- **Vendor:** CompTIA
- **Exam Code:** CAS-004
- **Exam Name:** CompTIA Advanced Security Practitioner (CASP+)
- **New Updated Questions from Braindump2go**
- **(Updated in September/2023)**

**QUESTION 468**
A domestic, publicly traded, online retailer that sells makeup would like to reduce the risks to the most sensitive type of data within the organization but also the impact to compliance. A risk analyst is performing an assessment of the collection and processing of data used within business processes. Which of the following types of data pose the GREATEST risk? (Choose two.)

A. Financial data from transactions
B. Shareholder meeting minutes
C. Data of possible European customers
D. Customers' shipping addresses
E. Deidentified purchasing habits
F. Consumer product purchasing trends

**Answer:** AC

**QUESTION 469**
A security engineer is creating a single CSR for the following web server hostnames:

```
- wwwint.internal
- www.company.com
- home.internal
- www.internal
```

Which of the following would meet the requirement?

A. SAN
B. CN
C. CA
D. CRL
E. Issuer

**Answer:** A

**QUESTION 470**
A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation. Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience. The current architecture includes:

```
- Directory servers
- Web servers
- Database servers
- Load balancers
- Cloud-native VPN concentrator
- Remote access server
```

The MSP must secure this environment similarly to the infrastructure on premises. Which of the following should the MSP put in place to BEST meet this objective? (Choose three.)

A. Content delivery network
B. Virtual next-generation firewall
C. Web application firewall
D. Software-defined WAN
E. External vulnerability scans
F. Containers

**Answer:** BCE

**QUESTION 471**
A security analyst has been tasked with providing key information in the risk register. Which of the following outputs or results would be used to BEST provide the information needed to determine the security posture for a risk decision? (Choose two.)

A. Password cracker
B. SCAP scanner
C. Network traffic analyzer
D. Vulnerability scanner
E. Port scanner
F. Protocol analyzer

**Answer:** CD

**QUESTION 472**
An organization is in frequent litigation and has a large number of legal holds. Which of the following types of functionality should the organization's new email system provide?

A. DLP
B. Encryption
C. E-discovery
D. Privacy-level agreements

**Answer:** C

**QUESTION 473**
A security engineer based in Iceland works in an environment requiring an on-premises and cloud-based storage solution. The solution should take into consideration the following:

```
1. The company has sensitive data.
2. The company has proprietary data.
3. The company has its headquarters in Iceland, and the data must always reside in that
country.
```

Which cloud deployment model should be used?

A. Hybrid cloud
B. Community cloud
C. Public cloud
D. Private cloud

**Answer:** A

**QUESTION 474**
When managing and mitigating SaaS cloud vendor risk, which of the following responsibilities belongs to the client?

A. Data
B. Storage
C. Physical security
D. Network

**Answer:** A

**QUESTION 475**
Which of the following should be established when configuring a mobile device to protect user internet privacy, to ensure the connection is encrypted, and to keep user activity hidden? (Choose two.)

A. Proxy
B. Tunneling
C. VDI
D. MDM
E. RDP
F. MAC address randomization

**Answer:** BF

**QUESTION 476**
An organization does not have visibility into when company-owned assets are off network or not connected via a VPN. The lack of visibility prevents the organization from meeting security and operational objectives. Which of the following cloud-hosted solutions should the organization implement to help mitigate the risk?

A. Antivirus
B. UEBA
C. EDR
D. HIDS

**Answer:** C

**QUESTION 477**
A company has retained the services of a consultant to perform a security assessment. As part of the assessment, the consultant recommends engaging with others in the industry to collaborate in regards to emerging attacks. Which of the following would BEST enable this activity?

A. ISAC
B. OSINT
C. CVSS
D. Threat modeling

**Answer:** A

**QUESTION 478**
A law firm experienced a breach in which access was gained to a secure server. During an investigation to determine how the breach occurred, an employee admitted to clicking on a spear-phishing link. A security analyst reviewed the event logs and found the following:

```
- PAM had not been bypassed.
- DLP did not trigger any alerts.
- The antivirus was updated to the most current signatures.
```

Which of the following MOST likely occurred?

A. Exploitation
B. Exfiltration
C. Privilege escalation
D. Lateral movement

**Answer:** A

**QUESTION 479**
A company processes sensitive cardholder information that is stored in an internal production database and accessed by internet-facing web servers. The company's Chief Information Security Officer (CISO) is concerned with the risks related to sensitive data exposure and wants to implement tokenization of sensitive information at the record level. The company implements a one-to-many mapping of primary credit card numbers to temporary credit card numbers. Which of the following should the CISO consider in a tokenization system?

A. Data field watermarking
B. Field tagging
C. Single-use translation
D. Salted hashing

**Answer:** C

**QUESTION 480**
A network administrator receives a ticket regarding an error from a remote worker who is trying to reboot a laptop. The laptop has not yet loaded the operating system, and the user is unable to continue the boot process. The administrator is able to provide the user with a recovery PIN, and the user is able to reboot the system and access the device as needed. Which of the following is the MOST likely cause of the error?

A. Lockout of privileged access account
B. Duration of the BitLocker lockout period
C. Failure of the Kerberos time drift sync
D. Failure of TPM authentication

**Answer:** D

**QUESTION 481**
A security engineer is concerned about the threat of side-channel attacks. The company experienced a past attack that degraded parts of a SCADA system, causing a fluctuation to 20,000rpm from its normal operating range. As a result, the part deteriorated more quickly than the mean time to failure. A further investigation revealed the attacker was able to determine the acceptable rpm range, and the malware would then fluctuate the rpm until the part failed. Which of the following solutions would be BEST to prevent a side-channel attack in the future?

A. Installing online hardware sensors
B. Air gapping important ICS and machines
C. Implementing a HIDS
D. Installing a SIEM agent on the endpoint

**Answer:** B

**QUESTION 482**
Which of the following is the primary reason that a risk practitioner determines the security boundary prior to conducting a risk assessment?

A. To determine the scope of the risk assessment

B. To determine the business owner(s) of the system
C. To decide between conducting a quantitative or qualitative analysis
D. To determine which laws and regulations apply

**Answer:** A

**QUESTION 483**
A security architect must mitigate the risks from what is suspected to be an exposed, private cryptographic key. Which of the following is the BEST step to take?

A. Revoke the certificate.
B. Inform all the users of the certificate.
C. Contact the company's Chief Information Security Officer.
D. Disable the website using the suspected certificate.
E. Alert the root CA.

**Answer:** A

**QUESTION 484**
An employee's device was missing for 96 hours before being reported. The employee called the help desk to ask for another device. Which of the following phases of the incident response cycle needs improvement?

A. Containment
B. Preparation
C. Resolution
D. Investigation

**Answer:** B

**QUESTION 485**
A security consultant has been asked to recommend a secure network design that would:

```
- Permit an existing OPC server to communicate with a new Modbus server that is
controlling electrical relays.
- Limit operational disruptions.
```

Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.
B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 102.
C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 5000.
D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.

**Answer:** D

**QUESTION 486**
A forensic investigator started the process of gathering evidence on a laptop in response to an incident. The investigator took a snapshot of the hard drive, copied relevant log files, and then performed a memory dump. Which of the following steps in the process should have occurred FIRST?

A. Preserve secure storage.
B. Clone the disk.

C. Collect the most volatile data.
D. Copy the relevant log files.

**Answer:** C

**QUESTION 487**
A company is designing a new system that must have high security. This new system has the following requirements:

```
- Permissions must be assigned based on role.
- Fraud from a single person must be prevented.
- A single entity must not have full access control.
```

Which of the following can the company use to meet these requirements?

A. Dual responsibility
B. Separation of duties
C. Need to know
D. Least privilege

**Answer:** B

**QUESTION 488**
A Chief Security Officer (CSO) is concerned about the number of successful ransomware attacks that have hit the company. The data indicates most of the attacks came through a fake email. The company has added training, and the CSO now wants to evaluate whether the training has been successful. Which of the following should the CSO implement?

A. Simulating a spam campaign
B. Conducting a sanctioned vishing attack
C. Performing a risk assessment
D. Executing a penetration test

**Answer:** A

**QUESTION 489**
A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

A. Mirror the blobs at a local data center.
B. Enable fast recovery on the storage account.
C. Implement soft delete for blobs.
D. Make the blob immutable.

**Answer:** C

**QUESTION 490**
To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

A. Include stable, long-term releases of third-party libraries instead of using newer versions.
B. Ensure the third-party library implements the TLS and disable weak ciphers.
C. Compile third-party libraries into the main code statically instead of using dynamic loading.
D. Implement an ongoing, third-party software and library review and regression testing.

**Answer:** D

**QUESTION 491**
After the latest risk assessment, the Chief Information Security Officer (CISO) decides to meet with the development and security teams to find a way to reduce the security task workload. The CISO would like to:

```
- Have a solution that uses API to communicate with other security tools.
- Use the latest technology possible.
- Have the highest controls possible on the solution.
```

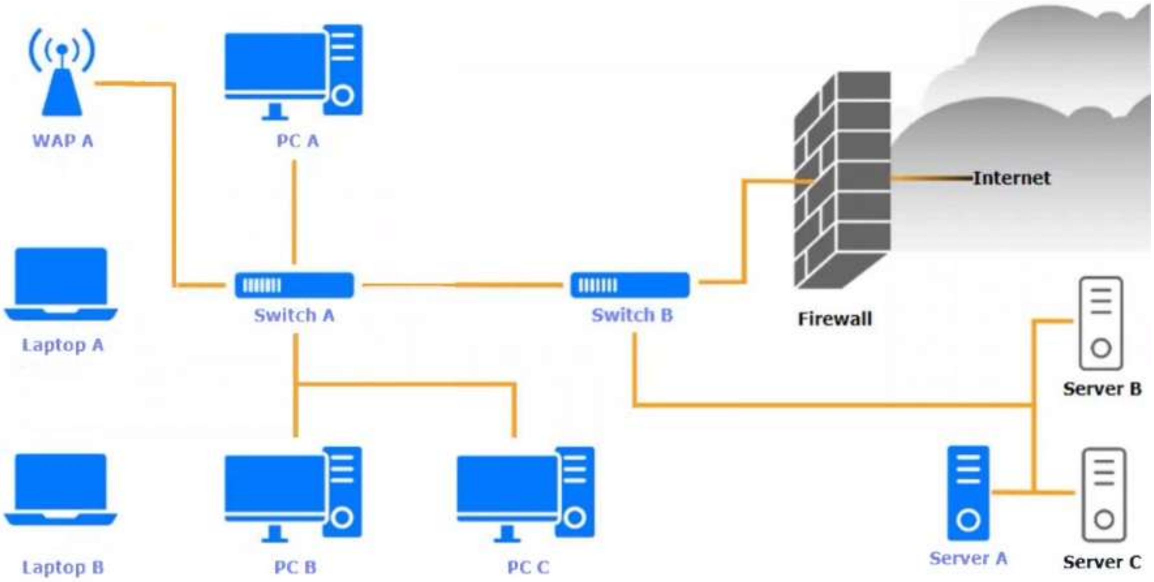
Which of following is the BEST option to meet these requirements?

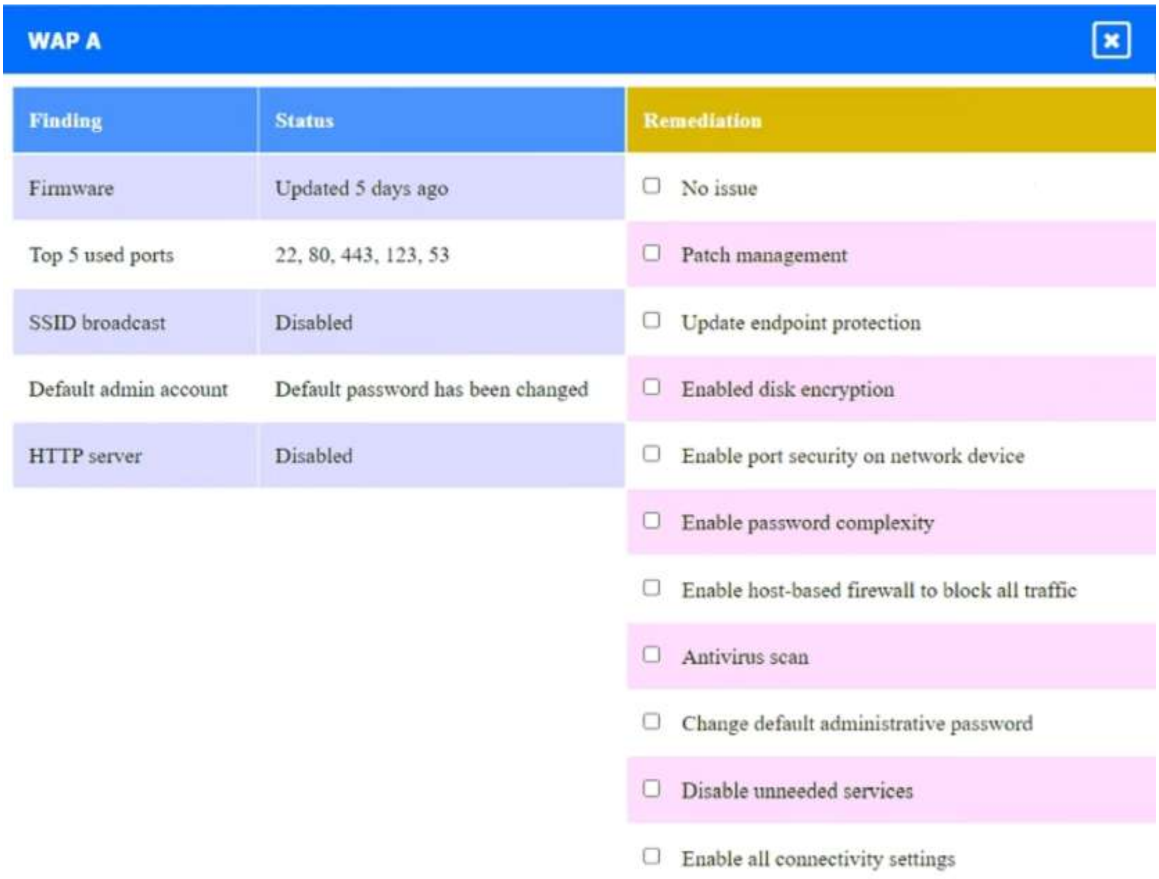
A. EDR
B. CSP
C. SOAR
D. CASB

**Answer:** C

**QUESTION 492**
**SIMULATION**
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:
- The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
- The SSH daemon on the database server must be configured to listen to port 4022.
- The SSH daemon must only accept connections from a single workstation.
- All host-based firewalls must be disabled on all workstations.
- All devices must have the latest updates from within the past eight days.
- All HDDs must be configured to secure data at rest.
- Cleartext services are not allowed.
- All devices must be hardened when possible.

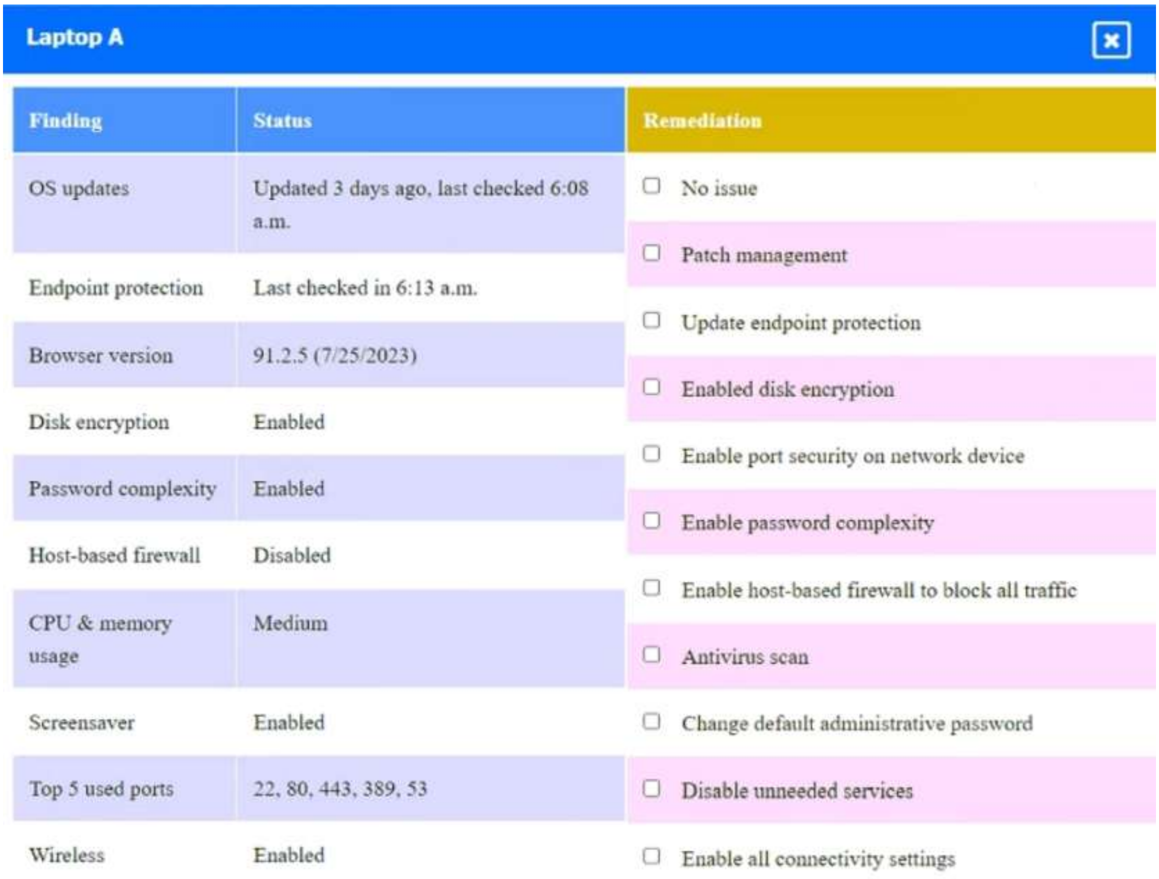
**INSTRUCTIONS**
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.
Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the PostgreSQL database via SSH.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





**WAP A** ☒

| Finding | Status | Remediation |
|---|---|---|
| Firmware | Updated 5 days ago | ☐ No issue |
| Top 5 used ports | 22, 80, 443, 123, 53 | ☐ Patch management |
| SSID broadcast | Disabled | ☐ Update endpoint protection |
| Default admin account | Default password has been changed | ☐ Enabled disk encryption |
| HTTP server | Disabled | ☐ Enable port security on network device |
| | | ☐ Enable password complexity |
| | | ☐ Enable host-based firewall to block all traffic |
| | | ☐ Antivirus scan |
| | | ☐ Change default administrative password |
| | | ☐ Disable unneeded services |
| | | ☐ Enable all connectivity settings |

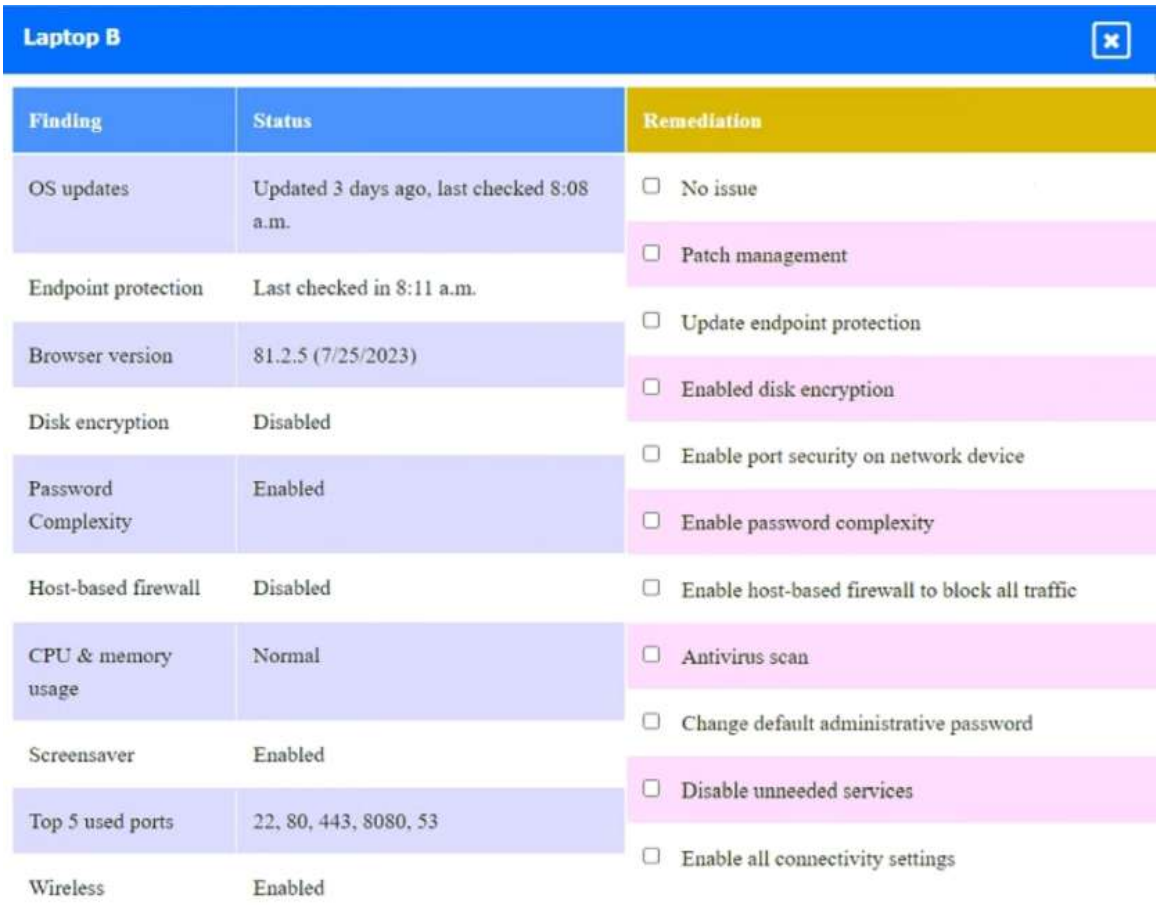


Laptop A

| Finding | Status |
|---|---|
| OS updates | Updated 3 days ago, last checked 6:08 a.m. |
| Endpoint protection | Last checked in 6:13 a.m. |
| Browser version | 91.2.5 (7/25/2023) |
| Disk encryption | Enabled |
| Password complexity | Enabled |
| Host-based firewall | Disabled |
| CPU & memory usage | Medium |
| Screensaver | Enabled |
| Top 5 used ports | 22, 80, 443, 389, 53 |
| Wireless | Enabled |

Remediation

- ☐ No issue
- ☐ Patch management
- ☐ Update endpoint protection
- ☐ Enabled disk encryption
- ☐ Enable port security on network device
- ☐ Enable password complexity
- ☐ Enable host-based firewall to block all traffic
- ☐ Antivirus scan
- ☐ Change default administrative password
- ☐ Disable unneeded services
- ☐ Enable all connectivity settings

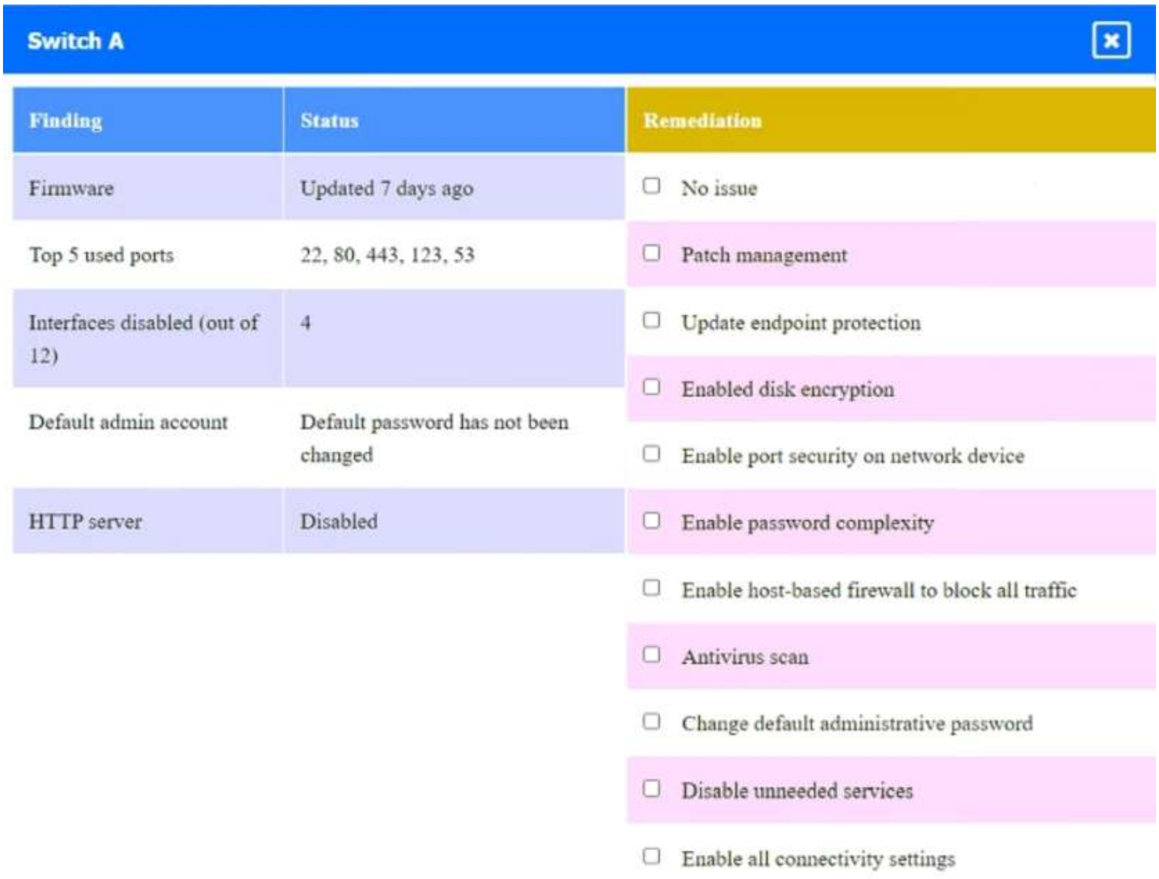


Laptop B

| Finding | Status |
|---|---|
| OS updates | Updated 3 days ago, last checked 8:08 a.m. |
| Endpoint protection | Last checked in 8:11 a.m. |
| Browser version | 81.2.5 (7/25/2023) |
| Disk encryption | Disabled |
| Password Complexity | Enabled |
| Host-based firewall | Disabled |
| CPU & memory usage | Normal |
| Screensaver | Enabled |
| Top 5 used ports | 22, 80, 443, 8080, 53 |
| Wireless | Enabled |

Remediation

- □ No issue
- □ Patch management
- □ Update endpoint protection
- □ Enabled disk encryption
- □ Enable port security on network device
- □ Enable password complexity
- □ Enable host-based firewall to block all traffic
- □ Antivirus scan
- □ Change default administrative password
- □ Disable unneeded services
- □ Enable all connectivity settings

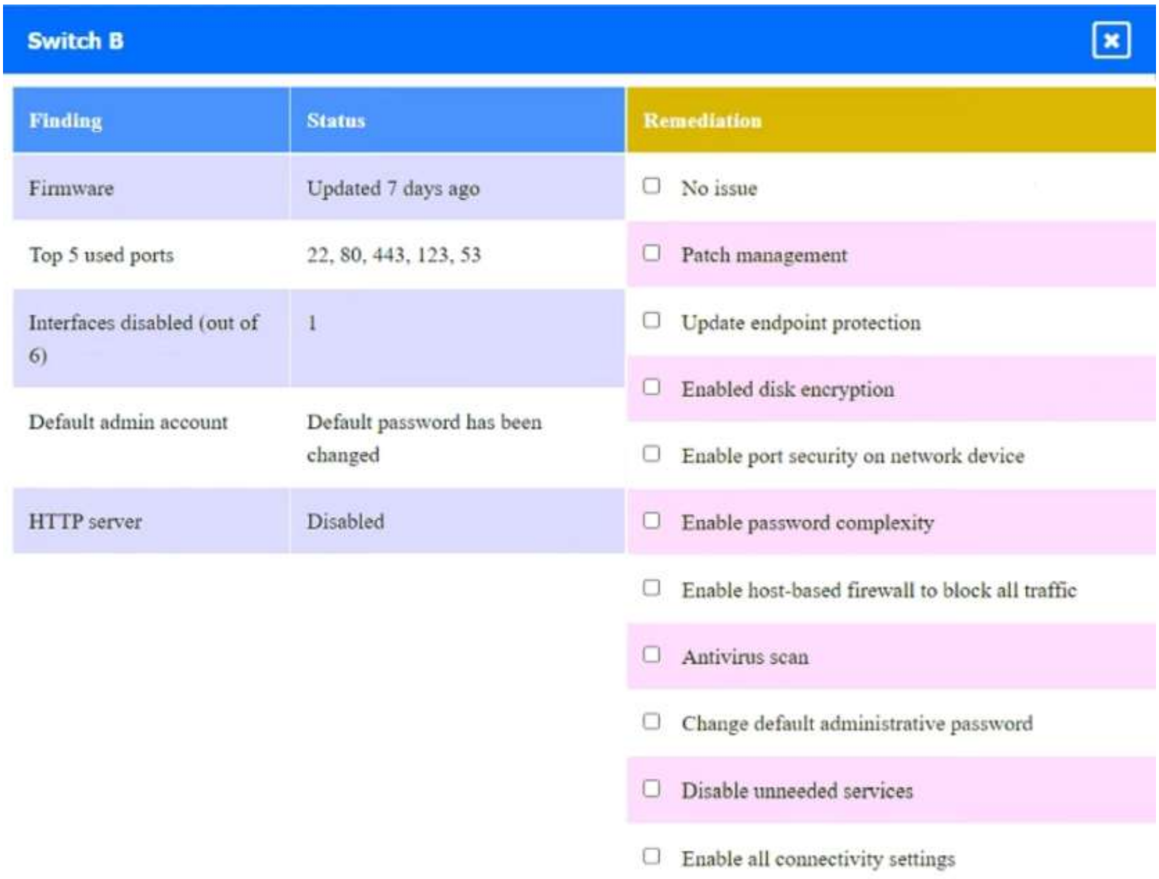


Switch A

| Finding | Status |
|---|---|
| Firmware | Updated 7 days ago |
| Top 5 used ports | 22, 80, 443, 123, 53 |
| Interfaces disabled (out of 12) | 4 |
| Default admin account | Default password has not been changed |
| HTTP server | Disabled |

Remediation

- □ No issue
- □ Patch management
- □ Update endpoint protection
- □ Enabled disk encryption
- □ Enable port security on network device
- □ Enable password complexity
- □ Enable host-based firewall to block all traffic
- □ Antivirus scan
- □ Change default administrative password
- □ Disable unneeded services
- □ Enable all connectivity settings

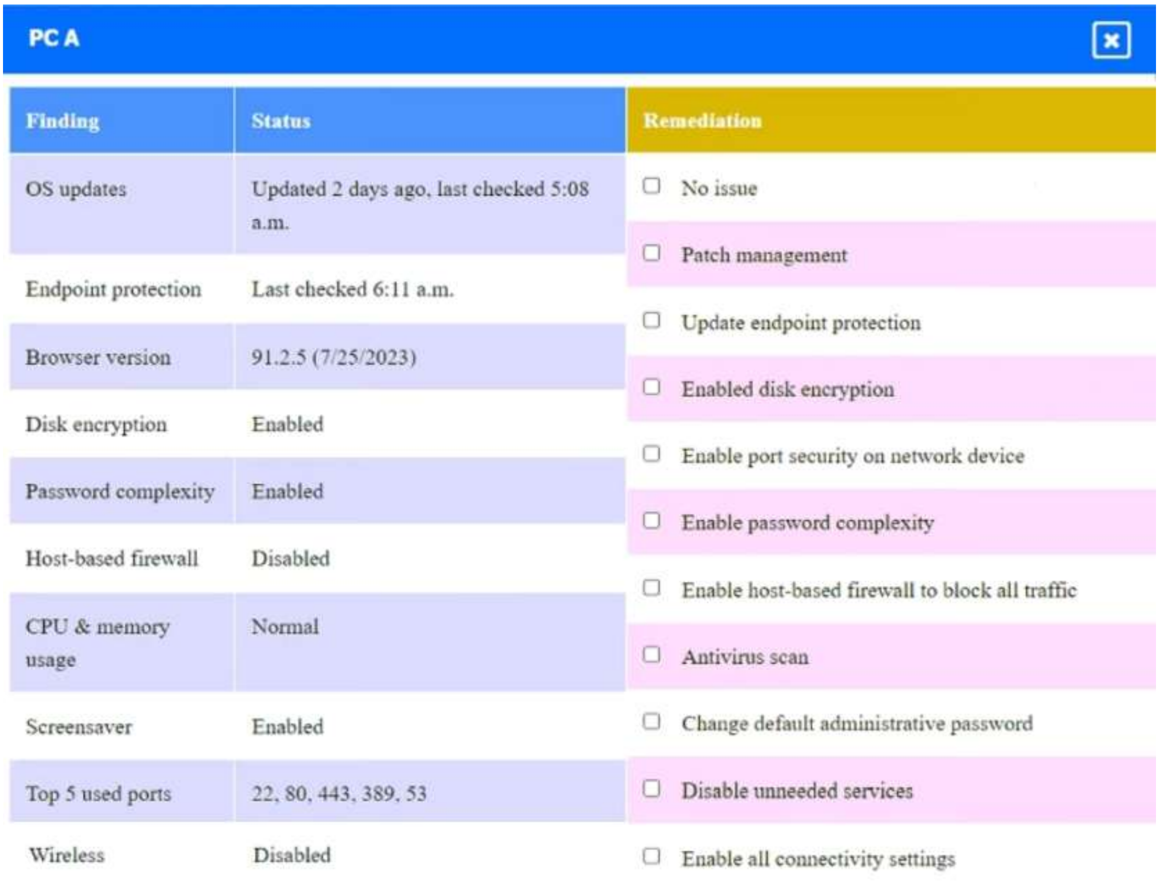


Switch B

| Finding | Status |
|---|---|
| Firmware | Updated 7 days ago |
| Top 5 used ports | 22, 80, 443, 123, 53 |
| Interfaces disabled (out of 6) | 1 |
| Default admin account | Default password has been changed |
| HTTP server | Disabled |

Remediation

- ☐ No issue
- ☐ Patch management
- ☐ Update endpoint protection
- ☐ Enabled disk encryption
- ☐ Enable port security on network device
- ☐ Enable password complexity
- ☐ Enable host-based firewall to block all traffic
- ☐ Antivirus scan
- ☐ Change default administrative password
- ☐ Disable unneeded services
- ☐ Enable all connectivity settings

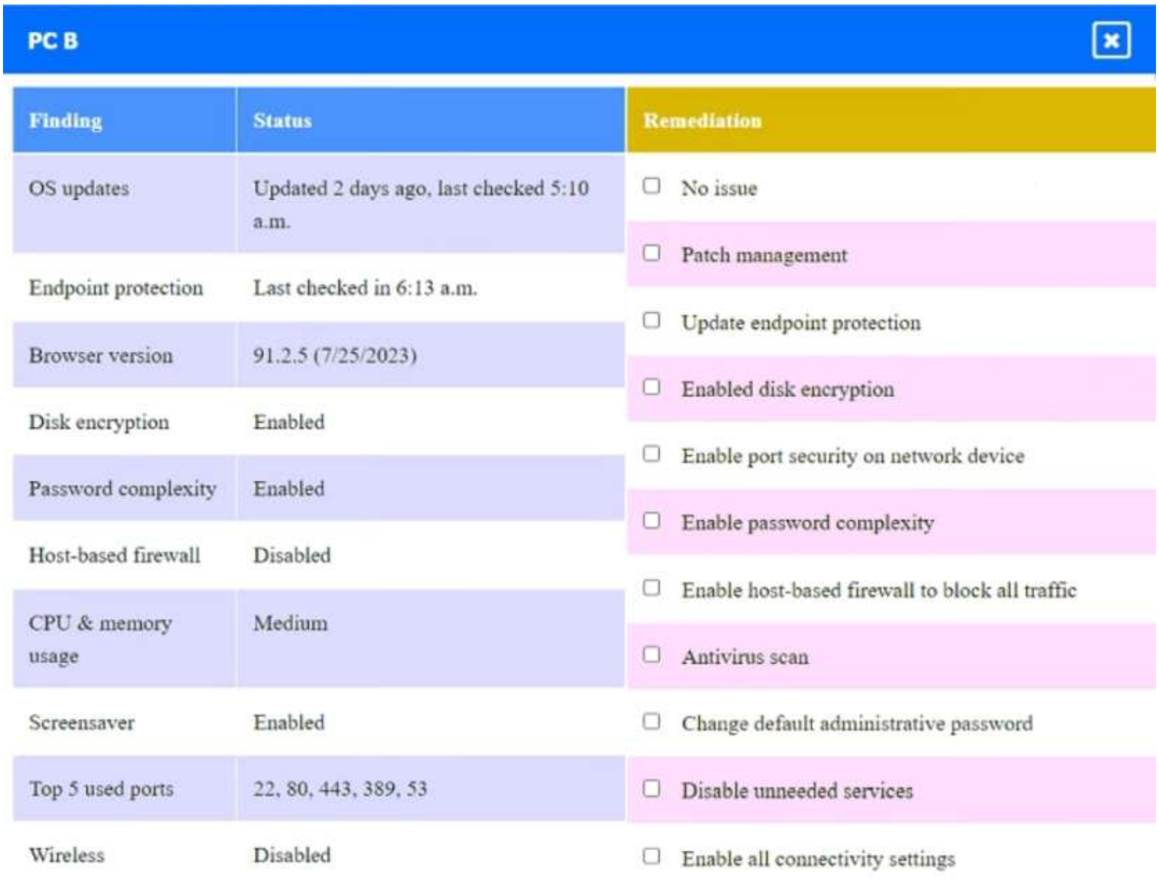


PC A

| Finding | Status |
|---|---|
| OS updates | Updated 2 days ago, last checked 5:08 a.m. |
| Endpoint protection | Last checked 6:11 a.m. |
| Browser version | 91.2.5 (7/25/2023) |
| Disk encryption | Enabled |
| Password complexity | Enabled |
| Host-based firewall | Disabled |
| CPU & memory usage | Normal |
| Screensaver | Enabled |
| Top 5 used ports | 22, 80, 443, 389, 53 |
| Wireless | Disabled |

Remediation

- ☐ No issue
- ☐ Patch management
- ☐ Update endpoint protection
- ☐ Enabled disk encryption
- ☐ Enable port security on network device
- ☐ Enable password complexity
- ☐ Enable host-based firewall to block all traffic
- ☐ Antivirus scan
- ☐ Change default administrative password
- ☐ Disable unneeded services
- ☐ Enable all connectivity settings

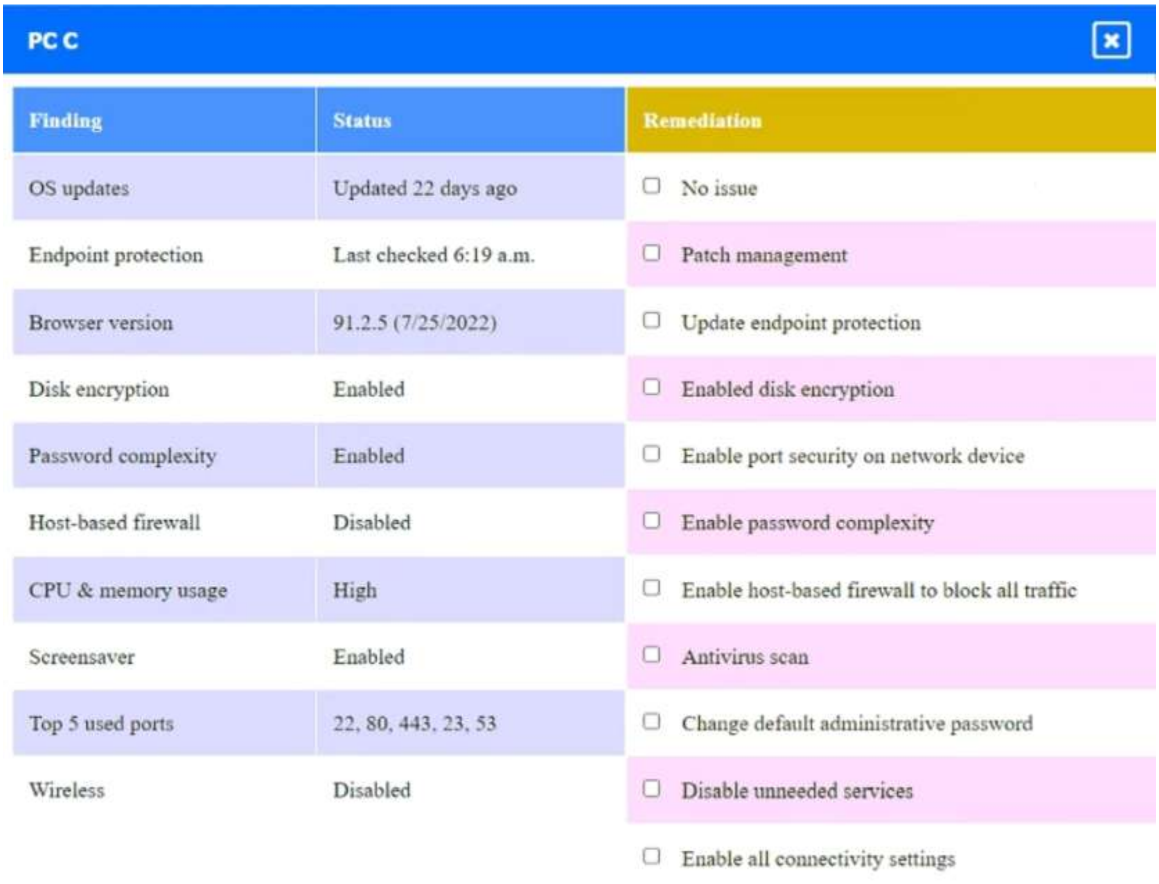


PC B

| Finding | Status |
|---|---|
| OS updates | Updated 2 days ago, last checked 5:10 a.m. |
| Endpoint protection | Last checked in 6:13 a.m. |
| Browser version | 91.2.5 (7/25/2023) |
| Disk encryption | Enabled |
| Password complexity | Enabled |
| Host-based firewall | Disabled |
| CPU & memory usage | Medium |
| Screensaver | Enabled |
| Top 5 used ports | 22, 80, 443, 389, 53 |
| Wireless | Disabled |

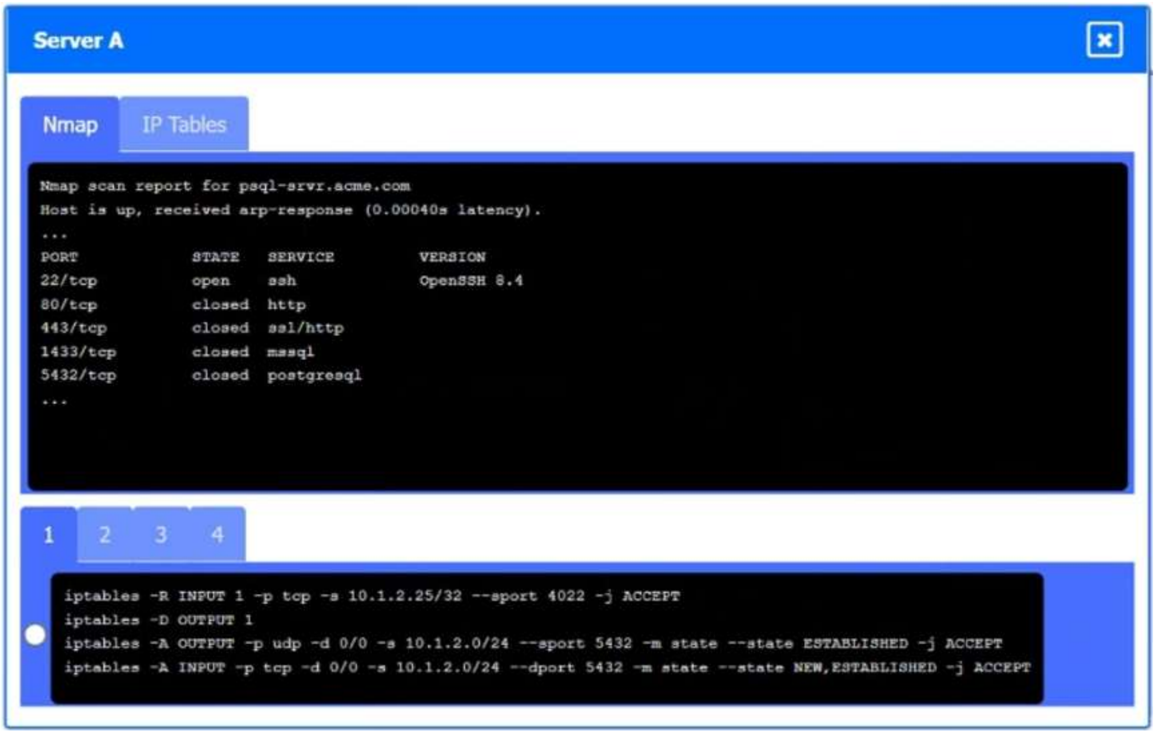
Remediation

- ☐ No issue
- ☐ Patch management
- ☐ Update endpoint protection
- ☐ Enabled disk encryption
- ☐ Enable port security on network device
- ☐ Enable password complexity
- ☐ Enable host-based firewall to block all traffic
- ☐ Antivirus scan
- ☐ Change default administrative password
- ☐ Disable unneeded services
- ☐ Enable all connectivity settings



PC C

| Finding | Status | Remediation |
|---|---|---|
| OS updates | Updated 22 days ago | □ No issue |
| Endpoint protection | Last checked 6:19 a.m. | □ Patch management |
| Browser version | 91.2.5 (7/25/2022) | □ Update endpoint protection |
| Disk encryption | Enabled | □ Enabled disk encryption |
| Password complexity | Enabled | □ Enable port security on network device |
| Host-based firewall | Disabled | □ Enable password complexity |
| CPU & memory usage | High | □ Enable host-based firewall to block all traffic |
| Screensaver | Enabled | □ Antivirus scan |
| Top 5 used ports | 22, 80, 443, 23, 53 | □ Change default administrative password |
| Wireless | Disabled | □ Disable unneeded services |
| | | □ Enable all connectivity settings |

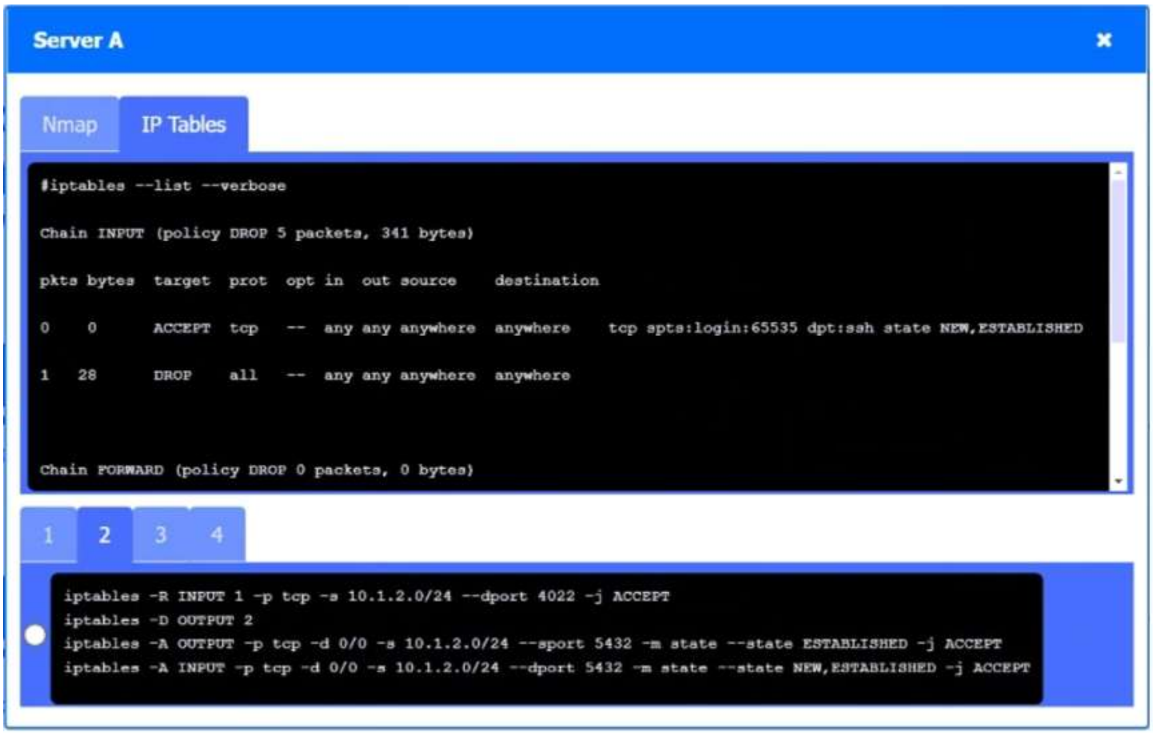


Server A

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT          STATE   SERVICE         VERSION
22/tcp        open    ssh             OpenSSH 8.4
80/tcp        closed  http
443/tcp       closed  ssl/http
1433/tcp      closed  mssql
5432/tcp      closed  postgresql
...
```

○

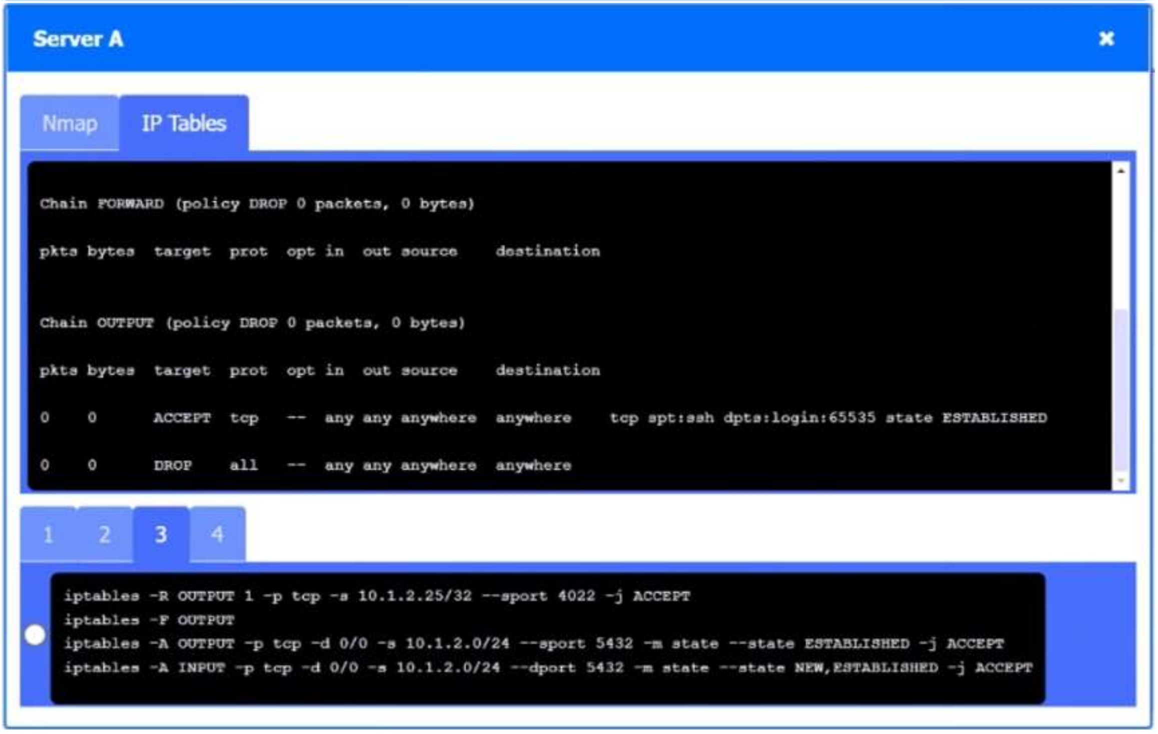
```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED

1   28      DROP    all   --  any any anywhere  anywhere


Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

○

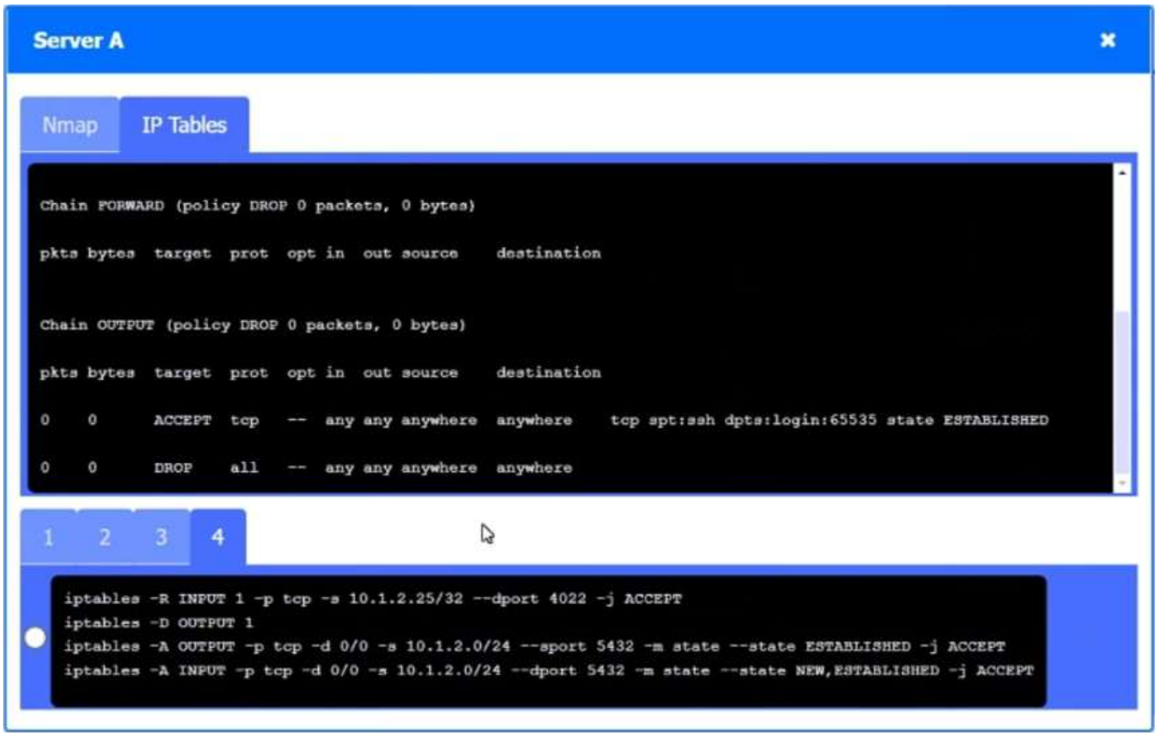
```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



```
Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes  target  prot  opt in  out source    destination


Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp spt:ssh dpts:login:65535 state ESTABLISHED

0    0      DROP    all   --  any any anywhere  anywhere
```

○

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```



```
Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes  target  prot  opt in  out source    destination


Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp spt:ssh dpts:login:65535 state ESTABLISHED

0    0      DROP    all   --  any any anywhere  anywhere
```

○

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

**Answer:**

WAP-A- Disable unneeded services
Laptop A- Disable unneeded services
Laptop B- Enabled Disk encryption & Disable unneeded services
Switch A- Change default administrative password & Disable unneeded services
Switch B- Disable unneeded services
PC-A - Disable unneeded services
PC-B - Disable unneeded services
PC-C - Patch management, Disable unneeded services

**QUESTION 493**
A new, online file hosting service is being offered. The service has the following security requirements:

```
- Threats to customer data integrity and availability should be remediated first.
- The environment should be dynamic to match increasing customer demands.
- The solution should not interfere with customers' ability to access their data at
anytime.
- Security analysts should focus on high-risk items.
```

Which of the following would BEST satisfy the requirements?

A. Expanding the use of IPS and NGFW devices throughout the environment
B. Increasing the number of analysts to identify risks that need remediation
C. Implementing a SOAR solution to address known threats
D. Integrating enterprise threat feeds in the existing SIEM

**Answer:** C

**QUESTION 494**
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts most of the responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

A. IaaS

B. SaaS
C. FaaS
D. PaaS

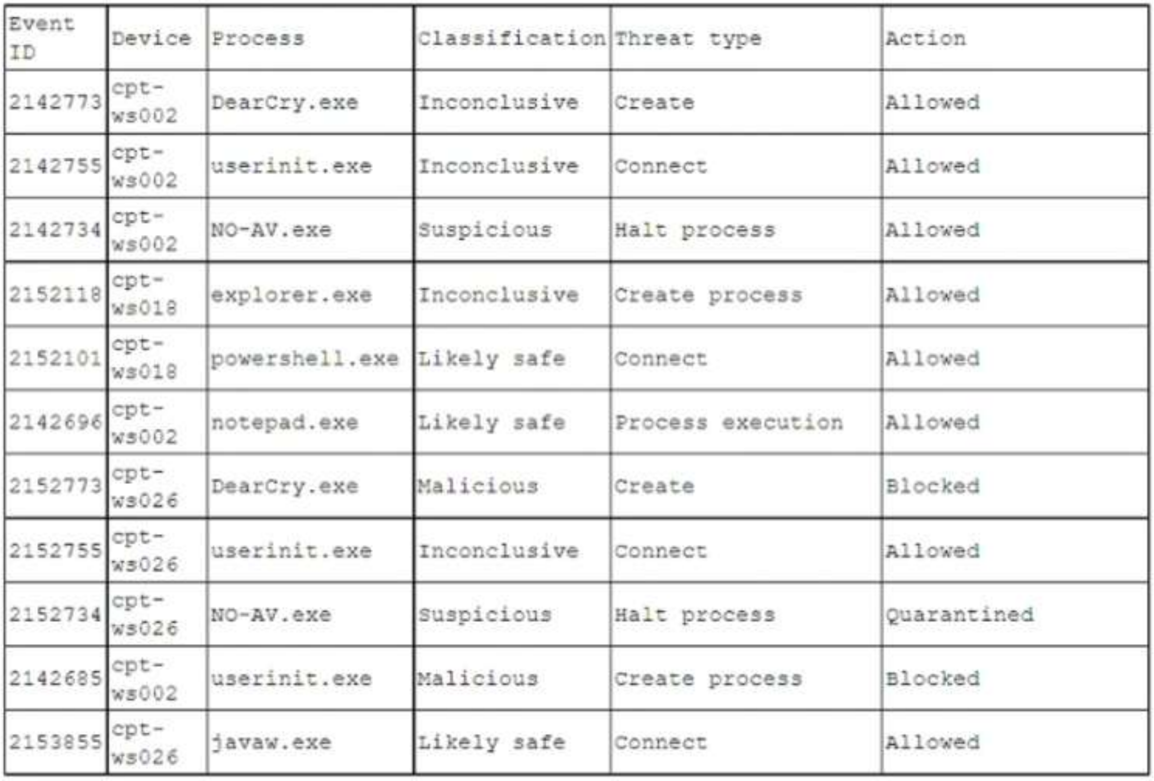
**Answer:** B

**QUESTION 495**
In comparison with traditional on-premises infrastructure configurations, defining ACLs in a CSP relies on:

A. cloud-native applications.
B. containerization.
C. serverless configurations.
D. software-defined networking.
E. secure access service edge.

**Answer:** D

**QUESTION 496**
A pharmaceutical company was recently compromised by ransomware. Given the following EDR output from the process investigation:



| Event ID | Device | Process | Classification | Threat type | Action |
|---|---|---|---|---|---|
| 2142773 | cpt-ws002 | DearCry.exe | Inconclusive | Create | Allowed |
| 2142755 | cpt-ws002 | userinit.exe | Inconclusive | Connect | Allowed |
| 2142734 | cpt-ws002 | NO-AV.exe | Suspicious | Halt process | Allowed |
| 2152118 | cpt-ws018 | explorer.exe | Inconclusive | Create process | Allowed |
| 2152101 | cpt-ws018 | powershell.exe | Likely safe | Connect | Allowed |
| 2142696 | cpt-ws002 | notepad.exe | Likely safe | Process execution | Allowed |
| 2152773 | cpt-ws026 | DearCry.exe | Malicious | Create | Blocked |
| 2152755 | cpt-ws026 | userinit.exe | Inconclusive | Connect | Allowed |
| 2152734 | cpt-ws026 | NO-AV.exe | Suspicious | Halt process | Quarantined |
| 2142685 | cpt-ws002 | userinit.exe | Malicious | Create process | Blocked |
| 2153855 | cpt-ws026 | javaw.exe | Likely safe | Connect | Allowed |

On which of the following devices and processes did the ransomware originate?

A. cpt-ws018, powershell.exe
B. cpt-ws026, DearCry.exe
C. cpt-ws002, NO-AV.exe
D. cpt-ws026, NO-AV.exe
E. cpt-ws002, DearCry.exe

**Answer:** C

**QUESTION 497**

A company has instituted a new policy in which all outbound traffic must go over TCP ports 80 and 443 for all its managed mobile devices. No other IP traffic is allowed to be initiated from a device. Which of the following should the organization consider implementing to ensure internet access continues without interruption?

A. CYOD
B. MDM
C. WPA3
D. DoH

**Answer:** D

**QUESTION 498**
A cloud security architect has been tasked with selecting the appropriate solution given the following:

```
- The solution must allow the lowest RTO possible.
- The solution must have the least shared responsibility possible.
- Patching should be a responsibility of the CSP.
```

Which of the following solutions can BEST fulfil the requirements?

A. PaaS
B. IaaS
C. Private
D. SaaS

**Answer:** D

**QUESTION 499**
A network administrator who manages a Linux web server notices the following traffic:

```
http://comptia.org/../../../../etc/shadow
```

Which of the following is the BEST action for the network administrator to take to defend against this type of web attack?

A. Validate the server certificate and trust chain.
B. Validate the server input and append the input to the base directory path.
C. Validate that the server is not deployed with default account credentials.
D. Validate that multifactor authentication is enabled on the server for all user accounts.

**Answer:** B

**QUESTION 500**
A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions.
Which of the following would BEST achieve that goal?

A. Utilize the SAN certificate to enable a single certificate for all regions.
B. Deploy client certificates to all devices in the network.
C. Configure certificate pinning inside the application.
D. Enable HSTS on the application's server side for all communication.

**Answer:** C

**QUESTION 501**
A corporation discovered its internet connection is saturated with traffic originating from multiple IP addresses across the internet. A security analyst needs to find a solution to address future occurrences of this type of attack.
Which of the following would be the BEST solution to meet this goal?

A. Implementing cloud-scrubbing services

B. Upgrading the internet link
C. Deploying a web application firewall
D. Provisioning a reverse proxy

**Answer:** A

**QUESTION 502**
A security engineer is working for a service provider and analyzing logs and reports from a new EDR solution, which is installed on a small group of workstations. Later that day, another security engineer receives an email from two developers reporting the software being used for development activities is now blocked. The developers have not made any changes to the software being used. Which of the following is the EDR reporting?

A. True positive
B. False negative
C. False positive
D. True negative

**Answer:** C

**QUESTION 503**
An organization has just been breached, and the attacker is exfiltrating data from workstations. The security analyst validates this information with the firewall logs and must stop the activity immediately. Which of the following steps should the security analyst perform NEXT?

A. Determine what data is being stolen and change the folder permissions to read only.
B. Determine which users may have clicked on a malicious email link and suspend their accounts.
C. Determine where the data is being transmitted and create a block rule.
D. Determine if a user inadvertently installed malware from a USB drive and update antivirus definitions.
E. Determine if users have been notified to save their work and turn off their workstations.

**Answer:** C

**QUESTION 504**
A security architect is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been implemented to prevent these types of risks?

A. Code reviews
B. Supply chain visibility
C. Software audits
D. Source code escrows

**Answer:** D

**QUESTION 505**
A company has decided that only administrators are permitted to use PowerShell on their Windows computers. Which of the following is the BEST way for an administrator to implement this decision?

A. Monitor the Application and Services Logs group within Windows Event Log.
B. Uninstall PowerShell from all workstations.
C. Configure user settings In Group Policy.
D. Provide user education and training.
E. Block PowerShell via HIDS.

**Answer:** C

**QUESTION 506**
A recent security audit identified multiple endpoints have the following vulnerabilities:

```
- Various unsecured open ports
- Active accounts for terminated personnel
- Endpoint protection software with legacy versions
- Overly permissive access rules
```

Which of the following would BEST mitigate these risks? (Choose three).

A. Local drive encryption
B. Secure boot
C. Address space layout randomization
D. Unneeded services disabled
E. Patching
F. Logging
G. Removal of unused accounts
H. Enabling BIOS password

**Answer:** DEG

**QUESTION 507**
A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client's systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
B. The change control board must review and approve a submission.
C. The information system security officer provides the systems engineer with the system updates.
D. The security engineer asks the project manager to review the updates for the client's system.

**Answer:** B

**QUESTION 508**
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTP.
C. Use OSINT techniques to evaluate and analyze the threats.
D. Implement a network-based intrusion detection system.

**Answer:** B

**QUESTION 509**
A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs. Which of the following is the MOST important consideration before making this decision?

A. Availability
B. Data sovereignty
C. Geography
D. Vendor lock-in

**Answer:** B

**QUESTION 510**
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS
B. PKI
C. CSRs
D. OCSP

**Answer:** D

**QUESTION 511**
ACSP, which wants to compete in the market, has been approaching companies in an attempt to gain business, The CSP is able to provide the same uptime as other CSPs at a markedly reduced cost. Which of the following would be the MOST significant business risk to a company that signs a contract with this CSP?

A. Resource exhaustion
B. Geographic location
C. Control plane breach
D. Vendor lock-in

**Answer:** D

**QUESTION 512**
A forensics investigator is analyzing an executable file extracted from storage media that was submitted for evidence. The investigator must use a tool that can identify whether the executable has indicators, which may point to the creator of the file. Which of the following should the investigator use while preserving evidence integrity?

A. ldd
B. bcrypt
C. SHA-3
D. ssdeep
E. dcfldd

**Answer:** E

**QUESTION 513**
A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks. Which of the following Is the MOST important infrastructure security design element to prevent an outage?

A. Supporting heterogeneous architecture
B. Leveraging content delivery network across multiple regions
C. Ensuring cloud autoscaling is in place
D. Scaling horizontally to handle increases in traffic

**Answer:** B

**QUESTION 514**
A security analyst is monitoring an organization's IDS and DLP systems for an alert indicating files were removed from the network. The files were from the workstation of an employee who was authenticated but not authorized to access the files. Which of the following should the organization do FIRST to address this issue?

A. Provide additional security awareness training.

B. Disable the employee's credentials until the issue is resolved.
C. Ask human resources to notify the employee that sensitive files were accessed.
D. Isolate the employee's network segment and investigate further.

**Answer:** D

**QUESTION 515**
In order to authenticate employees who, call in remotely, a company's help desk staff must be able to view partial information about employees because the full information may be considered sensitive. Which of the following solutions should be implemented to authenticate employees?

A. Data scrubbing
B. Field masking
C. Encryption in transit
D. Metadata

**Answer:** B

**QUESTION 516**
A systems administrator was given the following IOC to detect the presence of a malicious piece of software communicating with its command-and-control server:

```
POST /malicious.php
User-Agent: Malicious Tool V 1.0
Host: www.malicious.com
```

The IOC documentation suggests the URL is the only part that could change. Which of the following regular expressions would allow the systems administrator to determine if any of the company hosts are compromised, while reducing false positives?

A. User-Agent: Malicious Tool.*
B. www\.malicious\.com\/malicious.php
C. Post /malicious\.php
D. Host: [a-z]*\.malicious\.com
E. malicious.*

**Answer:** D

**QUESTION 517**
A security consultant has been asked to identify a simple, secure solution for a small business with a single access point. The solution should have a single SSID and no guest access. The customer facility is located in a crowded area of town, so there is a high likelihood that several people will come into range every day. The customer has asked that the solution require low administrative overhead and be resistant to offline password attacks. Which of the following should the security consultant recommend?

A. WPA2-Preshared Key
B. WPA3-Enterprise
C. WPA3-Personal
D. WPA2-Enterprise

**Answer:** C

**QUESTION 518**
A security consultant is designing an infrastructure security solution for a client company that has provided the following requirements:

```
- Access to critical web services at the edge must be redundant and highly available.
- Secure access services must be resilient to a proprietary zero-day vulnerability in a
single component.
```

```
- Automated transition of secure access solutions must be able to be triggered by
defined events or manually by security operations staff.
```

Which of the following solutions BEST meets these requirements?

A. Implementation of multiple IPSec VPN solutions with diverse endpoint configurations enabling user optionality in the selection of a remote access provider.
B. Remote access services deployed using vendor-diverse redundancy with event response driven by playbooks.
C. Two separate secure access solutions orchestrated by SOAR with components provided by the same vendor for compatibility.
D. Reverse TLS proxy configuration using OpenVPN/OpenSSL with scripted failover functionality that connects critical web services out to endpoint computers.

**Answer:** B

**QUESTION 519**
A software company decides to study and implement some new security features in the software it develops in C++ language. Developers are trying to find a way to avoid a malicious process that can access another process's execution area. Which of the following techniques can the developers do?

A. Enable NX.
B. Move to Java.
C. Execute SAST.
D. Implement memory encryption.

**Answer:** A

**QUESTION 520**
A security architect recommends replacing the company's monolithic software application with a containerized solution. Historically, secrets have been stored in the application's configuration files. Which of the following changes should the security architect make in the new system?

A. Use a secrets management tool.
B. Save secrets in key escrow.
C. Store the secrets inside the Dockerfiles.
D. Run all Dockerfiles in a randomized namespace.

**Answer:** A

**QUESTION 521**
Law enforcement officials informed an organization that an investigation has begun. Which of the following is the FIRST step the organization should take?

A. Initiate a legal hold.
B. Refer to the retention policy.
C. Perform e-discovery.
D. Review the subpoena.

**Answer:** A