定されたダイナミックルールの数	0
Firepower 推奨事項を使用するかどうか	いいえ（False）
グローバルしきい値が無効かどうか	いいえ（False）
グローバルしきい値が更新されているかどうか	いいえ（False）
Snort2 IPS 親ポリシー UUID	abba00a0-cf29-425c-9d75-49699aadc898
Snort2 IPS ポリシー UUID	0e6aa778-69f2-11eb-8e9e-6475e0e0131b
機密データ検出が有効かどうか	いいえ（False）
SNMP 対応ルールの数	0

データ ポイント	値の例
設定された抑制ルールの数	0
設定されたしきい値ルールの数	0
合格した Snort2 IPS カスタムルールの数	1
置換を伴う Snort2 IPS カスタムルールの数	1
Snort2 IPS カスタムルールの数	9
割り当て済みの Snort2 ネットワーク分析ポリシーデバイスの数	0
追加された Snort2 ネットワーク分析ポリシー カスタム インスタンスの数	該当なし
最後に変更されたタイムスタンプ	2021-02-15 14:15:50
Snort2 ネットワーク分析親ポリシー UUID	abba00a0-cf29-425c-9d75-49699aadc898
Snort2 ネットワーク分析ポリシー UUID	e889a48c-6f96-11eb-969d-7075e0e0131b
Snort2 ネットワーク分析のポリシーユーザー無効インスペクタ	dns
Snort2 ネットワーク分析のポリシーユーザー編集インスペクタ	dce_rpc
Snort2 ネットワーク分析のポリシーユーザー有効インスペクタ	http_inspect、dce_rpc
Snort3 IPS に割り当てられたデバイスの数	0
有効なカスタムルールのグループの数	0
除外されたカスタムルールのグループの数	0
追加されたカスタムルールのグループの数	0
Snort3 IPS ルールオーバーライドの数	0
Snort3 IPS 親ポリシー UUID	7003
Snort3 IPS ポリシー UUID	4294973084

データ ポイント	値の例

Snort3 IPS ポリシー除外ルールグループ	<pre>[{
	"containerRuleGroupUuid":
	"c4f4121b-d8e0-5086-9ae3-064062109492",
	"leafRuleGroupUuids": [
	
	"e15f11b4-a2fc-5e7a-9549-b6638972bdf5",
	
	"d0ae8e7a-d36d-52bc-b129-a320082fb4f5"
	]
	}]</pre>

Snort3 IPS ポリシー追加ルールグループ	<pre>[{
	"containerRuleGroupUuid":
	"c4f4121b-d8e0-5086-9ae3-064062109492",
	"leafRuleGroupUuids": [
	
	"e15f11b4-a2fc-5e7a-9549-b6638972bdf5",
	
	"d0ae8e7a-d36d-52bc-b129-a320082fb4f5"
	]
	}]</pre>

Snort3 IPS ポリシー オーバーライド ルール グループ	<pre>[{
	"containerRuleGroupUuid":
	"c4f4121b-d8e0-5086-9ae3-064062109492",
	"leafRuleGroupUuids": [
	
	"e15f11b4-a2fc-5e7a-9549-b6638972bdf5",
	
	"d0ae8e7a-d36d-52bc-b129-a320082fb4f5"
	]
	}]</pre>

オーバーライドされたルールグループの数	10
Snort3 IPS カスタムルールのグループの数	2
Snort3 IPS カスタムルールの数	1
抑制された Snort3 IPS ルールの数	0
しきい値を持つ Snort3 IPS ルールの数	0
割り当て済みの Snort3 ネットワーク分析ポリシーデバイスの数	0
追加された Snort3 ネットワーク分析ポリシー カスタム インスタンスの数	該当なし
編集された Snort3 ネットワーク分析ポリシー デフォルト インスタンスの数	該当なし
Snort3 ネットワーク分析親ポリシー UUID	7303
Snort3 ネットワーク分析ポリシー UUID	4294978428

データ ポイント	値の例
Snort3 ネットワーク分析のポリシーユーザー無効インスペクタ	該当なし
Snort3 ネットワーク分析のポリシーユーザー編集インスペクタ	該当なし
Snort3 ネットワーク分析のポリシーユーザー有効インスペクタ	該当なし

管理対象クラスタデータ

Cisco Success Network は、登録済み Management Center に関連付けられているすべての管理対象クラスタに関する情報を収集します。次の表では、管理対象クラスタに関して収集およびモニターされる情報について説明します。

表 *4:* 管理対象クラスタのテレメトリデータ

データ ポイント	値の例
クラスタモデル	Cisco Threat Defense for VMware
クラスタ名	vFTDCluster
クラスタ サイズ	3
管理対象クラスタの合計数	1

導入情報

展開を設定した後、影響を受けるデバイスにその変更を展開する必要があります。次の表に、影響を受けるデバイスの数と成功か失敗かの情報を含む展開のステータスなど、設定の展開に関して収集し、モニターするデータを示します。

表 *5:* 導入情報

データ ポイント	値の例
ジョブ ID（Job ID）	8589985199

データ ポイント	値の例
アクセスポリシーのポリシーファイルの数	0 以上の整数値
アクセスポリシーのポリシーアイデンティティの数	
アクセスポリシーのポリシー IPS の数	
アクセスポリシーの NS ネットワークの数	
アクセスポリシーのオブジェクトの数	
アクセスポリシーのポリシー SSL の数	
アクセスポリシーの UI AC ルールの数	
変更されたインターフェイスの数	
変更されたオブジェクトの数	
変更されたルールの数	
コンテナタイプ	STANDALONE
CSM スナップショットの期間	1568
CSM スナップショットの終了時刻	1637750908871
CSM スナップショットの開始時刻	1637750907303
DC スナップショットの期間	24328
DC スナップショットの終了時刻	1637750933923
DC スナップショットの開始時刻	1637750909595
デルタ CLI の数	17
デルタ CLI のフェーズ 2 時間生成	523
デルタ CLI の合計時間生成	1040
展開の終了時刻	1637751003157
展開エラーメッセージ	
展開の開始時刻	1637750906704
展開ステータス	SUCCEEDED
展開タイプ	NORMAL_DEPLOYMENT

データ ポイント	値の例
デバイス モデル	Cisco Threat Defense for VMWare
デバイスの OS バージョン	Version "X.X.X"
デバイスパッケージの期間	5217
デバイスパッケージの終了時刻	1637750942073
デバイスパッケージの開始時刻	1637750936856
デバイス UUID	80e4ae98-4ceb-11ec-9593-90baf6bd6a9b
ダーティページ	
Management Center からダウンロードされたファイルの期間。	9699
Management Center からダウンロードされたファイルの終了時刻。	1637750951798
Management Center からダウンロードされたファイルの開始時刻。	1637750942099
アクティブからコピーされたファイルサイズのカウント	0 以上の整数値
フル展開かどうか。	はい（True）
アクティブ時の http ステータスの再試行回数	0 以上の整数値
適用された LINA の期間	291
適用された LINA の終了時刻	1637751001327
適用された LINA の開始時刻	1637751001036
コピーされた LINA ファイルの期間	0
コピーされた LINA ファイルの終了時刻	0
コピーされた LINA ファイルの開始時刻	0

データ ポイント	値の例
ページタイプ	[PIX_INTERFACE_NKP, *_SINGLE_NKP, PG.PLATFORM.PixInterface, PG.FIREWALL.PrefilterPolicy, PG.PLATFORM.NgfwInlineSetPage, PG.PLATFORM.AutomaticApplicationBypassPage, PG.TEMPLATE.TemplatePolicy, PG.PLATFORM.NgfwNetworkVirtualizationEndPoint, PG.PLATFORM.NgfwVirtualRouterPage, PG.PLATFORM.AsaBGPPage, PG.PLATFORM.PixDDnsPage, PG.PLATFORM.NgfwPolicyBasedRouteTablePage, PG.PLATFORM.PixStaticRouteTablePage, PG.PLATFORM.PixMBoundaryPage, PG.PLATFORM.AsaOSPFv3Page, PG.PLATFORM.PixIGMPPage, PG.PLATFORM.PixOSPFPage, PG.PLATFORM.NgfwECMPZonePage, PG.PLATFORM.PixDhcpdPage, PG.PLATFORM.PixPIMPage, PG.PLATFORM.F1IPv6StaticRouteTablePage, PG.PLATFORM.PixDhcpRelayPage, PG.PLATFORM.PixAsaEigrpPage, PG.PLATFORM.PixMroutePage, PG.PLATFORM.PixRipPix72Page, PG.FIREWALL.NGFWAccessControlPolicy, NetworkDiscovery, Snort3IntrusionPolicy, Snort3NetworkAnalysisPolicy, DNSPolicy]
ポリシーバンドルのサイズ	141908
実行中の CLI 設定の数	163
設定で取得を実行する回数	0 以上の整数値
セカンダリノード情報のリスト	
選択したページ	
Snort エクスポート ARC の数	0 以上の整数値
Snort エクスポートアクセス制御の数	0 以上の整数値
Snort エクスポートの高度なアクセス制御の数	0 以上の整数値
Snort エクスポートアプリケーションのアクセス制御の数	0 以上の整数値
Snort エクスポート DNS ポリシーのアクセス制御の数	0 以上の整数値

データ ポイント	値の例
Snort エクスポート ファイル ポリシーのアクセス制御の数	0 以上の整数値
Snort エクスポート IP レピュテーションのアクセス制御の数	0 以上の整数値
Snort エクスポート ID ポリシーのアクセス制御の数	0 以上の整数値
Snort エクスポート インテリジェント アプリケーション バイパスのアクセス制御の数	0 以上の整数値
Snortエクスポート侵入ポリシーのアクセス制御の数	0 以上の整数値
アクセス制御のSnortエクスポートランプ軽量ポリシーの数。	0 以上の整数値
アクセス制御のSnortエクスポートネットワーク分析ポリシーの数	0 以上の整数値
アクセス制御のSnortエクスポートネットワーク検出の数	0 以上の整数値
アクセス制御の Snort エクスポート プレフィルタ ポリシーの数	0 以上の整数値
アクセス制御としてのSnortエクスポートQOSポリシーの数	0 以上の整数値
Snortエクスポート SSL ポリシーのアクセス制御の数	0 以上の整数値
アクセス制御の Snort エクスポート Snort3 侵入ポリシーの数	0 以上の整数値
アクセス制御のSnortエクスポート変数セットの数	0 以上の整数値
アクセス制御のSnortエクスポートディテクタの数	0 以上の整数値
Snort エクスポート Beaker の数。	0 以上の整数値
Snort エクスポート地理位置情報の数	0 以上の整数値
Snort エクスポート LSP の数	0 以上の整数値

データ ポイント	値の例
Snort エクスポート NGFW ポリシーの数	0 以上の整数値
Snort エクスポート プラットフォーム設定の数	0 以上の整数値
Snort エクスポート センサー クラスタリングの数	0 以上の整数値
Snort エクスポート センサー ポリシーの数	0 以上の整数値
Snort エクスポート Snort の数	0 以上の整数値
Snort エクスポート状態共有の数	0 以上の整数値
アクティブ時の Snort 準備の期間	27218
アクティブ時の Snort 準備の終了時刻	1637750983442
アクティブ時の Snort 準備の開始時刻	1637750956224
Snort 再起動のステータス	いいえ（False）
アクティブ時の Snort 信号の期間	17537
アクティブ時の Snort 信号の終了時刻	1637751000981
アクティブ時の Snort 信号の開始時刻。	1637750983444

TLS/SSL インスペクション イベント データ

Firepower システムは、デフォルトではセキュア ソケット レイヤ（SSL）プロトコルまたはその後継である Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。TLS/SSL インスペクションを使用すると、暗号化トラフィックをインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセス コントロールを使用して検査したりできます。次の各表では、暗号化されたトラフィックについて Cisco Success Network と共有する統計情報について説明します。

ハンドシェイク プロセス

システムで TCP 接続での TLS/SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうかが判定されます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。

表 *6 : TLS/SSL* インスペクション : ハンドシェイクのテレメトリ データ

データ ポイント	値の例
システムは、トラフィックが**復号できず**次の状態となった場合、適用されたアクションを報告します。 • ブロック • TCP リセットによるブロック • 復号されない	0 以上の整数値
システムは、トラフィックが次の方法で**復号できた**場合、適用されたアクションを報告します。 • 既知の秘密キーを使用する。 • 置換キーのみを使用する。 • 自己署名証明書へ再署名する。 • サーバー証明書へ再署名する。	0 以上の整数値
暗号化されたトラフィックをブロックするように設定された SSL ルールの数。	0 以上の整数値
暗号化されたトラフィックをブロックし、接続をリセットするように設定された SSL ルールの数。	0 以上の整数値
着信トラフィックを復号するように設定された SSL ルールの数。	0 以上の整数値
発信トラフィックを復号するように設定された SSL ルールの数。	0 以上の整数値
暗号化されたトラフィックを復号しないように設定された SSL ルールの数。	0 以上の整数値
暗号化されたトラフィックをログに記録するように設定された SSL ルールの数。	0 以上の整数値
AC ポリシーに侵入が設定されているかどうか。	いいえ（False）
侵入が設定された AC ルールの数。	0 以上の整数値

データ ポイント	値の例
Threat Intelligence Director（TID）が有効かどうか。	はい（True）
トラフィック侵入の検出と防御を実行するために脅威ライセンスが必要だった AC ルールの数。	0 以上の整数値
脅威ライセンスがトラフィック侵入の検知と防御に使用されるかどうか。	はい（True）
URL フィルタリングが設定された AC ルールの数。	0 以上の整数値
脅威ライセンスが必要な AC ルールの数。	0 以上の整数値
URL ライセンスが必要な AC ルールの数	0 以上の整数値
脅威ライセンスが URL フィルタリングに使用されるかどうか。	はい（True）
SSL ハンドシェイクメッセージを処理するように設定されたアクションの数。	0 以上の整数値

キャッシュ データ

TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッションデータをキャッシュに保存し、それによりフルハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバー証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

表 *7: TLS/SSL* インスペクション：キャッシュのテレメトリ データ

データ ポイント	値の例
	0 以上の整数値

データ ポイント	値の例
システムは暗号化されたセッションデータおよびサーバ証明書データをキャッシュし、**キャッシュ**について SSL 接続ごとにレポートします。具体的な内容は次のとおりです。 • SSLセッション情報がキャッシュされた回数。 • SSL証明書検証キャッシュがヒットした回数。 • SSL 証明書検証キャッシュのルックアップが失敗した回数。 • SSL 元証明書キャッシュがヒットした回数。 • SSL 元証明書キャッシュのルックアップが失敗した回数。 • SSL 再署名証明書キャッシュがヒットした回数。 • SSL 再署名証明書キャッシュのルックアップが失敗した回数。 • Client Hello ダイジェスト キャッシュ エントリの回数。 • Client Hello ダイジェストキャッシュが削除された回数。 • Client Hello ダイジェストキャッシュがヒットした回数。 • Client Hello ダイジェスト キャッシュ メモリが使用された回数。 • Client Hello ダイジェストキャッシュがヒットしなかった回数。 • エンドポイント証明書キャッシュエントリの回数。 • エンドポイント証明書キャッシュメモリが使用された回数。 • 外部証明書キャッシュエントリの回数。 • 外部証明書キャッシュメモリが使用された回数。 • 内部 CA キャッシュエントリ。 • 内部CAキャッシュメモリが使用された回数。	

データ ポイント	値の例
• オブジェクト リスト キャッシュ エントリの回数。 • オブジェクト リスト キャッシュ メモリが使用された回数。 • 元の証明書キャッシュエントリの回数。 • 元の証明書キャッシュエントリのメモリが使用された回数。 • 元の証明書キャッシュが削除された回数。 • 元の証明書キャッシュがヒットした回数。 • 元の証明書キャッシュメモリが使用された回数。 • 元の証明書キャッシュがヒットしなかった回数。 • 再署名された証明書キャッシュエントリの回数。 • 再署名された証明書キャッシュエントリのメモリが使用された回数。 • 再署名された証明書キャッシュが削除された回数。 • 再署名された証明書キャッシュがヒットした回数。 • 再署名された証明書キャッシュメモリが使用された回数。 • 再署名された証明書キャッシュがヒットしなかった回数。 • サーバー名キャッシュエントリの回数。 • サーバー名キャッシュが削除された回数。 • サーバー名キャッシュがヒットした回数。 • サーバー名キャッシュメモリが使用された回数。 • サーバー名キャッシュがヒットしなかった回数。 • セッション ID キャッシュエントリの回数。	

データ ポイント	値の例
• セッション ID キャッシュが削除された回数。 • セッション ID キャッシュがヒットした回数。 • セッション ID キャッシュ メモリが使用された回数。 • セッション ID キャッシュがヒットしなかった回数 • セッション チケット キャッシュ エントリの回数。 • セッション チケット キャッシュが削除された回数。 • セッション チケット キャッシュがヒットした回数。 • セッション チケット キャッシュ メモリが使用された回数。 • セッション チケット キャッシュがヒットしなかった回数。 • SSL キャッシュ合計メモリの回数。 • SSL キャッシュ合計メモリが使用された回数。 • URL 再試行キャッシュ エントリの回数。 • URL 再試行キャッシュが削除された回数。 • URL 再試行キャッシュがヒットした回数。 • URL 再試行キャッシュ メモリが使用された回数。 • URL 再試行キャッシュがヒットしなかった回数。	
Management Center で SSL の使用が有効になっているかどうか。	はい（True）

証明書のステータス

システムは暗号化されたトラフィックを評価し、暗号化サーバーの証明書のステータスを報告します。

表 *8 : TLS/SSL* インスペクション：証明書ステータスのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたトラフィックを暗号化サーバーの**証明書ステータス**に基づいて評価し、報告します。 • SSL 証明書が有効な接続の数。 • SSL 証明書の有効期限が切れている接続の数。 • SSL 証明書の発行者が無効な接続の数。 • SSL 証明書に無効な署名が含まれている接続の数。 • SSL証明書がチェックされない接続の数。 • SSL 証明書がまだ有効になっていない接続の数。 • SSL 証明書が取り消された接続の数。 • SSL 証明書が自己署名されている接続の数。 • SSL 証明書が不明な接続の数。	0 以上の整数値

失敗の理由

システムは暗号化されたトラフィックを評価し、システムがトラフィックの復号化に失敗している場合は失敗の理由を報告します。

表 *9 : TLS/SSL* インスペクション：失敗のテレメトリデータ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、システムが次の理由のためにトラフィックの復号化に失敗している場合は**失敗の理由**を報告します。 • 復号エラー。 • ハンドシェイク中のポリシー判定の実行。 • ハンドシェイク前のポリシー判定の実行。 • 圧縮がネゴシエートされている。 • キャッシュされていないセッション。 • インターフェイスがパッシブモード。 • 不明な暗号スイート。 • サポートされていない暗号スイート。	0 以上の整数値

バージョン（Version）

システムは暗号化されたトラフィックを評価し、ネゴシエートされた TLS/SSL バージョンを接続ごとに報告します。

表 *10 : TLS/SSL* インスペクション：バージョンのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、次のようなネゴシエートされた**バージョン**を SSL 接続ごとに報告します。 • SSLv2 のネゴシエート。 • SSLv3 のネゴシエート。 • 不明なバージョンのネゴシエート。 • TLSv1.0 のネゴシエート。 • TLSv1.1 のネゴシエート。 • TLSv1.2 のネゴシエート。 • TLSv1.3 のネゴシエート。	0 以上の整数値

Snort 再起動データ

管理対象デバイス上の Snort プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。ユーザー定義のアプリケーションの作成/削除を行うか、システムまたはカスタム アプリケーション ディテクタを有効化/無効化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスの再起動が続行されていることが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内の任意の管理対象デバイスで発生します。

表 *11 : Snort* 再起動のテレメトリ データ

データ ポイント	値の例
カスタムアプリケーションディテクタを有効または無効にした場合の Snort 再起動の数。	0 以上の整数値
カスタムアプリケーションディテクタを作成または変更した場合の Snort 再起動の数。	0 以上の整数値

Snort3 データ

次の表に、Snort3 プロセスに関する収集およびモニター対象のデータを示します。これには、TCP/IP およびその他のネットワークプロトコルのパケット パフォーマンス モニタリングに関するセッション固有の情報が含まれます。

表 *12 : Snort3* テレメトリデータ

データ ポイント	値の例
キャッシュまたはフローメモリの容量がいっぱいになったためにプルーニングされたセッションの数。	0 以上の整数値
Snort がフローの開始を認識しなかったセッションの数。	0 以上の整数値
ミッドストリームを検出するセッションの数。	0 以上の整数値

データ ポイント	値の例
システムは、**遅延**の基本レベルを決定するために使用されるパケットパフォーマンスモニタリングに関連する次のカウントを報告します。 • 合計検出時間のしきい値を超えたパケットの数。 • ルールのしきい値を超えたパケットの数。 • SSL パケットタイムアウトの数。 • 合計パケット数がモニターされる。 • 検出にかかった合計時間。 • パケットによる検出にかかった最大時間。 • ルールのしきい値を超えたルールツリーの数。 • 評価済みルールの合計数。 • 一時停止後に再度有効になったルールの数。	0 以上の整数値
TCP セッションの最大数。	0 以上の整数値
エレファントフローの最大数	0 以上の整数値
処理された TCP データのバイト数。	0 以上の整数値
UDP セッションの最大数。	0 以上の整数値
処理された UDP データのバイト数。	0 以上の整数値
IP セッションの最大数（ICMP/UDP/TCP 以外）。	0 以上の整数値
処理された IP データのバイト数（ICMP/UDP/TCP 以外）。	0 以上の整数値
FTP セッションの最大数。	0 以上の整数値
処理された FTP データのバイト数	0 以上の整数値
HTTP セッションの最大数。	0 以上の整数値
SMTP セッションの最大数。	0 以上の整数値
処理された SMTP データのバイト数。	0 以上の整数値

データ ポイント	値の例
POP セッションの最大数。	0 以上の整数値
処理された POP データのバイト数	0 以上の整数値
SSH セッションの最大数。	0 以上の整数値
処理された SSH データのバイト数。	0 以上の整数値
処理された SSL パケットの数。	0 以上の整数値
無視された SSL パケットの数。	0 以上の整数値
無視された SSL セッションの数。	0 以上の整数値
SSL セッションの最大数。	0 以上の整数値
HTTP/2 セッションの最大数。	0 以上の整数値
処理された HTTP/2 データの最大バイト数（total_bytes）。	0 以上の整数値
処理された HTTP データの最大バイト数（total_bytes）。	0 以上の整数値
データ収集の開始時刻（Unix エポック形式）。	整数文字列
Snort のクリーン終了リストの数。	0 以上の整数値
Snort の予期しない終了リストの数。	0 以上の整数値
Snort3 侵入ポリシーに Firepower 推奨事項が使用されるかどうか。	いいえ（False）
無効になっているルールが Snort3 侵入ポリシー推奨設定で受け入れられるかどうか。	いいえ（False）
Snort3 侵入ポリシー推奨設定が最後に更新された時刻。	1625032449791
Snort3 侵入ポリシーの推奨事項の数。	12
Snort3 侵入ポリシーに推奨されるセキュリティ レベル。	"LEVEL_2"

次の表に、Snort3 ランタイム XTLS トラフィック情報を示します。

データ ポイント	値の例
証明書 DND 判定数。	1

データ ポイント	値の例
証明書 DR 判定数。	1
証明書 DRK 判定数。	2
証明書 DKK 判定数。	3
証明書 DP 判定数。	4
Client Hello Definitive DND エントリの回数。	5
フロー オーバー サブスクリプションの数。	6
SSLv3 のネゴシエート。	7
TLSv1.0 のネゴシエート。	8
TLSv1.1 のネゴシエート。	9
TLSv1.2 のネゴシエート。	10
TLSv1.3 のネゴシエート。	11
復号された TLSv1.3 フロー。	12
esni の要求。	13
作成された XTLS フローの数。	14
再開された SH セッションの数。	15
暗号のネゴシエート。	{ "TLS_RSA_WITH_AES_128_CBC_SHA": 3},{ "TLS_RSA_WITH_AES_256_CBC_SHA": 1}
サポートされていない暗号スイート。	{"DHE-DSS-AES256-GCM-SHA384" }
ドロップされた暗号。	{ }
不正な証明書。	{ "www.gmail.com": 4},{ "www.reddit.com": 3}
不明な証明書。	{ "www.youtube.com": 4}
不明な認証局。	{ "www.youtube.com": 4}

次の表に、Snort3 クラッシュ情報を示します。

データ ポイント	値の例
カスタムアプリケーションディテクタのバージョン。	0 以上の整数値
データ収集ライブラリ（DAQ）のパケットトレース。	0 以上の整数値
データ収集ライブラリ（DAQ）のデータメッセージ。	0 以上の整数値
データ収集ライブラリ（DAQ）のヘッダーメッセージ。	0 以上の整数値
データ収集ライブラリ（DAQ）のタイプ。	0 以上の整数値
IMS ビルド	1403
IMS バージョン	6.7.0
ISP バージョン	lsp-dev-20200710-1754
モデル	Cisco Firepower 2120 Threat Defense
モデル番号	72
NAVL バージョン	98
プロセス ID 番号（PID）	12368
Signal	6
Snort ビルド	4.116
Snort バージョン	3.0.1
SSP ビルド	99.15.1.245
タイム スタンプ（Time Stamp）	15991116699.963031
VDB ビルド	336
VDBバージョン（VDB Version）	4.5.0

コンテキスト クロス起動データ

コンテキストクロス起動機能を使用すると、Management Center の外部の Web ベースのリソースにおける潜在的な脅威に関する詳細情報をすばやく検索できます。Management Center のイベントビューアまたはダッシュボードのイベントから、外部リソースの関連情報を直接クリッ

クできます。これにより、そのIPアドレス、ポート、プロトコル、ドメイン、またはSHA 256ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

表 *13*：コンテキスト クロス起動のテレメトリ データ

データ ポイント	値の例
Management Center 上に設定されているコンテキストクロス起動リソースの数。	0 以上の整数値
Management Center 上で有効になっているコンテキストクロス起動リソースの数。	0 以上の整数値
ドメイン変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
IP 変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
SHA 256 変数を含むコンテキストクロス起動インスタンスの数。	0 以上の整数値
Management Center 上で有効になっている Stealthwatch 設定リソースの数。	0 以上の整数値
ログホストがある Stealthwatch 設定の数。	0 以上の整数値
Management Center 上のストアイベントの Stealthwatch 設定の数。	0 以上の整数値
SAL 統合ウィザードで使用されるセットアップのタイプは One Box。	0 以上の整数値

イベント概要

侵入ポリシーとマルウェアおよびファイルポリシーは、一致したトラフィックのイベントを生成し、キャプチャされた攻撃の情報をログに記録します。次の表では、侵入、ファイル、およびマルウェアイベントについて Cisco Success Network と共有される統計情報について説明します。

表 *14:* イベント概要テレメトリ

データポイント	値の例
システムは、過去24時間の次の侵入イベントデータを報告します。 • 次のアクションが適用された侵入イベント： • ブロック • 部分的にブロック • ブロックされる • 削除（Drop） • ドロップされる • 部分的にドロップ • ドロップ対象 • ドロップされた可能性が高い • アラート • 対処 • 対処する • 拒否（Reject） • 拒否する • 書き換え • 書き換える • 侵入イベントの合計数。	0 以上の整数値。
システムは、過去24時間の次のマルウェアイベントデータを報告します。 • ブロックされたマルウェアイベントの数。 • マルウェアイベントの合計数。 • ファイルイベントの合計数。	0 以上の整数値。
ネットワーク検出ホストの合計数。	0 以上の整数値。

クラウドイベントの設定

Cisco Success Network は、Management Center が Cisco Cloud に送信するさまざまなタイプのイベントに関する情報を収集します。次の表では、クラウドイベント設定に関して収集およびモニターされる統計情報について説明します。

表 *15*: クラウドイベント設定

データポイント	値の例
Cisco Cloud へのイベント送信から除外されたデバイスの数。	0 以上の整数値。
Management Center は Cisco Cloud にイベントを送信するように設定されていますか。	いいえ（False）
Management Center はセキュリティ関連の接続イベントを送信するように設定されていますか。	いいえ（False）
Management Center はすべての接続イベントを送信するように設定されていますか。	いいえ（False）
Management Center は検出イベントを送信するように設定されていますか。	いいえ（False）
Management Center はファイルおよびマルウェアイベントを送信するように設定されていますか。	いいえ（False）
Management Center は侵入イベントを送信するように設定されていますか。	いいえ（False）
Cisco Cloud への侵入パケットの送信が有効になっていますか。	いいえ（False）

VPN データ

次の表では、Threat Defense デバイスに登録されているさまざまな証明書オブジェクトに関して Cisco Success Network に報告されるデータについて説明します。

表 *16 : VPN* テレメトリデータ

データ ポイント	値の例
EST オブジェクトの証明書登録。	0 以上の整数値
手動オブジェクトの証明書登録。	
PKCS12 オブジェクトの証明書登録。	
SCEP オブジェクトの証明書登録。	
自己署名オブジェクトの証明書登録。	
証明書登録。	
証明書が登録されているデバイスの数。	

次の表に、Threat Defense デバイスで設定されたリモートアクセス VPN ポリシーに関して Cisco Success Network と共有されるデータ（接続プロファイルやダイナミック アクセス ポリシーの数など）を示します。

データ ポイント	値の例
ローカルにフォールバックする接続プロファイル。	2
ローカル認証を使用する接続プロファイル。	2
RADIUS を使用する接続プロファイル。	0 以上の整数値
レルムを使用する接続プロファイル。	1403
SAML を使用する接続プロファイル。	6.7.0
RAVPN が設定されたデバイス。	lsp-dev-20200710-1754
ロードバランシングが有効になっているデバイス。	Cisco Firepower 2120 Threat Defense
ダイナミック アクセス ポリシー。	72
ダイナミック アクセス ポリシー レコード。	98
RAVPN 接続プロファイル。	12368
RAVPN ポリシー。	6
IKEv2 を使用する RAVPN ポリシー。	4.116
SSL を使用する RAVPN ポリシー。	3.0.1

次の表に、脅威防御デバイスのさまざまなサイト間 VPN トポロジ設定に関して Cisco Success Network と共有されるデータを示します。

データ ポイント	値の例
S2S VPN が設定されたデバイス。	0 以上の整数値
証明書認証を使用する S2S IKEv1 VPN。	
証明書認証を使用する S2S IKEv2 VPN。	
S2S VPN エクストラネット エンドポイント。	
S2S VPN フルメッシュトポロジ。	
S2S VPN ハブおよびスポークトポロジ。	
S2S VPN IKEv1 トポロジ。	
S2S VPN IKEv2 トポロジ。	
S2S VPN ポイントツーポイント トポロジ。	
S2S VPN VTI トポロジ。	

Maria DB のデータ

Management Center は、Maria DB を使用して設定データを保存します。次の表では、収集およびモニタ対象の MariaDB データベース情報について説明します。

データ ポイント	値の例
Maria DB の CPU ステータス。	[{ "timestamp" : "123124312", "value" : "1%" }, { "timestamp" : "123124312", "value" : "2%" }, { "timestamp" : "123124312", "value" : "24%" }]
Maria DB のメモリステータス。	[{ "timestamp" : "123124312", "value" : "1gb" }, { "timestamp" : "123124312", "value" : "2gb" }, { "timestamp" : "123124312", "value" : "24gb" }]
DB 接続の数。	[{ "timestamp" : "123124312", "value" : 1 }, { "timestamp" : "123124312", "value" : 2 }, { "timestamp" : "123124312", "value" : 24 }]
DB ファイルシステムのサイズ。	[{ "location" : "/var/lib/mysql/cfgdb/", "value" : "1gb" }, { "location" : "/var/lib/mysql/sfsnort/", "value" : "2gb" }, { "location" : "/var/lib/mysql/", "value" : "24gb" }]
DB バイナリログのサイズ。	"20gb"

データ ポイント	値の例
DB のサイズ。	{ "cfgdb" : "5gb", "sfsnort" : "5gb", "Total_Db_size": "25gb" }
DB インデックスのサイズ。	{ "cfgdb" : "5gb", "sfsnort" : "5gb", "Total_Db_size": "25gb" }
サイズ別の上位 10 テーブル。	{ "cfgdb": [{ "table_name" : "<tb1>", "row_count" : 4990, "size" : "500mb" }, { "table_name" : "<tb2>", "row_count" : 4990, "size" : "500mb" }], "sfsnort": [{ "table_name" : "<tb1>", "row_count" : 4990, "size" : "500mb" }, { "table_name" : "<tb2>", "row_count" : 4990, "size" : "500mb" }] }
システムは、EM ピアからのデータのスロークエリをキャプチャします。	
クエリ。	SELECT * from EM_peers
クエリ時間。	2.37s (4s)
実行されたクエリの数。	0 以上の整数値。
検査された行の数。	0 以上の整数値。
影響を受けた行の数。	0 以上の整数値。
システムは、センサーからのデータのスロークエリをキャプチャします。	
クエリ。	SELECT * from sensors
クエリ時間。	2.37s (4s)
実行されたクエリの数。	0 以上の整数値。
検査された行の数。	0 以上の整数値。
影響を受けた行の数。	0 以上の整数値。
CLI のグローバルステータス。	"STRING"

Management Center ヘルスモニタリング

Management Center のヘルスモニターでは、さまざまなヘルスインジケータを追跡して、ファイアウォールシステムのハードウェアとソフトウェアが正常に動作することを確認します。次の表では、Management Center および Threat Defense のヘルス モニタリング ステータスについて説明します。

データ ポイント	値の例
システムは、Management Center の次のヘルスステータスを報告します。 • 単一のユーザーが作成できるカスタムダッシュボードの最大数 • ダッシュボードを作成したユーザーの数	0 以上の整数値
システムは、Threat Defense の次のヘルスステータスを報告します。 • 単一のユーザーがダッシュボードを作成できる顧客の最大数 • ダッシュボードを作成したユーザーの数	0 以上の整数値

アイデンティティの使用状況

ユーザアイデンティティ情報を使用すると、ポリシー違反、攻撃、ネットワークの脆弱性の発生源を特定し、特定のユーザまで遡って追跡することができます。次の表に、ポリシーのアイデンティティ使用状況について Cisco Success Network と共有される情報の説明を示します。

データ ポイント	値の例
システムは、アクセス コントロール ポリシーの次のアイデンティティ使用状況を報告します。 • アクセスルールの数。 • アクセスポリシーの数。 • 一意のレルム参照の数。 • 一意のユーザーグループ参照の数。 • 一意のユーザー参照の数。 • ABP によるルールの数。 • SGT によるルールの数。 • ユーザーグループ参照によるルールの数。 • ユーザー参照によるルールの数。	0 以上の整数値

データ ポイント	値の例
システムは、アクセス コントロール ポリシーの次のアイデンティティ使用状況を報告します。 • アクティブなルールの数。 • アイデンティティ ポリシーの数。 • 認証ルールの数。 • 一意のレルム シーケンスの数。 • 一意のレルムの数。 • パッシブ ルールの数。	0 以上の整数値
システムは、アイデンティティ ソース ステータスの次のアイデンティティ使用状況を報告します。 • 設定されている IS の数。 • 有効になっている SXP の数。 • 有効になっているディレクトリ セッションの数。	0 以上の整数値
システムは、レルム ステータスの次のアイデンティティ使用状況を報告します。 • AD レルムの数。 • LDAP ディレクトリの数。 • LDAP レルムの数。 • LDAP ディレクトリの数。 • ローカル レルムの数。 • レルム シーケンスの数。	0 以上の整数値

データ ポイント	値の例
システムは、プロキシの次のアイデンティティ使用状況を報告します。 • プロキシを持つレルムの数。 • ISEプロキシに使用されるデバイスの数。 • プロキシシーケンスの数。 • スタンドアロンプロキシデバイスの数。 • レルムプロキシに使用されるデバイスの合計数。 • レルムプロキシに使用されるデバイスの最大数。 • レルムプロキシに使用されるデバイスの最小数。 • プロキシとして使用されるデバイスの数。	0 以上の整数値

テレメトリ ファイルの例

次に、Management Center とその管理対象デバイスに関してポリシーと展開の情報をストリーミングするための Cisco Success Network テレメトリファイルの例を示します。

```
{
  "version" : "1.0",
  "metadata" : {
    "topic" : "fmc.telemetry",
    "contentType" : "application/json"
  },
  "payload" : {
    "recordType" : "CST_FMC",
    "recordVersion" : "7.4.0",
    "recordedAt" : 1669918170779,
    "fmc" : {
      "cloud_service" : {
        "amp_setting" : {
          "enableAutomaticMalwareUpdates" : 1,
          "enableDataSharing" : 0,
          "lastUpdateTimestamp" : 1669841433,
          "licensed" : 1,
          "proxyEnabled" : 0
        },
        "url_filtering" : {
          "cacheTimeout" : 0,
          "enableAutomaticUpdates" : 1,
          "enableURLFilter" : 1,
          "licensed" : 1,
          "queryVendors" : 2,
          "userPreference" : 1
        }
```

```
},
"deviceInfo" : {
  "SecureX" : {
    "isSecureXEnabled" : 0
  },
  "deviceModel" : "Secure Firewall Management Center for VMware",
  "deviceName" : "FMC1-FASTPOD",
  "deviceUuid" : "052f72b2-6f3e-11ed-rt4f5-59804da3174c",
  "isSsoEnabled" : 0,
  "serialNumber" : "None",
 "smartLicenseProductInstanceIdentifier" : "9ba0f39d-p07ji-421b-8053-6299fa26f0ab",

  "smartLicenseVirtualAccountName" : "ABC1",
  "systemUptime" : 263436000,
  "udiProductIdentifier" : "FS-VMW-ER-K9",
  "primaryFMCRemoteManagementAccess" : "FQDN",
  "secondaryFMCRemoteManagementAccess" : "FQDN"
},
"fmcUpgradeData" : { },
"scheduleTasks" : {
  "tasks" : [
    {
      "comment" : "This was automatically set up during installation.",
      "creation_date" : 1669656848,
      "name" : "Weekly Software Download",
      "time_data" : {
        "by_day" : [
          6
        ],
        "by_hour" : [
          2
        ],
        "by_minute" : [
          "10"
        ],
        "by_month" : [ ],
        "by_month_day" : [ ],
        "by_set_position" : [ ],
        "by_week_number" : [ ],
        "by_year_day" : [ ],
        "frequency_type" : "weekly",
        "interval" : 1,
        "start_date" : "01/05/2019",
        "support_dst" : 1,
        "timedate" : 1546654200,
        "tz" : "America/New_York"
      },
      "type_name" : "Download Latest Update"
    },
    {
      "comment" : "This was automatically set up during installation.",
      "creation_date" : 1669656852,
      "name" : "Weekly config only backup",
      "time_data" : {
        "by_day" : [
          0
        ],
        "by_hour" : [
          2
        ],
        "by_minute" : [
          0
        ],
        "by_month" : [ ],
```

```
            "by_month_day" : [ ],
            "by_set_position" : [ ],
            "by_week_number" : [ ],
            "by_year_day" : [ ],
            "frequency_type" : "weekly",
            "interval" : 1,
            "start_date" : "01/06/2019",
            "support_dst" : 1,
            "timedate" : 1546740000,
            "tz" : "America/New_York"
          },
          "type_name" : "Backup"
        }
      ]
    },
    "versions" : {
      "items" : [
        {
          "type" : "SOFTWARE",
          "version" : "7.4.0-1475"
        },
        {
          "lastUpdated" : 1669866005000,
          "type" : "SNORT_RULES_DB",
          "version" : "2022-11-28-001-vrt"
        },
        {
          "lastUpdated" : 1669881833000,
          "type" : "VULNERABILITY_DB",
          "version" : "361"
        },
        {
          "type" : "GEOLOCATION_DB",
          "version" : "2022-11-21-101"
        }
      ]
    }
  },
  "managedDevices" : {
    "items" : [
      {
        "deviceInfo" : {
          "containerStatus" : "Standalone",
          "deviceManager" : "FMC",
          "deviceModel" : "Cisco Firepower Threat Defense for VMware",
          "deviceName" : "192.168.7.149",
          "deviceUuid" : "96b75a84-6f3d-12rdc-96a6-e2422bc5a2bf",
          "deviceVersion" : "7.4.0-1475",
          "isConnected" : true,
          "serialNumber" : "9AWE1PEM4P2",
          "snort3Toggled" : false,
          "snort3ToggledWithComment" : "",
          "snortEngine" : "SNORT3",
          "remoteBranchConnectivity" : "Inbound"
        },
        "deviceSettings" : {
          "attemptedRemoteDeployHA" : false,
          "certVisibility" : false,
          "fmcAccessInfo" : {
            "IPAllocationTypeList" : [
              "N/A"
            ],
            "accessThrough" : "Management interface"
          },
```

```
  "mgmtInterfaceConvergence" : true,
  "netFlow" : {
      "netFlowEnabled" : false,
       "numberOfCollectors" : 0,
       "numberOfTrafficClasses" : 0
  },
  "nszValue" : false,
  "ogsValue" : true,
  "vrfInfo" : {
    "literal" : false,
    "numberOfStaticRoutes" : 0,
    "vrfCount" : 0
  },
  "onboardingMethod": "USING_SERIAL_NUMBER_VIA_CDO"
},
"ftdMemoryCGroupStatistics" : [
  {
    "meanMemorySwapUsageBytes" : 5.207097946E7,
    "meanMemoryUsageBytes" : 5.206894039E7,
    "memoryCGroupName" : "System/ProcessHigh",
    "peakMemorySwapUsageBytes" : 1574682624,
    "peakMemoryUsageBytes" : 1574674432,
    "stdDevMemorySwapUsage" : 957106.41,
    "stdDevMemoryUsage" : 954302.27
  },
  {
    "meanMemorySwapUsageBytes" : 2.2863022975E8,
    "meanMemoryUsageBytes" : 228563747,
    "memoryCGroupName" : "System/ProcessMedium",
    "peakMemorySwapUsageBytes" : 965337088,
    "peakMemoryUsageBytes" : 960196608,
    "stdDevMemorySwapUsage" : 3854598.89,
    "stdDevMemoryUsage" : 2914561.18
  },
  {
    "meanMemorySwapUsageBytes" : 9.8453439805E8,
    "meanMemoryUsageBytes" : 9.8453448572E8,
    "memoryCGroupName" : "privileged",
    "peakMemorySwapUsageBytes" : 987504640,
    "peakMemoryUsageBytes" : 987504640,
    "stdDevMemorySwapUsage" : 31431.74,
    "stdDevMemoryUsage" : 31265.9
  },
  {
    "meanMemorySwapUsageBytes" : 286504.12,
    "meanMemoryUsageBytes" : 286523.87,
    "memoryCGroupName" : "normal",
    "peakMemorySwapUsageBytes" : 36343808,
    "peakMemoryUsageBytes" : 36343808,
    "stdDevMemorySwapUsage" : 75561.78,
    "stdDevMemoryUsage" : 75584.27
  },
  {
    "meanMemorySwapUsageBytes" : 3502151.01,
    "meanMemoryUsageBytes" : 3502080,
    "memoryCGroupName" : "restricted",
    "peakMemorySwapUsageBytes" : 77656064,
    "peakMemoryUsageBytes" : 23068672,
    "stdDevMemorySwapUsage" : 2695.67,
    "stdDevMemoryUsage" : 0
  },
  {
    "meanMemorySwapUsageBytes" : 0,
    "meanMemoryUsageBytes" : 0,
```

```
  "memoryCGroupName" : "rest-agent",
  "peakMemorySwapUsageBytes" : 0,
  "peakMemoryUsageBytes" : 0,
  "stdDevMemorySwapUsage" : 0,
  "stdDevMemoryUsage" : 0
},
{
  "meanMemorySwapUsageBytes" : 5.2469167188E8,
  "meanMemoryUsageBytes" : 5.2469178715E8,
  "memoryCGroupName" : "Detection-Snort3",
  "peakMemorySwapUsageBytes" : 555659264,
  "peakMemoryUsageBytes" : 555659264,
  "stdDevMemorySwapUsage" : 123621.9,
  "stdDevMemoryUsage" : 123587.29
},
{
  "meanMemorySwapUsageBytes" : 1.92944950325E9,
  "meanMemoryUsageBytes" : 1.92877869444E9,
  "memoryCGroupName" : "System",
  "peakMemorySwapUsageBytes" : 3940163584,
  "peakMemoryUsageBytes" : 3192242176,
  "stdDevMemorySwapUsage" : 1.8285574795E8,
  "stdDevMemoryUsage" : 1.8113682802E8
},
{
  "meanMemorySwapUsageBytes" : 0,
  "meanMemoryUsageBytes" : 0,
  "memoryCGroupName" : "System/default",
  "peakMemorySwapUsageBytes" : 0,
  "peakMemoryUsageBytes" : 0,
  "stdDevMemorySwapUsage" : 0,
  "stdDevMemoryUsage" : 0
},
{
  "meanMemorySwapUsageBytes" : 0,
  "meanMemoryUsageBytes" : 0,
  "memoryCGroupName" : "qemu",
  "peakMemorySwapUsageBytes" : 0,
  "peakMemoryUsageBytes" : 0,
  "stdDevMemorySwapUsage" : 0,
  "stdDevMemoryUsage" : 0
},
{
  "meanMemorySwapUsageBytes" : 1.7874486112E8,
  "meanMemoryUsageBytes" : 1.7870017999E8,
  "memoryCGroupName" : "System/ActionQueueScrape",
  "peakMemorySwapUsageBytes" : 1487872000,
  "peakMemoryUsageBytes" : 1446891520,
  "stdDevMemorySwapUsage" : 5783036.92,
  "stdDevMemoryUsage" : 5530633.87
},
{
  "meanMemorySwapUsageBytes" : 5.0285961409E8,
  "meanMemoryUsageBytes" : 5.0267548869E8,
  "memoryCGroupName" : "System/ProcessLow",
  "peakMemorySwapUsageBytes" : 1205043200,
  "peakMemoryUsageBytes" : 751620096,
  "stdDevMemorySwapUsage" : 1.7946871779E8,
  "stdDevMemoryUsage" : 1.7939477583E8
},
{
  "meanMemorySwapUsageBytes" : 7.9608501366E8,
  "meanMemoryUsageBytes" : 7.9573099445E8,
  "memoryCGroupName" : "System/SFDataCorrelator",
```

```
    "peakMemorySwapUsageBytes" : 2138398720,
    "peakMemoryUsageBytes" : 1774387200,
    "stdDevMemorySwapUsage" : 3.437121236E7,
    "stdDevMemoryUsage" : 3.164608653E7
  }
],
"ftdProcessExitStatistics" : [
  {
    "managedRestarts" : 0,
    "processName" : "adi",
    "unexpectedExits" : 0
  }
],
"ftdUpgradeData" : { },
"malware" : {
  "malwareLicenseUsed" : true,
  "numberOfACRulesNeedMalwareLicense" : 1,
  "numberOfACRulesWithMalware" : 1
},
"snort3RuntimeStatistics" : {
  "firewallStatistics" : {
    "dce_rpcAllowedFlows" : 0,
    "dce_rpcDeniedFlows" : 0,
    "dnp3AllowedFlows" : 0,
    "dnp3DeniedFlows" : 0,
    "dnsAllowedFlows" : 0,
    "dnsDeniedFlows" : 0,
    "ftp_telnetAllowedFlows" : 0,
    "ftp_telnetDeniedFlows" : 0,
    "http2AllowedFlows" : 0,
    "http2DeniedFlows" : 0,
    "httpAllowedFlows" : 0,
    "httpDeniedFlows" : 0,
    "imapAllowedFlows" : 0,
    "imapDeniedFlows" : 0,
    "modbusAllowedFlows" : 0,
    "modbusDeniedFlows" : 0,
    "otherAllowedFlows" : 2216,
    "otherDeniedFlows" : 0,
    "popAllowedFlows" : 0,
    "popDeniedFlows" : 0,
    "quicAllowedFlows" : 0,
    "quicDeniedFlows" : 0,
    "rpcAllowedFlows" : 0,
    "rpcDeniedFlows" : 0,
    "sipAllowedFlows" : 0,
    "sipDeniedFlows" : 0,
    "smtpAllowedFlows" : 0,
    "smtpDeniedFlows" : 0,
    "sshAllowedFlows" : 0,
    "sshDeniedFlows" : 0,
    "sslAllowedFlows" : 0,
    "sslDeniedFlows" : 0
  },
  "ftpStatistics" : {
    "ftpDataBytesProcessed" : 0,
    "maxFTPsessions" : 0
  },
  "http2Statistics" : {
    "http2DataBytesProcessed" : 0,
    "maxHTTP2Sessions" : 0
  },
  "httpStatistics" : {
    "httpDataBytesProcessed" : 0,
```

```
  "maxHTTPSessions" : 325
},
"popStatistics" : {
  "maxPOPSessions" : 0,
  "popDataBytesProcessed" : 0
},
"sessionStatistics" : {
  "highCpuUtilisedElephantFlows" : 0,
  "ipDataBytesProcessed" : 27792,
  "maxElephantFlows" : 0,
  "maxIPSessions" : 10,
  "maxTCPSessions" : 13675,
  "maxUDPSessions" : 120,
  "midStreamSessions" : 0,
  "prunedSessions" : 2216,
  "systemUnderDuress" : 0,
  "tcpDataBytesProcessed" : 0,
  "totalElephantFlowsBypassed" : 0,
  "totalElephantFlowsDethrottled" : 0,
  "totalElephantFlowsExempted" : 0,
  "totalElephantFlowsThrottled" : 0,
  "udpDataBytesProcessed" : 0
},
"smbStatistics" : {
  "totalEncryptedSessions" : 0,
  "totalMultichannelSessions" : 0,
  "totalSMB1Sessions" : 0,
  "totalSMB2Sessions" : 0
},
"smtpStatistics" : {
  "maxSMTPSessions" : 5,
  "smtpDataBytesProcessed" : 0
},
"snortLatency" : {
  "maxTimeSpent" : 0,
  "packetTimeouts" : 0,
  "ruleEvaluationsExceededLatency" : 0,
  "rulesReenabled" : 0,
  "totalNumberOfRuleEvalauations" : 4542,
  "totalPacketsMonitored" : 0,
  "totalTimeSpentInDetection" : 0
},
"sshStatistics" : {
  "maxSshSessions" : 80,
  "sshDataBytesProcessed" : 0
},
"sslStatistics" : {
  "maxSslSessions" : 0,
  "packetsProcessed" : 0,
  "sessionsIgnored" : 0
},
"xtlsStatistics" : {
  "badCertificate" : [ ],
  "cert_dkk_verdicts" : 0,
  "cert_dnd_verdicts" : 0,
  "cert_dp_verdicts" : 0,
  "cert_dr_verdicts" : 0,
  "cert_drk_verdicts" : 0,
  "certificateUnknown" : [ ],
  "client_hello_definitive_dnd" : 0,
  "decrypted_tls_1_3_flows" : 0,
  "droppedCiphers" : [ ],
  "flow_created" : 0,
  "flow_over_subscriptions" : 0,
```

```
      "negotiatedCiphers" : [ ],
      "negotiated_ssl_version_3_0" : 0,
      "negotiated_tls_version_1_0" : 0,
      "negotiated_tls_version_1_1" : 0,
      "negotiated_tls_version_1_2" : 0,
      "negotiated_tls_version_1_3" : 0,
      "requested_esni" : 0,
      "sh_session_resume" : 0,
      "unknownCertificateAuthority" : [ ],
      "unsupportedCiphers" : [ ]
    }
  },
  "sslCacheStats" : { },
  "sslUsage" : {
    "isSSLEnabled" : true
  },
  "ssl_rules_counter" : {
    "block" : {
      "apps" : 0,
      "cert_statuses" : 0,
      "cipher_suites" : 0,
      "decryption_certs" : 0,
      "dst_networks" : 0,
      "dst_services" : 0,
      "dst_zones" : 0,
      "external_certs" : 0,
      "issuer_dns" : 0,
      "logging" : 0,
      "replace_public_key" : 0,
      "src_networks" : 0,
      "src_services" : 0,
      "src_zones" : 0,
      "ssl_versions" : 0,
      "subject_dns" : 0,
      "urls" : 0,
      "users" : 0,
      "vlan_tags" : 0
    },
    "block_with_reset" : {
      "apps" : 0,
      "cert_statuses" : 0,
      "cipher_suites" : 0,
      "decryption_certs" : 0,
      "dst_networks" : 0,
      "dst_services" : 0,
      "dst_zones" : 0,
      "external_certs" : 0,
      "issuer_dns" : 0,
      "logging" : 0,
      "replace_public_key" : 0,
      "src_networks" : 0,
      "src_services" : 0,
      "src_zones" : 0,
      "ssl_versions" : 0,
      "subject_dns" : 0,
      "urls" : 0,
      "users" : 0,
      "vlan_tags" : 0
    },
    "decrypt_known_key" : {
      "apps" : 0,
      "cert_statuses" : 0,
      "cipher_suites" : 0,
      "decryption_certs" : 0,
```

```
    "dst_networks" : 0,
    "dst_services" : 0,
    "dst_zones" : 0,
    "external_certs" : 0,
    "issuer_dns" : 0,
    "logging" : 0,
    "replace_public_key" : 0,
    "src_networks" : 0,
    "src_services" : 0,
    "src_zones" : 0,
    "ssl_versions" : 0,
    "subject_dns" : 0,
    "urls" : 0,
    "users" : 0,
    "vlan_tags" : 0
  },
  "decrypt_resign" : {
    "apps" : 0,
    "cert_statuses" : 0,
    "cipher_suites" : 0,
    "decryption_certs" : 0,
    "dst_networks" : 0,
    "dst_services" : 0,
    "dst_zones" : 0,
    "external_certs" : 0,
    "issuer_dns" : 0,
    "logging" : 0,
    "replace_public_key" : 0,
    "src_networks" : 0,
    "src_services" : 0,
    "src_zones" : 0,
    "ssl_versions" : 0,
    "subject_dns" : 0,
    "urls" : 0,
    "users" : 0,
    "vlan_tags" : 0
  },
  "do_not_decrypt" : {
    "apps" : 0,
    "cert_statuses" : 0,
    "cipher_suites" : 0,
    "decryption_certs" : 0,
    "dst_networks" : 0,
    "dst_services" : 0,
    "dst_zones" : 0,
    "external_certs" : 0,
    "issuer_dns" : 0,
    "logging" : 0,
    "replace_public_key" : 0,
    "src_networks" : 0,
    "src_services" : 0,
    "src_zones" : 0,
    "ssl_versions" : 0,
    "subject_dns" : 0,
    "urls" : 0,
    "users" : 0,
    "vlan_tags" : 0
  },
  "monitor" : {
    "apps" : 0,
    "cert_statuses" : 0,
    "cipher_suites" : 0,
    "decryption_certs" : 0,
    "dst_networks" : 0,
```

```
            "dst_services" : 0,
            "dst_zones" : 0,
            "external_certs" : 0,
            "issuer_dns" : 0,
            "logging" : 0,
            "replace_public_key" : 0,
            "src_networks" : 0,
            "src_services" : 0,
            "src_zones" : 0,
            "ssl_versions" : 0,
            "subject_dns" : 0,
            "urls" : 0,
            "users" : 0,
            "vlan_tags" : 0
          }
        },
        "threat" : {
          "acPolicyHasIntrusion" : false,
          "acRulesWithIntrusion" : 1,
          "isTIDEnabled" : true,
          "numberOfACRulesNeedThreatLicense" : 0,
          "threatLicenseUsed" : true
        },
        "urlFiltering" : {
          "acRulesWithURLFiltering" : 0,
          "numberOfACRulesNeedThreatLicense" : 0,
          "numberOfACRulesNeedURLLicense" : 0,
          "urlFilteringLicenseUsed" : true
        },
       "ftdModelMigrationStatistics" : [
          {
             "elapsedTime" : 6366,
             "errors" : "",
             "isCompleted" : true,
             "isReset" : false,
             "numberOfInterfaces" : 18,
             "sourceContainerStatus" : "Standalone",
             "sourceDeviceModel" : "Cisco Firepower 2130 Threat Defense",
             "sourceDeviceUuid" : "a8eee3f4-aa19-rt24-bda7-857745t8d45a",
             "sourceDeviceVersion" : "7.2.0",
             "targetContainerStatus" : "Standalone",
             "targetDeviceModel" : "Cisco Secure Firewall 3105 Threat Defense",
             "targetDeviceVersion" : "7.3.0",
          }
        ]
       }
    ]
  },
  "policyData" : {
    "AccessPolicyInfo" : [
      {
        "assignedSnort2Devices" : 0,
        "assignedSnort3Devices" : 1,
        "customIpsPolicyCount" : 1,
        "customNapPolicyCount" : 1,
        "enabledIpsSyslog" : false,
        "encryptedVisibilityEngine" : true,
        "overrideSyslogDestination" : false,
        "parentPolicyUUID" : "8589935770",
        "policyUUID" : "8589935771",
        "portScanSettings" : {
          "inspectionMode" : "Disabled"
        },
        "systemIpsPolicyCount" : 1,
```

```
    "systemNapPolicyCount" : 0
  }
],
"MigratedSnort3IntrusionPolicyInfo" : {
  "migratedPolicies" : 0,
  "policiesFailureCount" : 0,
  "policiesFailureReason" : [
    "N/A"
  ],
  "policiesPartialFailureCount" : 0,
  "policiesPartialFailureReason" : [
    "N/A"
  ],
  "policiesSuccessCount" : 0
},
"PrefilterPolicyInfo" : [
  {
    "assignedDevices" : 1,
    "isSytemDefined" : true
  }
],
"Snort2IntrusionPolicyInfo" : {
  "Snort2IpsList" : [
    {
      "isSystemDefined" : true,
      "policyName" : "No Rules Active",
      "policyUUID" : "apqr416e-3127-23ds-9f4v-d463d19aa744"
    },
    {
      "assignedSnort2Devices" : 0,
      "customEnabledRules" : 0,
      "dynamicConfiguredRules" : 0,
      "firepowerRecommendationsUsed" : false,
      "globalThresholdDisabled" : false,
      "globalThresholdUpdated" : false,
      "isSystemDefined" : false,
      "overridenRules" : 0,
      "parentPolicyUUID" : "apqr416e-3127-11ds-9f4c-d463d19aa744",
      "policyUUID" : "765f93a0-6g42-11ed-5tgf-2e944da3174c",
      "sensitiveDataDetectionEnabled" : false,
      "snmpEnabledRules" : 0,
      "suppressionConfiguredRules" : 0,
      "thresholdConfiguredRules" : 0
    }
  ],
  "customClassification" : 0,
  "customClassificationInUse" : 0,
  "customRuleWithPass" : 0,
  "customRuleWithReplace" : 0,
  "customRules" : 0
},
"Snort2NetworkAnalysisPolicyInfo" : [
  {
    "assignedSnort2Devices" : 0,
    "customInstancesAdded" : [
      "N/A"
    ],
    "isSystemDefined" : false,
    "lastModifiedTimestamp" : "2022-11-28 17:31:05",
    "parentPolicyUUID" : "apqr00a0-bv29-425c-9d75-49679aadc898",
    "policyUUID" : "703e0600-6f42-11ed-8d96-2e944da3174c",
    "userDisabledInspectors" : [
      "N/A"
    ],
```

```
      "userEditedInspectors" : [
        "N/A"
      ],
      "userEnabledInspectors" : [
        "N/A"
      ]
    }
  ],
  "Snort3IntrusionPolicyInfo" : {
    "Snort3IpsList" : [
      {
        "FirepowerRecommendationsUsed" : false,
        "assignedSnort3Devices" : 1,
        "enabledCustomRuleGroupCount" : 0,
        "excludedRuleGroups" : [ ],
        "excludedRuleGroupsCount" : 0,
        "includedRuleGroups" : [ ],
        "includedRuleGroupsCount" : 0,
        "overridenRuleGroups" : [ ],
        "overridenRuleGroupsCount" : 0,
        "overridenRules" : 4,
        "parentPolicyUUID" : "7005",
        "policyUUID" : "8589935680"
      }
    ],
    "customRuleGroups" : 1,
    "customRules" : 4,
    "rulesWithSuppression" : 0,
    "rulesWithThreshold" : 0
  },
  "Snort3NetworkAnalysisPolicyInfo" : [
    {
      "assignedSnort3Devices" : 1,
      "customInstancesAdded" : [
        "N/A"
      ],
      "defaultInstancesEdited" : [
        "N/A"
      ],
      "parentPolicyUUID" : "7303",
      "policyUUID" : "8589935556",
      "userDisabledInspectors" : [
        "N/A"
      ],
      "userEditedInspectors" : [
        "N/A"
      ],
      "userEnabledInspectors" : [
        "N/A"
      ]
    }
  ]
},
"deploymentData" : { },
"analysis" : {
  "cloudEventConfig" : {
    "excludedDevices" : 0,
    "sendingConnection" : false,
    "sendingConnectionAll" : false,
    "sendingDiscovery" : false,
    "sendingEvents" : false,
    "sendingFile" : false,
    "sendingIntrusion" : false,
    "sendingPackets" : false
```

```
  },
  "crossLaunchInfo" : {
    "count" : 28,
    "enabledCount" : 28,
    "iocInfo" : [
      {
        "domain" : 10,
        "ip" : 9,
        "sha256" : 9
      }
    ]
  },
  "eventCount" : {
    "fileTotal" : 0,
    "ipsAlert" : 1045,
    "ipsBlock" : 0,
    "ipsDrop" : 0,
    "ipsDropped" : 0,
    "ipsPartialBlock" : 0,
    "ipsPartiallyDropped" : 0,
    "ipsReact" : 0,
    "ipsReject" : 0,
    "ipsRewrite" : 0,
    "ipsTotal" : 1045,
    "ipsWouldBlock" : 0,
    "ipsWouldDrop" : 0,
    "ipsWouldHaveDropped" : 0,
    "ipsWouldReact" : 0,
    "ipsWouldReject" : 0,
    "ipsWouldRewrite" : 0,
    "malwareBlocked" : 0,
    "malwareTotal" : 0,
    "networkDiscoveryHost" : 1198
  },
  "stealthwatchConfig" : {
    "crossLaunchEnabled" : 0,
    "hasLogHost" : 0,
    "isLinaLoggingEnabled" : 0,
    "isOneBox" : 0,
    "numLogHosts" : 0,
    "numUnusedLogHosts" : 0,
    "storeEventsFmc" : 1
  }
},
"theme" : {
  "light" : 10
},
"SSLStats" : {
  "action" : {
    "block" : 0,
    "block_with_reset" : 0,
    "decrypt_resign_self_signed" : 0,
    "decrypt_resign_self_signed_replace_key_only" : 0,
    "decrypt_resign_signed_cert" : 0,
    "decrypt_with_known_key" : 0,
    "do_not_decrypt" : 0
  },
  "cache_status" : {
    "cached_session" : 0,
    "cert_validation_cache_hit" : 0,
    "cert_validation_cache_miss" : 0,
    "orig_cert_cache_hit" : 0,
    "orig_cert_cache_miss" : 0,
    "resigned_cert_cache_hit" : 0,
```

```
      "resigned_cert_cache_miss" : 0,
      "session_cache_hit" : 0,
      "session_cache_miss" : 0
    },
    "cert_status" : {
      "cert_expired" : 0,
      "cert_invalid_issuer" : 0,
      "cert_invalid_signature" : 0,
      "cert_not_checked" : 0,
      "cert_not_yet_valid" : 0,
      "cert_revoked" : 0,
      "cert_self_signed" : 0,
      "cert_unknown" : 0,
      "cert_valid" : 0
    },
    "failure_reason" : {
      "decryption_error" : 0,
      "handshake_error_before_verdict" : 0,
      "handshake_error_during_verdict" : 0,
      "ssl_compression" : 0,
      "uncached_session" : 0,
      "undecryptable_in_passive_mode" : 0,
      "unknown_cipher_suite" : 0,
      "unsupported_cipher_suite" : 0
    },
    "version" : {
      "ssl_v20" : 0,
      "ssl_v30" : 0,
      "ssl_version_unknown" : 0,
      "tls_v10" : 0,
      "tls_v11" : 0,
      "tls_v12" : 0,
      "tls_v13" : 0
    }
  },
  "snortRestart" : {
    "appDetectorSnortRestartCnt" : 0,
    "appSnortRestartCnt" : 0
  },
  "localUrlCount" : {
    "items" : [ ]
  },
  "vpnData" : {
    "certificate" : {
      "certificateEnrollmentESTObjects" : 0,
      "certificateEnrollmentManualObjects" : 0,
      "certificateEnrollmentPKCS12Objects" : 0,
      "certificateEnrollmentSCEPObjects" : 0,
      "certificateEnrollmentSelfSignedObjects" : 0,
      "certificateEnrollments" : 0,
      "devicesWithCertificateEnrollments" : 0
    },
    "remoteAccessVpn" : {
      "connectionProfilesWithFallbackToLocal" : 0,
      "connectionProfilesWithLocalAuthentication" : 0,
      "connectionProfilesWithOverriddenSAMLIDPCertificate" : 0,
      "connectionProfilesWithRADIUS" : 0,
      "connectionProfilesWithRealm" : 0,
      "connectionProfilesWithSAML" : 0,
      "connectionProfilesWithWebAuthNEnabled" : 0,
      "devicesConfiguredWithRAVPN" : 0,
      "devicesEnabledWithLoadBalancing" : 0,
      "dynamicAccessPolicies" : 0,
      "dynamicAccessPolicyRecords" : 0,
```

```
    "ravpnConnectionProfiles" : 0,
    "ravpnPolicies" : 0,
    "ravpnPoliciesWithIKEv2" : 0,
    "ravpnPoliciesWithSSL" : 0
  },
  "siteToSiteVpn" : {
    "devicesConfiguredWithS2SVpn" : 0,
    "s2sIKEv1VpnWithCertificateAuthentication" : 0,
    "s2sIKEv2VpnWithCertificateAuthentication" : 0,
    "s2sVpnExtranetEndpoints" : 0,
    "s2sVpnFullMeshTopologies" : 0,
    "s2sVpnHubAndSpokeTopologies" : 0,
    "s2sVpnIKEv1Topologies" : 0,
    "s2sVpnIKEv2Topologies" : 0,
    "s2sVpnPointToPointTopologies" : 0,
    "s2sVpnVTITopologies" : 0
  }
},
"fmc_healthmon" : {
  "fmc" : {
    "stats" : {
      "maxCustomDashboardsCreatedBySingleUser" : 0,
      "numUsersCreatedDashboard" : 0
    }
  },
  "ftd" : {
    "stats" : {
      "maxCustomDashboardsCreatedBySingleUser" : 0,
      "numUsersCreatedDashboard" : 0
    }
  }
},
"identityUsage" : {
  "accessControlPolicyStats" : {
    "accessRules" : 1,
    "numberOfAccessPolicies" : 1,
    "numberOfUniqueRealmReference" : 0,
    "numberOfUniqueUserGroupReference" : 0,
    "numberOfUniqueUserReference" : 0,
    "rulesWithABP" : 0,
    "rulesWithSGT" : 0,
    "rulesWithUserGroupReference" : 0,
    "rulesWithUserReference" : 0
  },
  "identityPolicyStats" : {
    "activeRules" : 0,
    "identityPolicies" : 1,
    "noAuthRules" : 0,
    "numberOfUniqueRealmSequences" : 0,
    "numberOfUniqueRealms" : 1,
    "passiveRules" : 1
  },
  "identitySource" : {
    "isISEConfigured" : 0,
    "isSXPEnabled" : 0,
    "isSessionDirectoryEnabled" : 0
  },
  "proxy" : {
    "devicesUsedAsProxy" : 0,
    "devicesUsedForISEProxy" : 0,
    "devicesUsedForRealmProxy" : {
      "max" : 0,
      "min" : 0,
      "total" : 0
```

```
    },
    "proxySequences" : 0,
    "realmsWithProxy" : 0,
    "standAloneProxyDevices" : 0
  },
  "realmStats" : {
    "ADRealms" : 1,
    "LDAPDirectories" : 1,
    "LDAPRealms" : 0,
    "LDAPsDirectories" : 0,
    "localRealms" : 0,
    "realmSequences" : 0
  }
},
"managedClusters" : {
  "totalClusterCount" : 0
},
"mariaDBData" : {
  "DBConnection_count" : [ ],
  "Db_file_system_size" : [
    {
      "location" : "/var/lib/mysql/cfgdb",
      "value" : "2.0G"
    },
    {
      "location" : "/var/lib/mysql/sfsnort",
      "value" : "295M"
    },
    {
      "location" : "/var/lib/mysql",
      "value" : "5.1G"
    }
  ],
  "Db_index_size" : {
    "Total_Db_size" : "520.9M",
    "cfgdb" : "431.3M",
    "sfsnort" : "89.5M"
  },
  "Db_size" : {
    "Total_Db_size" : "1402.6M",
    "cfgdb" : "1289.6M",
    "sfsnort" : "112.9M"
  },
  "Global_status_CLI" : "EMPTY",
  "MariaDb_CPU_stats" : [
    {
      "timestamp" : "1669746257",
      "value" : "0.6633333333333331"
    },
    {
      "timestamp" : "1669785857",
      "value" : "0.8"
    },
    {
      "timestamp" : "1669800257",
      "value" : "0.8"
    },
    {
      "timestamp" : "1669803857",
      "value" : "0.8116666666666668"
    },
    {
      "timestamp" : "1669807457",
      "value" : "0.9"
```

```
    },
    {
      "timestamp" : "1669811057",
      "value" : "0.9"
    },
    {
      "timestamp" : "1669814657",
      "value" : "0.9"
    },
    {
      "timestamp" : "1669818257",
      "value" : "0.9"
    },
    {
      "timestamp" : "1669821857",
      "value" : "0.9"
    },
    {
      "timestamp" : "1669825457",
      "value" : "0.9"
  ],
  "MariaDb_memory_stats" : [
    {
      "timestamp" : "1669746257",
      "value" : "1135789875.1999998"
    },
    {
      "timestamp" : "1669749857",
      "value" : "1139567752.5333333"
    },
    {
      "timestamp" : "1669753457",
      "value" : "1154918331.7333333"
    },
    {
      "timestamp" : "1669757057",
      "value" : "1156227072"
    },
    {
      "timestamp" : "1669771457",
      "value" : "1156243456"
    },
    {
      "timestamp" : "1669793057",
      "value" : "1386346837.3333333"
    },
    {
      "timestamp" : "1669796657",
      "value" : "1386582016"
    },
    {
      "timestamp" : "1669800257",
      "value" : "1387066163.1999998"
    },
    {
      "timestamp" : "1669832657",
      "value" : "1389006848"
    }
  ],
  "Slow_query_data" : [
    {
      "query" : "SELECT uuid,revision,type FROM EORevisionStore",
      "query_exec_count" : "2",
      "query_time" : "71.93s (143s)",
```

```
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "63075.5 (126151)"
        },
        {
          "query" : "SELECT uuid FROM rule_opts  order by uuid",
          "query_exec_count" : "2",
          "query_time" : "42.18s (84s)",
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "978411.0 (1956822)"
        },
        {
          "query" : "UPDATE rule_header set performance='S' WHERE  uuid IN ( 'S', 'S',
'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S' )",
          "query_exec_count" : "1",
          "query_time" : "34.09s (34s)",
          "rows_affected" : "19627.0 (19627)",
          "rows_examined" : "58643.0 (58643)"
        },
        {
          "query" : "select count(*) from rule_opts",
          "query_exec_count" : "2",
          "query_time" : "26.58s (53s)",
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "978411.0 (1956822)"
        },
        {
          "query" : "SELECT  rule_opts.sid,  rule_opts.gid FROM rule_opts LEFT JOIN
rule_header  ON  rule_opts.sid = rule_header.sid AND  rule_opts.gid = rule_header.gid
WHERE ( rule_header.sid  IS NULL  OR  rule_header.gid  IS NULL )",
          "query_exec_count" : "2",
          "query_time" : "25.58s (51s)",
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "1956822.0 (3913644)"
        },
        {
          "query" : "SELECT *, unix_timestamp(now()) - time_of_last_ping as ping_delta,
 HEX(domain_uuid) as domain_uuid FROM sensor WHERE id = 'S'",
          "query_exec_count" : "1",
          "query_time" : "19.28s (19s)",
          "rows_affected" : "0.0 (0)",
          "rows_examined" : "1.0 (1)"
        }
      ],
      "Top_ten_table_by_size" : {
        "cfgdb" : [
          {
            "row_count" : 953876,
            "size" : "464.98M",
            "table_name" : "rule_opts"
          },
          {
            "row_count" : 59190,
            "size" : "346.52M",
            "table_name" : "eorevisionstore"
          },
          {
            "row_count" : 47033,
            "size" : "252.61M",
            "table_name" : "eostore"
          },
          {
            "row_count" : 53196,
            "size" : "107.44M",
            "table_name" : "rule_header"
```

```
    },
    {
      "row_count" : 311244,
      "size" : "85.29M",
      "table_name" : "eoattributes"
    },
    {
      "row_count" : 15,
      "size" : "80.52M",
      "table_name" : "sf_policy_pdl"
    },
    {
      "row_count" : 48251,
      "size" : "72.28M",
      "table_name" : "bb_snort3_intrusion_rule_history"
    },
    {
      "row_count" : 45902,
      "size" : "52.61M",
      "table_name" : "bb_snort3_intrusion_rule_data"
    },
    {
      "row_count" : 71579,
      "size" : "45.70M",
      "table_name" : "ids_event_msg_map"
    },
    {
      "row_count" : 68940,
      "size" : "40.73M",
      "table_name" : "eocontainerstore"
    }
  ],
  "sfsnort" : [
    {
      "row_count" : 60905,
      "size" : "27.70M",
      "table_name" : "ids_event_msg_map"
    },
    {
      "row_count" : 568181,
      "size" : "25.43M",
      "table_name" : "rna_vuln_software"
    },
    {
      "row_count" : 464576,
      "size" : "17.87M",
      "table_name" : "geolocation_ipv4_country"
    },
    {
      "row_count" : 12933,
      "size" : "17.59M",
      "table_name" : "rna_vuln"
    },
    {
      "row_count" : 27328,
      "size" : "13.55M",
      "table_name" : "health_alarm_syslog"
    },
    {
      "row_count" : 171944,
      "size" : "13.30M",
      "table_name" : "geolocation_ipv6_country"
    },
    {
```

```
            "row_count" : 116193,
            "size" : "13.18M",
            "table_name" : "cpe_software_map"
          },
          {
            "row_count" : 95676,
            "size" : "13.06M",
            "table_name" : "rna_fp_vuln_map"
          },
          {
            "row_count" : 116193,
            "size" : "11.49M",
            "table_name" : "rna_software_list"
          },
          {
            "row_count" : 32934,
            "size" : "5.55M",
            "table_name" : "vendor_mac_list"
          }
        ]
      },
      "binlog_size" : "2.6G"
    },
    "csdacInfo" : {
        "CSDACConnectorsConfigured" : [
        [
          "azuread-meta-connector",
          1
        ],
        [
          "aws",
          2
        ],
        [
          "o365",
          2
        ],
        [
          "github",
          1
        ]
      ],
      "CSDACFiltersConfigured" : [
        [
          "aws",
          2
        ]
      ],
      "availableConnectorTypes" : [
        "azure",
        "gcp",
        "azuread-meta-connector",
        "aws",
        "vcenter",
        "azure-servicetags",
        "github",
        "o365"
      ],
      "isCSDAConFMCEnabled" : true,
      "totalCSDACinFMCConnectorsConfigured" : 6,
      "totalCSDACinFMCRulesConfigured" : 2     }
}
}
```

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。