[Feb 27, 2023 Latest CS0-002 PDF Dumps & Real Tests Free Updated Today [Q81-Q98

[Feb 27, 2023] Latest CS0-002 PDF Dumps & Real Tests Free Updated Today
CS0-002 Dumps With 100% Verified Q&As - Pass Guarantee or Full Refund

Conclusion

So, passing CS0-002 exam is your essential step towards being CompTIA CySA+ certified. Choose the best study guides, training courses and other options that suit you most and will assist you in preparation for this exam.
Keep in mind that the CySA+ certification is only valid for three years after you've taken the initial exam. You're required to complete 60 CEUs (Continuous Education Units) to remain certified after this period. The CEUs can be acquired via training or by earning related certifications. However, you would have to pay $50 to submit the completed activities and have your CEUs.

NEW QUESTION 81

A security analyst is reviewing the following log from an email security service.

```
Rejection type:          Drop
Rejection description:   IP found in RBL
Event time:              Today at 16:06
Rejection information:   mail.comptia.org
                         http://www.spamfilter.org/query?P=192.167.28.243

From address:            user@comptex.org
To address:              tests@comptia.org
IP address:              192.167.28.243
Remote server name:      192.167.28.243
```


Which of the following BEST describes the reason why the email was blocked?
* The To address is invalid.
* The email originated from the www.spamfilter.org URL.
* The IP address and the remote server name are the same.
* The IP address was blacklisted.
* The From address is invalid.

NEW QUESTION 82

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?
* An IPS signature modification for the specific IP addresses
* An IDS signature modification for the specific IP addresses
* A firewall rule that will block port 80 traffic
* A firewall rule that will block traffic from the specific IP addresses

NEW QUESTION 83

A cybersecurity analyst is conducting packet analysis on the following:

Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010281	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044812	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:43:b3:3f:23:e3
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:43:b3:3f:23:e3

Which of the following is occurring in the given packet capture?
* ARP spoofing
* Broadcast storm
* Smurf attack
* Network enumeration
* Zero-day exploit

NEW QUESTION 84

A security administrator has uncovered a covert channel used to exfiltrate confidential data from an internal database server through a compromised corporate web server. Ongoing exfiltration is accomplished by embedding a small amount of data extracted from the database into the metadata of images served by the web server. File timestamps suggest that the server was initially compromised six months ago using a common server misconfiguration. Which of the following BEST describes the type of threat being used?
* APT
* Zero-day attack
* Man-in-the-middle attack
* XSS

NEW QUESTION 85

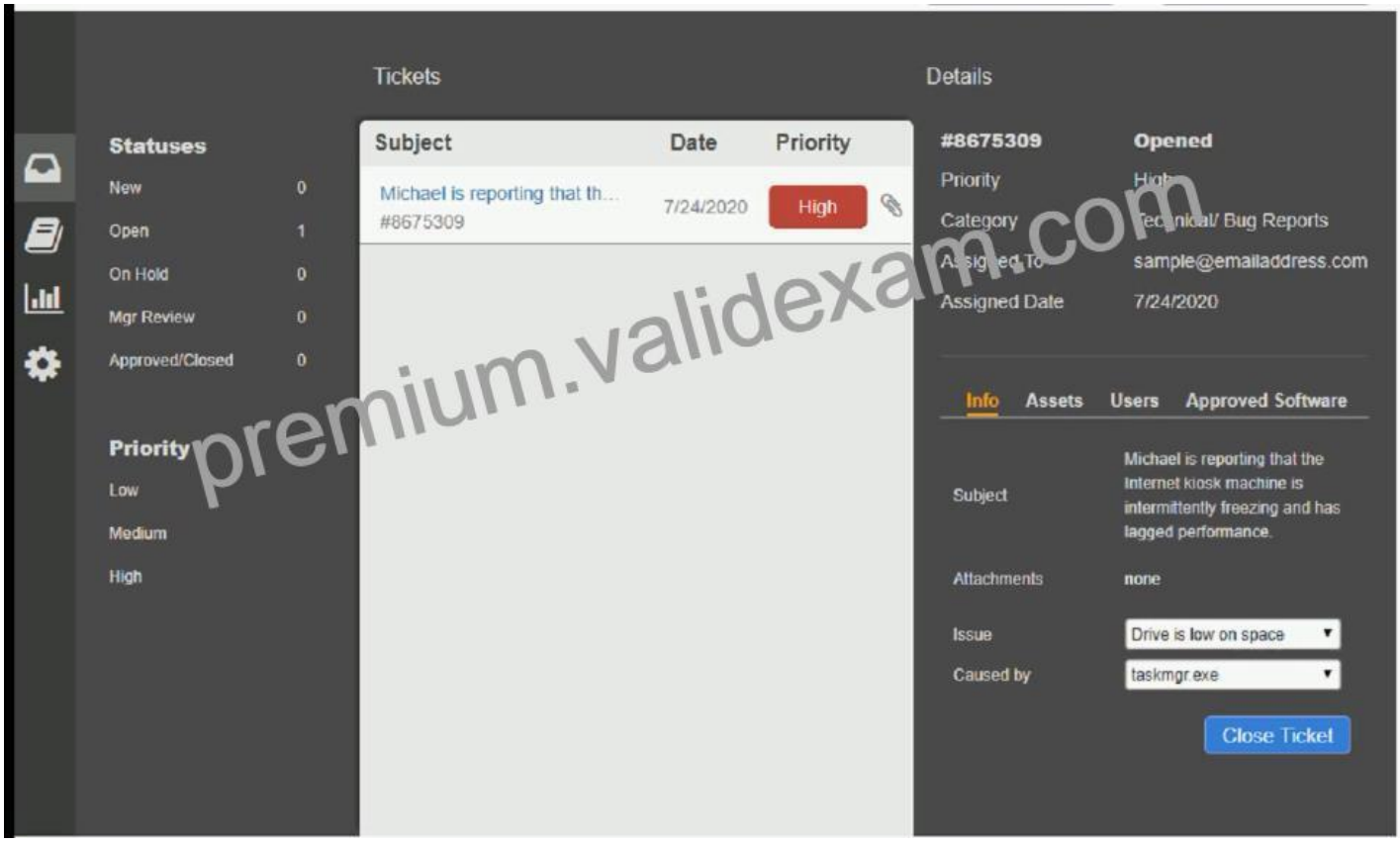
While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?
* Block the sender In the email gateway.
* Delete the email from the company’s email servers.
* Ask the sender to stop sending messages.
* Review the message in a secure environment.

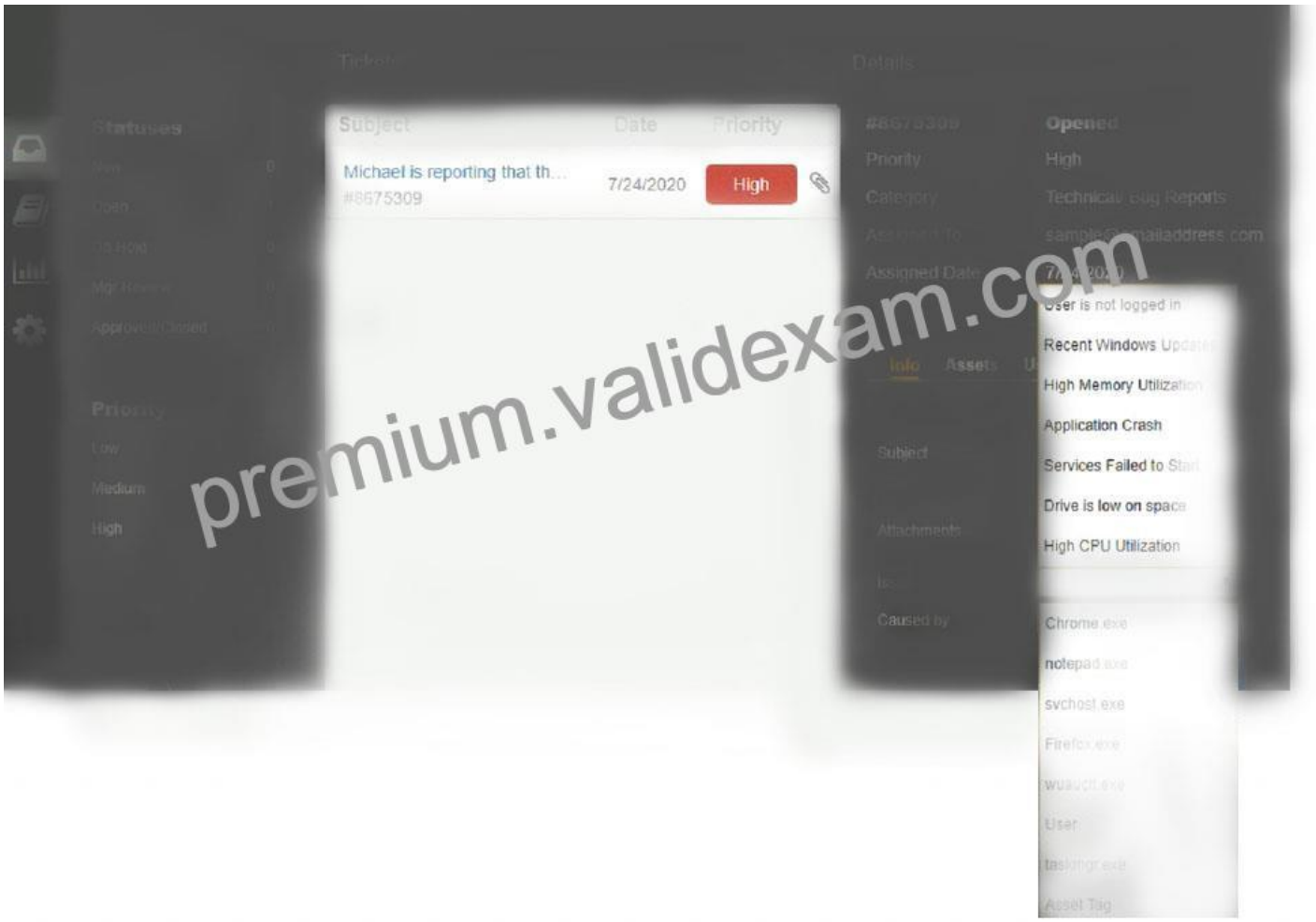
NEW QUESTION 86

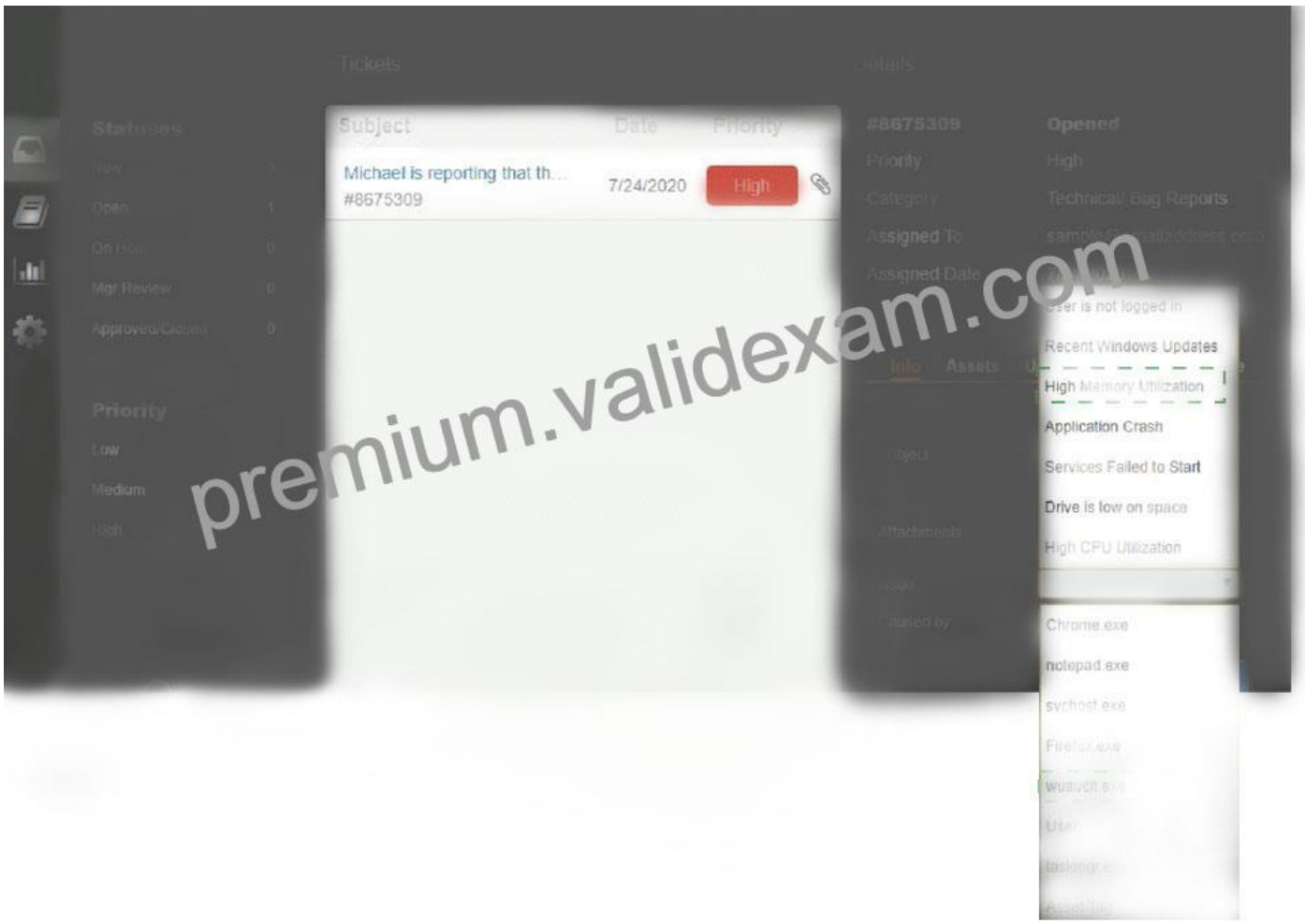
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.

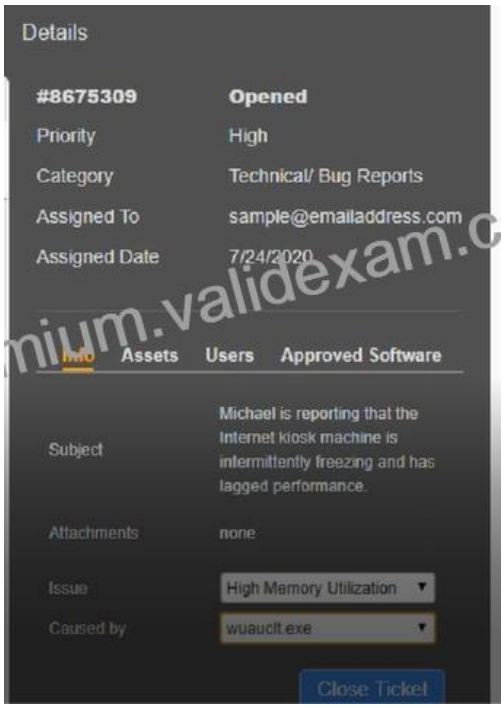
INSTRUCTIONS

Click on me ticket to see the ticket details Additional content is available on tabs within the ticket First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu If at any time you would like to bring back the initial state of the simulation, please click the Reset All button









NEW QUESTION 87

Management is concerned with administrator access from outside the network to a key server in the company. Specifically, firewall rules allow access to the server from anywhere in the company. Which of the following would be an effective solution?
* Honeypot
* Jump box
* Server hardening
* Anti-malware

NEW QUESTION 88

An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC.

Which of the following is the BEST approach for supply chain assessment when selecting a vendor?
* Gather information from providers, including datacenter specifications and copies of audit reports.
* Identify SLA requirements for monitoring and logging.
* Consult with senior management for recommendations.
* Perform a proof of concept to identify possible solutions.

NEW QUESTION 89

A company’s asset management software has been discovering a weekly increase in non- standard software installed on end users’ machines with duplicate license keys. The security analyst wants to know if any of this software is listening on any non-standard ports, such as 6667.

Which of the following tools should the analyst recommend to block any command and control traffic?
* Netstat
* NIDS
* IPS
* HIDS

NEW QUESTION 90

As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?
* Organizational policies
* Vendor requirements and contracts
* Service-level agreements
* Legal requirements

NEW QUESTION 91

Given the following access log:

```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get
/js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c1%3ba=e(HTTP/1.1" 403 22

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height | |
1;a=e( HTTP/1.1" 303 333

access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option;F .tbody=F
.tfoot=F .colorgroup=F .caption=F .thread;F .th=F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1"
403 338
```

Which of the following accurately describes what this log displays?
* A vulnerability in jQuery
* Application integration with an externally hosted database
* A vulnerability scan performed from the Internet
* A vulnerability in Javascript

NEW QUESTION 92

Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).
* To establish a clear chain of command
* To meet regulatory requirements for timely reporting
* To limit reputation damage caused by the breach
* To remediate vulnerabilities that led to the breach
* To isolate potential insider threats
* To provide secure network design changes

NEW QUESTION 93

An information security analyst is compiling data from a recent penetration test and reviews the following output:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 16:06 UTC
Nmap scan report for 10.79.95.173.rdns.datacenters.com (10.79.95.173)
Host is up (0.026s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Microsoft ftpd
22/tcp   open  ssh     SilverSHielD sshd (protocol 2.0)
80/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  https?
691/tcp  open  resvc?
5060/tcp open  sip     Barracuda NG Firewall (Status: 200 OK)
Nmap done: 1 IP address (1 host up) scanned in 158.22 seconds
```

The analyst wants to obtain more information about the web-based services that are running on the target.

Which of the following commands would MOST likely provide the needed information?
* ping -t 10.79.95.173.rdns.datacenters.com
* telnet 10.79.95.173 443
* ftpd 10.79.95.173.rdns.datacenters.com 443
* tracert 10.79.95.173

NEW QUESTION 94

A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor’s instructions and generated a report of vulnerabilities that ran against the same target server.

Tool A reported the following:

```
The target host (192.168.10.13) is missing the following patches:
CRITICAL KB50227328: Windows Server 2016 June 2019 Cumulative Update
CRITICAL KB50255293: Windows Server 2016 July 2019 Cumulative Update
HIGH MS19-055: Cumulative Security Update for Edge (2863871)
```

Tool B reported the following:

```
Methods GET HEAD OPTIONS POST TRACE are allowed on 192.168.10.13:80
192.168.10.13:443 uses a self-signed certificate
Apache 4.2.x < 4.2.28 Contains Multiple Vulnerabilities
```

Which of the following BEST describes the method used by each tool? (Choose two.)
* Tool A is agent based.
* Tool A used fuzzing logic to test vulnerabilities.
* Tool A is unauthenticated.
* Tool B utilized machine learning technology.
* Tool B is agent based.
* Tool B is unauthenticated.

NEW QUESTION 95

When reviewing a compromised authentication server, a security analyst discovers the following hidden file:

```
root@ldap1:~# cat .pass.txt
jsmith:Welcome123:18073:0:99999:7:::
mjones4:Welcome123:18073:0:99999:7:::
egreen1:Welcome123:18073:0:99999:7:::
rbarger:Welcome123:18073:0:99999:7:::
mhemm1:Welcome123:18073:0:99999:7:::
mgill:Welcome123:18073:0:99999:7:::
cyoung1:Welcome123:18073:0:99999:7:::
gkiepper3:Welcome123:18073:0:99999:7:::
```

Further analysis shows these users never logged in to the server. Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?
* A rogue LDAP server is installed on the system and is connecting passwords. The analyst should recommend wiping and reinstalling the server.
* A password spraying attack was used to compromise the passwords. The analyst should recommend that all users receive a unique password.
* A rainbow tables attack was used to compromise the accounts. The analyst should recommend that future password hashes contains a salt.

* A phishing attack was used to compromise the account. The analyst should recommend users install endpoint protection to disable phishing links.

NEW QUESTION 96

An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?
* Tokenization of sensitive data
* Establishment o’ data classifications
* Reporting on data retention and purging activities
* Formal identification of data ownership
* Execution of NDAs

NEW QUESTION 97

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application.

Which of the following is a security concern when using a PaaS solution?
* The use of infrastructure-as-code capabilities leads to an increased attack surface.
* Patching the underlying application server becomes the responsibility of the client.
* The application is unable to use encryption at the database level.
* Insecure application programming interfaces can lead to data compromise.

NEW QUESTION 98

An organization’s internal department frequently uses a cloud provider to store large amounts of sensitive dat a. A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?
* Sandbox the virtual machine.
* Implement an MFA solution.
* Update lo the secure hypervisor version.
* Implement dedicated hardware for each customer.

2023 Valid CS0-002 test answers & CompTIA Exam PDF: https://www.validexam.com/CS0-002-latest-dumps.html]