CompTIA.CAS-005-JPN.v2026-11-06.q249

試験コード：	CAS-005-JPN
試験名称：	CompTIA SecurityX Certification Exam (CAS-005日本語版)
認証ベンダー：	CompTIA
無料問題の数：	249
バージョン：	v2026-11-06
ページの閲覧量：	103
問題集の閲覧量：	2494

https://www.jpnshiken.com/shiken/CompTIA.CAS-005-JPN.v2026-11-06.q249.html

質問: **1**
SOCエンジニアは、一連のタスクを最小限の労力で迅速に自動化するソリューションを設計しています。以下の目標を達成する必要があります。
- IOCは検証されなければならない
- すべてのファイアウォールとメールゲートウェイで、悪意のあるドメインをブロックする必要があります。
- 業務状況を確認するメールを送信する必要があります。

この目標を達成するための最良の方法はどれですか？
A. APIを使用してIOCに対してクエリを実行する
B. TAXIIサーバーを使用してSTIXファイルを共有する
C. SCAPを実行してベースラインを設定します
D. プレイブックの展開と実行
正解: **D** (コメントを発表する)
Executing automated playbooks enables a SOAR workflow that orchestrates multiple security tasks with minimal manual effort. A playbook can verify indicators of compromise, automatically push blocking rules to firewalls and email gateways, and send notification emails once the actions are completed. This approach automates the entire response sequence and ensures it is performed quickly and consistently.

質問: **2**
プロセッサが暗号化キーを知らない場合でも、暗号化されたデータを意味のある形で操作できるようにするのは、次のうちどれですか？
A. 同等者の同時認証
B. 封筒暗号化
C. 関連データを含む認証済み暗号化
D. 準同型暗号
正解: (正解を表示します)
Homomorphic encryption allows for the manipulation and computation of encrypted data without needing to decrypt it, meaning the processor does not require access to the encryption key. This enables meaningful operations on encrypted data while maintaining confidentiality.

質問: **3**
ジョン・ドウのメールアカウントが侵害されました。攻撃者のジョン・ドウのアカウントへのアクセス権は削除され、多要素認証(MFA)が導入されました。攻撃者は、経理部のジョー・ローを騙して、メールのやり取りを通じて不正な請求書を支払わせました。セキュリティアナリストは、ジョー・ローが最初に受信したメールのヘッダーを解析しています。



攻撃者がどのようにして請求書の支払いを済ませることができたのかを最もよく説明しているのは、次のうちどれですか？

A. 攻撃者はジョン・ドウのパスワードを推測しました。

B. 攻撃者が新しいドメインを登録しました。

C. 攻撃者のメールは、検証にドメインキーを使用していませんでした。

D. メールが送信者ポリシーフレームワークのチェックに失敗しました。

正解: (正解を表示します)

The email headers show that the message originated from an external mail server associated with a different domain while the visible sender address appears to be from the legitimate company domain. At the same time, the SPF check passed for the sending infrastructure, indicating the sending domain authorized that mail server. This pattern is consistent with a look- alike or newly registered domain used to impersonate a trusted sender, enabling the attacker to send convincing invoice emails that appear legitimate to the recipient.

質問: **4**

最高セキュリティ責任者(CSO)は、セキュリティチームに対し、以下の要件を満たす技術的制御策を実施するよう要請した。

- ローカルNASとクラウドベースのファイルストレージとの間のトラフィックを監視します
リポジトリ
- 現場スタッフが機密性の高い顧客の個人情報にアクセスするのを防ぎます
ファイルリポジトリにある文書は、偶発的または意図的に
個人向けSaaSソリューションで機密文書を共有する
文書属性を利用して誤検出を減らす
・エージェントレスであり、従業員のデスクトップやノートパソコンにはインストールされません。

インストールおよび設定を行った場合、以下のうちどれがCSOの要件を最もよく満たすでしょうか？

(2つ選択してください。)

A. DLP

B. NGFW

C. UTM

D. UEBA

E. CASB
F. ヒップ
正解: **(**正解を表示します**)**
DLP (Data Loss Prevention): A network-based DLP solution can inspect traffic to and from on- prem NAS devices as well as cloud storage, using document fingerprinting and content-aware rules to reduce false positives without requiring agents on endpoints.
CASB (Cloud Access Security Broker): An agentless CASB sits inline (or via API) between users and cloud services - both sanctioned and unsanctioned - preventing uploads of sensitive PII to personal SaaS apps and enforcing attribute-based policies on documents in cloud repos.

質問: **5**
ユーザーが http://10.1.1.1 のウェブページにアクセスしようとしました。以前はウェブページで認証が不要でしたが、現在はブラウザで認証情報の入力を求められます。問題の再発を防ぎ、認証情報の漏洩の可能性を減らすには、以下のどの対策が最も効果的でしょうか？
A. アクセスポイントに802.1x EAP-TTLSを実装して、悪意のある双子のリスクを軽減する
B. DNS セキュリティを使用するように内部サービスを移行しています
C. Webサーバーの設定を変更し、認証にX509証明書を利用する
D. IDS がなりすまし攻撃を検出するための新しいルールをインストールする
正解: **(**正解を表示します**)**
The change from no authentication to requiring credentials suggests a shift in security posture for the web service. Using X.509 certificates for authentication provides a secure, certificate-based authentication method that can eliminate reliance on passwords and reduce the risk of credential exposure. This approach ensures encrypted and authenticated connections, preventing unauthorized access in the future.

質問: **6**
ある企業が顧客向けに外部アプリケーションを作成しました。セキュリティ研究者によると、このアプリケーションには認証と認可を回避するために悪用される可能性のある深刻なLDAPインジェクションの脆弱性があるとのことです。この問題を最も効果的に解決するには、次のうちどの対策が適切でしょうか？
(2つ選択してください。)
A. 入力サニタイズを実施します。
B. SIEMを導入する。
C. 容器を使用する。
D. OSにパッチを適用します。
E. WAFを導入します。
F. リバースプロキシをデプロイします。
G. IDSを導入する。
正解: **(**正解を表示します**)**
Conduct input sanitization: The primary safeguard against LDAP injection is to validate and cleanse all user-supplied inputs before they're incorporated into LDAP queries. By enforcing strict whitelists (allowing only expected characters or patterns) and escaping or rejecting any special LDAP-filter metacharacters, you eliminate the injection vectors at the source.
Deploy a WAF: While you're remediating the code, a properly configured Web Application Firewall can provide an additional layer of defense by detecting and blocking known LDAP injection payloads (e.g., *)(uid=*))(|(uid=*) in incoming requests. This helps mitigate exploitation risk in the short term and serves as a compensating control until the application is fully secured.

質問: **7**

グローバル企業のセキュリティ管理者が、個人識別情報を含むシステムのパスワード複雑性ルールを更新したいと考えています。この情報を得るのに最適なリソースは次のうちどれでしょうか？
A. NIST
B. GDPR
C. CMMI
D. カップ
正解: **(**正解を表示します**)**
NIST (National Institute of Standards and Technology): Provides comprehensive password guidelines (e.g., SP 800-63B) widely used for securing systems, including handling PII. GDPR (General Data Protection Regulation): Focuses on data privacy laws rather than technical password policies.
CMMI (Capability Maturity Model Integration): Addresses process improvement, not password complexity.
COPPA (Children's Online Privacy Protection Act): Focuses on child data privacy, not password rules.

質問: **8**
DNP3にとってセキュリティ上の懸念事項となるのは次のうちどれですか？
A. 自由形式のメッセージにはサポートが必要です。
B. 利用可能な機能コードは標準化されていません。
C. 認証が割り当てられていません。
D. これはオープンソースのプロトコルです。
正解: **C (**コメントを発表する**)**
Original DNP3 lacks built-in authentication for its messages, making it vulnerable to spoofing and replay attacks. Secure extensions (Secure DNP3) add cryptographic authentication, but legacy deployments without these extensions remain at risk.

質問: **9**
ある組織は、クラウドプロバイダーが管理する無料の暗号鍵ではなく、自社管理の暗号鍵を使用していました。最高情報セキュリティ責任者 ©ISO)は毎月の請求書を確認し、自社管理の暗号鍵が予想以上にコストが高いことに気づきました。強固なセキュリティ体制を維持しながらコストを削減するために、CISOは次のうちどれを推奨すべきでしょうか？
A. オンプレミスの HSM を使用してキーをローカルで管理します。
B. パブリックとして分類されるデータのクラウド プロバイダー キーの構成を調整します。
C. クラウドにデプロイされたすべての新しいリソースでクラウド管理キーの使用を開始します。
D. クラウド プロバイダーがキャッシュされたキーを使用できるように、キーのローテーション期間を 1 年に延長します。
正解: **(**正解を表示します**)**
Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk- based decision. Public data, by definition, is not confidential.
Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider- managed keys are often free or significantly cheaper.
Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer-managed keys where appropriate, while optimizing costs for less sensitive data.

質問: **10**
ある企業が最近マルウェアに感染しました。根本原因分析の結果、複数のユーザーが独自のアプリケーションをインストールしていることが判明しました。さらなる侵害を防ぐため、同社はシステム上で実行できるアプリケーションを承認されたアプリケーションのみに制限することを決定しました。以下の対策のうち、企業が実施すべきものはどれですか？

A. 署名
B. アクセス制御
C. ヒップ
D. 許可証リスト
正解: **(**正解を表示します**)**
To prevent unauthorized applications from running, the company needs a mechanism to explicitly define and enforce which applications are allowed to execute. "Permit listing" (often referred to as
"whitelisting" in security contexts) is the most effective solution here. It involves creating a list of approved applications, and only those on the list are permitted to run, blocking all others by default. This directly addresses the root cause--users installing unapproved software--by restricting execution to only authorized programs.

質問: **11**
ある企業がWindows ServerからLinuxベースのサーバーに移行しようとしています。セキュリティエンジニアは、すべてのLinuxサーバーでセキュリティソフトウェアを管理する構成管理ソリューションを導入する必要があります。以下の構成ファイルスニペットのうち、どれが最も適切でしょうか？

A.
```
---
- name: deployment
  hosts: linux_servers
  remote_user: root

  tasks:
  - name: Install security software
    ansible.builtin.apt:
```

B.
```
<xml>

<hosts>linux_servers</hosts>
<os_type>Linux_3.1</os_type>
<SELinux>true</SELinux>
<source>com.canonical.io</source>
```

C.
```
{"name":"deployment",
  "hosts":"linux_servers,"
  "remote_user":"Administrator,"
}
{"tasks":"name":"Install security software",
    "com.microsoft.store.latest"
}
```

D.
```
{"task":"install",
 "hosts": "linux_servers"
 "remote_user": "root"
 "se_linux":"false"
 "application": "AppX"
```

正解: **A (**コメントを発表する**)**
Chosen option has YAML syntax for an Ansible playbook, which is the industry-standard configuration management tool for automating tasks on Linux servers. It is specifically designed for Linux environments and supports package installation and security software deployment at scale.

質問: **12**
セキュリティアナリストは、セキュリティインシデントに関連するWebサーバーからログを収集します。
アナリストはログに以下のエントリを発見した。
SELECT user FROM Customers WHERE userID = "SRequest(userID)"
以下のうち、この事件の再発を防ぐことができるのはどれですか？
A. URLエンコーディング
B. クエリパラメータ化
C. データサニタイズ
D. SQL出力エンコーディング
正解: **(**正解を表示します**)**
Query parameterization ensures that user input is treated strictly as data, not as executable SQL code. This prevents SQL injection attacks like the one shown in the log entry, thereby eliminating the vulnerability that led to the incident.

質問: **13**
ある組織は、特定の脆弱性の影響を受ける資産をより正確に特定するためのプラットフォームを導入したいと考えています。この目標を達成するために最適な基盤となるコンポーネントは次のうちどれですか？
A. サセ
B. CMDB
C. SBoM
D. SLM
正解: **(**正解を表示します**)**
A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets.

質問: **14**
敵対的シミュレーション演習中に、外部チームが組織に検知されることなく機密情報やシステムにアクセスすることに成功しました。組織は、この事態を最も効果的に解決するために、以下のどの対策を講じるべきでしょうか？
A. 攻撃者特性分析のためのハニーポットの設定
B. 攻撃者によるシミュレーターの活用
C. 攻撃者のためのハニーネットワークの構築
D. 偽アカウントと偽書類の利用
正解: **(**正解を表示します**)**
Utilizing decoy accounts and documents (often referred to as honeytokens) is the best mitigation strategy in this scenario. Decoy accounts and documents are designed to look like legitimate, sensitive data or systems, but they are actually trapping. If an adversary accesses these decoys, it can trigger alerts and give the organization an early warning of the intrusion. This helps the organization detect unauthorized access more quickly and provides the opportunity to respond before actual damage is done.

質問: **15**

あるウェブサービスプロバイダーが、現在実施されていない要件を含む非常に大規模な契約を獲得しました。契約上の要件を満たすためには、同社は以下の基準を達成する必要があります。
- 稼働率99.99%
- 読み込み時間3秒
応答時間 = 1.0秒未満
コンピューティング環境に関して、セキュリティエンジニアは要件を最も満たすために、次のうちどれを推奨すべきでしょうか？(3つ選択してください。)
A. 本社にファイアウォールを設置する
B. コンテンツ配信ネットワークの展開
C. サーバークラスタの実装
D. ベアメタルロードを採用したアプリケーション
E. ストレージの入出力を下げる
F. バックアップサーバーへのRAIDの実装
G. すべての開発者ワークステーションに冗長電源を採用
正解: **(**正解を表示します**)**
To meet the high uptime, load time, and response time requirements, the following recommendations would be most effective:
Deploying a content delivery network (CDN): A CDN can distribute content across multiple locations globally, reducing load times by serving content from the nearest edge server to the user.
Implementing server clusters: Server clusters can ensure high availability and load balancing, which is essential for maintaining 99.99% uptime and improving response times during high traffic periods.
Lowering storage input/output (I/O): Reducing storage I/O can improve performance by speeding up data access and enhancing the system's ability to meet load time and response time requirements.
These solutions directly address the performance and availability metrics that are required for the contract. Other options like implementing RAID, using redundant power for workstations, or installing firewalls would not directly contribute to the high availability or performance requirements.

質問: **16**
セキュリティチームは、通常の営業時間外に、あり得ない移動やブルートフォース攻撃の可能性に関するアラートを受け取ります。さらにログを調査した結果、特定のユーザーが標的とされ、未知のサイトへのデータ転送が試みられたことが判明しました。これらの問題を軽減するために、チームは次のうちどれを行うべきでしょうか？
A. ファイアウォールルールを作成して、それらのユーザーが機密データにアクセスできないようにします。
B. アップロード活動を承認されたサイトのみに制限する。
C. ファイル転送に関連する送信元と宛先のパケットキャプチャを継続的に実行できるようにします。
D. 営業時間外は、該当ユーザーのログイン操作を無効にします。
正解: **(**正解を表示します**)**
The security team has identified that certain users are being targeted by what appears to be impossible travel and brute-force attacks, followed by attempts to transfer data to an unknown site. To mitigate this, the best approach is to restrict uploading activity to only authorized sites. This ensures that even if the attackers gain access to the user accounts, they will not be able to exfiltrate data to unknown or unauthorized locations.
This control directly addresses the data exfiltration risk by preventing unauthorized file uploads, regardless of whether the attacker successfully compromises user credentials.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
最近のセキュリティ イベント中に、非本番環境から本番環境へのアクセスにより、権限のないユーザーが次の操作を実行できました。
承認されていないソフトウェアをインストールする
計画外の構成変更を行う
調査中に、以下のことが判明しました。
IAMチームによって複数の新規ユーザーが一括追加されました
最近、追加のファイアウォールとルーターが追加されました
脆弱性評価は30日以上無効になっています
アプリケーション許可リストは2週間変更されていません
さまざまなタイプのトラフィックのログが利用できませんでした
エンドポイントは10日以上パッチが適用されていない
適切な監視を確実に行うために、次のうちどのアクションを実行する必要があると考えられますか? (2 つ選択してください)
A. IAM チームによる一括ユーザー作成を無効にする
B. すべてのセキュリティおよびネットワークデバイスのログ保存期間を、すべてのトラフィックに対して180日間に延長します。
C. アプリケーションの許可リストを毎日確認する
D. 新しいパッチ/ホットフィックスが利用可能になったらすぐに、すべてのエンドポイントとネットワークデバイスを定期的に更新します。
E. すべてのネットワークおよびセキュリティデバイスがSIEMに関連データを送信していることを確認する
F. ファイアウォールルールを設定して、本番環境から非本番環境へのトラフィックのみを許可します。
正解: **B,E (**コメントを発表する**)**
Extend log retention for all security and network devices to 180 days for all traffic The incident investigation was hampered because "logs were unavailable for various types of traffic," which is a direct monitoring/forensics gap. Longer and more comprehensive retention is needed so security teams can reconstruct events and spot suspicious cross-environment access.
Ensure all network and security devices are sending relevant data to the SIEM Proper monitoring requires centralized, correlated visibility; without all firewalls, routers, and other security tools feeding events to the SIEM, lateral movement from non-prod to prod can go undetected. Centralized logging from "all services and infrastructure components" is a core monitoring best practice.

質問: **18**
企業の内部ネットワークでセキュリティ侵害が発生しており、脅威アクターは依然として活動しています。業務上の要件により、この環境のユーザーは複数のマシンを同時に利用することが許可されています。
次のログ スニペットがあるとします。

Time	User	Process	Status	Machine
10:11	user-a	.exe	blocked	machine02
10:15	user-b	setup.exe	blocked	machine02
10:15	user-A	appwiz.exe	blocked	machine01
10:16	user-c	appwiz.CPL	blocked	machine03
11:17	user-c	cmd.exe	blocked	machine03
11:18	user-h	msconfig.exe	blocked	machine04
11:19	user-d	firefox.exe	blocked	machine04
11:19	user-d	cmd.com	blocked	machine01

CompTIA
jpnshiken.com

有効なユーザーに影響を与えずにインシデントを最も効果的に封じ込めるために、セキュリティアナリストが無効にする必要があるアカウントは次のどれですか?

A. ユーザーa

B. ユーザーb

C. ユーザーc

D. ユーザーd

正解: **C** (コメントを発表する)

User user-c is showing anomalous behavior across multiple machines, attempting to run administrative tools such as cmd.exe and appwiz.CPL, which are commonly used by attackers for system modification. The activity pattern suggests a lateral movement attempt, potentially indicating a compromised account.

質問: **19**

セキュリティ管理者はアラートを自動化する必要があります。サーバーは構造化されたログファイルを生成し、それを解析してアラームがトリガーされたかどうかを判断する必要があります。以下のコード関数が与えられた場合：

```
def parse_logs(logfile):
    with open(logfile) as log_file:
        parsed_log = json.load(log_file)
    if parsed_log["error_log"]["system_1"]["InAlarmState"]:
        print("System is in an alarm state!")
```

コードが解析するログ入力として最も可能性が高いのは、次のうちどれですか？

A.
```
["error_log]
    ["system_1"]
        ["InAlarmState": True]
```

B. <"error_log"><"system_1"></"InAlarmstate"="True"></"system_1"></"error_l

C. そして">

```
error_log:
    - system_1:
      InAlarmState: True
```

D. <"error_log": {"system_1": {"InAlarmState": True }}}

正解: **D** (コメントを発表する)
Based on the provided Python code snippet, the answer <"error_log": {"system_1":
{"InAlarmState": True }} is a minimal example of the JSON data structure that would cause the code's if condition to evaluate as True.
The code checks for the presence and value of a nested key:
Python
if parsed_log["error_log"]["system_1"]["InAlarmState"]:
print("System 1 is in an alarm state!")

質問: **20**
アプリケーションセキュリティエンジニアがワークロードのIAM構成を調べています。以下は、デコードされたペイロードとヘッダーのサンプルです。

CompTIA

```
{
  "alg": "None",
  "typ": "JWT"
}
{
  "sub": "user_98765",
  "iat": 1680000000,
  "exp": 1680003600,
  "role": "svc_account",
  "refresh": true,
  "token_id": "abc123"
}
```

次のうち、最も懸念されるリスクはどれですか？
A. 横方向の動き
B. 特権の拡大
C. クレデンシャルスタッフィング
D. デシリアライゼーションによるRCE
正解: **B** (コメントを発表する)
The JWT header shows the algorithm set to "None", which means the token is not cryptographically signed or verified. This allows an attacker to modify the token payload and change claims such as the role field to gain elevated permissions. Because the token could be altered to assign higher privileges, the most significant risk is unauthorized privilege escalation within the application.

質問: **21**
最高情報セキュリティ責任者(CISO)がセキュリティチームに対し、SOCが業界のISACからIoCを受け取っているかどうかを尋ねました。CISOがこの情報を入手しようとしている最も可能性の高い理由は次のうちどれですか？
A. SOCが類似組織に対する既知の攻撃を検出できるようにするため
B. SOCが潜在的な攻撃を積極的に防止していることを確認する
C. SOCオーケストレーションプレイブックが最新の状態であることを確認する
D. SOCが業界のベストプラクティスに準拠していることを保証する
正解: (正解を表示します)
Industry Information Sharing and Analysis Centers distribute indicators of compromise related to threats observed across organizations within the same sector. By ingesting these indicators, the SOC can detect attacks, malicious infrastructure, and adversary techniques that have already targeted similar organizations. This allows the SOC to identify and respond to known threats affecting the industry more quickly.

質問: **22**
ある企業が、セキュリティ上の脆弱性を特定し、関係者を潜在的なインシデントに備えさせるために、第三者のコンサルタントを雇ってサイバーセキュリティインシデントシミュレーションを実施しました。この活動を最も適切に表しているのは次のうちどれですか？
A. テーブルトップエクササイズ
B. ウォークスルーレビュー
C. 学んだ教訓
D. 事業影響分析
正解: **A (**コメントを発表する**)**
A tabletop exercise is a discussion-based simulation where key stakeholders, including management and technical teams, gather to walk through a hypothetical cybersecurity incident.
The goal is to identify security gaps, assess response strategies, and prepare for real-world incidents. During this exercise, participants typically discuss their roles and decisions in handling the incident, but no actual systems are impacted.

質問: **23**
インシデント対応チームは、複数のワークステーションのオフラインバックアップからの復旧を完了しました。これらのワークステーションは、十分なトレーニングプログラムが実施されていたにもかかわらず、ユーザーがスピアフィッシング攻撃の被害に遭った後、ランサムウェア攻撃を受けました。再発リスクを最も効果的に低減するために、教訓の検証段階で考慮すべき質問は次のうちどれでしょうか？
(2つ選択してください。)
A. スピアフィッシング攻撃の仕掛け人に対して法的措置を取る機会はありますか？
B. 内部および外部のどの関係者に情報漏洩を通知する必要がありますか？
C. オフラインバックアップからの復旧速度を向上させるために、どのような方法が利用できますか？
D. 侵害につながった測定可能なユーザー行動は何でしたか？
E. ユーザー研修が失敗した場合に、どのような技術的対策を実施すれば防御策となるでしょうか？
F. スピアフィッシング攻撃の標的となることが多いユーザーロールはどれですか？
正解: **(**正解を表示します**)**
What measurable user behaviors were exhibited that contributed to the compromise?
During the lessons-learned phase, it's important to analyze the specific user behaviors that led to the successful spear-phishing attack, even after a robust training program. This could involve understanding patterns such as clicking on suspicious links, failing to verify emails, or not reporting unusual activity. By identifying these behaviors, the organization can target specific areas for improvement in training or behavior modification.
Which technical controls, if implemented, would provide defense when user training fails?
Since users fell victim to the spear-phishing attack despite training, it's critical to implement technical controls that can provide an additional layer of defense. This may include email filtering to block phishing attempts, multi-factor authentication (MFA), endpoint detection and response (EDR) tools, and sandboxing for suspicious attachments. These controls will help prevent or mitigate attacks when training alone is insufficient.

質問: **24**
ある企業は、開発環境で個人情報（PII）データに関するインシデントが発生した後、プライバシー要件を遵守するためにプロセスを変更したいと考えています。機能テストを実行するために、QAチームは指定された形式の有効なデータを依然として使用する必要があります。開発ライフサイクルに影響を与えずにリスクに対処するには、次のうちどれが最適ですか？
A. QA環境に移動する前にデータを暗号化する

B. 個人を特定できないようにデータを切り捨てる
C. 大規模言語モデルを使用して合成データを生成する
D. 機密フィールドにトークン化を活用する
正解: **D (**コメントを発表する**)**
Tokenization replaces sensitive data (e.g., PII) with non-sensitive placeholders while maintaining format consistency, ensuring compliance without disrupting testing. This method is commonly used for PCI-DSS and GDPR compliance while preserving data structure for functional tests.

質問: **25**
IT部門は現在、エンタープライズDLPソリューションの導入に取り組んでいます。リスク軽減に関しては、デューデリジェンスとベストプラクティスに従う必要があります。承認された変更が適切に計画され、実行されることを保証するものは次のうちどれですか？
A. リスク管理
B. ネットワーク管理
C. 構成管理
D. 変更管理
正解: **(**正解を表示します**)**
Change management establishes a formal process for planning, approving, testing, scheduling, and documenting all authorized modifications. This ensures that deploying or updating the DLP solution follows controlled steps, reducing the risk of unplanned disruptions or misconfigurations.

質問: **26**
あるアプリケーションでは、個人情報(PII)の保存が必要です。システムエンジニアは、鍵管理に外部デバイスを使用するソリューションを実装する必要があります。次のうち、最適なソリューションはどれですか？
A. SBoM
B. HSM
C. TPM
D. vTPM
正解: **(**正解を表示します**)**

質問: **27**
最近合併した2社は、社内認証ストアを統合することなく、両社間でアプリケーションへのアクセスを統一したいと考えています。以下の技術戦略のうち、この目的を最も効果的に達成できるのはどれでしょうか？
A. 連邦
B. 半径
C. TACACS+
D. MFA
E. ABAC
正解: **(**正解を表示します**)**
Federation allows two or more organizations to establish a trust relationship for sharing authentication and authorization information without merging internal authentication stores. With federation, users from both companies can access resources in the other company's environment by using their own credentials, typically through a centralized identity provider (IdP). This approach allows the companies to keep their authentication systems separate but still provide seamless access to applications and services, making it ideal for scenarios like mergers where complete consolidation of authentication systems might not be immediate.

質問: **28**
セキュリティアナリストが、一般公開されている銀行アプリケーションを支える、脆弱性があり非推奨となっているランタイムエンジンを特定しました。開発者は、最新の開発環境への移行には少なくとも1か月かかると見込んでいます。移行期間中にサービスを中断することなく、リスクを最も効果的に軽減できる対策は次のうちどれでしょうか？
A. コードの準備が整うまでシステムをシャットダウンします
B. 影響を受けるランタイムエンジンのアンインストール
C. 影響を受けるポート上のトラフィックを選択的にブロックする
D. 署名を用いたIPSおよびWAFの設定
正解: **(**正解を表示します**)**
To mitigate the risk of the vulnerable and deprecated runtime engine while the developers transition to a more modern environment, configuring an Intrusion Prevention System (IPS) and a Web Application Firewall (WAF) with appropriate signatures would provide protection without disrupting the service. These security controls can help detect and block known exploits targeting the vulnerable runtime engine. By applying these measures, the application can continue running while minimizing the risk of exploitation from external threats.

質問: **29**
外部のSaaSソリューションユーザーから、ロールベースアクセス制御モジュールに関連するバグが報告されました。このバグにより、マルチテナント展開モデルにおけるクライアントセグメンテーションに関連するシステムロジックをバイパスすることが可能になります。
開発者はバグレポートを評価した結果、同じバグが以前のリリースで特定され、修正されていたことを発見しました。その後、開発者は、プラットフォームの以前のバージョンから既存のソフトウェアコンポーネントを統合した際に、バグが再び発生したと判断しました。このシナリオを防ぐための最良の方法は、次のうちどれですか？
A. 回帰テスト
B. コード署名
C. 自動テストと再テスト
D. ユーザー受け入れテスト
E. ソフトウェア構成分析
正解: **(**正解を表示します**)**
Regression testing is a software testing practice that ensures that recent code changes have not adversely affected existing functionalities. In this scenario, the reintroduction of a previously fixed bug indicates that changes or integrations brought back the old issue. Implementing comprehensive regression testing would help detect such reintroductions by systematically retesting the existing functionalities whenever changes are made to the codebase. This practice is crucial in maintaining the integrity of the application, especially in complex systems where multiple components interact.

質問: **30**
ある政府機関は、国際ローミング中に政府発行のデバイスで携帯電話ネットワークへのアクセスを無効にする設定を導入しました。この機関はモバイルホットスポットを発行し、職員にインターネットアクセスにそれを使用することを義務付けています。この機関の根拠として最も適切なものは次のうちどれですか？
A. SIMハイジャックの脆弱性から保護するため
B. キャリアOTA攻撃ベクトルから防御する
C. 悪意のある無線接続をブロックする
D. プロトコルを従来の3Gにダウングレードしようとする試みを防ぐため
E. 指向性電磁干渉をフィルタリングする
正解: **B (**コメントを発表する**)**

By disabling direct cellular roaming and requiring mobile hotspots, the agency reduces exposure to foreign carriers' over-the-air (OTA) update mechanisms. This defends against carrier-based OTA attack vectors that could compromise devices when connected to international networks.

質問: **31**
ある下請け業者が、大手航空機メーカー向けにセーフティクリティカルな航空電子機器ソフトウェアを開発しています。あるインシデント発生後、第三者調査機関は同社に対し、開発ライフサイクルにおいて形式手法の導入を開始するよう勧告しました。以下の調査結果のうち、調査機関の勧告を最も直接的に裏付けるものはどれですか。
A. システムの部品表に商用ライブラリとオープンソース ライブラリが含まれていませんでした。
B. 会社には、動的かつインタラクティブなアプリケーション セキュリティ テスト標準が欠けています。
C. コードベースには、機能要件と非機能要件への追跡可能性が欠けています。
D. 実装されたソフトウェアは、コンピューティング リソースとメモリ リソースを効率的に管理しません。
正解: **(**正解を表示します**)**
Formal methods in software development focus on rigorously proving correctness and ensuring that all software components align with defined requirements. Lack of traceability to functional and non-functional requirements directly points to a gap in ensuring the software meets its specified goals, which formal methods would address by providing a mathematically verified framework to ensure compliance throughout the development process.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
モバイル管理者は、管理対象デバイスに適切なモバイル設定が適用されていることを確認するために、以下のモバイルデバイスのDHCPログを確認しています。



モバイル管理者は、以下のどのモバイル構成設定を確認しているのでしょうか？
A. サービスセット識別子認証
B. 無線ネットワークへの自動接続
C. 相互認証付き802.1X
D. MACアドレスのランダム化
正解: **(**正解を表示します**)**
The DHCP logs show multiple distinct MAC addresses associated with the same user and device (UserA-MobileDevice). This behavior suggests that the device is using MAC address randomization, a feature designed to enhance privacy by generating a unique, temporary MAC address when connecting to wireless networks. The mobile administrator is verifying this setting to ensure that the mobile devices are properly randomizing their MAC addresses for added security.

質問: **33**
メールセキュリティソリューションのレビュー中に、セキュリティアナリストは以下の情報を収集します。

File	Sender	Action	Time stamp
Invoice.rar	(External) jdoe@comptia.org	Quarantine	10:00:00
Cchrome.exe	(Internal) johnd@corp.com	Quarantine	10:15:00
Invoice.docx	(External) jdoe@comptia.org	Allowed	10:20:00

メールゲートウェイにおけるメールセキュリティソリューションを改善するための最良の方法は、次のうちどれですか？
A. サンドボックスの展開
B. HIDSの実装
C. 許可リストを有効にする
D. シグネチャベースの検出の設定
正解: **(**正解を表示します**)**

質問: **34**
サイトAのSCADAコントローラに障害が発生した場合、エンジニアはサイトBからサイトAのポンプを制御できません。セキュリティアナリストは、同様の障害が再度発生した場合でも、サイトBのSCADAコントローラからサイトAのポンプを制御できる安全なソリューションを提供する必要があります。次のうち、最も費用対効果の高いソリューションはどれですか？
A. サイトAとサイトB間の直接ファイバー接続を取得し、その使用を重要なSCADAコントローラトラフィックのみに制限します。
B. 各サイトにバックアップ SCADA コントローラをインストールし、OT ネットワークから分離して、これらのバックアップ コントローラを高可用性ペアとして割り当てます。
C. エアギャップネットワークセグメントを用意することでOT環境を分離します。各サイトのSCADAコントローラーをこのネットワークセグメントに配置することで、システム停止を最小限に抑えます。
D. サイト A とサイト B の OT ネットワーク セグメント内に VPN コンセントレータを構成し、この暗号化されたトンネルを介してコントローラが他のサイトのポンプのセカンダリ デバイスとして機能できるようにします。
正解: **(**正解を表示します**)**
Configuring VPN concentrators inside the OT network segments allows secure, encrypted communication between Site A and Site B. This setup enables each SCADA controller to act as a backup for the other site's pumps during outages, while being cost-effective compared to dedicated fiber or deploying redundant controllers.

質問: **35**
セキュリティ担当者は、企業環境にサードパーティ製ソリューションを導入する前に、デューデリジェンスを実施します。セキュリティ担当者は、データ主体のアクセス要求に対応するプロセスが整備されていることをサードパーティから証明する必要があります。セキュリティ担当者がコンプライアンス維持のために最も求めているのは、次のうちどれでしょうか。
A. 情報セキュリティ基準
B. 電子情報開示の要件
C. プライバシー規制
D. 認定要件
E. レポートフレームワーク
正解: **(**正解を表示します**)**
Privacy regulations, such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), require companies to provide data subject access request (DSAR) handling processes. A DSAR allows individuals to request details about their personal data stored by a company and request modifications or deletions.

質問: **36**
ある企業は、APIリクエストに基づく新しいサーバーレスソリューションを導入した後、クラウド環境のコストが増加していることに気づきました。不明なIPアドレスからの無効なリクエストが多数、しかも短時間で多数発見されました。この問題を解決し、コストを削減し、セキュリティを向上させるには、次のうちどのソリューションが最も効果的でしょうか？
A. 既知の顧客に対してデジタル証明書を使用し、それらの証明書を通じてAPI認証を実行する
B. リクエストレート制限を定義し、未知のIPからの新しいリクエストを既知の悪意のあるIPのリストと比較する
C. APIリクエストの認証プロセスと通常の使用状況に応じた適切なレート制限の設定
D. 既知の顧客がいる地域からのAPIリクエストのみを許可する
正解: **(**正解を表示します**)**
Implementing authentication for API requests ensures only legitimate users can access the service, while setting rate limits helps prevent abuse and controls costs associated with excessive or malicious traffic. This directly addresses both the security and cost concerns.

質問: **37**
限られた予算で運営する場合に組織のリスク許容度を決定することの重要性を最もよく説明しているのは次のどれですか?
A. リスク選好度は、影響度が高く発生確率が低いイベントの受け入れに直接影響します。
B. 組織のリスク許容度は組織によって異なります
C. 予算上のプレッシャーがすべての企業でリスク軽減計画を推進する
D. リスク選好度は、どの侵害が公表されるかに直接影響します。
正解: **A (**コメントを発表する**)**
Risk appetite defines the level of risk an organization is willing to accept. When budgets are constrained, understanding this threshold is essential to prioritize resources and determine whether to accept, mitigate, or transfer high-impact, low-likelihood risks.

質問: **38**
同社の顧客サービスチームは、新たな脆弱性に関する顧客からの問い合わせを多数受けています。顧客サービスチームが顧客に直接伝えるための、一貫性のあるメッセージとしては、次のうちどれが適切でしょうか？
A. コミュニケーションプラン
B. 対応プレイブック
C. 災害復旧手順
D. 自動化されたランブック
正解: **(**正解を表示します**)**
A response playbook is a detailed document that outlines predefined steps, procedures, and templates for responding to specific incidents or situations. In this case, it would provide the customer service team with a consistent, clear, and accurate message to deliver to clients regarding the new vulnerability. The playbook would ensure that all team members are providing uniform responses to inquiries, reducing confusion and ensuring that the company's communication is coherent and accurate.

質問: **39**
セキュリティアナリストは、業界のベストプラクティスと確立されたフレームワークに準拠したシステムインフラストラクチャを設計する必要があります。アナリストはまず、次のうちどれを行うべきでしょうか？
A. 集中ログ層を確立する。
B. データラベル付けとデータ分類モデルを割り当てます。

C. 脆弱性管理プログラムを実施する。
D. セキュリティ管理のギャップ評価を実施する。
正解: **(**正解を表示します**)**
Performing a gap assessment identifies the differences between the organization's current security posture and the requirements defined in established frameworks and industry best practices. This evaluation provides a baseline understanding of which controls already exist, which are missing, and which require improvement. The results guide the prioritization and implementation of appropriate security measures to align the infrastructure with the selected frameworks.

質問: **40**
セキュリティアーキテクトがコードの一部を調査した結果、以下のことが判明しました。
char username[20]
char password[20]
ユーザー名を取得します
checkUserExists(username)
セキュリティアーキテクトは、コードのリリースを承認する前に、以下のどの変更を要求すべきでしょうか？
A. ユーザー名には英数字のみ使用可能です。
B. パスワード変数を長くして、より安全なパスワードをサポートします。
C. 20文字を超える入力を禁止します。
D. checkUserExists関数にパスワードパラメータを追加します。
正解: **(**正解を表示します**)**
The use of gets() allows an attacker to overflow the 20-byte username buffer by entering more data than it can hold. Enforcing a 20-character limit (for example, by switching to fgets(username, sizeof(username), stdin)) prevents buffer overruns and eliminates this class of vulnerability.

質問: **41**
組織は特殊なエンドポイントを管理したいと考えており、次のような機能を提供するソリューションを必要としています。
* 構成を集中管理
* ポリシーをプッシュします。
* デバイスをリモートワイプする
* 資産インベントリを管理する
これらの要件を最もよく満たすために、組織は次のどれを行う必要がありますか?
A. 構成管理データベースを使用する
B. モバイル デバイス管理ソリューションを実装します。
C. コンテキストポリシー管理を構成する
D. ソフトウェア資産管理ツールを導入する
正解: **(**正解を表示します**)**
To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.
MDM Capabilities:
Central Management: MDM allows administrators to manage the configurations of all devices from a central console.
Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.
Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.

Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.
Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.

質問: **42**
ある企業は、顧客契約において、アプリケーションの脆弱性を特定するために外部監査を受ける必要があるという要件を設けています。外部監査人を雇う前に、企業が行うべき最善の行動は次のうちどれでしょうか？
A. 監査のための証拠を集める。
B. 内部監査評価を実施する。
C. 監査から得られた教訓を特定する。
D. 監査テスト用のサンプルを選択します。
正解: **B (**コメントを発表する**)**
Conducting an internal audit assessment before hiring an external auditor allows the company to identify any potential vulnerabilities or gaps internally. This ensures that the organization is well-prepared for the external audit and can address issues proactively.

質問: **43**
A社とD社は合併します。A社のコンプライアンスレポートによると、支店保護が実施されていません。セキュリティアナリストは、ソフトウェア開発ライフサイクルに対する潜在的な脅威が対処されていることを確認する必要があります。この基本的な作業を完了する際に、アナリストは次のうちどれを考慮すべきでしょうか？
A. 開発者が本番環境に昇格できない場合
B. DASTコードが単一のコードリポジトリに保存されている場合
C. DASTスキャンが定期的に実施される場合
D. 役割ベースのトレーニングが実施されている場合
正解: **(**正解を表示します**)**
The analyst is tasked with addressing potential threats to the software development life cycle (SDLC) after identifying that branch protections are not in place in Company A's compliance reports. Branch protections are critical for secure code management, preventing unauthorized or risky changes (e.g., direct pushes to main, unreviewed merges).
Branch protections typically enforce peer review, code scanning, and other gates before code reaches production.
If developers cannot promote to production directly, it ensures there's a proper approval or CI/CD pipeline in place-a fundamental control to prevent insecure or unauthorized code changes.
This aligns exactly with the compliance finding and the need to secure the SDLC.

質問: **44**
ある組織が新しいソフトウェアの導入を計画しています。プロジェクトマネージャーは、導入ライフサイクルの様々なフェーズに関与する役割のリストを作成します。プロジェクトマネージャーは、これらの役割を追跡するために、以下のどれを使用すべきでしょうか？
A. CMDB
B. リコールツリー
C. ITIL
D. RACIマトリックス
正解: **(**正解を表示します**)**
A RACI matrix is used to define and track roles and responsibilities in a project by identifying who is Responsible, Accountable, Consulted, and Informed for each task or phase.
It's the best tool for the project manager to manage role assignments throughout the deployment life cycle.

質問: **45**
アナリストは、企業への攻撃を成功させるための複数の解決策を用意しました。これらの解決策は、ダウンタイムを最小限に抑えて実行する必要があります。アナリストは次のうちどれを実行すべきでしょうか？
A. 仮想ラボにすべてのソリューションを一度に実装し、攻撃シミュレーションを実行します。メトリクスを収集し、それに基づいて最適なソリューションを選択します。
B. 仮想ラボで各ソリューションを1つずつ実装し、その都度メトリック収集を実行します。収集後、攻撃シミュレーションを実行し、各ソリューションをロールバックしてから次のソリューションを実装します。最適なメトリックに基づいて最適なソリューションを選択します。
C. 仮想ラボで各ソリューションを1つずつ実装し、攻撃シミュレーションを毎回実行しながらメトリクスを収集します。各ソリューションをロールバックしてから、次のソリューションを実装します。最適なメトリクスに基づいて、最適なソリューションを選択します。
D. すべてのソリューションを仮想ラボに一度に実装し、メトリクスを収集します。収集後、攻撃シミュレーションを実行します。最適なメトリクスに基づいて、最適なソリューションを選択します。
正解: **(**正解を表示します**)**
To minimize downtime, testing should occur in a virtual lab, not production. The best approach is to test solutions methodically: implement one solution at a time, run an attack simulation, collect metrics, roll back, and repeat. This isolates each solution's effectiveness, ensuring accurate metrics for decision-making without production impact.

質問: **46**
リアルタイムの財務処理を行う組織が、新しいバックアップソリューションを導入しようとしています。次のようなビジネス要件があります。
バックアップ ソリューションは、バックアップが侵害される可能性のリスクを軽減する必要があります。
バックアップ ソリューションは、ランサムウェア攻撃に対して耐性がなければなりません。
バックアップからの復元にかかる時間は、バックアップ データの整合性よりも重要ではありません。
運用データの複数のコピーを維持する必要があります。
次のバックアップ戦略のうち、これらの要件を最もよく満たすものはどれですか?
A. セカンダリの不変データベースを作成し、ライブデータを継続的に追加する
B. 2つの接続されたストレージアレイを活用し、アレイが常に同期されるようにする
C. データベース上でリモートジャーナリングを有効にして、リアルタイムトランザクションがミラーリングされるようにする
D. データベースに改ざん防止機能を設定し、データが意図せず変更されないようにする
正解: **(**正解を表示します**)**
Creating a secondary, immutable database and adding live data continuously best meets the requirements because immutability ensures backup data cannot be altered or compromised, including during ransomware attacks. This approach preserves data integrity and maintains multiple copies, aligning with the priority on data integrity over restore speed.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
ソフトウェアエンジニアは、Webアプリケーションの開発をサポートするCI / CDパイプラインを作成しています。DevSecOpsチームは構文エラーを特定する必要があります。次のうち、DevSecOpsチームのタスクに最も関連するものはどれですか？
A. 静的アプリケーションセキュリティテスト

B. ソフトウェア構成分析
C. ランタイムアプリケーションの自己保護
D. Webアプリケーションの脆弱性スキャン
正解: **(**正解を表示します**)**
Static Application Security Testing (SAST) analyzes source code, bytecode, or binaries without executing the program, making it highly relevant for identifying syntax errors during the development process. This approach is ideal for the DevSecOps team's task of identifying errors before deployment.

質問: **48**
セキュリティアーキテクトは、以下のようなデータフィールドへの入力によるセキュリティ上の影響を防ぎたいと考えています。
'AND 1=1#
この目的を達成するのに最適な方法は次のうちどれですか？
A. API
B. コーディング基準
C. Base64エンコード
D. サンドボックス
正解: **(**正解を表示します**)**
The root of SQL injection (e.g., ' AND 1=1#) is unsafe string concatenation in application code. A robust secure-coding standard mandates parameterized queries (or stored procedures), strict input validation/whitelisting, and escaping of any user-supplied data. By embedding these practices into your development guidelines and enforcing them through code reviews and automated scans, you eliminate SQL injection and similar input-based attacks at the source.

質問: **49**
ある企業は、業界標準に準拠するために、クラウド環境のコンプライアンスを向上 ·自動化したいと考えています。この目標を達成するために、企業は以下のどのリソースを活用すべきでしょうか？
A. ジェンキンス
B. パイソン
C. アンシブル
D. PowerShell
正解: **(**正解を表示します**)**
Automating compliance in cloud environments requires a tool that can enforce configurations, manage infrastructure as code, and align with industry standards (e.g., NIST, ISO).

質問: **50**
過去に傍受された通信は、現在の暗号鍵が将来侵害された場合でも、安全に維持されなければなりません。この要件を最もよく満たすのは次のどれですか。
A. トークン化
B. キーストレッチ
C. 前方秘匿性
D. 同等の同時認証
正解: **(**正解を表示します**)**
Forward secrecy (FS) ensures that past encrypted data remains secure even if encryption keys are compromised in the future. It generates ephemeral session keys that are not reused.

質問: **51**
ベンダーロックインに伴うリスクとして、次のうちどれが該当しますか？(2つ選択してください。)
A. クライアントはデータをシームレスに移行できます。
B. ベンダーは製品提供内容を変更する場合があります。
C. 顧客は十分なレベルのサービスを受けている。
D. 顧客はサービスの質の低下を実感する。
E. クライアントはマルチクラウドのアプローチを活用できます。
F. クライアントは相互運用性の向上を実感します。
正解: **(**正解を表示します**)**
Vendor lock-in occurs when a client is overly dependent on a vendor, limiting flexibility. Risks include:
Option B: Vendors changing offerings (e.g., features, pricing) can disrupt the client, a key lock-in risk.
Option D: Decreased quality of service may result from reliance on a single vendor without alternatives.

質問: **52**
セキュリティ アナリストは、特定のユーザーが会社のリソースにアクセスできない理由をトラブルシューティングしています。アナリストは次の情報を確認します。

User	Source IP	Source location	User assigned location	MFA satisfied?	Sign-in status
SALES1	8.11.4.16	Germany	France	Yes	Blocked
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	192.168.4.18	France	France	No	Allowed
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	8.11.4.16	Germany	France	Yes	Blocked
SALES2	8.11.4.20	France	France	Yes	Allowed

jpexshiken.com CompTIA
問題の原因として最も可能性が高いのは次のどれですか?
A. ローカル ネットワーク アクセスは、MFA 要件をバイパスするように構成されています。
B. ネットワークの位置情報の識別が認証サーバーによって誤認されています
C. 別の場所からの管理者アクセスは会社のポリシーによってブロックされています
D. 一部のユーザーはモバイルデバイスでOTPコードを受信できるように設定していません
正解: **(**正解を表示します**)**
The SALES1 user is consistently being blocked despite satisfying MFA requirements, and the source IP is in Germany while the user assigned location is France. This indicates that the authentication server might be misidentifying the network geolocation or incorrectly associating the IP address with a different location, leading to the blockage of access.

質問: **53**
SOCアナリストは、侵入テスト担当者がペイロードの作成と実行に成功した事象を調査している。アナリストは、影響を受けたサーバーから以下のコマンド履歴を取得した。
$ uname -a && env
$ vim foo.c
$ gcc foo.c /tmp/lockfile
$ chmod +x /tmp/lockfile

$ ./tmp/lockfile
サーバーのセキュリティを向上させるために、アナリストは以下のうちどれを実施すべきでしょうか？
A. カーネルがサポートするASLR制御
B. 許可リストによるアプリケーション制御
C. グローバル書き込み可能なフォルダに関するOSの制限
D. 特定のプロセスを終了させるEDRシグネチャ
正解: (正解を表示します)
The command history shows that the attacker created a source file, compiled it into an executable using the system compiler, placed it in a temporary directory, made it executable, and ran it. This indicates the system allows arbitrary compilation and execution of binaries. Implementing application allow-listing would restrict execution to only approved binaries and scripts, preventing unauthorized compiled payloads from running even if an attacker manages to create them on the system.

質問: **54**
最高情報セキュリティ責任者は、組織のベースラインワークロードが展開前に標準化されていることを確認し、変更があった場合は直ちに承認済みの構成に戻す必要があります。これらの目標達成を支援する最善の方法は次のうちどれですか？
(2つ選択してください。)
A. CNAPP
B. SIEM
C. IaC
D. PowerShellスクリプト
E. 自動パッチ適用
F. コードアシスト
正解: (正解を表示します)
A cloud-native application protection platform continuously monitors cloud workloads and configurations to detect drift from approved baselines and automatically enforce security policies across environments. This helps ensure workloads remain aligned with the approved configuration after deployment.
Infrastructure as code defines infrastructure and workload configurations through version- controlled templates, enabling standardized environments to be deployed consistently. If configuration drift occurs, the defined templates can be reapplied to immediately restore systems to the approved baseline configuration.

質問: **55**
セキュリティアーキテクトは、標的型攻撃と思われる攻撃によって公共の場で従業員の携帯電話が盗まれた事例を調査しています。デバイスはメールや社内文書などの社内リソースにアクセスでき、その一部はアプリケーションストレージに保存される可能性があります。情報漏洩から会社を守るのに最適な方法は次のうちどれですか (2つ選択してください)。
A. 一定期間電話がチェックインしない場合はリモートワイプ手順を実装します
B. 設定されたタイムアウトで生体認証アクセス制御を強制する
C. 携帯電話がオフィスの近くにある必要がある企業アプリケーション用にジオフェンシングを設定します
D. MDMソリューションを活用してモバイルアプリケーションのサイドローディングを防止する
E. 会社のリソースへのアクセスに使用するデバイス証明書を有効にします
F. アプリケーション制御を使用して、インストールできるアプリケーションを制限します
正解: (正解を表示します)

質問: **56**

セキュリティ担当者は、夜間にMFAプッシュ通知が過剰に届くというユーザーからの苦情を複数受けました。セキュリティチームは調査を行い、ユーザーアカウント認証に関する悪意のある活動が疑われると判断しました。セキュリティ担当者がMFA通知を制限するための最適な方法は次のうちどれでしょうか？
A. FID02デバイスのプロビジョニング
B. MFAに基づくテキストメッセージの展開
C. メールによるOTPの有効化
D. プロンプト駆動型MFAの設定
正解: **D** (コメントを発表する)
Prompt-driven MFA means that MFA prompts are triggered only when there is suspicious activity or a specific need for authentication, rather than being sent regularly. This approach would reduce the excessive notifications while still ensuring security, addressing the user's complaints effectively.

質問: **57**
以下のAIに関する懸念事項のうち、入力データのサニタイズによって最も適切に対処できるのはどれですか？
A. モデル反転
B. 即時注射
C. データポイズニング
D. 説明不可能なモデル
正解: **B** (コメントを発表する)
Prompt injection occurs when attackers manipulate input to alter the behavior of an AI model.
Input sanitization helps prevent this by filtering or validating user input, ensuring that malicious commands or instructions don't reach or influence the model's processing logic.

質問: **58**
監査結果によると、いくつかのユーザーエンドポイントはフルディスク暗号化を使用していません。修復プロセス中に、コンプライアンスアナリストはエンドポイントのテストの詳細を確認し、エンドポイントデバイスの構成がフルディスク暗号化をサポートしていないことに気付きました。デバイスを交換する必要がある最も可能性の高い理由は次のうちどれですか？
A. HSM は古くなっており、メーカーによるサポートは終了しています
B. vTPM が正しく初期化されていないため、破損しています。
C. HSMは一般的な脆弱性に対して脆弱であり、ファームウェアのアップグレードが必要です
D. マザーボードは OEM サプライヤーの TPM で構成されていません。
E. HSMはシーリングストレージをサポートしていません
正解: (正解を表示します)
The most likely reason the endpoint cannot utilize full disk encryption is that the device lacks a TPM (Trusted Platform Module), which is often required for full disk encryption solutions. Many modern encryption technologies rely on the TPM to securely store encryption keys. If the motherboard was not configured with a TPM by the original equipment manufacturer (OEM), the device would not support full disk encryption and would need to be replaced or upgraded to a compatible device.

質問: **59**
セキュリティエンジニアは、組織のバグ報奨金プログラムを通じて、カスタムアプリケーションの特定コンポーネントにおけるリモートコード実行に関する報告を受け取りました。経営陣は、当該コンポーネントを適切に保護し、同様の問題の発生を未然に防ぎたいと考えています。アプリケーション内のその他の脆弱な箇所を発見するための最適なアプローチは、次のうちどれでしょうか？
A. 脆弱性を発見するために、エクスプロイトフレームワークを活用する。
B. ファジングテストを使用して、アプリケーションの潜在的な脆弱性を発見します。

C. ソフトウェア構成分析ツールを使用して、既知の脆弱性を報告する。
D. アプリケーションをリバースエンジニアリングして、脆弱なコードパスを探します。
E. HTTPインターセプトプロキシの使用を分析して、問題を動的に明らかにします。
正解: **(**正解を表示します**)**
Fuzz testing is a technique used to identify vulnerabilities by inputting a large volume of random, unexpected, or malformed data into the application. It helps uncover vulnerabilities like buffer overflows, input validation issues, and other security flaws that may not be immediately apparent.
By systematically testing different inputs and paths in the application, fuzz testing can identify previously undiscovered vulnerabilities and help secure the component against potential exploits.

質問: **60**
セキュリティアーキテクトが、検出機能をサポートするために、組織のクラウド本番環境にSOARソリューションを導入しています。次のうち、最も可能性の高いメリットはどれでしょうか？
A. セキュリティオペレーションセンターのパフォーマンス向上
B. ファイアウォールログの自動収集タスク
C. クラウド資源の利用効率を最適化
D. リスクの可視性の向上
正解: **A (**コメントを発表する**)**
A SOAR platform streamlines and automates repetitive detection and response workflows, like alert triage, enrichment, and ticketing, freeing up analysts to focus on high-value tasks. This orchestration capability reduces mean time to acknowledge and respond, directly boosting overall SOC efficiency and performance.

質問: **61**
規制対象企業がインフラ全体の刷新を進めている。同社は、業務上重要なプロセスを古い2008年版Windowsサーバー上で稼働させている。このサーバーが故障した場合、同社は数百万ドルの収益を失うことになる。同社は次のうちどの対策を講じるべきか？
A. リスクは事業を行う上でのコストとして受け入れる。
B. プロジェクトの優先順位付けのために、組織的なリスク登録簿を作成する。
C. ネットワーク補償制御を実装する。
D. 故障が発生した場合の費用を補償するために保険に加入する。
正解: **(**正解を表示します**)**
The most appropriate action is to create an organizational risk register for project prioritization. This helps the company document and assess risks, prioritize critical systems, and determine which systems, such as the old 2008 Windows server running a business-critical process, need to be addressed most urgently. A risk register ensures that resources are allocated properly and that mitigation plans are in place for the most critical systems to prevent revenue loss in the event of a failure.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**

保護対象の企業データが最近流出しました。SOCはネットワーク侵入や外部からの物理的な侵入の兆候を一切発見できず、DLPシステムも異常なアクティビティを報告していません。インシデント対応チームはテキストファイルが暗号化されていることを確認し、以下の内容を調査しています。

```
Delivered-To: janedoe@email.net
MessageID: <sdflkh038-kdhen7-23hd7s-afdzx.xt.local>
Created at: Sat, Jan 20, 2024 at 10:50 PM (Delivered after 10 seconds)
From: Jane Doe <janedoe@company.com>
To: janedoe@email.net
Subject: Grocery List for Next Week's Meal Prep
SPF: PASS with IP 12.34.56.78
DKIM: 'PASS' with domain email.company.com
DMARC: 'PASS'

Body:
Make sure not to forget any of the items.
Regards,
Jane Doe Engineer @ Company

Attachments: groceryitem.txt
Attachment Virus Scan: 'PASS'
```

jpnshiken.com
CompTIA

チームが取るべき最も適切な行動は次のうちどれですか？

A. メールのセキュリティ設定を確認し、適切な設定になっているか確認してください。

B. 従業員が漏洩したデータにアクセスできたかどうかを調査する。

C. 添付ファイルをサードパーティ製のウイルススキャンソフトでスキャンし、結果を独自に確認してください。

D. ハードウェアを分析し、悪用された可能性のある、検出されていないサプライチェーンの脆弱性を特定する。

正解: **(**正解を表示します**)**

Since the exfiltration occurred via an encrypted text file sent by an internal account and no external intrusion or DLP alerts were found, the most appropriate next step is to investigate whether the employee legitimately had access to the leaked data. This helps determine if it was an insider threat or misuse of authorized access.

質問: **63**

ある企業は、脆弱性を迅速に修正し、本番環境へデプロイするために、マイクロサービスアーキテクチャを採用しています。すべてのマイクロサービスは同じLinuxプラットフォーム上で実行されています。コードをデプロイする前に、ベースOSのアップデートにかなりの時間を費やしていました。このプロセスを効率化するために、企業は以下のどれを実施すべきでしょうか？

A. ゴールデンイメージを作成するときに Terraform スクリプトを使用する

B. 30 日ごとに apt-update を実行する cron ジョブを作成します。

C. スナップショットを使用して、既存のコンピューティング インスタンスにコードをデプロイします。

D. 集中更新サーバーを展開します。

正解: **(**正解を表示します**)**

Creating golden images with Terraform enables automated, consistent, and up-to-date deployment of microservices with a pre-patched base OS. This significantly reduces time spent on manual updates and accelerates production deployment in a microservices environment.

質問: **64**

セキュリティ エンジニアが ECC を格子ベースの暗号化技術に置き換えた理由として最も適切なのは次のどれですか。

A. 計算効率が高く、完全な前方秘匿性を提供します。

B. ECC よりもブルートフォース攻撃に対して耐性があります。
C. 一時的なキー交換とデジタル署名をサポートします。
D. 現在、堅牢な PQC 手法と考えられています。
E. 暗号化された状態のままデータの処理を可能にします。
正解: **(**正解を表示します**)**
Lattice-based schemes, such as Learning With Errors (LWE) or Ring-LWE, are among the leading candidates in NIST's post-quantum cryptography standardization process because their underlying hard problems resist known quantum-algorithm speedups. Replacing ECC with a lattice-based algorithm directly addresses the threat posed by future quantum computers, making it the preferred choice for long-term cryptographic agility.

質問: **65**
あるソフトウェア開発者が、新しいソフトウェアパッケージに必要なコードを作成しています。このコードは、リモートIDの有効性を検証するためのプロトコルを使用する必要があります。開発者は、コードに次のうちどれを実装すべきでしょうか？
A. RSA
B. OCSP
C. HSTS
D. CRL
正解: **B (**コメントを発表する**)**
The Online Certificate Status Protocol (OCSP) lets your application query a trusted responder in real time to confirm that a peer's X.509 certificate hasn't been revoked. Embedding OCSP checking in your TLS/SSL handshake ensures the remote identity you connect to remains valid without needing to download and parse full CRLs.

質問: **66**
病院が空調システムを遠隔で第三者に監視させる場合の要件は以下のとおりです。
- ベンダーはシステムの状態を継続的に監視できなければならず、
それに応じて対応してください。
- ベンダーは、HVACシステムへのネットワークアクセスのみを持つ必要があります。
- HVACシステムにアクセスできるのは、ベンダーのみでなければなりません。
以下のうち、病院の要件を最も満たしているのはどれですか？
A. リモートシステム監視を可能にするためのRDPジャンプボックスの導入
B. リバースWebプロキシを実装し、インターネットからのアクセスを許可する
C. ベンダーの監視アプライアンスを内部ネットワークにインストールし、外部へのSSL接続を許可する。
D. サイト間VPNトンネルを作成し、システムへの制限付きアクセスを許可する
正解: **(**正解を表示します**)**

質問: **67**
ある企業は、社内で開発されたビジネスクリティカルなアプリケーションの脅威モデリングを実施したいと考えています。最高情報セキュリティ責任者（CISO）は、アプリケーションの可用性が99.999%を維持し、承認されたユーザーが明示的に閲覧を許可されたデータにのみアクセスできることを最も懸念しています。以下の脅威モデリングフレームワークのうち、このシステムに関するCISOの懸念に直接対応するものはどれですか？
A. CAPEC
B. STRIDE
C. ATT&CK

D. TAXII
正解: **B (**コメントを発表する**)**
STRIDE is a threat-modeling framework that focuses on six key threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
This directly addresses the CISO's concerns about ensuring high availability (99.999%) and restricting data access to only authorized users, making it the most suitable choice.

質問: **68**
あるグローバル製造企業は、製品製造に不可欠な社内アプリケーションを保有している。
このアプリケーションは更新できず、本番環境で利用可能である必要があります。セキュリティアーキテクトがアプリケーションのセキュリティを実装しています。アーキテクトが取るべき行動として最も適切なのは次のうちどれですか？
A. アプリケーションへの無線アクセスを禁止します。
B. ネットワークタップを使用して侵入検知機能を展開する
C. アプリケーションの使用に関する許容使用ポリシーを作成する
D. アプリケーションへのアクセスが必要なユーザー向けに、別のネットワークを作成する
正解: **(**正解を表示します**)**
Placing the application and its users on a separate, segmented network limits exposure and reduces the risk of compromise, especially since the application cannot be updated. This approach ensures availability while applying strong network-level security controls.

質問: **69**
セキュリティエンジニアが、サーバークラッシュ後にSIEMログを確認しています。以下のイベントリストは、SIEMから収集されたアクションの時系列を表しています。

```
(1:30:01:231) System : PID: 334 - Explorer.exe
(1:30:03:523) System : PID: 1231 - Mssbuild.exe as child from 334
(1:33:12:312) System : PID: 3324 - Powershell.exe as child from 1231
(1:34:34:864) System : PID: 4554 - LSSASS.exe as child from 3324
(1:35:56:131) System : PID: 7662 - LSSASS.exe - SAM access from 3324
```

このSIEMログに最も関連している可能性が高いのは、次のうちどのTTP(戦術、技術、手順)でしょうか？
A. 横方向の動き
B. 認証情報のダンプ
C. データ漏洩
D. LOLBins 使用
正解: **(**正解を表示します**)**
The logs show processes associated with credential dumping, specifically LSASS.exe access, which is commonly targeted to extract stored credentials from memory for later use by attackers.

質問: **70**
セキュリティチームは、特定の社内リソースにアクセスできないユーザーに関するエスカレーションされたサポートチケットを受け取ります。社内には以下の構成が存在します。
- デバイス証明書は、すべての企業資産に展開されています。
- 固有のユーザー証明書のテンプレートが設定されています。
セキュリティアップデートは30日ごとにインストールされます。

管理者権限は特定のホストに紐づいています。
チケットには以下の所見が記載されています。
・当該ユーザーは90日以上休職中です。
内部脆弱性スキャンでは、デバイスに問題は検出されませんでした。
シングルサインオンは期待どおりに動作します。
特権システムにはアクセスできません。
以下のうち、根本原因を最もよく表しているのはどれですか？
A. ユーザーの管理者認証情報が90日後に期限切れになった可能性があります。
B. テンプレートに誤った証明書拡張子が追加されました。
C. ユーザーが休暇中だったため、パッチ適用サイクルが複数回スキップされました。
D. 使用されているデバイスには、ユーザーバインディングが設定されていません。
正解: **(**正解を表示します**)**

質問: **71**
ある組織は、従業員がテンプレート開発、編集、調査、スケジュール管理などの一般的なタスクを完了できるよう支援する、AI搭載のデジタルワーカーを開発しています。AIワークロードの一環として、組織はプラットフォーム内にガードレールを実装したいと考えています。AI環境を保護するために、同社は次のうちどれを行うべきでしょうか？
A. プラットフォームの機能を機密性の低い機能のみに制限する
B. トレーニングモデルの有効性を向上させる。
C. システムに自己統治能力を与える
D. エンドユーザーに組織の方針を承認してもらうことを要求する。
正解: **(**正解を表示します**)**
Limiting the platform's abilities to only non-sensitive functions is the best way to secure the AI environment. By restricting the AI's scope to tasks that do not involve sensitive or critical information, the company can mitigate the risk of accidental data exposure or misuse while still allowing the AI to assist employees in non-sensitive activities. This approach helps implement guardrails that align with security best practices.

質問: **72**
最近のコンプライアンス監査で明らかになった重要な調査結果によると、ある企業には過剰な権限設定の問題があることが判明しました。従業員が役割や部署を変更すると、権限が徐々に拡大していくことが原因です。この問題を軽減するための最善策は、次のうちどれでしょうか？
(2つ選択してください。)
A. 業務領域ごとに定義された異なるアクセス制御を設定する
B. 役割ベースのアクセス ポリシーの実装
C. 必要最小限の特権ポリシーの設計
D. 義務的な休暇制度の導入
E. 定期的なアクセスレビューの実施
F. 定期的な職務交代が必要
正解: **B,E (**コメントを発表する**)**
Role-based access control (RBAC) ensures that permissions are tied to job roles rather than individuals, making it easier to update or change access when someone switches roles.
Periodic access reviews help detect and correct excessive permissions by regularly reviewing who has access to what and removing any unnecessary privileges.

質問: **73**
セキュリティエンジニアが、ドメイン間のデータと通信をセグメント化する新しいツールを評価しています。この評価では、データ伝送制御を検出されずに回避する方法を特定する必要があります。セキュリティエンジニアは、次のうちどの手法を使用すべきでしょうか？
A. 機械学習統計分析
B. ファジングテスト
C. 隠蔽チャネル分析
D. プロトコル分析
正解: **C (**コメントを発表する**)**
Covert channel analysis is the technique best suited for assessing how data transmission controls can be bypassed without detection. Covert channels involve using a system or communication protocol in unintended ways to transmit data secretly. This analysis helps identify potential hidden channels that might bypass security controls and allow unauthorized communication between domains.

質問: **74**
ある組織は、新たなソーシャルエンジニアリング攻撃やフィッシング攻撃への対策トレーニングに注力しています。この組織が最も懸念しているのは、次のうちどれですか？
A. 既存の規制コンプライアンスを満たす
B. AIサポートボットへの過度の依存
C. エクスプロイトの品質を向上させる生成AIツール
D. AIモデルを用いた差分分析
正解: **C (**コメントを発表する**)**
The organization is concerned that generative AI tools can increase the quality and sophistication of phishing and social engineering attacks, making them harder to detect and more convincing to victims.

質問: **75**
ある企業のヘルプデスクには、財務部門からwww.bank.comへのアクセスに関する問題に関する問い合わせが多数寄せられている。セキュリティオペレーションセンターは、以下のセキュリティログを確認した。

User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.138/24	Legal	www.bank.com	98.17.62.78	200

以下のうち、問題の原因として最も可能性が高いのはどれですか？
A. 再帰DNS解決が失敗しています
B. DNSレコードが改ざんされています。
C. DNSトラフィックがシンクホールされています。
D. DNSの設定が間違っています。
正解: **(**正解を表示します**)**
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination.
This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.

In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.

質問: **76**
ある企業は最近、新しいアプリケーションをサポートするために、追加のクラスタを構築するために新しいサーバーを導入しました。企業のセキュリティポリシーでは、すべての新しいサーバーは耐障害性を備えている必要があると規定されています。新しいクラスタは、スムーズなフェイルオーバーを実現するために高可用性構成になっています。最近の停電後、フェイルオーバーは成功しましたが、両方のクラスタで重要なデータが失われ、復旧時間に影響が出ました。
将来停電が発生した際に遅延を最小限に抑えるために、以下のうちどれを設定する必要がありますか？
A. 複製
B. キャッシング
C. コンテナ化
D. 冗長性
E. 高可用性
正解: **A** (コメントを発表する)
Replication ensures data consistency by synchronizing copies of data across clusters. This would prevent data loss during power outages.
Caching provides faster data retrieval but does not ensure data persistence. Containerization improves deployment consistency but does not address resilience or data integrity.
Redundancy relates to additional hardware or systems but does not guarantee up-to-date data. High availability addresses system uptime but does not prevent data loss.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu　**604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
サイバーセキュリティアーキテクトは、脆弱性管理を改善し、多数の脆弱性チェックをオーケストレーションすることを目指しています。主な制約事項は以下のとおりです。
- コンテナ化されたマイクロサービスは512個あります
脆弱性データは複数のスキャナーから取得されます。
- CISの基準値は遵守されなければならない
スキャン作業はスケジュール設定が必要です。
以下の自動化ワークフローのうち、この目的に最も適しているのはどれですか？
A. エンドポイントデータ収集システムの採用
B. XCCDFスキャナの展開
C. SOCアナリストによるCVSSレポートの活用
D. リポジトリスキャナを使用してIaCセキュリティを強制する
正解: (正解を表示します)
XCCDF (Extensible Configuration Checklist Description Format) is part of the SCAP framework and is designed to automate security configuration checks and enforce security baselines such as CIS benchmarks. It enables standardized vulnerability and compliance scanning, supports scheduling of scans, and allows orchestration of large numbers of configuration checks across systems. This makes it well suited for enforcing CIS baselines and automating vulnerability assessments across many containerized services.

質問: **78**
ある組織は、すべてのインスタンスにわたって安全なクラウドアーキテクチャを実装したいと考えています。以下の要件が与えられています。
標準的なネットワークテンプレートを確立する。
導入は一貫性のあるものでなければならない。
セキュリティポリシーは、大規模に変更できるものでなければならない。
以下の技術のうち、これらの要件を満たすものはどれですか？
A. サーバーレス展開モデル
B. コンテナオーケストレーション
C. コードとしてのインフラストラクチャ
D. CLIクラウド管理
E. APIゲートウェイ
正解: **C (**コメントを発表する**)**
Infrastructure as code defines cloud infrastructure, network configurations, and security policies in version-controlled configuration files that can be deployed automatically. This approach allows organizations to create standardized templates for networks, ensure consistent deployments across environments, and update security policies centrally so changes can be applied at scale to all instances.

質問: **79**
ソフトウェア開発ライフサイクルにおけるセキュリティ監査の一環として、プロダクトマネージャーは、ビルド前に本番環境にデプロイされるアプリケーション内で使用されるコードとモジュールの完全な表現を実証し、その証拠を提供する必要があります。必要な証拠として最も適切なものはどれですか？
A. ソフトウェア構成分析
B. ランタイムアプリケーション検査
C. 静的アプリケーションセキュリティテスト
D. 対話型アプリケーションセキュリティテスト
正解: **A (**コメントを発表する**)**
Software composition analysis identifies and inventories all open-source and third-party components included in an application and produces a detailed software bill of materials. This provides a complete representation of the code libraries and modules used in the application before the build process. The generated inventory serves as evidence during audits that the organization has visibility into the components included in the production-deployed application.

質問: **80**
アーキテクトは、外部サービスをサポートするために外部インフラストラクチャを確保しています。以下のコンポーネントが使用されています。
- バックエンド用に複数のポッドとノードを備えた1つのKubernetesクラスタ
サービス
- Web層として2つのVM Linuxインスタンスを使用
- SQLベースのデータベース1つ
同社は2つの対策にしか資金を割けず、レジリエンス(回復力)を最優先事項としなければならない。この目標を達成するために同社が実施すべき最も効果的な対策は次のうちどれか？(2つ選択してください。)
A. IAMポリシーが適用されます
B. ワークロードサービスへのRASP
C. コンテンツ配信ネットワーク

D. SQLインスタンス上のデータベースファイアウォール
E. Web層におけるIPS
F. アプリケーションロードバランサー
正解: **C,F** (コメントを発表する)
A content delivery network improves resilience by distributing incoming traffic across globally distributed edge nodes, absorbing traffic spikes and helping mitigate denial-of-service conditions before requests reach the infrastructure. This protects the web tier and backend services from overload and improves availability for external users.
An application load balancer distributes incoming requests across the two web-tier virtual machines and backend services, preventing a single instance from becoming a point of failure.
Load balancing enables high availability and fault tolerance by automatically directing traffic to healthy instances if one becomes unavailable.

質問: **81**
サイバーセキュリティアーキテクトは、最近複数の企業を買収したグローバル企業の検知 ·監視機能をレビューしています。アーキテクトは、買収した企業が検知と監視に異なるベンダーを利用していることを発見しました。アーキテクトの目標は以下のとおりです。
* 既知の脅威の検出に役立つユースケースのコレクションを作成する
* これらのユースケースを一元化されたライブラリに含めて、すべての企業で使用できるようにする 次のうちどれが、この目標を達成するための最良の方法でしょうか?
A. シグマルール
B. Arielクエリ言語
C. UBAルールとユースケース
D. TAXII/STIXライブラリ
正解: **A** (コメントを発表する)
To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option.
Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.
Centralized Rule Management: By using Sigma rules, the cybersecurity architect can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.
Ease of Use and Flexibility: Sigma provides a structured and straightforward format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

質問: **82**
コンテナを使用してアプリケーションを実行する企業は、プライベートリポジトリ内のすべてのコンテナイメージの脆弱性を特定する必要があります。セキュリティチームは、特定の脆弱性に対して対応すべきかどうかを迅速に評価できる必要があります。以下のうち、セキュリティチームが最小限の労力で目的を達成できるのはどれでしょうか？
A. SASTスキャンレポート
B. 中央集権型SBoM
C. CISベンチマーク準拠レポート
D. 認証済み脆弱性スキャン
正解: (正解を表示します)
A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in a private repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities.
Why Centralized SBoM?

Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.
Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.
Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.
Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.

質問: **83**
量子コンピューティングの進歩により、企業や国が新しい暗号化アルゴリズムを導入する主な理由はどれですか?
A. 大きな素数に基づく暗号化システムは、悪用される可能性が高くなります。
B. ゼロトラスト セキュリティ アーキテクチャでは、準同型暗号化が必要になります。
C. 完全な前方秘匿性により、高度なファイアウォール監視技術の導入が妨げられる
D. 量子コンピュータは悪意のある人物がIPトラフィックをリアルタイムでキャプチャすることを可能にする
正解: **(**正解を表示します**)**
Quantum computing threatens traditional encryption methods, especially those based on large prime number factorization (e.g., RSA), because quantum algorithms like Shor's algorithm can break them efficiently. This drives the need for post-quantum cryptography.

質問: **84**
ある企業は、自社のVPNソリューションにゼロデイ脆弱性を発見したため、既存のオンプレミスシステムをクラウドホスト型リソースに置き換える計画を立てています。エンジニアは、信頼性の高い接続を実現するための適切なソリューションを見つける必要があります。次の機能のうち、最も関連性の高いものはどれですか？
A. コンテナオーケストレーション
B. マイクロセグメンテーション
C. 条件付きアクセス
D. セキュアアクセスサービスエッジ
正解: **(**正解を表示します**)**
SASE combines network security (e.g., SWG, CASB, ZTNA, FWaaS) with WAN capabilities (SD- WAN) into a single cloud-delivered service. It is designed to provide secure and optimized access to cloud resources, replacing traditional VPNs with Zero Trust principles. This directly addresses the need for trusted connectivity while mitigating risks like VPN vulnerabilities.

質問: **85**
セキュリティエンジニアは、次の要件を満たすソリューションを開発していますか?
* すべてのエンドポイントは SIEM を使用してテレメトリを確立できる必要があります。
* すべてのエンドポイントを XDR プラットフォームに統合できる必要があります。
* SOCサービスはXDRプラットフォームを監視できる必要がある
セキュリティ エンジニアが要件を満たすために実装する必要があるのは次のうちどれですか。
A. CDRと中央ログ
B. HIDS と vTPM
C. WAFとsyslog
D. HIPSとホストベースファイアウォール
正解: **D (**コメントを発表する**)**

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

質問: **86**
データ漏洩を防ぐために、企業のセキュリティ リーダーはユーザー教育を次の範囲に拡張することを決定しました。
* 健全なセキュリティ文化を構築します。
* 規制要件に準拠します。
* インシデント報告を改善します。
次のどれが彼らの目的を最も満たすでしょうか?
A. DoS攻撃を実行する
B. 定期的な侵入テストのスケジュール設定
C. フィッシングキャンペーンのシミュレーション
D. 偽のランサムウェアの展開
正解: (正解を表示します)
Simulating a phishing campaign helps users recognize phishing attempts and enhances overall security awareness. It is a practical way to improve incident reporting and ensure that users understand common attack vectors. This directly supports creating a healthy security culture, complying with regulatory requirements related to security training, and improving the response to security incidents.

質問: **87**
ある企業は、研究成果を業務に役立てることを目指し、研究能力への投資を検討しています。セキュリティアーキテクトが推奨する最適な選択肢は次のうちどれですか？
A. ダークウェブ監視
B. 脅威インテリジェンスプラットフォーム
C. ハニーポット
D. 継続的な敵対者エミュレーション
正解: (正解を表示します)
Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.

質問: **88**
最高情報セキュリティ責任者 (CIO)は、ランサムウェアによる業務への影響を懸念しています。ランサムウェア攻撃が発生した場合、データの整合性を維持し、RPO（目標復旧時点）を1時間未満に抑える必要があります。以下のストレージ戦略のうち、このビジネス要件を最もよく満たすものはどれですか？
A. フルディスク暗号化
B. リモートジャーナリング
C. 不変
D. RAID 10
正解: (正解を表示します)
Immutable storage prevents data from being altered or deleted, ensuring integrity even during a ransomware attack. Combined with frequent snapshots, it can achieve an RPO of less than one hour, best meeting the business requirements.

質問: **89**
コンプライアンス担当者が事業影響分析を実施しており、事業部門のリーダーに有意義なデータを収集してもらいたいと考えています。複数の事業部門リーダーは、担当者が必要とするデータの種類についてより詳しい情報を求めています。コンプライアンス担当者にとって最も有益なデータの種類は次のうちどれでしょうか？(2つ選択してください。)
A. 在庫詳細
B. 適用される契約上の義務
C. ダウンタイムに伴うコスト
D. ネットワーク図
E. 緊急時対応計画
F. クリティカルプロセス
正解: **C,F (**コメントを発表する**)**
Costs associated with downtime help quantify the financial impact of disruptions, which is essential for a business impact analysis (BIA).
Critical processes identify essential functions that must be prioritized for recovery, allowing the compliance officer to assess the consequences of interruptions effectively.

質問: **90**
ある企業のSIEM(セキュリティ情報イベント管理システム)は、誤検知と見逃しを継続的に報告しています。セキュリティ運用チームは、報告エラーの可能性をトラブルシューティングするために、構成変更を実施しました。必要な分析プロセスを最も効果的にサポートする情報源は次のうちどれですか？
(2つ選択してください。)
A. 第三者機関のレポートとログ
B. トレンド
C. ダッシュボード
D. アラートの失敗
E. ネットワークトラフィックの概要
F. 手動レビュープロセス
正解: **(**正解を表示します**)**
The best sources of information to support the analysis process for troubleshooting false positives and false negatives in a SIEM are:
Trends - Analyzing trends helps identify patterns in alerts, such as recurring false positives or missed detections (false negatives), allowing the team to adjust rules or thresholds accordingly.
Alert failures - Reviewing alert failures (e.g., missed detections or incorrect alerts) provides direct insight into why the SIEM is generating false positives or negatives, helping refine detection logic.

質問: **91**
法廷でデジタル証拠を提出するには、その証拠は以下の条件を満たしている必要があります。
A. 素材。
B. 有形。
C. 一貫性があります。
D. 保存されている。
正解: **(**正解を表示します**)**

For any evidence, digital or otherwise, to be admissible in court, it must be both relevant to the issues at hand (i.e., material) and authentic. "Material" evidence has a legitimate and effective influence on proving a fact in dispute. In practice, this means the digital artifacts you collect must directly relate to the elements of the case and help establish or refute a key point.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
シミュレーション
製品開発チームは、リリース前にレビューを受けるため、コードスニペットを提出しました。
説明書
コードスニペットを分析し、各コードスニペットに対して1つの脆弱性と1つの修正方法を選択してください。
シミュレーションを初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。
コードスニペット1



コードスニペット2

Code Snippet 1 Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103



API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer((‘192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = ‘ldapsearch -D “cn=‘ + userId + ‘” -W -p 389
                          -h loginserver.comptia.org
                          -b “dc=comptia,dc=org” -s sub -x “(objectclass=*)”’
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

jpnshiken.com
CompTIA

Answer Area

Code Snippet 1

Vulnerability 1

- ○ Cross-site request forgery
- ○ Server-side request forgery
- ○ Insecure direct object reference
- ○ SQL injection
- ○ Cross-site scripting

Fix 1

- ○ Perform input sanitization of the `userid` field.
- ○ Perform output encoding of `queryResponse`.
- ○ Ensure `userid` belongs to logged-in user.
- ○ Implement anti-forgery tokens.
- ○ Inspect URLs and disallow arbitrary requests.

Code Snippet 2

Vulnerability 2

- ○ Denial of service
- ○ SQL injection
- ○ Credentials passed via GET
- ○ Authorization bypass
- ○ Command injection

Fix 2

- ○ Perform input sanitization of the `userid` field.
- ○ HTTP POST should be used for sensitive parameters.
- ○ Implement prepared statements and bind variables.
- ○ Remove the `serve_forever` instruction.
- ○ Prevent the "authenticated" value from being overridden by a GET parameter.

jpnshiken.com CompTIA

正解:

Answer Area

Code Snippet 1

Vulnerability 1

- ○ Cross-site request forgery
- ○ Server-side request forgery
- ○ Insecure direct object reference
- ○ SQL injection
- ○ Cross-site scripting

Code Snippet 2

Vulnerability 2

- ○ Denial of service
- ○ SQL injection
- ○ Credentials passed via GET
- ○ Authorization bypass
- ○ Command injection

Fix 1

- ○ Perform input sanitization of the `userid` field.
- ○ Perform output encoding of `queryResponse`.
- ○ Ensure `userid` belongs to logged-in user.
- ○ Implement anti-forgery tokens.
- ○ Inspect URLs and disallow arbitrary requests.

Fix 2

- ○ Perform input sanitization of the `userid` field.
- ○ HTTP POST should be used for sensitive parameters.
- ○ Implement prepared statements and bind variables.
- ○ Remove the `serve_forever` instruction.
- ○ Prevent the "authenticated" value from being overridden by a GET parameter.

jpnshiken.com CompTIA.

質問: **93**

セキュリティアナリストがJavaで書かれた新しいアプリケーションを評価しています。セキュリティアナリストは、実行時に存在する脆弱性を特定する必要があります。目的を達成しつつ、最も網羅的な脆弱性リストを提供する方法は次のうちどれでしょうか？
A. 入力検証
B. 動的解析
C. サイドチャネル分析
D. ファジングテスト
E. 静的解析
正解: **(**正解を表示します**)**
Dynamic analysis is the most appropriate technique for assessing vulnerabilities during runtime.
It involves testing the application while it is running, which allows the security analyst to observe the application's behavior, detect vulnerabilities that emerge during execution, and understand how the application interacts with its environment. This provides a comprehensive view of vulnerabilities that may not be detected through static code analysis, as it accounts for issues like memory corruption, data leaks, and runtime exceptions.

質問: **94**
セキュリティ エンジニアには次の要件が与えられます。
* エンドポイントは内部署名されたアプリケーションのみを実行する必要があります
* 管理者アカウントでは許可されていないソフトウェアをインストールできません。
* 許可されていないソフトウェアを実行しようとする試みは記録される必要があります
これらの要件を最もよく満たすのは次のどれですか?
A. ディレクトリ管理と制御を通じて適切なアカウントアクセスを維持する
B. アプリケーションにプッシュされる更新を監視するための CSPM プラットフォームの実装
C. ソフトウェアのインストール試行を監視し、対応するための EDR ソリューションを導入する
D. ブロックされたハッシュとエンタープライズ信頼ルート証明書を使用したアプリケーション制御の構成
正解: **D (**コメントを発表する**)**
Application control with blocked hashes and enterprise-trusted root certificates ensures that only internally signed applications can be executed, aligning with the requirement to limit executable files to those signed by the organization. By blocking unauthorized hashes, the control prevents unauthorized software installations. This approach also meets the requirement to log attempts to run unauthorized software, as such events can be captured and logged by the application control solution.

質問: **95**
意思決定の参考となる大量の行動観察データを収集するプロセスをサポートするのは次のどれですか。
A. 線形回帰
B. 分散コンセンサス
C. ビッグデータ
D. 機械学習
正解: **(**正解を表示します**)**
Collecting a large pool of behavioral observations requires handling vast datasets, which is the domain of Big Data. Big Data technologies enable the storage, processing, and analysis of large- scale data (e.g., user behavior logs) to inform decisions, a key capability in security analytics.

質問: **96**

システム管理者は、継続的なスキャン活動の結果として生じた脆弱性をエンジニアと連携して処理し、対処します。管理者が直面する主な課題は、有効な検出結果と無効な検出結果を区別することです。システム管理者が適切に設定されているかどうかを確認する可能性が高い項目は次のうちどれですか。
A. レポートの保存期間
B. 資格情報をスキャンしています
C. エクスプロイト定義
D. テストのリズム
正解: **(**正解を表示します**)**
When differentiating between valid and invalid findings from vulnerability scans, the systems administrator should verify that the scanning credentials are properly configured. Valid credentials ensure that the scanner can authenticate and access the systems being evaluated, providing accurate and comprehensive results. Without proper credentials, scans may miss vulnerabilities or generate false positives, making it difficult to prioritize and address the findings effectively.

質問: **97**
第三者機関が、顧客の生データを見ることなく、顧客のデータを分析し、分析結果を提供できるシステムを導入しました。この機関は、次のうちどれを導入しているのでしょうか？
A. 非同期キー
B. 準同型暗号
C. データレイク
D. 機械学習
正解: **(**正解を表示します**)**
Homomorphic encryption allows computations to be performed directly on encrypted data, producing encrypted results that, when decrypted by the data owner, yield the correct analysis output-while the third party never has access to the underlying plaintext. This perfectly matches the requirement of analyzing data without ever seeing the raw values.

質問: **98**
インシデント対応訓練後、セキュリティ管理者は以下の表を確認します。

Service	Risk rating	Criticality rating	Alert severity
Public website	Medium	Low	Low
Email	High	High	High
Human resources systems	High	Medium	Medium
Phone system	High	Critical	Critical
Intranet	Low	Low	Low

今後、迅速なインシデント対応を最大限に支援するために、管理者は以下のうちどれを行うべきでしょうか？
A. 電話システムの障害発生時にITサポートへのアラートを自動化する。
B. サービスステータス監視用のダッシュボードを有効にする
C. 公開ウェブサイトへのログイン失敗時にメールを送信する
D. 人事システムの自動隔離を設定する
正解: **B (**コメントを発表する**)**
Enabling dashboards for service status monitoring is the best action to support rapid incident response. Dashboards provide real-time visibility into the status of critical systems, enabling quicker identification of issues and a more informed, proactive response during an incident. By having a centralized view of service status, the security administrator can respond more quickly and efficiently to any disruptions.

質問: **99**
クラウドエンジニアは、以下の点について適切な解決策を特定する必要があります。
・社内外のクラウド リソースへの安全なアクセスを提供する。
・トンネルの分岐交通の流れをなくす。
- IDおよびアクセス管理機能を有効にする。
以下の解決策のうち、最も適切なものはどれですか？
A. マイクロセグメンテーション
B. PAM
C. SD-WAN
D. SIX
正解: **(**正解を表示します**)**
SASE (Secure Access Service Edge) is the most appropriate solution because it combines network security and WAN capabilities, providing secure access to both internal and external resources, eliminating split-tunnel traffic, and offering robust identity and access management capabilities. It integrates security directly into the network architecture, which meets all the listed requirements.

質問: **100**
最近の評価において、セキュリティアナリストは以下の点を観察した。

Hostname	BIOS password	Fully patched	Firewall status
Sales2	welcome!	No	Active
Accounting1	$$m0neY	Yes	Active
Marketing6	HiTHER3	Yes	Inactive
Operations3	welcome!	Yes	Active

アナリストは今後、脆弱性に対処するために次のうちどれを使用すべきでしょうか？
A. システムイメージの強化
B. 多層防御
C. 最も恵まれない人々
D. OSアップデート
正解: **(**正解を表示します**)**

質問: **101**
セキュリティエンジニアは、特定のリスクを軽減するためのMDMソリューションを提案したいと考えています。MDMソリューションは、以下の要件を満たす必要があります。
* モバイル デバイスは、信頼ゾーンを離れた場合は無効にする必要があります。
* モバイルデバイスを紛失した場合、データにアクセスできなくなります。
セキュリティ エンジニアは、MDM ソリューションで次のオプションのうちどれを有効にする必要がありますか? (2 つ選択してください)。
A. フルディスク暗号化
B. ジオフェンシング
C. ジオタグ
D. コンテナ化

E. 許可/ブロックリスト
F. パッチ管理
正解: **A,B** (コメントを発表する)

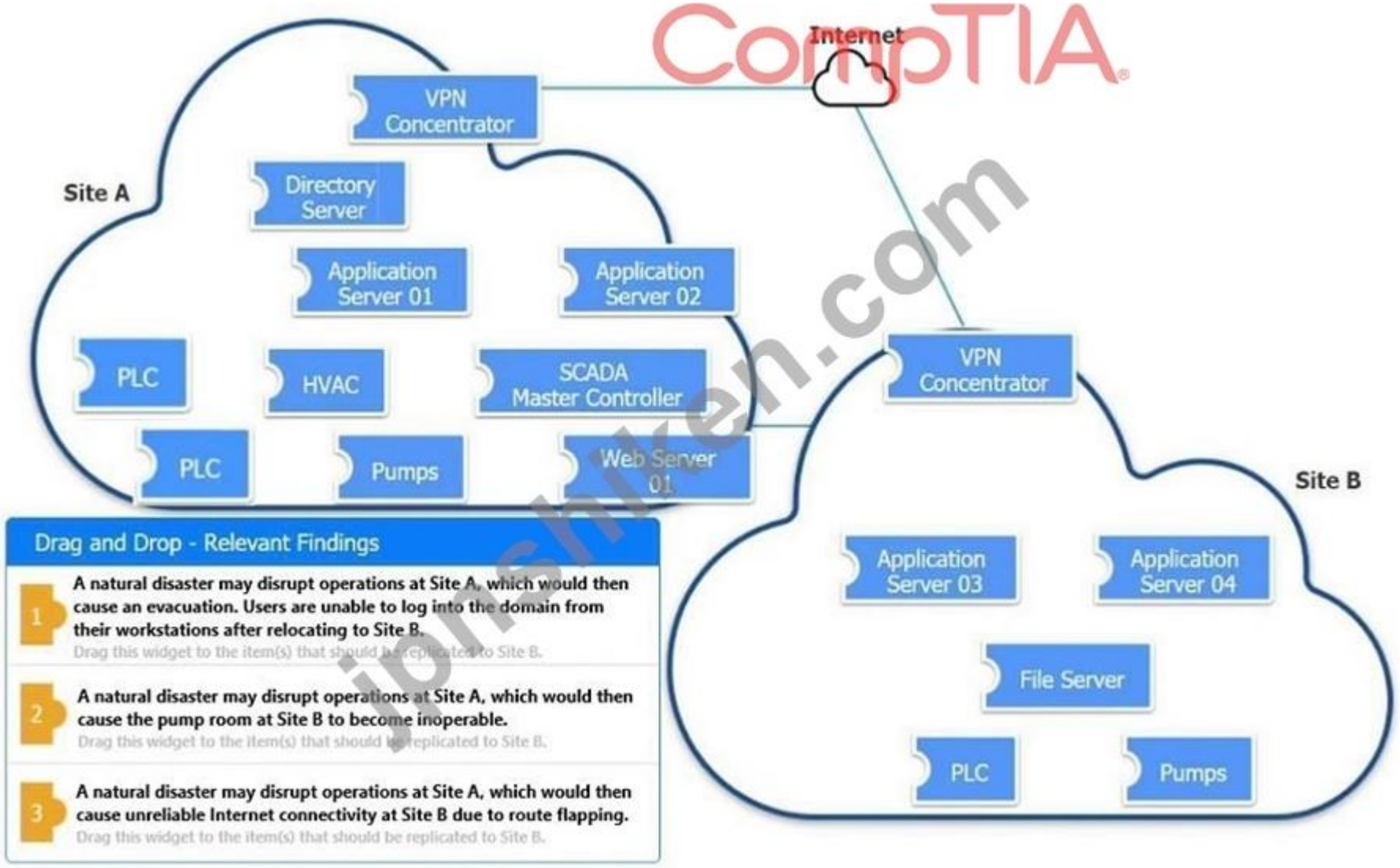
質問: **102**
あるゲーム開発者は新規市場への参入を目指しており、法律顧問から年齢制限を設けて登録手続きを義務付けるようアドバイスを受けました。法律顧問の懸念を最もよく表しているのは次のうちどれですか。
A. GDPR
B. LGPD
C. PCI DSS
D. COPPA
正解: (正解を表示します)
The Children's Online Privacy Protection Act (COPPA) requires online services, like games, to implement age-related sign-up requirements and obtain verifiable parental consent when collecting personal information from children under 13 in the U.S. This best aligns with the legal counsel's concerns.

質問: **103**
セキュリティアーキテクトは、SOCチーム向けに以下の要件を満たす新しいデータソースを統合したいと考えています。
- インシデントのエスカレーションには具体的なデータポイントを含める必要があります
- 事故に対する明確な是正措置を盛り込むべきである
対応チーム
適時性と正確性が最も重要な要素です
建築家の目的を達成するための最良の方法は、次のうちどれですか？
A. 既知の脆弱性データベース
B. インシデントエスカレーションプレイブックを確認する
C. インシデントスコアリングの妥当性検証
D. ISACからの業界脅威情報
正解: (正解を表示します)
Industry threat feeds from an ISAC provide timely and accurate intelligence that includes indicators of compromise, contextual details, and recommended mitigation or remediation actions. These feeds are structured so SOC teams can incorporate them directly into monitoring and incident escalation processes, ensuring alerts include relevant data points and actionable response guidance for the incident response team.

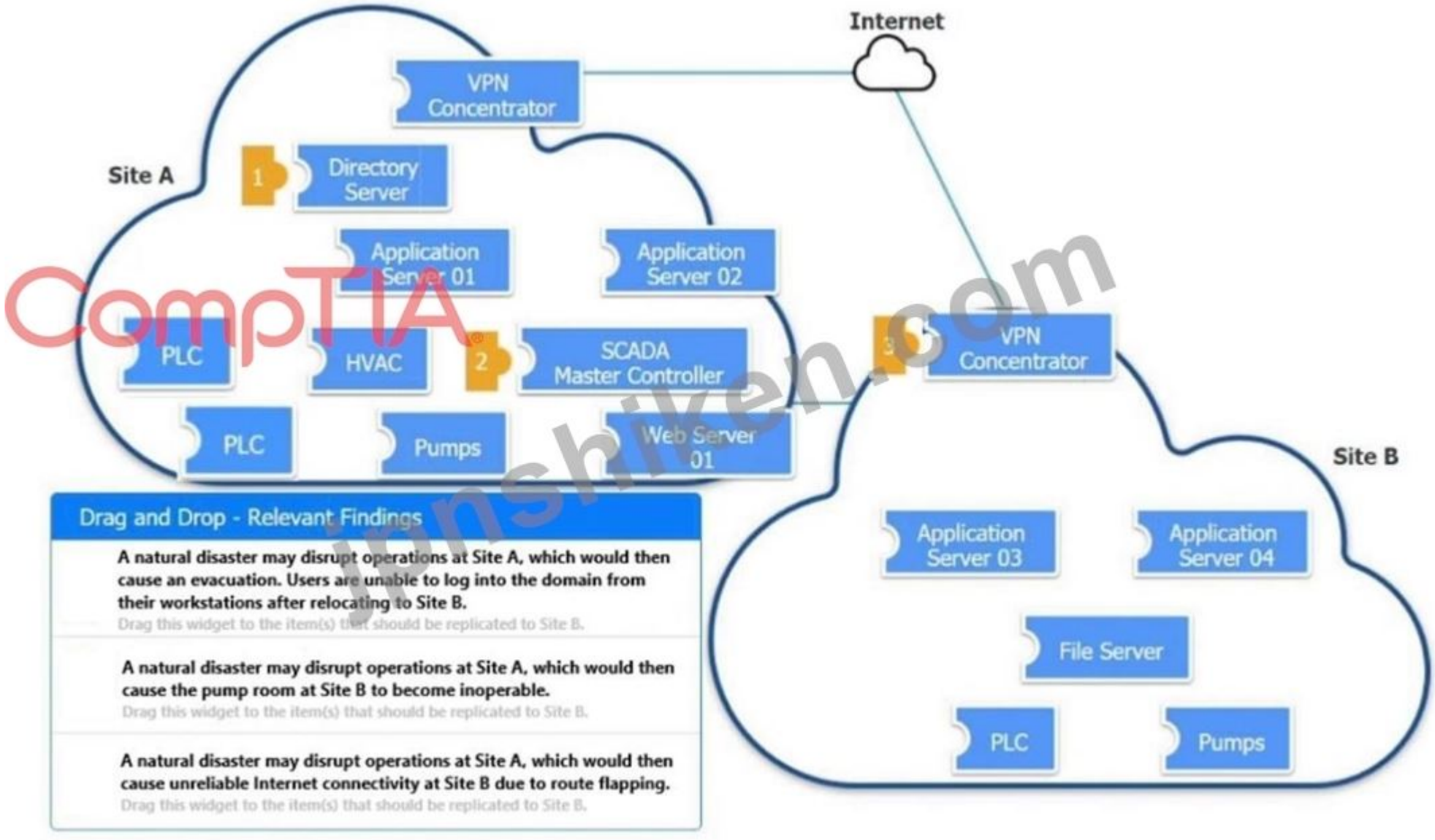
質問: **104**
ある組織は、以下のデータ型を含むデータ分類ポリシーに基づいてアクセス制御システムを実装したいと考えています。
- 機密
- 制限付き
- 内部
- 公開フラグによる審査
アクセス制御システムは、ユーザーをグループにマッピングするためにSSOフェデレーションをサポートする必要があります。各グループは、そのグループに割り当てられた分類でデータを処理および保存するシステムにのみアクセスできる必要があります。組織は、システムとリソースへの影響を最小限に抑えつつ要件を強制するために、次のうちどれを実施すべきでしょうか？

A. データ分類タイプに基づいてすべてのリソースにタグを割り当てるタグ付け戦略と、属性ベースのアクセス制御を強制するシステム
B. 人事部の信頼できる情報源システムで定義された内部ロールにデータ型をマッピングするロールベースのアクセス制御
C. データ型に基づくネットワークマイクロセグメンテーション、およびユーザープリンシパルに基づく強制アクセス制御を実施するネットワークアクセス制御システム
D. 内部LDAPによって管理され、システムごとに適用されるルールに基づくSSOシステムによるルールベースのアクセス制御戦略。
正解**: (**正解を表示します**)**
Tagging strategy: All resources (e.g., systems, files, databases) can be assigned tags based on their classification type (Confidential, Restricted, Internal, Public Flag for Review). This allows the access control system to easily associate resources with their respective data classifications without needing significant changes to the underlying systems.
Attribute-based access control (ABAC): ABAC allows access control decisions to be based on attributes (such as user group, resource tags, or data classification). By using ABAC, the system can enforce rules dynamically, allowing users in specific groups (mapped through SSO federation) to only access resources that match their assigned data classification.

質問**: 105**
シミュレーション
ある組織は、災害復旧と事業継続のための計画を立てている。
説明書
以下のシナリオと指示を確認してください。それぞれの関連する所見を、影響を受けるホストと照合してください。
シナリオ3を適切なホストに関連付けた後、ホストをクリックして、その検出結果に対する適切な是正措置を選択してください。
それぞれの調査結果は複数回使用される可能性があります。
シミュレーションを初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。


Internet
VPN Concentrator
Site A
Directory Server
Application Server 01
Application Server 02
PLC
HVAC
SCADA Master Controller
PLC
Pumps
Web Server 01
VPN Concentrator
Site B
Application Server 03
Application Server 04
File Server
PLC
Pumps
Drag and Drop - Relevant Findings
1
A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.
Drag this widget to the item(s) that should be replicated to Site B.
2
A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
Drag this widget to the item(s) that should be replicated to Site B.
3
A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.
Drag this widget to the item(s) that should be replicated to Site B.

正解:



Explanation:
Given that there is little connection between the two clouds when site A is down and cause an evacuation I would say directory server is damaged causing domain issues. 1 - Directory Server.
SCADA system controls the pumps so 2 - SCADA. Last is route flapping that is VPN concentrator, now dont make the mistake i did put 3 in site B not A as for the added option used the BGP routing, if bgp route is set to go through site A that might cause issues so 3 - VPM Concentrator (Site B) (BGP route option).

質問: **106**
インシデントが発生した後、チームは教訓のレビュー中に次のように報告しました。
* さらなる分析のための重要な情報が失われました。
* コミュニケーションの連鎖を活用しなかった
* 適切な対応のための正しい手順に従わなかった
これらの発見に対処するための最良の方法は、次のうちどれでしょうか?
A. インシデント対応業務の技術的能力を向上させるための、より優れたフォレンジックツールの予算を要求しています。
B. さまざまなシナリオのプレイブックを作成し、定期的にテーブルトップ演習を実施する

C. 新しいチームメンバー全員に専門的なインシデント対応の認定資格を要求する
D. インシデント対応ポリシーを公開し、セキュリティ意識向上プログラムの一環として実施する
正解: (正解を表示します)
Building playbooks for different incident scenarios provides a structured, repeatable process for the team to follow, ensuring critical steps are followed, information is not lost, and communication is effectively managed. Regular table-top exercises help familiarize the team with these procedures, allowing them to practice and refine their response capabilities before a real incident occurs. This directly addresses the issues raised in the lessons-learned review.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
ある組織は、自社のインフラストラクチャにおける脆弱性を特定するための脅威モデルを作成したいと考えています。以下のどれを優先すべきでしょうか？
A. 既知の脆弱性が悪用されている外部向けインフラストラクチャ
B. 70以上の既知の脆弱性を持つ内部インフラストラクチャ
C. リスクスコアが低く、悪用される脆弱性が知られていない外部向けインフラストラクチャ
D. リスクスコアが高く、リソースへのローカルアクセスでのみ悪用される可能性がある外部向けインフラストラクチャ
正解: (正解を表示します)
External-facing infrastructure with known exploited vulnerabilities poses the highest immediate risk, as it is directly accessible to attackers and already associated with active threats.
This should be the top priority in any threat modeling effort.

質問: **108**
アナリストは、脅威ハンティング機能を実行する際に、侵入分析のダイヤモンドモデルを使用します。アナリストは、可能性のある敵、関連するインフラストラクチャ、および標的を特定します。このモデルを効果的に使用するために、脅威ハンターが文書化する必要があるのは次のうちどれですか？
A. 知識
B. 機能
C. フェーズ
D. 方法論
正解: (正解を表示します)
The Diamond Model of Intrusion Analysis requires the documentation of capabilities, as this refers to the adversary's tools, techniques, and procedures (TTPs) used during the attack.
Identifying and documenting the adversary's capabilities is essential for effective threat-hunting, as it helps understand how the adversary operates and can guide the detection of similar future attacks.

質問: **109**
管理者は、社内のモバイルデバイス群をPKIに統合し、デバイスのWLAN NAC設定を既存のワークステーションやノートパソコンと整合させようとしています。数千台のデバイスを、費用対効果、時間効率、そしてセキュリティに配慮した方法で再構成する必要があります。この目標を達成するには、以下のどのアクションが最も効果的でしょうか？

2つ選択してください）
A. 既存のMDMソリューションを使用して、認証と登録のためのディレクトリサービスと統合する
B. netAuth拡張キー使用証明書テンプレートの展開
C. serverAuth拡張キー使用証明書テンプレートの展開
D. clientAuth拡張キー使用証明書テンプレートの展開
E. 一括デバイス登録用に OTP を使用して CA で SCEP を構成する
F. CA に CSR を送信して、すべてのデバイスで使用できる単一の証明書を取得します。
正解: **A,E (**コメントを発表する**)**
Using the existing MDM solution integrated with directory services automates authentication and enrollment, making the process scalable, secure, and cost-effective. Configuring SCEP with a one-time password enables secure bulk enrollment of many devices efficiently.

質問: **110**
監査の結果、旧型プラットフォームが30日以上ログを保持していないことが判明しました。このプラットフォームは、新しいテクノロジーとの相互運用性を考慮して分割されています。暫定的な解決策として、IT部門はログの保持期間を120日に変更しました。セキュリティエンジニアは、ログが適切に保持されるようにするために、次のうちどれを行うべきでしょうか？
A. ログを保存するスケジュールタスクを毎晩設定します
B. しきい値に達したときにログをエクスポートするようにイベントベースのトリガーを設定します。
C. SIEMを設定してログを集約する
D. ログをSQLデータベースに移動するためのPythonスクリプトを設定します。
正解: **(**正解を表示します**)**
A SIEM (Security Information and Event Management) solution is specifically designed to collect, store, and aggregate logs from various systems. By configuring the SIEM to aggregate the logs, the security engineer can ensure that the logs are properly retained, analyzed, and correlated for compliance and security purposes. This solution provides long-term storage and easier access to logs for investigations.

質問: **111**
最近、同じ業種の2つの大手エンジニアリング企業が、サイバー脅威への対策を共同で行うことを決定しました。この共同アプローチを最もよく表しているのは次のうちどれですか？
A. NDA
B. SOW
C. SLA
D. 覚書
正解: **(**正解を表示します**)**
An MOU (Memorandum of Understanding) is the best choice in this scenario, as it represents an agreement between two parties outlining the intention to collaborate or work together on a common goal, without creating legally binding obligations. In this case, the two engineering companies are uniting to approach cyberthreats in a unified way, and an MOU would formalize this cooperative arrangement and define the terms of their collaboration.

質問: **112**
セキュリティアナリストが、ユーザーが特定の数字の順序で0から9までの番号のボタンをタッチすることで施錠された部屋に入れるようにするタッチスクリーンデバイスを設計しています。アナリストは、デバイスを使用するたびに番号がランダムに表示されるようにキーパッドを設計しました。以下のうち、設計上のトレードオフを最もよく表しているのはどれですか？(2つ選択してください。)

A. ユーザーが数字を入力する際に、誰かがパターンを見逃すリスクが軽減されます。
B. 乱数列を生成するルーチンは簡単に実装できます。
C. このデザインでは、ユーザーにとって数字の入力がより難しくなります。
D. このデバイスは数値を計算するために追加の電力が必要です。
E. エンドユーザーはアクセス番号を覚えるのがより難しくなります。
F. 弱いアクセス番号や簡単に推測できるアクセス番号の方が可能性が高い。
正解: **A,C** (コメントを発表する)
A: Randomizing the keypad reduces the risk of shoulder-surfing attacks by eliminating predictable patterns.
C: Randomization increases the cognitive load on users, making it harder to input numbers quickly.
D: Additional computational power is minimal and not typically a trade-off.
E and F: Remembering access numbers or weak passwords are unrelated to keypad randomization.

質問: **113**
企業の事業影響度分析(BIA)では、1時間以上のデータ損失は事業にとって壊滅的な打撃となることが示されています。この要件を満たすために、次のうちどれを実施する必要がありますか？
A. RPO
B. RTO
C. SLA
D. DRP
E. BCP
正解: (正解を表示します)
RPO (Recovery Point Objective): Specifies the maximum acceptable amount of data loss measured in time. If data loss of more than one hour is unacceptable, the RPO should be set to less than or equal to one hour.
RTO (Recovery Time Objective): Refers to the acceptable duration of system downtime, which is not relevant to the question.
The BCP, DRP, and SLA do not directly address data loss.

質問: **114**
セキュリティ管理者は、Web サイトのコンポーネントから次のコード スニペットを確認しています。

```
<link rel="stylesheet" type="text/css" font-weight: normal;
font-style: normal;
if ((is_admin() " (function_exists ('get_hex_cache'))) !== true {add_action('wp-head' .
'get_hex_cache',12) function get_hex_cache () { return print ((hex2bin('3c7',
(file_get_contents ('dir_' /inc.tmp )....
```

inc.tmp ファイルを確認すると、次のことがわかります。

```
21487592579325342038509345083453432452523435235345523453242353424523453452345389627656385793257839537854362038263053280450832 5
```

不正確さの原因として最も可能性が高いのは次のどれですか?
A. コンテンツ管理ソリューション プラグインが悪用されました。
B. 検索エンジンのボットがファイアウォールでブロックされています。
C. 関連するスタイルシートが破損しています。

D. WAF は透過モードに設定されています。
正解: **A (**コメントを発表する**)**
The code snippet includes obfuscated PHP code that loads and executes content from a temporary file (inc.tmp) via hex2bin(file_get_contents(...)), often seen in web malware injections. This strongly suggests that a CMS plug-in has been exploited to inject malicious code into the website.

質問: **115**
AIモデルに対するサービス拒否攻撃を最もよく説明しているのは、次のうちどれですか？
A. 大規模で計算負荷の高いデータセットを投稿するユーザー
B. 信頼性が低く、検証されていないモデル出力
C. AIサービスのAPIを攻撃する攻撃者
D. モデルの出力結果を利用して、そのパラメータやアーキテクチャを理解する
正解: **(**正解を表示します**)**
An AI model denial-of-service attack occurs when an attacker intentionally submits very large or computationally expensive inputs that force the model to consume excessive processing resources. This overwhelms the model's inference capacity, degrades performance, and can prevent legitimate users from receiving responses, effectively disrupting the availability of the AI service.

質問: **116**
セキュリティエンジニアが、マルチホーム構成のLinuxシステムに対して脆弱性管理スキャンを実行しています。エンジニアは、各脆弱性が各システムのNICの数で乗算されるため、脆弱性の数が多くなっていることに気づきました。脆弱性の重複を排除し、特定のホストに脆弱性を関連付けるために、エンジニアは次のうちどれを行うべきでしょうか？
A. SCAPスキャナを使用してください。
B. エージェントをデプロイします。
C. 検出スキャンを開始します。
D. Nmapスキャンを実行します。
正解: **B (**コメントを発表する**)**
Deploying an agent on the systems will allow for more accurate and centralized vulnerability management. The agent can deduplicate vulnerabilities by associating them with a specific host, regardless of how many network interface cards (NICs) the system has. This helps eliminate the issue of vulnerabilities being counted multiple times for each NIC. Agents can also collect data from the system more accurately and ensure that vulnerabilities are tied to the correct host.

質問: **117**
ある企業は、ビジネスアナリストが購入依頼のリンクを含むメールを受信するための新しいプロセスを導入した。この新しいプロセスでは、リンクは新しいメールを介して送信する必要がある。
注文処理を中断することなくこのプロセスを保護するための最良の方法は、次のうちどれですか？
A. ブラウザ分離ソリューションの導入
B. 潜在的に悪意のあるリンクをすべてブロックします
C. セキュリティ意識向上トレーニングの実施
D. DNSフィルタリングの実装
正解: **(**正解を表示します**)**

Deploying a browser isolation solution would be the best way to secure this process without disrupting order fulfillment. It allows users to click on links within emails while keeping any potentially harmful content isolated from the rest of the network. This prevents malicious links from affecting internal systems while still enabling users to complete their tasks without disruption.

質問: **118**
外部の脅威アクターが公共インフラプロバイダーを攻撃した。この攻撃への対応とその後の活動において、様々なプロバイダーが対応活動中に得られた情報を共有した。
攻撃後、エネルギー関連企業は自社の状況と対応に関するデータを共有した。

Company	SIEM	UEBA	DLP	ISAC member	TIP integration	Time to detect	Time to respond
1	Yes	No	Yes	Yes	Yes	10 minutes	20 minutes
2	Yes	Yes	Yes	Yes	No	20 minutes	40 minutes
3	Yes	Yes	No	No	Yes	12 minutes	24 minutes

将来の攻撃から身を守るために、対処すべき最も重要な問題は次のうちどれですか？
A. UEBAシステムの導入失敗
B. DLPシステムの導入失敗
C. 業界ISACへの参加失敗
D. TIPとの統合に失敗
正解: **D** (コメントを発表する)
Company 2, which has SIEM, UEBA, DLP, and ISAC membership-still shows the slowest detection (20 min) and response (40 min) times. Its only gap is lack of integration with a Threat Intelligence Platform (TIP). Automating the intake, normalization, and enrichment of shared indicators via a TIP lets the SIEM/UEBA/DLP correlate new threat data in real time, cutting both mean time to detect and mean time to respond.

質問: **119**
ある企業は脆弱性管理プログラムに問題を抱えています。新しいデバイスやIPが定期的に追加 削除されるため、脆弱性レポートに一貫性がなくなります。脆弱性管理プロセスを改善するために、企業が実行すべきアクションは次のどれですか？
A. 導入および廃止されたすべての新規資産に関する週次レポートをリクエストします
B. DHCP リース期間を延長して、デバイスが同じアドレスを長期間維持できるようにします。
C. ネットワーク上の不正なデバイスを回避するためにシャドーIT検出プロセスを実装する
D. 脆弱性管理ツールを使用して、11 のランドスケープ全体で定期的な検出スキャンを実行します。
正解: **D** (コメントを発表する)
To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool.
Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.
Consistency in Reporting: By continuously discovering and scanning new and existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.
Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.

質問: **120**

営業時間外に、リモートコンソールアプリケーションから建物内のカメラにリモートアクセスされ、無効化されました。セキュリティアナリストが以下のログを確認しました。

```
l1 Dec 16:03:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (Windows NT 5.1) Gecko
l1 Dec 16:33:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0(Windows NT 5.1) Gecko
l1 Dec 22:30:23 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
l1 Dec 23:00:23 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
l1 Dec 23:05:43 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
l1 Dec 23:35:43 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
l2 Dec 00:30:53 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
```

脅威を最も効果的に軽減するためにアナリストが実行すべきアクションは次のうちどれですか?

A. Web アプリケーションに WAF 保護を実装します。

B. カメラのファームウェアをアップグレードします。

C. 承認された IP からの接続のみを許可します。

D. ファイアウォールで IP 104.18.16.29 をブロックします。

正解: **(**正解を表示します**)**

The logs show successful admin access from both an internal IP (192.168.2.5) and an external IP (104.18.16.29). Since external access during off-hours indicates compromise, the best long-term mitigation is to restrict remote access so only approved IPs can connect. This prevents unauthorized external access while maintaining legitimate internal management.

質問: **121**

シミュレーション

あなたは、会社の特権ネットワークから得られたNmapスキャンの結果を解釈する任務を負ったセキュリティアナリストです。

同社の耐震強化ガイドラインには、以下の内容が記載されています。

デバイスごとにプライマリサーバーまたはサービスが1つ必要です。

デフォルトポートのみを使用してください。

安全性の低いプロトコルは無効にする必要があります。

説明書

Nmapの出力結果を使用して、ネットワーク上のデバイスとその役割、および閉じるべき開いているポートを特定します。

Nmapによって検出された各デバイスについて、以下の情報を含むデバイスエントリを 検出されたデバイス」リストに追加します。

- デバイスのIPアドレス
- デバイスの主要なサーバーまたはサービス(各IPアドレスは1つのサービス/ポートのみに関連付けられることに注意してください)
- 強化ガイドラインに基づいて無効にする必要があるプロトコル(強化ガイドラインに準拠するために複数のポートを閉じる必要がある場合があることに注意してください)。シミュレーションの初期状態に戻したい場合は、[すべてリセット] ボタンをクリックしてください。

NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE  SERVICE  VERSION
25/tcp    closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp   open   ssl/smtp smtpd
587/tcp   open   ssl/smtp smtpd
443/tcp   open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE  SERVICE  VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open   http     Microsoft IIS httpd 7.5
443/tcp   open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
```

Devices Discovered (0)

Add Device For

- 10.1.45.65
- 10.1.45.66
- 10.1.45.67
- 10.1.45.68

cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
443/tcp	open	ssl/http-proxy	SonicWALL SSL-VPN http proxy

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux 2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).

NMAP Scan Output

Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	CrushFTP sftpd (protocol 2.0)
8080/tcp	open	http	CrushFTP web interface

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports

PORT	STATE	SERVICE	VERSION
25/tcp	closed	smtp	Barracuda Networks Spam Firewall smtpd

Devices Discovered (1)

Add Device For 10.1.45.66

IP Address 10.1.45.65

Role

- SFTP Server
- Email Server
- FTP Server
- UTM Appliance
- Web Server
- Database Server
- AD Server

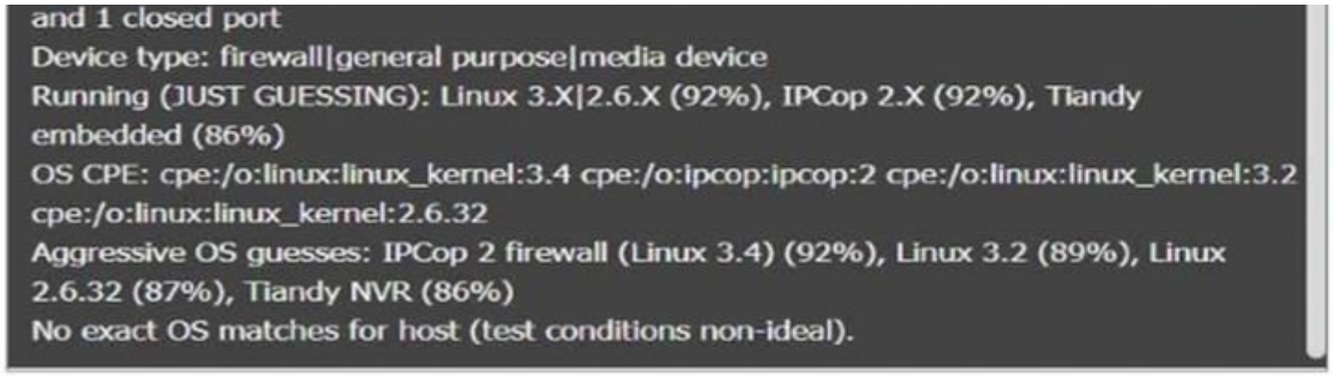
Disable Protocols 20/tcp

```
415/tcp  open   ssl/smtp smtpd
587/tcp  open   ssl/smtp smtpd
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE  VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp   closed ssh
80/tcp   open   http     Microsoft IIS httpd 7.5
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE         VERSION
21/tcp  open  ftp             Pure-FTPd
443/tcp open  ssl/http-proxy  SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
```

- [ ] 21/tcp
- [ ] 22/tcp
- [ ] 25/tcp
- [ ] 80/tcp
- [ ] 415/tcp
- [ ] 443/tcp
- [ ] 8080/tcp



正解:
10.1.45.65 SFTP Server Disable 8080
10.1.45.66 Email Server Disable 415 and 443
10.1.45.67 Web Server Disable 21, 80
10.1.45.68 UTM Appliance Disable 21

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 122
セキュリティエンジニアは、OpenSSHベースのアプリケーションにおけるSWEET32の脆弱性を修復し、既存の設定を確認する必要があります。セキュリティエンジニアは次のうちどれを行うべきでしょうか？(2つ選択してください。)
A. Twofishのアルゴリズムを無効にする
B. cat /etc/sshd/ssh_config | grep "HMAC"
C. RSAアルゴリズムを無効にする
D. cat /etc/sshd/ssh_config | grep "PermitRootLogin"
E. 3DESアルゴリズムを無効にする
F. cat /etc/sshd/ssh_config | grep "Ciphers"
正解: **(**正解を表示します**)**
SWEET32 exploits the 64-bit block size of 3DES, so disabling 3DES algorithms mitigates the vulnerability.
Reviewing the Ciphers configuration in ssh_config ensures only secure ciphers are enabled, confirming 3DES is removed and stronger algorithms are enforced.

質問: 123
ある製薬会社は、化学物質の製造に自動制御システムを採用しています。最近、これらのシステムのセキュリティ強化を目的とした実験を行ったところ、セキュリティエンジニアは、コントローラがネットワーク遅延の増加に対して感度が低いことを発見しました。この問題に対する最適な対策は次のうちどれでしょうか？
A. 制御システムコマンドジャーナルの整合性チェックを実行する
B. システム構成に関するベースラインレビューの実施
C. 不適切な形式のコマンドを破棄するプロキシを統合する
D. 制御システム間のインライン暗号化の実装

E. プロトコルアクセラレータのデプロイと構成
正解: **D (**コメントを発表する**)**
The test showed that the control systems are not sensitive to additional network latency. This means security controls that introduce latency can be safely deployed without disrupting operations. Implementing in-line encryption between the control systems would protect command and telemetry traffic from interception or manipulation while maintaining system functionality.
Since latency is not a concern, encryption becomes a viable and effective control for securing communications within the industrial control environment.

質問: **124**
ある組織は、タイポスクワッティングを利用したフィッシングキャンペーンの増加に気づきました。セキュリティアナリストは、フィッシングキャンペーンで使用されているドメインと比較して、一般的に使用されているドメインのデータを拡充する必要があります。アナリストはログフォワーダーを使用して、ネットワークログをSIEMに転送します。セキュリティアナリストがこの分析を実行できるのは次のうちどれですか？
A. acron ジョブを使用して、ドメインを定期的に更新および比較します。
B. ドメインに一致するパーサーを作成します。
C. 一致するドメイン名をすべて除外するクエリを開発します。
D. SIEM にドメイン別のトラフィックの割合を表示するダッシュボードを実装します。
正解: **(**正解を表示します**)**
To enrich the data for analysis, the security analyst needs to compare the legitimate domains against those used in phishing campaigns. Creating a parser that matches domains allows the SIEM to automatically identify and analyze the domains in the logs, helping detect typosquatting and other malicious domain usage. This method allows for efficient and automated processing of log data to identify potential threats.

質問: **125**
企業のアプリケーションのセキュリティ監査で、顧客アカウントのパスワードが手動で設定されており、有効期限がないことが判明しました。同社は、限られた予算内でパスワードの問題を解決したいと考えています。
顧客への影響を最小限に抑えつつ、30日間で目標を達成する必要があります。会社は次のうちどれを行うべきでしょうか？
A. 各ユーザーに連絡してパスワードをリセットしてください。
B. 特権アクセス管理ソリューションを設定します。
C. OAuth 2 を可能にする認証方法を移行します。
D. セルフサービス型の認証情報リセットポータルを実装する。
正解: **(**正解を表示します**)**

質問: **126**
セキュリティアナリストが次のログを確認しています:

Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

jpnshiken.com
CompTIA

セキュリティアナリストがさらに調査する必要がある可能性のあるイベントは次のうちどれですか?

A. 実行が阻止されたマクロ

B. 漏洩したパスワードを含むテキストファイル

C. この環境で実行された悪意のあるファイル

D. 機密情報が不適切に公開されたPDF

正解: **(**正解を表示します**)**

The dll file with a 10 MB size is allowed to be executed in the c:\temp directory. Since DLL (Dynamic Link Library) files are often associated with executable code and can be used for malicious purposes, this should be investigated further. The fact that it is allowed to run raises suspicion, and the location of the file (temp directory) is commonly used by malware for executing unauthorized processes.

質問: **127**

セキュリティイベントの調査中、アナリストはユーザーが不明な送信元からのメールの添付ファイルを開いた証拠を発見しました。ユーザーが添付ファイルを開いた直後、複数のサーバーでネットワークとリソースへの大規模なアクティビティが発生しました。サーバーを調査した結果、アナリストはサーバーがランサムウェアによって暗号化されていることを発見しました。ランサムウェアは48時間以内に身代金を要求し、支払わなければすべてのデータを破壊すると脅迫しています。会社にはランサムウェアへの対応計画がありません。アナリストが経営陣にインシデントを報告した後、次に取るべきステップは次のうちどれですか？

A. 法執行機関に通報する

B. 48時間以内に身代金を支払う

C. 影響を受けたサーバーの即時復旧を要請する

D. 感染拡大を防ぐためにサーバーを隔離する

正解: **(**正解を表示します**)**

質問: **128**

セキュリティアナリストは、サポート対象外のオペレーティングシステムを実行している仮想サーバーをサポートするネットワーク構造を設計しています。サポート対象外のオペレーティングシステムには個人情報が含まれており、業務上非常に重要です。以下の情報が与えられた場合：

- PIIサーバー名はlegacy-boxで、マシンIPは
192.168.1.100
- ジャンプボックスサーバー名はjump-boxで、IPアドレスは192.168.1.10です。
- 社内ネットワークのIPアドレス体系は192.168.1.0/24です。

以下のIPアドレスを持つマシンはアクセスが必要です

- 192.168.1.3
- 192.168.1.4

アナリストは、個人情報保護サーバーを最も安全に保護するために、次のうちどの行動をとるべきでしょうか？
A. ジャンプボックスとレガシーボックスにデュアルNICを設定し、仮想ネットワークIPアドレスと企業ネットワークIPアドレスの両方を割り当てます。
B. レガシーボックスのホストファイアウォールルールとルートを変更して、192.168.1.3と192.168.1.4のみにRDP接続を許可する。
C. ジャンプボックス上でホストファイアウォールルールとルートを設定し、192.168.1.3と192.168.1.4のみがRDP接続できるようにする。
D. レガシーボックス上でホストファイアウォールルールとルートを実装し、192.168.1.0/24 からの RDP 接続のみを許可し、それ以外はすべて拒否します。
正解: **(**正解を表示します**)**
The unsupported server contains PII and should be isolated as much as possible from the corporate network. The most secure design is to require administrators to connect first to the jump box and then access the legacy server from there, limiting direct exposure of the legacy system. Configuring firewall rules and routing on the jump box so only the two authorized workstations can RDP to it creates a controlled access path while keeping the legacy server better protected behind that intermediary system.

質問: **129**
最近の監査で、次の情報に基づいて、ある会社のシステムが評価されました。

Department	System	Status	Notes
Accounting	TaxReporting	OK	
Human resources	HRIS	OK	
Manufacturing	ProductionControl	WARNING	EOL software detected
Support	ServiceDesk	WARNING	Patches available

攻撃対象領域を減らすための最良の方法はどれですか?
A. 製造業における影響を受けるすべての機械に EDR ソリューションを導入する
B. 製造ネットワークをファイアウォールでセグメント化し、ルールを監視モードに設定する
C. ソフトウェアへの脅威を監視および検出するためのIDSをインラインで設定する
D. アプリケーション対応ファイアウォールを実装し、アプリケーションアクセスに対する厳格なルールを記述する
正解: **(**正解を表示します**)**
The ProductionControl system is running end-of-life (EOL) software, which poses a high security risk. Since the software cannot be updated, the best way to reduce the attack surface is to use an application-aware firewall with strict access rules, limiting exposure while maintaining necessary functionality.

質問: **130**
脆弱性評価中にスキャンを行うと、次の結果が明らかになります。
Windows Server 2016 修正プログラム KB87728 が未適用 - CVSS 3.1 スコア: 8.1 [高] - 影響を受けるホスト: 172.16.15.2 レビュープロセスの後半で、修復チームはこの結果を誤検知としてマークしました。今後のスキャンでこの問題を回避するための最適な方法は、次のうちどれですか？
A. CMDBから最新の資産リストを取得する
B. サーバー上で認証スキャンを実行しています
C. フィンガープリンティングサーバ用の高度なポリシーを使用してセンサーを構成する
D. プロセスの早い段階で修復チームとスキャン実行を調整する
正解: **(**正解を表示します**)**
Authenticated scans allow the scanner to verify installed patches and configurations, reducing false positives.

質問: **131**
セキュリティアナリストが次の脆弱性評価レポートを確認しています。
192.168.1.5、ホスト = Server1、CVSS 7.5、Web サーバー、リモート実行可能 = はい、エクスプロイト = はい

205.1.3.5、ホスト = Server2、CVSS 6.5、バインドサーバー、リモート実行可能 = はい、エクスプロイト = POC
207.1.5.7、ホスト = Server3、CVSS 5.5、電子メールサーバー、リモート実行可能 = はい、エクスプロイト = はい
192.168.1.6、ホスト = Server4、CVSS 9.8、ドメイン コントローラ、リモート実行可能 = はい、エクスプロイト = はい インターネットに接続されたホストに対する攻撃を最小限に抑えるために、最初にパッチを適用する必要があるのは次のどれですか。
A. サーバー1
B. サーバー2
C. サーバー3
D. サーバー4
正解: **B (**コメントを発表する**)**
The question focuses on internet-facing hosts, implying external exposure. CVSS scores, remote executability, and exploit availability guide prioritization. Server2 (205.1.3.5, CVSS 6.5, Bind Server) has a public IP, suggesting it's internet-facing, unlike Server1 and Server4 (192.168.x.x, private IPs). Server3 (207.1.5.7, CVSS 5.5) is also public but has a lower score and risk compared to Server2's proof-of-concept (POC) exploit. Server2's Bind Server (DNS) role is critical and commonly targeted, making it the priority.

質問: **132**
ある企業が、顧客向けにビデオトレーニングを提供する新しいオンラインアプリケーションを導入する計画を立てている。
設計の一環として、アプリケーションは以下の要件を満たす必要があります。
- すべてのユーザーにとって高速
- 世界中のユーザーが利用可能
- 攻撃から保護されています
これらの要件を満たすために、会社が使用すべき最適な部品は次のうちどれですか？(2つ選択してください。)
A. WAF
B. IPS
C. CDN
D. SIX
E. VPN
F. CASB
正解: **A,C (**コメントを発表する**)**
A Web Application Firewall (WAF) protects the application from attacks such as injection and cross-site scripting. A Content Delivery Network (CDN) improves performance and availability by caching content closer to users worldwide.

質問: **133**
ある企業が、重要なワークロードをデータセンターからクラウドに移行しました。このワークロードは、膨大な計算量を要するデータ処理を必要とする大規模なデータセットを使用しています。このワークロードを使用する事業部門は、次のような成長パターンを予測しています。
* ストレージ要件は 6 か月ごとに 2 倍になります。
* 計算要件は年間を通じて変動します。
* 平均的な計算要件は毎年倍増します。
事業部門の要件に対応するために、会社は次のどれを行う必要がありますか?
A. ストレージ用にクラウドベースの CDN を、コンピューティング用にロードバランサーをデプロイします。
B. 垂直自動スケーリング モードでコンピューティングとストレージを組み合わせます。
C. コンピューティングおよびストレージ リソース用のロード バランサーを実装します。

D. 水平方向にスケーリングするコンピューティングおよびストレージ インフラストラクチャを計画します。
正解: **(**正解を表示します**)**
Horizontal scaling allows the company to add more compute and storage nodes as demand increases. This approach is ideal for handling rapid growth in storage, fluctuating compute needs, and long-term doubling of processing demands, ensuring scalability and flexibility in a cloud environment.

質問: **134**
ソフトウェア開発会社は、ソフトウェアサプライチェーンにおける第三者リスクを軽減する必要がある。
この目的を最も効果的に達成するために、企業は開発環境において以下のどの手法を用いるべきでしょうか？
A. ソフトウェア構成分析の実施
B. 多要素認証を必須とする
C. コーディング基準の確立と遵守状況の監視
正解: **A** (コメントを発表する)
D. 堅牢な単体テストおよび回帰テストスキームの実装
Software Composition Analysis (SCA) tools inventory and continuously monitor all third-party and open-source components in your codebase, flagging known vulnerabilities and license issues before they make it into production. This directly addresses supply-chain risk by ensuring you know exactly which external libraries you're using and whether they contain any security flaws.

質問: **135**
セキュリティ アナリストが次の認証ログを確認しています。

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

アナリストが最初に行うべきことはどれですか?
A. User2のアカウントを無効にする
B. User12のアカウントを無効にする
C. User8のアカウントを無効にする
D. User1 のアカウントを無効にする
正解: **(**正解を表示します**)**
The logs show multiple failed login attempts for User1 in rapid succession from the same machine (VM01), followed by a successful login, indicating a likely brute-force attack or account compromise. The analyst should disable User1's account immediately to prevent further unauthorized access.

質問: **136**

ある脅威インテリジェンス企業の事業目標は、顧客がAPIを介して様々なTIPに直接データを統合できるようにすることです。同社は、以下の目標を可能な限り多く達成したいと考えています。
* コンピューティングのコストを可能な限り削減します。
* すべてのユーザーが利用できることを保証します。
* 潜在的な攻撃対象領域を減らします。
* 提供されたデータの整合性を確保します。
企業が目標を最もよく達成するために考慮すべきは次のどれですか?
A. アカウントに固有のAPI秘密鍵を設定する
B. パブリックディレクトリに IoC のリストを公開する
C. 登録ユーザーごとにレート制限を実装する
D. 利用可能なすべてのデータのハッシュを提供する
正解: **A (**コメントを発表する**)**
Configuring a unique API secret key for accounts ensures only authenticated users can access the API, reducing the attack surface while maintaining data integrity and availability. It also supports efficient resource use by restricting unauthorized access, aligning with the business objectives.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
ある企業は、グローバル企業ネットワーク全体に展開されているソフトウェアに特定のソフトウェアライブラリが含まれているかどうかを迅速に評価する必要があります。このような評価が必要になった際に、企業のSOCが迅速に対応するために最も効果的な方法は次のうちどれですか。
A. SOCスタッフのみにアクセスが制限されたサーバー上でSAST/DASTレポートを維持する
B. すべてのソフトウェアベンダーにサードパーティのリスク軽減策を証明することを契約で義務付ける
C. すべてのサプライヤーと社内開発者に徹底したSBoMの実装を要求する
D. すべてのソフトウェアベンダーと社内開発者のリストを維持するためのGRCツールの実装
正解: **(**正解を表示します**)**
A Software Bill of Materials (SBoM) provides an inventory of all libraries and components in deployed software. Maintaining SBoMs allows the SOC to quickly identify affected systems when a vulnerable library is discovered, enabling a rapid and accurate response.

質問: **138**
AIの出力が不正確になる理由を最もよく説明しているのは、次のうちどれですか？
A. モデル中毒
B. 社会工学
C. 出力処理
D. 迅速な注射
正解: **(**正解を表示します**)**
Model poisoning involves deliberately feeding malicious or biased data into an AI model during training, leading to inaccurate or manipulated outputs. It directly affects the model's behavior and reliability.

質問: **139**
監査担当者が、インシデントの原因を特定するために、Webアプリケーションのログをレビューしている。
ウェブアプリケーションのアーキテクチャは、インターネットからアクセス可能なアプリケーションロードバランサー、プライベートサブネット内の複数のウェブサーバー、アプリケーションサーバー、および階層構成のデータベースサーバー1台で構成されています。アプリケーションロードバランサーはログを保存できません。以下はログのサンプルです。

```
Web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200 453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```

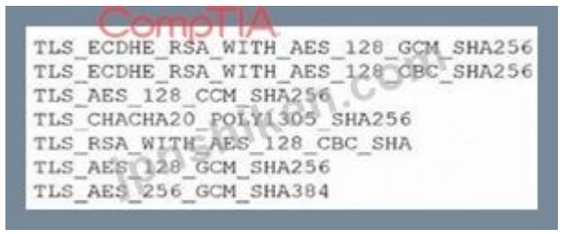
監査人は、将来発生する可能性のある事象の原因を特定できるようにするために、以下のうちどれを推奨すべきでしょうか？
A. ロードバランサーで X-Forwarded-For ヘッダーを有効にします。
B. アプリケーションサーバーにソフトウェアベースのHIDSをインストールします。
C. 信頼できる認証局によって署名された証明書をインストールします。
D. データベースサーバー上のストアドプロシージャを使用します。
E. Webサーバーから受信した$_SERVER['REMOTE_ADDR']の値を保存します。
正解: **(**正解を表示します**)**
In a tiered setup behind a proxy or load balancer, the web servers' REMOTE_ADDR will only ever show the balancer's IP, not the true client's.
By configuring the load balancer to inject the X-Forwarded-For HTTP header with the original client IP, that value can be logged by the web servers (and propagated downstream), ensuring every request can be traced back to the real source address.

質問: **140**
開発者は、ミッションクリティカルなアプリケーションを保護するために使用される鍵を生成するために、ワークステーションを使用しました。セキュリティエンジニアは、鍵生成情報の不正な漏洩リスクを低減する必要があります。このプロセスのセキュリティを向上させるための最良の方法は次のうちどれですか？
A. HSM
B. SED
C. FDE
D. TPM
正解: **(**正解を表示します**)**
A hardware security module provides a dedicated, tamper-resistant hardware environment for generating, storing, and managing cryptographic keys. Keys are created and used within the protected hardware boundary and are never exposed in plaintext to the host system. This significantly reduces the risk of unauthorized disclosure compared with generating keys on a workstation where they could be accessed by malware or unauthorized users.

質問: **141**

ある企業が、データベースに保存されているデータを隠蔽するためのソリューションを探しています。そのソリューションは、以下の要件を満たす必要があります。
生産環境を効率的に保護する
- アプリケーションに変更を加える必要はありません
- プレゼンテーション層で操作する
以下のどの手法を用いるべきでしょうか？
A. マスキング
B. ステガノグラフィー
C. アルゴリズム
D. ランダム置換
正解: (正解を表示します)
Dynamic data masking works at the presentation layer, sitting between your database and application-and transforms sensitive fields (for example, showing "J*** S****" instead of "John Smith") without altering the underlying data or touching the application code. This approach efficiently protects production systems, requires no changes to the application, and enforces masking policies in real time.

質問: **142**
システムエンジニアは、リモートワークのみの従業員向けにSaaSアプリケーションを使用する企業向けにSSOを設定しようとしています。SaaSアプリケーションにおける特権操作は、最低限のセキュリティ要件を満たす社内モバイルデバイスからのみ許可する必要がありますが、その他のアクティビティについてはBYODも許可する必要があります。この目的に最も適した方法は次のうちどれですか？
A. 企業のネットワーク セキュリティ境界外からの接続をすべてブロックします。
B. 企業のデバイスにマシン証明書をインストールし、クライアントに対してチェックを実行します。
C. デバイスの認証と継続的な承認制御を構成します。
D. 企業のクラウドベースの MDM ソリューションを使用して、アプリケーション保護ポリシーを展開します。
正解: (正解を表示します)
Device attestation ensures that only corporate-approved devices can perform privileged actions in SaaS applications. Continuous authorization monitors ongoing device compliance, dynamically adjusting permissions based on security posture.

質問: **143**
ウェブサイトの脆弱性スキャンを実行したところ、次の暗号化スイートが見つかりました。


次のアクションのうちどれが脆弱性を修正しますか?
A. 暗号ブロック連鎖を利用した暗号を削除する
B. 暗号の順序を最強から最弱に並べ替える
C. Webトラフィックを監視するためのWAFの導入
D. ウェブサイトの新しいSSL証明書を再発行する
正解: (正解を表示します)
Cipher suites that use CBC (Cipher Block Chaining), such as

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 and
TLS_RSA_WITH_AES_128_CBC_SHA, are vulnerable to padding oracle and related attacks.
Removing CBC-based ciphers ensures only modern and secure cipher suites (e.g., GCM, ChaCha20) are used, remediating the vulnerability.

質問: **144**
ある組織は、ランサムウェア攻撃への備えが不十分であると判断しました。セキュリティ管理者は、組織のランサムウェア攻撃への対応を改善し、監視する方法を検討しています。管理者が取るべき最善の行動は次のうちどれでしょうか？
A. バックアップテストを実施する。
B. 回復目標点を定義する。
C. 事業影響分析を実施する。
D. 暗号化キーの長さを確認します。
正解: **A (**コメントを発表する**)**
Conducting backup testing is the best action to take in order to improve preparedness for a ransomware attack. Ensuring that backups are regularly tested and can be restored is crucial to recovering from a ransomware attack. Without reliable backups, a successful recovery from an attack could be delayed or impossible.

質問: **145**
あるホテルチェーンは、顧客が従業員の介助なしに客室のチェックインとチェックアウトを行えるように、POSシステムを導入したいと考えています。これらのシステムは、実行が承認された特定のプログラムへのアクセスを制限し、その他のプログラムはすべてブロックする必要があります。この目標を最も効果的に達成するために、同社は次のうちどれを設定すべきでしょうか？
A. 新規イメージを使用したアプリケーション制御。アプリケーションは完全に構成されており、ベースラインとして構築され、他のアプリケーションの実行をブロックします。
B. システム上で発生した疑わしいアクティビティをすべて監視およびブロックするホストベースの侵入検知システム
C. これらのシステムではマルウェア対策ソフトが無効になっており、承認されたアプリケーションファイルの場所のみがバイパスされます。
D. すべてのセキュリティイベントと一部のカスタムアプリケーションログについて、システムからイベントログを収集します。
正解: **(**正解を表示します**)**
Application control using a baseline image ensures only pre-approved programs are allowed to run, effectively blocking all others. This is the best approach for restricting point-of-sale systems to specific functions and maintaining system integrity in an unattended environment.

質問: **146**
ベンダー評価の際、アナリストは監査レポートに含まれる補完的なユーザーエンティティ制御の一覧を確認します。セキュリティチームとこの一覧を確認する際に、最も重要な考慮事項は次のうちどれですか？
A. 組織はユーザーエンティティ制御をどのように実装し、監視するのか
B. CSPがユーザーエンティティに代わって制御を実行する方法
C. 組織は、CSPによるユーザーエンティティ制御の実行をどのように監視すべきか
D. ユーザーエンティティがCSPのユーザーエンティティ制御の実装をどのように監査するか
正解: **A (**コメントを発表する**)**
User entity controls are responsibilities that must be implemented by the organization, so determining how to implement and monitor them is critical.
Monitoring the CSP or auditing their implementation pertains to the CSP's responsibilities, not complementary user entity controls.

質問: **147**
最近、ユーザー認証に関するセキュリティインシデントがいくつか発生しました。セキュリティチームは、以下の点を確実にするための技術的な対策を実施する必要がありま

す。
ユーザーアカウントは不正アクセスが困難です。
-特定の認証情報は、特定のアプリケーションでのみ使用されます。
ユーザーは、特定の用途に指定された機能のみを実行できます。
役割。
パスワードはユーザー認証に必要な唯一の要件ではありません。
セキュリティチームは、組織全体でロールベースのアクセス制御とパスワードの複雑性要件を有効にしました。セキュリティチームは、以下の追加措置のうちどれを講じる必要がありますか？(2つ選択してください。)
A. MFAを有効にします。
B. 強制アクセス制御を有効にする。
C. パスワードの長さは15文字以上である必要があります。
D. 特権アクセス管理システムを実装する。
E. OAuthを有効にする。
F. ログイン失敗をネットワーク全体でログに記録することを必須とする。
正解: **(**正解を表示します**)**
Enable MFA: Multi-factor authentication ensures that passwords alone are insufficient to compromise accounts, directly satisfying the requirement that credentials can't be the only factor for authentication.
Implement a PAM system: A Privileged Access Management solution enforces just-in-time, just- enough access for high-risk credentials and applications, ensuring those credentials are only used for their designated systems and functions. This also dovetails with RBAC to tightly control role permissions for sensitive accounts.

質問: **148**
クラウドエンジニアは、メールの認証をサポートし、メールセキュリティ情報をサードパーティプラットフォームに送信してさらに分析できるように、メールセキュリティプロトコルを設定したいと考えています。これらの要件を満たすために、次のうちどれを設定する必要がありますか？(2つ選択してください。)
A. DMARC
B. DKIM
C. TLS
D. SPF
E. DNSSEC
F. MX
正解: **(**正解を表示します**)**
DKIM (DomainKeys Identified Mail) adds a cryptographic signature to outbound messages, ensuring recipients can verify they haven't been tampered with and truly originated from your domain.
DMARC (Domain-based Message Authentication, Reporting & Conformance) leverages both DKIM (and SPF) to validate incoming mail and critically provides reporting ("rua"/"ruf" tags) so you can forward delivery, failure, and forensic data to any third-party analytics or threat-intel platform.

質問: **149**
同業他社を標的としたマルウェア攻撃の報告を受け、ある組織は、自社のシステムが同様の攻撃の影響を受ける可能性があるかどうかを判断するために、包括的なIoC(侵害指標)リストを作成したいと考えています。このリストを作成するのに最適なツールは次のうちどれでしょうか？
A. シミュレーター
B. 砂場爆発

C. アンチウイルス
D. エンドポイント検出と応答
正解: **B (**コメントを発表する**)**
By detonating threat samples in a sandbox environment, you can safely execute the malware and extract a full spectrum of indicators of compromise - file and payload hashes, dropped filenames and registry keys, network IOCs (domains, IPs, URLs), mutex names, and more. These artifacts form a comprehensive IoC list you can then feed into your monitoring tools (EDR, SIEM, firewalls) to hunt for and block any matching activity across your environment.

質問: **150**
ギャップ分析の結果、ある組織はBYOD(私物端末の業務利用)が重大なリスクであると判断しました。組織はBYODの使用を禁止する管理ポリシーを導入しましたが、組織のリソースへのアクセス時にBYOD資産が不正に使用されることを防ぐための技術的な対策は実施していません。BYODデバイスのリスクを最も効果的に軽減するために、組織は以下のどの対策を実施すべきでしょうか？(2つ選択してください。)
A. クラウドIAMでトークンベースのMFAの使用を強制
B. 条件付きアクセス、ユーザーとデバイスのバインディングを強制する
C. NAC、デバイス構成要件を強制する
D. PAM。ローカルパスワードポリシーを適用します。
E. SD-WAN。外部プロキシを介してWebコンテンツフィルタリングを強制する。
F. DLP(データ保護機能の強化)
正解: **B,C (**コメントを発表する**)**
Conditional access allows the organization to restrict access based on device trust, enforcing user-to-device binding and blocking unauthorized BYOD devices.
Network Access Control (NAC) ensures only compliant and authorized devices can connect to the network, enforcing security configurations and reducing BYOD risks.

質問: **151**
ある組織の取締役会は、最高情報セキュリティ責任者に対し、第三者管理プログラムの構築を依頼しました。この依頼の理由として最も適切なのは次のうちどれですか？
A. リスク移転
B. サプライチェーンの可視性
C. サポートの可用性
D. 脆弱性管理
正解: **(**正解を表示します**)**
A third-party management program is typically designed to manage the risks associated with external vendors, partners, or service providers. One of the key goals of such a program is to ensure supply chain visibility. This means the organization wants to understand and manage the risks posed by third parties in its supply chain, including security risks, compliance issues, and the overall integrity of its external relationships.
By implementing a third-party management program, the organization can monitor and assess the security posture of its vendors, ensuring that they align with the company's risk management practices and that the supply chain remains secure.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**

インフラ最適化計画の一環として、ある企業は統合アーキテクチャから地域ごとに分割されたフェデレーションアーキテクチャに移行しました。長年勤務している従業員は以前よりも快適な環境で業務を行えるようになりましたが、新規採用の従業員は地域間を移動する際に深刻なパフォーマンスの問題に直面しています。同社は以下の情報を精査しています。

Date and time	Region	Employee	System	Status
1/25/2024 8:00 a.m.	Americas	1	Building	Access granted
1/25/2024 8:05 a.m.	Americas	1	EMP1-LT	Log-in success
1/25/2024 4:55 p.m.	Americas	1	EMP1-LT	Log-out success
1/26/2024 9:00 a.m.	Europe	1	Building	Access granted
1/26/2024 9:15 a.m.	Europe	1	EMP1-LT	Log-in success
1/26/2024 4:55 p.m.	Europe	1	EMP1-LT	Log-out success

Date and time	Region	Employee	System	Status
1/25/2024 8:00 a.m.	Americas	2	Building	Access granted
1/25/2024 8:05 a.m.	Americas	2	EMP1-LT	Log-in success
1/25/2024 4:55 p.m.	Americas	2	EMP1-LT	Log-out success
1/26/2024 9:00 a.m.	Europe	2	Building	Access denied
1/26/2024 9:01 a.m.	Europe	2	Building	Access denied
1/26/2024 9:02 a.m.	Europe	2	Building	Access denied

CompTIA
jpnshiken.com

以下のうち、この問題を解決するために最も効果的な対策はどれですか？

A. 影響を受ける従業員のために、影響を受ける領域に新しいユーザーエントリを作成します。
B. 全地域のユーザーIDを同期し、継続的な同期を確保する
C. 欧州地域の物理アクセス制御システムの再起動
D. シングルサインオンアプリケーションと接続されたセキュリティ機器との再同期

正解: **B** (コメントを発表する)

The performance issues for new employees traveling between regions are likely due to identity management inconsistencies in the federated architecture. Synchronizing user identities across regions ensures that user credentials are up-to-date and available in all regions, improving performance and access reliability when employees travel between regions.

質問: **153**

セキュリティ アナリストが SIEM を確認して、次のレポートを生成します。

Log source	Destination IP	Source IP	Hostname	Event ID	Action	Time
DEV001	192.168.1.2	192.168.2.2	VM001	9928	Deny connection	4:55:28
DEV001	192.168.3.2	192.168.2.2	VM001	1912	IPS Alert	7:21:41
DEV001	10.1.1.1,192.168.2.2,VM001,1822 Malware detection,8:11:12					
DEV001	10.1.1.1	192.168.2.2	VM001	9927	Allow connection	8:15:32

その後、インシデント対応チームはVM001ホストへの攻撃が実行されたことを検知しました。SIEMプラットフォームのアラートプロセスを強化するために、セキュリティアナリストは次のうちどれを行うべきでしょうか？

A. EDR ソリューションを SIEM に新しいログ ソースとして含めます。

B. SIEM ソリューションでログ相関を実行します。

C. SIEM 上のデータの解析を改善します。

D. マルウェアを検出するための新しいルール セットを作成します。

正解: **(**正解を表示します**)**

The logs show related events (e.g., malware detection, IPS alert, and eventual connection allowance) from the same source and host. Log correlation connects these related events across time to generate meaningful, actionable alerts. Enhancing correlation would have helped detect the attack pattern earlier.

質問: **154**

セキュリティアナリストは、以前の通信なしでフィッシング攻撃を送信するメールドメインがメールボックスに配信されないようにする必要があります。次のメールヘッダーがレビューされています。

Date	Sending domain	Reply-to domain	Subject
April 16	sales.com	sales-mail.com	Updated Security Questions
April 18	vendor.com	vendor.com	New Sales Catalog
April 18	partner.com	partner.com	B2B Sales Increase
April 19	hr-saas.com	hr-saas.com	Employee Payroll Update Request
April 19	vendor.com	vendor.com	Password Requirements Not Met

セキュリティアナリストが取るべき最善のアクションは次のどれですか?

A. hr-saas.com は認識されたドメインではないため、この com からのメッセージをブロックします。

B. 異常なセキュリティ警告通知を含むすべてのメッセージをIT管理者に転送します

C. メールヘッダーにsales-mail.comが含まれるすべてのメッセージを隔離する

D. 疑わしいメッセージを繰り返し送信しようとするベンダーのcomをブロックします

正解: **(**正解を表示します**)**

The email with the "sales-mail.com" domain stands out, as it is a suspicious "reply-to" domain that is different from the sending domain. This inconsistency could be indicative of phishing attempts. Quarantining these emails ensures they are reviewed before being delivered, helping mitigate potential risks without blocking legitimate communications from

the recognized sales domain.

質問: **155**
病院の警備チームは、患者が画面に表示されているものを見ないようにするため、従業員用モニターの向きを変えるようにロビーを再設計することを提案しました。このチームが対処しようとしている可能性が最も高い懸念事項は次のうちどれでしょうか？
A. 状況認識
B. 社会工学
C. プライバシー
D. 物理的セキュリティ
正解: (正解を表示します)
Reorienting employee monitors prevents patients or visitors from viewing sensitive information displayed on screens. In a hospital environment, this protects confidential patient data and other sensitive information from unauthorized observation. This control addresses privacy concerns by reducing the risk of visual exposure of protected information.

質問: **156**
エンジニアがレガシーコードを最新のアプリケーションに手動で統合する際に、以下の部分が表示されます。

```
..] ...
02] int len = 20;
03] char destination[len];
04] if (strlen(source) > 8) {
05]   strcpy(destination, source);
06] } else {
07]   printf("Error: Too short.\n");
08] }
..] ...
```

エンジニアは、以下の関数または式のどれを修正すべきでしょうか？
A. Line [03];
String destination[len];
B. Line [03];
char source[20];
C. Line [04];
if (sizeof(source) > 8)
D. Line [04];
Remove if-else clause
E. Line [05];
snprintf (...);
F. Line [05];
memcpy(...);
正解: (正解を表示します)
The unsafe operation is the unbounded copy performed by strcpy(destination, source). This can overflow the destination buffer if the source string is larger than the available space, regardless of the length check shown. Replacing that copy with snprintf(...) adds an explicit size boundary and ensures the write stays within the destination buffer, which is the appropriate secure modification when integrating legacy code into a modern application.

質問: **157**

最新およびレガシーの金融アプリケーションを混在させたサービスを提供するWebアプリケーションサーバーで、OpenSSLを含む共通ライブラリの更新を目的とした定期アップグレードが先日実施されました。複数のユーザーからサーバーへの接続試行に失敗したとの報告が寄せられています。初期トリアージを担当した技術者は、以下の点を確認しました。
* 5 年以上経過したクライアント アプリケーションが最も影響を受けるようです。
* Web サーバーのログには、影響を受けるホストによる最初の接続試行が表示されます。
* 失敗した接続については、ログに 暗号が利用できません」と表示されます。
この状況を安全に改善できる可能性が高いのは次のどれですか?
A. サーバーは、SSL 3.0 アプリケーションとの下位互換性を保つように構成する必要があります。
B. Galois/Counter モードまたは同等の AES をサポートするようにクライアント アプリケーションを変更する必要があります。
C. 電子コードブックの動作モードを強制するには、クライアントの TLS 構成を設定する必要があります。
D. 楕円曲線暗号をサポートするには、サーバー側のデジタル署名アルゴリズムを変更する必要があります。
正解: **(**正解を表示します**)**
The error "cipher unavailable" suggests that the upgraded OpenSSL library on the server has dropped support for older, insecure cipher suites. To safely remediate this, client applications need to be updated to support modern, secure cipher modes such as AES in Galois/Counter Mode (GCM). This maintains security without reintroducing deprecated protocols.

質問: **158**
ITチームは、アカウントがロックアウトされているという従業員からの報告を受けました。アナリストは、会社がオフィスを構えていない国からブルートフォース攻撃が行われていることを確認しました。この問題に対処するのに最適なソリューションは次のうちどれですか？
A. ユーザーアカウントへの条件付きアクセス
B. ログイン失敗回数の上限を解除する
C. すべてのアプリケーションでSSOを実装する
D. 60日ごとにパスワードのローテーションを強制する
正解: **(**正解を表示します**)**
Conditional access policies allow authentication attempts to be restricted based on contextual factors such as geographic location, device posture, and risk signals. By blocking or requiring additional verification for logins originating from countries where the organization does not operate, the system can prevent or significantly reduce brute-force attempts coming from those regions while allowing legitimate access for authorized users.

質問: **159**
ある企業は、ソフトウェア開発ライフサイクルにおけるセキュアコーディングの実践を改善し、より優れたセキュリティ基準を導入するための新たなロードマップを策定する必要があります。この目標を達成するための最善の方法は次のうちどれでしょうか？
A. ソフトウェア保証成熟度モデルの評価を実施し、最終結果としてロードマップを作成する。
B. 主要アプリケーションに対する脅威モデリング演習を実施し、必要なセキュリティ実装に基づいたロードマップを作成する
C. 最高情報セキュリティ責任者が定義したセキュリティ分野のロードマップと年間目標に基づき、セキュアコーディングのベストプラクティスを含む新たなロードマップを作成する。
D. OWASPセキュアコーディングマニュアルのベストプラクティスを用いて、新たなロードマップを策定する
正解: **A (**コメントを発表する**)**
Performing a Software Assurance Maturity Model (SAMM) assessment provides a structured way to evaluate current secure software practices and generate a tailored improvement road map. It aligns well with the goal of enhancing secure coding practices and implementing better security standards across the SDLC.

質問: **160**

システム管理者は、社内のAIベースのツールを使用して、APIを使用して社内サービスに接続するコードを生成します。コードのテスト後、システム管理者はAPIを使用してデータを収集し、社内システムに送信します。最高情報セキュリティ責任者は、セキュリティエンジニアにシステム管理者のプロセスをレビューするように依頼しました。セキュリティエンジニアは、次のうちどれを最初に行うべきでしょうか？
A. アプリケーションのソースコードにハードコードされた秘密情報がないか確認します。
B. モデルのセキュリティを確保するために、迅速なテスト手法を使用する。
C. 管理者が使用したAIツールの有効性をレビューする。
D. 出力生成に使用された大規模言語モデルを分析します。
正解: **(**正解を表示します**)**
When reviewing generated code that interacts with APIs and posts data to internal services, the first security check should be for hard-coded credentials such as API keys, tokens, or secrets embedded in the source code. AI-generated code commonly includes sensitive values directly in the code during examples or testing, which can expose credentials and allow unauthorized access to internal systems. Identifying and removing embedded secrets is the most immediate and critical security validation step before evaluating the AI tool or model used to generate the code.

質問: **161**
組織は、外部の要件に従ってシステムとデータを分類する必要がある。
このタスクを実行するのに最も適した役割は次のうちどれですか？
A. システム管理者
B. データ所有者
C. データプロセッサ
D. データ管理者
E. データスチュワード
正解: **(**正解を表示します**)**
The Data owner is the role best qualified to classify systems and data according to external requirements. The data owner is responsible for the oversight of data assets within the organization, including determining how data is classified and ensuring that it meets relevant regulatory or compliance standards. This role involves setting policies and guidelines for data usage, classification, and security.

質問: **162**
ある組織が、その組織が使用するウェブサーバーアプリケーションのインスタンスを標的とする外国の敵対勢力に関する情報を受け取った。その情報には以下の内容が含まれる。
攻撃の発信元IPアドレス
- 影響を受けるデバイス上で共通コマンドが実行されます
- デバイスが影響を受けたことを示す指標
- デバイス上で攻撃を阻止するために実行できる対策
組織はまず、次のうちどれを行うべきでしょうか？
A. インシデント対応プレイブックを作成する
B. 戦術、技術、手順を構築する
C. SnortとYARAのルールを作成する
D. ユーザー行動分析の設定
正解: **C (**コメントを発表する**)**
The intelligence already provides actionable indicators such as attacker IP addresses, commands used, signs of compromise, and remediation steps. The first step is to operationalize this intelligence for detection by creating IDS and malware detection signatures. Snort rules can detect network activity from the known attacker infrastructure and

command patterns, while YARA rules can identify malicious artifacts or behaviors on affected systems. This enables immediate detection and monitoring for the described attack.

質問: **163**
現在、ある企業は勤務時間外に発生するインシデントへの対応を、手作業によるプロセスで行っている。予算上の制約から、SOC(セキュリティオペレーションセンター)の設置や人材採用は選択肢にない。
以下の解決策のうち、現在のリスクを最も効果的に低減できるのはどれでしょうか？
A. ファイアウォールと統合されたNIPSを実装し、外部境界からの悪意のあるアクセス試行をブロックするための新しいルールを作成します。
B. 適切なランブックを設計し、統合されたセキュリティツールを使用してセキュリティオーケストレーションと自動化を実装します。
C. ログ記録機能を改善し、それらのログを既存のSIEMと統合し、より優れたセキュリティダッシュボードを作成します。
D. 攻撃の試みを防止するために、新しいエンドポイントセキュリティツールを評価し、導入する。
正解: **B (**コメントを発表する**)**

質問: **164**
コンプライアンスマネージャーは、環境におけるリスクを特定するための取り組みを計画しています。マネージャーは、重要な資産やプロセス、潜在的な障害点の特定など、取り組みの重要な側面について事業部門のリーダーと話し合いたいと考えています。これらの話し合いの中で、以下のうちどれが最も重要でしょうか？
A. サブプロセッサのリスク
B. リスク受容基準
C. 修復戦略
D. リスク選好度とリスク許容度
正解: **(**正解を表示します**)**
During risk identification discussions with business unit leaders, understanding the organization's risk appetite and tolerance is essential. These define how much risk the organization is willing to accept in pursuit of its objectives and help guide which assets, processes, and potential failure points are considered most critical. This context allows the security team to prioritize risks appropriately and align the engagement with the organization's strategic risk management expectations.

質問: **165**
ある企業が、インバウンド接続に関連する不審なアクティビティを検出しました。セキュリティ検出ツールではこのアクティビティを分類できません。この課題を克服するために、企業が最適なソリューションは次のうちどれですか？
A. インタラクティブなハニーポットを実装します。
B. ネットワーク トラフィックを既知の IoC にマップします。
C. ダークウェブを監視します。
D. UEBA を実装します。
正解: **(**正解を表示します**)**
An interactive honeypot can actively engage with suspicious inbound connections, capturing detailed attacker behavior and tactics, which helps identify and categorize unknown or ambiguous threats more effectively.

質問: **166**
ある企業が、自社のウェブサイトに関して顧客から複数の苦情を受けています。エンジニアは、ウェブサーバーのログを解析するパーサーを実装し、次のような出力を生成します。

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

jpnshiken.com CompTIA

問題を最も効果的に解決するために、会社が実施すべきは次のどれですか?

A. IDS

B. CDN

C. WAF

D. NAC

正解: **B (**コメントを発表する**)**

To improve global response times (e.g. India/Australia seeing multi-second load times) and offload traffic from your origin web servers, deploying a Content Delivery Network is the most effective solution.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**

侵入テスト担当者が、Webアプリケーションで予期しない動作を引き起こす状況を発見した。

これにより、インタープリタのデバッグ情報がダンプされます。これには、インタープリタのバージョン、バイナリファイルのフルパス、およびプロセスを実行しているユーザーIDが含まれます。このリスクを最も効果的に軽減できる対策は次のうちどれですか？

A. アプリケーションにメッセージ処理ルーチンを含める。

B. コンパイル型プログラミング言語を採用する。

C. すべてのビルドに対してSAST脆弱性スキャンを実行します。

D. ユーザーが入力した内容を検証します。

正解: **(**正解を表示します**)**

By implementing structured error-handling routines (e.g., try/catch blocks with generic user-facing error messages and internal logging of detailed debug information), you prevent the application from exposing sensitive interpreter details to end users. This practice ensures that, even when an unexpected condition occurs, only a sanitized error page is shown, mitigating information-leakage risks at their source.

質問: **168**

ダム・バルメーカーの主席セキュリティアナリストが、ICSネットワークにおける異常動作に関連するセキュリティインシデントを調査している。トラブルシューティングの一環としてコントローラが再起動され、その際に以下の問題が特定された。

セキュアブートに失敗しました。

ファームウェアの不一致 期待値 :UXFDC479 実際値 :0x79F31B

調査の結果、この改変されたファームウェアバージョンが、現場の他の複数のコントローラでも確認されました。公式ベンダーのファームウェアバージョンには、このチェック

サムは含まれていません。MITRE ATT&CKフレームワークのICS向けステージのうち、この手法が含まれるのはどのステージでしょうか？
A. 回避
B. 持続性
C. コレクション
D. 横方向の動き
正解: (正解を表示します)
The technique described in the scenario, where modified firmware with an altered checksum is found on multiple controllers, aligns with the Persistence stage of the MITRE ATT&CK framework for ICS (Industrial Control Systems). Persistence involves ensuring that an adversary can maintain access to a system even after reboots, credential changes, or other defensive measures. The manipulation of firmware is a classic method used by attackers to ensure that they can maintain control over a system or device across reboots or resets, which is a key characteristic of the Persistence stage.

質問: **169**
ある企業が最近、製造工場を買収しました。買収企業は、セキュリティ体制に影響を与えない統合ネットワークの構築を計画しています。この製造工場は30年以上稼働しており、設備のライフサイクルに応じた交換を行っていません。この目的を達成するための最適な方法は次のうちどれでしょうか？
A. WAFの実装とレガシーIT機器のパッチ適用
B. 特定のポリシーでSD-WANを拡張する
C. サイト間VPNを使用し、製造工場をSIEMに統合する
D. 製造工場にプロキシサーバーを導入する
正解: (正解を表示します)
The best answer is B because the question asks for a way to create a unified network while not weakening the acquiring company's security posture. In CompTIA SecurityX CAS-005, SD-WAN is explicitly part of Security Architecture, under "Deperimeterization: SASE, SD-WAN, and software-defined networking." The same official objective set also lists "Network architecture:
segmentation, microsegmentation, VPN..." and "Security boundaries... secure zones." Those objective areas support a policy-based integration approach in which the plant can be connected while maintaining segmentation, security zones, and centralized enforcement.
This is especially important because the manufacturing plant is old and has not followed an equipment refresh life cycle. That strongly suggests there may be legacy systems, operational technology, and devices that cannot be rapidly modernized or patched. A policy-driven SD-WAN design is more effective than simply connecting the site because it allows the acquiring company to preserve trust boundaries and apply differentiated controls to plant traffic. That aligns directly with CompTIA's official SecurityX emphasis on segmentation, secure zones, and deperimeterization technologies.

質問: **170**
セキュリティアナリストは、静的アプリケーションのセキュリティレビューを実施する必要があります。このアプリケーションは、主に公開されているオープンソースモジュールで構成されています。アナリストは、以下の表をレビューします。

Application	Module use	Module age
SalesForecastingWebApp	Encryption	38 days
SalesForecastingWebApp	Sending email	492 days
SalesForecastingWebApp	Input sanitization	203 days
SalesForecastingWebApp	Chatbot	39 days

セキュリティアナリストが最も推奨する可能性が高い対策は次のうちどれでしょうか？
A. クロスサイトスクリプティングをブロックするためのWAFのインストール
B. すべてのWebクライアント接続に対してTLSを設定する
C. 独自モジュールへの移行

D. 脆弱なサードパーティ製ソースコードの更新
正解: (正解を表示します)
The table shows that some open-source modules, such as the email module (492 days old) and input sanitization module (203 days old), are outdated. The most effective mitigation is to update vulnerable third-party source code to the latest secure versions, reducing exposure to known vulnerabilities.

質問: **171**
セキュリティアーキテクトは、DevSecOpsおよびSOARイニシアチブのためにコンテナオーケストレーターを有効にする必要があります。エンジニアは、構成管理の自動化に使用されるいくつかのAnsible YAMLファイルに次の内容が含まれていることを発見しました。

```
 hostnamectl
OMPTIA001

 cat /etc/ansible/ansible.cfg
inventory]
nable_plugins = kubernetes.core.k8s

 cat /etc/ansible/projects/roles/k8/default/main.ym
--
 Name: Create a Kubernetes Service Objects
 kubernetes.core.k8s:
   state: present
   definition:
        apiVersion: v2
        kind: Service

 cat /etc/kubernetes/manifests
```

jpshiken.com
CompTIA

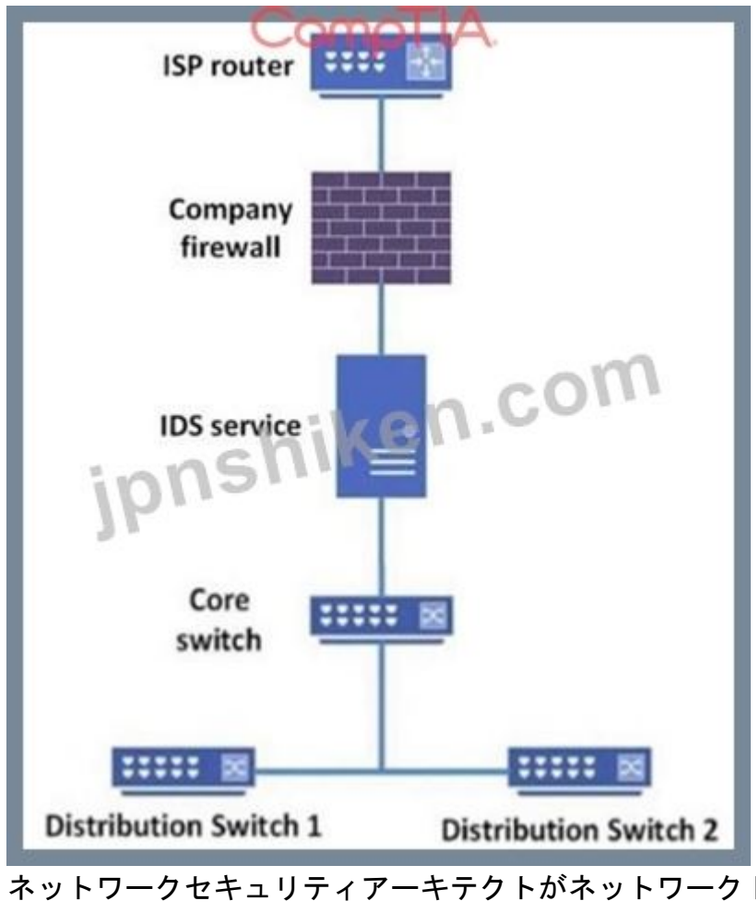
このコンテンツに含まれるセキュリティ上の問題を修正するために、エンジニアは以下のうちどれを行うべきでしょうか？
A. main.ymlファイルでkubernetes.core.k8smoduleをkubernetes.core.k8s_serviceに更新します。
B. hostnamectlコマンドを使用してCOMPTIA001ホスト名をlocalhostに更新します。
C. main.ymlファイルでstate: presentmoduleをstate: absentに更新します。
D. ansible.cfg ファイルを更新または削除します。
E. マニフェストファイル内の insecure-bind-address を localhost から COMPTIA001 に更新します。
正解: (正解を表示します)
The Ansible configuration file (/etc/ansible/ansible.cfg) contains an enable_plugins directive that allows Kubernetes modules to interact with Kubernetes resources. However, it does not enforce secure practices for managing these interactions, which could potentially expose sensitive data or allow unauthorized changes if not correctly configured or overly permissive.
The insecure configuration in the Ansible YAML file or the ansible.cfgfile should be reviewed or updated to enforce stricter security. Specifically, the configuration might inadvertently expose Kubernetes services to untrusted sources, and enabling plugins like kubernetes.core.k8s without sufficient control could lead to vulnerabilities.
Updating or removing the ansible.cfgfile ensures that secure defaults are applied, or more secure plugin configurations can be explicitly added, addressing the underlying issue.

質問: **172**
セキュリティ担当者は、特別プロジェクトに従事する全職員に対し、アクセスするすべての情報のレベルに応じたセキュリティクリアランスの取得を義務付けています。このネットワーク上のデータは、各クリアランス保持者と同じレベルで保護されなければなりません。また、情報へのアクセスの必要性は、データ所有者によって検証される必要が

あります。セキュリティ担当者は、これらの要件を満たすために、次のうちどれを行うべきでしょうか？
A. 特定のIPアドレスからの担当者のみがファイルにアクセスできるようにするルールを作成します。
B. ファイルにラベルを付け、正式なアクセス承認を要求する。
C. 各ファイルに属性を割り当て、承認されたユーザーがファイルを共有できるようにします。
D. ユーザーに役割を割り当て、役割に基づいてファイルへのアクセスを許可します。
正解: **(**正解を表示します**)**
To meet the requirement of ensuring that data is protected at the clearance level of each personnel member and that access is based on the need to know, labeling the files according to their classification level is an effective method. Labels indicate the sensitivity of the data and ensure that only individuals with the appropriate clearance and need-to-know access are authorized to view or modify the files.
By requiring formal access authorization from the data owner, the security officer ensures that access is explicitly verified before any personnel can access data at a given classification level.

質問: **173**
ユーザーがヘルプデスクにチケットを送信し、アカウントが時々認証されないという報告を受けました。アナリストは、ユーザーの以下のログを確認します。
ユーザーのアクセスが拒否される理由を最もよく説明するのは次のどれですか?
A. パスワードが正しく入力されていません
B. 時間ベースのアクセス制限
C. アカウントの侵害
D. ユーザーとデバイスのバインドが無効です
正解: **(**正解を表示します**)**
The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non- business hours, reducing the risk of security incidents.

質問: **174**
図に示すネットワークにおいて、ネットワークセキュリティアーキテクトが以下の目的を達成するためにネットワークトラフィックのキャプチャ作業を行っています。
脅威インテリジェンスベンダーと共有するための関連トラフィックを収集する。
- 潜在的なネットワークを示す可能性のあるトラフィックのみを収集する
侵入。
収集した予算とリソースの要件を最小限に抑える
渋滞。



jpnshiken.com

ネットワークセキュリティアーキテクトがネットワークトラフィックをキャプチャする最良の方法は次のうちどれですか？

A. ISPルーターにネットワークタップを設置する
B. コアスイッチでスパンポートを設定する
C. ファイアウォールに透過型プロキシをデプロイする
D. IDSデバイスにネットワークハブを接続する

正解: **(**正解を表示します**)**

Configuring a SPAN (port mirroring) session on the core switch allows the architect to mirror selected network traffic to the IDS service for monitoring and analysis. This approach enables capturing only specific traffic flows relevant to potential intrusion activity by filtering VLANs or interfaces, which reduces the volume of collected data. SPAN functionality is built into most switches, making it a cost-effective solution that minimizes additional hardware and operational resources while still providing visibility into traffic that could indicate network attacks.

質問: **175**

ある企業が、セキュリティ責任者(CISO)が関連する法令遵守規則を調査する必要のある新しいサービス製品を開発しています。以下のうち、CISOの行動を最も適切に表しているのはどれですか？

A. データ保持
B. データ分類
C. デューデリジェンス
D. 参照フレームワーク

正解: **(**正解を表示します**)**

Due diligence involves investigating and verifying processes, regulations, or environments to ensure compliance with laws and standards.

質問: **176**
DevOps エンジニアが、Kubernetes の本番環境にアプリケーション コンテナ イメージをデプロイするための CI/CD パイプラインを構築します。セキュリティ エンジニアは、セキュリティ対策が施されていないイメージのデプロイを防止したいと考えています。この目的を達成するために、エンジニアはパイプライン内で以下のどのセキュリティ ソリューションを使用すべきでしょうか？
A. 脆弱性スキャン
B. 静的コード解析
C. 信頼できる証明
D. プライベートリポジトリ
正解: **(**正解を表示します**)**
Trusted attestation ensures that only container images meeting defined security and integrity requirements are allowed in the pipeline. This prevents the deployment of unsecured or tampered images into the Kubernetes production environment.

質問: **177**
サイバーセキュリティインシデント発生後、セキュリティアナリストは、攻撃者が侵害されたサーバー上で使用したバイナリを収集することに成功した。その後、アナリストは次のコマンドを実行した。

```
root@kali> strings binary.exe
..........sdfa....as.d.as
...s...2.3.3.1..5..6.6.....>@34..4.....133
.....http://192.168.1.2/?=cmd.exe whoami....
.......ipconfig....5.6.2...g..q23..45.56>56.
..22312....
evil.info......
.....2185ks99//283jf////.....
c:\\windows\\system32\\temps.xml
1.2..34.....e.gt.gv.....5.65.
public\\temps.bin
.........
auy66
Microsoft Windows win32
```

以下の選択肢のうち、アナリストが行おうとしていることを最も適切に表しているのはどれですか？
A. バイナリによって実行されたコマンドのタイムラインを再構築する
B. 攻撃に使用されたバイナリからIoCを抽出する
C. 安全な環境で攻撃を再現する
D. バイナリをデバッグして低レベル命令を解析する
正解: **B (**コメントを発表する**)**
The command strings binary.exeis used to extract human-readable strings from a binary file. This can help the security analyst find indicators of compromise (IoCs), such as IP addresses (e.g., http://192.168.1.2/?=cmd.exe), file paths, and potentially malicious domain names or commands embedded in the binary. This process aids in identifying critical information that can be used for further investigation or remediation of the attack.

質問: **178**
最近のセキュリティ監査に基づき、ある企業は、境界防御戦略が近年の成長に対応できていないことを発見しました。この問題に対処するため、同社は以下の要件を満たすソリューションを求めています。
- 複数のネットワークセキュリティ技術を単一のものに統合
- 異なるセキュリティコンテキストを持つ複数のVPNをサポート
- アプリケーション層セキュリティ(OSIモデルの第7層)のサポート

これらの要件を満たす上で、以下の技術のうちどれが最も適切な解決策となるでしょうか？
A. NATゲートウェイ
B. リバースプロキシ
C. NGFW
D. 巣
正解: **(**正解を表示します**)**
A Next-Generation Firewall (NGFW) consolidates traditional firewall functions (stateful packet inspection, VPN termination) with advanced capabilities such as intrusion prevention, application- layer (L7) inspection, and support for multiple VPN contexts. This single-footprint device can host separate VPN tunnels with distinct security policies while enforcing deep-packet and application- level controls across all traffic.

質問: **179**
セキュリティアナリストが不審なログインアクティビティを調査したところ、SIEMで以下のデータを確認しました。

Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

CompTIA
jpnshiken.com

アナリストが取るべき最も適切な行動は次のうちどれですか？
A. 正しくキャプチャされていないディレクトリサーバーのログ構成設定を更新してください。
B. 管理者アカウントの所有者にパスワードを変更してもらい、クレデンシャルスタッフィング攻撃を防いでください。
C. 従業員が自分の業務領域外のアプリケーションにログインできないようにする。
D. 高リスクな活動に関連付けられたアカウントを無効にする自動化を実装します。
正解: **(**正解を表示します**)**
The ADMIN account is showing a failure to authenticate on LDAP-US and a high-risk level, which is a cause for concern. The most appropriate action would be to implement automation to disable accounts that have been associated with high-risk activity (like this one). This helps prevent further misuse or potential attacks using compromised credentials.

質問: **180**
ある企業が、Webアプリケーションの新しいバージョンを本番環境に移行する準備を進めています。CI/CDパイプラインにおけるセキュリティスキャンや品質保証の過程で、重大な問題は報告されていません。この企業は次に、次のうちどの行動を取るべきでしょうか？
A. テストブランチをメインブランチにマージします。
B. 本番環境アプリケーションに対して脅威モデリングを実施する。
C. 提出されたコードに対して単体テストを実施します。
D. テストブランチに対してピアレビューを実施する。
正解: **(**正解を表示します**)**
A peer review is the essential next step once automated scans and QA pass but before merging or deploying code. It brings human insight to catch logic flaws, security oversights, or architectural issues that tools may miss. Conducting the review on the test branch ensures feedback can be addressed without impacting the main branch or

production timeline.

質問: **181**
他の暗号化方式と比較した場合、準同型暗号化の利点を最もよく表しているのは次のうちどれですか？
A. 高度なハッシュルーチンによってデータの整合性が保護されています。
B. フィールド固有のトークン化のサポートが追加されました。
C. 事前共有キーは不要になります。
D. 資源利用率が低い。
正解: **(**正解を表示します**)**

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
ある企業では、他のシステムと比較してタイムスタンプが変更されたログを発見しました。セキュリティチームは、インシデント対応のためのログ記録と監査を改善することを決定しました。この目標を最も効果的に達成するために、セキュリティチームは以下のどれを実施すべきでしょうか？
A. ファイル監視ツールを SIEM と統合します。
B. ログ ソリューションを変更し、既存の SIEM と統合します。
C. ログの取り込みのみを許可する中央ログサーバーを実装します。
D. 24 時間ごとにログをローテーションしてバックアップし、バックアップを暗号化します。
正解: **(**正解を表示します**)**
A central logging server ensures logs are collected in a tamper-proof manner and only ingested (not modified). This prevents attackers from altering logs locally.
Key concepts: Logs should be centrally stored to prevent tampering. Enabling log forwarding to a secure SIEM improves integrity.

質問: **183**
セキュリティエンジニアは、開発者エンドポイントとクラウドプロバイダーのデータストレージバケット間のアクセスを制限する制御を実装する必要があります。開発者はプロジェクトの一環として、機密ファイルを日常的にバケットに保存します。セキュリティエンジニアは、意図しないデータ漏洩のリスクを低減しなければなりません。
以下のうち、最も適切な対策はどれですか？
A. クラウドプロバイダーのKMSを使用したサーバー側暗号化を必須とする。
B. ローカルシステムに対してコンテキスト認識型再認証を実装する。
C. 仮想プライベートクラウドにACLをデプロイして、パブリックアクセスを防止します。
D. プロキシで特定のURLへのHTTP POSTおよびPUTトラフィックを制限します。
正解: **C (**コメントを発表する**)**
Applying an ACL on the virtual private cloud to restrict bucket access ensures that sensitive files are not exposed publicly. This limits access to only authorized endpoints, reducing the risk of unintended data exposure while still allowing developers to use the storage securely.

質問: **184**

セキュリティアナリストは、最新の脆弱性スキャン中に、会社の専用IoTサブネット上に新しいデバイスを発見しました。スキャン結果には、デフォルトのユーザー名とパスワードに加え、多数のオープンポートと安全でないプロトコルが示されています。カメラはIoTサブネット内のセキュリティサーバーにビデオを送信する必要があります。セキュリティアナリストは、カメラを安全に運用するために、次のうちどれを推奨すべきでしょうか？

A. カメラの設定を強化してください。

B. カメラのログをSIEMに送信する。

C. カメラのビデオストリームを暗号化します。

D. カメラを隔離された区画に設置します。

正解: (正解を表示します)

Harden the camera configuration by changing default usernames and passwords, disabling unnecessary open ports, and ensuring that secure protocols (such as HTTPS, SSH, or others) are used instead of insecure ones (like HTTP or Telnet). This is a critical step in securing IoT devices and protecting them from being exploited. Since the camera is part of the IoT subnet and has been identified with vulnerabilities such as default credentials and open ports, hardening the configuration is the most direct and effective solution to secure its operation.

質問: **185**

ある企業は、自社製品の一部であるサードパーティ製ハードウェアデバイスの設定ミスや脆弱性に関する報告を受けました。潜在的な問題を早期に特定するために、企業が最適な解決策は次のうちどれですか？

A. プロバイダーから提供された各デバイスに対して脆弱性テストを実行する

B. ベンダーの生産ラインで定期的なレッドチーム演習を実施する

C. アプリケーションとベンダーアプライアンス間の統合のための監視プロセスの実装

D. 適切なサプライチェーンリスク管理プログラムの実装

正解: (正解を表示します)

Implementing a proper supply chain risk management program is the best way to identify potential issues earlier in the process. This program involves assessing the risks and vulnerabilities of third-party hardware and software during the procurement process and throughout the lifecycle of the product. By establishing a strong risk management framework, the company can proactively detect and address misconfigurations and vulnerabilities before the products are released or deployed.

質問: **186**

レガシーアプリケーションに対するSASTレポートの結果に基づき、セキュリティエンジニアは脆弱性があると指摘された以下のコードスニペットをレビューしています。

```
[01] #include <stdio.h>
[02] #include <string.h>
[03] ...
[04]  char input[256] = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
[05]  ...
[06]  char transmit[20] = "0000";
[07]  char *ret_xmit;
[08]  printf("To be submitted: \"%s\"\n", input);
[09]  result in ret_xmit
[10]  ret_xmit = strcpy(transmit, input);
[12]  return 0;
[13] }
```

変更する必要のある脆弱なコード行は、次のうちどれですか？

A. ライン[02]

B. ライン[04]
C. ライン[07]
D. ライン[08]
E. ライン[10]
正解: **(**正解を表示します**)**
The use of strcpy in line 10 is vulnerable because it does not check the size of the destination buffer, leading to a potential buffer overflow when copying the large input string into the smaller transmit array.

質問: **187**
セキュリティエンジニアは、一部の旧式システムが依然として使用されているか、適切に廃止されていないことを発見した。さらに調査を進めた結果、未知の、潜在的に悪意のあるサーバーが、会社になりすましてメールを送信していることも判明した。
セキュリティエンジニアは、レビューのために以下のデータを抽出します。

Server IP	DNS	Status	Auth. pass rate
200.100.50.25	marketing.company.com	Authorized	97%
200.50.25.10	29mail.mycrosoft.info	Unauthorized	0%
210.20.20.5	mail.google.com	Authorized	100%

セキュリティエンジニアは次に、以下のどの行動を取るべきでしょうか？(2つ選択してください。)
A. DKIMセレクターを回転させて別のキーを使用します。
B. DMARC ポリシーを変更して、サーバーへの参照を拒否し削除します。
C. SPFレコードから不要なサーバーを削除します。
D. SPFレコードを変更して、ハードフェイルパラメータを強制します。
E. MXレコードを更新して、プライマリメールサーバーのみが含まれるようにします。
F. DMARCポリシーを 「なし」に変更し、メールフローを監視して新しいベースラインを確立します。
正解: **B,D (**コメントを発表する**)**
Changing the DMARC policy to "reject" and removing references to the unauthorized server will prevent malicious emails from being delivered, strengthening protection against spoofing.
Enforcing the hard fail parameter in the SPF record ensures that emails from unauthorized servers are rejected, further securing the organization's email infrastructure.

質問: **188**
セキュリティ エンジニアは、コンテナー イメージに対して次の要件を持つ DevOps チームを支援しています。
コンテナ イメージがハッシュ化され、バージョン管理が使用されていることを確認します。
コンテナ イメージが最新であり、脆弱性がスキャンされていることを確認します。
これらの要件を満たすために、セキュリティ エンジニアは次のどれを行う必要がありますか?
A. コンテナ イメージ上でクラスターを有効にし、ACL を使用してメッシュを構成します。
B. CI/CD パイプライン内で新しいセキュリティと品質のチェックを有効にします。
C. コンテナ イメージの監査を有効にし、構成の変更を監視します。
D. ベンダー リポジトリからコンテナ イメージをプルし、直接操作にデプロイできるようにします。
正解: **B (**コメントを発表する**)**
Implementing security and quality checks in a CI/CD pipeline ensures that:
- Container images are scanned for vulnerabilities before deployment.

- Version control is enforced, preventing unauthorized changes.
- Hashes validate image integrity.

質問: **189**
キオスク型ワークステーションを提供する企業が、ワークステーションのセキュリティ実装を改善したいと考えています。同社は、攻撃者が起動プロセス中にワークステーションを制御し、データの流れを変更する可能性があることを懸念しています。以下の解決策のうち、懸念事項に最も適切に対処できるものはどれですか？
A. デジタル署名されたモジュールのみの読み込みを許可する
B. 使用していない接続ポートをすべて取り外す
C. ブートローダーパスワードの作成
D. 特定のオペレーティングシステムのみを許可するように設定
正解: **(**正解を表示します**)**

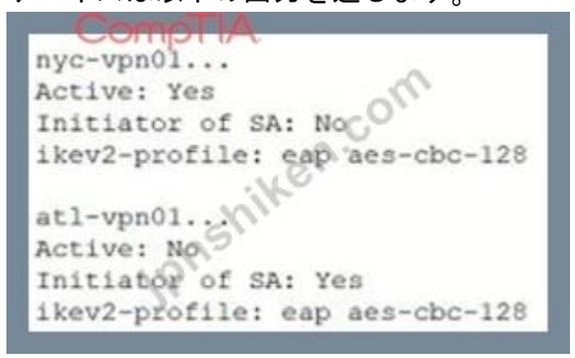
質問: **190**
金融業界の複数の企業が同様の事件の影響を受けた後、脅威インテリジェンスと攻撃に使用されたマルウェアに関する情報を共有しました。これらの攻撃が同一の攻撃者によって行われているかどうかを最も適切に特定するために、企業は次のうちどれを行うべきでしょうか？(2つ選択してください。)
A. 一般的なTTP(戦術、技術、手順)を探します。
B. IoC抽出を使用します。
C. マルウェアの逆コンパイルを実行します。
D. コードスタイロメトリーを適用します。
E. マルウェアのハッシュ値を検証します。
F. マルウェアの爆発を利用する。
正解: **(**正解を表示します**)**

質問: **191**
ある組織は最近、新しいメールDLPソリューションを導入しました。会社のメールアドレスから一致する個人のメールアドレスに送信されたメールは多数のアラートを生成しましたが、メールの内容には会社のデータは含まれていませんでした。セキュリティチームは、一般的な個人用メールサービスへのメールをすべてブロックすることなく、送信されるメールの数を減らす必要があります。セキュリティチームが最初に導入すべき対策は次のうちどれですか？
A. 送信メールを自動的に検疫します。
B. 許容使用ポリシーを作成します。
C. 電子メールの暗号化標準を適用します。
D. フィッシングに焦点を当てたセキュリティ意識向上トレーニングを実施します。
正解: **(**正解を表示します**)**
An acceptable use policy (AUP) defines what is considered appropriate use of corporate email and prevents unnecessary emails to personal accounts. This helps in reducing false DLP alerts while maintaining compliance.

質問: **192**
セキュリティチームは、リターン指向プログラミングを悪用した攻撃が、同社の公開アプリケーションに対して行われていることを懸念しています。同社は、公開サーバーに以下のどの対策を実装すべきでしょうか？
A. エイズ
B. ASLR

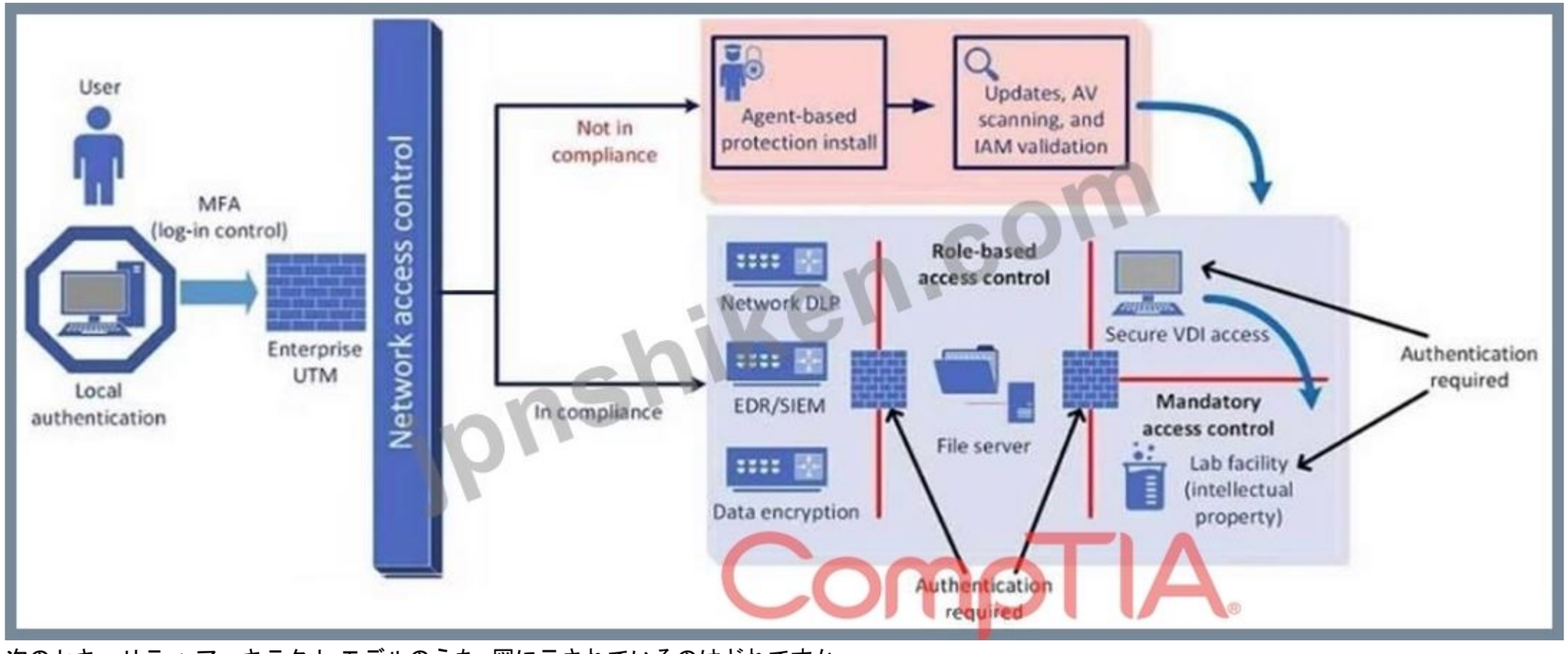
C. TPM
D. HSM
正解: **B (**コメントを発表する**)**
Return-Oriented Programming relies on attackers knowing or predicting the locations of "gadgets" in memory. Address Space Layout Randomization (ASLR) thwarts this by randomly arranging key data areas, like the stack, heap, and loaded libraries, each time a program runs, preventing attackers from reliably chaining gadgets and executing ROP exploits.

質問: **193**
セキュリティエンジニアが、ニューヨーク市とアトランタ間のサイト間VPNの障害をトラブルシューティングしています。このトンネルは、2台のVPNコンセントレータで事前共有キーを使用して構成されています。アトランタサイトは、ニューヨーク市サイトからの接続を常にリッスンするように構成する必要があります。セキュリティエンジニアは、両方のデバイスで次のコマンドを実行します。
暗号化IKE2の詳細を表示
デバイスは以下の出力を返します。



セキュリティエンジニアは、この問題を解決するために、次のうちどの行動を取るべきでしょうか？
A. 暗号スイートをAES256-GCMを使用するように変更します。
B. アトランタ拠点のスタッフに連絡して、VPNコンセントレータを再起動してください。
C. 3つ目のVPNコンセントレータを追加します。
D. ニューヨーク市のサイトをイニシエータとして設定します。
正解: **(**正解を表示します**)**
The output shows that the Atlanta VPN is set as the initiator but is inactive, while the New York City VPN is active but not initiating the Security Association (SA). Since Atlanta is supposed to always listen, the New York City site must be configured as the initiator to establish the tunnel successfully.

質問: **194**
ある企業は、保護されるべき知的財産データを備えた研究施設を実装する計画を立てています。以下は、セキュリティアーキテクトが提案したセキュリティ図です。



次のセキュリティ アーキテクト モデルのうち、図に示されているのはどれですか。

A. アイデンティティとアクセス管理モデル

B. エージェントベースのセキュリティモデル

C. 境界保護セキュリティモデル

D. ゼロトラストセキュリティモデル

正解**: D (**コメントを発表する**)**

The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.

Key Characteristics of Zero Trust in the Diagram:

Role-based Access Control: Ensures that users have access only to the resources necessary for their role.

Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.

Network Access Control: Ensures that devices meet security standards before accessing the network.

Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.

This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.

質問**: 195**

ある組織は最近、組織環境における情報セキュリティ管理体制の監査を第三者機関に依頼しました。監査結果を検討した後、最高情報セキュリティ責任者(CISO)は、ネットワークセキュリティのための包括的な防御戦略の予算を承認しました。CISOが追加予算を承認した最も可能性の高い理由は次のうちどれでしょうか？

A. 他の部署に未使用の予算があったため、それをITセキュリティに振り替えました。

B. 潜在顧客からセキュリティコンプライアンスレポートを求める声がますます増えている。

C. 以前のネットワークアーキテクチャには、簡単に回避できる制御機能が含まれていました。

D. 監査担当者は、PCI OSS自己評価アンケートで低いスコアを報告しました。

正解: (正解を表示します)
The most likely reason for approving additional budget is that the audit revealed the existing network security controls could be easily bypassed. This justifies investing in a stronger, defense- in-depth network security strategy.

質問: **196**
複数のユーザーがシステムへのログイン時にMFA(多要素認証)の使用を継続的に求められています。セキュリティチームは、ユーザーアカウントのセキュリティを低下させることなく、この種の問題に対処できるポリシー変更を実施する予定です。以下のルール変更のうち、最も安全なものはどれですか？
A. 企業ネットワークからのアクティビティの場合、ログイン時にMFAを要求しない条件付きアクセスルールを作成する
B. ログイン場所に関係なく、どのユーザーアカウントでログインしてもMFAを要求しない条件付きアクセスルールを作成する
C. 会社のメールプロバイダーにログインする時のみMFAを要求する条件付きアクセスルールを作成する
D. すべてのログイン時にMFAを要求する条件付きアクセスルールを作成するが、パスワードの複雑さに関する要件の一部は削除する。
正解: (正解を表示します)
A conditional access rule that exempts MFA when authentication originates from the trusted corporate network reduces unnecessary MFA prompts while maintaining strong security controls.
The corporate network is considered a controlled and monitored environment where additional security measures such as network access controls, endpoint management, and internal monitoring already reduce risk. This approach improves usability for internal users while still enforcing MFA for external or untrusted locations, preserving strong protection against credential compromise.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **197**
ある企業が最近、ランサムウェア攻撃に見舞われました。同社はRPO（復旧ポイント目標）要件を満たすスケジュールでシステムとデータのバックアップを実行していましたが、バックアップ管理者はオフラインバックアップから重要なシステムとデータをRPOを満たすように復旧することができませんでした。最終的に、システムとデータはRPO要件から6ヶ月遅れの情報で復旧されました。
同様の攻撃のリスクを軽減するために、企業が実行すべきアクションは次のどれですか?
A. バックアップ テープは、オフサイトの場所に送信される前に、適切な保持スケジュールで暗号化し、ラベルを付けます。
B. 手動のビジネス プロセスの復元を含むビジネス継続プロセスを実装します。
C. IT おもなネットワークとプロセスの定期的な災害復旧テストを実行します。
D. 卓上演習を実施し、IT 部門と重要なビジネス機能を使用して RACI マトリックスを更新および検証します。
正解: **C** (コメントを発表する)
Understanding the Ransomware Issue:
The key issue here is that backups were not recoverable within the required RPO timeframe.
This means the organization did not properly test its backup and disaster recovery (DR) processes. To prevent this from happening again, regular disaster recovery testing is essential.
Why Option C is Correct:
Disaster recovery testing ensures that backups are functional and can meet business continuity needs.
Frequent DR testing allows organizations to identify and fix gaps in recovery strategies. Regular testing ensures that recovery meets the RPO & RTO (Recovery Time Objective) requirements.

質問: **198**
ある企業が、サブスクリプション型サービスの電子商取引を行うためのアプリケーションを開発しています。このアプリケーションは、以前に保存された支払い方法を使用して定期的な取引を実行できる必要があります。次のうち、最も適切なものはどれですか？
A. HSMによるトークン化
B. フィールドレベル暗号化機能を備えた自己暗号化ディスク
C. データ保持を最小限に抑えるためのNX/XN実装
D. アプリケーションユーザー向けのトークンベースアクセス
E. アドレス空間配置ランダム化
正解: **A (**コメントを発表する**)**
trying to connect a remote site to the central
Tokenization through an HSM (Hardware Security Module) is the most appropriate solution for securely storing and using previously saved payment methods for recurring transactions.
Tokenization replaces sensitive data (like credit card numbers) with a token, which is a non- sensitive equivalent that cannot be reversed without the corresponding HSM. This ensures that sensitive payment information is never stored in an accessible format and protects customer data from breaches while still enabling the application to perform transactions.

質問: **199**
ある企業は、OTシステムを社内ネットワークの他の領域から隔離しています。これらのシステムは、インターネット経由でベンダーに利用状況情報を報告することが義務付けられています。以下のうち、侵害や妨害行為を最も効果的に防止できるのはどれですか？(2つ選択してください。)
A. 許可リストの実装
B. ネットワーク動作の監視
C. 保存データの暗号化
D. ブート整合性チェックの実行
E. 毎日の健康チェックを実施する
F. サイト間IPSec VPNの実装
正解: **(**正解を表示します**)**
Implementing allow lists restricts communication to only approved addresses or services, reducing exposure to unauthorized access. Establishing a site-to-site IPSec VPN secures data transmission over the internet, protecting OT systems from interception or tampering.
質問: **200**
企業のSIEMは、企業の資産インベントリとユーザーイベントを関連付けるように設計されています。次のレポートを例に挙げます。

Hostname	Account	Attempted Logins	Failed Logins	Successful Logins
Server 1	SalesUser	3	0	3
Server 2	AccountingUser	5	1	4
Server 3				
Server 4	Administrator	2	2	0
Server 4	HR.User	5	0	5
Server 5	Administrator	0	0	0

Comshiken.com
CompTIA
セキュリティエンジニアがログ監査の一環として最初に調査する必要があるのは次のうちどれですか?
A. ログを送信していないエンドポイント
B. 攻撃者がネットワーク内で横方向に移動している可能性を示唆するアクティビティ

C. Syslogサーバーの設定が誤っており、誤検出が発生しています
D. 管理者アカウントの不正使用の試み
正解: **(**正解を表示します**)**
Understanding the Security Event:
Administrator accounts are highly privileged and require strict monitoring. Server 4 shows failed login attempts for the administrator account. This could indicate a brute-force attack or unauthorized access attempt.
The fact that none of the admin login attempts were successful suggests someone was trying to guess the credentials.

質問: **201**
準同型暗号化の一般的な使用例を最もよく表しているのは次のうちどれですか?
A. 認証されていないユーザーによるアクセスを防ぐために、プライベートクラウド内の複数のノードに独自のデータを保存
B. 保存中のデータとCSPとの間で処理のために転送中のデータの機密性を維持する
C. 転送中の不正アクセスを防ぐために、復号化後にサーバー上でデータを処理します。
D. 情報を公開することなく、機密データをCSPに送信し、多数のリソースで処理する
正解: **(**正解を表示します**)**

質問: **202**
押収したノートパソコンからファイルハッシュを取得する最も適切な理由は次のうちどれですか？
A. 各ファイルのメタデータ改ざんを防止するため
B. 後で各ファイルの整合性を検証する
C. 各ファイルに固有の識別子を生成する
D. ファイルの保管履歴を維持するため
正解: **(**正解を表示します**)**
Obtaining file hashes from a confiscated laptop is primarily done to ensure that the integrity of each file can be validated later. By generating a hash of each file, investigators can later compare the hash values to ensure that no files have been altered or tampered with during the investigation process. This helps confirm that the files remain unchanged from the time they were seized.

質問: **203**
24時間稼働の製造施設の情報セキュリティマネージャーは、組織に対する潜在的なリスクについて契約内容を精査しています。この契約は、営業時間外におけるプリンターおよび複合機のサポートに関するものです。セキュリティマネージャーがリスクとして最も可能性が高いと判断するのは、次のうちどれでしょうか？
A. ロックされた印刷ジョブの印刷設定
B. デバイスをサポートする企業との間でNDA(秘密保持契約)が締結されていない
C. サービスプロバイダーが提供するその他のサービスを規定するMSAが存在しないこと
D. 社内での機器導入前の管理体制の不備
正解: **B (**コメントを発表する**)**
When external technicians are granted access to printers and multifunction devices that buffer or store sensitive documents, there's a real risk they could view, copy, or exfiltrate data. Without a non-disclosure agreement in place, there is no contractual obligation preventing them from disclosing or misusing any confidential information they encounter. This gap presents a clear confidentiality risk that the information security manager should remediate.

質問: **204**
リモートワークを推進するグローバル企業が新しいVPNソリューションを導入しました。数百人のユーザーにVPNソリューションを展開したところ、ヘルプデスクに社内およ

び社外から利用可能なアプリケーションへのアクセス速度が遅いという報告が寄せられ始めました。セキュリティアナリストは、以下の点について確認しました。
VPN クライアント ルーティング:
0.0.0.0/0 eth1
この問題を解決するためにアナリストは次のどのソリューションを使用する必要がありますか?
A. サーバーをスクリーンされたサブネットに移動します。
B. スプリットトンネリングを有効にします。
C. NAC ソリューションを構成します。
D. DNS over HTTPS を実装します。
正解: **B** (コメントを発表する)
Enable split tunneling to resolve the issue of slow access. The current VPN client routing (0.0.0.0/0 routing through the VPN) forces all traffic, both internal and external, through the VPN, leading to slow performance for external applications. Split tunneling allows only internal traffic to go through the VPN, while external traffic bypasses the VPN, improving performance for external applications.

質問: **205**
災害復旧計画を作成する際に、以下の項目のうちどれを含めるべきですか？
A. 冗長性
B. テスト演習
C. オートスケーリング
D. 競合他社の所在地
正解: **B** (コメントを発表する)
Testing exercises are a critical component of a disaster recovery (DR) plan because they ensure that the plan works effectively in a real-world scenario. Testing allows organizations to validate their recovery procedures, identify potential gaps, and make improvements before an actual disaster occurs. It helps ensure that all team members are familiar with their roles and that the recovery process can be executed smoothly.

質問: **206**
アナリストは、導入中の新しいアプリケーションのリスク評価を実施したいと考えています。以下の情報があります。
* 新規アプリケーションの合計予算割り当ては利用できません。
* 回復時間目標が設定されていません。
* ダウンタイム損失の計算は提供できません。
次の記述のうち、定性的な評価が最良の選択肢である理由を説明しているものはどれですか。
A. アナリストはアプリケーション開発の業務経験を持っています。
B. 他の種類のリスク評価を実施するのに十分なメトリックがありません。
C. 組織のリスク レジスターは、ビジネス ユニット全体のすべてのリスクと軽減策を追跡します。
D. 組織は、あらゆる停止の金銭的価値を知りたいと考えています。
正解: **B** (コメントを発表する)
A qualitative risk assessment is appropriate when quantitative data such as budget, downtime costs, or RTOs are unavailable. It relies on expert judgment, likelihood, and impact categories rather than precise metrics, making it the best option in this scenario.

質問: **207**
組織全体は、暗号化された資料に個別にアクセスできる従業員による内部脅威を懸念しています。この問題に対処する最も効果的な手法は次のうちどれですか？

A. MFA を使用した SSO
B. 飽和とハッシュ
C. ハードウェアトークンを使用したアカウント連携
D. SAE
E. キー分割
正解: **(**正解を表示します**)**
Key splitting involves dividing the encryption key into multiple parts, where no single individual holds the entire key. This technique prevents any one person from being able to decrypt the encrypted material by themselves, thus reducing the risk of insider threats.

質問: **208**
小売業界のISACは最近、ソーシャルエンジニアリングの手口に関する報告書を発表しました。この手口では、少人数のグループが従業員の注意をそらす一方で、悪意のある人物が決済システムに高度なカードスキマーを仕掛けます。最高情報セキュリティ責任者（CISO）は、セキュリティ意識向上のためのトレーニング、技術的管理策の導入、そして既に導入されているガバナンスによって、この脅威から十分に保護できると考えています。取締役会はこれらの管理策をテストしたいと考えています。CISOが推奨すべき対策は次のうちどれですか？
A. ダークウェブ監視
B. 敵対者エミュレーションエンゲージメント
C. サプライチェーンリスクコンサルティング
D. 卓上演習
正解: **B (**コメントを発表する**)**
Adversary emulation engagement involves simulating realistic attack scenarios, including social engineering tactics, to test the effectiveness of existing security controls and employee response in a controlled environment.

質問: **209**
最近の報告によると、ソフトウェアツールが悪用されているようです。攻撃者はユーザーアクセス制御を回避し、データベースに侵入することができました。セキュリティアナリストは脆弱性を発見し、緩和策を提案する必要があります。
アナリストは次の出力を生成します。

```
:\>whoami
ocal-user
:\>netuser local-user Welcome!
he command completed successfully!
:\>dbloader.exe local-user Welcome!
nsufficient Permissions. Now Closing...
:\>strings dbloader.exe
 This program cannot be run in DOS Mode
Bl0ad3r!
oad Database jmp
82(*nx
i3jN*jk
ahn82mk0a
:\>dbloader.exe admin dBl0ad3r!
oading Database. Please Wait...
```

jpnshiken.com
CompTIA

アナリストが最も推奨すると思われるのは次のうちどれでしょうか?

A. 適切なEDRツールをインストールしてハッシュパスをブロックする
B. ファズテストを実行するためにソフトウェア開発に追加の時間をかける
C. ソースコードからハードコードされた資格情報を削除する
D. ユーザーがローカルパスワードを変更できないようにする
正解: **(**正解を表示します**)**
The stringsoutput reveals hard-coded credentials (admin dBl0ad3r!) within the dbloader.exebinary. Attackers can exploit these to bypass access controls. The analyst should recommend removing hard-coded credentials to mitigate this vulnerability.

質問: **210**
ある組織の脆弱性管理チームは、本番サーバーのスキャン結果から以下の出力結果をレビューしています。
ID検索 | 概要
脆弱な暗号ライブラリ | このデバイスは脆弱な暗号ライブラリの使用を許可します。
サポート終了済みのサードパーティライブラリ | 稼働中のサービスには、サポート終了済みのサードパーティライブラリが含まれています。
リモートサービスが検出されました | デバイスはTCPポート21でFTPを実行しています。
サポート終了となったオペレーティングシステム | オペレーティングシステムはサポート終了状態になりました。
データベースが検出されました | このデバイスにはデータベースがインストールされています。
チームはまず、次のうちどれを行うべきでしょうか？
A. デバイスの前に踏み台ホストを配置します。
B. データベースサービスへのポートを閉じます。
C. メーカーがサポートするオペレーティングシステムにアップグレードしてください。
D. 実行中のFTPサービスを無効にします。
正解: **C (**コメントを発表する**)**
The end-of-life operating system is the highest-priority foundational issue because it affects the overall security posture of the host. An unsupported OS no longer receives vendor security updates, which increases exposure across the entire system, including services and libraries running on it. From a SecurityX perspective, vulnerability management and asset lifecycle issues are part of security operations and enterprise resilience. Resolving the unsupported platform first addresses the broadest root problem. CompTIA's SecurityX exam coverage includes security operations, vulnerability management activities, and proper hardware/software asset management as core skills.

質問: **211**
セキュリティエンジニアが、社内で開発されたWebアプリケーションの以下のコードをレビューしている。このアプリケーションは、従業員が複数の社内サーバー上のドキュメントを操作できるようにするものである。
ユーザーは、ドキュメントの URL をパラメータとしてアプリケーションに渡すことで、解析するドキュメントを指定できます。アプリケーションは、次の Python 呼び出しを実行します: response = requests.get(url) エンジニアは、デプロイ前にアプリケーションのセキュリティを向上させたいと考えています。次のうち、実装するのに最適なものはどれですか?
A. 出力エンコーディング
B. インデックス
C. コードスキャナ
D. WAF
正解: **(**正解を表示します**)**

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**
ある組織は、脅威モデリング機能を含むSOCの構築を目的としたセキュリティコンサルタントを雇用しました。初期段階では、コンサルタントはシステムエンジニアと連携し、環境内のアンチパターンを特定します。
このフェーズでエンジニアがコンサルタントに開示する必要がある最も重要なことはどれですか?
A. 最新のインフラストラクチャアクセスレビューの結果
B. データセンターで使用されているパッチ適用不可能なIoTデバイスのリスト
C. 実稼働環境をカバーするネットワークおよびデータフロー図
D. 最新のソフトウェア構成分析の結果
E. 使用中のクラウドリソースとSaaS製品の現在のインベントリ
正解: **(**正解を表示します**)**
In the context of establishing a Security Operations Center (SOC) with a threat-modeling function, it's crucial to understand how data flows within the organization's systems. Network and data flow diagrams provide a visual representation of the system's architecture, illustrating how data moves between components, which is essential for identifying potential security weaknesses and antipatterns. Antipatterns are common responses to recurring problems that are ineffective and risk- inducing. By analyzing these diagrams, the consultant can pinpoint areas where security controls may be lacking or misconfigured, thereby facilitating the development of effective threat models.

質問: **213**
最新のリスク評価を受けて、最高情報セキュリティ責任者(CISO)は、セキュリティ業務の作業負荷を軽減する方法を見つけるため、開発チームとセキュリティチームと会合を開くことを決定しました。CISOは以下のことを望んでいます。
- 他のセキュリティシステムと通信するためのAPIを使用するソリューションを用意する
ツール。
最新の技術を可能な限り活用する。
ソリューションに対して可能な限り高いレベルの制御を確保する。
これらの要件を満たすための最適な選択肢は次のうちどれですか？
A. EDR
B. CSP
C. SOAR
D. CASB
正解: **(**正解を表示します**)**
A SOAR platform is explicitly built to integrate via APIs with your existing security tools (EDR, SIEM, firewalls, ticketing systems, etc.), orchestrate automated workflows, and apply rich, customizable controls (playbooks, role-based access, audit logging). It's also one of the newest
"X as a Service" technologies in the market for reducing manual security tasks and streamlining incident response.

質問: **214**
開発者は、本番環境での使用を想定して、個人用ラップトップで暗号化素材を作成・管理してきました。セキュリティエンジニアは、より安全なプロセスを導入する必要があります。エンジニアが採用すべき最適な戦略は次のうちどれでしょうか？
A. BIOSを無効にしてUEFIに移行する

B. vTPMハードウェア上の秘密の管理
C. LMIを防ぐためにシールドを採用
D. HSM上の鍵マテリアルの管理
正解: (正解を表示します)
Managing key material on a Hardware Security Module (HSM) is the best strategy to secure cryptographic material. HSMs are specialized devices designed to generate, store, and manage cryptographic keys securely. By using an HSM, the security engineer can ensure that cryptographic keys are protected in a secure, tamper-resistant environment, rather than being stored on developers' personal laptops where they are more vulnerable to theft or mishandling.

質問: **215**
セキュリティエンジニアは、本番環境に導入される前に、本番コンテナが自動的に脆弱性スキャンされるようにする必要があります。エンジニアは、コミットごとに脆弱性スキャンを自動的に組み込むために、次のうちどれを使用すべきでしょうか？
A. コードリポジトリ
B. CI/CDパイプライン
C. 統合開発環境
D. コンテナオーケストレーター
正解: (正解を表示します)
The best solution for automatically scanning containers for vulnerabilities before they are accepted into the production environment is to incorporate vulnerability scanning into the CI/CD pipeline. Continuous Integration (CI) and Continuous Deployment (CD) pipelines can be configured to automatically trigger security scans, including container vulnerability assessments, every time code is committed or changes are pushed. This ensures that vulnerabilities are detected early in the development cycle before the containers are deployed to production.

質問: **216**
脆弱性評価中にスキャンを行うと、次の結果が明らかになります。
Windows Server 2016 修正プログラム KB87728 が未適用 - CVSS 3.1 スコア: 8.1 [高] - 影響を受けるホスト: 172.16.15.2 レビュープロセスの後半で、修復チームはこの結果を誤検知としてマークしました。今後のスキャンでこの問題を回避するための最適な方法は、次のうちどれですか？
A. CMDBから最新の資産リストを取得する
B. サーバー上で認証スキャンを実行しています
C. フィンガープリンティングサーバ用の高度なポリシーを使用してセンサーを構成する
D. プロセスの早い段階で修復チームとスキャン実行を調整する
正解: (正解を表示します)
Authenticated scans allow the vulnerability scanner to log in to the target system and directly verify installed patches, system configurations, and software versions. This provides accurate information about whether specific hotfixes or updates are present. Without authentication, scanners rely on external fingerprinting and banner analysis, which can misidentify patch status and lead to false positives. Using authenticated scanning significantly improves accuracy and reduces incorrect vulnerability findings.

質問: **217**
ある企業は、クラウドベースのサービスを更新するために、インフラストラクチャコードをリモートリポジトリに保存しています。コードはリポジトリに保存されるたびに開発環境に自動的にデプロイされます。開発者は、開発環境での軽微なコードの問題やセキュリティ管理チェックの失敗を理由に、デプロイが頻繁に失敗するのではないかと懸念しています。セキュリティエンジニアは、デプロイの失敗を減らすために、次のうちどれを推奨すべきでしょうか？ 2つ選択してください。）
A. ソフトウェア構成分析
B. コミット前のコードリンティング
C. リポジトリブランチの保護

D. 自動回帰テスト
E. コード送信承認ワークフロー
F. パイプラインコンプライアンススキャン
正解**: B,D (**コメントを発表する**)**
Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.
Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.

質問**: 218**
ある組織は、マルチプラットフォーム環境全体にわたるインシデント対応プロセスの有効性を高めたいと考えています。セキュリティエンジニアは、組織が既に使用しているインシデント対応ツールを使用して、改善を実施する必要があります。セキュリティエンジニアは次のうちどれを使用すべきでしょうか？
A. プレイブック
B. イベントコレクター
C. 集中ログ
D. エンドポイント検出
正解**: (**正解を表示します**)**
Playbooks standardize and automate incident response steps across a multiplatform environment using existing tools. This increases effectiveness and consistency in handling security incidents.

質問**: 219**
ある大規模組織が、世界中のユーザーが利用できる生成AIプラットフォームを導入しました。ベータテスト中に得られたフィードバックに基づき、エンジニアは世界中のユーザーにとってユーザーインターフェースの遅延とページ読み込みパフォーマンスに問題があることを特定しました。現在、このインフラストラクチャは2つの独立したデータセンターで管理されており、高可用性ネットワークとロードバランサーを使用して接続されています。これらのパフォーマンス問題に対処するための最適な方法は、次のうちどれですか？
A. CDNを使用するようにアプリケーションを構成する
B. 大規模言語モデルのキューイングを可能にするRASPの実装
C. 第三データセンター内でのリモートジャーナリング
D. SASE を使用したトラフィック シェーピング
正解**: A (**コメントを発表する**)**
Using a Content Delivery Network (CDN) is the best way to reduce latency and improve page- loading performance for international users by caching and serving content closer to their geographic location. This directly addresses the performance issues reported during beta testing.

質問**: 220**
セキュリティアーキテクトは、エンタープライズシステムの耐障害性を設計するための要件を確立しており、この試験運用は他の物理的な場所にも拡大される予定です。システムは以下の要件を満たす必要があります。
- 一度の環境災害に耐えられること
- 重大な可用性喪失から24時間以内に復旧可能
- 1つのサイト間VPNソリューションに対する積極的な攻撃に耐えられること
以下の設計要素のうち、セキュリティを維持しながらこれらの要件を最もよく満たすものはどれですか？(2つ選択してください)
A. インターネットゲートウェイにおける負荷分散接続試行とデータ入力

B. 完全冗長構成で地理的に分散した待機サイトを割り当てる。
C. 異なるベンダーのルーターをレイヤリングして使用する
D. 他国各地に冷蔵拠点を設置するためのスペースをリースする。
E. 冗長なIDプロバイダーソリューションを導入する。
F. 会社の各拠点ごとに、オフサイトに保存する週次バックアップを完全に実施する。
正解: **(**正解を表示します**)**
Allocating fully redundant and geographically distributed standby sites ensures survivability against an environmental catastrophe and supports recovery within 24 hours. Deploying redundant identity provider solutions ensures continuity of authentication and access control, maintaining security and resilience even if one VPN or site is compromised.

質問: **221**
データ流出の申し立てを調査している地方自治体は、悪意のあるユーザーの行動の痕跡を確認するよう依頼されました。調査員はVMのフォレンジックイメージを取得し、それをセキュリティ保護されたUSBドライブにダウンロードして政府と共有しました。ドライブを政府に引き渡すプロセスにおいて、考慮すべき事項は次のどれですか？
A. ボラティリティの順序
B. 法的問題
C. 転送中の暗号化
D. 保管の連鎖
E. 鍵交換
正解: **(**正解を表示します**)**
質問: **222**
セキュリティエンジニアは、会社のノートパソコンが盗難に遭った場合でも、企業の機密情報が漏洩しないようにする必要があります。この要件を満たす最適なアクションは次のうちどれですか？
A. 企業データと多要素認証のためのデスクトップサービスの利用
B. 特定のIPアドレスの明示的な許可リストを使用し、シングルサインオンを展開する
C. モバイルデバイス管理を導入し、より強力なパスワードを要求する
D. セキュリティモバイルレポートポリシーの更新とデータ侵害の監視
正解: **(**正解を表示します**)**
Utilizing Desktop as a Service (DaaS) means that data and applications are hosted in the cloud rather than on the local device. In the event of a laptop theft, no sensitive data resides on the device, thereby preventing unauthorized access. Coupling DaaS with multifactor authentication (MFA) adds an additional layer of security, ensuring that only authorized users can access the cloud-hosted data and applications. This combination effectively mitigates the risk of data exposure due to device theft.

質問: **223**
ユーザーがアプリケーションへのアクセスに関する問題をヘルプデスクに報告します。ヘルプデスクはユーザーのログを確認します。

Time	Internal IP	Public IP	IP Geolocation	Application	Action
8:47 PM	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	HR System	Allow
8:49 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 PM	192.168.1.5	104.18.16.29	Toronto	HR System	Deny

jpnshiken.com CompTIA

この問題の原因として最も可能性が高いのは次のどれですか?

A. ユーザーが誤って NGFW のジオブロック ルールに違反しました。

B. 脅威アクターがユーザーのアカウントを侵害し、ログインしようとしました。

C. ユーザーは、営業時間外に人事システムにアクセスできません。

D. ユーザーは承認されたサブネットから接続を試行しませんでした。

正解: **A** (コメントを発表する)

The logs show that the user connected from Toronto (104.18.16.29) and Los Angeles (95.67.137.12) within minutes. The sudden location change is a typical trigger for geoblocking in a Next-Generation Firewall (NGFW), leading to the HR System being denied.

質問: **224**

最近発生したセキュリティインシデントを調査した後、SOCアナリストはチーム全体が使用できるリファレンスガイドを作成するよう指示されました。アナリストは、将来のインシデントに対処するために、次のうちどれを作成すべきでしょうか？

A. 根本原因分析

B. コミュニケーションプラン

C. ランブック

D. 学んだ教訓

正解: **C** (コメントを発表する)

A runbook is a step-by-step procedural guide that SOC analysts reference during live incidents. It documents the specific actions to take, such as how to triage alerts, gather forensic artifacts, escalate issues, and contain threats, ensuring consistency and speeding up response times across the team.

質問: **225**

COL システムに依存している企業は、新しいソリューションが利用可能になるまでシステムを運用し続けなければなりません。この目標を達成するための最も安全な方法はどれですか?

A. システムを分離し、ファイアウォールルールを適用して必要なエンドポイントのみへのアクセスを許可する

B. 強力な認証情報の適用と監視機能の向上

C. ITチームによる必要なメンテナンスを実行するためにシステムアクセスを制限する

D. システムを遮蔽されたサブネットに配置し、内部リソースからのアクセスをブロックする

正解: **A** (コメントを発表する)

To ensure the most secure way of keeping a legacy system (COL) operating until a new solution is available, isolating the system and enforcing strict firewall rules is the best approach. This method minimizes the attack surface by restricting access to only the necessary endpoints, thereby reducing the risk of unauthorized access and potential security breaches. Isolating the system ensures that it is not exposed to the broader network, while firewall rules control the traffic that can reach the system, providing a secure environment until a replacement is implemented.

質問: **226**
長期間にわたり、少数のネットワーク侵入試行が継続的に発生しています。調査の結果、SOCアナリストは、ネットワークから既知の悪意のあるホストへトラフィックが送信されており、その発信元が不正なネットワークデバイスであることを発見しました。ネットワーク侵入に最も使用されている可能性が高い攻撃手法は次のうちどれでしょうか？
A. ランサムウェア
B. バッファオーバーフロー
C. サプライチェーン
D. 社会工学
正解: **(**正解を表示します**)**

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **227**
ある組織が最近、異なるEDRソリューションを運用している別の企業を買収しました。SOCアナリストは、侵害されたエンドポイントの隔離を自動化したいと考えています。誤検知のリスクを軽減し、悪意のあるコードの拡散を最も効果的に抑制できるワークフローは次のうちどれですか？
A. SOARソリューションを使用して、TIPプラットフォーム経由でエンティティを検索し、API経由でエンドポイントを分離する
B. 各EDR管理コンソールにポリシーを設定し、アラートをトリガーするすべてのエンドポイントを分離する
C. さまざまなポータルですべてのアラートを手動で確認し、それらを分離するためのアクションを実行します。
D. 重要でないアラートをすべて自動的に抑制し、SOCアナリストにこれらのアラートを確認するよう依頼するメールを送信する
正解: **(**正解を表示します**)**
Using a SOAR solution integrated with a Threat Intelligence Platform (TIP) enables automated, intelligence-driven decisions to isolate endpoints via APIs. This workflow balances automation with validation to reduce false positives while quickly containing threats, especially across multiple EDR platforms.

質問: **228**
ある組織では最近、購入凍結を実施し、エンドポイントのライフサイクル管理に影響が出ています。エンドポイントを交換せずにリスクを軽減するために、セキュリティ管理者は次のうちどれを行うべきでしょうか？
A. システムイメージを再作成する
B. 不要なサービスを削除する
C. EDRを展開する
D. サポート終了したデバイスを廃棄する
正解: **(**正解を表示します**)**

質問: **229**
侵入テスト担当者は、以下のルーター設定を検証します。
set-system services ssh root login-allow
set-system services web-management https allow
set-system services syslog file interactive
set-system services log mode stream

set-interfaces 0 family inet address 10.12.14.1/8
以下の変更のうち、セキュリティを強化するための最良の方法はどれですか？
A. ユーザー対話型セッションに特定の暗号を設定する
B. 暗号化されていない端末接続へのアクセスを無効にします
C. ネットワークセグメンテーション制御を有効にする
D. デバイスの自動パッチ適用と再起動の設定
正解: **(**正解を表示します**)**
The most obvious security weakness shown in the configuration is the interface address
10.12.14.1/8, which places the device in an extremely broad network range instead of a tightly bounded segment. From a SecurityX perspective, the strongest improvement is to reduce unnecessary trust exposure by applying segmentation and tighter network boundaries.
CompTIA's official SecurityX objectives explicitly call out "Network architecture: segmentation, microsegmentation, virtual local area networks (VLANs), virtual routing and forwarding (VRF), software-defined networking (SDN)" and also emphasize "Security boundaries:
secure zones, access control lists (ACLs), virtual private network (VPN)" under Security Architecture.

質問: **230**
セキュリティアナリストは、正当なサードパーティボット関連トラフィックで知られるIPアドレスに関連付けられたリクエストを発見しました。アナリストは、これらのリクエストが悪意のあるものであるかどうかを判断するために、次のうちどれを使用すべきでしょうか？
A. ユーザーエージェント文字列
B. リクエストのバイト長
C. Webアプリケーションヘッダー
D. HTMLエンコーディングフィールド
正解: **(**正解を表示します**)**
User-agent string is the best option for determining whether requests are malicious. The user- agent string provides information about the client making the request, including the browser or bot in use. By analyzing the user-agent, the security analyst can differentiate between legitimate traffic (such as from a recognized browser) and bot-related traffic (which often uses generic or suspicious user-agent strings).

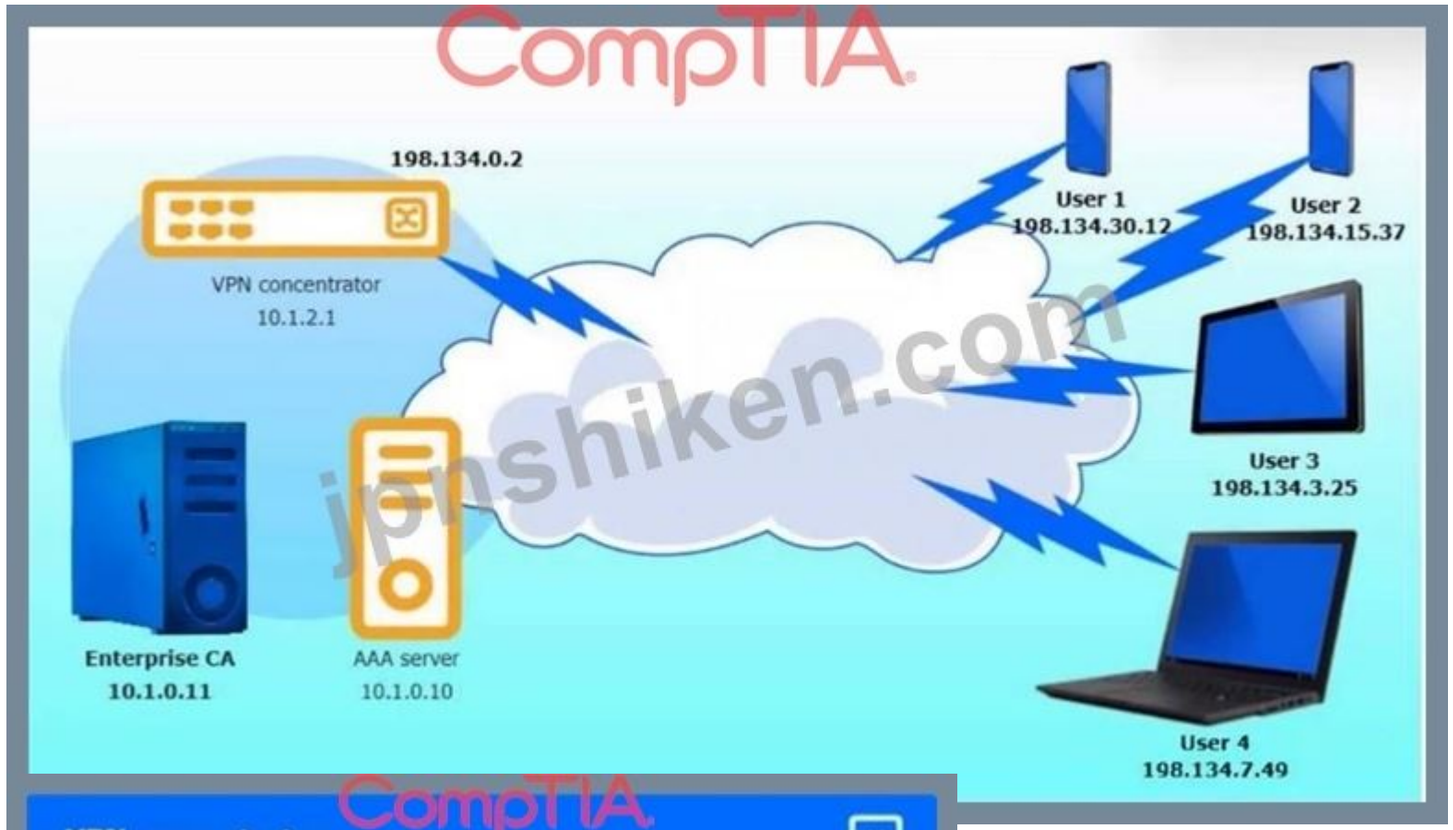
質問: **231**
攻撃者はハードウェアメーカーのコードベースに侵入し、コードがコンパイルされる前にマルウェアを挿入しました。悪意のあるコードは現在、多くの業界やセクターのハードウェアレベルで実行されています。
このタイプのベンダー リスクを最もよく表すカテゴリは次のどれですか。
A. SDLC攻撃
B. サイドロード攻撃
C. リモートコード署名
D. サプライチェーン攻撃
正解: **D (**コメントを発表する**)**

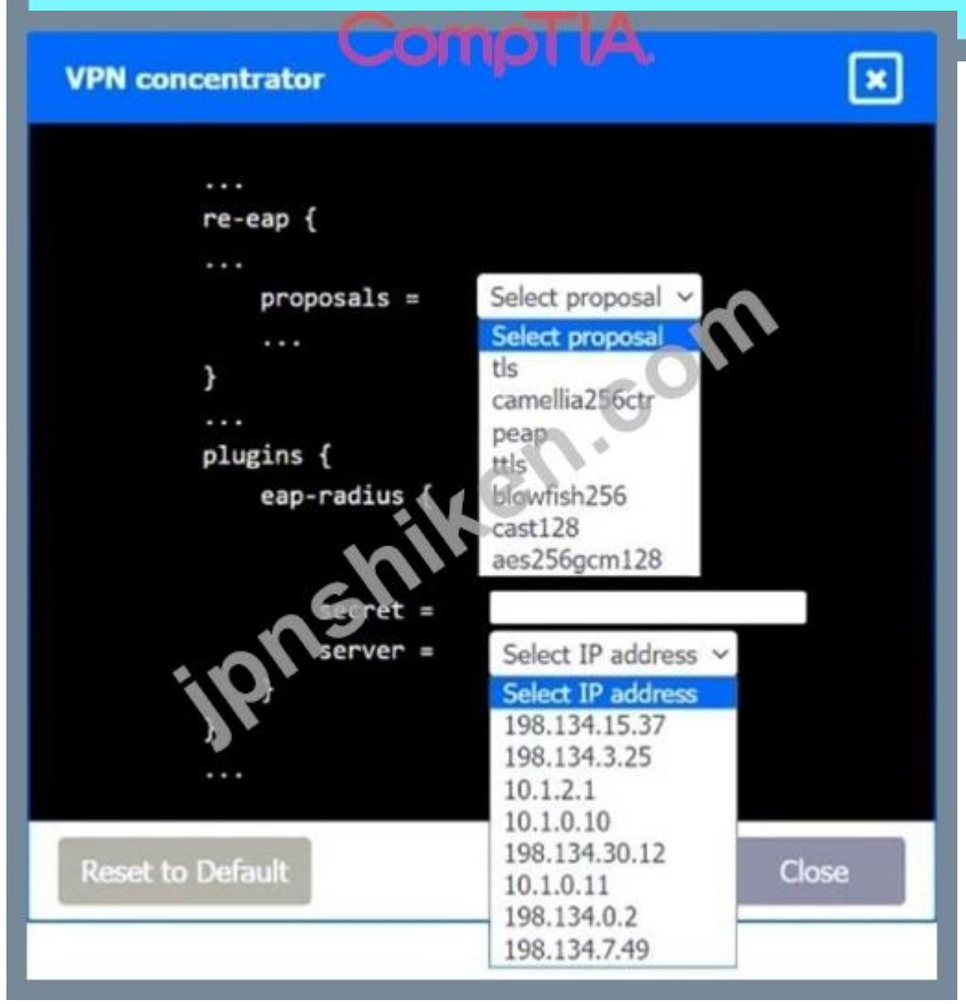
質問: **232**
ウェブアプリケーションサーバーが、パッチ未適用のリモートコード実行(RCE)脆弱性を抱えた旧式のオペレーティングシステムで稼働している。対応するアプリケーションコードが変更されるまで、サーバーをアップグレードすることはできない。
以下の補償対策のうち、悪用を最も効果的に防ぐことができるのはどれか？
A. セグメンテーション

B. CASB
C. ヒップ
D. UEBA
正解: **A (**コメントを発表する**)**
Segmentation is a compensating control that helps mitigate risks by isolating critical systems or vulnerable systems from the rest of the network. In this case, the web application server running a legacy operating system with an unpatched remote code execution (RCE) vulnerability can be isolated through network segmentation. This limits the potential for attackers to exploit the vulnerability by restricting access to the server and preventing lateral movement within the network. By segmenting the server, the attack surface is reduced, and the risk of successful exploitation is minimized until the system can be properly patched.

質問: **233**
セキュリティエンジニアがレガシーサーバーを評価しており、FTPが実行されているかどうか、またどのポートで実行されているかを確認する必要があります。重要なアプリケーションの動作に影響を与えるため、このサービスを停止することはできません。このサービスが悪用されるのを防ぐためのファイアウォールルールを作成するために必要な情報を提供するコマンドはどれですか？
A. service --status-all | grep ftpd
B. chkconfig --list
C. netstat -tulpn
D. systemctl list-unit-file --type service ftpd
E. サービス ftpd の状態
正解: **C (**コメントを発表する**)**
The netstat -tulpn command displays all listening TCP (-t) and UDP (-u) sockets, shows the program name/PID that owns each socket (-p), and omits name resolution for speed (-n). This provides both confirmation that the FTP daemon is running and the exact port number it's bound to, which you can then use to craft your firewall rule.

質問: **234**
シミュレーション
IPSecソリューションが導入されています。VPNコンセントレータとAAAサーバの両方の設定ファイルが図に示されています。
以下の要件を満たすように設定ファイルを完成させてください。
- EAP方式では、相互証明書ベース認証(発行されたクライアント証明書を使用)を使用する必要があります。
- IKEv2暗号スイートは、最も安全な認証モードに設定する必要があります。
秘密情報には、少なくとも1つの大文字、1つの小文字、1つの数字、および1つの特殊文字が含まれている必要があり、また、最低8文字の長さが必要です。
説明書
AAAサーバーとVPNコンセントレータをクリックして設定を完了してください。該当するフィールドに入力し、ドロップダウンメニューから選択してください。
シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。


198.134.0.2
VPN concentrator
10.1.2.1
Enterprise CA
10.1.0.11
AAA server
10.1.0.10
User 1
198.134.30.12
User 2
198.134.15.37
User 3
198.134.3.25
User 4
198.134.7.49


VPN concentrator
...
re-eap {
...
proposals =
...
}
...
plugins {
eap-radius {
secret =
server =
}
}
...
Select proposal
Select proposal
tls
camellia256ctr
peap
ttls
blowfish256
cast128
aes256gcm128
Select IP address
Select IP address
198.134.15.37
198.134.3.25
10.1.2.1
10.1.0.10
198.134.30.12
10.1.0.11
198.134.0.2
198.134.7.49
Reset to Default
Close



正解:

VPN Concentrator

Proposal: aes256gcm128

Server IP: 10.1.0.10 (this is the AAA server)

Secret: Str0ng@Key (example that meets all character requirements)

AAA Server

Default EAP type: tls

IP Address: 10.1.2.1 (this is the VPN concentrator)
■
Secret: Str0ng@Key (must match the VPN concentrator)
■

質問: **235**
ある企業は、安全性の低いネットワーク上で文書を転送するための、非常に安全な方法を必要としています。文書は機密性が高く、ネットワーク通信が傍受された場合でも文書の暗号化が保証されなければなりません。以下の暗号化技術のうち、どれが最適な選択肢でしょうか？
A. 非対称
B. 対称
C. ワンタイムパッド
D. 軽量
正解: **(**正解を表示します**)**

質問: **236**
マルウェア研究者は、認証情報窃取マルウェアが特定のメモリレジスタを監視し、企業ネットワーク内での横方向の移動に使用するパスワードを収集していることを発見しました。このマルウェアはTCP 4444を使用して他のワークステーションと通信しています。横方向の移動を最も効果的に抑制するには、以下の対策が考えられます。
A. エッジファイアウォールの有効化
B. ホストファイアウォールの有効化
C. CPUのNXビットの設定
D. Active Directory サーバーで ASLR を有効にする
E. すべてのシステムでUEFIの使用を強制する
正解: **(**正解を表示します**)**

質問: **237**
セキュリティアーキテクトは、社内開発アプリケーションのソフトウェア開発ライフサイクルにおいて、セキュリティ制御を実装する必要があります。アーキテクトは、アプリケーションの作成に使用されたコンポーネントを特定する必要があります。セキュリティアーキテクトは、この要件を満たすために、次のうちどれを使用すべきでしょうか？
A. A/Bテスト
B. SAST
C. IAST
D. SBoM
正解: **D (**コメントを発表する**)**
A Software Bill of Materials (SBoM) provides a detailed inventory of all components, libraries, and dependencies used in an application. This allows the security architect to track and manage risks associated with the software supply chain throughout the development life cycle.

質問: **238**
エンジニアがオンプレミスでホストされているWebアプリケーションのスケーリング問題に直面しており、サーバーレスアーキテクチャへの移行を検討しています。このプロジェクトには、以下のクラウドの利点のうちどれを活用するのが最適でしょうか？
A. ホスティング費用の節約
B. リソースプロビジョニングの自動化
C. 地理的に冗長化されたホスティングを提供します
D. パッチ適用が不要

正解: (正解を表示します)
The best cloud benefit for moving to a serverless architecture in this case is Automation of resource provisioning. Serverless computing automatically scales resources based on demand without requiring manual intervention. This helps to address the scaling issues the engineer is facing by dynamically adjusting resource allocation as needed, improving performance and efficiency without manual effort.

質問: **239**
従業員はバッジを使って勤務時間を記録します。バッジリーダーは施設の制約によりアップグレードできません。バッジリーダーのソフトウェアはレガシープラットフォームを使用しており、ERPソリューションへの接続が必要です。バッジリーダーのセキュリティを確保するには、次のうちどれが最適ですか？
A. セグメンテーション
B. 脆弱性スキャン
C. マルウェア対策
正解: (正解を表示します)
Segmentation is the best option to ensure the security of legacy badge readers that cannot be upgraded. Segmentation isolates the legacy devices on a separate network segment to minimize their exposure to potential threats. This approach reduces the attack surface by preventing unauthorized access from other parts of the network while still allowing necessary connectivity to the enterprise resource planning (ERP) system.

質問: **240**
SIEM(セキュリティ情報イベント管理)システムは、最近リポジトリへの一時的なアクセス権を付与された第三者のデータベース管理者が、データベース内の機密性の高い業務コンテンツにアクセスした後にアラートを生成した。
SIEMは、今回のインシデント以前にも同様のアラートを生成していました。以下のうち、アラートの原因を最もよく説明しているのはどれですか？
A. データベースフィールドのトークン化
B. データベースデコイ
C. データベースアクティビティ監視
D. データベースの整合性の強制
正解: **C** (コメントを発表する)
Database activity monitoring (DAM) tracks user actions within databases and generates alerts for anomalous behavior, such as unauthorized access to sensitive content. Database field tokenization protects sensitive data but does not monitor access. Database decoy involves creating fake data to detect misuse but is unrelated to monitoring. Database integrity enforcement ensures data accuracy but does not generate access alerts.

質問: **241**
ある中央銀行は、ハードウェアのサプライチェーンにおいて、特定の原産国に対する許可リストの設定を含む厳格なリスク軽減策を実施しています。この銀行に対するサイバー脅威を最もよく表しているのは、次のうちどれですか。
A. 戦時中に部品を入手できる能力
B. 脆弱性およびその他の可用性攻撃
C. 物理的インプラントと改ざん
D. 承認された製造基準に適合していない
正解: **C** (コメントを発表する)
The allow list for specific countries of origin as a risk mitigation indicates that the central bank is focused on preventing physical implants and tampering in hardware. This is a form of supply chain attack where malicious actors may insert malicious hardware components into devices, leading to potential compromises in security. By restricting the countries of origin, the bank is likely aiming to prevent such vulnerabilities.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **242**
ある企業が最近SaaS企業を買収し、ギャップ分析を実施しました。ギャップ分析の結果、SDLC全体にわたってセキュリティ管理が欠如しており、複数の脆弱な本番リリースが発生していたことが判明しました。今後、脆弱なコードが本番環境にデプロイされるリスクを最も効果的に低減できるセキュリティツールは次のうちどれでしょうか？
A. 静的アプリケーションセキュリティテスト
B. 回帰テスト
C. コード署名
D. サンドボックス
正解: **A** (コメントを発表する)
Static application security testing (SAST) is the best tool for identifying security vulnerabilities in code early in the Software Development Life Cycle (SDLC). SAST tools analyze source code or binaries for vulnerabilities without executing the program, allowing teams to catch and address security issues before the code is pushed to production. This aligns with reducing the risk of vulnerable code being released.

質問: **243**
境界ファイアウォール構成を検証するためのベスト プラクティスが含まれているのは次のどれですか。
A. CIS controls
B. MITRE ATT&CK
C. NIST CSF
D. ISO 27001
正解: (正解を表示します)
CIS Controls provide prescriptive best practices for validating and hardening firewall configurations, including rule review, change management, and regular audits to ensure perimeter defenses are properly configured.

質問: **244**
最近、ある医療システムがランサムウェア攻撃に見舞われました。その結果、取締役会は既存のネットワークセキュリティを強化するため、セキュリティコンサルタントを雇うことを決定しました。セキュリティコンサルタントは、医療ネットワークが完全にフラットで、特権アクセス制限がなく、個人の医療情報を含むサーバーへのRDPアクセスがオープンであることを発見しました。コンサルタントが修復計画を策定する中で、これらの課題を解決するのに最適なソリューションは次のどれですか (3つ選択してください)。
A. SD-WAN
B. リモートアクセスVPN
C. NAC
D. ネットワークセグメンテーション
E. BGP
F. MFA
G. PAM
正解: (正解を表示します)

質問: **245**

セキュリティアナリストが、公開リポジトリにある以下のコードについて、潜在的なリスクがないか調査しています。



セキュリティアナリストは、脆弱性を修復するために、まず次のうちどれを推奨すべきでしょうか？

A. 役割に基づいたセキュリティ意識向上トレーニングの開発

B. ソリューションで使用された秘密の取り消し

C. 公開表示からコードを削除する

D. SASTでアプリケーションをスキャンする

正解: **B** (コメントを発表する)

The code includes a hard-coded secret (access_token), which is a security vulnerability. The first action should be to revoke this secret immediately to prevent unauthorized access, as it is exposed in the public repository. Once the secret is revoked, the secret management process should be improved, such as by using environment variables or secure vault solutions.

質問: **246**

侵入テスト中に、複数のユーザーからネットワーク上の特定のファイル共有にアクセスできないとの報告があった。アナリストがネットワークトラフィックを分析したところ、LLMNRとSMBに関連するパケットが多数検出され、それらが侵入テスト担当者のコンピュータにリダイレクトされていることが分かった。

以下の攻撃のうち、どれが問題の原因となっていますか？

A. SMB総当たり攻撃

B. ディレクトリファジング

C. NTLMリレー

D. ネットワークポイズニング

正解: (正解を表示します)

The presence of a large number of LLMNR responses redirecting SMB traffic to the penetration tester indicates name resolution poisoning. In this attack, the attacker responds to LLMNR queries before legitimate hosts, convincing systems that the attacker's machine is the requested resource. As a result, SMB connections and authentication attempts are redirected to the attacker's system, disrupting normal access to fileshares and enabling credential capture.

質問: **247**

ソフトウェア会社は、社内のコード リポジトリに基づいて新しいアプリケーションを導入しました。複数の顧客から、アプリケーションのテストに使用したワークステーションでマルウェア対策アラートが報告されています。アラートの原因として最も考えられるのは次のどれですか。

A. 誤ったコードコミットの設定

B. 安全でないバンドルライブラリ

C. 無効なコード署名証明書

D. データ漏洩

正解: (正解を表示します)

Unsecure bundled libraries are the most likely cause of anti-malware alerts. If the application includes third-party components with known vulnerabilities or malicious behavior, endpoint security tools may flag it during testing.

質問: **248**

システム管理者は、企業のクラウドストレージ環境におけるセキュリティ保証を強化する必要がある。管理者は、データが悪意を持って、あるいは意図せず変更されたかどうかを特定することが最善のアプローチであると判断した。システム管理者は、以下のどの手法を定期的に使用すべきか？
A. 干渉
B. 改ざん防止
C. ハッシュ化
D. 日記をつける
正解: **(**正解を表示します**)**
Hashing is the best technique for identifying whether data has been maliciously or inadvertently modified. By generating and storing hash values for files or data, the administrator can periodically recheck the hashes to ensure that the data has not been altered. If the hash value changes, it indicates that the data has been modified. This technique provides an efficient and secure way to ensure data integrity.

質問: **249**
内部ユーザーは、外部組織の受信者を除くすべての受信者に暗号化されたメールを正常に送信できます。内部ユーザーがこの外部受信者に暗号化されたメールを送信しようとすると、セキュリティエラーメッセージが表示されます。この問題は、暗号化されていないメールには影響しません。外部受信者は、内部ユーザーに暗号化されたメールを送信できます。この問題の最も可能性の高い原因は次のうちどれですか？
A. 外部受信者の秘密鍵の有効期限が、内部ユーザーがシステムにアクセスするために使用しているSSH鍵の有効期限と一致しません。
B. 外部受信者は、CAによって取り消されていない有効期限切れの公開鍵/秘密鍵ペアを持っています。
C. 社内ユーザーの会社のメールサーバーで、OCSPとCRLの設定が正しく実装されていません。
D. 外部受信者のメールアドレスと、外部受信者の公開鍵に関連付けられているメールアドレスが一致しません。
正解: **(**正解を表示します**)**
In a Public Key Infrastructure (PKI) system, when sending encrypted emails, the recipient's public key is used for encryption. If the public key is associated with a different email address than the one being used by the recipient, the email encryption will fail, causing a security error. This is because the system is trying to encrypt the message using a public key that doesn't match the recipient's actual email address.
Since the issue only occurs with one external recipient, and the internal user can send encrypted emails to all others, this suggests the problem is likely due to a mismatch between the email address and the public key used for encryption, rather than other potential issues like expired keys or incorrect settings.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**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/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」