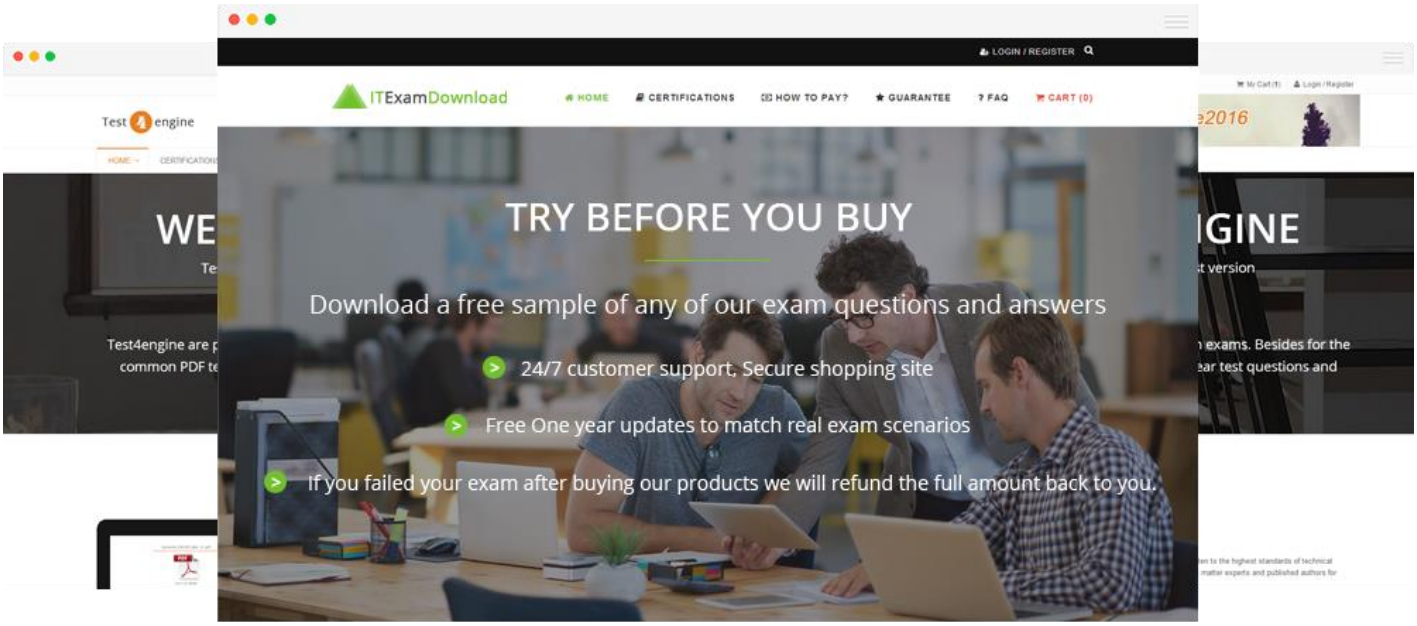
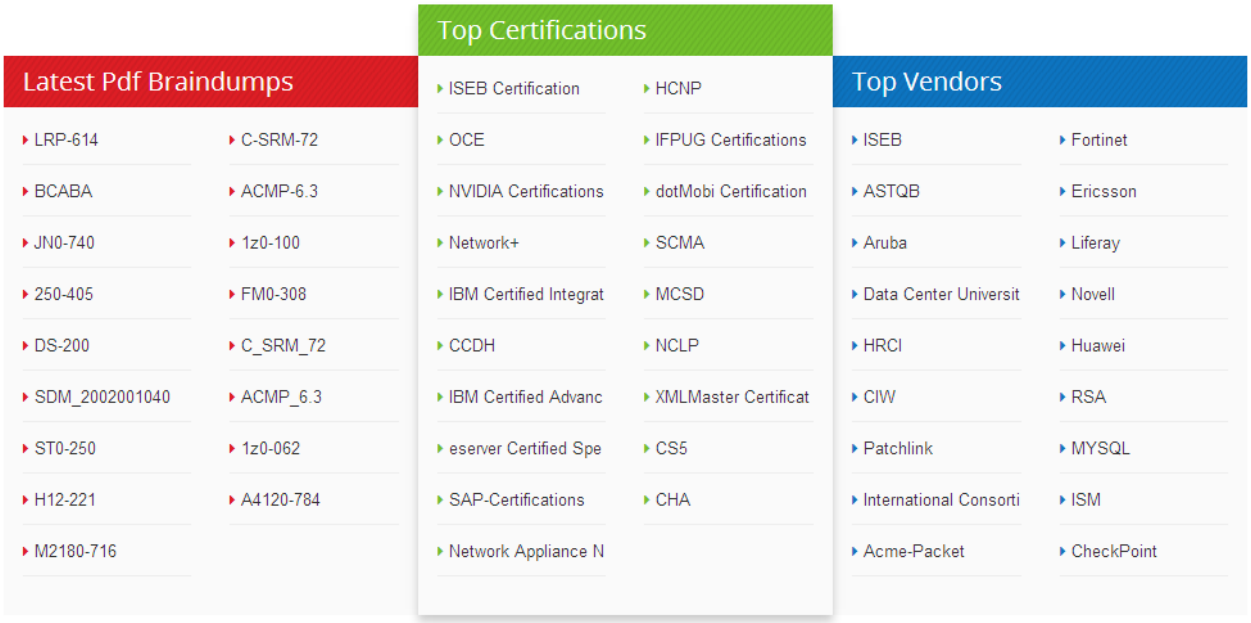
ITExamDownload





http://www.itexamdownload.com

Provide the latest exam dumps for you. Download the free reference for study

Exam : **210-255J**

Title : Implementing Cisco Cybersecurity Operations

Vendor : Cisco

Version : DEMO

QUESTION NO: 1
通信先に基づいて、ホストの1つが潜在的に侵害されていることをどのように確認しますか？
A.Talos IP＆Domain Reputation Centerでホストの通信先を検索します。
B.各IPアドレスまたはドメインからホストが送受信したトラフィックの量を分析します。
C.内部ホストと通信しているホストに対してStealthwatchアラームがトリガーされたかどうかを確認します。
D.Firepowerアプライアンスをチェックして、悪意のあるファイルがダウンロードされたかどうかを確認します。
Answer: A

QUESTION NO: 2
ファイルをダウンロードするためにWiresharkのどこに移動しますか？
A.ファイル>テキストのエクスポート
B.ファイル>バイナリのエクスポート
C.ファイル>ファイルのエクスポート
D.ファイル>オブジェクトのエクスポート
Answer: D

QUESTION NO: 3
Common Vulnerability Scoring System（CVSS）の3つのメトリック、つまり「スコア」は次のうちどれですか？（該当するものをすべて選択。）
A.ベースラインスコア
B.基本スコア
C.環境スコア
D.時間スコア
Answer: BCD

QUESTION NO: 4
銀行、製造会社、大学、または連邦政府機関などの親組織にインシデント処理サービスを提供するCSIRTカテゴリはどれですか？
A.内部CSIRT
B.全国CSIRT
C.調整センター
D.分析センター
E.ベンダーチーム
F.インシデント対応プロバイダー
Answer: A

QUESTION NO: 5
前駆体のどの例が真実ですか？
A.管理者は、パスワードが変更されたことを発見しました。

B.ホストに対してポートスキャンが実行されたことを示すログ。
C.ホストがマルウェアに感染しているという通知。
D.監査ログエントリなしでデバイス構成がベースラインから変更されました。
Answer: B

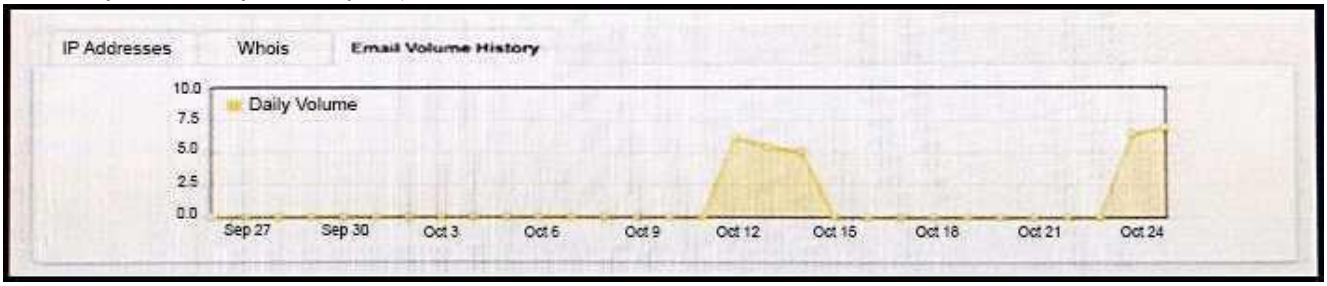
QUESTION NO: 6
脅威アクターについてのどの記述が真実ですか？
A.脅威にさらされている企業資産です。
B.脅威にさらされる資産です。
C.彼らは攻撃の加害者です。
D.彼らは攻撃の犠牲者です。
Answer: C

QUESTION NO: 7
検出されたファイルを一意に識別するために使用される一般的なアーティファクトは何ですか？
A.ハッシュ
B.タイムスタンプ
C.ファイルサイズ
Answer: A

QUESTION NO: 8
VERISスキーマの被害者層を正しく説明しているのは、次の2つのステートメントですか？（2つ選択してください。）
A.被害者の人口統計セクションでは、インシデントの影響を受ける組織について説明していますが、特定していません。
B.被害者層セクションでは、単一組織内のさまざまなタイプの組織または部門を比較します。
C.被害者の人口統計セクションでは、事件に関する一般情報を収集します。
D.被害者の人口統計セクションでは、位置情報データを使用して、被害者の組織名と脅威アクターを特定します。
Answer: AB

QUESTION NO: 9
次のうち、企業CSIRTの責任のいくつかの例と、それが作成するのに役立つポリシーはどれですか？（該当するものをすべて選択。）
A.ベンダー顧客ネットワークのスキャン
B.インシデントの分類と処理
C.情報の分類と保護
D.情報発信
E.記録の保持と破棄
Answer: BCDE

QUESTION NO: 10
展示を参照してください。 電子メールのボリューム履歴が異常に高いことがわかります。 どの潜在的な結果が本当ですか？



A.ドメインから送信された電子メールは、受信者によってフィルタリングされる場合があります。
B.ドメインに送信されたメッセージは、トラフィックが停止するまでキューに入れられる場合があります。
C.ネットワーク内のいくつかのホストが危険にさらされる可能性があります。
D.ネットワークの輻輳が原因でパケットがドロップされる場合があります。
Answer: C

QUESTION NO: 11
プロセスとスレッドについて正しいものは次のうちどれですか？
A.各スレッドは、プライマリプロセスと呼ばれる単一のプロセスで始まりますが、そのサービスのいずれかから追加のプロセスを作成することもできます。
B.各サービスは、プライマリハイブと呼ばれる単一のハイブから始まりますが、そのハイブのいずれかから追加のスレッドを作成することもできます。
C.各プロセスは、プライマリスレッドと呼ばれる単一のスレッドで開始されますが、任意のスレッドから追加のスレッドを作成することもできます。
D.各ハイブは、プライマリスレッドと呼ばれる単一のスレッドで始まりますが、任意のスレッドから追加のスレッドを作成することもできます。
Answer: C

QUESTION NO: 12
侵入分析に関連する2つのHTTPヘッダーフィールドはどれですか？ （2つ選択）。
A.ユーザーエージェント
B.ホスト
C.接続
D.言語
E.ハンドシェイクタイプ
Answer: AB

QUESTION NO: 13
次のLinuxファイルシステムのうち、ジャーナリングをサポートするだけでなく、パフォーマンスと信頼性を向上させるためにファイルデータを保存するようなファイルシステムの重要なデータ構造を変更するものはどれですか。
A. GRUB

B. LILO
C. Ext4
D. FAT32
Answer: C

QUESTION NO: 14
遡及的なセキュリティ手法を使用する場合、何に対処できますか？
A.影響を受けるホストでソフトウェアの更新が必要な場合
B.影響を受けるシステム
C.影響を受けるシステムの交換が必要な場合
D.マルウェアがまだネットワークに残っている理由
Answer: B

QUESTION NO: 15
結果を説明する分析手法と、各結果の可能性はどの程度ですか？
A.決定論的
B.探索的
C.確率的
D.説明的
Answer: C

QUESTION NO: 16
NACを自動的に実施するために使用される業界をリードするアプローチはどのテクノロジーですか？
A.SNMP
B.ポートセキュリティ
C.IGMP
D.802.1x
Answer: D