

Lead2Passed



Lead2Passed

HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

Login / Register My Shopcart (1)

Input your exam code ...



Try before you buy

Download a free sample of any of our exam questions and answers

- ✓ Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
- ✓ PDF format: Easy to read and print learning materials, our products are available in PDF file format.
- ✓ Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.



365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.



Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

<http://www.lead2passed.com>

Valid Certification Exam Dumps Materials and Study Guide -
Lead2Passed

Exam : **C2150-612J**

Title : **IBM Security QRadar SIEM
V7.2.6 Associate Analyst**

Vendor : **IBM**

Version : **DEMO**

QUESTION NO: 1

セキュリティアナリストは、特定の日に違反を検索するよう求められました。要求者は時間枠の痛みはありませんでしたが、使用する送信元ホスト情報と関連するネットワーク、送信先IPおよびユーザー名を持っていました。

セキュリティアナリストは、要求された情報を検索するためにどのフィルタを使用できますか？

- A. オフェンスID、送信元IP、ユーザー名
- B. 大きさ、送信元IP、送信先IP
- C. 説明、宛先IPホスト名
- D. 特定の区間、ユーザー名、宛先IP

Answer: D

QUESTION NO: 2

どのQRadarアドオン・コンポーネントが、DMZから内部ネットワークに通信できる暗号化されていないプロトコルのリストを生成できますか？

- A. QRadar Risk Manager
- B. QRadar Flow Collector
- C. QRadar インシデントフォレンジック
- D. QRadar脆弱性マネージャー

Answer: A

QUESTION NO: 3

どのタイプのルールで、保存された検索を必要とし、それを共通のパラメーターに基づいてグループ化する必要があるか

- A. フロールール
- B. イベントルール
- C. 共通の規則
- D. 異常ルール

Answer: B

QUESTION NO: 4

netflowフローソースを使用することの2つの利点は何ですか？（2つ選んでください）

- A. データペイロードを含めることができます。
- B. ルータのインタフェース情報を含めることができます。
- C. フローに関係するユーザー名を含めることができます。
- D. リモートアドレスのASN番号を含めることができます。
- E. ネットワークへのアクセスに使用される認証方法を含めることができます。

Answer: B D

QUESTION NO: 5

不明または誤ったQReaderカテゴリにあると判断されたと解析されたイベントを修正するための効果的な方法は何ですか。

- A. ペイロードからカテゴリを抽出するためのDSM拡張を作成します。

- B.ペイロードから適切なカテゴリを抽出するためのカスタムプロパティを作成します。
- C.イベントの詳細を開き、マップイベントを選択してそれを正しいカテゴリに割り当てます。
- D.カスタムルールを作成し、Rule Responseを使って適切なカテゴリの新しいイベントを送信します。

Answer: B

QUESTION NO: 6

次世代ファイアウォールのどの機能が以前のファイアウォールでは利用できないのですか？

- A.VPNサポート
- B.レイヤ3ベースのファイアウォールルール
- C.統合署名ベースのIPSエンジン
- D.ネットワークとポートアドレス変換 (NAT)

Answer: D

QUESTION NO: 7

外部分析のためにイベントデータをどこからエクスポートできますか？

- A.[違反]タブから攻撃を選択して右クリックし、イベントデータのエクスポートを選択します。
- B.イベントの一覧ページから処理を選択して、XMLにエクスポートまたはCSVにエクスポートをクリックします。
- C.違反の要約ページからアクションを選択して、XMLにエクスポートまたはCSVにエクスポートをクリックします。
- D.[違反]タブから攻撃を選択し、アクションをクリックし、XMLにエクスポートまたはCSVにエクスポートを選択します。

Answer: C

QUESTION NO: 8

[ログアクティビティ]タブに表示される情報は2つありますか。(2つ選んでください)

- A.犯罪
- B.脆弱性
- C.ファイアウォールイベント
- D.宛先バイト
- E.内部QRadarメッセージ

Answer: C D