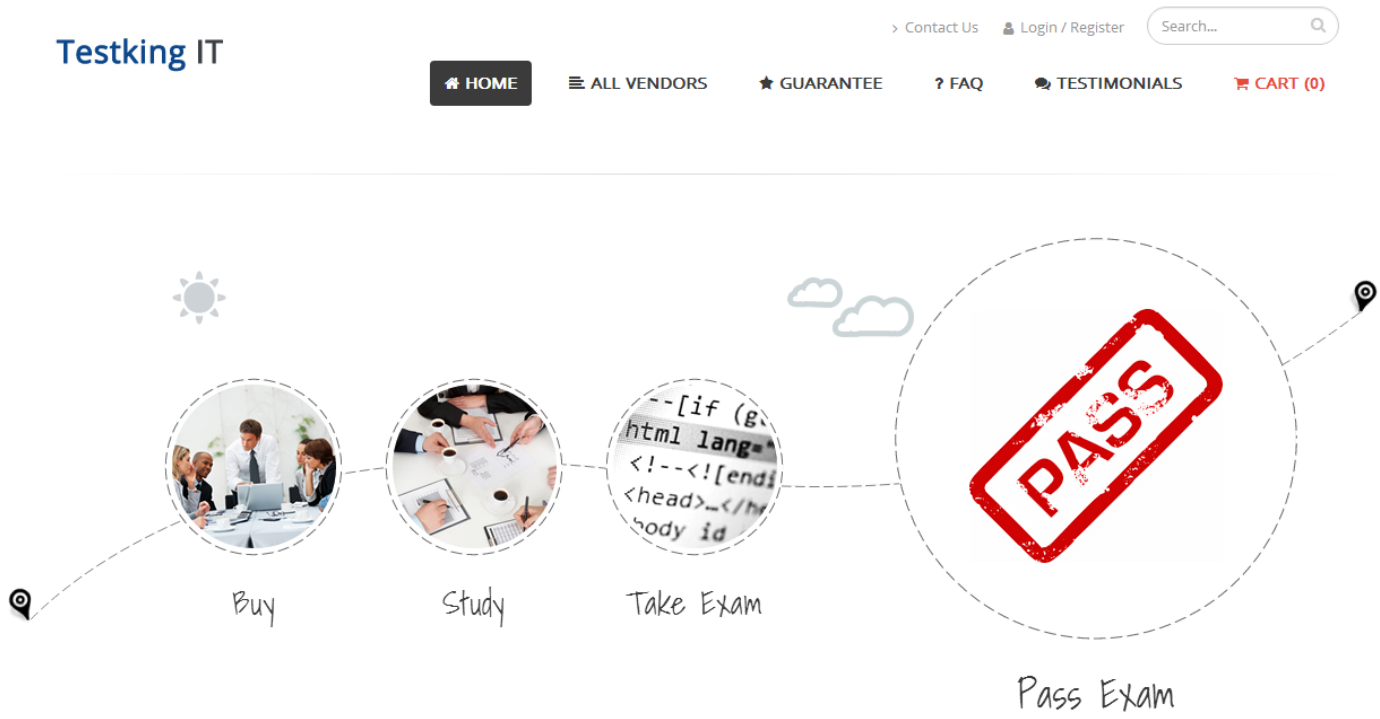
# TestkingIT




Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

**48236+** customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

[http://www.testkingit.com/](http://www.testkingit.com/)

Latest practice material - Exam Cram - TestKingIT

**Exam** : **200-201J**

**Title** : Understanding Cisco Cybersecurity Operations Fundamentals (200-201日本語版)

**Vendor** : Cisco

**Version** : DEMO

**QUESTION NO: 1**
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
***Answer:*** D
Explanation:
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.

**QUESTION NO: 2**
ある会社の従業員が添付ファイル付きのメールを受け取りました。このメールが不審な送信元からのものだったため、添付ファイルを開かないことにしました。セキュリティアナリストはその後の調査で、このファイルがマルウェアであると結論付けました。この事象はサイバーキルチェーンモデルのどのカテゴリに該当するでしょうか?
**A.** 武器化
**B.** インストール
**C.** 搾取
**D.** 配達
***Answer:*** D

**QUESTION NO: 3**
展示を参照してください。

```
10.20.1.21 - - [05/Mar/2018:20:04:30 +0000] "GET
/user?name=%3B/bin/sh%20-c%20id HTTP/1.1" 200 178 "-"
"Wget/1.17.1 (linux-gnu)"
```

Web アプリケーションに対してどの攻撃が試みられていますか?
**A.** SQL インジェクション
**B.** 中間者攻撃
**C.** コマンドインジェクション
**D.** サービス拒否
***Answer:*** C
Explanation:
The exhibit shows an HTTP GET request with a parameter that includes; /bin/sh -c id.
This indicates a command injection attempt, where the attacker is trying to execute shell commands on the server.
Command injection vulnerabilities allow an attacker to execute arbitrary commands on the

host operating system via a vulnerable application.
The use of/bin/shand the-cflag is typical in command injection exploits to run shell commands, such asid, which returns user identity information.
References
OWASP Command Injection
Analyzing HTTP Requests for Injection Attacks
Web Application Security Testing Guidelines

**QUESTION NO: 4**
HTTPS 接続では対称暗号化はどのように使用されますか?
**A.** 対称暗号化アルゴリズムは公開鍵と秘密鍵の証明書を使用します
**B.** 暗号化はRSA-2048に基づいています
**C.** 対称鍵は暗号化に使用されます
**D.** 鍵交換プロセスは信頼性が高く安全です
***Answer:*** C

**QUESTION NO: 5**
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。
***Answer:*** D
Explanation:
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

**QUESTION NO: 6**
IDS の機能は何ですか?
**A.** 疑わしいファイルを検出してブロックするデバイスまたはソフトウェア
**B.** ウイルスやマルウェアを防ぐエンドポイント保護ソフトウェア
**C.** 詳細な分析とデバッグを実行するために使用されるフォレンジックツール
**D.** 悪意のあるネットワーク活動を監視および識別するソフトウェアまたはデバイス
***Answer:*** D

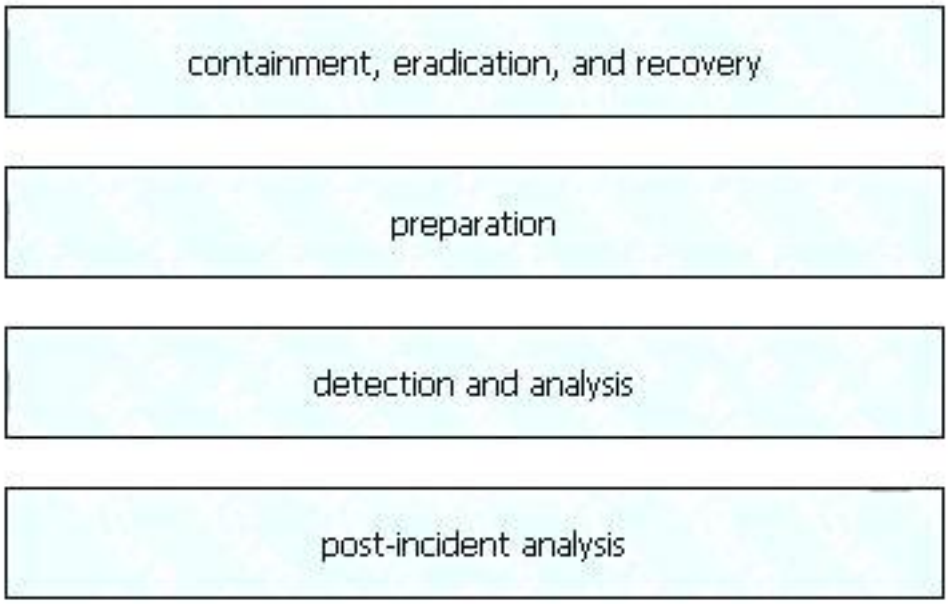
**QUESTION NO: 7**
左の要素を右のインシデント処理の正しい順序にドラッグ アンド ドロップします。

| | |
|---|---|
| preparation | create communication guidelines for effective incident handling |
| containment, eradication, and recovery | gather indicators of compromise and restore the system |
| post-incident analysis | document information to mitigate similar occurrences |
| detection and analysis | collect data from systems for further investigation |

***Answer:***

| | |
|---|---|
| preparation | containment, eradication, and recovery |
| containment, eradication, and recovery | preparation |
| post-incident analysis | detection and analysis |
| detection and analysis | post-incident analysis |

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




**QUESTION NO: 8**
CVSSのどのメトリックが、宛先の銀行口座番号を取得して別の銀行口座番号に置き換える攻撃を示していますか？
**A.**整合性
**B.**守秘義務
**C.**可用性

**D.**スコープ

***Answer:*** A

Explanation:

Integrity is a metric in CVSS that measures the impact of a vulnerability on the trustworthiness and veracity of the data or information in a system. A vulnerability that affects the integrity of a system can allow an attacker to modify, delete, or corrupt the data or information without authorization. An example of such a vulnerability is a bank account number tampering attack, where an attacker changes the destination bank account number of a transaction to redirect the funds to their own account. References: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) - Cisco, page 2-17; 200-201 CBROPS - Cisco, exam topic 1.3.c

**QUESTION NO: 9**

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。

***Answer:*** D

Explanation:

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

**QUESTION NO: 10**

重要なタスクを実行するために複数の人を必要とするセキュリティ原則はどれですか?

**A.** 最小権限

**B.** 知る必要がある

**C.** 職務の分離

**D.** デューデリジェンス

***Answer:*** C

Explanation:

Separation of duties is a security principle that requires more than one person to perform a

critical task, such as authorizing a transaction, approving a budget, or granting access to sensitive data. Separation of duties reduces the risk of fraud, error, abuse, or conflict of interest by preventing any single person from having too much power or privilege. Least privilege, need to know, and due diligence are other security principles, but they do not require more than one person to perform a critical task. References: Separation of Duty (SOD) - Glossary | CSRC - NIST Computer Security ..., Separation of Duties | Imperva

**QUESTION NO: 11**
エンジニアは、入力および出力の境界トラフィックを復号化し、ネットワーク セキュリティ デバイスが悪意のある送信通信を検出できるようにすることで、コマンド アンド コントロール通信を検出するようにネットワーク
システムを構成する必要があります。このタスクを達成するにはどのテクノロジーを使用する必要がありますか?
**A.** 静的 IP アドレス
**B.** 署名
**C.** デジタル証明書
**D.** 暗号スイート
***Answer:*** C
Explanation:
Digital certificates are essential for decrypting ingress and egress perimeter traffic, as they provide the necessary encryption keys for secure communications. By using digital certificates, network security devices can inspect the decrypted traffic to detect any malicious outbound communications that may indicate command-and-control activity.

**QUESTION NO: 12**
エージェントレス保護と比較した場合、エージェントベースの保護にはどのような利点がありますか?
**A.** 維持費を下げる
**B.** 一元化されたプラットフォームを提供します
**C.** すべてのトラフィックをローカルで収集して検出します
**D.** 多数のデバイスを同時に管理します
***Answer:*** C
Explanation:
Agent-based protection is a type of endpoint security that uses software agents installed on the devices to monitor and protect them. Agent-based protection can collect and detect all traffic locally, which means it can operate without relying on a network connection or a centralized server. Agent-based protection can also provide more granular and comprehensive visibility and control over the devices. References:
https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco-cybersecurity-operations- fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1-028093.html
(Module 2: Security Concepts, Lesson 2.3:
Endpoint Security)

**QUESTION NO: 13**
DDoS 攻撃の 2 つのカテゴリは何ですか? (2 つ選択してください。)

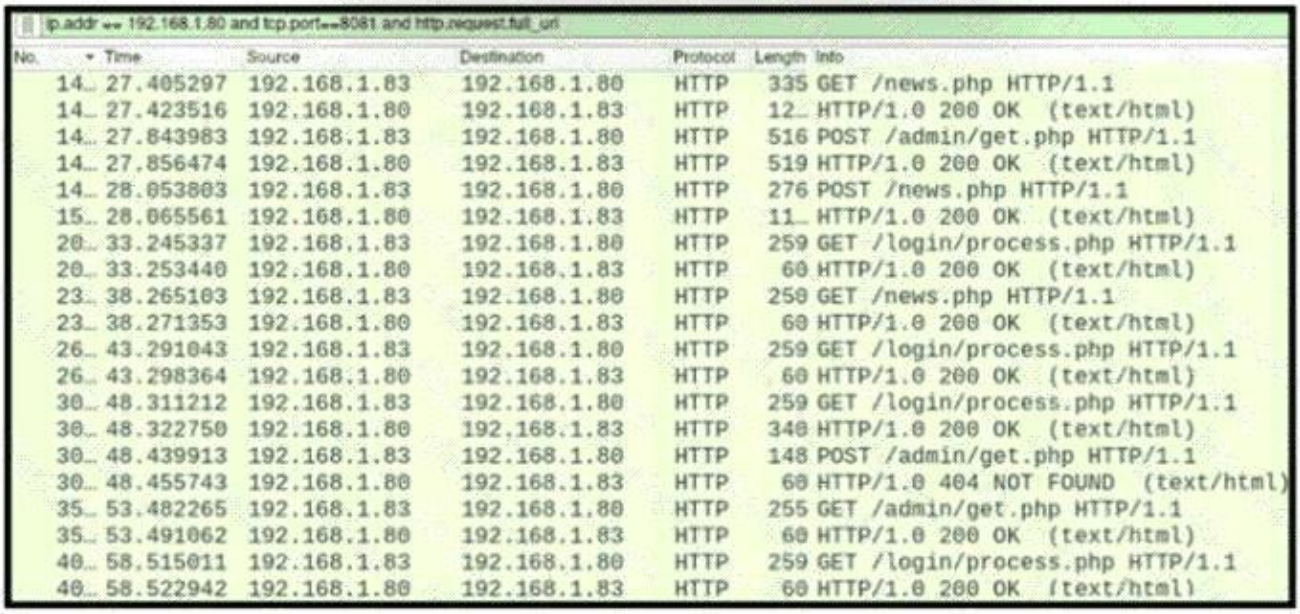
**A.** スプリットブレイン
**B.** フィッシング
**C.** 直接
**D.** 反射
**E.** スキャン
***Answer:*** C D

**QUESTION NO: 14**
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 |

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
***Answer:*** C
Explanation:
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

**QUESTION NO: 15**
展示品を参照してください。


ip.addr == 192.168.1.80 and tcp.port==8081 and http.request.full_uri

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 14… | 27.405297 | 192.168.1.83 | 192.168.1.80 | HTTP | 335 | GET /news.php HTTP/1.1 |
| 14… | 27.423516 | 192.168.1.80 | 192.168.1.83 | HTTP | 12… | HTTP/1.0 200 OK (text/html) |
| 14… | 27.843983 | 192.168.1.83 | 192.168.1.80 | HTTP | 516 | POST /admin/get.php HTTP/1.1 |
| 14… | 27.856474 | 192.168.1.80 | 192.168.1.83 | HTTP | 519 | HTTP/1.0 200 OK (text/html) |
| 14… | 28.053803 | 192.168.1.83 | 192.168.1.80 | HTTP | 276 | POST /news.php HTTP/1.1 |
| 15… | 28.065561 | 192.168.1.80 | 192.168.1.83 | HTTP | 11… | HTTP/1.0 200 OK (text/html) |
| 20… | 33.245337 | 192.168.1.83 | 192.168.1.80 | HTTP | 259 | GET /login/process.php HTTP/1.1 |
| 20… | 33.253440 | 192.168.1.80 | 192.168.1.83 | HTTP | 60 | HTTP/1.0 200 OK (text/html) |
| 23… | 38.265103 | 192.168.1.83 | 192.168.1.80 | HTTP | 250 | GET /news.php HTTP/1.1 |
| 23… | 38.271353 | 192.168.1.80 | 192.168.1.83 | HTTP | 60 | HTTP/1.0 200 OK (text/html) |
| 26… | 43.291043 | 192.168.1.83 | 192.168.1.80 | HTTP | 259 | GET /login/process.php HTTP/1.1 |
| 26… | 43.298364 | 192.168.1.80 | 192.168.1.83 | HTTP | 60 | HTTP/1.0 200 OK (text/html) |
| 30… | 48.311212 | 192.168.1.83 | 192.168.1.80 | HTTP | 259 | GET /login/process.php HTTP/1.1 |
| 30… | 48.322750 | 192.168.1.80 | 192.168.1.83 | HTTP | 340 | HTTP/1.0 200 OK (text/html) |
| 30… | 48.439913 | 192.168.1.83 | 192.168.1.80 | HTTP | 148 | POST /admin/get.php HTTP/1.1 |
| 30… | 48.455743 | 192.168.1.80 | 192.168.1.83 | HTTP | 60 | HTTP/1.0 404 NOT FOUND (text/html) |
| 35… | 53.482265 | 192.168.1.83 | 192.168.1.80 | HTTP | 255 | GET /admin/get.php HTTP/1.1 |
| 35… | 53.491062 | 192.168.1.80 | 192.168.1.83 | HTTP | 60 | HTTP/1.0 200 OK (text/html) |
| 40… | 58.515011 | 192.168.1.83 | 192.168.1.80 | HTTP | 259 | GET /login/process.php HTTP/1.1 |
| 40… | 58.522942 | 192.168.1.80 | 192.168.1.83 | HTTP | 60 | HTTP/1.0 200 OK (text/html) |

ネットワーク管理者は、キャプチャしたトラフィックを分析して、疑わしいネットワークアクティビティを調査しています。エンジニアは異常な動作に気づき、送信中のリクエストとデータのヘッダーにデフォルトのユーザー
エージェントが存在することを発見しました。何が起こっているのでしょうか。

**A.** リクエストの頻度によるサービス拒否攻撃の指標

**B.**
ガベージフラッド攻撃攻撃者は開いているポートにガベージバイナリデータを送信しています

**C.** データ流出の指標となるHTTPリクエストはプレーンテキストでなければならない

**D.** キャッシュバイパス攻撃:
攻撃者はキャッシュ不可能なコンテンツに対するリクエストを送信しています

***Answer:*** D

Explanation:
The presence of a default user agent in the headers of requests and data being transmitted suggests a cache bypassing attack. In this scenario, the attacker is likely requesting noncacheable content to avoid detection by caching mechanisms that could otherwise identify and block malicious traffic.

**QUESTION NO: 16**
システムのソフトウェアの脆弱性を利用してマルウェアを拡散するために、脅威の攻撃者がWeb ページで使用するツールはどれですか。

**A.** スクリプトキディキット

**B.** エクスプロイトキット

**C.** 脆弱性キット

**D.** ルートキット

***Answer:*** B

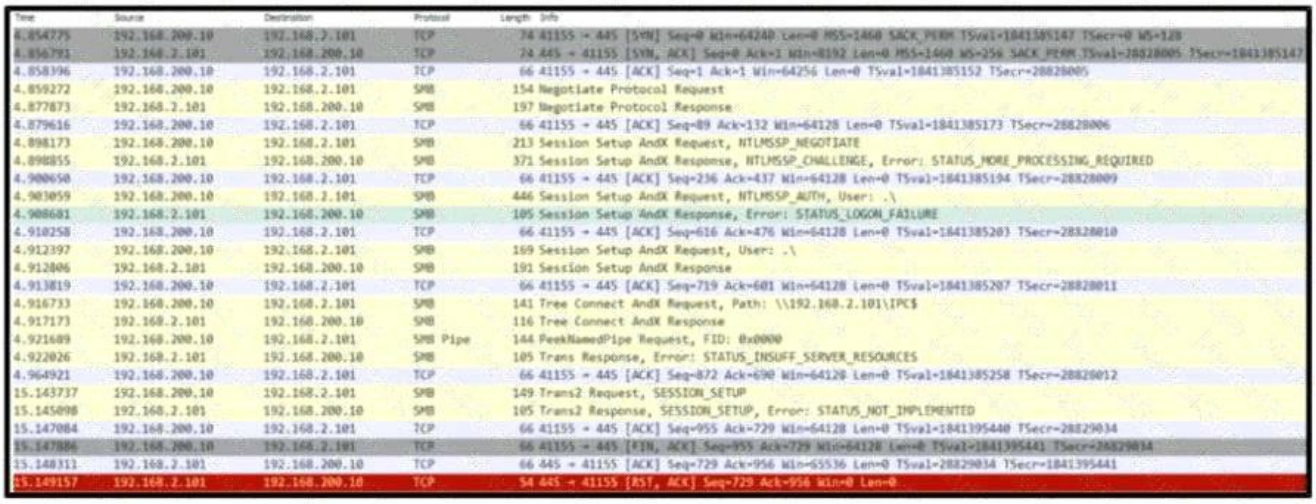
**QUESTION NO: 17**
攻撃者が 4
桁の数字のパスワードのみを使用し、ユーザー名を使用しない認証システムを使用してネッ

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
***Answer:*** B
Explanation:
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

**QUESTION NO: 18**
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
***Answer:*** A
Explanation:
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

**QUESTION NO: 19**
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.** 監視ソフトウェア間のトランザクションログです。
**B.** 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。
**C.** 2 つのネットワーク デバイス間の送信の概要です。
**D.** ユーザーが開始した各セッション内の Cookie を追跡します。
***Answer:*** C

**QUESTION NO: 20**



展示を参照してください。.pcap
ファイルに基づいて、どのプロトコルの脆弱性がセッションの確立に悪用されたかを確認します。
**A.** SMB
**B.** TCP
**C.** 交渉
**D.** IP
***Answer:*** A

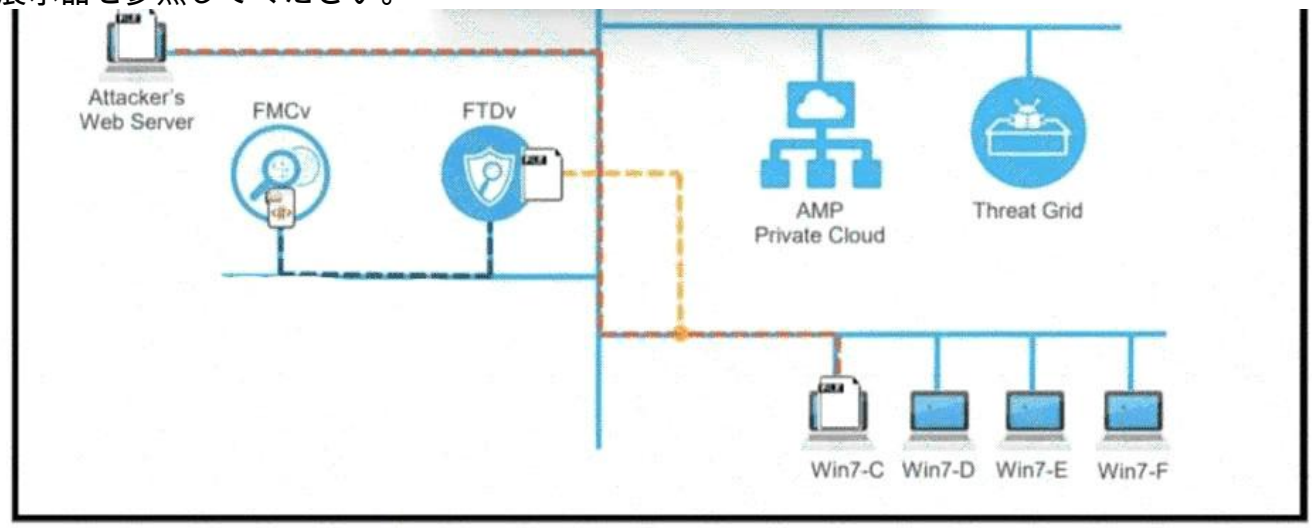
**QUESTION NO: 21**
補強証拠とは何ですか?
**A.** 脅威アクターに対するさらなる制限措置のためにサイバー警察に提供できる証拠
**B.** ハードドライブの正確なコピーなど、法廷で原本のまま提出できる証拠
**C.** 何らかの初期の証拠によって推論された理論や仮定を支持する傾向がある証拠
**D.** 指紋など、事実の結論への外挿に依存する証拠
***Answer:*** C

**QUESTION NO: 22**
脅威とリスクの違いは何ですか?
**A.** 脅威は、システムの弱点を利用する可能性のある潜在的な危険を表します
**B.** リスクは、システム内の既知および識別された損失または危険を表します
**C.** リスクは、システムの不確実性との非意図的な相互作用を表します
**D.** 脅威は、物理的または論理的に攻撃または侵害にさらされている状態を表します。
***Answer:*** A
Explanation:
A threat represents a potential danger that could exploit a weakness in a system while risk is associated with the potential impact or loss that could occur if a threat exploits a vulnerability in the system. So, option A which states "Threat represents a potential danger that could take advantage of a weakness in a system" is correct. References := Cisco Certified CyberOps Associate Overview

**QUESTION NO: 23**

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
***Answer:*** D
Explanation:
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

**QUESTION NO: 24**
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
***Answer:*** D
Explanation:
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

**QUESTION NO: 25**
スケアウェア攻撃とは何ですか?

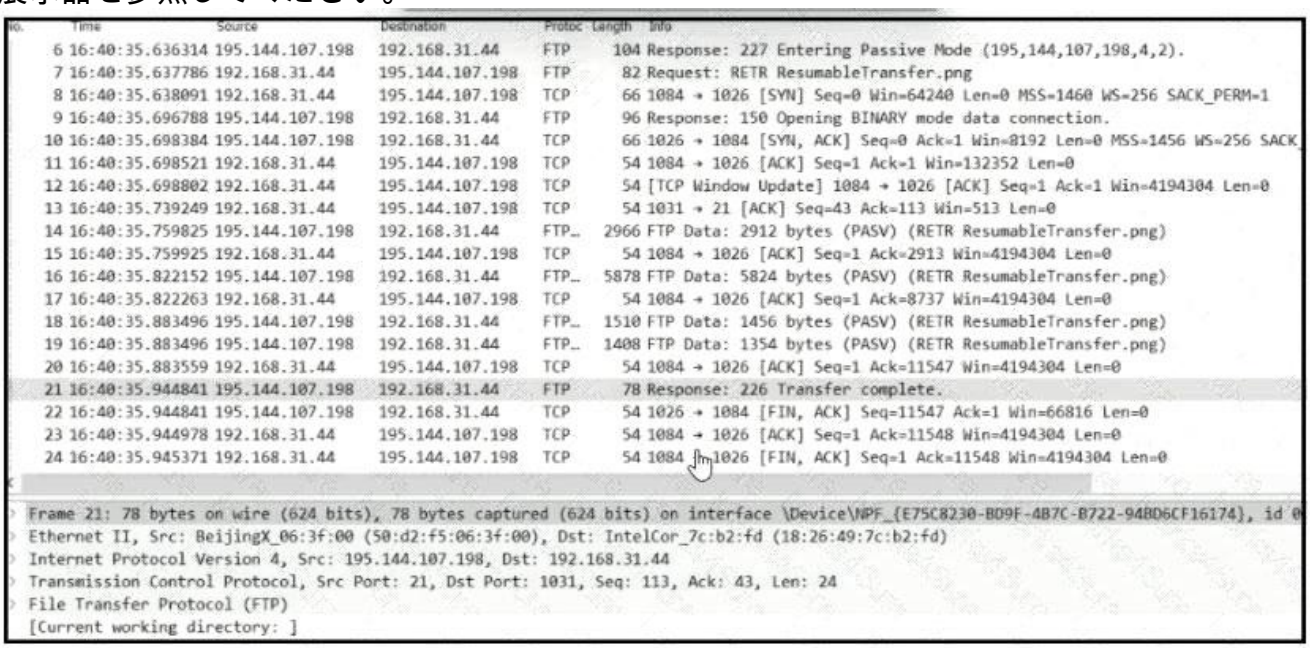
**A.** スプーフィングされた電子メール
アドレスを使用して、ユーザーをだましてログイン資格情報を提供させます。
**B.** 偽のトラフィックで標的の Web サイトを圧倒します
**C.** コンピューターへのゲーム
アクセスと、コンピューターに保存されているデータの暗号化
**D.** 色が点滅するポップアップ ウィンドウを引き起こす悪意のあるコードを挿入します。
***Answer:*** D
Explanation:
Scareware is a type of malware attack that tricks users into believing their computer 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

**QUESTION NO: 26**
低帯域幅攻撃はどの手法ですか?
**A.** ソーシャル エンジニアリング
**B.** セッションハイジャック
**C.** 回避
**D.** フィッシング
***Answer:*** D
Explanation:
Phishing is considered a low-bandwidth attack because it does not require the use of significant network resources. Instead, it relies on social engineering to deceive individuals into providing sensitive information or clicking on malicious links, often through email or other communication methods1.

**QUESTION NO: 27**
統計的検出と比較した場合のルールベース検出とは何ですか?
**A.** ユーザーの身元の証明
**B.** ユーザーの行動の証明
**C.** ユーザーの行動の可能性
**D.** ユーザーのアイデンティティの改ざん
***Answer:*** B
Explanation:
Rule-based detection is a type of intrusion detection system (IDS) that uses predefined rules or signatures to identify malicious or suspicious activity. Rule-based detection can provide proof of a user's action, such as an attempt to exploit a known vulnerability or execute a malicious command. Rule-based detection can also provide a high level of accuracy and specificity, but it requires constant updates and maintenance of the rules or signatures.
References: https://learningnetworkstore.cisco.com/on-demand-e-learning/understanding-cisco- cybersecurity-operations-fundamentals-cbrops-v1.0/CSCU-LP-CBROPS-V1 -028093.html (Module 4: Attack Methods, Lesson 4.2: Attack Techniques)

**QUESTION NO: 28**
アクセス制御の観点から見た承認と認証の違いは何ですか?
**A.**
認可は特定のリソースの作成者を定義し、認証はリソース自体へのアクセスを許可します。
**B.**
認証は、システムがユーザーが有効かどうかを検証し、承認は割り当てられた必要なリソースを適用して提供します。
**C.**
認証はシステムリソースへのアクセスを管理し、認可プロセスはユーザーがリソースを作成できるかどうかを定義します。
**D.**
認可は、特定のユーザーがシステム内で認証されているかどうかを追跡し、認証は認可方法を識別する役割を果たします。
***Answer:*** B

**QUESTION NO: 29**
展示品を参照してください。




Wireshark 内の TCP
ストリーム経由で抽出可能なファイルが含まれているフレーム番号はどれですか?
**A.** 7、14、21
**B.** 7と21
**C.** 14、16、18、19
**D.** 7 から 21
***Answer:*** A
Explanation:
The file that is extractable via TCP stream within Wireshark is the one that has the Content-Type header set to application/octet-stream, which indicates binary data. Thisheader is present in frames 7, 14, and 21, which are part of the same TCP stream. The other frames have different Content-Type headers, such as text/html or image/jpeg, which are not

extractable as binary files. References := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 3: Network Intrusion Analysis, Lesson 3.2: Analyze Data from Common TCP/IP Protocols, Topic 3.2.3: HTTP

**QUESTION NO: 30**
コマンド アンド コントロール サーバーの機能は何ですか?
**A.** ネットワークデバイスで開いているポートを列挙します
**B.** セカンダリ ペイロードをマルウェアにドロップします。
**C.** 侵害後にネットワークの制御を取り戻すために使用されます。
**D.** 侵害されたシステムに命令を送信します。
***Answer:*** D
Explanation:
A command and control server (C2 or C&C) is a server that is used by attackers to communicate with and control compromised systems, such as bots, zombies, or backdoors. The C2 server can send instructions to the compromised systems, such as executing commands, downloading files, uploading data, or launching attacks.
The C2 server can alsoreceive information from the compromised systems, such as system information, keystrokes, screenshots, or credentials. 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

**QUESTION NO: 31**
SOC チームは、進行中のポート
スキャンを検出しました。調査の結果、チームはスキャンが会社のサーバーをターゲットにしていると結論付けました。サイバー キル チェーン
モデルによると、このタイプのイベントにはどのステップを割り当てる必要がありますか。
**A.** 目標に対するアクション
**B.** 配達
**C.** 偵察
**D.** 搾取
***Answer:*** C

**QUESTION NO: 32**
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

***Answer:*** D

Explanation:

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.

**QUESTION NO: 33**

これらのうち、セキュリティインシデントに関連するSOCメトリックを説明しているのはどれですか？

**A.**インシデントの検出にかかる時間

**B.**インシデントのリスクを評価するのにかかる時間

**C.**インシデントによって引き起こされた停止の確率

**D.**インシデントによって引き起こされる妥協と影響の確率

***Answer:*** A

Explanation:

SOC metrics in relation to security incidents typically refer to the time it takes to detect the incident. These metrics are crucial for evaluating the effectiveness of incident response and remediation efforts by SOC teams. For example, metrics like the Mean Time to Detect (MTTD) enable organizations to assess how quickly they can identify a security incident, which is essential for reducing the impact of the incident on the organization.

**QUESTION NO: 34**

エンジニアが Wireshark でトラフィックをフィルタリングして、LAN 10.11.x.x のトラフィックのみを表示することにより、PCAP ファイルをさらに分析できるようにするのはどのフィルターですか?

**A.** src=10.11.0.0/16 and dst=10.11.0.0/16

**B.** ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16

**C.** ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16

**D.** src==10.11.0.0/16 and dst==10.11.0.0/16

***Answer:*** B

Explanation:

In Wireshark, to filter traffic for a specific LAN, the correct syntax uses ip.src== and ip.dst== to specify the source and destination IP addresses. The /16 denotes the subnet mask, indicating that we are interested in the entire 10.11.x.x range. This filter will show all traffic where both the source and destination IP addresses fall within the specified LAN, excluding any internet traffic. References: The information is based on the Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course, which covers network intrusion analysis and the use of tools like Wireshark for traffic analysis1.

**QUESTION NO: 35**

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
***Answer:*** D
Explanation:
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