PSE Cortex Professional Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. In what way can anomaly detection algorithms benefit a business using PSE Cortex?

A. By increasing data governance practices

B. By providing real-time notifications of abnormal behaviors

C. By improving data processing speeds

D. By minimizing stakeholder involvement

2. What allows the use of predefined roles to assign access rights to Cortex XDR users?

A. Restrictions security profile

B. Cloud Identity Engine

C. Endpoint Groups

D. Role-based Access Control (RBAC)

3. When configuring Cortex XDR logging, which log type is crucial for monitoring multiple endpoint events?

A. Authentication logs

B. System logs

C. Analytic logs

D. Threat logs

4. How does the PSE Cortex enable real-time data processing?

A. By running scheduled batch jobs at night

B. By utilizing stream processing frameworks and tools

C. By storing data in a Hadoop ecosystem

D. By compressing data for faster transmission

5. Which task setting allows context output to a specific key?

A. Extend context.

B. Task output.

C. Stop on errors.

D. Tags.

6. A General Purpose Dynamic Section can be added to which two layouts for incident types?

A. "Close" Incident Form

B. Incident Summary

C. Incident Quick View

D. "New/Edit" Incident Form

7. What should a Cortex XDR Pro administrator do to confirm false positives in a suspicious process creation security event?

A. Contact support and ask for a security exception.

B. In the Cortex XDR security event, review the specific parent process, child process, and command line arguments.

C. Add the specific parent process, child process, and command line argument to the whitelist.

D. Disable the Prevent Malicious Child Process Execution module.

8. Why is continuous learning important in deploying machine learning models with PSE Cortex?

A. It decreases model accuracy over time

B. It ensures models adapt to new data and improve predictions

C. It minimizes the need for user input

D. It simplifies the deployment process

9. What is the significance of API management in PSE Cortex?

A. It helps in data backup and recovery

B. It allows seamless integration of external applications and services

C. It monitors data traffic volume

D. It enhances user interface design capabilities

10. Which service helps uncover attackers wherever they hide by combining world-class threat hunters with Cortex XDR technology?

A. Cloud Identity Engine (CIE)

B. Threat Intelligence Platform (TIP)

C. Virtual Desktop Infrastructure (VDI)

D. Managed Threat Hunting (MTH)

Answers

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

Explanations

1. In what way can anomaly detection algorithms benefit a business using PSE Cortex?

A. By increasing data governance practices

B. By providing real-time notifications of abnormal behaviors

C. By improving data processing speeds

D. By minimizing stakeholder involvement

Anomaly detection algorithms are particularly beneficial for businesses because they enable the identification of unusual patterns or behaviors in data. By providing real-time notifications of these abnormalities, organizations can quickly respond to potential issues, whether they be operational inefficiencies, security threats, or undesirable changes in customer behavior. This proactive approach allows businesses to mitigate risks effectively and make informed decisions based on timely insights. In contrast, while improving data governance practices is important, it doesn't directly result from anomaly detection algorithms. Similarly, while data processing speeds might enhance performance, anomaly detection focuses primarily on identifying irregularities rather than accelerating processing. Minimizing stakeholder involvement is contrary to the purpose of engaging relevant parties during anomaly investigations, as their insights can be crucial in understanding the context of detected anomalies. Thus, the real-time notification capability is the standout advantage provided by anomaly detection within the PSE Cortex framework.

2. What allows the use of predefined roles to assign access rights to Cortex XDR users?

A. Restrictions security profile

B. Cloud Identity Engine

C. Endpoint Groups

D. Role-based Access Control (RBAC)

The use of predefined roles to assign access rights to Cortex XDR users is supported by Role-based Access Control (RBAC). RBAC is a crucial security feature that simplifies the management of user permissions by associating them with roles rather than individual users. Each role is defined with specific permission levels, which allows administrators to efficiently control access across various functionalities within the system. Assigning predefined roles enables organizations to implement a principle of least privilege, ensuring that users have no more access than necessary for their job functions. This structured approach not only enhances security by minimizing the risk of unauthorized access but also streamlines user management, as roles can be easily adjusted or updated without needing to change permissions for each individual user. In contrast, other options like the Restrictions security profile, Cloud Identity Engine, and Endpoint Groups play different roles in the security landscape but do not specifically cater to the assignment of access rights through predefined roles in the same way that RBAC does.

3. When configuring Cortex XDR logging, which log type is crucial for monitoring multiple endpoint events?

A. Authentication logs

B. System logs

C. Analytic logs

D. Threat logs

Analytic logs are essential for monitoring multiple endpoint events because they provide insights into the behavior and performance of endpoints across the network. They aggregate data from various sources, allowing security teams to analyze patterns, identify anomalies, and correlate events that occur on different endpoints. This comprehensive view is crucial for detecting potential threats and understanding the broader context of endpoint activity. Unlike authentication logs, which focus primarily on user access and identity verification, or system logs that capture general operating system events, analytic logs synthesize information from various events to give a more holistic understanding of endpoint interactions. Threat logs specifically deal with detected threats and incidents, but they do not provide the breadth of analysis that analytic logs offer in terms of user behavior and endpoint performance over time. Thus, for a thorough monitoring approach, analytic logs play a pivotal role.

4. How does the PSE Cortex enable real-time data processing?

A. By running scheduled batch jobs at night

B. By utilizing stream processing frameworks and tools

C. By storing data in a Hadoop ecosystem

D. By compressing data for faster transmission

The PSE Cortex enables real-time data processing primarily by utilizing stream processing frameworks and tools. This approach allows the system to ingest and process data continuously, handling data streams in real time as they arrive, rather than relying on delayed processing methods. Stream processing is crucial for scenarios where immediate insights and actions are necessary, such as monitoring events, detecting anomalies, or reacting to changes in data as they happen. By leveraging frameworks designed for stream processing, the PSE Cortex can efficiently manage high-velocity data flows, ensuring that computations and analyses occur instantaneously. This capability leads to more agile decision-making and responsive applications, essential for businesses that need up-to-the-minute information. In contrast, running scheduled batch jobs limits data processing to specific times and delays insights until after batches are complete. Storing data in a Hadoop ecosystem focuses on processing large volumes of data in batch mode, which is not suitable for real-time applications. Compression of data for faster transmission can enhance speed but does not inherently provide the continuous processing capability required for real-time data analysis. Therefore, the choice that correctly identifies the PSE Cortex's method for real-time data processing is the one that highlights its reliance on stream processing frameworks and tools.

5. Which task setting allows context output to a specific key?

A. Extend context.

B. Task output.

C. Stop on errors.

D. Tags.

In the context of task settings, extending context typically refers to the capability to modify or add additional information to a context object, which is often structured as key-value pairs. When you extend context, you can specify which key you want to output data to, enabling precise control over how data is stored and referenced for subsequent tasks or actions within a workflow. This is particularly useful when you want to maintain organized and accessible data, as it allows different parts of your process to share and use relevant context information seamlessly. In contrast, task output generally refers to the result generated by a specific task but does not imply the ability to selectively assign this result to a specific context key. Stop on errors focuses on error handling strategies and doesn't involve the manipulation of context data. Tags are often used to categorize or label information but do not facilitate the specific output of context values to keys. Thus, extending context is the most suitable choice for directing output to a specific key within the context data structure.

6. A General Purpose Dynamic Section can be added to which two layouts for incident types?

A. "Close" Incident Form

B. Incident Summary

C. Incident Quick View

D. "New/Edit" Incident Form

The correct choice is that a General Purpose Dynamic Section can be added to the Incident Summary layout. This selection is based on the functionality and purpose of Dynamic Sections within the context of incident management. A General Purpose Dynamic Section is designed to display varying fields and data depending on the context of the incident. The Incident Summary layout serves as an overview of the incident details, making it suitable for dynamic sections which can adapt to showcase different information based on the situation or specific incident configurations. In contrast, other layouts like the "Close" Incident Form, Incident Quick View, and "New/Edit" Incident Form have more defined purposes that typically do not accommodate the flexible nature of Dynamic Sections as effectively. The "Close" form is focused on finalizing incidents rather than displaying variable information, while the Quick View aims for quick access to essential information without the complexity of dynamic data updates. The "New/Edit" form is also structured to standardize the input process, which limits the ability to incorporate dynamically changing data fields.

7. What should a Cortex XDR Pro administrator do to confirm false positives in a suspicious process creation security event?

A. Contact support and ask for a security exception.

B. In the Cortex XDR security event, review the specific parent process, child process, and command line arguments.

C. Add the specific parent process, child process, and command line argument to the whitelist.

D. Disable the Prevent Malicious Child Process Execution module.

A Cortex XDR Pro administrator should review the specific parent process, child process, and command line arguments to confirm false positives in a suspicious process creation security event. This step is essential because analyzing these details provides context around the event, allowing the administrator to better understand the nature of the process in question. For instance, examining the command line arguments can reveal whether the process was initiated with parameters that indicate it is benign or malicious. The relationship between the parent and child processes is also critical; a legitimate application may create child processes, but an unknown or suspicious parent process might indicate malicious intent. By gathering this specific information, the administrator can make an informed judgment on whether the event is a true threat or a false positive, ensuring that security measures are accurately applied and potential disruptions to legitimate processes are minimized.

8. Why is continuous learning important in deploying machine learning models with PSE Cortex?

A. It decreases model accuracy over time

B. It ensures models adapt to new data and improve predictions

C. It minimizes the need for user input

D. It simplifies the deployment process

Continuous learning is crucial in deploying machine learning models with PSE Cortex because it enables models to adapt to new data and improve predictions over time. As data distributions can shift due to various factors, such as changes in user behavior, market dynamics, or external influences, models can become less effective if they are not updated with new information. By incorporating continuous learning, the model can adjust its parameters and learn from fresh data inputs, ensuring that it remains relevant and accurate in its predictions. This adaptive learning process helps maintain the model's performance, reduces the risk of obsolescence, and ultimately enhances decision-making processes in real-time applications. Continuous learning supports ongoing enhancement, allowing businesses to leverage the most current insights from their data, leading to better outcomes and informed strategies.

9. What is the significance of API management in PSE Cortex?

A. It helps in data backup and recovery

B. It allows seamless integration of external applications and services

C. It monitors data traffic volume

D. It enhances user interface design capabilities

API management plays a crucial role in PSE Cortex by facilitating the seamless integration of external applications and services. This is significant because it enables organizations to connect various software systems, allowing them to communicate and work together efficiently. With effective API management, developers can create, publish, and oversee APIs, ensuring that different components of the system can interact securely and efficiently. This integration capability is essential for building a cohesive ecosystem where data and functionality can flow freely between different platforms. It enables organizations to leverage existing tools and services while also adding new functionalities, ultimately enhancing operational efficiency, innovation, and responsiveness to business needs. The ability to integrate diverse systems is foundational in fostering collaboration and maintaining agility in evolving technological environments.

10. Which service helps uncover attackers wherever they hide by combining world-class threat hunters with Cortex XDR technology?

A. Cloud Identity Engine (CIE)

B. Threat Intelligence Platform (TIP)

C. Virtual Desktop Infrastructure (VDI)

D. Managed Threat Hunting (MTH)

The service that effectively uncovers attackers wherever they hide is Managed Threat Hunting (MTH). This service leverages a combination of skilled threat hunters and Cortex XDR technology to proactively search for threats across an organization's environment. Managed Threat Hunting provides organizations with advanced detection capabilities that go beyond traditional security measures. By employing expert threat hunters who analyze potential risks and weaknesses, MTH enhances the security posture by identifying and responding to threats that may not be detected by standard automated systems. Cortex XDR plays a crucial role in this service by providing a comprehensive, integrated detection and response platform that combines data from various sources, such as endpoints, networks, and cloud environments. This combination allows for a more holistic view of the threat landscape, enabling threat hunters to spot anomalies and sophisticated attacker behaviors that could indicate a breach. In contrast, services like the Cloud Identity Engine focus primarily on identity and access management, while the Threat Intelligence Platform is designed to aggregate threat data but does not directly involve active hunting. Virtual Desktop Infrastructure is related to providing desktop environments over the internet and does not have a direct connection to threat detection methodologies. Thus, Managed Threat Hunting stands out as the service explicitly designed for uncovering attackers using a proactive approach.