Free Questions for 312-39 by certsdeals

Shared by Francis on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Banter is a threat analyst in Christine Group of Industries. As a part of the job, he is currently formatting and structuring the raw data.

He is at which stage of the threat intelligence life cycle?

Options:

A- Dissemination and Integration

B- Processing and Exploitation

C- Collection

D- Analysis and Production

Answer:

B

Question 2

Question Type: MultipleChoice

An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP.

Which SIEM deployment architecture will the organization adopt?

Options:

A- Cloud, MSSP Managed

B- Self-hosted, Jointly Managed

C- Self-hosted, MSSP Managed

D- Self-hosted, Self-Managed

Answer:

C

Question 3

Question Type: **MultipleChoice**

Which of the log storage method arranges event logs in the form of a circular buffer?

Options:

A- FIFO

B- LIFO

C- non-wrapping

D- wrapping

Answer:

D

Question 4

Question Type: MultipleChoice

Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

Options:

A- Dictionary Attack

B- Rainbow Table Attack

C- Bruteforce Attack

D- Syllable Attack

Answer:

A

Question 5

Question Type: MultipleChoice

Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

Options:

A- Rule-based detection

B- Heuristic-based detection

C- Anomaly-based detection

D- Signature-based detection

Answer:

C

Question 6

Question Type: MultipleChoice

Which of the following can help you eliminate the burden of investigating false positives?

Options:

A- Keeping default rules

B- Not trusting the security devices

C- Treating every alert as high level

D- Ingesting the context data

Answer:

D

Question 7

Question Type: MultipleChoice

Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.

Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?

Options:

A- Threat pivoting

B- Threat trending

C- Threat buy-in

D- Threat boosting

Answer:

B

Question 8

Question Type: MultipleChoice

Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?

Options:

A- Command Injection Attacks

B- SQL Injection Attacks

C- File Injection Attacks

D- LDAP Injection Attacks

Answer:

A

Question 9

Question Type: MultipleChoice

Which of the following attack can be eradicated by filtering improper XML syntax?

Options:

A- CAPTCHA Attacks

B- SQL Injection Attacks

C- Insufficient Logging and Monitoring Attacks

D- Web Services Attacks

Answer:

B