



# CLARUSWAY

WAY TO REINVENT YOURSELF



# CompTIA (10A-10B)

# AGENDA



- ▶ **10A - Implement Endpoint Security (17)**
- ▶ **10B - Mobile Device Hardening (1)**
- ▶ **TOTAL: 18**



# **10A - Implement Endpoint Security**

# 10A - Implement Endpoint Security



**NO.1** A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

- (A). Deploying PowerShell scripts
- (B). Pushing GPO update
- (C). Enabling PAP
- (D). Updating EDR profiles

# 10A - Implement Endpoint Security



**NO.1** A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

(A). Deploying PowerShell scripts

(B). Pushing GPO update

(C). Enabling PAP

(D). Updating EDR profiles

# 10A - Implement Endpoint Security



**NO.2** A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would best detect the presence of a rootkit in the future?

- (A). FDE
- (B). NIDS
- (C). EDR
- (D). DLP

# 10A - Implement Endpoint Security



**NO.2** A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would best detect the presence of a rootkit in the future?

(A). FDE

(B). NIDS

(C). EDR

(D). DLP



# 10A - Implement Endpoint Security



**NO.3** A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

- (A). Hashing
- (B). Tokenization
- (C). Encryption
- (D). Segmentation

# 10A - Implement Endpoint Security



**NO.3** A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

- (A). Hashing
- (B). Tokenization
- (C). Encryption
- (D). Segmentation

# 10A - Implement Endpoint Security



**NO.4** A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

- (A). Host-based firewall
- (B). Web application firewall
- (C). Access control list
- (D). Application allow list

# 10A - Implement Endpoint Security



**NO.4** A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

(A). Host-based firewall

(B). Web application firewall

(C). Access control list

(D). Application allow list

# 10A - Implement Endpoint Security



**NO.5** A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

- (A). Place posters around the office to raise awareness of common phishing activities
- (B). Implement email security filters to prevent phishing emails from being delivered
- (C). Update the EDR policies to block automatic execution of downloaded programs
- (D). Create additional training for users to recognize the signs of phishing attempts

# 10A - Implement Endpoint Security



**NO.5** A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

- (A). Place posters around the office to raise awareness of common phishing activities
- (B). Implement email security filters to prevent phishing emails from being delivered
- (C). Update the EDR policies to block automatic execution of downloaded programs
- (D). Create additional training for users to recognize the signs of phishing attempts

# 10A - Implement Endpoint Security



**NO.6** A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

- (A). SPF
- (B). GPO
- (C). NAC
- (D). FIM

# 10A - Implement Endpoint Security



**NO.6** A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

- (A). SPF
- (B). GPO
- (C). NAC
- (D). FIM



# 10A - Implement Endpoint Security



**NO.7** Which of the following can best protect against an employee inadvertently installing malware on a company system?

- (A). Host-based firewall
- (B). System isolation
- (C). Least privilege
- (D). Application allow list

# 10A - Implement Endpoint Security



**NO.7** Which of the following can best protect against an employee inadvertently installing malware on a company system?

- (A). Host-based firewall
- (B). System isolation
- (C). Least privilege
- (D). Application allow list

# 10A - Implement Endpoint Security



**NO.8** An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

- (A). Segmentation
- (B). Isolation
- (C). Patching
- (D). Encryption

# 10A - Implement Endpoint Security



**NO.8** An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

(A). Segmentation

(B). Isolation

(C). Patching

(D). Encryption

# 10A - Implement Endpoint Security



**NO.9** Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

- (A). IDS
- (B). ACL
- (C). EDR
- (D). NAC

# 10A - Implement Endpoint Security



**NO.9** Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

- (A). IDS
- (B). ACL
- (C). EDR
- (D). NAC

# 10A - Implement Endpoint Security



**NO.10** A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

- (A). Partition
- (B). Asymmetric
- (C). Full disk
- (D). Database

# 10A - Implement Endpoint Security



**NO.10** A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

- (A). Partition
- (B). Asymmetric
- (C). Full disk
- (D). Database



# 10A - Implement Endpoint Security



**NO.11** Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

- (A). Configure all systems to log scheduled tasks
- (B). Collect and monitor all traffic exiting the network
- (C). Block traffic based on known malicious signatures
- (D). Install endpoint management software on all systems

# 10A - Implement Endpoint Security



**NO.11** Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

- (A). Configure all systems to log scheduled tasks
- (B). Collect and monitor all traffic exiting the network
- (C). Block traffic based on known malicious signatures
- (D). Install endpoint management software on all systems

# 10A - Implement Endpoint Security



**NO.12** Which of the following would be the best way to block unknown programs from executing?

- (A). Access control list
- (B). Application allow list
- (C). Host-based firewall
- (D). DLP solution

# 10A - Implement Endpoint Security



**NO.12** Which of the following would be the best way to block unknown programs from executing?

- (A). Access control list
- (B). Application allow list
- (C). Host-based firewall
- (D). DLP solution

# 10A - Implement Endpoint Security



**NO.13** Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

- (A). The device has been moved from a production environment to a test environment
- (B). The device is configured to use cleartext passwords
- (C). The device is moved to an isolated segment on the enterprise network
- (D). The device is moved to a different location in the enterprise
- (E). The device's encryption level cannot meet organizational standards
- (F). The device is unable to receive authorized updates

# 10A - Implement Endpoint Security



**NO.13** Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

- (A). The device has been moved from a production environment to a test environment
- (B). The device is configured to use cleartext passwords
- (C). The device is moved to an isolated segment on the enterprise network
- (D). The device is moved to a different location in the enterprise
- (E). The device's encryption level cannot meet organizational standards
- (F). The device is unable to receive authorized updates

# 10A - Implement Endpoint Security



**NO.14** A company implemented an MDM policy to mitigate risks after repeated instances of employees losing company-provided mobile phones. In several cases, the lost phones were used maliciously to perform social engineering attacks against other employees.

Which of the following MDM features should be configured to best address this issue? (Select two).

- A. Screen locks
- B. Remote wipe
- C. Full device encryption
- D. Push notifications
- E. Application management
- F. Geolocation

# 10A - Implement Endpoint Security



**NO.14** A company implemented an **MDM policy** to mitigate risks after repeated instances of employees losing company-provided mobile phones. In several cases, the lost phones were used maliciously to perform social engineering attacks against other employees.

Which of the following MDM features should be configured to best address this issue? (Select two).

A. Screen locks

B. Remote wipe

C. Full device encryption

D. Push notifications

E. Application management

F. Geolocation



# 10A - Implement Endpoint Security



**NO.15** An organization has too many variations of a single operating system and needs to standardize the arrangement prior to pushing the system image to users.

Which of the following should the organization implement first?

- A. Standard naming convention
- B. Mashing
- C. Network diagrams
- D. Baseline configuration

# 10A - Implement Endpoint Security



**NO.15** An organization has too many variations of a single operating system and needs to **standardize the arrangement** prior to pushing the system image to users.

Which of the following should the organization implement first?

- A. Standard naming convention
- B. Mashing
- C. Network diagrams
- D. Baseline configuration

# 10A - Implement Endpoint Security



**NO.16** A systems administrator is auditing all company servers to ensure they meet the minimum security baseline. While auditing a Linux server, the systems administrator observes the `/etc/shadow` file has permissions beyond the baseline recommendation.

Which of the following commands should the systems administrator use to resolve this issue?

- A. `chmod`
- B. `grep`
- C. `dd`
- D. `passwd`

# 10A - Implement Endpoint Security



**NO.16** A systems administrator is auditing all company servers to ensure. They meet the minimum security baseline. While auditing a Linux server, the systems administrator observes the `/etc/shadow` file **has permissions beyond the baseline recommendation.**

Which of the following commands should the systems administrator use to resolve this issue?

- A. `chmod`
- B. `grep`
- C. `dd`
- D. `passwd`

# 10A - Implement Endpoint Security



**NO.17** A bank set up a new server that contains customers' PII.

Which of the following should the bank use to make sure the sensitive data is not modified?

- A. Full disk encryption
- B. Network access control
- C. File integrity monitoring
- D. User behavior analytics

# 10A - Implement Endpoint Security



**NO.17** A bank set up a new server that contains customers' **PII**.

Which of the following should the bank use to make sure the sensitive data is not modified?

- A. Full disk encryption
- B. Network access control
- C. File integrity monitoring
- D. User behavior analytics



# **10B - Mobile Device Hardening**

# 10B - Mobile Device Hardening



**NO.1** Which of the following is a primary security concern for a company setting up a BYOD program?

- (A). End of life
- (B). Buffer overflow
- (C). VM escape
- (D). Jailbreaking



# 10B - Mobile Device Hardening



**NO.1** Which of the following is a primary security concern for a company setting up a BYOD program?

- (A). End of life
- (B). Buffer overflow
- (C). VM escape
- (D). Jailbreaking



# 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



BGA  
SECURITY

IBBN

gravity  
IT RESOURCES



proximus

northramp



ease  
LEARNING

