

# Free Questions for 312-39 by certsinside

Shared by Porter on 24-05-2024

For More Free Questions and Preparation Resources

**Check the Links on Last Page** 

# **Question 1**

**Question Type:** MultipleChoice

What does Windows event ID 4740 indicate?

#### **Options:**

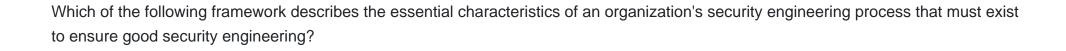
- A- A user account was locked out.
- B- A user account was disabled.
- C- A user account was enabled.
- D- A user account was created.

#### **Answer:**

Α

# **Question 2**

**Question Type:** MultipleChoice



#### **Options:**

- A- COBIT
- B- ITIL
- C- SSE-CMM
- D- SOC-CMM

#### **Answer:**

С

# **Question 3**

**Question Type:** MultipleChoice

Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex  $(\%27)[(\))((\%6F)]o[(\%4F))((\%72)]r[(\%52))/ix$ .

#### **Options:**

- A- SQL Injection Attack
- **B-** Parameter Tampering Attack
- C- XSS Attack
- **D-** Directory Traversal Attack

#### **Answer:**

Α

### **Question 4**

#### **Question Type:** MultipleChoice

Which of the following are the responsibilities of SIEM Agents?

- 1. Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
- 2. Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.

3. Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
4. Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.
Options:
A- 1 and 2
B- 2 and 3
C- 1 and 4
D- 3 and 1
Answer:
A

# **Question 5**

**Question Type:** MultipleChoice

Which of the following Windows event is logged every time when a user tries to access the "Registry" key?

Options:		
<b>A-</b> 4656		
<b>B-</b> 4663		
<b>C-</b> 4660		
D- 4657		
Answer:		
A		
Question 6 Question Type: MultipleChoice		
Question 6		
Question 6		
Question 6 Question Type: MultipleChoice		
Question 6 Question Type: MultipleChoice		

B- Not Found Error
C- Internal Server Error
D- Forbidden Error
Answer:
D
Question 7
Question Type: MultipleChoice
Which of the following factors determine the choice of SIEM architecture?
Options:
A- SMTP Configuration
B- DHCP Configuration

C- DNS Configuration

D- Network Topology

Question	8
uestion Type: N	<b>IultipleChoice</b>
Identify the even	ent severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future
Options:	
	it
A- Failure Aud	it
A- Failure Aud B- Warning	it
Options:  A- Failure Aud B- Warning C- Error D- Information	it
A- Failure Aud B- Warning C- Error	it

# **Question 9**

#### **Question Type:** MultipleChoice

Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

### **Options:**

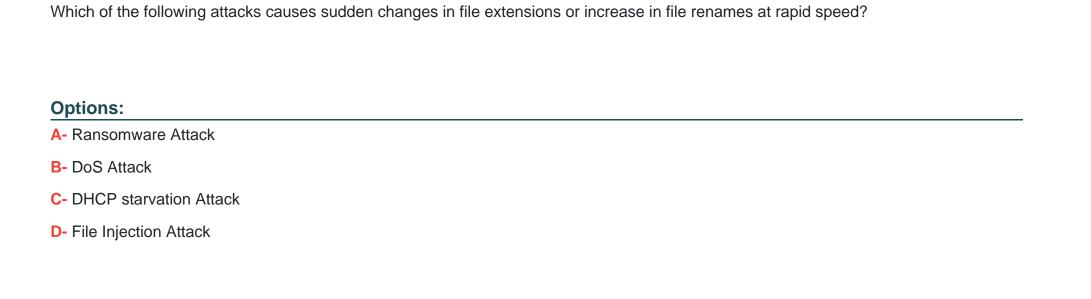
- A- De-Militarized Zone (DMZ)
- **B-** Firewall
- **C-** Honeypot
- **D-** Intrusion Detection System

#### **Answer:**

С

# **Question 10**

**Question Type:** MultipleChoice



**Answer:** 

### To Get Premium Files for 312-39 Visit

https://www.p2pexams.com/products/312-39

### **For More Free Questions Visit**

https://www.p2pexams.com/eccouncil/pdf/312-39

