PSE Prisma Pro Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which security measures are implemented in PSE Prisma Pro?

- **A. Encryption, access controls, and user authentication**
- **B. Open access without any controls**
- **C. Basic password protection only**
- **D. None, as it operates on public data**

2. What is the role of user permissions in PSE Prisma Pro?

- **A. They dictate the level of access and control users have over data and functionalities**
- **B. They allow unrestricted access to all users**
- **C. They are not utilized within PSE Prisma Pro**
- **D. They only apply to administrative users**

3. Which of the following is NOT a function of the AWS WAF?

- **A. Filtering incoming web traffic**
- **B. Monitoring user behavior**
- **C. Protecting against DDoS attacks**
- **D. Regulating API calls**

4. On which two options can Prisma Compute container defenders be installed?

- **A. Google Kubernetes Engine**
- **B. A Kubernetes DaemonSet**
- **C. Oracle Functions service**
- **D. Azure SQL database instances**

5. Which three anomaly policies are predefined in Prisma Cloud?

- **A. Unusual user activity, Excessive login failures, Suspicious file activity**
- **B. Excessive login failures, Account hijacking attempts, Denial-of-service activity**
- **C. Unusual user activity, Excessive login failures, Account hijacking attempts**
- **D. Account hijacking attempts, Suspicious file activity, Denial-of-service activity**

6. What is the primary purpose of PSE Prisma Pro?

- **A. To facilitate advanced business management and decision-making processes**
- **B. To provide a platform for social media management**
- **C. To create online learning environments**
- **D. To manage cloud storage solutions**

7. How does PSE Prisma Pro handle large datasets?

- **A. Through optimized processing and efficient data storage techniques**
- **B. By limiting data to small sample sizes**
- **C. With manual data entry processes**
- **D. Only using analytical tools outside of the software**

8. How does PSE Prisma Pro enhance data analysis capabilities?

- **A. By offering manual data entry forms**
- **B. Through advanced algorithms and machine learning tools**
- **C. By limiting data access to administrators only**
- **D. With basic spreadsheet functionalities**

9. In what way does PSE Prisma Pro assist in customer relationship management (CRM)?

- **A. By randomly selecting customer profiles for analysis**
- **B. By analyzing customer data to enhance engagement and support strategies**
- **C. By automating all customer service interactions**
- **D. By storing customer data in isolated systems**

10. What is necessary to completely trust images from a specific domain in a registry?

- **A. Trust all images without condition**
- **B. Specify a wildcard for the domain**
- **C. Include specific image tags**
- **D. Establish user credentials**

Answers

1. A
2. A
3. B
4. A
5. C
6. A
7. A
8. B
9. B
10. B

Explanations

1. Which security measures are implemented in PSE Prisma Pro?

A. Encryption, access controls, and user authentication

B. Open access without any controls

C. Basic password protection only

D. None, as it operates on public data

In PSE Prisma Pro, various security measures are implemented, which include encryption, access controls, and user authentication. Encryption is a crucial security mechanism that ensures data is transformed into a secure format that cannot be easily read or accessed by unauthorized users. This helps protect sensitive information throughout its lifecycle, whether at rest or in transit. Access controls dictate who can view or use specific resources within the system, ensuring that only authorized users have access to certain data or functionalities. This minimizes the risk of unauthorized access and potential data breaches. User authentication is the process of verifying the identity of users trying to access the system. This typically involves methods such as passwords, biometric scans, or two-factor authentication, which further bolster security by ensuring that only legitimate users can gain entry. Together, these measures create a robust security framework that is essential for protecting data integrity and confidentiality, particularly in environments that handle sensitive information. The other choices do not accurately represent the security posture of PSE Prisma Pro, as they suggest a lack of adequate security protocols.

2. What is the role of user permissions in PSE Prisma Pro?

A. They dictate the level of access and control users have over data and functionalities

B. They allow unrestricted access to all users

C. They are not utilized within PSE Prisma Pro

D. They only apply to administrative users

User permissions in PSE Prisma Pro serve a critical function by defining the level of access that different users have in relation to data and functionalities within the system. This means that depending on their assigned permissions, users may be restricted or granted specific rights to view, modify, or manage various elements of the application. This structured approach to permissions helps ensure that sensitive data is protected and that users only interact with the aspects of the application that are relevant to their roles or responsibilities. For example, a regular user may have insights into basic data, whereas an administrative user might possess the ability to alter settings, manage user accounts, or access detailed analytics. By controlling access through permissions, PSE Prisma Pro enhances security, maintains compliance with data protection regulations, and improves operational efficiency, making it an essential component of the system's overall management. This system of user permissions is fundamental for the effective governance of data and functionality within PSE Prisma Pro.

3. Which of the following is NOT a function of the AWS WAF?

A. Filtering incoming web traffic

B. Monitoring user behavior

C. Protecting against DDoS attacks

D. Regulating API calls

The AWS WAF (Web Application Firewall) is designed to help protect web applications by filtering and monitoring HTTP and HTTPS requests. Its primary functions include filtering incoming web traffic based on defined rules, protecting applications against common web exploits, and helping to manage specific types of threats, including DDoS attacks. The function of monitoring user behavior is not a direct capability of the AWS WAF. Instead, AWS WAF focuses more on the traffic itself rather than analyzing user behavior or patterns over time, which is typically handled by other AWS services or security solutions. The ability to filter incoming web traffic ensures only legitimate requests reach the application and can help block unwanted requests, while also providing the capability to protect against DDoS attacks by controlling traffic levels to the web application. Regulating API calls is another aspect that could be managed by other AWS services, but it's not a primary function of the AWS WAF itself. Thus, monitoring user behavior is distinct from the typical operational focus of AWS WAF.

4. On which two options can Prisma Compute container defenders be installed?

A. Google Kubernetes Engine

B. A Kubernetes DaemonSet

C. Oracle Functions service

D. Azure SQL database instances

Prisma Compute container defenders can be installed on Google Kubernetes Engine and a Kubernetes DaemonSet. Google Kubernetes Engine (GKE) is a managed environment for deploying containerized applications using Kubernetes. It provides robust support for container orchestration, scaling, and monitoring, making it a suitable platform for running container defenders that provide security functions. A Kubernetes DaemonSet is another valid option because it ensures that a copy of a specific pod runs on all or a subset of nodes in a Kubernetes cluster. This is particularly useful for deploying security agents across all nodes to monitor and protect container workloads consistently. The other options, such as Oracle Functions service and Azure SQL database instances, do not support the deployment of Prisma Compute container defenders because they aren't built for running containerized workloads in the same manner as Kubernetes environments. Oracle Functions is a serverless computing service, and Azure SQL database is a managed relational database service, which are not designed for container orchestration or running security agents like the defenders provided by Prisma.

5. Which three anomaly policies are predefined in Prisma Cloud?

A. Unusual user activity, Excessive login failures, Suspicious file activity

B. Excessive login failures, Account hijacking attempts, Denial-of-service activity

C. Unusual user activity, Excessive login failures, Account hijacking attempts

D. Account hijacking attempts, Suspicious file activity, Denial-of-service activity

The correct answer highlights three anomaly policies that are essential for monitoring and mitigating potential security threats within Prisma Cloud. Unusual user activity is a critical anomaly policy because it helps identify atypical behavior from users that could indicate compromised accounts or insider threats. Such deviations from normal usage patterns prompt security teams to investigate potential security incidents. Excessive login failures serve as another vital indicator. This policy flags instances where there are repeated failed attempts to access an account, which can point to brute force attacks or unauthorized access attempts. By detecting this early, organizations can take preventive measures to protect their resources. Account hijacking attempts are also a significant focus in the Prisma Cloud anomaly policies. Monitoring for signs of account hijacking ensures that any unusual access patterns leading to unauthorized usage of user accounts are identified and addressed promptly. These policies work together to create a robust security posture by ensuring that various angles of potential security threats are monitored, allowing organizations to respond promptly to incidents before they escalate.

6. What is the primary purpose of PSE Prisma Pro?

A. To facilitate advanced business management and decision-making processes

B. To provide a platform for social media management

C. To create online learning environments

D. To manage cloud storage solutions

The primary purpose of PSE Prisma Pro is to facilitate advanced business management and decision-making processes. This platform is specifically designed to enhance organizational performance by providing analytical tools and data visualization that assist businesses in making informed strategic decisions. These capabilities allow users to better analyze their operations, optimize resource allocation, and improve overall productivity. In contrast, options that reference social media management, online learning environments, or cloud storage solutions do not align with the core function of PSE Prisma Pro, as these areas focus on different aspects of technology and business. Instead, PSE Prisma Pro's emphasis lies in integrating data-driven insights into business practices to support complex decision-making and management strategies.

7. How does PSE Prisma Pro handle large datasets?

A. Through optimized processing and efficient data storage techniques

B. By limiting data to small sample sizes

C. With manual data entry processes

D. Only using analytical tools outside of the software

PSE Prisma Pro effectively manages large datasets by utilizing optimized processing and efficient data storage techniques. This approach allows the software to handle the complexities and volume associated with extensive data management. Optimized processing ensures that data can be processed faster and more efficiently, minimizing the demand on system resources while maximizing performance. Efficient data storage techniques help organize and store data in a way that allows for quick retrieval and analysis, making it feasible to work with larger datasets without encountering significant slowdowns or performance issues. This capability is essential for users who need to perform in-depth analyses or maintain large repositories of data, as it enhances the overall productivity and user experience within the platform.

8. How does PSE Prisma Pro enhance data analysis capabilities?

A. By offering manual data entry forms

B. Through advanced algorithms and machine learning tools

C. By limiting data access to administrators only

D. With basic spreadsheet functionalities

PSE Prisma Pro enhances data analysis capabilities primarily through advanced algorithms and machine learning tools. These technologies enable the software to process large datasets efficiently, identify patterns, and generate insights that would be challenging to uncover through traditional methods. The integration of machine learning allows for predictive analytics, which helps users make informed decisions based on data trends and behaviors rather than just looking at historical data. This capability is particularly beneficial for organizations seeking to optimize their operations, improve customer experiences, and drive strategic planning. The advanced algorithms also typically include features for data cleaning, transformation, and visualization, further amplifying analytical power and enabling users to derive actionable insights quickly and accurately. Other options, such as manual data entry forms or limiting access to administrators, do not contribute to enhancing data analysis capabilities and instead may hinder effective data management and usability. Similarly, basic spreadsheet functionalities lack the sophisticated analytical features that advanced algorithms and machine learning provide.

9. In what way does PSE Prisma Pro assist in customer relationship management (CRM)?

A. By randomly selecting customer profiles for analysis

B. By analyzing customer data to enhance engagement and support strategies

C. By automating all customer service interactions

D. By storing customer data in isolated systems

PSE Prisma Pro plays a critical role in customer relationship management (CRM) by analyzing customer data to enhance engagement and support strategies. This capability allows businesses to gain insights into customer behavior, preferences, and needs. By understanding this data, organizations can tailor their interactions with customers, personalize experiences, and improve overall service quality. When data is analyzed effectively, it can inform strategies that lead to better customer satisfaction and loyalty. For instance, businesses can identify patterns that indicate when a customer might need more support or what products they might be interested in, allowing for proactive engagement rather than reactive response. This analysis fosters a deeper connection between the company and its customers, ultimately leading to improved retention and positive word-of-mouth. This approach stands in contrast to simply selecting customer profiles randomly, automating all interactions without a personalized touch, or storing customer data in isolated systems, which limit the ability to analyze and utilize that data effectively. Each of these alternatives would not yield the same level of actionable insights or enhance customer engagement in the way that thorough data analysis does.

10. What is necessary to completely trust images from a specific domain in a registry?

A. Trust all images without condition

B. Specify a wildcard for the domain

C. Include specific image tags

D. Establish user credentials

To completely trust images from a specific domain in a registry, specifying a wildcard for the domain is essential because it allows for broader trust across multiple images that belong to that domain. A wildcard permits trust for not just a single image, but for any images that match the pattern established by the wildcard. This is especially useful in environments where multiple related images are often pulled from the same domain, streamlining the trust process with a single configuration. By using a wildcard, the system can automatically apply trust settings to all images within the specified domain without the need to individually categorize or tag each image. This ensures that as new images are added to the domain, they will also be trusted, maintaining security and efficiency in the deployment pipeline. On the other hand, simply trusting all images without condition would pose security risks, as it could allow malicious images to be executed. Including specific image tags can create more granularity and control but requires ongoing management to keep track of what images are being trusted. Establishing user credentials is an important step for authentication and governance but doesn't directly address the issue of trust related specifically to images from a domain.