312-85높은통과율시험자료 - 312-85시험대비최신공부자료

EMC DEP-3CR1 PowerProtect Cyber Recovery Exam 3

질문 # 26
An enterprise customer needs a Cyber Recovery solution to be implemented. As an outcome from a previous workshop, the following backup environment needs to be protected to the CR Vault.
Location 1: 4 PowerProtect DDs
Location 2: 4 PowerProtect DDs
Location 3: 2 PowerProtect DDs
Location 4: 2 PowerProtect DDs
The customer wants to implement a CR Vault in a 5th location.
How many Cyber Recovery systems must be installed at a minimum level?

- A. 0
- B. 1
- C. 2
- D. 3

정답□B

질문 # 27
What vault status is displayed if none of the PowerProtect DD systems in the CR Vault are able to communicate with the Cyber Recovery software?

- A. Unknown
- B. Unlocked
- C. Locked
- D. Degraded

정답□B

질문 # 28
.....

DEP-3CR1높은 통과율 시험대비 덤프공부:
https://www.koreadumps.com/DEP-3CR1_exam-braindumps.html

- DEP-3CR1시험문제집 □ DEP-3CR1시험대비 덤프데모 다운 □ DEP-3CR1시험덤프 □ 무료 다운로드를 위해 지금 www.itdumpskr.com 에서 □ DEP-3CR1 □검색DEP-3CR1높은 통과율 인기 덤프문제
- DEP-3CR1최신버전 덤프공부 □ DEP-3CR1높은 통과율 인기 덤프문제 □ DEP-3CR1시험대비 덤프데모문제 □ 지금□ www.itdumpskr.com □에서▶ DEP-3CR1 ◀를 검색하고 무료로 다운로드하세요DEP-3CR1높은 통과율 인기 덤프문제
- DEP-3CR1덤프문제 □ DEP-3CR1시험패스 가능 덤프 □ DEP-3CR1시험대비 공부하기 □ 검색만 하면□ www.itdumpskr.com □에서 ★ DEP-3CR1 ★무료 다운로드DEP-3CR1최신기출자료
- 최신버전 DEP-3CR1시험대비 덤프 최신자료 덤프문제 □ 검색만 하면□ www.itdumpskr.com □에서▷ DEP-3CR1 ◁무료 다운로드DEP-3CR1시험패스 가능한 인증공부자료
- DEP-3CR1최신버전 덤프공부 □ DEP-3CR1합격보장 가능 덤프공부 □ DEP-3CR1시험대비 덤프데모 다운 □ 지금□ www.itdumpskr.com □을(를) 열고 무료 다운로드를 위해▶ DEP-3CR1 ◀를 검색하십시오DEP-3CR1시험패스 가능 덤프
- DEP-3CR1최신버전 덤프공부 □ DEP-3CR1시험대비 공부하기 □ DEP-3CR1덤프문제 □|

DEP-3CR1시험대비덤프최신자료 & DEP-3CR1높은통과율시험대비덤프공부

BONUS!!! ExamPassdump 312-85 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=13EWU_83yhJ5Wpa0fASBvbGU7dUUdRrF0

ExamPassdump의 ECCouncil인증 312-85덤프는 거의 모든 실제시험문제 범위를 커버하고 있습니다.ECCouncil인증 312-85시험덤프를 구매하여 덤프문제로 시험에서 불합격성적표를 받을시ExamPassdump에서는 덤프비용 전액 환불을 약속드립니다.

ECCouncil 312-85 (인증된 위협 인텔리전스 분석가) 자격증 시험은 위협 인텔리전스 분석 분야에서 전문성을 증명하고자 하는 사람들에게 인기 있는 자격증입니다. 이 자격증 시험은 IT 전문가, 보안 분석가, 그리고 위협 인텔리전스 전문가들이 사이버 위협을 식별하고 완화하는 기술과 지식을 향상시키고자 하는 사람들을 대상으로 디자인되었습니다.

>> 312-85높은 통과율 시험자료 <<

312-85시험대비 최신 공부자료 & 312-85덤프공부자료

ECCouncil인증 312-85시험은 멋진 IT전문가로 거듭나는 길에서 반드시 넘어야할 높은 산입니다. ECCouncil인증 312-85시험문제패스가 어렵다한들ExamPassdump덤프만 있으면 패스도 간단한 일로 변경됩니다. ExamPassdump의 ECCouncil인증 312-85덤프는 100%시험패스율을 보장합니다. ECCouncil인증 312-85시험문제가 업데이트되면

ECCouncil인증 312-85덤프도 바로 업데이트하여 무료 업데이트서비스를 제공해드리기에 덤프유효기간을 연장해는것으로 됩니다.

CTIA 인증 시험은 후보자가 다양한 위협 지능 영역에서 지식과 기술을 보여 주어야하는 엄격하고 어려운 시험입니다. 시험은 100 개의 객관식 질문으로 구성되며 4 시간 내에 완료해야합니다. 시험에 합격하려면 후보자는 최소 점수 70%를 달성해야합니다.

최신 Certified Threat Intelligence Analyst 312-85 무료샘플문제 (Q78-Q83):

질문 # 78
A consortium was established in a collaborative effort to strengthen the cybersecurity posture of multiple organizations within an industry sector. The participating entities decided to adopt a threat intelligence exchange architecture in which all threat data is collected, analyzed, and disseminated through a single central hub.
What type of threat intelligence exchange architecture was implemented in this scenario?

- A. Decentralized exchange architecture
- B. Centralized exchange architecture
- C. Federated exchange architecture
- D. Hybrid exchange architecture

정답：B

설명：
A model where all threat data is collected, analyzed, and distributed through a single central hub defines a Centralized Exchange Architecture.
In this architecture:
* All participants send their data to a central system.
* The central hub processes, correlates, and redistributes intelligence.
* It ensures uniform analysis, consistency, and efficient management.
Why the Other Options Are Incorrect:
* A. Decentralized: Each participant shares data directly with others without a central hub.
* B. Federated: Each organization maintains its own data but participates in shared analysis through agreed protocols.
* C. Hybrid: Combines elements of centralized and decentralized systems for flexibility.
Conclusion:
The described setup represents a Centralized Exchange Architecture.
Final Answer: D. Centralized exchange architecture
Explanation Reference (Based on CTIA Study Concepts):
CTIA classifies centralized architectures as systems that collect and distribute threat data through a single authoritative node.

질문 # 79
While analyzing a series of security incidents, you notice a pattern of attacks originating from specific geographical locations. To gain deeper insight into the spatial aspects of these threats, what contextualization method would you employ to understand the geographic origin and distribution of the attacks?

- A. Policy context
- B. Temporal context
- C. Spatial context
- D. Historical context

정답：C

설명：
Spatial context refers to analyzing the geographical and location-based factors of threat intelligence. When attacks are observed from specific regions or IP addresses associated with certain areas, spatial context helps identify where the attacks originate and how geographical distribution influences threat behavior.
Spatial analysis allows a threat analyst to:
* Identify regions that frequently serve as sources of malicious activity.
* Correlate attacks with geopolitical or regional factors.
* Assess the proximity and connectivity between threat sources and targets.
Why the Other Options Are Incorrect:

* Policy context: Focuses on organizational policies and regulatory frameworks.
* Historical context: Involves studying past data to understand patterns or trends over time.
* Temporal context: Relates to the timing and frequency of attacks, not location.
Conclusion:
To analyze attack patterns based on geography, the analyst must use Spatial Context.
Final Answer: D. Spatial context
Explanation Reference (Based on CTIA Study Concepts):
CTIA's "Contextualization of Threat Intelligence Data" section defines spatial context as understanding threat data based on geographical attributes and origin distribution.

질문 # 80
Jian is a member of the security team at Trinity, Inc. He was conducting a real-time assessment of system activities in order to acquire threat intelligence feeds. He acquired feeds from sources like honeynets, P2P monitoring. infrastructure, and application logs.
Which of the following categories of threat intelligence feed was acquired by Jian?

- A. Proactive surveillance feeds
- B. CSV data feeds
- C. Internal intelligence feeds
- D. External intelligence feeds

정답：C

설명:
Internal intelligence feeds are derived from data and information collected within an organization's own networks and systems. Jian's activities, such as real-time assessment of system activities and acquiring feeds from honeynets, P2P monitoring, infrastructure, and application logs, fall under the collection of internal intelligence feeds. These feeds are crucial for identifying potential threats and vulnerabilities within the organization and form a fundamental part of a comprehensive threat intelligence program. They contrast with external intelligence feeds, which are sourced from outside the organization and include information on broader cyber threats, trends, and TTPs of threat actors.
References:
"Building an Intelligence-Led Security Program" by Allan Liska
"Threat Intelligence: Collecting, Analysing, Evaluating" by M-K. Lee, L. Healey, and P. A. Porras

질문 # 81
Alice, an analyst, shared information with security operation managers and network operations center (NOC) staff for protecting the organizational resources against various threats. Information shared by Alice was highly technical and include threat actor TTPs, malware campaigns, tools used by threat actors, and so on.
Which of the following types of threat intelligence was shared by Alice?

- A. Tactical threat intelligence
- B. Strategic threat intelligence
- C. Operational threat intelligence
- D. Technical threat intelligence

정답：A

설명:
The information shared by Alice, which was highly technical and included details such as threat actor tactics, techniques, and procedures (TTPs), malware campaigns, and tools used by threat actors, aligns with the definition of tactical threat intelligence. This type of intelligence focuses on the immediate, technical indicators of threats and is used bysecurity operation managers and network operations center (NOC) staff to protect organizational resources. Tactical threat intelligence is crucial for configuring security solutions and adjusting defense mechanisms to counteract known threats effectively.References:
* "Tactical Cyber Intelligence," Cyber Threat Intelligence Network, Inc.
* "Cyber Threat Intelligence for Front Line Defenders: A Practical Guide," by James Dietle

질문 # 82
A threat analyst wants to incorporate a requirement in the threat knowledge repository that provides an ability to modify or delete

past or irrelevant threat data.
Which of the following requirement must he include in the threat knowledge repository to fulfil his needs?

- A. Evaluating performance
- B. Searchable functionality
- C. Protection ranking
- D. Data management

정답：D

설명：
Incorporating a data management requirement in the threat knowledge repository is essential to provide the ability to modify or delete past or irrelevant threat data. Effective data management practices ensure that the repository remains accurate, relevant, and up-to-date by allowing for the adjustment and curation of stored information. This includes removing outdated intelligence, correcting inaccuracies, and updating information as new insights become available. A well-managed repository supports the ongoing relevance and utility of the threat intelligence, aiding in informed decision-making and threat mitigation strategies.References:
* "Building and Maintaining a Threat Intelligence Library," by Recorded Future
* "Best Practices for Creating a Threat Intelligence Policy, and How to Use It," by SANS Institute

질문 # 83
.....