Eccouncil

(312-85)

Certified Threat Intelligence Analyst

Total: **88 Questions**

Link:

The use of the "related:" search operator yields a list of domains that Google perceives as being relevant to or associated with the specified URL. This presents a robust approach for Moses to unveil sites that may attempt to impersonate his organization, thereby flagging possible fraudulent activity. This search operator analyzes backlinks, semantic content, and overall site relevance.

Evaluation of Other Options

B. info: www.infothech.org
This operator will display information Google has on the page, such as cached links or snippets, rather than providing similar websites. It fails to accomplish the goal of identifying impersonators.

C. link: www.infothech.org
The “link:” operator is used to find backlinks to the specified URL, which would not reveal any related websites but rather serve to highlight external sites that reference InfoTec Inc. This is not conducive to identifying fake domains.

D. cache: www.infothech.org
The "cache:" operator presents the last cached version of the webpage, which does not provide insights into similar or potentially fraudulent entities but merely serves as an archival view of the existing site.

References

Google Search Operators - Advanced Search Techniques
Understanding Google Search Operators
Advanced Google Search Operators List

Question: 5

A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.
Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?

A. Threat modelling
B. Application decomposition and analysis (ADA)
C. Analysis of competing hypotheses (ACH)
D. Automated technical analysis

Answer: C

Explanation:

C is correct because Analysis of Competing Hypotheses (ACH) systematically evaluates multiple theories by assessing the evidence supporting each, facilitating a robust determination of the most consistent theory regarding the malware in question.

ACH is explicitly designed to handle multiple competing hypotheses, allowing a structured approach to weigh the validity of each theory against the gathered data. This methodology minimizes biases by engaging in a systematic elimination process, enabling analysts to focus on the most plausible scenario based on comprehensive evidence. This approach is particularly useful in environments with high uncertainty, and it enhances decision-making processes by taking into account various perspectives and their corresponding evidential backing.

Option D: While it is important to consider risks related to strategic business decisions, this intelligence does not directly support the tactical and operational requirements of a Red Team. Red Teams focus primarily on the technical aspects of network security and vulnerability testing rather than broader business strategic considerations.

References:

1. https://www.eccouncil.org/certification/certified-threat-intelligence-analyst-ctia/
2. https://www.sans.org/cyber-security-training-resources/threat-intelligence/
3. https://www.nist.gov/publications/threat-intelligence-reference-information-sharing-activities-guide

Question: 8

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

Answer: C

Explanation:

C is correct because Michael is in the process of identifying and analyzing threats that he has gathered, making these threats "known unknowns."

Reasoning:
In the realm of cyber-threat intelligence, "known unknowns" refer to threats that are recognized but not fully understood. Michael has gathered information about potential threats, indicating his awareness of those threats (the "known" aspect). However, he is currently analyzing the information to better understand the nature of these threats, which aligns with the defining characteristics of "known unknowns". This stage encompasses the acknowledgment of the existence of specific threats alongside the realization that their full impact, intention, and the means of addressing them remain unclear.

Critique of Other Options:

A. **Unknown unknowns**: This category represents threats or risks that are entirely unrecognized and as such, cannot be prepared for. Michael's actions demonstrate that he has already identified specific threats, negating this option.

B. **Unknowns unknown**: Contradictory in nature, this concept refers to factors that are not just unidentified, but also whose existence is unknown. As Michael is actively analyzing known threats, this classification does not apply to his current intelligence stage.

D. **Known knowns**: This stage indicates a complete understanding of threats and their implications. Since Michael is still in the analysis phase and seeking to comprehend the identified threats further, he does not have established knowledge, which makes this option incorrect as well.

References:

B.Mandated trust

C.Direct historical trust

D.Validated trust

Answer: D

Explanation:

D is correct because it describes a model where trust is established based on the validated evidence provided by one organization to another.

In a validated trust model, the trustworthiness of the information shared between organizations relies not only on past interactions but also on the rigor and quality of the evidence gathered and assessed. This model emphasizes objective verification, whereby the first organization's ability to substantiate its claims with demonstrable evidence enhances the trust that the second organization develops. This improves the efficacy of threat sharing by ensuring that the shared intelligence is reliable and actionable, thus promoting collaboration based on proven reliability.

Critique of other options:

A. **Mediated trust**: This type involves a third-party intermediary that builds trust based on its own assessments and credentials. This is incorrect as Garry's model does not necessitate a mediating entity, focusing instead on direct evidence between the partnering organizations.

B. **Mandated trust**: This form is inherently based on regulatory or compliance requirements rather than evidence-based trust building. In contrast to Garry's approach which hinges on quality evidence, mandated trust lacks the nuance of assessing past relationships or autonomous evidence validation, leading to a more rigid and less adaptable model.

C. **Direct historical trust**: This model relies on past experiences and historical interactions between organizations. While it can provide a framework for trust, it does not emphasize the need for ongoing validation of new evidence as described in Garry's approach. Historical trust can be influenced by outdated perceptions, whereas validated trust seeks current, concrete proof of reliability.

References:

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6918720/
https://www.csoonline.com/article/3516150/a-guide-to-creating-an-anomaly-detection-framework.html
https://www.privacyinternational.org/report/4088/security-and-privacy-implications-threat-intelligence-sharing

Question: 13

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

logins from locations without business relationships signal possible account compromise or credential theft. In this context, the anomalous logins suggest that an attacker may be exploiting legitimate user credentials, aligning with the recognized patterns of unfamiliar or suspicious locations.

Critical Evaluation of Other Options:

A. Unusual outbound network traffic: While this indicator is crucial for identifying data exfiltration or command-and-control communications, the scenario primarily describes login activity rather than data leaving the network. Thus, it does not fit the context presented.

B. Unexpected patching of systems: This indicator pertains to unplanned or unauthorized changes in system configurations or updates. The situation illustrates login irregularities rather than adjustments or vulnerabilities in systems, making this option irrelevant.

C. Unusual activity through privileged user accounts: Although the pattern of logins may suggest compromised accounts, the details provided in the scenario do not specify whether the accounts involved are privileged. This indicator would be more applicable if the logins were specifically associated with high-level access accounts.

In conclusion, the scenario distinctly highlights geographical anomalies, making option D the most relevant indicator of compromise in this context.

References:

https://www.cisecurity.org/white-papers/cybersecurity-essentials-introduction
https://www.sans.org/white-papers/38586
https://www.cert.org/conferences/2019/general/cybersecurity-indicators-of-compromise-trends-and-strategy-102019-1.pdf

Question: 16

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

Answer: C

Explanation:

C is correct because "Attack origination points" encapsulate the multiple entry vectors an attacker systematically utilizes to infiltrate a target's network.

In Advanced Persistent Threats (APTs), attackers often explore various entry points through repeated attempts to breach a target's defenses. This multipronged approach indicates a strategic commitment to persistence, allowing adversaries to adapt and refine their tactics based on the target's responses. The characteristic of attack origination points emphasizes the continuous and varied methods used to achieve unauthorized access, distinguishing APT from simpler cyber threats characterized by single-vector assaults.

Evaluation of Other Options:

Question: 20

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

Answer: C

Explanation:

C is correct because the analysts are converting raw data into useful information, indicating engagement in the processing and exploitation phase of the threat intelligence lifecycle.

In the threat intelligence lifecycle, the "Processing and Exploitation" phase focuses on the organization, aggregation, and conversion of raw data gathered from diverse sources into structured information. This phase utilizes various techniques such as statistical analysis and machine learning, which aligns with the activities mentioned regarding Cybersol Technologies' team of analysts. By applying these techniques, the team is effectively enabling the transformation of unrefined data into actionable intelligence, which is a hallmark of this specific lifecycle stage.

Evaluation of Other Options:

A. **Dissemination and Integration**: This phase involves sharing processed intelligence with stakeholders and integrating it into operational workflows. The current focus on data conversion indicates that the team has not yet reached the dissemination stage.

B. **Planning and Direction**: This initial phase involves defining intelligence requirements and operational priorities. The team's activities of processing data do not correspond with strategizing or setting objectives, which characterizes this phase.

D. **Analysis and Production**: While this phase includes the synthesis of collected information into coherent reports or intelligence products, it occurs after the data is first processed. The team's current actions are more aligned with the earlier step of converting raw data rather than the higher-level analysis and strategic production of intelligence outputs.

References:

https://www.cybrary.it/course/cyber-threat-intelligence/
https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/threat-intelligence
https://www.nist.gov/publications/threat-intelligence-framework

Question: 21

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. 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

Answer: A

Explanation:

A is correct because it presents a logical sequence that aligns with project management principles for initiating and managing a threat intelligence program effectively.

The correct sequence begins with a project charter review (Step 1), ensuring stakeholder alignment. Following this, identifying all deliverables (Step 9) and specific activities (Step 8) establishes a comprehensive foundation for the upcoming steps. This approach streamlines the designation of tasks (Step 2) while maintaining clarity in project scope. Identifying the sequence of activities (Step 3) and their dependencies (Step 4) accurately reflects the interrelations between tasks, facilitating precise scheduling. Estimating resource requirements (Step 7) and the duration of each activity (Step 6) allows for thoughtful planning, culminating in the development of a final schedule (Step 5). This structured approach fosters efficiency and accountability in implementing the threat intelligence program.

Option B is incorrect as it omits the foundational steps of defining activities (Step 8) and reviewing the project charter (Step 1) early, leading to potential misalignment on project objectives. Option C fails to account for the identification of deliverables and resources before scheduling the timeline, which can compromise project clarity and efficiency. Lastly, Option D presents a misalignment in sequencing by placing 'final schedule development' too early in the process without complete inputs regarding activities, dependencies, and resources, risking project integrity.

References:

https://www.pmi.org/learning/library/project-management-best-practices-8328
https://www.cio.com/article/243046/what-is-project-management-everything-you-need-to-know.html
https://www.projectmanagement.com/Articles/203088/Initiating-Project-Management-Processes

Question: 24

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

Answer: D

Explanation:

D. Blueliv threat exchange network is the most suitable option for Kim due to its focus on threat intelligence sharing and collaboration.

https://www.cia.gov/the-world-factbook/
https://www.nap.edu/catalog/23430/communicating-unemployment-and-inflation-in-the-face-of-varying-expectations
https://www.rand.org/pubs/monograph_reports/MR1770.html