CertiProf

CSFPC

Cyber Security Foundation

QUESTION & ANSWERS

Question: 1

What physical characteristics can affect the usability of security mechanisms?

A. Ambient temperature

B. Pollution

C. Noise

D. All of the above

Answer: D

Explanation/Reference:

Page 156. CYBOK

Question: 2

_____ reflects on the potential harmful effect of design choices before technological innovations are put into large-scale deployment

A. Saltzer and Schroeder Principles

B. The Precautionary Principle

C. Latent Design Conditions

D. NIST Principles

Answer: B

Explanation/Reference:

Page 12. CYBOK

Question: 3

One of the main benefits of analyzing the malware structure that may include the libraries and toolkits and coding techniques, we may find some important data that is possibly helpful to attribution.

A. Which means being able to identify the likely author and operator

B. To understand what damage can be done due to the malware program

C. To be able to know the amount of data that has been lost or corrupted

D. Both B and C are correct, and A is incorrect

Answer: A

Explanation/Reference:

Page 207. CYBOK

Question: 4

The process of developing and evaluating options to address exposure is called?

A. Threat Management

B. Failure Management

C. Incident Management

D. Risk Management

Answer: D

Question: 5

In Security Architecture and Lifecycle “to group users and data into broad categories using role-access requirements, together with formal data classification and user clearance” is part of which step?

A. First Step

B. Second Step

C. Last Step

D. Third Step

Answer: B

Explanation/Reference:

Page 15. CYBOK

Question: 6

Syslog provides a generic logging infrastructure that constitutes an extremely efficient data source for many uses. This new specification introduces several improvements over the original implementation. A Syslog entry is a timestamped text message coming from an identified source.

A. Timestamp, Hostname, Process, Priority, and PID

B. DNS and Routing info, Data security gateway ID

C. Authentication ID, Encryption and decryption info, and data privacy flag

D. Routers CPU ID, Transport Layer Security protocol info, and Syslog current version

Answer: A

Explanation/Reference:

Page 262. CYBOK

Question: 7

According to The US Government NIST guidelines, “Conduct” is the phase where

A. Threats, vulnerabilities, likelihood and impact are identified

B. Inform about the actions

C. Continually update the risk assessment

D. Identifying the purpose

Answer: A

Explanation/Reference:

Page 33. CYBOK
