PaloAltoNetworks.PCCET.v2022-02-01.q28

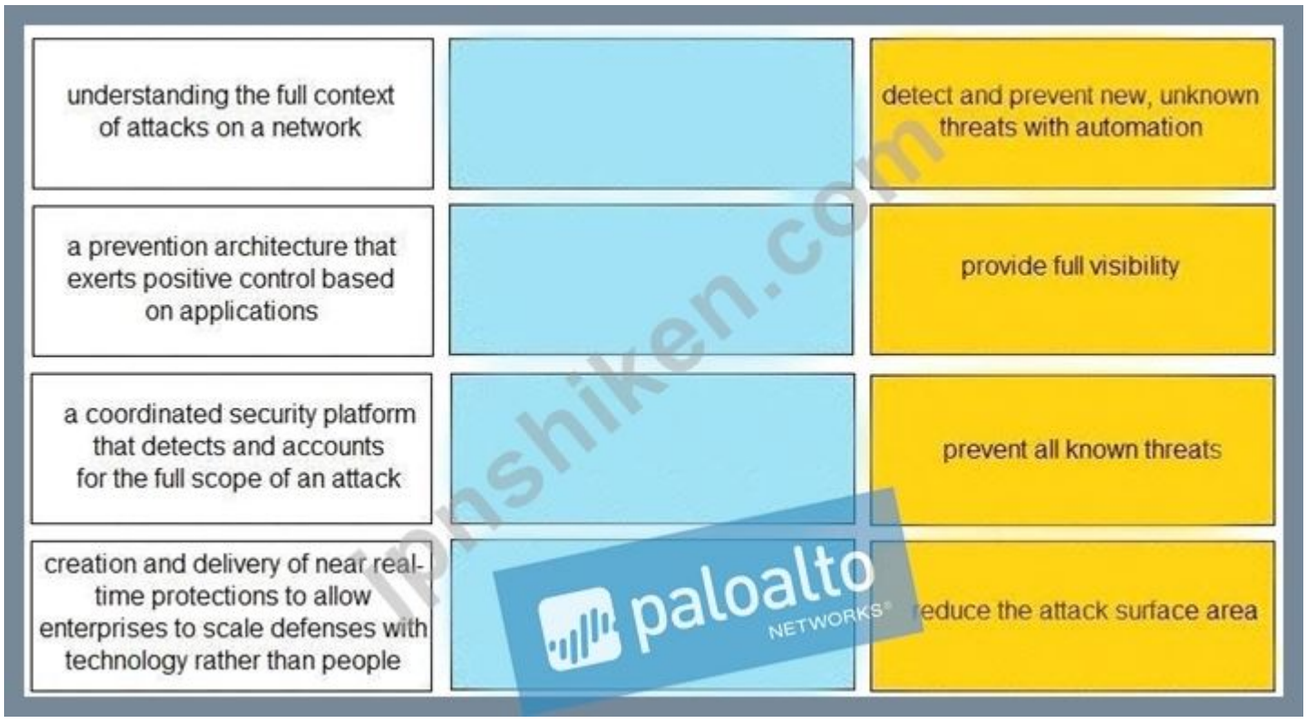
試験コード：	PCCET
試験名称：	Palo Alto Networks Certified Cybersecurity Entry-level Technician
認証ベンダー：	Palo Alto Networks
無料問題の数：	28
バージョン：	v2022-02-01
ページの閲覧量：	535
問題集の閲覧量：	4715

https://www.jpnshiken.com/shiken/PaloAltoNetworks.PCCET.v2022-02-01.q28.html

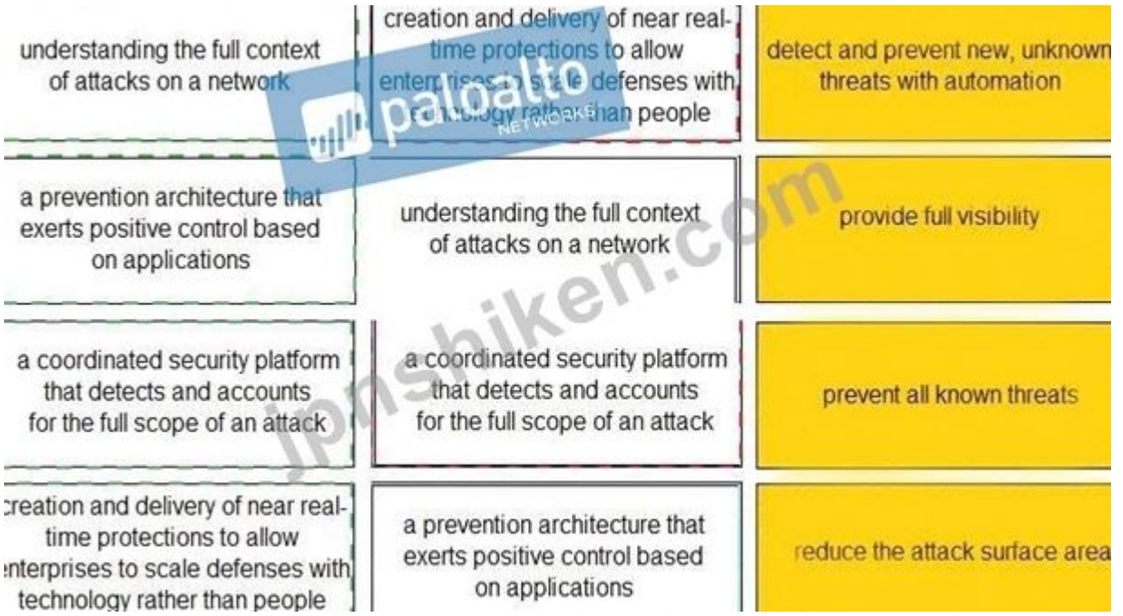
質問: **1**
シグニチャベースのウイルス対策ソフトウェアがマルウェアを検出した場合、保護を提供するために3つのことを行いますか？
（3つ選択してください。）
A. 感染したファイルの拡張子を削除します
B. base64を使用して感染ファイルを復号化します
C. システム管理者に警告する
D. 感染したファイルを隔離する
E. 感染したファイルを削除します
正解: **A,D,E (**コメントを発表する**)**

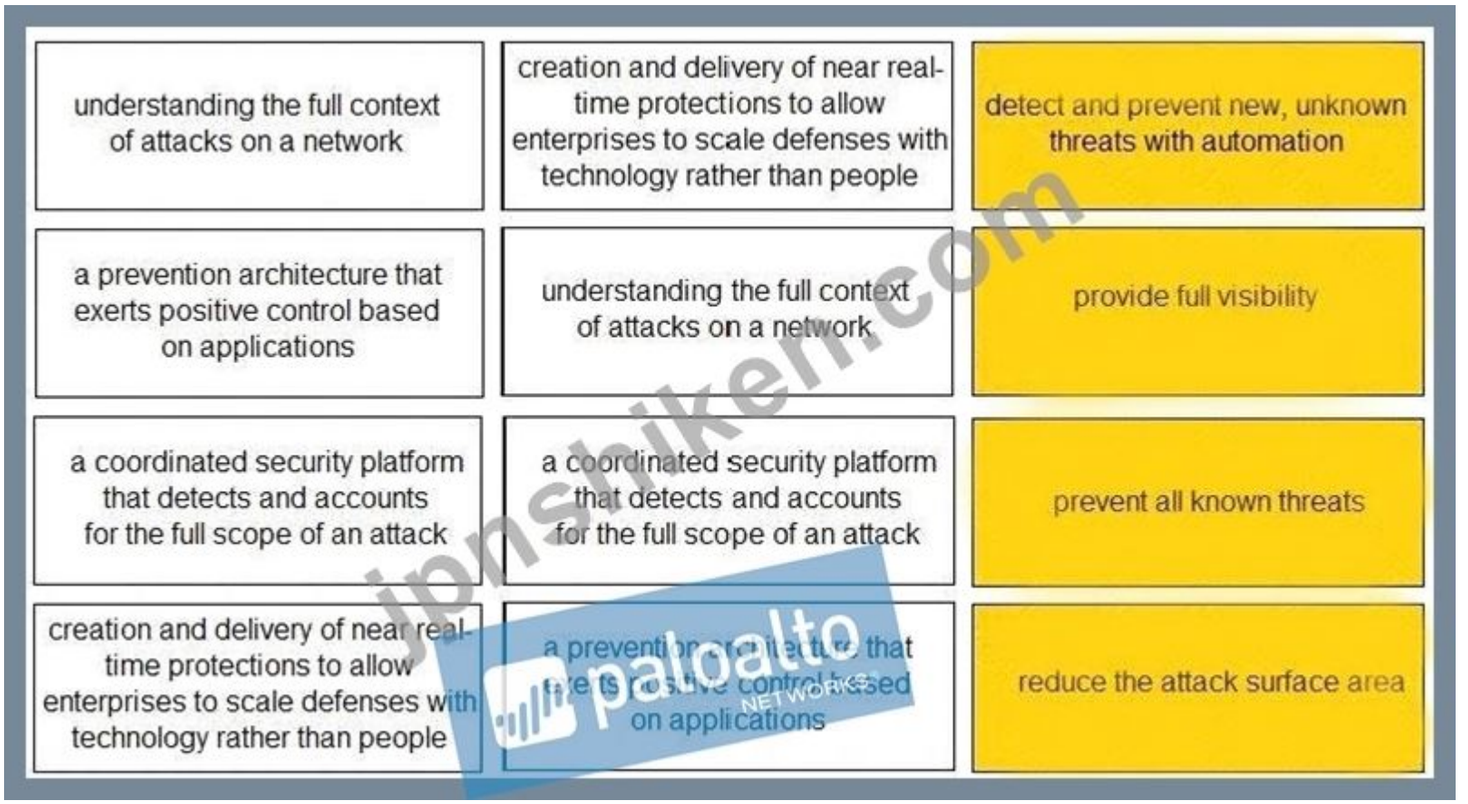
質問: **2**
ネイティブハイパーバイザーは次のように実行されます。
A. ホストコンピューターのハードウェア上に直接
B. ネットワークスループットに極端な要求がある
C. オペレーティングシステムの環境内
D. 特定のプラットフォームのみ
正解: **(**正解を表示します**)**

質問: **3**
各説明をセキュリティオペレーティングプラットフォームのキー機能に一致させます。


understanding the full context of attacks on a network
detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications
provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack
prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people
reduce the attack surface area
paloalto NETWORKS
ipnshiken.com

正解:


understanding the full context of attacks on a network
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people
detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications
understanding the full context of attacks on a network
provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack
a coordinated security platform that detects and accounts for the full scope of an attack
prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people
a prevention architecture that exerts positive control based on applications
reduce the attack surface area
paloalto NETWORKS
ipnshiken.com



質問: **4**
ホストネットワークまたは対応する従来のデータセンターから仮想化環境に出入りするデータパケットを表す用語はどれですか。
A. ゾーン間トラフィック
B. 南北交通
C. ゾーン内トラフィック
D. 東西の交通
正解: **B** (コメントを発表する)

質問: **5**
エンタープライズネットワークから離れないようにする必要があるPIIの例は、どのオプションですか？
A. クレジットカード番号
B. 企業秘密
C. 国家安全保障情報
D. 対称暗号化キー
正解: (正解を表示します)
説明/参照：

質問: **6**
ディレクトリサービスデータベースに含まれる2つのネットワークリソースはどれですか？ 2つ選択してください。）
A. ユーザー

B. エンドポイントのターミナルシェルタイプ
C. サービス
D. / etc / shadowファイル
正解: **(**正解を表示します**)**

質問: **7**
Prisma SaaSは、認可されたSaaSアプリケーションをどのように保護しますか？
A. Prismaアクセスは、Uniform Resource Locator（URL）Web分類を使用して、保護と共有の可視性を提供します
B. Prisma SaaSは、認可されたSaaSアプリケーションは安全であるため、保護を提供しません
C. Prisma SaaSは、組織の内部印刷およびファイル共有サービスに接続して、保護と共有の可視性を提供します
D. Prisma SaaSは、認可された外部サービスプロバイダーのSaaSアプリケーションサービスに直接接続して、保護と共有の可視性を提供します
正解: **(**正解を表示します**)**

質問: **8**
ホスト192.168.19.36/27はどのサブネットに属しますか？
A. 192.168.19.16
B. 192.168.19.64
C. 192.168.19.0
D. 192.168.19.32
正解: **D (**コメントを発表する**)**

質問: **9**
公開ウェブサイトから入手できる一般的な脆弱性エクスポージャーカタログを維持している非営利組織はどれですか？
A. MITRE
B. 国土安全保障省
C. サイバーセキュリティ脆弱性研究センター
D. サイバーセキュリティおよび情報保証局
正解: **(**正解を表示します**)**

質問: **10**
どのエンドポイントツールまたはエージェントが動作ベースの保護を実施できますか？
A. Cortex XDR
B. AutoFocus
C. DNSセキュリティ
D. MineMeld
正解: **(**正解を表示します**)**

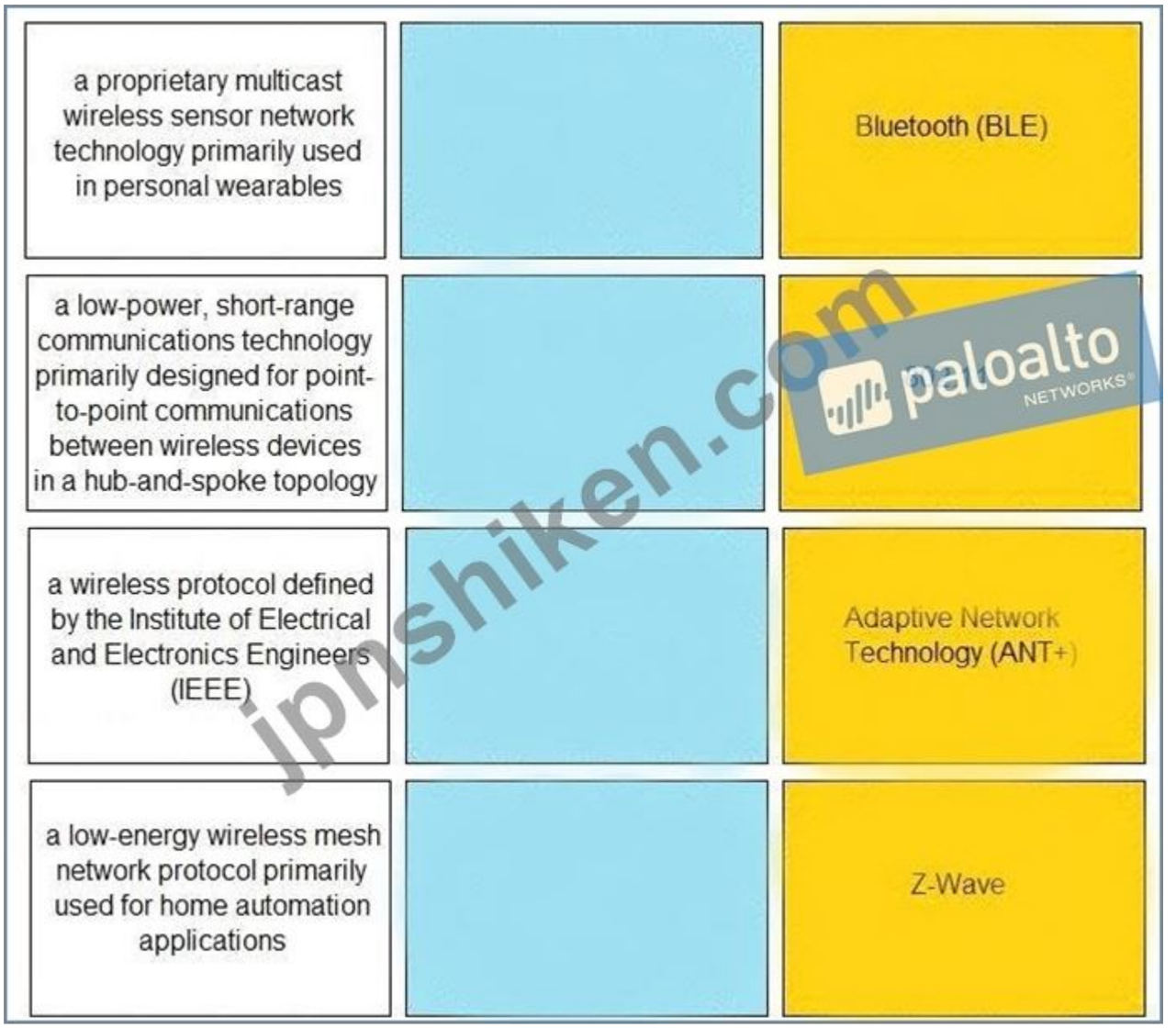
質問: **11**

ゼロトラストアーキテクチャを実装するために使用されるコアコンポーネントはどれですか？
A. VPNコンセントレーター
B. セグメンテーションプラットフォーム
C. Webアプリケーションゾーン
D. コンテンツID
正解: **B (**コメントを発表する**)**

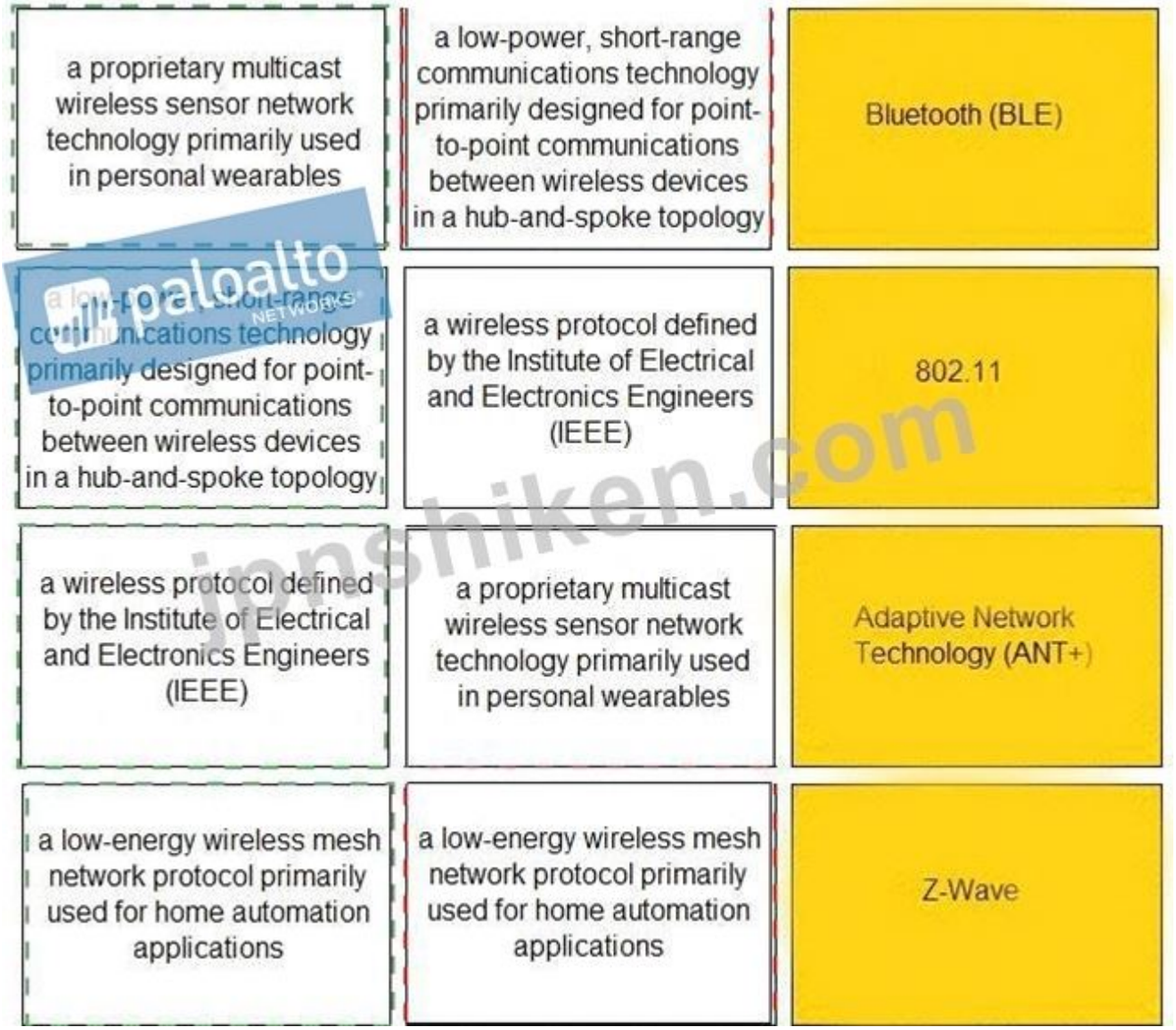
質問: **12**
Webサイトへのアクセスを識別および制御し、マルウェアやフィッシングページをホストするWebサイトから組織を保護するように次世代ファイアウォールを構成できるようにすることで、App-IDを補完するPalo AltoNetworksサブスクリプションサービスはどれですか。
A. WildFire
B. URLフィルタリング
C. 脅威の防止
D. DNSセキュリティ
正解: **(**正解を表示します**)**

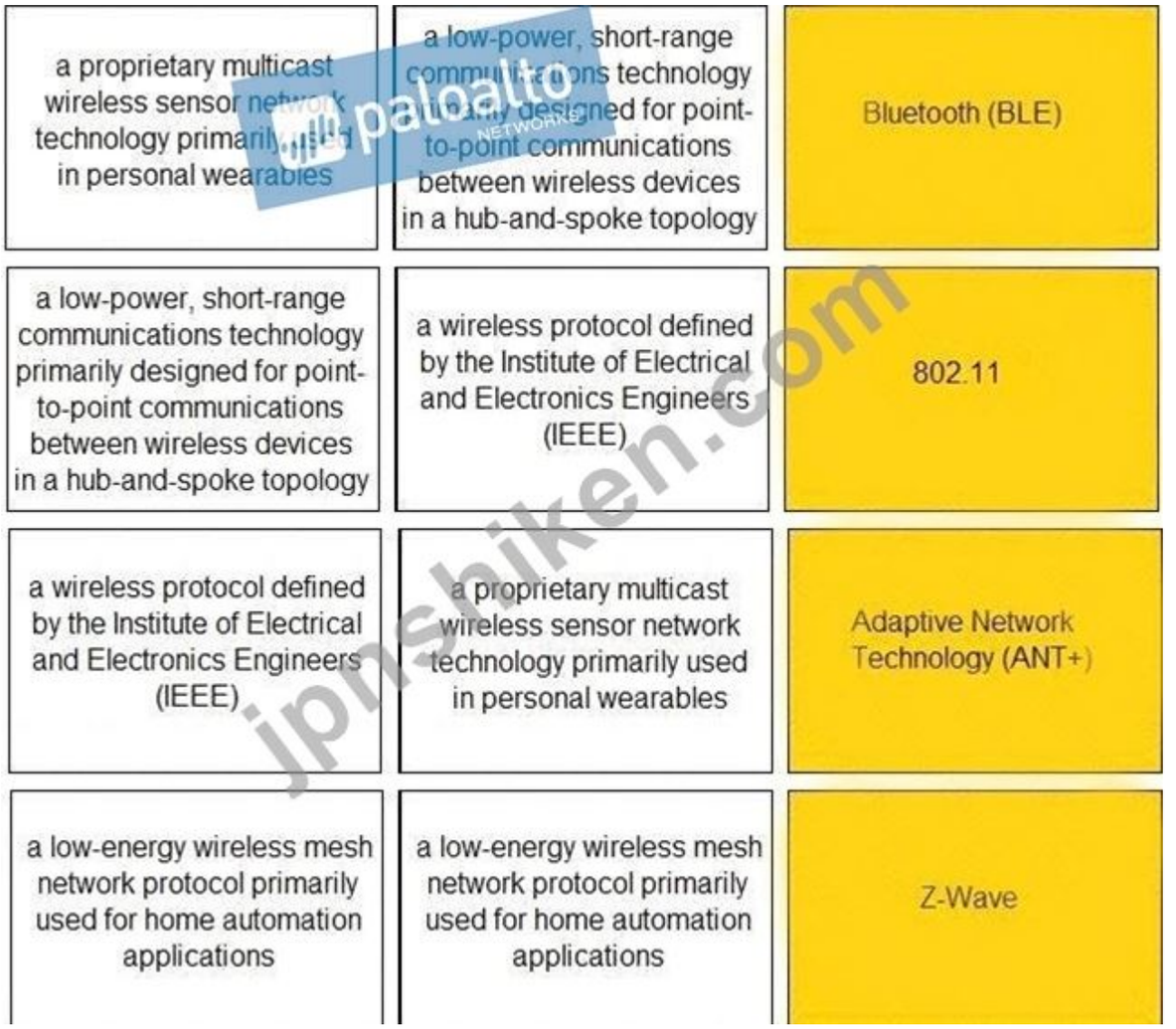
質問: **13**
デバイストラフィックをインターネットに直接送信できるIPsec機能はどれですか。
A. スプリットトンネリング
B. IKEセキュリティアソシエーション
C. Diffie-Hellmanグループ
D. d。認証ヘッダー ÁH）
正解: **(**正解を表示します**)**

質問: **14**
IoT接続の説明をテクノロジーと一致させます。



正解:





質問: **15**
OSIモデルのLayer7で動作するTCP / IPサブプロトコルはどれですか？
A. UDP
B. NFS
C. SNMP
D. MAC
正解: **C** (コメントを発表する)

質問: **16**
対象のシステムからSIEMデータレイクへの変換されたフローを確保するために、SIEMが正しく動作するために必要なものは何ですか？
A. インフラストラクチャとコンテナ
B. コネクタとインターフェース
C. データセンターとUPS
D. コンテナと開発者
正解: (正解を表示します)

質問: **17**
クラウドコンピューティングプラットフォームで実行されているオペレーティングシステムを完全に制御したい場合、顧客はどのモデルを選択しますか？
A. DaaS
B. SaaS
C. IaaS
D. PaaS
正解: **(**正解を表示します**)**

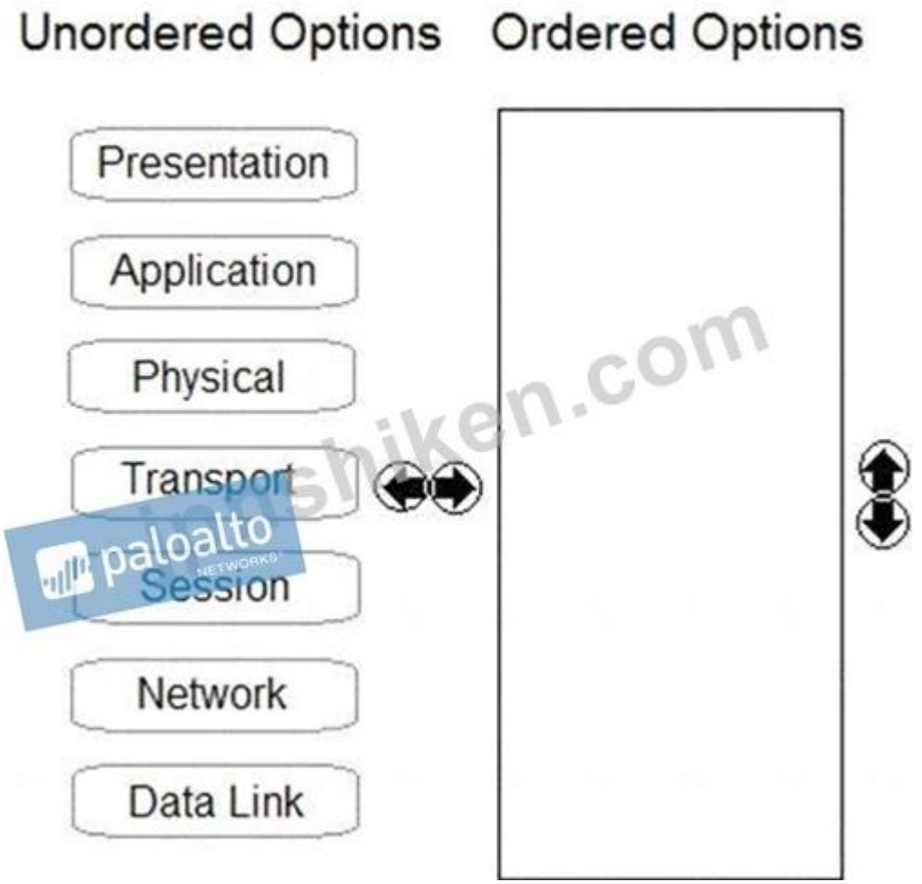
質問: **18**
どのパロアルトネットワークスツールが、セキュリティ分析を加速するネットワーク自動化への予防的で予防ベースのアプローチを可能にしますか？
A. MineMeld
B. WildFire
C. AutoFocus
D. Cortex XDR
正解: **D (**コメントを発表する**)**

質問: **19**
セキュリティの自動化とソリューションの最終的な検証を担当し、セキュリティの問題に対するマシン主導の対応を通じて一貫性を確保するのに役立つ組織機能はどれですか？
A. DevOps
B. SecOps
C. SecDevOps
D. NetOps
正解: **(**正解を表示します**)**

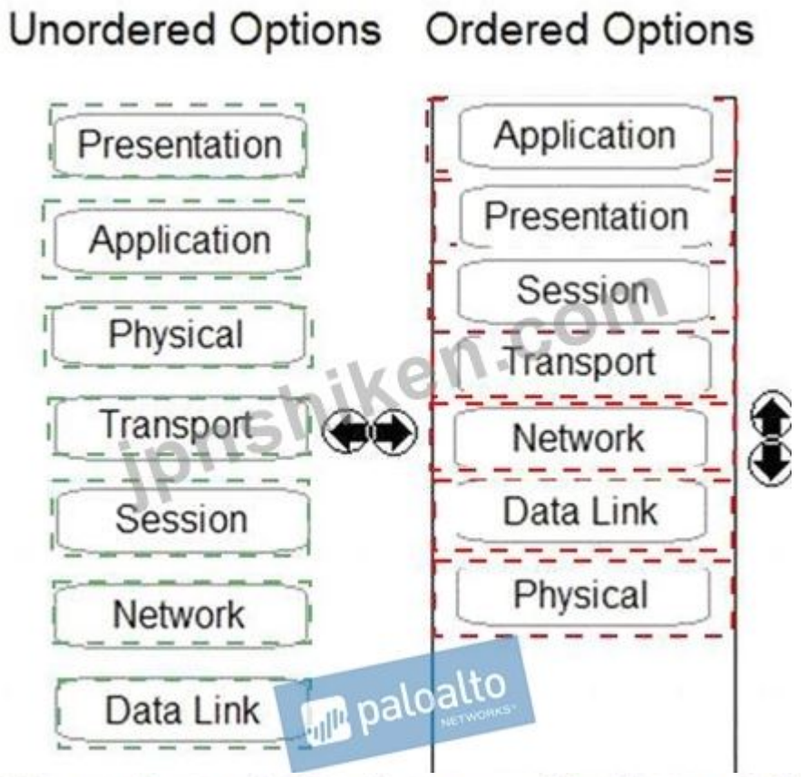
質問: **20**
どのタイプのサービスとしてのソフトウェア（SaaS）アプリケーションがビジネス上のメリットを提供し、展開が速く、必要なコストが最小限で、無限にスケーラブルですか？
A. 良性
B. 許容

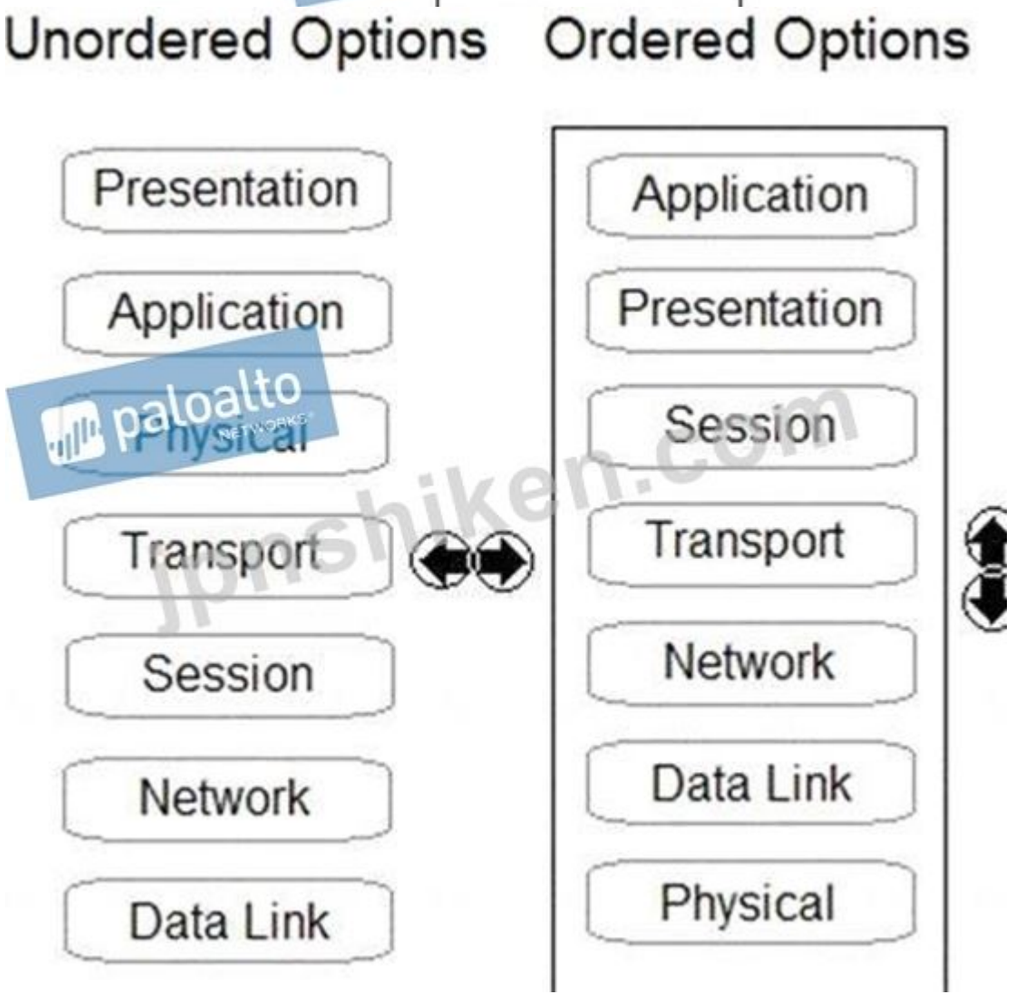
C. 認可済み
D. 安全
正解: **C** (コメントを発表する)
説明/参照：

質問: **21**
上部にLayer7、下部にLayer1があるOSIモデルを注文します。



正解:

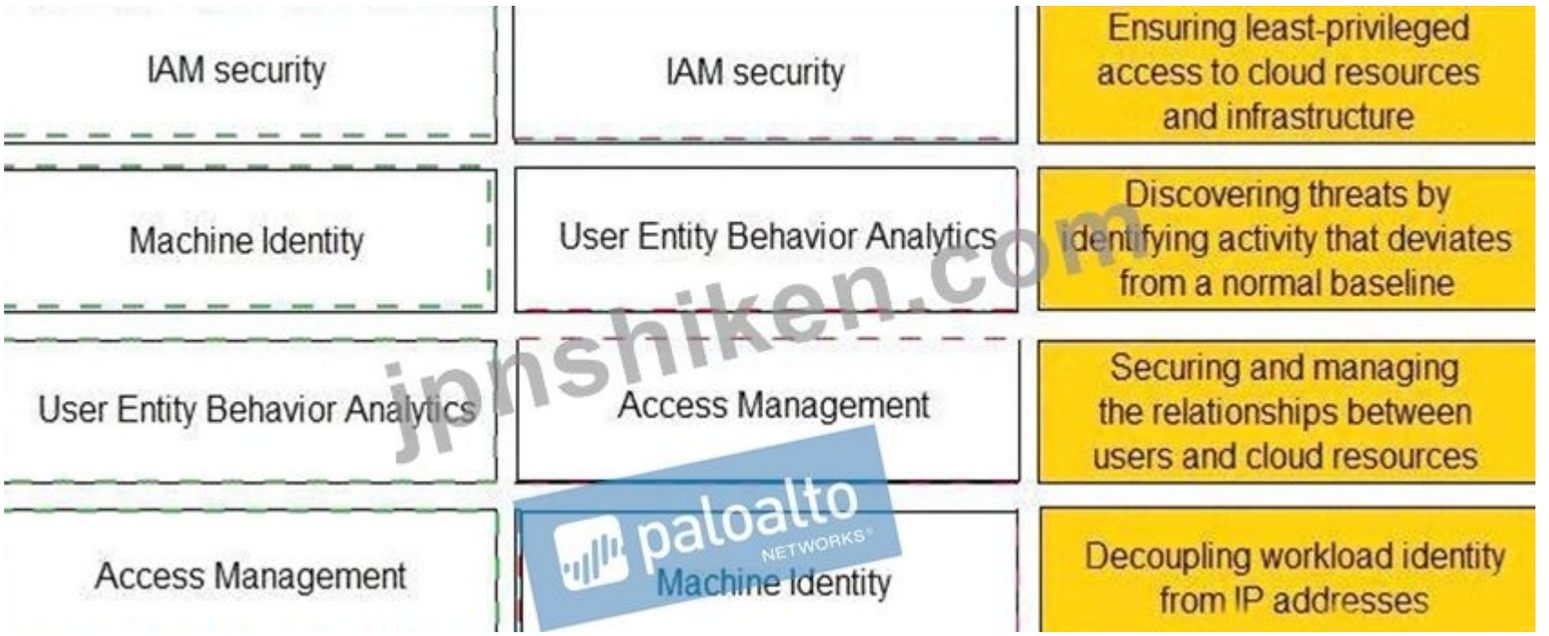

Unordered Options
Ordered Options
Presentation
Application
Physical
Transport
Session
Network
Data Link
Application
Presentation
Session
Transport
Network
Data Link
Physical

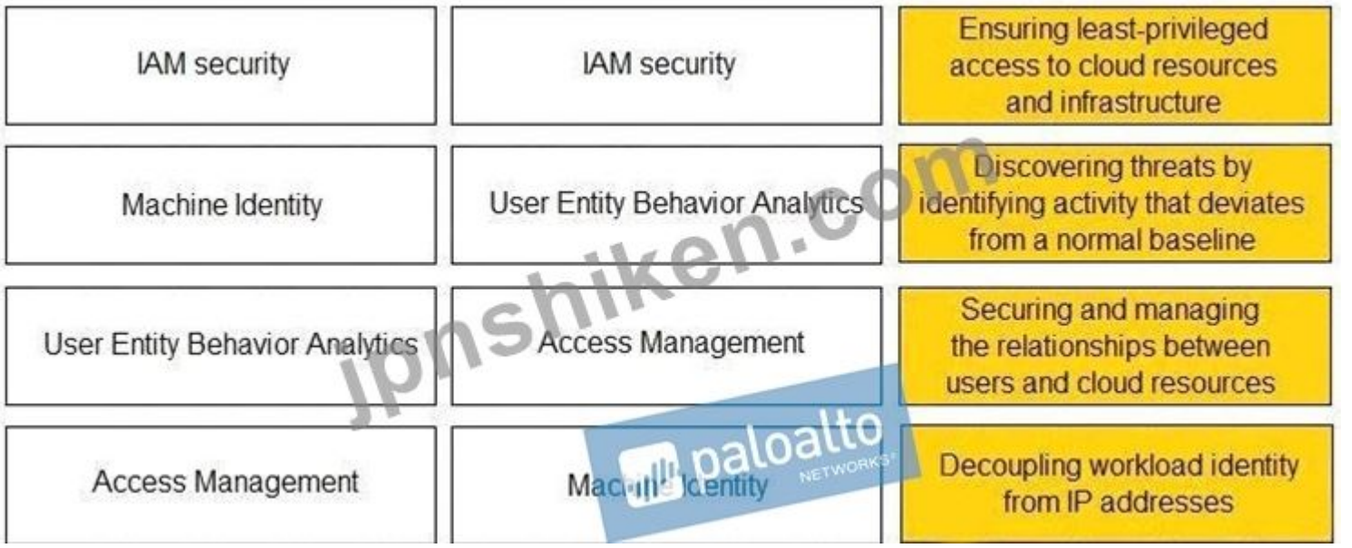

Unordered Options
Ordered Options
Presentation
Application
Transport
Session
Network
Data Link
Application
Presentation
Session
Transport
Network
Data Link
Physical

質問: **22**

Identity and Access Management (IAM) のセキュリティ制御を適切な定義と一致させます。

正解:





質問: **23**
どのエンドポイントツールまたはエージェントが動作ベースの保護を実施できますか？
A. AutoFocus
B. Cortex XDR
C. DNSセキュリティ
D. MineMeld
正解: (正解を表示します)
説明

質問: **24**
Prisma Cloudアプリケーションのセキュリティのどの柱が、クラウドリソースとSaaSアプリケーションが正しく構成されていることを保証しますか？
A. 可視性、ガバナンス、コンプライアンス
B. ダイナミックコンピューティング
C. セキュリティの計算
D. ネットワーク保護
正解: (正解を表示します)

質問: **25**
セキュリティテクノロジーやその他のデータフローからの入力に基づいて機能する標準化され自動化されたプレイブックの実行を通じてインシデント対応を加速できるシステムは、何として知られていますか？
A. ステップ
B. SIEM
C. SOAR
D. XDR
正解: (正解を表示します)

質問: **26**
接続を開始する被害者に依存するWi-Fi攻撃のタイプはどれですか？
A. パラガー
B. みらい
C. 邪悪な双子
D. Jasager
正解: (正解を表示します)

質問: **27**
エンドポイントでは、アプリケーションをエクスプロイトから保護するためにどの方法を使用する必要がありますか？
A. エンドポイントベースのファイアウォール
B. 強力なユーザーパスワード
C. ソフトウェアパッチ
D. フルディスク暗号化
正解: (正解を表示します)

質問: **28**
衛星によって提供されるIoT接続テクノロジーはどれですか？
A. 4G / LTE
B. 2G / 2.5G
C. VLF
D. Lバンド
正解: (正解を表示します)