SC-100$^{Q\&As}$

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

QUESTION 1

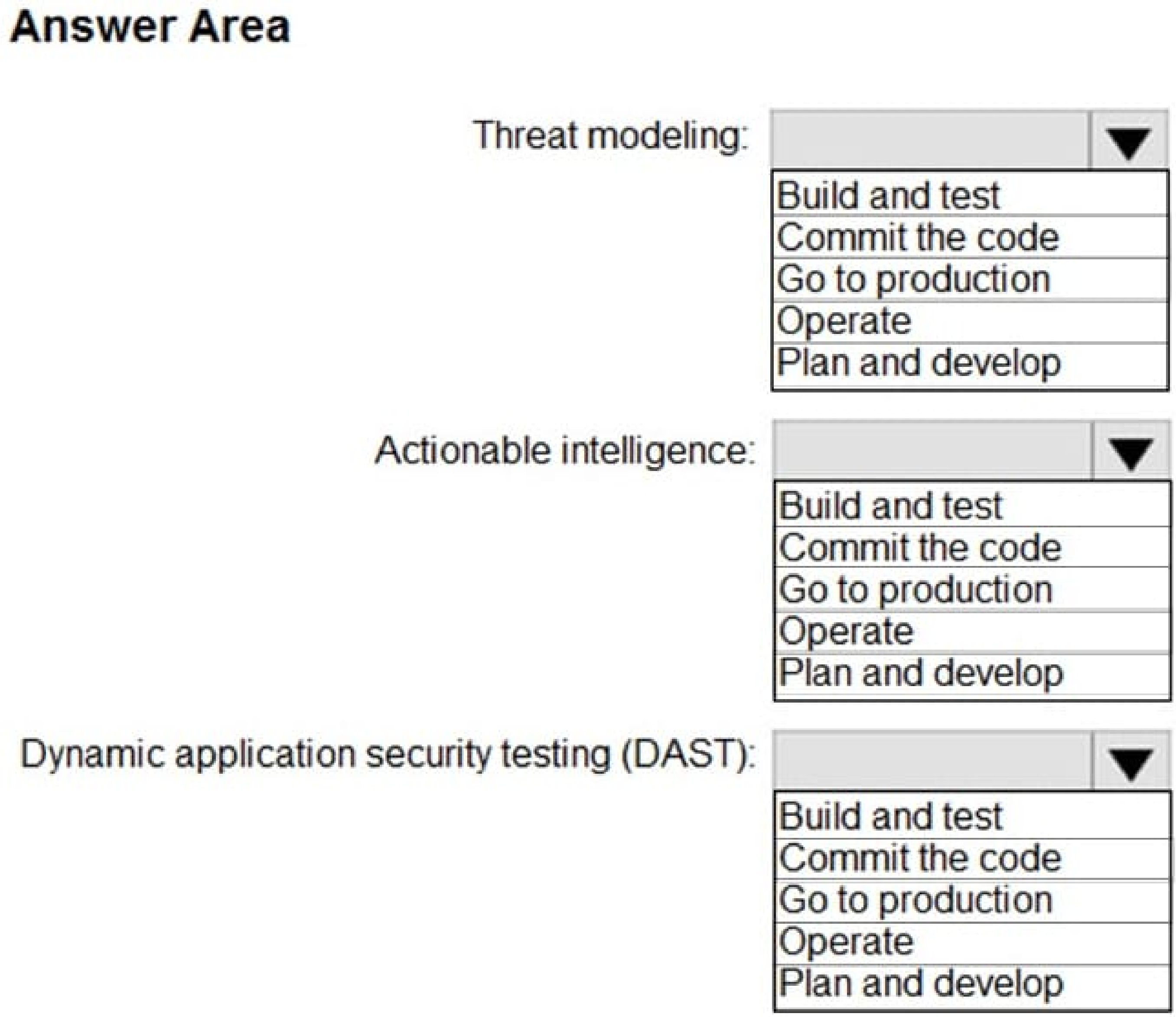
HOTSPOT

You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure.

During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Threat modeling:

- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

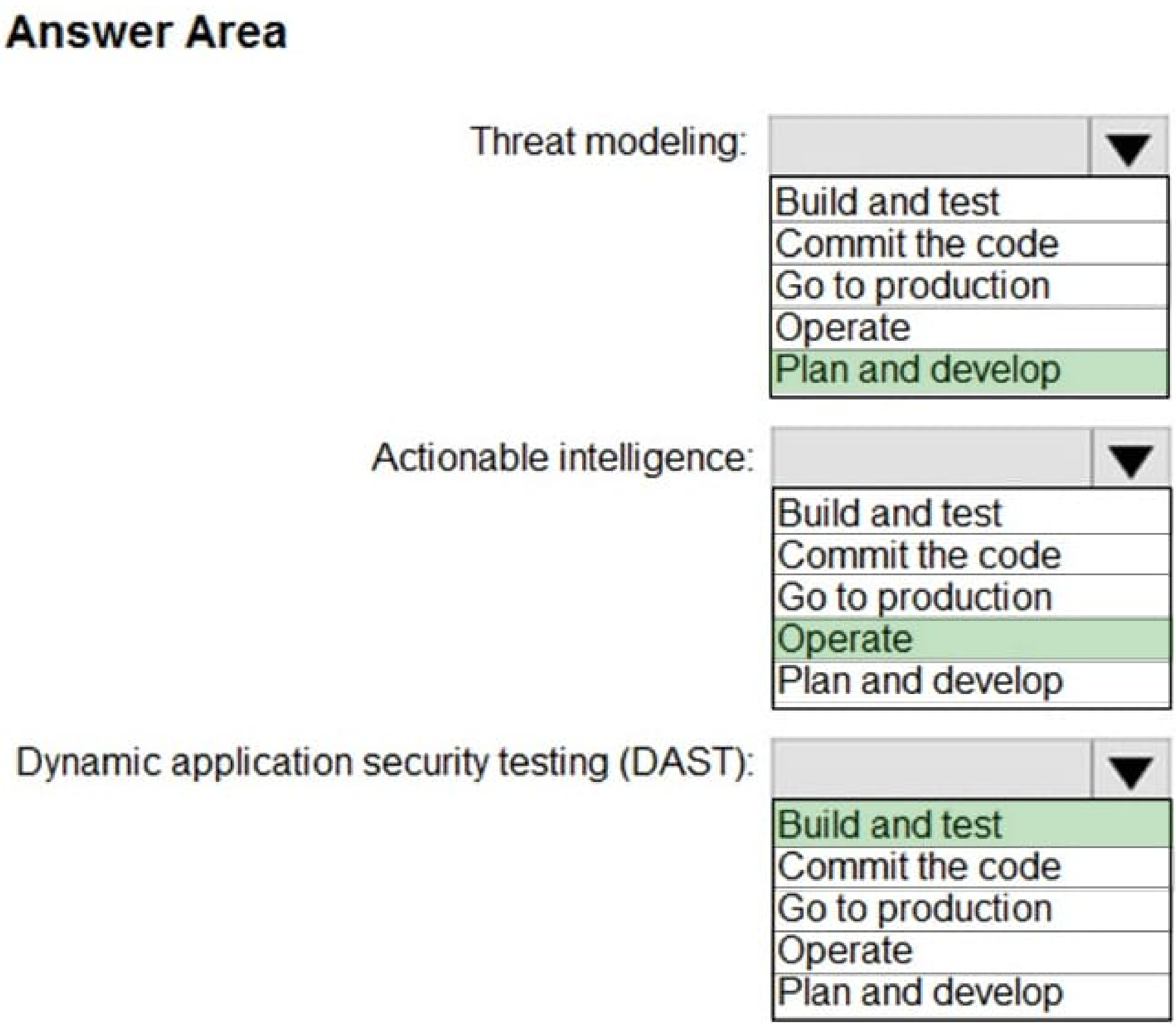
Actionable intelligence:

- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

Dynamic application security testing (DAST):

- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

Correct Answer:



Answer Area

Threat modeling: ▼

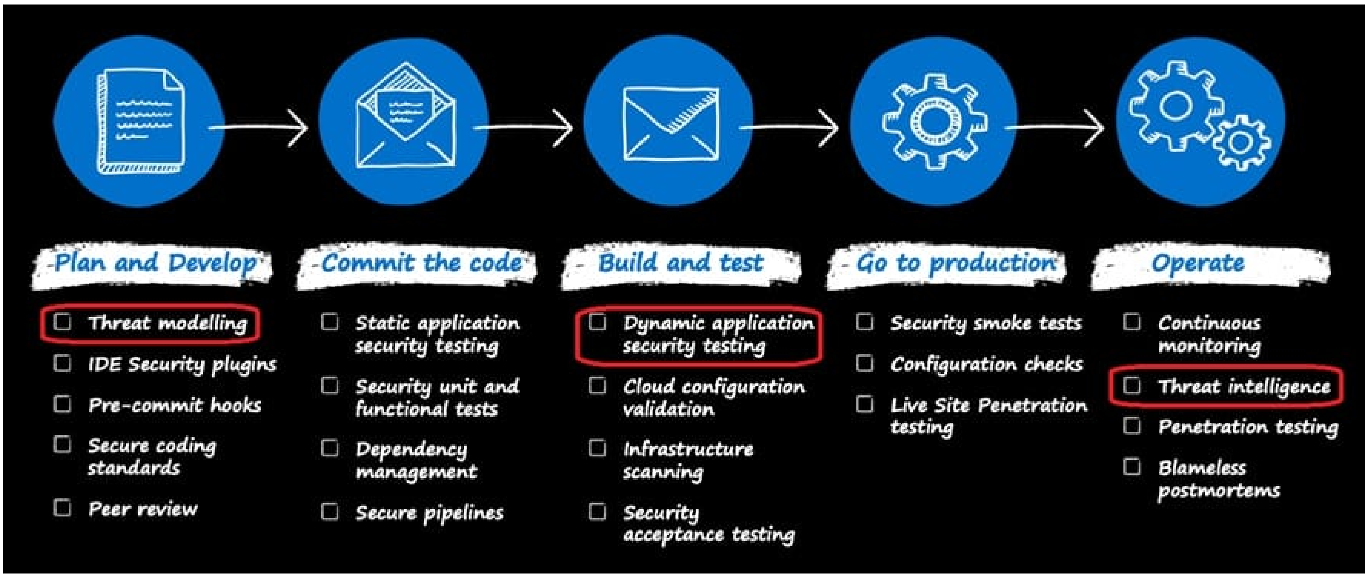
- Build and test
- Commit the code
- Go to production
- Operate
- [✓ Plan and develop]

Actionable intelligence: ▼

- Build and test
- Commit the code
- Go to production
- [✓ Operate]
- Plan and develop

Dynamic application security testing (DAST): ▼

- [✓ Build and test]
- Commit the code
- Go to production
- Operate
- Plan and develop



Plan and develop

Box 1: Plan and develop

Typically, modern development follows an agile development methodology. Scrum is one implementation of agile methodology that has every sprint start with a planning activity. Introducing security into this part of the development process should focus on:

*

Threat modeling to view the application through the lens of a potential attacker

*

IDE security plug-ins and pre-commit hooks for lightweight static analysis checking within an integrated development environment (IDE).

*

Peer reviews and secure coding standards to identify effective security coding standards, peer review processes, and pre-commit hooks. It\\'s not mandatory to add all these steps. But each step helps reveal security issues early, when they\\'re much cheaper and easier to fix.

Box 2: Operate

Go to production and operate

When the solution goes to production, it\\'s vital to continue overseeing and managing the security state. At this stage in the process, it\\'s time to focus on the cloud infrastructure and overall application.

Configuration and infrastructure scanning

Penetration testing

Actionable intelligence

The tools and techniques in this guidance offer a holistic security model for organizations who want to move at pace and experiment with new technologies that aim to drive innovation. A key element of DevSecOps is data-driven, event-driven

processes. These processes help teams identify, evaluate, and respond to potential risks. Many organizations choose to integrate alerts and usage data into their IT service management (ITSM) platform. The team can then bring the same

structured workflow to security events that they use for other incidents and requests.

Box 3: Build and test

Build and test

Many organizations use build and release pipelines to automate and standardize the processes for building and deploying code. Release pipelines let development teams make iterative changes to sections of code quickly and at scale. The

teams won\\'t need to spend large amounts of time redeploying or upgrading existing environments.

Using release pipelines also lets teams promote code from development environments, through testing environments, and ultimately into production. As part of automation, development teams should include security tools that run scripted, automated tests when deploying code into testing environments. The tests should include unit testing on application features to check for vulnerabilities or public endpoints. Testing ensures intentional access.

Dynamic application security testing (DAST)

In a classical waterfall development model, security was typically introduced at the last step, right before going to production. One of the most popular security approaches is penetration testing or pen testing. Penetration testing lets a team

look at the application from a black-box security perspective, as in, closest to an attacker mindset.

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-devops-security

QUESTION 2

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions.

You are evaluating the security posture of the customer.

You discover that the AKS resources are excluded from the secure score recommendations.

You need to produce accurate recommendations and update the secure score.

Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable Defender plans.

B. Configure auto provisioning.

C. Add a workflow automation.

D. Assign regulatory compliance policies.

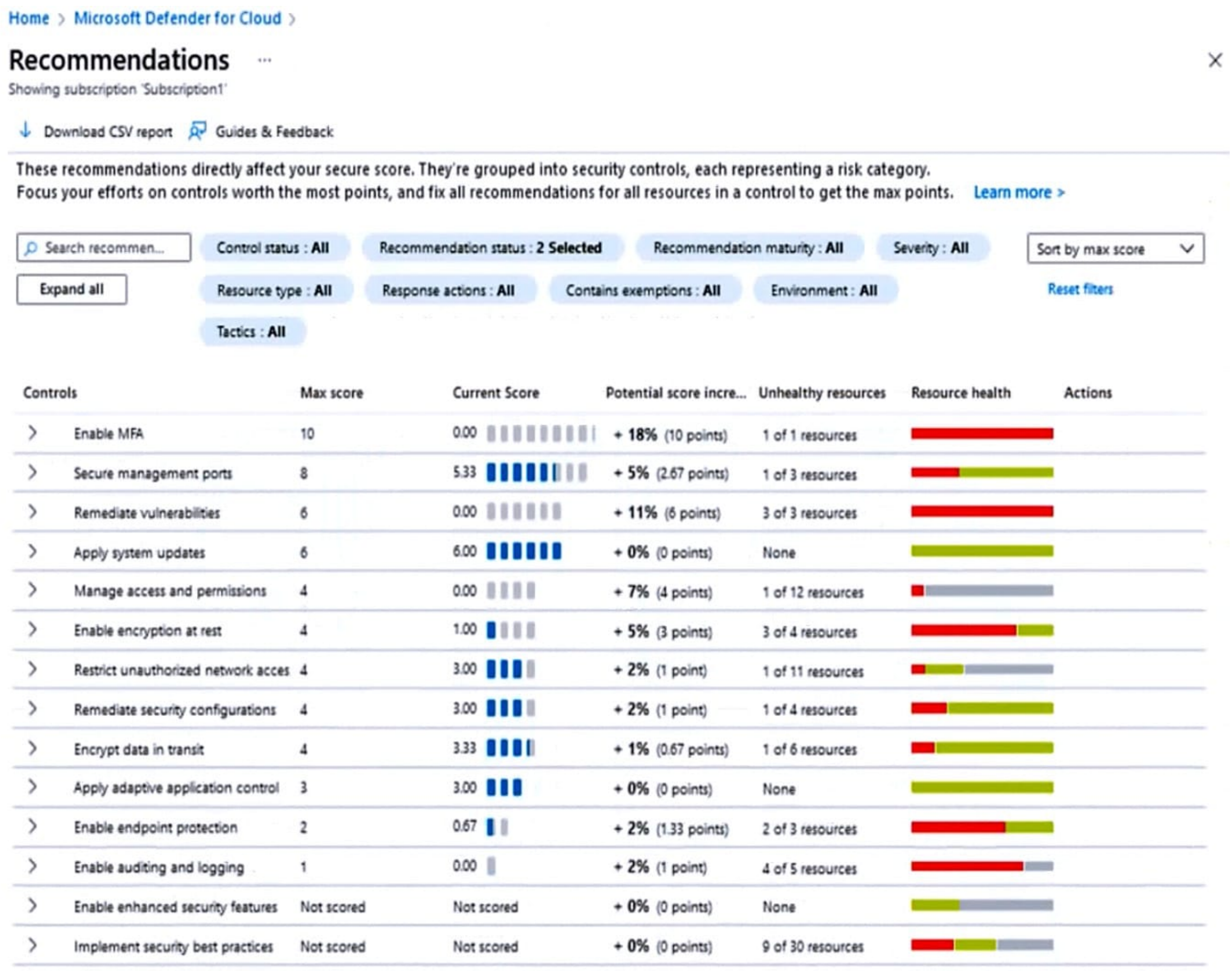
E. Review the inventory.

Correct Answer: AB

QUESTION 3

HOTSPOT

You open Microsoft Defender for Cloud as shown in the following exhibit.



Home > Microsoft Defender for Cloud >

Recommendations

Showing subscription 'Subscription1'

These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category.
Focus your efforts on controls worth the most points, and fix all recommendations for all resources in a control to get the max points. Learn more >

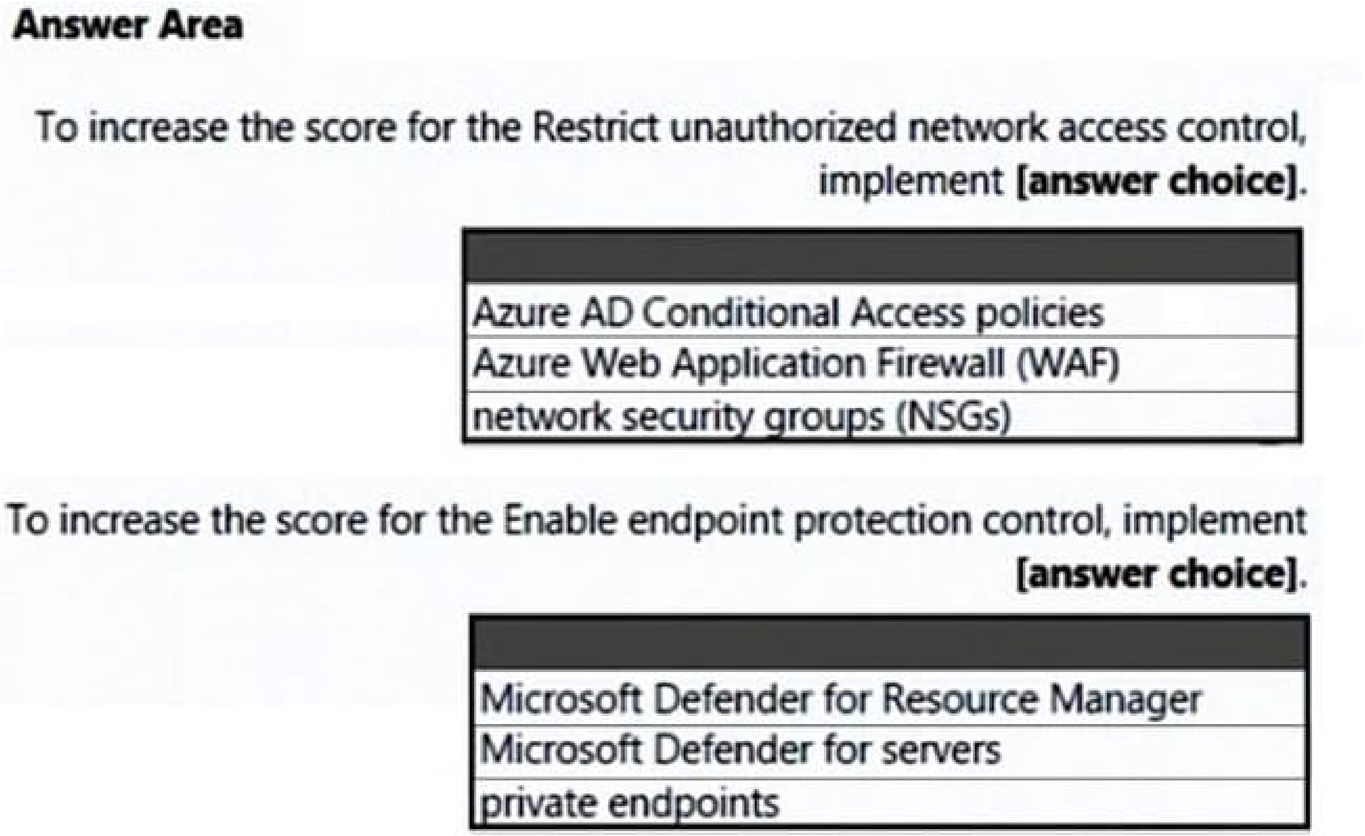
Control status : All | Recommendation status : 2 Selected | Recommendation maturity : All | Severity : All | Resource type : All | Response actions : All | Contains exemptions : All | Environment : All | Tactics : All

	Controls	Max score	Current Score	Potential score incre...	Unhealthy resources	Resource health	Actions
>	Enable MFA	10	0.00	+ 18% (10 points)	1 of 1 resources	🟥	
>	Secure management ports	8	5.33	+ 5% (2.67 points)	1 of 3 resources	🟥🟩	
>	Remediate vulnerabilities	6	0.00	+ 11% (6 points)	3 of 3 resources	🟥	
>	Apply system updates	6	6.00	+ 0% (0 points)	None	🟩	
>	Manage access and permissions	4	0.00	+ 7% (4 points)	1 of 12 resources	🟥⬜	
>	Enable encryption at rest	4	1.00	+ 5% (3 points)	3 of 4 resources	🟥🟩	
>	Restrict unauthorized network acces	4	3.00	+ 2% (1 point)	1 of 11 resources	🟥🟩⬜	
>	Remediate security configurations	4	3.00	+ 2% (1 point)	1 of 4 resources	🟥🟩	
>	Encrypt data in transit	4	3.33	+ 1% (0.67 points)	1 of 6 resources	🟥🟩	
>	Apply adaptive application control	3	3.00	+ 0% (0 points)	None	🟩	
>	Enable endpoint protection	2	0.67	+ 2% (1.33 points)	2 of 3 resources	🟥🟩	
>	Enable auditing and logging	1	0.00	+ 2% (1 point)	4 of 5 resources	🟥⬜	
>	Enable enhanced security features	Not scored	Not scored	+ 0% (0 points)	None	🟩⬜	
>	Implement security best practices	Not scored	Not scored	+ 0% (0 points)	9 of 30 resources	🟥🟩⬜	

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

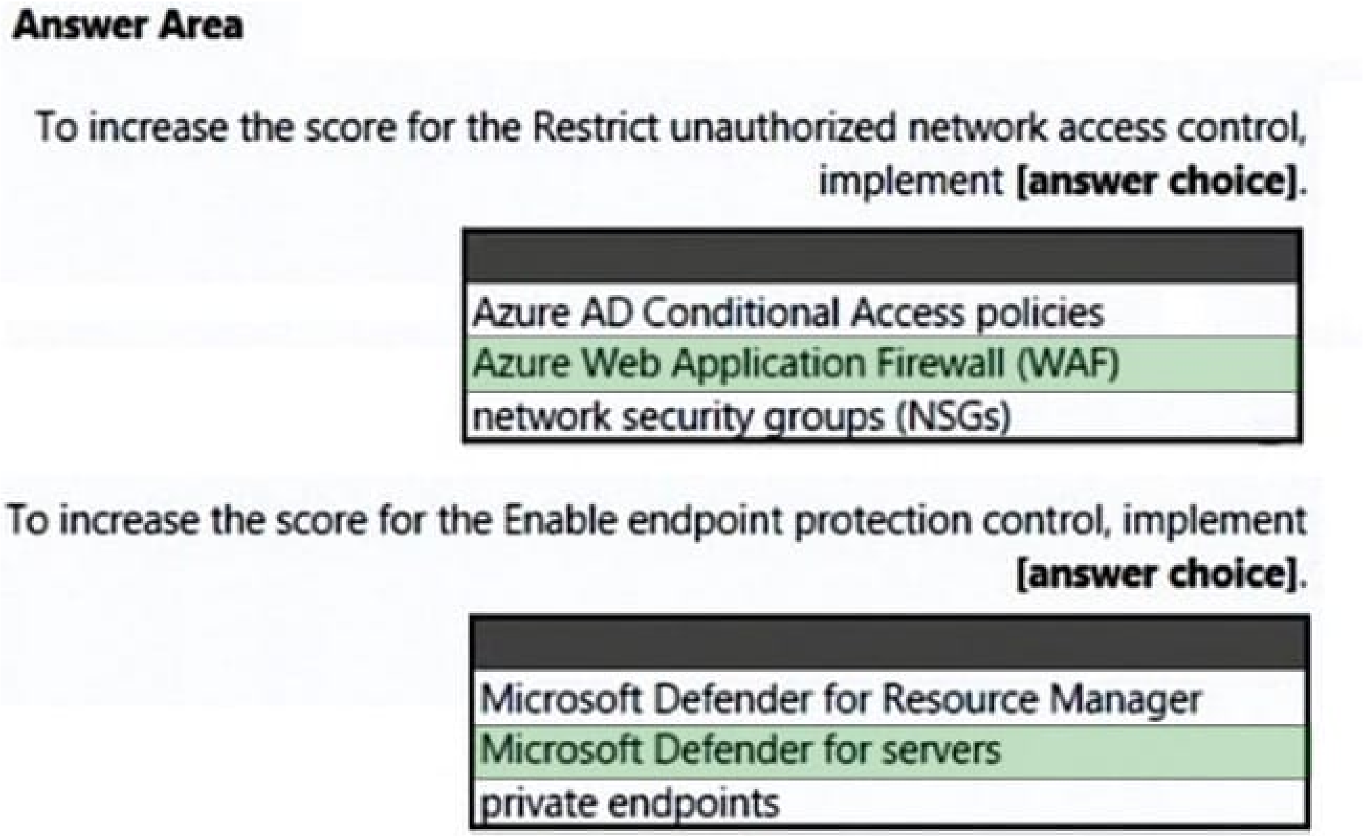
To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

Azure AD Conditional Access policies
Azure Web Application Firewall (WAF)
network security groups (NSGs)

To increase the score for the Enable endpoint protection control, implement **[answer choice]**.

Microsoft Defender for Resource Manager
Microsoft Defender for servers
private endpoints

Correct Answer:



Answer Area

To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

- Azure AD Conditional Access policies
- [✓ Azure Web Application Firewall (WAF)]
- network security groups (NSGs)

To increase the score for the Enable endpoint protection control, implement **[answer choice]**.

- Microsoft Defender for Resource Manager
- [✓ Microsoft Defender for servers]
- private endpoints

Box 1: Azure Web Application Firewall (WAF)

Restrict unauthorized network access control: 1 resource out of 11 needs to be addresses.

Restrict unauthorized network access - Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.

Use these recommendations to manage Defender for Cloud\\'s adaptive network hardening settings, ensure you configured Azure Private Link for all relevant PaaS services, enable Azure Firewall on your virtual networks, and more.

Note: Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway.

Azure WAF protects inbound traffic to the web workloads, and the Azure Firewall inspects inbound traffic for the other applications. The Azure Firewall will cover outbound flows from both workload types.

Incorrect:

Not network security groups (NSGs).

Box 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization\\'s endpoints for active threat detection and response solutions such as Microsoft Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn\\'t found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).

Incorrect:

Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they\\'re performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity. Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 4

You have an Azure subscription that contains virtual machines.

Port 3389 and port 22 are disabled for outside access.

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

1.

Prevent the need to enable ports 3389 and 22 from the internet.

2.

Only provide permission to connect the virtual machines when required.

3.

Ensure that administrators use the Azure portal to connect to the virtual machines.

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

NOTE: Each correct selection is worth one point.

A. Configure Azure VPN Gateway.

B. Enable Just Enough Administration (JEA).

C. Configure Azure Bastion.

D. Enable just-in-time (JIT) VM access.

E. Enable Azure AD Privileged Identity Management (PIM) roles as virtual machine contributors.

Correct Answer: CD

C: Bastion provides secure remote access.

It uses RDP/SSH session is over TLS on port 443.

Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network.

It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don\\'t need a public IP address, agent, or special client

software.

D: Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud\\'s just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect

to a VM.

Meets the requirement: Only provide permission to connect the virtual machines when required

Incorrect:

Not B: Does not address: Only provide permission to connect the virtual machines when required

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell. With JEA, you can:

Reduce the number of administrators on your machines using virtual accounts or group-managed service accounts to perform privileged actions on behalf of regular users.

Limit what users can do by specifying which cmdlets, functions, and external commands they can run.

Better understand what your users are doing with transcripts and logs that show you exactly which commands a user executed during their session.

Not E: Does not help with the remote access.

Note: Classic Virtual Machine Contributor: Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they\\'re connected to.

Reference: https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

QUESTION 5

You have an on-premises network and a Microsoft 365 subscription.

You are designing a Zero Trust security strategy.

Which two security controls should you include as part of the Zero Trust solution? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. Always allow connections from the on-premises network.

B. Disable passwordless sign-in for sensitive accounts.

C. Block sign-in attempts from unknown locations.

D. Block sign-in attempts from noncompliant devices.

Correct Answer: CD