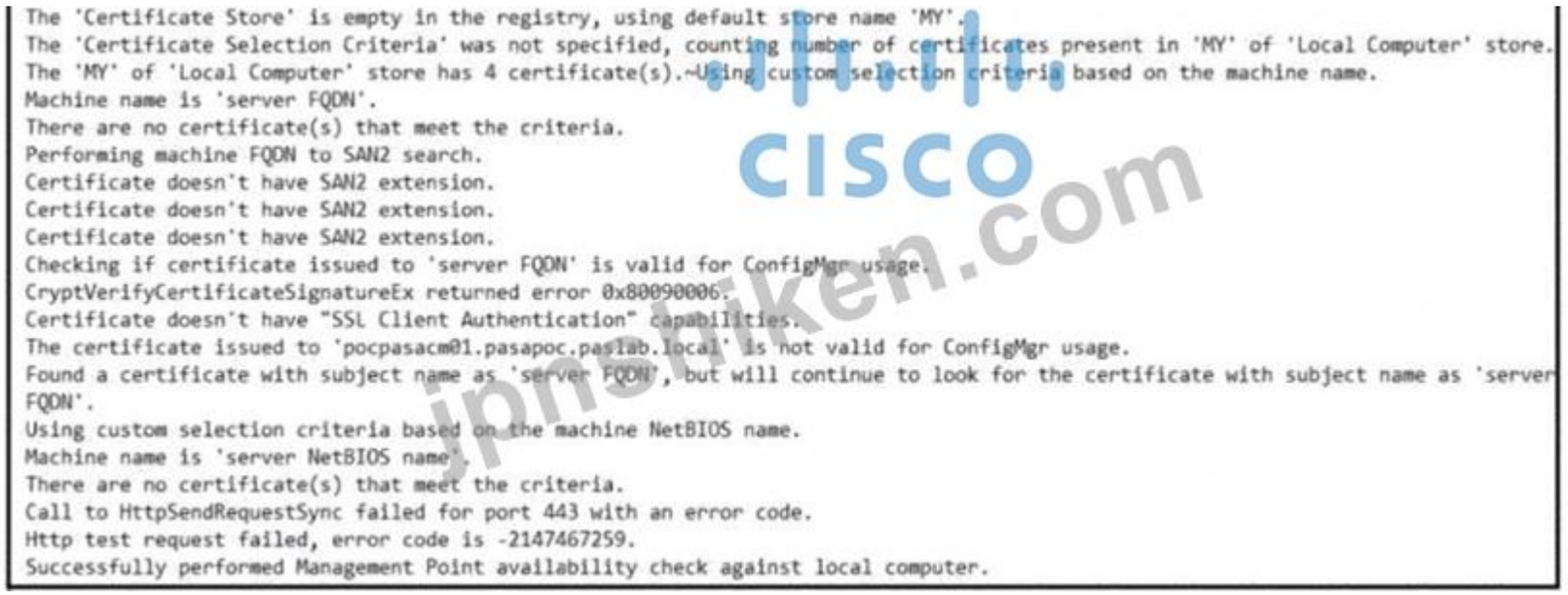
Cisco.200-201J.v2026-09-19.q210

試験コード：	200-201J
試験名称：	Understanding Cisco Cybersecurity Operations Fundamentals (200-201日本語版)
認証ベンダー：	Cisco
無料問題の数：	210
バージョン：	v2026-09-19
ページの閲覧量：	110
問題集の閲覧量：	3250

https://www.jpnshiken.com/shiken/Cisco.200-201J.v2026-09-19.q210.html

質問: **1**



図を参照してください。この問題を特定して解決するために、エンジニアはどのような一連のアクションを実行する必要がありますか？

A. IIS サーバーを再インストールして証明書の詳細をデフォルトにリセットし、サーバーに接続してみます。

B. 中間証明書を削除し、各サーバーに CA ルート証明書をインストールします。

C. 証明書テンプレートにクライアント認証を追加し、証明書を再発行して適用します。

D. 異なるバージョンの CA 機関を実装し、中間証明書をインストールします。

正解: **(**正解を表示します**)**

質問: **2**

非対称暗号化に対する対称暗号化の利点は何ですか？

A. キーはデータ型に応じてオンデマンドで生成されます。

B. データ送信用に1回限りの暗号化キーが生成されます

C. 大量のデータを送信するのに適しています。

D. セッション用のより高速な暗号化メカニズムです

正解: **D (**コメントを発表する**)**

Symmetric encryption is a type of encryption that uses the same key to encrypt and decrypt data. Asymmetric encryption is a type of encryption that uses a pair of keys: a public key and a private key. The public key can be used to encrypt data, but only the private key can decrypt it, and vice versa. An advantage of

symmetric encryption over asymmetric encryption is that it is faster and more efficient for encrypting large amounts of data, such as in sessions or bulk transfers. Asymmetric encryption is slower and more computationally intensive, but it is more secure and suitable for key exchange or digital signatures. References := Cisco Cybersecurity Operations Fundamentals, Module 2: Security Monitoring, Lesson 2.3: Cryptography and PKI,

質問: **3**



図を参照してください。セキュリティエンジニアは、SNORT IPS/IDSから悪意のあるトラフィックを報告するアラートを複数受信しました。SNORTログを調べることで、エンジニアは何を理解するべきでしょうか？

A. リモートの脅威が、Windows システムの複数のポートに対して EternalBlue 攻撃を実行します。

B. リモートの脅威が、複数のホストと異なるポートに対して EternalBlue 攻撃を実行します。

C. 内部脅威が、ホスト 192.168.2.101 および 192.168.200.10 のポート 445 に対して EternalBlue 攻撃を実行します。

D. 内部の脅威が、ポート 445 上の Windows システムに対して EternalBlue 攻撃を実行します。

正解: **(**正解を表示します**)**

質問: **4**

エンドポイントベースの攻撃におけるルートキットの使用について説明しているものは何ですか?

A. システム上でサービス拒否を引き起こすリモートコード実行

B. 攻撃者がシステムのルートアクセスを無効にするために使用する脆弱性のセット

C. リモートコード実行に使用できるエクスプロイト

D. 攻撃者が検出を回避しながら侵害されたシステムの制御を維持するために使用するツールのセット

正解: **D (**コメントを発表する**)**

質問: **5**

不正アクセスから保護する必要がある個人情報とは何ですか?

A. 生年月日

B. 運転免許証番号

C. 性別

D. 郵便番号

正解: **B (**コメントを発表する**)**

Personally Identifiable Information (PII) refers to any data that can be used to identify a specific individual.
Safeguarding PII is critical to protect individuals' privacy and prevent identity theft. A driver's license number (B) is considered PII because it is unique to an individual and can be used to confirm their identity.

Other examples of PII include social security numbers, passport numbers, and financial account numbers. It is important to protect such information from unauthorized access to maintain personal privacy and security.
Identifying and Safeguarding Personally Identifiable Information (PII)2.

質問: **6**
IPv4 プロトコル ヘッダーから収集される 2 つの情報はどれですか? (2つ選んでください。)
A. トラフィックの宛先となる UDP ポート
B. トラフィックの送信元の TCP ポート
C. パケットの送信元 IP アドレス
D. パケットの宛先 IP アドレス
E. トラフィックの送信元の UDP ポート
正解: **(**正解を表示します**)**
The IPv4 protocol header contains various fields that provide essential information for routing and delivery of packets across an IP network. Two key pieces of information collected from the IPv4 header are the source IP address and the destination IP address of the packet. These addresses are crucial for identifying where a packet is coming from and where it is intended to go12.
References := The structure and fields of the IPv4 header, including the source and destination IP addresses, are explained in detail in networking resources and documentation, such as the ComputerNetworkingNotes tutorial on IPv4 Header Structure1, and the Engineering LibreTexts on the IPv4 Header2.

質問: **7**
攻撃者が組織のネットワークに侵入しました。5タプルのアプローチを使用して、分析者は、グループ化されたログのセットで侵害されたホストを分離するためにどのデータポイントを使用する必要がありますか？
A. イベント名、ログソース、時刻、ソースIP、およびホスト名
B. プロトコル、送信元IP、送信元ポート、宛先IP、および宛先ポート
C. イベント名、ログソース、時刻、ソースIP、およびユーザー名
D. プロトコル、ログソース、ソースIP、宛先IP、およびホスト名
正解: **D (**コメントを発表する**)**
The 5-tuple approach consists of protocol, source IP address, source port number, destination IP address, and destination port number to uniquely identify sessions between endpoints on a network. References := Cisco Cybersecurity Source Documents Reference:https://blogs.cisco.com/security/the-dreaded-5-tuple

質問: **8**
デジタル通信において、ユーザー T0n2262144790 と D4n4126220794 の間で公開鍵を安全に交換するにはどの方法が推奨されますか?
A. ハードウェア セキュリティ モジュール
B. かなり良いプライバシー
C. セキュアな多目的インターネットメール拡張機能
D. 自動証明書管理環境
正解: **(**正解を表示します**)**

質問: **9**
「価格控除」という件名の悪意のある添付ファイルを含む空メールはどのような攻撃ですか?
A. 中間者攻撃

B. スミッシング
C. フィッシング攻撃
D. 整合性違反
正解: (正解を表示します)
A phishing attack often involves sending emails that appear to be from reputable sources with the goal of inducing individuals to reveal personal information, such as passwords and credit card numbers. In this case, the email with the subject "price deduction" containing a malicious attachment is designed to trick the recipient into opening the attachment, which can then execute harmful software on their device

質問: **10**
SI EM セキュリティ システムと SOAR セキュリティ システムの違いは何ですか?
A. SOAR はさまざまな種類のログとイベント データ インフラストラクチャ コンポーネントを取り込み、SIEM はエンドポイント セキュリティ ソフトウェアと外部の脅威インテリジェンス フィードからデータを取得できます。
B. SOAR はセキュリティ データを一元的に収集して保存し、実用的なインテリジェンスに変換します。SIEM により、SOC チームは手動タスクを自動化および調整できます。
C. SIEM は不審なアクティビティを検出した場合にアラートを生成し、SOAR は調査パスのワークフローを自動化し、アラートにかかる時間を削減します。
D. SIEM はデータ収集、標準化、ケース管理、分析を組み合わせて多層防御のコンセプトを実現し、SOAR はセキュリティ データのウイルス対策ログ、ファイアウォール ログ、ダウンロードされたファイルのハッシュを収集します。
正解: (正解を表示します)
SIEM (Security Information and Event Management) systems are designed to collect, correlate, and analyze security event data from various sources to provide insights into potential security issues. They raise alerts when detecting suspicious activities. SOAR (Security Orchestration, Automation, and Response) systems, on the other hand, focus on automating and orchestrating incident response processes. They automate investigation path workflows and reduce the time spent on alerts by executing predefined actions and workflows in response to security events or incidents. References: The differences between SIEM and SOAR are highlighted in various cybersecurity resources, including those provided by Palo Alto Networks and Exabeam, which explain that while SIEM primarily focuses on collecting and analyzing security event data, SOAR extends these capabilities through automation, orchestration, and predefined incident response playbooks

質問: **11**
展示品を参照してください。



この出力は何を示していますか?

A. サーバー上で HTTPS ポートが開いています。
B. サーバーの SMB ポートが閉じられています。
C. サーバーの FTP ポートが開いています。
D. サーバーの電子メール ポートが閉じられています。
正解**: D (**コメントを発表する**)**
What Are Ports 139 And 445? SMB has always been a network file sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems. SMB uses either IP port
139 or 445. Port 139 - SMB originally ran on top of NetBIOS using port 139. NetBIOS is an older transport layer that allows Windows computers to talk to each other on the same network. Port 445 - Later versions of SMB (after Windows 2000) began to use port 445 on top of a TCP stack. Using TCP allows SMB to work over the internet. https://www.varonis.com/blog/smb-port SMB Ports 139 and 445 are open Email Ports 25 and 110 are closed Therefore "D. Email Ports are closed on the Server."

質問**: 12**
ゼロトラスト セキュリティ モデルは何を意味しますか?
A. ゼロトラスト セキュリティとは、デフォルトではネットワーク内外から誰も信頼されないことを意味します
B. ゼロトラストでは、システムを自ら悪用するのに十分な権限をユーザーに与えるべきではないと述べています
C. ゼロ トラストはアクセス制御に対処し、個人は特定のタスクを実行するために必要な最小限のアクセス権限のみを持つべきであると規定します。
D. ゼロトラストでは、サブジェクトにオブジェクトへの明示的なアクセス権が与えられない限り、そのオブジェクトへのアクセスを拒否する必要があると述べています。
正解**: A (**コメントを発表する**)**

質問: **13**
組織内で特定の役割を遂行するために必要な権限のみを従業員に与える慣行は何ですか?
A. 最小権限
B. 知る必要がある
C. 完全性の検証
D. デューデリジェンス
正解: **(**正解を表示します**)**
The principle of least privilege states that users and processes should be granted only the minimum permissions necessary to perform their specific role or function within an organization. This reduces the attack surface and limits the potential damage of a compromised account or process. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.2: Security Principles Cisco Certified CyberOps Associate Overview, Exam Topics, 1.1 Explain the CIA triad

質問: **14**
エンジニアは、1 週間前にインシデント管理チームからのインシデントのチケットの作成に取り組んでいます。外部 Web アプリケーションが DDoS 攻撃の対象となった サーバー リソースが枯渇し、2 時間後にクラッシュしました。エンジニアは攻撃者と使用された手法を特定できました 攻撃から 3 時間後にサーバーは復旧し、エンジニアはブラックホール フィルタリングによる軽減策の実装を推奨し、インシデント チケットを IR チームに返送しました NIST SP800-61 によると、どの段階でインシデント対応のエンジニアは仕事を終えましたか?
A. 準備
B. インシデント後のアクティビティ
C. 封じ込めの根絶と回復
D. 検出と分析
正解: **C (**コメントを発表する**)**
According to NIST SP800-61, the incident response phase called "Containment, Eradication, and Recovery" involves containing the incident, eradicating the threat, and recovering from the incident2. In the scenario described, the engineer worked on containing the DDoS attack by identifying the attacker and the technique used, which is part of the containment process. The recommendation to implement Blackhole filtering is part of the eradication process, where measures are taken to prevent the attack from happening again. Finally, restoring the server is part of the recovery process, where normal operations are resumed. Therefore, the engineer finished work during the "Containment, Eradication, and Recovery" phase. References: NIST SP800-61 Computer Security Incident Handling Guide2.

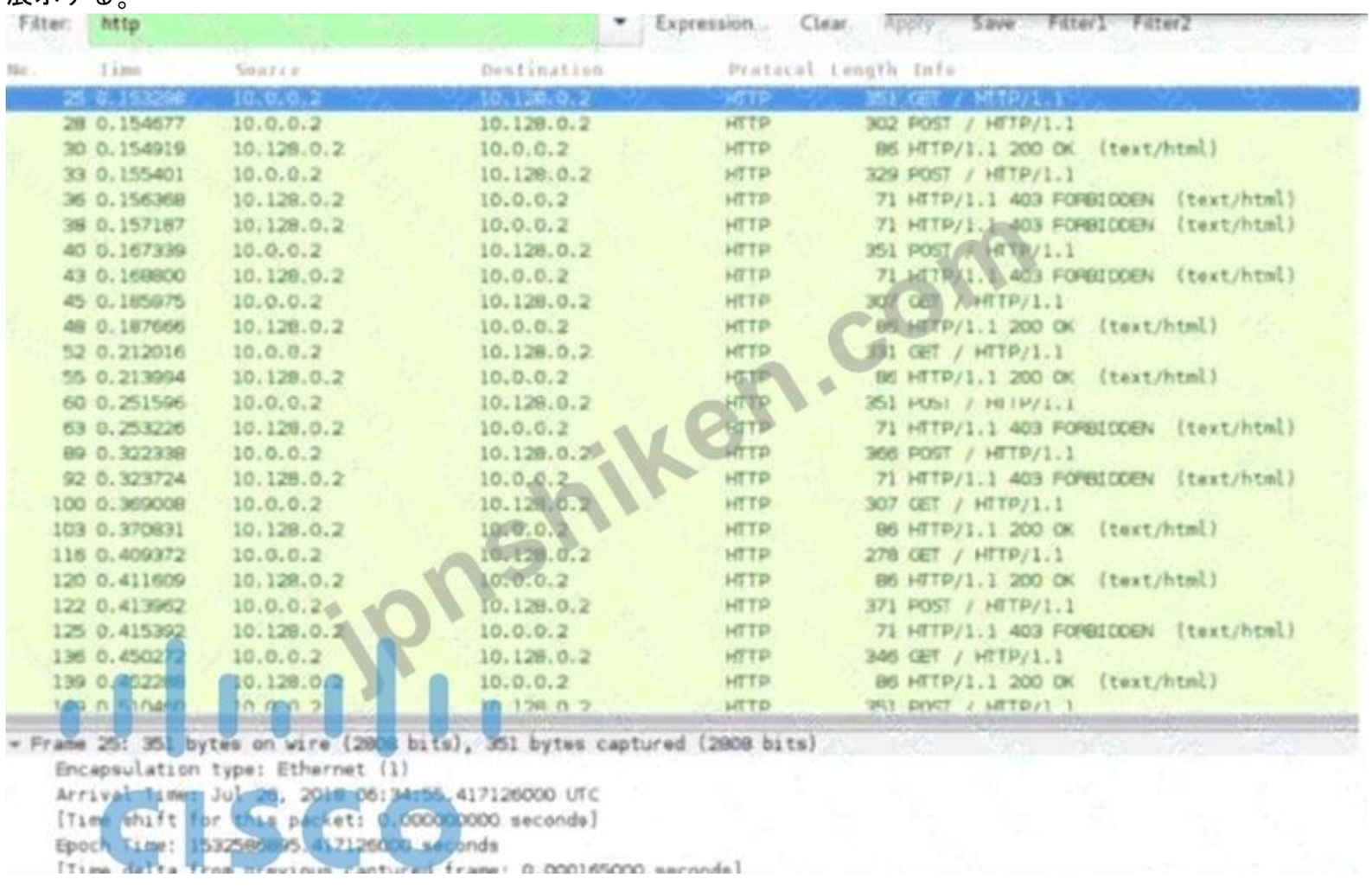
質問: **15**
Windows プロセスの仮想アドレス空間とは何ですか?
A. メモリ内のオブジェクトの物理的な位置
B. 物理メモリに常駐するページのセット
C. オペレーティング システムに組み込まれたシステム レベルのメモリ保護機能
D. 使用可能な仮想メモリ アドレスのセット
正解: **D (**コメントを発表する**)**
The virtual address space for a Windows process is the set of virtual memory addresses that can be used by the process. Each process has its own virtual address space that is isolated from other processes. The virtual address space is divided into regions that have different attributes, such as read-only, read-write, execute, and so on. The virtual address space is mapped to the physical memory by the operating system using a data structure called a page table. References:

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 4: Host-Based Analysis, Lesson 4.1: Windows Operating System Virtual Address Space

質問: **16**
調査における侵害指標の役割は何ですか?
A. 攻撃がなぜ発生したのかという疑問に答えるのに役立ちます。
B. システムまたはネットワーク上の潜在的に悪意のあるアクティビティを識別します。
C. 非フォレンジックデータなので、簡単に検出できます。
D. 何が、なぜ起こったのかを説明します。
正解: **B** (コメントを発表する)

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
展示する。



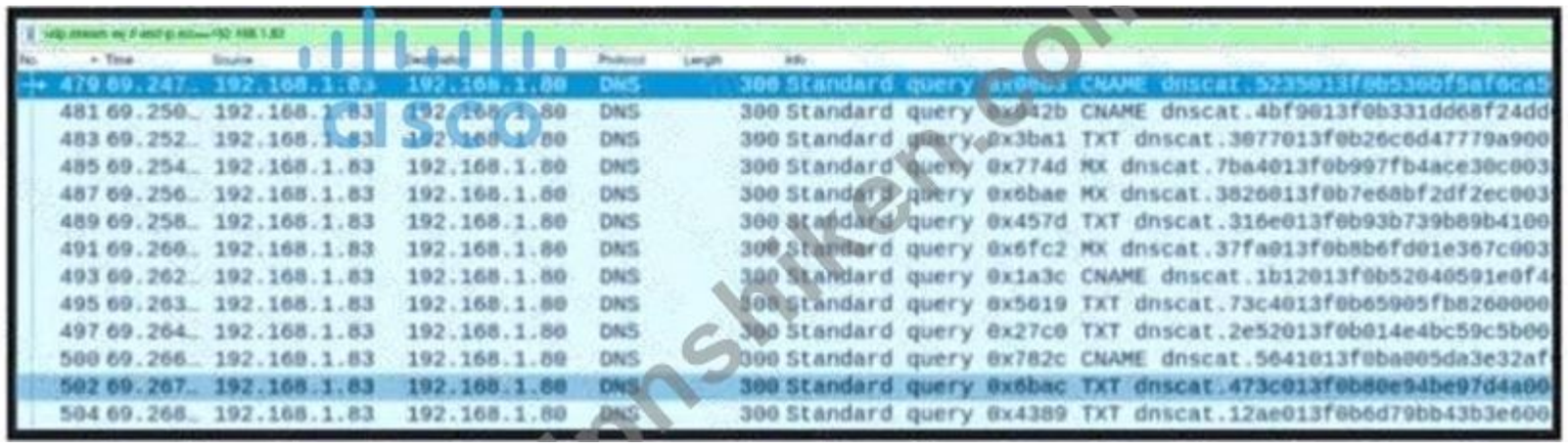
エンジニアは、Web アプリケーションの速度低下に関するチケットを受け取り、トラフィックの薬物分析を行ったところ、Web サーバーに対する攻撃の可能性を疑いました。エンジニアは Wiresharat トラフィック キャプチャをどのように解釈すべきですか?
A. 10.0.0.2 は GET/HTTP/1.1 および Post リクエストを送信し、ターゲットは HTTP/1.1 で応答します。したがって、200 OC および HTTP/1.1 403。これは HTTP フラッドの試みです。
B. 10.0.0.2 は HTTP FORBIDDEN /1.1 And Post リクエストを送信しますが、ターゲットは HTTP/1.1 200 Get および HTTP/1.1 403 で応答します。これは HTTP GET フラッド攻撃です。
C. 10.128.0.2 は POST/1.1 および POST リクエストを送信し、ターゲットはそれに応じて HTTP/1.1 200 Ok および HTTP/1.1 403 で応答します。これは HTTP 予約帯域幅のフラッドです。
D. 10.128.0.2 は HTTP/FORBIDDEN/ 1.1 および Get リクエストを送信し、ターゲットは HTTP/1.1 200 OK および HTTP/1.1 403 で応答します。これは HTTP キャッシュ バイパス攻撃です。
正解**: B (**コメントを発表する**)**
When analyzing Wireshark traffic for potential attacks, an engineer should look for patterns that indicate abnormal behavior, such as:
Excessive Requests: A high number of requests over a short period could suggest an attempt to overwhelm the server, known as an HTTP flood.
Status Codes: Repeated 403 Forbidden responses may indicate that the server is rejecting requests due to a security rule being triggered.
Request Types: A mix of GET and POST requests could be used in various attack scenarios, including bandwidth flooding or cache bypassing.

質問**: 18**
展示品を参照してください。

```
<IMG SRC=j%41vascript:alert(‘attack’)>
```

この文字列にはどのような攻撃方法が描かれているのでしょうか?
A. クロスサイトスクリプティング
B. 中間者攻撃
C. SQLインジェクション
D. サービス拒否
正解**: A (**コメントを発表する**)**
The image shows a piece of code within a bordered rectangular area.
It is a string of HTML code that appears to be an example of an attack, specifically "<IMG SRC=j%
41vascript:alert('attack')>".
The code suggests an attempt to execute JavaScript within an image source attribute, indicative of a cross-site scripting attack.

質問**: 19**



No.	Time	Source	Destination	Protocol	Length	Info
479	69.247…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x6ba3 CNAME dnscat.5235013f0b536bf5af6ca5
481	69.250…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x942b CNAME dnscat.4bf9013f0b331dd68f24dd
483	69.252…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x3ba1 TXT dnscat.3077013f0b26c6d47779a900
485	69.254…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x774d MX dnscat.7ba4013f0b997fb4ace30c003
487	69.256…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x6bae MX dnscat.3820013f0b7e68bf2df2ec003
489	69.258…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x457d TXT dnscat.316e013f0b93b739b89b4100
491	69.260…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x6fc2 MX dnscat.37fa013f0b8b6fd01e367c003
493	69.262…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x1a3c CNAME dnscat.1b12013f0b52040591e0f4
495	69.263…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x5619 TXT dnscat.73c4013f0b65905fb8260000
497	69.264…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x27c0 TXT dnscat.2e52013f0b014e4bc59c5b00
500	69.266…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x782c CNAME dnscat.5641013f0ba005da3e32af
502	69.267…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x6bac TXT dnscat.473c013f0b80e94be97d4a00
504	69.268…	192.168.1.83	192.168.1.80	DNS	300	Standard query 0x4389 TXT dnscat.12ae013f0b6d79bb43b3e600

添付資料を参照してください。ネットワークエンジニアは、あるホストがインターネット上の不明なドメインと通信しているという報告を受けました。ネットワークエンジニアはパケットキャプチャを収集しましたが、使用された手法やペイロードを特定できませんでした。攻撃者はどのような手法を使用しているのでしょうか？

A. ティアドロップ
B. セッションハイジャック
C. トンネリング
D. 増幅
正解: **C** (コメントを発表する)

質問: **20**
インシデント対応計画とは何ですか？
A. 資産の損失や業務の中断につながる可能性のあるイベントへの組織的なアプローチ
B. サービスライフサイクルと継続的な改善を確実にするためのセキュリティ管理への組織的アプローチ
C. ディザスタリカバリと運用サービスのタイムリーな復旧への組織的なアプローチ
D. 規制に沿ったシステムバックアップとデータアーカイブへの組織的アプローチ
正解: (正解を表示します)
An incident response plan is a document that defines the roles and responsibilities, procedures, and processes for detecting, analyzing, containing, eradicating, recovering, and learning from security incidents. The purpose of an incident response plan is to minimize the impact of incidents on the organization's assets, operations, and reputation, and to restore normal operations as quickly as possible. An incident response plan is not the same as a security management plan, a disaster recovery plan, or a backup and archiving plan, although they may be related or complementary. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 92; NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, page 2-3

質問: **21**
すべての小文字のみに一致する正規表現はどれ?
A. [az]+
B. [^az]+
C. az+
D. a*z+
正解: **A** (コメントを発表する)
The regex [a#z]+ matches one or more lowercase letters from a to z. The plus sign (+) indicates that the preceding character set [a#z] can appear one or more times, thus matching strings of only lowercase letters1.

References := This explanation is consistent with standard regex syntax as described in various programming and scripting languages documentation

質問: **22**
調査中の情報管理の対象となる情報はどれですか?
A. 証拠を集めていた会社
B. 重要な資産のリスト
C. 証拠収集の方法
D. 脆弱な資産のリスト
正解: **(**正解を表示します**)**

質問: **23**
ステートフルパケットインスペクションとディープパケットインスペクションの2つの違いは何ですか？ 2つ選択してください）
A. ステートフルインスペクションはTCP状態追跡が可能であり、ディープパケットフィルタリングはTCP送信元ポートと宛先ポートのみをチェックします
B. ディープパケットインスペクションはマルウェアをブロックできますが、ステートフルインスペクションはできません
C. ディープパケットインスペクションはレイヤー3および4で動作し、ステートフルインスペクションはOSIモデルのレイヤー3で動作します
D. ディープパケットインスペクションはTCP状態監視のみが可能であり、ステートフルインスペクションはTCPとUDPを検査できます。
E. ステートフルインスペクションはパケットデータインスペクションが可能ですが、ディープパケットインスペクションはできません
正解: **(**正解を表示します**)**
A: Stateful inspection tracks the state of network connections, such as TCP streams, to determine if a packet is part of an established connection.
B: Deep packet inspection examines the data part (payload) of a packet and can identify, block, or reroute packets with specific types of malware. Stateful inspection does not inspect the payload for malware.

質問: **24**

```
13:52:21  sshd[2346]: Connection closed by 10.10.10.10 [preauth]
13:52:21  sshd[2346]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:21  sshd[2349]: Failed password for root from 10.10.10.10 port 57654 ssh2
13:52:21  sshd[2349]: Connection closed by 10.10.10.10 [preauth]
13:52:21  sshd[2349]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:22  sshd[2351]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:24  sshd[2351]: Failed password for root from 10.10.10.10 port 57656 ssh2
13:52:24  sshd[2351]: Connection closed by 10.10.10.10 [preauth]
13:52:24  sshd[2353]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:24  sshd[2355]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:26  sshd[2353]: Failed password for root from 10.10.10.10 port 57658 ssh2
13:52:26  sshd[2353]: Connection closed by 10.10.10.10 [preauth]
13:52:26  sshd[2355]: Failed password for root from 10.10.10.10 port 57660 ssh2
13:52:26  sshd[2355]: Connection closed by 10.10.10.10 [preauth]
13:52:28  sshd[2357]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:28  sshd[2358]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:30  sshd[2358]: Failed password for root from 10.10.10.10 port 57664 ssh2
13:52:30  sshd[2357]: Failed password for root from 10.10.10.10 port 57662 ssh2
13:52:30  sshd[2358]: Connection closed by 10.10.10.10 [preauth]
13:52:30  sshd[2357]: Connection closed by 10.10.10.10 [preauth]
13:52:32  sshd[2362]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:32  sshd[2361]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:34  sshd[2362]: Failed password for root from 10.10.10.10 port 57668 ssh2
13:52:34  sshd[2361]: Failed password for root from 10.10.10.10 port 57666 ssh2
13:52:34  sshd[2362]: Connection closed by 10.10.10.10 [preauth]
13:52:34  sshd[2361]: Connection closed by 10.10.10.10 [preauth]
13:52:35  sshd[2365]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:36  sshd[2367]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:38  sshd[2365]: Failed password for root from 10.10.10.10 port 57670 ssh2
13:52:38  sshd[2367]: Failed password for root from 10.10.10.10 port 57672 ssh2
13:52:38  sshd[2365]: Connection closed by 10.10.10.10 [preauth]
13:52:38  sshd[2367]: Connection closed by 10.10.10.10 [preauth]
13:52:50  sshd[2372]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:50  sshd[2370]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.10  user=root
13:52:52  sshd[2372]: Failed password for root from 10.10.10.10 port 57676 ssh2
13:52:52  sshd[2370]: Failed password for root from 10.10.10.10 port 57674 ssh2
13:52:52  sshd[2370]: Connection closed by 10.10.10.10 [preauth]
13:52:52  sshd[2372]: Connection closed by 10.10.10.10 [preauth]
```

展示を参照してください。SOC アナリストが侵害されたシステムの 1 つの Auth.log ファイル ログを調査しています。このイベント ログの考えられる理由は何ですか?

A. 10.10.10.10 からの Linux へのブルートフォース攻撃

B. Windows 10.10.10.10 からのブルートフォース攻撃

C. 通常のLinuxログで、10.10.10.10は正当なホストです

D. WindowsエンドポイントIに対するパスワードクラッキングDoS攻撃

正解: **(**正解を表示します**)**

質問: **25**

ループバック IP アドレス (127.0.0.1) に一致する正規表現はどれですか?

A. %127.0.0.1%

B. 127\.0\.0\.1

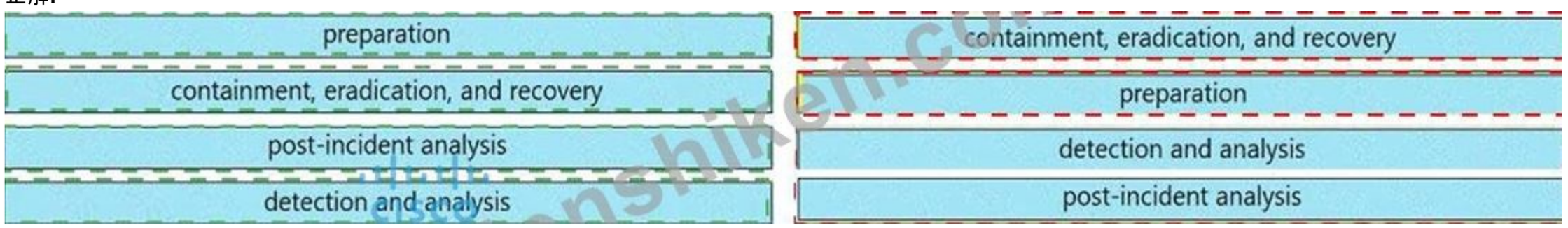
C. 127[.0.].0.\

D. &127%0%0%1
正解: **(**正解を表示します**)**

質問: **26**
左の要素を右のインシデント処理の正しい順序にドラッグ アンド ドロップします。



正解:



Explanation:
A close-up of several blue rectangular boxes Description automatically generated



質問: **27**
エンジニアは、監視のために様々なネットワークデバイスからデータを収集する必要があります。エンジニアはローカルネットワークからイベントを収集し、その情報をパケットスニッフィングに利用する必要があります。ソリューションはトラフィックの正確なコピーを作成し、完全な忠実性を提供する必要があります。エンジニアはどのソリューションを使用すべきでしょうか？
A. NAT
B. タップ
C. SPANポート
D. トンネリング
正解: **B (**コメントを発表する**)**
A network TAP (Test Access Point) is a hardware device designed to create an exact, full-fidelity copy of network traffic for monitoring and packet analysis. TAPs operate at the physical layer and replicate all packets-including errors and malformed frames-without dropping traffic.

This makes TAPs ideal for packet sniffing, intrusion detection, and forensic analysis where accuracy and completeness are critical. TAPs do not rely on switch resources and do not introduce packet loss during periods of high traffic.
SPAN (mirror) ports can also copy traffic but are dependent on switch processing capacity and may drop packets during congestion, making them unreliable for full-fidelity capture. NAT modifies traffic, and tunneling encapsulates data rather than copying it.
Cybersecurity operations documentation consistently identifies TAPs as the preferred solution when exact traffic replication is required.
Therefore, the correct answer is tap.

質問: **28**
アナリストが SOC 環境でのインシデントを調査しています。ログのグループからセッションを識別するために使用される方法はどれですか?
A. シーケンス番号
B. IP 識別子
C. タイムスタンプ
D. 5タプル
正解: **D (**コメントを発表する**)**

質問: **29**
エンジニアが侵害を発見し、脅威の侵入ポイントを特定して、アクセスを削除しました。エンジニアは、ホスト、脅威アクターの IP アドレス、および脅威アクターが標的としたアプリケーションを特定できました。NIST SP 800-61 インシデント処理ガイドに従って、エンジニアが取るべき次のステップは何ですか?
A. 脅威から回復します。
B. 脅威を分析します。
C. 脅威から学んだ教訓を特定します。
D. 類似の脅威の可能性を減らします。
正解: **A (**コメントを発表する**)**
After a breach has been discovered and the immediate threat has been addressed by identifying and removing the threat's access, the next step according to the NIST SP 800-61 Incident Handling Guide is to recover from the threat. This involves restoring systems to normal operation, confirming that the systems are functioning normally, and applying patches or other remediation measures to prevent similar breaches in the future1.
References :=
* Understanding NIST SP 800-61: The Computer Security Incident Handling Guide

質問: **30**
展示を参照してください。

```
GET /item.php?id=34' or sleep(10)
```

この要求は、データベースによって駆動される Web アプリケーション サーバーに送信されました。どのタイプの Web サーバー攻撃が表されますか?
A. ブラインド SQL インジェクション
B. ヒープメモリの破損
C. パラメータ操作
D. コマンドインジェクション
正解: **A (**コメントを発表する**)**

質問: **31**
公開鍵インフラストラクチャ (PKI) とは何ですか?
A. PKI はユーザーと送信者の ID を検証し、対称暗号化を使用して安全な通信チャネルを作成します。
B. PKI はパケット損失を防止し、非対称暗号化を使用して安全な通信チャネルを作成します。
C. PKI はユーザーと送信者の ID を検証し、非対称暗号化を使用して安全な通信チャネルを作成します。
D. PKI はパケット損失を防止し、対称暗号化を使用して安全な通信チャネルを作成します。
正解: **(**正解を表示します**)**

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
最初の証拠から生じる理論または仮定を支持する証拠のタイプはどれですか?
A. 確率論的
B. 間接
C. 最高
D. 確証的
正解: **(**正解を表示します**)**
Corroborative evidence is the type of evidence that supports a theory or an assumption that results from initial evidence. It provides additional support to the initial findings, strengthening the theory or assumption by confirming the same facts or pointing towards the same conclusion with independent pieces of evidence4567. References := Types of evidence (article) | Lessons | Khan Academy, Evidence: Fundamental Concepts and the Phenomenal Conception, Navigating Scientific Evidence: Types and Definitions, How Courts Work - American Bar Association

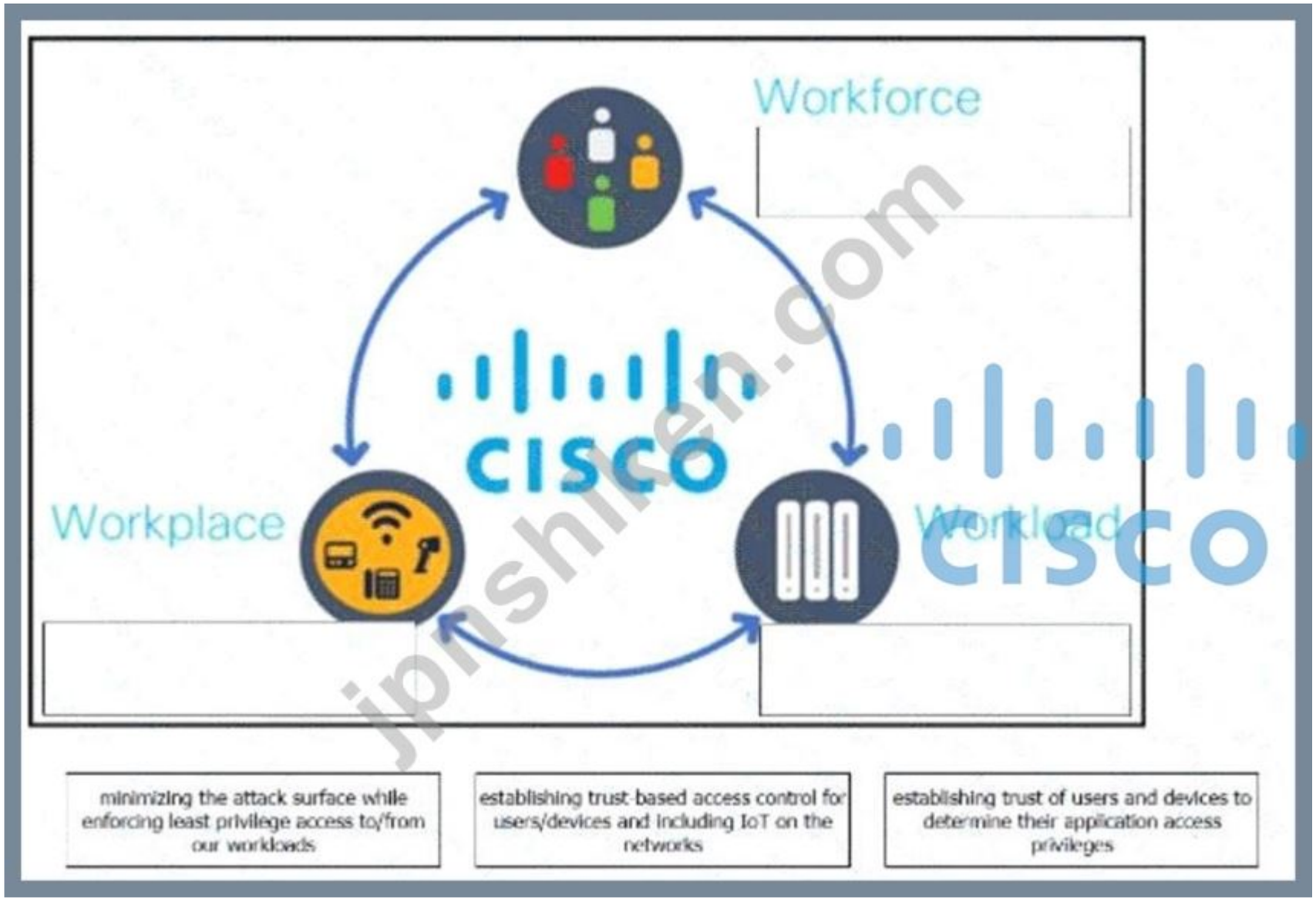
質問: **33**
脆弱性管理とは何ですか？
A. 侵入ポイントの明確化と狭小化に焦点を当てたセキュリティ慣行。
B. 脅威を認めるのではなく、アクションを実行するセキュリティ慣行。
C. 既存の弱点を特定して修正するプロセス。
D. サービスの中断から回復し、ビジネスクリティカルなアプリケーションを復元するプロセス
正解: **(**正解を表示します**)**
Vulnerability management is a proactive approach to securing systems by identifying and fixing vulnerabilities before they can be exploited by attackers. It involves scanning systems for known weaknesses, prioritizing and assessing the risks of those vulnerabilities, and applying patches or other remediation measures to mitigate them. Vulnerability management helps reduce the attack surface and prevent potential breaches. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 11.
Reference:https://www.brinqa.com/vulnerability-management-primer-part-2-challenges/

質問: **34**

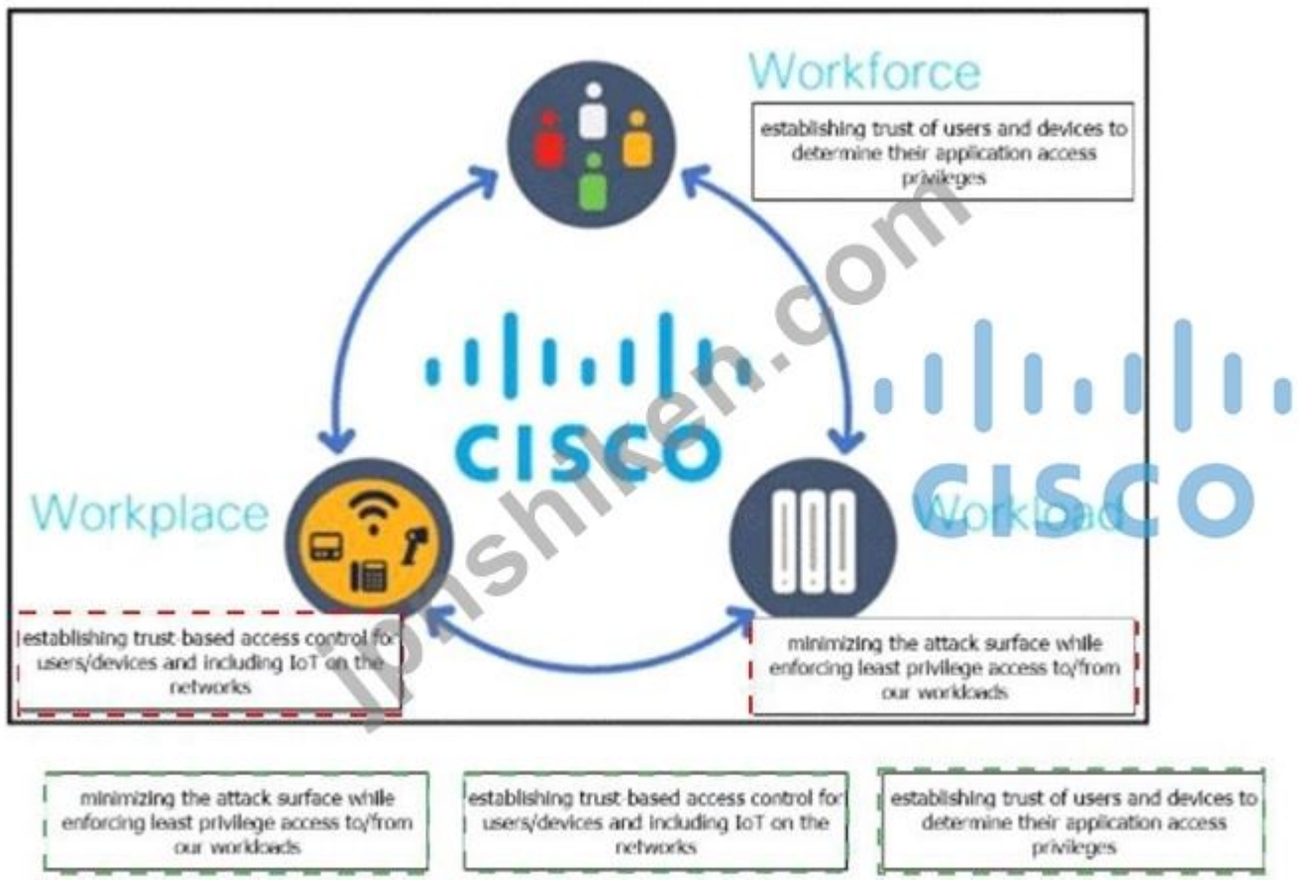
法医学調査において、改ざんされたディスク イメージと改ざんされていないディスク イメージの主な違いは何ですか?
A. 改ざんされていない画像は暗号化され、改ざんされた画像は暗号化されません。
B. 改ざんされた画像はハッシュ値が異なり、改ざんされていない画像はハッシュ値が変更されていません。
C. 改ざんされたイメージには管理者のみがアクセスでき、改ざんされていないイメージにはすべてのユーザーがアクセスできます。
D. 改ざんされていない画像は圧縮され、改ざんされた画像は圧縮されません。
正解: **(**正解を表示します**)**
In digital forensics, hash values are used to verify the integrity of disk images. When a disk image is created, cryptographic hash functions such as MD5 or SHA-256 are calculated and recorded. These hashes act as a digital fingerprint of the data at the time of acquisition.
An untampered disk image maintains the same hash value throughout the investigation, proving that the data has not been altered. A tampered disk image, however, will produce a different hash value because even the smallest modification to the data changes the resulting hash. This difference immediately indicates that the integrity of the evidence has been compromised.
Options A, C, and D are incorrect because encryption, access permissions, and compression do not define whether an image is tampered. Cybersecurity and forensic documentation consistently emphasizes hash verification as the primary method for validating forensic integrity.
Therefore, the key difference is that a tampered image has a different hash value, making Option B correct.

質問: **35**
フォレンジックプロセスのどのフェーズで、収集されたデータから情報を抽出するためのツールと手法が使用されますか？
A. 調査
B. 試験
C. レポート
D. コレクション
正解: **(**正解を表示します**)**
During the examination phase of the forensic process, digital forensic investigators use various tools and techniques to extract and analyze information from the collected data. This phase involves detailed scrutiny of the data to uncover relevant evidence and is critical for the success of the forensic investigation.
The explanation aligns with the standard phases of digital forensics, which include identification, preservation, examination, documentation, and presentation as outlined in digital forensics literature and guidelines.

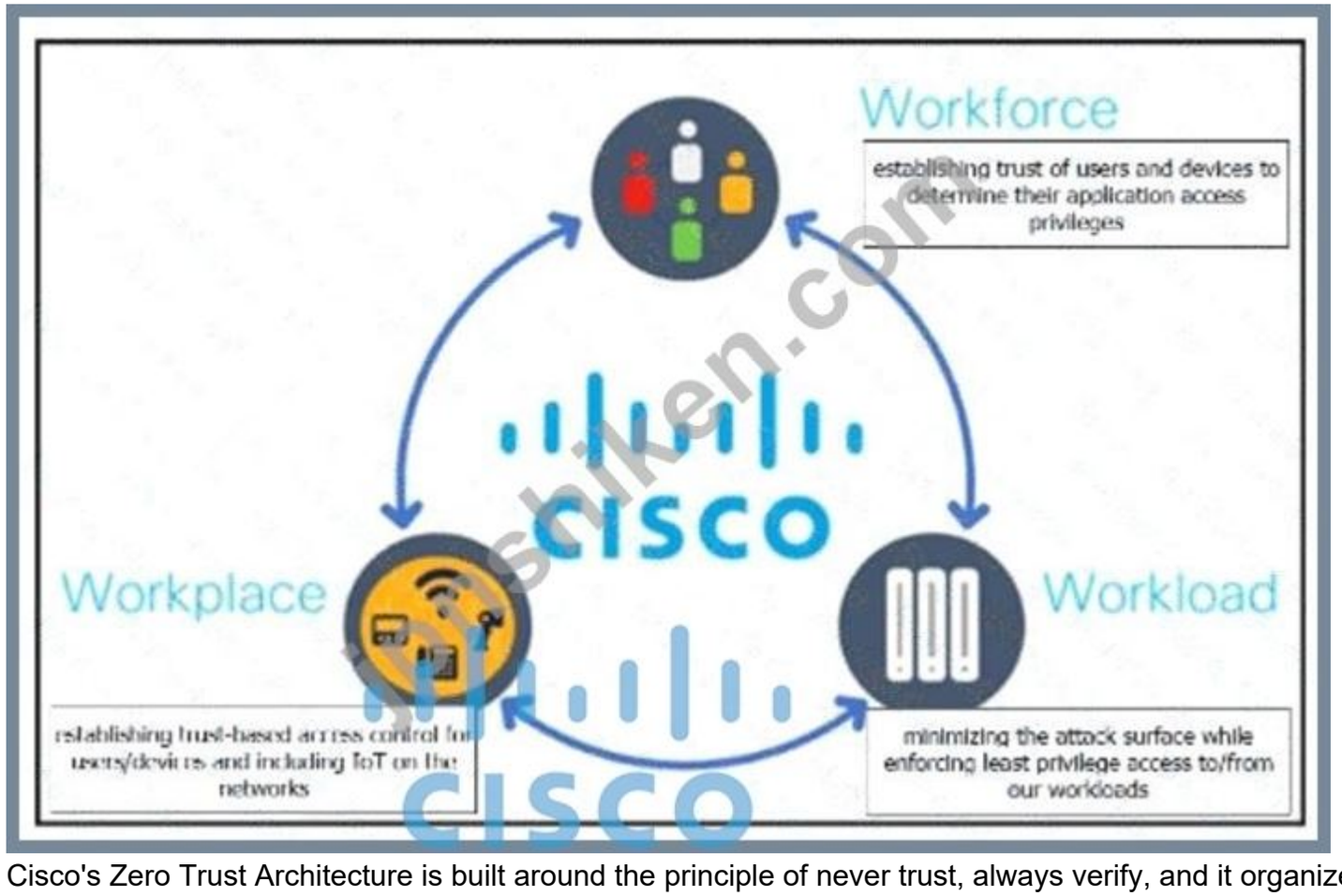
質問: **36**
Cisco Zero Trust アーキテクチャは、ゼロトラストの道のりを3つの重要な領域に簡素化します。定義を図にドラッグ＆ドロップして、シスコの視点からゼロトラストを説明してください。


Workforce
Workplace
Workload
CISCO
minimizing the attack surface while enforcing least privilege access to/from our workloads
establishing trust-based access control for users/devices and including IoT on the networks
establishing trust of users and devices to determine their application access privileges

正解:



Explanation:



Cisco's Zero Trust Architecture is built around the principle of never trust, always verify, and it organizes zero trust controls into three interconnected domains: Workforce, Workplace, and Workload. Each domain addresses a different aspect of access control and risk reduction.

The Workforce pillar focuses on user identity and endpoint posture. Cisco zero trust ensures that users and their devices are continuously verified before granting access to applications. This includes validating identity, device health, and context to determine appropriate access privileges.
The Workplace pillar addresses the network environment where users and devices connect. This includes enterprise networks, branch offices, and IoT environments. Cisco applies trust-based access controls to ensure that only authorized and compliant devices can communicate on the network, regardless of location.
The Workload pillar protects applications and services running in data centers, cloud environments, and containers. The goal is to reduce the attack surface by enforcing least-privilege access, ensuring that workloads only communicate with explicitly authorized services and users.
Cybersecurity operations documentation emphasizes that effective zero trust requires visibility and enforcement across all three areas. Cisco's model simplifies implementation by clearly defining responsibilities and controls within each domain, enabling organizations to reduce lateral movement, limit blast radius, and improve overall security posture.

質問: **37**
エンドポイントの攻撃対象領域を減らす 2 つのコンポーネントはどれですか? (2つ選んでください。)
A. セキュア ブート
B. 負荷分散
C. 監査ログ レベルの増加
D. USB ポートの制限
E. エンドポイントでの完全なパケット キャプチャ
正解: **(正解を表示します)**
Secure boot and restricting USB ports are two components that can reduce the attack surface on an endpoint.
The attack surface is the sum of all paths for data into and out of the environment. Reducing the attack surface means minimizing the number and complexity of these paths, and thus reducing the opportunities for attackers to exploit vulnerabilities or gain unauthorized access. Secure boot is a feature that ensures that only trusted and verified code can run during the boot process, preventing malware or unauthorized software from compromising the system. Restricting USB ports is a policy that limits the use of USB devices, such as flash drives or external hard drives, that can introduce malware or exfiltrate data from the endpoint.
[Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 4: Network Intrusion Analysis], [Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 5: Security Policies and Procedures]

質問: **38**
統計的検出とルールベースの検出モデルの違いは何ですか?
A. ルールベースの検出には、一定期間における正当なユーザーの行動に関連するデータの収集が含まれます。
B. 統計的検出は一定期間のユーザーの正当なデータを定義し、ルールベースの検出はそれをIF/THENベースで定義します
C. 統計的検出には、オブジェクトがその動作を実行する前に、その意図した動作に関するオブジェクトの評価が含まれます。
D. ルールベースの検出は、一定期間にわたるユーザーの正当なデータを定義し、統計的検出は、IF/THEN ベースでそれを定義します。
正解: **(正解を表示します)**
Statistical detection involves collecting data over time to define what is considered normal behavior or legitimate data for users or systems. It then uses statistical analysis to identify abnormal behavior that could indicate a security incident. Rule-based detection uses predefined rules or patterns that are based on known threats or vulnerabilities - it operates on an IF/THEN basis where if certain conditions are met then an alert is triggered. References := Cisco Cybersecurity Operations Fundamentals

質問: **39**



添付資料を参照してください。従業員が不明な送信者から添付ファイル付きのメールを受信し、フィッシング詐欺として報告しました。エンジニアは詳細な分析のためにそのファイルをCuckooにアップロードしました。エンジニアはCuckooから提供されたレポートから何を解釈すべきでしょうか？

A. Win32.polip.a.exe は実行可能ファイルであり、悪意のあるファイルとしてフラグが付けられる必要があります。

B. ファイルはクリーンであり、リスクはありません。

C. Cuckoo は悪意のあるファイルをクリーンアップし、使用できるように準備しました。

D. ファイルの MD5 は悪意のあるものとして識別されませんでした。

正解: **(**正解を表示します**)**

The Cuckoo report indicates that the file is a PE32 executable for MS Windows, which is typically an executable file format. The presence of the watermark "CHINESEDUMPS" and the detection ratio from VirusTotal suggest that the file is recognized by multiple antivirus engines as potentially harmful. This aligns with option A, suggesting that the file, named Win32.polip.a.exe, should be considered malicious and flagged accordingly.

The information provided is based on standard practices for analyzing potentially malicious files using tools like Cuckoo and services like VirusTotal, which are commonly referenced in cybersecurity documentation, including Cisco's cybersecurity training materials.

質問: **40**

NetFlow ログ セッションの ACK フラグと RST フラグの違いは何ですか?

A. RST フラグは TCP 接続の開始を確認し、ペイロードのデータが完了すると ACK フラグが応答します。

B. ACK フラグは TCP 接続の開始を確認し、ペイロードのデータが完了すると RST フラグが応答します。

C. RST フラグは前のセグメントの受信を確認し、ACK フラグは接続の自発的な終了を可能にします

D. ACK フラグは前のセグメントの受信を確認し、RST フラグは接続の自発的な終了を可能にします

正解: **D (**コメントを発表する**)**

In NetFlow log sessions within TCP connections; ACK flag is used for acknowledging that data has been successfully received while RST flag is used when there's an error or when closing a connection spontaneously without following standard procedures. References := Cisco Cybersecurity source documents or study guide

質問: **41**

展示品を参照してください。



エンジニアは、Web アプリケーションの速度低下に関するチケットを受け取りました。エンジニアは #netstat -an コマンドを実行します。エンジニアは結果をどのように解釈する必要がありますか?

A. Webアプリケーションは一般的な正当なトラフィックを受信しています

B. エンジニアはより多くのデータを収集する必要があります。

C. Web アプリケーション サーバーがサービス拒否攻撃を受けています。

D. サーバーは、Web アプリケーションとそのデータベースの間で中間者攻撃を受けています。

正解: **(**正解を表示します**)**

The #netstat -an command output typically displays a list of all open ports and associated connections. If the web application is slowed down, the engineer would look for unusual patterns such as an excessive number of connections to the web server which could indicate a denial-of-service attack. However, without specific details from the #netstat -an output, it's not possible to determine the exact cause of the issue. Therefore, the engineer would need to gather more data, possibly including checking server logs, resource usage, and network traffic patterns to diagnose the problem accurately.

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) provides knowledge on network monitoring tools and interpreting their output to identify potential security incidents.

質問: **42**

スライディング ウィンドウの異常検出とは何ですか?

A. 運用および管理プロセスの変化を検出します。

B. 通常の動作に合わない珍しいパターンを特定します。

C. 所有するアプリケーションのリクエストの応答時間を定義します。

D. 最も低い特権/許可レベルをソフトウェアに適用します

正解: **(**正解を表示します**)**

Sliding window anomaly detection is a technique used in cybersecurity to identify unusual patterns or behaviors that deviate from the norm. It involves analyzing segments of data over a period of time, referred to as a 'window,' and comparing them against typical patterns. Anomalies are detected when observed behaviors significantly differ from expected patterns, indicating potential security incidents or issues that require further investigation. References: An adaptive sliding window for anomaly detection of time series in wireless sensor networks

質問: **43**

エンジニアは、既知の TOR 出口ノードを持つトラフィックがネットワーク上で発生したというセキュリティ アラートを受け取ります。

このトラフィックの影響は?
A. 感染後に通信するランサムウェア
B. 著作権で保護されたコンテンツをダウンロードするユーザー
C. データ流出
D. ユーザーによるファイアウォールの回避
正解: **(**正解を表示します**)**
Traffic with a known TOR exit node is often associated with data exfiltration, where sensitive information is transferred from within the network to an external location. TOR networks are used to anonymize the traffic, making it difficult to trace back to the source. References := Cisco Cybersecurity Operations Fundamentals - Module 2: Security Monitoring

質問: **44**
フォレンジック プロセスのどの段階で、特定のイベントに関連するデータがラベル付けされ、その整合性を維持するために記録されますか?
A. 審査
B. 調査
C. コレクション
D. 報告
正解: **(**正解を表示します**)**
During the collection phase of the forensic process, data related to a specific event is labeled and recorded to preserve its integrity. This step ensures that the data remains unaltered and authentic from the time of collection until it is presented as evidence, maintaining the chain of custody. References := Cisco Cybersecurity Operations Fundamentals - Module 6: Security Incident Investigations

質問: **45**
脅威とエクスプロイトの違いは何ですか？
A. 脅威はシステム内のフローを利用した結果であり、エクスプロイトはシステムを制御した結果です。
B. 脅威は資産に対する潜在的な攻撃であり、エクスプロイトは資産の脆弱性を利用します
C. エクスプロイトは攻撃ベクトルであり、脅威は攻撃が通過しなければならない潜在的な経路です。
D. エクスプロイトは攻撃パスであり、脅威は潜在的な脆弱性を表します
正解: **B (**コメントを発表する**)**
A threat is a possible danger that might exploit a vulnerability to breach the security and cause harm to an asset. An asset is anything of value that needs to be protected, such as data, systems, or networks. A vulnerability is a weakness or flaw in the security that can be exploited by a threat. An exploit is a piece of code or a technique that takes advantage of a vulnerability to compromise the security and perform malicious actions on an asset. References := Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.1: The CIA Triad and Security Concepts, Topic 1.1.3: Threats, Vulnerabilities, and Exploits

質問: **46**
ユーザーは「Hr405-report2609-empl094.exe」という名前の電子メールの添付ファイルを受け取りましたが、実行しませんでした。このタイプのイベントには、サイバーキルチェーンのどのカテゴリを割り当てる必要がありますか？
A. インストール
B. 偵察
C. 兵器化
D. 配達

正解: (正解を表示します)
Delivery is the fourth phase of the cyber kill chain, which is a model to describe the stages of a cyberattack.
Delivery refers to the transmission of the weaponized payload to the target system, such as via email attachments, web links, USB drives, or network connections.
Delivery does not necessarily imply successful installation or execution of the payload, which are subsequent phases of the kill chain. References :
= Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 31.

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu **564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
改ざんされたディスクイメージと改ざんされていないディスクイメージの違いは何ですか?
A. 改ざんされたイメージには、同じ保存および計算されたハッシュが含まれます。
B. 改ざんされた画像が証拠として使用されます。
C. 改ざんされていないイメージはフォレンジック調査に使用されます。
D. 改ざんされていない画像は証拠として保存するために意図的に変更されています
正解: (正解を表示します)
Tampered images are disk images that have been modified or altered in some way after they were captured from the original source. Tampered images may have different stored and computed hash values, which indicate that the integrity of the image has been compromised. Tampered images are not reliable or valid sources of evidence for forensic investigations, as they may contain false or misleading information.
Untampered images are disk images that have not been changed or manipulated after they were acquired from the original source. Untampered images have the same stored and computed hash values, which verify that the image is an exact copy of the original disk. Untampered images are used for forensic investigations, as they preserve the original state and content of the disk and provide accurate and trustworthy evidence. References:
* Contrasting tampered and untampered disk images
* What is a difference between tampered and untampered disk images?

質問: **48**
Web サーバーがユーザーからの入力を受け入れてそれを bash シェルに渡す場合、どの攻撃方法に対して脆弱になりますか?
A. ハッシュ衝突
B. 入力検証
C. コマンドインジェクション
D. 整数オーバーフロー
正解: (正解を表示します)

質問: **49**
「色」と「色」に一致する正規表現は?
A. colo?ur
B. col[08]+our

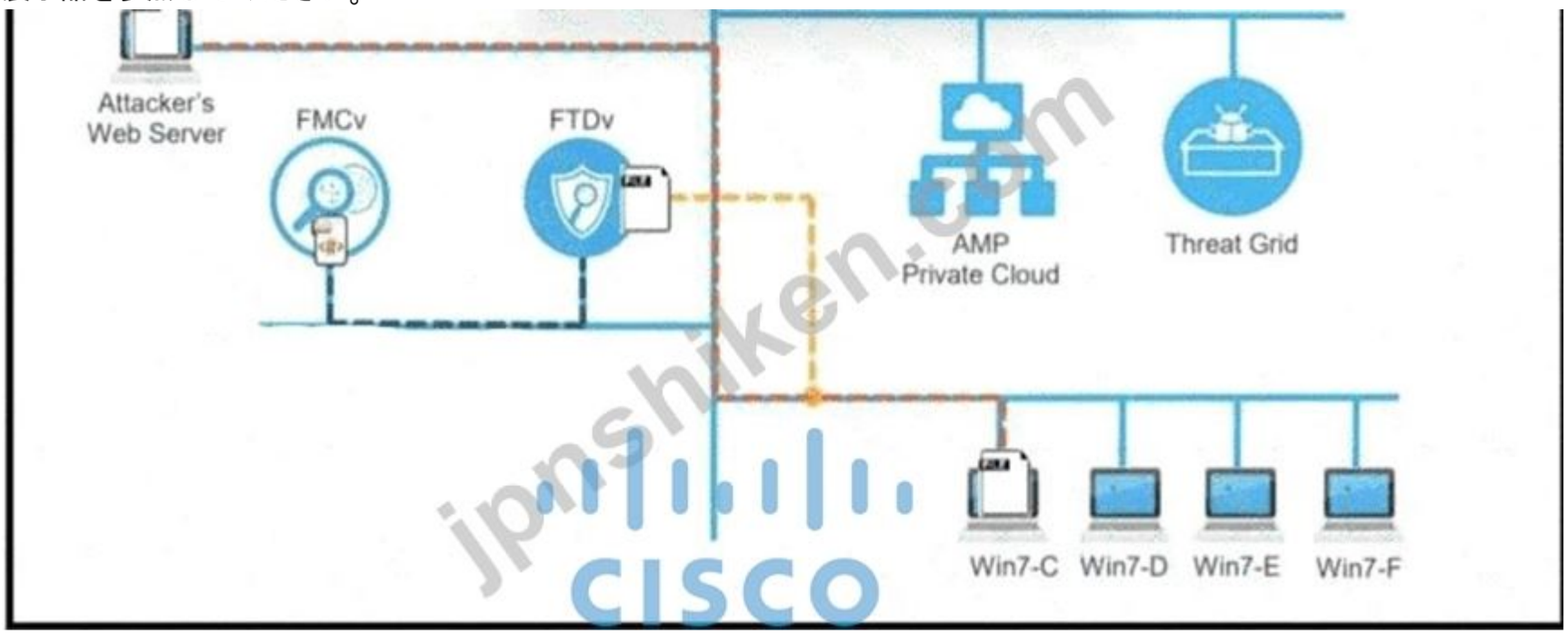
C. colou?r
D. col[09]+our
正解: **A (**コメントを発表する**)**
The regular expression that matches both "color" and "colour" is colo?ur. In this expression, the ? denotes that the preceding character u is optional, meaning it may appear zero or one time. This allows the expression to match both the American spelling "color" and the British spelling "colour".
References := Understanding regular expressions is fundamental in various computing tasks, including cybersecurity operations. The Cisco Cybersecurity Operations Fundamentals (CBROPS) material covers the use of regular expressions for searching through logs and data, which is a critical skill for a cybersecurity analyst.

質問: **50**
データのカプセル化とは何ですか?
A. 閲覧履歴はセッションごとに自動的に消去されます。
B. 送信ホストのプロトコルにより、パケット ヘッダーに追加データが追加されます。
C. データは逆方向に暗号化されているため、使用できません。
D. 少数のパブリック IP アドレスで複数のホストをサポートできます。
正解: **(**正解を表示します**)**
* Data encapsulation is a process in networking where the protocol stack of the sending host adds headers (and sometimes trailers) to the data.
* Each layer of the OSI or TCP/IP model adds its own header to the data as it passes down the layers, preparing it for transmission over the network.
* For example, in the TCP/IP model, data starts at the application layer and is encapsulated at each subsequent layer (Transport, Internet, and Network Access) before being transmitted.
* This encapsulation ensures that the data is correctly formatted and routed to its destination, where the headers are stripped off in reverse order by the receiving host.
References
* Networking Fundamentals by Cisco
* OSI Model and Data Encapsulation Process
* Understanding TCP/IP Encapsulation

質問: **51**
ランサムウェアの機能である回避手法はどれですか?
A. extended sleep calls
B. encryption
C. resource exhaustion
D. encoding
正解: **B (**コメントを発表する**)**
Encryption is an evasion technique that is a function of ransomware, which is a type of malware that encrypts the victim's files or system and demands a ransom for the decryption key. Encryption is used by ransomware to prevent the victim from accessing their data and to avoid detection by antivirus or other security tools. Encryption can also be used by other types of malware to hide their communication, configuration, or payload from analysis. References:
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 3: Network Intrusion Analysis, Lesson 3.4: Malware Cisco Certified CyberOps Associate Overview, Exam Topics, 3.4 Compare and contrast types of malware

質問: **52**
ネットワーク アドレス変換を実行するレイヤー 3 デバイスによって分離された 2 つのデバイスからのログ メッセージを比較する場合、どのような問題が発生しますか。
A. ログメッセージ内のIPアドレスが一致しません
B. ログ メッセージのタイムスタンプが異なります。
C. ログメッセージに誤った情報が含まれています
D. ログメッセージ内のIPアドレスが一致する
正解: **A** (コメントを発表する)

質問: **53**
展示品を参照してください。



ワークステーションがインターネットから悪意のある docx ファイルをダウンロードし、そのコピーが FTDv に送信されます。FTDv はファイル ハッシュを FMC に送信し、より強力なデータ可視性があれば発生するはずだったタイル イベントが記録されます。
A. トラフィックはネットワーク内の任意のセグメントで監視されます。
B. 悪意のあるトラフィックは複数のデバイスでブロックされる
C. 追加のセキュリティレベルが設けられていただろう
D. リアルタイムのデータに関する詳細情報が提供される
正解: (正解を表示します)
With stronger data visibility, detailed information about the data in real-time is provided. This enhanced visibility allows for a more comprehensive analysis of network traffic, enabling security professionals to identify and mitigate threats more effectively. References := Cisco Cybersecurity Operations Fundamentals

質問: **54**
Linux および Mac OS X オペレーティング システムを使用するオープンソースのパケット キャプチャ ツールはどれですか?
A. ネットスカウト
B. tcpdump
C. ソーラーウィンズ

D. netsh
正解: **(**正解を表示します**)**
tcpdump is an open-source packet capture tool that uses the libpcap library to capture network traffic on Linux and Mac OS X operating systems. It can display the contents of packets in various formats, filter packets based on criteria, and save packets to a file. tcpdump is a command-line tool that can be run on a terminal or a remote shell1 References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Module 2: Security Monitoring

質問: **55**
2020年9月の脅威インテリジェンスフィードによると、Egregorと呼ばれる新しいマルウェアが導入され、多くの攻撃で使用されました。Egregorの配布は、RDPエクスプロイトを使用して被害者のワークステーションにインストールされたCobalt Strikeを介して行われ、マルウェアは被害者のデータをコマンドおよび制御サーバーに盗み出します。このデータは、被害者がデータを公開することにより、支払いまたは損失を強制するために使用されます。どのタイプの攻撃が説明されていますか？
A. マルウェア攻撃
B. ランサムウェア攻撃
C. クジラフィッシング
D. 内部脅威
正解: **(**正解を表示します**)**
Ransomware is a type of malware that encrypts the victim's data and demands a ransom for the decryption key. The attacker may also threaten to publish or delete the data if the ransom is not paid. In this case, the Egregor malware is distributed through a Cobalt Strike, which is a penetration testing tool that can be used to deploy payloads on compromised systems. The malware exfiltrates the victim's data to a command and control server and uses it as leverage to extort money from the victim. References := Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.3: Malware Attacks

質問: **56**
脆弱性とエクスプロイトの 2 つの違いは何ですか? (2 つ選択してください。)
A. 脆弱性はハードウェアとソフトウェアの両方に存在し、エクスプロイトはソフトウェアベースの脆弱性に対してのみ使用できます。
B. 脆弱性は通常ダークウェブに存在し、エクスプロイトのツールや方法はパブリックウェブで見つかります。
C. 脆弱なソフトウェアまたはハードウェアにパッチが適用されるまで、ゼロデイエクスプロイトを使用して脆弱性を悪用することができます。
D. 既知の脆弱性には特別な CVE 番号が割り当てられ、エクスプロイトは脆弱性を利用するプロセスを使用します。
E. ゼロデイエクスプロイトは既知の脆弱性を悪用するために使用され、企業の資産に対してサイバー攻撃が行われる可能性があります。
正解: **C,D (**コメントを発表する**)**

質問: **57**
ファイアウォールのディープ パケット インスペクションはどのレイヤーで調査されますか?
A. インターネット
B. 輸送
C. アプリケーション
D. データリンク
正解: **(**正解を表示します**)**
Deep packet inspection (DPI) is a sophisticated method of examining the content of data packets as they pass through a network checkpoint, including both the header and the data payload. DPI is typically performed at the application layer of the Open Systems Interconnection (OSI) model. This allows the inspection

process to evaluate the actual content of the packets, not just the header information, enabling the identification of various types of threats and the enforcement of network policies1.
References := The explanation aligns with the information provided by Digital Guardian, which details how DPI works and at which layer it is applied1.

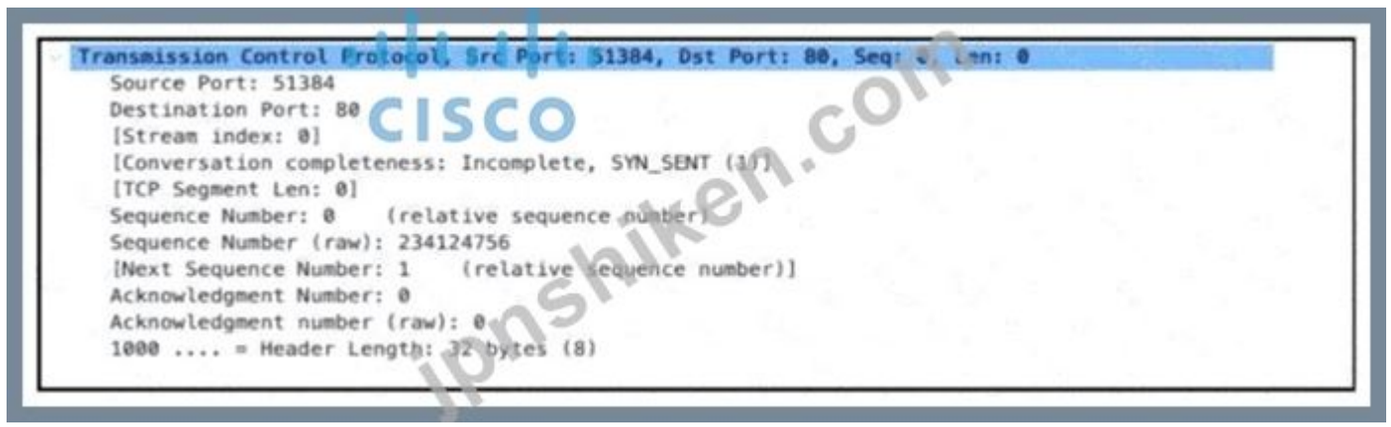
質問: **58**
サイバーアトリビューションは調査で何を特定しますか?
A. 攻撃の原因
B. 攻撃の悪用
C. 悪用された脆弱性
D. 攻撃の脅威アクター
正解: **D (**コメントを発表する**)**
Cyber attribution identifies the threat actors of an attack in an investigation. Threat actors are the individuals, groups, organizations, or states that are responsible for conducting or sponsoring a cyberattack. Threat actors can have different motives, such as financial gain, espionage, sabotage, activism, or warfare. Cyber attribution can help investigators to determine the identity, location, affiliation, and motivation of the threat actors, as well as to hold them accountable and impose sanctions or legal actions. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 5: Security Policies and Procedures, Lesson
5.2: Incident Response, Topic 5.2.3: Cyber Attribution, page 5-14.

質問: **59**

```
Mar  6 10:20:44 user sshd[12706]: Accepted publickey for user from
10.150.251.240 port 55796 ssh2: RSA
SHA256:ABCD1231231239HR4J8VzPUNHZKA3o
Mar  6 10:20:44 user sshd[12706]: pam_unix(sshd:session): session opened for
user user by (uid=0)
Mar  6 10:20:44 user systemd-logind[1069]: New session 450 of user user.
Mar  6 10:20:44 user systemd: pam_unix(systemd-user:session): session
opened for user user by (uid=0)
```

展示を参照してください。この出力に基づいて、このシステムでは何が起こったのでしょうか？
A. ユーザーが SHA256 ハッシュ アルゴリズムを使用して新しい HTTP セッションを作成しました。
B. ユーザーは、送信元ポート 55796 を使用して SSH でシステムに接続しました。
C. ユーザーは 450 回の試行後にシステムに接続しました。
D. リモート アクセス VPN を使用してシステムに接続したユーザー。
正解: **(**正解を表示します**)**

質問: **60**



展示を参照してください。このパケットから識別されるアラートはどれですか？

A. SYNフラッド

B. SSDP増幅

C. TCPフラグメンテーション攻撃

D. フラグル攻撃

正解: **A** (コメントを発表する)

質問: **61**



添付資料を参照してください。攻撃者はNmapを使用してサーバーをスキャンしました。このスキャンから攻撃者は何を入手しましたか？

A. PERT 状態が返されるのを妨げるファイアウォール デバイスを識別しました。

B. サーバー上で開いているSMBポートを特定しました

C. サーバー上で実行されているプロセスに関する情報を収集しました

D. Active Directoryユーザーのリストを収集しました

正解: **B** (コメントを発表する)

The Nmap scan results show that several ports, including ftp (21/tcp), ssh (22/tcp), telnet (23/tcp), smtp (25 /tcp), and http (80/tcp), are listed as "filtered". This typically indicatesthat a firewall is filtering the traffic to these ports, making it impossible to determine whether they are open without further investigation. However, the question specifically asks about SMB ports, which are not shown in the provided Nmap scan results. Therefore, based on the information given, we cannot confirm that the attacker identified open SMB ports on the server. The correct answer would require additional evidence not present in the scan results. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course materials and official Cisco documentation provide insights into interpreting Nmap scan results and identifying port states. These resources can be found at the Cisco Learning Network Store and Cisco's official training and certifications webpage

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
展示品を参照してください。



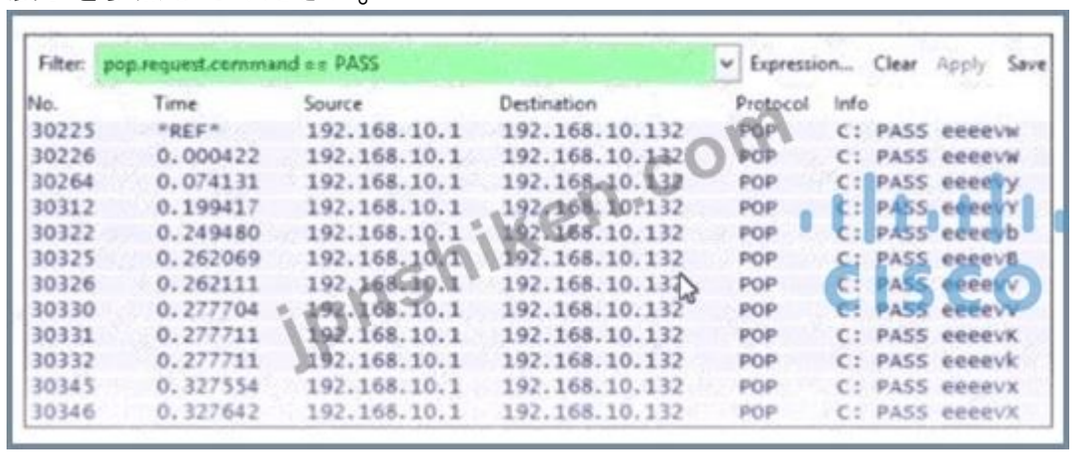
このパケットキャプチャから何を解釈すればよいでしょうか?
A. 81.179.179.69 は、UDP プロトコルを使用して、ポート 80 から IP アドレス 192.168.122.100 のポート 50272 にパケットを送信しています。
B. 192.168.122.100 は、TCP プロトコルを使用して、ポート 50272 から IP アドレス 81.179.179.69 のポート 80 にパケットを送信しています。
C. 192.168.122.100 は、UDP プロトコルを使用して、ポート 80 から IP アドレス 81.179.179.69 のポート 50272 にパケットを送信しています。
D. 81.179.179.69 は、TCP UDP プロトコルを使用して、ポート 50272 から IP アドレス 192.168.122.100 のポート 80 にパケットを送信しています。
正解: **(**正解を表示します**)**
The packet capture exhibit shows that the source IP address is 192.168.122.100 and it is sending a packet from source port 50272 to destination port 80 of destination IP address 81.179.179.69 using TCP protocol.
The TCP protocol is indicated by the Protocol field which has the value 6. The source and destination ports are indicated by the SrcPort and DstPort fields respectively. The source and destination IP addresses are indicated by the SrcAddr and DstAddr fields respectively. References := Cisco Cybersecurity Operations Fundamentals - Module 3: Network Data and Event Analysis

質問: **63**
2 つのサービス拒否攻撃とは何ですか? (2つ選んでください。)
A. MITM
B. TCP connections
C. ping of death
D. UDP flooding
E. code red

正解: **C,D** (コメントを発表する)
Ping of Death involves sending oversized or malformed pings to crash the target system, while UDP flooding overwhelms the target with UDP packets to consume its resources and disrupt services. These are both examples of denial of service attacks, which aim to prevent legitimate users from accessing a system or service.
References := Cisco Cybersecurity Operations Fundamentals - Module 4: Network Intrusion Analysis

質問: **64**
脆弱性管理プロセスについて説明しているものは何ですか?
A. ソフトウェアの脆弱性を特定、分類、軽減するための循環的なアプローチ
B. 製品のパフォーマンスの一貫性を確立し維持するためのシステムエンジニアリングプロセス
C. 機密性の高い企業データにアクセスするデバイスを安全に監視および監督する
D. 定期的にリリースされるホットフィックスとパッチの展開が含まれます
正解: (正解を表示します)

質問: **65**
攻撃者が 4 桁の数字のパスワードのみを使用し、ユーザー名を使用しない認証システムを使用してネットワークを侵害しようとする場合、どのような攻撃方法が使用されますか?
A. SQL インジェクション
B. 辞書
C. リプレイ
D. クロスサイト スクリプティング
正解: (正解を表示します)
A dictionary attack is a method used to break into a password-protected computer or server by systematically entering every word in a dictionary as a password. In the context of an authentication system that uses only 4- digit numeric passwords, a dictionary attack would involve trying all possible combinations of 4-digit numbers until the correct one is found.
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course materials discuss various attack methods, including dictionary attacks, and how they can be used to compromise networks

質問: **66**
展示を参照してください。


このパケット キャプチャから特定されるアラートはどれですか?
A. 中間者攻撃

B. ARP ポイズニング
C. ブルートフォース攻撃
D. SQL インジェクション
正解: **(**正解を表示します**)**
The screenshot shows multiple POP requests with the command PASS, which is typically used for password entry. The rapid succession and variation of these requests suggest an attempt to guess the password, characteristic of a brute-force attack. Remember, always verify with additional data or context when possible, as packet captures can contain vast amounts of information and may require thorough analysis for accurate interpretation.

質問: **67**
ネットワークを介して送信する前にトラフィックを小さなセグメントに分割することによって実現される回避手法のタイプはどれですか?
A. プロキシ
B. トンネリング
C. 断片化
D. 暗号化
正解: **(**正解を表示します**)**

質問: **68**
攻撃ベクトルと攻撃対象領域の違いは何ですか?
A. 攻撃面は、ユーザーの入力または検証を必要とする脆弱性を識別します。攻撃ベクトルは、ユーザーの操作に依存しない脆弱性を識別します。
B. 攻撃ベクトルは、悪用される可能性のあるコンポーネントを識別します。攻撃表面は、攻撃がネットワークに侵入するためにたどる可能性のあるパスを識別します。
C. 攻撃対象領域は、攻撃に対して脆弱なネットワーク部分を認識します。攻撃ベクトルは、これらの脆弱性でどの攻撃が可能であるかを識別します。
D. 攻撃ベクトルは、攻撃の潜在的な結果を特定します。攻撃面は、特定された脆弱性に対していくつかの方法を使用して攻撃を開始します。
正解: **(**正解を表示します**)**
An attack vector is the method or technique that an attacker uses to exploit a vulnerability in a system or network. An attack vector can be a software, hardware, or human component that can be manipulated to gain unauthorized access, execute malicious code, or cause damage. An attack surface is the sum of all the possible attack vectors that are exposed by a system or network. An attack surface can be reduced by applying security measures such as patching, hardening, firewalling, and encrypting. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 1-4; 200-201 CBROPS - Cisco, exam topic
1.1.c

質問: **69**
データベースからの情報の読み取り、書き込み、または消去に使用される脆弱性の種類はどれですか？
A. クロスサイトスクリプティング
B. クロスサイトリクエストフォージェリ
C. バッファオーバーフロー
D. SQLインジェクション
正解: **D (**コメントを発表する**)**
SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL statements on a database server. This can result in reading, writing, or erasing information from the database, as well as bypassing authentication, executing commands, or compromising the server. SQL injection exploits the lack of

input validation or output encoding in web applications that interact with databases. References := Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.2: Web Application Attacks

質問: **70**
多層防御戦略の原則は次のうちどれですか?
A. 従業員ごとに必要な最小限のリソースを特定します。
B. セグメント ネットワーク権限に最小限のネットワーク権限を割り当てます。
C. ジョブ機能を実行するために必要な最小限の権限を提供します。
D. 不正な変更を防ぐために管理アカウントを無効にします。
正解: **(**正解を表示します**)**
* Defense-in-depth is a layered security strategy that aims to protect information and resources through multiple security measures.
* One of its key principles is the concept of least privilege, which means providing users and systems with the minimum level of access necessary to perform their job functions.
* By assigning only the necessary permissions, the attack surface is reduced, and the potential damage from a compromised account or system is minimized.
* This principle helps in mitigating the risk of unauthorized access and limits the capabilities of an attacker if they gain access to an account.
References
* Defense-in-Depth Strategy by NIST
* Principle of Least Privilege in Cybersecurity
* Layered Security Approach Explained

質問: **71**
攻撃者は、潜在的なターゲット デバイスでリッスンしているネットワーク ポートを特定するために何を使用しますか?
A. 中間者
B. ポートスキャン
C. SQL インジェクション
D. ping スイープ
正解: **(**正解を表示します**)**
Port scanning is a technique that an attacker uses to discover which network ports are open, closed, or filtered on a target device. By sending packets to different ports and observing the responses, an attacker can identify the services and applications running on the device, as well as potential vulnerabilities that can be exploited.
Port scanning is a common reconnaissance activity that precedes an attack. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 2-6; 200-201 CBROPS - Cisco, exam topic
1.1.a

質問: **72**
エンドデバイス間のIPトレーサビリティを妨げるテクノロジーはどれですか？
A. 暗号化
B. 負荷分散
C. NAT / PAT
D. トンネリング

正解: (正解を表示します)
NAT (Network Address Translation) and PAT (Port Address Translation) are technologies that modify the IP address information in packet headers as they pass through a router or firewall, making it difficult to trace the communication back to the originating end-device.

質問: **73**
すべてのリソースの開発、運用、保守、アップグレード、および廃棄を最もよく表す管理概念はどれですか?
A. 資産
B. 構成
C. パッチ
D. 脆弱性
正解: (正解を表示します)

質問: **74**
展示品を参照してください。

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

どのイベントが発生していますか?
A. 「submit」という名前のバイナリが VM cuckoo1 上で実行されています。
B. VM cuckoo1 で実行するためにバイナリが送信されています
C. VM cuckoo1 上のバイナリが評価のために送信されています
D. URL に悪意のあるバイナリが含まれているかどうかが評価されています
正解: (正解を表示します)
The command "$ cuckoo submit --machine cuckoo1 /path/to/binary" indicates that a binary located at "/path /to/binary" is being submitted to be run on a virtual machine named "cuckoo1". This is a common practice in cybersecurity to analyze the behavior of suspicious files in an isolated environment. References: Cisco Cybersecurity documents or resources are needed for more detailed information.

質問: **75**
エンジニアは、TCP 帯域幅の使用状況、応答時間、遅延を可視化し、詳細なパケット検査と組み合わせて、ネットワーク トラフィック フローによって未知のソフトウェアを特定する必要があります。この目標を達成するために、エンジニアが使用すべき Cisco Application Visibility and Control の 2 つの機能はどれですか? (2 つ選んでください。)
A. 管理と報告
B. トラフィック フィルタリング
C. アダプティブ AVC
D. メトリクスの収集とエクスポート
E. アプリケーションの認識
正解: **D,E** (コメントを発表する)
Cisco Application Visibility and Control (AVC) provides features like metrics collection and exporting (D) for visibility on TCP bandwidth usage, response time, and latency. Application recognition (E) combined with deep packet inspection helps in identifying unknown software by its network traffic flow. References := Cisco CyberOps Associate - Module 2: Security Concepts

質問: **76**
ユーザーは、コンテンツを開く前に、標的を絞ったスピアフィッシングメールを受信し、疑わしいと特定しました。このタイプのイベントは、サイバーキルチェーンモデルのどのカテゴリに属しますか？
A. 兵器化
B. 配達
C. 搾取
D. 偵察
正解: **(**正解を表示します**)**
The delivery phase of the Cyber Kill Chain model involves the transmission of the weapon to the targeted environment. In the case of a spear-phishing email, the delivery is the act of sending the email to the user. The email itself is the weapon, designed to exploit the recipient's trust to cause a breach

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu **564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
エンジニアは、プロキシ サーバーからログを取得し、受け取ったデータに基づいて実際のイベントを生成する必要があります。
このタスクを達成するためにエンジニアはどのテクノロジーを使用すべきですか?
A. 火力
B. 電子メール セキュリティ アプライアンス
C. Web セキュリティ アプライアンス
D. ステルスウォッチ
正解: **(**正解を表示します**)**
Stealthwatch is the technology that an engineer should use to fetch logs from a proxy server and generate actual events based on the data received. Cisco Secure Network Analytics, formerly known as Stealthwatch, provides the capability to configure proxy server logs so that the Flow Collector can receive the information. The Stealthwatch Management Console then displays this information on the Flow Proxy Records page, which includes URLs and application names of the traffic inside a network going through the proxy server1.
References :=
* Cisco Secure Network Analytics Proxy Log Configuration Guide

質問: **78**
ネットワーク エンジニアは NetFlow レポートで、内部ホストが外部 DNS サーバーに多数の DNS リクエストを送信していることに気付きました。SOC アナリストがエンドポイントをチェックしたところ、エンドポイントが感染し、ボットネットの一部になっていることが判明しました。エンドポイントは複数の DNS リクエストを送信していますが、その IP アドレスは偽装されていました。有効な外部ソース 感染したエンドポイントはどのような攻撃に関与していますか?1?
A. DNS ハイジャック
B. DNS トンネリング
C. DNS フラッディング
D. DNS 増幅

正解: (正解を表示します)
The attack described is a DNS amplification attack. It involves infected endpoints sending DNS requests with spoofed IP addresses to external DNS servers. The DNS servers then send large responses to the spoofed addresses, which are actually the targets of the attack. This can result in a significant amount of traffic being directed at the target, overwhelming their network resources. DNS amplification is a type of Distributed Denial of Service (DDoS) attack that leverages the DNS protocol to amplify the attack traffic.

質問: **79**
サイバーセキュリティの文脈における脅威インテリジェンスの定義は何ですか?
A. ITインフラストラクチャの更新と強化
B. 高度な防御機構の設計と実装
C. 高度なサイバー攻撃の設計と実行
D. 潜在的なセキュリティ脅威に関連する情報と分析
正解: (正解を表示します)

質問: **80**
サンドボックスプロセス間通信サービスとは何ですか?
A. サンドボックス間の通信を妨げるサンドボックス内のルールの集まり。
B. インターフェイス上でアクティブ化されるネットワーク サービスのコレクションであり、ポート間通信を可能にします。
C. プロセス間のアクティビティの調整を可能にするインターフェイスのコレクション。
D. サンドボックス間の通信を可能にするホスト サービスのコレクション。
正解: (正解を表示します)
A sandbox interprocess communication service refers to the mechanisms that allow different processes within a sandboxed environment to communicate with each other. Theseinterfaces are crucial for coordinating activities among processes, especially in a restricted environment like a sandbox where direct interaction with the operating system or other processes might be limited for security reasons. This communication is essential for complex applications that require different processes to work together to perform tasks.
References := The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) material covers various security technologies and how they can be used to protect systems, which includes the use of sandboxing to isolate and monitor potentially malicious code

質問: **81**
展示品を参照してください。

File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552f5c3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6E
PEiD	None matched
Yara	• embedded_pe (Contains an embedded PE32 file) • embedded_win_api (A non-Windows executable contains win32 API • vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

ibnshiken.com

エンジニアは、電子メールからダウンロードされた PDF ファイルの Cuckoo Sandbox レポートを分析しています。
このファイルの状態はどうなっていますか?
A. ファイルは PEiD 脅威シグネチャと一致しましたが、シグネチャ リストが最新であるため、疑わしい特徴は特定されませんでした。
B. ファイルには Windows 以外の実行ファイルが埋め込まれていますが、疑わしい機能は確認されていません。
C. ファイルには Windows 32 実行ファイルが埋め込まれており、Yara フィールドにはさらに分析が必要な疑わしい機能がリストされています。
D. ファイルには実行可能ファイルが埋め込まれており、PEiD 脅威シグネチャと一致してさらに分析されました。
正解: **(**正解を表示します**)**

質問: **82**
展示品を参照してください。



2021-01-05 19:47:15	52.114.132.22	443	self.events.data.micr…	Client Hello
2021-01-05 19:47:16	52.109.88.35	443	nexusrules.officeapps…	Client Hello
2021-01-05 19:47:53	204.79.197.200	443	www.bing.com	Client Hello
2021-01-05 19:48:48	185.225.36.38	80	infoprocenter.com	GET /wp-admin/MSInfo/ HTTP/1.1
2021-01-05 19:48:48	144.217.79.200	80	miprimercamino.com	GET /cgi-bin/AJ09AzChrK/ HTTP/
2021-01-05 19:48:58	125.0.215.60	80	125.0.215.60	POST /bgi93n6v5xtgj/k3i3a/u46l
2021-01-05 19:49:06	125.0.215.60	80	125.0.215.60	POST /vs7e7ht0yjohr8/qag42y9/c
2021-01-05 19:49:10	125.0.215.60	80	125.0.215.60	POST /avkbtr3s7rxvxz7a1g/puv2i
2021-01-05 19:49:11	52.109.8.20	443	nexusrules.officeapps…	Client Hello
2021-01-05 19:49:11	104.236.52.89	8080	104.236.52.89:8080	POST /krhp52joegfy8i7b/lkc1rvr
2021-01-05 19:49:14	125.0.215.60	80	125.0.215.60	POST /ylcp/gjga2kgpe/5ayyt/ HT
2021-01-05 19:49:15	52.109.8.20	443	nexusrules.officeapps…	Client Hello
2021-01-05 19:49:15	104.236.52.89	8080	104.236.52.89:8080	POST /6y9ra6iqzi302y7vrna/sihg
2021-01-05 19:49:19	125.0.215.60	80	125.0.215.60	POST /ngslvujkk0hi/yhky2nwmv/i
2021-01-05 19:49:19	104.236.52.89	8080	104.236.52.89:8080	POST /tn9gpiuk/zsit42fjx98m4rr
2021-01-05 19:49:19	104.236.52.89	8080	104.236.52.89:8080	POST /tn9gpiuk/zsit42fjx98m4rr
2021-01-05 19:49:25	125.0.215.60	80	125.0.215.60	POST /het5/jd55lt85h/h9gu0nw8r
2021-01-05 19:49:25	104.236.52.89	8080	104.236.52.89:8080	POST /z1x928hdy3f92jatt/dytq2c
2021-01-05 19:49:38	125.0.215.60	80	125.0.215.60	POST /yajtvsgegx08cw/ HTTP/1.1
2021-01-05 19:51:28	52.114.128.43	443	v20.events.data.micro…	Client Hello
2021-01-05 19:51:29	52.114.128.43	443	v10.events.data.micro…	Client Hello
2021-01-05 19:51:46	52.114.20.14	443	self.events.data.micr…	Client Hello
2021-01-05 19:55:14	13.107.246.13	443	oti.store.microsoft.c…	Client Hello

何が起こっているのでしょうか?

A. 診断のために暗号化された Web セッションと暗号化されていない Web セッションを監視します。

B. マルウェア通信とボットネット活動の可能性を特定する

C. 分散アプリケーション環境におけるパフォーマンスの最適化のためのセッションログのレビュー

D. ネットワーク容量テスト中のトラフィックフローの分析

正解: **A** (コメントを発表する)

質問: **83**

行動検出と比較した場合のルールベースの検出の違いは何ですか?

A. ルールベースの検出は特定のタイプの攻撃に関連するパターンを検索し、行動はシグネチャごとに識別します。

B. ルールベースのシステムは、行動が変化しても、新しいデータで変化しないパターンを確立しています。

C. 行動システムは数百人のユーザーから事前に定義されたパターンですが、ルールベースはシグネチャを使用して潜在的に異常なパターンにフラグを立てます。

D. 行動システムは特定の攻撃シグネチャに一致するシーケンスを見つけ、ルールベースは潜在的な攻撃を識別します。

正解: (正解を表示します)

Rule-based detection involves identifying malicious activities based on predefined rules or patterns of known attacks; it does not adapt or change with new data. In contrast, behavioral detection adapts over time by learning from new data; it identifies malicious activities based on deviations from established norms or behaviors. References: Cisco Certified CyberOps Associate Overview, Section 1.0: Security Concepts, Subsection 1.1: Compare and contrast the characteristics of data obtained from taps, NetFlow, and packet capture)

質問: **84**

スケアウェア攻撃とは何ですか?

A. スプーフィングされた電子メール アドレスを使用して、ユーザーをだましてログイン資格情報を提供させます。

B. 偽のトラフィックで標的の Web サイトを圧倒します

C. コンピューターへのゲーム アクセスと、コンピューターに保存されているデータの暗号化

D. 色が点滅するポップアップ ウィンドウを引き起こす悪意のあるコードを挿入します。

正解: (正解を表示します)

Scareware is a type of malware attack that tricks users into believing their computer is infected with a virus, prompting them to download and pay for fake antivirus software. The attack often uses popup windows with flashing colors (D) to create a sense of urgency and scare the user into taking immediate action.
Cisco Certified CyberOps Associate certification materials

質問: **85**
エンジニアは、Cisco ASA ファイアウォールで正規表現 ｢"\.(pd][Oo][Cc)|[Xx][LI][Ss]|[Pp][Pp][Tt]) HTTP/1 .[01]" を設定しました。この正規表現は何をするのでしょうか?
A. HTTP ネットワーク セッションでドキュメントをキャプチャします。
B. HTTP v1.0 および v1.1 で .doc、.xls、.pdf ファイルをキャプチャします。
C. HTTP v1.0 の .doc、.xls、および .ppt ファイル拡張子をキャプチャします。
D. HTTPv1.0 および v1.1 で Word、Excel、および PowerPoint ファイルをキャプチャします。
正解: **(**正解を表示します**)**
The regular expression provided is:.\.(pd][Oo][Cc)|[Xx][LI][Ss]|[Pp][Pp][Tt]) HTTP/1 .[01] This regular expression is designed to match file extensions for Word (.doc), Excel (.xls), and PowerPoint (.
ppt) files in HTTP network sessions.
The regular expression uses character classes and alternatives to match different case variations of these file extensions.
The part.\.(pd][Oo][Cc)|[Xx][LI][Ss]|[Pp][Pp][Tt])matches the file extensions, andHTTP/1 .[01]ensures that the match is in the context of HTTP version 1.0 or 1.1.
References
Cisco ASA Regular Expressions Documentation
Understanding Regular Expressions in Network Security
Filtering and Capturing HTTP Traffic with Regex

質問: **86**
展示品を参照してください。

Employee Name	Role
Employee 1	Chief Accountant
Employee 2	Head of Managed Cyber Security Services
Employee 3	System Administration
Employee 4	Security Operation Center Analyst
Employee 5	Head of Network & Security Infrastructure Services
Employee 6	Financial Manager
Employee 7	Technical Director

jpnshiken.com

会社のワークステーションが侵害された場合、どの関係者が関与する必要がありますか?
A. 従業員 1 従業員 2、従業員 3、従業員 4、従業員 5、従業員 7
B. 従業員 1、従業員 2、従業員 4、従業員 5
C. 従業員4、従業員6、従業員7
D. 従業員 2、従業員 3、従業員 4、従業員 5
正解: **(**正解を表示します**)**
When a company workstation is compromised, the stakeholders that must be involved are the ones who are responsible for the security incident response process. According to the table, these are Employee 4 (Security Operation Center Analyst), Employee 6 (Head of Network and Security Infrastructure Services),

and Employee 7 (Technical Director). The other employees have different roles that are not directly related to the incident response process, such as accounting, financial management, or system administration. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.4: Security Monitoring, Topic 1.4.1: Security Operations Center

質問: **87**



展示を参照してください。何が起こっているのでしょうか?

A. サービス拒否

B. DNS増幅攻撃

C. ARPポイズニング

D. ブルートフォース攻撃

正解: **(**正解を表示します**)**

質問: **88**

悪用されたデバイスの永続的な制御を維持するために何が使用されますか?

A. ルートキット

B. ARPスプーフィング

C. DDoS

D. 暗号化

正解: **A (**コメントを発表する**)**

A rootkit is a type of malicious software specifically designed to maintain persistent, unauthorized control over a compromised system while evading detection. Rootkits operate by embedding themselves deep within the operating system, often at the kernel level, allowing attackers to hide processes, files, network connections, and registry entries.

Once installed, a rootkit enables long-term access even after system reboots, making it a powerful persistence mechanism. Attackers use rootkits to maintain control, execute commands, capture credentials, and install additional malware without alerting security tools or administrators.

Option B, ARP spoofing, is a network-level attack used for traffic interception, not persistence. Option C, DDoS, is an availability attack and does not provide control over a device. Option D, encryption, is a defensive technology and does not grant persistence.

Cybersecurity operations and incident response documentation consistently identify rootkits as high-severity threats because of their stealth, durability, and ability to undermine trust in the operating system. Detecting rootkits often requires specialized tools, integrity checks, and sometimes full system reimaging.

Therefore, the technology used to maintain persistent control of an exploited device is a rootkit, making Option A the correct answer.

質問: **89**
TapポートとSPANポートから取得したデータの違いは何ですか？
A. Tapは指定されたポートからの既存のトラフィックをミラーリングしますが、SPANはより詳細な分析のためにより構造化されたデータを提示します。
B. SPANは、ネットワークデバイスとネットワークの間でトラフィックを変更せずに受動的に分割しますが、Tapは応答時間を変更します。
C. SPANはメディアエラーの検出を改善し、Tapはデータの可視性を低下させたトラフィックへの直接アクセスを提供します。
D. Tapは物理層から監視デバイスにトラフィックを送信し、SPANはスイッチから宛先へのネットワークトラフィックのコピーを提供します
正解: **(**正解を表示します**)**
Tap and SPAN are two methods of capturing network traffic for analysis. Tap (Test Access Point) is a hardware device that is inserted between two network devices and sends a copy of all traffic to a monitoring device. SPAN (Switched Port Analyzer) is a software feature that allows a network switch to replicate traffic from one or more source ports to a destination port, where a monitoring device is connected. Both methods provide visibility into network traffic, but Tap is more reliable and less intrusive than SPAN, as it does not affect the network performance or introduce errors. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 68.
Reference:https://www.gigamon.com/resources/resource-library/white-paper/to-tap-or-to-span.html

質問: **90**
インライントラフィックモニタリングとタップモードトラフィックモニタリングの違いは何ですか？
A. インラインは他のデバイスを検査せずにトラフィックを監視し、タップモードはトラフィックにタグを付けて監視デバイスからのデータを検査します。
B. タップモードはトラフィックの方向を監視し、インラインモードは監視デバイスを通過するときにパケットデータを保持します。
C. タップモードはパケットとその内容を最高速度で監視し、インラインモードは分析のためにパケットパスを描画します。
D. インラインモードはトラフィックパスを監視し、ワイヤ速度でトラフィックを調べます。タップモードは、ネットワークを通過するトラフィックを監視します。
正解: **(**正解を表示します**)**
Inline mode is used for monitoring the traffic path and can examine any traffic at wire speed. This means that it can analyze data packets as they pass through in real-time. On the other hand, tap mode is used for monitoring traffic as it traverses across the network but does not have the capability to examine data at wire speed like inline mode. References: The information can be referenced from Cisco's official documentation on cybersecurity operations and fundamentals.
Reference:https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config- guide-v65/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

質問: **91**
展示品を参照してください。

```
nmap 10.19.140.2

Starting Nmap 6.40 ( http://nmap.org ) at 2019-07-21 16:39 EDT
Nmap scan report for 10.19.140.2
Host is up (0.061s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
199/tcp  open  smux
443/tcp  open  https
8000/tcp open  http-alt
8181/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds
```

ipnshiken.com

攻撃者は会社のネットワークへの最初のアクセス権を取得し、横方向の移動技術を進め、機密データを検索するために Nmap スキャンを実行しました。攻撃者はスキャンからどの 2 つの要素を特定できますか? (2 つ選択してください。)
A. ワークロードと構成の詳細
B. ユーザーアカウントとSID
C. サーバーが処理しているユーザー数とリクエスト数
D. サーバーの機能と目的
E. 実行中のサービス
正解: **(**正解を表示します**)**
An Nmap scan can provide detailed information about a network including the functionality and purpose of servers on that network as well as any services that are currently running on those servers. This information can be used by an attacker to identify potential vulnerabilities or targets for exploitation during a cyber attack.
References := Cisco Cybersecurity Training

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
アナリストは、正当なセキュリティ アラートが無視されたことを発見しました。ネットワーク トラフィックにこの影響を与えた署名はどれですか?
A. 真陰性
B. 偽陰性
C. 偽陽性
D. 真陽性
正解: **(**正解を表示します**)**
A false negative occurs when an intrusion detection system (IDS) fails to detect and report actual malicious activity. This means that a legitimate security alert has been dismissed or overlooked, allowing potentially harmful traffic to pass through the network undetected. The impact of false negatives can be significant as they represent missed opportunities to stop or mitigate security threats1.
References := Cisco documentation on security systems, such as IPS (Intrusion Prevention System), discusses the importance of accurately detecting malicious activity and the risks associated with false negatives, which include the failure to trigger alerts for actual attacks1.

質問: **93**
ユーザーは悪意のある添付ファイルを受け取りましたが、実行しませんでした。侵入を分類するカテゴリは?
A. 兵器化
B. インストール
C. 配達
D. 偵察
正解: **C (**コメントを発表する**)**

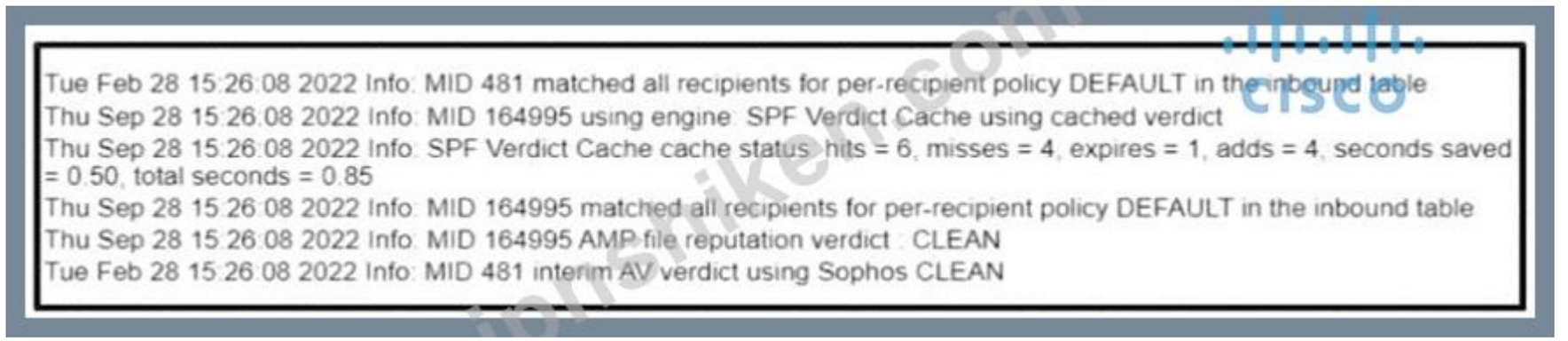
質問: **94**

どのプロセスがアプリケーションレベルの許可リストを表しますか?
A. すべてを許可し、特定のアプリケーション プロトコルを拒否します
B. すべてを許可し、特定の実行可能ファイルを拒否します
C. 特定の形式のファイルを許可し、実行可能ファイルを拒否します
D. 特定のファイルを許可し、それ以外はすべて拒否します
正解: **(**正解を表示します**)**
Application-level allow list refers to the practice of specifying an index of approved applications that are permitted to be executed in a system environment or network, which means only specific files are allowed while everything else is denied by default, enhancing security.

質問: **95**
2つのサービス拒否（DoS）攻撃とは何ですか？ 2つ選択してください）
A. ポートスキャン
B. SYNフラッド
C. 中間者
D. フィッシング
E. ティアドロップ
正解: **(**正解を表示します**)**
SYN flood and teardrop are two types of denial-of-service (DoS) attacks, which aim to disrupt the availability of a service or a system by overwhelming it with malicious traffic or requests. A SYN flood attack exploits the TCP three-way handshake process by sending a large number of SYN packets to the target's port, without completing the connection. This causes the target to allocate resources for half-open connections, eventually exhausting its memory or bandwidth. A teardrop attack exploits the IP fragmentation process by sending malformed or overlapping IP fragments to the target, causing it to crash or reboot when trying to reassemble them. References := Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.3: Common Network Application Operations and Attacks, Topic 1.3.4: Denial-of-Service Attacks

質問: **96**
攻撃の兆候を表すオプションはどれですか?
A. 従業員のワークステーション上のスパムメール
B. AV ソフトウェアによるウイルス検出
C. 企業に対するフィッシングの試みをブロックしました
D. 削除後数分以内にマルウェアが再感染
正解: **D (**コメントを発表する**)**
Indicators of attack (IoAs) are signs that an attack may be in progress or imminent. Malware reinfection within a few minutes of removal (D) is a strong IoA because it suggests that the attacker has a persistent mechanism to redeploy malware, indicating an active compromise of the system.
Cisco's Cybersecurity Operations Fundamentals documents

質問: **97**



展示を参照してください。どのような種類のデータフィルタリングが提供されていますか？

A. ウェブ

B. アプリケーション

C. メール

D. ファイアウォール

正解: **D** (コメントを発表する)

質問: **98**

どのイベントがビッシング攻撃ですか？

A. 組織から廃棄されたドキュメントを取得する

B. 企業ネットワークで脆弱性スキャナーを使用する

C. 公共のホットスポットの近くに不正なアクセスポイントを設置する

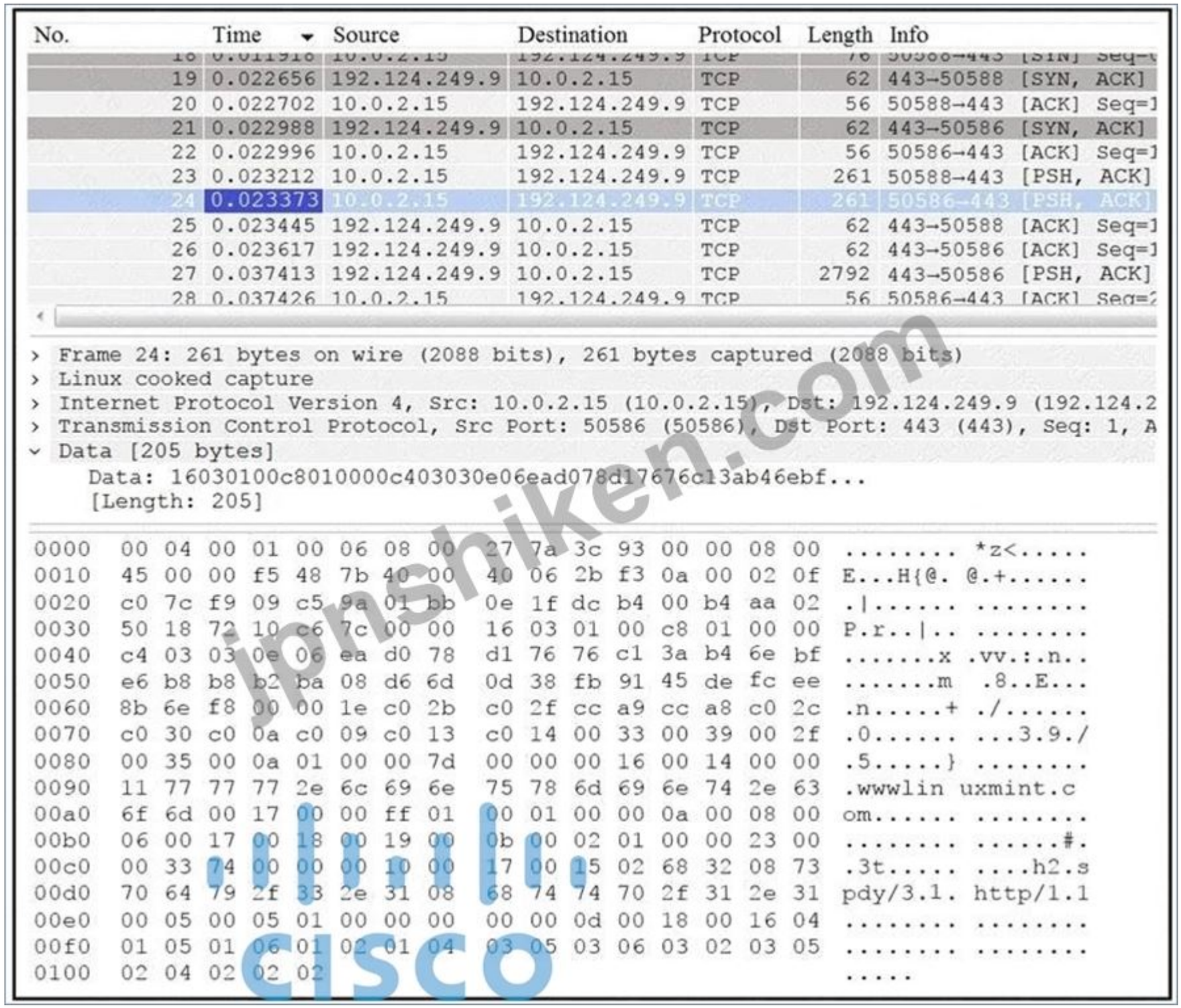
D. 通話中にテクニカルサポートエージェントになりすます

正解: (正解を表示します)

Vishing is an attack where fraudsters impersonate legitimate entities via phone calls to deceive individuals into providing sensitive information or performing actions that compromise security. References := Cisco Cybersecurity Source Documents Reference:https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of- phishing-attacks

質問: **99**

展示品を参照してください。



この PCAP ファイルにはどのアプリケーション プロトコルが含まれていますか?

A. SSH

B. TCP

C. TLS

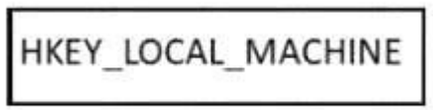
D. HTTP

正解: **D (**コメントを発表する**)**

The PCAP file in the exhibit shows a Transmission Control Protocol (TCP) communication between two IP addresses. In the data section of the packet capture, "pdy/3.1... http/1" isvisible, indicating that HTTP (Hypertext Transfer Protocol) is being used as the application protocol for this communication.

References := The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course material covers the analysis of network traffic using tools like packet analyzers to identify application protocols in use1.

質問: **100**
展示品を参照してください。



この展示物ではどのコンポーネントを識別できますか?
A. ローカルマシン上の信頼されたルート証明書ストア
B. Windows PowerShell 動詞
C. Windows レジストリ ハイブ
D. Windows サービス マネージャーのローカル サービス
正解: **(**正解を表示します**)**
The exhibit shows "HKEY_LOCAL_MACHINE," which is a Windows Registry hive. The registry is a database used to store low-level settings for the operating system and for applications that opt to use the registry. The other options are not related to the exhibit, as they are either a part of the Windows Certificate Manager, a naming convention for Windows PowerShell commands, or a component of the Windows Services Manager. References := Cisco Cybersecurity
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives
https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%
20registry%20hive%20contains,detected%20hardware%20and%20device%20drivers.

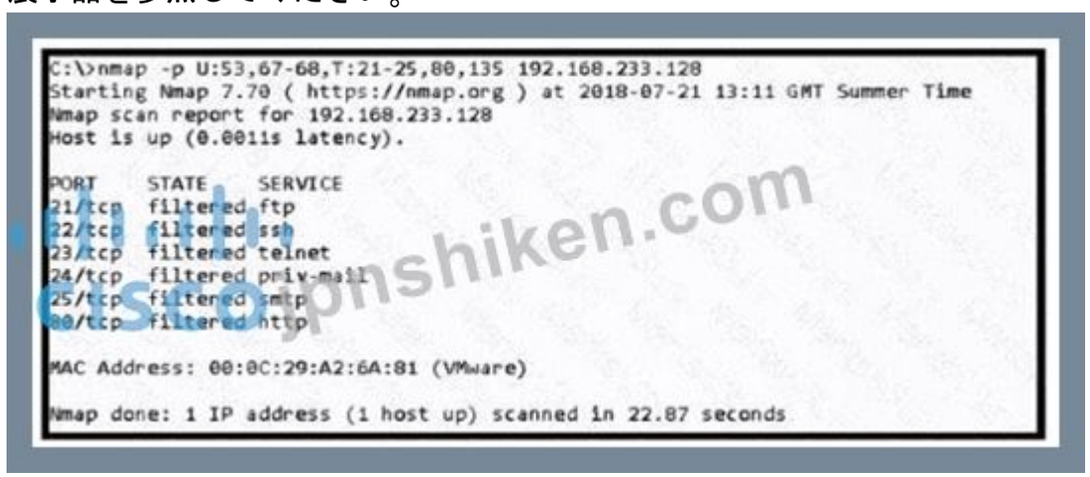
質問: **101**
回避技術とは何ですか?
A. アプリケーションまたはシステムに安全でない悪意のあるコードを挿入する
B. 侵入防止システムデータベースから更新ソースを削除する
C. 1つ以上の数学的手法を使用してデジタルデータをブロックする
D. ウイルス対策データベースに存在しないシグネチャを構築するペイロードを構築する
正解: **D (**コメントを発表する**)**

質問: **102**
SOC 環境での脆弱性管理指標とは何ですか?
A. コード署名の実施
B. フルアセットスキャン
C. インターネットに公開されたデバイス
D. 単一要素認証
正解: **(**正解を表示します**)**
In a Security Operations Center (SOC) environment, a vulnerability management metric is a quantifiable measure used to assess the effectiveness of the vulnerability management program. A full assets scan is a metric that can be used to determine the coverage and frequency of vulnerability scans across all assets. This helps in identifying unscanned assets and ensuring that all parts of the network are regularly checked for vulnerabilities1.
References :=

SOC Metrics: Security Metrics & KPIs for Measuring SOC Success
Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Vulnerability Management Program Top 10 Vulnerability Management Metrics & KPIs To Measure Success

質問: **103**
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アーティファクトはどれですか?
A. ファイルのタイムスタンプ
B. ファイル拡張子
C. ファイルサイズ
D. ファイルハッシュ
正解: **(**正解を表示します**)**
A file hash is a unique identifier that is used to detect a specific file. It is generated by running a file through a cryptographic hash function, which produces a string of characters that represents the contents of the file. If even a single bit in the file changes, the resulting hash will be different, making it an effective way to identify files uniquely.

質問: **104**
展示品を参照してください。



攻撃者は Nmap を使用してサーバーをスキャンしました。
攻撃者はこのスキャンから何を入手したのでしょうか?
A. Active Directory ユーザーのリストを収集しました。
B. サーバー上で開いているSMBポートを特定しました
C. ポート状態が返されない原因となっているファイアウォールデバイスを特定しました
D. サーバー上で実行されているプロセスに関する情報を収集しました
正解: **(**正解を表示します**)**

質問: **105**
正当なトラフィックをブロックすることでネットワーク トラフィックに影響を与えるシグネチャはどれですか?
A. 偽陰性
B. 真陽性
C. 真陰性
D. 偽陽性

正解: **(**正解を表示します**)**
A false positive in network security is when a benign action is incorrectly flagged as malicious, leading to legitimate traffic being blocked. This can disrupt normal network operations and access to services, as the security system mistakenly identifies normal behavior as a threat1.
References := The concept of false positives and their impact on network traffic is discussed in various cybersecurity resources, including Cisco's own training materials and discussions on network security best practices1.

質問: **106**
攻撃対象領域と脆弱性の違いは何ですか?
A. 攻撃対象領域とは、システムまたはリソースを利用する方法であり、脆弱性とは、脆弱性によって利用される特定の手法です。
B. 攻撃対象領域は、ソフトウェアまたはシステムが潜在的な攻撃に対してどのようにさらされるかを表し、脆弱性は潜在的なリスクを露出させる実際の弱点です。
C. 脆弱性はシステムまたはリソースを悪用する方法であり、攻撃対象領域は脆弱性によって利用される特定の手法です。
D. 脆弱性は、ソフトウェアまたはシステムが潜在的な攻撃に対してどのようにさらされるかを表し、攻撃対象領域は潜在的なリスクを露出させる実際の弱点です。
正解: **B (**コメントを発表する**)**

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu **564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
NISTSP800-86によると。揮発性と見なされる2種類のデータはどれですか？ 2つ選択してください。）
A. ファイルを交換する
B. 一時ファイル
C. ログインセッション
D. ダンプファイル
E. 空き容量
正解: **(**正解を表示します**)**
Volatile data is information that is stored in memory or other temporary storage that is lost when the power is turned off or lost. According to NIST SP 800-86, login sessions and swap files are considered volatile because they exist in the system's memory and can be lost or changed rapidly

質問: **108**
サイバーキルチェーンモデルの武器化ステップに一致するアクションはどれですか?
A. 脆弱なサーバーを悪用するための特定のマルウェアを開発する
B. 既知のスクリプトを脆弱性に一致させます。
C. トロイの木馬を作成し、!! を被害者に配信します。
D. サーバー上の開いているサービスとポートをスキャンします。
正解: **C (**コメントを発表する**)**

The weaponization step in the Cyber Kill Chain Model involves the creation or use of a specific weapon (malware, exploit) designed to leverage a vulnerability. This phase follows the reconnaissance phase where the attacker gathers information and precedes the delivery phase where the weapon is delivered to the target. Developing specific malware to exploit a vulnerable server is a precise example of weaponization.
References
Lockheed Martin Cyber Kill Chain Model
Understanding the Weaponization Phase in Cyber Attacks
Steps in the Cyber Kill Chain

質問: **109**
フォレンジック調査員が最近の侵害事件を分析しています。外部 USB ドライブが接続され、組織外にデータを送信していることが判明しましたが、USB ドライブの所有者は特定できませんでした。ビデオ監視により、2 か月間に 6 人が影響を受けた資産と密接な接触があったことが示されています。このような種類の証拠はどのように分類する必要がありますか?
A. 直接的な証拠
B. 間接的な証拠
C. 補強証拠
D. 最良の証拠
正解: **(**正解を表示します**)**

質問: **110**
ソーシャル エンジニアリング攻撃を説明するシナリオはどれですか。
A. 企業のセキュリティに関する情報を収集しようとする悪意のある内部者
B. 最近、機密情報が盗まれたデータ侵害が発生した企業
C. 悪意のあるURLを記載した、正当な企業を装ったテキストメッセージ
D. ワークステーションで不審なファイルが検出されました
正解: **(**正解を表示します**)**

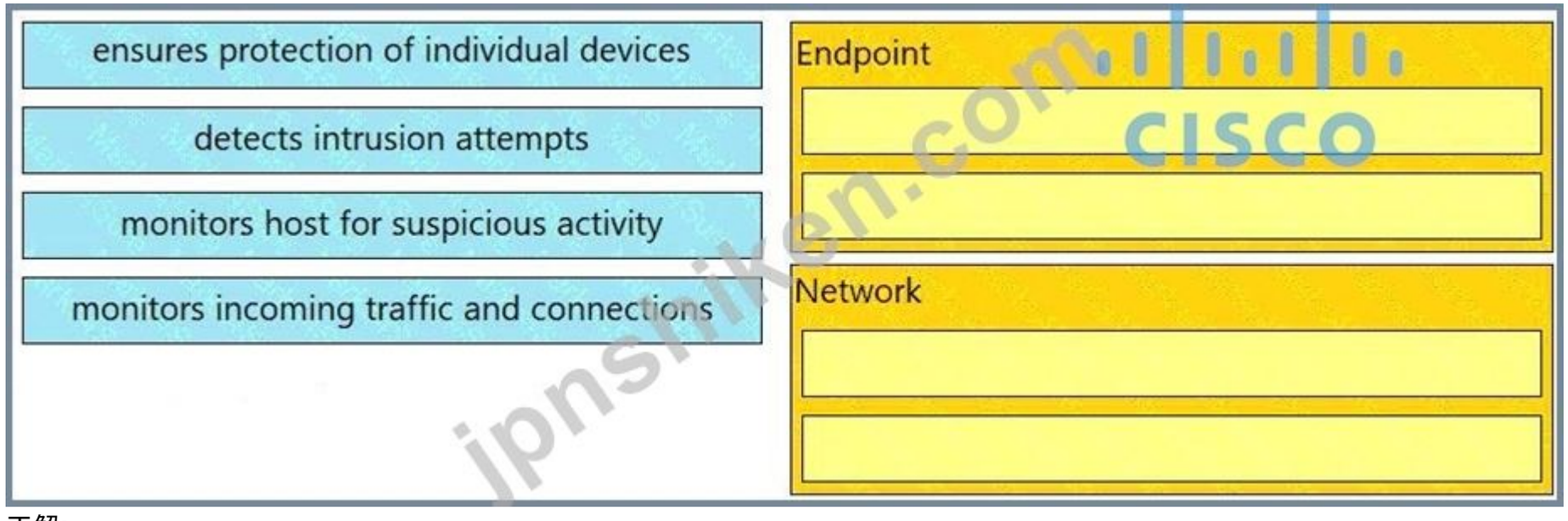
質問: **111**
NetFlow はトラフィック ミラーリングとどのように違いますか?
A. NetFlow はメタデータとトラフィック ミラーリング クローン データを収集します。
B. トラフィック ミラーリングはスイッチのパフォーマンスに影響を与えますが、NetFlow には影響しません。
C. トラフィック ミラーリングは、NetFlow よりも運用コストが低くなります。
D. NetFlow は、トラフィック ミラーリングよりも多くのデータを生成します。
正解: **(**正解を表示します**)**
NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic. It collects metadata of the IP traffic flowing across networking devices like routers and switches. On the other hand, Traffic mirroring involves capturing all the data packets that flow through a particular point in the network to analyze or inspect them later. References := Cisco Cybersecurity Operations Fundamentals

質問: **112**
揮発性の証拠を説明するものはどれですか?
A. ログ

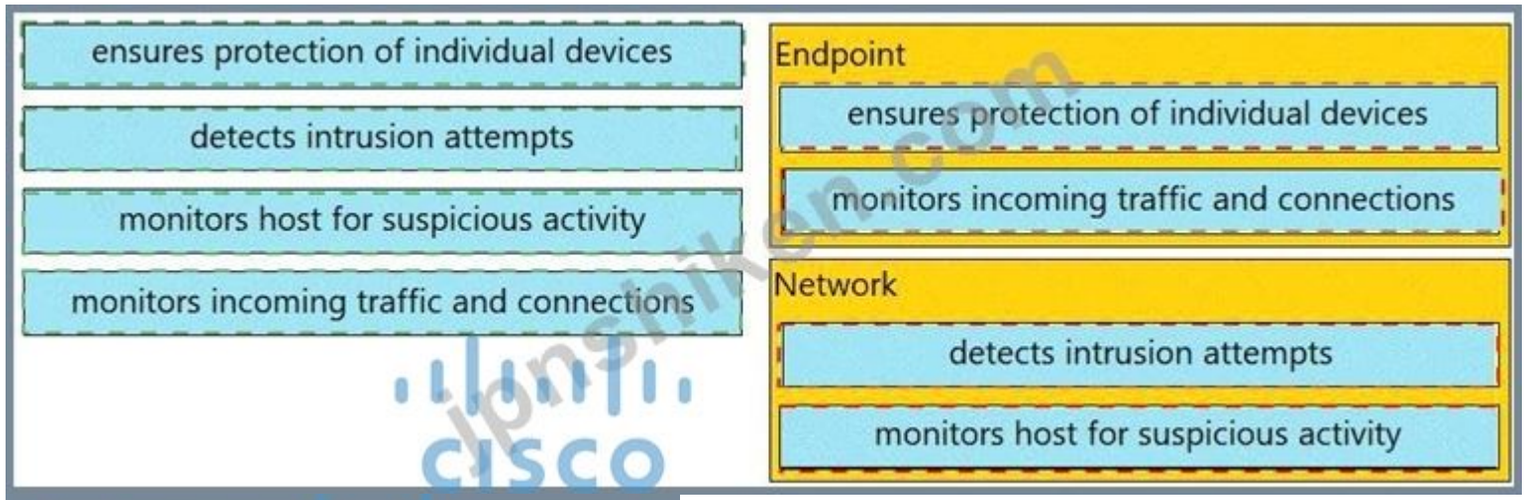
B. レジスタとキャッシュ
C. ディスクとリムーバブルドライブ
D. ユーザー名
正解: **B** (コメントを発表する)

質問: **113**
2つのサービス拒否攻撃はどれですか？ 2つ選択してください。）
A. TCP connections
B. ping of death
C. man-in-the-middle
D. code-red
E. UDP flooding
正解: (正解を表示します)
The ping of death is a type of attack that involves sending oversized or malformed packets using the ICMP protocol to crash, freeze, or reboot the target system1.
UDP flooding is an attack method that sends a large number of User Datagram Protocol (UDP) packets to random ports on a remote host, causing the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP Destination Unreachable packet. This process can saturate the network and the resources of the host, leading to denial of service2.
Cloudflare's explanation of common DoS attacks1.
Wikipedia's description of denial-of-service attack methods

質問: **114**
左側の用途を右側のセキュリティ システムの種類にドラッグ アンド ドロップします。



正解:





質問: **115**
疑わしいユーザーが、組織内の侵害されたホストから接続を開きました。トラフィックはルーターを通過しており、ネットワーク管理者はこのフローを特定できました。管理者は、必要なデータを収集するために 5 タプルに従っていました。このアプローチに基づいて収集された情報はどれですか?
A. NAT
B. ユーザー名
C. プロトコル
D. 直接パス
正解: **A (**コメントを発表する**)**

質問: **116**
従業員は、同僚のアドレスからドメインコントローラーのパスワードを要求する電子メールを受信しました。
従業員は、送信者のアドレス内に文字がないことに気づきました。この事件は何を説明していますか？
A. ブルートフォース攻撃
B. インサイダー攻撃
C. ショルダーサーフィン
D. ソーシャルエンジニアリング
正解: **(**正解を表示します**)**
Social engineering is a tactic used by attackers to manipulate individuals into divulging confidential information, such as passwords. In this scenario, the attacker is impersonating a colleague by using a similar email address with a missing letter, attempting to trick the employee into revealing sensitive information.

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course and materials provide insights into various types of cybersecurity threats, including social engineering, and how to recognize and respond to them.

質問: **117**
脅威ハンティングとは何ですか？
A. 潜在的な脅威を軽減するための脆弱性評価レポートの管理。
B. 侵入や侵害の可能性のある兆候を積極的に検出することに焦点を当てています。
C. インテリジェンスデータを取得するためにシステムに侵入するように競合他社と敵対者を追跡します。
D. サーバーの可用性を変更してサーバーを意図的に中断しようとしています
正解: **(**正解を表示します**)**
Threat hunting is a proactive cybersecurity technique that involves searching for indicators of compromise or signs of intrusion within an organization's network or systems. Unlike automated detection systems, threat hunting is typically carried out by security analysts who use their knowledge and intuition to identify subtle, unusual patterns that may indicate a security breach. The goal of threat hunting is to identify and mitigate threats before they can cause significant damage.
The CBROPS course material covers the concept of threat hunting as part of the skill set required for cybersecurity operations analysts, who are responsible for identifying and mitigating cyber threats

質問: **118**



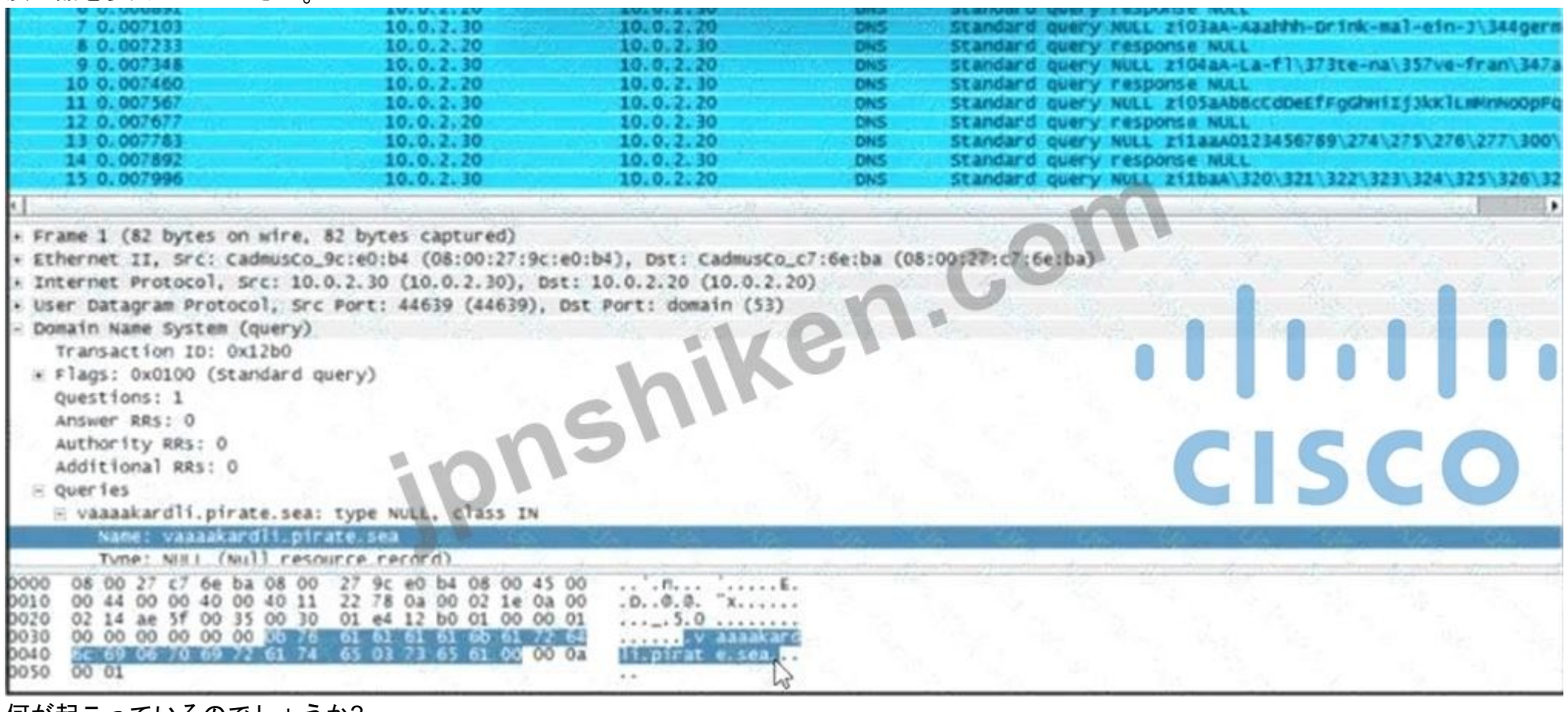
添付資料を参照してください。エンジニアは、これらのイベントをイベントログを生成したソーステクノロジーにマッピングする必要があります。生成されたログはどのテクノロジーに属しているのでしょうか？
A. プロキシ
B. ファイアウォール
C. ウイルス対策
D. IPS
正解: **D (**コメントを発表する**)**

質問: **119**
ACK フラグと RST フラグの違いは何ですか?
A. ACK フラグはストリーム内の前のパケットの受信を検証し、同じセッションが RST フラグによって閉じられています。
B. RST フラグは通信を確立し、ACK フラグは、期待するホストに明示的に送信されなかった自発的な接続をキャンセルします。
C. ACK フラグは、宛先に送信される次のパケットを検証し、RST フラグは、宛先が到達可能であることを示すために RST が返すものです。
D. RST フラグは、ハンドシェイク プロセス内で接続が信頼できるものであることを識別し、ACK フラグは、送信元と宛先の間でセッションを開いて応答を準備します。
正解: **(**正解を表示します**)**

ipnshiken.com

質問: **120**
改ざんされたディスクイメージと改ざんされていないディスクイメージの違いは何ですか?
A. 改ざんされたイメージには、同じ保存および計算されたハッシュが含まれます。
B. 改ざんされていない画像は、証拠として保存するために意図的に変更されています。
C. 改ざんされた画像が証拠として使用されます。
D. 改ざんされていないイメージはフォレンジック調査に使用されます。
正解: **(**正解を表示します**)**
The difference between tampered and untampered disk images is:
Tampered Images: These are disk images that have been altered or modified in some way after their initial creation. The stored hash and the computed hash will not match if the image has been tampered with.
Untampered Images: These are disk images that have not been altered since their creation. They are considered authentic and reliable for forensic investigations. The stored hash and the computed hash will match, confirming that the image has remained unchanged.
Therefore, the correct answer is: D. Untampered images are used for forensic investigations.

質問: **121**
展示品を参照してください。



jpnshiken.com

何が起こっているのでしょうか?
A. ARPフラッド
B. DNS増幅
C. ARP ポイズニング
D. DNSトンネリング
正解: **B (**コメントを発表する**)**

DNS amplification is a type of Distributed Denial of Service (DDoS) attack where an attacker uses publicly accessible open DNS servers to flood a target with DNS response traffic. The goal is to overwhelm the target with traffic, causing a denial of service.

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu **564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
ペイロードとヘッダー情報を分析するためにエンジニアはどのタイプのデータを取得する必要がありますか?
A. フレームチェックシーケンス
B. アラート データ
C. フルパケット
D. セッションログ
正解: **C** (コメントを発表する)
To analyze both payload and header information, an engineer must capture the full packet data. This includes all protocol and payload information for the traffic, allowing for a comprehensive analysis of the data being transmitted5678. References: Full packet capture is a common practice in network monitoring and security, as it provides detailed insights into the data transmitted over the network, including both payload and header information

質問: **123**
セキュリティ専門家が、組織内で最近発生した重大な侵害に関するインシデントを調査しています。部門の重要なサーバーでトロイの木馬が検出されたため、24か月間の会計データが影響を受けています。セキュリティ アナリストがインシデントを調査し、定期的な AV スキャン中にトロイの木馬を検出したインシデント対応チームのメンバーが証拠目的でサーバーのイメージを作成していたことを発見しました。セキュリティ アナリストは、2 つのイメージのハッシュを比較するために再度イメージを作成しましたが、それらは異なっており、一致しませんでした。
セキュリティアナリストはどのような種類の証拠を扱っていますか?
A. 整合性が侵害された画像
B. チェックサム違反の画像
C. 改ざんされた画像
D. 改ざんされていない画像
正解: (正解を表示します)

質問: **124**
脆弱性管理フレームワークの目的は何ですか?
A. システムの脆弱性を特定、削除、および軽減します
B. ソースコードの脆弱性を検出して削除します
C. ネットワーク上で脆弱性スキャンを実行します
D. 報告された脆弱性のリストを管理します
正解: (正解を表示します)

A vulnerability management framework is a set of processes and tools that helps an organization identify, assess, prioritize, remediate, and mitigate system vulnerabilities. A vulnerability management framework aims to reduce the attack surface and the risk of compromise by applying security patches, hardening configurations, implementing security controls, and monitoring the system status. A vulnerability management framework is an essential component of a security operations center (SOC). References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 2-14; 200-201 CBROPS - Cisco, exam topic 1.2.b

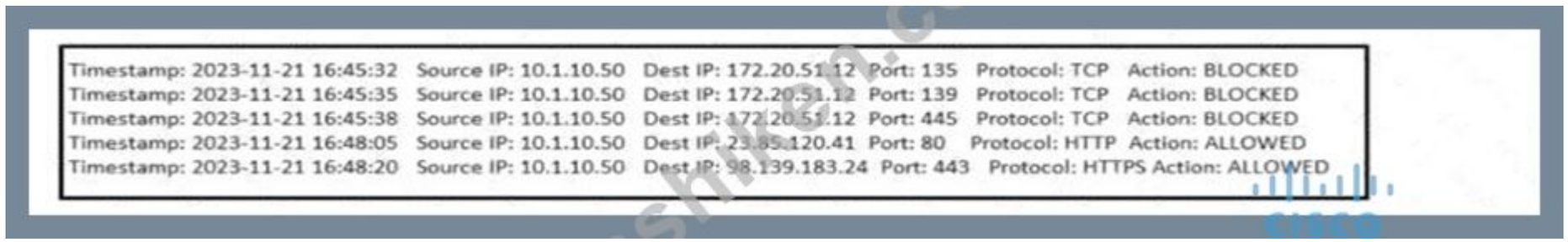
質問: **125**
この正規表現は何をするのでしょうか?
192|172).(168|1[6-9]|2[0-9]|3[0-1]).[0-9]{1,3}.[0-9]{1,3}\b
A. 172.16.0.0/16 IP アドレス範囲内の任意の IP アドレスに一致します。
B. 10.0.0.0/8 IP アドレス範囲を除くプライベート IP アドレスを検索します。
C. テキストから 192.168.0.0/16 の IP アドレス範囲を含む行を抽出します。
D. テキスト内にプライベート IP アドレスが含まれる行を検索します。
正解: **B (**コメントを発表する**)**

質問: **126**
組織の IT インフラストラクチャに存在する既知の弱点や欠陥を検索して報告するテクノロジの名前は何ですか?
A. 脆弱性スキャナー
B. アイデンティティとアクセス管理
C. 構成管理
D. モバイルデバイス管理
正解: **(**正解を表示します**)**
A vulnerability scanner is a core security technology used to identify known weaknesses, misconfigurations, and exploitable flaws within an organization's IT infrastructure. These tools systematically scan systems, networks, applications, and devices to compare them against databases of known vulnerabilities, such as missing patches, insecure services, outdated software versions, and weak configurations.
Vulnerability scanners operate by probing systems using signatures, checks, and authenticated or unauthenticated methods to determine exposure to threats. The results are typically presented in detailed reports that include severity ratings, affected assets, and remediation guidance. This makes vulnerability scanning an essential foundational activity in cybersecurity operations, risk management, and compliance programs.
The other options do not fulfill this function. Identity and access management focuses on user authentication, authorization, and access control, not weakness detection. Configuration management ensures systems remain in a desired state but does not actively discover vulnerabilities. Mobile device management is limited to controlling and securing mobile endpoints rather than assessing infrastructure-wide weaknesses.
From an operational perspective, vulnerability scanning supports proactive defense by allowing organizations to identify and remediate issues before attackers exploit them. It is commonly integrated into continuous monitoring programs, patch management workflows, and security assessments. As emphasized in cybersecurity operations documentation, vulnerability scanners are a primary mechanism for visibility into an organization's attack surface.

質問: **127**
SQL インジェクションはどのように防止されますか?
A. アドレス空間レイアウトのランダム化
B. ユーザー入力を検証し、サニタイズします。
C. ...非特権ユーザーとして Web サーバー内で

D. ...コストプロファイリング
正解: **(**正解を表示します**)**
* SQL injection is a type of injection attack where malicious SQL statements are inserted into an entry field for execution.
* The primary way to prevent SQL injection is by validating and sanitizing user input. This involves checking the input for malicious content and ensuring it adheres to expected patterns.
* Prepared statements (parameterized queries) are also highly effective, as they treat user input as data rather than executable code.
* Implementing these practices ensures that any input received from users does not manipulate SQL queries in a harmful way.
References
* OWASP SQL Injection Prevention Cheat Sheet
* Best Practices for Input Validation and Sanitization
* Secure Coding Guidelines

質問: **128**
ハイエンド テクノロジーを開発する組織が内部監査を受けています。組織は 2 つのデータベースを使用しています。メイン データベースには特許情報が保存され、セカンダリ データベースには従業員の名前と連絡先情報が保存されます。コンプライアンス チームは、インフラストラクチャを分析して保護されたデータを特定するよう求められます。この 2 つのうちどれですか保護されるデータの種類を特定する必要がありますか? (2つお選びください)
A. 個人識別情報 (PII)
B. ペイメント カード業界 (PCI)
C. 保護された炉床情報 (PHI)
D. 知的財産 (IP)
E. サーベンス -オクスリー法 (SOX)
正解: **(**正解を表示します**)**
Protected data refers to any information that is legally guarded or sensitive due to its nature. In the context of the organization described, the main database contains Intellectual Property (IP), which includes patents that are legally protected forms of inventions and designs. The secondary database holds Personally Identifiable Information (PII), which comprises data that can be used to identify individuals, such as names and contact details. Both IP and PII are considered protected data and should be identified during an internal audit to ensure they are handled according to legal and regulatory standards. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

質問: **129**


展示を参照してください。どのような種類のイベントが行われていますか？
A. 分散型サービス拒否(DDoS)攻撃
B. マルウェアが横方向に拡散しようとしている
C. 正当なウェブ閲覧アクティビティ
D. ユーザーがファイル共有にアクセスしようとしています
正解: **B (**コメントを発表する**)**

質問: **130**
認証局はセキュリティにどのように影響しますか？
A. サーバーと通信するときにクライアントIDを検証します。
B. SSL証明書を要求するときにクライアントIDを認証します。
C. SSL証明書を要求するときにドメインIDを認証します。
D. SSL証明書のドメインIDを検証します。
正解: **D (**コメントを発表する**)**
A certificate authority (CA) is a trusted entity that issues and manages digital certificates for secure communication over the internet. A digital certificate is a document that contains the public key and the identity of the owner of the key. A CA impacts security by validating the domain identity of the SSL certificate, which is a type of digital certificate that enables encrypted communication between a web server and a web browser. The CA verifies that the domain name in the certificate matches the domain name of the web server, and signs the certificate with its own private key. The web browser can then verify the signature of the CA and trust the identity of the web server. References := Cisco Cybersecurity Operations Fundamentals, Module 2: Security Monitoring, Lesson 2.3: Cryptography and PKI, Topic 2.3.2: Public Key InfrastructureReference: https://en.wikipedia.org/wiki/Certificate_authority

質問: **131**
検出を防ぐために通常よりも遅いアクションを実行する回避方法はどれですか?
A. タイミング攻撃
B. トラフィックの断片化
C. リソースが枯渇しました
D. トンネリング
正解: **B (**コメントを発表する**)**
Traffic fragmentation is an evasion technique where an attacker splits malicious payloads into smaller packets. This can help avoid detection since some security systems may not reassemble these packets to inspect the complete payload.

質問: **132**
システム管理者は、特定のレジストリ情報が正確であることを確認しています。
HKEY_LOCAL_MACHINE ハイブにはどのタイプの構成情報が含まれていますか?
A. ファイル拡張子の関連付け
B. システムのハードウェア、ソフトウェア、およびセキュリティ設定
C. 現在ログインしているユーザー (フォルダーとコントロール パネルの設定を含む)
D. ビジュアル設定を含む、システム上のすべてのユーザー
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

質問: **133**
エンジニアは、NISTフレームワークとISOフレームワークを比較する必要があります。エンジニアは、読み取り可能なドキュメントとして比較し、比較ビデオレビューを視聴することを行いました。Windows10OSを使用します。エンジニアはブラウザを起動してNISTドキュメントを検索し、同じブラウザで新しいタブを開いて比較のためにISOドキュメントを検索しましたエンジニアはビデオを見ようとしましたが、OSに音声の問題があったため、エンジニアはトラブルシューティ

ングするには最初に、エンジニアはCMDを起動し、ドライバパスを調べてから、レジストリエディタで対応するレジストリをロックしました。エンジニアはタスクマネージャで 'Audiosrv」を有効にして自動起動し、問題は解決しました。エンジニアはOSに触れましたか？ 2つ選択してください）

A. 権限
B. PowerShellログ
C. サービス
D. MBR
E. プロセスとスレッド

正解: **C,E** (コメントを発表する)

The engineer engaged with the service component by enabling "Audiosrv," which is the Windows Audio Service responsible for managing audio for Windows-based programs. By setting it to auto-start, the engineer ensured that the service would run automatically upon system startup. Additionally, the engineer interacted with process and thread management by using the Task Manager to modify the behavior of the "Audiosrv" service.
The information is based on standard operating procedures for troubleshooting audio issues in Windows OS, which involves services and processes management.

質問: **134**

ネットワーク セキュリティにおいてセッション データはどのような目的で使用されますか?

A. ユーザーが開始した各セッション内の Cookie を追跡します。
B. 2 つのネットワーク デバイス間の送信の概要です。
C. 監視ソフトウェア間のトランザクションログです。
D. ログの取得に使用されるパラメータのセットが含まれます。

正解: (正解を表示します)

質問: **135**

随意アクセス制御（DAC）と役割ベースのアクセス制御（RBAC）の違いは何ですか？

A. DACには、特定のオブジェクトに対する特定のユーザーの明示的な承認が必要であり、RBACには特定の条件が必要です。
B. ユーザーが特定の条件を満たすとRBACアクセスが許可され、DACではユーザーおよびグループレベルで権限が適用されます。
C. RBACはDACの拡張バージョンであり、時間に基づいて認証のレベルを追加できます。
D. DAC管理者はユーザーとグループに権限を渡し、RBACでは権限が特定のグループに適用されます

正解: (正解を表示します)

In RBAC, access is based on the roles that users have within an organization, and permissions to perform certain operations are assigned to specific roles. DAC, on the other hand, is a type of access control where the access rights are determined by the owner of the resource or the resource itself.

質問: **136**

展示品を参照してください。



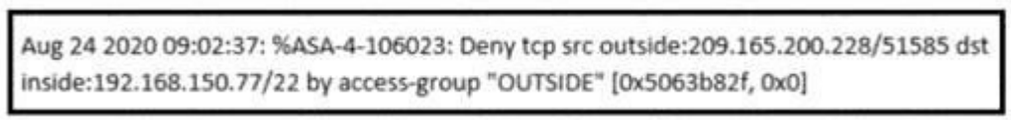
どの技術でログが生成されましたか?

A. antivirus

B. IPS/IDS
C. proxy
D. firewall
正解: (正解を表示します)
The log in the exhibit is generated by an Intrusion Prevention System (IPS) or Intrusion Detection System (IDS). It contains information about a TCP connection attempt, including the source IP address, destination IP address, and other details related to the connection. The presence of "TCP MISS" indicates that the system detected an anomaly or potential threat during the connection attempt. References := Cisco Cybersecurity Operations Fundamentals

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
展示を参照してください。



アナリストはCiscoASAデバイスからこのアラートを受信し、多数のアクティビティログが生成されました。このタイプの証拠はどのように分類されるべきですか？
A. 間接
B. 状況
C. 裏付け
D. 最高
正解: (正解を表示します)
The alert from the Cisco ASA device and the numerous activity logs are examples of circumstantial evidence.
Circumstantial evidence is evidence that relies on an inference or deduction to connect it to a conclusion of fact, such as a security incident or an attack. Circumstantial evidence does not directly prove the fact in question, but rather suggests or implies it. In this case, the alert and the logs indicate that a TCP connection attempt was denied by an access group, but they do not directly prove that an attack occurred or who was behind it. There could be other explanations for the denied connection, such as a misconfiguration, a network error, or a legitimate request. Therefore, this type of evidence is circumstantial and requires further investigation and analysis to confirm or rule out the possibility of an attack. References := Circumstantial evidence - Wikipedia; Circumstantial Evidence - Definition, Examples, Cases, Processes; Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 92.

質問: **138**
会社の受付係は、資産を盗むという脅迫の電話を受けましたが、それがソーシャル エンジニアリングの試みであると仮定して、何も行動を起こしませんでした。48 時間以内に複数の資産が侵害され、機密情報の機密性に影響しました。この事件の犯人は?
A. 脅威にさらされている会社の資産
B. 脅威にさらされている顧客資産
C. 攻撃の加害者
D. 攻撃の犠牲者

正解: (正解を表示します)
In this scenario, the threat actor refers to the individuals or entities responsible for the attack that resulted in a breach of assets and sensitive information. The receptionist received a threatening call but did not take action, leading to an actual breach within 48 hours. References: The explanation is inferred from general cybersecurity knowledge as specific details are not provided in the Cisco Cybersecurity documents linked.

質問: **139**
SSL 証明書は、クライアントとサーバー間のセキュリティにどのように影響しますか?
A. クライアントとサーバー間の認証されたチャネルを有効にすることによって
B. クライアントとサーバー間の統合チャネルを作成することにより
C. クライアントとサーバー間の承認されたチャネルを有効にすることにより
D. クライアントとサーバーの間に暗号化されたチャネルを作成することによって
正解: (正解を表示します)
An SSL certificate enables the establishment of a secure connection between the client and the server using the TLS protocol. The client and the server exchange keys and agree on a cipher suite to encrypt and decrypt the data transmitted over the network. References := Cisco Cybersecurity Source Documents

質問: **140**
コンプライアンスアナリストは、顧客から、削除依頼にもかかわらず個人データが不法に保持されているという苦情を受けました。この企業は欧州に拠点を置いており、GDPRを遵守する必要があります。収集されるデータはメールアドレス0524l9i75@gmail.comのみです。コンプライアンスアナリストはどのように対応すべきでしょうか?
A. データを削除しないでください。メールアドレスはPIIとはみなされません。
B. 顧客の出身地に関係なくデータを削除します
C. 顧客がEU出身の場合はデータを削除します
D. データコンプライアンス違反について法務チームに通知する
正解: (正解を表示します)
Under the General Data Protection Regulation (GDPR), an email address that can be linked to an individual is classified as personal data, regardless of whether it contains a real name. The regulation grants individuals the right to erasure, also known as the "right to be forgotten," when they request deletion of their personal data and no lawful basis for retention exists.
Because the company is based in Europe, GDPR applies to its data processing activities. Additionally, GDPR protections extend not only to EU citizens but also to any individual whose data is processed by an EU- based organization, depending on context. Therefore, deletion should not be conditional on the customer's geographic location.
Option A is incorrect because email addresses are considered personal data under GDPR. Option C is incomplete and misleading because GDPR obligations are not limited only to confirmed EU residents in this scenario. Option D may be appropriate if systemic noncompliance is identified, but the immediate and correct action is to honor the deletion request.
Cybersecurity and compliance documentation emphasizes minimizing data retention and responding promptly to data subject requests. As no lawful justification for retaining the email exists, it must be deleted.
Therefore, the correct action is to delete the data regardless of where the customer is from.

質問: **141**
2 つのエンドポイント間で TLS が観察される場合、どの回避方法が使用されていますか?
A. X.509証明書認証

B. 難読化
C. トラフィック挿入
D. 暗号化
正解: (正解を表示します)

質問: **142**
インシデント対応プロセスのどのステップで、SIEM のログを通じて攻撃しているホストを調査しますか?
A. 検出と分析
B. 準備
C. 根絶
D. 封じ込め
正解: (正解を表示します)
In the incident response process, detection and analysis involve researching an attacking host through logs in a Security Information and Event Management (SIEM) system. This step helps in identifying, validating, and managing potential security incidents. References := Cisco CyberOps Associate - Module 3: Security Monitoring

質問: **143**
最も多くのストレージ スペースを必要とするデータ収集のタイプはどれですか?
A. alert data
B. transaction data
C. session data
D. full packet capture
正解: (正解を表示します)
Full packet capture requires the largest amount of storage space because it involves recording all packets that pass through a network, including all headers and payloads. This type of data collection is comprehensive and allows for detailed analysis, but due to the volume of data it encompasses, it demands significant storage capacity1.
References := The Cisco Secure Network Analytics Data Store Design Guide discusses the storage requirements for different types of network data collection, highlighting the substantial storage needs for full packet captures1.

質問: **144**
Heartbleed 脆弱性とは何ですか?
A. バッファオーバーフロー
B. サービス拒否
C. 情報開示
D. コマンドインジェクション
正解: (正解を表示します)

質問: **145**
最大のストレージ スペースを必要とするセキュリティ監視データの種類は?
A. トランザクションデータ

B. 統計データ
C. セッションデータ
D. 完全なパケット キャプチャ
正解: **D** (コメントを発表する)
Full packet capture data involves storing the entire content of packets that traverse a network. This type of data is comprehensive and allows for detailed analysis but requires a significant amount of storage space compared to other data types like transaction, statistical, or session data. References := Cisco Cybersecurity Operations Fundamentals - Module 3: Network Data and Event Analysis

質問: **146**
ディープパケットインスペクションとステートフルインスペクションの違いは何ですか？
A. ディープパケットインスペクションはレイヤー7までの洞察を提供し、ステートフルインスペクションはレイヤー4までの洞察のみを提供します。
B. ディープパケットインスペクションは、その複雑な署名により安全性が高く、ステートフルインスペクションでは人の介入が少なくて済みます。
C. ステートフルインスペクションは、その複雑な署名により安全性が高く、ディープパケットインスペクションは人間の介入が少なくて済みます。
D. ステートフルインスペクションはトランスポート層でデータを検証し、ディープパケットインスペクションはアプリケーション層でデータを検証します
正解: (正解を表示します)
Deep packet inspection (DPI) analyzes the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination. Stateful inspection, on the other hand, tracks the state of active connections and determines which network packets to allow through the firewall. While stateful inspection tracks the state of connections (Layer 4 - transport layer), DPI goes further by examining the payload of the packet (Layer 7 - application layer).
Cisco's official documentation and cybersecurity courses would explain the differences between deep packet inspection and stateful inspection, including their respective layers of operation.

質問: **147**
どの攻撃がリソース枯渇の回避手法を表していますか？
A. SQLインジェクション
B. 中間者
C. ブルースナーフィング
D. サービス拒否
正解: (正解を表示します)
A denial-of-service attack represents the evasion technique of resource exhaustion, where the attacker overwhelms a system's resources, making the system unusable and unable to handle legitimate requests. References := Cisco Cybersecurity Source Documents
Reference:https://www.ciscopress.com/articles/article.asp?p=3100055&seqNum=3

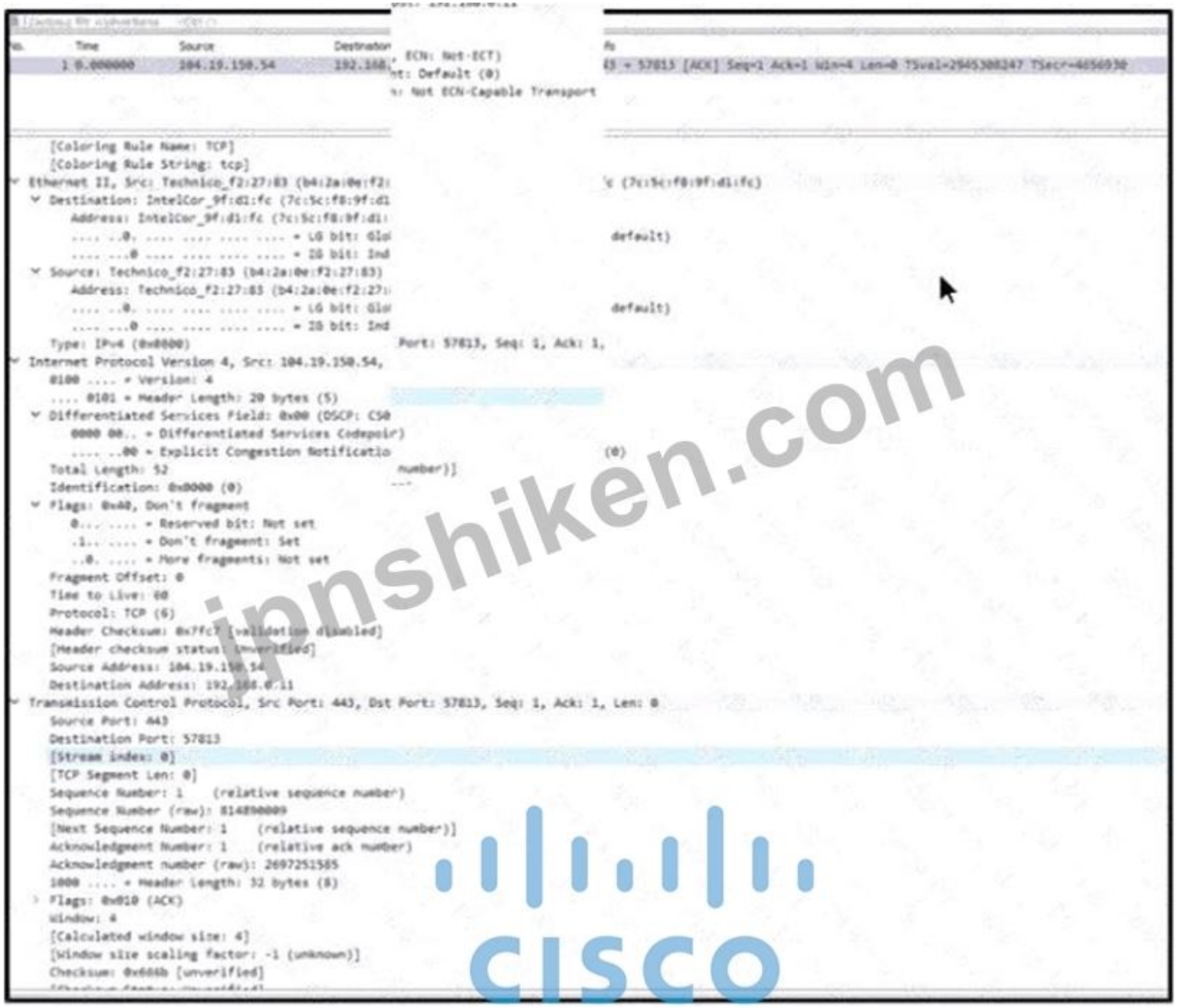
質問: **148**
脆弱性への攻撃はどのように分類されますか?
A. 目標に対するアクション
B. 配達
C. 搾取
D. インストール
正解: (正解を表示します)

Attacking a vulnerability is categorized as exploitation, which is the third phase of the cyberattack lifecycle.
Exploitation is the process of taking advantage of a vulnerability in a system, application, or network to gain access, escalate privileges, or execute commands. Action on objectives, delivery, and installation are other phases of the cyberattack lifecycle, but they do not involve attacking a vulnerability. Action on objectives is the final phase, where the attacker achieves their goal, such as stealing data, disrupting services, or destroying assets. Delivery is the second phase, where the attacker delivers the malicious payload, such as malware, phishing email, or malicious link, to the target. Installation is the fourth phase, where the attacker installs the malicious payload on the compromised system or network to maintain persistence or spread laterally. References: What is a Cyberattack? | IBM, Recognizing the seven stages of a cyber-attack - DNV

質問: **149**
セキュリティの専門家が、CDFS 形式で保存された ISO ファイルである証拠のコピーに取り組んでいます。このファイルはどのタイプの証拠ですか?
A. Windows で作成した CD データのコピー
B. Mac ベースのシステムで作成された CD データのコピー
C. Linux システムで作成された CD データのコピー
D. Android ベースのシステムで作成された CD データのコピー
正解: **A (**コメントを発表する**)**
The CDFS (Compact Disc File System) format is associated with the ISO 9660 standard, which is a file system for optical disc media. It is commonly used in Windows systems for CDs. When a security expert works on an ISO file saved in CDFS format, it typically indicates that the data was prepared or copied using a Windows-based system. This is because CDFS is the file system that Windows uses to read and write CDs, and the ISO file is an image of that CD data1.
References :=
* Understanding CDFS (Compact Disc File System): A Comprehensive Guide2.
* What type of evidence is this file? - VCEguide.com

質問: **150**
強制アクセス制御 (MAC) と任意アクセス制御 (DAC) の主な違いは何ですか?
A. MAC は最も厳格なアクセス制御であり、DAC はオブジェクトベースのアクセスです。
B. DAC は OS によって制御され、MAC はアクセス リストの所有者によって制御されます。
C. DAC は最も厳格なアクセス制御であり、MAC はオブジェクトベースのアクセスです。
D. MAC は OS によって制御され、DAC はアクセス リストの所有者によって制御されます。
正解: **(**正解を表示します**)**

質問: **151**



図を参照してください。エンジニアは、ログのグループ化されたセット内で侵害されたホストを分離するために、5タプルアプローチを使用する必要があります。エンジニアはどのデータを使用する必要がありますか?

A. b4:2a0ef227 83

B. 57813

C. 66

D. 7c:5c:f8:9f:d1:fc

正解: **(**正解を表示します**)**

ipnshiken.com

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
攻撃の痕跡（IoA）と侵入の痕跡（IoC）の違いは何ですか？
A. IoAはセキュリティ違反が発生した証拠であり、IoCを使用すると、組織は脆弱性が悪用される前に行動することができます。
B. IoAはセキュリティ違反の責任者を指し、IoCは結果として生じる損失を指します。
C. IoCはセキュリティ違反が発生した証拠であり、IoAを使用すると、組織は脆弱性が悪用される前に行動することができます。
D. IoCはセキュリティ違反の責任者を指し、IoAは結果として生じる損失を指します。
正解: **(**正解を表示します**)**
Indicators of Compromise (IoC) are pieces of forensic data, such as system log entries or files, that suggest an intrusion may have occurred. Indicators of Attack (IoA) are signs that an attack may be underway, allowing organizations to take action before any potential breach occurs.
The CBROPS course materials cover the concepts of IoC and IoA, explaining how they are used in cybersecurity operations to detect and prevent security incidents.

質問: **153**
非対称暗号を使用する利点は何ですか？
A. 1つのキーでデータを復号化します
B. 高速データ転送
C. 安全なデータ転送
D. 1つのキーでデータを暗号化します
正解: **(**正解を表示します**)**
Asymmetric cryptography, also known as public key cryptography, involves two keys: a public key for encryption and a private key for decryption. This method ensures that even if the public key is known, only the holder of the private key can decrypt the message, thus providing a secure way to transfer data. References: Asymmetric encryption is beneficial for secure data transfer because it allows message authentication, non-repudiation, and detects tampering, although it is slower than symmetric encryption

質問: **154**
展示品を参照してください。

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=1476292607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Wireshark 内で抽出可能なファイルが含まれているパケットはどれですか?
A. 2317
B. 1986
C. 2318
D. 2542
正解: **(**正解を表示します**)**
Packet number 2318 is the one that contains a file that is extractable within Wireshark. This can be determined by the information provided in the packet details, which typically includes an HTTP GET request indicating the retrieval of a file, such as an image or document1.

質問: **155**
脆弱性とリスクの違いは何ですか?
A. リスクとは潜在的な弱点の評価であり、脆弱性とは資産の再構成である。
B. リスクとは、エクスプロイトが適用される可能性のある危険であり、脆弱性とは、脅威の主体を表すものである。
C. 脆弱性は攻撃対象領域であり、リスクは攻撃のベクトルである。
D. 脆弱性とは悪用される可能性のある弱点であり、リスクとは損失や損害の可能性である。
正解: **(**正解を表示します**)**

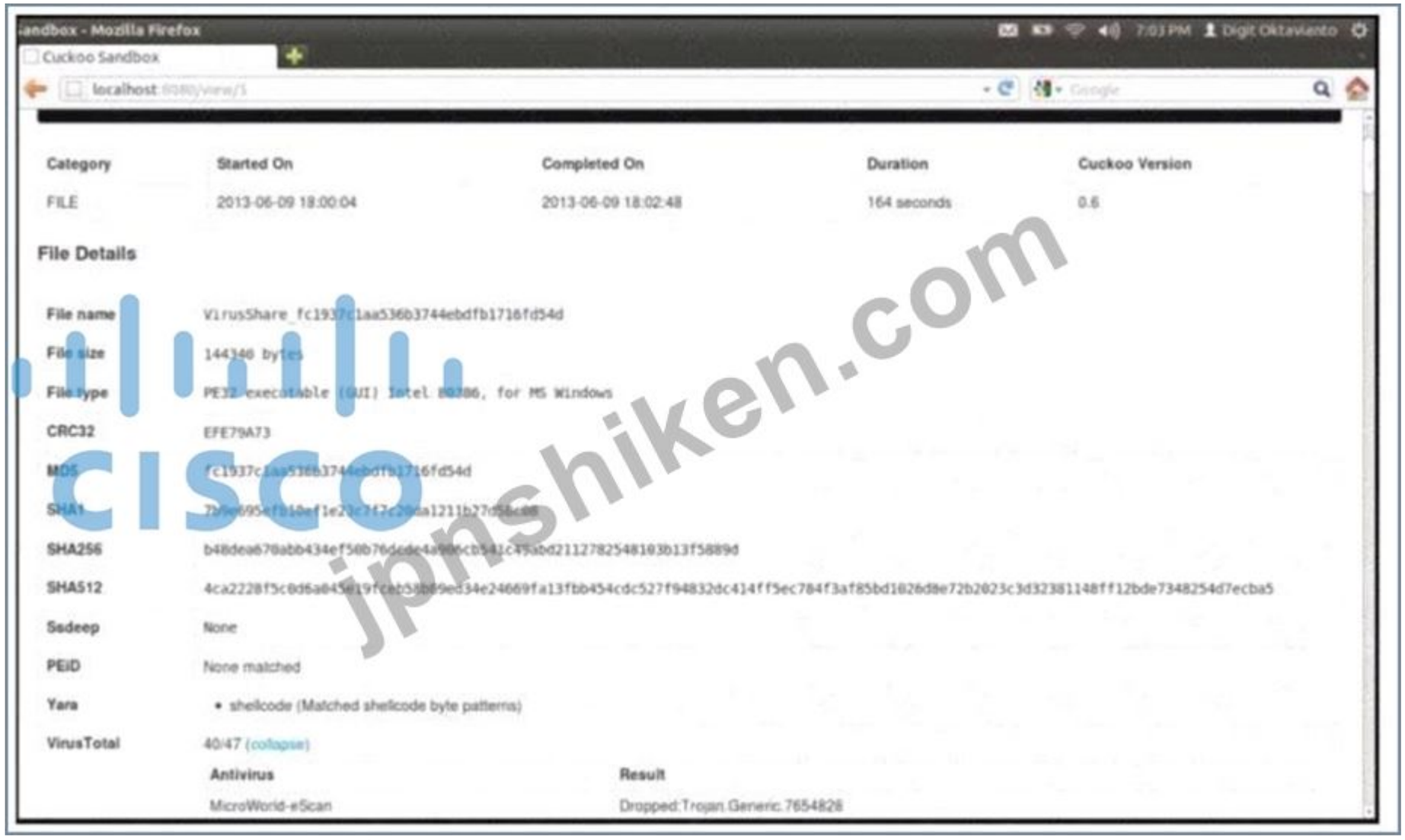
質問: **156**
メール転送エージェント (MTA) によって実装される電子メールのグレーリストとは何ですか?
A. 組織外から送信されたメールを隔離する
B. 認識されない送信者からのメールを拒否する
C. フィッシング詐欺の可能性があるメールを返す
D. 不明な送信者からのメールを一時的に許可する
正解: **D (**コメントを発表する**)**
Email greylisting is an anti-spam technique used by mail transfer agents to reduce unsolicited and malicious email traffic. When an email is received from an unknown sender, the MTA temporarily rejects the message with a request for retransmission. Legitimate mail servers are configured to retry delivery after a short delay, while many spam and malicious servers do not.
By allowing emails from unknown senders temporarily after a retry, greylisting effectively filters out a large volume of automated spam without relying on content inspection or signatures. This makes it a lightweight and effective control in email security architectures.
Option A describes quarantining, which is different from greylisting. Option B refers to permanent blocking, which greylisting does not do. Option C relates to phishing detection rather than delivery control behavior.
Security monitoring documentation highlights greylisting as a behavior-based control that leverages standard SMTP retry mechanisms. Once a sender successfully retries, they are typically whitelisted for future deliveries.
Therefore, email greylisting works by temporarily delaying emails from unknown senders, making Option D the correct answer.

質問: **157**
TORは転送中にデータコンテンツをどのように変更しますか？
A. 両側を保護する宛先およびソース情報をスプーフィングします。
B. コンテンツと宛先情報を複数のレイヤーで暗号化します。
C. トレーサビリティを回避して、宛先トラフィックを複数のソースにリダイレクトします。

D. 受信者に到達する前に、複数の宛先を経由して送信元トラフィックをトラバースします
正解: **(**正解を表示します**)**
TOR is a network that enables anonymous communication over the internet by routing the traffic through a series of relays or nodes. TOR alters the data content during transit by encrypting it and the destination information over multiple layers, using a technique called onion routing. Each layer of encryption can only be decrypted by a specific relay in the network, which reveals the next destination. This way, no single relay knows the complete path or the content of the data, making it difficult to trace or monitor the communication. References := Cisco Cybersecurity Operations Fundamentals, Module 2: Security Monitoring, Lesson 2.1: The Network as a Sensor, Topic 2.1.3: Network Data Exfiltration Techniques

質問: **158**
セキュリティ エンジニアは、アドウェアを引き起こす既知の問題から会社を守る必要があります。最近、システムに損害を与える可能性のある新たな事件が発生しました。このシナリオにはどのようなセキュリティ概念が存在しますか?
A. エクスプロイトとパッチ適用
B. リスクと証拠
C. 分析と修復
D. 脆弱性と脅威
正解: **D (**コメントを発表する**)**
* The security scenario involves protecting the company from known issues that trigger adware and addressing a recent incident that could harm the system.
* This scenario involves identifying vulnerabilities (weaknesses in the system that can be exploited) and threats (potential harm that can exploit these vulnerabilities).
* A vulnerability is an inherent flaw in the system, while a threat is an event or condition that has the potential to exploit the vulnerability.
* The security engineer needs to assess both the vulnerabilities present and the threats that could exploit these vulnerabilities to implement effective protection measures.
References
* Cisco Cybersecurity Operations Fundamentals
* Concepts of Vulnerability and Threat in Cybersecurity
* Best Practices in Vulnerability Management

質問: **159**
展示を参照してください。



この Cuckoo サンドボックス レポートは何を示していますか?

A. ファイルはスパイウェアです。

B. ファイルを実行すると、安全でないポートが開きます。

C. ファイルを実行すると、コマンド インタープリターが開きます。

D. ファイルはランサムウェアです。

正解: **(**正解を表示します**)**

The Cuckoo sandbox report shows the analysis results of a file named "VirusShare_fc1937c1aa536b3744ebfb1716fd5f4d".

The file type is identified as a PE32 executable for MS Windows.

The "Yara" section indicates that the file contains shellcode, which matches specific shellcode byte patterns.

Shellcode typically indicates that the file will execute a payload, often used to open a command interpreter or execute commands directly.

Additionally, the antivirus result shows that the file was identified as containing a trojan (Trojan.Generic.7654828), which is consistent with behaviors such as opening a command interpreter for malicious purposes.

References

Cuckoo Sandbox Documentation

Analysis of Shellcode Behavior

Understanding Trojan Malware Functionality

cisco jpnshiken.com

質問: **160**
データの整合性を向上させるために IPS イベントを削除する場合、どのプロセスが使用されますか?
A. データの正規化
B. データの可用性
C. データ署名
D. データ保護
正解: **(**正解を表示します**)**

質問: **161**
あるマーケティング会社のデータプライバシー担当者は、元顧客から、同社が保有するすべての個人情報を削除するよう依頼を受けました。同社はグローバルに事業を展開しており、国際的なデータ保護基準に準拠しています。顧客に関して保持されている情報は、固有の顧客ID「051473912」のみで、氏名、住所、その他の個人を特定できる情報とは直接関連付けられていません。データプライバシー担当者はどのような措置を講じるべきでしょうか?
A. 顧客 ID が、クライアントを識別できる追加情報と一緒に保存されている場合は、データを削除します。
B. すべてのグローバルプライバシー規制に準拠するために、データを直ちに削除します。
C. 顧客 ID 自体は国際標準では PSI として認められないため、データを保持します。
D. 顧客 ID は常に PSI とみなされ、保持できないため、法務チームに相談してください。
正解: **(**正解を表示します**)**

質問: **162**
開発者は、リモート Windows 環境でタスクを実装する必要があります。開発者は、PowerShell を介してエンタープライズ アプリケーション用のスクリプトを使用することを決定しました。なぜ機能が動作しないのでしょうか?
A. Ext4 を実装する必要があります。
B. WMI を構成する必要があります。
C. MBR を設定する必要があります。
D. シンボリックリンクを有効にする必要があります。
正解: **C (**コメントを発表する**)**

質問: **163**
実際に攻撃対象領域と脆弱性を比較した場合の違いを説明するものは何ですか?
A. OS を更新すると攻撃対象領域が縮小され、個別のオプションのパッチをインストールすることでシステム内の脆弱性が修正され解決されます。
B. リモート コード実行を許可する SMB サーバーは脆弱性であり、ポート 139 を閉じると攻撃対象領域が縮小されます。
C. 攻撃対象領域はデータベースを標的とした SQL インジェクションであり、データベース テーブルは悪用される可能性のある脆弱性です。
D. SMB の脆弱性を修正すると攻撃対象領域が縮小され、未使用のポートが開いていることがシステム内の脆弱性となります。
正解: **(**正解を表示します**)**

質問: **164**
リスクにさらされる可能性のある活動を排除するリスクアプローチはどれですか?
A. リスク回避
B. リスク保持
C. リスク軽減

D. リスク認識
正解: **(**正解を表示します**)**

質問: **165**
SOC メトリック MTTC はインシデント分析で何を提供しますか?
A. 攻撃者が環境にアクセスできる平均時間
B. インシデントが発生したことを検出するまでにかかる平均時間
C. インシデントによって引き起こされた問題を解決するのにかかる平均時間
D. インシデントを認識して停止するまでにかかる平均時間
正解: **D (**コメントを発表する**)**

質問: **166**
強制アクセス制御 (MAC) と随意アクセス制御 (DAC) の違いは何ですか?
A. DAC はすべてのレベルの制御の中で最も厳格であり、MAC はオブジェクトベースのアクセスです。
B. MAC は所有者の裁量で制御され、DAC は管理者によって制御されます。
C. MAC はすべてのレベルの制御の中で最も厳格であり、DAC はオブジェクトベースのアクセスです。
D. DAC はオペレーティング システムによって制御され、MAC は管理者によって制御されます。
正解: **(**正解を表示します**)**

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu **564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
攻撃者が低レベルのユーザー アカウントを侵害して機密データにアクセスするリスクを軽減する原則はどれですか。
A. 職務の分離
B. 権限分離
C. 最小権限
D. アクセス制限
正解: **(**正解を表示します**)**

質問: **168**
脆弱性と攻撃対象領域の違いは何ですか?
A. 攻撃対象領域はデータベースを標的とした SQL インジェクションであり、データベースは悪用される可能性のある脆弱性です。
B. 脆弱性とは、アプリケーションの弱点を悪用されるリスクであり、対象となるアプリケーション自体が攻撃対象領域となります。
C. 攻撃対象領域は特定の資産に対する測定されたリスクの合計であり、脆弱性は測定されていない悪用可能なリスクである。
D. 脆弱性とは、Webアプリケーションを悪用するために送信される、サニタイズされていないユーザー入力であり、ブラウザはWebアプリケーションの攻撃対象領域です。

正解: **B** (コメントを発表する)

質問: **169**
ルールベースの検出と統計的検出の比較は何ですか?
A. 統計は測定データに基づきますが、ルールベースでは評価された確率アプローチが使用されます。
B. ルールベース 事前にわかっている仮定と統計データに基づきます。
C. ルールベースでは事前にわかっているデータが使用され、統計は仮定に基づいています。
D. 統計では確率アプローチが使用されますが、ルールベースでは測定データに基づきます。
正解: (正解を表示します)
* Rule-based detection methods rely on predefined rules and patterns that are known beforehand. These rules are created based on prior knowledge of what constitutes normal and abnormal behavior.
* Statistical detection, on the other hand, involves analyzing data to identify anomalies. It is based on assumptions about what normal behavior looks like and uses statistical methods to detect deviations from this norm.
* Rule-based systems are typically straightforward but may miss novel attacks that do not match existing rules.
* Statistical methods can detect previously unknown threats by recognizing patterns that deviate from established baselines but may produce more false positives.
References
* Intrusion Detection Systems (IDS) Concepts
* Comparative Studies on Rule-based and Statistical Anomaly Detection
* Understanding Anomaly Detection in Network Security

質問: **170**
攻撃者は 2 人のユーザー間で交換されるネットワーク トラフィックをどのように観察しますか?
A. ポートスキャン
B. 中間者
C. コマンドインジェクション
D. サービス拒否
正解: (正解を表示します)
A man-in-the-middle (MITM) attack occurs when an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. In this scenario, an attacker can observe network traffic exchanged between two users by placing themselves in between their communication channel. References := Cisco Blogs - New Cybersecurity and Cloud Skills to Protect Companies from Cybersecurity Attacks of the Future

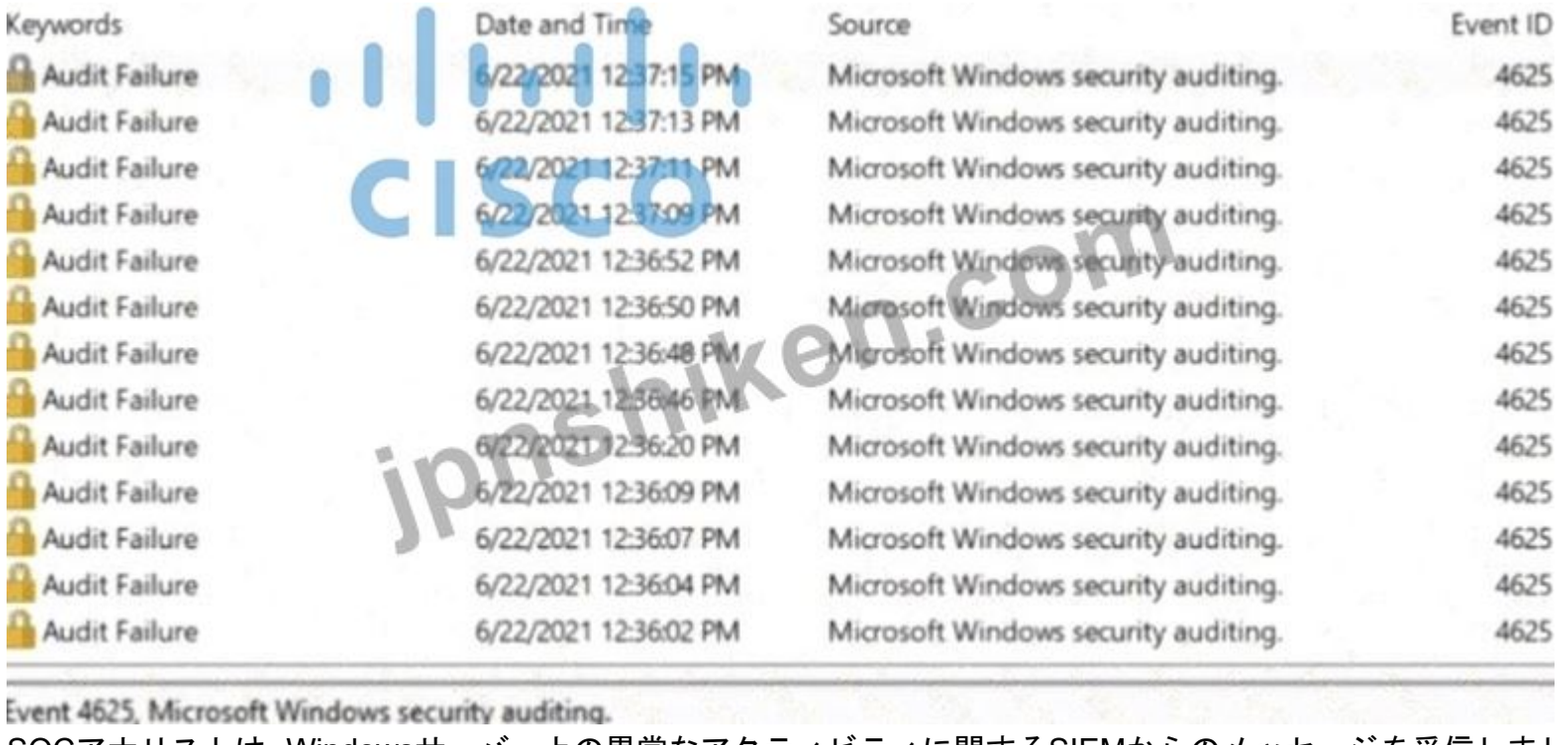
質問: **171**
Web アプリケーションとの間で送受信されるすべてのメッセージの整合性と信頼性を保証するセキュリティ技術はどれですか?
A. ハイパーテキスト転送プロトコル
B. SSL証明書
C. トンネリング
D. VPN
正解: (正解を表示します)
SSL Certificate guarantees the integrity and authenticity of all messages transferred to and from a web application. It encrypts the data transferred between the user's browser and the website, ensuring that all data passed between them remains private and integral. References := Cisco CyberOps Engineer - Module 3:

Secure Communications

質問: **172**
インライントラフィック問い合わせとトラフィックミラーリングの違いは何ですか？
A. トラフィックミラーリングがデータに追加のタグを適用するため、インライン問い合わせはそれほど複雑ではありません。
B. トラフィックミラーリングは、トラフィックを分析ツールに直接転送するのではなく、コピーします
C. インラインは、他の分析ツールに送信する前にパケットを変更するのではなく、整合性を維持するためにトラフィックを複製します。
D. トラフィックミラーリングにより、トラフィック分析が高速化され、遅延のためにインライン化が大幅に遅くなります。
正解: **(**正解を表示します**)**
Traffic mirroring is a technique that copies the traffic from a source port or VLAN to a destination port or VLAN, where it can be analyzed by a security device or tool. Traffic mirroring does not affect the original traffic flow and does not introduce any latency or modification to the packets. Inline traffic interrogation is a technique that forwards the traffic directly to the security device or tool, where it can be inspected and modified before being sent to the destination. Inline traffic interrogation can introduce latency and affect the performance of the network. References:
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, Module 2: Security Monitoring, Lesson 2.2: Network Security Monitoring Tools
200-201 CBROPS - Cisco, Exam Topics, 2.0 Security Monitoring, 2.2 Describe the impact of various technologies on security monitoring Cisco Certified CyberOps Associate Overview - Cisco Learning Network, Videos, 2.2 Describe the impact of various technologies on security monitoring

質問: **173**
エンジニアがセキュリティ侵害を調査するために完全なパケット キャプチャを使用する必要があるのはなぜですか?
A. エンジニアが疑わしいパケットに焦点を当てて悪意のあるアクティビティを特定できるように、各パケット内に設定されている TCP フラグをキャプチャします。
B. エンジニアが分析するためのメタデータ (並べ替え、解析、インデックス付けされた IP トラフィック パケット データなど) を収集します。
C. エンジニアがメタデータに従って入ってくる脅威を識別するための完全な TCP ストリームを提供します。
D. イベントを再構築し、エンジニアが侵害中に何が起こったかを確認して根本原因を特定できるようにします。
正解: **(**正解を表示します**)**
Full packet capture (FPC) is a valuable tool for investigating security breaches because it provides comprehensive data that can be used to reconstruct the event and identify the root cause. By capturing every packet, FPC allows engineers to see exactly what took place during the breach, including the TCP flags set within each packet, which can help focus on suspicious packets to identify malicious activity. It also collects metadata, including IP traffic packet data that is sorted, parsed, and indexed, and provides the full TCP streams to follow the metadata to identify the incoming threat

質問: **174**
展示品を参照してください。



Keywords	Date and Time	Source	Event ID
Audit Failure	6/22/2021 12:37:15 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:37:13 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:37:11 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:37:09 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:52 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:50 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:48 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:46 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:20 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:09 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:07 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:04 PM	Microsoft Windows security auditing.	4625
Audit Failure	6/22/2021 12:36:02 PM	Microsoft Windows security auditing.	4625

Event 4625, Microsoft Windows security auditing.

cisco
jpnshiken.com

SOCアナリストは、Windowsサーバー上の異常なアクティビティに関するSIEMからのメッセージを受信しました。アナリストはWindowsイベントログを確認し、多数の監査失敗ログを確認しました。何が起こっているのでしょうか？

A. Windows はログの監査に失敗しました

B. 通常のWindowsログ

C. ブルートフォース攻撃

D. DoS攻撃

正解: **(**正解を表示します**)**

Windows Security Event ID 4625 is generated when an account fails to log on. When a SOC analyst observes a large number of Audit Failure events occurring in rapid succession, this is a strong indicator of a brute- force authentication attack.

Brute-force attacks involve repeatedly attempting different username and password combinations to gain unauthorized access to a system. These attacks commonly target Windows servers exposed to internal or external networks and often focus on privileged or commonly used accounts. The repeated failures shown in the exhibit indicate that authentication attempts are being made unsuccessfully over a short time period, which is abnormal for standard user behavior.

Option A is incorrect because the logs clearly show that Windows auditing is functioning correctly and recording failures. Option B is incorrect because normal Windows activity does not generate large volumes of failed authentication events in a short time frame. Option D is incorrect because a Denial-of-Service (DoS) attack targets system availability and resource exhaustion, not authentication mechanisms.

Cybersecurity operations documentation highlights failed login storms as one of the most common indicators of credential-based attacks. SIEM platforms are designed to alert analysts on such patterns because they often precede account compromise or lateral movement attempts.

質問: **175**

展示品を参照してください。

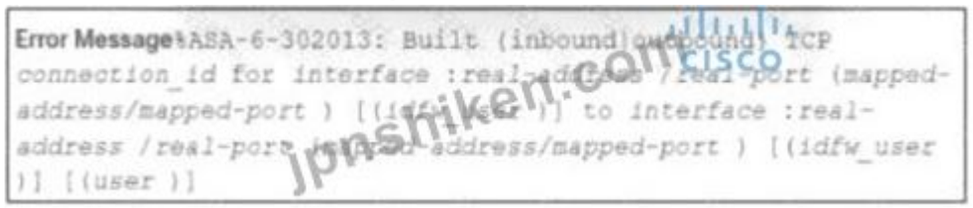
```
SELECT * FROM people WHERE username = '' OR '1'='1';
```

どのような種類の攻撃が実行されていますか?

A. SQLインジェクション

B. クロスサイトスクリプティング
C. クロスサイトリクエストフォージェリ
D. コマンドインジェクション
正解: **(**正解を表示します**)**
The exhibit shows a SQL query that is attempting to bypass login controls by modifying the query to always return true. This is a common tactic used in SQL injection attacks where malicious SQL statements are inserted into an entry field for execution. References := Cisco Cybersecurity Source Documents
Reference:https://www.w3schools.com/sql/sql_injection.asp

質問: **176**
展示品を参照してください。



疑わしいスキャン アクティビティ インシデントの分析中に、アナリストは複数のローカル TCP 接続イベントを発見しました。これらのログはどのテクノロジによって提供されましたか?
A. ウイルス対策
B. プロキシ
C. IDS/IPS
D. ファイアウォール
正解: **D (**コメントを発表する**)**
The logs indicating multiple local TCP connection events are typically provided by a firewall. Firewalls are responsible for monitoring and controlling incoming and outgoing network traffic based on predetermined security rules, and they generate logs that detail such events, which can be used for further analysis and incident response. References := Cisco Cybersecurity Operations Fundamentals

質問: **177**
脆弱性と脅威の関係は?
A. 脆弱性を悪用する脅威
B. 脆弱性は、脅威によって引き起こされる潜在的な損失の計算です。
C. 脅威を悪用する脆弱性
D. 脅威は、脆弱性によって引き起こされる潜在的な損失の計算です。
正解: **A (**コメントを発表する**)**
A vulnerability refers to a weakness or flaw in a system that can be exploited by threats (such as hackers or malware) to gain unauthorized access, cause damage, etc. Threats exploit these vulnerabilities to impact the confidentiality, integrity, or availability of information and systems. References: Cisco Cybersecurity Associate

質問: **178**
DDoS 増幅攻撃に使用されるプロトコルはどれですか? (2 つ選択してください。)
A. ICMPv6
B. NTP

C. TCP
D. DNS
E. HTTP
正解: **(**正解を表示します**)**

質問: **179**
改ざんされたディスク イメージと改ざんされていないディスク イメージの 2 つの違いは何ですか? (2つお選びください。)
A. 改ざんされた画像はセキュリティ調査プロセスで使用されます
B. 改ざんされていない画像は法執行機関の証拠として使用できます。
C. 保存されている既存のハッシュが計算されたハッシュと一致する場合、画像は改ざんされていません。
D. 保存されたハッシュと計算されたハッシュが同一の場合、画像は改ざんされます
E. 改ざんされた画像は根本原因分析レポートの要素として使用されます
正解: **(**正解を表示します**)**
An untampered disk image is one that has not been altered since its creation. This is verified by comparing the stored hash of the image at the time of creation with a newly computed hash; if they match, the image is considered untampered. Tampered images, on the other hand, may be used during the root cause analysis process to understand how and what was altered12. References: The differences between tampered and untampered disk images are discussed in cybersecurity literature, including Cisco's certification guides, which explain the importance of hash matching for verifying the integrity of disk images

質問: **180**
攻撃の兆候を説明している記述はどれですか?
A. 内部ホストは業務範囲外の国と通信します。
B. 組織に対するフィッシングの試みは、モール AV によってブロックされます。
C. 重要なパッチが不足しています。
D. AV ソフトウェアによって悪意のあるファイルが検出されました。
正解: **(**正解を表示します**)**
* Indicators of Attack (IoA) refer to observable behaviors or artifacts that suggest a security breach or ongoing attack.
* When internal hosts communicate with countries outside the business range, it may indicate data exfiltration or command-and-control communication to an external threat actor.
* Unlike Indicators of Compromise (IoC) which indicate that a system has already been compromised, IoAs are often used to identify malicious activity in its early stages.
* Monitoring for unusual outbound connections is a crucial aspect of detecting advanced persistent threats (APTs) and other sophisticated attacks.
References
* Difference Between Indicators of Compromise and Indicators of Attack
* Cyber Threat Detection Using Indicators of Attack
* Network Monitoring for Anomalous Behavior

質問: **181**
CMS プラグインは、インターネットからアクセス可能な 2 つのファイル (myplugin html と、悪用可能な php) を作成します。新しく発見されたエクスプロイトは、インジェクションの脆弱性 (m 悪用可能な php) を利用します。この脆弱性を悪用するには、特定の変数を含む HTTP POST を、悪用可能な php に送信する必要が

あります。セキュリティ エンジニアは、myplugin html への HTTP GET 要求のみで構成される、Web サーバーへのトラフィックに気付きました。このアクティビティはどのカテゴリに該当しますか。
A. 認識
B. 兵器化
C. 搾取
D. インストール
正解: **A** (コメントを発表する)

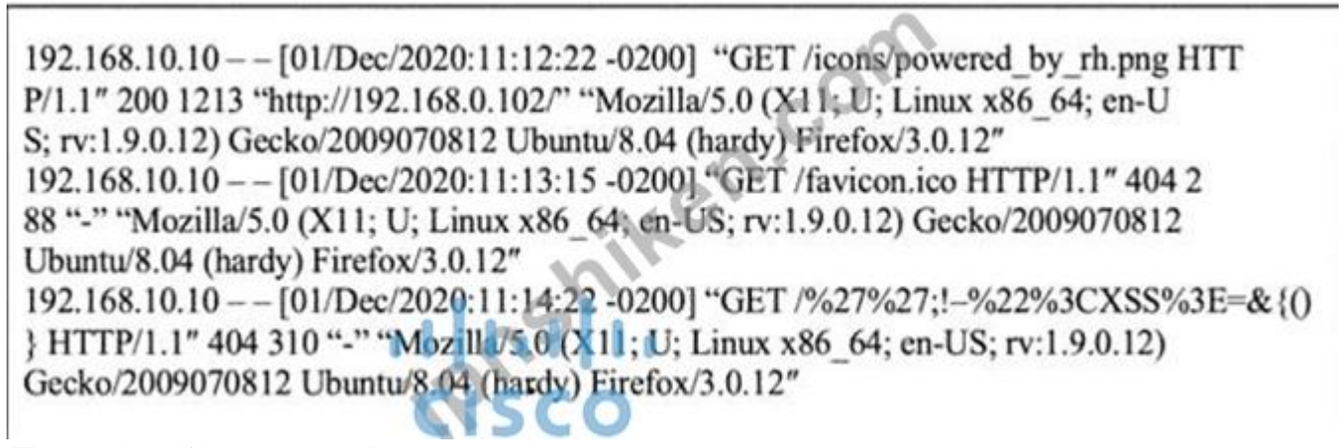
有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
ある会社がIIS7 5を使用して、Webサーバーの侵害に遭遇しました。調査の結果、攻撃者がTLS １2を使用した安全な通信でデータを読み取って変更し、エクスポートグレードの暗号化への接続をダウングレードして機密情報を傍受したことを発見しました。エンジニアは、将来同様のインシデントを軽減し、クライアントとサーバーが常に最も安全なプロトコルバージョンと暗号化パラメーターとネゴシエートするようにする必要があります。エンジニアはどのアクションを推奨しますか？
A. TLS v13にアップグレードします。
B. 最新のIISバージョンをインストールします。
C. TLS1.1にダウングレードします。
D. 侵入検知システムを導入する
正解: (正解を表示します)
Upgrading to TLS v1.3 is recommended because it eliminates outdated cryptographic functions and reduces the risk of downgrade attacks, which can occur when attackers force connections to use weaker encryption.
TLS v1.3 only supports secure cipher suites and algorithms, enhancing the security of communications.

質問: **183**
ネットワークの異常を検出するためにどのタイプのデータが使用されますか?
A. 統計データ
B. アラート データ
C. トランザクションデータ
D. メタデータ
正解: (正解を表示します)
* Statistical data is crucial for detecting anomalies within a network because it provides a baseline of normal behavior.
* Anomaly detection involves comparing current network data against historical statistical data to identify deviations from expected patterns.
* This method helps in identifying unusual activities that could signify a security threat, such as unusual login attempts, data transfers, or access patterns.
* Statistical data analysis tools use metrics such as mean, variance, and standard deviation to flag anomalies, aiding in proactive threat detection.
References

* Cisco Cybersecurity Operations Fundamentals
* Network Anomaly Detection Techniques
* Statistical Methods in Cybersecurity

質問: **184**
展示品を参照してください。



展示では何が起こっているのでしょうか?
A. 通常のGETリクエスト
B. XML 外部エンティティ攻撃
C. 安全でない逆シリアル化
D. クロスサイトスクリプティング攻撃
正解: **(**正解を表示します**)**
Based on the image details, the exhibit shows a series of HTTP requests with the method GET, which are used to retrieve data from a web server. There is no evidence of any malicious payload or parameter in these requests, so they are likely regular GET requests. The other options are types of web application attacks that exploit different vulnerabilities, such as XML External Entities, insecure deserialization, and cross-site scripting. References := Cisco Cybersecurity Reference:https://www.tutorialspoint.com/http/http_requests.htm
https://github.com/gwroblew/detectXSSlib/blob/master/test/attacks.txt

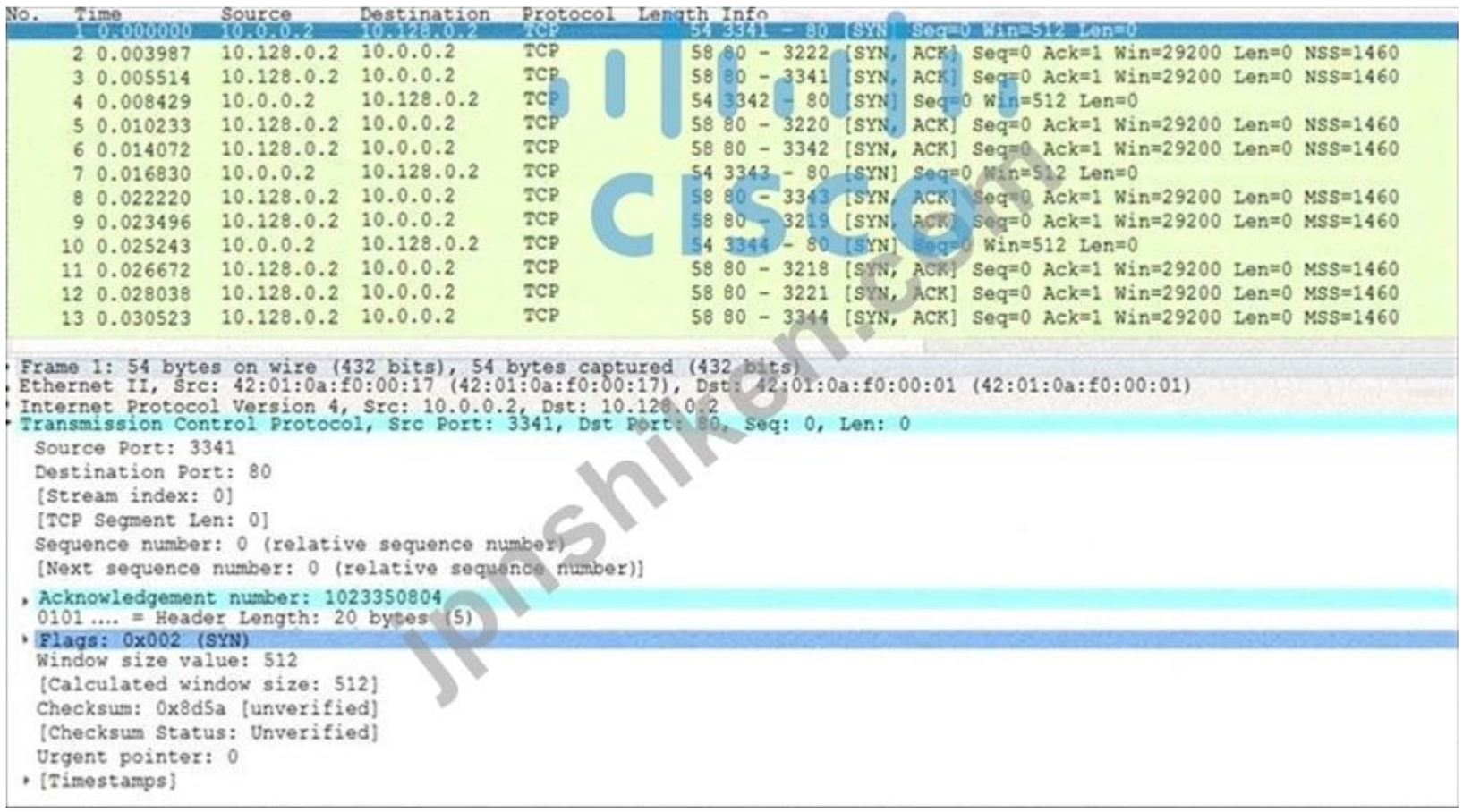
質問: **185**
アナリストは、インターネット上のコマンドおよび制御サーバーと通信しているように見えるネットワーク内のホストを調査しています。このパケットキャプチャを収集した後、アナリストは通信に使用された技術とペイロードを判別できません。



攻撃者はどの難読化手法を使用していますか？

A. SHA-256ハッシュ
B. ROT13暗号化
C. Base64エンコーディング
D. TLS暗号化
正解: **D** (コメントを発表する)

質問: **186**
展示品を参照してください。



このネットワーク トラフィックでは何が起こっているのでしょうか?

A. 複数の送信元から単一の宛先 IP に向けて送信される SYN パケットの割合が高い。
B. 単一の送信元 IP から複数の宛先 IP に送信される ACK パケットの割合が高い。
C. 単一の送信元 IP から複数の宛先 IP に送信される ACK パケットのフラッド。
D. 単一の送信元 IP から単一の宛先 IP に送信される SYN パケットのフラッド。
正解: **(**正解を表示します**)**
The exhibit shows a high rate of SYN packets being sent from multiple sources towards a single destination IP. This is indicative of a SYN flood attack, where the attacker sends a succession of SYN requests to a target' s system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. References := Cisco Cybersecurity Operations Fundamentals - Module 4: Network Intrusion Analysis

質問: **187**
TLS ハンドシェイクのネゴシエーション フェーズでクライアントがサーバーに送信する情報を識別するリストはどれですか?
A. ClientStart、ClientKeyExchange、サポートされる暗号スイート、および推奨される圧縮方法
B. ClientStart、サポートされる TLS バージョン、サポートされる暗号スイート、および推奨される圧縮方法
C. ClientHello、サポートされる TLS バージョン、サポートされる暗号スイート、および推奨される圧縮方法
D. ClientHello、ClientKeyExchange、サポートされる暗号スイート、および推奨される圧縮方法
正解: **(**正解を表示します**)**
During the negotiation phase of the TLS handshake, the client sends a "ClientHello" message to the server which includes information about TLS versions it supports, cipher-suites it supports and suggested compression methods. This initiates communication protocols for secure connection. References := Cisco Cybersecurity source documents or study guide

質問: **188**
自動車会社は、ラリースポーツカー用に新しいタイプのエンジンと特別なブレーキを提供しています。同社は、エンジンと技術情報に関する発明と特許のデータベースを持っています。顧客は、登録して身元を確認した後、会社のWebサイトからデータベースにアクセスできます。顧客はどのタイプの保護されたデータにアクセスしますか？
A. IPデータ
B. PIIデータ
C. PSIデータ
D. PHIデータ
正解: **(正解を表示します)**
IP data stands for Intellectual Property data, which is any data that represents the creations of the mind, such as inventions, patents, designs, or artistic works. IP data is protected by law and has commercial value for its owners. In this case, the automotive company has a database of IP data for their engines and technical information, which customers can access after they register and identify themselves. References := Cisco Cybersecurity Operations Fundamentals, Module 1: Security Concepts, Lesson 1.2: Data Protection, Topic
1.2.1: Data Types

質問: **189**
オフライン監査ログには、システムの侵害につながる脆弱性を悪用した疑いのあるセッションのソース IP アドレスが含まれています。
このIPアドレスはどのような証拠ですか?
A. 最良の証拠
B. 補強証拠
C. 間接的な証拠
D. 法医学的証拠
正解: **(正解を表示します)**
The source IP address from an audit log that indicates a session which may have exploited a vulnerability is considered corroborative evidence. This type of evidence supports other evidence that suggests a security breach occurred. In the context of cybersecurity, corroborative evidence can help establish that an attack was carried out and can be used in conjunction with other data points to build a case during an investigation.
References := The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training material discusses the types of data needed to investigate security incidents, which includes understanding the role of different types of evidence in building a security incident case1.

質問: **190**
展示品を参照してください。

```
Firewall Log:
Date: 2023-10-15 10:15:23
Source IP: 192.168.1.10
Destination IP: 10.0.0.5
Action: Allowed
Description: Connection established from internal network.

Authentication Log:
Date: 2023-10-15 10:16:45
User: jdoe
Source IP: 192.168.1.10
Authentication Status: Successful
Description: User logged in from internal IP address.

System Event Log:
Date: 2023-10-15 10:17:30
Event ID: 4625
Source: Windows Security Auditing
Description: An account failed to log on. Account Name: cisconame
Workstation Name: WORKSTATION-01

Network Traffic Log:
Date: 2023-10-15 10:18:10
Source IP: 192.168.1.10
Destination IP: 10.0.0.20
Protocol: HTTP
Activity: Data transfer observed.
```

ipnshiken.com

アナリストは、データ窃盗の可能性に関するIDSアラートを受け取りました。複数のシステムから追加のログセットが収集され、分析されました。これらのログは、IDSからの主要なアラートに関連してどのような種類の証拠を提供しますか？

A. 補強証拠

B. 主要な証拠

C. 状況証拠

D. 二次証拠

正解: **(**正解を表示します**)**

In cybersecurity operations, evidence classification is critical for incident investigation and validation. An Intrusion Detection System (IDS) alert serves as the initial indicator of suspicious activity, such as potential data exfiltration. However, IDS alerts alone are often insufficient to confirm malicious behavior, as they may produce false positives or incomplete context.

The additional logs collected-such as firewall logs, authentication logs, system event logs, and network traffic logs-are used to support, validate, and confirm the original alert. These logs show related activity from the same source IP, including successful authentication, failed login attempts, and observed data transfers over HTTP. When multiple independent data sources align with the original IDS alert, they strengthen the confidence that the activity is real and malicious.
This type of supporting information is known as corroborative evidence. Corroborative evidence does not stand alone as the initial detection but reinforces the validity of primary evidence by confirming the same behavior across different systems and logs. Cybersecurity operations documentation emphasizes log correlation as a foundational SOC function precisely for this reason.
Primary evidence would be the original IDS alert itself, as it directly detected the suspicious activity.
Circumstantial evidence implies indirect inference without direct linkage, which is not the case here because the logs clearly relate to the same host and timeline.
Secondary evidence typically refers to derivative or summarized data rather than direct system-generated records.
By correlating IDS alerts with firewall, authentication, and network logs, analysts build a reliable incident narrative and reduce false positives. Therefore, the logs collected provide corroborative evidence, making Option A the correct answer.

質問: **191**
署名ベースの検出と動作ベースの検出の違いは何ですか？
A. シグネチャベースは、攻撃にリンクされている可能性のある動作を識別しますが、動作ベースには、アラートの前に一致するルールの定義済みセットがあります。
B. 動作ベースは、攻撃にリンクされる可能性のある動作を識別しますが、シグネチャベースには、アラートの前に一致するルールの定義済みセットがあります。
C. 動作ベースは既知の脆弱性データベースを使用しますが、署名ベースは既存のデータをインテリジェントに要約します。
D. シグニチャベースは既知の脆弱性データベースを使用しますが、動作ベースは既存のデータをインテリジェントに要約します。
正解: (正解を表示します)
Behavior-based detection monitors the behavior of programs in real-time. If a piece of software acts similarly to known malware after it's been executed, behavior-based detection can stop it in its tracks. Signature-based detection involves searching for known patterns of data within executable code; if a pattern matches a "signature" in the system's database that is considered malicious. References: Cisco Cybersecurity Operations Fundamentals

質問: **192**
すべてのプロセスを root または管理者として実行すると、どのセキュリティ原則に違反しますか?
A. 最小権限の原則
B. ロールベースのアクセス制御
C. 職務の分離
D. 信頼できるコンピューティングベース
正解: (正解を表示します)
Running all processes as root or administrator violates the principle of least privilege, which states that users and processes should be granted only the minimum permissions necessary to perform their specific role or function within an organization. Running all processes as root or administrator gives them full access and control over the system, which increases the risk of unauthorized actions, malicious attacks, and accidental errors. It also makes it easier for attackers to escalate their privileges and compromise the system. References:
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.2: Security Principles Cisco Certified CyberOps Associate Overview, Exam Topics, 1.1 Explain the CIA triad

質問: **193**
ルールベースの検出は動作検出とどの程度異なりますか?

A. 動作システムは特定の接続動作に一致するシーケンスを見つけ、ルールベースのシステムは潜在的なゼロデイ攻撃を識別します。
B. ルールベースのシステムは、特定の種類の攻撃にリンクされたパターンを検索し、動作システムはシグネチャごとに攻撃を識別します。
C. 行動システムには複雑な環境向けのパターンがあり、ルールベースのシステムは中小規模の企業で使用できます。
D. ルールベースのシステムには事前定義されたパターンがあり、動作ベースのシステムは環境に固有のパターンを学習します。
正解**: D (**コメントを発表する**)**
Rule-based detection systems operate using predefined patterns and signatures to identify known threats.
These patterns are based on prior knowledge of attack methods and vulnerabilities.
Behavioral detection systems, on the other hand, analyze the normal behavior of a network or system to establish a baseline. They thenmonitor for deviations from this baseline, which may indicate potential threats.
Rule-based systems are effective at detecting known threats but may struggle with novel or zero-day attacks that do not match existing signatures.
Behavioral systems can detect unknown threats by recognizing abnormal activities, making them useful in identifying zero-day exploits and other sophisticated attacks.
References
Comparison of Rule-based and Behavioral Detection Methods in IDS
Advantages of Behavioral Analysis in Network Security
Cybersecurity Detection Techniques

質問**: 194**
アナリストは、さまざまなオペレーティング システムの機能を調査しています。
オペレーティング システムを決定する際に考慮しなければならない Windows Management Instrumentation の機能は何ですか?
A. Microsoft Services for Linux がインストールされている Linux デバイスを照会します
B. 自動化された方法で Windows オペレーティング システムを展開します
C. Active Directory を操作するための効率的なツールです。
D. インストールされているハードウェアとソフトウェアを説明する Common Information Model があります。
正解**: D (**コメントを発表する**)**
Windows Management Instrumentation (WMI) provides a unified way for users to request system information, including hardware and software inventory data. The Common Information Model (CIM) is an open standard that defines how managed elements in an IT environment are represented as a common set of objects and relationships between them. References: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4 /admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_01100.html

質問**: 195**
防御-m-深さの原則を説明するものは何ですか？
A. 新しいワークステーションの設置に関する正確なガイドラインを定義する
B. 組織内の重要な資産の分類
C. ゲストWi-Fiをフォーカルネットワークから分離する
D. 予期しない資産の誤動作に対するアラートの実装
正解**: (**正解を表示します**)**
The defense-in-depth principle is a strategy of applying multiple layers of security controls to protect an asset from threats. It is based on the assumption that no single security measure is sufficient to prevent all attacks, and that each layer adds more protection and reduces the risk of compromise. One example of applying

the defense-in-depth principle is implementing alerts for unexpected asset malfunctions, which can indicate a potential security breach or incident. References: Cisco Cybersecurity Operations Fundamentals, Module 1:
Security Concepts, Lesson 1.1: The CIA Triad and Security Concepts, Topic 1.1.4: Defense-in-Depth Principle

質問: **196**
ネットワークで使用するアプローチを決定するために、インライン トラフィック調査とトラフィック タッピングを比較する場合、セキュリティ アナリストは何を考慮すべきですか?
A. 質問をタップすると、トラフィックを分析するために信号が別のポートに複製されます
B. タッピング質問は、悪意のあるトラフィックを検出してブロックします
C. インライン インタロゲーションにより、トラフィックのコピーを表示して、トラフィックがセキュリティ ポリシーに準拠していることを確認できます。
D. インライン インタロゲーションは悪意のあるトラフィックを検出しますが、トラフィックをブロックしません
正解: (正解を表示します)
Traffic tapping involves replicating network traffic and sending it to a separate port where it can be analyzed without affecting the original traffic flow. This allows security analysts to monitor and analyze traffic for potential threats without the risk of blocking legitimate traffic.
This explanation is based on general network security concepts, as the current page does not provide specific Cisco documentation.

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu **564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **197**
繰り返し使用するためにペイロードを保存せずに実行するクロスサイト スクリプティング攻撃の分類はどれですか?
A. 保存されています
B. 反射
C. DOM
D. CSRF
正解: (正解を表示します)
Reflective XSS, also known as Non-Persistent XSS, occurs when an attacker sends a malicious script to a user through a web application, and the script is executed immediately in the user's browser without being stored on the server. This type of attack is typically carried out by including the malicious script in a URL, which is then sent to the victim. When the victim clicks on the link, the script runs in their browser, reflecting the attacker's actions without storing the payload for repeated use12. References: OWASP Foundation's documentation on Cross-Site Scripting (XSS) provides detailed information on the different types of XSS attacks, including Reflective XSS

質問: **198**
NIST Special Publication 800-61 r2 に記載されているインシデント対応プロセスの 2 つの要素は?
(2つ選んでください。)
A. 検出と分析
B. 事後活動

C. 脆弱性管理
D. リスク評価
E. 脆弱性のスコアリング
正解: **(**正解を表示します**)**
NIST Special Publication 800-61 r2 outlines the incident response process including detection and analysis, which involves identifying and validating the occurrence of incidents, and post-incident activity that focuses on lessons learned and improvements to be made after an incident has occurred. References := NIST Special Publication 800-61 r2

質問: **199**
ホストベースのファイアウォールはワークステーションを何から保護しますか?
A. ゼロデイ脆弱性
B. 不要なトラフィック
C. 悪意のある Web スクリプト
D. ウイルス
正解: **(**正解を表示します**)**
Host-based firewalls are designed to protect individual workstations from unwanted traffic by filtering incoming and outgoing network communications based on predefined security rules. They can block unauthorized access attempts and prevent potentially harmful traffic from reaching the system.

質問: **200**
エンジニアは、HRから送信元アドレスHRjacobm @companycomのフィッシングメールを大量に受信しました。
このシナリオの脅威アクターは何ですか？
A. フィッシングメール
B. 送信者
C. HR
D. レシーバー
正解: **(**正解を表示します**)**
In the context of phishing emails, the threat actor is the entity that is responsible for initiating the threat, which in this case is the sender of the phishing emails. The sender is impersonating the HR department to deceive the receiver into believing that the emails are legitimate

質問: **201**
インライントラフィックインテロゲーション（TAPS）とトラフィックミラーリング（SPAN）の違いは何ですか？
A. トラフィックミラーリングはデータに追加のタグを適用し、SPANは整合性を変更せず、全二重ネットワークを提供するため、TAPSの問い合わせはより複雑です。
B. SPANはより効率的なトラフィック分析をもたらし、TAPSはミラーリングによって引き起こされる遅延のためにかなり遅くなります。
C. TAPSはトラフィックを複製して整合性を維持し、SPANはパケットを他の分析ツールに送信する前に変更します
D. SPANポートは物理層エラーを除外し、一部のタイプの分析をより困難にし、TAPSは物理エラーを含むすべてのパケットを受信します。
正解: **D (**コメントを発表する**)**
The main difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN) lies in how they handle network traffic for analysis purposes. TAPS, or Test Access Points, are hardware devices that create a copy of the traffic between two network points without altering the data. This means TAPS can transmit both send and receive data streams simultaneously on separate dedicated channels, ensuring all data, including physical layer errors, is received by the

monitoring or security device in real-time. On the other hand, SPAN, or Switch Port Analyzer, is a feature that duplicates network packets seen on one port to another port for analysis. However, SPAN ports can filter out physical layer errors, which may limit the types of analyses that can be performed as some errors will not be represented in the mirrored traffic.
The distinction between TAPS and SPAN is covered in the Cisco CyberOps Associate CBROPS 200-201 course, which provides foundational knowledge for network monitoring and security analysis1. Additionally, industry resources such as Garland Technology's comparison of TAPS and SPAN highlight the differences in performance and integrity of the traffic being analyzed

質問: **202**
どのデータキャプチャにペイロードとヘッダー情報が含まれますか?
A. アラートデータ
B. セッションログ
C. フルパケット
D. フレームチェックシーケンス
正解: **(**正解を表示します**)**

質問: **203**
攻撃対象領域は攻撃ベクトルとどのように異なりますか？
A. 攻撃ベクトルは攻撃の潜在的な結果を認識し、攻撃対象領域は攻撃の方法を選択しています。
B. 攻撃対象領域は、攻撃の脆弱な部分を識別し、攻撃ベクトルは、それらの部分に対して実行可能な攻撃を指定します。
C. 攻撃対象領域は外部の脆弱性を軽減し、攻撃ベクトルは軽減手法と考えられる回避策を特定します。
D. 攻撃ベクトルは悪用される可能性のあるコンポーネントと一致し、攻撃対象領域は悪用される可能性のあるパスを分類します
正解: **(**正解を表示します**)**
An attack surface is the sum of all the points where an attacker can try to enter or extract data from an environment. It includes all the hardware, software, network, and human components that are exposed to potential threats. An attack vector is the path or means by which an attacker can exploit a vulnerability in the attack surface. It describes the type, source, and technique of an attack, such as phishing, malware, denial-of- service, etc. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.1: The CIA Triad and Security Concepts, Topic 1.1.3: Threats, Vulnerabilities, and Exploits

質問: **204**
調査員は、CDFS 形式で保存されている ISO ファイルのコピーを調査しています。このファイルはどのような種類の証拠ですか?
A. Mac ベースのシステムを使用してコピーされた CD からのデータ
B. Linux システムを使用してコピーされた CD からのデータ
C. Windows システムを使用してコピーされた DVD からのデータ
D. Windows を使用してコピーした CD のデータ
正解: **(**正解を表示します**)**
CDFS stands for Compact Disc File System, which is a file system used by Mac OS to store data on CDs.
CDFS is also known as ISO 9660, which is a standard format for data interchange on optical discs. CDFS allows files to be accessed by different operating systems, such as Windows, Linux, and Mac OS. Therefore, an ISO file that is stored in CDFS format is data from a CD copied using Mac-based system.
References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 4: Network Intrusion Analysis, Lesson 4.4: File Type Analysis, Topic 4.4.1: File Systems, page 4-40.

質問: **205**
脆弱性とリスクの違いは何ですか？
A. 脆弱性は、考えられる悪意のあるエントリポイントの合計であり、リスクは、不正なエントリ自体の可能性を表します。
B. リスクはエクスプロイトが適用される潜在的な脅威であり、脆弱性は脅威自体を表します
C. 脆弱性は、悪用される可能性のあるセキュリティの欠陥を表し、リスクはそれが引き起こす可能性のある潜在的な損害です。
D. リスクは、攻撃者がネットワークに侵入するために使用する潜在的な脅威であり、脆弱性はエクスプロイトです
正解: **C (**コメントを発表する**)**
Vulnerability refers to a weakness or flaw in a system that can be exploited by threats. Risk, on the other hand, is the potential for loss or damage when a threat exploits a vulnerability. The risk is essentially the impact or consequence of a vulnerability being exploited

質問: **206**
セキュリティ エンジニアは、企業全体のホスト/エンドポイント テクノロジを企業のすべての企業 PC に展開します。経営陣は、すべての PC で選択されたアプリケーションのセットをブロックするようエンジニアに要求します。
このタスクを実行するには、どのテクノロジーを使用すべきですか?
A. アプリケーションのホワイトリスト/ブラックリスト
B. ネットワーク NGFW
C. ホストベースの IDS
D. ウイルス対策/スパイウェア対策ソフトウェア
正解: **A (**コメントを発表する**)**
Application whitelisting/blacklisting is a technology used to control which applications are allowed to execute on a company's corporate PCs. Whitelisting allows only approved applications to run, while blacklisting prevents specific applications from running. This approach is effective for managing application usage across an enterprise.

質問: **207**
HTTPSトラフィックのスクリーニングが難しいのはなぜですか？
A. HTTPSは内部で使用され、トラフィックをスクリーニングします または、分離のために外部の関係者は困難です。
B. 通信は暗号化され、転送中のデータは保護されます。
C. デジタル証明書はセッションを保護し、データはランダムな間隔で送信されます。
D. トラフィックは特定の宛先にトンネリングされ、受信者以外はアクセスできません。
正解: **(**正解を表示します**)**
HTTPS traffic is difficult to screen because it is encrypted using the SSL/TLS protocol, which secures the data in transit between the client and the server. This encryption ensures that any intercepted traffic cannot be easily read or tampered with by third parties. Screening or inspecting this encrypted traffic would require decrypting it, which poses significant challenges and potential security risks12.
The concept of HTTPS and its implications on traffic screening are discussed in various cybersecurity resources, including Cisco's cybersecurity training materials3.
Cloudflare provides an explanation of HTTPS inspection and the challenges associated with it

質問: **208**

サイバー攻撃者は、企業が使用しているソフトウェアのセキュリティ上の欠陥に気づきました。彼らは、この欠陥を悪用してソフトウェアに保存されているパスワードを抽出するために、特定のワームをカスタマイズすることにしました。このイベントは、サイバー キル チャム モデルのどのカテゴリに属しますか?

A. 偵察
B. 配達
C. 搾取
D. 兵器化

正解: **D** (コメントを発表する)

質問: **209**

ネットワークのプロファイリングに使用される 2 つの要素はどれですか? (2つ選んでください。)

A. セッション時間
B. 総スループット
C. 実行中のプロセス
D. リスニングポート
E. OS フィンガープリント

正解: **B,D** (コメントを発表する)

Profiling a network involves various elements that provide insights into its characteristics and behaviors. Total throughput is crucial as it measures the amount of data passing from a source to a destination in a given period, reflecting the network's capacity and usage patterns1. Listening ports are also essential for profiling because they represent the entry points for network services, indicating which services are available and potentially vulnerable1.

References :=

* Network profiling tools and techniques discussed in online resources23.
* Direct explanations of network profile elements

質問: **210**

期待される結果を確認するためにシナリオに値を割り当てている特定のタイプの分析はどれですか?

A. 決定論的
B. 探索的
C. 確率論的
D. 説明

正解: (正解を表示します)

This type of analysis is deterministic because it assigns fixed values to the scenario and calculates the expected outcomes based on those values. Deterministic analysis does not account for uncertainty or randomness in the scenario. References: https://learningnetworkstore.cisco.com/on-demand-e-learning /understanding-cisco-cybersecurity-operations-fundamentals-cbrops-v1-0/CSCU-LP-CBROPS-V1-028093.
html (Module 3, Lesson 3.1.2)

有効的な**200-201J**問題集はJPNTest.com提供され、**200-201J**試験に合格することに役に立ちます！JPNTest.comは今最新**200-201J**試験問題集を提供します。JPNTest.com 200-201J試験問題集はもう更新されました。ここで**200-201J**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/200-201J-mondaishu　**564**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」