QUESTION 170
You are designing a ransomware response plan that follows Microsoft Security Best Practices.
You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.
What should you include in the recommendation?

A. Windows Defender Device Guard
B. Microsoft Defender for Endpoint
C. Azure Files
D. BitLocker Drive Encryption (BitLocker)
E. protected folders

Answer: E
Explanation:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide

QUESTION 171
You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.
You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.
You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.
What should you recommend?

A. a managed identity in Azure
B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)
C. a group managed service account (gMSA)
D. an Azure AD user account that has a password stored in Azure Key Vault

Answer: A
Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

QUESTION 172
You have an Azure Kubernetes Service (AKS) cluster that hosts Linux nodes.
You need to recommend a solution to ensure that deployed worker nodes have the latest kernel updates. The solution must minimize administrative effort.
What should you recommend?

A. The nodes must restart after the updates are applied.
B. The updates must first be applied to the image used to provision the nodes.

C. The AKS cluster version must be upgraded.

Answer: B

QUESTION 173
You have the following on-premises servers that run Windows Server:
- Two domain controllers in an Active Directory Domain Services (AD DS) domain
- Two application servers named Server1 and Server2 that run ASP.NET web apps
- A VPN server named Served that authenticates by using RADIUS and AD DS

End users use a VPN to access the web apps over the internet.
You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).
What should you include in the recommendation?

A. Publish the web apps by using Azure AD Application Proxy.
B. Configure the VPN to use Azure AD authentication.
C. Configure connectors and rules in Microsoft Defender for Cloud Apps.
D. Configure web protection in Microsoft Defender for Endpoint.

Answer: A

QUESTION 174
You are designing a security operations strategy based on the Zero Trust framework.
You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts.
What should you do?

A. Enable built-in compliance policies in Azure Policy.
B. Enable self-healing in Microsoft 365 Defender.
C. Automate data classification.
D. Create hunting queries in Microsoft 365 Defender.

Answer: B
Explanation:
https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/self-healing-in-microsoft-365-defender/ba-p/1729527

QUESTION 175
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You need to enforce ISO 27001:2013 standards for new resources deployed to the subscription. The solution must ensure that noncompliant resources are automatically detected.
What should you use?

A. Azure Blueprints
B. the regulatory compliance dashboard in Defender for Cloud
C. Azure Policy
D. Azure role-based access control (Azure RBAC)

Answer: C

QUESTION 176
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an

unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps
B. Azure Security Benchmark compliance controls in Defender for Cloud
C. app registrations in Azure AD
D. application control policies in Microsoft Defender for Endpoint

Answer: D

QUESTION 177
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

A. From Defender for Cloud, add a regulatory compliance standard.
B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.
C. From Defender for Cloud, review the Azure security baseline for audit report.
D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Answer: A

QUESTION 178
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. app registrations in Azure AD
B. Azure AD Conditional Access App Control policies
C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps
D. adaptive application controls in Defender for Cloud

Answer: D

QUESTION 179
You have a customer that has a Microsoft 365 subscription and an Azure subscription.
The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules.
What should you include in the solution?

A. Microsoft Sentinel
B. Microsoft Purview Information Protection
C. Microsoft Intune
D. Microsoft Defender for Endpoint

Answer: D

QUESTION 180

You have an on-premises datacenter and an Azure Kubernetes Service (AKS) cluster named AKS1.
You need to restrict internet access to the public endpoint of AKS1. The solution must ensure that AKS1 can be accessed only from the public IP addresses associated with the on-premises datacenter.
What should you use?

A. a private endpoint
B. a network security group (NSG)
C. a service endpoint
D. an authorized IP range

Answer: D
Explanation:
https://learn.microsoft.com/en-us/azure/aks/limit-egress-traffic

QUESTION 181
You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux.
You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:
- Identify missing updates and insecure configurations.
- Use the Qualys engine.
What should you use?

A. Microsoft Defender for Servers
B. Microsoft Defender Threat Intelligence (Defender TI)
C. Microsoft Defender for Endpoint
D. Microsoft Defender External Attack Surface Management (Defender EASM)

Answer: A
Explanation:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-enable-servers-plan

QUESTION 182
You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials.
You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials.
What should you include in the recommendation?

A. Azure AD Application Proxy
B. Azure AD B2C
C. an Azure AD enterprise application
D. a relying party trust in Active Directory Federation Services (AD FS)

Answer: A
Explanation:
To enable users to authenticate to App1 by using their Azure AD credentials, you should include an Azure AD enterprise application in your recommendation. An Azure AD enterprise application is an instance of an application that is integrated with Azure AD. You can add App1 as an enterprise application in your Azure AD tenant and configure it to support single sign-on (SSO) using Azure AD. This will allow users to authenticate to App1 using their Azure AD credentials.
https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal

QUESTION 183
You have a Microsoft 365 tenant.
Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant.

You need to design a security strategy to meet the following requirements:
- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1.
What should you include in the design?

A. Microsoft Entra Identity Governance
B. connected apps in Microsoft Defender for Cloud Apps
C. access policies in Microsoft Defender for Cloud Apps
D. Azure AD Application Proxy

Answer: A
Explanation:
Microsoft Entra Identity Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.
https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview

QUESTION 184
You have an Azure subscription.
You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar.
Developers use Azure DevOps to deploy web apps to App Service Environments. When a new app is deployed, a CNAME record for the app is registered in contoso.com.
You need to recommend a solution to secure the DNS record for each web app. The solution must meet the following requirements:
- Ensure that when an app is deleted, the CNAME record for the app is removed also.
- Minimize administrative effort.
What should you include in the recommendation?

A. Microsoft Defender for Cloud Apps
B. Microsoft Defender for DevOps
C. Microsoft Defender for App Service
D. Microsoft Defender for DNS

Answer: C
Explanation:
Defender for App Service identifies any DNS entries remaining in your DNS registrar when an App Service website is decommissioned - these are known as dangling DNS entries.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction#dangling-dns-detection
Microsoft Defender for DNS provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction#dangling-dns-detection

QUESTION 185
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Purview, SharePoint Online, and OneDrive for Business.
You need to recommend a ransomware protection solution that meets the following requirements:
- Mitigates attacks that make copies of files, encrypt the copies, and then delete the original files
- Mitigates attacks that encrypt files in place
- Minimizes administrative effort
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use:

- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

To mitigate attacks that encrypt files in place, use:

- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

Answer:

Answer Area

To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use:

- Data loss prevention (DLP) policies
- **The Recycle Bin**
- Versioning

To mitigate attacks that encrypt files in place, use:

- Data loss prevention (DLP) policies
- The Recycle Bin
- **Versioning**

Explanation:
https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection