AZ-900 Bootcamp Questions
APRIL 05 2024

Questions:

40	G H	is there an ELK like stack to monitor fast movign SIEM data?	10:59 am
39	G H	what is the servcie that will remdiate isseus automatilly if you code a remdiation step (e.g. if comprmised server, delete it when issue found)?	10:58 am
38	G H	what do most develoeprs use in terms of ARM/BICEP/etc?	10:50 am
36	N T	How much of this course % covers the MS requirements for taking exam. How much readying the your github links add to % to MS requirements	10:24 am
33	G H	Regarding conditional access and finding all the third party VPN IP addreses you might want to block, does Microsoft have something simliar to the AWS Web Application Firewall (WAF) , which you pay to block IP addresses from known bad actors using IP match conditions?	10:04 am
32	S A	I was referring to AZ-104 Azure administrator certification. Bit more details and links to prepare best for AZ-104	09:52 am

- 32: Please use the following resources:
  - https://learn.microsoft.com/en-us/credentials/certifications/azure-administrator/?practice-assessment-type=certification
  - https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/az-104
  - https://learning.oreilly.com/certifications/guides/AZ-104:-Microsoft-Certified-Azure-Administrator-Associate/0636920428220/

- 33: Yes. It is called Azure Web Application Firewall (WAF)
  - https://azure.microsoft.com/en-us/products/web-application-firewall/
  - https://learn.microsoft.com/en-us/azure/application-gateway/understanding-pricing
  - https://learn.microsoft.com/en-us/azure/web-application-firewall/
  - Application Gateway >> https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag
  - Azure FrontDoor >> https://learn.microsoft.com/en-us/azure/web-application-firewall/shared/manage-policies
- 36: It is hard to tell. We covered all AZ-900 learning objectives, and you should go through both links in the slide deck, and resource TEXT file.
- 38: Terraform and Bicep are used a lot. I still see many companies continuing to continue using ARM, but I suggest you learn ARM + (either Bicep, or Terraform). Terraform is multicloud which is a nice touch.
- 39: In the security context, services such as (not limited to) Microsoft Defender for Cloud, and Azure Sentinel can remediate security risks, but they need to be configured correctly:
  - Sentinel: https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=azure-portal%2CLAC%2Cafter-onboarding%2Cincidents%2Cazure
  - Defender: https://learn.microsoft.com/en-us/azure/defender-for-cloud/implement-security-recommendations
- 40:
  - Microsoft Sentinel (Cloud-native SIEM Solution)
    - https://azure.microsoft.com/en-us/products/microsoft-sentinel

Good luck!
Reza