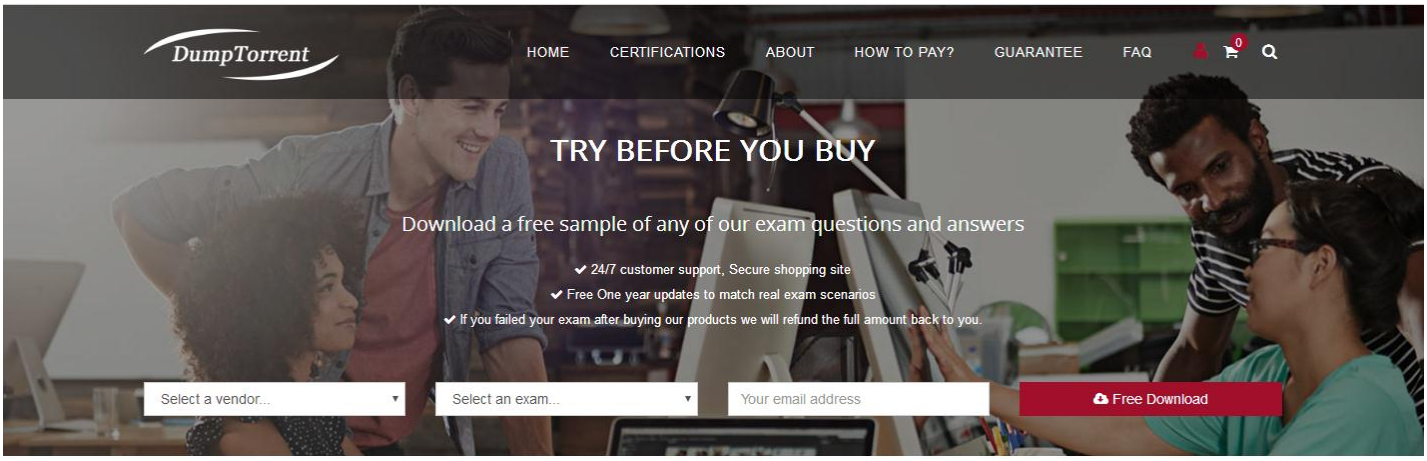
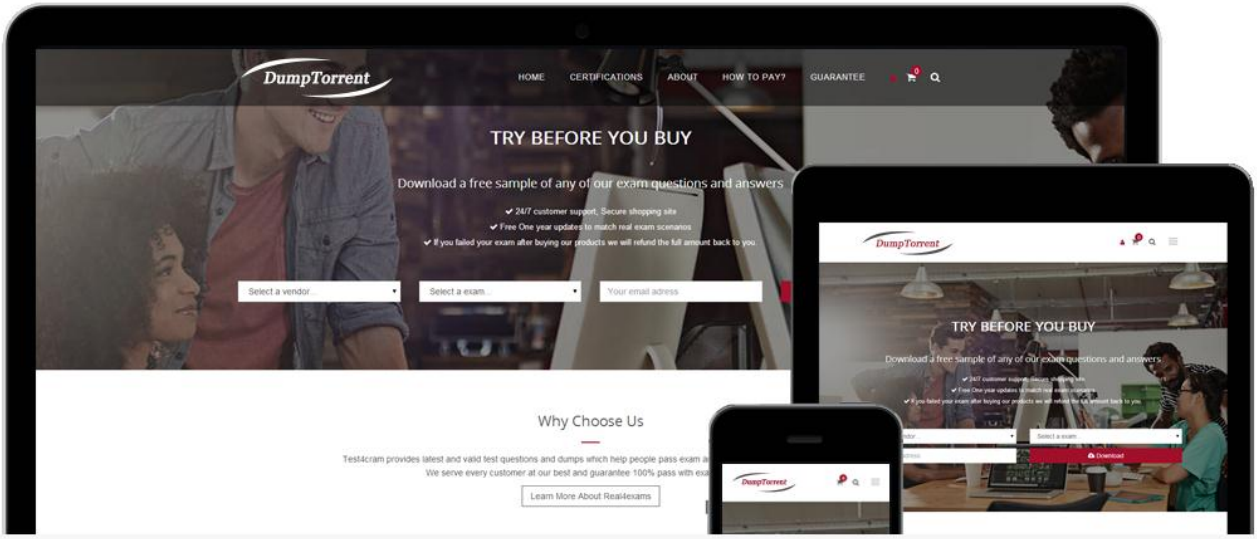
DumpTorrent





QUALITY AND VALUE

ExamsTorrent Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all vce.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our ExamsTorrent testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

ExamsTorrent offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.dumptorrent.com

High-quality Exam Torrent & Valid Test Dumps & Reliable Guide Torrent

Exam : **CS0-002J**

Title : CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-002日本語版)

Vendor : CompTIA

Version : DEMO

QUESTION NO: 1
インシデント対応計画では、侵害が発生した場合に、重要なデータを含むシステムを最初に優先順位付けする必要があります。次の種類のデータのうち、重要なものとして分類される可能性が最も高いのはどれですか?
A. 暗号化されたデータ
B. データ
C. マスクされたデータ
D. マーケティングデータ
Answer: B
Explanation:
PII stands for personally identifiable information, and it is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, or biometric data. PII data is considered critical because it can be used by attackers to commit identity theft, fraud, or other crimes. PII data is also subject to various laws and regulations that require organizations to protect it from unauthorized access, use, or disclosure1.

QUESTION NO: 2
ネットワーク アプライアンス
メーカーは新世代のデバイスを構築しており、チップセットのセキュリティ向上を組み込みたいと考えています。管理チームは、チップセットのファームウェア
バージョンをダウングレードすることによって再発する可能性のあるセキュリティ上の弱点を防ぐ方法をセキュリティ
チームに実装することを望んでいます。この目的を達成できるのは次のうちどれですか?
A. UEFI
B. ハードウェアセキュリティモジュール
C. eFUSE
D. 証明書署名付きアップデート
Answer: C
A) UEFI is not correct. UEFI stands for Unified Extensible Firmware Interface, and it is a standard that defines the software interface between an operating system and a platform firmware. UEFI can provide security features, such as secure boot, which verifies the integrity of the boot loader and prevents unauthorized code execution during the boot process. However, UEFI does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset2.
B) A hardware security module is not correct. A hardware security module (HSM) is a physical device that provides secure storage and processing of cryptographic keys and operations. An HSM can protect sensitive data and transactions, such as encryption, decryption, signing, or verification, from unauthorized access or tampering. However, an HSM does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset3.
D) Certificate signed updates are not correct. Certificate signed updates are a method of ensuring the authenticity and integrity of firmware updates by using digital certificates and signatures. Certificate signed updates can prevent malicious or corrupted firmware updates

from being installed on the chipset, but they do not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset.
1: What Is an eFUSE? 2: What Is UEFI? 3: What Is a Hardware Security Module (HSM)?
Explanation:
The correct answer is C. eFUSE. An eFUSE is a type of electronic fuse that can be programmed to permanently alter the functionality or configuration of a chipset. An eFUSE can be used to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset, by locking the firmware to a specific version or preventing unauthorized modifications. An eFUSE can also provide other benefits, such as anti-tampering, anti-counterfeiting, and device authentication1.

QUESTION NO: 3
サイバーセキュリティ アナリストは、現在 Web
サーバーとして使用されているサーバーを強化する必要があります www company com をブラウザーに入力したときにサーバーにアクセスできる必要があります さらに、Web ページには、リモートの請負業者によって実行される頻繁な更新が必要です
次の出力が与えられた場合:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT        STATE    SERVICE
22/tcp      open     ssh
23/tcp      open     telnet
53/tcp      open     domain
80/tcp      open     http
443/tcp     open     https
```

次のうち、サーバーを強化するためにサイバーセキュリティ
アナリストが推奨すべきものはどれですか? (2 つ選択)。
A. DNS サービスをアンインストールする
B. 脆弱性スキャンを実行します
C. サーバーの IP をプライベート IP アドレスに変更します
D. Telnet サービスを無効にします
E. ホストベースのファイアウォールでポート 80 をブロックする
F. SSH ポートを非標準ポートに変更します
Answer: D,F
Explanation:
Disabling the Telnet service would harden the server by removing an insecure protocol that transmits data in cleartext and could allow unauthorized access to the server. Changing the SSH port to a non-standard port would harden the server by reducing the exposure to brute-force attacks or port scans that target the default SSH port (22). Uninstalling the DNS service, performing a vulnerability scan, changing the server's IP to a private IP address, or blocking port 80 with the host-based firewall would not harden the server or could affect its

functionality as a web server. Reference:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

QUESTION NO: 4
セキュリティ
アナリストは、重要な情報を入手するために、対象を絞ったシステムの脆弱性スキャンを実行しました。結果が出力された後、アナリストは OVAL XML
言語を使用して、発見されたリスクを検討および計算しました。セキュリティ
アナリストは次のタイプのスキャンのうちどれを実行しましたか?
A. アクティブ
B. ネットワークマップ
C.パッシブ
D. 外部
Answer: A
Explanation:
An active scan is a type of system vulnerability scan that involves sending probes or packets to the target system, and analyzing the responses or behaviors of the system. An active scan can help obtain critical information about the system, such as open ports, running services, operating system, software versions, etc. An active scan can also use OVAL XML language to review and calculate the discovered risk. OVAL stands for Open Vulnerability and Assessment Language, and it is a standard for describing and exchanging information about system vulnerabilities and configurations.

QUESTION NO: 5
クラウド評価の実施中に、セキュリティ アナリストはプラウラー
スキャンを実行します。これにより、レポート内に次の情報が生成されます。

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

プラウラーのレポートに基づいて、次のうちどれが最も推奨されていますか?
A. CloudDev アクセス キー 1 を削除します。
B. BusinessUsr アクセス キー 1 を削除します。
C. アクセスキー 1 を削除します。
D. アクセスキー 2 を削除します。
Answer: C
Explanation:
Prowler is a tool that can scan AWS environments for security issues and compliance violations. The Prowler report shows that there are two access keys for CloudDev user: access key 1 and access key 2. Access key 1 has not been used in more than 90 days, which violates the AWS CIS benchmark 1.4 (Ensure access keys are rotated every 90 days or less). Therefore, the best recommendation is to delete access key 1 and use access key 2 instead. Deleting CloudDev access key 1, deleting BusinessUsr access key 1, or deleting

access key 2 are not appropriate recommendations based on the Prowler report. Reference: https://github.com/toniblyx/prowler

QUESTION NO: 6
SDLC shoukJ セキュリティの次のフェーズのうち、最初に関与するのはどれですか?
A. デザイン
B. メンテナンス
C. 実装
D. 分析
E. 計画
F. テスト
Answer: E
Explanation:
The software development life cycle (SDLC) is a process that consists of several phases that guide the development of software applications or systems. Security should be involved in every phase of the SDLC, but especially in the planning phase, which is the first phase where the scope, objectives, requirements, and resources of the project are defined. By involving security in the planning phase, potential risks and threats can be identified and mitigated early in the process, which can save time, money, and effort later on. Design, maintenance, implementation, analysis, and testing are other phases of the SDLC, but they are not the first phase where security should be involved. Reference: https://www.bmc.com/blogs/software-development-life-cycle-phases/

QUESTION NO: 7
機密データを含む従来の医療機器にはパッチを適用できません。機器のセキュリティ体制を改善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. レガシー システムを WAR の背後に移動します。
B. レガシー システムにエア ギャップを実装します。
C. レガシー システムを境界ネットワークに配置します。
D. レガシー システムとローカル ネットワークの間に VPN を実装します。
Answer: B
Explanation:
Implementing an air gap for the legacy systems is the best solution to improve their security posture. An air gap is a physical separation of a system or network from any other system or network that may pose a threat. An air gap can prevent any unauthorized access or data transfer between the isolated system or network and the external environment. Implementing an air gap for the legacy systems can help to protect them from being exploited by attackers who may take advantage of their unpatched vulnerabilities .

QUESTION NO: 8
セキュリティ アナリストは、次のプロキシ ログ エントリに気付きました。

```
Received From: (proxy)
192.168.2.1>/
Usr/local/var/logs/access.log
Rule: 5022 fired (level 10) >
0 192.168.2.101 TCP_DENIED/403 1382 CONNECT 63.51.205.114:25 NONE/text/html
2 192.168.2.101 TCP_DENIED/403 1378 CONNECT 12.19.101.4:25 NONE/text/html
0 192.168.2.101 TCP_DENIED/403 1390 GET http://www.ebay.com/NONE/text/html
3 192.168.2.101 TCP_DENIED/403 1378 CONNECT 16.9.161.24:25 NONE/text/html
5 192.168.2.101 TCP_DENIED/403 1392 GET http://www.news.com/ NONE/text/html
```

ログエントリに基づいて、ユーザーが行おうとしているのは次のうちどれですか?

A. 外部ホストに対して DoS 攻撃を使用します。

B. データを抽出します。

C. ネットワークをスキャンします。

D. メールを中継します。

Answer: C

Explanation:

Scanning the network is what the user is attempting to do based on the log entries. The log entries show that the user is sending ping requests to various IP addresses on different ports using a proxy server. Ping requests are a common network diagnostic tool that can be used to test network connectivity and latency by sending packets of data and measuring their response time. However, ping requests can also be used by attackers to scan the network and discover active hosts, open ports, or potential vulnerabilities .

QUESTION NO: 9

会社の従業員がインターネットからアプリケーションをダウンロードします。インストール後、従業員は顕著なパフォーマンスの問題を経験し始め、ファイルがデスクトップに表示されます。

Process name	Username	CPU %	Memory
Chrome.exe	JSmith	11	63.528MB
Word.exe	JSmith	6	16.327MB
Explorer.exe	system	3	5120Kb
mstsc.exe	system	9	5.306MB
taskmgr.exe	system	1	3580Kb

タスク マネージャーで実行されているプロセスを考慮して、セキュリティアナリストが最も可能性の高いシステム侵害の兆候として特定するプロセスは次のうちどれですか?

A. Chrome.exe

B. Word.exe

C. Explorer.exe

D. mstsc.exe

E. taskmgr.exe

Answer: D

Explanation:

mstsc.exe is the process name for Remote Desktop Connection, a program that allows users

to connect to remote computers or servers over a network or the Internet12. mstsc.exe is an indicator of system compromise if the user did not initiate or authorize a remote connection, as it may mean that an attacker has gained access to the system and is using it to connect to other systems or exfiltrate data3.

QUESTION NO: 10
最高情報セキュリティ責任者は、ネットワーク上の特定のトラフィックをリダイレクトするためのセキュリティ対策を講じるよう要求しました。この問題を最もよく解決するのは次のうちどれですか?
A. シンクホール
B. ブロックリストに登録
C. ジオブロッキング
D. サンドボックス化
Answer: A
Explanation:
Sinkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to a server of your choosing. It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks1.
For example, sinkholing can be used to redirect traffic from a botnet or a malware-infected host to a server under the control of the defender, where the traffic can be analyzed, blocked, or neutralized. This can help identify and isolate compromised devices, prevent command-and-control communication, and disrupt malicious activities2.
The other options are not the best solutions for the following reasons:
Blocklisting is a technique for preventing access to or communication with certain IP addresses, domains, or applications that are known or suspected to be malicious. Blocklisting can be implemented using firewalls, routers, proxies, or software tools. Blocklisting can protect a network from unwanted or harmful traffic, but it does not redirect the traffic to a different destination.
Geoblocking is a technique for restricting access to or communication with certain IP addresses, domains, or applications based on their geographic location. Geoblocking can be implemented using firewalls, routers, proxies, or software tools. Geoblocking can protect a network from unauthorized or undesirable traffic from specific regions or countries, but it does not redirect the traffic to a different destination.
Sandboxing is a technique for isolating and executing potentially malicious code or applications in a separate and secure environment. Sandboxing can be implemented using virtual machines, containers, or software tools. Sandboxing can protect a network from malware infection or damage, but it does not redirect the network traffic to a different destination.

QUESTION NO: 11
セキュリティアナリストは、ランサムウェアが複数の会社のワークステーションのディスクを暗号化したインシデントを処理しています。将来この種の事件を防ぐために最も効果的なのは次のうちどれですか？
A.

ステートフルファイアウォールの代わりにUTMを実装し、ゲートウェイアンチウイルスを有効にします。
B.
ワークステーションをバックアップして、リカバリを容易にし、ゴールドイメージを作成します。
C. ランサムウェア認識プログラムを確立し、安全で検証可能なバックアップを実装します。
D.
仮想マシンの乳製品スナップショットを使用してすべてのエンドポイントを仮想化します。
Answer: C
Explanation:
Ransomware is a type of malware that encrypts the files or disks of a victim's device and demands a ransom for the decryption key. Ransomware can cause significant damage, disruption, and data loss for individuals and organizations. To prevent this type of incident in the future, the best strategy is to combine user education and data protection. A ransomware awareness program can help users recognize and avoid potential ransomware attacks, such as phishing emails, malicious attachments, or compromised websites. A secure and verifiable backup system can help users recover their data in case of a ransomware infection, without paying the ransom or relying on the attackers. A backup system should be regularly tested and updated, and stored offline or in a separate location from the original data.

QUESTION NO: 12
セキュリティ アナリストは、複数のホスト
マシンを観察しているときに、プログラムがデータをバッファに上書きしていることに気付きました。次のコントロールのうち、この問題を最も緩和するのはどれですか?
A. データ実行防止
B. 出力エンコーディング
C. プリペアド ステートメント
D. パラメータ化されたクエリ
Answer: A
Explanation:
Data execution prevention (DEP) is a security feature that prevents code from being executed in memory regions that are marked as data-only. This helps mitigate buffer overflow attacks, which are a type of attack where a program overwrites data to a buffer beyond its allocated size, potentially allowing malicious code to be executed. DEP can be implemented at the hardware or software level and can prevent unauthorized code execution in memory buffers. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention

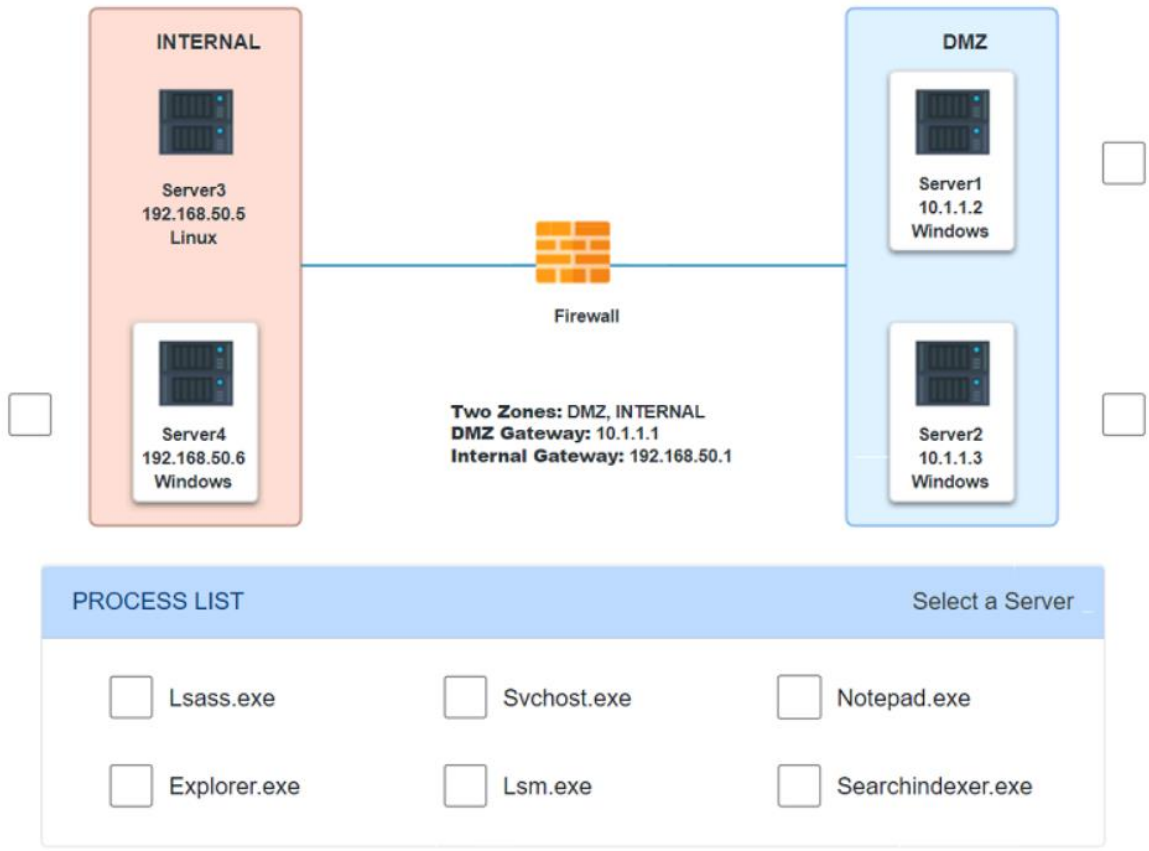
QUESTION NO: 13
以下は、システム構成をチェックする自動化されたアプローチを提供しますか?
A. SCAP
B. CI/CD
C. OVAL

D. Scripting
E. SOAR
Answer: A
Explanation:
SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications that allows automated configuration and vulnerability management of systems. SCAP provides an automated approach to checking a system configuration by using standardized expressions and formats to evaluate the system's compliance with predefined policies or benchmarks. CI/CD, OVAL, scripting, or SOAR are other terms related to automation or security, but they do not provide an automated approach to checking a system configuration. Reference: https://csrc.nist.gov/projects/security-content-automation-protocol

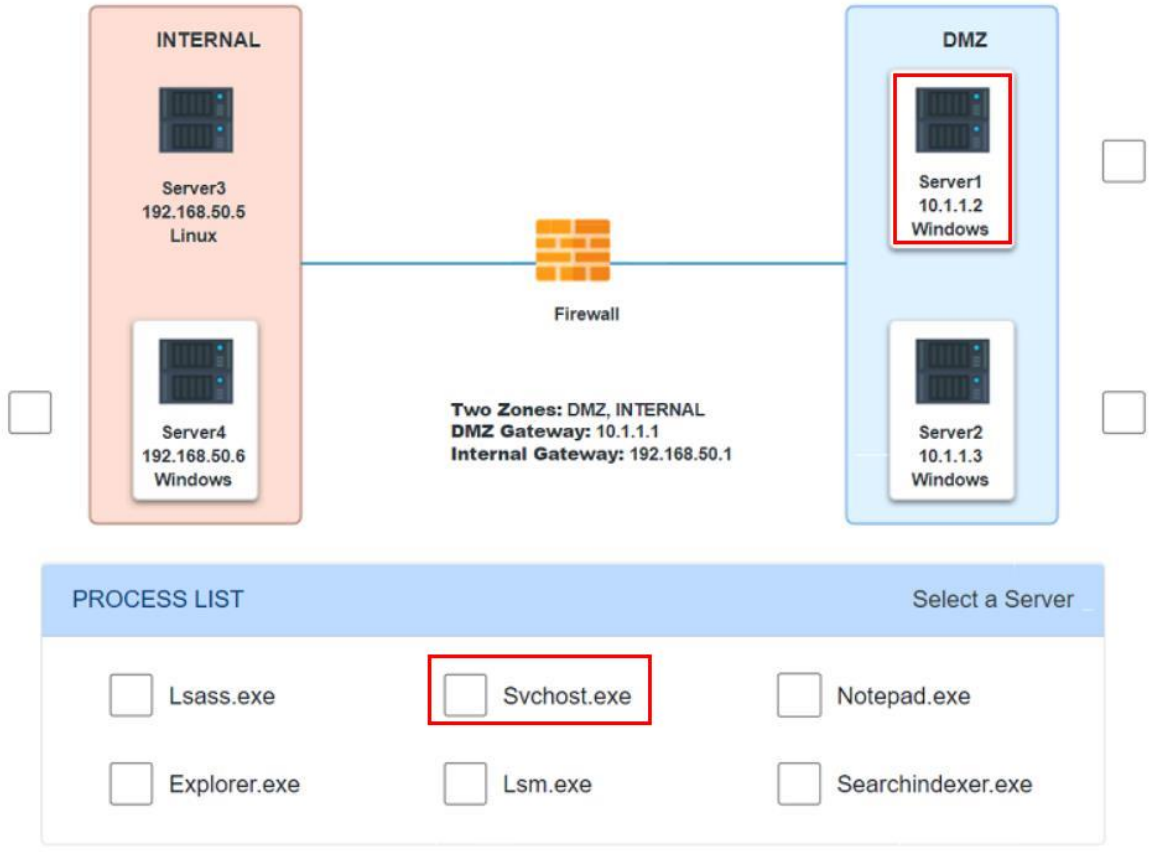
QUESTION NO: 14
環境内のサーバーにマルウェアが存在する可能性があります。
アナリストには、環境内のサーバーからコマンドの出力が提供され、サーバーの 1 つで実行されているプロセスがマルウェアである可能性があることを判断するために、すべての出力ファイルを確認する必要があります。
説明書
サーバー 1、2、および 4 はクリック可能です。マルウェアをホストするサーバーとプロセスを選択します。

Server1 Log

```
C:\Users\Team3>netstat -oan

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:49184          0.0.0.0:0              LISTENING       540
  TCP    0.0.0.0:49190          0.0.0.0:0              LISTENING       532
  TCP    10.1.1.2:57433         192.168.50.6:443       ESTABLISHED     1276
  TCP    10.1.1.2:50125         192.168.50.6:445       ESTABLISHED     276
  TCP    10.1.1.2:52349         192.168.50.6:139       ESTABLISHED     276
  TCP    10.1.1.2:139           0.0.0.0:0              LISTENING       4
  TCP    10.1.1.2:3389          172.30.0.148:49242     ESTABLISHED     348
  TCP    10.1.1.2:50741         172.30.0.101:445       ESTABLISHED     4
  TCP    10.1.1.2:50777         172.30.0.4:135         TIME_WAIT       0
  TCP    10.1.1.2:50778         172.30.0.4:49157       TIME_WAIT       0
  TCP    [::]:135               [::]:0                 LISTENING       540
  TCP    [::]:445               [::]:0                 LISTENING       4

C:\Users\Team3>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
```


INTERNAL
Server3
192.168.50.5
Linux
Server4
192.168.50.6
Windows
Firewall
Two Zones: DMZ, INTERNAL
DMZ Gateway: 10.1.1.1
Internal Gateway: 192.168.50.1
DMZ
Server1
10.1.1.2
Windows
Server2
10.1.1.3
Windows
PROCESS LIST
Select a Server
Lsass.exe
Svchost.exe
Notepad.exe
Explorer.exe
Lsm.exe
Searchindexer.exe

Answer:


INTERNAL
Server3
192.168.50.5
Linux
Server4
192.168.50.6
Windows
Firewall
Two Zones: DMZ, INTERNAL
DMZ Gateway: 10.1.1.1
Internal Gateway: 192.168.50.1
DMZ
Server1
10.1.1.2
Windows
Server2
10.1.1.3
Windows
PROCESS LIST
Select a Server
Lsass.exe
Svchost.exe
Notepad.exe
Explorer.exe
Lsm.exe
Searchindexer.exe

QUESTION NO: 15
予防的な脅威ハンティング手法として、ハンターは、利用可能な脅威インテリジェンス情報から導き出される可能性のある攻撃シナリオに基づいて、状況に応じたケースを作成する必要があります。シナリオの基礎を形成した後、脅威ハンターは脅威評価のフレームワークを確立するために次のうちどれを構築できますか？
A. 重要な資産リスト
B. 脅威ベクトル
C. 攻撃プロファイル
D. 仮説
Answer: D
Explanation:
A hypothesis is a statement that can be tested by threat hunters to establish a framework for threat assessment. A hypothesis is based on situational awareness and threat intelligence information, and describes a possible attack scenario that may affect the organization. A hypothesis can help to guide threat hunters in their investigation by providing a clear and specific question to answer, such as "Is there any evidence of lateral movement within our network?" or "Are there any signs of data exfiltration from our servers?".

QUESTION NO: 16
企業がプライバシー ポリシーとセキュリティ
ポリシーの両方を導入することが重要である理由を最もよく説明しているものは次のうちどれですか?
A. プライベート
データは設計上安全ではないため、異なるプログラムによって両方のポリシーに確実に対処できるようになります。
B. セキュリティ
ポリシーにより、データがプライバシー規制に準拠していることが自動的に保証されます。
C. プライバシー
ポリシーは、消費者および企業の機密データを保護するためのすべての規制を満たします。
D.
どちらの政策にも重複する部分がありますが、その違いは規制上の影響を与える可能性があります。
Answer: D
Explanation:
The correct answer is D. Both policies have some overlap, but the differences can have regulatory consequences. Privacy and security policies are both important for companies to protect their data and comply with various laws and regulations. However, privacy and security policies are not the same, and they have different goals and requirements.
Privacy policies are nontechnical controls that define how a company collects, uses, shares, and protects personal information from its customers, employees, or partners. Privacy policies are based on the principles of data minimization, consent, transparency, and accountability. Privacy policies aim to respect the rights and preferences of data subjects and comply with different privacy regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA)1.

Security policies are technical or nontechnical controls that define how a company protects its data and systems from unauthorized access, modification, or destruction. Security policies are based on the principles of confidentiality, integrity, and availability. Security policies aim to prevent or mitigate the impact of cyberattacks and comply with different security standards, such as the Payment Card Industry Data Security Standard (PCI DSS) or the ISO/IEC 27000 series2.
Privacy and security policies have some overlap, as they both involve data protection and compliance. However, they also have some differences, as they address different aspects and risks of data processing. For example, a company may have a strong security policy that encrypts its data, but it may still violate a privacy policy if it collects or shares more data than necessary or without consent. Conversely, a company may have a clear privacy policy that informs its customers about its data practices, but it may still suffer a security breach if it does not implement adequate security measures3.

QUESTION NO: 17
組織は、ユーザーが管理者アカウントにログインすることを禁止しています。ユーザーが昇格されたアクセス許可を必要とする場合。ユーザーのアカウントは管理者グループの一部である必要があり、ユーザーは必要に応じて一時的にのみアクセス許可をエスカレートする必要があります。システム
アクティビティをレビューする際、組織には次のレポートの優先順位があります。
* 成功した管理者ログイン レポートの優先度 - 高
* 管理者ログインの失敗を報告する優先度 - 中
* 一時的に権限を昇格できませんでした - 低
* 成功した一時的な権限の昇格 - 報告不可
セキュリティ アナリストがサーバーの syslog を確認すると、次のように表示されます。
次のイベントのうち、レポートの優先度が最も高いのはどれですか?

A. `<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success`

B. `<100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success`

C. `<100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success`

D. `<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe`

A. オプション A
B. オプション B
C. オプション C
D. オプション D
Answer: A
Explanation:
Option A shows a successful administrator login from an IP address that is not part of the organization's network. This is a high reporting priority event, because it violates the organization's policy that prohibits users from logging in to the administrator account and it could indicate a compromise of the administrator credentials or a malicious insider. Option B shows a failed administrator login from an IP address that is part of the organization's network. This is a medium reporting priority event, because it could indicate an unauthorized attempt to access the administrator account. Option C shows a failed temporary elevated permission request from a user account that is part of the organization's network. This is a

low reporting priority event, because it could indicate a user error or a legitimate need for elevated permission that was denied. Option D shows a successful temporary elevated permission request from a user account that is part of the organization's network. This is a non-reportable event, because it complies with the organization's policy that allows users to escalate permission only as needed and on a temporary basis. Reference: https://www.sans.org/reading-room/whitepapers/logging/detecting-attacks-systems-microsoft-windows-event-logs-2074

QUESTION NO: 18
次の攻撃手法のうち、Modbus
資産に対して迅速に成功する可能性が最も高いのはどれですか?
A. リモートコード実行
B. バッファオーバーフロー
C. 認証されていないコマンド
D. 証明書のなりすまし
Answer: C
Explanation:
Modbus is a communication protocol that is widely used in industrial control systems (ICS). Modbus does not have any built-in security features, such as authentication or encryption, which makes it vulnerable to various attacks. One of the most common and effective attack techniques against Modbus assets is to send unauthenticated commands to manipulate or disrupt the operation of the devices. Remote code execution, buffer overflow, and certificate spoofing are other attack techniques, but they have less likelihood of quick success against Modbus assets. Reference: https://www.sciencedirect.com/science/article/pii/S2405959517300045

QUESTION NO: 19
ソーシャルメディア会社が買収を計画しています。買収に先立って、最高セキュリティ責任者 (CSO) は、将来の企業のサイバーセキュリティ体制をより深く理解し、サプライチェーンのリスクを特定するために、完全なレポートを望んでいます。CSO の目的を最もよくサポートするものは次のうちどれですか?
A.第三者評価
B. 覚書
C.機密保持契約
D. ソフトウェアソースの信頼性
Answer: A
Explanation:
Third-party assessment. A third-party assessment is a process that explores the risk posed to your organization by third-party vendors along the supply chain. This process evaluates the likelihood that your business is exposed to different third-party risks such as compliance risk, operational risk, financial risk, security risk and cybersecurity risk1.
A third-party assessment can help the CSO gain a better understanding of the prospective company's cybersecurity posture by:
Providing an independent and objective evaluation of the vendor's security policies, controls, and practices.

Identifying any gaps or weaknesses in the vendor's security posture that could compromise your organization's data, systems, or reputation.
Recommending actions or improvements to mitigate or reduce the identified risks and enhance the vendor's security performance.
A third-party assessment can also help the CSO identify risks in the supply chain by:
Mapping and tracing the data flow and dependencies among the vendor and its subcontractors or suppliers.
Assessing how the vendor and its subcontractors or suppliers safeguard data and comply with relevant regulations and standards.
Detecting any signs of malicious or negligent behavior by the vendor or its subcontractors or suppliers that could harm your organization or its customers.

QUESTION NO: 20
サイバーセキュリティ
アナリストは、脅威インテリジェンスを通じてインシデント対応活動をサポートしています。アナリストが実行する可能性が最も高いのは次のうちどれですか?
A. 要件分析と収集計画
B. 封じ込めと根絶
C. 回復とインシデント後のレビュー
D. 指標の充実と研究の方向転換
Answer: D
Explanation:
Indicator enrichment and research pivoting are steps in the threat intelligence process that involve gathering additional information and context about the indicators of compromise (IoCs) that are related to an incident, and using them to identify other potential sources of threat data or evidence. For example, an analyst can enrich an IoC such as an IP address by looking up its geolocation, reputation, or associated domains, and then pivot to other sources of threat intelligence that may have more information about the IP address or its activities.

QUESTION NO: 21
企業の従業員の大多数は、古いワークステーションが原因で職務を遂行できないと述べているため、企業は BYOD
を導入することを決定しました。提案されたソリューションを保護するために、セキュリティ アナリストが最も推奨する可能性が高いのは次のうちどれですか?
A. Linux ベースのシステムと、すべての BYOD ユーザー向けの Linux
に関する必須トレーニング
B. クライアント デバイス用のファイアウォール環境と BYOO ユーザー用の安全な VDL
C. 標準化されたマルウェア対策プラットフォームと統一されたオペレーティング システム ベンダー
D. 802.1X は、BYOD ユーザー ハードウェアに会社のポリシーを適用します。
Answer: B
Explanation:
VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network.
A firewalled environment for client devices and a secure VDI (Virtual Desktop Infrastructure)

for BYOD users would be the most likely recommendation for securing the proposed solution. A firewalled environment can help isolate and protect the client devices from unauthorized network access or attacks. A secure VDI can provide a virtualized desktop environment for BYOD users that can be centrally managed and controlled by the organization. A VDI can also prevent data leakage or malware infection from BYOD devices, as the data and applications are stored on the server side rather than on the device itself5.

QUESTION NO: 22
シニア リーダーシップ チームの進行中の nsk
管理活動の一環として、最高情報セキュリティ責任者は、セキュリティ
アナリストに、新しいビジネス
イニシアチブまたは既存のビジネスに対する重要な変更に対応するための適切なトレーニングとテスト方法を調整するように命じました。管理チームは新しいビジネスを検討したいと考えています。既存のインフラストラクチャを使用して機密データを処理および保存するプロセス セキュリティ アナリストが調整するのに適しているのは、次のうちどれですか?
A. ブラックボックス侵入テストの取り組み
B. 卓上エクササイズ
C. 脅威モデリング
D. ビジネス インパクト分析
Answer: C
Explanation:
Threat modeling is a process that helps identify and analyze the potential threats and vulnerabilities of a system or process. It can help evaluate the security risks and mitigation strategies of a new business process that would use existing infrastructure to process and store sensitive data. A black-box penetration testing engagement, a tabletop exercise, or a business impact analysis are other methods that can be used to assess the security or resilience of a system or process, but they are not as appropriate as threat modeling for coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones. Reference: https://owasp.org/www-community/Application_Threat_Modeling

QUESTION NO: 23
次のうち、HSM を最もよく表しているのはどれですか?
A.
暗号化を管理し、トラフィックを復号化し、ライブラリ呼び出しを維持するコンピューティング デバイス
B. デジタル
キーを管理し、暗号化/復号化機能を実行し、その他の暗号化機能を維持するコンピューティング デバイス
C. 物理キーを管理し、デバイスを暗号化し、強力な暗号機能を作成するコンピューティング デバイス
D.
アルゴリズムを管理し、エントロピー機能を実行し、デジタル署名を維持するコンピューティング デバイス
Answer: B

Explanation:
HSM (Hardware Security Module) is a computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functions2. HSM is a dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. HSM can store cryptographic keys that are used for encryption, authentication, digital signatures, and other security functions. HSM can also generate random keys that are unique to each device and never leave the chip. HSM can protect these keys from unauthorized access or tampering by using hardware isolation and encryption3. HSM can also measure and verify the integrity of the operating system and firmware on a device by using a process called attestation. HSM does not manage cryptography (A), as cryptography is the science or art of creating and using secret codes. HSM does not manage physical keys, as physical keys are tangible objects that are used to lock or unlock something. HSM does not manage algorithms (D), as algorithms are sets of rules or instructions that are used to solve problems or perform tasks.

QUESTION NO: 24
組織には次の脆弱性修復ポリシーがあります。
* 本番環境サーバーの場合:
* CVSS スコアが 9.0 以上の脆弱性は 48 時間以内に修正する必要があります。
* CVSS スコアが 5.0 ~ 8.9 の脆弱性は 96 時間以内に修正する必要があります。
* 下位環境の脆弱性は最大 2 週間修正されないままになる場合があります。
* すべての脆弱性修復は、運用環境に適用する前にテスト環境で検証する必要があります。
組織には、運用環境とテスト環境という 2 つの環境があります。accountingProd
サーバーは、機密性の高い情報を含む唯一のサーバーです。
最近の脆弱性スキャンにより、次のレポートが提供されました。

Hostname	Environment	Vulnerability	CVSS score
timecardProd	Production	OS missing patch KB035	8.2
timecardTest	Testing	OS missing patch KB035	8.2
expenseProd	Production	OS missing patch KB022	7.1
expenseTest	Testing	OS missing patch KB022	7.1
accountingProd	Production	OS missing patch KB022	7.1
accountingTest	Testing	OS missing patch KB022	7.1
stagingTest	Testing	OS missing patch KB044	9.8

最初にパッチを適用する必要があるサーバーを特定するものは次のうちどれですか? (2つ選択してください)
A. タイムカード製品

B. タイムカードTesl
C. 経費製品
D. 経費テスト
E. 会計製品
F. 会計テスト
G. ステージングテスト
Answer: C,E
Explanation:
These servers should be patched first because they have vulnerabilities with CVSS scores of 9.0 and 8.9 respectively, which fall under the policy of remediating within 48 hours and 96 hours for production environment servers. The other servers either have lower CVSS scores, are in lower environments, or do not contain highly sensitive information.

QUESTION NO: 25
セキュリティ
アナリストは生データを関連付け、ランク付けし、人間または機械によって解釈されて結論を導き出し、実用的な推奨事項を作成するレポートに追加します。セキュリティ
アナリストが行っているインテリジェンス サイクルの次のステップはどれですか?
A. 分析と生産
B. 処理と利用
C. 普及と評価
D. データ収集
E. 企画・演出
Answer: B
Explanation:
Processing and exploitation is the step in the intelligence cycle that involves converting raw data into a format that can be used for analysis and producing intelligence products that can be disseminated to consumers. The security analyst is performing this step by correlating, ranking, and enriching raw data into a report. Analysis and production, dissemination and evaluation, data collection, and planning and direction are other steps in the intelligence cycle, but they do not match the description of the security analyst's task. Reference: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-cycle.html