



CERTSWARRIOR

# GIAC GCTD

## GIAC Cloud Threat Detection (GCTD)

**Questions&AnswersPDF**

**ForMoreInformation:**

**<https://www.certswarrior.com/>**

## Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

# Latest Version: 6.0

## Question: 1

Which AWS service would you use to detect and alert on unauthorized access to sensitive data stored in Amazon S3 buckets?

Response:

- A. AWS GuardDuty
- B. Amazon RDS
- C. AWS Lambda
- D. Amazon EC2

**Answer: A**

## Question: 2

What is the purpose of enabling AWS Config in an AWS environment?

Response:

- A. To manage billing
- B. To monitor and assess resource configurations, track changes, and ensure compliance with security policies
- C. To disable unused services
- D. To increase file transfer speed

**Answer: B**

## Question: 3

Your organization uses a combination of AWS and Azure for cloud services. To improve security monitoring, you want to centralize logs from both cloud environments into a single platform. Which steps should you take to achieve this?

Response:

- A. Enable billing alerts to monitor log storage costs
- B. Set up AWS CloudWatch Logs and Azure Monitor, and use a third-party SIEM tool like Splunk to centralize logs from both environments
- C. Disable logging to reduce the number of logs collected
- D. Manually download logs from both environments and store them locally

**Answer: B**

### Question: 4

Which AWS service would you use to set up alerts for unusual network traffic patterns or potential security incidents in your VPC?

Response:

- A. Amazon S3
- B. AWS CloudFormation
- C. AWS Lambda
- D. AWS CloudWatch

**Answer: D**

### Question: 5

What is the role of Amazon CloudWatch in investigating AWS environments?

Response:

- A. To store data
- B. To monitor and collect metrics, logs, and events from AWS resources, providing insights into performance and security issues
- C. To manage user accounts
- D. To reduce cloud storage costs

**Answer: B**

### Question: 6

What is the main purpose of enabling logging and monitoring in a cloud environment?

Response:

- A. To improve the user experience
- B. To collect real-time data for detecting security incidents and performance issues
- C. To reduce cloud service costs
- D. To restrict access to specific cloud resources

**Answer: B**

### Question: 7

When investigating potential security incidents in Azure, which tool can help you track network traffic patterns and detect unusual activity?

Response:

- A. Azure Firewall
- B. Azure Traffic Manager
- C. Azure Network Watcher
- D. Azure Active Directory

**Answer: C**

### Question: 8

Why is it important to monitor data retention policies in cloud storage environments?

Response:

- A. To increase the speed of data access
- B. To ensure compliance with regulatory requirements and avoid over-retention of sensitive data
- C. To reduce cloud storage costs
- D. To prevent users from accessing their own data

**Answer: B**

### Question: 9

Which service would you use in Azure to monitor storage usage, track data access, and generate alerts for unusual activities on storage accounts?

Response:

- A. Azure Security Center
- B. Azure Sentinel
- C. Azure AD
- D. Azure Blob Storage Diagnostics

**Answer: B**

### Question: 10

What is the primary goal of network flow monitoring in cloud environments?

Response:

- A. To increase cloud storage capacity
- B. To reduce latency between services
- C. To manage cloud billing
- D. To detect unusual traffic patterns and potential security incidents

<b>Answer: D</b>
------------------



# CERTSWARRIOR

## *FULL PRODUCT INCLUDES:*

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



**For More Information – Visit link below:**

**<https://www.certswarrior.com>**

**16 USD Discount Coupon Code: U89DY2AQ**