EDUSUM

#1 Online Certification Guide

Excel at CAS-004 CASP+ Exam: Proven Study Methods for Triumph

CompTIA CASP+ CERTIFICATION QUESTIONS & ANSWERS

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

Table of Contents

Getting Ready for the CAS-004 Exam:

Use proven study tips and techniques to **prepare** for the CAS-004 exam confidently. Boost your readiness, improve your understanding regarding the Cybersecurity, and increase your chances of success in the CompTIA CompTIA Advanced Security Practitioner (CASP+) with our comprehensive guide. Start your journey towards exam excellence today.

CompTIA Advanced Security Practitioner (CASP+) Certification Details:

Exam Name	CompTIA Advanced Security Practitioner (CASP+)
Exam Code	CAS-004
Exam Price	$509 (USD)
Duration	165 mins
Number of Questions	90
Passing Score	Pass / Fail
Books / Training	**CertMaster Learn for CASP+** **CompTIA CASP+ Certification Training**
Schedule Exam	**Pearson VUE**
Sample Questions	**CompTIA CASP+ Sample Questions**
Practice Exam	**CompTIA CAS-004 Certification Practice Exam**

Explore CAS-004 Syllabus:

Topic	Details
Security Architecture 29%	
Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.	- Services • Load balancer • Intrusion detection system (IDS)/network intrusion detection system (NIDS)/wireless intrusion detection system (WIDS) • Intrusion prevention system (IPS)/network intrusion prevention system (NIPS)/wireless intrusion prevention system (WIPS) • Web application firewall (WAF) • Network access control (NAC)

Topic	Details
	• Virtual private network (VPN) • Domain Name System Security Extensions (DNSSEC) • Firewall/unified threat management (UTM)/next-generation firewall (NGFW) • Network address translation (NAT) gateway • Internet gateway • Forward/transparent proxy • Reverse proxy • Distributed denial-of-service (DDoS) protection • Routers • Mail security • Application programming interface (API) gateway/Extensible Markup Language (XML) gateway • Traffic mirroring - Switched port analyzer (SPAN) ports - Port mirroring - Virtual private cloud (VPC) - Network tap • Sensors - Security information and event management (SIEM) - File integrity monitoring (FIM) - Simple Network Management Protocol (SNMP) traps - NetFlow - Data loss prevention (DLP) - Antivirus - Segmentation • Microsegmentation • Local area network (LAN)/virtual local area network (VLAN) • Jump box • Screened subnet • Data zones • Staging environments • Guest environments

Topic	Details
	- VPC/virtual network (VNET) - Availability zone - NAC lists - Policies/security groups - Regions - Access control lists (ACLs) - Peer-to-peer - Air gap - Deperimeterization/zero trust - Cloud - Remote work - Mobile - Outsourcing and contracting - Wireless/radio frequency (RF) networks - Merging of networks from various organizations - Peering - Cloud to on premises - Data sensitivity levels - Mergers and acquisitions - Cross-domain - Federation - Directory services - Software-defined networking (SDN) - Open SDN - Hybrid SDN - SDN overlay
Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	- Scalability - Vertically - Horizontally - Resiliency - High availability - Diversity/heterogeneity - Course of action orchestration

Topic	Details
	• Distributed allocation • Redundancy • Replication • Clustering - Automation • Autoscaling • Security Orchestration, Automation, and Response (SOAR) • Bootstrapping - Performance - Containerization - Virtualization - Content delivery network - Caching
Given a scenario, integrate software applications securely into an enterprise architecture.	- Baseline and templates • Secure design patterns/ types of web technologies - Storage design patterns • Container APIs • Secure coding standards • Application vetting processes • API management • Middleware - Software assurance • Sandboxing/development environment • Validating third-party libraries • Defined DevOps pipeline • Code signing • Interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST) - Considerations of integrating enterprise applications • Customer relationship management (CRM) • Enterprise resource planning (ERP) • Configuration management database (CMDB)

Topic	Details
	• Content management system (CMS) • Integration enablers - Directory services - Domain name system (DNS) - Service-oriented architecture (SOA) - Enterprise service bus (ESB) - Integrating security into development life cycle • Formal methods • Requirements • Fielding • Insertions and upgrades • Disposal and reuse • Testing - Regression - Unit testing - Integration testing • Development approaches - SecDevOps - Agile - Waterfall - Spiral - Versioning - Continuous integration/continuous delivery (CI/CD) pipelines • Best practices - Open Web Application Security Project (OWASP) - Proper Hypertext Transfer Protocol (HTTP) headers
Given a scenario, implement data security techniques for securing enterprise architecture.	- Data loss prevention • Blocking use of external media • Print blocking • Remote Desktop Protocol (RDP) blocking • Clipboard privacy controls • Restricted virtual desktop infrastructure (VDI) implementation • Data classification blocking

Topic	Details
	- Data loss detection • Watermarking • Digital rights management (DRM) • Network traffic decryption/deep packet inspection • Network traffic analysis - Data classification, labeling, and tagging • Metadata/attributes - Obfuscation • Tokenization • Scrubbing • Masking - Anonymization - Encrypted vs. unencrypted - Data life cycle • Create • Use • Share • Store • Archive • Destroy - Data inventory and mapping - Data integrity management - Data storage, backup, and recovery • Redundant array of inexpensive disks (RAID)
Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.	- Credential management • Password repository application - End-user password storage - On premises vs. cloud repository • Hardware key manager • Privileged access management - Password policies • Complexity

Topic	Details
	• Length • Character classes • History • Maximum/minimum age • Auditing • Reversable encryption - Federation • Transitive trust • OpenID • Security Assertion Markup Language (SAML) • Shibboleth - Access control • Mandatory access control (MAC) • Discretionary access control (DAC) • Role-based access control • Rule-based access control • Attribute-based access control - Protocols • Remote Authentication Dial-in User Server (RADIUS) • Terminal Access Controller Access Control System (TACACS) • Diameter • Lightweight Directory Access Protocol (LDAP) • Kerberos • OAuth • 802.1X • Extensible Authentication Protocol (EAP) - Multifactor authentication (MFA) • Two-factor authentication (2FA) • 2-Step Verification • In-band • Out-of-band - One-time password (OTP)

Topic	Details
	• HMAC-based one-time password (HOTP) • Time-based one-time password (TOTP) - Hardware root of trust - Single sign-on (SSO) - JavaScript Object Notation (JSON) web token (JWT) - Attestation and identity proofing
Given a set of requirements, implement secure cloud and virtualization solutions.	- Virtualization strategies • Type 1 vs. Type 2 hypervisors • Containers • Emulation • Application virtualization • VDI - Provisioning and deprovisioning - Middleware - Metadata and tags - Deployment models and considerations • Business directives - Cost - Scalability - Resources - Location - Data protection • Cloud deployment models - Private - Public - Hybrid - Community - Hosting models • Multitenant • Single-tenant - Service models • Software as a service (SaaS) • Platform as a service (PaaS) • Infrastructure as a service (IaaS) - Cloud provider limitations

Topic	Details
	• Internet Protocol (IP) address scheme • VPC peering - Extending appropriate on-premises controls - Storage models • Object storage/file-based storage • Database storage • Block storage • Blob storage • Key-value pairs
Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.	- Privacy and confidentiality requirements - Integrity requirements - Non-repudiation - Compliance and policy requirements - Common cryptography use cases • Data at rest • Data in transit • Data in process/data in use • Protection of web services • Embedded systems • Key escrow/management • Mobile security • Secure authentication • Smart card - Common PKI use cases • Web services • Email • Code signing • Federation • Trust models • VPN • Enterprise and security automation/orchestration
Explain the impact of emerging technologies on enterprise security and privacy.	- Artificial intelligence - Machine learning - Quantum computing - Blockchain - Homomorphic encryption

Topic	Details
	• Private information retrieval • Secure function evaluation • Private function evaluation - Secure multiparty computation - Distributed consensus - Big Data - Virtual/augmented reality - 3-D printing - Passwordless authentication - Nano technology - Deep learning • Natural language processing • Deep fakes - Biometric impersonation
Security Operations 30%	
Given a scenario, perform threat management activities.	- Intelligence types • Tactical - Commodity malware • Strategic - Targeted attacks • Operational - Threat hunting - Threat emulation - Actor types • Advanced persistent threat (APT)/nation-state • Insider threat • Competitor • Hacktivist • Script kiddie • Organized crime - Threat actor properties • Resource - Time - Money

Topic	Details
	- Supply chain access - Create vulnerabilities - Capabilities/sophistication - Identifying techniques - Intelligence collection methods - Intelligence feeds - Deep web - Proprietary - Open-source intelligence (OSINT) - Human intelligence (HUMINT) - Frameworks - MITRE Adversarial Tactics, Techniques, & Common knowledge (ATT&CK) - ATT&CK for industrial control system (ICS) - Diamond Model of Intrusion Analysis - Cyber Kill Chain
Given a scenario, analyze indicators of compromise and formulate an appropriate response.	- Indicators of compromise - Packet capture (PCAP) - Logs - Network logs - Vulnerability logs - Operating system logs - Access logs - NetFlow logs - Notifications - FIM alerts - SIEM alerts - DLP alerts - IDS/IPS alerts - Antivirus alerts - Notification severity/priorities - Unusual process activity - Response - Firewall rules - IPS/IDS rules

Topic	Details
	- ACL rules - Signature rules - Behavior rules - DLP rules - Scripts/regular expressions
Given a scenario, perform vulnerability management activities.	- Vulnerability scans • Credentialed vs. non-credentialed • Agent-based/server-based • Criticality ranking • Active vs. passive - Security Content Automation Protocol (SCAP) • Extensible Configuration Checklist Description Format (XCCDF) • Open Vulnerability and Assessment Language (OVAL) • Common Platform Enumeration (CPE) • Common Vulnerabilities and Exposures (CVE) • Common Vulnerability Scoring System (CVSS) • Common Configuration Enumeration (CCE) • Asset Reporting Format (ARF) - Self-assessment vs. third-party vendor assessment - Patch management - Information sources • Advisories • Bulletins • Vendor websites • Information Sharing and Analysis Centers (ISACs) • News reports
Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.	- Methods • Static analysis • Dynamic analysis • Side-channel analysis • Reverse engineering - Software

Topic	Details
	- Hardware - Wireless vulnerability scan - Software composition analysis - Fuzz testing - Pivoting - Post-exploitation - Persistence - Tools - SCAP scanner - Network traffic analyzer - Vulnerability scanner - Protocol analyzer - Port scanner - HTTP interceptor - Exploit framework - Password cracker - Dependency management - Requirements - Scope of work - Rules of engagement - Invasive vs. non-invasive - Asset inventory - Permissions and access - Corporate policy considerations - Facility considerations - Physical security considerations - Rescan for corrections/changes
Given a scenario, analyze vulnerabilities and recommend risk mitigations.	- Vulnerabilities - Race conditions - Overflows - Buffer - Integer - Broken authentication - Unsecure references - Poor exception handling

Topic	Details
	• Security misconfiguration • Improper headers • Information disclosure • Certificate errors • Weak cryptography implementations • Weak ciphers • Weak cipher suite implementations • Software composition analysis • Use of vulnerable frameworks and software modules • Use of unsafe functions • Third-party libraries - Dependencies - Code injections/malicious changes - End of support/end of life - Regression issues - Inherently vulnerable system/application • Client-side processing vs. server-side processing • JSON/representational state transfer (REST) • Browser extensions - Flash - ActiveX • Hypertext Markup Language 5 (HTML5) • Asynchronous JavaScript and XML (AJAX) • Simple Object Access Protocol (SOAP) • Machine code vs. bytecode or interpreted vs. emulated - Attacks • Directory traversal • Cross-site scripting (XSS) • Cross-site request forgery (CSRF) • Injection - XML - LDAP - Structured Query Language (SQL) - Command

Topic	Details
	- Process • Sandbox escape • Virtual machine (VM) hopping • VM escape • Border Gateway Protocol (BGP)/route hijacking • Interception attacks • Denial-of-service (DoS)/DDoS • Authentication bypass • Social engineering • VLAN hopping
Given a scenario, use processes to reduce risk.	- Proactive and detection • Hunts • Developing countermeasures • Deceptive technologies - Honeynet - Honeypot - Decoy files - Simulators - Dynamic network configurations - Security data analytics • Processing pipelines - Data - Stream • Indexing and search • Log collection and curation • Database activity monitoring - Preventive • Antivirus • Immutable systems • Hardening • Sandbox detonation - Application control • License technologies • Allow list vs. block list • Time of check vs. time of use

Topic	Details
	- Atomic execution - Security automation - Cron/scheduled tasks - Bash - PowerShell - Python - Physical security - Review of lighting - Review of visitor logs - Camera reviews - Open spaces vs. confined spaces
Given an incident, implement the appropriate response.	- Event classifications • False positive • False negative • True positive • True negative - Triage event - Preescalation tasks - Incident response process • Preparation • Detection • Analysis • Containment • Recovery • Lessons learned - Specific response playbooks/processes • Scenarios - Ransomware - Data exfiltration - Social engineering • Non-automated response methods • Automated response methods - Runbooks - SOAR

Topic	Details
	- Communication plan - Stakeholder management
Explain the importance of forensic concepts.	- Legal vs. internal corporate purposes - Forensic process • Identification • Evidence collection - Chain of custody - Order of volatility 1. Memory snapshots 2. Images - Cloning • Evidence preservation - Secure storage - Backups • Analysis - Forensics tools • Verification • Presentation - Integrity preservation • Hashing - Cryptanalysis - Steganalysis
Given a scenario, use forensic analysis tools.	- File carving tools • Foremost • Strings - Binary analysis tools • Hex dump • Binwalk • Ghidra • GNU Project debugger (GDB) • OllyDbg • readelf • objdump • strace • ldd

Topic	Details
	• file - Analysis tools • ExifTool • Nmap • Aircrack-ng • Volatility • The Sleuth Kit • Dynamically vs. statically linked - Imaging tools • Forensic Toolkit (FTK) Imager • dd - Hashing utilities • sha256sum • ssdeep - Live collection vs. post-mortem tools • netstat • ps • vmstat • ldd • lsof • netcat • tcpdump • conntrack • Wireshark
Security Engineering and Cryptography 26%	
Given a scenario, apply secure configurations to enterprise mobility	- Managed configurations • Application control • Password • MFA requirements • Token-based access • Patch repository • Firmware Over-the-Air

Topic	Details
	• Remote wipe • WiFi - WiFi Protected Access (WPA2/3) - Device certificates • Profiles • Bluetooth • Near-field communication (NFC) • Peripherals • Geofencing • VPN settings • Geotagging • Certificate management • Full device encryption • Tethering • Airplane mode • Location services • DNS over HTTPS (DoH) • Custom DNS - Deployment scenarios • Bring your own device (BYOD) • Corporate-owned • Corporate owned, personally enabled (COPE) • Choose your own device (CYOD) - Security considerations • Unauthorized remote activation/deactivation of devices or features • Encrypted and unencrypted communication concerns • Physical reconnaissance • Personal data theft • Health privacy • Implications of wearable devices • Digital forensics of collected data • Unauthorized application stores • Jailbreaking/rooting • Side loading

Topic	Details
	• Containerization • Original equipment manufacturer (OEM) and carrier differences • Supply chain issues • eFuse
Given a scenario, configure and implement endpoint security controls.	- Hardening techniques • Removing unneeded services • Disabling unused accounts • Images/templates • Remove end-of-life devices • Remove end-of-support devices • Local drive encryption • Enable no execute (NX)/execute never (XN) bit • Disabling central processing unit (CPU) virtualization support • Secure encrypted enclaves/memory encryption • Shell restrictions • Address space layout randomization (ASLR) - Processes • Patching - Firmware - Application • Logging • Monitoring - Mandatory access control • Security-Enhanced Linux (SELinux)/Security-Enhanced Android (SEAndroid) • Kernel vs. middleware - Trustworthy computing • Trusted Platform Module (TPM) • Secure Boot • Unified Extensible Firmware Interface (UEFI)/basic input/output system (BIOS) protection • Attestation services

Topic	Details
	• Hardware security module (HSM) • Measured boot • Self-encrypting drives (SEDs) - Compensating controls • Antivirus • Application controls • Host-based intrusion detection system (HIDS)/Host-based intrusion prevention system (HIPS) • Host-based firewall • Endpoint detection and response (EDR) • Redundant hardware • Self-healing hardware • User and entity behavior analytics (UEBA)
Explain security considerations impacting specific sectors and operational technologies.	- Embedded • Internet of Things (IoT) • System on a chip (SoC) • Application-specific integrated circuit (ASIC) • Field-programmable gate array (FPGA) - ICS/supervisory control and data acquisition (SCADA) • Programmable logic controller (PLC) • Historian • Ladder logic • Safety instrumented system • Heating, ventilation, and air conditioning (HVAC) - Protocols • Controller Area Network (CAN) bus • Modbus • Distributed Network Protocol 3 (DNP3) • Zigbee • Common Industrial Protocol (CIP) • Data distribution service - Sectors

Topic	Details
	- Energy - Manufacturing - Healthcare - Public utilities - Public services - Facility services
Explain how cloud technology adoption impacts organizational security.	- Automation and orchestration - Encryption configuration - Logs • Availability • Collection • Monitoring • Configuration • Alerting - Monitoring configurations - Key ownership and location - Key life-cycle management - Backup and recovery methods • Cloud as business continuity and disaster recovery (BCDR) • Primary provider BCDR • Alternative provider BCDR - Infrastructure vs. serverless computing - Application virtualization - Software-defined networking - Misconfigurations - Collaboration tools - Storage configurations • Bit splitting • Data dispersion - Cloud access security broker (CASB)
Given a business requirement, implement the appropriate PKI solution.	- PKI hierarchy • Certificate authority (CA) • Subordinate/intermediate CA • Registration authority (RA)

Topic	Details
	- Certificate types • Wildcard certificate • Extended validation • Multidomain • General purpose - Certificate usages/profiles/templates • Client authentication • Server authentication • Digital signatures • Code signing - Extensions • Common name (CN) • Subject alternate name (SAN) - Trusted providers - Trust model - Cross-certification - Configure profiles - Life-cycle management - Public and private keys - Digital signature - Certificate pinning - Certificate stapling - Certificate signing requests (CSRs) - Online Certificate Status Protocol (OCSP) vs. certificate revocation list (CRL) - HTTP Strict Transport Security (HSTS)
Given a business requirement, implement the appropriate cryptographic protocols and algorithms.	- Hashing • Secure Hashing Algorithm (SHA) • Hash-based message authentication code (HMAC) • Message digest (MD) • RACE integrity primitives evaluation message digest (RIPEMD) • Poly1305 - Symmetric algorithms

Topic	Details
	- Modes of operation - Galois/Counter Mode (GCM) - Electronic codebook (ECB) - Cipher block chaining (CBC) - Counter (CTR) - Output feedback (OFB) • Stream and block - Advanced Encryption Standard (AES) - Triple digital encryption standard (3DES) - ChaCha - Salsa20 - Asymmetric algorithms • Key agreement - Diffie-Hellman - Elliptic-curve Diffie-Hellman (ECDH) • Signing - Digital signature algorithm (DSA) - Rivest, Shamir, and Adleman (RSA) - Elliptic-curve digital signature algorithm (ECDSA) - Protocols • Secure Sockets Layer (SSL)/Transport Layer Security (TLS) • Secure/Multipurpose Internet Mail Extensions (S/MIME) • Internet Protocol Security (IPSec) • Secure Shell (SSH) • EAP - Elliptic curve cryptography • P256 • P384 - Forward secrecy - Authenticated encryption with associated data - Key stretching • Password-based key derivation function 2 (PBKDF2)

Topic	Details
	• Bcrypt
Given a scenario, troubleshoot issues with cryptographic implementations.	- Implementation and configuration issues • Validity dates • Wrong certificate type • Revoked certificates • Incorrect name • Chain issues - Invalid root or intermediate CAs - Self-signed • Weak signing algorithm • Weak cipher suite • Incorrect permissions • Cipher mismatches • Downgrade - Keys • Mismatched • Improper key handling • Embedded keys • Rekeying • Exposed private keys • Crypto shredding • Cryptographic obfuscation • Key rotation • Compromised keys
Governance, Risk, and Compliance 15%	
Given a set of requirements, apply the appropriate risk strategies.	- Risk assessment • Likelihood • Impact • Qualitative vs. quantitative • Exposure factor • Asset value • Total cost of ownership (TCO) • Return on investment (ROI) • Mean time to recovery (MTTR)

Topic	Details
	• Mean time between failure (MTBF) • Annualized loss expectancy (ALE) • Annualized rate of occurrence (ARO) • Single loss expectancy (SLE) • Gap analysis - Risk handling techniques • Transfer • Accept • Avoid • Mitigate - Risk types • Inherent • Residual • Exceptions - Risk management life cycle • Identify • Assess • Control - People - Process - Technology - Protect - Detect - Respond - Restore • Review • Frameworks - Risk tracking • Risk register • Key performance indicators - Scalability - Reliability - Availability • Key risk indicators - Risk appetite vs. risk tolerance

Topic	Details
	• Tradeoff analysis • Usability vs. security requirements - Policies and security practices • Separation of duties • Job rotation • Mandatory vacation • Least privilege • Employment and termination procedures • Training and awareness for users • Auditing requirements and frequency
Explain the importance of managing and mitigating vendor risk.	- Shared responsibility model (roles/responsibilities) • Cloud service provider (CSP) - Geographic location - Infrastructure - Compute - Storage - Networking - Services • Client - Encryption - Operating systems - Applications - Data - Vendor lock-in and vendor lockout - Vendor viability • Financial risk • Merger or acquisition risk - Meeting client requirements • Legal • Change management • Staff turnover • Device and technical configurations - Support availability - Geographical considerations - Supply chain visibility - Incident reporting requirements

Topic	Details
	- Source code escrows - Ongoing vendor assessment tools - Third-party dependencies • Code • Hardware • Modules - Technical considerations • Technical testing • Network segmentation • Transmission control • Shared credentials
Explain compliance frameworks and legal considerations, and their organizational impact.	- Security concerns of integrating diverse industries - Data considerations • Data sovereignty • Data ownership • Data classifications • Data retention • Data types - Health - Financial - Intellectual property • Personally identifiable information (PII) • Data removal, destruction, and sanitization - Geographic considerations • Location of data • Location of data subject • Location of cloud provider - Third-party attestation of compliance - Regulations, accreditations, and standards • Payment Card Industry Data Security Standard (PCI DSS) • General Data Protection Regulation (GDPR) • International Organization for Standardization (ISO) • Capability Maturity Model Integration (CMMI)

Topic	Details
	- National Institute of Standards and Technology (NIST) - Children’s Online Privacy Protection Act (COPPA) - Common Criteria - Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) - Legal considerations - Due diligence - Due care - Export controls - Legal holds - E-discovery - Contract and agreement types - Service-level agreement (SLA) - Master service agreement (MSA) - Non-disclosure agreement (NDA) - Memorandum of understanding (MOU) - Interconnection security agreement (ISA) - Operational-level agreement - Privacy-level agreement
Explain the importance of business continuity and disaster recovery concepts.	- Business impact analysis - Recovery point objective - Recovery time objective - Recovery service level - Mission essential functions - Privacy impact assessment - Disaster recovery plan (DRP)/business continuity plan (BCP) - Cold site - Warm site - Hot site - Mobile site - Incident response plan

Topic	Details
	- Roles/responsibilities - After-action reports - Testing plans - Checklist - Walk-through - Tabletop exercises - Full interruption test - Parallel test/simulation test

Prepare with CAS-004 Sample Questions:

Question: 1

A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software.

Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.

Which of the following techniques would be BEST suited for this requirement?

a) Deploy SOAR utilities and runbooks.
b) Replace the associated hardware.
c) Provide the contractors with direct access to satellite telemetry data.
d) Reduce link latency on the affected ground and satellite segments.

Answer: a

Question: 2

A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise.

The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.

Which of the following would be BEST for the company to implement?

a) A WAF
b) An IDS
c) A SIEM
d) A honeypot

Answer: d

Question: 3

An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial patches against a recent exploit that could gain root access.

Which of the following describes the administrator's discovery?

a) A vulnerability
b) A threat
c) A breach
d) A risk

Answer: a

Question: 4

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

Question: 5

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) 8
b) 0.5
c) 50
d) 36,500

Answer: b

Question: 6

Which of the following is the GREATEST security concern with respect to BYOD?

a) The filtering of sensitive data out of data flows at geographic boundaries
b) Removing potential bottlenecks in data transmission paths
c) The transfer of corporate data onto mobile corporate devices
d) The migration of data into and out of the network in an uncontrolled manner

Answer: d

Question: 7

A company recently migrated from on-premises to cloud to meet a new requirement that the cloud provider reacts to any security vulnerabilities related to the underlying service.
Which of the following risk handling techniques is described?

a) Avoid
b) Transfer
c) Accept
d) Mitigate

Answer: b

Question: 8

Many of an organization's recent security incidents on the corporate network involve third-party software vulnerabilities. Which of the following would reduce the risk presented by these vulnerabilities?

a) Only allow approved applications to be installed on workstations.
b) Block all malicious and hard to manage applications from being installed.
c) Perform software composition analysis for all software developed in-house.
d) Properly manage third-party libraries in the development environment.

Answer: a

Question: 9

An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

a) NIST
b) GDPR
c) PCI DSS
d) ISO

Answer: c

Question: 10

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

a) NDA
b) MOU
c) BIA
d) SLA

Answer: d

Study Tips to Pass the CompTIA Advanced Security Practitioner Exam:

Understand the CAS-004 Exam Format:

Before diving into your study routine, it's essential to familiarize yourself with the CAS-004 exam format. Take the time to review the **exam syllabus**, understand the test structure, and identify the key areas of focus. Prior knowledge of what to expect on exam day will help you tailor your study plan.

Make A Study Schedule for the CAS-004 Exam:

To effectively prepare for the CAS-004 exam, make a study schedule that fits your lifestyle and learning style. Set specific time slots for studying each day and focus on the topics based on their importance and your proficiency level. Consistency is a must, so stick to your schedule and avoid procrastination.

Study from Different Resources:

Make sure to expand beyond one source of study material. Utilize multiple resources such as textbooks, online courses, practice exams, and study guides to understand the CAS-004 exam topics comprehensively. Each resource offers unique insights and explanations that can enhance your learning experience.

Practice Regularly for the CAS-004 Exam:

Practice makes you perfect for the CAS-004 exam preparation as well. Regular practice allows you to reinforce your knowledge of key concepts, enhance your problem-solving skills, and familiarize yourself with the exam format. Dedicate time to solving practice questions and sample tests to gauge your progress.

Take Breaks and Rest:

While it's essential to study, taking breaks and allowing yourself to rest is equally important. Overloading your brain with information without adequate rest can lead to burnout and decreased productivity. Set short breaks during your study sessions to recharge and maintain focus.

Stay Organized During the CAS-004 Exam Preparation:

Stay organized throughout your CAS-004 study journey by keeping track of your progress and materials. Maintain a tidy study space, use folders or digital tools to organize your notes and resources, and create a checklist of topics to cover. An organized approach helps you stay on track and minimize stress.

Seek Clarification from Mentors:

Feel free to seek clarification if you encounter any confusing or challenging concepts during your study sessions. Reach out to peers, instructors, or online forums for assistance. Clarifying doubts early on will prevent misunderstandings and ensure you have a solid grasp of the material.

Regular Revision Plays A vital Role for the CAS-004 Exam:

Consistent revision is essential for the long-term retention of information. Review previously covered topics to reinforce your understanding and identify any areas requiring additional attention. Reviewing regularly will help solidify your knowledge and boost your confidence.

Practice Time Management for the CAS-004 Exam:

Effective time management is crucial on exam day to ensure you complete all sections within the allocated time frame. During your practice sessions, simulate CAS-004 exam conditions and practice pacing yourself accordingly. Develop strategies for tackling each section efficiently to maximize your score.

Stay Positive and Confident:

Lastly, always have a positive mindset and believe in your abilities. Stay confident in your preparation efforts and trust that you have adequately equipped yourself to tackle the CAS-004 exam. Visualize success, stay focused, and approach the exam calmly and confidently.

Benefits of Earning the CAS-004 Exam:

- Achieving the CAS-004 certification opens doors to new career opportunities and advancement within your field.
- The rigorous preparation required for the CAS-004 exam equips you with in-depth knowledge and practical skills relevant to your profession.
- Holding the CAS-004 certification demonstrates your expertise and commitment to excellence, earning recognition from peers and employers.

- Certified professionals often grab higher salaries and enjoy greater earning potential than their non-certified counterparts.
- Obtaining the CAS-004 certification validates your proficiency and credibility, instilling confidence in clients, employers, and colleagues.

Discover the Reliable Practice Test for the CAS-004 Certification:

EduSum.com brings you comprehensive information about the CAS-004 exam. We offer genuine practice tests tailored for the CAS-004 certification. What benefits do these practice tests offer? You'll encounter authentic exam-like questions crafted by industry experts, providing an opportunity to enhance your performance in the actual exam. Count on EduSum.com for rigorous, unlimited access to CAS-004 practice tests over two months [link to product page], enabling you to bolster your confidence steadily. Through dedicated practice, many candidates have succeeded in streamlining their journey towards obtaining the CompTIA Advanced Security Practitioner (CASP+).

Concluding Thoughts:

Preparing for the CAS-004 exam requires dedication, strategy, and effective study techniques. These study tips can enhance your preparation, boost your confidence, and improve your chances of passing the exam with flying colors. Remember to stay focused, stay organized, and believe in yourself. Good luck!