PassQueen
a.k.a dumpsqueen.com

Certified Threat Intelligence Analyst (CTIA)

ECCouncil 312-85

Version Demo

Total Demo Questions: 11

Total Premium Questions: 112

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Threat Intelligence	17
Topic 2, Cyber Threats and Kill Chain Methodology	15
Topic 3, Requirements, Planning, Direction, and Review	12
Topic 4, Data Collection and Processing	19
Topic 5, Data Analysis	20
Topic 6, Intelligence Reporting and Dissemination	12
Topic 7, Threat Intelligence Tools and Technologies	17
Total	112

QUESTION NO: 1

An analyst wants to disseminate the information effectively so that the consumers can acquire and benefit out of the intelligence.

Which of the following criteria must an analyst consider in order to make the intelligence concise, to the point, accurate, and easily understandable and must consist of a right balance between tables, narrative, numbers, graphics, and multimedia?

A. The right time

B. The right presentation

C. The right order

D. The right content

ANSWER: B

Explanation:

The right presentation is correct because dissemination is not merely the act of delivering intelligence; it requires packaging the intelligence in a form that its intended consumers can rapidly understand and use in decisions. A well-designed presentation makes analytic findings concise, accurate, and focused on the consumer's needs, while using an appropriate balance of narrative explanation, quantitative data, tables, visualizations, and other media. This balance lets decision-makers grasp the key judgment and its operational relevance without having to interpret excessive technical detail or disconnected raw data. Presentation should also make the intelligence accessible to the particular audience, such as executives who need a clear strategic summary or technical defenders who need actionable indicators and supporting context. The U.S. intelligence community's analytic standards emphasize clear, logical, and well-supported communication of analytic conclusions, including conveying uncertainty in a manner appropriate to the audience. Similarly, the CISA threat-information-sharing guidance highlights the value of actionable, contextualized information for recipients. These principles support selecting the right presentation format and structure so consumers can effectively acquire, comprehend, and benefit from the intelligence. See ODNI Intelligence Community Directive 203 and CISA Information Sharing.

QUESTION NO: 2

A threat intelligence analyst has identified a suspicious domain, but the domain was registered only two days ago and has no known malicious reputation. The analyst wants to determine whether the domain is likely to be part of a phishing campaign before creating a blocking rule.

Which of the following information would provide the most useful contextual enrichment?

A. Domain registration, certificate, hosting, and passive DNS information

B. The desktop wallpaper used by the analyst

C. The number of users assigned to the SOC

D. The operating system version on the mail server

ANSWER: A

Explanation:

Domain registration, certificate, hosting, and passive DNS information is correct. Enriching a suspicious domain with registration details, certificate transparency records, hosting relationships, historical DNS resolutions, and related domains helps an analyst assess whether it is associated with malicious infrastructure. For example, a recently registered domain using a brand-like name, sharing hosting or certificates with known phishing sites, and resolving to infrastructure previously used for malicious activity would present stronger evidence than age alone. This contextual analysis supports a defensible decision before operationalizing an indicator. See CISA STIX and TAXII resources and IETF RFC 8499: DNS Terminology.

QUESTION NO: 3

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 organizationâ€™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

ANSWER: A

Explanation:

related: www.infothech.org is the appropriate query because the `related:` Google Search operator requests sites that Google considers similar to the specified website. For threat-intelligence reconnaissance, this provides a quick starting point for locating domains with comparable content, branding, purpose, or audience to an organization's legitimate web presence. Such results can help an analyst identify web properties that warrant further validation for possible brand impersonation, typosquatting, phishing infrastructure, or other fraudulent use of a similar online identity.

The operator should be entered with the target domain immediately following the colon, as shown. Results should be treated as leads rather than conclusive evidence: similarity is determined by Google's indexing and ranking systems and does not itself establish that a site is malicious or owned by an attacker. Moses should subsequently examine candidate domains, registration details, certificates, page content, redirects, and reputation data to determine whether a fake site is present. Google documents search-refinement techniques in its Search Help, while CISA provides guidance on recognizing and responding to phishing and impersonation threats in its phishing guidance.

QUESTION NO: 4

While conducting an investigation, an analyst discovers that an attacker compressed documents from multiple file shares into password-protected archive files before transferring them to an external server.

Which of the following MITRE ATT&CK techniques is demonstrated by the attacker?

A. Data from Local System

B. Archive Collected Data

C. Data Encrypted for Impact

D. Exfiltration Over Web Service

ANSWER: B

Explanation:

Archive Collected Data is correct. Adversaries commonly archive collected files into formats such as ZIP, RAR, or 7z before exfiltration. Archiving helps consolidate data, reduce the number of transfers, and may make content inspection more difficult. Password protection adds an additional layer of obfuscation that can hinder automated inspection of the archive. Analysts should investigate unusual archive creation, command-line compression utilities, access to sensitive file shares, and subsequent outbound transfers from the affected system. MITRE ATT&CK documents this behavior as Archive Collected Data. See MITRE ATT&CK: Archive Collected Data.

QUESTION NO: 5

A threat intelligence team has identified several possible explanations for suspicious activity. Before publishing its assessment, the team deliberately searches for evidence that would disprove its preferred explanation and gives equal consideration to alternative explanations.

Which of the following cognitive biases is the team attempting to reduce?

A. Anchoring bias

B. Confirmation bias

C. Availability bias

D. Recency bias

ANSWER: B

Explanation:

Confirmation bias is correct because confirmation bias occurs when analysts favor evidence that supports an existing belief or preferred hypothesis while discounting inconsistent evidence. By actively seeking disconfirming evidence and considering alternatives, the team reduces the risk of reaching a conclusion prematurely.

Structured analytic techniques such as Analysis of Competing Hypotheses help mitigate confirmation bias by requiring analysts to compare all plausible hypotheses against the available evidence and focus on inconsistencies. The method is discussed in the CIA publication Psychology of Intelligence Analysis.

QUESTION NO: 6

ABC is a well-established cyber-security company in the United States. The organization implemented the automation of tasks such as data enrichment and indicator aggregation. They also joined various communities to increase their knowledge about the emerging threats. However, the security teams can only detect and prevent identified threats in a reactive approach.

Based on threat intelligence maturity model, identify the level of ABC to know the stage at which the organization stands with its security and vulnerabilities.

A. Level 2: increasing CTI capabilities

B. Level 3: CTI program in place

C. Level 1: preparing for CTI

D. Level 0: vague where to start

ANSWER: A

Explanation:

Level 2: increasing CTI capabilities is correct because the organization has moved beyond initial planning and is actively developing operational cyber-threat-intelligence capabilities. Automating indicator aggregation and data enrichment shows that it has begun integrating intelligence-related processes into security operations, reducing manual handling and making collected indicators more actionable. Its participation in threat-intelligence communities also demonstrates that it is consuming and sharing external information to improve awareness of emerging threats.

These are hallmark activities of an organization increasing its CTI capability: it has established useful collection, processing, and collaboration practices, but its intelligence use remains primarily reactive. The team can identify and prevent threats once relevant indicators or known threat information are available, rather than consistently anticipating adversary behavior, producing strategic intelligence, or driving proactive, intelligence-led decisions across the organization. In the maturity progression used in CTIA-oriented training, this places the organization at the stage where CTI capabilities are expanding, rather than at a fully mature program stage. EC-Council describes CTIA as covering the collection, analysis, and dissemination of threat intelligence to support defensive decisions: EC-Council CTIA. The value of automated, structured threat-information sharing is also reflected in the MISP Project.

QUESTION NO: 7

Karry, a threat analyst at an XYZ organization, is performing threat intelligence analysis. During the data collection phase, he used a data collection method that involves no participants and is purely based on analysis and observation of activities and processes going on within the local boundaries of the organization.

Identify the type data collection method used by the Karry.

A. Active data collection

B. Passive data collection

C. Exploited data collection

D. Raw data collection

ANSWER: B

Explanation:

Passive data collection is correct because the described approach obtains intelligence by observing and analyzing existing activity, processes, and artifacts within the organization without directly engaging participants or deliberately interacting with the environment to elicit information. In a threat-intelligence context, this can include reviewing internal logs, network telemetry, security alerts, system configurations, historical incident records, and operational workflows. The analyst is collecting information that is already being generated by the organization's normal operations, rather than changing conditions, querying individuals, or stimulating a response.

This approach is valuable during collection because it minimizes disruption to business systems and users while providing evidence grounded in the organization's actual environment. The resulting observations can establish a baseline of normal activity, reveal suspicious patterns, and support subsequent analysis of adversary behaviors and risks. NIST describes continuous monitoring as maintaining awareness of information-system security through ongoing observation and assessment, which aligns closely with this nonintrusive collection approach. See NIST SP 800-137, Information Security Continuous Monitoring. For threat-intelligence context, MITRE's guidance on using defensive telemetry is also relevant: MITRE ATT&CK Resources.

QUESTION NO: 8

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. Federated exchange architecture

C. Hybrid exchange architecture

D. Centralized exchange architecture

ANSWER: D

Explanation:

Centralized exchange architecture is correct because the scenario explicitly describes a single central hub that receives threat data from all participating organizations, performs analysis, and disseminates the resulting intelligence back to the community. This model places collection, correlation, governance, and distribution functions under one authoritative exchange point. It can give the consortium a consistent view of reported indicators, adversary activity, and intelligence priorities, while enabling standardized processing and centralized quality control before intelligence is shared.

In threat intelligence sharing, an exchange architecture defines how participants contribute, manage, and consume intelligence. A centralized model is characterized by the hub-and-spoke arrangement described here: member organizations submit data to the hub, and the hub enriches, analyzes, curates, and redistributes intelligence. This approach is particularly useful where the consortium requires common handling procedures, uniform dissemination policies, and coordinated operational oversight. It also supports the use of structured intelligence-sharing mechanisms and trusted sharing communities, such as those supported by STIX and TAXII specifications. For background on these standards, see OASIS CTI documentation and the CISA information-sharing resources.

QUESTION NO: 9

John, a threat intelligence analyst in CyberTech Company, was asked to obtain information that provides greater insight into the current cyber risks. To gather such information, John needs to find the answers to the following questions:

Why the organization might be attacked?

How the organization might be attacked?

Who might be the intruders?Identify the type of security testing John is going to perform.

A. White box testing

B. Intelligence-led security testing

C. Black box testing

ANSWER: B

Explanation:

Intelligence-led security testing is correct because it uses relevant threat intelligence to focus a security assessment on the adversaries most likely to target a particular organization, their motivations, and the techniques they are likely to use. The questions concerning why the organization may be attacked, how an attack may occur, and who the potential intruders are correspond directly to understanding adversary intent, capability, and identity. This intelligence provides the context needed to create realistic attack scenarios and assess whether controls can detect, prevent, and respond to threats that are meaningful to the organization's risk profile.

Rather than treating testing solely as a technical search for weaknesses, intelligence-led security testing begins with threat-actor information, current campaigns, targeting patterns, and likely attack paths. The resulting exercise is tailored to business assets, sector exposure, and credible adversary behavior. This makes the findings more actionable for prioritizing defensive improvements and validating resilience against targeted attacks. EC-Council's threat-intelligence training emphasizes analyzing threat actors, tactics, techniques, procedures, and indicators to support risk-informed defensive decisions. See the EC-Council Certified Threat Intelligence Analyst overview and CREST's Intelligence-Led Testing Guide for further context on applying intelligence to realistic security testing.

QUESTION NO: 10

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.

ANSWER: C

Explanation:

Jim should monitor network traffic for malicious file transfers, file integrity monitoring, and event logs. Data staging is the adversary practice of collecting and consolidating targeted information in a central location—such as a workstation, server, network share, or temporary directory—so it can be packaged and exfiltrated later. Detecting it requires visibility into unusual file creation, copying, movement, compression, and access activity, particularly where sensitive files are gathered into locations that do not normally hold them. File integrity monitoring can identify unexpected changes and newly created archive or staging files, while endpoint and server event logs can reveal the responsible accounts, processes, access paths, and timing. Network telemetry further helps analysts identify anomalous internal file transfers or movement to systems that may be serving as collection points. Correlating these sources allows Jim to identify the staging activity early, contain affected hosts, preserve evidence, and prevent the pending export of data. MITRE ATT&CK describes this behavior under Data Staged and recommends monitoring relevant file, process, and network activity: MITRE ATT&CK: Data Staged. Centralized collection and analysis of security logs is also a core detection practice described by NIST SP 800-92, Guide to Computer Security Log Management.

QUESTION NO: 11

Kira works as a security analyst in an organization. She was asked to define and set up the requirements before collecting threat intelligence information. The requirements should focus on what must be collected in order to fulfil production intelligence.

Which of the following categories of threat intelligence requirements should Kira focus on?

A. Production requirements

B. Intelligence requirements

C. Business requirements

D. Collection requirements

ANSWER: D

Explanation:

Collection requirements is correct because this category translates the intelligence-production need into specific information that must be acquired. Before analysts can collect threat intelligence, they need a defined scope identifying the relevant data types, sources, entities, indicators, events, time frames, and collection priorities. These requirements guide the collection effort toward information that can support the intended intelligence product rather than gathering data without a defined purpose. In practical terms, collection requirements provide the actionable bridge between an organization's intelligence needs and the data-gathering activities used to satisfy those needs. They help an analyst determine what information should be sought from internal telemetry, security tools, external reporting, threat-sharing communities, open sources, or other approved sources. Clearly documented collection requirements also support efficient use of resources, repeatable collection processes, and traceability from collected material to the resulting intelligence production. This aligns with the intelligence-cycle concept that collection is planned and directed according to established requirements. The Office of the Director of National Intelligence overview of intelligence describes intelligence as supporting decision-making through a structured process, while the CISA information-sharing guidance highlights the value of timely, relevant cyber threat information for defensive action.