CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (3A-3B-3C)

AGENDA

- 3A - Cryptographic Algorithms (3)
- 3B - Public Key Infrastructure (5)
- 3C - Cryptographic Solutions (12)
- TOTAL: 20

3A - Cryptographic Algorithms

3A - Cryptographic Algorithms

NO.1 A software developer released a new application and is distributing application files via the developer's website.

Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?

A. Hashes
B. Certificates
C. Algorithms
D. Salting

3A - Cryptographic Algorithms

NO.1 A software developer released a new application and is distributing application files via the developer's website.

Which of the following should the developer post on the website to allow users **to verify the integrity** of the downloaded files?

A. Hashes
B. Certificates
C. Algorithms
D. Salting

3A - Cryptographic Algorithms

NO.2 A security administrator identifies an application that is storing data using MD5.

Which of the following best identifies the vulnerability likely present in the application?

A. Cryptographic
B. Malicious update
C. Zero day
D. Side loading

3A - Cryptographic Algorithms

NO.2 A security administrator identifies an application that is storing data using MD5.

Which of the following best identifies the vulnerability likely present in the application?

A. Cryptographic
B. Malicious update
C. Zero day
D. Side loading

3A - Cryptographic Algorithms

NO.3 Which of the following is an algorithm performed to verify that data has not been modified?

A. Hash

B. Code check

C. Encryption

D. Checksum

3A - Cryptographic Algorithms

NO.3 Which of the following is an algorithm performed **to verify that data has not been modified?**

A. Hash

B. Code check

C. Encryption

D. Checksum

3B - Public Key Infrastructure

3B - Public Key Infrastructure

NO.1 A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Select two).

A. Key escrow
B. TPM presence
C. Digital signatures
D. Data tokenization
E. Public key management
F. Certificate authority linking

3B - Public Key Infrastructure

NO.1 A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Select two).

A. Key escrow
B. TPM presence
C. Digital signatures
D. Data tokenization
E. Public key management
F. Certificate authority linking

3B - Public Key Infrastructure

NO.2 A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multi cloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would best meet the architect's objectives?

A. Trusted Platform Module
B. IaaS
C. HSMaaS
D. PaaS

3B - Public Key Infrastructure

NO.2 A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multi cloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would best meet the architect's objectives?

A. Trusted Platform Module
B. IaaS
C. HSMaaS
D. PaaS

3B - Public Key Infrastructure

NO.3 Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP
B. CSR
C. CA
D. CRC

3B - Public Key Infrastructure

NO.3 Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP
B. CSR
C. CA
D. CRC

3B - Public Key Infrastructure

NO.4 A certificate vendor notified a company that recently invalidated certificates may need to be updated. Which of the following mechanisms should a security administrator use to determine whether the certificates installed on the company's machines need to be updated?

A. SCEP
B. OCSP
C. CSR
D. CRL

3B - Public Key Infrastructure

NO.4 A certificate vendor notified a company that recently invalidated certificates may need to be updated. Which of the following mechanisms should a security administrator use to determine whether the certificates installed on the company's machines need to be updated?

A. SCEP
B. OCSP
C. CSR
D. CRL

3B - Public Key Infrastructure

NO.5 A spoofed identity was detected for a digital certificate.

Which of the following are the type of unidentified key and the certificate that could be in use on the company domain?

A. Private key and root certificate

B. Public key and expired certificate

C. Private key and self-signed certificate

D. Public key and wildcard certificate

3B - Public Key Infrastructure

NO.5 A **spoofed identity** was detected for a digital certificate.

Which of the following are the type of unidentified key and the certificate that could be in use on the company domain?

A. Private key and root certificate

B. Public key and expired certificate

C. Private key and self-signed certificate

D. Public key and wildcard certificate

3C - Cryptographic Solutions

3C - Cryptographic Solutions

NO.1 Which of the following describes the process of concealing code or text inside a graphical image?

A. Symmetric encryption
B. Hashing
C. Data masking
D. Steganography

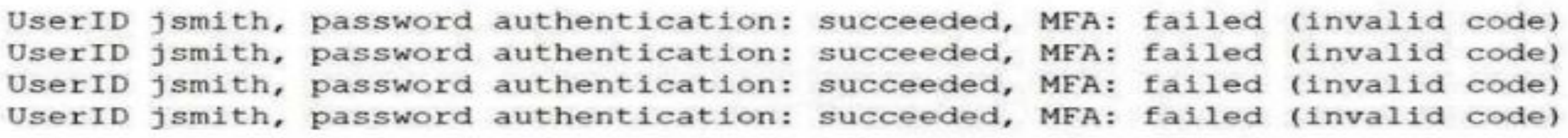
3C - Cryptographic Solutions

NO.1 Which of the following describes the process of concealing code or text inside a graphical image?

A. Symmetric encryption
B. Hashing
C. Data masking
D. Steganography

3C - Cryptographic Solutions

NO.2 A security analyst reviews domain activity logs and notices the following:



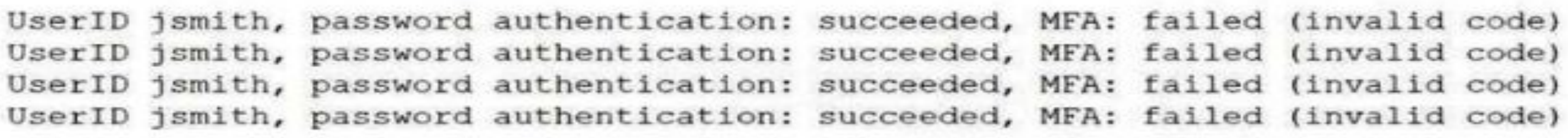
```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.
B. A keylogger is installed on [smith's workstation
C. An attacker is attempting to brute force ismith's account.
D. Ransomware has been deployed in the domain.

3C - Cryptographic Solutions

NO.2 A security analyst reviews domain activity logs and notices the following:



```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.
B. A keylogger is installed on [smith's workstation
C. An attacker is attempting to brute force ismith's account.
D. Ransomware has been deployed in the domain.

3C - Cryptographic Solutions

NO.3 A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest
B. Masking
C. Data classification
D. Permission restrictions

3C - Cryptographic Solutions

NO.3 A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest
B. Masking
C. Data classification
D. Permission restrictions

3C - Cryptographic Solutions

NO.4 In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

A. Key stretching
B. Tokenization
C. Data masking
D. Salting

3C - Cryptographic Solutions

NO.4 In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

A. Key stretching
B. Tokenization
C. Data masking
D. Salting

3C - Cryptographic Solutions

NO.5 Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching
B. Data masking
C. Steganography
D. Salting

3C - Cryptographic Solutions

NO.5 Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching
B. Data masking
C. Steganography
D. Salting

3C - Cryptographic Solutions

NO.6 A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

A. EAP
B. DHCP
C. IPSec
D. NAT

3C - Cryptographic Solutions

NO.6 A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

A. EAP
B. DHCP
C. IPSec
D. NAT

3C - Cryptographic Solutions

NO.7 An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

A. Data in use
B. Data in transit
C. Geographic restrictions
D. Data sovereignty

3C - Cryptographic Solutions

NO.7 An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

A. Data in use
B. Data in transit
C. Geographic restrictions
D. Data sovereignty

3C - Cryptographic Solutions

NO.8 Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

A. Encryption
B. Hashing
C. Masking
D. Tokenization

3C - Cryptographic Solutions

NO.8 Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

A. Encryption
B. Hashing
C. Masking
D. Tokenization

3C - Cryptographic Solutions

NO.9 Which of the following explains why an attacker cannot easily decrypt passwords using a rainbow table attack?

A. Digital signatures
B. Salting
C. Hashing
D. Perfect forward secrecy

3C - Cryptographic Solutions

NO.9 Which of the following explains why an attacker cannot easily decrypt passwords using a **rainbow table attack?**

A. Digital signatures

B. Salting

C. Hashing

D. Perfect forward secrecy

3C - Cryptographic Solutions

NO.10 A software developer would like to ensure, the source code cannot be reverse engineered or debugged.

Which of the following should the developer consider?

A. Version control

B. Obfuscation toolkit

C. Code reuse

D. Continuous integration

E. Stored procedures

3C - Cryptographic Solutions

NO.10 A software developer would like to ensure, the **source code cannot be reverse engineered or debugged.**

Which of the following should the developer consider?

A. Version control

B. Obfuscation toolkit

C. Code reuse

D. Continuous integration

E. Stored procedures

3C - Cryptographic Solutions

NO.11 Which of the following methods would most likely be used to identify legacy systems?

A. Bug bounty program
B. Vulnerability scan
C. Package monitoring
D. Dynamic analysis

3C - Cryptographic Solutions

NO.11 Which of the following methods would most likely be used to **identify legacy systems?**

A. Bug bounty program
B. Vulnerability scan
C. Package monitoring
D. Dynamic analysis

3C - Cryptographic Solutions

NO.12 Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

A. To track the status of patching installations
B. To find shadow IT cloud deployments
C. To continuously the monitor hardware inventory
D. To hunt for active attackers in the network

3C - Cryptographic Solutions

NO.12 Which of the following would best explain why a security analyst is **running daily vulnerability scans** on all corporate endpoints?

A. To track the status of patching installations

B. To find shadow IT cloud deployments

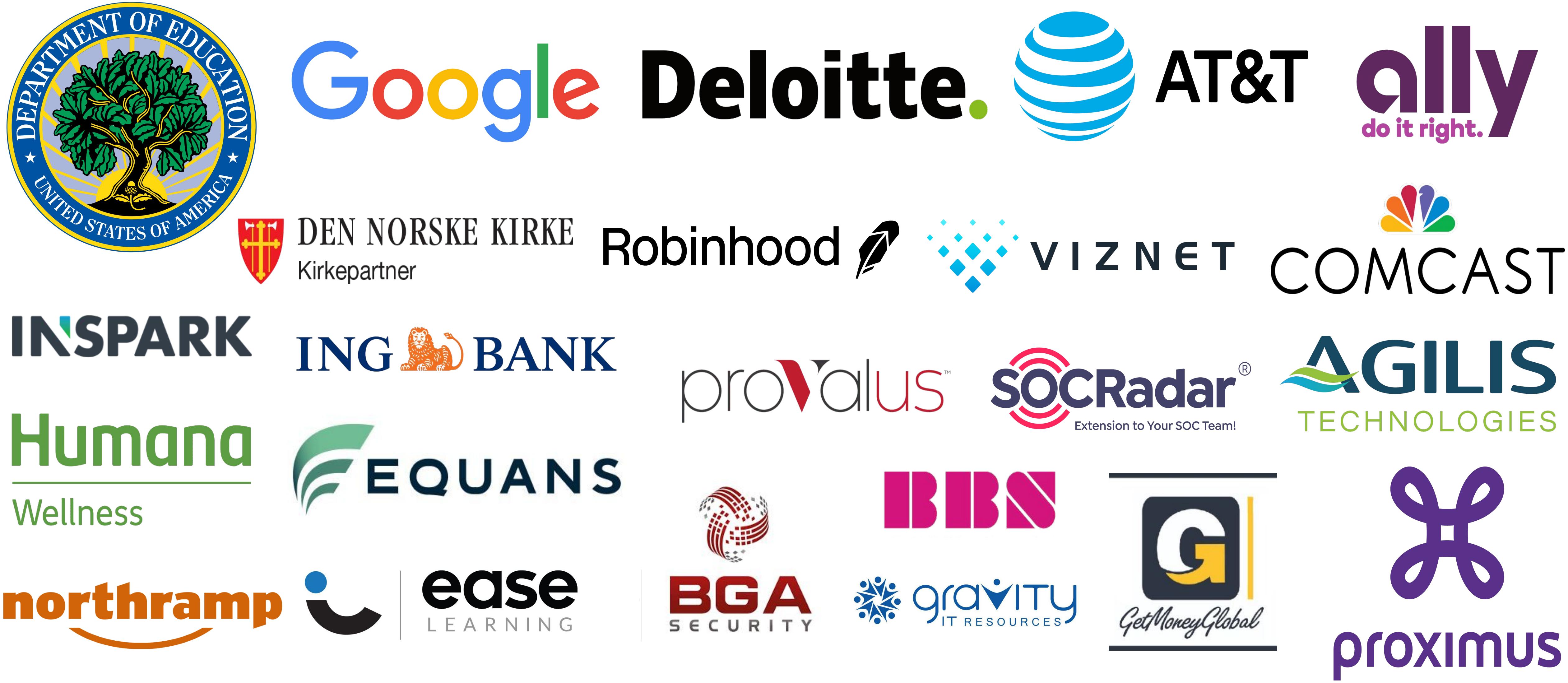
C. To continuously the monitor hardware inventory

D. To hunt for active attackers in the network

THANKS!

Any questions?

Our Graduates are Hired By


DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA
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
BBS
gravity
IT RESOURCES
GetMoneyGlobal
proximus
northramp
ease
LEARNING