CWNP CSAE-101

CWNP Security Administrator and Engineer Certification Questions & Answers

Exam Summary – Syllabus – Questions

CSAE-101

CWNP Certified Security Administrator and Engineer

40 Questions Exam – 70% Cut Score – Duration of 100 minutes

Table of Contents:

Know Your CSAE-101 Certification Well:

The CSAE-101 is best suitable for candidates who want to gain knowledge in the CWNP Wireless IoT solutions. Before you start your CSAE-101 preparation you may struggle to get all the crucial Security Administrator and Engineer materials like CSAE-101 syllabus, sample questions, study guide.

But don't worry the CSAE-101 PDF is here to help you prepare in a stress-free manner.
The PDF is a combination of all your queries like-

- What is in the CSAE-101 syllabus?
- How many questions are there in the CSAE-101 exam?
- Which Practice test would help me to pass the CSAE-101 exam at the first attempt?

Passing the CSAE-101 exam makes you CWNP Certified Security Administrator and Engineer. Having the Security Administrator and Engineer certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CWNP CSAE-101 Security Administrator and Engineer Certification Details:

Exam Name	CWNP Security Administrator and Engineer
Exam Code	CSAE-101
Exam Price	$399 USD
Duration	100 minutes
Number of Questions	40
Passing Score	70%
Recommended Training	**Prometric**
Sample Questions	**CWNP CSAE-101 Sample Questions**
Practice Exam	**CWNP Certified Security Administrator and Engineer Practice Test**

CSAE-101 Syllabus:

Section	Weight	Objectives
Security Concepts and Terminology	15%	- Understand and evaluate security controls • Security control categories and types - Technical controls - Managerial controls - Operational controls - Physical controls • Defense-in-depth strategies • Control effectiveness measurement and validation • Gap analysis and remediation planning - Explain how the following core security principles apply to enterprise environments • CIA triad implementation (Confidentiality, Integrity, Availability) • Non-repudiation mechanisms • AAA framework deployment (Authentication, Authorization, Accounting) • Zero Trust architecture • Control plane and data plane security • Policy-driven access control systems • Policy enforcement points - Describe and distinguish among these physical security systems • Access control systems and badge management • Video surveillance systems (CCTV, IP cameras) • Environmental controls (HVAC, fire suppression) • Physical intrusion detection sensors • Lighting and perimeter security • Security guard operations and integration

Section	Weight	Objectives
		- Describe and distinguish among these deception and disruption technologies • Honeypot deployment and management • Honeynet architecture design • Honeyfile and honeytoken strategies • Integration with threat intelligence platforms • Deception technology for threat detection - Explain these cryptographic solutions and the roles they play in enterprise security • PKI infrastructure deployment and management • Certificate lifecycle management (issuance, renewal, revocation) • Encryption implementation - Full-disk encryption - Partition encryption - File encryption - Volume encryption - Database encryption - Transport encryption • Key management systems and HSM integration • Digital signatures and key stretching • Hashing and salting techniques • Blockchain and open public ledger technologies • Certificate management - Certificate Authority (CA) - Certificate Revocation List (CRL) - Online Certificate Status Protocol (OCSP) - Certificate Signing Request (CSR) generation - Understand how to apply change management processes for security • Security-focused change approval workflows

Section	Weight	Objectives
		• Impact analysis and risk assessment for changes • Backout plans and rollback procedures • Configuration management and version control • Documentation standards for security changes • Stakeholder management in change processes
Threats and Vulnerabilities	15%	- Analyze threat actors, attributes, and motivations • Threat actor types - Nation-state actors - Organized crime - Hacktivists - Insider threats - Shadow IT • Threat actor attribution and profiling • Actor attributes (internal/external, resources/funding, sophistication level) • Motivations (data exfiltration, espionage, financial gain, disruption, war) • Attack vector analysis across multiple surfaces • TTPs (tactics, techniques, and procedures) mapping to MITRE ATT&CK - Assess and mitigate attack vectors and surfaces • Message-based attacks (email, SMS, instant messaging) • Image-based and file-based attack vectors • Voice call and removable device threats • Social engineering campaigns (phishing, vishing, smishing, pretexting, watering hole) • Supply chain attacks (MSPs, vendors, suppliers)

Section	Weight	Objectives
		• Vulnerable and unsupported software management • Network-based attack surfaces (wireless, wired, Bluetooth) • Default credential and open port management - Identify and classify vulnerabilities across environments • Application vulnerabilities (memory injection, buffer overflow, race conditions, malicious updates) • OS-based and web-based vulnerabilities (SQL injection, XSS) • Hardware and firmware vulnerabilities • Virtualization vulnerabilities (VM escape, resource reuse) • Cloud-specific and supply chain vulnerabilities • Mobile device vulnerabilities (side loading, jailbreaking) • Zero-day vulnerability management • Misconfiguration identification - Analyze and respond to indicators of malicious activity • Malware analysis - Ransomware - Trojans - Worms - Rootkits - Spyware - Bloatware - Viruses - Keyloggers - Logic bombs • Physical attack indicators (brute force, RFID cloning, environmental)

Section	Weight	Objectives
		• Network attack detection (DDoS, DNS attacks, wireless attacks, on-path, credential replay) • Application attack identification (injection, buffer overflow, replay, privilege escalation, forgery, directory traversal) • Cryptographic attack recognition (downgrade, collision, birthday) • Password attacks (spraying, brute force) • Behavioral indicators (account lockout, concurrent sessions, impossible travel, resource consumption, out-of-cycle logging, missing logs) - Implement comprehensive mitigation techniques • Network segmentation and isolation strategies • Access control lists and permission management • Application allow listing and isolation • Patch management programs • Encryption and monitoring implementation • Least privilege enforcement • Configuration enforcement and compliance • Secure decommissioning procedures • Hardening techniques (encryption, endpoint protection, HIPS, port/protocol disabling, default password changes, software removal)
Security Controls	30%	- Engineer security architecture for diverse contexts • On-premises vs. centralized vs. decentralized architecture • Enterprise network security (network infrastructure, network edge, internetwork connectivity, physical and logical isolation/segmentation, SDN, Zero Trust architecture)

Section	Weight	Objectives
		• Cloud security architecture (IaaS, PaaS, SaaS, public, private and hybrid) • Industrial network architecture security (ICS, /SCADA, DCS, PLC, HMI, and RTOS) • IoT system and network security • Security for common architectural components - Embedded systems security - Infrastructure as code (IaC) security - Serverless and microservices security - Containerization security • Architecture considerations (availability, resilience, cost, responsiveness, scalability, ease of deployment, risk transference, ease of recovery, patch management, power, compute) - Design and implement enterprise infrastructure security • Infrastructure device considerations (placement, attributes, attack surface, connectivity, failure modes) • Security zone design and segmentation • Failure mode planning (fail-open vs. fail-closed) • Network appliance deployment (jump servers, proxy servers, IPS/IDS, load balancers, sensors) • Port security implementation (802.1X, EAP) • Firewall architecture (WAF, UTM, NGFW, Layer 4/Layer 7) • Selection of effective security controls - Implement secure remote communication and access solutions • VPN architecture (site-to-site, remote access) • Tunneling protocols (TLS, IPSec)

Section	Weight	Objectives
		• SD-WAN security implementation • SASE (Secure Access Service Edge) architecture • Remote access security controls - Engineer comprehensive data protection strategies • Data types and classifications - Regulated data - Trade secrets - Intellectual property - Legal information - Financial information - Sensitive data - Confidential data - Public data - Restricted data - Private data - Critical data • Data state protection (at rest, in transit, in use) • Data sovereignty and geolocation compliance • Methods to secure data - Geographic restrictions - Encryption - Hashing - Masking - Tokenization - Obfuscation - Segmentation - Permission restrictions - Anonymization • Database activity monitoring and encryption • DLP implementation and policy tuning - Design resilience and recovery architecture • High availability strategies (load balancing vs. clustering) • Site resilience planning (hot, cold, warm sites)

Section	Weight	Objectives
		• Geographic dispersion strategies • Platform diversity and multi-cloud systems • Capacity planning • Testing (tabletop exercises, failover, simulation, parallel processing) • Backup strategies - Onsite/offsite storage - Backup frequency - Backup encryption - Snapshots - Recovery procedures - Replication - Journaling - Media Rotation • Power resilience (generators, UPS, redundant power supply, multiple utility feeds)
Security Monitoring	20%	- Administer secure computing resources across platforms • Secure baseline management (establishment, deployment, maintenance) • System hardening across multiple platforms - Mobile devices - Workstations - Switches and routers - Cloud infrastructure - Servers - ICS/SCADA - Embedded systems - RTOS - IoT devices • Wireless device security (site surveys, heat maps, WPA3, AAA/RADIUS, authentication protocols)

Section	Weight	Objectives
		• Mobile device management (MDM deployment, BYOD/COPE/CYOD, mobile policies, application distribution) • Application security (input validation, secure cookies, code analysis, code signing, sandboxing) - Manage assets throughout the lifecycle • Acquisition and procurement (security requirements, vendor evaluation, supply chain security) • Assignment and classification • Monitoring and tracking (inventory, enumeration, change tracking, license management) • Disposal and decommissioning (sanitization, destruction, certification, retention compliance) - Implement and operate vulnerability management programs • Vulnerability identification methods - Vulnerability scanning (authenticated, unauthenticated) - Application security testing (SAST, DAST, SCA) - Threat feed integration - Penetration testing - Bug bounty programs - System and process audits • Vulnerability analysis (confirmation, CVSS/CVE, OSV, classification, prioritization, environmental factors, risk alignment) • Remediation and validation (patching programs, compensating controls, exceptions, verification testing)

Section	Weight	Objectives
		• Vulnerability reporting - Deploy and manage security monitoring systems • SIEM (deployment, configuration, management, tuning) • XDR (extended detection and response) • Log management (aggregation, correlation, analysis, retention) • Alert management (generation, tuning, response workflows) • Compliance monitoring (SCAP security content automation scanning, benchmarks, drift detection) • Monitoring tools deployment - Antivirus and anti-malware - Data Loss Prevention (DLP) - SNMP traps - NetFlow - Network taps - Packet capture systems • Reporting and dashboards - Engineer and operate advanced security capabilities • Network security capabilities - Firewall management (rules, ACLs, ports/protocols, screened subnets) - IPS/IDS administration (trends, signatures, active vs. passive) - Network Access Control (NAC) • Content filtering and inspection - Web filtering (agent-based, proxy, URL scanning, reputation) - DNS filtering (sinkholing, threat protection) - Email security (DMARC, DKIM, SPF, gateway)

Section	Weight	Objectives
		• Operating system security (Group Policy, SELinux, security baselines) • Protocol security (secure protocols, TLS versions, cipher suites) • Endpoint security (EDR/XDR, UEBA) • File integrity monitoring - Administer identity and access management systems • User lifecycle management (provisioning, de-provisioning, least privilege) • Identity proofing and verification • Federation and SSO (LDAP, OAuth, SAML, OpenID Connect) • Access control models (MAC, DAC, RBAC, ABAC) • Multi-factor authentication (implementations, factors, risk-based authentication) • Password management (policy enforcement, passwordless authentication) • Privileged Access Management - PAM platform deployment - Just-in-time (JIT) access - Password vaulting - Session management - Account discovery • Access reviews and attestation - Implement security automation and orchestration • Automation use cases (provisioning, guardrails, ticketing, vulnerability scanning, compliance checking) • Integration capabilities (APIs, webhooks, custom scripts) • CI/CD security automation (scanning, testing, compliance gates) • Benefits and considerations

Section	Weight	Objectives
		- Execute incident response operations • Incident response process (preparation, detection, containment, eradication, recovery, lessons learned) • Training and testing (tabletop exercises, simulations, debriefs) • Root cause analysis • Threat hunting (hypothesis-driven, intelligence-driven, baseline deviation) • Digital forensics (chain of custody, acquisition, preservation, analysis, reporting) - Conduct security investigations • Log analysis - Firewall logs - Application logs - Endpoint logs - OS-specific security logs - IPS/IDS logs - Network logs - Metadata • Data source correlation (SIEM, vulnerability scans, packet captures, threat intelligence) • Investigation documentation
Security Governance	20%	- Implement effective security governance frameworks • Policies and standards development - Acceptable Use Policy (AUP) - Information security policies - Business continuity policy - Disaster recovery policy - SDLC policy - Access control standards - Encryption standards • Procedures (change management, onboarding/offboarding, playbooks)

Section	Weight	Objectives
		• External considerations (regulatory, legal, industry standards, geographic scope) • Governance structures (board oversight, committees, governance models) • Roles and responsibilities (owners, controllers, processors, custodians, responsibility matrices) • Monitoring and revision - Manage organizational risk through structured processes • Risk identification • Risk assessment (ad hoc, recurring, continuous) • Risk analysis - Qualitative analysis (probability, impact, risk matrix) - Quantitative analysis (SLE, ALE, ARO) - Environmental variables • Risk register management • Risk tolerance and appetite • Risk treatment strategies - Risk transfer - Risk acceptance (exemptions, exceptions) - Risk avoidance - Risk mitigation • Risk reporting • Business impact analysis (RTO, RPO, MTTR, MTBF) - Administer third-party risk management programs • Vendor assessment (questionnaires, audits, certifications) • Supply chain analysis (mapping, dependencies, fourth-party risk) • Vendor selection and due diligence

Section	Weight	Objectives
		• Agreement management - Service Level Agreement (SLA) - Memorandum of Agreement (MOA) - Memorandum of Understanding (MOU) - Master Service Agreement (MSA) - Statement of Work (SOW) - Non-Disclosure Agreement (NDA) - Business Partnership Agreement (BPA) - Data Processing Agreement (DPA) • Ongoing monitoring • Rules of engagement - Maintain comprehensive compliance programs • Compliance reporting and monitoring • Automation and dashboards • Privacy compliance programs - GDPR (General Data Protection Regulation) - CCPA (California Consumer Privacy Act) - HIPAA (Health Insurance Portability and Accountability Act) - PCI DSS (Payment Card Industry Data Security Standard) • Data governance (inventory, classification, retention) • Attestation processes • Internal audits (compliance assessments, control testing, gap analysis) • External audit coordination (regulatory exams, financial audits, third-party assessments) - Conduct security assessments and testing • Internal assessments (compliance, controls, vulnerabilities, architecture) • Audit coordination • Penetration testing programs - Testing types (physical, network, application, social engineering)

Section	Weight	Objectives
		- Testing methodologies (offensive, defensive, integrated) - Testing environments (known, partially-known, unknown) - Testing phases (planning, reconnaissance, exploitation, reporting) • Reconnaissance operations - Passive reconnaissance (OSINT, DNS enumeration, social media) - Active reconnaissance (port scanning, service enumeration, network mapping) - Implement security awareness and culture programs • Training programs - Delivery methods (CBT, instructor-led, microlearning, newsletters) - Content topics (phishing, social engineering, password security, data handling, OPSEC) • Phishing simulations (campaign design, execution, metrics, remedial training) • Policy communication • User guidance (quick reference guides, job aids, role-specific guides) • Situational awareness (threat notifications, advisories) • Reporting procedures (incident reporting, anonymous channels) • Culture development - Security champions programs - Gamification and incentives - Awareness metrics - Executive sponsorship

CWNP CSAE-101 Sample Questions:

Question: 1

In a Zero Trust architecture, which assumption fundamentally differentiates it from traditional perimeter-based security models?

a) Every access request must be continuously verified
b) Encryption is optional within trusted zones
c) Trust is granted after initial authentication
d) Internal networks are inherently trusted

Answer: a

Question: 2

What is the primary security benefit of deploying a honeypot within an enterprise network?

a) Blocking malicious traffic at the perimeter
b) Detecting attacker behavior and techniques
c) Encrypting sensitive data stores
d) Enforcing authentication policies

Answer: b

Question: 3

Mapping adversary behavior to tactics, techniques, and procedures (TTPs) primarily supports which security activity?

a) Asset inventory management
b) Threat modeling and attribution
c) Patch deployment scheduling
d) Data classification enforcement

Answer: b

Question: 4

Why are documented rollback procedures critical in security-focused change management?

a) They ensure rapid recovery if a change introduces risk
b) They reduce audit scope
c) They eliminate the need for testing
d) They replace incident response plans

Answer: a

Question: 5

Which access model provides secure connectivity to internal resources without extending the internal network to the client?

a) Site-to-site VPN
b) Network-layer remote access VPN
c) Zero Trust network access
d) Layer 2 tunneling

Answer: c

Question: 6

An organization measures how well existing controls reduce identified risks and compares results against target risk levels. What activity is being performed?

a) Threat modeling
b) Control effectiveness validation
c) Vulnerability scanning
d) Incident response testing

Answer: b

Question: 7

Which two factors should be evaluated when selecting the placement of security appliances? (Select two.)

a) Network traffic flow patterns
b) Device cosmetic appearance
c) Failure impact and redundancy
d) End-user preference

Answer: a, c

Question: 8

What is the primary objective of conducting vendor security assessments?

a) Negotiating contract pricing
b) Identifying and managing third-party risk
c) Reducing internal audit workload
d) Accelerating vendor onboarding

Answer: b

Question: 9

Secure decommissioning of systems primarily ensures which security outcome?

a) Improved system availability
b) Prevention of data remanence
c) Faster asset replacement
d) Simplified patch management

Answer: b

Question: 10

Which data classification typically requires the strongest access controls and monitoring?

a) Public data
b) Confidential data
c) Sensitive data
d) Regulated data

Answer: d

Study Guide to Crack CWNP Security Administrator and Engineer CSAE-101 Exam:

- Getting details of the CSAE-101 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CSAE-101 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CWNP provided training for CSAE-101 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CSAE-101 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CSAE-101 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CSAE-101 Certification

Make NWExam.com your best friend during your CWNP Security Administrator and Engineer exam preparation. We provide authentic practice tests for the CSAE-101 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CSAE-101 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CSAE-101 exam.

Start Online practice of CSAE-101 Exam by visiting URL
https://www.nwexam.com/cwnp/csae-101-cwnp-security-administrator-and-engineer-csae