300-745완벽한덤프공부자료 & 300-745퍼펙트최신덤프문제

참고: Fast2test에서 Google Drive로 공유하는 무료, 최신 300-745 시험 문제집이 있습니다: https://drive.google.com/open?id=1oweE3ni-LhRLA4UwAHWk6RmkQiLSOfzF

Cisco 300-745 덤프에 대한 자신감이 어디서 시작된것이냐고 물으신다면Cisco 300-745덤프를 구매하여 시험을 패스한 분들의 희소식에서 온다고 답해드리고 싶습니다. 저희Cisco 300-745덤프는 자주 업데이트되고 오래된 문제는 바로 삭제해버리고 최신 문제들을 추가하여 고객님께 가장 정확한 덤프를 제공해드릴수 있도록 하고 있습니다.

Cisco 300-745 시험요강:

주제	소개
주제 1	• Applications: Focuses on selecting security solutions to protect applications and designing secure architectures for cloud-native, containerized, and serverless environments using segmentation. Also addresses security design impacts of emerging technologies like AI, ML, and quantum computing.
주제 2	• Secure Infrastructure: Covers selecting security approaches for endpoints, identities, email, and modern environments like hybrid work, IoT, SaaS, and multi-cloud. Includes choosing VPN • tunneling solutions, securing management planes, and selecting the appropriate firewall architecture based on business needs.

주제 3	• Artificial Intelligence, Automation, and DevSecOps: Explores AI's role in securing network infrastructure, selecting tools for automated security architectures such as SOAR, IaC, and API tooling, and integrating security into DevSecOps workflows and pipelines to minimize deployment risk.
주제 4	• Risk, Events, and Requirements: Covers SOC incident handling and response tools, modifying security designs to mitigate or respond to incidents, and applying frameworks like MITRE CAPEC, NIST SP 800-37, and SAFE. Includes matching regulatory and compliance requirements to business scenarios.

시험패스에 유효한 300-745완벽한 덤프공부자료 인증시험

300-745인증시험패스는 쉬운 일은 아닙니다. 높은 전문지식은 필수입니다.하지만 자신은 이 방면 지식이 없다면 Fast2test가 도움을 드릴 수 있습니다. Fast2test의 전문가들이 자기만의 지식과 지금까지의 경험으로 최고의 IT인증 관련자료를 만들어 여러분들의 고민을 해결해드릴 수 있습니다. 우리는 최고의300-745인증시험문제와 답을 제공합니다. Fast2test는 최선을 다하여 여러분이 한번에300-745인증시험을 패스하도록 도와드릴 것입니다. 여러분은 우리 Fast2test 선택함으로 일석이조의 이익을 누릴 수 있습니다. 첫째는 관여지식은 아주 알차게 공부하실 수 있습니다.둘째는 바로 시험을 안전하게 한번에 통과하실 수 있다는 거죠.그리고 우리는 일년무료 업데이트서비스를 제공합니다.덤프가 업뎃이되면 우리는 모두 무료로 보내드립니다.만약 시험에서 실패한다면 우리 또한 덤프비용전액을 환불해 드립니다.

최신 CCNP Security 300-745 무료샘플문제 (Q67-Q72):

질문 # 67
What is a use for AI in securing network infrastructure?

- A. traffic shaping
- B. load balancing
- C. quality of service
- D. known day zero attack detection

정답：D

설명：
AI enhances network security by detecting zero-day attacks through behavior analysis, anomaly detection, and pattern recognition. This allows threats to be identified and mitigated even before traditional signatures are available.

질문 # 68
A manufacturing company implemented IoT devices throughout their smart factory and needs a security solution that meets these requirements:
* Protect IoT devices from network-based attacks.
* Visibility into communication patterns.
* Anomaly detection for IoT traffic.
Which firewall technology or feature should be recommended?

- A. transparent firewall
- B. IPS/IDS
- C. traditional firewall
- D. zone-based firewall

정답：B

설명：
In a smart factory environment, IoT devices often use specialized industrial protocols (like Modbus, PROFINET, or EtherNet/IP) and have limited built-in security. To meet the requirements of protecting these devices from network-based attacks while gaining visibility into communication patterns and detecting anomalies, anIPS/IDS (Intrusion Prevention/Detection System)is the most effective solution.

Modern Cisco Secure Firewall (NGFW) systems integrate advanced IPS/IDS capabilities that go beyond simple port-based filtering. They provide deep packet inspection (DPI) to identify specific IoT protocols and baseline "normal" behavior. When an IoT device suddenly begins communicating with an unknown external IP or attempts to use a command it has never used before, the IPS/IDS can trigger an alert or block the traffic as an anomaly.
While aZone-Based Firewall(Option A) or aTraditional Firewall(Option C) can segment traffic and control access between zones, they generally lack the granular visibility and behavior-based anomaly detection required for IoT security. ATransparent Firewall(Option B) is a deployment mode that makes the firewall
"invisible" at Layer 2, which is useful for insertion into existing networks but does not inherently provide the required anomaly detection. Therefore, IPS/IDS is the primary technology within the Cisco Security Infrastructure that addresses the need for signature-based protection combined with behavioral visibility for specialized IoT traffic.
═══════

질문 # 69
A manufacturing company recently experienced a network-down scenario due to malware spread on the management network. The company wants to implement a solution to detect and mitigate a similar threat in the future and protect the overall network. Which solution meets the requirements?

- A. IPsec VPN
- B. endpoint detection and response
- C. encrypted threat analysis
- D. RADIUS

정답： B

설명:
Endpoint Detection and Response (EDR) provides continuous monitoring, detection, and automated mitigation of malware at the endpoint level. By stopping threats before they spread across the management network, EDR protects the overall infrastructure from similar network- down scenarios in the future.

질문 # 70
An IT company experienced the spread of malicious content between user endpoints, which impacted business critical resources. The company wants to implement a solution to control communication between individual endpoints on the network. Which approach achieves the goal?

- A. TrustSec
- B. posture
- C. profiling
- D. RADIUS

정답： A

설명:
Cisco TrustSec enables software-defined segmentation by assigning Security Group Tags (SGTs) to endpoints and enforcing communication policies. This allows granular control of traffic between individual endpoints, preventing the spread of malicious content across the network.

질문 # 71
Which design policy addresses harmful content creation by generative AI?

- A. retrieval augmented generation
- B. human in the loop
- C. watermarking
- D. quantum resistant encryption

정답： B

설명:
The creation of harmful content (such as hate speech, misinformation, or malicious code) by generative AI models is a major concern

in modern security design. The most effective design policy to mitigate this is the Human-in-the-loop (HITL)approach. This involves integrating human oversight and intervention at various stages of the AI's operation, particularly during the verification of the model's output before it is published or acted upon.
According to Cisco SDSI objectives regarding AI security, HITL ensures that automated decisions are subject to ethical judgment and contextual awareness that AI currently lacks. Humans can provide "Reinforcement Learning from Human Feedback" (RLHF) to tune the model's safety filters, ensuring it refuses to generate toxic or prohibited content. WhileWatermarking(Option B) helps identify content as AI-generated after the fact, it does not prevent thecreationof harmful material.Retrieval Augmented Generation (RAG)(Option C) is a technique for grounding AI in specific data to reduce "hallucinations" but doesn't inherently filter for harmful intent.Quantum resistant encryption(Option A) is a cryptographic standard unrelated to content moderation. HITL remains the primary safeguard for ensuring AI outputs align with safety guidelines and organizational requirements.

질문 # 72
......