A. SaaS
B. PaaS
C. IaaS
D. DaaS

Correct Answer: C

QUESTION 60
A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboars are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. Loss of proprietary information
B. Damage to the company's reputation
C. Social engineering
D. Credential exposure

Correct Answer: A
Explanation:
In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information think phishing, spoofing. That is not being demonstrated in this question. The company is protecting themselves from loss of proprietary information by clearing it all out. so that if anyone in the tour is looking to take it they will be out of luck

QUESTION 61
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

Correct Answer: C

QUESTION 62
In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

A. Identification
B. Preparation
C. Eradiction
D. Recovery
E. Containment

Correct Answer: E

QUESTION 63
A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A.   An air gap
B.   A Faraday cage
C.   A shielded cable
D.   A demilitarized zone

Correct Answer: A

QUESTION 64
A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

A.   A capture-the-flag competition
B.   A phishing simulation
C.   Physical security training
D.   Baste awareness training

Correct Answer: B

QUESTION 65
A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

A.   RA1D 0
B.   RAID1
C.   RAID 5
D.   RAID 10

Correct Answer: C
Explanation:
https://techgenix.com/raid-10-vs-raid-5/

QUESTION 66
The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A.   A script kiddie
B.   Shadow IT
C.   Hacktivism
D.   White-hat

Correct Answer: B
Explanation:
Shadow IT solutions increase risks with organizational requirements for control, documentation,

security, reliability, etc

https://en.wikipedia.org/wiki/Shadow_IT

QUESTION 67
A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

A. Discretionary
B. Rule-based
C. Role-based
D. Mandatory

Correct Answer: D

QUESTION 68
Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

Correct Answer: C

QUESTION 69
After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

A. Multifactor authentication
B. Something you can do
C. Biometric
D. Two-factor authentication

Correct Answer: D

QUESTION 70
A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

A. dd
B. chmod
C. dnsenum
D. logger

Correct Answer: A

QUESTION 71
An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

Correct Answer: B

QUESTION 72
A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

A. MSSP
B. SOAR
C. IaaS
D. PaaS

Correct Answer: B

QUESTION 73
Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

A. Watering-hole attack
B. Credential harvesting
C. Hybrid warfare
D. Pharming

Correct Answer: A

QUESTION 74
Which of the following is the purpose of a risk register?

A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies
C. To identify the risk, the risk owner, and the risk measures
D. To formally log the type of risk mitigation strategy the organization is using

Correct Answer: C
Explanation:
The Risk Register displays a list of all risks recorded and displays various risk details, including

the residual risk level, risk source, risk owner, risk stage, and the treatment status of the risk.
https://kb.wisc.edu/security/110450

QUESTION 75
A Chief Information Security Officer (CISO) needs to create a policy set that meets international
standards for data privacy and sharing. Which of the following should the CISO read and
understand before writing the policies?

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

Correct Answer: B
Explanation:
GDPR is an international standard for data protection and privacy.

QUESTION 76
A system administrator needs to implement an access control scheme that will allow an object's
access policy be determined by its owner. Which of the following access control schemes BEST
fits the requirements?

A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Attribute-based access control

Correct Answer: B

QUESTION 77
Which of the following would be the BEST method for creating a detailed diagram of wireless
access points and hot-spots?

A. Footprinting
B. White-box testing
C. A drone/UAV
D. Pivoting

Correct Answer: A

QUESTION 78
A cybersecurity administrator needs to add disk redundancy for a critical server. The solution
must have a two-drive failure for better fault tolerance. Which of the following RAID levels should
the administrator select?

A. 0
B. 1
C. 5
D. 6

Correct Answer: D