Free Questions for SY0-601 by actualtestdumps

Shared by Jacobson on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After a web server was migrated to a cloud environment, user access to that server was Wocked Ever though an on-premises firewall configuration has been modified to reflect the cloud infrastructure, users are still experiencing access issues. Which of the following most likely needs to be configured?

Options:

A- Security group

B- Load balancer pool

C- Resource allocation

D- Storage permissions

Answer:

A

Question 2

Question Type: MultipleChoice

Which of the following techniques would most likely be used as a part of an insider threat reduction strategy to uncover relevant indicators?

Options:

A- Blocking known file sharing sites

B- Requiring credit monitoring

C- Implementing impossible travel alerts

D- Performing security awareness training

Answer:

C

Question 3

Question Type: MultipleChoice

A developer recently launched a new log-in page for a customer-facing website. Multiple customers are unable to log in because email address and password combinations are failing. The web servers begin to perform slowly and eventually crash Which of the following would most likely have prevented this issue?

Options:

A- Input validation

B- Request throttling

C- Enabling SSL on the web servers

D- Password rotation policies

Answer:

A

Question 4

Question Type: **MultipleChoice**

Which of the following assists in training employees on the importance of cybersecurity?

Options:

A- Phishing campaigns

B- Acceptable use policy

C- Employee handbook

D- Social media analysis

Answer:

A

Question 5

Question Type: **MultipleChoice**

A company wants to improve its access standards to prevent threat actors from togging in to the corporate network with compromised credentials in addition to MF

Options:

A- the Chief Information Security Officer wants an additional layer of protection enabled based on certain criteria Which of the following is the best way to provide additional protection?

A- Conditional access policies

B- Kerbaos access ticketing

C- Terminal access controller

D- Enabled key vaults

Answer:

A, A

Question 6

Question Type: MultipleChoice

An analyst is reviewing log data from a SIEM alert about a suspicious event Threat intelligence indicates threats from domains originating in known malicious countries The analyst examines the following data.

Description	Source IP	Destination IP	Action	Count
Traffic from malicious IP	177.45.38.61	10.100.11.35	Allow	14
Traffic from malicious IP	177.45.38.61	10.100.11.188	Allow	22
Brute-force attempt	177.45.38.61	10.100.11.35	Deny	117
Traffic from malicious IP	177.45.38.61	10.100.11.35	Allow	3
Brute-force attempt	177.45.38.61	10.100.11.250	Deny	151
Brute-force attempt	177.45.38.61	10.100.11.64	Deny	19

The Chief information Security Officer asks the analyst determine whether the SIEM alerts can be attributed to the domains m the threat intelligence report. Which of the following tools would bii allow the analyst to make this determination?

Options:

A- nsleskup

B- netstat

C- curl

D- arp

Answer:

A