GCFR Q&As

GIAC Cloud Forensics Responder (GCFR)

Pass GIAC GCFR Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/gcfr.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

The Azure PowerShell output below is an example of which of the following?


```
{
  "Name": "Contributor",
  "Id": "b24988vf-6180-42a0-ab55-20f7382dd24c",
  "IsCustom": false,
  "Description": "Manage everything except access to resources.",
  "Actions": [
    "*"
  ],
  "NotActions": [
    "Microsoft.Authorization/*/Delete",
    "Microsoft.Authorization/*/Write",
    "Microsoft.Authorization/elevateAccess/Action",
    "Microsoft.Blueprint/blueprintAssignments/write",
    "Microsoft.Blueprint/blueprintAssignments/delete"
  ],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
```


A. Role assignment

B. Managed identity

C. Role definition

D. Service principal

Correct Answer: B

QUESTION 2

What AWS service will allow an organization to set custom compliance metrics and force compliance on an organizational, sub-organizational, or individual account level?

A. Config

B. Cognllo

C. Inspector

D. Security Hub

Correct Answer: A

QUESTION 3

In Azure, which of the following describes a "Contributor"?

A. A collection of permissions such as read, write, and delete

B. A designation on a PKI certificate

C. A specification of who can access a resource group

D. An object representing an entity

Correct Answer: A

QUESTION 4

What is the recommended storage type when creating an initial snapshot of a VM in Azure for forensic analysis?

A. Standard SSD

B. Ultra Disk

C. Premium SSD

D. Standard HDD

Correct Answer: D

QUESTION 5

What type of AWS log is the following snippet an example of?

```
2 123456789010 eni-7149f0ca153968301 10.1.1.15 10.1.1.21 21142 22 6 2 88
1654648298 1654648351 ACCEPT OK
```

A. Web Application firewall Log

B. VPC Flow Log

C. Load Balancer Log

D. Route 53 Query Log

Correct Answer: B

QUESTION 6

Which cloud model should an organization negotiate access to logs as pert of contract negotiation prior to using the service?

A. IaaS

B. PaaS

C. Saas

Correct Answer: B

QUESTION 7

A company using PaaS to host and develop their software application is experiencing a DOS attack. What challenge will a DFIR analyst experience when investigating this attack?

A. Restricted access to their application logs

B. Resource scaling will affect access to logs

C. Network logs are unavailable for review

D. Network monitoring disabled by the company

Correct Answer: C

QUESTION 8

What Amazon EC2 instance prefix should be monitored to detect potential crypto mining?

A. C

B. P

C. R

D. I

Correct Answer: B

QUESTION 9

Which of the following operating systems are used by Blackberry 10 and found in some vehicles and medical devices?

A. Bada

B. POSIX

C. QNX

D. UNIX

Correct Answer: C

QUESTION 10

Which is the effective access when aws user is assigned to an S3 bucket?

A. A user must have an employee account

B. A user must have an account under any AWS account

C. A user must be under the same AWS account as the S3 bucket

D. A user must have the AWS IAM role assigned

Correct Answer: C

QUESTION 11

The attack technique "Access Kubelet API" falls under which Mitre ATTandCK tactic?

A. Execution

B. Credential Access

C. Discovery

D. Initial Access

Correct Answer: C

QUESTION 12

Which of the following is the smallest unit of computing hardware in Kubernetes?

A. Cluster

B. Node

C. Container

D. Pod

Correct Answer: D

QUESTION 13

How is storage account, cs21003200042c87633, created in an Azure resource group?

A. PowerShell Cloud Shell audit logging was enabled

B. A Bash Cloud Shell was used

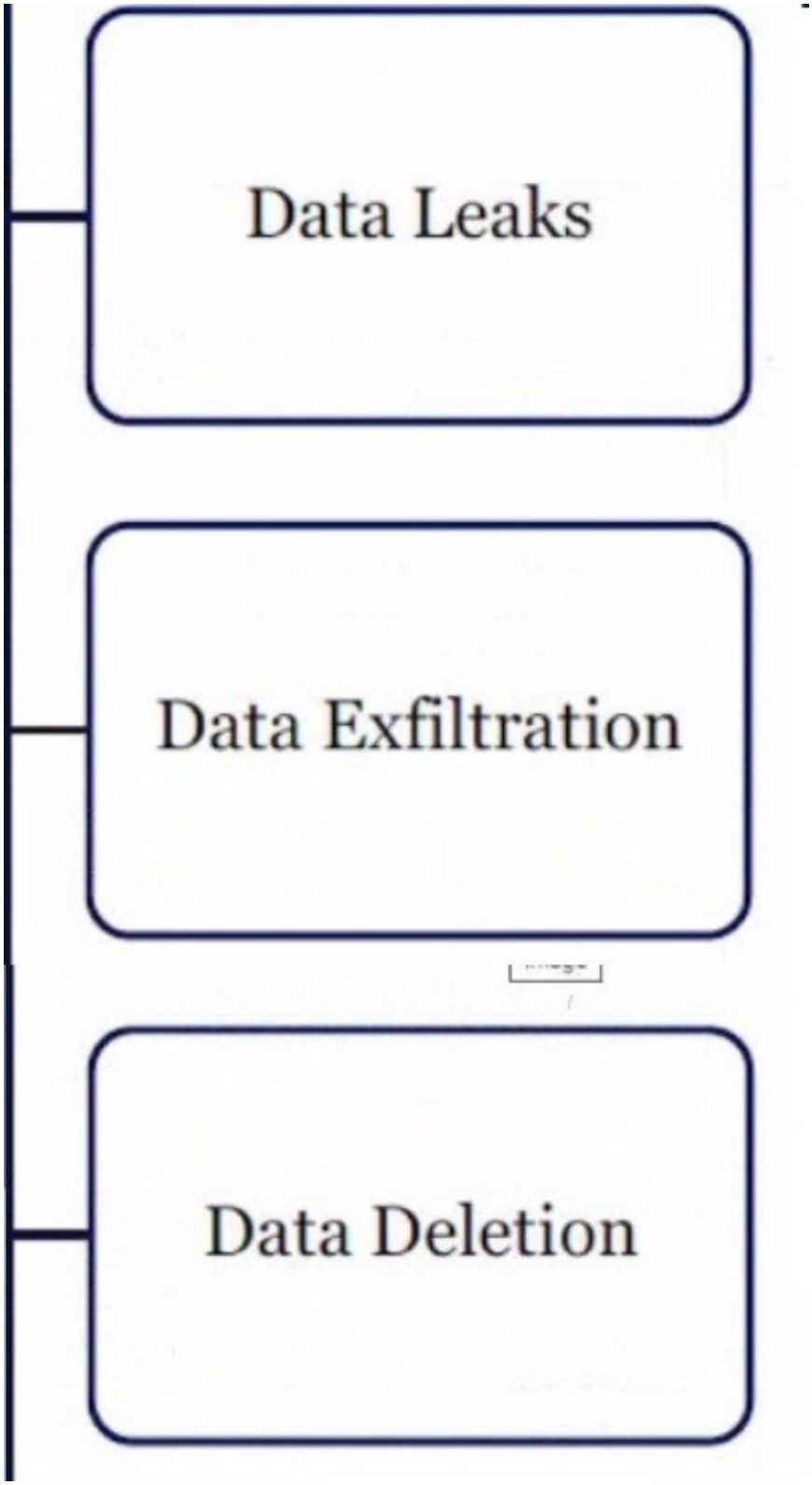
C. PowerShell Cloud Shell was used

D. Azure CLI was used from a Windows machine

Correct Answer: B

QUESTION 14

What is shown in the screenshot?



A. Google threat types

B. Windows event channels

C. Mitre ATTandCK tactics

D. CIS critical controls

Correct Answer: C

QUESTION 15

Which cloud service provider produces sampled flow logs?

A. GCP

B. Azure

C. AWS

Correct Answer: A