시험패스에유효한CCSK최신업데이트버전덤프문제최신버전덤프샘플문제다운받기

ExamPassdump CCSK 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=1R7dWKYNVvHyZHTlS8jNRKlouxh_jz-x7

ExamPassdump의 Cloud Security Alliance인증CCSK시험대비덤프는 실제시험문제 출제경향을 충분히 연구하여 제작한 완벽한 결과물입니다.실제시험문제가 바뀌면 덤프를 제일 빠른 시일내에 업데이트하도록 하기에 한번 구매하시면 1년동안 항상 가장 최신의Cloud Security Alliance인증CCSK시험덤프자료를 제공받을수 있습니다.

The Cloud Security Alliance (CSA)은 안전한 클라우드 컴퓨팅을 위한 모범 사례와 교육을 촉진하는 비영리 기관입니다. 이 기관의 주요 이니셔티브 중 하나는 Cloud Security Knowledge (CCSK) 인증 프로그램입니다. 이 프로그램은 클라우드 보안에 대한 지식과 역량을 평가하고 검증하는 것을 목적으로 설계되었습니다.

클라우드 보안 얼라이언스(CSA)는 비영리 단체로, 기업과 개인들을 위해 클라우드 컴퓨팅 사용을 촉진하는 것을 목표로 합니다. CSA가 추진한 가장 중요한 이니셔티브 중 하나는 클라우드 보안 지식 인증(CCSK) 시험 개발입니다. CCSK는 클라우드 기반 인프라 및 응용 프로그램 보안을 책임지는 개인들의 지식과 기술을 테스트하는 자격증입니다.

>> CCSK최신 업데이트버전 덤프문제 <<

CCSK최신 업데이트버전 덤프문제 완벽한 시험 기출문제

ExamPassdump의Cloud Security Alliance인증CCSK자료는 제일 적중률 높고 전면적인 덤프임으로 여러분은 100%한번에 응시로 패스하실 수 있습니다. 그리고 우리는 덤프를 구매 시 일년무료 업뎃을 제공합니다. 여러분은 먼저 우리 ExamPassdump사이트에서 제공되는Cloud Security Alliance인증CCSK시험덤프의 일부분인 데모 즉 문제와 답을 다운받으셔서 체험해보실 수 잇습니다.

CCSK v4.0 시험은 클라우드 기술과 함께 일하는 IT 전문가에게 필수적인 자격증입니다. 이 자격증은 클라우드 보안 최상의 실천 방법에 대한 포괄적인 이해를 제공하며 개인이 이 분야의 전문성을 증명하는 데 도움이 됩니다. 이 자격증은 산업 리더들에게 널리 인정되며 개인의 경력을 발전시키고 수익을 높일 수 있습니다.

최신 Cloud Security Knowledge CCSK 무료샘플문제 (Q70-Q75):

질문 # 70
Which type of security tool is essential for enforcing controls in a cloud environment to protect endpoints?

- A. Unified Threat Management (UTM).
- B. Endpoint Detection and Response (EDR).
- C. Intrusion Detection System (IDS).
- D. Web Application Firewall (WAF).

정답：B

설명：
Endpoint Detection and Response (EDR) is a critical security tool for cloud environments that monitors, detects, and responds to endpoint threats.
Why EDR is Essential for Cloud Security?
* Real-Time Threat Detection & Response
* EDR continuously monitors endpoint activity (e.g., cloud VMs, servers, containers).
* Detects anomalous behavior, malware, and unauthorized access attempts.
* Automated Remediation & Forensics
* Uses Machine Learning (ML) & AI to analyze cloud endpoint telemetry.
* Supports automated response actions (isolating infected endpoints, rolling back malicious changes).
* Cloud-Native Security Integration
* Works with Cloud Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR).
* Enables proactive threat hunting in hybrid and multi-cloud environments.
* Complements Other Cloud Security Tools
* WAF (Web Application Firewall) protects against web-based attacks (OWASP Top 10) but does not provide endpoint security.
* UTM (Unified Threat Management) is more suited for traditional perimeter security (firewalls, IPS/IDS).
* IDS (Intrusion Detection System) only detects threats, whereas EDR actively responds to them
.
This aligns with:
* CCSK v5 - Security Guidance v4.0, Domain 7 (Infrastructure Security)
* Cloud Controls Matrix (CCM) - Endpoint Security Controls.

질문 # 71
Which type of AI workload typically requires large data sets and substantial computing resources?

- A. Training
- B. Inference
- C. Data Preparation
- D. Evaluation

정답：A

설명：
Among AI workloads,Trainingrequires themost computational power and data resources.
Why AI Training is Computationally Intensive?
* Large datasets:
* AI models (e.g., deep learning, neural networks)require millions or billions of labeled data points.
* Training involvesprocessing massive amounts of structured/unstructured data.

* High computational power:
* Training deep learning modelsinvolves runningmultiple passes (epochs) over data, adjusting weights, and optimizing parameters.
* Requiresspecialized hardwarelikeGPUs (Graphics Processing Units),TPUs (Tensor Processing Units), andHPC (High-Performance Computing).
* Long training times:
* AI model training can takedays, weeks, or even monthsdepending on complexity.
* Cloud platforms offerdistributed computing (multi-GPU training, parallel processing, auto- scaling).
* Cloud AI Training Benefits:
* Cloud providers (AWS, Azure, GCP) offer ML training serviceswithon-demand scalable compute instances.
* Supportsframeworks like TensorFlow, PyTorch, and Scikit-learn.
This aligns with:
* CCSK v5 - Security Guidance v4.0, Domain 14 (Related Technologies - AI and ML Security)
* Cloud AI Security Risks and AI Data Governance (CCM - AI Security Controls)

질문 # 72
What is an important step in conducting forensics on containerized and serverless environments?

- A. Isolating network traffic and analyzing network packets frequently
- B. Regularly updating antivirus and anti-malware software
- C. Capturing container logs and snapshots, and leveraging serverless execution logs
- D. Implementing endpoint detection and response (EDR) solutions

정답：C

설명：
The CSA Security Guidance v4.0, Domain 9: Incident Response highlights that traditional forensic techniques don't always apply in cloud-native environments like containers and serverless platforms. Instead, forensic investigators must capture ephemeral data such as logs, snapshots, and execution traces early and often.
"Forensic techniques must adapt to cloud-native environments such as containers and serverless. Important forensic data - including container logs, snapshots, and function execution logs - may be short-lived or non-persistent, so timely collection is critical."
- CSA Security Guidance v4.0, Domain 9: Incident Response
Key points:
Containers and serverless functions are often short-lived.
You need to capture logs and memory state before they're destroyed.
Serverless platforms (like AWS Lambda, Azure Functions) often provide execution logs via services like CloudWatch or Application Insights.
Incorrect options:
A: EDR is typically focused on traditional endpoints, not containers/serverless.
B: Useful in general, but not specific or always applicable to serverless/container forensics.
C: Antivirus doesn't apply well to ephemeral or function-based environments.
Reference:
CSA Security Guidance v4.0 - Domain 9: Incident Response (Container and Serverless Forensics) CCM v3.0.1 - DSI-05, IVS-04 (Covers logging and snapshot control)

질문 # 73
Which of the following from the governance hierarchy provides specific goals to minimize risk and maintain a secure environment?

- A. Implementation guidance
- B. Control objectives
- C. Policies
- D. Control specifications

정답：B

설명：
Control objectives are specific goals or outcomes designed to minimize risk and maintain a secure environment. They are part of a broader governance framework and provide clear, measurable targets that organizations aim to achieve in order to meet security, compliance, and operational goals. Control objectives help guide the implementation of security measures and ensure the organization's security posture aligns with its risk management strategy.

Implementation guidance provides detailed instructions on how to implement controls but does not set specific goals. Policies define the high-level principles and rules that guide behavior and decision-making, but they are more general than control objectives. Control specifications typically define how specific controls are implemented but do not establish the overarching goals that guide risk management.

질문 # 74
Which of the following adds abstraction layer on top of networking hardware and decouples network control plane from the data plane?

- A. VLANs
- B. Virtual Private Networks
- C. Converged Networks
- D. Software Defined Networks

정답：D

설명：
Software Defined Networking(SDN):A more complete abstraction layer on top of networking hardware, SDNs decouple the network control plane from the data. This allows us to abstract networking from the traditional limitations of a LAN.
Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

질문 # 75
.....