

# ECCouncil Valid 212-82 Exam Dumps: Certified Cybersecurity Technician - PassTorrent Bring Candidates good Latest Dumps Ppt



*ECCouncil*

*212-82*  
*Certified Cybersecurity Technician (CCT)*

- Up to Date products, reliable and verified.
- Questions and Answers in PDF Format.

**Full Version Features:**

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24 Hours Live Chat Support

**For More Information:**

<https://www.testsexpert.com/>

• **Product Version**

Visit us at <https://www.testsexpert.com/212-82/>

P.S. Free & New 212-82 dumps are available on Google Drive shared by PassTorrent: <https://drive.google.com/open?id=1FRUSqZZGVOd8xd17f8H-OYrJwf99udt9>

PassTorrent also provides three months of free updates, if for instance, the content of Certified Cybersecurity Technician (212-82) exam questions changes after you purchase the 212-82 Practice Exam. So just jump straight toward PassTorrent for your preparation for the ECCouncil 212-82 certification exam.

ECCouncil 212-82 (Certified Cybersecurity Technician) certification exam is a comprehensive and globally recognized credential that demonstrates an individual's proficiency in cybersecurity technology. 212-82 exam is designed to equip professionals with the necessary skills to identify and mitigate potential cybersecurity threats and vulnerabilities in an organization's technology infrastructure. Certified Cybersecurity Technician certification is ideal for individuals who are looking to advance their careers in cybersecurity, particularly in the role of a cybersecurity technician.

>> Valid 212-82 Exam Dumps <<

**Latest Released ECCouncil Valid 212-82 Exam Dumps - 212-82 Certified Cybersecurity Technician**

Quality first, service second! We put much attention and resources on our products quality of 212-82 real questions so that our pass rate of the 212-82 training braindump is reaching as higher as 99.37%. As for service we introduce that "Pass Guaranteed". We believe one customer feel satisfied; the second customer will come soon for our 212-82 Study Guide. If you want to have a look at our 212-82 practice questions before your payment, you can just free download the demo to have a check on the web.

## **ECCouncil Certified Cybersecurity Technician Sample Questions (Q38-Q43):**

### **NEW QUESTION # 38**

CyberX, an acclaimed cybersecurity firm with a diverse clientele ranging from financial institutions to healthcare providers, has been approached by NexusCorp. NexusCorp, a global supply chain giant, seeks assistance in drafting a new security policy after a series of cyber-attacks that highlighted vulnerabilities in its existing protocols. While NexusCorp uses state-of-the-art technology, its security policies have not kept pace.

It needs a policy that acknowledges its complex organizational structure, vast geographic spread, and diversity in employee tech proficiency.

Which should be CyberX's primary consideration in this scenario?

- A. Regular update schedules for software and hardware components.
- **B. Stakeholder involvement in policy formulation.**
- C. Use of the latest encryption algorithms.
- D. Emphasis on stringent password policies.

**Answer: B**

Explanation:

\* Inclusion of Diverse Perspectives:

\* Involving stakeholders in policy formulation ensures that the security policy considers the diverse needs and perspectives of different departments and employees across NexusCorp's complex organizational structure.

### **NEW QUESTION # 39**

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

- A. ISO 2002
- B. PII
- C. PCIDSS
- **D. HIPPA/PHI**

**Answer: D**

Explanation:

HIPPA/PHI is the regulation that is mostly violated in the above scenario. HIPPA (Health Insurance Portability and Accountability Act) is a US federal law that sets standards for protecting the privacy and security of health information. PHI (Protected Health Information) is any information that relates to the health or health care of an individual and that can identify the individual, such as name, address, medical records, etc. HIPPA/PHI requires covered entities, such as health care providers, health plans, or health care clearinghouses, and their business associates, to safeguard PHI from unauthorized access, use, or disclosure. In the scenario, the medical company experienced a major cyber security breach that exposed the personal medical records of many patients on the internet, which violates HIPPA/PHI regulations. PII (Personally Identifiable Information) is any information that can be used to identify a specific individual, such as name, address, social security number, etc. PII is not specific to health information and can be regulated by various laws, such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), etc. PCI DSS (Payment Card Industry Data Security Standard) is a set of standards that applies to entities that store, process, or transmit payment card information, such as merchants, service providers, or payment processors. PCI DSS requires them to protect cardholder data from unauthorized access, use, or disclosure. ISO 2002 (International Organization for Standardization 2002) is not a regulation, but a standard for information security management systems that provides guidelines and best practices for organizations to manage their information security risks.

### **NEW QUESTION # 40**

The IH&R team in an organization was handling a recent malware attack on one of the hosts connected to the organization's

network. Edwin, a member of the IH&R team, was involved in reinstating lost data from the backup media. Before performing this step, Edwin ensured that the backup does not have any traces of malware. Identify the IH&R step performed by Edwin in the above scenario.

- A. Eradication
- B. Incident containment
- **C. Recovery**
- D. Notification

**Answer: C**

Explanation:

Recovery is the IH&R step performed by Edwin in the above scenario. IH&R (Incident Handling and Response) is a process that involves identifying, analyzing, containing, eradicating, recovering from, and reporting on security incidents that affect an organization's network or system. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Recovery can include reinstating lost data from the backup media, applying patches or updates, reconfiguring settings, testing functionality, etc. Recovery also involves ensuring that the backup does not have any traces of malware or compromise. Eradication is the IH&R step that involves removing all traces of the incident from the system or network, such as malware, backdoors, compromised files, etc. Incident containment is the IH&R step that involves implementing appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization. Notification is the IH&R step that involves informing relevant stakeholders, authorities, or customers about the incident and its impact.

#### NEW QUESTION # 41

Matias, a network security administrator at an organization, was tasked with the implementation of secure wireless network encryption for their network. For this purpose, Matias employed a security solution that uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data.

Identify the type of wireless encryption used by the security solution employed by Matias in the above scenario.

- A. WPA2 encryption
- **B. WPA3 encryption**
- C. WEP encryption
- D. WPA encryption

**Answer: B**

Explanation:

WPA3 encryption is the type of wireless encryption used by the security solution employed by Matias in the above scenario. WPA3 encryption is the latest and most secure version of Wi-Fi Protected Access, a protocol that provides authentication and encryption for wireless networks. WPA3 encryption uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data. WPA3 encryption also provides enhanced protection against offline dictionary attacks, forward secrecy, and secure public Wi-Fi access. WPA2 encryption is the previous version of Wi-Fi Protected Access, which uses Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) for data encryption. WEP encryption is an outdated and insecure version of Wi-Fi security, which uses RC4 stream cipher for data encryption. WPA encryption is an intermediate version of Wi-Fi security, which uses TKIP for data encryption.

#### NEW QUESTION # 42

PolarFin, a global finance institution, is in the process of migrating to a new transactional system. Given the sensitivity of financial data and international regulations it adheres to, PolarFin needs an encryption algorithm that provides strong security and is also widely accepted internationally. The algorithm should also support both encryption and decryption functions. Which cryptographic algorithm should PolarFin consider as its primary choice for this transition?

- A. HMAC (Hash-Based Message Authentication Code)
- B. Blowfish
- **C. RSA (Rivest Shamir Adleman)**
- D. DES (Data Encryption Standard)

**Answer: C**

\* RSA is a widely accepted and strong public-key cryptographic algorithm that supports both encryption and decryption functions. It is based on the mathematical difficulty of factoring large prime numbers.

• • • • •

**212-82 Latest Dumps Ppt:** <https://www.passtorrent.com/212-82-latest-torrent.html>

- 2026 Latest PassTorrent 212-82 PDF Dumps and 212-82 Exam Engine Free Share: <https://drive.google.com/open?id=1FRUSqZZGVod8xd17f8H-OYrJwf99udt9>