PaloAltoNetworks.PCCSE.v2024-03-01.q186

試験コード:	PCCSE
試験名称:	Prisma Certified Cloud Security Engineer
認定資格:	Palo Alto Networks
無料問題数:	186
バージョン:	v2024-03-01
アクセス数:	2459
ページビュー数:	1860
https://www.jpnpdf.com/PaloAltoNetworks.PCCSE.v2024-03-01.q186-mondaishu.html	

最新問題: **1**

スキャン結果を表形式で標準出力に正しく出力し、結果をコンソールに送信しながらスキャン結果を JSON ファイルに書き込むコマンドはどれですか?

A.

```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
--user <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--stdout-tabular
--output-file scan-results.json
nginx:latest
```

B.

```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
--username <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--details
--json-output scan-results.json
nginx:latest
```

C.

```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
-u <COMPUTE_CONSOLE_USER>
-p <COMPUTE_CONSOLE_PASSWD>
--details
--output-file scan-results.json
nginx:latest
```

D.
```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
--user <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--details
--file-output scan_results.json
nginx:latest
```


Answer: A (メーッセージを残す**)**

画像に示されているコマンドは、Prisma Cloud スイートの一部であるTwistcli コマンドライン ツールで画像をスキャンするために使用されます。正しいコマンドを特定するには、表形式で標準出力への出力を指定し、スキャン結果を JSON ファイルに書き込むコマンドを特定する必要があります。

オプション A では、stdout に出力する正しい方法である --stdout フラグと、ファイルの .json 形式を使用した --output-file を使用します。--address フラグは、コンソール アドレスの指定に正しく使用されています。したがって、オプション A は要件を満たす正しいコマンドです。

最新問題**: 2**

コンソールは Kubernetes クラスターで実行されており、このクラスター内のノードに Defender をデプロイする必要があります。

デフォルトのコンソール サービス名を使用して Kubernetes に Defender をデプロイする手順を示すオプションはどれですか?

A. コンソールのデプロイメント ページから、コンソール識別子のポッド名を選択し、DaemonSet ファイルを生成し、DaemonSet をツイストロック名前空間に適用します。

B. デプロイメント ページから、コンソールでクラウド認証情報を構成し、クラウド検出による Kubernetes ノードの自動保護を許可します。

C. コンソールのデプロイメント ページから、コンソール識別子としてTwistlock-consoleを選択し、DaemonSetファイルを生成し、DaemonSetをtwistlock名前空間に適用します。

D. コンソールのデプロイメント ページから、コンソール識別子としてTwistlock-consoleを選択し、curl | コマンドを実行します。マスター Kubernetes ノード上の bash スクリプト。

Answer: C (メーッセージを残す**)**

参照：

Kubernetes クラスターに Defender をデプロイするには、Prisma Cloud コンソールから DaemonSet 構成を生成する必要があります。「twistlock-console」は通常、コンソール識別子として使用され、ディフェンダーとコンソール間の通信を容易にします。生成された DaemonSet ファイルは、Kubernetes クラスター、特に「twistlock」名前空間内に適用され、包括的な保護のためにクラスター内の各ノードに Defender が確実にデプロイされます。この方法は、クラスター全体にエージェントを展開するための Kubernetes のベスト プラクティスに沿っており、Prisma Cloud のセキュリティ機能のシームレスでスケーラブルな展開を保証します。

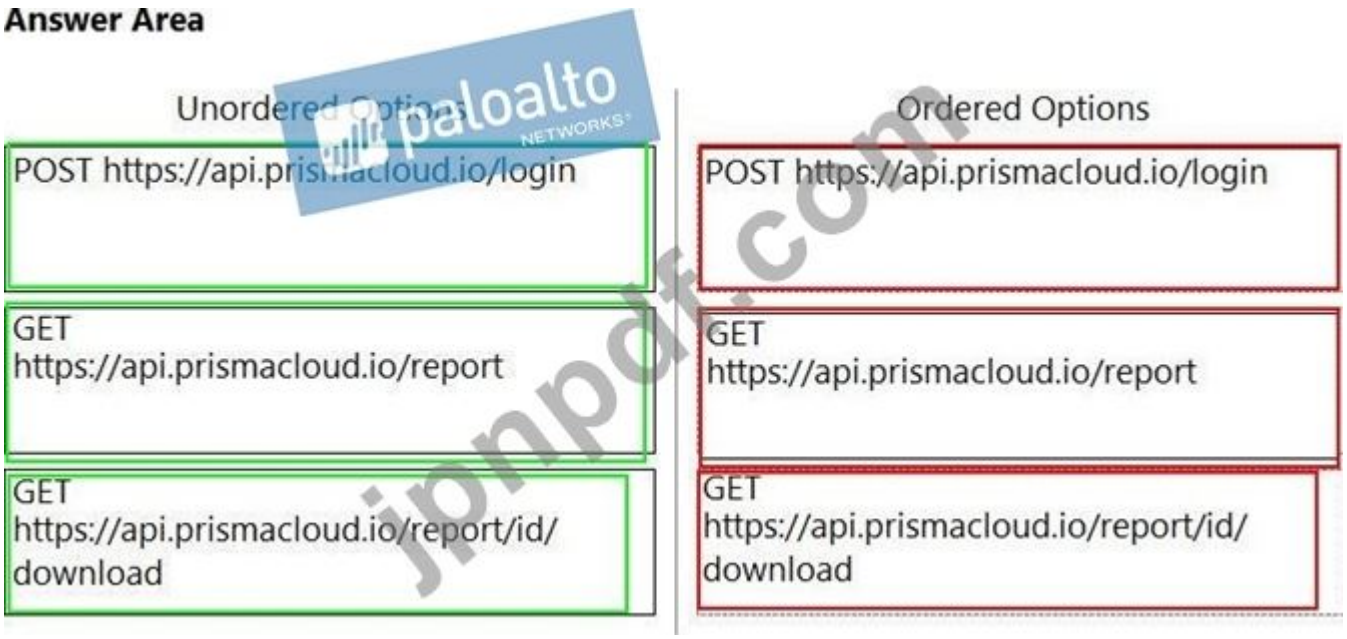
最新問題**: 3**

管理者は、Prisma Cloud Enterprise テナントから既存のコンプライアンス レポートをダウンロードするカスタム サービスを作成する任務を負っています。

このサービスの API はどの順序で実行されますか?

(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)

Answer:
Answer Area



最新問題: **4**
コンソール内でコンプライアンス レポートを作成するために使用できる 2 つの頻度オプションはどれですか? (2つお選びください。)
A. 1 回限り
B. 毎月
C. 定期的
D. 毎週
Answer: (解答を表示する**)**
Prisma Cloud 内では、コンプライアンス レポートを作成する際、管理者は特定のニーズに基づいてこれらのレポートの生成を柔軟にスケジュールできます。使用可能な頻度オプションには、指定した時刻にレポートを 1 回生成する 「ワンタイム」と、毎週レポートを繰り返し生成できる 「毎週」が含まれます。これらのオプションにより、組織はコンプライアンス レポートを運用要件に合わせて調整できるようになり、コンプライアンス体制に関する最新の洞察を定期的に得ることができます。

最新問題: **5**

Prisma Cloud 管理者は、API 経由でレポートを取得する任務を負っています。Prisma Cloud テナントは、app2.pnsmacfoudjo にあります。正しい API エンドポイントは何ですか?
A. https //api2-prismacloud io
B. https://api pnsmacloud.cn
C. https://api2eu-prismacioud.io
D. https://api.prismactoud.io
Answer: (解答を表示する**)**

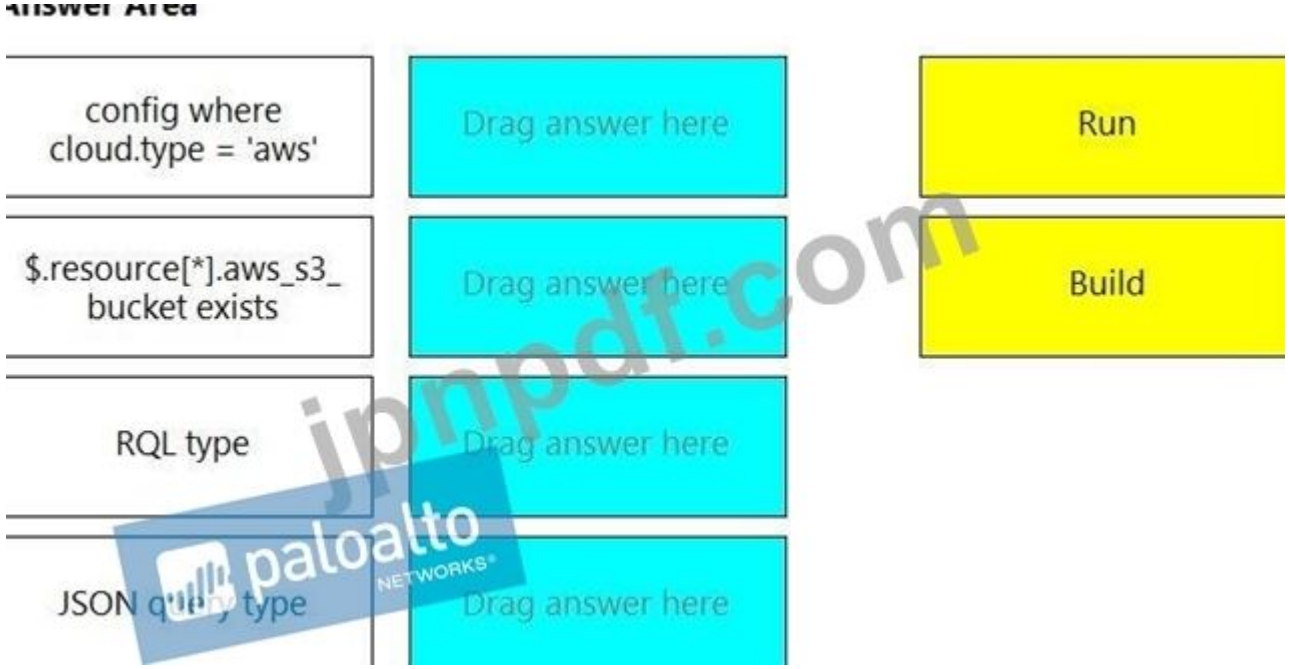
最新問題**: 6**
顧客が Prisma Cloud Enterprise Edition を購入した場合、パロアルトネットワークスはどのコンポーネントをホストして実行しますか?
A. ディフェンダー
B. コンソール
C. ジェンキンス
D. ツイストクリ
Answer: B (メーッセージを残す**)**
Prisma Cloud Enterprise Edition では、Palo Alto Networks がコンソール コンポーネントをホストし、実行します。コンソールは Prisma Cloud の中央管理インターフェイスとして機能し、顧客がこのコンポーネントを自分でホストすることなく、ポリシーの設定、アラートの表示、およびクラウド セキュリティ体制の管理を行うことができます。

最新問題**: 7**
セキュリティ チームは、[監視] > [イベント] で多数の異常を発見します。インシデント対応チームは開発者と協力して、これらの異常が誤検知であると判断します。
セキュリティ チームがこのイメージについて再学習することを選択した場合、どのような影響がありますか?
A. 検出された異常は自動的にモデルに追加されます。
B. モデルが削除され、初期学習状態に戻ります。
C. モデルは削除され、Defender は 24 時間解放されます。
D. モデルは保持され、新しい学習期間中に観察された新しい動作は既存のモデルに追加されます。
Answer: (解答を表示する**)**

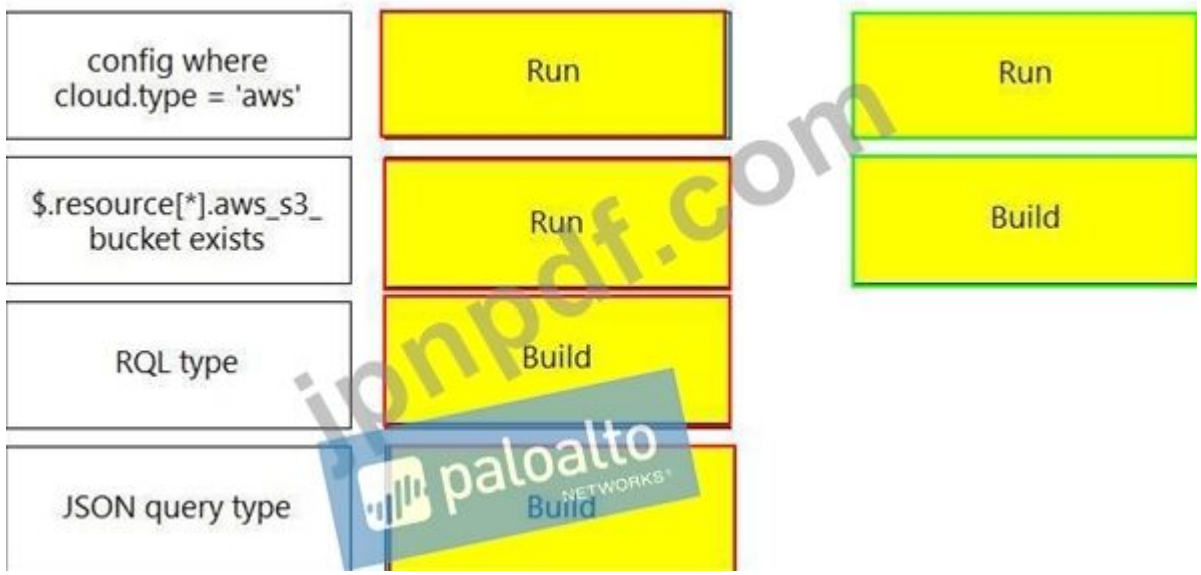
最新問題**: 8**
Defender のデバッグ ログはどこで表示できますか? (2つお選びください。)
A. /var/lib/twistlock/defender.log
B. コンソールから、 管理」> ディフェンダー」> 管理」> ディフェンダー」の順に選択します。デプロイされたディフェンダーのリストからディフェンダーを選択し、[アクション] > [ログ] をクリックします。
C. /var/lib/twistlock/log/defender.log
D. コンソールから、 管理」> ディフェンダー」> デプロイ」> ディフェンダー」の順に選択します。デプロイされたディフェンダーのリストからディフェンダーを選択し、[アクション] > [ログ] をクリックします。
Answer: A,B (メーッセージを残す**)**

最新問題**: 9**

ビルドおよび実行サブタイプを含むカスタム ポリシーを作成したいと考えています。各例のクエリ タイプを一致させます。
(プルダウン リストから回答を選択します。回答は複数回使用することも、まったく使用しないこともできます。)



Answer:
Answer Area



参照：
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy.html

最新問題**: 10**
Prisma Cloud Compute Edition を識別するオプションはどれですか?
A. ダウンロード可能な自己ホスト型ソフトウェア
B. Prisma Cloud へのプラグイン
C. Software-as-a-Service (SaaS)
D. APT でインストールされたパッケージ
Answer: (解答を表示する**)**

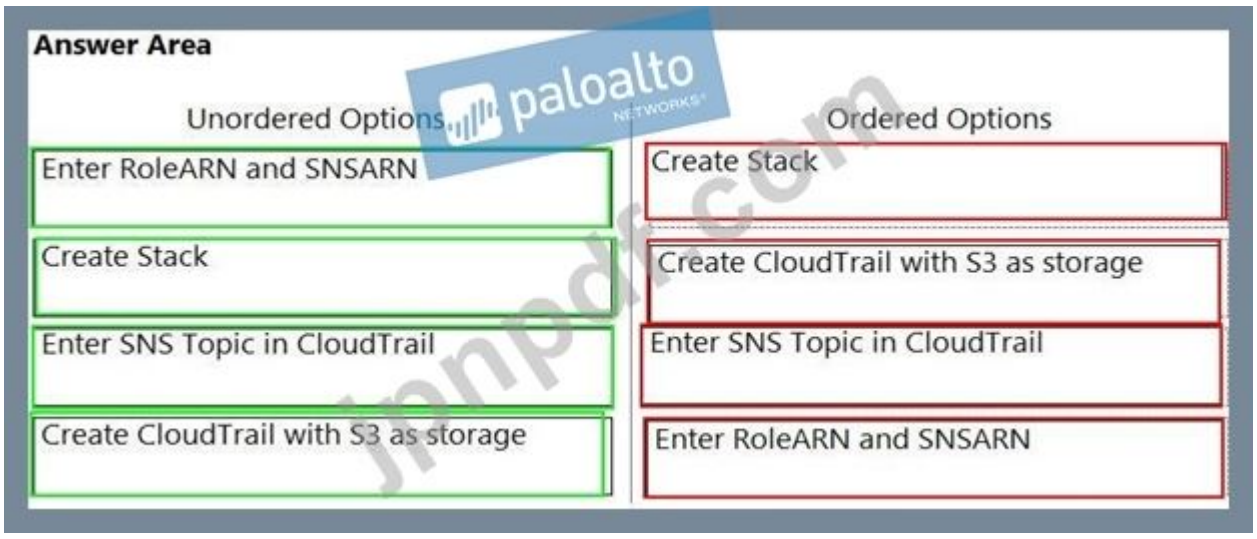
最新問題: **11**
管理者は、AWS で実行されている Kubernetes クラスターにコンソールをデプロイしました。管理者は、デフォルトの Prisma Compute Console 設定と同じポートでリッスンするように、TCP パススルー モードでロード バランサも設定しました。
ビルド パイプラインで、管理者は、twistcli が HTTPS 経由でコンソールと通信できるようにしたいと考えています。Twistcli が Prisma Compute API にアクセスするにはどのポートを使用する必要がありますか?
A. 8083
B. 8081
C. 8084
D. 443
Answer: A (メーッセージを残す**)**
https://docs.prismacloudcompute.com/docs/compute_edition_21_04/tools/twistcli.html#connectivity-to-console

最新問題: **12**
セキュリティ チームは、特定の実行中のコンテナを CNAF ポリシーの対象にしたいと考えています。管理者は、コンテナをターゲットとするポリシーの範囲をどのように設定する必要がありますか?
A. ポリシーの範囲をイメージ名に設定します。
B. ポリシーの範囲をホスト名に設定します。
C. ポリシーの範囲を Defender 名に設定します。
D. ポリシーのスコープを名前空間に設定します。
Answer: D (メーッセージを残す**)**

最新問題: **13**
お客様は、前日の未解決アラートが解決されたことに気づきました 自動修復が設定されていません このアラート ステータスの変化を説明する 2 つの理由はどれですか? (2つお選びください)
A. ポリシーが変更されました。
B. アラートが外部統合に送信されました
C. リソースが削除されました。
D. ユーザーがアラート ステータスを手動で変更しました
Answer: A,C (メーッセージを残す**)**

最新問題: **14**
データセキュリティ機能で使用するAWSアカウントのオンボーディングに関連する手順を注文します。

Answer:



最新問題: **15**
Prisma Cloud の管理者は、Docker エンジンに対してロールベースのアクセス制御を有効にしたいと考えています。
このタスクを実行するには、最初にどの構成手順が必要ですか?
A. 最初にアイデンティティ プロバイダーを使用し、次にコンソールを使用するように Docker の認証シーケンスを構成します。
B. Defender のリスナー タイプを TCP に設定します。
C. 最初に ID プロバイダーを使用し、次にコンソールを使用するように Defender の認証シーケンスを構成します。
D. Docker のリスナー タイプを TCP に設定します。
Answer: C (メーッセージを残す**)**

最新問題: **16**
Prisma Cloud での SSO 統合を正確に特徴づけているのはどれですか?
A. Prisma Cloud API にアクセスする必要がある管理者は、構成後に SSO を使用できます。
B. Okta、Azure Active Directory、PingID などが SAML 経由でサポートされます。
C. Prisma Cloud は IdP で開始される SSO をサポートし、その SAML エンドポイントは POST メソッドと GET メソッドをサポートします。

D. 管理者は、Prisma Cloud が監視するすべてのクラウド アカウントに対して異なるアイデンティティ プロバイダー (IdP) を設定できます。
Answer: C (メーッセージを残す**)**
セクション: (なし)
説明

最新問題**: 17**
Prisma Cloud で新しいアマゾン ウェブ サービス (AWS) アカウントをオンボードするときの外部 ID の機能は何ですか?
A. これは、Monitor & Protect モードが選択されている場合にのみ必要となる一意の識別子です。
B. PrismaCloudApp スタックのデフォルト名です。
C. Prisma Cloud ロールのリソース名です。
D. データを抽出するために、Prisma Cloud アカウントと AWS アカウントの間に信頼関係を確立する UUID です。
Answer: D (メーッセージを残す**)**

最新問題**: 18**
リソース エクスプローラー ページの感嘆符は?を表します。
A. リソースが削除されました
B. リソースにコンプライアンス違反があります
C. リソースにアラートがあります
D. リソースは最近変更されました
Answer: D (メーッセージを残す**)**

最新問題**: 19**
アクセス キーの使用に関する正しい記述は次のうちどれですか? (2つお選びください。)
A. アクセス キーは API 呼び出しに使用されます
B. いつでも最大 2 つのアクセス キーをアクティブにできます
C. システム管理者はすべてのユーザーのアクセス キーを作成できます
D. アクセス キーには有効期限が必要です
Answer: B,C (メーッセージを残す**)**

最新問題**: 20**
Prisma Cloud の管理者は、ホスト間の接続や構成されたネットワーク オブジェクトへの接続を含む、すべての接続を監視するためのグラフィカル ビューを取得する必要があります。

このタスクを実行するために管理者はどの設定を有効または構成しますか?
A. ADEM
B. WAAS 分析
C. テレメトリ
D. クラウド ネイティブ ネットワーク ファイアウォール
E. ホストの洞察
Answer: D (メーッセージを残す)
参照：
ホスト間の接続や Prisma Cloud 内の設定されたネットワーク オブジェクトへの接続を含むすべての接続を監視するためのグラフィカル ビューを取得するには、有効化または設定する適切な機能がクラウド ネイティブ ネットワーク ファイアウォール (オプション D) です。Prisma Cloud のクラウド ネイティブ ネットワーク ファイアウォールは、ネットワーク トラフィックの可視性を提供し、クラウド環境内のネットワーク フローの監視と制御を可能にし、管理者がホスト間通信とネットワーク オブジェクトへの接続を視覚化して保護できるようにします。ADEM (オプション A) および WAAS Analytics (オプション B) は、接続を監視するための Prisma Cloud の機能とは関係ありません。テレメトリ (オプション C) にはデータとメトリックの収集が含まれますが、特に接続のグラフィカル ビューは提供されません。Host Insight (オプション E) は、ホスト関連のアクティビティと脆弱性を可視化することに重点を置いていますが、ここで説明したグラフィカルな方法でのネットワーク接続の監視については特に扱いません。

最新問題**: 21**
セキュリティ チームはカスタム ポリシーを作成するように依頼されました。
この目標を達成するためにチームが使用できる 2 つの方法はどれですか? (2つお選びください)
A. 新しいポリシーを追加します
B. すぐに使えるポリシーでクエリを編集します
C. すぐに使えるポリシーを無効にします
D. 既存のポリシーのクローンを作成します
Answer: C,D (メーッセージを残す)

最新問題**: 22**
管理者は、ユーザーが 5 秒以内に 5 つの .tar.gz ファイルを投稿できないようにレート制限を適用したいと考えています。
管理者は何を設定する必要がありますか?
A. 平均レート 5 の DoS 保護の禁止、および WAAS 上の .tar.gz のファイル拡張子と一致する
B. バースト レート 5 および CNNF の .tar.gz に一致するファイル拡張子による DoS 保護の禁止
C. バースト レート 5 および WAAS 上の .tar gz に一致するファイル拡張子による DoS 保護の禁止
D. 平均レート 5、および CNNF の .tar.gz でファイル拡張子が一致する DoS 保護の禁止
Answer: A (メーッセージを残す)
.tar.gz ファイルを投稿するユーザーにレート制限を強制するには、管理者はサービス拒否 (DoS) 保護の禁止を平均レート 5 で構成し、Web アプリケーションと API 上の .tar.gz のファイル拡張子を一致させる必要があります。セキュリティ (WAAS) システム。これにより、指定されたレートを超えた場合にアクションが確実にブロックされ、潜在的な DoS 攻撃に対する保護が提供されます。

最新問題**: 23**
Prisma Cloud の新しい API リリース情報を受け取ることができるクラウド サービス プロバイダーはどれですか?

A. AWS、Azure、GCP、Oracle、IBM
B. AWS、Azure、GCP、Oracle、Alibaba
C. AWS、Azure、GCP、IBM
D. AWS、Azure、GCP、IBM、アリババ
Answer: B (メーッセージを残す**)**
パロアルトネットワークスによって開発された Prisma Cloud は、さまざまなクラウド サービス プロバイダー (CSP) にわたる包括的なクラウド セキュリティ機能で知られています。統合とサポートは、AWS (Amazon Web Services)、Azure (Microsoft のクラウド)、GCP (Google Cloud Platform)、Oracle Cloud、Alibaba Cloud などの主要な CSP にまで及びます。この幅広いサポートにより、マルチクラウド環境を活用する組織は、すべてのクラウド資産にわたって一貫したセキュリティ体制を維持できます。Prisma Cloud によってサポートされる CSP に関する情報は通常、公式ドキュメントとリリース ノートに記載されており、各 CSP に固有の機能、統合、拡張機能が詳しく説明されています。

最新問題**: 24**
アマゾン ウェブ サービス (AWS) クラウド内の自動化された方法を使用して、ID およびアクセス管理 (IAM) モジュールで修復を使用するプロセスを合理化するために必要な 2 つのアクションはどれですか? (2つお選びください。)
A. Azure Service Bus と統合します。
B. boto3 をインストールし、ライブラリを要求します。
C. IAM Azure 修復スクリプトを構成します。
D. IAM AWS 修復スクリプトを構成します。
Answer: B,D (メーッセージを残す**)**

最新問題**: 25**
顧客がコンテナ監査を検討しており、監査によりクリプトマイナー攻撃が特定されました。この監査が発生した可能性がある 3 つのオプションはどれですか? （3つお選びください。）
A. 一般的なクリプトマイナー ポートの使用法が見つかりました。
B. マイニングされた通貨の価値が $100 を超えています。
C. マイニングされた通貨はユーザー トークンに関連付けられます。
D. コンテナーの長時間にわたる高い CPU 使用率が検出されました。
E. 共通のクリプトマイナー プロセス名が見つかりました。
Answer: A,D,E (メーッセージを残す**)**

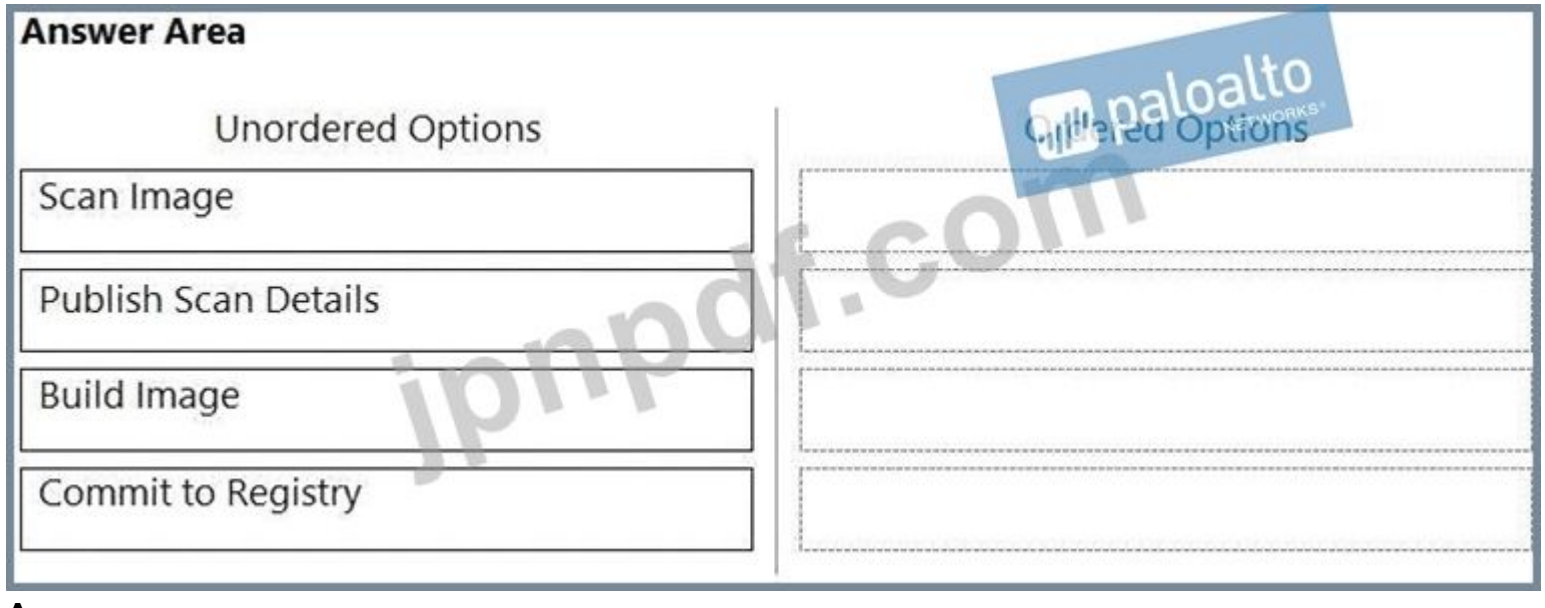
最新問題**: 26**
Prisma Cloud API とのインターフェイスに必要な 2 つのリクエスト ヘッダーはどれですか? (2つお選びください。)
A. コンテンツタイプ:アプリケーション/xml
B. x-redlock-auth
C. コンテンツタイプ:application/json
D. >x-redlock-request-id
Answer: (解答を表示する**)**

最新問題**: 27**

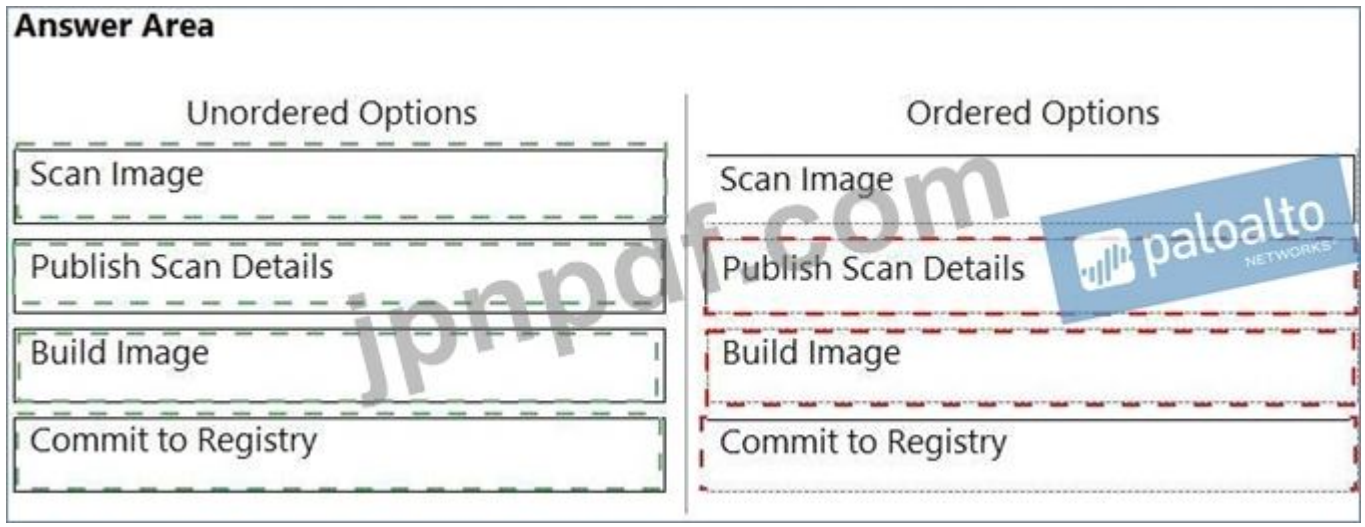
パブリック クラウド アカウントを Prisma Cloud Enterprise にオンボーディングしました。構成リソースの取り込みはオンボードアカウントの資産インベントリに表示されますが、アカウント内の構成資産に対してアラートは生成されません。
構成ポリシーは Prisma Cloud Enterprise テナントで有効になり、それらのポリシーは既存のアラート ルールに関連付けられます。これらのポリシーに一致する調査の ROL ステートメントは、構成リソースの結果を正常に返します。
アラートが生成されないのはなぜですか?
A. パブリック クラウド アカウントは構成リソースにアクセスしません。
B. パブリック クラウド アカウントはアラート ルールに関連付けられていません。
C. パブリック クラウド アカウントはアラート通知に関連付けられていません。
D. パブリック クラウド アカウントでは監査証跡の取り込みが有効になっていません。
Answer: (解答を表示する)

最新問題: **28**
Runtime Defense のインシデント エクスプローラー セクションに反映される 3 つのインシデント タイプはどれですか? 3つお選びください。)
A. ポート スキャン
B. ブルートフォース
C. 暗号マイナー
D. SQL インジェクション
E. クロスサイト スクリプティング
Answer: A,B,D (メーッセージを残す)

最新問題: **29**
Jenkins パイプライン スキャンのステップの順序は何ですか?
(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)



Answer:



説明

中程度の信頼度で自動的に生成されるテーブルの説明

最新問題: 30

導入アドバイザーは、クラウド セキュリティ体制管理の導入の進捗状況を測定するためにどのカテゴリを使用しますか?

A. 基礎、高度、最適化

B. 可視性、セキュリティ、およびコンプライアンス

C. 可視性、コンプライアンス、ガバナンス、脅威の検出と対応

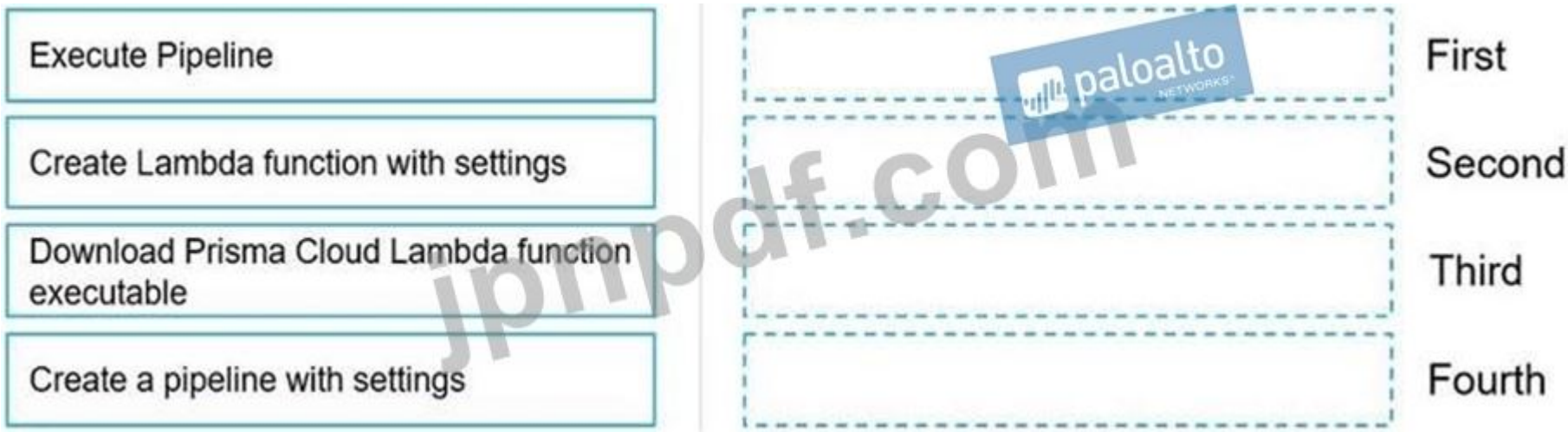
D. ネットワーク、異常、監査イベント

Answer: (解答を表示する**)**

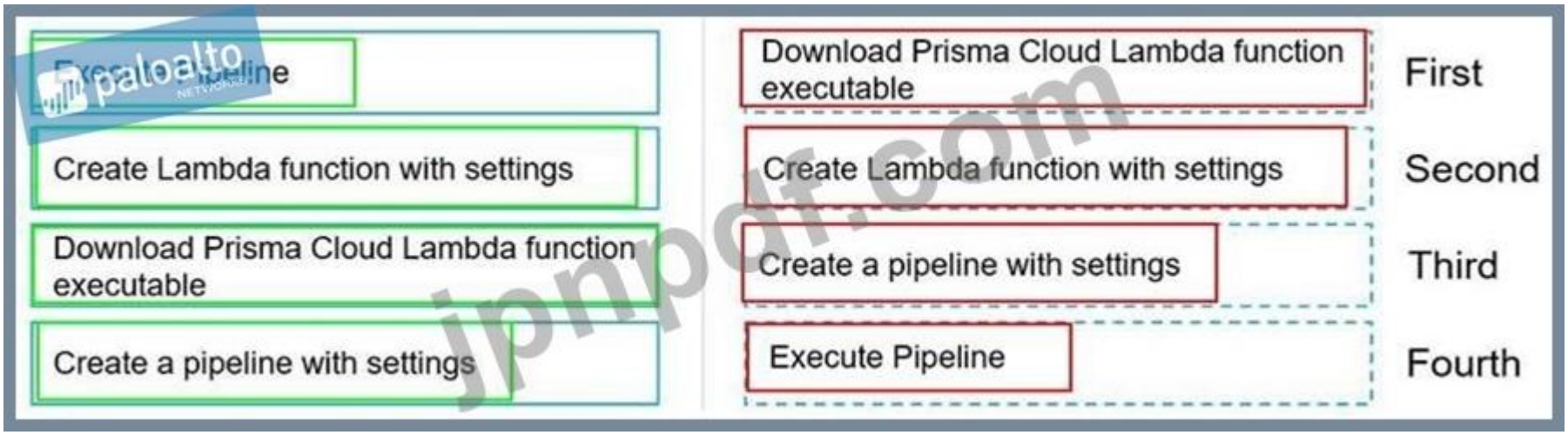
導入アドバイザーは、可視性、コンプライアンス、ガバナンス、脅威の検出と対応という 4 つのカテゴリを使用して、クラウド セキュリティ体制管理の導入の進捗状況を測定します。可視性は、環境内のリソースを識別し、セキュリティ制御が確実に実施されるようにするのに役立ちます。コンプライアンスは、環境が規制および業界標準を確実に満たすようにするのに役立ちます。ガバナンスは、環境が安全であり、ポリシーに従って管理されていることを確認するのに役立ちます。脅威の検出と対応は、脅威を迅速かつ効果的に検出して対応するのに役立ちます。

最新問題: 31

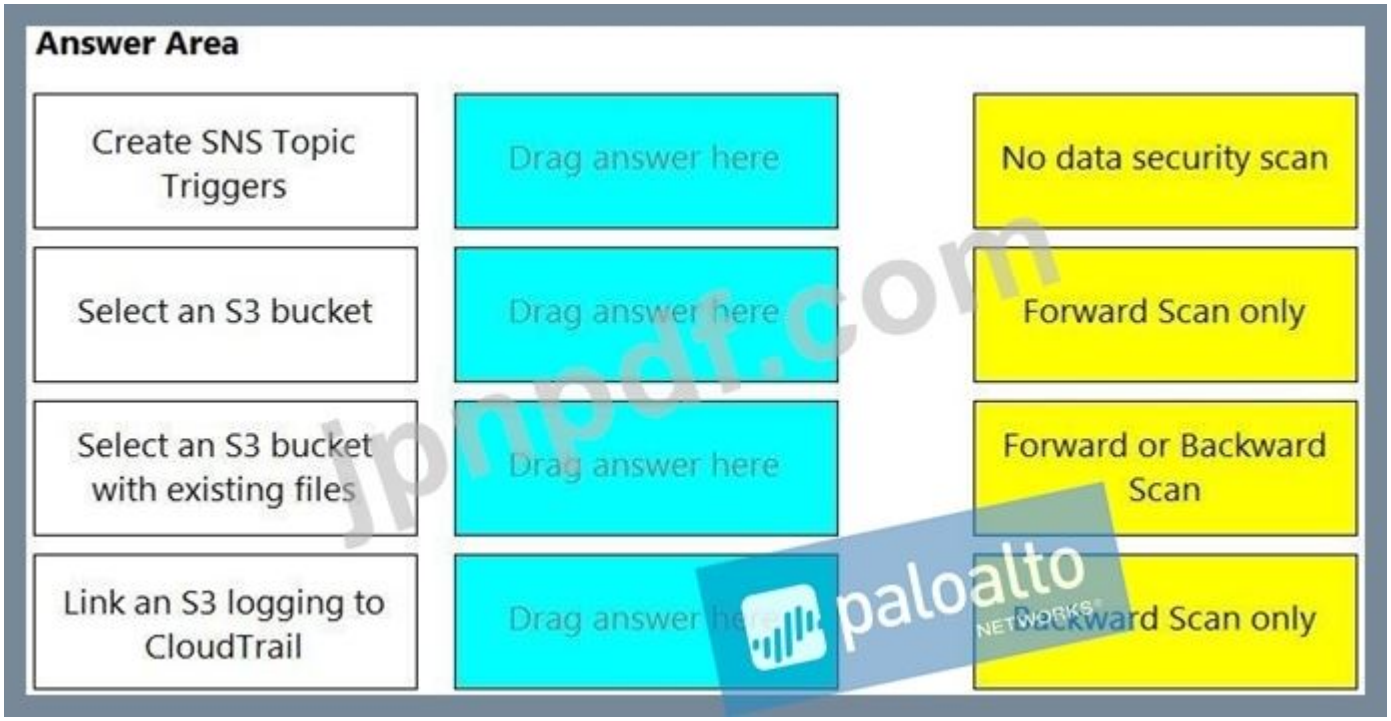
ステップを正しい順序に移動して、AWS DevOps を使用してサーバーレス スキャンを設定および実行します。



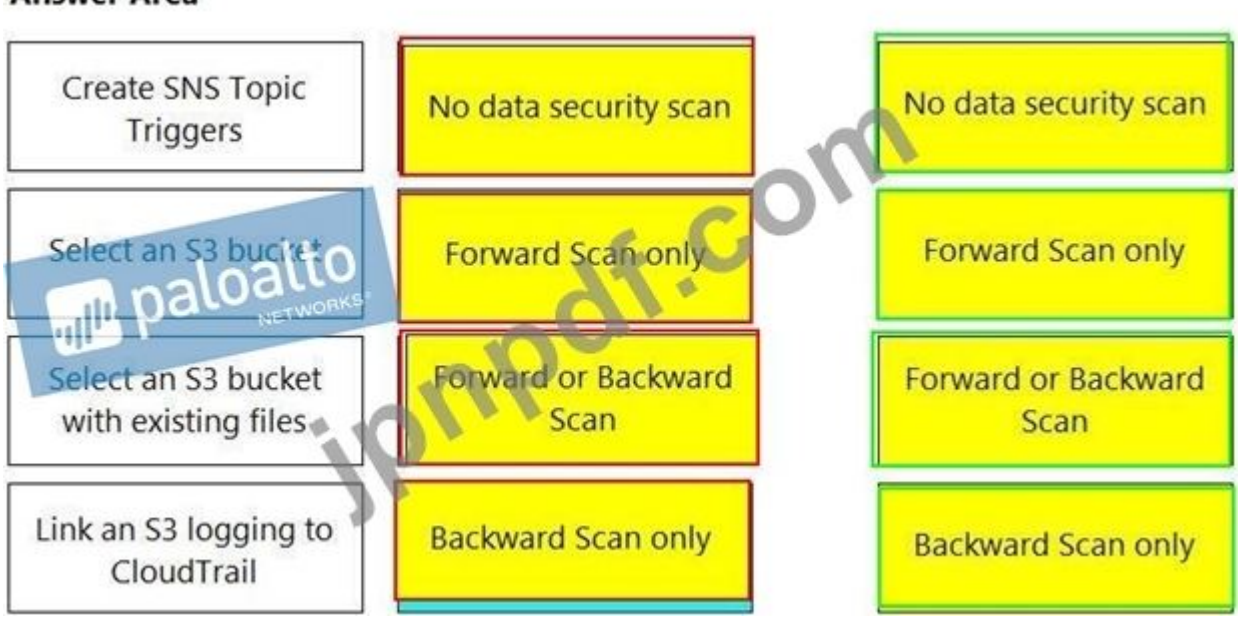
Answer:



最新問題**: 32**
特定の操作ごとに正しいスキャン モードを一致させます。
(プルダウン リストから回答を選択します。回答は複数回使用することも、まったく使用しないこともできます。)



Answer:



最新問題**: 33**

システム管理者の役割を持つユーザーが Prisma Cloud で生成できるアクセス キーの最大数はいくつですか?

A. 1

B. 2

C. 3

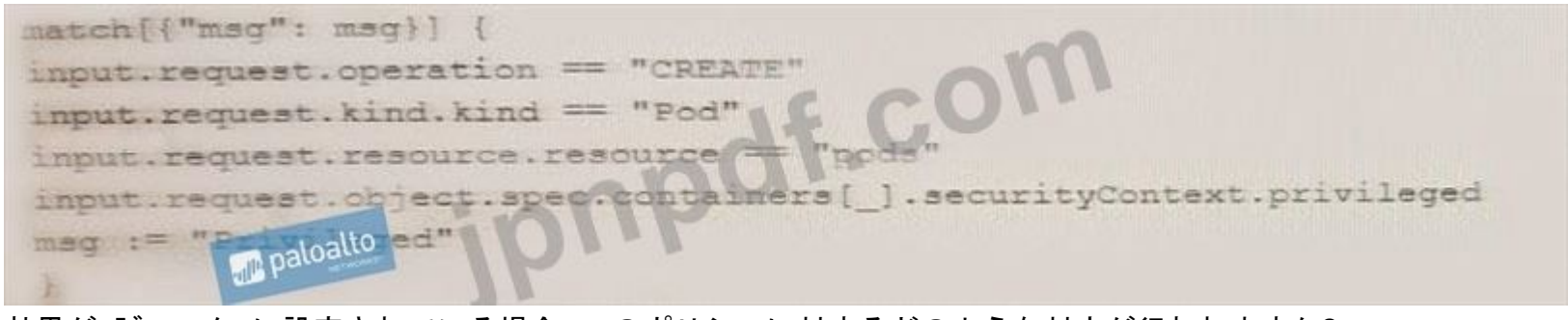
D. 4

Answer: B (メーッセージを残す**)**

参照：

Prisma Cloud では、システム管理者の役割を持つユーザーは最大 2 つのアクセス キーを生成できます。これらのキーは API アクセスと自動化に使用され、Prisma Cloud の機能との安全かつ制御された対話を可能にします。

最新問題: **34**
このアドミッション コントロール ポリシーを確認してください。



効果が 「ブロック」に設定されている場合、このポリシーに対するどのような対応が行われますか?
A. ポリシーは特権ポッドの作成をブロックします。
B. ポリシーは特権ホスト上のすべてのポッドをブロックします
C. ポリシーは、特権ポッドが作成されたときに管理者にのみ警告します。
D. ポリシーは Defender を特権付き Defender に置き換えます。
Answer: D (メーッセージを残す)

最新問題: **35**
コンプライアンス チームは、Prisma Cloud ポリシーをコンプライアンス フレームワークに関連付ける必要があります。このタスクを実行するには、チームはどのオプションを選択する必要がありますか?
A. カスタム コンプライアンス
B. ポリシー
C. コンプライアンス
D. アラート ルール
Answer: A (メーッセージを残す)
Prisma Cloud ポリシーとコンプライアンス フレームワークの関連付けは、Prisma Cloud のカスタム コンプライアンス機能を通じて行われます。この機能により、チームは Prisma Cloud のすぐに使用できる (OOTB) ポリシーをさまざまなコンプライアンス標準およびフレームワークにマッピングできるため、組織は特定の規制要件や内部コンプライアンス義務に従ってコンプライアンスのレポートと管理を調整できます。
オプション A: カスタム コンプライアンスは、Prisma Cloud ポリシーを組織の特定のコンプライアンス ニーズに合わせてカスタマイズおよび調整する柔軟性を提供するため、正しい選択です。これにより、コンプライアンス チームはカスタム コンプライアンス標準を作成し、既存の Prisma Cloud ポリシーをこれらの標準にマッピングし、組織独自のコンプライアンス体制を反映するコンプライアンス レポートを生成できます。
参照：
Prisma Cloud コンプライアンス ドキュメント: ポリシーをこれらの標準に関連付ける方法など、Prisma Cloud 内でのカスタム コンプライアンス標準の設定と管理に関する詳細なガイダンスを提供します。
コンプライアンス管理のベスト プラクティス: クラウド環境における効果的なコンプライアンス管理戦略についての洞察を提供し、多様な規制要件を満たすためのカスタマイズ可能なコンプライアンス フレームワークの役割を強調します。

最新問題: **36**
Prisma Cloud ポリシーを表示するアクセス権を持つ 2 つの役割はどれですか? (2つお選びください。)

A. セキュリティの構築と導入
B. 監査人
C. 開発 SecOps
D. ディフェンダーマネージャー
Answer: (解答を表示する**)**
Prisma Cloud では、ポリシーを表示するアクセス権を持つロールには、Auditor と Dev SecOps が含まれます。監査者の役割は通常、コンプライアンスと監視に焦点を当てており、ユーザーは変更を加えずに構成、ポリシー、およびコンプライアンスのステータスを確認できます。Dev SecOps の役割は、CI/CD パイプライン内でのセキュリティ実践の統合に重点を置き、開発、セキュリティ、運用の間のギャップを埋めます。どちらの役割も、その機能を効果的に実行するために Prisma Cloud ポリシーにアクセスする必要があり、クラウド環境とアプリケーションのライフサイクル全体にわたってセキュリティとコンプライアンスが維持されることが保証されます。

最新問題**: 37**
データ セキュリティ モジュールで利用できる 3 種類の分類はどれですか? (3つお選びください。)
A. 個人を特定できる情報
B. 悪意のある IP
C. 準拠規格
D. 財務情報
E. マルウェア
Answer: A,D,E (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security.html

最新問題**: 38**
Jenkins パイプライン スキャンのステップの順序は何ですか?
(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)

Answer:

最新問題: **39**
顧客には、ransomWare という名前のプロセスが実行されたときに、イメージ topSecret:latest からコンテナを終了するという要件があります。
この要件を満たすために、管理者は Prisma Cloud Compute をどのように構成すればよいでしょうか?
A. コンテナ モデルを手動再学習に設定し、デフォルトのランタイム ルールをプロセス保護のためにブロックするように設定します。
B. 再学習するコンテナ モデルを設定し、プロセス保護を防ぐデフォルトのランタイム ルールを設定します。
C. コンテナに対して 『ルールにコピー」を選択し、拒否されたプロセス リストに ransomWare プロセスを追加し、アクションを 『ブロック」に設定します。
D. 特定のコンテナ名を対象とした新しいランタイム ポリシーを追加し、ransomWare プロセスを拒否されたプロセス リストに追加し、アクションを 『防止」に設定します。
Answer: C (メーッセージを残す)

最新問題: **40**
顧客には、ransomWare という名前のプロセスが実行されたときに、イメージ topSecret:latest からコンテナを終了するという要件があります。
この要件を満たすために、管理者は Prisma Cloud Compute をどのように構成すればよいでしょうか?
A. コンテナ モデルを手動再学習に設定し、デフォルトのランタイム ルールをプロセス保護のためにブロックするように設定します。
B. 再学習するコンテナ モデルを設定し、プロセス保護を防ぐデフォルトのランタイム ルールを設定します。
C. 特定のコンテナ名を対象とした新しいランタイム ポリシーを追加し、ransomWare プロセスを拒否されたプロセス リストに追加し、アクションを 『防止」に設定します。
D. コンテナに対して 『ルールにコピー」を選択し、拒否されたプロセス リストに ransomWare プロセスを追加し、アクションを 『ブロック」に設定します。
Answer: (解答を表示する)
『ansomWare」という名前のプロセスが実行されたときにイメージ 『opSecret:latest」のコンテナを終了するには、管理者は特に問題のコンテナを対象とした新しいランタイム ポリシーを Prisma Cloud Compute に作成する必要があります。このポリシー内の拒否されたプロセス リストに 『ansomWare」プロセスを追加し、アクションを 『防止」に設定すると、Prisma Cloud Compute は対象のコンテナ内で指定されたプロセスの実行をアクティブに監視し、次の場合にはコンテナを終了する予防措置を講じます。プロセスが検出されます。この

アプローチにより、組織が特定した特定の脅威に対処する正確で的を絞ったセキュリティ対策が可能になり、それによって全体的なセキュリティ体制が強化され、機密ワークロードを潜在的な侵害から保護できます。

最新問題: **41**
既存の ECS クラスターの場合、Amazon ECS にコンソールをインストールするために必要な手順を示すオプションはどれですか?
A. コンソールは ECS クラスターでネイティブに実行できません。ワンボックス展開を使用する必要があります。
B. リリース tarball をダウンロードして抽出します。AWS からのダウンロード タスク
コンソールタスク定義の作成 タスク定義のデプロイ
C. リリース tarball をダウンロードして解凍します。
EFS ファイル システムを作成し、クラスター内の各ノードにマウントする コンソール タスク定義を作成する タスク定義を展開する
D. リリース tarball をダウンロードして解凍します。
各ノードにコンソール データ用の独自のストレージがあることを確認する コンソール タスク定義を作成する タスク定義を展開する
Answer: C (メーッセージを残す**)**

最新問題: **42**
パブリック クラウド アカウントを Prisma Cloud Enterprise にオンボーディングしました。構成リソースの取り込みはオンボードアカウントの資産インベントリに表示されますが、アカウント内の構成資産に対してアラートは生成されません。
構成ポリシーは Prisma Cloud Enterprise テナントで有効になり、それらのポリシーは既存のアラート ルールに関連付けられます。これらのポリシーに一致する調査の ROL ステートメントは、構成リソースの結果を正常に返します。
アラートが生成されないのはなぜですか?
A. パブリック クラウド アカウントはアラート通知に関連付けられていません。
B. パブリック クラウド アカウントでは監査証跡の取り込みが有効になっていません。
C. パブリック クラウド アカウントは構成リソースにアクセスしません。
D. パブリック クラウド アカウントはアラート ルールに関連付けられていません。
Answer: (解答を表示する**)**
Prisma Cloud Enterprise では、オンボードされたパブリック クラウド アカウントの構成資産に対してアラートを生成するには、そのアカウントが、有効な構成ポリシーと一致するアラート ルールに関連付けられていることが重要です。アカウントがアラート ルールにリンクされていない場合、または既存のアラート ルールが構成ポリシーと一致しない場合、構成リソースの取り込みが表示されていてもアラートは生成されず、RQL ステートメントは構成リソースの結果を返します。この要件は、セキュリティ インシデントを迅速に特定して対処するために、適切に構造化されたアラート メカニズムの必要性を強調しています。

最新問題: **43**
顧客は、50 台の Defender が接続された開発環境を持っています。開発環境で 30 個のスタンドアロン Defender をアップグレードするためのメンテナンス期間は月曜日に設定されていますが、残りの 20 個のスタンドアロン Defender をアップグレードできるメンテナンス期間は日曜日までありません。
この状況を管理するには、どの推奨アクションが最適ですか?
A. 開発環境内のすべてのスタンドアロン Defender をアップグレードするのに適したメンテナンス期間を見つけます。
B. パロアルトネットワークスでサポートケースを開き、自動アップグレードを手配します。

C. メンテナンス期間中にアップグレードする必要がある Defender に対応する行にある個別の [Actions] > [Upgrade] ボタンをクリックして、Defender のサブセットをアップグレードします。
D. [管理] > [ディフェンダー] > [管理] に移動し、[ディフェンダー] をクリックし、スケジューラを使用して、メンテナンス期間中に自動的にアップグレードするディフェンダーを選択します。
Answer: D (メーッセージを残す**)**

最新問題**: 44**
Prisma Cloud Compute の 監視」セクションにあるインシデント エクスプローラーの目的は何ですか?
A. 進行中の攻撃を特定するために、大量の監査データを手動で分類します。
B. インシデントに対するより迅速かつ効果的な対応を可能にするために、コンソールが実行されるホストに大量のフォレンジック データを保存します。
C. 個々のイベントを関連付けて潜在的な攻撃を特定し、一連のプロセス、ファイル システム、およびネットワーク イベントを提供してインシデントの包括的なビューを提供します。
D. 防御者によって生成されたすべての監査イベントを特定して抑制します *
Answer: C (メーッセージを残す**)**
Prisma Cloud Compute の モニター」セクションにあるインシデント エクスプローラーの目的は、個々のイベントを関連付けることによってインシデントの包括的なビューを提供することです。これは、一連のプロセス、ファイル システム、ネットワーク イベントを通じて潜在的な攻撃を特定するのに役立ち、インシデントのタイムラインと影響の全体像を把握できます。

最新問題**: 45**
Defender がアドミッション コントローラーとして機能するように構成されている Kubernetes オブジェクトの 種類」はどれですか?
A. 変更中のWebhookConfiguration
B. DestinationRules
C. WebhookConfiguration の検証中
D. ポッドセキュリティポリシー
Answer: (解答を表示する**)**
Kubernetes のコンテキストでは、アドミッション コントローラーは、オブジェクトが永続化される前、リクエストが認証および許可された後に、Kubernetes API サーバーへのリクエストをインターセプトするコードの一部です。アドミッション コントローラーを使用すると、オブジェクトを作成または更新する前に、複雑な検証およびポリシー制御をオブジェクトに適用できます。
ValidatingWebhookConfiguration は、Kubernetes オブジェクトの作成、更新、または削除のリクエストが構成で定義されたルールに一致する場合に、サービス (アドミッション Webhook) にアドミッション検証リクエストを送信するように API サーバーに指示する Kubernetes オブジェクトです。その後、Webhook はカスタム ロジックに基づいてリクエストを承認または拒否できます。
MutatingWebhookConfiguration は似ていますが、オブジェクトが作成または更新される前に変更するために使用されます。これは、保護または検証機能で動作するアドミッション コントローラーの主な機能ではありません。
DestinationRules は Istio サービス メッシュに関連しており、Kubernetes アドミッション コントロールには関係ありません。
PodSecurityPolicies (PSP) は Kubernetes のアドミッション コントローラーの一種ですが、Kubernetes によって事前定義されており、ValidatingWebhookConfiguration のような特定の構成オブジェクトを必要としません。PSP は、Kubernetes の最新バージョンでも非推奨になりました。

したがって、正解は C. ValidatingWebhookConfiguration です。これは、リクエストを検証するためのアドミッション Webhook を構成するために使用される Kubernetes オブジェクトであり、Prisma Cloud でアドミッション コントローラーとして機能する Defender の役割と一致しています。
提供されたドキュメントからの参照:
アップロードされたドキュメントには、Kubernetes オブジェクトや Prisma Cloud と Kubernetes の統合に関する具体的な詳細は含まれていません。ただし、この説明は、Kubernetes 環境のセキュリティを保護するための一般的な Kubernetes の実践および Prisma Cloud の機能と一致しています。

最新問題**: 46**
セキュリティ チームは、実行中の特定のコンテナを CMAF ポリシーの対象にしたいと考えています。管理者は、コンテナを対象とするポリシーの範囲をどのように設定すればよいですか?
A. ポリシーのスコープを名前空間に設定します
B. ポリシーの範囲を Defender 名に設定します。
C. ポリシーのスコープをイメージ名に設定します
D. ポリシーの範囲をホスト名に設定します
Answer: (解答を表示する**)**

最新問題**: 47**
お客様は、すべての Defender を一度にアップグレードせずにコンソールをアップグレードする必要がある大規模な環境を持っています。
Defender のローリング アップグレードを実行する前の 2 つの前提条件は何ですか? (2つお選びください。)
A. ローリング アップグレード前の最新のTwistcli ツールの手動インストール
B. ローリング アップグレードの実行前に、すべての Defender が読み取り専用モードに設定されます。
C. コンソールをインストールできる 2 番目の場所
D. ローリング アップグレードを実行するには追加のワークロード ライセンスが必要です
E. バージョン n-1 の既存のコンソール
Answer: B,E (メーッセージを残す**)**
セキュリティ ポリシーの適用とクラウド ワークロードの保護を担当するコンポーネントである Defender のローリング アップグレードを実行する前に、前提条件の 1 つはバージョン n-1 の既存のコンソール (オプション E) であることです。これにより、Defender を管理するコンソールに互換性があり、アップグレードされた Defender をサポートできることが保証されます。ローリング アップグレードにより、中断が最小限に抑えられ、アップグレード プロセス中の継続的な保護が保証されます。リストされている他のオプションは、Defender ローリング アップグレードの前提条件に直接関係しません。

最新問題: **48**
エアギャップ環境で実行する必要がある場合、どの製品をインストールする必要がありますか?
A. Prisma Cloud Jenkins プラグイン
B. セルフホスト型プラグインを備えた Prisma Cloud
C. Prisma Cloud エンタープライズ エディション
D. Prisma Cloud Compute Edition
Answer: D (メーッセージを残す**)**

最新問題: **49**
顧客は Prisma Cloud 経由で会社の AWS アカウントを監視したいと考えていますが、現時点では監視するリソース構成のみが必要です。
このアカウントをオンボーディングするために必要な 2 つの情報はどれですか? (2つお選びください。)
A. Active Directory ID
B. 外部 ID
C. サブスクリプション ID
D. ロール ARN
E. クラウドトレイル
Answer: (解答を表示する**)**

最新問題: **50**
ビルド ポリシーと実行構成ポリシーの違いについて正しい 2 つの記述はどれですか? (2つお選びください。)
A. ビルド ポリシーを使用すると、IaC テンプレートのセキュリティ構成の誤りをチェックし、これらの問題が運用環境に影響を与えないようにすることができます。
B. ビルドおよび監査イベント ポリシーは、構成ポリシー セットに属します。
C. 実行ポリシーとネットワーク ポリシーは構成ポリシー セットに属します。
D. ポリシーを実行してリソースを監視し、これらのクラウド リソースのデプロイ後に潜在的な問題がないか確認します。
E. 実行ポリシーは、環境内のネットワーク アクティビティを監視し、実行時の潜在的な問題をチェックします。
Answer: (解答を表示する**)**

最新問題: **51**
ビルド ポリシーと実行構成ポリシーの違いについて正しい 2 つの記述はどれですか? (2つお選びください。)
A. ビルド ポリシーを使用すると、IaC テンプレートのセキュリティ構成の誤りをチェックし、これらの問題が運用環境に影響を与えないようにすることができます。
B. 実行ポリシーは、環境内のネットワーク アクティビティを監視し、実行時の潜在的な問題をチェックします。
C. ポリシーを実行してリソースを監視し、これらのクラウド リソースのデプロイ後に潜在的な問題がないか確認します
D. ビルドおよび監査イベント ポリシーは構成ポリシー セットに属します
E. 実行ポリシーとネットワーク ポリシーは構成ポリシー セットに属します
Answer: B,D (メーッセージを残す**)**

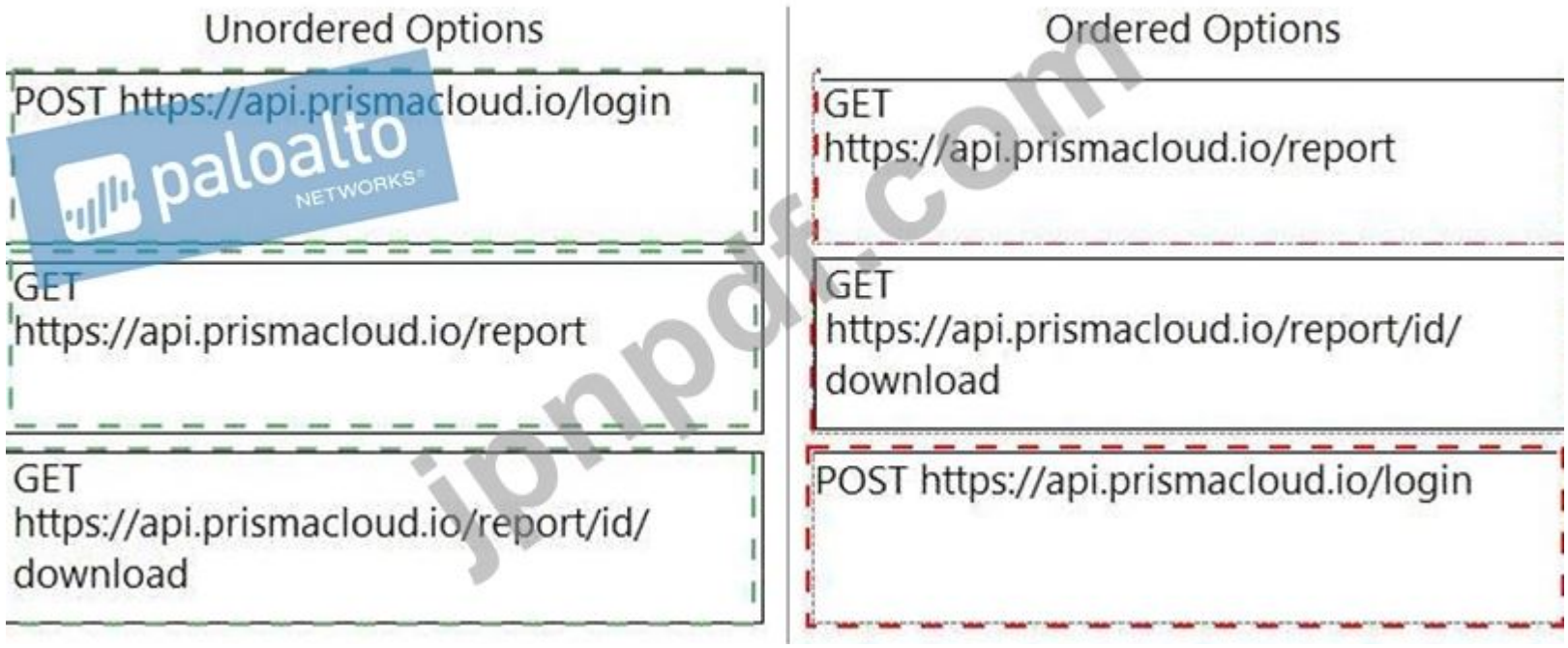
最新問題: **52**

開発チームは、環境内のポッドからのクロスサイト スクリプティング攻撃をブロックしたいと考えています。チームはこの攻撃から保護するために CNAF ポリシーをどのように構築する必要がありますか?
A. 特定のリソースを対象としたホスト CNAF ポリシーを作成し、XSS 攻撃保護のチェックボックスをオンにして、アクションを 防止」に設定します。
B. 特定のリソースを対象としたコンテナ CNAF ポリシーを作成し、XSS 攻撃保護のチェックボックスをオンにして、アクションをアラートに設定します。
C. 特定のリソースを対象としたコンテナ CNAF ポリシーを作成し、XSS 保護のチェックボックスをオンにして、防止するアクションを設定します。
D. 特定のリソースを対象としたコンテナ CNAF ポリシーを作成します。 明示的に許可された受信 IP ソース」をポッドの IP アドレスに設定する必要があります。
Answer: (解答を表示する**)**
環境内のポッドをクロスサイト スクリプティング (XSS) 攻撃から保護するには、開発チームは Container Cloud Native Application Firewall (CNAF) ポリシーを作成する必要があります。このポリシーは、XSS 保護のオプションをオンにし、アクションを 防止」に設定して、特定のリソース (特定のポッドまたはポッドのセットなど) を対象にする必要があります。この構成により、ターゲットのコンテナーに向けられた XSS 攻撃が効果的にブロックされます。

最新問題**: 53**
管理者は、Prisma Cloud Enterprise テナントから既存のコンプライアンス レポートをダウンロードするカスタム サービスを作成する任務を負っています。
このサービスの API はどの順序で実行されますか?
(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)

Answer:

Answer Area



説明

自動的に生成されたグラフィカル ユーザー インターフェイスの説明を含む画像

最新問題: **54**

Prisma Cloud 内のアウトバウンド通知の例は何ですか?

A. テナブル

B. AWS インスペクター

C. クアリス

D. PagerDuty

Answer: D (メーッセージを残す)

最新問題: **55**
どのコンテナ イメージ スキャンが正しく構築されていますか?
A. Twistcli イメージ スキャン --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/ 最新 --details
B. Twistcli イメージ スキャン --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest
C. Twistcli 画像スキャン --address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest
D. Twistcli イメージ スキャン --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest
Answer: B (メーッセージを残す)

最新問題: **56**
Prisma Cloud Data Security ではどのデータ ストレージ タイプがサポートされていますか?
A. IBM クラウド オブジェクト ストレージ
B. AWS S3 バケット
C. Oracle オブジェクト ストレージ
D. Google ストレージ クラス
Answer: (解答を表示する)
Prisma Cloud Data Security は、AWS S3 バケット (B) を含むさまざまなデータ ストレージ タイプをサポートします。AWS S3 (Simple Storage Service) は、スケーラビリティ、データ可用性、セキュリティ、パフォーマンスを提供する、広く使用されているオブジェクト ストレージ サービスです。S3 バケットを保護する Prisma Cloud の機能は、これらのバケット内に保存されたデータが不正アクセス、データ侵害、その他のセキュリティ脅威から確実に保護されるため、ストレージのニーズに AWS を活用している組織にとって非常に重要です。Prisma Cloud は、S3 バケットに保存されたデータに対する包括的な可視性を提供し、データ分類、コンプライアンス監視、脅威検出を可能にして機密データを効果的に保護します。

最新問題: **57**
顧客の環境には次のような複数の違反があります。
ユーザー名前空間が有効になっています
LDAPサーバーが有効になっています
SSHルートが有効になっています
管理者はこれらの結果を確認するためにコンソールのどのセクションを使用する必要がありますか?
A. レーダー
B. 管理
C. 脆弱性
D. コンプライアンス
Answer: B (メーッセージを残す)

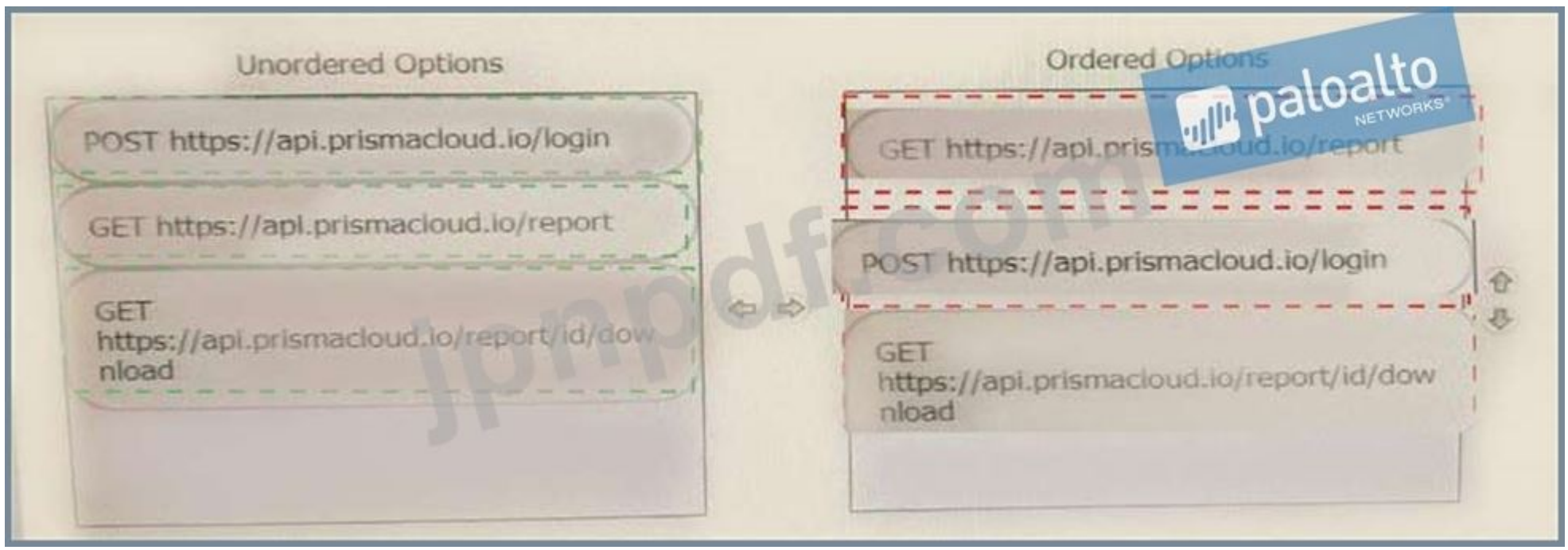
最新問題: **58**
Prisma Cloud での SSO 統合を正確に特徴づけているのはどれですか?
A. Prisma Cloud は IdP で開始される SSO をサポートし、その SAML エンドポイントは POST メソッドと GET メソッドをサポートします。

B. Okta、Azure Active Directory、PingID などが SAML 経由でサポートされます。
C. 管理者は、Prisma Cloud が監視するすべてのクラウド アカウントに対して異なるアイデンティティ プロバイダー (IdP) を構成できます。
D. Prisma Cloud API にアクセスする必要がある管理者は、構成後に SSO を使用できます。
Answer: A (メーッセージを残す**)**

最新問題**: 59**
コンピューティングでコンテナーおよびホスト ディフェンダーをデプロイするためにアクセスする必要がある DevOps ユーザーには、どのロールを割り当てる必要がありますか?
A. 開発者
B. クラウド プロビジョニング管理者
C. システム管理者
D. セキュリティの構築と導入
Answer: D (メーッセージを残す**)**

最新問題**: 60**
管理者は、Prisma Cloud Enterprise から既存のコンプライアンス レポートをダウンロードするカスタム サービスを作成する任務を負っています。
テナント - このサービスの API はどの順序で実行されますか? (最初のステップから最後のステップまで、正しい順序でステップをドラッグします)

Answer:



最新問題: **61**
[防御] > [コンプライアンス] > [コンテナとイメージ] > [CI] のルールで利用できるコンプライアンス チェックのタイプはどれですか?
A. ホスト
B. コンテナ
C. 関数
D. 画像
Answer: (解答を表示する)
Palo Alto Networks の Prisma Cloud 内の [防御] > [コンプライアンス] > [コンテナとイメージ] > [CI] のコンテキストでは、コンプライアンス チェックはセキュリティ体制とコンテナ イメージのコンプライアンスに焦点を当てています。したがって、このセクションで利用できるコンプライアンス チェックの種類はイメージに関連しており、展開前にイメージがセキュリティのベスト プラクティスとコンプライアンス標準に準拠していることを確認します。

最新問題: **62**
顧客がコンテナ監査を検討しており、監査によりクリプトマイナー攻撃が特定されました。この監査が発生した可能性がある 3 つのオプションはどれですか? 3つお選びください。）
A. マイニングされた通貨はユーザー トークンに関連付けられます。
B. マイニングされた通貨の価値が $100 を超えています。
C. 一般的なクリプトマイナー ポートの使用法が見つかりました。

D. 共通のクリプトマイナープロセス名が見つかりました
E. コンテナーの長時間にわたる高い CPU 使用率が検出されました。
Answer: A,C,D (メーッセージを残す)

最新問題**: 63**
セキュリティ チームは、Web アプリケーション コンテナを SQLi 攻撃から保護したいと考えていますか? 管理者はコンテナを保護するためにどのタイプのポリシーを作成する必要がありますか?
A. コンプライアンス
B. ランタイム
C. CNAF
D. CNNF
Answer: D (メーッセージを残す)

最新問題**: 64**
開発チームは、環境内のポッドからのクロスサイト スクリプティング攻撃をブロックしたいと考えています。チームはこの攻撃から保護するために CNAF ポリシーをどのように構築する必要がありますか?
A. 特定のリソースを対象としたコンテナ CNAF ポリシーを作成します。 明示的に許可された受信 IP ソース」をポッドの IP アドレスに設定する必要があります。
B. 特定のリソースを対象としたコンテナ CNAF ポリシーを作成し、XSS 攻撃保護のチェックボックスをオンにして、アクションをアラートに設定します。
C. 特定のリソースを対象としたコンテナ CNAF ポリシーを作成し、XSS 保護のチェックボックスをオンにして、防止するアクションを設定します。
D. 特定のリソースを対象としたホスト CNAF ポリシーを作成し、XSS 攻撃保護のチェックボックスをオンにして、アクションを 防止」に設定します。
Answer: D (メーッセージを残す)

最新問題**: 65**
Console v20.04 と Kubernetes の展開で Defender をアップグレードするには、どの 2 つのオプションを使用できますか? (2つお選びください。)
A. Defender を削除してから、新しい DaemonSet をデプロイします。これにより、Defender はデプロイごとに自動的に更新されなくなります。
B. Defenders DaemonSet を削除し、Cloud Discovery を使用して Defenders を自動的に再デプロイします。
C. 提供されたcurl | を実行します。コンソールから bash スクリプトを使用して Defender を削除し、Cloud Discovery を使用して Defender を自動的に再デプロイします。
D. Defender を自動的にアップグレードします。
Answer: B,C (メーッセージを残す)

最新問題**: 66**
Prisma Cloud Compute の初期展開中に、顧客は環境内の脆弱性に気づきます。
デフォルトの脆弱性ポリシーを正しく説明しているのはどれですか?

A. 重大度に関係なく、すべての脆弱性について警告します。
B. 3 つ以上の重大な脆弱性があるコンテナに対してアラートを生成します。
C. コンテナに重大な脆弱性が含まれている場合、30 日後にコンテナをブロックします。
D. 脆弱性を含むすべてのコンテナをブロックします。
Answer: A (メーッセージを残す**)**

最新問題**: 67**
カスタム ネットワーク ポリシーを作成する手順はどのような順序ですか?
(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)

Answer:

Answer Area

参照：
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy.html

最新問題: **68**
Prisma Cloud での SSO 統合を正確に特徴づけているのはどれですか?
A. Prisma Cloud は IdP で開始される SSO をサポートし、その SAML エンドポイントは POST メソッドと GET メソッドをサポートします。
B. Okta、Azure Active Directory、PingID などが SAML 経由でサポートされます。
C. 管理者は、Prisma Cloud が監視するすべてのクラウド アカウントに対して異なるアイデンティティ プロバイダー (IdP) を設定できます。
D. Prisma Cloud API にアクセスする必要がある管理者は、構成後に SSO を使用できます。
Answer: (解答を表示する**)**
セクション: (なし)
説明

最新問題: **69**
API を使用して取得できるポリシーの 2 つの属性はどれですか? (2つお選びください。)
A. ポリシーラベル
B. ポリシー署名
C. ポリシーモード
D. ポリシー違反
Answer: A,C (メーッセージを残す**)**

Prisma Cloud API を使用すると、ユーザーはポリシー ラベル (オプション A) やポリシー モード (オプション C) などのポリシーのさまざまな属性を取得できます。ポリシー ラベルはポリシーの分類と整理に役立ちますが、ポリシー モードはポリシーがどのように適用されるか (警告、強制など) を決定します。ポリシー署名 (オプション B) は、ポリシーの内部識別と処理に関連するため、API を介して取得用に公開される標準属性ではありません。ポリシー違反 (オプション D) は、ポリシー違反から生じる結果またはイベントであり、API 経由で取得できるポリシー自体の属性ではありません。

最新問題**: 70**
myimage:latest という名前のイメージをTwistcli でスキャンし、コンソールから結果を取得できる API 呼び出しはどれですか?
A. $Twistcli 画像スキャン \
--アドレス <COMPUTE_CONSOLE> \
--user <COMPUTER_CONSOLE_USER> \
--パスワード <COMPUTER_CONSOLE_PASSWD> \
--verbose \
私の画像: 最新
B. $Twistcli 画像スキャン \
--アドレス <COMPUTE_CONSOLE> \
--user <COMPUTER_CONSOLE_USER> \
--パスワード <COMPUTER_CONSOLE_PASSWD> \
- 詳細 \
私の画像: 最新
C. $Twistcli 画像スキャン \
--アドレス <COMPUTE_CONSOLE> \
--user <COMPUTER_CONSOLE_USER> \
--パスワード <COMPUTER_CONSOLE_PASSWD> \
私の画像: 最新
D. $Twistcli 画像スキャン \
--アドレス <COMPUTE_CONSOLE> \
--user <COMPUTER_CONSOLE_USER> \
--パスワード <COMPUTER_CONSOLE_PASSWD> \
- コンソール \
私の画像: 最新
Answer: (解答を表示する**)**
Twistcli を使用して myimage:latest という名前のイメージをスキャンし、コンソールから結果を取得できる API 呼び出しには、Prisma Cloud Compute コンソールのアドレス、ユーザー、パスワード以外に追加のフラグは必要ありません。--verbose、--details、および --console フラグは、スキャンの実行と結果の取得には必要ありません。必要なパラメータを指定したTwistcliコマンドによってスキャンが開始され、完了すると、結果がPrisma Cloud Computeコンソールで確認できるようになります。
このプロセスへの参照は、Prisma Cloud Compute ドキュメントで提供されています。このドキュメントでは、twistcli コマンドライン ツールを使用してコンテナ イメージをスキャンし、分析とアクションのために Compute Console から結果を取得する手順の概要が説明されています。

最新問題: **71**
管理者は、コンテナに対して実行時監査が生成されたことを確認します。監査メッセージは 疑わしい名前 wikipedia.com の DNS 解決。タイプ A」です。
なぜこのメッセージが監査として表示されるのでしょうか?
A. このドメインを呼び出すプロセスはコンテナ モデルの一部ではありませんでした。
B. Layer7 ファイアウォールは、これを異常な動作として検出しました。
C. DNS はコンテナ モデルの一部として学習されなかった、または DNS 許可リストに追加されませんでした。
D. これはマルウェアのソースとして知られている DNS です。
Answer: C (メーッセージを残す)

最新問題: **72**
顧客は Defender を Prisma Cloud Enterprise に接続しています。Defender は OpenShift の DaemonSet としてデプロイされています。管理者はホスト上の脆弱性のレポートをどのように入手すればよいでしょうか?
A. [防御] > [脆弱性] > [ホスト] に移動します。
B. [モニター] > [脆弱性] > [CVE ビューアー] に移動します。
C. [モニター] > [脆弱性] > [ホスト] に移動します。
D. [防御] > [脆弱性] > [VM イメージ] に移動します。
Answer: A (メーッセージを残す)

最新問題: **73**
Prisma Cloud ではどの認証メカニズムがサポートされていますか?
A. コンソール UI および API の証明書ベースの認証
B. API の SAML ベースの認証
C. コンソール UI のみの証明書ベースの認証
D. API のみの証明書ベースの認証
Answer: A (メーッセージを残す)

最新問題: **74**
ネットワーク上のリソースの 1 つが、デフォルト構成ポリシーのアラートをトリガーしました。
次のリソース JSON スニペットがあるとします。

どの RQL が脆弱性を検出しましたか?

A.
```
config from cloud.resource where cloud.type = 'aws' AND api.name ='aws-ec2-describe-images' AND json.rule =
image.platform contains windows and image.imageId contains ami-1e542176
```

B.
```
config from cloud.resource where api.name = 'aws-ecs-service' AND json.rule = launchType equals EC2 as X; config
from cloud.resource where api.name = 'aws-ecs-cluster' AND json.rule = status equals ACTIVE and
registeredContainerInstancesCount equals 0 as Y; filter '$.X.ckusterArn equals $.Y.clusterArn'; show Y;
```

C.
```
config from cloud.resource where cloud.type = 'aws' and api.name = 'aws-iam-get-credential-report' AND json.rule
= '(access_key_1_active is true and access_key_1_last_rotated != N/A and
_DateTime.ageInDays(access_key_1_last_rotated) > 90) or (access_key_2_active is true and
access_key_2_last_rotated != N/A and _DateTime.ageInDays(access_key_2_last_rotated) > 90)'
```

D.
```
config from cloud.resource where cloud.type = 'aws' AND api.name ='aws-ec2-describe-secutity-groups' AND
json.rule = isShared is false and (ipPermissions[?any((ipProtocol equals tcp or ipProtocol equals icmp or
ipProtocol equals icmpv6 or ipProtocol equals udp) and (ipRanges[*] contains 0.0.0.0/0 or ipv6Ranges[*].cidrIpv6
```

Answer: (解答を表示する)

最新問題: **75**

顧客は PCI 要件に関心があり、環境内で特権コンテナが起動できないようにする必要があります。

特権コンテナを使用しない」にはどのアクションを設定する必要がありますか?

A. 失敗

B. ブロック

C. アラート

D. 防止する

Answer: D (メーッセージを残す)

最新問題: **76**

コード セキュリティの一部として Prisma Cloud でサポートされている 2 つの統合開発環境 (IDE) プラグインはどれですか? (2つお選びください。)

A. Visual Studio コード

B. IntelliJ

C. BitBucket

D. CircleCI

Answer: A,B (メーッセージを残す)

Palo Alto Networks の Prisma Cloud は、統合開発環境 (IDE) プラグインとの統合を通じて、クラウド セキュリティ機能を開発環境に拡張します。利用可能なオプションのうち、Visual Studio Code と IntelliJ は、コード セキュリティ機能の一部として Prisma Cloud でサポートされています。これらの IDE プラグインを使用すると、開発者はセキュリティに関する洞察を開発ワークフローに直接組み込むことができ、コードベースの脆弱性やコンプライアンス問題の早期検出と修復が容易になります。多用途性と広範なプラグイン エコシステムで知られる Visual Studio Code と、強力なコーディング支援と人間工学に基づいたデザインで人気の IntelliJ は、どちらも開発者によって広く使用されています。Prisma Cloud との統合により、コードの脆弱性、構成ミス、セキュリティ ポリシーへの準拠をシームレスにスキャンできるようになり、セキュリティを開発ライフサイクルの初期段階に移すことで DevSecOps 文化を促進します。

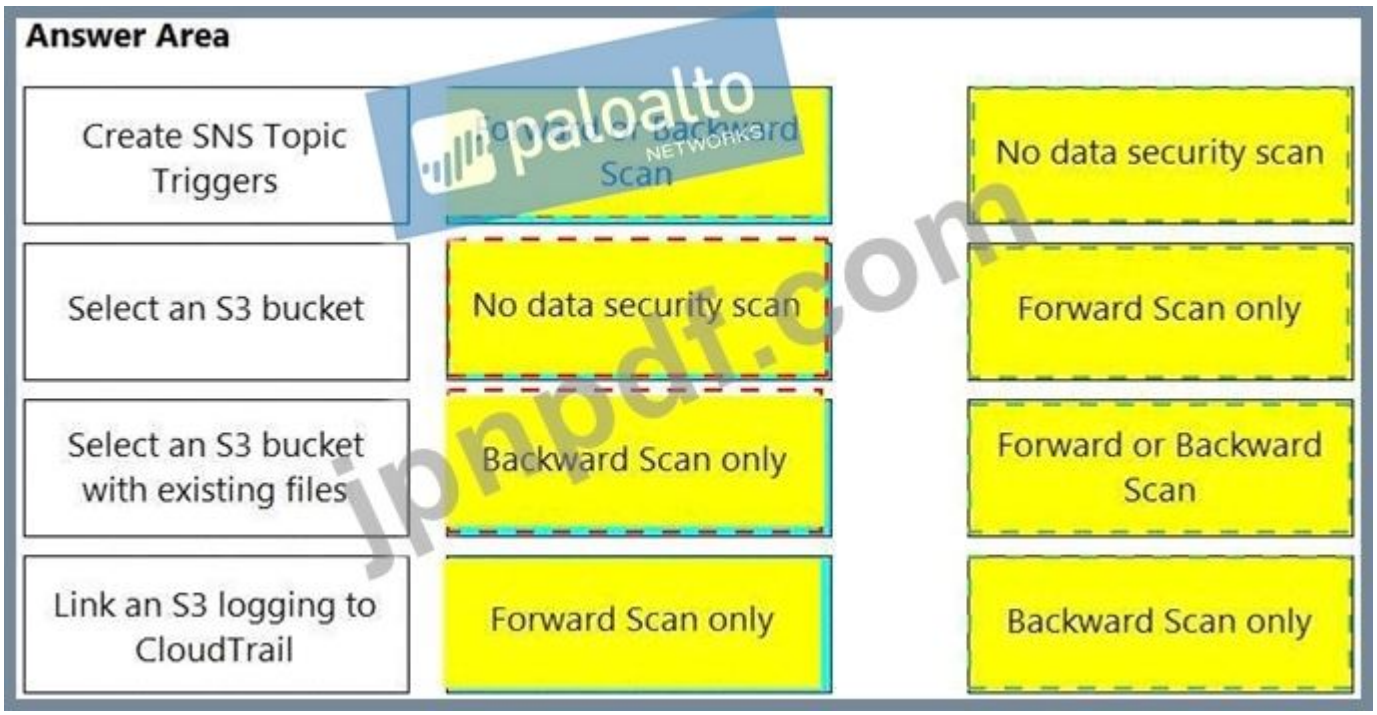
最新問題: **77**
AWS 内の S3 バケットが、「AWS S3 バケットはパブリックにアクセス可能」という Prisma Cloud Default ポリシーに違反してアラートを生成しました。ポリシー定義は次のとおりです。
config where cloud.type = 'aws' AND api.name='aws-s3api-get-bucket-acl' AND json.rule="(((acl.grants[? (@.grantee=='AllUsers')] size > 0) または、policyStatus.isPublic が true) かつ publicAccessBlockConfiguration が存在しない) または ((acl.grants[? (@.grantee=='AllUsers')] size > 0) かつ publicAccessBlockConfiguration.ignorePublicAcis が false) または (policyStatus.isPublic が true で、publicAccessBlockConfiguration.restrictPublicBuckets が false))、websiteConfiguration が存在しません」このアラートはなぜ生成されましたか?
A. クラウド アカウント内のイベント
B. S3 バケットの構成
C. 異常な動作
D. S3 バケットへのネットワーク トラフィック
Answer: D (メーッセージを残す)

最新問題: **78**
管理者は、ホストに対して実行時監査が生成されたことを確認します。監査メッセージは次のとおりです。
「サービス ポストフィックスは、/bin/sh /usr/libexec/postfix/postfix-script.stop を実行することにより、機能 SHELL を取得しようとしました。重大度の低い監査、イベントはランタイム モデルに自動的に追加されます。」どのランタイム ホスト ポリシー ルールが根本原因ですかこのランタイム監査は?
A. ファイルの整合性のための特定の構成を含むカスタム ルール
B. ネットワーク用の特定の構成を含むカスタム ルール
C. 機能について警告するデフォルトのルール
D. 不審な実行時の動作を警告するデフォルトのルール
Answer: D (メーッセージを残す)

最新問題: **79**
特定の操作ごとに正しいスキャン モードを一致させます。
(プルダウン リストから回答を選択します。回答は複数回使用することも、まったく使用しないこともできます。)

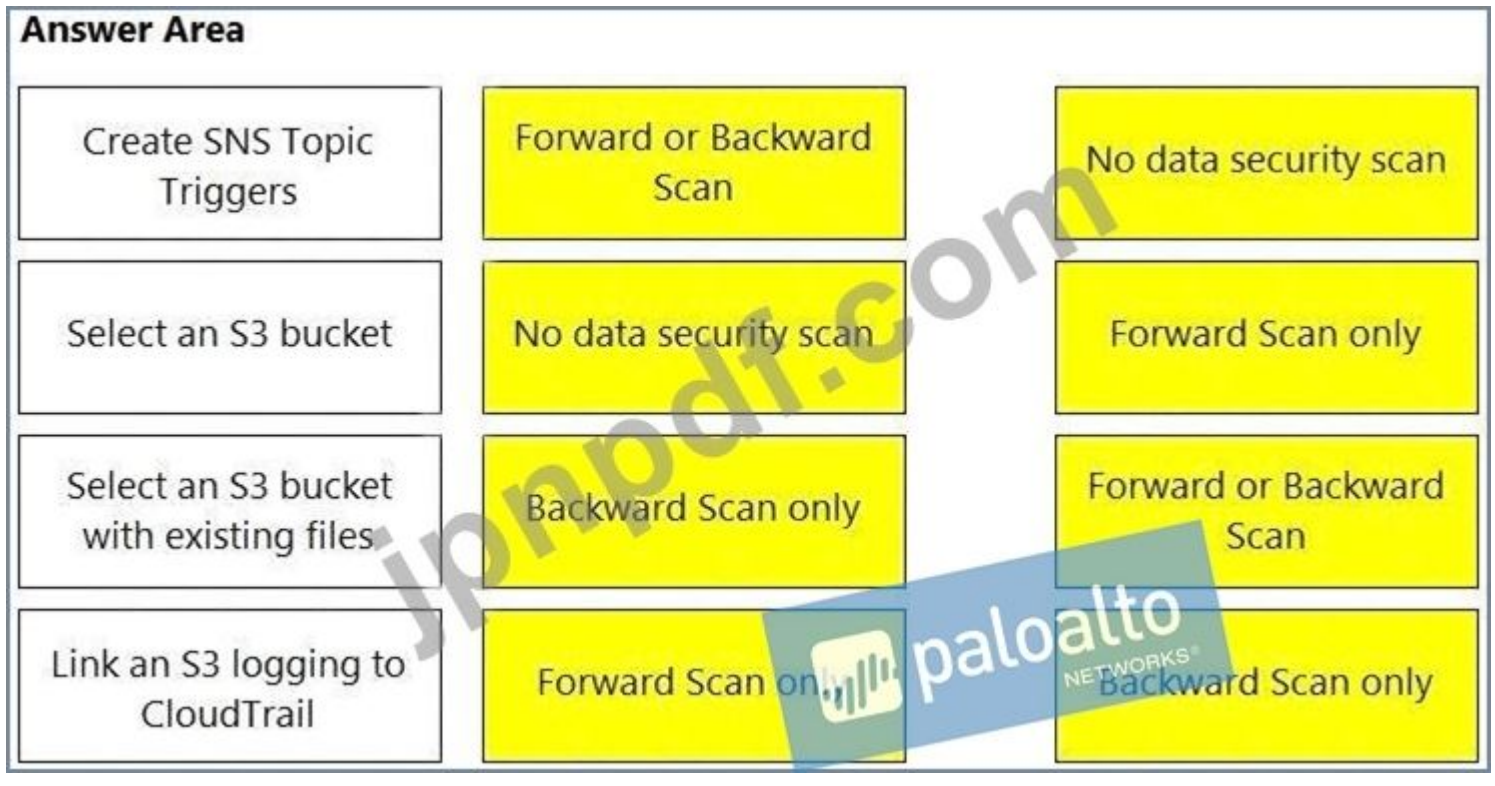
Answer Area

Answer:



説明

自動生成される図の説明



最新問題: 80
以下はどのように分類されますか?
* バックドアアカウントへのアクセス
* ハイジャックされたプロセス
*横方向の動き
* ポートスキャン
A. アドミッション コントローラー
B. インシデント
C. モデル
D. 監査
Answer: D (メーッセージを残す)

最新問題: 81
Kubernetes セットアップのどのコンポーネントが管理リクエストを承認、変更、または拒否できますか?
A. Kube コントローラー
B. Terraform コントローラー
C. アドミッション コントローラー
D. コントロール プレーン
Answer: C (メーッセージを残す)
Kubernetes 環境では、アドミッション コントローラーは、管理リクエストが Kubernetes API サーバーによって処理される前に承認、変更、または拒否する役割を担う重要なコンポーネントです。アドミッション コントローラーはゲートキーパーとして機能し、事前定義されたルールとポリシーのセットに対してリクエストを評価することでガバナンスとポリシー制御を実施します。リクエストを検証および変更して、準拠し承認された変更のみが続行できるようにします。この機能は、Kubernetes クラスターのセキュリティと整合性を維持す

るために不可欠です。これにより、不正なアクションや潜在的に有害なアクションの実行を防ぐことができ、クラスター全体のセキュリティ体制において重要な役割を果たします。

最新問題: **82**
異常ポリシーは、異常なネットワークとユーザーのアクティビティを識別するためにどの 2 つのログを使用しますか? (2つお選びください。)
A. 監査
B. ネットワーク フロー
C. トラフィック
D. ユーザー
Answer: A,B (メーッセージを残す**)**

最新問題: **83**
Prisma Cloud 環境でのポリシー違反に対して外部通知を有効にする必要がある 2 つのサービスはどれですか? (2つお選びください。)
A. SQS
B. Splunk
C. QROC
D. 電子メール
Answer: (解答を表示する**)**

最新問題: **84**
Prisma Cloud 管理者は新しいポリシーを設定しました。
このポリシーをコンプライアンス標準に割り当てるにはどの手順を使用する必要がありますか?
A. ポリシーを編集し、ステップ 3 (コンプライアンス標準) に進み、下部の [+] をクリックしてコンプライアンス標準を選択し、他のボックスに入力して、[確認] をクリックします。
B. カスタム ポリシーを既存の標準に追加することはできません。
C. ポリシーの 「コンプライアンス標準」セクションを開き、保存します。
D. [コンプライアンス] タブからコンプライアンス標準を作成し、[ポリシーに追加] を選択します。
Answer: D (メーッセージを残す**)**

最新問題: **85**
セキュリティ チームは、[監視] > [イベント] で多数の異常に気づきました。インシデント対応チームは開発者と協力して、これらの異常が誤検知であると判断します。
セキュリティ チームがこのイメージについて再学習することを選択した場合、どのような影響がありますか?
A. モデルは削除され、Defender は 24 時間再学習します。
B. 検出された異常は自動的にモデルに追加されます。
C. モデルが削除され、初期の学習状態に戻ります。
D. モデルは保持され、新しい学習期間中に観察された新しい動作は既存のモデルに追加されます。
Answer: D (メーッセージを残す**)**

Prisma Cloud では、異常が検出され、セキュリティ チームが特定のイメージの再学習を選択した場合、そのイメージの既存の動作モデルは削除されません。代わりに、システムはモデルを保持し、新しい学習期間に入り、その間、イメージに基づいてコンテナーの動作を観察します。この期間中に新しい動作が観察された場合、それらは既存のモデルに追加され、それによってコンテナの現在の運用プロファイルを反映するようにモデルが改良および更新されます。このアプローチにより、モデル内ですでに確立されている貴重な洞察とパターンを維持しながら、コンテナーの動作の変化に動的に適応できます。Relearn 機能は Prisma Cloud の適応機能の一部であり、コンテナ化されたアプリケーションの進化する性質を反映する正確で最新の動作モデルを維持できるようになります。

最新問題: **86**
Azure クラウドで ID およびアクセス管理 (IAM) アラートの自動修復を実現するには、どの 2 つの変数を変更する必要がありますか? (2 つお選びください。)
A. SB_QUEUE_KEY
B. YOUR_ACCOUNT_NUMBER
C. API_ENDPOINT
D. SQS_QUEUE_NAME
Answer: B,C (メーッセージを残す**)**

最新問題: **87**
アップグレード中にコンソールにアクセスできない場合、Defender はどのように動作しますか?
A. 防御者は、コンソールをアップグレードする前に最後にキャッシュされたポリシーと設定を使用して、アラートを継続しますが、強制はしません。
B. Web ソケットが再確立されるまで、ディフェンダーはフェイルクローズされます。
C. Web ソケットが再確立されるまで、ディフェンダーはフェールオープンします。
D. 防御者は、コンソールをアップグレードする前に最後にキャッシュされたポリシーと設定を使用して、引き続きアラートを発行し、強制します。
Answer: D (メーッセージを残す**)**
アップグレード中にコンソールにアクセスできない場合、Defender はアップグレード前に最後にキャッシュされたポリシーと設定を使用して警告を発し、強制を続けます (オプション D)。この動作により、中央管理コンソールが一時的に利用できなくなった場合でも、セキュリティの実施がアクティブかつ一貫した状態に保たれます。キャッシュされたポリシーにより、Defender は最新の既知の構成に基づいてセキュリティ体制を維持し、脅威に対する継続的な保護と確立されたセキュリティ ポリシーへの準拠を確保できます。このアプローチは、中断のないセキュリティの適用を保証するという Prisma Cloud の設計原則を反映しており、それによってメンテナンス期間中に潜在的な脆弱性から環境を保護します。

最新問題: **88**
デプロイされたイメージの上位クリティカル CVE はどこにありますか?
A. 監視 → 脆弱性 → イメージ
B. 防御 → 脆弱性 → 画像
C. モニター → 脆弱性 → 脆弱性エクスプローラー
D. 防御 → 脆弱性 → コード リポジトリ
Answer: B (メーッセージを残す**)**

デプロイされたイメージの上位クリティカル CVE は、クラウド セキュリティ コンソールの [防御] → [脆弱性] → [イメージ] セクションで確認できます。このセクションでは、重大度、修復ステータス、外部ソースへの参照など、デプロイされたイメージに関連付けられた CVE の詳細を提供します。また、ユーザーは特定された CVE に対してアクションを実行し、環境の安全性を確保することもできます。

最新問題**: 89**
Azure AD 内でセキュリティ グループを作成し、アプリケーションを作成するための十分なアクセス許可を持つユーザーを表示する出力を正しく生成する IAM Azure RQL クエリはどれですか?
A. api.name = 'azure-active-directory-authorization-policy' かつ json.rule =defaultUserRolePermissions.allowedToCreateSecurityGroups が true であり、defaultUserRolePermissions.allowedToCreateApps が true である構成
B. api.name = 'azure-active-directory-authorization-policy' かつ json.rule =defaultUserRolePermissions が存在する、cloud.resource からの構成
C. api.name = 'azure-active-directory-authorization-policy' かつ json.rule =defaultUserRolePermissions.allowedToCreateSecurityGroups が false で、defaultUserRolePermissions.allowedToCreateApps が true であるネットワークからの構成
D. cloud.resource からの構成。api.name = 'azure-active-directory-authorization-policy' かつ json.rule =defaultUserRolePermissions.allowedToCreateSecurityGroups が true、defaultUserRolePermissions.allowedToCreateApps が true
Answer: D (メーッセージを残す**)**
Azure AD 内でセキュリティ グループを作成し、アプリケーションを作成するための十分なアクセス許可を持つユーザーを表示するための正しい RQL クエリは、オプション D です。このクエリは、ユーザーに関連する承認ポリシー設定を確認することによって、Azure Active Directory (Azure AD) 内のポリシーを評価するように特に設計されています。デフォルトのロール権限。このクエリは、azure-active-directory-authorization-policy API をターゲットにして構成 (cloud.resource からの構成) を取得し、ユーザーにセキュリティ グループの作成を許可するかどうかを指示する JSON ルールに基づいてそれらの構成をフィルター処理します (defaultUserRolePermissions.allowedToCreateSecurityGroups が true です)。) とアプリケーション (defaultUserRolePermissions.allowedToCreateApps が true)。このクエリは、両方の条件が満たされていることを確認することで包括的なチェックを行います。これは、ユーザーが Azure AD 内でセキュリティ グループとアプリケーションを作成する機能を組み合わせて持つために必要です。
Prisma Cloud およびクラウド セキュリティ原則のコンテキストでは、RQL (リソース クエリ言語) は、セキュリティ ポリシーへの準拠を確保するために、クラウド環境内のリソースの構成状態をクエリするために利用されます。オプション D の RQL 構文は、 Prisma Cloud の可視性と制御資格ガイド」や クラウド セキュリティ体制管理ツールのガイド。」これらの文書では、安全で準拠したクラウド環境を維持するために、クラウド リソース構成の継続的な監視と検証の重要性を強調しています。これは、オプション D のような対象を絞った RQL クエリによって効果的に達成されます。
参照：
Prisma Cloud Visibility and Control Qualification Guide」では、クラウド環境における可視性とコンプライアンスの重要性について説明しています。これは、リソース構成をクエリするための RQL の使用に直接当てはまります。
クラウド セキュリティ体制管理ツールのガイド」では、クラウド環境全体にわたる包括的な可視性とガバナンスの必要性を強調し、Azure AD でユーザーのアクセス許可を評価するために使用される特定の RQL クエリの背後にある理論的根拠をさらにサポートしています。

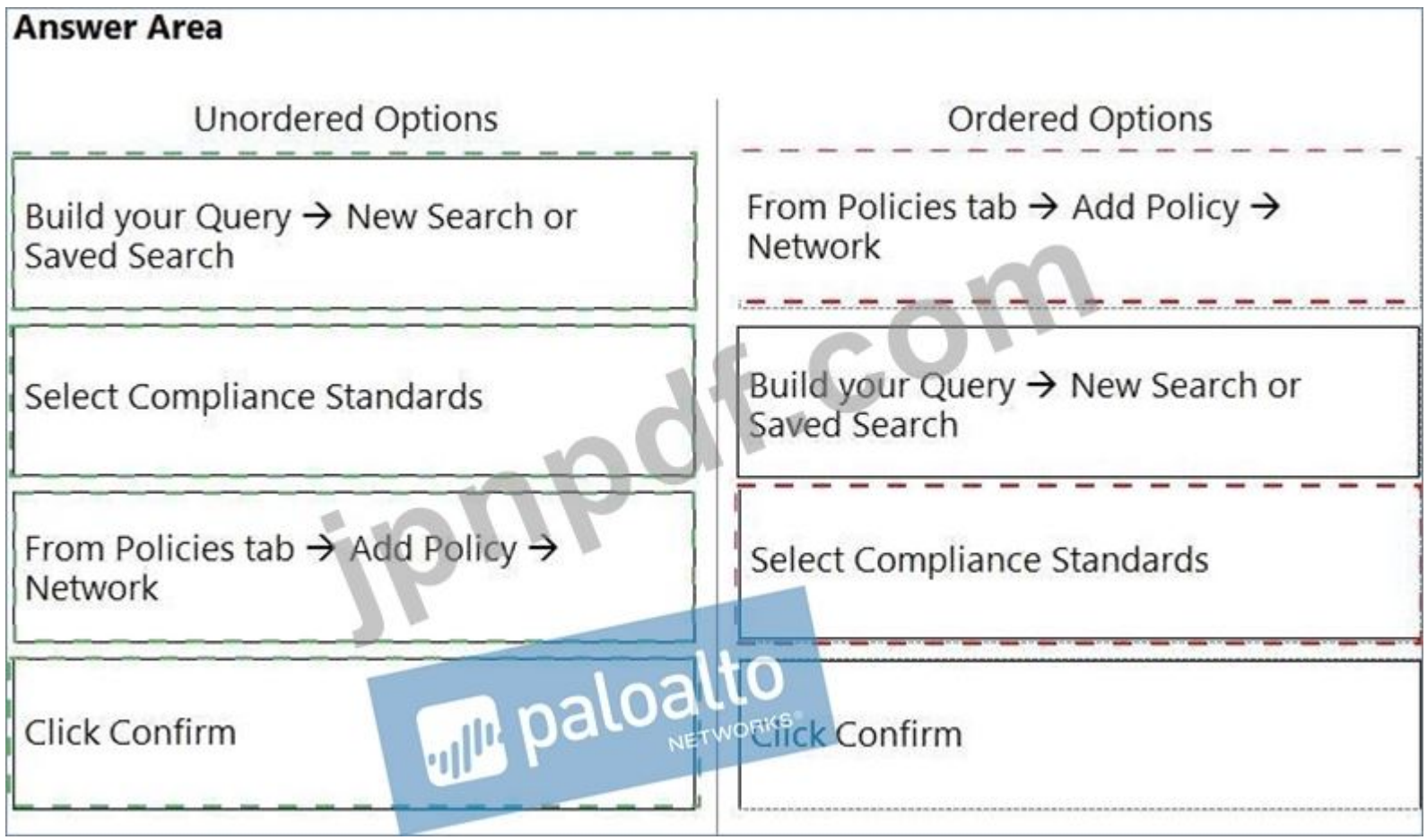
最新問題**: 90**

アマゾン ウェブ サービス (AWS) クラウド内の自動化された方法を使用して、ID およびアクセス管理 (IAM) モジュールで修復を使用するプロセスを合理化するために必要な 2 つのアクションはどれですか? (2つお選びください。)
A. boto3 をインストールし、ライブラリをリクエストします。
B. IAM Azure 修復スクリプトを構成します。
C. Azure Service Bus と統合します。
D. IAM AWS 修復スクリプトを構成します。
Answer: A,D (メーッセージを残す**)**
アマゾン ウェブ サービス (AWS) クラウド内、特に Identity and Access Management (IAM) モジュール内で自動修復方法を利用するには、boto3 ライブラリとリクエスト ライブラリのインストールと IAM AWS 修復スクリプトの構成という 2 つの重要なアクションが必要です。
boto3 ライブラリは AWS の Python 用 SDK で、Python 開発者は Amazon S3 や Amazon EC2 などのサービスを利用するソフトウェアを作成できます。リクエスト ライブラリは、人間向けに設計された Python HTTP ライブラリであり、HTTP サービスとの簡単な対話を可能にします。これらのライブラリは、IAM 内での修復タスクの自動化など、AWS サービスのスクリプト作成の基礎となります。
IAM AWS 修復スクリプトの構成は、2 番目の重要な手順です。このスクリプトは、過剰なアクセス許可、未使用の IAM ロール、不適切に設定されたポリシーなど、特定されたセキュリティ問題の修復を自動化するために AWS IAM と対話するように調整されています。このスクリプトは boto3 ライブラリを使用して AWS サービスと通信し、IAM 設定をセキュリティのベストプラクティスに合わせるために必要な変更を適用します。
これらのアクションは、自動化を活用して AWS 内の IAM セキュリティを強化し、IAM 設定が最小権限の原則やその他のセキュリティのベストプラクティスに確実に準拠するようにするために不可欠です。このアプローチは、クラウド セキュリティに関する Prisma Cloud の機能と推奨事項と一致しており、 Prisma Cloud の可視性と制御の資格ガイド」や クラウド セキュリティ体制管理ツールのガイド」などのリソースで説明されているように、堅牢なセキュリティ体制を維持するための自動化の重要性を強調しています。。」参照：
Prisma Cloud Visibility and Control Qualification Guide」では、クラウド環境内での自動セキュリティ制御と修復の重要性を強調し、AWS での IAM 修復のためのスクリプトとライブラリの使用をサポートしています。
クラウド セキュリティ体制管理ツールのガイド」では、クラウド セキュリティにおける自動化、特にコンプライアンスを確保しリスクを最小限に抑えるための IAM 構成の管理と修正の重要性を強調しています。

最新問題**: 91**
カスタム ネットワーク ポリシーを作成する手順はどのような順序ですか?
(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)

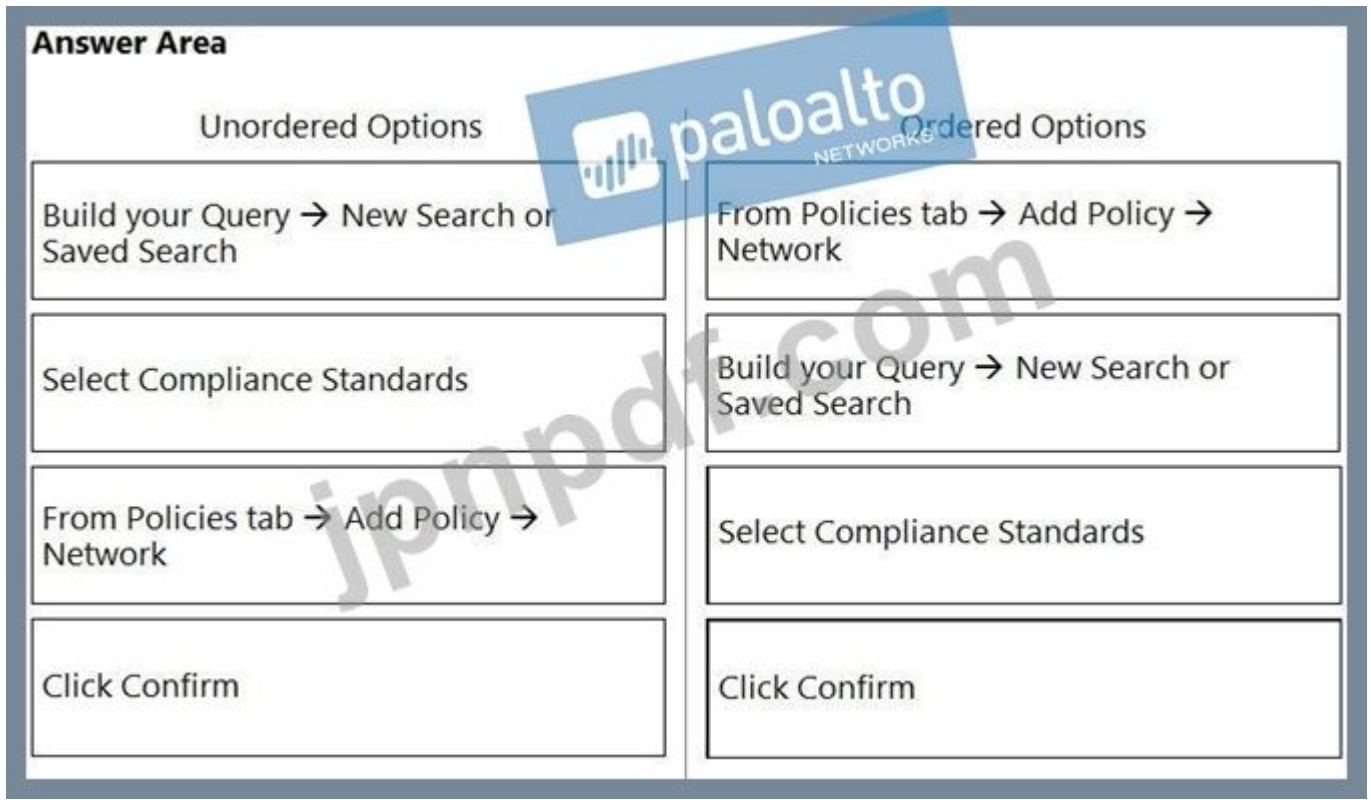
Answer Area

Answer:



説明

自動的に生成された表の説明を含む画像



最新問題: **92**
ビルドおよび実行ポリシーについて正しいのはどれですか?
A. ポリシーの主なタイプは 4 つあり、監査イベントです。建てる。ネットワークと実行。
B. 実行ポリシーは、環境内のネットワーク アクティビティを監視し、実行時の潜在的な問題をチェックします。
C. ビルド ポリシーを使用すると、IaC テンプレートのセキュリティ構成ミスをチェックできます。
D. すべてのタイプのポリシーで、自動修復がデフォルトで有効になっています。
Answer: B (メーッセージを残す)

最新問題: **93**
API を使用して取得できるポリシーの 2 つの属性はどれですか? (2つお選びください。)
A. ポリシーラベル
B. ポリシー署名
C. ポリシーモード
D. ポリシー違反
Answer: (解答を表示する)

最新問題: **94**
ネットワーク上のリソースの 1 つが、デフォルト構成ポリシーのアラートをトリガーしました。
次のリソース JSON スニペットがあるとします。

どの RQL が脆弱性を検出しましたか?

A.
```
config from cloud.resource where api.name = 'aws-ecs-service' AND json.rule = launchType equals EC2 as X; config
from cloud.resource where api.name = 'aws-ecs-cluster' AND json.rule = status equals ACTIVE and
registeredContainerInstancesCount equals 0 as Y; filter '$.X.ckusterArn equals $.Y.clusterArn'; show Y;
```

B.
```
config from cloud.resource where cloud.type = 'aws' and api.name = 'aws-iam-get-credential-report' AND json.rule
= '(access_key_1_active is true and access_key_1_last_rotated != N/A and
_DateTime.ageInDays(access_key_1_last_rotated) > 90) or (access_key_2_active is true and
access_key_2_last_rotated != N/A and _DateTime.ageInDays(access_key_2_last_rotated) > 90)'
```

C.
```
config from cloud.resource where cloud.type = 'aws' AND api.name ='aws-ec2-describe-images' AND json.rule =
image.platform contains windows and image.imageId contains ami-1e542176
```

D.
```
config from cloud.resource where cloud.type = 'aws' AND api.name ='aws-ec2-describe-secutity-groups' AND
json.rule = isShared is false and (ipPermissions[?any((ipProtocol equals tcp or ipProtocol equals icmp or
ipProtocol equals icmpv6 or ipProtocol equals udp) and (ipRanges[*] contains 0.0.0.0/0 or ipv6Ranges[*].cidrIpv6
```

Answer: B (メーッセージを残す)
脆弱性を検出した正しい RQL (リソース クエリ言語) は次のとおりです。
Cloud.resource からの設定、ここで、cloud.type = 'aws' および api.name = 'aws-iam-get-credential-report' AND json.rule = '(access_key_1_active が true および access_key_1_last_rotated != N/A および DateTime.ageInDays (access_key_1_last_rotated) > 90) または (access_key_2_active is true and access_key_2_last_rotated != N/A and _DateTime.ageInDays (access_key_2_last_rotated) > 90)' この RQL は、AWS IAM ユーザーのアクセス キーの年齢をチェックして、アクセス キーがローテーションされていることを確認するように設計されています。推奨期間内 (通常は 90 日)。この期間内にアクセス キーがローテーションされなかった場合、古いキーが危険にさらされる可能性があるため、セキュリティ リスクまたは脆弱性があるとみなされます。アクセス キーのローテーションを強制することで、不正アクセスのリスクを最小限に抑えます。
このタイプのポリシー チェックの参考資料は、キー侵害の潜在的な影響を最小限に抑えるためにアクセス キーの定期的なローテーションを推奨するクラウド セキュリティのベスト プラクティスに見られます。Prisma Cloud などの CSPM ツールには、これらのベスト プラクティスへの準拠を自動化するためのチェックが含まれています。

最新問題: **95**
管理者は、1 つ以上の RDS インスタンスが侵害されたこと、および SOC が運用 RDS インスタンスがパブリックにアクセスできないようにする必要があることを SOC に通知します。

セキュリティのベスト プラクティスに従うために、SOC はどのアクションを実行する必要がありますか?
A. AWS RDS データベース インスタンスはパブリックにアクセス可能」ポリシーを有効にし、アラートごとに、それが本番インスタンスであることを確認して、手動で修復します。
B. AWS S3 バケットはパブリックにアクセス可能」ポリシーを有効にし、各アラートを手動で修正します。
C. AWS S3 バケットはパブリックにアクセス可能」ポリシーを有効にし、自動修復アラート ルールにポリシーを追加します。
D. AWS RDS データベース インスタンスはパブリックにアクセス可能です」ポリシーを有効にし、自動修復アラート ルールにポリシーを追加します。
Answer: D (メーッセージを残す**)**

最新問題**: 96**
セキュリティ監査人は、ホスト上で所定のコンプライアンス チェックが実行されていることを確認する必要があります。有効なホスト コンプライアンス ポリシーはどのオプションですか?
A. 関数が過度に寛容でないことを確認します。
B. 準拠した Docker デーモン構成を確認します
C. イメージが root 以外のユーザーで作成されていることを確認します
D. ホスト デバイスがコンテナに直接公開されていないことを確認します。
Answer: (解答を表示する**)**

最新問題**: 97**
Prisma Cloud 管理者は、API 経由でレポートを取得する任務を負っています。Prisma Cloud テナントは app2.prismacloud.io にあります。正しい API エンドポイントは何ですか?
A. https://api.prismacloud.io
B. https://api2.eu.prismacloud.io
C. httsp://api.prismacloud.cn
D. https://api2.prismacloud.io
Answer: D (メーッセージを残す**)**
https://prisma.pan.dev/api/cloud/api-urls/
app2.prismacloud.io にあるテナントの Prisma Cloud API にアクセスする場合、使用する正しい API エンドポイントは https://api2.prismacloud.io になります。このエンドポイントは、app2.prismacloud.io でホストされる Prisma Cloud サービス インスタンスに対応し、API リクエストが処理のためにサービスの適切なインスタンスに確実に送信されるようにします。
URL での api2 の使用は、これが Prisma Cloud サービスの 2 番目のインスタンス、または地理的または機能的な別のパーティションであることを示しており、負荷分散、冗長性、またはさまざまなユーザー セットにサービスを提供するために使用される可能性があります。API 通信と認証を確実に成功させるには、Prisma Cloud コンソール URL に対応する正しいエンドポイントを使用することが重要です。

最新問題**: 98**
お客様は、50 台の Defender が接続されている開発環境を持っています。開発環境内の 30 台のスタンドアロン Defender をアップグレードするためのメンテナンス期間が月曜日に設定されていますが、日曜日まで残りの 20 台のスタンドアロン Defender をアップグレードできるメンテナンス期間はありません。

この状況を管理するには、どの推奨アクションが最適ですか?
A. パロアルトネットワークスでサポートケースを開き、自動アップグレードを手配します。
B. 開発環境内のすべてのスタンドアロン Defender をアップグレードするのに適したメンテナンス ウィンドウを見つけます。
C. メンテナンス期間中にアップグレードする必要がある Defender に対応する行にある個別の [Actions] > [Upgrade] ボタンをクリックして、Defender のサブセットをアップグレードします。
D. [管理] > [ディフェンダー] > [管理] に移動し、[ディフェンダー] をクリックし、スケジューラを使用してメンテナンス期間中に自動的にアップグレードするディフェンダーを選択します。
Answer: B (メーッセージを残す**)**

最新問題**: 99**
カスタム ポリシー シーケンスには CLI 修復コマンドをいくつ追加できますか?
A. 5
B. 2
C. 4
D. 1
Answer: A (メーッセージを残す**)**

最新問題**: 100**
顧客は PCI 要件に関心があり、環境内で特権コンテナが起動できないようにする必要があります。
特権コンテナを使用しない」にはどのアクションを設定する必要がありますか?
A. 防止する
B. アラート
C. ブロック
D. 失敗
Answer: C (メーッセージを残す**)**
説明
Block-Defender は、ポリシーに違反するプロセスが実行しようとすると、コンテナ全体を停止します。
https://docs.prismacloudcompute.com/docs/enterprise_edition/runtime_defense/runtime_defense_containers.htm

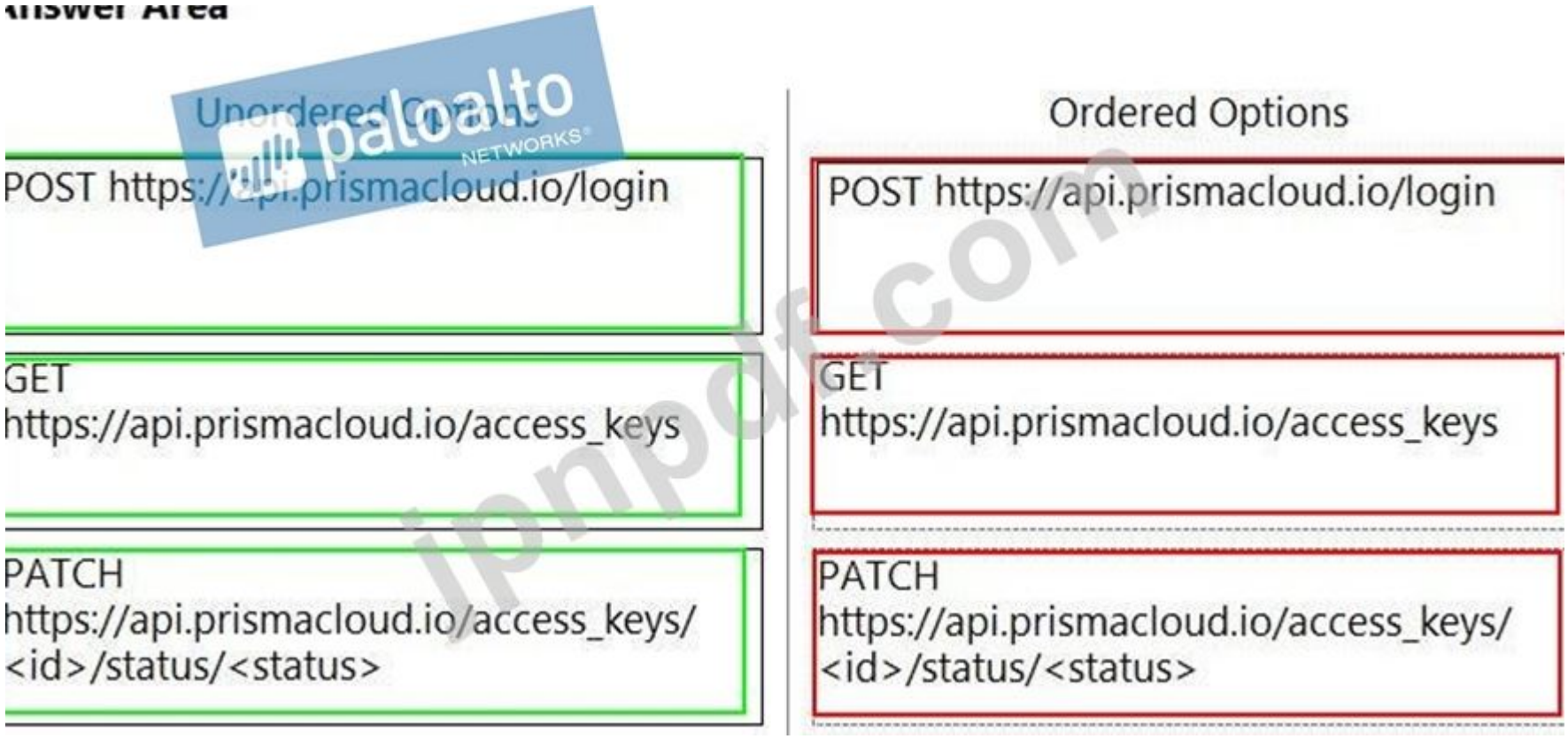
最新問題**: 101**
管理者は、root アカウントによって実行されるアクティビティを検出して警告する必要があります。
どのポリシー タイプを使用する必要がありますか?
A. 構成実行
B. 構成ビルド
C. ネットワーク
D. 監査イベント
Answer: D (メーッセージを残す**)**
root アカウントによって実行されるアクティビティを検出して警告するには、監査イベント ポリシーを使用する必要があります。監査イベント ポリシーは、セキュリティの脅威に関連する可能性のある不審なアクティビティやイベントを検出するために使用できるポリ

シーの一種です。このタイプのポリシーを使用すると、管理者は root アカウントによって実行されるアクティビティを監視し、警告することができます。
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/prisma-cloud-threat-detection
root アカウントによって実行されるアクティビティを検出して警告するために使用する正しいポリシー タイプは、 監査イベント」ポリシーです。監査イベント ポリシーは、一連の時系列イベントを発生順に監視および記録するように設計されており、通常はユーザーのアクティビティやシステム内の変更を追跡するために使用されます。root アカウントが何らかのアクションを実行すると、監査イベント ポリシーによってこれらのイベントがログに記録され、管理者が確認して、不審なアクティビティや不正なアクティビティが検出された場合にアラートを設定できるようになります。このタイプのポリシーは、root 権限で実行されるすべてのアクションが正当で承認されていることを確認するのに役立つため、セキュリティとコンプライアンスの目的で非常に重要です。
これについては、CSPM (Cloud Security Posture Management) ソリューションを提供するほとんどのクラウド セキュリティ プラットフォームで参照できます。たとえば、Palo Alto Networks の Prisma Cloud では、監査イベントはアクティビティ監視機能の一部であり、ユーザーのアクティビティとシステムの変更を追跡して、不審なアクションや不正なアクションの調査を容易にします。

最新問題**: 102**
SSN やクレジット カード番号に関連する重要な機密データが調査中に [ダッシュボード] > [データ ビュー] で表示されないようにするための正しい方法は何ですか?
A. [設定] > [データ] > [データ パターン] に移動し、SSN パターンを検索して編集し、近接キーワードを変更します。
B. [ポリシー] > [データ] > [クローン] > [公開された財務情報を含むオブジェクトの変更] に移動し、ファイル公開を非公開に変更します。
C. [設定] > [データ] > [スニペット マスキング] に移動し、[フル マスク] を選択します。
D. [設定] > [クラウド アカウント] > [クラウド アカウントの編集] > [アカウント グループの割り当て] に移動し、制限された権限を持つグループを選択します。
Answer: B (メーッセージを残す**)**

最新問題**: 103**
管理者は、30 日間使用されなかったアクセス キーを自動的に非アクティブ化するスクリプトを作成する必要があります。
このタスクを実行するには、どの順序で API 呼び出しを使用する必要がありますか? (ステップを最初のステップから最後のステップまで正しい順序にドラッグします。) 選択して配置します。

Answer:



最新問題: 104

nginx:latest イメージの脆弱性とコンプライアンス問題をスキャンするには、Prisma CloudTwistcli ツールでどのコマンドを使用する必要がありますか?

A.
```
$ twistcli images build
--console-address <COMPUTE_CONSOLE>
--user <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--details
```

B.
```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
--username <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--details
nginx:latest
```

C.
```
$ twistcli images scan
--address <COMPUTE_CONSOLE>
--user <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--details
nginx:latest
```

D.
```
$ twistcli images scan
--console-address <COMPUTE_CONSOLE>
--user <COMPUTE_CONSOLE_USER>
--password <COMPUTE_CONSOLE_PASSWD>
--output-file scan-results.json
nginx:latest
```

Answer: (解答を表示する**)**

Prisma Cloud のTwistcli ツールを使用して nginx:latest イメージの脆弱性とコンプライアンス問題をスキャンするための正しいコマンドは、オプション D に示されています。このコマンドは、コンソール アドレス、ユーザー名、およびパスワードの指定されたパラメーターを使用して、twistcli イメージ スキャンを使用し、結果は scan-results.json という名前のファイルに保存されます。これにより、スキャン結果を構造化された形式で保存して確認できるため、脆弱性やコンプライアンス問題のさらなる分析と追跡に役立ちます。

最新問題**: 105**

IntelliJ アプリケーションで Prisma Cloud プラグインを認証するときに必須の 3 つのフィールドはどれですか?
（3つお選びください。）

A. アクセスキー
B. 秘密鍵
C. アセット名
D. タグ
E. Prisma Cloud API URL

Answer: (解答を表示する**)**

最新問題**: 106**

Defender タイプ Container Defender - Linux に当てはまる 2 つのステートメントはどれですか?

A. ユーザー空間のランタイム保護として実装されます。
B. サービスとしてデプロイされます。
C. コンテナとしてデプロイされます。
D. ファイルシステムのランタイム防御ができません。
Answer: A,C (メーッセージを残す)
Prisma Cloud の Defender タイプ 「Container Defender - Linux」は、通常、コンテナとしてデプロイされます。この展開方法により、Defender をコンテナ化された環境にシームレスに統合し、ランタイム保護とコンテナ アクティビティの監視を提供できます。Container Defender はコンテナとして実行することで、Kubernetes などのコンテナ オーケストレーション プラットフォームのネイティブ機能を活用して、コンテナ化された環境内で脅威の検出、脆弱性管理、コンプライアンスの強制などのセキュリティ機能を提供できます。このアプローチにより、セキュリティ保護がコンテナ化されたアプリケーションの動的かつスケーラブルな性質と密接に連携することが保証されます。

最新問題: **107**
複数のアマゾン ウェブ サービス (AWS) クラウド アカウントが使用されている場合に、Okta を Prisma Cloud と統合するための 2 つの重要な要件は何ですか? (2つお選びください。)
A. スーパー管理者の権限
B. IAM セキュリティ モジュールの有効なサブスクリプション
C. プライマリ AWS アカウントの Okta API トークン
D. Okta アプリの複数のインスタンス
Answer: (解答を表示する)
複数のアマゾン ウェブ サービス (AWS) クラウド アカウントを管理するために Okta を Prisma Cloud と統合する場合、次の 2 つの重要な要件があります。
スーパー管理者権限: このレベルの権限は、Okta を Prisma Cloud と統合する個人が、プラットフォームと AWS アカウント全体で必要な構成と統合を行うための十分な権限を持っていることを確認するために必要です。スーパー管理者権限により、インテグレーターは必要なすべての設定にアクセスし、ロールを管理し、制限なく統合を実行できるようになります。
Okta アプリの複数のインスタンス: AWS の性質とアカウントの管理方法により、各 AWS クラウド アカウントは Okta 内で別個のエンティティとして扱われる必要があります。これには、Okta アプリケーションの複数のインスタンスを、統合する AWS クラウド アカウントごとに 1 つずつセットアップする必要があります。このアプローチにより、アカウントごとのアクセスとアクセス許可の正確な制御と管理が可能になり、最小限の権限のベストプラクティスに沿って、セキュリティ構成が各 AWS アカウントの特定のニーズに合わせて調整されるようになります。
これらの要件は、シームレスで安全な統合プロセスを確保し、Okta を通じて複数の AWS アカウントにわたる一元的な ID 管理を可能にし、マルチクラウド環境全体のセキュリティ体制を強化するために重要です。

最新問題: **108**
Web-Application and API Security（WAAS）は、どの 2 つのプロトコルに対して保護を提供しますか? (2つお選びください。)
A. HTTP
B. SSH
C. AJP 経由の Tomcat Web コネクタ
D. TLS
Answer: A,D (メーッセージを残す)
Web-Application and API Security（WAAS）は、Web アプリケーションと API をさまざまな脅威や脆弱性から保護することに重点を置いた Prisma Cloud 内の機能です。保護を提供する主なプロトコルは、HTTP (ハイパーテキスト転送プロトコル) と TLS (トランスポート層セキュリティ) です。HTTP は World Wide Web のデータ通信の基礎であり、TLS はコンピュータ ネットワーク上で通信セキュリティを提供するために設計された暗号化プロトコルです。SSH（Secure Shell）は安全なリモート ログインおよびその他の安全なネットワーク サービス用のプロトコルであり、AJP（Apache JServ Protocol）経由の Tomcat Web Connector は Tomcat サーバ通信に使用されますが、これらは WAAS 保護の主な焦点ではありません。

最新問題: **109**
顧客は自動修復を有効にしたいと考えています。
どのポリシー タイプに修復用の CLI コマンドが組み込まれていますか?
A. 異常
B. 監査イベント
C. ネットワーク
D. 構成
Answer: D (メーッセージを残す)
参照：
Prisma Cloud では、Config ポリシーに自動修復用の CLI コマンドが組み込まれています。これらのポリシーは、クラウド環境内の構成ミスを特定するのに役立ち、手動介入なしで修復コマンドを自動的に実行して構成を修正できます。この機能は、クラウド リソースがベスト プラクティスとコンプライアンス標準に従って構成されていることを確認することで、クラウド セキュリティ体制を維持するための Prisma Cloud の包括的なアプローチの一部です。

最新問題: **110**
顧客データベース内の疑わしい IP からの接続に関する情報を提供するポリシー タイプはどれですか?
A. 異常
B. 脅威の検出
C. ネットワーク
D. オートフォーカス
Answer: C (メーッセージを残す)
顧客データベース内の疑わしい IP からの接続に関する情報を提供するには、ネットワーク ポリシー タイプを使用する必要があります。Prisma Cloud 内のネットワーク ポリシーは、既知の悪意のある IP アドレスまたは不審な IP アドレスからの接続の検出など、ネットワーク トラフィックを監視および制御するように設計されています。この機能は、潜在的な脅威や不正アクセスの試みを特定するために非常に重要であるため、オプション C が正解となります。

最新問題**: 111**
ある組織は、アカウント グループ 臨床試験」の 重大度が高い」アラートについて、Slack 経由ですぐに通知を受け取りたいと考えています。
組織がこの目標を達成するために使用できる手順を示すオプションはどれですか?
A. 1. Slack 統合を構成する
2. アラート ルールを作成する
3. [ポリシーの選択] タブで重大度をフィルターし、[高] を選択します。
4. [アラート通知の設定] タブで、[Slack] を選択し、チャネルを設定します。
5. 頻度を 発生次第」に設定します。
B. 1. [ポリシーの選択] タブで重大度をフィルターし、[高] を選択します。
2. [アラート通知の設定] タブで、[Slack] を選択し、チャネルを設定します。
3. 頻度を 発生次第」に設定します。
4. Slack 統合の構成
5. アラート ルールを作成する
C. 1. Slack 統合を構成する
2. アラート ルールを作成し、アカウント グループとして 臨床試験」を選択します。
3. [ポリシーの選択] タブで重大度をフィルターし、[高] を選択します。
4. [アラート通知の設定] タブで、[Slack] を選択し、チャネルを設定します。
5. 頻度を 発生次第」に設定します。
D. 1. アラート ルールを作成し、アカウント グループとして 臨床試験」を選択します。
2. [ポリシーの選択] タブで重大度をフィルタし、[高] を選択します。
3. [アラート通知の設定] タブで、[Slack] を選択し、チャネルを設定します。
4. 頻度を 発生次第」に設定します。
5. Slack 統合をセットアップして構成を完了します
Answer: D (メーッセージを残す)

最新問題**: 112**
Web Application and API Security (WAAS) ボット保護の一部である 2 つのボット タイプはどれですか? (2つお選びください。)
A. ユーザー定義のボット
B. チャットボット
C. 不明なボット
D. 顧客ボット
Answer: C,D (メーッセージを残す)

最新問題**: 113**
お客様は、構成ミスから環境を強化したいと考えています。
ホストに対する Prisma Cloud Compute Compliance の適用では、どの 3 つのオプションがカバーされますか? 3つお選びください。)
A. Docker デーモンの構成
B. ホスト構成

C. ホスト クラウド プロバイダーのタグ
D. Defender エージェントのないホスト
E. Docker デーモン構成ファイル
Answer: A,B,C (メーッセージを残す)

最新問題**: 114**
Defender のデバッグ ログはどこで表示できますか? (2つお選びください。)
A. /var/lib/twistlock/defender.log
B. コンソールから、 管理」> ディフェンダー」> 管理」> ディフェンダー」。デプロイされたディフェンダーのリストからディフェンダーを選択し、[アクション] > [ログ] をクリックします。
C. コンソールから、 管理」 > ディフェンダー」 > デプロイ」 > ディフェンダー」の順に選択します。デプロイされたディフェンダーのリストからディフェンダーを選択し、[アクション] > [ログ] をクリックします。
D. /var/lib/twistlock/log/defender.log
Answer: B,D (メーッセージを残す)
Prisma Cloud では、Defender のデバッグ ログは、Defender の動作動作のトラブルシューティングと理解に不可欠です。ログには、次の 2 つの主な方法でアクセスできます。
A) 最初の方法 (B) では、Prisma Cloud Console のユーザー インターフェイスを使用します。[管理] > [ディフェンダー] > [管理] > [ディフェンダー] に移動すると、管理者はリストからデプロイされたディフェンダーを選択し、[アクション] > [ログ] をクリックしてそのログにアクセスできます。この方法は、Defender ホストに直接アクセスする必要がなく、コンソールから直接ログを表示する便利な方法を提供します。
D) 2 番目の方法 (D) では、Defender が展開されているホストのファイル システムからログに直接アクセスします。Defender ログの正しいパスは /var/lib/twistlock/log/defender.log です。この方法は、ホストに直接アクセスできる状況で役立ち、生のログ ファイルを調べることでより詳細なトラブルシューティングが可能になります。
オプション A と C は、指定されたパスとナビゲーション手順が Prisma Cloud のロギング システムの構造と機能を正確に反映していないため、不正確です。

最新問題**: 115**
顧客は自動修復を有効にしたいと考えています。
どのポリシー タイプに修復用の CLI コマンドが組み込まれていますか?
A. 構成
B. 異常
C. 監査イベント
D. ネットワーク
Answer: A (メーッセージを残す)

最新問題**: 116**
FP9 インスタンスを終了する権限を持つ Lambda 関数について警告するカスタム ID およびアクセス管理 (1AM) ポリシーの作成に役立つ RQL クエリはどれですか?
A. iam からの構成。dest.cloud.type = 'AWS' AND source.cloud.service.name = 'lambda1 AND source.cloud.resource.type = 'function1 AND dest.cloud.service.name = 'ec2' AND action.name = 'ec2:TerminateInstances'

B. iam からの構成。dest.cloud.type = 'AWS' AND source.cloud.service.name = 'ec2' AND source.cloud.resource.type = 'instance' AND dest.cloud.service。name = 'lamda' AND action.name = 'ec2:TerminateInstances'
C. Cloud.resource からの iam。ここで、dest.cloud.type = 'AWS' AND source.cloud.service.name = 'lambda' AND source.cloud.resource.type = 'function' AND dest.cloud。service.name = 'ec2' AND action.name = 'ec2:TerminateInstances'
D. cloud.resource からの iam。cloud.type が「AWS」であり、cloud.resource.type が「lambda function」であり、cloud.service.name =「ec2」であり、action.name が「ec2:TerminateInstances」である。
Answer: (解答を表示する**)**
EC2 インスタンスを終了する権限を持つ Lambda 関数でアラートを発行するカスタム Identity and Access Management (IAM) ポリシーを作成するには、正しい RQL クエリ構造に、ソース サービス (Lambda)、宛先サービス (EC2)、およびその特定のアクションを指定することが含まれます。関心 ('ec2:TerminateInstances')。クエリでは、Lambda 関数 ('source.cloud.service.name = 'lambda' および 'source.cloud.resource.type = 'function') に、「ec2:TerminateInstances」を実行できる権限が付与されている設定を識別する必要があります。' EC2 インスタンスに対するアクション ('dest.cloud.service.name = 'ec2')。このクエリは、EC2 リソースの可用性に不注意または悪意を持って影響を与える可能性のある過度に許容的な機能に関連する潜在的なリスクを特定し、軽減するのに役立ちます。

最新問題**: 117**
顧客は、環境内のポート スキャン ネットワーク アクティビティについて通知を受け取りたいと考えています。この動作を検出するポリシー タイプはどれですか?
A. 構成
B. ネットワーク
C. 異常
D. ポートスキャン
Answer: C (メッセージを残す**)**

最新問題**: 118**
異常なコンピューティング プロビジョニングを有効にした後に適用できるアクションはどれですか?
A. スパムボットによって引き起こされたアクティビティを検出します。
B. クラウド環境内外のクライアントからの異常なサーバー ポート アクティビティまたは異常なプロトコル アクティビティを検出します。
C. AutoFocus を使用して、コンピューティング インスタンスの不正なネットワークが作成される可能性を検出します。
D. 誤って、またはクリプトジャッキングにより、コンピューティング インスタンスの不正なネットワークが作成される可能性を検出します。
Answer: D (メッセージを残す**)**
Prisma Cloud で異常なコンピューティング プロビジョニングを有効にすると、コンピューティング インスタンスの作成に関連する異常な潜在的に不正なアクティビティを検出できるようになります。この機能は、構成ミスにより偶然、またはクリプトジャッキングなどの目的で悪意を持って、コンピューティング インスタンスの不正なネットワークが確立される可能性があるシナリオを特定するのに特に役立ちます。クリプトジャッキングには、暗号通貨をマイニングするために他人のコンピューティング リソースを不正に使用することが含まれます。異常なコンピューティング プロビジョニングは、コンピューティング リソースのプロビジョニングにおける異常なパターンを強調することで、そのようなアクティビティを特定するのに役立ちます。

最新問題: **119**
管理者には、すべての Console ログと Defender ログを Splunk に取り込む必要があります。
Prisma Cloud Compute でこの要件を満たすのはどのオプションですか?
A. ロギングの API 設定を有効にします。
B. コンソールで CSV エクスポートを有効にします。
C. コンソールで syslog オプションを有効にします。
D. コンソールで Splunk オプションを有効にします。
Answer: D (メーッセージを残す)
Prisma Cloud Compute は、オペレーショナル インテリジェンスおよびセキュリティ情報およびイベント管理 (SIEM) の主要なプラットフォームである Splunk とのネイティブ統合機能を提供します。Prisma Cloud コンソール内で Splunk オプションを有効にすることで、管理者はコンソールと Defender のログを Splunk にシームレスに転送できます。この統合により、Prisma Cloud Compute によって提供される詳細なセキュリティ データを活用して、Splunk 内での高度な分析、リアルタイム監視、包括的なインシデント対応ワークフローが容易になります。

最新問題: **120**
組織のユーザーは、前日にログインした後、Prisma Cloud Console にログインできません。
コンソールのどの領域がこの問題に関する意見を提供しますか?
A. アクセス制御
B. 監査ログ
C. ユーザーとグループ
D. SSO
Answer: B (メーッセージを残す)

最新問題: **121**
Prisma Cloud で SSO を設定するときに、IdP 側で入力する必要があるのは次のうちどれですか?
(2つお選びください。)
A. SSO 証明書
B. アサーション コンシューマ サービス (ACS) URL
C. ユーザー名
D. SP (サービスプロバイダー) エンティティ ID
Answer: A,D (メーッセージを残す)

最新問題: **122**

組織は、アカウント グループの 「70 位以上」アラートに対して直ちに通知を受け取りたいと考えています。
Slack 経由の 「臨床試験」 この目標を達成するために組織が使用できる手順を示すオプションはどれですか?
A. 1. アラート ルールを作成し、アカウント グループとして 「臨床試験」を選択します。
2. [ポリシーの選択] タブで 70 をフィルターし、[高] を選択します。
3. [アラート通知の設定] タブで [Slack] を選択し、チャネルを設定します。
4. 頻度を 「発生次第」に設定します。
5. Slack 統合をセットアップして構成を完了します
B. 1 Slack 統合を構成する
2. アラート ルールを作成する
3. [ポリシーの選択] タブで、70 をフィルターし、[高] を選択します。
4. [アラート通知の設定] タブで、[Slack] を選択し、チャネルを設定します。
5. 頻度を 「発生次第」に設定します。
C. 1. Slack 統合を構成する
2 アラート ルールを作成し、アカウント グループとして 「臨床試験」を選択します
3. [ポリシーの選択] タブで 70 をフィルターし、[高] を選択します。
4. [アラート通知の設定] タブで [Slack] を選択し、チャネルを設定します。
5. 頻度を 「発生次第」に設定します。
D. 1. [ポリシーの選択] タブで 70 をフィルターし、[高] を選択します。
2. [アラート通知の設定] タブで [Slack] を選択し、
3. 頻度を 「発生次第」に設定します。
4. Slack 統合の構成
5. アラート ルールを作成する
Answer: C (メーッセージを残す)

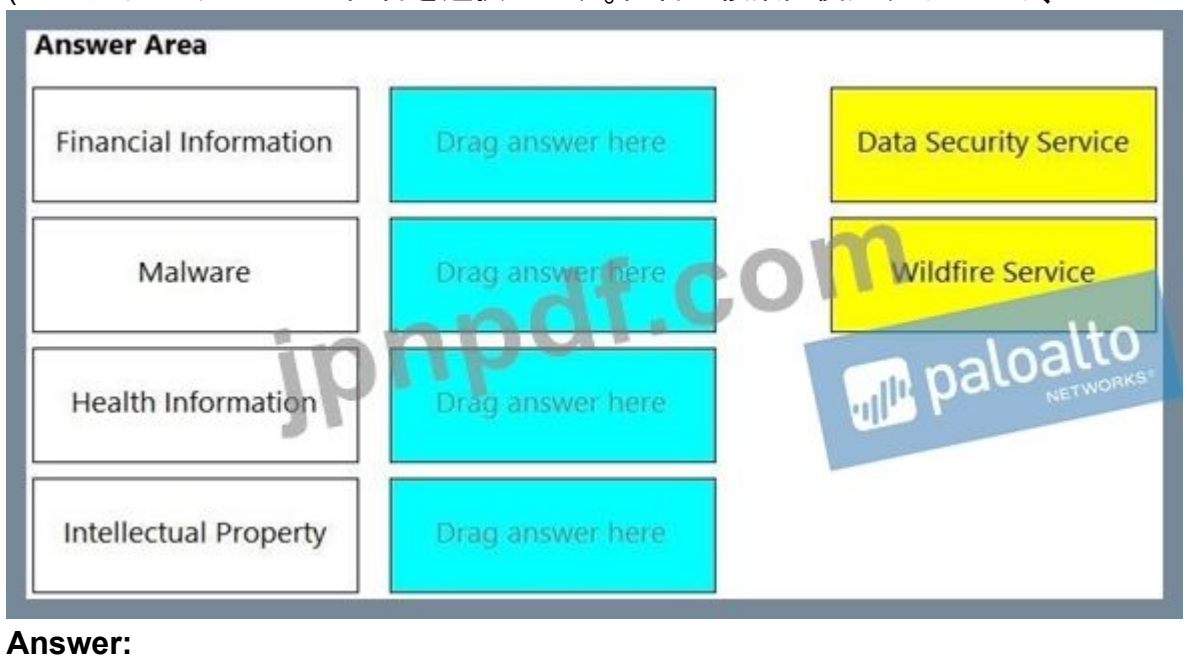
最新問題**: 123**
エアギャップ環境で実行する必要がある場合、どの製品をインストールする必要がありますか?
A. Prisma Cloud Jenkins プラグイン
B. Prisma Cloud Compute Edition
C. セルフホスト型プラグインを備えた Prisma Cloud
D. Prisma Cloud エンタープライズ エディション
Answer: (解答を表示する)
参照：
Prisma Cloud Compute Edition は、インターネットに直接アクセスできないエアギャップ環境に適した製品です。このエディションは隔離された環境にインストールして運用でき、外部接続を必要とせずにクラウド セキュリティ機能を提供します。

最新問題**: 124**
管理者は Prisma Cloud Enterprise にアクセスできます。
単一コンテナー Defender を EC2 ノードにデプロイする手順は何ですか?
A. コンソールでクラウド認証情報を構成し、クラウド検出による ec2 ノードの自動保護を許可します。

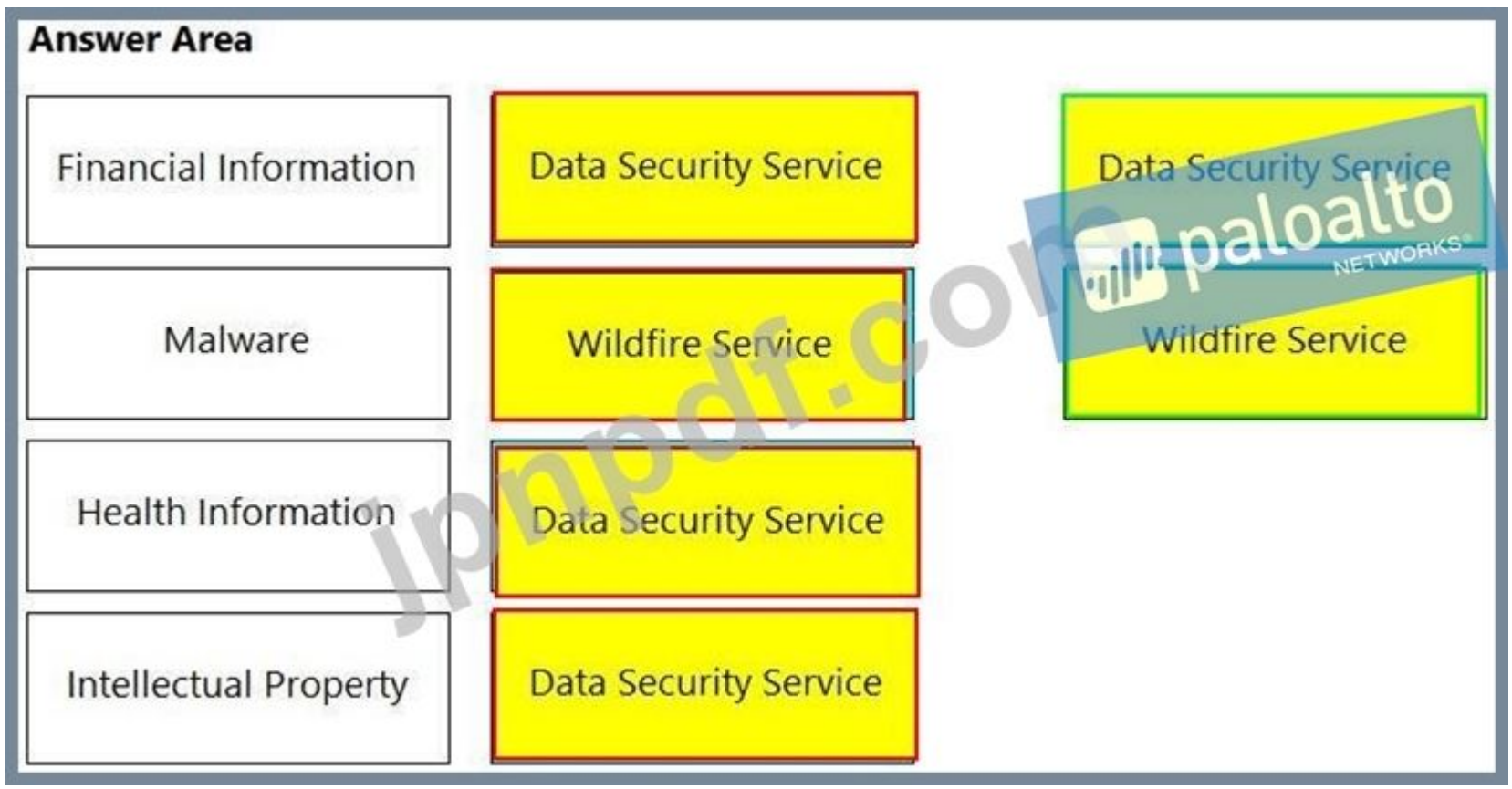
B. curl | を実行します。ec2 ノード上の bash スクリプト。
C. DaemonSet ファイルを生成し、DaemonSet をツイストロック名前空間に適用します。
D. Defender イメージを ec2 ノードにプルし、curl | をコピーして実行します。bash スクリプトを作成し、Defender を起動して、実行されていることを確認します。
Answer: C (メーッセージを残す)

最新問題**: 125**
どのコンテナ イメージ スキャンが正しく構築されていますか?
A. Twistcli イメージ スキャン --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/ la test
B. Twistcli 画像スキャン --address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest
C. Twistcli イメージ スキャン --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest
D. Twistcli イメージ スキャン --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/ 最新 --details
Answer: B (メーッセージを残す)
Prisma Cloud の TwistCLI ツールを使用してコンテナ イメージをスキャンするための正しい構成は、オプション B です。このコマンドは、Prisma Cloud コンソールのアドレスと、そのタグを含むスキャン対象のイメージを指定します。TwistCLI ツールは、セキュリティを CI/CD パイプラインに統合する Prisma Cloud の機能の一部であり、ビルド プロセスの一部としてイメージの脆弱性をスキャンできるため、安全なイメージのみがデプロイされるようになります。

最新問題**: 126**
左側の各露出タイプを評価するサービスを右側に一致させます。
(プルダウン リストから回答を選択します。回答は複数回使用することも、まったく使用しないこともできます。)



Answer:



参照：

https://www.paloaltonetworks.com/prisma/cloud/cloud-data-security

最新問題**: 127**

Prisma Cloud Compute Edition のコンソール イメージの取得について正しいのはどれですか?

A. 基本認証を使用して Prisma Cloud Console イメージを取得するには:

1. registry.paloaltonetworks.com にアクセスし、「docker login」を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。

B. 基本認証を使用して Prisma Cloud Console イメージを取得するには:

1. registry.twistlock.com にアクセスし、「docker login」を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。

C. URL 認証を使用して Prisma Cloud Console イメージを取得するには:

1. registry-url-auth.twistlock.com にアクセスし、ユーザー証明書を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。

D. URL 認証を使用して Prisma Cloud Console イメージを取得するには:

1. registry-auth.twistlock.com にアクセスし、ユーザー証明書を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。

Answer: A (メーッセージを残す**)**

Prisma Cloud Console イメージを取得するには、Palo Alto Networks が提供する特定のレジストリにアクセスし、「docker login」による基本認証を使用して認証する必要があります。認証されると、ユーザーは「docker pull」コマンドを使用して Prisma Cloud コンソール イメージをプルできます。このプロセスは、Prisma Cloud コンソールを環境に展開するための初期セットアップの一部であり、ユーザーは Prisma Cloud の中央管理インターフェイスとして機能するコンソールを実行するために必要なイメージを取得できるようになります。

特定のレジストリ URL や認証方法などの詳細な手順は通常、Prisma Cloud ドキュメントに記載されており、ユーザーがコンソール イメージを正常に取得して展開するために必要な情報を確実に入手できるようにします。

最新問題: **128**
この情報を考慮すると、次のようになります。
コンソールは https://prisma-console.mydomain.local にあります。ユーザー名は:cluster パスワードは:password123 スキャンするイメージは:myimage:latest コンテナーの脆弱性をスキャンし、それぞれの脆弱性の詳細は?
A. Twistcli イメージ スキャン --console-address https://prisma-console.mydomain.local -u クラスター -p パスワード 123 -- 詳細 myimage:latest
B. Twistcli イメージ スキャン --address https://prisma-console.mydomain.local -u クラスター -p パスワード 123 --details myimage:latest
C. Twistcli イメージ スキャン --address prisma-console.mydomain.local -u クラスター -p パスワード 123 --vulnerability- 詳細 myimage:latest
D. Twistcli イメージ スキャン --console-address prisma-console.mydomain.local -u クラスター -p パスワード 123 -- 脆弱性の詳細 myimage:latest
Answer: (解答を表示する**)**

最新問題: **129**
セキュリティ チームには、環境の脆弱性を確実にスキャンするという要件があります。脆弱性ポリシーを構成するための 3 つのオプションは何ですか? 3つお選びください。)
A. パッケージ タイプに基づく個々のアクション
B. ブロックされたリクエストの出力詳細度
C. ベンダー修正が利用可能な場合にのみポリシーを適用します
D. 各重大度レベルの個別の猶予期間
E. ブロックされたリクエストのメッセージをカスタマイズします
Answer: A,C,D (メーッセージを残す**)**
Prisma Cloud 内で脆弱性ポリシーを構成するには、脆弱性管理とポリシー適用のさまざまな側面に対応するいくつかのオプションが必要です。オプション A、C、および D は、脆弱性ポリシーの有効な構成です。
A) パッケージの種類に基づいた個別のアクションにより、特定の種類のソフトウェア パッケージで見つかった脆弱性に対する個別の対応が可能になり、修復プロセスをより詳細に制御できるようになります。
C) ベンダーの修正が利用可能な場合にのみポリシーを適用すると、ソフトウェア ベンダーによってパッチまたはアップデートがリリースされた脆弱性の修復に優先順位を付けることができ、最も実用的なセキュリティ問題に対処する際にリソースを効率的に使用できます。
D) 重大度レベルごとに個別の猶予期間を設定することで、組織は重大度に基づいて脆弱性に対処するための異なる時間枠を定義でき、優先順位を付けたリスクベースの脆弱性管理アプローチが可能になります。
これらの構成は、脆弱性の性質、修正の可用性、各脆弱性に関連するリスク レベルに基づいたカスタマイズと優先順位付けを可能にすることで、包括的な脆弱性管理戦略をサポートします。

最新問題: **130**
Prisma Cloud は、脆弱性のインポートを許可し、クラウド内のリスクに関する追加のコンテキストを提供する 3 つの外部システムをサポートしていますか? 3つお選びください。)

A. Splunk
B. Amazon GuardDuty
C. クアリス
D. Amazon インスペクター
E. ServiceNow
Answer: A,B,E (メーッセージを残す)
Prisma Cloud はさまざまな外部システムと統合し、脆弱性をインポートし追加のコンテキストを提供することでセキュリティ機能を強化します。提供されるオプションには次のようなものがあります。
A) Splunk: Prisma Cloud は Splunk と統合して、脅威の検出とセキュリティ分析を強化できるため、正しい選択となります。
B) Amazon GuardDuty: Prisma Cloud は、Amazon GuardDuty の調査結果を利用して、AWS 環境内の脆弱性に関する追加の脅威インテリジェンスとコンテキストを提供し、それが正しい選択となるようにします。
E) ServiceNow: Prisma Cloud は、インシデント管理とワークフロー自動化のために ServiceNow と統合でき、脆弱性のコンテキストと修復機能を提供するため、正しい選択となります。オプション C (Qualys) と D (Amazon Inspector) は、脆弱性を Prisma Cloud にインポートするための統合外部システムとして、提供されたドキュメントに明示的に記載されていません。

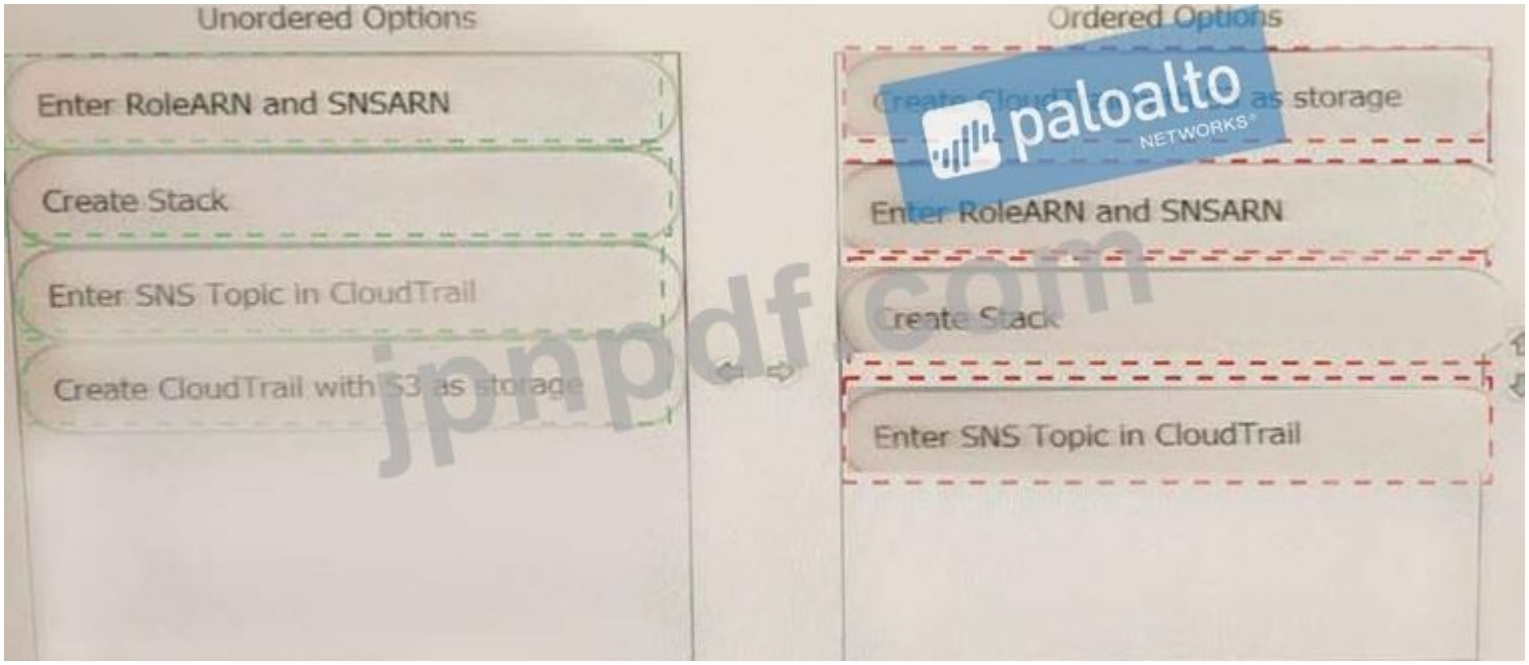
最新問題**: 131**
Prisma Cloud Compute Edition のコンソール イメージを取得するための正しい手順はどれですか?
A. 基本認証を使用して Prisma Cloud コンソール イメージを取得するには:
1. registry.twistlock.com にアクセスし、「docker login」を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。
B. URL 認証を使用して Prisma Cloud Console イメージを取得するには:
1. registry-url-auth.twistlock.com にアクセスし、ユーザー証明書を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。
C. URL 認証を使用して Prisma Cloud コンソール イメージを取得するには:
1. registry-auth.twistlock.com にアクセスし、ユーザー証明書を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。
D. 基本認証を使用して Prisma Cloud コンソール イメージを取得するには:
1. registry.paloaltonetworks.com にアクセスし、「docker login」を使用して認証します。
2. 「docker pull」を使用して、Prisma Cloud Console イメージを取得します。
Answer: (解答を表示する)
パロアルトネットワークスのクラウド セキュリティ スイートの一部である Prisma Cloud は、さまざまな環境に展開するために取得できるコンソール イメージを提供します。これらのイメージを取得するための正しいプロセスには、広く使用されているコンテナ化プラットフォームである Docker での基本認証を使用することが含まれます。ユーザーはまず、公式のパロアルトネットワークレジストリ (registry.paloaltonetworks.com) にアクセスする必要があります。ここでは、資格情報の入力を求める「docker login」コマンドを使用して認証する必要があります。認証が成功すると、ユーザーは「docker pull」コマンドを使用して Prisma Cloud コンソール イメージを取得できます。この方法により、コンテナ イメージの管理と展開のベスト プラクティスに沿って、組織のインフラストラクチャ内に展開するための最新のコンソール イメージへの安全なアクセスが保証されます。

最新問題**: 132**

Defender はどのくらいの頻度でコンソールとログを共有しますか?
A. 10 分ごと
B. 30 分ごと
C. 1 時間ごと
D. リアルタイム
Answer: D (メーッセージを残す)
Prisma Cloud では、Defender はワークロードを監視および保護することでクラウド環境を保護する上で重要な役割を果たします。Defender と Prisma Cloud Console 間の通信はリアルタイムで行われるため、脅威、脆弱性、コンプライアンス問題を即座に検出できます。このリアルタイム通信は、最新のセキュリティ体制を維持し、潜在的なセキュリティ インシデントに迅速に対応するために不可欠です。Defender と Console の通信はリアルタイムであるため、セキュリティ チームは最新の情報を入手し、リスクを軽減するために迅速な措置を講じることができます。

最新問題**: 133**
データセキュリティ機能で使用するAWSアカウントのオンボーディングに関連する手順を注文します。

Answer:



最新問題: **134**
顧客は、前日の未解決のアラートが解決されたことに気づきました。自動修復が構成されていませんでした。
このアラート ステータスの変化を説明する 2 つの理由はどれですか? (2つお選びください。)
A. アラートが外部統合に送信されました。
B. リソースが削除されました。
C. ユーザーがアラート ステータスを手動で変更しました。
D. ポリシーが変更されました。
Answer: (解答を表示する**)**

最新問題: **135**
異常なプロトコル アクティビティ (内部) ネットワーク異常により、生成されるアラートが多すぎます。管理者は、完全に無効にすることなく、生成されるイベントの数が最小限になるオプションに調整するよう求められています。
この目標を達成するには、管理者はどの戦略を使用する必要がありますか?
A. ポリシーを無効にします
B. アラートの性質を保守的に設定します
C. トレーニングしきい値を低に変更します
D. アラートの性質を 「アグレッシブ」に設定します
Answer: B (メーッセージを残す**)**
ポリシーを完全に無効にすることなく、 異常なプロトコル アクティビティ (内部)」ネットワーク異常によって生成されるアラートの数を減らすには、アラートの性質を保守的 (オプション B) に設定することが最も効果的な戦略です。この構成により、異常検出の感度が調整され、真のセキュリティ脅威を検出する能力を損なうことなく、誤検知の可能性が低減され、アラート疲労が最小限に抑えられます。異常検出に対してより保守的なアプローチを採用することで、管理者は、最も重大で有害な可能性のあるアクティビティのみがアラートをトリガーするようにし、セキュリティの警戒と運用効率のバランスを維持できます。

最新問題: **136**

Prisma Cloud Compute の初期展開中に、顧客は環境内の脆弱性に気づきます。
デフォルトの脆弱性ポリシーを正しく説明しているのはどれですか?
A. 脆弱性を含むすべてのコンテナをブロックします。
B. 3 つ以上の重大な脆弱性があるコンテナに対してアラートを生成します。
C. コンテナに重大な脆弱性が含まれている場合、30 日後にコンテナをブロックします。
D. 重大度に関係なく、すべての脆弱性について警告します。
Answer: D (メーッセージを残す)
デフォルトでは、Prisma Cloud の脆弱性ポリシーは、脆弱性の重大度に基づいてフィルタリングせずに、コンテナおよびイメージ全体で検出されたすべての脆弱性について警告するように構成されています。このデフォルト設定により、管理者は潜在的なセキュリティ問題をすべて認識できるようになり、環境のセキュリティ体制を包括的に把握できるようになります。管理者は、コンテキスト、重大度、組織の資産への影響に基づいて、これらの脆弱性を評価し、優先順位を付けることができます。

最新問題: **137**
CloudFormation テンプレートに関して正しいのはどれですか?
A. ネストされた参照、マクロ、または組み込み関数に対するスキャンのサポートは現在存在しません。
B. 単一のテンプレートまたはテンプレート ファイルの zip アーカイブを単一の API リクエストでスキャンすることはできません。
C. JSON のスキャン サポートが提供されます。HTML 形式と YAML 形式。
D. スキャンをリクエストするには、リクエスト ヘッダー フィールド「cloudformation-version」が必要です。
Answer: (解答を表示する)

最新問題: **138**
Prisma Cloud の管理者は、Docker エンジンに対してロールベースのアクセス制御を有効にしたいと考えています。
このタスクを実行するには、最初にどの構成手順が必要ですか?
A. 最初にアイデンティティ プロバイダーを使用し、次にコンソールを使用するように Docker の認証シーケンスを構成します。
B. Defender のリスナー タイプを TCP に設定します。
C. Docker のリスナー タイプを TCP に設定します。
D. 最初に ID プロバイダーを使用し、次にコンソールを使用するように Defender の認証シーケンスを構成します。
Answer: (解答を表示する)
Prisma Cloud 環境で Docker エンジンのロールベースのアクセス制御 (RBAC) を有効にするには、最初の構成手順で Docker のリスナー タイプを TCP に設定します。この変更により、Docker がネットワーク経由の接続を受け入れることができるようになり、Prisma Cloud Defender との統合が容易になり、RBAC ポリシーを適用できるようになります。TCP でリッスンするように Docker を構成することは、Docker デーモンと Prisma Cloud Defender 間の通信を可能にするために不可欠です。Prisma Cloud Defender は、RBAC の強制ポイ

ントとして機能し、どのユーザーまたはサービスがロールと権限に基づいて Docker エンジン上でアクションを実行できるかを制御します。この設定は、きめ細かいアクセス制御を実装し、環境内での Docker 操作のセキュリティを強化するための基礎となります。

最新問題**: 139**
Web Application and API Security (WAAS) ボット保護の一部である 2 つのボット タイプはどれですか? (2つお選びください。)
A. チャットボット
B. ユーザー定義のボット
C. 不明なボット
D. 顧客ボット
Answer: B,C (メーッセージを残す**)**
Prisma Cloud エコシステム内の Web Application and API Security (WAAS) ボット保護には、「ユーザー定義ボット」と「不明なボット」の 2 つの主要なカテゴリを含む、さまざまなタイプのボットが含まれています。ユーザー定義ボットとは、組織がその動作と目的に基づいて明示的に識別および分類したボットを指します。これらには、検索エンジン クローラーや内部自動化ツールなどの正規のボットが含まれる場合があり、これらはユーザーが設定した事前定義された基準に基づいて認識され、許可されます。
一方、不明なボットには、ユーザーまたはシステムによって明示的に識別または分類されていないボットが含まれます。これらには、データの収集、DDoS 攻撃の実行、または Web アプリケーションや API の脆弱性の悪用を試みる悪意のあるボットが含まれる可能性があります。未知のボットの分類は、ボットの動作を監視および分析して潜在的な脅威を特定し、適切な措置を講じることができるため、セキュリティを維持するために非常に重要です。
Prisma Cloud とクラウドネイティブ アプリケーションの保護に重点を置いている状況では、ユーザー定義ボットと未知のボットの区別は重要です。WAAS ボット保護に対する Prisma Cloud のアプローチは、ボット トラフィックをきめ細かく制御できるように設計されており、組織が有益なボット アクティビティと有害なボット アクティビティを区別できるようになります。これは、「Prisma-Cloud-Visibility-and-Control-Qualification-Guide」や「Guide-to- CSPM-ツール電子メール-ソーシャル-LP-コピー。」これらのリソースは、幅広い Web ベースの脅威から保護するためのボット トラフィックの管理を含む、包括的なセキュリティ対策の重要性を強調しています。
参照：
「Prisma-Cloud-Visibility-and-Control-Qualification-Guide」では、包括的なセキュリティ戦略の一環としてボット トラフィックの管理を含む、クラウド環境における可視性と制御の重要性について説明しています。
「CSPM-Tools-Email-Social-LP-Copy へのガイド」では、クラウド内の Web アプリケーションと API に関連するリスクを管理および軽減するための、WAAS ボット保護などの高度なセキュリティ ツールと実践の必要性を強調しています。

最新問題**: 140**
コンプライアンスレポートを作成する頻度はどれくらいですか? (2つお選びください。)
A. 毎月
B. 毎週
C. 1 回
D. 定期的
Answer: A,D (メーッセージを残す**)**

最新問題**: 141**

異常ポリシーは、異常なネットワークとユーザーのアクティビティを識別するためにどの 2 つのログを使用しますか? (2つお選びください。)
A. ネットワーク フロー
B. 監査
C. トラフィック
D. ユーザー
Answer: A,B (メーッセージを残す**)**
Prisma Cloud の異常ポリシーは、ネットワーク フロー ログ (A) と監査ログ (B) を利用して、異常なネットワークとユーザーのアクティビティを特定します。ネットワーク フロー ログは、ネットワーク全体のトラフィック フローを可視化し、悪意のあるアクティビティやネットワークの構成ミスを示す可能性のある通信パターンの異常を検出するのに役立ちます。監査ログはシステム内のユーザーのアクションを記録し、セキュリティを侵害する可能性のある未承認または不審な操作に関する洞察を提供します。これらのログを分析することで、異常ポリシーは確立されたベースラインから逸脱する異常を効果的に特定し、潜在的なセキュリティ脅威をタイムリーに検出して対応できるようにします。

最新問題**: 142**
コンピューティングでコンテナーおよびホスト ディフェンダーをデプロイするためにアクセスする必要がある DevOps ユーザーには、どのロールを割り当てる必要がありますか?
A. クラウド プロビジョニング管理者
B. セキュリティの構築と導入
C. システム管理者
D. 開発者
Answer: B (メーッセージを残す**)**
Prisma Cloud 内のコンピューティングにコンテナーおよびホスト ディフェンダーをデプロイするためのアクセス権が必要な DevOps ユーザーに割り当てる必要があるロールは、通常は 『セキュリティの構築とデプロイ」です。このロールは、アプリケーション ライフサイクルの開発および展開フェーズに関与するユーザーに必要な権限を提供するように設計されています。これにより、コンテナーやホスト ディフェンダーの導入などのセキュリティ対策をワークフローに統合できるようになります。この役割を担うことで、DevOps チームはビルドおよびデプロイメントのプロセスにセキュリティを確実に組み込むことができ、コンテナ化されたホストベースのアプリケーションのセキュリティを最初から維持できるようになります。

最新問題**: 143**
セキュリティ チームには、環境の脆弱性を確実にスキャンするという要件があります。脆弱性ポリシーを構成するための 3 つのオプションは何ですか? 3つお選びください。)
A. 各重大度レベルの個別の猶予期間
B. ベンダー修正が利用可能な場合にのみポリシーを適用します
C. ブロックされたリクエストの出力詳細度
D. パッケージ タイプに基づく個別のアクション
E. ブロックされたリクエストのメッセージをカスタマイズします
Answer: A,C,D (メーッセージを残す**)**

最新問題**: 144**

あなたには、Terraform の Prisma Cloud ビルド ポリシーを構成するというタスクが与えられています。このポリシーを完了するにはどのような種類のクエリが必要ですか?
A. YAML
B. CloudFormation
C. JSON
D. Terraform
Answer: C (メーッセージを残す)

最新問題: **145**
データ セキュリティ モジュールで利用できる 3 種類の分類はどれですか? （3つお選びください。）
A. マルウェア
B. 準拠規格
C. 個人を特定できる情報
D. 悪意のある IP
E. 財務情報
Answer: A,B,E (メーッセージを残す)

最新問題: **146**
Web アプリケーションおよび API セキュリティ (WAAS) ボット保護における不明なボットに属する 2 つのボット カテゴリはどれですか? (2つお選びください。)
A. ニュースボット
B. 検索エンジン クローラー
C. Web スクレイパー
D. HTTP ライブラリ
Answer: C,D (メーッセージを残す)
Prisma Cloud の Web-Application and API Security (WAAS) ボット保護では、未知のボットがその動作と特性に基づいて分類されます。Web スクレイパーと HTTP ライブラリは、未知のボットのカテゴリに分類されます。Web スクレイパーは、多くの場合許可なしに Web サイトからデータを抽出する自動化されたスクリプトまたはプログラムであり、HTTP ライブラリは HTTP リクエストを行うために使用されるツールです。どちらも無害に使用できますが、悪意のある活動に使用される可能性があるため、さらなる分析が必要な未知のボットとして分類されます。

最新問題: **147**
Prisma Cloud Compute Edition を識別するオプションはどれですか?
A. APT でインストールされたパッケージ
B. ダウンロード可能な自己ホスト型ソフトウェア
C. Software-as-a-Service (SaaS)
D. Prisma Cloud へのプラグイン
Answer: B (メーッセージを残す)

Prisma Cloud Compute Edition は、B. ダウンロード可能な自己ホスト型ソフトウェアとして識別されます。このオプションは、Prisma Cloud Compute Edition が組織が独自のインフラストラクチャ内に導入できるソリューションであり、セキュリティ プラットフォームのインストール、構成、管理を制御できることを示します。

最新問題: **148**
開発チームは Web フロントエンドをホストするポッドを構築しており、これらのポッドをアプリケーション ファイアウォールで保護したいと考えています。
このポッドをレイヤ 7 攻撃から保護するには、どのタイプのポリシーを作成する必要がありますか?
A. 開発チームは、ホスト上のすべてのリソースを対象とした WAAS ルールを作成する必要があります。
B. 開発チームは、ネットワーク保護を備えたランタイム ポリシーを作成する必要があります。
C. 開発チームは、これらのポッドが実行されるホストの WAAS ルールを作成する必要があります。
D. 開発チームは、ポッドのイメージ名を対象とした WAAS ルールを作成する必要があります。
Answer: A (メーッセージを残す)

最新問題: **149**
管理者は、継続的インテグレーション (CI) パイプラインでスキャンされたイメージのコンプライアンス ポリシーを取得したいと考えています。
API 経由で画像にアクセスできるようにするには、どのエンドポイントが正常に実行されますか?
A. GET /api/v22.01/policies/compliance
B. GET /api/v22.01/policies/compliance/ci
C. GET /api/v22.01/policies/compliance/ci/images
D. GET /api/v22.01/policies/compliance/ci/serverless
Answer: A (メーッセージを残す)
Prisma Cloud の API を介して継続的インテグレーション (CI) パイプラインでスキャンされたイメージのコンプライアンス ポリシーを取得するには、使用する正しいエンドポイントは GET /api/v22.01/policies/compliance (A) です。このエンドポイントは、CI パイプライン内のイメージに適用されるポリシーを含む、Prisma Cloud 内で定義されたコンプライアンス ポリシーの包括的なリストへのアクセスを提供します。これにより、管理者はプログラムでポリシーを取得してレビューし、イメージが展開される前に組織のコンプライアンス基準を満たしていることを確認できます。他のオプション (B、C、D) では、Prisma Cloud がコンプライアンス ポリシーにアクセスするために使用する標準 API エンドポイント形式と一致しないエンドポイントを指定しているため、不正確になります。

最新問題: **150**
正味有効なアクセス許可を計算するために使用される 3 つの AWS ポリシー タイプと ID はどれですか? (3 つ選択してください)。
A. AWS サービス コントロール ポリシー (SCP)
B. AWS IAM グループ
C. AWS IAM ロール
D. AWS IAM ユーザー
E. AWS IAM タグポリシー
Answer: (解答を表示する)
AWS では、正味有効なアクセス許可は、さまざまなポリシー タイプと ID に基づいて計算されます。正しい選択肢は次のとおりです。

A) AWS サービス コントロール ポリシー (SCP): SCP は AWS Organizations で組織内のすべてのアカウントのアクセス許可を管理するために使用され、正味有効なアクセス許可に影響を与えます。
B) AWS IAM グループ: IAM グループは、ユーザーのコレクションに対する一連の権限を定義し、ユーザーの有効な権限に影響を与えます。
C) AWS IAM ロール: IAM ロールは、一連のアクセス許可を引き受けるための一時的なセキュリティ認証情報を提供し、実質的に有効なアクセス許可に影響を与えます。オプション D (AWS IAM ユーザー) と E (AWS IAM タグ ポリシー) もアクセス許可の定義に役割を果たしますが、A、B、C は正味有効アクセス許可の計算に使用される主なタイプであり、正しい選択となります。

最新問題**: 151**
顧客がコンテナ監査を検討しており、監査によりクリプトマイナー攻撃が特定されました。この監査が発生した可能性がある 3 つのオプションはどれですか? （3つお選びください。）
A. 一般的なクリプトマイナー ポートの使用法が見つかりました。
B. マイニングされた通貨はユーザー トークンに関連付けられます。
C. 共通のクリプトマイナー プロセス名が見つかりました。
D. マイニングされた通貨の価値が $100 を超えています。
E. コンテナーの長時間にわたる高い CPU 使用率が検出されました。
Answer: B,C,E (メーッセージを残す**)**

最新問題**: 152**
顧客には、サーバーレス機能の脆弱性をスキャンするという要件があります。
スキャンを構成する正しいオプションは何ですか?
A. [防御] > [コンプライアンス] > [クラウド プラットフォーム] ページからサーバーレス レーダーを構成します。
B. サーバーレス Defender を関数に埋め込みます。
C. [防御] > [脆弱性] > [機能] ページから機能スキャン ポリシーを構成します。
D. Lambda レイヤーを使用して、Defender を関数にデプロイします。
Answer: (解答を表示する**)**
Prisma Cloud では、AWS Lambda 関数などのサーバーレス関数の脆弱性をスキャンする機能は、クラウド セキュリティ体制管理 (CSPM) とコンプライアンスを確保するために不可欠な部分です。具体的には、選択肢 C は正解です。Prisma Cloud には、「防御 > 脆弱性 > 機能」ページで、サーバーレス機能の脆弱性に関連するポリシーを定義するための専用セクションが用意されています。この機能を使用すると、管理者はサーバーレス機能の既知の脆弱性を自動的にスキャンするポリシーを作成および管理し、機能が展開される前に組織のセキュリティ標準に準拠していることを確認できます。このアプローチは、「クラウド セキュリティ体制管理ツールのガイド」ドキュメン

トで概要が説明されているように、サーバーレス機能を含むクラウド セキュリティのさまざまな側面をカバーする Prisma Cloud の包括的なセキュリティ モデルと一致しています。

最新問題: **153**
顧客は、複数のクラウドに展開されたサーバーレス機能を持っています。
「過度に寛容なサービス アクセス」コンプライアンス チェックの対象となるサーバーレス クラウド プロバイダーはどれですか?
A. アリババ
B. GCP
C. AWS
D. アズール
Answer: (解答を表示する**)**
参照：
「過度に寛容なサービスアクセス」コンプライアンスチェックの対象となるサーバーレスクラウドプロバイダーはAWS（Amazon Web Services）です。AWS が提供するサーバーレス コンピューティング プラットフォームである AWS Lambda には、操作を実行するために必要以上の権限が割り当てられている機能があり、セキュリティ リスクにつながる可能性があります。
Prisma Cloud などの CSPM ツールのコンテキストでは、過度に寛容なサービス アクセスのチェックには、通常、AWS Lambda 関数に付加されたポリシーを検査して、最小特権の原則に準拠していることを確認することが含まれます。このようなチェックは、攻撃者によって悪用される可能性がある広すぎる権限を特定して修正するのに役立ちます。
これについては、AWS の Lambda セキュリティのベストプラクティスで参照できます。そこでは、Lambda 関数がタスクを実行するために必要な最小限の権限を付与することの重要性が強調されており、それによって潜在的な攻撃対象領域が削減されます。

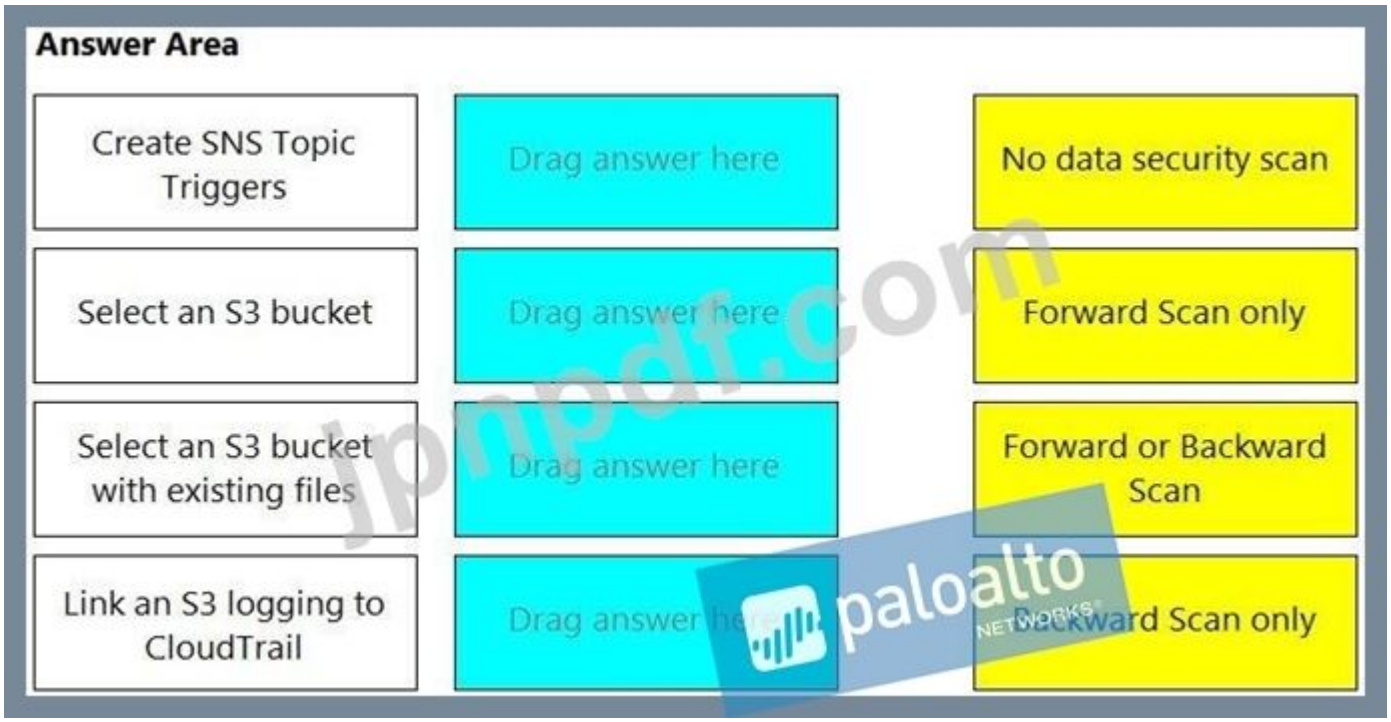
最新問題: **154**
どのコンテナ スキャンが正しく構築されていますか?
A. Twistcli イメージ スキャン -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 -- コンテナ myimage/latest
B. Twistcli イメージ スキャン --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest
C. Twistcli 画像スキャン -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 --details myimage/latest
D. Twistcli 画像スキャン -u api -p api --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest
Answer: C (メーッセージを残す**)**
Prisma Cloud (旧称 Twistlock) が提供する TwistCLI ツールを使用したコンテナ スキャンの正しい構成をオプション C に示します。このコマンドは、TwistCLI ツールを使用してコンテナ イメージをスキャンし、必要な認証資格情報 (ユーザー名とパスワードに 「u」を付けたもの) を指定します。' および '-p' フラグ)、Prisma Cloud インスタンスのアドレス ('-address' フラグを使用)、およびスキャンするイメージ (この場合は 'myimage/latest')。「-details」フラグを含めることは、詳細なスキャン結果を取得するための一般的な方法であり、詳細な分析と修復作業に不可欠です。このコマンド構造は、Prisma Cloud の公式リソースとガイドに記載されている、画像スキャン目的での TwistCLI の標準的な使用法と一致しています。

最新問題: **155**
Prisma Cloud の管理者は、ホスト間の接続や構成されたネットワーク オブジェクトへの接続を含む、すべての接続を監視するためのグラフィカル ビューを取得する必要があります。
このタスクを実行するために管理者はどの設定を有効または構成しますか?
A. クラウド ネイティブ ネットワーク ファイアウォール

B. WAAS 分析
C. テレメトリ
D. ホストの洞察
E. ADEM
Answer: A (メーッセージを残す**)**

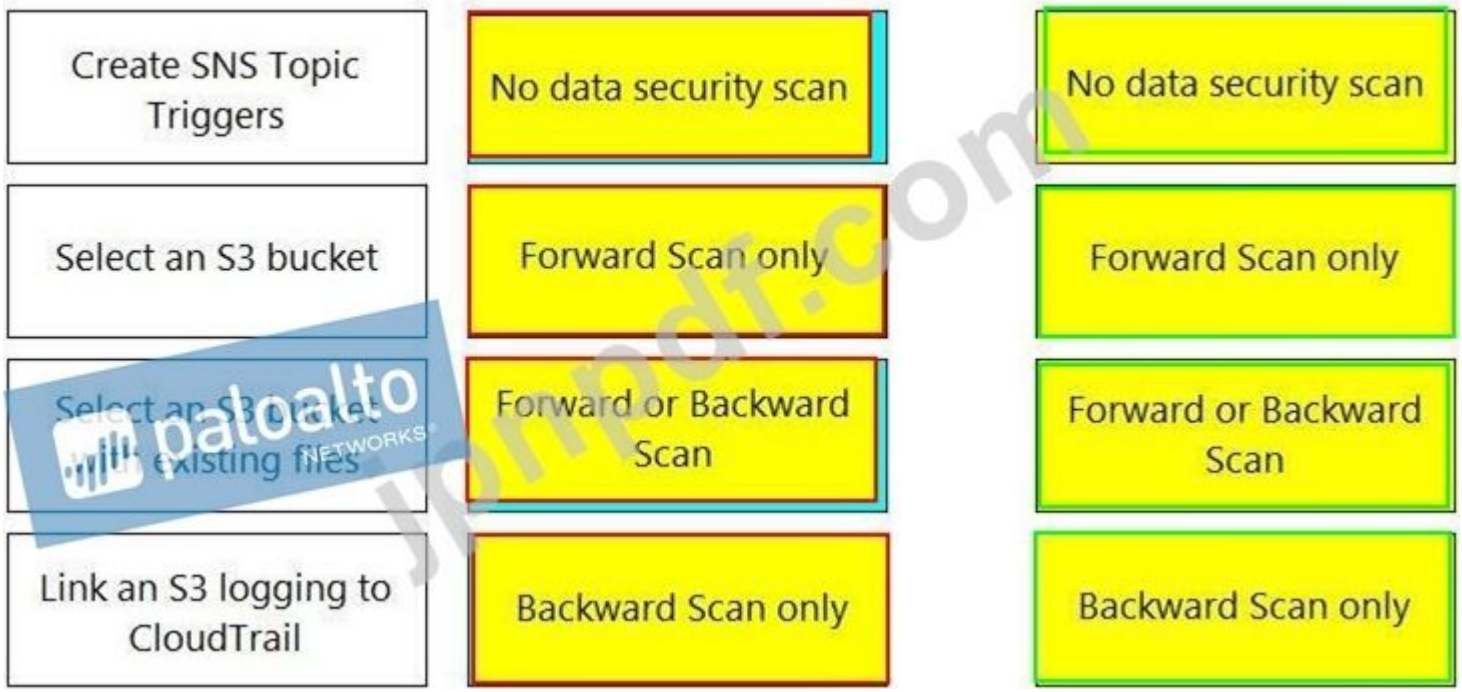
最新問題**: 156**
Prisma Cloud ソフトウェア リリース 22.06 (Kepler) では、どのレジストリ タイプが追加されますか?
A. Azure Container Registry
B. Google アーティファクト レジストリ
C. IBM Cloud Container Registry
D. ソナタイプ ネクサス
Answer: B (メーッセージを残す**)**
Kepler リリースと呼ばれる Prisma Cloud ソフトウェア リリース 22.06 では、サポートされるレジストリ タイプとして Google Artifact Registry が追加されたことが重要な更新でした。Google Artifact Registry は、コンテナ イメージと言語パッケージ (Maven や npm など) を保存、管理、保護するように設計されています。チームがアーティファクトと依存関係を管理するための単一の場所を提供し、ソフトウェア開発および展開プロセス全体の一貫性とセキュリティを向上させます。Prisma Cloud のこのアップデートは、最新のクラウドネイティブ テクノロジーとサービスをサポートし、最新のクラウド環境を保護する機能を強化するというプラットフォームの取り組みを反映しています。

最新問題**: 157**
特定の操作ごとに正しいスキャン モードを一致させます。
(プルダウン リストから回答を選択します。回答は複数回使用することも、まったく使用しないこともできます。)



Answer:

Answer Area



最新問題**: 158**
どのコンテナ イメージ スキャンが正しく構築されていますか?
A. ツイストCIIイメージスキャン -docker-address https://us-west1クラウドツイストロックcom/us-3-123456?89 myimage/latest
B. twistcii イメージ スキャン -address https7/us-west1 cloud.twistlockxom/us-3-123456789 myimage/latest
C. Twistcli イメージ スキャン -address https //us-west1 cloudTwistlock com/us-3-123456789 -container myimage/latest
D. Twistcli 画像スキャン -アドレス https://us-west1。Cloud.twistlock.com/us-3-123456789 -container myimage/latest -details
Answer: B (メーッセージを残す**)**

最新問題**: 159**
お客様は、構成ミスから環境を強化したいと考えています
ホストに対する Prisma Cloud Compute Compliance の適用では、どの 3 つのオプションがカバーされますか? 3つお選びください。)
A. Docker デーモンの構成
B. ホスト構成
C. Defender エージェントのないホスト
D. ホスト クラウド プロバイダーのタグ
E. Docker デーモン構成ファイル
Answer: B,C,E (メーッセージを残す**)**

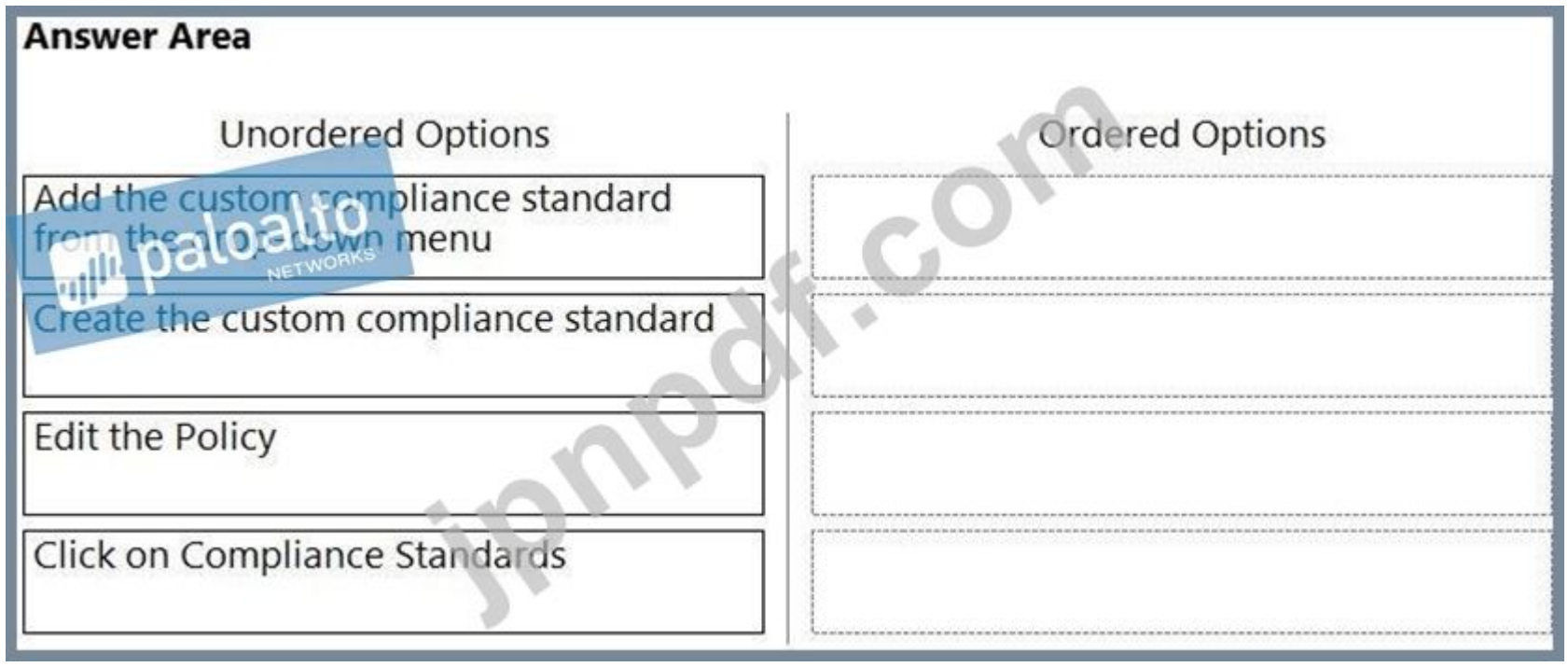
最新問題**: 160**
Prisma Cloud ソフトウェア リリース 22.06 (Kepler) では、どのレジストリ タイプが追加されますか?
A. ソナタイプ ネクサス
B. Google アーティファクト レジストリ
C. IBM Cloud Container Registry
D. Azure Container Registry

Answer: D (メーッセージを残す)

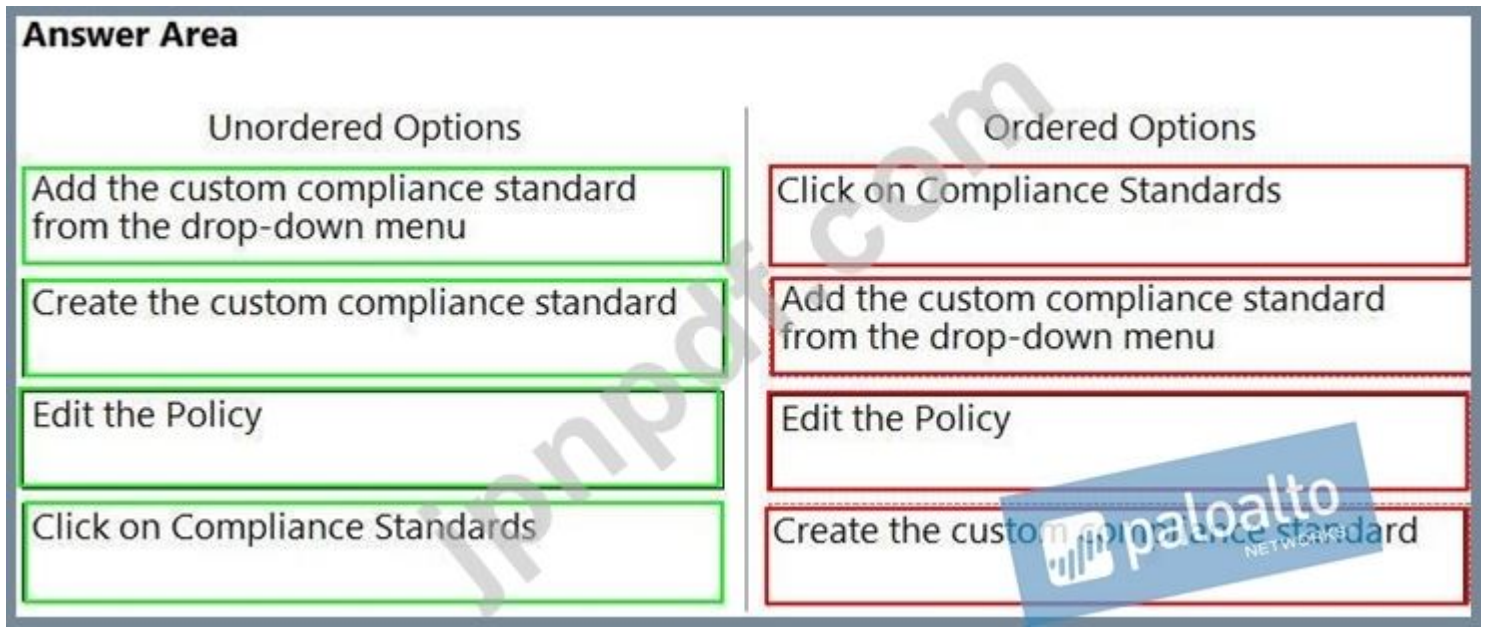
最新問題: **161**
コンテナ ランタイム モデルの学習フェーズ中に、Prisma Cloud は何時間の 「ドライ ラン」期間に入りますか?
A. 4
B. 48
C. 1
D. 24
Answer: (解答を表示する)
Prisma Cloud とそのコンテナ ランタイム モデルのコンテキストでは、学習フェーズは、システムがコンテナ アクティビティの通常の動作とパターンを観察して理解する重要な期間です。この 「ドライラン」期間により、Prisma Cloud は正常とみなされるベースラインを確立でき、後で異常や悪意のあるアクティビティを特定するのに役立ちます。この学習フェーズには通常 48 時間が使用され、さまざまな時間と条件にわたって十分な量のデータが収集され、一般的なコンテナーの操作を包括的に理解できるようになります。

最新問題: **162**
Prisma Cloud 管理者は新しいポリシーを設定しました。
このポリシーをコンプライアンス標準に割り当てるにはどの手順を使用する必要がありますか?
A. ポリシーを編集し、ステップ 3 (コンプライアンス標準) に進み、下部の [+] をクリックしてコンプライアンス標準を選択し、他のボックスに入力して、[確認] をクリックします。
B. [コンプライアンス] タブからコンプライアンス標準を作成し、[ポリシーに追加] を選択します。
C. ポリシーの 「コンプライアンス標準」セクションを開き、保存します。
D. カスタム ポリシーを既存の標準に追加することはできません。
Answer: A (メーッセージを残す)
新しいポリシーを Prisma Cloud のコンプライアンス標準に割り当てるには、管理者はポリシーを編集し、コンプライアンス標準が管理されるステップに移動する必要があります。「」ボタンをクリックすると、管理者はポリシーを特定のコンプライアンス標準に追加し、必要な詳細を入力して割り当てを確認できます。これにより、カスタム ポリシーが選択したコンプライアンス標準に統合され、コンプライアンス チェックに新しく定義されたポリシー基準が確実に含まれるようになります。

最新問題: **163**
ポリシーをカスタム コンプライアンス標準にマッピングする手順はどの順序ですか?
(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)



Answer:



最新問題: **164**

次の RQL があるとします。

```
event from cloud.audit_logs where operation IN ('v1.compute.urlMaps.update', 'v1.compute.urlMaps.delete',
'v1.compute.backendServices.delete', 'v1.compute.backendBuckets.delete', 'v1.compute.backendServices.update',
'v1.compute.globalForwardingRules.delete', 'v1.compute.urlMaps.delete', 'v1.compute.targetHttpsProxies.delete',
'v1.compute.targetHttpsProxies.setSslPolicy', ''v1.compute.targetHttpsProxies.setSslCertificates')
```

RQL によって識別される監査イベント スニペットはどれですか?

A.

```
"eventTime": "2021-05-19T14:34:08Z", "eventSource": "iam.amazonaws.com", "eventName": "AttachRolePolicy",
"awsRegion": "us-east-1"
```

```
"payload": { > "requestMetadata": { "callerSuppliedUserAgent": "Terraform/0.14.0
(+https://www.terraform.io) Terraform-Plugin-SDK/2.1.0 terraform-provider-
google/3.50.0,gzip(gfe)", "callerIp": "34.235.226.252" }, "request": { "@type":
"type.googleapis.com/compute.backendServices.delete"
```


B.


```
"resource": "projects/_/buckets/gvtest110221", "permission": "storage.buckets.setIamPolicy",
 "resourceAttributes": {}, "granted": true
```


C.


```
"userIdentity": { "type": "Root", "principalId": "6849955112A19", "arn":
"arn:aws:iam::6849955112A9:root", "accountId": "689995514A219", "accessKeyId": ""
```


D.

Answer: D (メーッセージを残す)

提供される RQL は、コンピューティング ファイアウォール ルールの作成や削除など、特定のネットワーク関連の操作をキャプチャするように設計されています。この RQL に一致する監査イベント スニペットはオプション D です。これは、そのリクエスト内に「compute.firewalls.delete」操作が含まれており、指定された RQL の基準と一致しています。

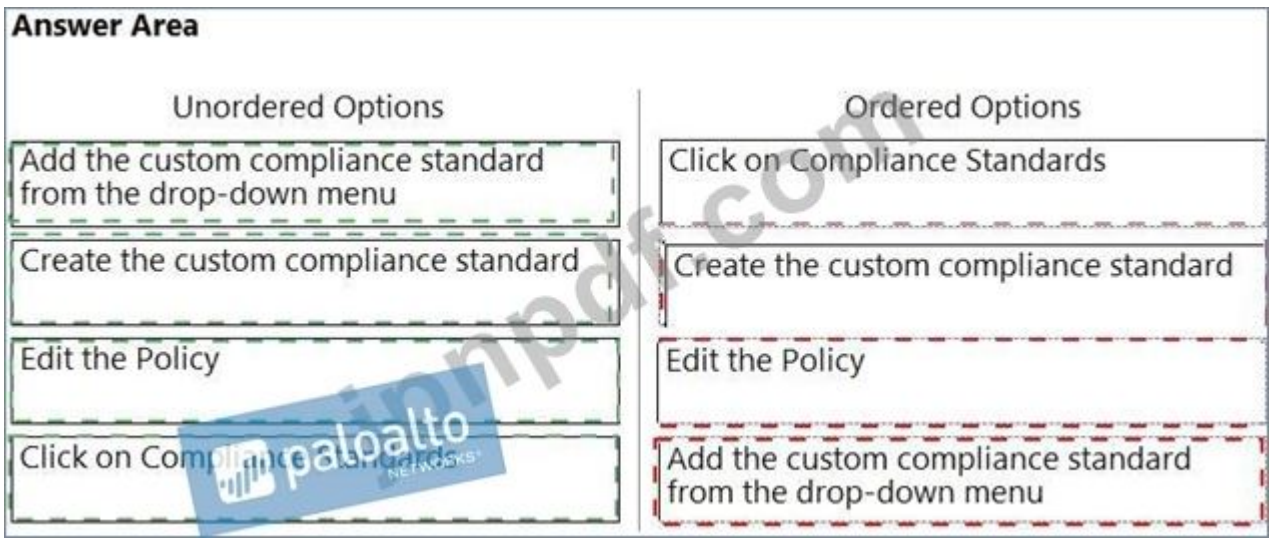
最新問題: **165**

ポリシーをカスタム コンプライアンス標準にマッピングする手順はどの順序ですか?

(最初のステップから最後のステップまで、ステップを正しい出現順序にドラッグします。)

Answer Area

Answer:



説明

1. 準拠規格をクリックします。
2. カスタムコンプライアンス標準を追加します。
3. ポリシーを編集します。
4. ドロップダウン メニューからコンプライアンス標準を追加します

https://docs.prismacloudcompute.com/docs/enterprise_edition/compliance/custom_compliance_checks.html#cre

最新問題**: 166**

セキュリティ チームはカスタム ポリシーを作成するように依頼されました。

この目標を達成するためにチームが使用できる 2 つの方法はどれですか? (2つお選びください。)

A. 新しいポリシーを追加します

B. 既存のポリシーのクローンを作成します

C. すぐに使えるポリシーを無効にします

D. すぐに使えるポリシーでクエリを編集します

Answer: A,B (メーッセージを残す**)**

Prisma Cloud のようなクラウド セキュリティ プラットフォーム内でカスタム ポリシーを作成する場合、セキュリティ チームは新しいポリシーを最初から追加するか、既存のポリシーを複製してカスタマイズの基盤として機能するかを柔軟に選択できます。新しいポリシーを追加すると、特定のセキュリティ要件に基づいて完全にカスタマイズされたルール セットを作成できます。一方、既存のポリシーのクローンを作成すると、すでに確立されているポリシーの構造を使用して迅速に開始でき、その後、特定のニーズに合わせて変更できます。このアプローチは、独自のセキュリティ シナリオに対処しながら、既存のポリシーとの一貫性を維持するのに有益です。すぐに使用できるポリシーを無効にする (オプション C)、またはすぐに使用できるポリシーのクエリを編集する (オプション D) は、ポリシーの適用をカスタマイズするために実行される可能性のあるアクションですが、新しいカスタム ポリシー。

最新問題: **167**
管理者はどのコンソール メニューでカスタム コンプライアンス チェックが失敗するか合格するかを確認しますか?
A. モニター > コンプライアンス
B. コンテナのセキュリティ > コンプライアンス
C. 防御 > コンプライアンス
D. カスタム > コンプライアンス
Answer: (解答を表示する**)**
Prisma Cloud では、 監視 > コンプライアンス」メニューは、管理者が事前定義されたコンプライアンス標準およびフレームワークとともにカスタム コンプライアンス チェックのステータスを確認できる一元的な場所です。このセクションでは、組織のコンプライアンス体制の包括的なビューを提供し、特定のコンプライアンス チェックが合格か不合格かを表示します。これにより、クラウド環境全体のコンプライアンス ステータスに関する詳細な洞察が可能になり、管理者がコンプライアンス違反の領域を特定し、コンプライアンス違反の原因を理解し、特定された問題に対処するための修正措置を講じることができます。

最新問題: **168**
Prisma Cloud Enterprise へのプログラムによる認証にはどの方法を使用する必要がありますか?
A. アクセスキー
B. シングル サインオン
C. SAML
D. 基本認証
Answer: (解答を表示する**)**

最新問題: **169**
コンソールのデフォルトの展開では、顧客はデフォルトで設定されているアラート付きコンプライアンス チェックを特定する必要があります。
顧客はコンソールのどこに移動する必要がありますか?
A. モニター > コンプライアンス
B. 防御 > コンプライアンス
C. 管理 > コンプライアンス
D. カスタム > コンプライアンス
Answer: (解答を表示する**)**
参照：
Palo Alto Networks の Prisma Cloud のコンテキストでは、デフォルトで設定されているアラート付きコンプライアンス チェックを識別するための正しいナビゲーションは、 防御」セクション、具体的には 防御 > コンプライアンス」にあります。このセクションは、ユーザーがコンプライアンス ポリシーとルールを構成および管理し、コンプライアンス ステータスを監視し、コンプライアンス違反に関連するアラートを確認できるように設計されています。 防御」セクションは、クラウド環境内の潜在的なセキュリティ リスクに対するコンプライアンス標準を含む防御策を設定するために調整されており、コンプライアンス関連のアラートと設定を管理および確認するための論理的な場所になります。

最新問題: **170**
SSO を構成する場合、Prisma Cloud によって監視されるすべてのクラウド アカウントに対して IdP プロバイダーをいくつ有効にできますか?
A. 2
B. 4
C. 1
D. 3
Answer: C (メーッセージを残す)
Prisma Cloud は、ユーザー認証プロセスを合理化するために、アイデンティティ プロバイダー (IdP) を使用したシングル サインオン (SSO) の構成をサポートしています。ただし、Prisma Cloud によって監視されるすべてのクラウド アカウントについて、一度に有効にできる IdP プロバイダーは 1 つだけです。この制限により、プラットフォーム全体で統一された認証メカニズムが確保され、複数の IdP 構成の管理に伴う複雑さと潜在的なセキュリティ リスクが軽減されます。

最新問題: **171**
Prisma Cloud Compute Edition のコンソール イメージの取得について正しいのはどれですか?
URL 認証を使用して Prisma Cloud Console イメージを取得するには;
A. 1. レジストリのTwistlock comにアクセスします。「docker login」を使用して認証します
2 「docker pull」を使用して Prisma Cloud Console イメージを取得します
URL 認証を使用して Prisma Cloud Console イメージを取得するには
B. 1 registry-urt-authTwistlock com にアクセスし、ユーザー証明書を使用して認証します
2. 「docker pull」を使用して Prisma Cloud Console イメージを取得します。
基本認証を使用して Prisma Cloud Console イメージを取得するには:
C. 1 レジストリ paloaltonetworks com にアクセスします。「docker login」を使用して認証します
2 「docker pull」を使用して Prisma Cloud Console イメージを取得します
D. 1 registry-auth.twistlock com にアクセスし、ユーザー証明書を使用して認証します。
2. 「docker pull」を使用して Prisma Cloud Console イメージを取得します。
基本認証を使用して Prisma Cloud Console イメージを取得するには
Answer: D (メーッセージを残す)

最新問題: **172**
セキュリティ要件に従って、管理者は Prisma Cloud アラートの電子メールを受信する人のリストを提供する必要があります。
管理者はこの電子メール受信者のリストをどこで見つけることができますか?
A. アラート ルール内のターゲット セクション。
B. アラート内の通知テンプレート セクション。
C. [設定] 内の [ユーザー] セクション。
D. アラート ルール内のアラート通知セクションを設定します。
Answer: (解答を表示する)
Prisma Cloud では、アラートの電子メールを受信している人のリストは、個別のアラート ルールの設定内で管理されます。

オプション D: アラート ルール内の [アラート通知の設定] セクションでは、管理者は Prisma Cloud によって生成されたアラートの電子メール受信者を指定できます。このセクションでは、アラートがトリガーされたときに電子メール通知を受信する受信者の選択など、アラート通知をカスタマイズできます。この粒度により、適切な関係者に特定のセキュリティ インシデントやコンプライアンス違反に関する情報が確実に提供され、タイムリーかつ適切な対応が容易になります。
参照：
Prisma Cloud アラート設定ドキュメント: 通知設定の構成方法や電子メール アラートの受信者の指定方法など、Prisma Cloud でアラート ルールを設定するプロセスについて詳しく説明します。
アラート管理のベスト プラクティス: 効果的なアラート管理戦略についての洞察を提供し、重要なセキュリティ情報が関係者に迅速に届くようにするための、的を絞ったアラート通知の重要性を強調します。

最新問題**: 173**
コンテナー イメージのスキャン コンプライアンス ルールで使用できる 3 つのアクションはどれですか? （3つお選びください。）
A. 許可する
B. スヌーズ
C. ブロック
D. 無視します
E. アラート
Answer: A,B,E (メーッセージを残す**)**
Prisma Cloud のコンテナ イメージ スキャン コンプライアンス ルールの場合、コンプライアンス違反が検出されたときに実行できるアクションは次のとおりです。
許可: このアクションは、コンプライアンス違反にもかかわらず、コンテナー イメージの使用を許可します。通常、違反に伴うリスクが受け入れられるか、最小限であるとみなされる場合に使用されます。
スヌーズ: このアクションは、指定された期間、コンプライアンス違反を一時的に無視します。すぐに修復できない場合に便利ですが、この問題は近い将来に解決される予定です。
アラート: このアクションは、コンテナー イメージの使用をブロックすることなく、関連する担当者またはシステムにコンプライアンス違反について通知するアラートを生成します。これにより、チームは適切な修復手順を決定しながら、コンプライアンスの問題を認識して追跡できるようになります。
これらのアクションにより、組織のポリシー、リスク許容度、修復能力に基づいてコンプライアンス違反を柔軟に管理できます。

最新問題**: 174**
この情報を考慮すると、次のようになります。
コンソールは https://prisma-console.mydomain.local にあります。ユーザー名は:cluster パスワードは:password123 スキャンするイメージは:myimage:latest コンテナーの脆弱性をスキャンし、それぞれの脆弱性の詳細は?
A. Twistcli イメージ スキャン --console-address https://prisma-console.mydomain.local -u クラスター -p パスワード 123 -- 詳細 myimage:latest
B. Twistcli イメージ スキャン --console-address prisma-console.mydomain.local -u クラスター -p パスワード 123 -- 脆弱性の詳細 myimage:latest
C. Twistcli イメージ スキャン --address prisma-console.mydomain.local -u クラスター -p パスワード 123 --vulnerability- 詳細 myimage:latest
D. Twistcli イメージ スキャン --address https://prisma-console.mydomain.local -u クラスター -p パスワード 123 --details myimage:latest

Answer: D (メーッセージを残す)
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_images

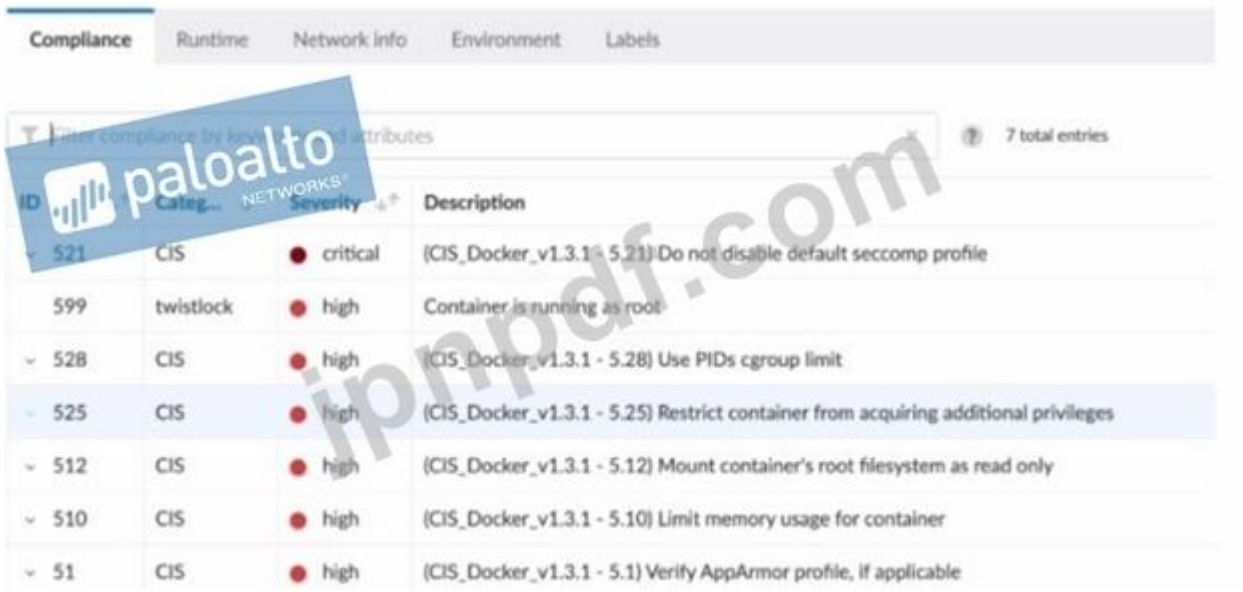
最新問題**: 175**
管理者は、DevSecOps チームから、Prisma Cloud Enterprise テナント内の既存のユーザーおよびユーザーに関連付けられた権限レベルをプログラムで継続的にクエリするスクリプトを作成するという要件を課されました。
このステップを実行するために必要な属性を決定するために、どの公開ドキュメントの場所を確認する必要がありますか?
A. Prisma Cloud 管理者ガイド (コンピューティング)
B. Prisma Cloud API リファレンス
C. Prisma Cloud Compute API リファレンス
D. Prisma Cloud Enterprise 管理者ガイド
Answer: C (メーッセージを残す)
Prisma Cloud 内でのユーザー情報と権限のスクリプト作成とプログラムによるクエリには、Prisma Cloud Compute API リファレンスが最適なリソースです。この API リファレンスでは、Prisma Cloud Compute モジュール内のユーザーと権限の管理を含む、コンピューティング関連のクエリに特化して調整された、利用可能なエンドポイント、リクエスト形式、応答構造に関する詳細情報を提供します。このリソースは、セキュリティ管理に対するプラットフォームの API ファーストのアプローチに沿った、自動化とサードパーティ システムとの統合をサポートする Prisma Cloud の包括的なドキュメントの一部です。

最新問題**: 176**
WAAS アクセス コントロールのファイル アップロード コントロールでは、すぐに使用できる 3 つのファイル タイプはどれですか? 3つお選びください。）
A. オーディオ
B. テキスト
C. 日記
D. 画像
E. ドキュメント
Answer: B,D,E (メーッセージを残す)

最新問題**: 177**
セキュリティ チームには、環境の脆弱性を確実にスキャンするという要件があります。脆弱性ポリシーを構成するための 3 つのオプションは何ですか? 3つお選びください。）
A. ブロックされたリクエストの出力詳細度
B. ベンダー修正が利用可能な場合にのみポリシーを適用します
C. 各重大度レベルの個別の猶予期間
D. ブロックされたリクエストのメッセージをカスタマイズします
E. パッケージ タイプに基づく個々のアクション
Answer: A,B,C (メーッセージを残す)

最新問題**: 178**

コンテナーとイメージのコンプライアンス ルールは、すべてのチェックを有効にすることで構成されています。ただし、コンテナのコンプライアンス ビューを確認すると、下の画像のエントリのみが表示されます。



次に取るべき適切な行動は何でしょうか?

A. 防御者をデプロイして、コンテナーのコンプライアンスを完全にスキャンします。

B. Prisma Cloud がコンプライアンス スキャンを完了するまで待って、再チェックします。

C. ルール オプションを変更して、コンプライアンス ルール編集ウィンドウに失敗したチェックと成功したチェックの両方をリストします。

D. コンプライアンス ルール編集ウィンドウに失敗したチェックのみをリストするようにルール オプションを変更します。

Answer: (解答を表示する)

提供されている画像は、フィルター処理されたコンプライアンス ビューを示しています。これには、さまざまな重大度を持つ特定のチェックと、コンテナーとイメージのコンプライアンスに関連する説明のみが表示されます。コンプライアンス ルールはすべてのチェックを有効にするように構成されていますが、エントリのサブセットのみが表示されるため、現在のビューが特定のエントリを表示するようにフィルタリングされていることを意味します。合格したチェックを含むすべてのチェックの包括的なビューを取得するには、ルール オプションを調整する必要があります。失敗したチェックと合格したチェックの両方をリストするオプションを選択すると、コンテナのコンプライアンス ステータスを完全に可視化して、コンプライアンスのどの側面も見落とされていないことを確認し、必要な情報をすべてレビューに利用できるようにすることができます。

最新問題: **179**

コンテナ ランタイム モデルの 3 つの状態とは何ですか? （3つお選びください。）

A. 開始中

B. 学習

C. アクティブ

D. 実行中

E. アーカイブ済み

Answer: (解答を表示する)

Prisma Cloud のコンテナ ランタイム モデルには通常、学習、アクティブ、アーカイブなどの状態が含まれます。学習状態では、Prisma Cloud がコンテナの動作を観察して、通常の操作を理解し、ベースラインを確立します。このフェーズでは、システムはセキュリティ ポリ

シーを積極的に適用しませんが、コンテナ アクティビティの典型的な動作とパターンを学習します。アクティブ状態は、システムが学習した動作と検出された異常に基づいてセキュリティ ポリシーをアクティブに適用する状態です。ベースラインから逸脱する不審または悪意のあるアクティビティを示すコンテナーは、構成されたポリシーに基づいてアラートまたはアクションをトリガーする場合があります。アーカイブ済み状態とは、アクティブではなくなったが、そのデータとアクティビティ ログが履歴分析やコンプライアンスの目的で保持されているコンテナを指します。

最新問題**: 180**
この情報を考慮すると、次のようになります。
コンソールは https://prisma-console.mydomain.local にあります。ユーザー名は:cluster パスワードは:password123 スキャンするイメージは:myimage:latest コンテナーの脆弱性をスキャンし、それぞれの脆弱性の詳細は?
A. Twistcli イメージ スキャン --console-address https://prisma-console.mydomain.local -u クラスター -p パスワード 123
-- 詳細 myimage:最新
B. Twistcli イメージ スキャン --address prisma-console.mydomain.local -u クラスター -p パスワード 123
--脆弱性-詳細 myimage:latest
C. Twistcli イメージ スキャン --address https://prisma-console.mydomain.local -u クラスター -p パスワード 123 --details myimage:latest
D. Twistcli イメージ スキャン --console-address prisma-console.mydomain.local -u クラスター -p パスワード 123 -- 脆弱性の詳細 myimage:latest
Answer: C (メーッセージを残す**)**

最新問題**: 181**
セキュリティ チームは、コンテナ化された Web アプリケーションに Cloud Native Application Firewall (CNAF) を展開しています。アプリケーションは NGINX コンテナーを実行しています。コンテナーはポート 8080 でリッスンしており、ホスト ポート 80 にマッピングされています。
アプリケーションを保護するには、チームは CNAF ルールでどのポートを指定する必要がありますか?
A. 8080
B. 443
C. 80
D. 8888
Answer: A (メーッセージを残す**)**

最新問題**: 182**
ビルドおよび実行サブタイプを含むカスタム ポリシーを作成したいと考えています。
各例のクエリ タイプを一致させます。

(プルダウン リストから回答を選択します。回答は複数回使用することも、まったく使用しないこともできます。)

Answer:

最新問題: **183**

Prisma Cloud 上の管理ユーザーにアカウント グループを割り当てると、リソースへのアクセスが制限されるのにどのように役立ちますか?

A. クラウド アカウント内の特定の種類のリソースへのアクセスのみを制限します。

B. クラウド アカウント内のすべてのリソースとデータへのアクセスを制限します。

C. アカウント グループ内のクラウド アカウントに関連するリソースとデータのみへのアクセスを制限します。

D. クラウド アカウント内のリソースへのアクセスは制限されません。

Answer: C (メーッセージを残す**)**

Prisma Cloud では、管理ユーザーをアカウント グループに割り当てることは、ユーザーのアクセスをリソースとデータの特定のサブセットに制限することにより、最小特権の原則を実装する方法です。アカウント グループはクラウド アカウントの論理的な集合であり、管理ユーザーを特定のアカウント グループに関連付けることにより、管理ユーザーのアクセスは、そのグループ内のクラウド アカウントに関連付けられたリソースとデータのみに制限されます。このメカニズムにより、ユーザーは自分の役割やタスクに必要な情報やリソースにのみアクセスできるようになり、クラウド環境内での不正なアクセスやアクションの可能性を最小限に抑えることでセキュリティが強化されます。

最新問題: **184**
管理者は、コンソール内からコンソール監査ログを確認したいと考えています。このデータを確認できる場合、管理者はコンソールのどのページを使用してこのデータを確認すればよいですか?
A. [管理] > [ディフェンダー] > [ログの表示] に移動します。
B. [モニター] > [イベント] > [ホスト ログ検査] に移動します。
C. [管理] > [ログの表示] > [履歴] に移動します。
D. 監査ログはコンソールの外部でのみ表示できます。
Answer: (解答を表示する**)**

最新問題: **185**
Prisma Cloud API に関するドキュメントの最も信頼性が高く広範なソースは何ですか?
A. ライブコミュニティ
B. docs.paloaltonetworks.com
C. Prisma Cloud 管理者ガイド
D. プリズマ.パン.dev
Answer: C (メーッセージを残す**)**

最新問題: **186**
Prisma Cloud Compute をアドミッション コントローラーとして使用するように Kubernetes を構成する場合、どの手順が含まれますか?
A. コンソール アドレスをコピーし、デフォルトの名前空間の構成マップを設定します。
B. Kubernetes にアドミッション コントローラーという名前の新しい名前空間を作成します。
C. コンソールからアドミッション コントローラー構成をコピーし、Kubernetes に適用します。
D. コンソールの [防御] > [アクセス] > [Kubernetes] ページから Kubernetes 監査を有効にします。
Answer: C (メーッセージを残す**)**
https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/access_control/open_policy_agent.html ステップ 2