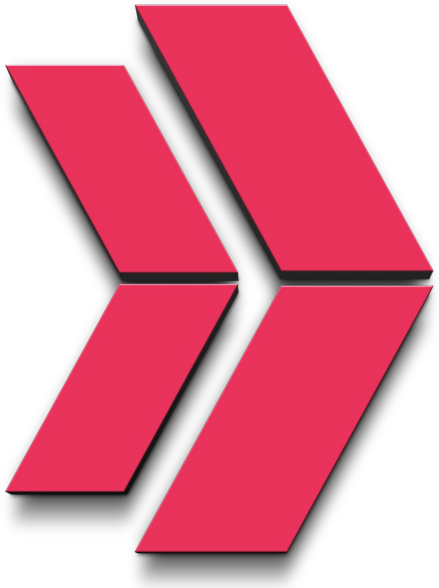


CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (4A-4B-4C)

AGENDA

- 4A - Authentication (5)
- 4B - Authorization (13)
- 4C - Identity Management (6)
- TOTAL: 24

4A - Authentication

4A - Authentication

NO.1 A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

A. Data masking
B. Encryption
C. Geolocation policy
D. Data sovereignty regulation

4A - Authentication

NO.1 A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

A. Data masking
B. Encryption
C. Geolocation policy
D. Data sovereignty regulation

4A - Authentication

NO.2 A network manager wants to protect the company's VPN by implementing multi factor authentication that uses: - Something you know - Something you have - Something you are Which of the following would accomplish the manager's goal?

A. Domain name, PKI, GeolP lookup
B. VPN IP address, company ID, facial structure
C. Password, authentication token, thumbprint
D. Company URL, TLS certificate, home address

4A - Authentication

NO.2 A network manager wants to protect the company's VPN by implementing multi factor authentication that uses: - Something you know - Something you have - Something you are Which of the following would accomplish the manager's goal?

A. Domain name, PKI, GeolP lookup
B. VPN IP address, company ID, facial structure
C. Password, authentication token, thumbprint
D. Company URL, TLS certificate, home address

4A - Authentication

NO.3 An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multi factor authentication
B. Permissions assignment
C. Access management
D. Password complexity

4A - Authentication

NO.3 An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multi factor authentication
B. Permissions assignment
C. Access management
D. Password complexity

4A - Authentication

NO.4 A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can Integrate easily into a user's workflow, and can utilize employee-owned devices.

Which of the following will meet these requirements?

A. Push notifications

B. Phone call

C. Smart card

D. Offline backup codes

4A - Authentication

NO.4 A company is currently utilizing usernames and passwords, and it wants to **integrate an MFA method** that is seamless, can Integrate easily into a user's workflow, and can utilize employee-owned devices.

Which of the following will meet these requirements?

A. Push notifications

B. Phone call

C. Smart card

D. Offline backup codes

4A - Authentication

NO.5 Which of the following best describes why the SMS OTP authentication method is more risky to implement than the TOTP method?

A. The SMS OTP method requires an end user to have an active mobile telephone service and SIM card.
B. Generally. SMS OTP codes are valid for up to 15 minutes while the TOTP time frame is 30 to 60 seconds
C. The SMS OTP is more likely to be intercepted and lead to unauthorized disclosure of the code than the TOTP method.
D. The algorithm used to generate on SMS OTP code is weaker than the one used to generate a TOTP code

4A - Authentication

NO.5 Which of the following best describes why the SMS OTP authentication method is more risky to implement than the TOTP method?

A. The SMS OTP method requires an end user to have an active mobile telephone service and SIM card.
B. Generally. SMS OTP codes are valid for up to 15 minutes while the TOTP time frame is 30 to 60 seconds
C. The SMS OTP is more likely to be intercepted and lead to unauthorized disclosure of the code than the TOTP method.
D. The algorithm used to generate on SMS OTP code is weaker than the one used to generate a TOTP code

4B - Authorization

4B - Authorization

NO.1 A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

A. Attribute-based
B. Time of day
C. Role-based
D. Least privilege

4B - Authorization

NO.1 A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

A. Attribute-based
B. Time of day
C. Role-based
D. Least privilege

4B - Authorization

NO.2 An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

4B - Authorization

NO.2 An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

4B - Authorization

NO.3 Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

A. Provisioning resources
B. Disabling access
C. Reviewing change approvals
D. Escalating permission requests

4B - Authorization

NO.3 Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

A. Provisioning resources
B. Disabling access
C. Reviewing change approvals
D. Escalating permission requests

4B - Authorization

NO.4 A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

A. If a security incident occurs on the device, the correct employee can be notified.
B. The security team will be able to send user awareness training to the appropriate device.
C. Users can be mapped to their devices when configuring software MFA tokens.
D. User-based firewall policies can be correctly targeted to the appropriate laptops.
E. When conducting penetration testing, the security team will be able to target the desired laptops.
F. Company data can be accounted for when the employee leaves the organization.

4B - Authorization

NO.4 A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

A. If a security incident occurs on the device, the correct employee can be notified.
B. The security team will be able to send user awareness training to the appropriate device.
C. Users can be mapped to their devices when configuring software MFA tokens.
D. User-based firewall policies can be correctly targeted to the appropriate laptops.
E. When conducting penetration testing, the security team will be able to target the desired laptops.
F. Company data can be accounted for when the employee leaves the organization.

4B - Authorization

NO.5 An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

A. Hardening
B. Employee monitoring
C. Configuration enforcement
D. Least privilege

4B - Authorization

NO.5 An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

A. Hardening
B. Employee monitoring
C. Configuration enforcement
D. Least privilege

4B - Authorization

NO.6 A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC
B. ACL
C. SAML
D. GPO

4B - Authorization

NO.6 A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC
B. ACL
C. SAML
D. GPO

4B - Authorization

NO.7 A systems administrator is working on a defense-in-depth strategy and needs to restrict activity from employees after hours.

Which of the following should the systems administrator implement?

A. Role-based restrictions
B. Attribute-based restrictions
C. Mandatory restrictions
D. Time-of-day restrictions

4B - Authorization

NO.7 A systems administrator is working on a defense-in-depth strategy and needs to **restrict activity from employees after hours.**

Which of the following should the systems administrator implement?

A. Role-based restrictions
B. Attribute-based restrictions
C. Mandatory restrictions
D. Time-of-day restrictions

4B - Authorization

NO.8 During a recent breach, employee credentials were compromised when a service desk employee issued an MFA bypass code to an attacker who called and posed as an employee.

Which of the following should be used to prevent this type of incident in the future?

A. Hardware token MFA
B. Biometrics
C. Identity proofing
D. Least privilege

4B - Authorization

NO.8 During a recent breach, employee credentials were compromised when a service desk employee **issued an MFA bypass code** to an attacker who called and posed as an employee.

Which of the following should be used to prevent this type of incident in the future?

A. Hardware token MFA
B. Biometrics
C. Identity proofing
D. Least privilege

4B - Authorization

NO.9 An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group.

Which of the following access controls is most likely causing the lack of access?

A. Role-based
B. Discretionary
C. Time of day
D. Least privilege

4B - Authorization

NO.9 An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the **account was never moved to the new group.**

Which of the following access controls is most likely causing the lack of access?

A. Role-based
B. Discretionary
C. Time of day
D. Least privilege

4B - Authorization

NO.10 A security administrator is configuring fileshares. The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties.

Which of the following best describes why the administrator performed these actions?

A. Encryption standard compliance
B. Data replication requirements
C. Least privilege
D. Access control monitoring

4B - Authorization

NO.10 A security administrator is **configuring fileshares**. The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties.

Which of the following best describes why the administrator performed these actions?

A. Encryption standard compliance
B. Data replication requirements
C. Least privilege
D. Access control monitoring

4B - Authorization

NO.11 Which of the following best describe why a process would require a two-person integrity security control?

A. To Increase the chance that the activity will be completed in half of the time the process would take only one user to complete
B. To permit two users from another department to observe the activity that is being performed by an authorized user
C. To reduce the risk that the procedures are performed incorrectly or by an unauthorized user
D. To allow one person to perform the activity while being recorded on the CCTV camera

4B - Authorization

NO.11 Which of the following best describe why a process would require a **two-person integrity security control**?

A. To Increase the chance that the activity will be completed in half of the time the process would take only one user to complete

B. To permit two users from another department to observe the activity that is being performed by an authorized user

C. To reduce the risk that the procedures are performed incorrectly or by an unauthorized user

D. To allow one person to perform the activity while being recorded on the CCTV camera

4B - Authorization

NO.12 Which of the following is best used to detect fraud by assigning employees to different roles?

A. Least privilege
B. Mandatory vacation
C. Separation of duties
D. Job rotation

4B - Authorization

NO.12 Which of the following is best used to **detect fraud** by assigning employees to different roles?

A. Least privilege
B. Mandatory vacation
C. Separation of duties
D. Job rotation

4B - Authorization

NO.13 An employee recently resigned from a company. The employee was responsible for managing and supporting weekly batch jobs over the past five years. A few weeks after the employee resigned. one of the batch jobs talked and caused a major disruption.

Which of the following would work best to prevent this type of incident from reoccurring?

A. Job rotation

B. Retention

C. Outsourcing

D. Separation of duties

4B - Authorization

NO.13 An employee recently resigned from a company. The employee was responsible for managing and supporting weekly batch jobs over the past five years. A few weeks after the employee resigned. one of the batch jobs talked and caused a major disruption.

Which of the following would work best to prevent this type of incident from reoccurring?

A. Job rotation

B. Retention

C. Outsourcing

D. Separation of duties

4C - Identity Management

4C - Identity Management

NO.1 An internet company has created a new collaboration application. To expand the user base, the company wants to implement an option that allows users to log in to the application with the credentials of other popular websites. Which of the following should the company implement?

A. SSO
B. CHAP
C. 802.1x
D. OpenID

4C - Identity Management

NO.1 An internet company has created a new collaboration application. To expand the user base, the company wants to implement an option that allows users to log in to the application with the credentials of other popular websites. Which of the following should the company implement?

A. SSO
B. CHAP
C. 802.1x
D. OpenID

4C - Identity Management

NO.2 A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A. SSO
B. LEAP
C. MFA
D. PEAP

4C - Identity Management

NO.2 A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A. SSO
B. LEAP
C. MFA
D. PEAP

4C - Identity Management

NO.3 During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company- owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

4C - Identity Management

NO.3 During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company- owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

4C - Identity Management

NO.4 A security analyst needs to propose a remediation plan for each item in a risk register. The item with the highest priority requires employees to have separate logins for SaaS solutions and different password complexity requirements for each solution.

Which of the following implementation plans will most likely resolve this security issue?

A. Creating a unified password complexity standard

B. Integrating each SaaS solution with the Identity provider

C. Securing access to each SaaS by using a single wildcard certificate

D. Configuring geofencing on each SaaS solution

4C - Identity Management

NO.4 A security analyst needs to propose a remediation plan for each item in a risk register. The item with the highest priority requires employees to have **separate logins for SaaS solutions** and different **password complexity** requirements for each solution.

Which of the following implementation plans will most likely resolve this security issue?

A. Creating a unified password complexity standard

B. Integrating each SaaS solution with the Identity provider

C. Securing access to each SaaS by using a single wildcard certificate

D. Configuring geofencing on each SaaS solution

4C - Identity Management

NO.5 An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in so the security team wants to reduce the number of credentials each employee must maintain.

Which of the following is the first step the security team should take?

A. Enable SAML

B. Create OAuth tokens.

C. Use password vaulting.

D. Select an IdP

4C - Identity Management

NO.5 An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in so the security team wants to **reduce the number of credentials each employee must maintain.**

Which of the following is the first step the security team should take?

A. Enable SAML

B. Create OAuth tokens.

C. Use password vaulting.

D. Select an IdP

4C - Identity Management

NO.6 A company is implementing a vendor's security tool in the cloud. The security director does not want to manage users and passwords specific to this tool but would rather utilize the company's standard user directory.

Which of the following should the company implement?

A. 802.1X

B. SAML

C. RADIUS

D. CHAP

4C - Identity Management

NO.6 A company is implementing a vendor's security tool in the cloud. The security director does not want to manage users and passwords specific to this tool but would rather **utilize the company's standard user directory.**

Which of the following should the company implement?

A. 802.1X

B. SAML

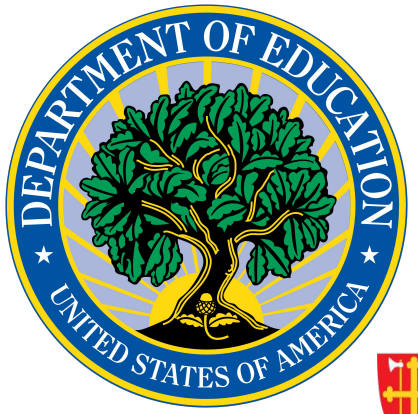
C. RADIUS

D. CHAP

THANKS!

Any questions?

Our Graduates are Hired By



Google

Deloitte.

AT&T

ally
do it right.

DEN NORSKE KIRKE
Kirkepartner

Robinhood

VIZNET

COMCAST

INSPARK

ING BANK

proValus

SOCRadar®
Extension to Your SOC Team!

AGILIS
TECHNOLOGIES

Humana
Wellness

EQUANS

BBS

BGA
SECURITY

gravity
IT RESOURCES

GetMoneyGlobal

proximus

northramp

ease
LEARNING