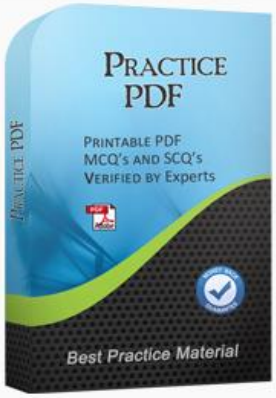
Actual4Cert

Actual4Cert

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

http://www.actual4cert.com/

We are a test cert center to provide the best and valid study material for all of you, and aim to help you pass.

Exam : **350-701J**

Title : Implementing and Operating Cisco Security Core Technologies (350-701日本語版)

Vendor : Cisco

Version : DEMO

QUESTION NO: 1
Cisco Email
Securityの2つの機能のうち、電子メールの脅威から組織を保護できるのはどれですか。（2つ選択してください）
A. 時間ベースのワンタイムパスワード
B. データ損失防止
C. ヒューリスティックベースのフィルタリング
D. ジオロケーションベースのフィルタリング
E. NetFlow
Answer: B D
Explanation:
Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.
Cisco Email Security appliance can now handle incoming mail connections and incoming messages from specific geolocations and perform appropriate actions on them, for example:
- Prevent email threats coming from specific geographic regions.
- Allow or disallow emails coming from specific geographic regions.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_00.html

QUESTION NO: 2
Cisco ASA FirePOWERモジュールがサポートする2つの展開モードはどれですか。（2つ選択してください。）
A. 透過モード
B. ルーテッドモード
C. インラインモード
D. アクティブモード
E. パッシブモニター専用モード
Answer: C D
Explanation:
You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm
/modules-sfr.html

QUESTION NO: 3
NetFlowフローで定義されている2つのフィールドはどれですか？（2つ選択してください）
A. サービスバイトのタイプ
B. サービスクラスビット
C. レイヤー4プロトコルタイプ
D. 宛先ポート

E. 出力論理インターフェース
Answer: A D
Explanation:
Explanation:
Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:
+ Ingress interface (SNMP ifIndex)
+ Source IP address
+ Destination IP address
+ IP protocol
+ Source port for UDP or TCP, 0 for other protocols
+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
+ IP Type of Service
Note: A flow is a unidirectional series of packets between a given source and destination.

QUESTION NO: 4
Cisco DNA Center で使用される Integration API の 2 つの機能はどれですか?
(2つ選んでください)
A. スイッチおよびルーターのソフトウェアをアップグレードする
B. 第三者報告
C. ITSM プラットフォームに接続する
D. ワイヤレス LAN コントローラーで新しい SSID を作成する
E. 新しい仮想ルーターを自動的にデプロイします
Answer: B C
Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/integration-api- westbound

QUESTION NO: 5
GETVPNとIPsecの違いは何ですか？
A. GETVPNは、中央ハブを使用せずに、遅延を削減し、MPLSを介した暗号化を提供します
B. GETVPNは、キー管理とセキュリティアソシエーション管理を提供します
C. GETVPNはIKEv2に基づいており、IKEv1をサポートしていません
D.
GETVPNは、すべてのデバイスを静的に構成することなく、複数のサイトでVPNネットワークを構築するために使用されます
Answer: C

QUESTION NO: 6
展示を参照してください。

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept' : application/json
    'content-type' : application/json
    'authorization' : Basic API Credentials
    'cache-control' : "no cache"
}
response = requests.request ("GET", url, headers = headers)
print (response.txt)
```

このPythonスクリプトを実行するとどうなりますか？

A. 侵害されたコンピュータとマルウェアの軌跡はCiscoAMPから受信されます

B. コンピュータとその現在の脆弱性のリストはCiscoAMPから受信されます

C. 侵害されたコンピュータとその侵害されたコンピュータはCiscoAMPから受信されます

D.
コンピュータ、ポリシー、およびコネクタのステータスのリストがCiscoAMPから受信されます

Answer: D

Explanation:

The call to API of "https://api.amp.cisco.com/v1/computers" allows us to fetch list of computers across your organization that Advanced Malware Protection (AMP) sees

Reference: https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.amp.cisco.com&api_resource=Computer&api_version=v1

QUESTION NO: 7

組織にポリシーが設定されたCiscoESAがあり、違反に割り当てられたアクションをカスタマイズしたいと考えています。組織は、メッセージのコピーを配信し、メッセージを追加してDLP違反としてフラグを立てることを望んでいます。この機能を提供するには、どのアクションを実行する必要がありますか？

A. コピーを他の受信者に配信および送信する

B. DLP違反通知を隔離して送信する

C. DLP違反でサブジェクトヘッダーを隔離および変更する

D. 免責事項のテキストを配信して追加する

Answer: D

Explanation:

Explanation:

You specify primary and secondary actions that the appliance will take when it detects a possible DLP violation in an outgoing message. Different actions can be assigned for different violation types and severities.

Primary actions include:

- Deliver
- Drop
- Quarantine

Secondary actions include:

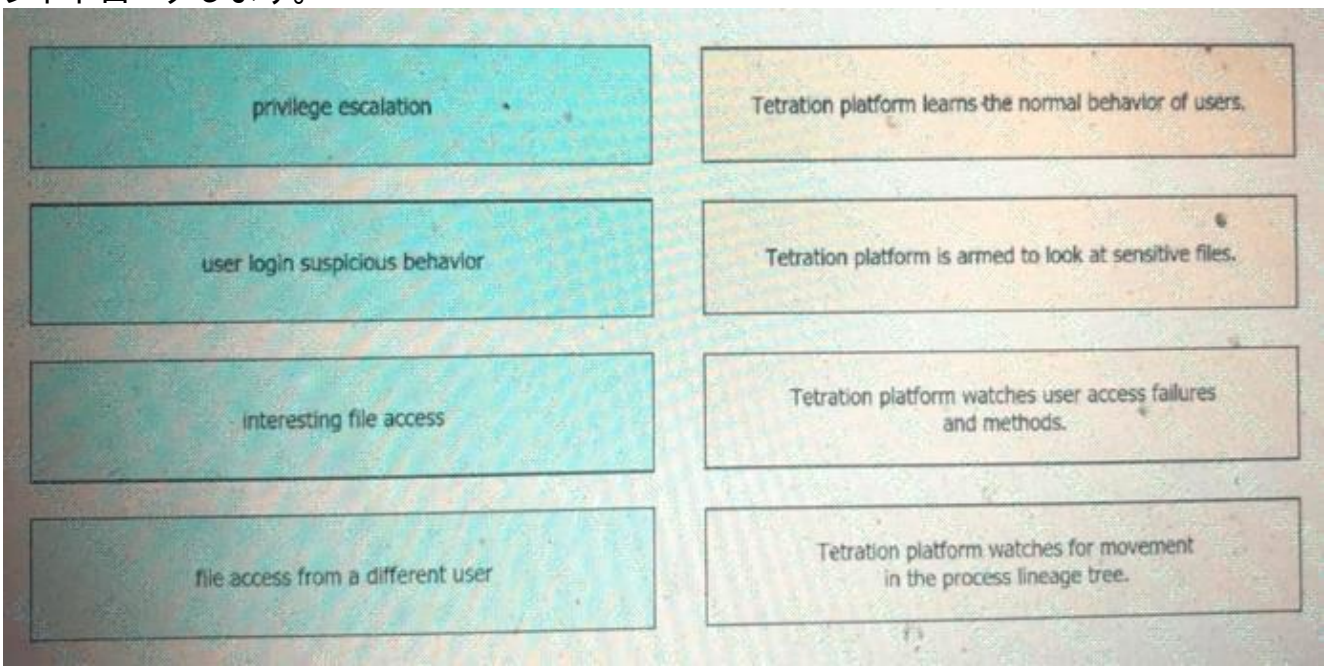
- Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a

perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.
- Encrypting messages. The appliance only encrypts the message body. It does not encrypt the message headers.
- Altering the subject header of messages containing a DLP violation.
- Adding disclaimer text to messages.
- Sending messages to an alternate destination mailhost.
- Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)
- Sending a DLP violation notification message to the sender or other contacts, such as a manager or DLP compliance officer.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

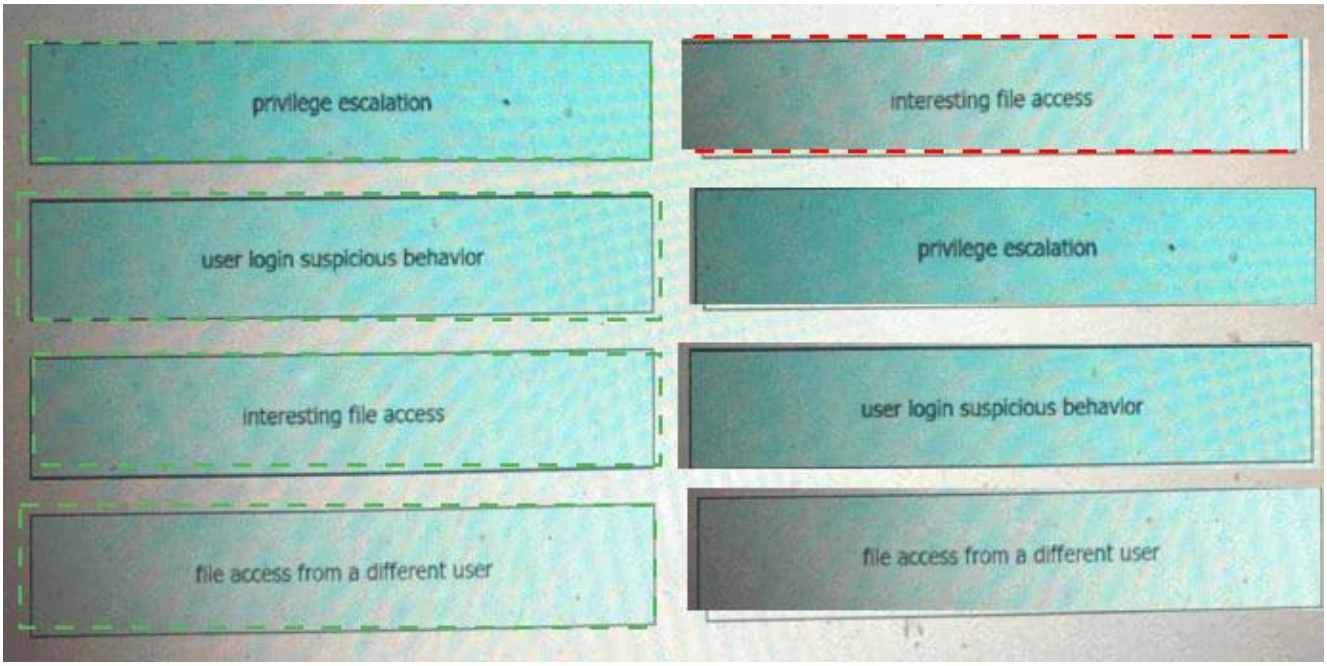
QUESTION NO: 8
Cisco
ISE内のどの機能が、ネットワークへのアクセスを提供する前にエンドポイントのコンプライアンスを検証しますか。
A. 姿勢
B. プロファイリング
C. pxGrid
D. MAB
Answer: A
Explanation:
Posture is a feature within Cisco ISE that verifies the compliance of an endpoint before providing access to the network. Posture assessment checks the state of the endpoint, such as the operating system, antivirus, firewall, patches, and so on, against the predefined policies. If the endpoint does not meet the policy requirements, it can be remediated by installing or updating the necessary software or configuration. Posture assessment can be done for both wired and wireless endpoints, as well as VPN clients. Posture assessment requires the installation of a posture agent on the endpoint, which communicates with the posture service on the ISE server. The posture agent can be either a persistent agent, which runs in the background and provides continuous assessment, or a temporal agent, which runs on-demand and is removed after the assessment is complete. Posture assessment can be integrated with 802.1X or web authentication methods for network access control.
References := Some possible references are:
* ISE Posture Prescriptive Deployment Guide
* ISE Posture Deployment Best Practices and Considerations
* Understanding ISE Posture Services

QUESTION NO: 9
Cisco
Tetrationプラットフォームの疑わしいパターンを、左側から右側の正しい定義にドラッグア

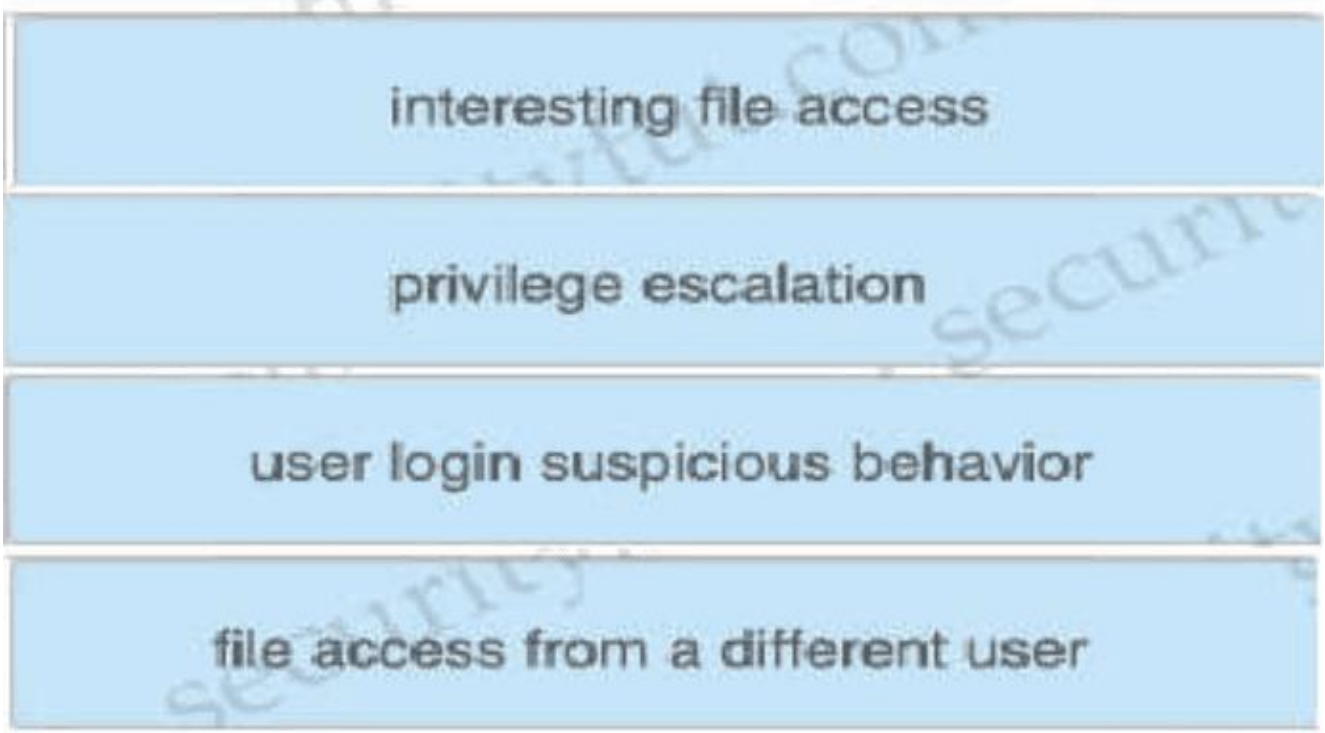
ンドドロップします。



Answer:



Explanation:



Explanation:
Cisco Tetration platform studies the behavior of the various processes and applications in the workload, measuring them against known bad behavior sequences. It also factors in the process hashes it collects. By studying various sets of malwares, the Tetration Analytics engineering team deconstructed it back into its basic building blocks. Therefore, the platform understands clear and crisp definitions of these building blocks and watches for them.
The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.
Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.
+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform.
Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics
/whitepaper-c11-740380.html

QUESTION NO: 10
どのCiscoDNACenter RESTful PNP
APIがデバイスをワークフローに追加し、要求しますか？
A. api/v1/fie/config
B. api/v1/onboarding/pnp-device/import
C. api/v1/onboarding/pnp-device
D. api/v1/onboarding/workflow
Answer: B
Explanation:
The Cisco DNA Center RESTful PNP API allows external applications to interact with the Plug and Play (PNP) service of Cisco DNA Center, which automates the onboarding and provisioning of network devices.
The PNP API has several endpoints for different operations, such as importing, claiming, updating, and deleting devices. The endpoint that adds and claims a device into a workflow is api/v1/onboarding/pnp-device
/import, which takes a JSON payload with the device information and the workflow ID. This endpoint creates a new device entry in the PNP database and associates it with the specified workflow. The workflow defines the configuration template, image, and license to be applied to the device during the provisioning process12. References:
* 1: See How to Use the Plug and Play API in DNA Center - Part 2
* 2: Cisco DNA Center Platform User Guide, Release 2.2.3

QUESTION NO: 11
Cisco DNA Centerのオープンプラットフォーム機能の機能は何ですか？
A. インテントベースのAPI
B. 自動化アダプター
C. ドメイン統合
D. アプリケーションアダプタ
Answer: A
Explanation:
Cisco DNA Center is an open and extensible platform that allows third-party applications and processes to exchange data and intelligence with Cisco DNA Center1. One of the features of the open platform capabilities of Cisco DNA Center is the intent-based APIs, which enable DNA Center to provide automation to applications2. Intent-based APIs allow applications to express their intent or desired outcome, and let DNA Center translate that intent into network configurations and policies3. Intent-based APIs simplify the interaction between applications and the network, and enable faster and more consistent service delivery.
1: Cisco DNA Center 2.3.5 Data Sheet - Cisco 2: Intent-Based Networking's Next Evolution: The DNA Center Platform - Cisco Blogs 3: Unlocking the Power of Open Platforms with Cisco DNA Center Platform

QUESTION NO: 12
シスコ内のどのグループが、サイバーセキュリティの専門家が進行中の最も蔓延している脅威を認識し続けるのに役立つ週刊ニュースレターを作成および発行していますか？

A. PSIRT
B. タロス
C. CSIRT
D. DEVNET
Answer: B
Explanation:
Explanation:
Talos Threat Source is a regular intelligence update from Cisco Talos, highlighting the biggest threats each week and other security news.
Reference: https://talosintelligence.com/newsletters

QUESTION NO: 13
どの攻撃が Web サーバー上のファイルへの不正アクセスを可能にしますか?
A. 分散型DoS攻撃
B. ブロードキャストストーム
C. DHCPスヌーピング
D. パストラバーサル
Answer: D

QUESTION NO: 14
組織内にMFAを実装することが重要なのはなぜですか？
A. 中間者攻撃が成功するのを防ぐため。
B. DoS攻撃が成功しないようにするため。
C. ブルートフォース攻撃が成功するのを防ぐため。
D. フィッシング攻撃の成功を防ぐため。
Answer: C
Explanation:
Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy1. MFA is important to implement inside of an organization because it can prevent brute force attacks from being successful. A brute force attack is a type of cyberattack that tries to guess the user's password or PIN by trying different combinations until it finds the correct one. This can be done manually or with automated tools. MFA can stop brute force attacks by requiring an additional factor of authentication that the attacker does not have, such as a phone, a token, a biometric, or a location. MFA can also reduce the risk of other types of attacks that rely on stealing or compromising the user's credentials, such as phishing, keylogging, or credential stuffing. References := 1:
What is Multi-Factor Authentication (MFA)? | OneLogin

QUESTION NO: 15
Cisco ESAでは防止できるがCiscoWSAでは防止できない攻撃はどれですか。
A. バッファオーバーフロー
B. DoS

C. SQLインジェクション
D. フィッシング
Answer: D
Explanation:
Explanation:
The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway:
Prevents the following:
+ Attacks that use compromised accounts and social engineering.
+ Phishing, ransomware, zero-day attacks and spoofing.
+ BEC with no malicious payload or URL.
Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

QUESTION NO: 16
Cisco Secure Cloud Analytics 管理者は、オンプレミス環境を監視するためにプライベート ネットワーク モニター
センサーを設定しています。このセンサーから取得される情報のうち、Secure Cloud Analytics ポータルへのリンクに使用されるものはどれですか。(2 つ選択してください。)
A. 一意のサービスキー
B. NAT ID
C. SSL証明書
D. パブリックIPアドレス
E. プライベートIPアドレス
Answer: A B

QUESTION NO: 17
Cognitive Threat Analyticsの2つの検出および分析エンジンとは何ですか？
（2つ選択してください。）
A. データの引き出し
B. コマンドおよび制御通信
C. インテリジェントプロキシ
D. snort
E. URLの分類
Answer: A B
Explanation:
Cisco Cognitive Threat Analytics helps you quickly detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment. The solution automatically identifies and investigates suspicious or malicious web-based traffic. It identifies both potential and confirmed threats, allowing you to quickly remediate the infection and reduce the scope and damage of an attack, whether it's a known threat campaign that has spread across multiple organizations or a unique threat you've never seen before.

Detection and analytics features provided in Cognitive Threat Analytics are shown below:
+ Data exfiltration: Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content
+ Command-and-control (C2) communication: Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPSencoded or anonymous traffic, including Tor, without any need to decrypt transferred content, detecting a broad range of threats
...
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at- aglance-c45-736555.pdf

QUESTION NO: 18
Cisco ASA Netflow v9セキュアイベントロギングの特徴は何ですか？
A. フロー作成、フローティアダウン、およびフロー拒否イベントを追跡します
B.
特定のフローのすべてのレコードをエクスポートするステートレスIPフロー追跡を提供します
C. フローを継続的に追跡し、10秒ごとに更新を提供します。
D. そのイベントはすべてのトラフィッククラスに並行して一致します。
Answer: A
Explanation:
The ASA and ASASM implementations of NetFlow Secure Event Logging (NSEL) provide a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow.
The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs).
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html

QUESTION NO: 19
DoS攻撃とDDoS攻撃の違いは何ですか？
A.
DoS攻撃は、コンピューターを使用してサーバーをTCPパケットとUDPパケットで溢れさせる攻撃ですが、DDoS攻撃は、複数のシステムがDoS攻撃で単一のシステムを標的にする攻撃です。
B.
DoS攻撃は、コンピューターを使用してサーバーをTCPおよびUDPパケットでフラッディングする場所ですが、DDoS攻撃は、コンピューターを使用して、LAN上に分散されている複数のサーバーをフラッディングする場所です。

C.
DoS攻撃は、コンピューターを使用してサーバーをUDPパケットでフラッディングする場所ですが、DDoS攻撃は、コンピューターを使用してサーバーをTCPパケットでフラッディングする場所です。
D.
DoS攻撃は、コンピューターを使用してサーバーをTCPパケットでフラッディングする場所ですが、DDoS攻撃は、コンピューターを使用してサーバーをUDPパケットでフラッディングする場所です。
Answer: A
Explanation:
A DoS (Denial of Service) attack is a type of cyberattack that aims to disrupt the normal functioning of a server, service, or network by overwhelming it with a large amount of traffic or requests. A DoS attack typically uses a single computer or device to launch the attack, sending TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) packets to the target server. TCP and UDP are two common protocols used to send data over the internet. TCP packets require a connection to be established between the sender and the receiver, and ensure that the data is delivered reliably and in order. UDP packets do not require a connection, and do not guarantee the delivery or order of the data. Both TCP and UDP packets can be used to flood a server with requests, consuming its resources and bandwidth, and preventing legitimate users from accessing the service.
A DDoS (Distributed Denial of Service) attack is a type of DoS attack that uses multiple computers or devices to launch the attack, creating a large network of attackers that can generate more traffic or requests than a single source. A DDoS attack often involves a botnet, which is a network of compromised computers or devices that are controlled by a malicious actor, usually through malware or hacking. The botnet can send TCP or UDP packets to the target server from different locations and IP addresses, making it harder to trace and block the attack. A DDoS attack can also target multiple servers or services that are distributed over a LAN (Local Area Network), such as a web hosting service or a cloud computing platform, affecting the availability and performance of the entire network.
The main difference between a DoS attack and a DDoS attack is the number and diversity of the sources that are involved in the attack. A DoS attack comes from a single source, while a DDoS attack comes from multiple sources. This makes a DDoS attack more powerful, faster, and harder to stop than a DoS attack.
References:
Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 1: Malware Threats, Lesson 2: Identifying Network Attacks, Topic: DoS and DDoS Attacks DoS Attack vs. DDoS Attack: Key Differences? | Fortinet What's the Difference Between a DOS and DDoS Attack? - How-To Geek

QUESTION NO: 20
プライベートネットワーク、パブリッククラウド、暗号化されたトラフィック全体の脅威を検出するソリューションはどれですか？
A. Cisco Stealthwatch
B. Cisco CTA
C. Cisco Encrypted Traffic Analytics

D. Cisco Umbrella

Answer: A

Explanation:

Cisco Stealthwatch is the only solution that detects threats across your private network, public clouds, and encrypted traffic. It uses network telemetry and advanced behavioral analytics to monitor network activity and identify anomalies that indicate potential threats. It also leverages Cisco Encrypted Traffic Analytics (ETA) to detect malware in encrypted traffic without decryption. Cisco Stealthwatch provides visibility, threat detection, and response across your entire network and cloud environment1234 References := 1: Cisco Stealthwatch detects threats across private networks, public clouds, and encrypted traffic - Cisco Blogs 2: The XDR Solution to the Ransomware Problem - Cisco Blogs 3: Network Threat Detection and Response with Cisco Stealthwatch - Locuz 4: Cisco Secure Network Analytics (Stealthwatch) - Cisco

QUESTION NO: 21

フィッシング攻撃からユーザーを保護するエンドポイントソリューションはどれですか？

A. Cisco Identity Services Engine

B. ISEポスチャモジュールを備えたCisco AnyConnect

C. Cisco AnyConnect with NetworkAccessManagerモジュール

D. CiscoAnyConnectとUmbrellaRoamingSecurityモジュール

Answer: D

Explanation:

Cisco AnyConnect with Umbrella Roaming Security module protects a user from a phishing attack by enforcing security at the DNS layer and blocking malicious domains that are used for phishing campaigns.

The Umbrella Roaming Security module integrates with the Cisco AnyConnect client and provides always-on security even when no VPN is active. The Umbrella Roaming Security module can replace the existing Cisco Umbrella roaming client or be part of a new AnyConnect deployment12.

Cisco Identity Services Engine (ISE) is not an endpoint solution, but a network access control and policy enforcement platform that can integrate with AnyConnect for posture assessment and compliance3. Cisco AnyConnect with ISE Posture module is used to check the compliance status of the endpoint device and apply the appropriate network access policy based on the posture result4. Cisco AnyConnect with Network Access Manager module is used to manage the network connections and profiles of the endpoint device and support various authentication methods5. Neither of these modules directly protect the user from a phishing attack.

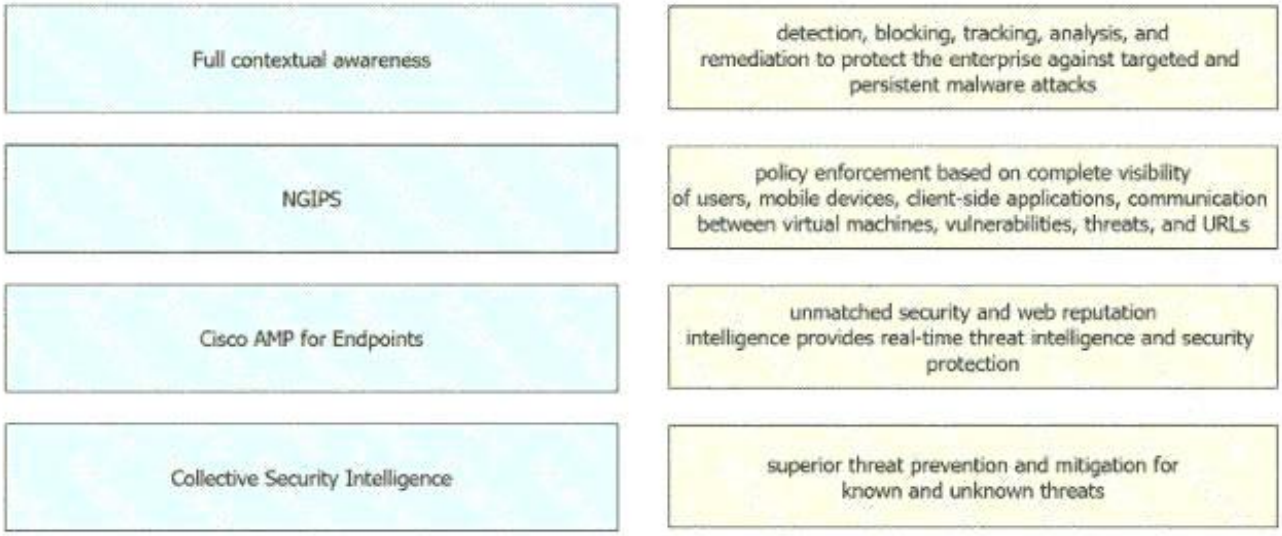
References :=

* Roaming Client: Umbrella Roaming Security (Integration with AnyConnect)
* Secure Umbrella Roaming: Cisco Secure Client (Formerly AnyConnect)
* Cisco Identity Services Engine
* [Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Posture Module]
* [Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9 - Network Access Manager Module]

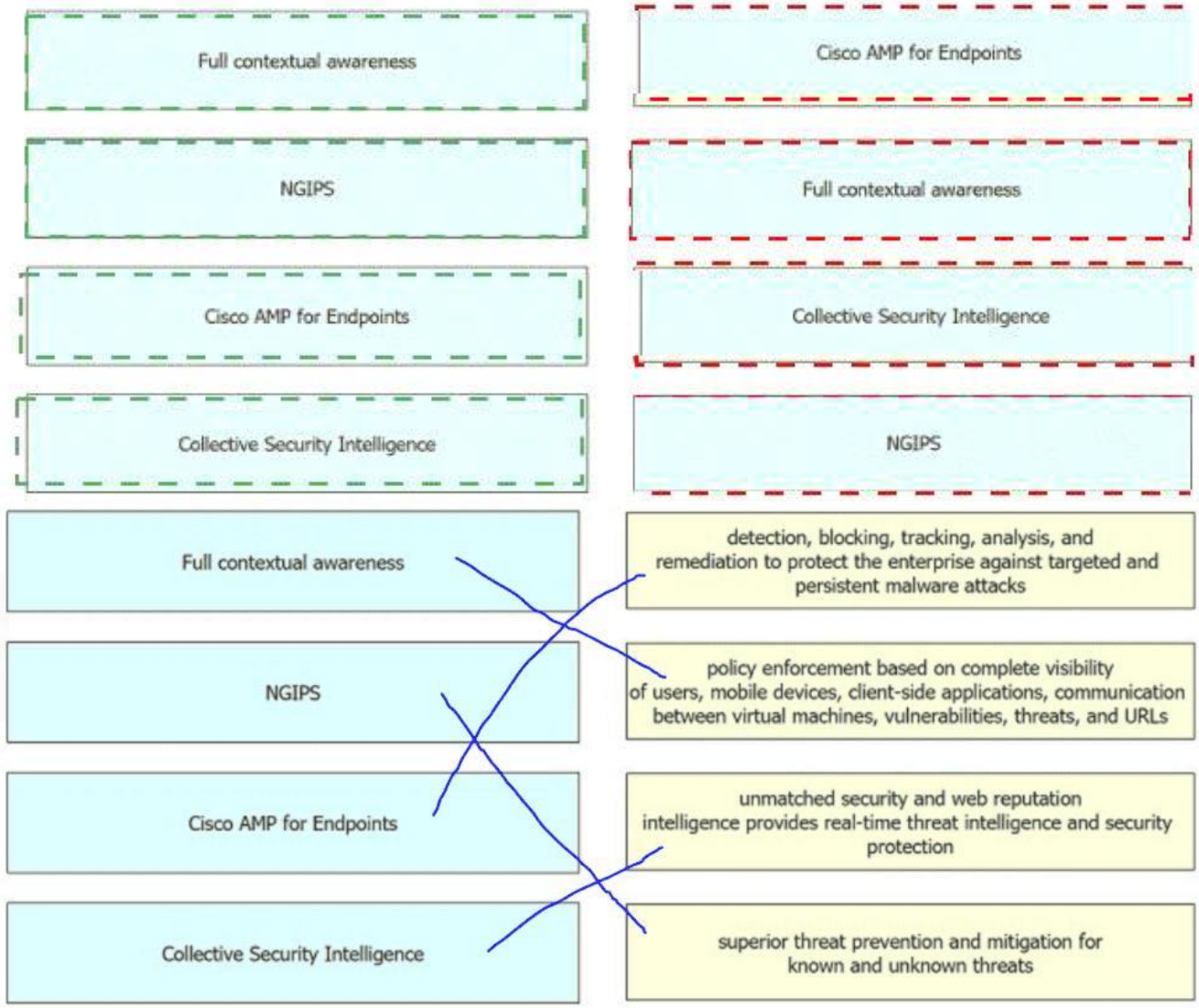
QUESTION NO: 22
組織には、Webアプリケーションをホストする2台のマシンがあります。マシン1はSQLインジェクションに対して脆弱ですが、マシン2はバッファオーバーフローに対して脆弱です。攻撃者がマシン1にアクセスできるが、マシン2にはアクセスできないようにするアクションは何ですか？
A. 2つのホスト間のパケットをスニッフィングする
B. 継続的なpingの送信
C. バッファのメモリがオーバーフローしています
D. 悪意のあるコマンドをデータベースに挿入する
Answer: D
Explanation:
A SQL injection attack is a type of attack that exploits a vulnerability in a web application that uses user- supplied data to construct SQL statements that interact with a database. By inserting malicious commands into the database, an attacker can execute arbitrary SQL queries or commands on the database server, which may result in data theft, data manipulation, or command execution. Machine 1 is vulnerable to SQL injection because it does not properly validate or sanitize the user input before using it in a SQL statement. Therefore, inserting malicious commands into the database would allow the attacker to gain access to machine 1.
A buffer overflow attack is a type of attack that exploits a vulnerability in a program that does not check the boundaries of a buffer (a temporary storage area for data) before copying data into it. By overflowing the buffer's memory, an attacker can overwrite adjacent memory locations, which may result in corrupting data, crashing the program, or executing malicious code. Machine 2 is vulnerable to buffer overflow because it does not properly handle the size or length of the data that it receives from the user or another source.
Therefore, overflowing the buffer's memory would allow the attacker to gain access to machine 2.
Sniffing the packets between the two hosts is a passive attack that involves capturing and analyzing the network traffic that flows between the two machines. This attack may reveal sensitive information, such as credentials, session tokens, or database queries, but it does not directly allow the attacker to gain access to either machine. Sending continuous pings is a type of denial-of-service attack that involves flooding the target machine with ICMP echo request packets, which may consume its network bandwidth or processing resources, but it does not directly allow the attacker to gain access to either machine. Therefore, neither sniffing the packets nor sending continuous pings would allow the attacker to gain access to machine 1 but not machine 2. References :=
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Web Security, SQL Injection Attacks
* Understanding SQL Injection - Cisco, SQL Injection Explained
* Buffer Overflow and SQL Injection: To Remotely Attack and ... - Springer, Buffer Overflow and SQL Injection Attacks

QUESTION NO: 23
セキュリティソリューションを左側から右側に提供するメリットにドラッグアンドドロップ

します。



Answer:



QUESTION NO: 24
Cisco WSAのレイヤ4トラフィックモニタの機能は何ですか？

A.
悪意のあるコンテンツが含まれていることがわかっているURLカテゴリからのトラフィックをブロックします
B. SSLトラフィックを復号化して、悪意のあるコンテンツを監視します
C. すべてのTCP/UDPポートで疑わしいトラフィックを監視します
D.
指定された機密情報をすべてのネットワークトラフィックで検索することにより、データの漏えいを防ぎます
Answer: C

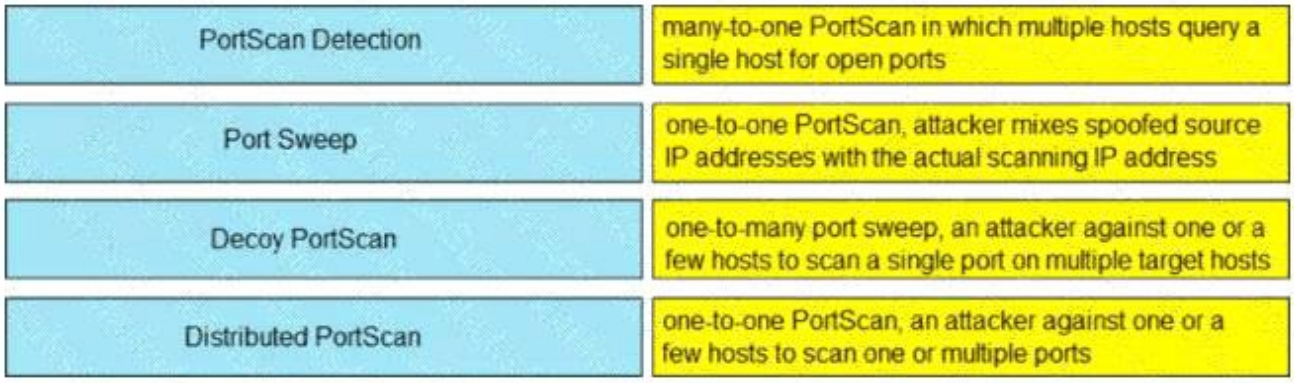
QUESTION NO: 25
ソーシャルエンジニアリングはどのタイプの攻撃ですか？
A. trojan
B. phishing
C. malware
D. MITM
Answer: B
Explanation:
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.

QUESTION NO: 26
公開鍵と秘密鍵を使用する暗号化のタイプはどれですか？
A. 非対称
B. 対称
C. 線形
D. 非線形
Answer: A
Explanation:
Asymmetric encryption, also known as public key cryptography, uses two different keys for encryption and decryption: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret. Data encrypted with the public key can only be decrypted with the private key, and vice versa. This ensures that only the intended recipient can access the encrypted data, and that the sender can prove their identity with a digital signature. Asymmetric encryption is widely used for securing Internet communications, such as TLS/SSL, which enables HTTPS. Some examples of asymmetric encryption algorithms are RSA, Diffie-Hellman, and Elliptic Curve Cryptography. The other options are not correct because they do not use a public key and private key. Symmetric encryption uses the same key for encryption and decryption, and is faster and more efficient than asymmetric encryption. However, symmetric encryption requires a secure way to exchange the key between the sender and the receiver, which can be facilitated by asymmetric encryption. Linear and nonlinear encryption are not types of encryption, but rather properties of

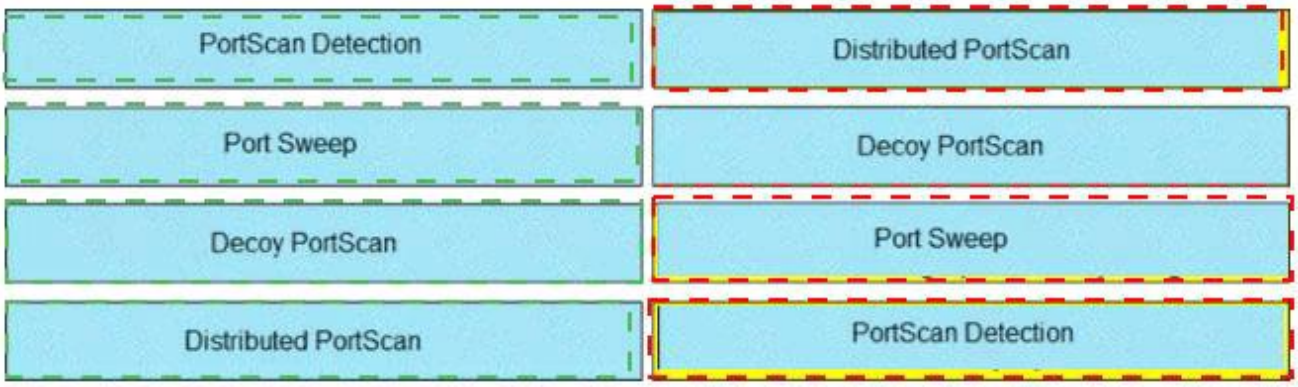
encryption algorithms. A linear encryption algorithm is one that can be expressed as a linear function, such as XOR. A nonlinear encryption algorithm is one that involves more complex mathematical operations, such as modular arithmetic or S-boxes. Nonlinear encryption algorithms are generally more secure and resistant to cryptanalysis than linear encryption algorithms. References :=
* Public-key cryptography - Wikipedia
* How does public key cryptography work? - Cloudflare
* Public and private encryption keys | PreVeil
* AES encryption, what are public and private keys?

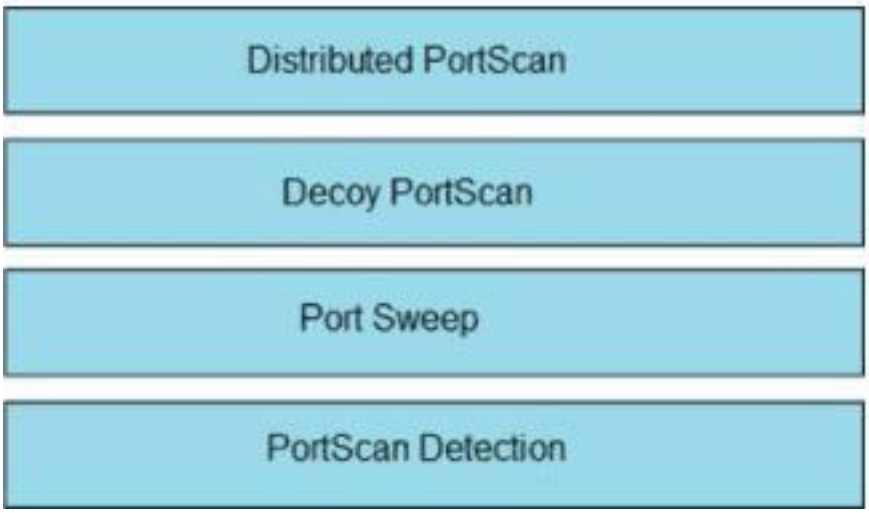
QUESTION NO: 27
EPP と EDR の違いは何ですか?
A. EDR は境界での防止にのみ焦点を当てます。
B. EPP
ソリューションを導入すると、エンジニアは最新の脅威を検出し、調査し、修復できるようになります。
C. EDR
ソリューションを導入すると、エンジニアは悪意のある動作の兆候が最初に現れたときに、問題のあるファイルにフラグを立てることができます。
D. EPP は主に、最前線の防御を回避して環境に侵入した脅威に焦点を当てます。
Answer: C

QUESTION NO: 28
右上の正しい定義に左から火力と次世代侵入防止システム検出器をドロップします。



Answer:





QUESTION NO: 29
データセキュリティのためのCiscoCloudlockの機能は何ですか？
A. データ損失防止
B. 悪意のあるクラウドアプリを制御します
C. 異常を検出します
D. ユーザーとエンティティの行動分析
Answer: A
Explanation:
The function of Cisco Cloudlock for data security is data loss prevention (DLP). Cisco Cloudlock is a cloud- native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cloudlock's simple, open, and automated approach uses APIs to manage the risks in your cloud app ecosystem1. One of the key features of Cloudlock is its DLP technology, which continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies as well as highly tunable custom policies. You can use Cloudlock's DLP to prevent data breaches, comply with regulations, and enforce data governance across SaaS, PaaS, and IaaS platforms2. References: 1:
Cisco Cloudlock - Cisco2: Cloudlock: Cloud User Security - Cisco Umbrella.

QUESTION NO: 30
Cisco Secure Web Appliance が Web
要求をチェックする際、ユーザー定義のポリシーと一致しない場合はどうなりますか?
A. 次の識別プロファイル ポリシーを適用します。
B. 高度なポリシーを適用します。
C. グローバルポリシーを適用します。
D. リクエストをブロックします。
Answer: C

QUESTION NO: 31
エンジニアは、Cisco AnyConnect セキュア モビリティ クライアント ソリューションと Cisco Secure Firewall を使用して、既存のリモート アクセス VPN

を変更する必要があります。現在、ユーザーによって生成されるトラフィックはすべて VPN
トンネルに送信されるため、エンジニアは一部のサーバーを除外し、代わりにそれらのサーバーに直接アクセスする必要があります。このヤギを実現するにはどの要素を変更する必要がありますか?

A. NAT の除外
B. 暗号化ドメイン
C. ルーティング テーブル
D. グループポリシー

Answer: D

Explanation:
To achieve the goal of excluding some servers from the VPN tunnel and accessing them directly, the engineer must modify the group policy that is applied to the remote access VPN users. The group policy contains the settings for split tunneling, which is a feature that allows the VPN client to route some traffic through the VPN tunnel and some traffic directly to the internet. Split tunneling can be configured based on the destination IP address, the application, or the domain name of the traffic. By modifying the group policy, the engineer can specify which servers or networks should be excluded from the VPN tunnel and accessed directly by the VPN client. This can improve the performance and efficiency of the VPN connection, as well as reduce the load on the VPN gateway and the corporate network. However, split tunneling also introduces some security risks, such as exposing the VPN client to internet threats, bypassing the corporate firewall and security policies, and leaking sensitive data. Therefore, the engineer must carefully evaluate the trade-offs and best practices of using split tunneling for remote access VPNs. References :=
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 3: Secure Connectivity, Lesson 3.1: Implementing and Troubleshooting Remote Access VPN, Topic 3.1.4:
Configure and Verify Remote Access VPN, Subtopic 3.1.4.2: Configure and Verify Split Tunneling
* VPN Split Tunneling: What It Is & Pros and Cons
* Cisco ASA - Enable Split Tunnel for Remote VPN Clients

QUESTION NO: 32
組織が複数のCiscoFTDアプライアンスを導入し、1つの集中型ソリューションを使用してそれらを管理したい組織にはローカルVMはありませんが、CiscoFTDに移行する必要のある既存のCiscoASAがあります。組織のニーズを満たすソリューションはどれですか。

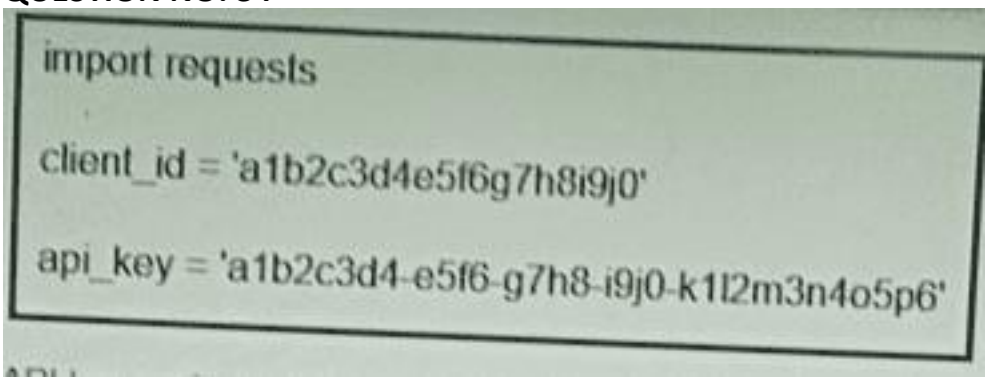
A. Cisco FMC
B. CSM
C. Cisco FDM
D. CDO

Answer: A

Explanation:
Cisco FMC is the centralized management solution for Cisco FTD appliances. It provides configuration, monitoring, analysis, and reporting capabilities for FTD devices. Cisco FMC

can also manage Cisco ASAs that have been converted to FTD devices. Cisco FMC can be deployed as a physical or virtual appliance, or as a cloud service (CDO). However, since the organization does not have a local VM, CDO is not an option.
Cisco FDM is the on-box management solution for FTD devices, which does not support centralized management or ASA migration. CSM is the legacy management solution for Cisco ASAs, which does not support FTD devices. References := Some possible references are:
* Cisco Firepower Management Center Configuration Guide, Version 6.7
* Install and Upgrade FTD on Firepower Appliances
* Firepower Threat Defense simplifies application security

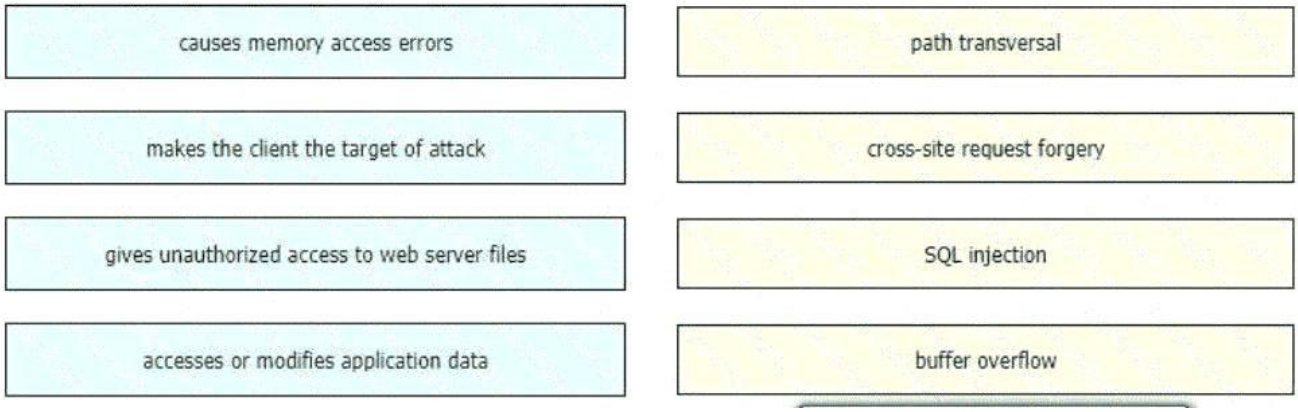
QUESTION NO: 33
ネットワークの可視性、脅威の検出、分析をパブリッククラウド環境に拡張するシスコのソリューションはどれですか。
A. Cisco Umbrella
B. Cisco Stealthwatch Cloud
C. Cisco Appdynamics
D. Cisco CloudLock
Answer: B
Explanation:
Cisco Stealthwatch Cloud is a network detection and response (NDR) solution that leverages pre-existing infrastructure to offer enterprise-wide, contextual visibility of network traffic from the private network to the public cloud1. It uses advanced analytics and machine learning to detect threats and anomalies across on- premises and cloud environments, and provides actionable alerts and recommendations to remediate them2. Cisco Stealthwatch Cloud is part of Cisco's XDR strategy, which converges its deep expertise and visibility across the network and endpoints into one turnkey, risk-based solution3. References: 3: Cisco Unveils New Solution to Rapidly Detect Advanced Cyber Threats and Automate Response 2: Cisco Secure Network Analytics - Cisco 1: Cisco Stealthwatch and Cisco Tetration Workload Security

QUESTION NO: 34


展示を参照してください。 API キーは操作中にどのような機能を実行しますか
https://api.amp.cisco.com/v1/computers?
A. リクエストをインポートします
B. HTTP 認証

C. HTTP 認証
D. デント ID を再生します
Answer: C
Explanation:
The API key is a secret token that is used to authenticate the client to the server. It is functionally equivalent to a username and password, and should be treated as such. The API key is passed as part of the HTTP header in the request, using the Authorization: Basic scheme. The API key is combined with the client ID and encoded in base64 format. For example, if the client ID is d16aff14860af496e848 and the API key is d01ed435-b00d-4a4d-a299-1806ac117e72, the HTTP header would look like this:
Authorization: Basic ZDE2YWZmMTQ4NjBhZjQ5NmU4NDg6ZDAxZWQ0MzUtYjAwZC00YTRkLWEyOTktMTgwNmFjMTE3Z The server then decodes the header and verifies the credentials. If the credentials are valid, the server grants access to the requested resource. If the credentials are invalid, the server returns an HTTP 401 Unauthorized error.
The API key performs the function of HTTP authentication, which is the process of verifying the identity of the client. HTTP authentication is different from HTTP authorization, which is the process of determining the permissions of the client. HTTP authorization is based on the scope of the API credential, which can be either read-only or read & write. The scope determines what actions the client can perform on the Cisco AMP for Endpoints data. Importing requests is not a function of the API key, but rather a Python module that allows sending HTTP requests. Playing dent ID is not a meaningful term in this context. Therefore, the correct answer is C). References:
* Secure Endpoint API - Cisco DevNet
* Overview of the Cisco AMP for Endpoints API - Cisco
* Configure AMP for Endpoints Event Stream Feature - Cisco

QUESTION NO: 35
エクスプロイトを左側から右側のセキュリティ脆弱性のタイプにドラッグアンドドロップします。



Answer:


causes memory access errors
gives unauthorized access to web server files
makes the client the target of attack
makes the client the target of attack
gives unauthorized access to web server files
accesses or modifies application data
accesses or modifies application data
causes memory access errors
gives unauthorized access to web server files
makes the client the target of attack
accesses or modifies application data
causes memory access errors