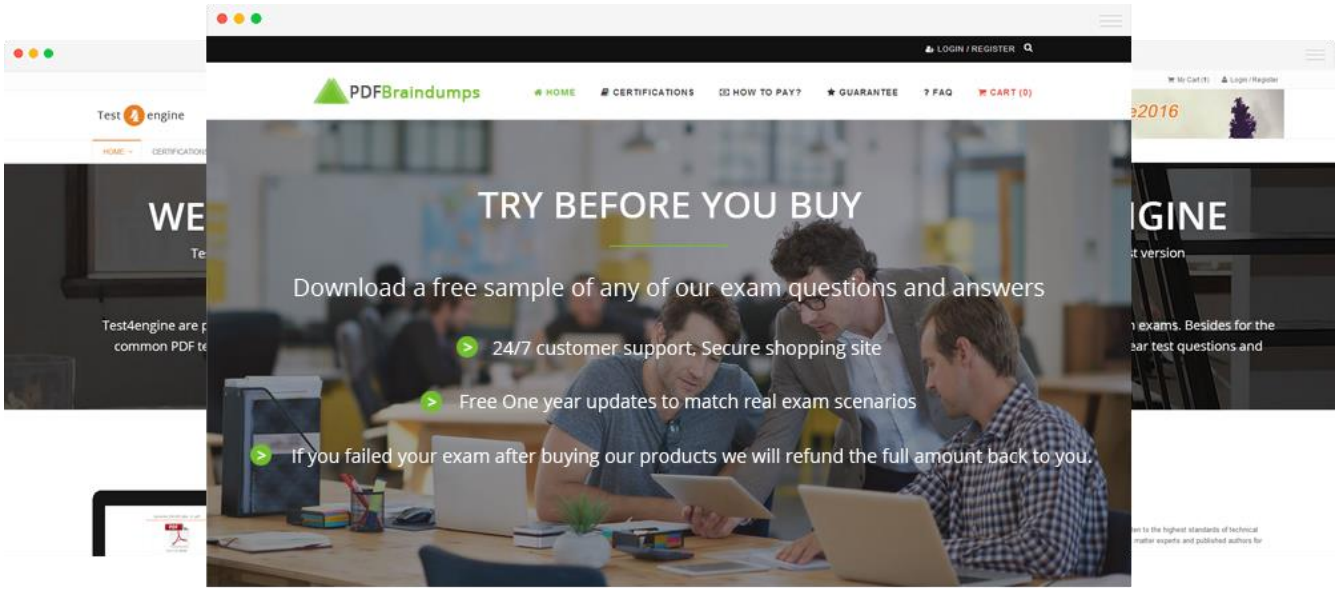
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **C1000-018J**

Title : IBM QRadar SIEM V7.3.2 Fundamental Analysis (C1000-018日本語版)

Vendor : IBM

Version : DEMO

QUESTION NO: 1
チェックポイントとQRadarの統合でサポートされているプロトコル構成はどれですか？（2つ選択してください。）
A. チェックポイントREST API
B. SFTP
C. JDBC
D. OPSEC / LEA
E. SYSLOG
Answer: D,E

QUESTION NO: 2
ログソースはどのように定義できますか？
A. ユーザーがQRadarコンソールを操作して日常業務を行うなどのデータ・ソース。
B. Netflowなどのデータソース。 J-FlowまたはsFlowデータ。
C.
イベントログを作成するファイアウォールや侵入防止システム（IPS）などのデータソース。
D. [ネットワークアクティビティ]タブにあるデータソース。
Answer: C

QUESTION NO: 3
QRadarのさまざまなフロータイプは何ですか？
A. タイプ1、タイプ2、タイプ3、タイプ4
B. 標準、タイプ1、タイプ2、タイプ3
C. L2L、L2R、R2R、R2L
D. 標準、タイプA、タイプB、タイプC
Answer: D

QUESTION NO: 4
有効なオフェンスの命名メカニズムとは何ですか？
この情報は次のようになります。
A. 関連するオフェンスの名前を置き換えます。
B. 関連するオフェンスの名前を設定または置換します。
C. 関連する犯罪の命名に含まれます。
D. 関連するオフェンスの名前を設定します。
Answer: D
Explanation
Under "Offense Naming", check "This information should contribute to the name of the associated offense(s)".

QUESTION NO: 5
アナリストは、重要な情報を検索するために、イベントからカスタムプロパティを作成しました。アナリストは、QRadarの効率とパフォーマンスを維持するために、重要な情報を探すときに検索されるイベント・ログとデータ量の数を減らす必要もあります。

アナリストはどの機能を使用する必要がありますか？
A. データベース管理
B. ログ管理
C. インデックス管理
D. イベント管理
Answer: D

QUESTION NO: 6
カスタムルールエンジン（CRE）はどのようにルールを評価しますか？
A. テストの重要度に基づいてテストを実行し、重要なテストを最初に実行します。
B.
最初にステートレステストを実行し、次にステートフルテストを実行して結果を評価します。
C. ルールテストを1行ずつ順番に実行し、テストが真である間続行します。
D. すべてのルールテストを同時に実行し、すべてのテストが完了した後に結果を評価します
Answer: B

QUESTION NO: 7
クローズされたオフェンスを再開する手順は何ですか？
A. クローズされたオフェンスを再開する新しいイベント/フローを待ちます。
B.
[管理]タブの[アクション中のオフェンス]をアクティブにし、ドロップダウンメニューを再度開きます。
C. クローズされたオフェンスを再開することはできません。
D.
[オフェンス]タブの[アクション/再度開く]ドロップダウンメニューでオフェンスをアクティブにします。
Answer: C
Explanation
Not possible to reopen a closed offense.