

Fortinet.NSE7_SOC_AR-7.6.v2026-10-02.q47

試験コード:	NSE7_SOC_AR-7.6
試験名称:	Fortinet NSE 7 - Security Operations 7.6 Architect
認定資格:	Fortinet
無料問題数:	47
バージョン:	v2026-10-02
アクセス数:	110
ページビュー数:	470
https://www.jpnpdf.com/Fortinet.NSE7_SOC_AR-7.6.v2026-10-02.q47-mondaishu.html	

最新問題: 1

Refer to the Exhibit:

An analyst wants to create an incident and generate a report whenever FortiAnalyzer generates a malicious attachment event based on FortiSandbox analysis. The endpoint hosts are protected by FortiClient EMS integrated with FortiSandbox. All devices are logging to FortiAnalyzer.

Which connector must the analyst use in this playbook?

- A. FortiSandbox connector
- B. FortiClient EMS connector
- C. FortiMail connector
- D. Local connector

Answer: A ([メッセージを残す](#))

* Understanding the Requirements:

* The objective is to create an incident and generate a report based on malicious attachment events detected by FortiAnalyzer from FortiSandbox analysis.

* The endpoint hosts are protected by FortiClient EMS, which is integrated with FortiSandbox. All logs are sent to FortiAnalyzer.

* Key Components:

* FortiAnalyzer: Centralized logging and analysis for Fortinet devices.

* FortiSandbox: Advanced threat protection system that analyzes suspicious files and URLs.

* FortiClient EMS: Endpoint management system that integrates with FortiSandbox for endpoint protection.

* Playbook Analysis:

* The playbook in the exhibit consists of three main actions: GET_EVENTS, RUN_REPORT, and CREATE_INCIDENT.

* EVENT_TRIGGER: Starts the playbook when an event occurs.

* GET_EVENTS: Fetches relevant events.

* RUN_REPORT: Generates a report based on the events.

* CREATE_INCIDENT: Creates an incident in the incident management system.

* Selecting the Correct Connector:

* The correct connector should allow fetching events related to malicious attachments analyzed by FortiSandbox and facilitate integration with FortiAnalyzer.

* Connector Options:

* FortiSandbox Connector:

- * Directly integrates with FortiSandbox to fetch analysis results and events related to malicious attachments.
- * Best suited for getting detailed sandbox analysis results.
- * Selected as it is directly related to the requirement of handling FortiSandbox analysis events.

* FortiClient EMS Connector:

- * Used for managing endpoint security and integrating with endpoint logs.

* サンドボックス分析イベントの取得とは直接関係ありません。

* サンドボックス分析イベントに直接関係しないため、選択されませんでした。

* FortiMailコネクタ :

- * メールセキュリティ、およびメール関連のログやイベントの処理に使用されます。

※サンドボックス分析イベントには適用されません。

* サンドボックス分析に関係がないため、選択されませんでした。

* ローカルコネクタ:

- * FortiAnalyzer内部のローカルイベントを処理します。

* 詳細なサンドボックス分析結果を取得するには、十分な具体性がない可能性があります。

* FortiSandboxとの必要な統合が実現できない可能性があるため、選択しませんでした。

* 実装手順 :

* ステップ 1: FortiSandbox が分析結果を FortiAnalyzer に送信するように設定されていることを確認します。

* ステップ 2: プレイブック内の FortiSandbox コネクタを使用して、悪意のある添付ファイルに関連するイベントを取得します。

* ステップ 3: FortiSandbox コネクタを使用するように GET_EVENTS アクションを設定します。

* ステップ 4: 取得したイベントに基づいて、RUN_REPORT および CREATE_INCIDENT アクションを設定します。

FortiSandbox 統合に関する Fortinet ドキュメント FortiSandbox 統合ガイド FortiAnalyzer イベント処理に関する Fortinet ドキュメント FortiAnalyzer 管理ガイド FortiSandbox コネクタを使用することで、アナリストは、プレイブックが FortiSandbox 分析に基づいてイベントを正確に取得し、必要なインシデントとレポートを生成することを確認できます。

最新問題: 2

自動化ステッチ9を実行するために使用できるFortiAnalyzerコネクタはどれですか？

A. FortiCASB

B. FortiMail

C. ローカル

D. FortiOS

Answer: (解答を表示する)

* 自動縫製の概要 :

FortiAnalyzerのオートメーションステッチとは、特定のイベントによってトリガーされる、あらかじめ定義された一連の自動アクションのことです。これらのアクションは、セキュリティインシデントへの対応を自動化し、効率性を向上させ、対応時間を短縮するのに役立ちます。

* FortiAnalyzerコネクタ :

FortiAnalyzerは、コネクタを介して様々なFortinet製品やその他のサードパーティ製ソリューションと統合します。これらのコネクタは通信とデータ交換を容易にし、集中管理と自動化を実現します。

* 自動縫製に使用可能なコネクタ :

* FortiCASB:

* FortiCASBは、SaaSアプリケーションのセキュリティ確保を支援するクラウドアクセスセキュリティブローカーです。

ただし、これは通常、FortiAnalyzer内で自動化ステッチを実行するために使用されるものではありません。

参照: Fortinet FortiCASB ドキュメント FortiCASB

FortiMail:

FortiMailはメールセキュリティソリューションです。ログやイベントをFortiAnalyzerに送信することはできますが、主に自動化ステッチの実行に使用されるものではありません。

参考資料 :Fortinet FortiMail ドキュメント FortiMail

地元 :

ローカルコネクタとは、FortiAnalyzerが自身で生成したログやイベントを処理する機能を指します。これは内部プロセスには役立ちますが、自動化のために他のFortinetデバイスと統合する用途には特に適していません。

参考資料 :Fortinet FortiAnalyzer 管理ガイド FortiAnalyzer ローカル FortiOS :

FortiOSは、FortiGateファイアウォール上で動作するオペレーティングシステムです。FortiAnalyzerは、FortiOSコネクタを使用してFortiGateデバイスと通信し、自動化処理を実行できます。これにより、FortiAnalyzerはFortiGateにコマンドを送信し、特定のイベントに応じて事前に定義されたアクションを実行できます。

参考資料 :Fortinet FortiOS 管理者ガイド FortiOS

詳細なプロセス :

ステップ1 :FortiAnalyzerでFortiOSコネクタを設定し、FortiGateデバイスとの通信を確立します。

ステップ2 :FortiAnalyzer内で、特定のイベントが発生したときに実行されるアクションを指定する自動化ステッチを定義します。

ステップ3 :トリガーとなるイベントが検出されると、FortiAnalyzerはFortiOSコネクタを使用して、必要なコマンドをFortiGateデバイスに送信します。

ステップ4 :FortiGateはコマンドを実行し、IPアドレスのブロック、ファイアウォールルールの更新、アラートの送信など、事前に定義されたアクションを実行します。

結論 :

FortiOSコネクタは、FortiGateデバイスとの統合を目的として特別に設計されており、FortiAnalyzerが自動化ステッチを効果的に実行できるようにします。

参考文献 :

Fortinet FortiOS 管理者ガイド : 自動化ステッチの設定と使用に関する詳細。

Fortinet FortiAnalyzer 管理者ガイド :コネクタと統合オプションに関する情報。

FortiAnalyzerはFortiOSコネクタを利用することで、自動化された連携処理を実行し、ネットワーク内のセキュリティ体制と対応能力を強化できます。

最新問題: **3**

展示資料を参照してください。

Excessive FTP Connections from 10.200.3.219

Subpattern: FTP_Traffic

Displaying 1 - 100 of 100

Sep 09, 2025, 05:00:45 PM - Sep 10, 2025, 05:00:45 PM

Event Receive Time	Destination IP	Sent Packets64	Received Packet...	Sent Bytes64	Received Bytes64	Duration
Sep 10, 2025, 05:00:07 PM	10.200.200.166	1	0	44 B	0B	11s
Sep 10, 2025, 05:00:07 PM	10.200.200.128	1	0	44 B	0B	11s
Sep 10, 2025, 05:00:07 PM	10.200.200.129	1	0	44 B	0B	11s
Sep 10, 2025, 05:00:07 PM	10.200.200.159	1	0	44 B	0B	11s
Sep 10, 2025, 05:00:07 PM	10.200.200.91	1	0	44 B	0B	11s

Raw Logs

Raw Message

```
<189>date=2025-09-10 time=13:58:46 devname="FortiGate-ISFW"
devid="FGVMSLTM24000847" eventtime=1757537925873767456 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice"
vd="root" srcip=10.200.3.219 srcport=55690 srcintf="port1"
srcintfrole="undefined" dstip=10.200.200.166 dstport=21 dstintf="port3"
dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=12754790 proto=6 action="timeout" policyid=1 policytype="policy"
poluid="703716b8-c06a-51ee-4b75-69d6ec904e3f" policyname="Any-Any"
service="FTP"trandisp="noop" appcat="unscanned" duration=11 sentbyte=44
rcvdbyte=0 sentpkt=1 rcvdpkt=0
```

宛先IPアドレスを除き、トラフィックの流れはすべて同一であると仮定します。この環境には、ネットワークアドレス変換 (NAT) モードで動作するFortiGateが1台のみ存在します。提示された証拠に基づいて、このFortiSIEMインシデントについてどのような2つの結論を導き出せますか？ 2つ選択してください)

- A. クライアント10.200.3.219はアクティブな偵察活動を行っています。
- B. FortiGate がパケットを宛先ホストにルーティングしていません。
- C. 宛先ホストが応答していません。
- D. FortiGate が戻りフローをブロックしています。

Answer: ([解答を表示する](#))

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明：

FortiSIEM 7.3インターフェースで提供されるトリガーイベントと生メッセージの分析に基づくと、次のようになります。

* アクティブ偵察 (A): 「トリガーイベント」テーブルには、単一の送信元 IP (10.200.3.219) が複数の異なる宛先 IP アドレス (10.200.200.166、.128、.129、.159、.91) 同じサービス (FTP/ポート 21) 上で接続を試みます。各試行は、送信パケット 1 つと受信パケット 0 個で構成されます。この『対 多』の連続接続試行のパターンは、アクティブ偵察の主要な手法である水平ポートスキャンの特徴です。

* 宛先ホストが応答していません (C): 生ログにはアクションが「timeout」と表示され、具体的には「sentpkt=1 rcvdpkt=0」と表示されます。FortiGate ログのロジック (FortiSIEM が解析) では、受信パケットがゼロの「timeout」は、ファイアウォールがパケットの送信を許可した (アクションが「deny」ではなかった) もの、セッションタイムアウト期間内にターゲットホストから SYN-ACK または応答が受信されなかったことを示します。これは、宛先ホストがオフライン、存在しない、またはトラフィックをサイレントに破棄していることを示しています。

他の選択肢が間違っている理由：

* FortiGate がルーティングを行っていない (B): FortiGate がパケットをルーティングしていない場合、ログには通常、「タイムアウト」で終了するセッション初期化の成功は表示されず、ルーティングエラー/拒否が表示されます。

44バイトが送信されたという事実は、FortiGateがトラフィックを処理し、転送を試みたことを示しています。

* FortiGate が戻りフローをブロックしています (D): FortiGate のセキュリティ ポリシーによって戻りフローがブロックされている場合、通常、戻りトラフィックに対してアクションが「拒否」としてログに記録され、セッション状態は一般的なセッション タイムアウト」ではなくポリシー違反を反映します。

最新問題: 4

Which three are threat hunting activities? (Choose three answers)

- A. Enrich records with threat intelligence.
- B. Automate workflows.
- C. Generate a hypothesis.
- D. Perform packet analysis.
- E. Tune correlation rules.

Answer: ([解答を表示する](#))

According to the specialized threat hunting modules and frameworks within FortiSOAR 7.6 and the advanced analytics capabilities of FortiSIEM 7.3 , threat hunting is defined as a proactive, human-led search for threats that have bypassed automated security controls. The three selected activities are core components of this lifecycle:

* Generate a hypothesis (C): This is the fundamental starting point of a " Structured Hunt. " Analysts develop a testable theory-based on recent threat intelligence (such as a new TTP identified by FortiGuard) or environmental risk-about how an attacker might be operating undetected in the network.

* Enrich records with threat intelligence (A): During the investigation phase, hunters use the Threat Intelligence Management (TIM) module in FortiSOAR to enrich technical data (IPs, hashes, URLs) with external context. This helps determine if an anomaly discovered during the hunt is indeed malicious or part of a known campaign.

* Perform packet analysis (D): Since advanced threats often live in the " gaps " between log files, hunters frequently perform deep-packet or network-flow analysis using FortiSIEM's query tools or integrated NDR (Network Detection and Response) data to identify suspicious lateral movement or C2 (Command and Control) communication patterns that standard alerts might miss.

Why other options are excluded:

* Automate workflows (B): While SOAR is designed for automation, the act of " automating " is a DevOps or SOC engineering task. Threat hunting itself is a proactive investigation; while playbooks can assist a hunter (e.g., by automating the data gathering), the act of hunting remains a manual or semi- automated cognitive process.

* Tune correlation rules (E): Tuning rules is a reactive maintenance task or a " post-hunt " activity.

Once a threat hunter finds a new attack pattern, they will then tune SIEM correlation rules to ensure that specific threat is detected automatically in the future. The tuning is the result of the hunt, not the activity of hunting itself.

最新問題: 5

提携組織が最近、分散型サービス拒否 (DDoS) 攻撃を受けましたが、攻撃者の身元とTTP（戦術 技術、手順）は不明です。貴社のSOC セキュリティオペレーションセンター）は、提携組織から関連する脅威情報を受け取っていませんが、同様の活動が貴社の環境でも発生している可能性があるかどうかを判断するよう求められています。最初に実行すべき脅威ハンティングアクションはどれですか？回答を1つ選択してください。

- A. 受信トラフィックがベースラインしきい値を超えた場合にアラートを発するようにSIEMルールを設定します。
- B. パケットアナライザーを使用して、重要なデバイス上のすべてのトラフィックフローをキャプチャして確認します。
- C. DDoS攻撃がネットワークに対してどのように実行されるかに基づいて、攻撃予測仮説を立ててください。
- D. 脅威インテリジェンスを使用して、すべての外部ソース IP アドレスの IP アドレスを充実させます。

Answer: ([解答を表示する](#))

Exact Extract: "What are two characteristics of threat hunting? ... It looks for undetected threats... It requires a hypothesis and investigation." Exact Extract: "By demonstrating competence in examining a simple threat hunting use case, you will be able to conduct threat hunting based on an easily verifiable hypothesis." The correct answer is C . This is a threat hunting scenario, not a normal alert-engineering scenario. You do not know the attacker identity, infrastructure, tools, or exact TTPs, so the first mature action is to form a hypothesis such as: "If a similar

DDoS campaign is targeting us, we may observe abnormal inbound request volume, source diversity, protocol concentration, SYN/UDP/HTTP flood patterns, or service degradation against exposed assets." That hypothesis then drives the FortiSIEM analytics search and evidence collection.

A is useful later, after the hunt identifies a reliable detection condition. B is too broad and operationally expensive as a first step. D is weak because no relevant threat intelligence has been received, and enriching every external IP is noisy and inefficient.

Technical Deep Dive: A good DDoS hunt should start with exposed services, normal traffic baselines, traffic volume anomalies, source ASN/country dispersion, destination service concentration, firewall deny/accept spikes, SYN-to-completion ratios, and web request rates. After confirming patterns, you tune FortiSIEM rules and FortiSOAR response playbooks.

FortiGate NP/CP acceleration may affect packet-forwarding performance under flood conditions, but the hunting workflow itself is driven by SIEM telemetry and hypothesis-based analytics.

最新問題: 6

展示資料を参照してください。

Refer to the exhibit.

operation: Get Device Information	
Input parameters	
Parameter	Description
Device IP	Specify the IP address of the device whose details you want to retrieve from the Fortinet FortiSIEM server.
Organization	(Optional) Specify the name of the organization for which you want to retrieve details of the device from the Fortinet FortiSIEM server.

FortiSIEMコネクタアクションの入力例を示します。

FortiSOAR上で、以下のことを実現できるプレイブックを作成したいとします。

IPアドレスを手動で入力してください。

図に示すコネクタアクションを使用して、そのIPアドレスを持つデバイスをFortiSIEM構成管理データベース（CMDB）から取得します。

SOCマネージャーに、FortiSIEMから取得した当該デバイスに関する情報を確認するよう依頼してください。

管理者が承認すれば、資産記録が作成されます。

どの手順の組み合わせと順序が、必要なプレイブックの手順数を最小限に抑えつつ、要件を満たすでしょうか？

A. 手動トリガー、2)コネクタアクション、3) 承認4)レコード作成

B. 1) 手動トリガー、2) 変数設定、3) コネクタアクション、4) 変数設定、5) 承認、6) レコード作成

C. 作成トリガー、2)コネクタアクション、3) 手動スキップ、4)レコードの作成

D. コネクタアクション、2) 承認3)レコード作成、4)レコード更新

Answer: [\(解答を表示する\)](#)

正確な抜粋: Cのプレイブックでは、ユーザーからの入力、具体的には IP アドレスも必要とします... IP アドレスを手動で入力できます。トリガー入力は ipAddress として保存され、後で動的値として参照できます。」正確な抜粋: Eコネクタを最初に構成する必要があります... 選択されたアクションは IP レピュテーションの取得です... IP レピュテーションの取得アクションには入力が必要です。トリガー ステップでは、トリガー入力から ipAddress パラメータを定義しました。これをこのステップに動的にマッピングできます。」正確な抜粋: Eコネクタ ステップの後には承認ステップがあります。説明を手動で追加することも、動的値ウィンドウを使用して説明フィールドなどのフィールドに入力することもできます。」正解は A です。ワークフローにはアナリストが提供する入力が必要なので、IP アドレスを入力する手動トリガーから始める必要があります。その IP アドレスは FortiSIEM デバイス情報の取得コネクタ アクションに直接渡されます。そのコネクタ アクションからの出力は、承認ステップを通じて SOC マネージャーに表示されます。承認されると、プレイブックは「レコードの作成」に進み、FortiSIEM CMDBの結果から資産レコードを作成します。

オプションBは冗長です。手動トリガー値とコネクタ出力はDynamic Values/Jinjaを介して直接参照できるため、変数設定ステップは不要です。オプションCは、On Createはイベント駆動型であり手動入力ではないため、またManual Taskは承認ステップと同じ承認/拒否ワークフローを提供しないため、誤りです。オプションDは、手動トリガーが欠落しており、不要なレコード更新ステップが追加されているため、誤りです。

技術的な詳細解説 :FortiSOARの基本的なパターンは、手動入力 # 外部検索 # 人間による承認 # レコード作成です。実装では、手動トリガーがdevice_ipを取得し、FortiSIEMコネクタアクションがその値をデバイスIPにマッピングします。承認ステップでは、ホスト名、IPアドレス、組織、デバイスタイプ、CMDB属性などの主要な返されたフィールドが表示され、レコード作成ステップでは、承認された出力がアセットモジュールにマッピングされます。これがSOARワークフローのオーケストレーションです。トラフィック転送やASIC検査パスが関与しないため、FortiGate NP/CPのハードウェアオフロードは関係ありません。

最新問題: 7

後続のタスクでトリガーイベントをトリガー変数として使用できるようにするプレイブックトリガーはどれですか？ 2つ選択してください。）

- A. イベント
- B. 事件
- C. 予定通り
- D. オンデマンド

Answer: A,B ([メッセージを残す](#))

* プレイブックのトリガーを理解する：

* プレイブックのトリガーは、FortiAnalyzerまたはFortiSOAR内の自動化されたワークフローの開始点です。

* これらのトリガーは、プレイブックの実行方法と実行タイミングを決定し、プレイブック内の後続タスクに関連情報（トリガー変数）を渡すことができます。

* プレイブックトリガーの種類：

* イベントトリガー：

特定のイベントが発生したときにプレイブックを起動します。

* イベントの詳細は、後続のタスクで変数として使用して、応答をカスタマイズできます。

* イベントの詳細をトリガー変数として使用できるため、選択しました。

* インシデント発生のトリガー：

* インシデントが作成または更新されたときに、プレイブックをアクティブ化します。

* インシデントの詳細は、後続のタスクで変数として利用できます。

* インシデントの詳細をトリガー変数として使用できるため、選択されました。

* スケジュールどおりにトリガー：

指定された時刻または間隔でプレイブックを実行します。

* トリガーイベントを本来的に使用して変数を後続のタスクに渡すことはありません。

トリガーイベントの詳細を渡す必要がないため、選択しませんでした。

* オンデマンドトリガー：

- * プレイブックを手動で、または必要に応じて実行します。
- * 後続のタスクで使用するためのトリガーイベントの詳細を自動的に含めることはありません。
- * 変数にトリガーイベントを使用しないため、選択されません。
- * 実装手順 :
- * ステップ 1: プレイブック構成で、イベントまたはインシデント トリガーの条件を定義します。
- * ステップ 2: トリガー イベントまたはインシデントの詳細を使用して、後続のタスクでアクションと応答をカスタマイズします。
- * ステップ 3: プレイブックをテストして、トリガー変数が正しく渡され、使用されていることを確認します。
- * 結論 :
- * イベントおよびインシデントトリガーは、特定の事象に基づいてプレイブックを起動するように特別に設計されており、トリガーの詳細を後続のタスクで使用できます。

Fortinet の Playbook 構成に関するドキュメント FortiSOAR Playbook ガイド EVENT および INCIDENT トリガーを使用することで、トリガー イベントを後続のタスクで変数として活用し、より動的で応答性の高い Playbook アクションを実現できます。

最新問題: 8

You are trying to create a playbook that creates a manual task showing a list of public IPv6 addresses. You were successful in extracting all IP addresses from a previous action into a variable called `ip_list`, which contains both private and public IPv4 and IPv6 addresses. You must now filter the results to display only public IPv6 addresses. Which two Jinja expressions can accomplish this task? (Choose two answers)

- A. `{{ vars.ip_list | ipv6addr('public') }}`
- B. `{{ vars.ip_list | ipaddr('public') | ipv6 }}`
- C. `{{ vars.ip_list | ipaddr('!private') | ipv6 }}`
- D. `{{ vars.ip_list | ipv6 | ipaddr('public') }}`

Answer: ([解答を表示する](#))

Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:

In FortiSOAR 7.6, the playbook engine utilizes the powerful `ipaddr` family of Jinja filters (derived from the Ansible `netaddr` library) to manipulate network data. To isolate public IPv6 addresses from a mixed list, the order of operations in the filter chain ensures the correct data is extracted:

- * Double Filtering Sequence (B): In the expression `{{ vars.ip_list | ipaddr('public') | ipv6 }}`, the first filter `ipaddr('public')` processes the entire list and retains only public addresses, including both IPv4 and IPv6 versions. The second filter in the pipe, `| ipv6`, then takes that subset of public addresses and filters them again to keep only those that conform to the IPv6 standard. The final result is a list containing only public IPv6 addresses.
- * Version-First Filtering (D): In the expression `{{ vars.ip_list | ipv6 | ipaddr('public') }}`, the logic is reversed but equally effective. The first filter `| ipv6` immediately strips all IPv4 and non-IP strings from the list, leaving only IPv6 addresses (both private and public). The subsequent filter `| ipaddr('public')` then evaluates these IPv6 addresses and discards any that fall within the private/unique-local ranges (like ULA or link-local), resulting in the same set of public IPv6 addresses.

Why other options are incorrect:

- * A (`ipv6addr 'public'`): While `ipv6addr` is a valid filter in many Ansible environments, FortiSOAR's standard documentation for manual task creation and data manipulation primarily emphasizes the use of the generic `ipaddr` filter with specific flags or chained version filters (like `| ipv6`) to ensure cross- compatibility with the underlying Python libraries used by the SOAR engine.
- * C (`!private` syntax): The `ipaddr` filter utilizes specific keywords for classification. While "not private" is the logical requirement, the filter expects positive assertions such as 'public', 'private', or 'multicast'. The `!private` syntax is not a supported or documented operator for this filter within the Fortinet SOC ecosystem.

最新問題: 9

展示資料を参照してください。

スパイフィッシングイベントハンドラーと関連するルールを設定しましたが、FortiAnalyzerはイベントを生成しませんでした。

FortiAnalyzerのログビューアを確認すると、生ログの図に示すように、FortiSandboxが適切なログを転送したことが確認できます。

FortiAnalyzerがイベントを生成するためには、FortiAnalyzerのどの設定を変更する必要がありますか？

A. [ログの種類] フィールドで、[ウイルス対策ログ (マルウェア)] を選択します。

B. FortiSandboxデータセレクトアを設定し、イベントハンドラに追加します。

C. [テキストによるログフィルタ] フィールドに、値 `!sub type malware..`を入力します。

D. 選択によりトリガー条件を変更します。グループ内で、ログフィールド `!malware name >`」に 2 つ以上の固有の値があります。

Answer: B (メッセージを残す)

* イベントハンドラー構成の理解：

* イベントハンドラーは、FortiSandboxなどの他のFortinet製品から転送されたログに基づいて、スパフィッシングなどの特定のセキュリティインシデントを検出するように設定されています。

* イベントハンドラには、イベントがトリガーされるべき条件を定義するルールが含まれます。

* 現在の構成の分析：

* 現在のイベントハンドラは `スパフィッシングハンドラ` という名前で、`スパフィッシングルール1` というタイトルのルールがあります。

ログビューアには、FortiSandboxによってログが転送されていることが示されていますが、FortiAnalyzerによってイベントは生成されていません。

* イベント処理の主要コンポーネント：

* ログタイプ : イベントハンドラをトリガーするログの種類を決定します。

* データセクター : イベントをトリガーするためにログが満たすべき条件を指定します。

* オートメーションステッチ : イベント発生時にトリガーできるオプションのアクション。

* 通知 : イベントが検出されたときにアラートがどのように伝達されるかを定義します。

* 問題の特定：

* FortiSandboxのログは正しく転送されているにもかかわらずイベントが生成されないため、問題はデータセクターの設定またはログタイプのマッチングにある可能性が高いです。

* データセクターは、FortiSandboxによって転送されるログを含めるように設定する必要があります。

* 解決：

* B. FortiSandboxデータセクターを設定し、イベントハンドラーに追加します。

FortiSandboxログ専用のデータセクターを設定し、それをイベントハンドラーに追加することで、FortiAnalyzerは転送されたログに基づいてイベントを正確に識別し、トリガーすることができます。

* ソリューションを実装するための手順：

* ステップ 1: FortiAnalyzer のイベント ハンドラー設定に移動します。

* ステップ 2: FortiSandbox によって転送されたログに一致する条件 (ログのサブタイプ、マルウェア検出の詳細など) を含む新しいデータセクターを追加します。

* ステップ 3: このデータセクターを既存のスパフィッシングイベントハンドラにリンクします。

* ステップ 4: 設定を保存し、テストしてイベントが生成されていることを確認します。

* 結論：

イベントハンドラー内でFortiSandboxデータセクターを正しく構成することで、FortiAnalyzerが関連するログに基づいてイベントを生成できるようになります。

：

Fortinet のイベント ハンドラーとデータ セクターに関するドキュメント FortiAnalyzer イベント ハンドラー Fortinet のデータ セクターの設定に関するナレッジ ベース FortiAnalyzer データ セクター FortiSandbox データ セクターを設定してイベント ハンドラーに追加することで、FortiAnalyzer は適切なログに基づいてイベントを正確に生成できるようになります。

最新問題: 10

展示資料を参照してください。

Configurations window

Summary Configurations Actions & Playbooks Agents

Visibility ⓘ Public Private

Server URL:*

fortisiem.cs.lab

Username:*

fortisoar-user

Password:*

Set Password

Password fields are write-only. If you do not change this field, your Password will not be overwritten.

Organization: ⓘ

FortiSIEM

Verify SSL:

☐



FortiSOAR上でFortiSIEMコネクタを設定しました。しかし、設定を保存しようとする、図に示すエラーが表示されます。考えられる原因を2つ挙げてください。

- A. 公開設定は「公開」に設定する必要があります。
- B. FortiSOARがFortiSIEMに接続できません。
- C. 組織はスーパーであるべきです。
- D. ユーザー認証情報がFortiSIEMと一致しません。

Answer: C,D (メッセージを残す)

正確な抜粋: FortiSOAR で FortiSIEM コネクタを構成するには、次のパラメータを定義する必要があります。サーバー URL... ユーザー名... パスワード... 組織: FortiSIEM サーバーでアクセスする組織の名前を指定します。テナントのないエンタープライズ展開モデルの場合、組織は super です。」正確な抜粋: 必要な最小限の権限は、インシデントに対する読み取りおよび更新アクセス、および高度な検索クエリの実行アクセスです。」正解は C と D です。エラーダイアログには、ステータスコード 401 と 無効な認証情報が提供されました」または 要求が承認されていません」が表示されます。401 応答は、FortiSOAR が FortiSIEM に到達したが、FortiSIEM が認証または認可を拒否したことを意味します。構成図では、組織の値は FortiSIEM に設定されています。テナントのないエンタープライズ展開の場合、ガイドでは組織は super である必要があると記載されています。

そのため、組織情報が間違っていると認証に失敗する可能性があります。もう一つの有効な原因は、FortiSIEMの認証情報が間違っていることです。ユーザー名とパスワードは、コネクタの設定パラメータとして必須だからです。

Aは誤りです。可視性は、FortiSOAR内部でコネクタ構成がパブリックかプライベートかを制御するものであり、FortiSIEM API認証の失敗を引き起こすものではありません。Bも誤りです。到達可能性の問題が発生した場合、通常は接続エラー、DNSエラー、タイムアウト、またはSSLエラーが発生し、FortiSIEMが生成する401認証応答は発生しません。

技術的な詳細分析 :FortiSOARコネクタのヘルスチェックは、トランスポート認証とAPI認証の両方を検証します。インストールと構成は完了しているものの、ヘルスチェックが401エラーで失敗しているため、ネットワークパスとコネクタのインストールが主な問題ではありません。FortiSIEMのユーザー名を修正してください。

/password を実行し、FortiSIEM にアカウントが存在すること、必要な権限が付与されていることを確認してから、適切な組織 テナントのないエンタープライズ展開の場合は通常 super) を設定します。これは API 認証および認可の動作であり、ファイアウォールのデータプレーンのトラフィック処理は分析されないため、FortiGate NP/CP のハードウェア オフロードは関係ありません。

最新問題: 11

FortiSIEMルールエンジンは、特定のサブパターンに対して集計条件 COUNT (一致したイベント)」を評価する際に、どの3つの要素を使用してカウントを決定しますか？ 3つ選択してください)

- A. 属性によるグループ化
- B. データソース
- C. 時間枠
- D. 検索フィルター
- E. インシデントアクション

Answer: A,C,D (メッセージを残す)

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明：

FortiSIEMのルールエンジンは、サブパターンを評価して複雑な攻撃動作を検出します。ルールでCOUNT (一致したイベント)などの集計条件を使用する場合、エンジンは特定のアーキテクチャパラメータに基づいてこの値を計算します。

* グループ化属性 (A): エンジンは、各固有の組み合わせごとに個別のカウンターを保持します。

サブパターンで定義された「グループ化」属性。たとえば、「送信元IPアドレス」でグループ化すると、エンジンは各固有IPアドレスのイベント数を個別に追跡します。

* 時間枠 C) カウントは特定の時間間隔 (例5分)を基準としています。エンジンは、このスライディングウィンドウまたは固定ウィンドウの範囲内にあるイベントのみをカウントします。イベントがこのウィンドウの範囲外になると、集計カウントには含まれなくなります。

* 検索フィルター D) :「検索フィルター」条件 (例イベントタイプ= ログイン失敗)」を満たすイベントのみが「一致イベント」とみなされます。このフィルターは、ルールエンジンがカウントを適用する前に処理するデータの範囲を定義します。

他の選択肢が間違っている理由：

* データソース B) データソースはログの出所を決定しますが、ルールエンジン自体は、生のデータソースではなく、解析された属性 (検索フィルターで定義)を使用してカウントを決定します。

複数のデータソースが同じフィルターやカウント結果に影響を与える可能性があります。

* インシデントアクション E) インシデントアクション (メールの送信やSOARプレイブックのトリガーなど)は、ルールの実行結果です。これらは、評価フェーズにおける内部ロジックやイベント数の計算には影響しません。

最新問題: 12

インシデントレポートを確認してください。

パケットキャプチャによると、ホストは通常のHTTPSトラフィックを模倣したTLSセッションを定期的に維持し、TCPポート8443を使用して単一の外部ホストと通信している。アナリストは、このトラフィックを潜在的なコマンド&コントロール攻撃であると指摘した。同時期に、ホストは攻撃者が制御するドメインに対して、サイズの大きいTXTペイロードを含むDNSクエリを頻繁に送信し、準備済みのファイルを転送していた。

この活動を最もよく表すMITRE ATT & CKの手法はどれですか？ 2つ選択してください)

- A. 非標準ポート
- B. リモートサービスの活用
- C. 代替プロトコルによる細胞除去
- D. アーティファクトを隠す

Answer: (解答を表示する)

FortiSIEM 7.3およびFortiSOAR 7.6で使用されているMITRE ATT & CKマッピングに従って、記述された動作は、次の技術に対応します。

* 非標準ポート (T1571): この手法では、攻撃者が通常関連付けられないプロトコルとポートの組み合わせを使用して通信を行います。インシデントレポートでは、標準ポート443ではなくTCP 8443でHTTPS (TLS) トラフィックが実行されていることが特定されます。FortiSIEMには、このようなプロトコルとポートの不一致を検出するように設計された「疑わしい典型的なマルウェアのバックコネクトポート」などの関連ルールが組み込まれています。

* 代替プロトコルによるデータ漏洩 (T1048): この手法では、攻撃者が主要なコマンドおよび制御 (C2) チャネルとは異なるプロトコルを使用してデータを漏洩させることでデータを盗み出すことを説明します。このシナリオでは、C2 チャネルはポート 8443 で HTTPS を介して確立されますが、攻撃者はサイズの大きいTXT ペイロードを使用したDNS クエリを使用してステージングされたファイルを転送します。DNS は、標準的なデータ転送監視および送信フィルタリングを回避するために使用される一般的な「代替プロトコル」です。

誤った選択肢の分析：

* リモートサービスの悪用 (B) この手法は、初期アクセスまたは横方向移動の戦術に分類され、SMBやRDPなどのネットワークサービスの脆弱性を利用してシステムへの侵入を図ることに重点を置いています。確立されたC2チャネルの維持やデータの持ち出しには適用されません。

* 痕跡の隠蔽 (D): これは、攻撃者がログファイルやレジストリキーなどの痕跡を削除することで、自身の存在を隠蔽しようとする防御回避技術です。攻撃者は「通常のトラフィックを模倣」していますが、非標準ポートの使用やDNSの漏洩といった具体的な行為は、より具体的な技術によって定義される主要な行動シグネチャです。

最新問題: 13

展示資料を参照してください。

脅威ハンティングモジュールを使用してデータを分析した結果、どのような結論が得られますか？

- A. スピアフィッシングは、機密情報を引き出すために使用されています。
- B. DNSトンネリングを使用して、ローカルネットワークから機密データを抽出しています。
- C. 偵察活動を用いて、メールサーバーから被害者の身元情報を収集しています。
- D. FTPは、データマイニングのためのコマンド&コントロール (C&C) 技術として使用されています。

Answer: B (メッセージを残す)

* 脅威ハンティングデータの理解：

* 提供された資料にある脅威ハンティングモニターには、さまざまなアプリケーションサービス、その使用回数、および送信バイト数、平均送信バイト数、最大送信バイト数などのデータメトリックが表示されます。

* 展示の2番目の部分は、特定の送信元IPアドレス (10.0.1.10)から宛先IPアドレス (8.8.8.8)への接続試行を一覧表示し、「接続失敗」メッセージが繰り返し表示されていることを示しています。

* アプリケーションサービスの分析：

* DNSは、非常に高い件数 (251,400)と注目すべき送信バイト数 (9.1 MB)を誇る、トップのアプリケーションサービスです。

* この大量のDNS トラフィックは、通常のDNS クエリとしては異例であり、DNS トンネリングの存在を示している可能性があります。

* DNSトンネリング：

* DNSトンネリングとは、攻撃者がDNSクエリとレスポンスにデータをエンコードすることでセキュリティ制御を回避するために用いる手法です。これにより、攻撃者は検出されることなくローカルネットワークからデータを抽出できます。

* 大量のDNSトラフィックと詳細なメトリクスから、DNSトンネリングが使用されている可能性が示唆される。

* 8.8.8.8への接続失敗：

* 送信元IPアドレス(10.0.1.10)から宛先IPアドレス(8.8.8.8)への接続試行が繰り返され、接続に失敗している場合は、外部サーバーとの通信を試みている可能性があります。

* Google DNS (8.8.8.8) は、その信頼性とグローバルな普及率から、DNS トンネリングによく使用されます。

* 結論：

* 大量のDNSトラフィックと接続試行の性質を考慮すると、DNSトンネリングがローカルネットワークから機密データを抽出するために使用されていると結論付けるのは妥当である。

* 他の選択肢が実現しにくい理由：

* スピアフィッシング A)：提供されたデータには、電子メールログやフィッシング指標など、スピアフィッシングの試みを示す証拠はありません。

* 偵察 C) データには、メールサーバーのスキャンやプロービングなどの典型的な偵察活動は示されていません。

* FTP C & C (D)：提供されたデータには、FTP トラフィックや FTP を使用したコマンドおよび制御通信の証拠はありません。

：

SANS Institute: " DNS トンネリング: DNS クエリによるデータ漏洩とトンネリングの検出方法 " SANS DNS トンネリング OWASP: " DNS トンネリング " OWASP DNS トンネリング 提供された脅威ハンティングデータを分析すると、DNS トンネリングがデータ漏洩に使用されていることが明らかになり、ネットワークから機密情報を抽出する高度な方法が示されています。

最新問題: 14

ネットワークを監視中に、1台のFortiGateデバイスが、トポロジー内の他のすべてのFortiGateデバイスよりも著しく多くのログをFortiAnalyzerIに送信していることが判明しました。

さらに、FortiGateデバイスが登録されているADOMは、常に割り当て量を超過しています。

考えられる解決策を2つ挙げてください。(2つ選択してください。)

A. 最初のFortiGateデバイスのストレージ容量を増やします。

B. 最初の FortiGate デバイス用に別の ADOM を作成し、異なるストレージ ポリシーを設定します。

C. 最初の FortiGate デバイスを再設定して、FortiAnalyzer に転送されるログの数を減らします。

D. 最初のFortiGateデバイスから送信されるデータをフィルタリングするために、データセレクトアを設定します。

Answer: B,C (メッセージを残す)

* 問題の理解：

* FortiGateデバイスのうち1台が、他のデバイスと比較して著しく大量のログを生成しており、ADOMのストレージ容量を超過しています。

* これにより、FortiAnalyzer内でのパフォーマンスの問題やログの効率的な管理の困難が生じる可能性があります。

* 考えられる解決策：

* 目標は、ログの量を管理し、ADOM が割り当て量を超えないようにしつつ、効果的なログ分析と監視を維持することです。

* 解決策 A: 最初の FortiGate デバイスのストレージ容量クォータを増やす：

ストレージ容量の割り当てを増やすことで一時的な緩和は得られるかもしれませんが、問題の根本原因である過剰なログ容量の解決にはなりません。

* 丸太の量は今後も増加し続ける可能性があるため、この解決策は長期的には持続可能ではないかもしれません。

長期的に見て効率的な解決策とはならないため、選定されませんでした。

* 解決策 B: 最初の FortiGate デバイス用に別の ADOM を作成し、異なるストレージ ポリシー セットを構成します。

* 個別の ADOM を作成することで、ログ量の多いデバイスに特化したストレージ ポリシーと管理をカスタマイズできます。

* これにより、ストレージ負荷を分散し、より厳格な、またはカスタマイズされた保持およびストレージポリシーを適用するのに役立ちます。

* ログの保存と整理を効果的に管理できるため選定しました。

* 解決策 C: 最初の FortiGate デバイスを再設定して、FortiAnalyzer に転送するログの数を減らします。

* FortiGateデバイスのログ設定を調整することで、FortiAnalyzerIに転送されるログの量を減らすことができます。

* これには、不要なログ記録の無効化、ログレベルの引き下げ、重要度の低いログのフィルタリングなどが含まれます。

* ログ容量過多の問題に直接対処できるため、選定しました。

* 解決策 D: 最初の FortiGate デバイスから送信されるデータをフィルタリングするようにデータセレクトアを設定します。

* データセレクトアを使用すると、FortiAnalyzerに送信されるログをフィルタリングして、関連するログのみが転送されるようにすることができます。

* これはログの量を減らすのに役立ちますが、重要なログを見落とさないようにするためには、詳細な設定と定期的な更新が必要になる場合があります。

* FortiGateデバイス上でログ設定を直接再構成するほど効果的ではない可能性があるため、選択しませんでした。

* 実装手順：

* 解決策Bの場合：

* ステップ 1: FortiAnalyzer にアクセスし、ADOM 管理セクションに移動します。

* ステップ 2: ログ量の多い FortiGate デバイス用に新しい ADOM を作成します。

* ステップ 3: FortiGate デバイスをこの新しい ADOM に登録します。

* ステップ 4: 新しい ADOM に対して、ログの保持と保存を管理するための特定のストレージ ポリシーを設定します。

* 解決策Cの場合：

* ステップ 1: FortiGate デバイスの設定インターフェースにアクセスします。

* ステップ 2 :ログ設定に移動します。

* ステップ 3: ログレベルを調整し、不要なログを無効にします。

* ステップ 4: 設定を保存し、FortiAnalyzer に送信されるログ ボリュームを監視します。

FortiAnalyzer ADOMとログ管理に関するFortinetドキュメント FortiAnalyzer管理ガイド FortiGateでのログ設定の構成に関するFortinetナレッジベース FortiGateロギングガイド ログ量の多いFortiGateデバイス用に個別のADOMを作成し、そのロギング設定を再構成することで、ログ量を効果的に管理し、ADOMがクォータを超えないようにすることができます。

最新問題: 15

添付資料を参照してください。

あなたは、複数のログ記録デバイスが登録されているネットワークにおける、新しいFortiAnalyzerの導入状況をレビューする任務を負っています。ネットワークトポロジーにはFortiAnalyzerは1台のみです。

どのような潜在的な問題点が見られますか？

A. 割り当てられたディスク容量が不足しています。

B. 分析データとアーカイブデータの比率が正しく設定されていません。

C. 分析データの保持期間が長すぎます。

D. アーカイブの保存期間が長すぎます。

Answer: B ([メッセージを残す](#))

* FortiAnalyzerのデータポリシーとディスク使用率について理解する：

* FortiAnalyzerは、データポリシーを使用してログの保存、保持、およびディスク使用量を管理します。

* データポリシーのセクションでは、分析およびアーカイブ目的でログがどのくらいの期間保持されるかを示します。

* 「ディスク使用率」セクションでは、割り当てられたディスク容量、分析およびアーカイブに使用される割合、ならびにディスク使用状況に基づいてアラートをトリガーするタイミングを指定します。

* 提供された証拠資料の分析：

* 分析用ログの保持期間 :60日間

* アーカイブ用ログの保持期間 :120日間

* ディスク割り当て :300 GB（最大441 GBまで利用可能）

* 分析 :アーカイブ比率 :30% :70%

* 使用率が90%に達したらアラートと削除を実行する

* 潜在的な問題点の特定：

* ディスク容量の割り当て: 割り当てられているディスク容量は、可能な 441 GB のうち 300 GB です。ログの量が多い場合は不足しないかもしれませんが、与えられたデータに基づくと、これが主な懸念事項ではありません。

* 分析とアーカイブの比率：分析に30%、アーカイブに70%という比率は異例です。

通常、リアルタイムまたは最新のデータ分析が優先されるため、分析用に割り当てられる割合は高くなります。一般的な構成としては、分析用70%、アーカイブ用30%といった比率が挙げられます。この比率が適切でないと、分析用の容量が不足し、リアルタイムの監視や分析に問題が生じる可能性があります。

* 保持期間: 保持期間が長いように見えるかもしれませんが、具体的なログ量やコンプライアンス要件がわからない限り、必ずしも問題を示すものではありません。

これらの期間の長さは、組織のニーズや法的要件によって異なる場合があります。

* 結論：

分析の結果、主な問題点として、分析データとアーカイブデータの比率が正しく設定されていないことが挙げられます。この設定ミスは、FortiAnalyzerのリアルタイムログ分析の有効性に重大な影響を与え、脅威の検出と対応の遅延につながる可能性があります。

参考文献：

FortinetのFortiAnalyzerデータポリシーとディスク管理に関するドキュメント。

FortiAnalyzerのログ管理とディスク使用率に関するベストプラクティス。

最新問題: **16**

展示資料を参照してください。

Threat Hunting Monitor



Threat Action (3)	2023-09-07 19:55:58 - 2023-09-07 20:55:57					
Threat Pattern (216)	#	Application Service	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
Threat Name (54)	1		251,400(68%)			
Threat Type (8)	2	DNS	109,486(30%)	9.1 MB	169.0 B	28.5 KB
File Hash (3)	3	HTTP	4,521(1%)	3.6 MB	1.2 KB	27.8 KB
File Name (8)	4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB	554.9 MB
Application Process (0)	5	SSL	249(< 1%)			
Application Name (32)	6	other	76(< 1%)	10.2 KB	138.0 B	500.0 B
Application Service (21)	7	udp/443	58(< 1%)	1019.8 KB	17.6 KB	17.6 KB
	8	NNTP	57(< 1%)			

Threat Hunting Monitor

#	↓Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

脅威ハンティングモジュールを使用してデータを分析した結果、どのような結論が得られますか？

- A. スピアフィッシングは、機密情報を引き出すために使用されています。
- B. DNSトンネリングを使用して、ローカルネットワークから機密データを抽出しています。
- C. 偵察活動を用いて、メールサーバーから被害者の身元情報を収集しています。
- D. FTPは、データマイニングのためのコマンド&コントロール (C&C) 技術として使用されています。

Answer: (解答を表示する)

* 脅威ハンティングデータの理解:

* 提供された資料にある脅威ハンティングモニターには、さまざまなアプリケーションサービス、その使用回数、および送信バイト数、平均送信バイト数、最大送信バイト数などのデータメトリックが表示されます。

* 展示の2番目の部分には、特定の送信元IPアドレス (10.0.1.10) から宛先IPアドレス (8.8.8.8) への接続試行がリストされており、「接続失敗」メッセージが繰り返し表示されています。

* アプリケーションサービスの分析:

* DNSは、非常に高い件数 (251,400) と注目すべき送信バイト数 (9.1 MB) を誇る、トップのアプリケーションサービスです。

* この大量の DNS トラフィックは、通常の DNS クエリとしては異例であり、DNS トンネリングの存在を示している可能性があります。

* DNSトンネリング:

* DNSトンネリングとは、攻撃者がDNSクエリとレスポンスにデータをエンコードすることでセキュリティ制御を回避するために用いる手法です。これにより、攻撃者は検出されることなくローカルネットワークからデータを抽出できます。

* 大量のDNSトラフィックと詳細なメトリクスから、DNSトンネリングが使用されている可能性が示唆される。

* 8.8.8.8への接続失敗:

* 送信元IPアドレス(10.0.1.10)から宛先IPアドレス(8.8.8.8)への接続試行が繰り返され、接続に失敗している場合は、外部サーバーとの通信を試みている可能性があります。

* Google DNS (8.8.8.8) は、その信頼性とグローバルな普及率から、DNS トンネリングによく使用されます。

* 結論:

* 大量のDNSトラフィックと接続試行の性質を考慮すると、DNSトンネリングがローカルネットワークから機密データを抽出するために使用されていると結論付けるのは妥当である。

* 他の選択肢が実現しにくい理由:

* スピアフィッシング A) : 提供されたデータには、電子メールログやフィッシング指標など、スピアフィッシングの試みを示す証拠はありません。

* 偵察 C) データには、メールサーバーのスキャンやプロービングなどの典型的な偵察活動は示されていません。

* FTP C&C (D): 提供されたデータには、FTP トラフィックやFTP を使用したコマンドおよび制御通信の証拠はありません。

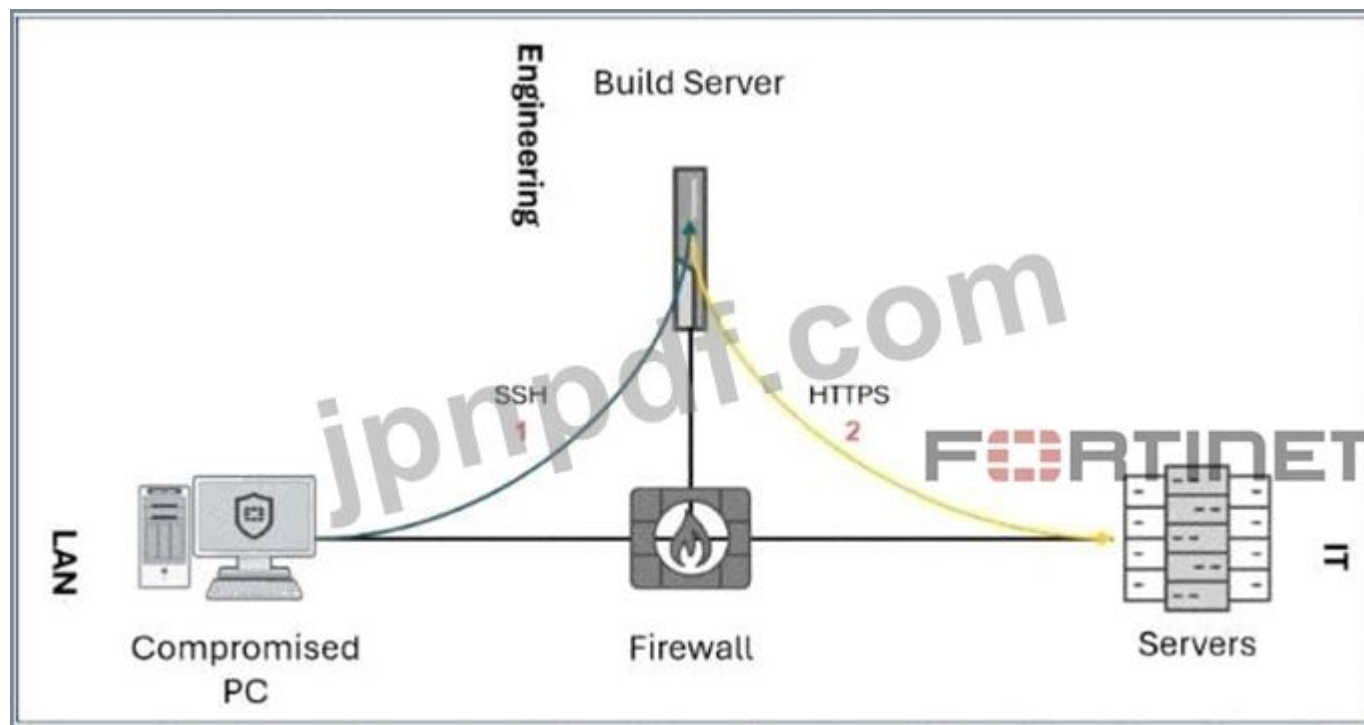
SANS Institute: "DNS トンネリング: DNS クエリによるデータ漏洩とトンネリングの検出方法" SANS DNS トンネリング OWASP: "DNS トンネリング" OWASP DNS トンネリング 提供された脅威ハンティングデータを分析すると、DNS トンネリングがデータ漏洩に使用されていることが明らかになり、ネットワークから機密情報を抽出する高度な方法が示されています。

有効な **NSE7_SOC_AR-7.6** 問題集は GoShiken.com が提供された合格しやすい NSE7_SOC_AR-7.6 試験問題集! GoShiken.com が最新の **NSE7_SOC_AR-7.6** 試験問題集を提供しています。GoShiken.com NSE7_SOC_AR-7.6 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE7_SOC_AR-7.6 問題集をゲットする人はこちら:

https://www.goshiken.com/Fortinet/NSE7_SOC_AR-7.6-mondaishu.html (9330%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 17

展示資料を参照してください。



侵害されたPCがエンジニアリングビルドサーバーへのSSH接続を確立し、そのサーバーがHTTPSトラフィックを中継して、本来LANからのアクセスをブロックするはずのサーバーに到達させる。この攻撃にはどの手法が用いられているか？

- A. ポートノッキング
- B. C2 チャネルを介した漏洩
- C. 中間者攻撃 (MITM)
- D. プロトコルトンネリング

Answer: D (メッセージを残す)

正確な抜粋：次に、SSH トンネリングを使用して、LAN デバイスが SOC ネットワーク内の一部のデバイスにアクセスできないようにするファイアウォール ルールを回避します。重要なネットワーク インフラストラクチャにアクセスできるようになります。」正解は D. プロトコルトンネリングです。図では、侵害された PC が SSH を使用して許可された中間システム (エンジニアリング ビルド サーバー) に接続し、そのパスを使用して、LAN ホストが通常直接アクセスできない内部サーバーに HTTPS トラフィックを中継している様子が示されています。これがトンネリングです。1 つのプロトコルまたはトラフィック フローが、別の許可されたチャネルを介してカプセル化または中継され、セグメンテーションまたはファイアウォール ポリシーを回避します。

Aは誤りです。ポートノッキングは、一連の接続試行によってポートを開くステルスアクセス制御メカニズムです。Bは誤りです。展示内容は内部サーバーへのアクセスに関するものであり、確立されたC2チャネルを介したデータの窃盗に関するものではありません。Cは誤りです。2つの被害者間のトラフィックの傍受や操作は行われておらず、ビルドサーバーがピボット/トンネルとして使用されています。

技術的な詳細分析: MITRE の用語では、この動作はトンネリング/プロキシスタイルの防御回避と横方向移動のサポートに該当します。実際の運用では、攻撃者は SSH ローカル転送、リモート転送、または動的 SOCKS プロキシを使用する可能性があります。たとえば、ssh -L 8443:internal-server:443 user@build-server または ssh -D 1080 user@build-server などです。Fortinet SOC の観点からは、FortiSIEM はワークステーションからビルドサーバーへの異常な SSH セッション、それに続くビルドサーバーから保護されたサーバーゾーンへの予期しない HTTPS 接続をフラグ付けする必要があります。FortiGate NP/CP オフロードは許可されたセッションを高速化する可能性があります、検出価値は ASIC の動作ではなく、ログの相関とセグメンテーション ポリシー違反から得られます。

最新問題: 18

FortiAnalyzerでインシデントを作成する方法は2つあります。どれを選択してください。2つ選択してください。)

- A. コネクタアクションを使用する
- B. イベントモニターページで手動で操作します。

C. プレイブックを実行する

D. カスタムイベントハンドラの使用

Answer: B,D ([メッセージを残す](#))

* FortiAnalyzerにおけるインシデント作成の理解：

* FortiAnalyzerでは、セキュリティイベントを追跡および管理するためのインシデントを作成できます。

* インシデントは、検出されたイベントと事前定義されたルールに基づいて、自動的に手動でも作成できます。

* 分析手法：

* オプション A: コネクタ アクションを使用すると、通常は他のシステムやサービスとの統合が必要となり、FortiAnalyzer 上でインシデントを直接作成する方法ではありません。

* オプション B: イベント モニター ページで関連するイベントを選択し、それらのイベントからインシデントを作成することで、インシデントを手動で作成できます。

* オプション C: プレイブックは応答やアクションを自動化できますが、インシデントの直接作成は通常、イベント ハンドラーまたは手動プロセスによって管理されます。

* オプション D: カスタムイベントハンドラーを設定することで、特定のイベントや条件に基づいてインシデントの作成をトリガーし、FortiAnalyzer 内でのプロセスを自動化できます。

* 結論：

* FortiAnalyzerでインシデントを作成する有効な方法は、イベントモニターページで手動で作成する方法と、カスタムイベントハンドラーを使用する方法の2つです。

参考文献：

FortiAnalyzerにおけるインシデント管理に関するFortinetのドキュメント。

FortiAnalyzerのイベント処理とカスタマイズに関するガイド。

最新問題: 19

ネットワークを監視中に、1台のFortiGateデバイスが、トポロジ内の他のすべてのFortiGateデバイスよりも著しく多くのログをFortiAnalyzerに送信していることが判明しました。

さらに、FortiGateデバイスが登録されているADOMは、常に割り当て量を超過しています。

考えられる解決策を2つ挙げてください。(2つ選択してください。)

A. 最初のFortiGateデバイスのストレージ容量を増やします。

B. 最初の FortiGate デバイス用に別の ADOM を作成し、異なるストレージ ポリシーを設定します。

C. 最初の FortiGate デバイスを再設定して、FortiAnalyzer に転送されるログの数を減らします。

D. 最初のFortiGateデバイスから送信されるデータをフィルタリングするために、データセレクトアを設定します。

Answer: B,C ([メッセージを残す](#))

* 問題の理解：

* FortiGateデバイスのうち1台が、他のデバイスと比較して著しく大量のログを生成しており、ADOMのストレージ容量を超過しています。

* これにより、FortiAnalyzer内でのパフォーマンスの問題やログの効率的な管理の困難が生じる可能性があります。

* 考えられる解決策：

* 目標は、ログの量を管理し、ADOM が割り当て量を超えないようにしつつ、効果的なログ分析と監視を維持することです。

* 解決策 A: 最初の FortiGate デバイスのストレージ容量クォータを増やす：

ストレージ容量の割り当てを増やすことで一時的な緩和は得られるかもしれませんが、問題の根本原因である過剰なログ容量の解決にはなりません。

* 丸太の量は今後も増加し続ける可能性があるため、この解決策は長期的には持続可能ではないかもしれません。

長期的に見て効率的な解決策とはならないため、選定されませんでした。

* 解決策 B: 最初の FortiGate デバイス用に別の ADOM を作成し、別のストレージ ポリシー セットを構成します。

* 個別の ADOM を作成することで、ログ量の多いデバイスに特化したストレージ ポリシーと管理をカスタマイズできます。

* これにより、ストレージ負荷を分散し、より厳格な、またはカスタマイズされた保持およびストレージポリシーを適用するのに役立ちます。

* ログの保存と整理を効果的に管理できるため選定しました。

- * 解決策 C: 最初の FortiGate デバイスを再設定して、FortiAnalyzer に転送するログの数を減らす:
- * FortiGate デバイスのログ設定を調整することで、FortiAnalyzer に転送されるログの量を減らすことができます。
- * これには、不要なログ記録の無効化、ログレベルの引き下げ、重要度の低いログのフィルタリングなどが含まれます。
- * ログ容量過多の問題に直接対処できるため、選定しました。
- * 解決策 D: 最初の FortiGate デバイスから送信されるデータをフィルタリングするようにデータセクターを設定します。
- * データセクタを使用すると、FortiAnalyzer に送信されるログをフィルタリングして、関連するログのみが転送されるようにすることができます。
- * これはログの量を減らすのに役立ちますが、重要なログを見落とさないようにするためには、詳細な設定と定期的な更新が必要になる場合があります。
- * FortiGate デバイス上でログ設定を直接再構成するほど効果的ではない可能性があるため、選択しませんでした。
- * 実装手順:
- * 解決策Bの場合:
- * ステップ 1: FortiAnalyzer にアクセスし、ADOM 管理セクションに移動します。
- * ステップ 2: ログ量の多い FortiGate デバイス用に新しい ADOM を作成します。
- * ステップ 3: FortiGate デバイスをこの新しい ADOM に登録します。
- * ステップ 4: 新しい ADOM に対して、ログの保持と保存を管理するための特定のストレージ ポリシーを設定します。
- * 解決策Cの場合:
- * ステップ 1: FortiGate デバイスの設定インターフェースにアクセスします。
- * ステップ 2 :ログ設定に移動します。
- * ステップ 3: ログレベルを調整し、不要なログを無効にします。
- * ステップ 4: 設定を保存し、FortiAnalyzer に送信されるログ ボリュームを監視します。
- :

FortiAnalyzer ADOMとログ管理に関するFortinetドキュメント FortiAnalyzer管理ガイド FortiGateでのログ設定の構成に関するFortinetナレッジベース FortiGateロギングガイド ログ量の多いFortiGateデバイス用に個別のADOMを作成し、そのロギング設定を再構成することで、ログ量を効果的に管理し、ADOMがクォータを超えないようにすることができます。

最新問題: 20

展示資料を参照してください。

脅威ハンティングモジュールを使用してデータを分析した結果、どのような結論が得られますか？

- A. スピアフィッシングは、機密情報を引き出すために使用されています。
- B. DNS トンネリングを使用して、ローカルネットワークから機密データを抽出しています。
- C. 偵察活動を用いて、メールサーバーから被害者の身元情報を収集しています。
- D. FTPは、データマイニングのためのコマンド&コントロール (C&C) 技術として使用されています。

Answer: (解答を表示する)

- * 脅威ハンティングデータの理解:
- * 提供された資料にある脅威ハンティングモニターには、さまざまなアプリケーションサービス、その使用回数、および送信バイト数、平均送信バイト数、最大送信バイト数などのデータメトリックが表示されます。
- * 展示の2番目の部分には、特定の送信元IPアドレス (10.0.1.10) から宛先IPアドレス (8.8.8.8) への接続試行がリストされており、接続失敗」メッセージが繰り返し表示されています。
- * アプリケーションサービスの分析:
- * DNSは、非常に高い件数 (251,400) と注目すべき送信バイト数 (9.1 MB) を誇る、トップのアプリケーションサービスです。
- * この大量の DNS トラフィックは、通常の DNS クエリとしては異例であり、DNS トンネリングの存在を示している可能性があります。
- * DNS トンネリング:

- * DNSトンネリングとは、攻撃者がDNSクエリとレスポンスにデータをエンコードすることでセキュリティ制御を回避するために用いる手法です。これにより、攻撃者は検出されることなくローカルネットワークからデータを抽出できます。
 - * 大量のDNSトラフィックと詳細なメトリクスから、DNSトンネリングが使用されている可能性が示唆される。
 - * 8.8.8.8への接続失敗:
 - * 送信元IPアドレス(10.0.1.10)から宛先IPアドレス(8.8.8.8)への接続試行が繰り返され、接続に失敗している場合は、外部サーバーとの通信を試みている可能性があります。
 - * Google DNS (8.8.8.8) は、その信頼性とグローバルな普及率から、DNS トンネリングによく使用されます。
 - * 結論 :
 - * 大量のDNSトラフィックと接続試行の性質を考慮すると、DNSトンネリングがローカルネットワークから機密データを抽出するために使用されていると結論付けるのは妥当である。
 - * 他の選択肢が実現しにくい理由 :
 - * スピアフィッシング A) : 提供されたデータには、電子メールログやフィッシング指標など、スピアフィッシングの試みを示す証拠はありません。
 - * 偵察 C) データには、メールサーバーのスキャンやプロービングなどの典型的な偵察活動は示されていません。
 - * FTP C&C (D): 提供されたデータには、FTP トラフィックやFTP を使用したコマンドおよび制御通信の証拠はありません。
- SANS Institute: "DNS トンネリング: DNS クエリによるデータ漏洩とトンネリングの検出方法" SANS DNS トンネリング OWASP: "DNS トンネリング" OWASP DNS トンネリング 提供された脅威ハンティングデータを分析すると、DNS トンネリングがデータ漏洩に使用されていることが明らかになり、ネットワークから機密情報を抽出する高度な方法が示されています。

最新問題: 21

FortiSOARのデフォルトのデータ取り込みウィザードを使用して、FortiSIEMからFortiSOARへのインシデント処理ワークフローを正しい順序で配置します。左側の列で各ワークフローコンポーネントを選択し、ドラッグして右側の列の空白位置に移動します。4つの正しいワークフローコンポーネントを正しい順序で配置し、最初のステップを列の一番上の最初の位置に配置します。

FortiSIEM event log

FortiSOAR event log

FortiSIEM incident

FortiSOAR incident

FortiSIEM alert

FortiSOAR alert

FortiSIEM indicator

FortiSOAR indicator

Incident handling workflow

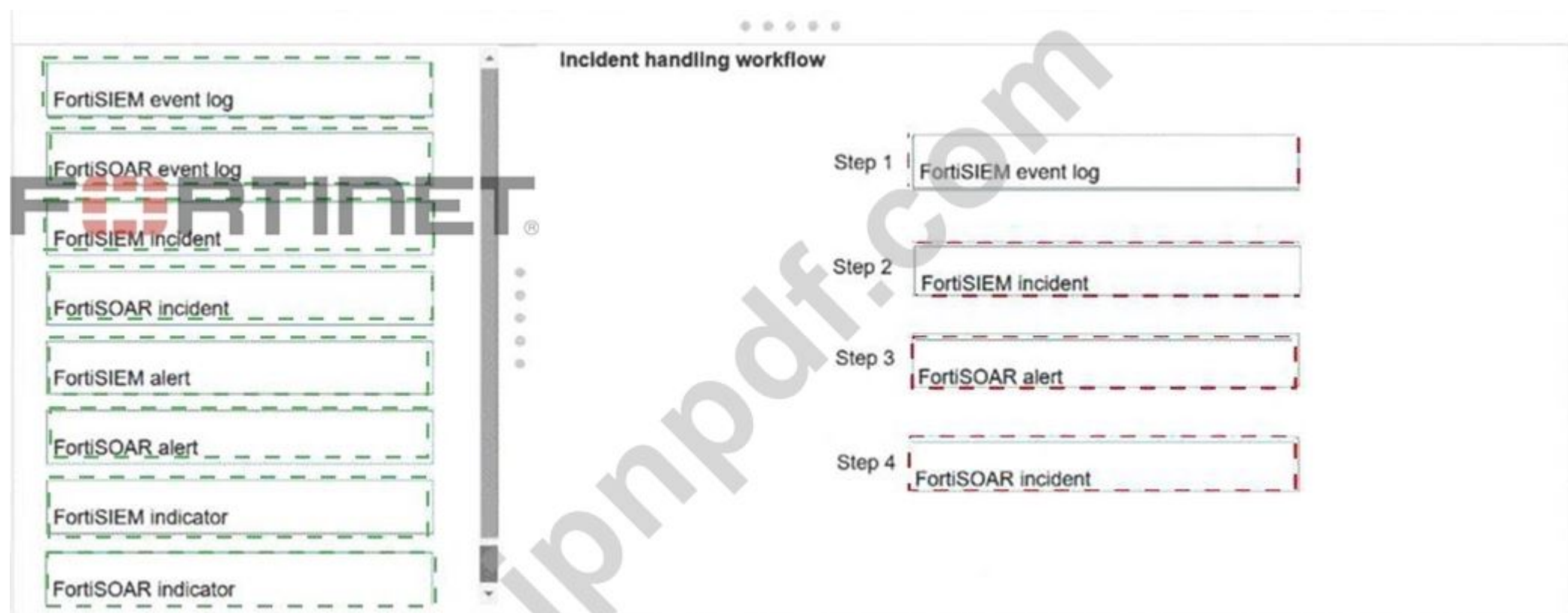
Step 1

Step 2

Step 3

Step 4

Answer:



Explanation:

ステップ1 :FortiSIEMイベントログ

ステップ2 :FortiSIEMインシデント

ステップ3 :FortiSOARアラート

ステップ4 :FortiSOARインシデント

正確な抜粋: FortiSIEM: イベント: イベントとは、監視対象デバイスから収集された単一のログまたはデータ ポイントを指します。これは、ファイアウォール ログやシステム アラートなど、FortiSIEM が受信する情報の最も基本的な単位です。」ガイドには、次の記述もあります。インシデント: FortiSIEM のインシデントは、関連ルールがトリガーされたときに作成されます。」正確な抜粋: このスライドでは、取り込みプロセス中に FortiSIEM インシデントと FortiSOAR アラートの間でフィールドをマッピングする方法について説明します。ウィザードを使用して、FortiSIEM データが FortiSOAR アラート フィールドにどのように入力されるかを定義します。」正確な抜粋: FortiSOAR は FortiSIEM インシデントをアラートとして取り込みます... アラートが有効な脅威でない場合は、アナリストはそれを誤検知として閉じることができます。そうでない場合は、アナリストはインシデントを開くことができます。」正しい順序は、FortiSIEM イベント ログ # FortiSIEM インシデント # FortiSOAR アラート # FortiSOAR インシデントです。FortiSIEM は、まず監視対象デバイスから生のイベント ログを受信します。これらのイベントが関連ルールに一致する場合、FortiSIEM は FortiSIEM インシデントを作成します。その後、FortiSOAR のデフォルトのデータ取り込みウィザードは、FortiSIEM インシデントを FortiSOAR インシデントとして直接ではなく、アラートとして FortiSOAR に取り込みます。トリアージと検証の後、アナリストまたはプレイブックはアラートを FortiSOAR インシデントにエスカレーションできます。

技術的な詳細解説 :FortiSIEMとFortiSOARは異なるオブジェクトモデルを使用します。FortiSIEMの「インシデント」とは、イベント分析による関連結果を意味します。FortiSOARの「アラート」は、そのSIEMインシデントから作成された最初のSOAR側のレコードです。FortiSOARの「インシデント」は、検証後に使用される上位レベルのケース管理コンテナです。この分離は意図的なものです。すべてのSIEMインシデントが完全なインシデント対応処理を必要とするわけではありません。このワークフローはログの取り込みとケースのオーケストレーションであり、ファイアウォールのパケットアクセラレーションではないため、FortiGate NP/CPのオフロードは関係ありません。

最新問題: 22

インシデントレポートを確認してください。

攻撃者は、公開されたプレスリリースから従業員の氏名、役職、メールの送信パターンを特定し、それらを利用して個別のメールを作成した。

これらのメールは、受信者に対し、企業ドメイン外のリンクを使用して添付された議題を確認するよう指示するものであった。
このレポートに最も適したMITRE ATT&CKの戦術はどれですか？ 2つ選択してください)

- A. 認識
- B. 発見
- C. 初期アクセス
- D. 防御回避

Answer: A,C (メッセージを残す)

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明：

FortiSIEM 7.3 インシデント相関にMITRE ATT&CKマッピングを使用)およびFortiSOAR 7.6 インシデント分類とプレイブックのトリガーにこれらの戦術を使用)の公式ドキュメントに基づく
くと、以下のようになります。

* 偵察 (戦術TA0043) この戦術は、攻撃者が標的設定を支援するために使用できる情報を能動的または受動的に収集する手法で構成されています。このシナリオでは、攻撃者は 公開された
プレスリリースから従業員の名前、役割、および電子メールのパターン」を特定します。これは、 被害者組織情報の収集 (1591)」および 公開技術データベースの検索 (1596)」に分類されま
す。この活動は侵害前に発生し、情報収集を伴うため、厳密には偵察です。

* 初期アクセス (戦術TA0001) この戦術は、さまざまな侵入経路を使用してネットワーク内で最初の足がかりを得る手法を対象としています。受信者にリンクを使用して添付された議題を
確認するよう指示するカスタマイズされた電子メールを送信する」行為は、フィッシングの定義です :スパイフィッシングリンク (1566.002)。これは、最初の侵入を得るために使用される具
体的な配信メカニズムです。

他の選択肢が間違っている理由：

* 発見 B) この戦術は、攻撃者が既にアクセス権を取得した後、内部ネットワークに関する情報を得るために使用する技術を含みます。攻撃者は公開されているプレスリリースを閲覧してい
るため、ネットワーク境界の外で活動しています。

* 防御回避 D) この戦術は、攻撃者が侵入全体を通して検出を回避するために使用する技術で構成されています。外部リンクを使用することで基本的な評判フィルターの一部を回避できる
可能性がありますが、レポートで説明されている主な目的は、接触とアクセスを確立することであり、これは初期アクセス戦術の中核です。

最新問題: 23

展示資料を参照してください。

Playbook

☐	Job ID ⇅	Playbook ⇅	Trigger ⇅	Start Time ⇅	End Time ⇅	Status ⇅
☐	2024-03-27 11:54:16.858411-07	Malicious File Detect	event[202403271000	2024-03-27 11:54:17-0700	2024-03-27 11:54:20-0700	failed(Scheduled:0/Running:0/Succe

Playbook Tasks

Playbook Tasks

Refresh

View Raw Log

Search...

☐	Task ID ↕	Task ↕	Start Time ↕	End Time ↕	Status ↕	
☐	placeholder_8fab0102_0955_447f_872d_2208c	Attach Data To Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	upstream_failed	
☐	placeholder_3db75c0a_1765_4479_81f8_2e1e8	Create Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	failed	
☐	placeholder_fa2a573c_ba4f_4565_baf0_4255bb	Get Events	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	success	

Raw Logs

```
[2024-03-27T11:54:19.817-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 216, in execute
    self.epid = FAZUtilsOperator.parse_input(context, self.epid, context_dict)
  File "/drive0/private/airflow/plugins/faz_utils_operator.py", line 118, in parse_input
```

悪意のあるファイル検出プレイブックは、イベントハンドラーが悪意のあるファイル検出イベントを生成したときにインシデントを作成するように構成されています。

悪意のあるファイル検出プレイブックの実行が失敗した理由は？

- A. インシデント作成タスクは入力として名前または番号を想定していましたが、誤ったデータ形式を受け取りました
- B. イベント取得タスクはイベントデータを取得できませんでした。
- C. Attach_Data_To_Incident インシデントタスクは整数を期待していましたが、不正なデータ形式を受け取りました。
- D. インシデントへのデータ添付タスクが失敗したため、プレイブックの実行が停止しました。

Answer: A ([メッセージを残す](#))

* プレイブック構成の理解 :

* 「悪意のあるファイル検出」プレイブックは、悪意のあるファイル検出イベントがトリガーされたときにインシデントを作成するように設計されています。

* プレイブックには、Attach_Data_To_Incident、Create Incident、Get Eventsなどのタスクが含まれています。

* プレイブック実行の分析 :

* この表示は、インシデント作成タスクが失敗し、インシデントへのデータ添付タスクも失敗したことを示しています。

* イベント取得タスクが成功しました。これは、イベントデータを取得できたことを示しています。

* 生ログの確認:

* 生ログには、incident_operator.py ファイル内の入力の解析に関連するエラーが示されています。

* エラーのトレースバックによると、タスクは特定の入力形式 おそらく名前または数値)を想定していましたが、誤ったデータ形式を受け取りました。

* 障害の原因特定 :

* インシデント作成タスクの失敗が根本原因です。入力形式が正しくなかったため、タスクが正しく処理されませんでした。

* その後、Attach_Data_To_Incident タスクは、インシデントが正常に作成されることを前提としているため、失敗しました。

* 結論 :

* プレイブックの実行が失敗した主な理由は、インシデント作成タスクが想定されていた名前や番号ではなく、誤ったデータ形式を受け取ったためです。

参考文献 :

Fortinetのプレイブックおよびタスク構成に関するドキュメント。

プレイブック実行におけるエラー処理とデバッグの実践方法。

最新問題: 24

脅威ハンティング活動に該当するのは次のうちどれですか？ 3つ選択してください)

A. 脅威インテリジェンスで記録を充実させる。

B. ワークフローを自動化する。

C. 仮説を立てる。

D. パケット解析を実行します。

E. 相関ルールを調整します。

Answer: A,C,D ([メッセージを残す](#))

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明 :

FortiSOAR 7.6 の特殊な脅威ハンティングモジュールとフレームワーク、および FortiSIEM 7.3 の高度な分析機能によると、脅威ハンティングとは、自動化されたセキュリティ制御を回避した脅威を、人間が主体となって積極的に探索することと定義されています。選択された 3 つのアクティビティは、このライフサイクルのコアコンポーネントです。

* 仮説の生成 (C): これは 「構造化ハント」の基本的な出発点です。アナリストは、最新の脅威インテリジェンス (FortiGuard によって特定された新しい TTP など) または環境リスクに基づいて、攻撃者がネットワーク内で検出されずにどのように活動しているかについての検証可能な理論を開発します。

* 脅威インテリジェンスでレコードを充実させる A) : 調査エーズでは、ハンターはFortiSOARの脅威インテリジェンス管理 (TIM) モジュールを使用して、技術データ (IPアドレス、ハッシュ値、URL) に外部コンテキストを追加します。これにより、ハント中に発見された異常が実際に悪意のあるものなのか、既知のキャンペーンの一部なのかを判断するのに役立ちます。

* パケット分析の実行 (D): 高度な脅威はログファイル間の 「ギャップ」に潜んでいることが多いため、ハンターはFortiSIEMのクエリツールまたは統合されたNDR (ネットワーク検出および応答) データを使用して、ディープパケット分析またはネットワークフロー分析を頻繁に実行し、標準的なアラートでは見逃される可能性のある疑わしい横方向の移動またはC2 (コマンドおよび制御) 通信パターンを特定します。

他の選択肢が除外される理由 :

* ワークフローの自動化 (B): SOAR は自動化のために設計されていますが、 自動化」という行為は DevOps または SOC エンジニアリングのタスクです。脅威ハンティング自体はプロアクティブな調査です。プレイブックはハンターを支援できますが (たとえば、データ収集を自動化することによって)、ハンティング行為は手動または半自動化された認知プロセスのままです。

* 相関ルールの調整 E) ルールの調整は、リアクティブメンテナンス作業、つまり 脅威ハンティング後」の活動です。脅威ハンターが新しい攻撃パターンを発見したら、SIEMの相関ルールを調整して、将来的にその特定の脅威が自動的に検出されるようにします。調整はハンティングの結果であり、ハンティング活動そのものではありません。

最新問題: 25

FortiAnalyzerでプレイブックをエクスポートする際に従うべきベストプラクティスはどれですか？ 2つ選択してください)

- A. エクスポートする前にプレイブックを無効にします。
- B. 関連するコネクタ設定を含めます。
- C. プレイブックをエクスポートして再インポートするのではなく、ADOM間でプレイブックを移動します。
- D. エクスポートされたプレイブックの名前がターゲット ADOM に存在しないことを確認します。

Answer: (解答を表示する)

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明：

FortiAnalyzer 7.4 SOC Analystの公式トレーニング資料 レッスン5：自動化およびFortiSOAR 7.6とFortiSIEM 7.3の統合に関するサポートドキュメントによると、プレイブックの移植性に関して、以下のベストプラクティスが推奨されています。

- * エクスポート前にプレイブックを無効にする (A): プレイブックをエクスポートすると、その現在の状態 (有効または無効) がエクスポートファイルに保持されます。有効になっているプレイブックが、トリガー条件がすぐに満たされる宛先 ADOM にインポートされると、自動的に実行が開始されます。エクスポート前にプレイブックを無効にすることは、アナリストがローカル構成を確認する前に、新しい環境で意図しない自動アクションが発生するのを防ぐための重要なベストプラクティスです。
- * 関連するコネクタ設定を含める B) FortiAnalyzerでは、エクスポート処理中に必要なコネクタ構成を含めることができます。このオプションを選択すると、エクスポートされたファイルには、プレイブックがタスクを実行するために使用するコネクタに必要なメタデータと構成が含まれます。これにより、すべてのコネクタを手動で再作成する必要なく、プレイブックがさまざまなFortiAnalyzerユニットまたはADOM間で機能し、移植性を維持できます。

他の選択肢が間違っている理由：

- * ADOM間でプレイブックを移動する C) デバイスを移動するのと同じ意味で、ADOM間で自動化プレイブックを移動するネイティブな 移動」機能はありません。自動化ロジックを転送するための標準でサポートされているワークフローは、エクスポートおよびインポートプロセスです。
- * ターゲットに名前が存在しないことを確認します (D):一意の名前を維持することは良い習慣ですが、FortiAnalyzer が名前の競合を自動的に処理するため、エクスポート プロセス自体では必須の ベスト プラクティス」ではありません。インポートされたプレイブックが既存のプレイブックと同じ名前である場合、システムは競合を回避するために新しいプレイブックの名前にタイムスタンプを自動的に追加します。

最新問題: 26

FortiAIを使用してプレイブックを設計したい場合、FortiSOARで必要な設定はどれですか？2つ選択してください。

- A. FortiSOAR機械学習エンジンをトレーニングします。
- B. OpenAIコネクタをインストールして設定します。
- C. PlaybookユーザーにCRUD権限を付与します。
- D. FortiAIソリューションパックをインストールし、構成ウィザードを実行します。

Answer: (解答を表示する)

抜粋：FortiSIEMおよびFortiSOAR上のFortiAI統合は、OpenAIのLLMに直接接続します...FortiAIを使用すると、独自のOpenAIライセンスキーを使用して、独自のOpenAIアカウントに接続できます。」このガイドでは、Content Hub > FortiAI Connectorの下にFortiSOARの設定方法も示されています。

正確な抜粋：FortiSOAR RBAC に基づいて、承認されたユーザーのみが FortiAI アシスタントを呼び出し、関連モジュールに対して CRUD 操作を実行できます。」正解は C と D です。プレイブックの設計に FortiAI を使用するには、FortiSOAR に FortiAI コンテンツがインストールされ、LLM サービスと通信できるように構成されている必要があります。さらに、FortiAI を呼び出

ユーザーは、関連するプレイブック モジュールに対する CRUD 権限を含む、適切な RBAC 権限を持っている必要があります。FortiAI は FortiSOAR の機械学習エンジンではないため、A は誤りです。B は、FortiSOAR 側の構成はローカル モデルのトレーニングではなく、FortiAI/FortiAI コネクタ コンテンツを介して処理されるため、誤解を招きます。技術的な詳細 :FortiAIはプレイブックのワークフローロジックを生成できますが、人間の検証の必要性を排除するものではありません。生成されたプレイブックでも、変数マッピング、コネクタ認証情報の検証、権限チェック、実行ログによるテストが必要になる場合があります。FortiGate NP/CPのオフロードは、ファイアウォールのデータプレーン処理ではなく、FortiSOARの自動化設計に関するものであるため、関係ありません。

最新問題: 27

ユーザー入力を変数として保存するために手動トリガーを使用する場合、その変数を参照するための正しいJinja式はどれですか？（回答を1つ選択してください）

- A. {{ vars.input.params.<variable_name> }}
- B. {{ globalVars.<variable_name> }}
- C. {{ vars.item.<variable_name> }}
- D. {{ vars.steps.<variable_name> }}

Answer: A (メッセージを残す)

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明：

FortiSOAR 7.6では、プレイブックエンジンはJinja2式を使用して動的データを処理します。プレイブックが手動トリガーで構成されている場合、管理者は、レコードからプレイブックを実行する際にアナリストが入力する必要のある入力フィールド (テキスト、選択リスト、チェックボックスなど)を定義できます。

* 入力パラメータのマッピング: この手動トリガーフェーズ中にユーザーが入力したデータはすべて、vars オブジェクト内の input.params ディクショナリに自動的にマッピングされます。したがって、特定の入力値を取得するための構文は {{ vars.input.params.variable_name }} です。

* 変数のスコープ:この特定のパスにより、変数が後続のステップの出力 (vars.steps) やグローバルに定義された変数 (globalVars) からではなく、最初のユーザー入力から取得されることが保証されます。

最新問題: 28

作戦室を作成し、ドメインの評判を調べるためのコネクタアクションを実行したいと考えています。

次に、チームがレビューできるように出力結果を保存する必要があります。しかし、出力結果が大量にあるため、作戦室に添付する情報量を制限したいと考えています。どうすればこれを実現できますか？

回答を1つ選択してください。

- A. 返された出力から、必要な出力キーのみを選択します。
- B. ワークスペースフィルターを適用して、関連するフィールドのみを表示します。
- C. [調査] タブを使用して、必要なフィールドのみをマッピングします。
- D. コネクタを実行する前に、プレイブックのログレベルを下げてください。

Answer: A (メッセージを残す)

正確な抜粋: ウォールーム レコードでコネクタ アクションを直接実行することで、ウォールームを調査できます。このスライドに示されている例では、このレコードで VirusTotal コネクタを使用してドメイン レピュテーションの取得アクションが直接実行されています。関連するチェックボックスのみを選択するか、[キー] を選択してすべての出力を選択できます。」正解は A です。ウォールームからコネクタ アクションを直接実行すると、FortiSOAR では返された出力キーのうち保存するものを選択できます。これが、ウォールームに添付されるものを制限する正しい方法です。B は、ワークスペース フィルタが表示/コラボレーションに影響し、保存されるコネクタ出力には影響しないため誤りです。C は不完全です。調査を実行するのは [調査] タブですが、具体的な制御は出力キーの選択です。D は、プレイブックのログ レベルではウォールームの証拠添付ファイルのサイズは制御されないため誤りです。

技術的な詳細解説：作戦室は、重大インシデント対応時の集中的な連携を目的として設計されています。コネクタの出力をすべて記録に書き込むと、ノイズが発生し、レビューが遅くなります。評判スコア、カテゴリ、検出結果、レジストラ、解決済みIPアドレス、最終分析サマリーなど、アナリストにとって有用なキーのみを選択してください。これにより、チームに情報過多な情報を送り込むことなく、証拠の質を維持できます。

最新問題: 29

展示資料を参照してください。

CSLAB Active Reconnaissance

Actions

Subpattern: Port_Scanning_LANtoSOC

Displaying 1 - 100 of 100

Jun 11, 2025, 01:45:00 PM - Jun 12, 2025, 01:45:00 PM

Event Receive Time	Event Name	Reporting IP	Source IP	Destination IP	Destination TCP/UDP Port
Jun 12, 2025, 01:44:28 PM	FortiGate-traffic-end-forward-client-rst	10.200.200.254	16 10.200.3.219	10.200.200.12	22
Jun 12, 2025, 01:44:28 PM	FortiGate-traffic-end-forward-server-rst	10.200.200.254	16 10.200.3.219	10.200.200.238	110
Jun 12, 2025, 01:43:53 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.183	443
Jun 12, 2025, 01:43:53 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.214	443
Jun 12, 2025, 01:43:53 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.81	443
Jun 12, 2025, 01:43:52 PM	FortiGate-traffic-end-forward-timeout	10.200.200.254	16 10.200.3.219	10.200.200.180	443

Event Attributes

Search...

Lines: 7

Item	Value
Destination IP	10.200.200.12
Destination TCP/UDP Port	22
Event Name	FortiGate-traffic-end-forward-client-rst
Event Receive Time	Jun 12, 2025, 01:44:28 PM
Event Type	FortiGate-traffic-end-forward-client-rst
Reporting IP	10.200.200.254
Source IP	10.200.3.219

FortiSIEMインシデントのトリガーイベントページを確認しています。トポロジにファイアウォールが1つしかないため、「レポートIP」列を削除したいと考えています。どのようにすれば削除できますか？（回答を1つ選択してください）

- A. インシデントアクションを設定する際に、トリガー属性セクションからレポートIPフィールドをクリアしてください。
- B. ルールサブパターン内のレポートIPフィールドの相関関係を無効にします。
- C. 解析ルールを使用して、生ログからレポートIP属性を削除します。
- D. このインシデントの表示列をカスタマイズします。

Answer: A (メッセージを残す)

正確な抜粋: "アクション: 編集アイコンをクリックして、このルールで生成する必要のあるインシデント属性とトリガー属性を定義します。ルールを保存する前に、少なくとも1つのインシデントを定義する必要があります。" 正確な抜粋: "トリガー属性: このイベントのダッシュボードおよびインシデント インターフェイスに列として含めるトリガー イベントの属性を選択します。" 正解は A です。レポート IP 列は、ルールの [アクションの定義 / インシデント アクション] 設定の [トリガー属性] 構成によって制御されます。そこでレポート IP が選択されている場合、FortiSIEM はそれをインシデント関連の列として表示します。トポロジにはファイアウォールが1つしかないため、レポート IP の値は重複しており、分析上の価値はほとんどありません。そのため、トリガー属性リストからレポート IP をクリアして削除します。

オプションBは、相関/グループ化ロジックがルール条件またはサブパターンで設定され、列を非表示にするために使用されるものではないため、誤りです。オプションCは無謀で不適切です。レポートIPは正規化されたイベント属性であり、表示列を変更するためだけに生ログやパーサー出力から削除すべきではありません。オプションDは表示レベルのアイデアに過ぎず、インシデントに対してどのイベント属性を公開するかを定義するルール生成トリガー属性には対応していません。

技術的な詳細解説 :FortiSIEMは、ルール検出ロジックとインシデント表示メタデータを分離します。

サブパターンフィルタとアグリゲートによって、インシデントがトリガーされるかどうかが決まります。トリガー属性によって、アナリストがインシデント列として表示する一致するイベントフィールドが決まります。この場合、解析、イベント正規化、または相関関係は変更されません。インシデントアクションの出力のみを調整して、アナリストが送信元IP、宛先IP、宛先ポートなどの有用なフィールドに集中できるようにします。これはファイアウォールのパケット転送やASICオフロードの動作ではなく、FortiSIEMイベント表示ロジックであるため、FortiGate NP/CPアクセラレーションは関係ありません。

最新問題: 30

以下のインシデントレポートを確認してください。

攻撃者は、貴社の従業員を標的としたフィッシングメールキャンペーンを利用しました。

そのメールは、IT部門など信頼できる情報源を装い、ログイン認証情報を要求した可能性が高い。

何も知らない従業員がメール内の悪意のあるリンクをクリックした結果、リモートアクセス型トロイの木馬 (RAT)がダウンロードされ、実行されてしまった。

RATは攻撃者にリモートアクセス権限と、侵害されたシステムへの足がかりを提供した。

このインシデントレポートは、MITRE ATT&CKのどの2つの戦術を網羅していますか？ 2つ選択してください。)

A. 初期アクセス

B. 防御回避

C. 横方向の動き

D. 持続性

Answer: A,D (メッセージを残す)

* MITRE ATT&CK戦術の理解 :

* MITRE ATT&CKフレームワークは、攻撃者が目的を達成するために使用するさまざまな戦術と技術を分類します。

戦術とは攻撃の目的を表し、技術とはそれらの目的を達成する方法を表す。

* インシデントレポートの分析 :

* フィッシングメールキャンペーン :この戦術は、システムへの初期アクセス権を取得するためによく使用されます。

* 悪意のあるリンクと RAT のダウンロード:悪意のあるリンクをクリックして RAT をダウンロードすることは、初期アクセスを確立したことを示しています。

* リモートアクセス型トロイの木馬 (RAT): RAT はインストールされると、攻撃者が長期間アクセスを維持できるようにするため、永続的な攻撃手段となります。

* MITRE ATT&CK戦術へのマッピング :

* 初回アクセス:

* この戦術は、ネットワーク内で最初の足がかりを得るために使用されるテクニックを網羅しています。

* 攻撃手法には、フィッシングや外部リモートサービスの悪用などが含まれます。

* フィッシングキャンペーンや悪意のあるリンクのクリックは、このカテゴリに該当します。

* 持続性 :

* この戦術には、敵対勢力が足場を維持するために用いる手法が含まれる。

* 手法としては、再起動後もシステム上に残存し、永続的に動作するマルウェアをインストールすることなどが挙げられる。

* このRATは永続的なリモートアクセスを提供するため、この戦術に適している。

* 除外事項:

* 防御回避:

- * これには、探知を回避し、防御を回避するための技術が含まれます。
- * より広い文脈では関連性があるかもしれないが、この事件報告書には、防御を回避するために取られた具体的な行動については記載されていない。
- * 横方向の動き：
- * これは、ネットワークを介して他のシステムへ移動することを含みます。
- * この報告書は、最初のアクセスと、そのアクセスを維持すること以外の措置については示していません。

結論：

- * インシデントレポートには、初期アクセスと永続化の戦術が記録されています。

参考文献：

MITRE ATT&CKフレームワークにおける初期アクセスおよび永続化戦術に関するドキュメント。

インシデント分析とMITRE ATT&CK戦術へのマッピング。

最新問題: 31

展示資料を参照してください。



アセットとIDデータベースの更新プレイブックの構成方法を説明している2つのオプションはどれですか？ 2つ選択してください。）

- A. プレイブックはローカルコネクタを使用しています。
- B. プレイブックはFortiMailコネクタを使用しています。
- C. プレイブックはオンデマンドトリガーを使用しています。
- D. プレイブックは FortiClient EMS コネクタを使用しています。

Answer: A,D (メッセージを残す)

* プレイブック構成の理解：

- * 「Update Asset and Identity Database」という名前のプレイブックは、エンドポイントとユーザー情報を使用してFortiAnalyzerのアセットおよびIDデータベースを更新するように設計されています。

- * この展示では、ON_SCHEDULE STARTER、GET_ENDPOINTS、UPDATE_ASSET_AND_IDENTITY という 3 つの主要コンポーネントを含むプレイブックを示しています。
 - * コンポーネントの分析：
 - * ON_SCHEDULE STARTER: このコンポーネントは、プレイブックがオンデマンドではなくスケジュールに基づいてトリガーされることを示します。
 - * GET_ENDPOINTS: このアクションはエンドポイントに関する情報を取得します。これはエンドポイント管理システムと連携することを示唆しています。
 - * UPDATE_ASSET_AND_IDENTITY: このアクションは、取得した情報を使用してFortiAnalyzerのアセットおよびIDデータベースを更新します。
 - * 選択肢の評価：
 - * オプション A: プレイブックに示されているアクションは、FortiAnalyzer で実行できる標準的なローカルアクションであり、ローカルコネクタの使用を示しています。
 - * オプション B: タスクはエンドポイントと ID 管理に関するものであり、電子メールに関するものではないため、プレイブックが FortiMail コネクタを使用しているという兆候はありません。
 - * オプション C: プレイブックは ON_SCHEDULE」トリガーを使用していますが、これはオンデマンド トリガーの説明と矛盾しています。
 - * オプション D: アクション GET_ENDPOINTS」は、エンドポイントを管理し、エンドポイントから情報を取得するエンドポイント管理システム おそらく FortiClient EMS)との統合を示唆しています。
 - * 結論：
 - * プレイブックは、アクションにローカルコネクタを使用するように構成されています。
 - * FortiClient EMSと連携してエンドポイント情報を取得し、FortiAnalyzerのアセットおよびIDデータベースを更新します。
- 参考文献：
- Fortinetのプレイブックアクションとコネクタに関するドキュメント。
- FortiAnalyzerとFortiClient EMSの統合ガイド。

有効な **NSE7_SOC_AR-7.6** 問題集は GoShiken.com が提供された合格しやすい NSE7_SOC_AR-7.6 試験問題集！ GoShiken.com が最新の **NSE7_SOC_AR-7.6** 試験問題集を提供しています。GoShiken.com NSE7_SOC_AR-7.6 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE7_SOC_AR-7.6 問題集をゲットする人はこちら：
https://www.goshiken.com/Fortinet/NSE7_SOC_AR-7.6-mondaishu.html (9330%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 32

FortiGateとFortiAnalyzer間の自動化ステッチ統合について説明しているのは、次のうちどれですか？

- A. FortiAnalyzer のイベント ハンドラは、イベントが作成されるときに自動化ステッチを実行します。
- B. FortiAnalyzer上で自動化ステッチが設定され、FortiOSコネクタを使用してFortiGateにマッピングされます。
- C. FortiAnalyzer のイベント ハンドラが FortiGate に通知を送信して自動化ステッチをトリガーするように構成されています。
- D. FortiGate のセキュリティ プロファイルが違反をトリガーし、FortiGate は FortiAnalyzer に Webhook コールを送信します。

Answer: D (メッセージを残す)

- * オートメーションステッチの概要 Fortinetソリューションのオートメーションステッチは、ネットワーク内で検出された特定のイベントに対して自動的に対応することを可能にします。この自動化により、手動による介入なしに脅威を迅速に軽減できます。
 - * FortiGateセキュリティプロファイル：
- FortiGateは、セキュリティプロファイルを使用してネットワークトラフィックに対するポリシーを適用します。これらのプロファイルには、ウイルス対策、Webフィルタリング、侵入防止などが含まれます。
- * セキュリティプロファイルが違反または特定のイベントを検出すると、事前に定義されたアクションをトリガーできます。
 - * Webhook呼び出し：
 - * FortiGateは、特定のセキュリティイベントを検出した際にWebhookコールを送信するように設定できます。

* Webhookとは、イベントによってトリガーされるHTTPコールバックであり、指定されたURLにデータを送信します。これにより、FortiGateはFortiAnalyzerなどの他のシステムと通信できるようになります。

* FortiAnalyzerとの統合：

* FortiAnalyzerは、様々なFortinetデバイスからログとイベントを収集し、一元的なログ記録と分析を提供します。

FortiGateからWebhookコールを受信すると、FortiAnalyzerはイベントをさらに分析し、レポートを生成し、設定されている場合、自動アクションを実行できます。

* Detailed Process：

* Step 1：A security profile on FortiGate triggers a violation based on the defined security policies.

* Step 2：FortiGate sends a webhook call to FortiAnalyzer with details of the violation.

* Step 3：FortiAnalyzer receives the webhook call and logs the event.

* Step 4：Depending on the configuration, FortiAnalyzer can execute an automation stitch to respond to the event, such as sending alerts, generating reports, or triggering further actions.

：

Fortinet Documentation: FortiOS Automation Stitches

FortiAnalyzer Administration Guide: Details on configuring event handlers and integrating with FortiGate.

FortiGate Administration Guide: Information on security profiles and webhook configurations.

By understanding the interaction between FortiGate and FortiAnalyzer through webhook calls and automation stitches, security operations can ensure a proactive and efficient response to security events.

最新問題: 33

キューとシフト管理機能を使用して、新しく作成された優先度の低いタスクをL1キューのメンバーに自動的に割り当てたいと考えています。しかし、タスクモジュールをモジュールタイプリストに追加できません。何が問題なのでしょう？回答を1つ選択してください。

- A. タスクモジュールでは、キューイング可能オプションが無効になっています。
- B. タスクモジュールには、より高い優先度のキューがあります。
- C. タスクモジュールは、キューおよびシフト管理ではサポートされていません。
- D. シフトベースの割り当ては無効になっています。

Answer: ([解答を表示する](#))

抜粋： キューを作成する最初のステップは、キュー定義ページで行います。ここで名前と説明を定義し、キューに関連付けるモジュールを指定します... モジュールをモジュールタイプで選択できるようにするには、アプリケーションエディターでキュー可能設定を有効にする必要があります。」

> モジュール。

正解はAです。FortiSOARでは、アプリケーションエディタ > モジュールで キュー可能」設定が有効になっているモジュールのみがキューのモジュールタイプ一覧に表示されるためです。問題はタスクの優先度やキューの優先度ではありません。優先度の高いキューは、複数のキューが同じレコード条件に一致する場合のタイブレークにのみ影響し、モジュールの選択を妨げるものではありません。タスクモジュールはFortiSOARレコードモジュールとして使用できるため、Cは最適な回答ではありません。シフトベースの割り当ても別個のものです。キューが存在する後にシフトの可用性に従って割り当てが行われるかどうかを制御しますが、モジュールがモジュールタイプ一覧に表示されるかどうかは制御しません。

技術的な詳細解説 :キューとシフトの管理はメタデータ駆動型です。まず、モジュールでキューを有効にする必要があります。次に、キュールールで、新しく作成された優先度の低いタスクなどのレコードを照合できます。その後、ユーザー割り当てロジックで、レコードをキューリーダーに割り当てたり、未割り当てのままにしたり、ラウンドロビン方式で分散させたりできます。必要に応じて、シフトベースの可用性を使用します。したがって、最初の修正方法は、[アプリケーション エディター] > [モジュール] > [タスク] > [キュー可能] を有効にすることです。

最新問題: 34

ユーザー入力を変数として保存するために手動トリガーを使用する場合、その変数を参照するための正しいJinja式はどれですか？（回答を1つ選択してください）

- A. {{ vars.input.params. <変数名> }}
- B. {{ globalVars. <変数名> }}

C. {{ vars.item. < 変数名 > }}

D. {{ vars.steps. < 変数名 > }}

Answer: [\(解答を表示する\)](#)

FortiSOAR 7.6 では、プレイブック エンジン は Jinja2 式を使用して動的データを処理します。プレイブックが手動トリガーで構成されている場合、管理者は、レコードからプレイブックを実行する際にアナリストが入力する必要のある入力フィールド(テキスト、選択リスト、チェックボックスなど)を定義できます。

* 入力パラメータのマッピング: この手動トリガーフェーズ中にユーザーが入力したデータはすべて、vars オブジェクト内の input.params ディクショナリに自動的にマッピングされます。したがって、特定の入力値を取得するための構文は {{ vars.input.params.variable_name }} です。

* 変数のスコープ: この特定のパスにより、変数が後続のステップの出力 (vars.steps) やグローバルに定義された変数 (globalVars) からではなく、最初のユーザー入力から取得されることが保証されます。

最新問題: 35

FortiSIEMで、以下の条件を満たすネストされたクエリを作成する必要があります。

* FortiSIEM Windowsエージェントによって検出されたすべてのデバイスを検索します。

* それらのデバイスの中から、Windowsログイン失敗イベントを生成したデバイスを特定します。

このネストされたクエリには、どの2つのクエリコンポーネントを使用すべきですか？2つ選択してください。

A. 外部イベントクエリ

B. 外部CMDBクエリ

C. 内部CMDBクエリ

D. 内部イベントクエリ

Answer: A,C ([メッセージを残す](#))

正確な抜粋: 上のスライドの例では、CMDBを参照する構造化検索を示しています...

属性: レポート IP 演算子: IN 値: デバイス: Windows... 属性: イベント タイプ 演算子: IN 値: イベント タイプ: ログオン失敗。正確な抜粋: FortiSIEM エージェント: ファイル、ログ監視、およびUEBA。」また、このガイドでは、Windows システムではFortiSIEM Windows エージェントを使用してログ転送と監視を行うことができると説明しています。

正解はAとCです。最初の要件はCMDBベースで、FortiSIEM Windowsエージェントによって検出されたデバイスを特定します。これはデバイスセットを生成するため、内部CMDBクエリに記述します。2番目の要件はイベントベースで、そのデバイスセットからWindowsログイン失敗イベントを生成したデバイスを見つけます。これは外部イベントクエリに記述し、イベント条件で内部CMDBクエリのデバイス結果を参照します。

技術的な詳細解説 :クリーンなネストされたクエリのロジックは次のとおりです。内部クエリは関連するアセットの集合を定義し、外部クエリはその集合がターゲットイベントを生成したかどうかをテストします。FortiSIEM では、イベントタイプ IN EventTypes: Logon Failure などのイベントフィルタを備えた CMDB ベースのデバイスグループがよく使用されます。

これにより、長いIPリストを手動で管理する必要がなくなり、検出機能がリアルタイムのインベントリと連動するようになります。

最新問題: 36

FortiAnalyzerをコレクターデバイスとして構成する場合、必ず実行しなければならない2つの手順はどれですか？ 2つ選択してください。)

A. ログ圧縮を有効にする。

B. アナライザーモードでFortiAnalyzerへのログ転送を設定します。

C. データポリシーをアーカイブに重点を置くように設定します。

D. 接続インターフェースでファブリック認証を設定します。

Answer: B,D ([メッセージを残す](#))

* FortiAnalyzerの役割を理解する:

* FortiAnalyzerは、コレクターモードとアナライザーモードという2つの主要なモードで動作します。

- * コレクターモード :さまざまなデバイスからログを収集し、詳細な分析のためにアナライザーモードで動作する別のFortiAnalyzerに転送します。
- * アナライザーモード：詳細なログ分析、レポート作成、およびインシデント管理機能を提供します。
- * FortiAnalyzerをコレクターデバイスとして構成する手順：
 - * A. ログ圧縮を有効にする：

ログ圧縮を有効にするとストレージ容量を節約できますが、FortiAnalyzerをコレクターモードで構成するために特に必要な手順ではありません。
 - * オプション項目であり、コレクター構成プロセスに直接関係しないため、選択していません。
 - * B. アナライザーモードでFortiAnalyzerへのログ転送を設定する：
 - * コレクターFortiAnalyzerによって収集されたログが、詳細な処理のためにアナライザーFortiAnalyzerに送信されることを保証するために不可欠です。
 - * FortiAnalyzerをコレクターデバイスとして構成する上で重要なステップであるため選択されました。
 - * ステップ 1: FortiAnalyzer インターフェースにアクセスし、ログ転送設定に移動します。
 - * ステップ 2: アナライザーモードで FortiAnalyzer の IP アドレスと必要な認証情報を指定して、ログ転送を設定します。

Fortinetのログ転送に関するドキュメント FortiAnalyzerのログ転送

C) データポリシーをアーカイブに重点を置くように設定する：

データポリシーの設定は通常、FortiAnalyzer内でログがどのように保存および管理されるかに関係しており、コレクターデバイスの設定においては、アーカイブに特化する必要は必ずしもありません。

コレクターモードの設定に必須の手順ではないため、選択しませんでした。

D) 接続インターフェースでファブリック認証を設定する：

セキュリティファブリック内のFortiAnalyzerデバイス間の安全かつ認証された通信を確保するために必要です。

安全な統合と通信に不可欠であるため、選定されました。

ステップ1 :FortiAnalyzerインターフェースにアクセスし、ファブリック認証設定に移動します。

ステップ2：他のFortinetデバイスおよびFortiAnalyzerへの接続に使用するインターフェースで、ファブリック認証を有効にします。

参考資料 :Fortinetのファブリック認証に関するドキュメント FortiAnalyzerファブリック認証の実装概要：

収集されたログがアナライザーに確実に送信されるように、ログ転送を設定してください。

セキュリティファブリック内での安全な通信と統合を確保するため、ファブリック認証を有効にしてください。

結論：

ログ転送とファブリック認証の設定は、FortiAnalyzerをコレクターデバイスとしてセットアップし、分析のために適切なログ収集と転送を確実に行うための重要な手順です。

参考文献：

Fortinet の FortiAnalyzer の役割と構成に関するドキュメント FortiAnalyzer 管理ガイド アナライザーモードで FortiAnalyzer にログ転送を設定し、接続インターフェイスでファブリック認証を有効にすることで、FortiAnalyzer をコレクター デバイスとして適切にセットアップできます。

最新問題: 37

You suspect your organization has been a victim of numerous incidents carried out by the same threat actor.

Which option allows you to group the incidents and track them? Choose one answer.

- A.** Add a common tag to correlate them.
- B.** Mark one incident as the parent and run a playbook to close the child incidents.
- C.** Select those incidents and use the Merge function.
- D.** Create a campaign and link related records to it.

Answer: D (メッセージを残す)

Exact Extract: "Campaigns are an extra layer of abstraction used when multiple incidents are tied to a single threat actor. Seemingly unrelated incidents may all be part of the same campaign against an organization." Exact Extract: "It can be difficult to determine if incidents are related and roll them into a campaign."

通常、関連するインシデント間のリンクは、単一の既知の脅威アクターを複数のインシデントに結び付ける一意に識別可能な情報に基づいています。」正解は D です。FortiSOAR では、キャンペーンは、同じ脅威アクターに関連していると思われる複数のインシデントをグループ化するための適切なオブジェクトです。これにより、SOC は、個別のインシデントを 1 つのレコードに統合することなく、より広範な攻撃者の活動を追跡できます。タグは検索に役立つかもしれませんが、同じ構造化された追跡レイヤーを提供しないため、キャンペーン レコードと比較すると弱いです。インシデントをマージすることも、複数の関連するインシデントを上位レベルのキャンペーンの下に保持するのではなく、レコードを結合するため、誤りです。1 つのインシデントを親としてマークし、子インシデントを閉じることは、運用上危険であり、キャンペーンの概念を表していません。

技術的な詳細解説 :キャンペーン追跡は、個別のインシデントが脅威アクターの指標、マルウェアファミリー、インフラストラクチャ、TTP、フィッシングテーマ、コマンド&コントロールパターン、またはMITRE ATT & CKマッピングを共有する場合に有効です。成熟したFortiSOARワークフローでは、アナリストは関連するインシデント、アラート、指標、マルウェアサンプル、タスク、およびレポートをキャンペーンレコードにリンクします。これにより、脅威インテリジェンスチームとインシデント対応チームは、スコープ、タイムライン、帰属の確信度、封じ込めの進捗状況、および教訓を単一の場所で追跡できます。これはファイアウォールパケット処理ではなく、FortiSOARのケース管理と脅威インテリジェンスの相関関係であるため、FortiGate NP/CPオフロードはここでは関係ありません。

最新問題: 38

苦痛のピラミッドモデルに基づくと、指標の価値と、敵対者がその指標を変更することの難しさを正確に表しているのは、次のうちどれですか？ 2つ選択してください)

- A. IPアドレスは、攻撃者が偽装したり、新しいリソースに移動させたりできるため、簡単に攻撃できます。
- B. 戦術、技術、手順は難しい。なぜなら、敵は自分たちの方法を適応させなければならないからだ。
- C. アーティファクトは、攻撃者がファイルパスやレジストリキーを変更できるため、簡単に作成できます。
- D. ツールは、多くの場合、複数の選択肢が存在するため、使いやすい。

Answer: A,B (メッセージを残す)

痛みのピラミッド (David Bianco) は、FortiSIEM 7.3およびFortiSOAR 7.6のカリキュラムで教えられている中核的な概念であり、SOCアナリストが脅威インテリジェンスと検出ロジックの優先順位付けを行うのに役立ちます。このモデルは、攻撃者が変更を強いられる「痛み」または労力に基づいて指標をランク付けします。

* IPアドレス (容易) これらは変更が「容易」と分類されます。攻撃者は、プロキシサービスをローテーションしたり、別のVPSを使用したり、侵害された新しいホストを利用したりするだけで、攻撃を継続できます。

ファイルハッシュよりも価値は高いものの、非常に一時的なものであるため、防御側にとって長期的な価値は比較的低い。

* TTP (タフ/ハード) これはピラミッドの頂点です。TTP (戦術、技術、手順) は、攻撃者が活動する基本的な方法を表します。防御側が戦術 (例えば、攻撃者が権限昇格を実行する特定の方法) を検知して阻止することに成功した場合、攻撃者は活動プロセス全体を再構築せざるを得なくなり、これは時間と労力がかかる作業です。

他の選択肢が間違っている理由:

* アーティファクト (C) ピラミッドによると、ネットワーク/ホストアーティファクトは「簡単」ではなく「厄介」に分類されます。攻撃者はこれらを変更することはできますが、コードやスクリプトの動作を変更する必要があるため、単にIPアドレスを切り替えるよりも手間がかかります。

* ツール (D) ツールは「難易度が高い」と分類されます。代替手段は存在するものの、攻撃者は通常、特定のツールセットを習得するために相当な時間を費やします。そのツールを効果的に使用する能力を失うと、攻撃者の効率は著しく低下します。

最新問題: 39

展示資料を参照してください。



これは、FortiAnalyzer 上での MITRE ATT&CK Enterprise マトリックスの出力の一部を示しています。

正しい記述はどれですか？ 2つ選択してください。）

- A. 戦術T1071には4つのテクニックがあります。
- B. 技術T1071には4つのサブ技術があります。
- C. 戦術T1071をカバーするイベントハンドラがあります。
- D. この戦術に関連するイベントは15件あります。

Answer: B,C (メッセージを残す)

* MITRE ATT&CKマトリックスの理解：

* MITRE ATT&CKフレームワークは、現実世界の観察に基づいた、攻撃者の戦術と技術に関する知識ベースです。

* マトリックス内の各戦術は攻撃手法の「理由」を表し、各手法は敵が戦術を実行する「方法」を表します。

* 提供された証拠資料の分析：

* この展示では、FortiAnalyzerに表示されたMITRE ATT&CKエンタープライズマトリックスの一部を示しています。

* 重点は技術T1071 (アプリケーション層プロトコル)に置かれており、そのサブ技術としてT1071.001、T1071.002、T1071.003、T1071.004というラベルが付けられています。

* 各サブテクニックは、コマンド&コントロール (C2)に使用される異なるタイプのアプリケーション層プロトコルを指定します。

* T1071.001 ウェブプロトコル

* T1071.002 ファイル転送プロトコル

* T1071.003 メールプロトコル

* T1071.004 DNS

* 重要なポイントの特定：

* T1071 の下位技術: 主要技術 T1071 の下には 4 つの下位技術がリストされており、ステートメント B が正しいことが確認されます。

* T1071のイベントハンドラ :FortiAnalyzerには、さまざまな戦術やテクニックを監視するためのイベントハンドラが含まれています。戦術T1071のイベントハンドラが存在するということは、これらの特定のサブテクニックに対してアクティブな監視とアラートが行われていることを示唆しており、ステートメントCが正しいことを裏付けています。

* 誤解を解消します：

* ステートメント A (戦術 T1071 の下に 4 つのテクニックがある) は誤りです。T1071 は 4 つのサブテクニックを持つ単一のテクニックだからです。

* ステートメントD (戦術に関連するイベントが15件)は誤解を招く表現です。15という数字は、アプリケーション層プロトコルに基づく技術の数を指しており、イベントの数とは直接関係ありません。

結論：

* 展示物の正確な解釈により、技術T1071の下に4つのサブ技術があり、戦術T1071をカバーするイベントハンドラーが存在することが確認されました。

参考文献：

MITRE ATT&CK フレームワークのドキュメント。

FortiAnalyzerのイベント処理とMITRE ATT&CKの統合に関するガイド。

最新問題: 40

展示資料を参照してください。



「False Positive Close」という名前のプレイブックを設定し、それを実行して動作を確認しようとしています。しかし、「実行」をクリックしてプレイブックを検索しても、リストに表示されません。この問題の原因として考えられるのは、次のうちどれですか？ 2つ選択してください)

- A. まず、アプリケーションエディタを使用してプレイブックを公開する必要があります。
- B. プレイブックの別のインスタンスが現在実行中です。
- C. アラートモジュールは、プレイブックが実行できるモジュールのリストに含まれていません。
- D. 手動トリガーは、実行するためにレコード入力が必要とするように設定されています。

Answer: (解答を表示する)

FortiSOAR 7.6 では、手動プレイブックは、手動トリガー手順で定義された特定の構成基準を満たしている場合にのみ、レコードの実行メニューに表示されます。

* モジュール範囲 (C): 手動トリガーを使用してプレイブックを作成する場合、管理者はどのモジュール (アラート、インシデント、インジケーターなど) がプレイブックを実行できるかを明示的に選択する必要があります。トリガー構成の「適用可能なモジュール」セクションでアラートモジュールが選択されていない場合、アナリストがアラートモジュールを表示しているときに、プレイブックは実行メニューから非表示のままになります。

* トリガー実行要件 (D): 手動トリガーは、レコードなし、単一のレコード、または複数のレコードで実行するように構成できます。プレイブックが「実行にはレコード入力が必要」で構成されている場合は、

設定が別の入力タイプに限定されている場合 (または選択ロジックに不一致がある場合)、正しい数のレコードが選択されない限り、メニューには表示されません。さらに、プレイブックがレコードが選択されていない場合にのみ実行されるように設計されている場合 (グローバルユーティリティ)、特定のレコードのコンテキストメニューには表示されません。

他の選択肢が間違っている理由：

* 公開 A) FortiSOARプレイブックは、アプリケーションエディタを介した別途の「公開」手順を必要とせずに表示されます。保存してアクティブ化 (オンに切り替え)すると、トリガー設定に基づいてすぐに使用できるようになります。

* 同時実行 B) FortiSOARでは、同じプレイブックの複数のインスタンスを同時に実行できます。プレイブックがアクティブに実行されていても、他のアナリストや後続の実行時にはメニューから非表示になりません。

最新問題: 41

展示資料を参照してください。

Investigation Actions

Investigation Actions:

1. **Identify and Isolate Affected Systems:** Begin by identifying the systems associated with the incident, specifically those linked to the IP addresses FortiGate-ISFW, FortiGate-NGFW, 10.200.200.254, and 100.64.2.21. Isolate these systems to prevent further data exfiltration.
2. **Analyze Network Traffic:** Examine network logs to trace the data flow and identify any unusual patterns or unauthorized data transfers. Focus on traffic related to the technique "Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol" (T1048.003).
3. **Review Security Alerts and Logs:** Check security alerts and logs from the incident reporting device and other security tools to gather more context about the exfiltration attempt.
4. **Conduct a Forensic Analysis:** Perform a forensic analysis on the affected systems to uncover any malware or unauthorized access points that facilitated the exfiltration.
5. **Assess Data Impact:** Determine the type and volume of data exfiltrated to assess the potential impact on the organization.
6. **Implement Mitigation Measures:** Based on findings, apply necessary security patches, update firewall rules, and enhance monitoring to prevent future incidents.

Remediation Actions

Remediation Actions:

1. **Immediate Containment:** Isolate the affected systems, including the devices with IPs FortiGate-ISFW, FortiGate-NGFW and 10.200.200.254, to prevent further data exfiltration. Disconnect these systems from the network to halt any ongoing unauthorized data transfers.
2. **Incident Analysis:** Conduct a thorough investigation to understand the scope and impact of the exfiltration. Analyze logs and network traffic to identify the data accessed and the method used for exfiltration.
3. **Patch and Update:** Ensure all systems, especially those involved in the incident, are updated with the latest security patches to close any vulnerabilities that may have been exploited.
4. **Enhance Monitoring:** Implement enhanced monitoring and alerting for unusual data transfer activities, particularly focusing on non-standard protocols that may be used for exfiltration.
5. **User Training:** Conduct cybersecurity awareness training for employees to recognize and report suspicious activities, emphasizing the importance of data protection.
6. **Review and Update Security Policies:** Reassess and update security policies and procedures to address any gaps identified during the incident analysis.

FortiSIEMでは、調査および修復の出力はどのように生成されますか？ (いずれか1つを選択してください)

- A. インシデントをエクスポートすることで
- B. インシデントレポートを実行する
- C. FortiAIを使用してインシデントを要約する
- D. インシデントのコンテキストタブを表示することで

Answer: C (メッセージを残す)

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明：

FortiSIEM 7.3における重要なイノベーションの一つは、FortiAIの統合です。FortiAIは、SOCアナリストがトリアージおよび対応プロセス中に支援する生成型AI機能を提供します。

* 生成型AIサマリー : インシデントが発生すると、FortiAIは基盤となるログ、相関ロジック、およびMITRE ATT&CKテクニック（図に示されている「代替プロトコルによるデータ漏洩」など）を自動的に分析して、人間が読みやすいサマリーを生成できます。

* 構造化された出力: 展示に表示されている出力、具体的には分類された調査アクション（影響を受けるシステムの特定、トラフィックの分析）と修復アクション（即時の封じ込め、パッチ適用、ユーザー研修）は、FortiAI サマリー要求の典型的な結果です。

* アナリストの効率性: この機能は、アナリストが静的なドキュメントやばらばらのログビューから推奨される対応計画を手動で組み立てる必要なく、即座に実行可能な手順を提供することで、「平均応答時間」(MTTR)を短縮するように設計されています。

他の選択肢が間違っている理由：

* インシデントのエクスポート (A): インシデントをエクスポートすると、通常、調査と修復のための AI 生成の戦略計画ではなく、ログ データとメタデータを含む生データ ファイル (CSV/JSON/PDF) が生成されます。

* インシデントレポートの実行 (B) : 標準インシデントレポートは、時間の経過に伴うインシデントに関する統計データと履歴データを提供します。単一のインシデントの固有の状況に合わせて、番号付きの具体的な調査手順を動的に生成するものではありません。

* Context tab (D): The Context tab in FortiSIEM is primarily used to view the CMDB information of the involved assets (e.g., host details, owner, location) and related historical events. While it provides the data needed for an investigation, it does not provide the list of actions to take.

最新問題: 42

FortiAnalyzerでインシデントを作成する方法は2つあります。どれを選択してください。2つ選択してください)

A. カスタムイベントハンドラを使用する

B. コネクタアクションの使用

C. イベントモニターページで手動で操作します。

D. プレイブックを実行する

Answer: A,D (メッセージを残す)

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract学習ガイドからの包括的かつ詳細な説明：

FortiAnalyzer 7.6および関連するSOCバージョンでは、インシデントはセキュリティイベントの追跡と分析のための集中管理コンテナとして機能します。インシデントを開始するには、主に2つの自動および手動の方法があります。

* カスタムイベントハンドラの使用 (A) FortiAnalyzerでは、イベントハンドラを使用して生ログからイベントを生成します。1最近のバージョンにおける重要な機能の一つは、カスタムイベントハンドラ内の「インシデントを自動的に作成する」設定です。2この設定を有効にすると、システムはトリガーされたイベントを自動的に新しいインシデントレコードに昇格させ、アナリストはインシデントが発生する前に個々のイベントを手動で確認する必要がなくなります。3

* プレイブックを実行する (D): プレイブックは、インシデントのライフサイクルを自動化する強力な手段です。4 プレイブックはイベントトリガーで構成でき、特定の条件に一致するイベントが発生するとすぐに実行されます。これらのプレイブックで利用できる主要なアクションの1つは、インシデントの作成アクションです。これは、トリガーとなったイベントのデータに基づいて、インシデントの詳細、重大度、カテゴリを自動的に入力できます。5 これにより、調査のために高精度のイベントが一貫してキャプチャされることが保証されます。

他の選択肢が間違っている理由：

* コネクタアクションの使用 (B): コネクタを使用すると、FortiAnalyzer は外部システム (ITSM や Security Fabric デバイスなど) と通信できますが、FortiAnalyzer 内で「インシデントの作成」を行うのは、外部統合に使用されるスタンドアロンのコネクタアクションではなく、内部イベントエンジンまたはプレイブック自動化の機能です。

* イベントモニターページで手動で行う (C): イベントモニターページでイベントを表示、フィルタリング、および確認することはできますが、インシデントを手動で発生させるプロセスは通常、インシデントモジュールから、またはログビューや FortiView でイベントを右クリックして「インシデントの発生」を選択することによって行われ、ハンドラーやプレイブックと同じアーキテクチャ上の意味で「イベントモニターページ」で発生すると定義されているコア機能ではありません。

最新問題: 43

インシデントレポートを確認してください。侵害された直後、感染したホストは自身のネットワーク構成と接続の詳細情報を収集し、応答するホストを特定するために複数の内部アドレスに少量の接続試行を開始しました。この活動を最もよく表すMITRE ATT & CKテクニックはどれですか？

2つ選択してください。

- A. システムネットワーク接続の検出
- B. ネットワークスニффイング
- C. 横方向の動き
- D. アクティブスキャン

Answer: A,D ([メッセージを残す](#))

正確な抜粋：MITRE ATT & CKは、14の戦術を通じてサイバー攻撃と侵入を分類および説明します...

これらのカテゴリは、さらに具体的な技術とサブ技術に細分化されます。」正確な抜粋：攻撃者は、ポート スキャンや IP ディスカバリーなどの技術を組み合わせてアクティブ偵察を実行し、優先度の高いターゲットを見つけます。」正解は A と D です。感染したホストは、まず自身のネットワーク構成と接続の詳細を収集しました。これはシステム ネットワーク接続の検出に該当します。MITRE では、この技術は侵害されたシステムとの間のネットワーク接続を一覧表示しようとするものと定義されています。後続の動作である、複数の内部アドレスに少量の接続試行を送信して応答するホストを特定する動作は、アクティブ スキャンに最もよく該当します。MITRE では、アクティブ スキャンはネットワーク トラフィックを通じて被害者のインフラストラクチャを調査するものと説明されています。

ネットワークスニッフイングは、このシナリオでは受動的なパケットキャプチャやインターフェース上のトラフィック監視について説明していないため、誤りです。ラテラルムーブメントも、MITREの戦術であり、ホスト検出活動に最適な手法ではないため、誤りです。ホストはまだ到達可能なシステムを検出している段階であり、別の内部システムに移動していません。技術的な詳細分析: Fortinet SOC の調査では、このシーケンスは侵害後の検出の典型的なパターンです。ipconfig、route print、netstat、Get-NetTCPConnection、arp -a などのコマンドは、システム ネットワーク接続の検出をサポートします。多数の内部 IP への低レートのプローブは、ノイズの多いスキャンよりもステルス性が高く、FortiGate のトラフィック ログ、Windows ファイアウォール イベント、または EDR テレメトリにまばらに表示される場合があります。FortiSIEM は、これを送信元ホスト、宛先の分散、ポートの多様性、および時間ウィンドウと関連付ける必要があります。FortiGate NP/CP チップは許可されたセッションを高速化する可能性があります、検出は ASIC 転送パス内ではなく、FortiSIEM のログとメタデータから行われます。

最新問題: 44

FortiAnalyzerは、侵害された可能性のあるIOCホストを特定するために、どの3つのエンドユーザーログを使用しますか？ 3つ選択してください)

- A. ウェブフィルタログ1
- B. メールフィルタログ
- C. DNSフィルタログ2
- D. アプリケーションフィルタログ
- E. IPSログ

Answer: ([解答を表示する](#))

Fortinet Security Fabric のコンテキストでは、FortiAnalyzer はさまざまなセキュリティログを脅威インテリジェンスデータベースと照合することにより、侵害の指標 (IOC) を検出します。3 IOC エンジン、各エンドユーザーの次のログを具体的に分析して、侵害されている可能性のあるホストを特定します。

* Webフィルタログ A) エンジンはWebフィルタリングログを解析し、ブラックリストに登録されたURL、悪意のあるドメイン、または既知のマルウェア配布サイトに関連付けられたIPへのアクセス試行を特定します。4 脅威データベースで一致するものが見つかった場合、ホストは侵害されているとフラグが立てられます。

* DNSフィルタログ C) DNSリクエストは侵害の主要な指標です。エンジンはこれらのログを監視し、既知のコマンド&コントロール C2)サーバーまたはドメイン生成アルゴリズム DGA) によって生成されたドメインに向けられたクエリを検出します。5

* IPSログ E) : 侵入防御システム (IPS) ログは、既知の攻撃のシグネチャ一致に関する重要なデータを提供します。最新のセキュリティオペレーション (SOC) カリキュラムでは、IPSログは Web ログやDNSログと併用され、ホストが現在感染しており、外部の脅威アクターと通信しようとしているかどうかを高精度で評価するために用いられます。

他の選択肢が間違っている理由：

- * メールフィルタログ (B): フィッシング攻撃 (初期アクセス) の検出には重要ですが、メールログは一般的に、FortiAnalyzer の侵害されたホストビューにおける IOC エンジンの行動に基づく「ロールホーム」検出の主要な情報源ではなく、コンテンツフィルタリングとアンチスパムに使用されます。
- * アプリケーションフィルタログ D) アプリケーション制御ログはソフトウェアの使用状況を可視化しますが、WebフィルタリングやDNSフィルタリングと比較すると、コアIOCエンジンがブラックリストに登録されたネットワーク宛先を特定するために使用する頻度は低くなります。

最新問題: **45**

展示資料を参照してください。

tojson

("data.results[?type=='FileHash-MD5']")

results

value

json_query

data

Jinja expression: {{ [slot 1]][slot 2][slot 3].[slot 4] }}

Slot 1

Slot 2

Slot 3

Slot 4

Exhibit

```
{
  "vars": {
    "artifacts": {
      "data": {
        "results": [
          {
            "type": "Host",
            "value": "malicious-site.com",
            "picklist_iri": "/api/3/picklists/3272abd8-alae-4663-8c47-6d1195e684d9"
          },
          {
            "type": "IP Address",
            "value": "123.123.123.123",
            "picklist_iri": "/api/3/picklists/c0beeda4-2c7a-4214-b7e5-53ba1649539c"
          },
          {
            "type": "Host",
            "value": "fortinet.com",
            "picklist_iri": "/api/3/picklists/3272abd8-alae-4663-8c47-6d1195e684d9"
          },
          {
            "type": "File",
            "value": "org.apache.tika.parser.pdf",
            "picklist_iri": "/api/3/picklists/0162241b-f5bf-4917-a150-00e920be47bd"
          },
          {
            "type": "FileHash-MD5",
            "value": "6aad63bcc3dd4e148f3724808955f912",
            "picklist_iri": "/api/3/picklists/0ca054f2-d923-4992-a4a7-c516e6df281e"
          },
          {
            "type": "FileHash-MD5",
            "value": "9fd2b1c0e4a37658bca9d0f1e2c34567",
            "picklist_iri": "/api/3/picklists/9a8b7c6d-5e4f-41a0-b123-0fedcba98765"
          }
        ]
      }
    }
  }
}
```

MD5ハッシュ値のみを表示するように結果をフィルタリングするための正しいJinja式は何ですか？

{{[スロット 1]|[スロット 2]|[スロット 3].[スロット 4]}}

左側の列からJinja式を選択し、ドラッグして右側の空白位置に移動します。正しい4つの手順を順番に配置し、最初の手順を最初のスロットに配置します。

The screenshot shows a security tool interface with a Jinja expression editor and a data preview section.

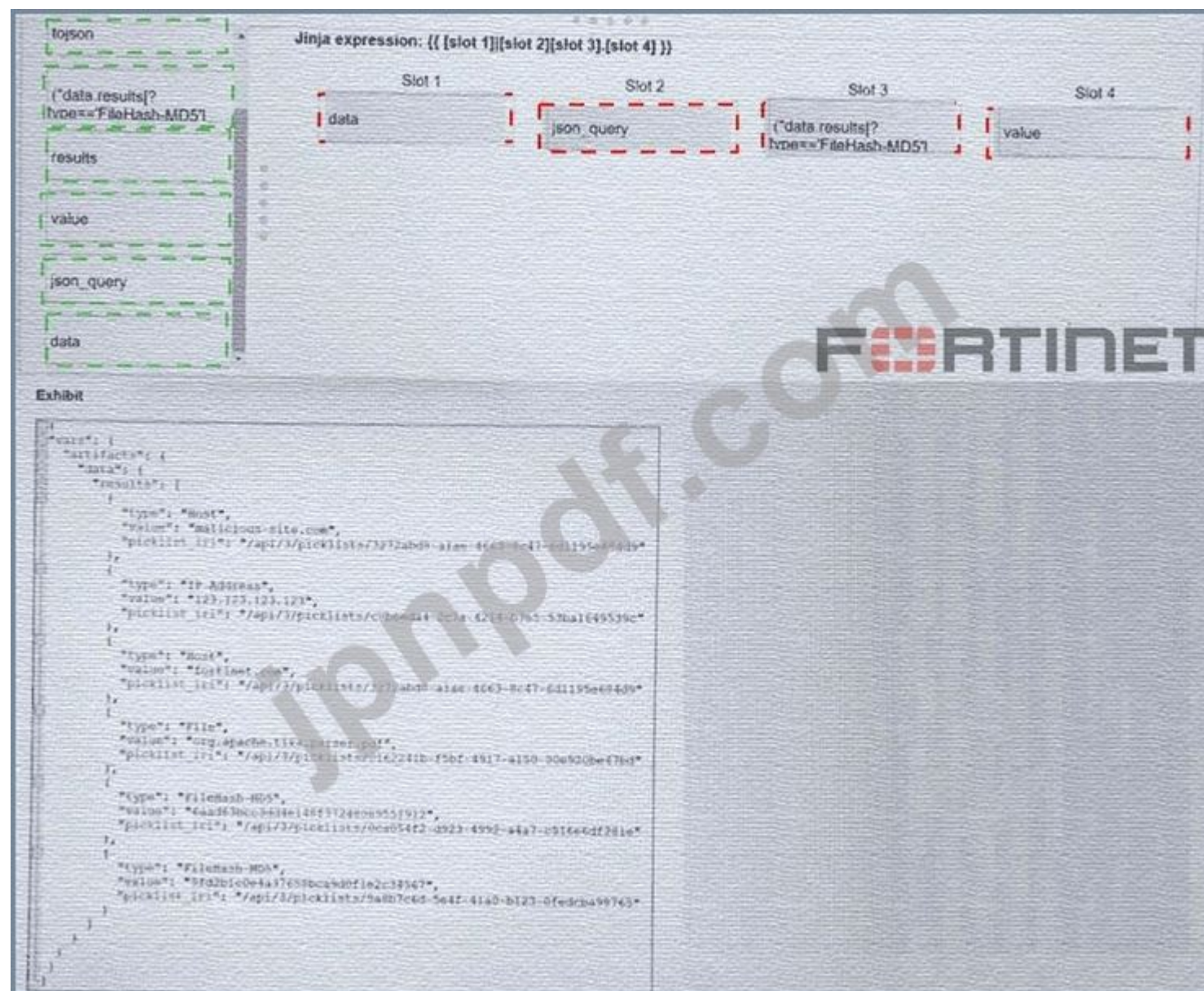
Jinja expression editor:

- Input field: Jinja expression: {{ [slot 1][slot 2][slot 3].[slot 4] }}
- Slots: Slot 1, Slot 2, Slot 3, Slot 4

Data preview (Exhibit):

```
{
  "data": {
    "results": [
      {
        "type": "Host",
        "value": "malicious-site.com",
        "picklist_id": "/api/3/picklists/3272ubdn-a1ae-4663-8c47-6d1155e484d9"
      },
      {
        "type": "IP Address",
        "value": "123.123.123.123",
        "picklist_id": "/api/3/picklists/c0be0da4-2c7a-6219-b305-57ba1649539c"
      },
      {
        "type": "Host",
        "value": "foxtinet.com",
        "picklist_id": "/api/3/picklists/3272ubdn-a1ae-4663-8c47-6d1155e484d9"
      },
      {
        "type": "File",
        "value": "org.apache.tika.patcher.pdf",
        "picklist_id": "/api/3/picklists/016724:b-f5bf-4917-a150-00e920be479d"
      },
      {
        "type": "FileHash-MD5",
        "value": "4a4d630cc3f4e148f172480e55f912",
        "picklist_id": "/api/3/picklists/0ca054f2-d923-4952-94a7-c91646df281e"
      },
      {
        "type": "FileHash-MD5",
        "value": "9fd201e0e4a37659bc9430f1e2c38547",
        "picklist_id": "/api/3/picklists/9a8b7c6d-5e4f-41a0-b123-0fedcba99765"
      }
    ]
  }
}
```

Answer:



Explanation:

スロット 1:data スロット 2:json_query スロット 3:('results[?type=='FileHash-MD5']') スロット 4:value 最終式: {{ vars.artifacts.data | json_query('results[?type=='FileHash-MD5']') .value }}

FortiSOAR 7.6、FortiSIEM 7.3 Exact Extract 学習ガイドからの包括的かつ詳細な説明:

FortiSOAR 7.6では、プレイブック内での高度なデータ操作には、json_query Jinja フィルタを介した JMESPath クエリの使用が必要となることがよくあります。複雑な JSON オブジェクト（図に示す vars.artifacts 辞書など）から特定のデータを抽出するには、アナリストは次の構造階層に従う必要があります。

* スロット 1 (データ): 展示に基づく、アーティファクト情報のルートは vars.artifacts の下にあります。

データ。したがって、「データ」がフィルタの出発点となります。

* スロット 2 (json_query): 高度なフィルタリング (特定のタイプの検索) を実行するには、json_query フィルタを適用する必要があります。これにより、プレイブックはリストを走査し、特定のキーと値のペアに一致する項目を見つけることができます。

* スロット 3 ('results[?type=='FileHash-MD5']'): これは JMESPath 式です。results 配列を調べてフィルター [...] を適用し、type 属性が FileHash-MD5 と完全に一致するオブジェクトのみを検索します。

* スロット 4 (値): 正しいオブジェクトが見つかったら、式は実際のハッシュを返す必要があります。JSON の例では、MD5 文字列は value という名前のキーに格納されています。

他の選択肢が間違っている理由:

* tojson: このフィルターは辞書/リストを JSON 文字列に変換しますが、これによりオブジェクトから「value」フィールドをさらにクエリする機能が損なわれます。

* 結果 (スタンドアロン スロットとして):「results」はパスの一部ですが、条件付きフィルタリングを可能にするために json_query 文字列内で処理されます。

最新問題: 46

Which two phases are part of the FortiSOAR incident handling process but are not phases in the NIST 800-61 Revision 2 model? Choose two answers.

- A. Preparation
- B. Confirmation
- C. Detection
- D. Identification

Answer: (解答を表示する)

正確な抜粋：FortiSOARでは、準備フェーズはSOAR導入前の責任とみなされるため、インシデント処理の範囲外であると想定しています。」正確な抜粋：FortiSOARでは、検出および分析フェーズは、検出、識別、および確認に拡張されます...識別フェーズでは、アナリストはインシデントに関連付けられたアラートを評価し、コンテキストを理解し、インジケータを充実させることができます。確認フェーズでは、アナリストはインシデントが真陽性か偽陽性かを確認できます。」正解はBとDです。NIST 800-61改訂版2では、準備、検出と分析、封じ込め、根絶、復旧、およびインシデント後の活動を含む、より広範なインシデント処理フェーズを使用しています。

FortiSOARは、準備段階をSOARの範囲外とみなし、NISTの検出と分析を、より運用上有用なFortiSOARのフェーズ（検出 識別、確認）に分割することで、このモデルを修正しています。したがって、識別と確認はFortiSOAR固有のフェーズ名であり、NISTの独立したフェーズではありません。

Aは誤りです。準備はNISTのフェーズですが、FortiSOARではインシデント処理ワークフローから除外されています。Cも最適な回答ではありません。検出はNISTの検出と分析を組み合わせたフェーズの一部であり、FortiSOARにも含まれています。

技術的な詳細解説：FortiSOARの分割は実用的です。検知とは、アラートまたはインシデントがFortiSOARに入力された時点です。識別とは、アナリストが問題を詳細化し、文脈化し、範囲を絞り込む段階です。確認とは、インシデントが真陽性か偽陽性かを検証する決定ポイントです。この粒度により、各フェーズに異なる自動化を適用できるため、プレイブックの設計が向上します。これはトラフィック処理ではなくインシデントライフサイクルモデリングであるため、FortiGate NP/CPオフロードはここでは関係ありません。

有効な **NSE7_SOC_AR-7.6** 問題集は GoShiken.com が提供された合格しやすい NSE7_SOC_AR-7.6 試験問題集！ GoShiken.com が最新の **NSE7_SOC_AR-7.6** 試験問題集を提供しています。GoShiken.com NSE7_SOC_AR-7.6 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE7_SOC_AR-7.6 問題集をゲットする人はこちら：

https://www.goshiken.com/Fortinet/NSE7_SOC_AR-7.6-mondaishu.html (9330%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 47

後続のタスクでトリガーイベントをトリガー変数として使用できるようにするプレイブックトリガーはどれですか？ 2つ選択してください。）

- A. イベント
- B. 事件
- C. 予定通り
- D. オンデマンド

Answer: A,B (メッセージを残す)

* プレイブックのトリガーを理解する：

* プレイブックのトリガーは、FortiAnalyzerまたはFortiSOAR内の自動化されたワークフローの開始点です。

* これらのトリガーは、プレイブックの実行方法と実行タイミングを決定し、プレイブック内の後続タスクに関連情報（トリガー変数）を渡すことができます。

* プレイブックトリガーの種類：

* イベントトリガー：

特定のイベントが発生したときにプレイブックを起動します。

* イベントの詳細は、後続のタスクで変数として使用して、応答をカスタマイズできます。

- * イベントの詳細をトリガー変数として使用できるため、選択しました。
- * インシデントトリガー：
- * インシデントが作成または更新されたときに、プレイブックをアクティブ化します。
- * インシデントの詳細は、後続のタスクで変数として利用できます。
- * インシデントの詳細をトリガー変数として使用できるため、選択されました。
- * スケジュールトリガー：

指定された時刻または間隔でプレイブックを実行します。

- * トリガーイベントを本来的に使用して変数を後続のタスクに渡すことはありません。

トリガーイベントの詳細を渡す必要がないため、選択しませんでした。

- * オンデマンドトリガー：

- * プレイブックを手動で、または必要に応じて実行します。

- * 後続のタスクで使用するためのトリガーイベントの詳細を自動的に含めることはありません。

- * 変数にトリガーイベントを使用しないため、選択されません。

- * 実装手順：

- * ステップ 1: プレイブック構成で、イベントまたはインシデント トリガーの条件を定義します。

- * ステップ 2: トリガー イベントまたはインシデントの詳細を使用して、後続のタスクでアクションと応答をカスタマイズします。

- * ステップ 3: プレイブックをテストして、トリガー変数が正しく渡され、使用されていることを確認します。

- * 結論：

- * イベントおよびインシデントトリガーは、特定の事象に基づいてプレイブックを起動するように特別に設計されており、トリガーの詳細を後続のタスクで使用できます。

：

Fortinet の Playbook 構成に関するドキュメント FortiSOAR Playbook ガイド EVENT および INCIDENT トリガーを使用することで、トリガー イベントを後続のタスクで変数として活用し、より動的で応答性の高い Playbook アクションを実現できます。

Valid NSE7_SOC_AR-7.6 Dumps shared by GoShiken.com for Helping Passing NSE7_SOC_AR-7.6 Exam! GoShiken.com now offer the **newest NSE7_SOC_AR-7.6 exam dumps**, the GoShiken.com NSE7_SOC_AR-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com NSE7_SOC_AR-7.6 dumps with Test Engine here: https://www.goshiken.com/Fortinet/NSE7_SOC_AR-7.6-mondaishu.html (93 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)