RC0-C02 Q&As

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A new piece of ransomware got installed on a company\\'s backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

A. Determining how to install HIPS across all server platforms to prevent future incidents

B. Preventing the ransomware from re-infecting the server upon restore

C. Validating the integrity of the deduplicated data

D. Restoring the data will be difficult without the application configuration

Correct Answer: D

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

QUESTION 2

The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO\\'s budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

A. The company should mitigate the risk.

B. The company should transfer the risk.

C. The company should avoid the risk.

D. The company should accept the risk.

Correct Answer: B

To transfer the risk is to deflect it to a third party, by taking out insurance for example.

QUESTION 3

A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have

been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company.

Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be $150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time

employee to respond to incidents per year.

Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company\\'s needs.

Bundled offering expected to be $100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.

Internal employee costs are averaged to be $80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

A. Based on cost alone, having an outsourced solution appears cheaper.

B. Based on cost alone, having an outsourced solution appears to be more expensive.

C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.

D. Based on cost alone, having a purchased product solution appears cheaper.

Correct Answer: A

The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the

company expense if $80,000 per year per FTE.

For the company to go alone it will cost $80,000 per annum per FTE = $400,000 over 5 years.

With Vendor a $150,000 + $200,000 (?FTE) = $350,000 With Vendor B = $100,000 it will be more expensive.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley and Sons, Indianapolis, 2012, p. 130

QUESTION 4

A business wants to start using social media to promote the corporation and to ensure that customers have a good experience with their products. Which of the following security items should the company have in place before implementation? (Select TWO).

A. The company must dedicate specific staff to act as social media representatives of the company.

B. All staff needs to be instructed in the proper use of social media in the work environment.

C. Senior staff blogs should be ghost written by marketing professionals.

D. The finance department must provide a cost benefit analysis for social media.

E. The security policy needs to be reviewed to ensure that social media policy is properly implemented.

F. The company should ensure that the company has sufficient bandwidth to allow for social media traffic.

Correct Answer: AE

QUESTION 5

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration

B. Security standards and training is performed as part of the project

C. Daily stand-up meetings are held to ensure security requirements are understood

D. For each major iteration penetration testing is performed

E. Security requirements are story boarded and make it into the build

F. A security design is performed at the end of the requirements phase

Correct Answer: AD

SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to

determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks.

Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs

is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.

For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.