Number: 312-85
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 312-85

Exam Name: Certified Threat Intelligence Analyst

Exam A

QUESTION 1
Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

A. Risk tolerance
B. Timeliness
C. Attack origination points
D. Multiphased

Correct Answer: D
Section:
Explanation:
Advanced Persistent Threats (APTs) are characterized by their 'Multiphased' nature, referring to the various stages or phases the attacker undertakes to breach a network, remain undetected, and achieve their objectives. This characteristic includes numerous attempts to gain entry to the target's network, often starting with reconnaissance, followed by initial compromise, and progressing through stages such as establishment of a backdoor, expansion, data exfiltration, and maintaining persistence. This multiphased approach allows attackers to adapt and pursue their objectives despite potential disruptions or initial failures in their campaign.
Reference:
'Understanding Advanced Persistent Threats and Complex Malware,' by FireEye
MITRE ATT&CK Framework, detailing the multiphased nature of adversary tactics and techniques

QUESTION 2
Lizzy, an analyst, wants to recognize the level of risks to the organization so as to plan countermeasures against cyber attacks. She used a threat modelling methodology where she performed the following stages:
Stage 1: Build asset-based threat profiles
Stage 2: Identify infrastructure vulnerabilities
Stage 3: Develop security strategy and plans
Which of the following threat modelling methodologies was used by Lizzy in the aforementioned scenario?

A. TRIKE
B. VAST
C. OCTAVE
D. DREAD

Correct Answer: C
Section:
Explanation:
The threat modeling methodology employed by Lizzy, which involves building asset-based threat profiles, identifying infrastructure vulnerabilities, and developing security strategies and plans, aligns with the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology. OCTAVE focuses on organizational risk and security practices, emphasizing self-directed risk assessments to identify and prioritize threats to organizational assets and develop appropriate security strategies and plans. This methodology is asset-driven and revolves around understanding critical assets, identifying threats to those assets, and assessing vulnerabilities, leading to the development of a comprehensive security strategy.
Reference:
The CERT Guide to System and Network Security Practices by Julia H. Allen
'OCTAVE Method Implementation Guide Version 2.0,' Carnegie Mellon University, Software Engineering Institute

QUESTION 3
Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.

What stage of the cyber-threat intelligence is Michael currently in?

A. Unknown unknowns
B. Unknowns unknown
C. Known unknowns
D. Known knowns

Correct Answer: C
Section:
Explanation:
The 'known unknowns' stage in cyber-threat intelligence refers to the phase where an analyst has identified threats but the specific details, implications, or full nature of these threats are not yet fully understood. Michael, in this scenario, has obtained information on threats and is in the process of analyzing this information to understand the nature of the threats better. This stage involves analyzing the known data to uncover additional insights and fill in the gaps in understanding, thereby transitioning the 'unknowns' into 'knowns.' This phase is critical in threat intelligence as it helps in developing actionable intelligence by deepening the understanding of the threats faced.
Reference:
'Intelligence Analysis: A Target-Centric Approach,' by Robert M. Clark
'Structured Analytic Techniques for Intelligence Analysis,' by Richards J. Heuer Jr. and Randolph H. Pherson

QUESTION 4
Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.
Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?

A. Data collection through passive DNS monitoring
B. Data collection through DNS interrogation
C. Data collection through DNS zone transfer
D. Data collection through dynamic DNS (DDNS)

Correct Answer: A
Section:
Explanation:
Passive DNS monitoring involves collecting data about DNS queries and responses without actively querying DNS servers, thereby not altering or interfering with DNS traffic. This technique allows analysts to track changes in DNS records and observe patterns that may indicate malicious activity. In the scenario described, Enrique is employing passive DNS monitoring by using a recursive DNS server to log the responses received from name servers, storing these logs in a central database for analysis. This approach is effective for identifying malicious domains, mapping malware campaigns, and understanding threat actors' infrastructure without alerting them to the fact that they are being monitored. This method is distinct from active techniques such as DNS interrogation or zone transfers, which involve sending queries to DNS servers, and dynamic DNS, which refers to the automatic updating of DNS records.
Reference:
SANS Institute InfoSec Reading Room, 'Using Passive DNS to Enhance Cyber Threat Intelligence'
'Passive DNS Replication,' by Florian Weimer, FIRST Conference Presentation

QUESTION 5
John, a professional hacker, is trying to perform APT attack on the target organization network. He gains access to a single system of a target organization and tries to obtain administrative login credentials to gain further access to the systems in the network using various techniques.
What phase of the advanced persistent threat lifecycle is John currently in?

A. Initial intrusion
B. Search and exfiltration

C. Expansion
D. Persistence

Correct Answer: C
Section:
Explanation:
The phase described where John, after gaining initial access, is attempting to obtain administrative credentials to further access systems within the network, is known as the 'Expansion' phase of an Advanced Persistent Threat (APT) lifecycle. This phase involves the attacker expanding their foothold within the target's environment, often by escalating privileges, compromising additional systems, and moving laterally through the network. The goal is to increase control over the network and maintain persistence for ongoing access. This phase follows the initial intrusion and sets the stage for establishing long-term presence and eventual data exfiltration or other malicious objectives.
Reference:
MITRE ATT&CK Framework, specifically the tactics related to Credential Access and Lateral Movement
'APT Lifecycle: Detecting the Undetected,' a whitepaper by CyberArk

QUESTION 6
Jim works as a security analyst in a large multinational company. Recently, a group of hackers penetrated into their organizational network and used a data staging technique to collect sensitive data. They collected all sorts of sensitive data about the employees and customers, business tactics of the organization, financial information, network infrastructure information and so on.
What should Jim do to detect the data staging before the hackers exfiltrate from the network?

A. Jim should identify the attack at an initial stage by checking the content of the user agent field.
B. Jim should analyze malicious DNS requests, DNS payload, unspecified domains, and destination of DNS requests.
C. Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs.
D. Jim should identify the web shell running in the network by analyzing server access, error logs, suspicious strings indicating encoding, user agent strings, and so on.

Correct Answer: C
Section:
Explanation:
In the scenario described, where attackers have penetrated the network and are staging data for exfiltration, Jim should focus on monitoring network traffic for signs of malicious file transfers, implement file integrity monitoring, and scrutinize event logs. This approach is crucial for detecting unusual activity that could indicate data staging, such as large volumes of data being moved to uncommon locations, sudden changes in file integrity, or suspicious entries in event logs. Early detection of these indicators can help in identifying the staging activity before the data is exfiltrated from the network.
Reference:
NIST Special Publication 800-61 Rev. 2, 'Computer Security Incident Handling Guide'
SANS Institute Reading Room, 'Detecting Malicious Activity with DNS and NetFlow'

QUESTION 7
Andrews and Sons Corp. has decided to share threat information among sharing partners. Garry, a threat analyst, working in Andrews and Sons Corp., has asked to follow a trust model necessary to establish trust between sharing partners. In the trust model used by him, the first organization makes use of a body of evidence in a second organization, and the level of trust between two organizations depends on the degree and quality of evidence provided by the first organization.
Which of the following types of trust model is used by Garry to establish the trust?

A. Mediated trust
B. Mandated trust
C. Direct historical trust
D. Validated trust

Correct Answer: D
Section:
Explanation:

In the trust model described, where trust between two organizations depends on the degree and quality of evidence provided by the first organization, the model in use is 'Validated Trust.' This model relies on the validation of evidence or credentials presented by one party to another to establish trust. The validation process assesses the credibility, reliability, and relevance of the information shared, forming the basis of the trust relationship between the sharing partners. This approach is common in threat intelligence sharing where the accuracy and reliability of shared information are critical.
Reference:
'Building a Cybersecurity Culture,' ISACA
'Trust Models in Information Security,' Journal of Internet Services and Applications

QUESTION 8
A threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.
Which of the following attacks is performed on the client organization?

A. DHCP attacks
B. MAC spoofing attack
C. Distributed Denial-of-Service (DDoS) attack
D. Bandwidth attack

Correct Answer: C
Section:
Explanation:
The attack described, where multiple connection requests from different geo-locations are received by a server within a short time span leading to stress and reduced performance, is indicative of a Distributed Denial-of-Service (DDoS) attack. In a DDoS attack, the attacker floods the target's resources (such as a server) with excessive requests from multiple sources, making it difficult for the server to handle legitimate traffic, leading to degradation or outright unavailability of service. The use of multiple geo-locations for the attack sources is a common characteristic of DDoS attacks, making them harder to mitigate.
Reference:
'Understanding Denial-of-Service Attacks,' US-CERT
'DDoS Quick Guide,' DHS/NCCIC

QUESTION 9
Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.
Which of the following phases of cyber kill chain methodology is Jame executing?

A. Reconnaissance
B. Installation
C. Weaponization
D. Exploitation

Correct Answer: C
Section:
Explanation:
In the cyber kill chain methodology, the phase where Jame is creating a tailored malicious deliverable that includes an exploit and a backdoor is known as 'Weaponization'. During this phase, the attacker prepares by coupling a payload, such as a virus or worm, with an exploit into a deliverable format, intending to compromise the target's system. This step follows the initial 'Reconnaissance' phase, where the attacker gathers information on the target, and precedes the 'Delivery' phase, where the weaponized bundle is transmitted to the target. Weaponization involves the preparation of the malware to exploit the identified vulnerabilities in the target system.
Reference:
Lockheed Martin's Cyber Kill Chain framework
'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,' leading to the development of the Cyber Kill Chain framework

QUESTION 10
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. Unexpected patching of systems
C. Unusual activity through privileged user account
D. Geographical anomalies

Correct Answer: D
Section:
Explanation:
The scenario described by Steve's observations, where multiple logins are occurring from different locations in a short time span, especially from locations where the organization has no business relations, points to 'Geographical anomalies' as a key indicator of compromise (IoC). Geographical anomalies in logins suggest unauthorized access attempts potentially made by attackers using compromised credentials. This is particularly suspicious when the locations of these logins do not align with the normal geographical footprint of the organization's operations or employee locations. Monitoring for such anomalies can help in the early detection of unauthorized access and potential data breaches.
Reference:
SANS Institute Reading Room, 'Indicators of Compromise: Reality's Version of the Minority Report'
'Identifying Indicators of Compromise' by CERT-UK

QUESTION 11
Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

A. Nation-state attribution
B. True attribution
C. Campaign attribution
D. Intrusion-set attribution

Correct Answer: B
Section:
Explanation:
True attribution in the context of cyber threats involves identifying the actual individual, group, or nation-state behind an attack or intrusion. This type of attribution goes beyond associating an attack with certain tactics, techniques, and procedures (TTPs) or a known group and aims to pinpoint the real-world entity responsible. True attribution is challenging due to the anonymity of the internet and the use of obfuscation techniques by attackers, but it is crucial for understanding the motive behind an attack and for forming appropriate responses at diplomatic, law enforcement, or cybersecurity levels.
Reference:
'Attribution of Cyber Attacks: A Framework for an Evidence-Based Analysis' by Jason Healey
'The Challenges of Attribution in Cyberspace' in the Journal of Cyber Policy

QUESTION 12
In a team of threat analysts, two individuals were competing over projecting their own hypotheses on a given malware. However, to find logical proofs to confirm their hypotheses, the threat intelligence manager used a de-biasing strategy that involves learning strategic decision making in the circumstances comprising multistep interactions with numerous representatives, either having or without any perfect relevant information.
Which of the following de-biasing strategies the threat intelligence manager used to confirm their hypotheses?

A. Game theory
B. Machine learning
C. Decision theory

D. Cognitive psychology

Correct Answer: A
Section:
Explanation:
Game theory is a mathematical framework designed for understanding strategic situations where individuals' or groups' outcomes depend on their choices and the choices of others. In the context of threat intelligence analysis, game theory can be used as a de-biasing strategy to help understand and predict the actions of adversaries and defenders. By considering the various strategies and potential outcomes in a 'game' where each player's payoff is affected by the actions of others, analysts can overcome their biases and evaluate hypotheses more objectively. This approach is particularly useful in scenarios involving multiple actors with different goals and incomplete information.
Reference:
'Game Theory and Its Applications in Cybersecurity' in the International Journal of Computer Science and Information Security
'Applying Game Theory to Cybersecurity' by the SANS Institute

QUESTION 13
Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts. During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.
In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

A. Dissemination and integration
B. Planning and direction
C. Processing and exploitation
D. Analysis and production

Correct Answer: C
Section:
Explanation:
The phase where threat intelligence analysts convert raw data into useful information by applying various techniques, such as machine learning or statistical methods, is known as 'Processing and Exploitation'. During this phase, collected data is processed, standardized, and analyzed to extract relevant information. This is a critical step in the threat intelligence lifecycle, transforming raw data into a format that can be further analyzed and turned into actionable intelligence in the subsequent 'Analysis and Production' phase.
Reference:
'Intelligence Analysis for Problem Solvers' by John E. McLaughlin
'The Cyber Intelligence Tradecraft Project: The State of Cyber Intelligence Practices in the United States (Unclassified Summary)' by the Carnegie Mellon University's Software Engineering Institute

QUESTION 14
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. Internal intelligence feeds
B. External intelligence feeds
C. CSV data feeds
D. Proactive surveillance feeds

Correct Answer: A
Section:
Explanation:
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.
Reference:
'Building an Intelligence-Led Security Program' by Allan Liska
'Threat Intelligence: Collecting, Analysing, Evaluating' by M-K. Lee, L. Healey, and P. A. Porras

QUESTION 15
Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?

A. Repeater
B. Gateway
C. Hub
D. Network interface card (NIC)

Correct Answer: B
Section:
Explanation:
A gateway in a network functions as a node that routes traffic between different networks, such as from a local network to the internet. In the context of cyber threats, a gateway can be utilized to monitor and control the data flow to and from the network, helping in the identification and analysis of malware communications, including traffic to external command and control (C2) servers. This makes it an essential component in detecting installed malware within a network by observing anomalies or unauthorized communications at the network's boundary. Unlike repeaters, hubs, or network interface cards (NICs) that primarily facilitate network connectivity without analyzing the traffic, gateways can enforce security policies and detect suspicious activities.
Reference:
'Network Security Basics,' Security+ Guide to Network Security Fundamentals
'Malware Command and Control Channels: A Journey,' SANS Institute InfoSec Reading Room

QUESTION 16
What is the correct sequence of steps involved in scheduling a threat intelligence program?
1. Review the project charter
2. Identify all deliverables
3. Identify the sequence of activities
4. Identify task dependencies
5. Develop the final schedule
6. Estimate duration of each activity
7. Identify and estimate resources for all activities
8. Define all activities
9. Build a work breakdown structure (WBS)

A. 1-->9-->2-->8-->3-->7-->4-->6-->5
B. 3-->4-->5-->2-->1-->9-->8-->7-->6
C. 1-->2-->3-->4-->5-->6-->9-->8-->7
D. 1-->2-->3-->4-->5-->6-->7-->8-->9

Correct Answer: A
Section:
Explanation:
The correct sequence for scheduling a threat intelligence program involves starting with the foundational steps of defining the project scope and objectives, followed by detailed planning and scheduling of tasks. The sequence starts with reviewing the project charter (1) to understand the project's scope, objectives, and constraints. Next, building a Work Breakdown Structure (WBS) (9) helps in organizing the team's work into manageable sections. Identifying all deliverables (2) clarifies the project's outcomes. Defining all activities (8) involves listing the tasks required to produce the deliverables. Identifying the sequence of activities (3) and estimating resources (7) and task dependencies (4) sets the groundwork for scheduling. Estimating the duration of each activity (6) is critical before developing the final schedule (5), which combines all these elements into a comprehensive plan. This approach ensures a structured and methodical progression from project initiation to execution.

Reference:
'A Guide to the Project Management Body of Knowledge (PMBOK Guide),' Project Management Institute
'Cyber Intelligence-Driven Risk,' by Intel471

QUESTION 17
Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.
Which of the following sharing platforms should be used by Kim?

A. Cuckoo sandbox
B. OmniPeek
C. PortDroid network analysis
D. Blueliv threat exchange network

Correct Answer: D
Section:
Explanation:
The Blueliv Threat Exchange Network is a collaborative platform designed for sharing and receiving threat intelligence among security professionals and organizations. It provides real-time information on global threats, helping participants to enhance their security posture by leveraging shared intelligence. The platform facilitates the exchange of information related to cybersecurity threats, including indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs) of threat actors, and other relevant data. This makes it an ideal choice for Kim, who is looking to gather and share threat information to develop security policies for his organization. In contrast, Cuckoo Sandbox is a malware analysis system, OmniPeek is a network analyzer, and PortDroid is a network analysis application, none of which are primarily designed for intelligence sharing.
Reference:
Blueliv's official documentation and resources
'Building an Intelligence-Led Security Program,' by Allan Liska

QUESTION 18
During the process of threat intelligence analysis, John, a threat analyst, successfully extracted an indication of adversary's information, such as Modus operandi, tools, communication channels, and forensics evasion strategies used by adversaries.
Identify the type of threat intelligence analysis is performed by John.

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

Correct Answer: D
Section:
Explanation:
Tactical threat intelligence analysis focuses on the immediate, technical indicators of threats, such as the tactics, techniques, and procedures (TTPs) used by adversaries, their communication channels, the tools and software they utilize, and their strategies for evading forensic analysis. This type of analysis is crucial for operational defenses and is used by security teams to adjust their defenses against current threats. Since John successfully extracted information related to the adversaries' modus operandi, tools, communication channels, and evasion strategies, he is performing tactical threat intelligence analysis. This differs from strategic and operational threat intelligence, which focus on broader trends and specific operations, respectively, and from technical threat intelligence, which deals with technical indicators like malware signatures and IPs.
Reference:
'Tactical Cyber Intelligence,' by Cyber Threat Intelligence Network, Inc.
'Intelligence-Driven Incident Response: Outwitting the Adversary,' by Scott J. Roberts and Rebekah Brown

QUESTION 19
SecurityTech Inc. is developing a TI plan where it can drive more advantages in less funds. In the process of selecting a TI platform, it wants to incorporate a feature that ranks elements such as intelligence sources, threat actors, attacks, and digital assets of the organization, so that it can put in more funds toward the resources which are critical for the organization's security.

Which of the following key features should SecurityTech Inc. consider in their TI plan for selecting the TI platform?

A. Search
B. Open
C. Workflow
D. Scoring

Correct Answer: D
Section:
Explanation:
Incorporating a scoring feature in a Threat Intelligence (TI) platform allows SecurityTech Inc. to evaluate and prioritize intelligence sources, threat actors, specific types of attacks, and the organization's digital assets based on their relevance and threat level to the organization. This prioritization helps in allocating resources more effectively, focusing on protecting critical assets and countering the most significant threats. A scoring system can be based on various criteria such as the severity of threats, the value of assets, the reliability of intelligence sources, and the potential impact of threat actors or attack vectors. By quantifying these elements, SecurityTech Inc. can make informed decisions on where to invest its limited funds to enhance its security posture most effectively.
Reference:
'Designing and Building a Cyber Threat Intelligence Capability' by the SANS Institute
'Threat Intelligence: What It Is, and How to Use It Effectively' by Gartner

QUESTION 20
Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.
What stage of ACH is Bob currently in?

A. Diagnostics
B. Evidence
C. Inconsistency
D. Refinement

Correct Answer: D
Section:
Explanation:
In the Analysis of Competing Hypotheses (ACH) process, the stage where Mr. Bob is applying analysis to reject hypotheses and select the most likely one based on listed evidence, followed by preparing a matrix with screened hypotheses and evidence, is known as the 'Refinement' stage. This stage involves refining the list of hypotheses by systematically evaluating the evidence against each hypothesis, leading to the rejection of inconsistent hypotheses and the strengthening of the most plausible ones. The preparation of a matrix helps visualize the relationship between each hypothesis and the available evidence, facilitating a more objective and structured analysis.
Reference:
'Psychology of Intelligence Analysis' by Richards J. Heuer, Jr., for the CIA's Center for the Study of Intelligence
'A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis' by the CIA

QUESTION 21
Moses, a threat intelligence analyst at InfoTec Inc., wants to find crucial information about the potential threats the organization is facing by using advanced Google search operators. He wants to identify whether any fake websites are hosted at the similar to the organization's URL.
Which of the following Google search queries should Moses use?

A. related: www.infothech.org
B. info: www.infothech.org
C. link: www.infothech.org

D. cache: www.infothech.org

Correct Answer: A
Section:
Explanation:
The 'related:' Google search operator is used to find websites that are similar or related to a specified URL. In the context provided, Moses wants to identify fake websites that may be posing as or are similar to his organization's official site. By using the 'related:' operator followed by his organization's URL, Google will return a list of websites that Google considers to be similar to the specified site. This can help Moses identify potential impersonating websites that could be used for phishing or other malicious activities. The 'info:', 'link:', and 'cache:' operators serve different purposes; 'info:' provides information about the specified webpage, 'link:' used to be used to find pages linking to a specific URL (but is now deprecated), and 'cache:' shows the cached version of the specified webpage.
Reference:
Google Search Operators Guide by Moz
Google Advanced Search Help Documentation

QUESTION 22
Henry. a threat intelligence analyst at ABC Inc., is working on a threat intelligence program. He was assigned to work on establishing criteria for prioritization of intelligence needs and requirements.
Which of the following considerations must be employed by Henry to prioritize intelligence requirements?

A. Understand frequency and impact of a threat
B. Understand data reliability
C. Develop a collection plan
D. Produce actionable data

Correct Answer: A
Section:
Explanation:
When prioritizing intelligence requirements, it is crucial to understand the frequency and impact of various threats. This approach helps in allocating resources effectively, focusing on threats that are both likely to occur and that would have significant consequences if they did. By assessing threats based on these criteria, Henry can ensure that the threat intelligence program addresses the most pressing and potentially damaging threats first, thereby enhancing the organization's security posture. This prioritization is essential for effective threat management and for ensuring that the most critical threats are addressed promptly.
Reference:
'Cyber Threat Intelligence: Prioritizing and Using CTI Effectively,' by SANS Institute
'Threat Intelligence: What It Is, and How to Use It Effectively,' by Gartner