QUESTION 1449
A security analyst just discovered that developers have access to production systems that are used for deployment and troubleshooting.
One developer, who recently left the company abused this access to obtain sensitive information.
Which of the following is the BEST account management strategy to prevent this from reoccurring?

A. Perform an account review and ensure least privilege is being followed for production access
B. Implement multifactor authentication for accessing production systems
C. Configure jump boxes and prevent access to production from any other system
D. Set up time-of-day restrictions that prevent access to production systems during business hours
E. Modify the AUP to prohibit developers from accessing production systems

Answer: E

QUESTION 1450
Following a breach, a forensic analyst reviewed system logs and determined that an attacker used an unknown account with elevated privileges on a computer to access organization files.
Which of the following MOST likely occurred to allow the attacker to access the files?

A. The attacker renamed a domain administrator account on the computer and used it to access the files
B. The attacker used Metasploit to identify the location of the organization's files and access them
C. The attacker used an active default administrator account to create new accounts with rights to access the files
D. The attacker used a pass-the-hash attack to access the network location and access the files

Answer: C

QUESTION 1451
Which of the following BEST represent detective controls? (Select TWO)

A. Security guard
B. Camera
C. Mantrap
D. Bollards
E. Fencing

Answer: AB

QUESTION 1452
A computer forensics analyst collected a thumb drive that contained a single file with 500 pages of text.

To ensure the file maintains its confidentiality, which of the following should the analyst use?

A. SHA
B. AES
C. SLA
D. NOA

Answer: B

QUESTION 1453
A security analyst is conducting a vulnerability scan and comes across a scheduled task that runs a batch script.
The analyst sees the following text when viewing the batch script s contents:

```
net use \\dc01\publicshare\files 1q2w3e4r /USER:ServiceAcct
copy \*.bak \\dc01\publicshare\files\*.bak
```

Which of the following is the MOST likely reason for the analyst to flag this task?

A. The credentials are not encrypted
B. The files are being sent to a public share
C. The wildcard parameters are incorrectly set
D. The password does not meet the minimum requirements

Answer: A

QUESTION 1454
An organization has defined secure baselines for all servers and applications.
Before any servers or applications are placed into production they must be reviewed for compliance deviations.
Which of the following actions would streamline the process and provide more consistent results?

A. Purchase a vulnerability scanner and upgrade the signatures to include compliance items based on the organization's secu baselines
B. Perform penetration testing against every server and generate automated reports that can be reviewed by all application an
C. Implement a configuration scanner that automatically reviews every server and application against the established baseline
D. Use a network scanner to identify non-compliant ports and services and have the server and application teams review the r

Answer: C

QUESTION 1455
Two companies need to exchange a large number of confidential files Both companies run high availability UTM devices.
They do not want to use email systems to exchange the data Since the data needs to be exchanged in both directions, which of the following solutions should a security analyst recommend7

A. Configuring the remote access feature on both UTMs
B. Configuring an FTP server in one company
C. Establishing a site-to-site VPN between the two companies
D. Exchanging data by using a free cloud-storage product

Answer: C

QUESTION 1456
A network administrator at a bank needs to create zones that will prevent an attacker from freely traversing the network in the event of a perimeter firewall breach.
The zones should allow the bank tellers to communicate with each other but prevent them from accessing Internet resources.
Which of the following should the network administrator implement?

A. Air gaps
B. A DMZ
C. A VPN
D. Proxies

Answer: B

QUESTION 1457
After receiving an alert regarding an anomaly in network traffic spikes a secunty analyst discovered a web server has a web-enabled application.
The application was recently installed and was being used by a group of developers that shared a set of default credentials.
During a switch migration, the server was unintentionally plugged into a switchport that was configured for DMZ access.
The analysis provided evidence showing the server was being accessed from international IP addresses via the web-enabled application and used to process and print shipping labels.
Which of the following would prevent this from happening?

A. Ensure the server operating system is part of the patch management process
B. Disable default usernames/passwords and unnecessary ports
C. Use DLP to prevent the use of USB printers and drives on the server
D. Implement NAT between the DMZ and the internal network

Answer: D

QUESTION 1458
A bank with high-profile customer accounts is concerned about collusion and fraud occurring between staff and customers at a specific branch.
Which of the following best practices would help detect any fraudulent activities?

A. Acceptable use policy
B. Continuous network monitoring
C. Job rotation
D. Least privilege
E. Separation of duties

Answer: C

QUESTION 1459
Which of the following cryptographic algorithms can be used for full-disk encryption?

A. AES
B. SHA-256
C. PBKDF2
D. RSA

Answer: A

QUESTION 1460
Before providing digital evidence for a case, a security analyst performed a full disk image of the compromised server using a forensic tool and asked a law enforcement officer to provide an in-person written confirmation of receipt. The security analyst was MOST interested in?

A. avoiding the volatility of the data
B. maintaining the chain of custody

C. confirming the legal hold
D. having a recovery point

Answer: B

QUESTION 1461
Which of the following must be updated prior to conducting weekly cyber hygiene scans of a network?

A. WIDS settings
B. Rainbow tables
C. Antivirus definitions
D. Vulnerability signatures

Answer: D

QUESTION 1462
A business sector is highly competitive and safeguarding trade secrets and critical information is paramount. On a seasonal basis an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock. Which of the following account management practices are the BEST ways to manage these accounts? (Select TWO)

A. Employ time-of-day restrictions
B. Employ password complexity
C. Employ a random key generator strategy
D. Employ an account expiration strategy
E. Employ a password lockout policy

Answer: AD

QUESTION 1463
A user contacts the help desk about getting a newly installed application to work.
When searching the logging servers for the user's IP address the help desk analyst finds the following output from the host-based firewall:

```
[12:14:15] Outbound connection DENIED to destination cc.abc.com on WINDOWS-ABCXYZ due to policy: Known Botnet
[12:14:16] Outbound connection DENIED to destination cc.abc.com on WINDOWS-ABCXYZ due to policy: Known Botnet
[12:14:18] Outbound connection DENIED to destination cc.abc.com on WINDOWS-ABCXYZ due to policy: Known Botnet
[12:14:19] Outbound connection DENIED to destination cc.abc.com on WINDOWS-ABCXYZ due to policy: Known Botnet
```

Which of the following is MOST likely occurring?

A. The host cc abc com is scanning the PC
B. The application needs host firewall rules
C. WINDOWS-ABCXYZ is an unknown host
D. The PC is infected with C2

Answer: D

QUESTION 1464
A software developer is building a secure application and is looking to store passwords securely.
Which of the following should the developer use?

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

Answer: B

QUESTION 1465
The legal department of a cafe chain wants to ensure customers who are using the free WIFI system acknowledge review of the AUP.
Which of the following would BEST meet this goal?

A. Utilize a captive portal whenever someone connects to WiFi
B. Perform a MITM technique to force the policy to display
C. Deploy a WPS solution to ensure compliance with the policy.
D. Give the password to people who sign the agreement only

Answer: A

QUESTION 1466
A security administrator at a software development company received the following loC:

simplefile.exe	493AC4A18AD1FAB103021AD34BC374AA
simplefile.cnf	39DA11377ACB3845DD1A35AD1FAB1032
simplefile.txt	104ABC5469AD59FE593DAD1FAB10D3A1
simplefile.png	848D49D12AA2F408CAD1FAB10EEA292B

Which of the following is the 8EST and fastest solution that will protect the company's computers from executing the malware without impacting the business'?

A. Add simplefile. to the execution blacklist
B. Use a script to remove the files from all company computers
C. Implement a new whitelist policy and exclude the loC names and hashes
D. Use a GPO to blacklist 493AC4A183AD1FABl0302lAD34BC374AA

Answer: D

QUESTION 1467
Which of the following would be MOST effective at stopping zero-day attacks on an endpoint? (Select TWO)

A. Deploying multivendor NGFWs
B. Deploying antivirus and anti-malware system tools
C. Implementing application whitelisting
D. Removing administrator rights from users
E. Implementing a web application firewall
F. Installing a reverse proxy

Answer: CD

QUESTION 1468
The use of a unique attribute inherent to a user as part of an UFA system is BEST described as:

A. something you do
B. something you have
C. something you know.
D. something you are.

Answer: D

QUESTION 1469
A security analyst discovers one of the business processes which generates 75% of the annual revenue, uses a legacy

system.
This creates a tolerable risk that can contribute to a 2% drop in revenue generation every quarter.
Which of the following would be the BEST response to this risk?

A. Mitigation
B. Avoidance
C. Insurance
D. Acceptance

Answer: D

QUESTION 1470
Which of the following reasons would explain why a vulnerability scanner is reporting a false negative? (Select TWO)

A. The vulnerability is present on the target system
B. The vulnerability scanner's definitions file is out of date
C. The scanner reporting system is unavailable.
D. The system was fully patched
E. The target's IDS is blocking the scanner
F. The vulnerability scanner's license limits were exceeded

Answer: AC

QUESTION 1471
A systems administrator is trying to reduce the amount of time backups take every night.
Which of the following backup types only includes changes since the most recent backup of any type?

A. Differential
B. Snapshot
C. Incremental
D. Full

Answer: A

QUESTION 1472
Hotspot Question
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Patch vulnerable systems
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Implement a host-based IPS
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services