solution to prevent users from accessing websites that contain adult content such as gambling sites. What should you include in the recommendation?

A. Microsoft Endpoint Manager
B. Compliance Manager
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Endpoint

Correct Answer: D

QUESTION 29
Your company is moving a big data solution to Azure.

The company plans to use the following storage workloads:

▪ Azure Storage blob containers
▪ Azure Data Lake Storage Gen2
▪ Azure Storage file shares
▪ Azure Disk Storage

Which two storage workloads support authentication by using Azure Active Directory (Azure AD)?

Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Disk Storage
B. Azure Storage blob containers
C. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Correct Answer: BD

QUESTION 30
You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers. In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Registry
B. Linux containers deployed to Azure Kubernetes Service (AKS)
C. Windows containers deployed to Azure Container Registry
D. Windows containers deployed to Azure Kubernetes Service (AKS)
E. Linux containers deployed to Azure Container Instances

Correct Answer: AB

QUESTION 31
Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool.
Which type of diagram should you create?

A. data flow
B. system flow
C. process flow
D. network flow

Correct Answer: A

QUESTION 32
You have a Microsoft 365 E5 subscription.

You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.

You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.

Which two components should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data loss prevention (DLP) policies
B. sensitivity label policies
C. retention label policies
D. eDiscovery cases

Correct Answer: AB

QUESTION 33
Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. Azure SQL Managed Instance
B. Azure Synapse Analytics dedicated SQL pools
C. Azure SQL Database
D. SQL Server on Azure Virtual Machines

Correct Answer: A

QUESTION 34
Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.

The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.

Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.

You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers.

Which three actions should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Implement Azure Firewall to restrict host pool outbound access.
C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
E. Deploy a Remote Desktop server to an Azure region located in France.

Correct Answer: BCD

QUESTION 35
Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.

You receive the following recommendations in Defender for Cloud

▪ Access to storage accounts with firewall and virtual network configurations should be restricted,
▪ Storage accounts should restrict network access using virtual network rules.
▪ Storage account should use a private link connection.
▪ Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations. What should you recommend?

A. Azure Storage Analytics
B. Azure Network Watcher
C. Microsoft Sentinel
D. Azure Policy

Correct Answer: D

QUESTION 36
You have Microsoft Defender for Cloud assigned to Azure management groups.

You have a Microsoft Sentinel deployment.

During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. workload protections in Defender for Cloud
B. threat intelligence reports in Defender for Cloud
C. Microsoft Sentinel notebooks
D. Microsoft Sentinel threat intelligence workbooks

Correct Answer: BD

QUESTION 37
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.

The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.

You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:

▪ Prevent the remote users from accessing any other resources on the network.
▪ Support Azure Active Directory (Azure AD) Conditional Access.
▪ Simplify the end-user experience.

What should you include in the recommendation?

A. Azure AD Application Proxy
B. Azure Virtual WAN
C. Microsoft Tunnel
D. web content filtering in Microsoft Defender for Endpoint

Correct Answer: A

QUESTION 38
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling adaptive network hardening.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A

QUESTION 39
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.

All the on-premises servers in the perimeter network are prevented from connecting directly to the internet.

The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

▪ Ensure that the security operations team can access the security logs and the operation logs.
▪ Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.

Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A.   Azure Active Directory (Azure AD) Conditional Access policies
B.   a custom collector that uses the Log Analytics agent
C.   resource-based role-based access control (RBAC)
D.   the Azure Monitor agent

Correct Answer: BC

QUESTION 40
Your company has a Microsoft 365 E5 subscription. Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

A.   insider risk management policies
B.   data loss prevention (DLP) policies
C.   sensitivity label policies
D.   retention policies
Correct Answer: B

QUESTION 41
You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:

▪ Encrypt cardholder data by using encryption keys managed by the company.
▪ Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A.   Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
B.   Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM