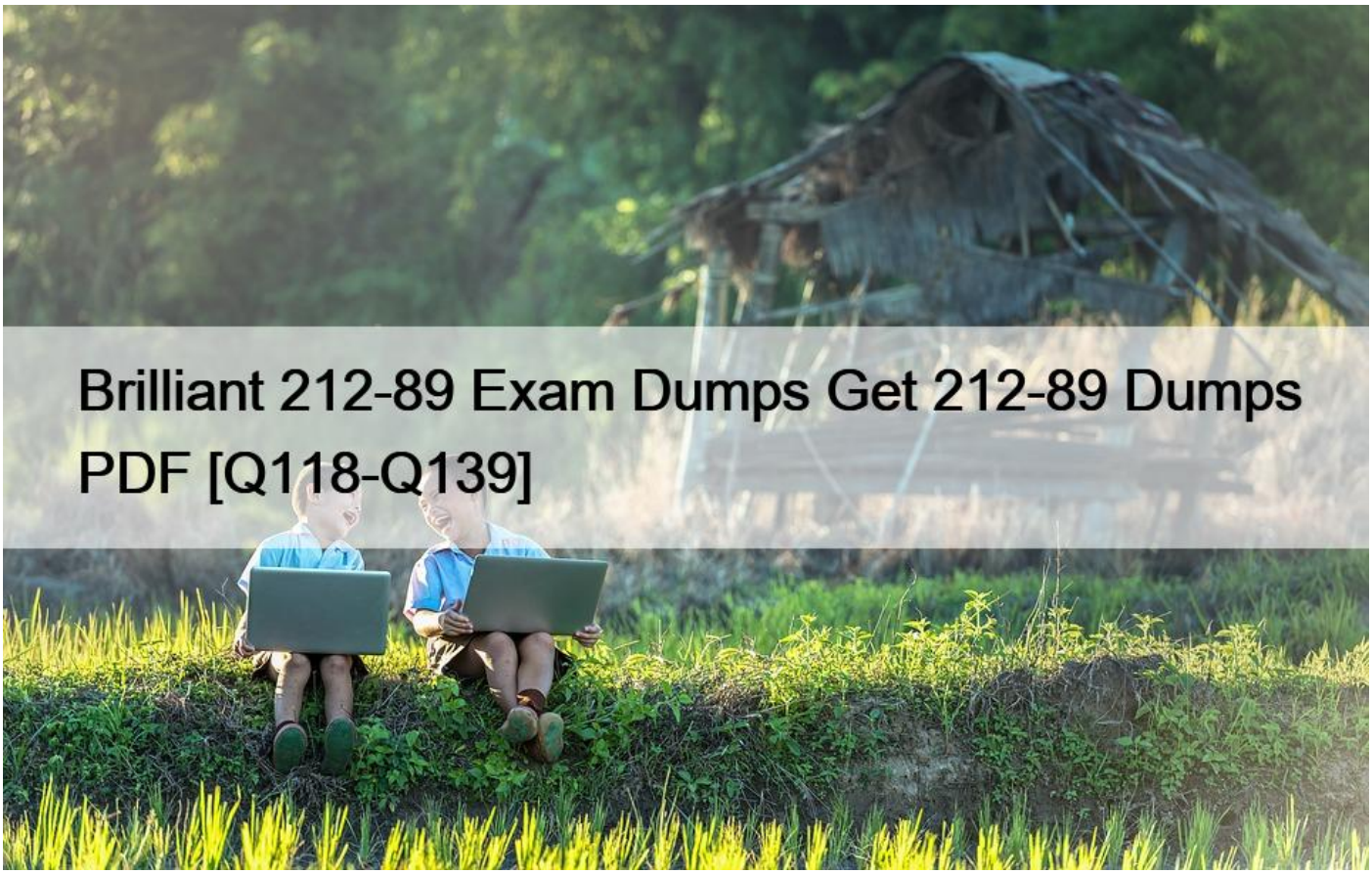
Brilliant 212-89 Exam Dumps Get 212-89 Dumps PDF [Q118-Q139



Brilliant 212-89 Exam Dumps Get 212-89 Dumps PDF
212-89 Dumps PDF - 212-89 Real Exam Questions Answers

Q118. Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

* To restore the original site, tests systems to prevent the incident and terminates operations
* To define the notification procedures, damage assessments and offers the plan activation
* To provide the introduction and detailed concept of the contingency plan
* To provide a sequence of recovery activities with the help of recovery procedures

Q119. Digital evidence must:

* Be Authentic, complete and reliable

* Not prove the attackers actions
* Be Volatile
* Cast doubt on the authenticity and veracity of the evidence

Q120. The ability of an agency to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy is known as:
* Business Continuity Plan
* Business Continuity
* Disaster Planning
* Contingency Planning

Q121. Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:
* Network and host log records
* Chain-of-Custody
* Forensic analysis report
* Chain-of-Precedence

Q122. One of the goals of CSIRT is to manage security problems by taking a certain approach towards the customers’ security vulnerabilities and by responding effectively to potential information security incidents. Identify the incident response approach that focuses on developing the infrastructure and security processes before the occurrence or detection of an event or any incident:
* Interactive approach
* Introductive approach
* Proactive approach
* Qualitative approach

Q123. In a qualitative risk analysis, risk is calculated in terms of:
* (Attack Success + Criticality) -(Countermeasures)
* Asset criticality assessment – (Risks and Associated Risk Levels)
* Probability of Loss X Loss
* (Countermeasures + Magnitude of Impact) – (Reports from prior risk assessments)

Q124. Introduction of malicious programs on to the device connected to the campus network (Trojan Horse, email bombs, virus, etc.) is called?
* Network Access
* Un authorize Access
* Inappropriate Usage
* Authorize Access

Q125. The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:
* If the insider’s technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
* If the insider’s technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.
* If the insider’s technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
* If the insider’s technical literacy and process knowledge are high, the risk posed by the threat will be high.

Q126. Jacobi san employee at a firm called Dolphin Investment. While he was on duty, he identified that his computer was facing some problems, and he wanted to convey the issue to the c once med authority in his organization. However, this organization

currently does not have a ticketing system to address such types of issues.

In the above scenario, which of the following ticketing systems can be employed by Dolphin Investment to allow Jacob to inform the c once med team about the incident?
* MISP
* Threat Connect
* ManageEngine ServiceDesk Plus
* IBM X Force Exchange

Q127. The goal of incident response is to handle the incident in a way that minimizes damage and reduces recovery time and cost. Which of the following does NOT constitute a goal of incident response?
* Dealing with human resources department and various employee conflict behaviors.
* Using information gathered during incident handling to prepare for handling future incidents in a better way and to provide stronger protection for systems and data.
* Helping personal to recover quickly and efficiently from security incidents, minimizing loss or theft and disruption of services.
* Dealing properly with legal issues that may arise during incidents.

Q128. Which of the following is not a countermeasure to eradicate cloud security incidents?
* Checking for data protection at both design and runtime
* Disabling security options such as two factor authentication and CAPTCHA
* Patching the database vulnerabilities and improving the isolation mechanism
* Removing the malware files and traces from the affected components

Q129. Which of the following terms may be defined as “a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization’s operation and revenues?
* Risk
* Vulnerability
* Threat
* Incident Response

Q130. An organization faced an information security incident where a disgruntled employee passed sensitive access

control information to a competitor. The organization’s incident response manager, upon investigation, found

that the incident must be handled within a few hours on the same day to maintain business continuity and

market competitiveness. How would you categorize such information security incident?
* High level incident
* Middle level incident
* Ultra-High level incident
* Low level incident

Q131. Which test is conducted to determine the incident recovery procedures effectiveness?
* Live walk-throughs of procedures
* Scenario testing
* Department-level test
* Facility-level test

Q132. Which of the following best describes an email issued as an attack medium, in which several messages are sent to a mailbox

to cause over fi ow?
* Spoofing
* Email-bombing
* Masquerading
* Smurf attack

Q133. James has been appointed as an incident handing and response (IH&R) team lead and was assigned to build an IH&R plan and his own team in the company. Identify the IH&R process step James is currently working on.
* Eradication
* Notification
* Preparation
* Recovery

Q134. Otis is an incident handler working in an organization called Delmont. Recently, the organization faced several setbacks in business, whereby its revenues are decreasing. Otis was asked to take charge and look into the matter. While auditing the enterprise security, he found traces of an attack through which proprietary information was stolen from the enterprise network and passed on to their competitors.

Which of the following information se cunty incidents did Delmont face?
* Email-based abuse
* Espionage
* Network and resource abuses
* Unauthorized access

Q135. Which among the following CERTs is an Internet provider to higher education institutions and various other research institutions in the Netherlands and deals with all cases related to computer security incidents in which a customer is involved either as a victim or as a suspect?
* NET-CERT
* DFN-CERT
* Funet CERT
* SURFnet-CERT

Q136. To effectively describe security incidents, it is necessary to adopt a common set of terminology and to categorize the incidents.

According to ECIH text, in which category would you place an incident that involves illegal file download by a suspected or unknown user?
* High level
* Low Level
* Middle level
* Ultra High Level

Q137. Your company sells SaaS, and your company itself is hosted in the cloud (using it as a PaaS).

In case of a malware incident in your customer’s database, who is responsible for eradicating the malicious software?
* The customer
* Your company
* The PaaS provider
* Building management

Q138. Which of the following encoding techniques replaces unusual ASCII characters with “%” followed by the character’s two-digit ASCII code expressed in hexadecimal?
* Unicode encoding
* URL encoding
* HTML encoding
* Base 64 encoding

Q139. Which of the following terms refers to vulnerable account management functions, including account update, recovery of forgotten or lost passwords, and password reset, that might weaken valid authentication schemes?
* Broken account management
* SQL injection
* Directory traversal
* Cross-site scripting

What Are Career Opportunities for ECIH Certified Specialists?

Once you pass the ECIH exam and achieve the related certification, there are many opportunities that you can enjoy. Some of the job titles you can readily apply for are: - IT Manager.- Security Analyst;- Cyber Forensic Investigator;- Risk Assessment Administrator;

When it comes to compensation, the average salary of the security analyst is around $69k per year, as revealed by Payscale.com, meanwhile, the income of a cyber forensic investigator is about $74k yearly as mentioned by the same site. Overall, you will see a drastic change in your salary when you achieve the ECIH certificate.

Valid 212-89 Test Answers & EC-COUNCIL 212-89 Exam PDF: https://www.vceprep.com/212-89-latest-vce-prep.html]