H13-231 Valid Study Guide - Your Trusted Partner to Pass HCIE-Intelligent Computing V1.0 - Lagunamarine

Lagunamarine focusses on building trust among customers and therefore we provide a Demo File for H13-231 Exam Dumps, These experts spent a lot of time before the H13-231 study materials officially met with everyone, Huawei H13-231 Customized Lab Simulation Applying for refund is simple that you send email to us for applying refund attached your failure score scanned, All you need to do is just check your email and begin to practice the questions in our H13-231 Pass4sures questions.

We achieved many things that others said weren't possible, Integrated circuits **Customized H13-231 Lab Simulation** are much smallerâ€”both transistors and wires are shrunk to micrometer sizes, compared to the millimeter or centimeter scales of discrete components.

Presentation Slide Text: Less Is More, This is part of structuring **Customized H13-231 Lab Simulation** content effectively, The second book' is targeted to programmers, How long is it before the zone expires?

It takes sharp procurement professionals to keep Valid SS-101 Study Guide updating and building relationships in what becomes a trading community, We encourage applications from candidates representing a broad range of **Customized H13-231 Lab Simulation** disciplines including the social sciences, humanities, law, computer science and engineering.

When a Sun Linux system is installed, the line printing package H13-231 is installed, but needs to be configured, The study material can easily be understood and does not need any explanation.
HOT H13-231 Customized Lab Simulation: HCIE-Intelligent Computing V1.0 - The Best Huawei H13-231 Valid Study Guide Lagunamarine focusses on building trust among customers and therefore we provide a Demo File for H13-231 Exam Dumps, These experts spent a lot of time before the H13-231 study materials officially met with everyone.

Applying for refund is simple that you send email to us for applying refund attached your failure score scanned, All you need to do is just check your email and begin to practice the questions in our H13-231 Pass4sures questions.

We treat it as our blame if you accidentally fail the HCIE-Intelligent Computing V1.0 exam and as a blot to our responsibility, Our company has successfully launched the new version of the H13-231 study materials.

And with our H13-231 exam questions, If you get one certification successfully with help of our H13-231 exam prep

materials you can find a high-salary job in more OC-13 Interactive EBook than one hundred countries worldwide where these certifications are available.

If you are the person who is willing to get H13-231 exam prep, our products would be the perfect choice for you, We are the professional company providing high pass-rate H13-231 practice test file serving for people who are determined to apply for this corporation or corporate agents' positions.
H13-231 Pass4sure Valid Questions & H13-231 Free Download Study Files & H13-231 Pdf Download Guide
High as 98 to 100 percent of exam candidates pass the exam after refer to the help of our H13-231 practice braindumps, And H13-231 study materials provide free trial service for consumers.

Many common workers have achieved economic freedom after passing the H13-231 exams, And the materials will be sent to your relative mail boxes in ten minutes.

Don't need a lot of time and money, only 30 **Customized H13-231 Lab Simulation** hours of special training, and you can easily pass your first time to attend H13-231 Exam Bootcamp exam, Passing an HCIE-Intelligent Computing Certification H13-231 exam rewards you in the form of best career opportunities.

Lagunamarine can provide you with everything you need, The H13-231 troytec review and practice questions are created and tested by our IT experts who are working in big IT companies all over the world.

Avail the opportunity of H13-231 dumps at Lagunamarine that helps you in achieving good scores in the exam, In addition, you must buy some useful materials and test questions to increase your passing rate.

NEW QUESTION: 1
Which of the following is NOT an example of a detective control?
A. Backup data restore
B. System Monitor
C. IDS
D. Monitor detector
Answer: A
Explanation:
The word NOT is used as a keyword in the question. You need to find out a security control from an given options which in not detective control. Backup data restore is a corrective control and not a detective control.
For your exam you should know below information about different security controls
Deterrent Controls Deterrent Controls are intended to discourage a potential attacker. Access controls act as a

deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process

must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls Detective controls warn when something has happened, and are the earliest point in the postincident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several

situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations. For your exam you should know below information about different security controls Deterrent Controls Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a

user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial.

Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

The other examples are belongs to detective control.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

NEW QUESTION: 2
When implementing a 6to4 tunnel, which IPv6 address is the correct translation of the IPv4 address
192.168.99.1?
A. c0a8:6301:2002::/48
B. 2002:c0a8:6301::/48
C. 2002:c0a8:6301::/8
D. 2002::/16
Answer: B
Explanation:
16 bits for the most significant 6to4 reserved bits (2002::/16) plus 32 bits source ipv4 address (traslated in HEX format) = 48 bits,

NEW QUESTION: 3
A customer needs the devices in their non-secure network to communicate in a secure manner. They are considering implementing Kerberos network authentication in their environment.
Which impact will this have when using iLO 5 with their HPE ProLiant Gen10 servers?
A. It will enhance iLO security by leveraging the key stored in the silicon root of trust.
B. It will enable Zero Sign in to log in to iLO without entering a user name and password.
C. It will enable two-factor authentication when users log on to iLO.
D. It will allow the servers' iLO to detect compromised firmware code.
Answer: C

Reliable C-ARP2P-2108 Braindumps Ebook
C1000-128 Hot Spot Questions
Exam MO-101 Price
Test sca_cap2 Passing Score
H12-723-ENU Authorized Certification