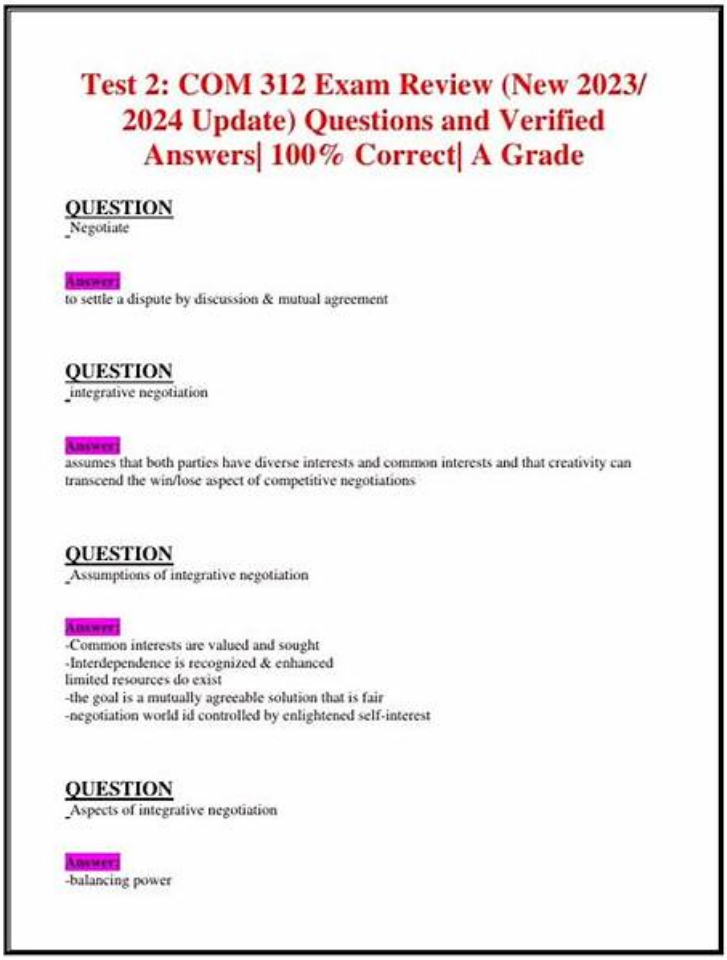
Standard 312-85 Answers & 312-85 Training Online



Test 2: COM 312 Exam Review (New 2023/ 2024 Update) Questions and Verified Answers| 100% Correct| A Grade

QUESTION
_Negotiate

Answer:
to settle a dispute by discussion & mutual agreement

QUESTION
_integrative negotiation

Answer:
assumes that both parties have diverse interests and common interests and that creativity can transcend the win/lose aspect of competitive negotiations

QUESTION
_Assumptions of integrative negotiation

Answer:
-Common interests are valued and sought
-Interdependence is recognized & enhanced
limited resources do exist
-the goal is a mutually agreeable solution that is fair
-negotiation world id controlled by enlightened self-interest

QUESTION
_Aspects of integrative negotiation

Answer:
-balancing power

What's more, part of that ActualVCE 312-85 dumps now are free: https://drive.google.com/open?id=1ftJTCpxKjBCeLJjcNBmX_xCd0usjTwlR

Now you do not need to worry about the relevancy and top standard of ActualVCE Certified Threat Intelligence Analyst (312-85) exam questions. These ECCouncil 312-85 dumps are designed and verified by qualified Certified Threat Intelligence Analyst (312-85) exam trainers. Now you can trust ActualVCE Certified Threat Intelligence Analyst (312-85) practice questions and start preparation without wasting further time.

The Certified Threat Intelligence Analyst (CTIA) is a certification exam offered by the EC-Council. The CTIA certification is a professional-level certification that is designed to validate the skills and knowledge of individuals who work in the field of threat intelligence analysis. The CTIA exam is designed to test the candidate's ability to collect, analyze, and disseminate threat intelligence data from various sources.

>> Standard 312-85 Answers <<

312-85 Training Online | Reliable 312-85 Mock Test

Contemporarily, social competitions stimulate development of modern science, technology and business, which revolutionizes our society's recognition to 312-85 exam and affect the quality of people's life. According to a recent report, those who own more than one skill certificate are easier to be promoted by their boss. To be out of the ordinary and seek an ideal life, we must master an extra skill to get high scores and win the match in the workplace. Our 312-85 Exam Question can help make your dream come true.

What's more, you can have a visit of our website that provides you more detailed information about the 312-85 guide torrent.

ECCouncil Certified Threat Intelligence Analyst Sample Questions (Q36-Q41):

NEW QUESTION # 36
Philip, a professional hacker, is planning to attack an organization. In order to collect information, he covertly collects information from the target person by maintaining a personal or other relationship with the target person.
Which of the following intelligence sources is used by Philip to collect information about the target organization?

- A. FISINT
- B. CHIS
- C. SOCMINT
- D. MASINT

Answer: B

Explanation:
The scenario describes a situation where Philip gathers intelligence through direct personal relationships or covert human contact with the target individual. This aligns with the intelligence source known as CHIS (Covert Human Intelligence Source).
CHIS refers to intelligence collected from a human source who provides information about individuals, groups, or organizations, often through personal relationships or covert interaction. This type of intelligence is gathered directly from people rather than technical or electronic means.
In the context of threat intelligence and security analysis, CHIS is part of Human Intelligence (HUMINT), which involves acquiring information through human interaction. Such sources can include insiders, informants, or individuals with access to sensitive details about the target organization.
Attackers or intelligence professionals use this method to gather sensitive or non-public information that cannot be obtained from open or technical sources. Philip's method of maintaining a personal relationship with the target person to collect information fits perfectly into this category.
Why the Other Options Are Incorrect:
* B. MASINT (Measurement and Signature Intelligence):This intelligence source collects and analyzes data obtained from sensors, measuring electromagnetic, acoustic, or nuclear signatures. It is a technical intelligence method and does not involve human relationships.
* C. SOCMINT (Social Media Intelligence):SOCMINT involves collecting intelligence from social media platforms such as Facebook, LinkedIn, Twitter, or Instagram. It uses publicly available data rather than personal interaction.
* D. FISINT (Foreign Instrumentation Signals Intelligence):This refers to intelligence derived from intercepted foreign instrument signals, such as telemetry or weapon system emissions. It is related to technical and signals intelligence, not human sources.
Conclusion:
Philip used a Covert Human Intelligence Source (CHIS) approach, which involves collecting intelligence through human interaction or relationships to gain insider knowledge about the target organization.
Final Answer: A. CHIS
Explanation Reference (Based on CTIA Study Concepts):
Based on the CTIA study guide section on "Sources of Threat Intelligence," CHIS is recognized as a human intelligence source derived from interpersonal contact, covert sources, or informants that provide insider-level information about an organization or target individual.

NEW QUESTION # 37
Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.
Which of the following key indicators of compromise does this scenario present?

- A. Unusual outbound network traffic
- B. Unusual activity through privileged user account
- C. Unexpected patching of systems
- D. Geographical anomalies

Answer: D

NEW QUESTION # 38
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. Operational threat intelligence
- C. Technical threat intelligence
- D. Strategic threat intelligence

Answer: A

Explanation:
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

NEW QUESTION # 39
Alice, a threat intelligence analyst at HiTech Cyber Solutions, wants to gather information for identifying emerging threats to the organization and implement essential techniques to prevent their systems and networks from such attacks. Alice is searching for online sources to obtain information such as the method used to launch an attack, and techniques and tools used to perform an attack and the procedures followed for covering the tracks after an attack.
Which of the following online sources should Alice use to gather such information?

- A. Hacking forums
- B. Job sites
- C. Financial services
- D. Social network settings

Answer: A

Explanation:
Alice, looking to gather information on emerging threats including attack methods, tools, and post-attack techniques, should turn to hacking forums. These online platforms are frequented by cybercriminals and security researchers alike, where information on the latest exploits, malware, and hacking techniques is shared and discussed. Hacking forums can provide real-time insights into the tactics, techniques, and procedures (TTPs) used by threat actors, offering a valuable resource for threat intelligence analysts aiming to enhance their organization's defenses.References:
* "Hacking Forums: A Ground for Cyber Threat Intelligence," by Digital Shadows
* "The Value of Hacking Forums for Threat Intelligence," by Flashpoint

NEW QUESTION # 40
Marry wants to follow an iterative and incremental approach to prioritize requirements in order to protect the important assets of an organization against attacks. She wants to set the requirements based on the order of priority, where the most important requirement must be met first for a greater chance of success. She wants to apply prioritization tasks, scenarios, use cases, tests, and so on.
Which of the following methodologies should Marry use to prioritize the requirements?

- A. Fusion analysis
- B. MoSCoW
- C. Data sampling
- D. Data visualization

Answer: B

Explanation:
The methodology described-iterative and incremental prioritization of requirements based on importance-perfectly aligns with the MoSCoW method.
MoSCoW stands for:
* M - Must have (critical requirements that are mandatory),
* S - Should have (important but not essential),
* C - Could have (desirable but optional),
* W - Won't have (this time) (deferred or out of scope).
It is widely used in security, risk management, and software development to determine the priority of tasks or requirements that should be implemented first.
By applying MoSCoW, Marry ensures that critical security requirements (such as protecting core assets) are addressed first before moving on to less critical ones.
Why the Other Options Are Incorrect:
* A. Data sampling: Refers to statistical analysis methods, not prioritization.
* C. Data visualization: Used to represent data graphically, not for setting priorities.
* D. Fusion analysis: Used to integrate multiple data sources for intelligence analysis, not requirement prioritization.
Conclusion:
Marry should use the MoSCoW prioritization methodology to structure and prioritize her organization's security requirements.
Final Answer: B. MoSCoW
Explanation Reference (Based on CTIA Study Concepts):
In CTIA's requirement prioritization and planning stages, MoSCoW is used to assign importance levels to intelligence and security requirements for efficient implementation.

NEW QUESTION # 41
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2025 ECCouncil 312-85 dumps are available on Google Drive shared by ActualVCE: https://drive.google.com/open?id=1ftJTCpxKjBCeLJjcNBmX_xCd0usjTwlR