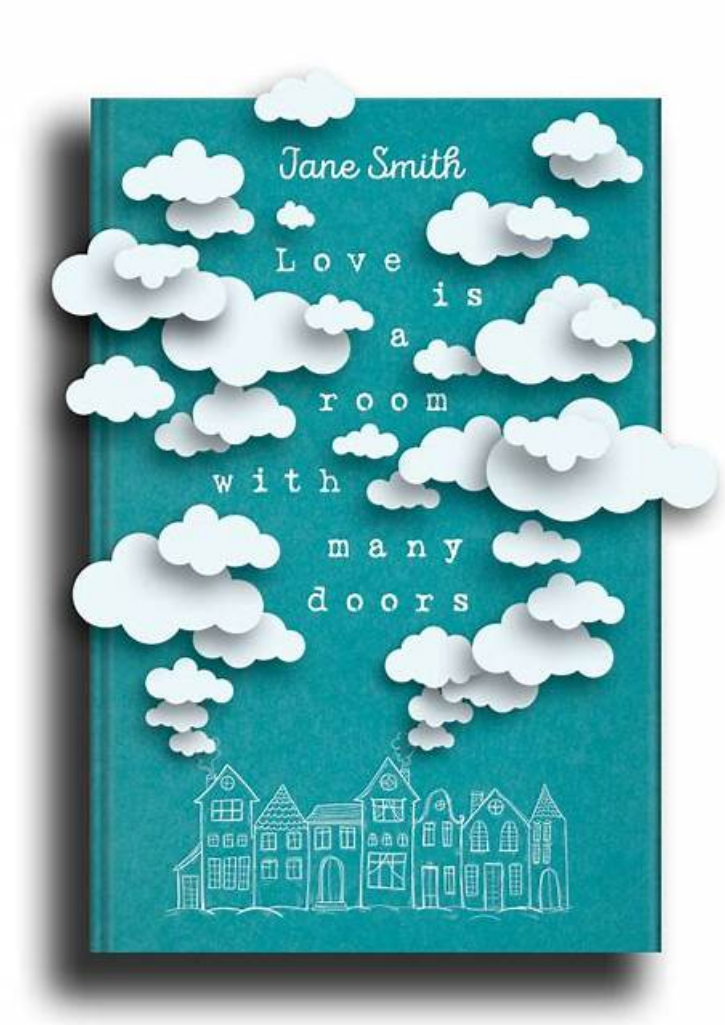
높은통과율300-220시험대비최신덤프덤프샘플문제



그리고 Itexamdump 300-220 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1kTqDr6QYK5X_-UJBVUpTlMvzM6VPBhpt

Itexamdump 의 Cisco인증 300-220덤프는Cisco인증 300-220시험에 도전장을 던진 분들이 신뢰할수 있는 든든한 길잡이 입니다. Cisco인증 300-220시험대비 덤프뿐만아니라 다른 IT인증시험에 대비한 덤프자료도 적중율이 끝내줍니다. Cisco인증 300-220시험이나 다른 IT인증자격증시험이나Itexamdump제품을 사용해보세요.투자한 덤프비용보다 훨씬 큰 이득을 보실수 있을것입니다.

Cisco 300-220 시험은 사이버 보안 분야에서 진출하고자하는 전문가들에게 필수적인 자격증 시험입니다. 이 시험은 CyberOps에 대한 Cisco 기술을 사용하여 위협 수색 및 방어 능력을 평가하는 것을 목적으로합니다. 이 시험은 네트워크 보안, 엔드 포인트 보호, 사고 대응 및 위협 인텔리전스를 포함한 다양한 주제를 다룹니다.

이 시험은 보안 기술, 위협 분석, 사고 대응, 네트워크 보안 및 엔드포인트 보안을 포함한 다양한 주제를 다룹니다. 후보자는 Cisco Stealthwatch, Cisco Umbrella, Cisco Firepower 및 Cisco Identity Services Engine (ISE)와 같은 Cisco 기술을 사용하여 사이버 보안 위협을 식별하고 대응하는 방법을 배우게 됩니다. 이 자격증 프로그램은 네트워크 보안의 최상의 권장 사항, 네트워크 분할, 접근 제어 및 안전한 통신 프로토콜도 다룹니다.

Cisco 300-220 시험은 Cisco Technologies를 사용하여 위협 사냥 및 네트워크 방어에 대한 지식과 기술을 향상시키려는 사이버 보안 전문가에게 이상적입니다. 이 시험은 또한 사이버 보안 및 네트워크 보안에 대한 전문 지식을 검증하려는 개인에게도 적합합니다. 시험에 합격 한 결과 후보자는 Cisco Technologies를 사용한 최신 위협 사냥 및 완화 기술에 대한 포괄적 인 이해를 가지고 있으며 사이버 공격을 효과적으로 방어 할 수 있음을 보여줍니다. 전반적으로 Cisco 300-220 시험은 사이버 보안 전문가가 경력을 발전시키고 현장에서의 전문 지식을 보여주는 훌륭한 방법입니다.

300-220시험대비 최신 덤프 100% 시험패스 덤프

Cisco인증300-220시험을 패스함으로 취업에는 많은 도움이 됩니다. Itexamdump는Cisco인증300-220시험패스로 꿈을 이루어주는 사이트입니다. 우리는Cisco인증300-220시험의 문제와 답은 아주 좋은 학습자료로도 충분한 문제집입니다. 여러분이 안전하게 간단하게Cisco인증300-220시험을 응시할 수 있는 자료입니다.

최신 CyberOps Associate 300-220 무료샘플문제 (Q14-Q19):

질문 # 14
In the Investigation and Validation phase of the Threat Hunting Process, what is done to confirm or refute the formed hypotheses?

- A. More data collection
- B. Detailed analysis
- C. Testing against known attacks
- D. Collaboration with external teams

정답：C

질문 # 15
Which of the following threat hunting techniques involves analyzing historical incident data and indicators of compromise?

- A. YARA rules
- B. Threat intelligence feeds
- C. Data correlation
- D. Threat modeling

정답：C

질문 # 16
What is the importance of threat intelligence in threat hunting?

- A. Threat intelligence allows threat hunters to anticipate and detect threats before they manifest.
- B. Threat intelligence is not necessary for effective threat hunting.
- C. Threat intelligence is only relevant for external threats, not internal threats.
- D. Threat intelligence provides real-time alerts to potential threats.

정답：A

질문 # 17
A mature SOC notices that several incidents over the past year involved attackers abusing legitimate administrative tools rather than deploying custom malware. Leadership asks the threat hunting team to improve detection coverage in a way that increases attacker cost rather than relying on easily replaceable indicators. Which detection strategy best aligns with this objective?

- A. Blocking known malicious file hashes at the endpoint
- B. Ingesting additional commercial threat intelligence feeds
- C. Creating alerts for newly registered domains
- D. Correlating attacker behavior across multiple MITRE ATT&CK techniques

정답：D

설명：
The correct answer iscorrelating attacker behavior across multiple MITRE ATT&CK techniques. This approach focuses onbehavioral detection, which is the cornerstone of effective threat hunting and advanced security operations.
Attackers who abuse legitimate administrative tools-often referred to asliving-off-the-land techniques- intentionally avoid malware-

based detections. File hashes, signatures, and known indicators provide minimal value because there may beno malicious files at all. Options A and D sit at the lowest levels of thePyramid of Pain, making them easy for adversaries to evade.
By correlating behavior across multiple ATT&CK techniques-such as credential access, lateral movement, privilege escalation, and command execution-defenders detecthowthe attacker operates rather thanwhat toolsthey use. This forces adversaries to fundamentally change tradecraft, which is costly, risky, and time- consuming.
Option C improves visibility but does not inherently raise attacker cost. Threat intelligence feeds are reactive and often lag behind active campaigns.
From a professional threat hunting perspective, correlating multiple low-signal behaviors into ahigh- confidence attack patternis how mature SOCs detect stealthy intrusions. This method also supports scalable detection engineering, improved alert fidelity, and reduced false positives.
This strategy directly aligns with higher tiers of theThreat Hunting Maturity Modeland the top of the Pyramid of Pain, making optionBthe correct answer.

질문 # 18
During the investigation phase of the threat hunting process, what activity is typically conducted?

- A. Refining hypotheses
- B. Mitigating the threat
- C. Collecting additional data
- D. Generating threat intelligence reports

정답：C

질문 # 19
.....

그 외, Itexamdump 300-220 시험 문제집 일부가 지금은 무료입니다: https://drive.google.com/open?id=1kTqDr6QYK5X_-UJBVUpTlMvzM6VPBhpt