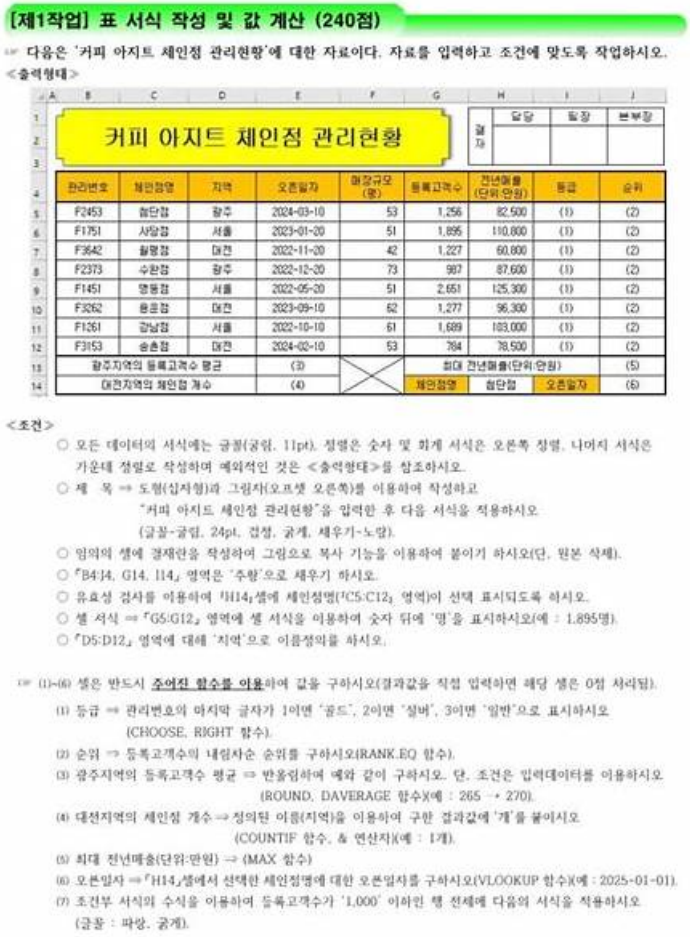
300-745최고품질인증시험기출문제완벽한시험기출문제



[제1작업] 표 서식 작성 및 값 계산 (240점)

☞ 다음은 '커피 아지트 체인점 관리현황'에 대한 자료이다. 자료를 입력하고 조건에 맞도록 작업하시오.

<출력형태>

결재	담당	팀장	본부장

커피 아지트 체인점 관리현황

관리번호	체인점명	지역	오픈일자	매장규모(평)	등록고객수	전년매출(단위:만원)	등급	순위
F2453	화단점	광주	2024-03-10	53	1,256	82,500	(1)	(2)
F1751	사랑점	서울	2023-01-20	51	1,895	110,800	(1)	(2)
F3642	월평점	대전	2022-11-20	42	1,227	60,800	(1)	(2)
F2373	수완점	광주	2022-12-20	73	987	87,600	(1)	(2)
F1451	명동점	서울	2022-05-20	51	2,651	125,300	(1)	(2)
F3262	용호점	대전	2023-09-10	62	1,277	96,300	(1)	(2)
F1261	강남점	서울	2022-10-10	61	1,689	103,000	(1)	(2)
F3153	송촌점	대전	2024-02-10	53	784	78,500	(1)	(2)
광주지역의 등록고객수 평균			(3)		최대 전년매출(단위:만원)			(5)
대전지역의 체인점 개수			(4)		체인점명	화단점	오픈일자	(6)

<조건>

○ 모든 데이터의 서식에는 글꼴(궁림, 11pt), 정렬은 숫자 및 회계 서식은 오른쪽 정렬, 나머지 서식은 가운데 정렬로 작성하며 예외적인 것은 <출력형태>를 참조하시오.

○ 제 목 ⇒ 도형(십자형)과 그림자(오프셋 오른쪽)를 이용하여 작성하고 "커피 아지트 체인점 관리현황"을 입력한 후 다음 서식을 적용하시오.
(글꼴-굴림, 24pt, 겹성, 굵게, 채우기-노랑).

○ 임의의 셀에 결재란을 작성하여 그림으로 복사 기능을 이용하여 붙이기 하시오(단, 원본 삭제).

○ 「B4:J4, G14, I14」 영역은 '주황'으로 채우기 하시오.

○ 유효성 검사를 이용하여 「H14」셀에 체인점명(「C5:C12」 영역)이 선택 표시되도록 하시오.

○ 셀 서식 ⇒ 「G5:G12」 영역에 셀 서식을 이용하여 숫자 뒤에 '명'을 표시하시오(예 : 1,895명).

○ 「D5:D12」 영역에 대해 '지역'으로 이름정의를 하시오.

☞ (1)~(6) 셀은 반드시 주어진 함수를 이용하여 값을 구하시오(결과값을 직접 입력하면 해당 셀은 0점 처리됨).

(1) 등급 ⇒ 관리번호의 마지막 글자가 1이면 '골드', 2이면 '실버', 3이면 '일반'으로 표시하시오.
(CHOOSE, RIGHT 함수).

(2) 순위 ⇒ 등록고객수의 내림차순 순위를 구하시오(RANK.EQ 함수).

(3) 광주지역의 등록고객수 평균 ⇒ 반올림하여 예와 같이 구하시오. 단, 조건은 입력데이터를 이용하시오.
(ROUND, DAVERAGE 함수)(예 : 265 → 270).

(4) 대전지역의 체인점 개수 ⇒ 정의된 이름(지역)을 이용하여 구한 결과값에 '개'를 붙이시오.
(COUNTIF 함수, & 연산자)(예 : 1개).

(5) 최대 전년매출(단위:만원) ⇒ (MAX 함수)

(6) 오픈일자 ⇒「H14」셀에서 선택한 체인점명에 대한 오픈일자를 구하시오(VLOOKUP 함수)(예 : 2025-01-01).

(7) 조건부 서식의 수식을 이용하여 등록고객수가 '1,000' 이하인 행 전체에 다음의 서식을 적용하시오.
(글꼴 : 파랑, 굵게).

Pass4Test 300-745 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=1nodQwQ1Z6mjxdb5nrDaIqTb-VsmzMbW9

우선 우리Pass4Test 사이트에서Cisco 300-745관련자료의 일부 문제와 답 등 샘플을 제공함으로 여러분은 무료로 다운받아 체험해보실 수 있습니다.체험 후 우리의Pass4Test에 신뢰감을 느끼게 됩니다. Pass4Test에서 제공하는Cisco 300-745덤프로 시험 준비하시면 편안하게 시험을 패스하실 수 있습니다.

Pass4Test의 Cisco 300-745덤프는 IT업계에 오랜 시간동안 종사한 전문가들의 끊임없는 노력과 지금까지의 노하우로 만들어낸Cisco 300-745시험대비 알맞춤 자료입니다. Pass4Test의 Cisco 300-745덤프만 공부하시면 여러분은 충분히 안전하게 Cisco 300-745시험을 패스하실 수 있습니다. Pass4Test Cisco 300-745덤프의 도움으로 여러분은 IT업계에서 또 한층 업그레이드 될것입니다

>> 300-745최고품질 인증시험 기출문제 <<

300-745퍼펙트 덤프자료, 300-745완벽한 공부문제

Cisco 300-745 덤프는 Cisco 300-745 시험의 모든 문제를 커버하고 있어 시험적중율이 아주 높습니다. Pass4Test는 Paypal과 몇년간의 파트너 관계를 유지하여 왔으므로 신뢰가 가는 안전한 지불방법을 제공해드립니다. Cisco 300-745시험탈락시 제품비용 전액환불조치로 고객님의 이익을 보장해드립니다.

Cisco 300-745 시험요강:

주제	소개
주제 1	• 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 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	• 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 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.

최신 CCNP Security 300-745 무료샘플문제 (Q68-Q73):

질문 # 68
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. RADIUS
- B. profiling
- C. posture
- D. TrustSec

정답：D

설명:
The spread of malicious content between endpoints is a classic case oflateral movement. To control and restrict communication between individual endpoints-regardless of their physical location or IP address- Cisco TrustSecis the recommended architectural approach. TrustSec moves away from traditional, IP-based Access Control Lists (ACLs), which are difficult to manage and scale, and instead usesScalable Group Tags (SGTs).
With TrustSec, every endpoint is assigned an SGT based on its role or security context (e.g., "Employee," "Contractor," or "HR"). Security policies are then defined in a centralized matrix (the egress policy matrix) that dictates which SGTs can talk to one another. For example, a policy can be set so that endpoints in the "Developer" group cannot communicate directly with endpoints in the "Sales" group, effectively preventing malware from hopping between machines. WhileRADIUS(Option A) is the protocol used for authentication, it does not perform the segmentation itself.Posture(Option C) checks the health of the device, andProfiling (Option D) identifies what the device is, but neither provides the policy-based traffic control of TrustSec. By implementing TrustSec, the company achievesmicro-segmentation, significantly reducing the internal attack surface and containing potential breaches within a single group, which is a core goal of modern secure infrastructure design.

질문 # 69
A developer is building new API functions for a cloud-based application. Before writing the code, the developer wants to ensure that destructive actions, including deleting and updating data, are properly protected by access control identifying sensitive fields such as those that contain passwords or personally identifiable information. Which approach must be used to score the risks proactively?

- A. Open API Specification Analysis
- B. CSPM
- C. SBOM Generation

- D. SAST

정답：A

설명：
In a DevSecOps environment, "shifting left" means identifying risks before a single line of application code is even executed.Open API Specification (OAS) Analysisis a proactive technique where the "contract" of the API (the YAML or JSON file defining its endpoints, methods, and data structures) is audited for security flaws.
By analyzing the OAS, security tools can proactively identify if "destructive" methods-like DELETE or PATCH-lack proper authorization scopes or if sensitive fields (like PII or passwords) are being exposed in responses where they shouldn't be. This allows the developer to "score" the risk based on the API's design before moving into the implementation phase.
WhileSAST (Static Application Security Testing)(Option B) is vital for finding vulnerabilities in written source code, it occursafterthe code is written.SBOM (Software Bill of Materials) Generation(Option C) tracks third-party libraries but doesn't analyze API logic.CSPM (Cloud Security Posture Management) (Option D) focuses on the misconfiguration of the cloud infrastructure (like open S3 buckets) rather than the internal logic of the API itself. OAS Analysis specifically addresses the developer's need to validate access controls and sensitive data handling during the design and definition stage of API development.

질문 # 70
A technology company has many remote workers who access corporate resources from various locations. The company must ensure that security policies are managed and enforced directly on endpoints, and endpoints are protected from threats regardless of location. Which firewall architecture meets the requirements?

- A. next-generation firewall
- B. traditional firewall
- C. web application firewall
- D. host-based firewall

정답：D

설명：
A host-based firewall enforces security policies directly on endpoints, ensuring they remain protected regardless of location. This architecture provides consistent defense for remote workers accessing corporate resources from outside the traditional network perimeter.

질문 # 71
A legal services company wants to prevent remote employees from accessing personal email and social media accounts while using corporate laptops. Which security solution enforces the policy?

- A. Cisco Umbrella
- B. Cisco TrustSec
- C. RADIUS server
- D. network monitoring tool

정답：A

설명：
In the modern landscape of remote work, a legal services company must enforce acceptable use policies (AUP) regardless of where a corporate laptop is located.Cisco Umbrellais the ideal architectural solution for this requirement. Umbrella acts as a Secure Internet Gateway (SIG) that operates primarily at the DNS and web layer. When a remote employee attempts to access a personal email site or a social media platform, Umbrella intercepts the DNS request and checks it against the organization's defined security policy.
Cisco Umbrella provides granularContent Filteringcapabilities, allowing administrators to block entire categories of websites, such as "Social Networking" or "Webmail," with a single click. This enforcement happens at the edge-before a connection is even established to the malicious or unauthorized site-making it highly efficient for remote users who may not be connected to the corporate VPN. WhileCisco TrustSec (Option A) andRADIUS(Option B) are powerful for internal network segmentation and authentication, they do not inherently provide the URL/domain-based categorization required to block specific web content for remote clients. Anetwork monitoring tool(Option D) provides visibility but lacks the active enforcement mechanism to block traffic. Therefore, Cisco Umbrella is the specified technology in the SDSI objectives for cloud-delivered web security and policy enforcement for a distributed workforce.

==========

질문 # 72
An agricultural company wants to enhance the cybersecurity posture by implementing a defense- in-depth strategy to protect against polymorphic malware threats. Currently, the company's security infrastructure relies solely on a stateful traditional edge firewall that does not provide adequate protection against malware variants. Which technology must be added to the company's security architecture to achieve the goal?

- A. heuristics-based IPS
- B. network performance monitor
- C. web application firewall
- D. physical security control

정답：A

설명:
A heuristics-based Intrusion Prevention System (IPS) analyzes traffic behavior and patterns, allowing it to detect and block polymorphic malware that constantly changes its signature to evade traditional defenses. Adding this technology strengthens the company's defense-in-depth strategy beyond the limitations of a stateful firewall.

질문 # 73
.....