Number: GCFR
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: GCFR

Exam Name: GIAC Cloud Forensics Responder

Exam A

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
Section:

QUESTION 2
Below is an extract from a Server Access Log showing a record for a request made to an AWS S3 bucket. What does the first field starting with '385f9e' represent?

```
385f9ef91a82f8ca241dbb08d21b781846f4b75b73589dec7a054f8781cef6eb labresearch
[31/May/2021:14:18:38 +0000] 10.246.62.156 arn:aws:sts::305681518678:assumed-
role/AWSServiceRoleForConfig/AWSConfig-Describe RPB2PVWVY52G8J0S
REST.GET.TAGGING - "GET /?tagging HTTP/1.1" 404 NoSuchTagSet 291 - 27 - "-"
"AWSConfig cfg/retry-mode/legacy" -
H9xRp+HGTSnP7lvh9gG/9Bfs62jSbfE61nKRYcGBJ/0Y+ZljBDlSNyqkaMIws3I9gon+w6kJBQY=
SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader labresearch.s3.us-east-
1.amazonaws.com TLSv1.2
```

A. Bucket Owner
B. Request ID
C. Host ID
D. Cipher Suite

Correct Answer: B
Section:

QUESTION 3
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
Section:

QUESTION 4
What logical AWS structure type is used to chain together accounts in a trust relationship which allows for single sign-on and cross-account management?

A. Subscription
B. Organisation
C. OU
D. Tenant

Correct Answer: B
Section:

QUESTION 5
An Azure blob is accessed using the link below. What is the name of the blob container?

```
https://ex-storage.blob.core.windows.net/mymovies/mov1.avi
```

A. ex-storage
B. mov.avi

C. mymovies
D. blob.core

Correct Answer: C
Section:

QUESTION 6
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
Section:

QUESTION 7
What Pub/Sub component is used to forward GCP logs to their final location?

A. Topic
B. Log Sink
C. Publication
D. Subscription

Correct Answer: B
Section:

QUESTION 8
Which of the following is the smallest unit of computing hardware in Kubernetes?

A. Cluster
B. Node
C. Container
D. Pod

Correct Answer: D
Section:

QUESTION 9
What is a best practice recommendation when using API keys for AWS access?

A. Delete the account's default access keys
B. Define specific role permissions
C. Enable MFA protection
D. Configure STS one-time tokens

Correct Answer: A
Section:

QUESTION 10
What would prevent GCP 1AM from linking to Google Workspace to manage users and groups?

A. A gcp-organization-admins group was not created
B. The connector was not configured to link the services
C. Inadequate Identity and Access Management license
D. Google Workspace cannot be linked to GCP 1AM

Correct Answer: D
Section:

QUESTION 11
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
Section:

QUESTION 12
An investigator confirms that phishing emails sent to users in an organization ate not being sent to their Gmall Spam folder. What is a possible cause for this?

A. The default setting for enhanced pre-delivery message scanning was changed
B. The security sandbox default configuration setting was changed
C. A third party application needs to be installed to detect phishing emails
D. Compliance based rules need to be configured to detect phishing emails

Correct Answer: A
Section:

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
Section:

QUESTION 14
An engineer has set up log forwarding for a new data source and wants to use that data to run reports and create dashboards in Kibana. What needs to be created in order to properly handle these logs?

A. Row
B. Parser
C. ingest script
D. Beat

Correct Answer: B
Section:

QUESTION 15
At what point of the OAuth delegation process does the Resource Owner approve the scope of access to be allowed?

A. After user credentials are accepted by the Authorization Server
B. Once the OAuth token is accepted by the Application
C. When the Resource Server receives the OAuth token
D. Before user credentials are sent to the Authentication Server

Correct Answer: A
Section:

QUESTION 16
Which cloud service provider produces sampled flow logs?

A. GCP
B. Azure
C. AWS

Correct Answer: A
Section:

QUESTION 17
What method does Google use to alert Gmail account holders that they may be under attack by government sponsored attackers?

A. Message upon successful logon
B. SMS text message
C. Email sent to the user
D. Alert sent to recovery account

Correct Answer: A
Section:

QUESTION 18

Which AW5 1AM policy element indicates the API that is in scope?

A. Effect
B. Version
C. Action
D. Resource

Correct Answer: C
Section:

QUESTION 19
Sensitive company data is found leaked on the internet, and the security team didn't get any alert and is unsure of how the breach occurred.
Which logs would be a preferable starting point for an investigation?

A. Identity and Access Management
B. Application
C. Resource Management
D. Endpoint

Correct Answer: A
Section:

QUESTION 20
An investigator is evaluating a client's Microsoft 365 deployment using the web portals and has identified that the Purview compliance portal states that the Unified Audit Logs are not enabled. Based on the additional Information gathered below, what is most likely the cause of this configuration message?
Subscription creation date: December 4, 2021 Number of administrators: 2 Number of non-administrative user accounts: 74 Last tenant administration change: December 4,2021

A. Explicitly been disabled by an administrator
B. License was downgraded lower than an E5 license
C. Tenant is configured to forward logs externally
D. Default configuration, service was never enabled

Correct Answer: D
Section:

QUESTION 21
At what organizational level are EC2 services managed by customers?

A. Data center
B. Regional
C. Global
D. Continental

Correct Answer: B
Section:

QUESTION 22
An investigator his successfully installed the ExchangeOnlineManagement module on their investigation system and is attempting to search a client's Microsoft 365 Unified Audit Log using PowerShell. PowerShell returns a 'command not found' error each time they try to execute the Search-UnifiedAuditLog cmdlet. How should the investigator troubleshoot this issue?

A. Ensure their system has .NFT version 4.b or later Installed
B. Ensure that MFA has been disabled for The account used
C. Check that they are using PowerShell Core
D. Check the permissions of the account used in Microsoft 365

Correct Answer: D
Section:

QUESTION 23
The attack technique 'Access Kubelet API' falls under which Mitre ATT&CK tactic?

A. Execution
B. Credential Access
C. Discovery
D. Initial Access

Correct Answer: C
Section:

QUESTION 24
An analyst successfully authenticated to Microsoft 365 using the following command. What would cause the analyst to be unable to search UAL events for a specific time period?
Ps> connect fxrhangeOnline userPrincipalName sysanalystatexanpteco.com

A. The tmdlets to search the UAl were not Imported into the session
B. The UAL cannot be searched when using Microsoft 365 PowerShell
C. The incorrect version of the FxhangeOnlineManagement module was installed
D. The ExchangeOnlineManagement module was not installed

Correct Answer: A
Section: