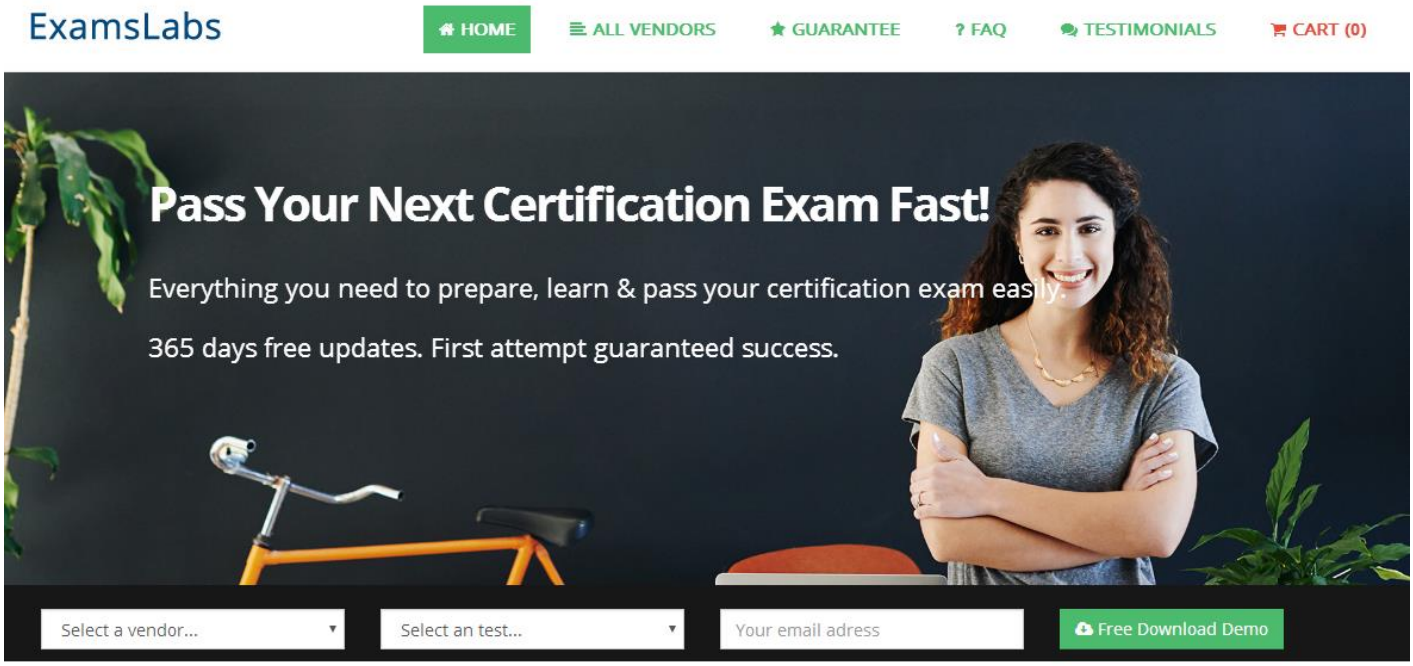
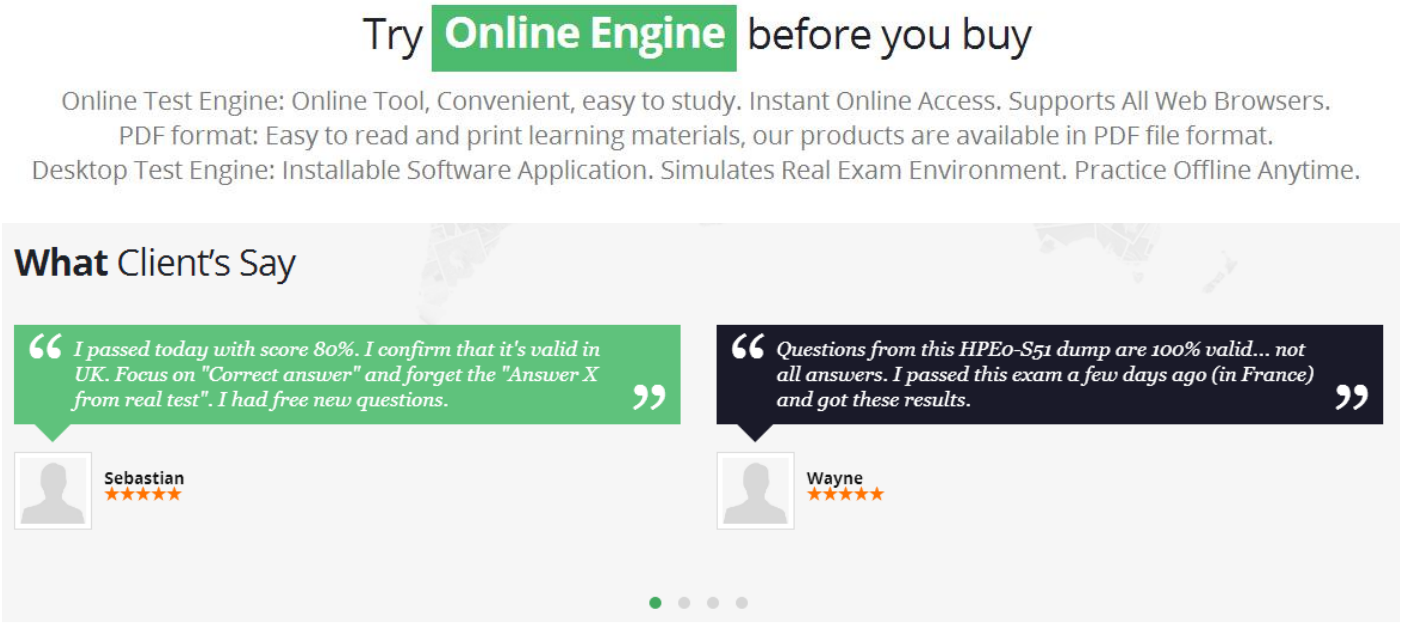
ExamsLabs





http://www.examslabs.com/

Latest Study Materials, Valid Dumps - ExamsLabs

Exam : **Ethics-In-Technology**

Title : WGU Ethics In Technology QCO1

Vendor : WGU

Version : DEMO

NO.1 An organization is concerned about its cybersecurity after identifying unauthorized records in its payroll database. The organization hires a consultant to test its cyberdefenses. The consultant executes several test attacks on the organization's software and successfully demonstrates that by using Structured Query Language (SOL) injection, the consultant can add rows to the payroll database without obtaining the proper permissions.
Which hacker classification does the consultant fall under?
A. Cybercriminal
B. White hat hacker
C. Cyberterrorist
D. Black hat hacker
Answer: B
The consultant was hired by the organization to test its cybersecurity and identify vulnerabilities. This is the role of a white hat hacker, also known as an ethical hacker.
Why White Hat Hacker?
* White hat hackers conduct security assessments legally and ethically to help organizations strengthen their cyber defenses.
* The consultant demonstrated SQL injection attacks in a controlled manner to expose weaknesses without malicious intent.
* Ethical hacking is a recognized practice under cybersecurity frameworks like NIST and ISO 27001.
* A. Cybercriminal - Engages in illegal hacking for personal or financial gain, whereas the consultant was hired to help the organization.
* C. Cyberterrorist - Motivated by political or ideological goals, not cybersecurity testing.
* D. Black Hat Hacker - Malicious hackers who exploit vulnerabilities for personal benefit, unlike ethical hackers.
Why Not the Other Options?Thus, the correct answer is B. White Hat Hacker, as the consultant was conducting authorized penetration testing.
* CEH (Certified Ethical Hacker) Guidelines.
* National Institute of Standards and Technology (NIST) Cybersecurity Framework.
* OWASP Top Ten Security Risks (2023).
References in Ethics in Technology:

NO.2 What is the first step in ethical decision-making for an IT professional?
A. Choose an alternative
B. Develop a problem statement
C. Implement a solution
D. Identify alternatives
Answer: B
The first step in ethical decision-making for IT professionals is to develop a problem statement, which involves clearly identifying and defining the ethical issue at hand. Before choosing solutions, an IT professional must fully understand the nature and scope of the problem.
* Ethical Decision-Making Models - Models like the Kidder Ethical Decision-Making Model and Rest's Four-Component Model emphasize problem identification as the first step.
* ACM Code of Ethics - Encourages IT professionals to assess issues carefully before taking action.
* Deontological Ethics (Kantian Ethics) - Ethical decisions require a clear understanding of duty and obligations, which begins with defining the problem.

* Business & IT Governance (COBIT Framework) - Ethical IT management requires problem assessment before action.
Relevant Ethical References in Technology:Thus, the correct first step in ethical decision-making is B. Develop a problem statement

NO.3 An incident handler discovers an unauthorized change in the security key vault's database file, which caused a disclosure of confidential information. Which ethical issue does this incident pose?
A. Property
B. Privacy
C. Access
D. Accuracy
Answer: B
The unauthorized change in the security key vault's database led to the disclosure of confidential information, which directly impacts privacy. Privacy concerns the protection of personal and sensitive information from unauthorized access, use, or exposure.
When confidential data is leaked, it violates fundamental principles of data privacy and security, raising ethical issues about how sensitive information is managed and protected.
* Privacy Ethics (Warren & Brandeis, 1890) - Defined privacy as "the right to be let alone."
* Data Protection Regulations - GDPR (Europe), CCPA (California), and HIPAA (for health data) enforce ethical handling of personal information.
* Confidentiality Principle in Cybersecurity - Ensuring only authorized access to sensitive information aligns with professional ethical standards (e.g., ACM Code of Ethics, IEEE Ethics Code).
* Ethical Hacking & Incident Handling - Ethical frameworks emphasize preventing breaches that compromise privacy.
Relevant Ethical References in Technology:Thus, this incident primarily raises concerns about privacy, making option B the correct answer.

NO.4 An auto manufacturer is developing a new line of autonomous vehicles. Multiple accidents, including fatalities, involving competitors' autonomous vehicles have already occurred. Management is concerned about potential liability, reputational damage, and financial loss. In response, the system safety engineer conducts a review at each stage of the software development process to record, assess, and account for detected issues.
Which type of log is the system safety engineer using?
A. Risk
B. Change
C. Hazard
D. Defect
Answer: C
A hazard log is a structured record of potential dangers, risks, and safety concerns identified throughout the development of a system-particularly in high-risk industries like autonomous vehicles. The system safety engineer is tracking issues that could lead to accidents, fatalities, or legal consequences, which aligns with hazard logging.
Unlike risk logs (which document broader business risks) or defect logs (which track software bugs), a hazard log focuses specifically on safety risks.
* ISO 26262 (Automotive Safety Standard) - Requires systematic hazard logging in autonomous

vehicle development.
* Utilitarian Ethics & Public Safety - Tracking hazards minimizes harm to the public and ensures ethical AI deployment.
* Product Liability & Ethics (Tort Law) - Ethical and legal responsibility requires addressing known safety concerns.
* ACM & IEEE Safety Standards - Developers must document hazards and mitigate risks in AI- drive n systems.
Relevant Ethical References in Technology:Thus, the correct answer is C. Hazard, as the engineer is recording and assessing safety risks in autonomous vehicles.

NO.5 A malicious hacker takes over several computers via the internet and causes them to flood a target site with high volumes of data queries and other small tasks. Which type of attack is the hacker performing against the target site?
A. Zero-day exploit
B. Ransomware
C. Denial-of-service (DoS)
D. Worm
Answer: C
A Denial-of-Service (DoS) attack is a cyberattack in which a hacker floods a target system with an overwhelming amount of requests, causing it to crash, slow down, or become unavailable. In this scenario, the hacker takes over multiple computers and forces them to flood a target site, which is a Distributed Denial-of-Service (DDoS) attack, a more advanced form of DoS.
* Cybersecurity Ethics (ACM & IEEE Codes of Ethics) - DoS attacks violate ethical and legal principles, causing harm to organizations and users.
* Hacking Ethics (White Hat vs. Black Hat Ethics) - Ethical hackers prevent DoS attacks, whereas malicious hackers exploit vulnerabilities.
* Cybercrime Laws (Computer Fraud and Abuse Act, GDPR, CFAA) - DoS attacks are illegal and punishable under international cybersecurity laws.
* Utilitarian Perspective on Cybersecurity - Defending against DoS attacks protects public and private digital infrastructure, benefiting society.
Relevant Ethical References in Technology:Thus, the correct answer is C. Denial-of-service (DoS), as the hacker floods the target site with excessive data queries.

NO.6 A robotics company engages an IT firm to deliver a marketing software solution. During the project, the robotics company asks for additional features that were not in the initial contract. The IT firm's project leader is unsure whether it can deliver these features but verbally agrees to the scope change. On delivery, the robotics company notes that several of the additional features are not included and that because of this, the solution is not compatible with certain legacy systems the company did not initially disclose.
Which factor might have mitigated the problem if the IT firm's project leader had abided by a professional code of ethics?
A. Improving decision-making around agreeing to additional scopes
B. Avoiding the delivery of an incompatible solution
C. Minimizing scope creep requests from the customer
D. Understanding the legal implications of noncontractual agreements

Answer: A

NO.7 An organization gathers data using various technologies to optimize sales processes for its current and prospective customers. The data consists of demographic, geographic, and behavioral customer changes.
Which data collection method is the organization using?
A. Advanced surveillance
B. Electronic discovery
C. Workplace monitoring
D. Consumer profiling
Answer: D
Consumer profiling is the practice of collecting and analyzing consumer data-including demographic, geographic, and behavioral attributes-to optimize sales strategies, enhance marketing efforts, and personalize customer experiences.
In this scenario, the organization gathers various types of customer data to improve its sales processes, which is a clear example of consumer profiling rather than surveillance or workplace monitoring.
* Privacy and Data Ethics (GDPR, CCPA) - Consumer profiling raises ethical concerns about informed consent, transparency, and data protection.
* Big Data Ethics (Tene & Polonetsky, 2012) - Ethical consumer profiling must ensure fair use, avoidance of bias, and non-discriminatory practices.
* Utilitarian vs. Deontological Perspectives - While profiling improves customer experiences, it must not violate privacy rights or enable unethical targeting.
* ACM Code of Ethics - Encourages responsible collection, use, and protection of consumer data.
Relevant Ethical References in Technology:Thus, since the company is gathering consumer data to optimize sales, the correct answer is D. Consumer profiling.