



SY0-501^{Q&As}

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

<https://www.lead4pass.com/sy0-501.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

1.
All access must be correlated to a user account.
2.
All user accounts must be assigned to a single individual.
3.
User access to the PHI data must be recorded.
4.
Anomalies in PHI data access must be reported.
5.
Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Select three.)

- A. Eliminate shared accounts.
- B. Create a standard naming convention for accounts.
- C. Implement usage auditing and review.
- D. Enable account lockout thresholds.
- E. Copy logs in real time to a secured WORM drive.
- F. Implement time-of-day restrictions.
- G. Perform regular permission audits and reviews.

Correct Answer: ACG

QUESTION 2

For each of the given items, select the appropriate authentication category from the drop down choices.



Item	Response
Fingerprint scan	<input type="text"/>
Hardware token	<input type="text"/>
Smart card	<input type="text"/>
Password	<input type="text"/>
PIN number	<input type="text"/>
Retina Scan	<input type="text"/>

Select the appropriate authentication type for the following items:

Hot Area:



Item	Response
Fingerprint scan	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
PIN number	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Retina Scan	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication



Correct Answer:



Item	Response
Fingerprint scan	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Hardware token	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Smart card	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Password	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
PIN number	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Retina Scan	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication



Biometrics refers to a collection of physical attributes of the human body that can be used as identification or an authentication factor. Fingerprints and retinas are physical attributes of the human body.

Two types of tokens exist, Time-based one-time password (TOTP) tokens and HMACbased one-time password (HOTP). TOTP tokens generate passwords at fixed time intervals, whereas HOTP tokens generate passwords not based on fixed

time intervals but instead based on a non-repeating one-way function, such as a hash or HMAC operation.

Smart cards can have Multi-factor and proximity authentication embedded into it.

PAP allows for two entities to share a password in advance and use the password as the basis of authentication. The same goes for PIN numbers.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 282, 285

http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle

http://en.wikipedia.org/wiki/Smart_card#Security

QUESTION 3

DRAG DROP

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.

Select and Place:



Correct Answer:



QUESTION 4

Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

- A. Retinal scan
- B. Passphrase
- C. Token fob
- D. Security question

Correct Answer: C

QUESTION 5

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?



- A. Remote wipe
- B. Full device encryption
- C. BIOS password
- D. GPS tracking

Correct Answer: B

[Latest SY0-501 Dumps](#)

[SY0-501 Practice Test](#)

[SY0-501 Study Guide](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.