200 XP

Knowledge check - Design solutions for security posture management in hybrid and multicloud environments

5 minutes

1. What is the purpose of Cloud Security Posture Management (CSPM)? *

- ○ To provide a comprehensive vulnerability assessment of all resources in the cloud environment.
- ○ To facilitate secure communication between hybrid and multicloud environments.
- ◉ To enable users to prevent and respond to threats, automate compliance requirements, and assess the security posture of their cloud environment.

✔ **CSPM helps users ensure their cloud environment is secure by assessing, identifying, preventing and responding to threats or vulnerabilities that could compromise it. Additionally, it automates compliance tasks and monitors security configuration across all cloud resources or services.**

- ○ To provide endpoint protection against advanced attacks.

2. What is Cloud Workload Protection in Microsoft Defender for Cloud? *

- ○ A feature that provides external attack surface management.
- ○ A feature that automates vulnerability assessments and compliance checks.
- ◉ A feature that surfaces workload-specific recommendations that lead you to the right security controls to protect your workloads.

✔ **Workload protection is designed specifically for addressing threats targeting cloud workloads such as applications or containers.**

- ○ A feature that provides security controls for DevOps teams and their CI/CD pipelines.

3. What is Azure Arc used for? *

- ○ To automatically scale compute resources in cloud environments.
- ○ To monitor network traffic and detect anomalies in cloud environments.
- ◉ To extend Azure management capabilities and tools to manage resources running outside of Azure datacenters.

✔ **Azure Arc enables enterprises to manage their infrastructure centrally from Azure portal, including servers, Kubernetes clusters, and applications running in distributed environments.**

- ○ To perform virtual machine backups and disaster recovery for cloud environments.

4. What is external attack surface management? *

- ○ A feature that secures data stored on public cloud services.
- ○ A feature that provides endpoint threat detection and response for cloud-connected devices.
- ○ An umbrella term used to describe tactics used by hackers to gain access to an organization's assets through external-facing entry points such as web applications, APIs, and remote offices.
- ◉ A feature that correlates information from various sources to provide a single view of the organization's security posture related to external attack surfaces.

✔ **External attack surface management allows organizations to have a unified view of their external assets so they can detect risks at the earliest possible time. The feature correlates information from various sources, including intelligence feeds, third-party tools, and internal organizational information to provide a complete view on external attack surface risk levels.**

Next unit: Summary - Design solutions for security posture management in hybrid and multicloud environments

Continue >