PassQueen
a.k.a dumpsqueen.com

CREST Practitioner Threat Intelligence Analyst

CREST CPTIA

Version Demo

Total Demo Questions: 15

Total Premium Questions: 159

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Threat Intelligence Fundamentals	40
Topic 2, Planning and Direction	15
Topic 3, Collection	32
Topic 4, Processing and Exploitation	18
Topic 5, Analysis and Production	26
Topic 6, Dissemination and Integration	10
Topic 7, Mix Questions	18
Total	159

QUESTION NO: 1

Which of the following is an attack that occurs when a malicious program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated?

A. Cross-site scripting

B. Insecure direct object references

C. Cross-site request forgery

D. SQL injection

ANSWER: C

Explanation:

Cross-site request forgery is the correct answer because it abuses the browser's existing authenticated relationship with a trusted web application. When a user has signed in to a site, their browser will commonly attach relevant session cookies or other credentials to requests sent to that site. An attacker can cause the victim's browser to submit a crafted request to an application where the victim is authenticated, potentially invoking a state-changing action under the victim's account. The key characteristic is that the application receives a request that appears to originate from the legitimate, logged-in user, even though the user did not intentionally initiate that action. Effective CSRF defenses ensure the application can distinguish genuine requests from attacker-induced ones, such as through unpredictable anti-CSRF tokens that are validated server-side, and appropriate cookie protections such as `SameSite`. OWASP's CSRF guidance describes this attack pattern and recommends token-based defenses for state-changing operations. For broader web-application security context, CSRF is also included in OWASP's catalogue of common application security risks. See the OWASP Cross-Site Request Forgery page and the OWASP CSRF Prevention Cheat Sheet.

QUESTION NO: 2

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

ANSWER: D

Explanation:

Tactical threat intelligence analysis is correct because the information extracted describes how an adversary conducts an intrusion. An adversary's modus operandi, the tools it uses, its communication channels, and methods for avoiding forensic detection are all behavioural details that help defenders understand and recognize the attacker's tactics, techniques, and procedures. This intelligence is directly actionable by security operations, detection engineering, incident response, and threat-hunting teams: it can inform monitoring priorities, detection logic, investigation hypotheses, and defensive controls.

Tactical intelligence connects observed adversary activity to repeatable patterns of tradecraft. For example, understanding an actor's preferred command-and-control approach or defence-evasion behaviour enables analysts to look for corresponding activity in endpoint, network, authentication, and cloud telemetry. It therefore provides the practical adversary context needed to improve near-term detection and response decisions. CREST identifies threat intelligence as a discipline that supports informed security decisions, while MITRE ATT&CK provides a widely used knowledge base for documenting adversary tactics and techniques in precisely this manner. See CREST Threat Intelligence and MITRE ATT&CK.

QUESTION NO: 3

In which of the following forms of bulk data collection are large amounts of data first collected from multiple sources in multiple formats and then processed to achieve threat intelligence?

A. Structured form

B. Hybrid form

C. Production form

D. Unstructured form

ANSWER: D

Explanation:

Unstructured form is correct because it describes the collection of raw, heterogeneous information before it has been normalized, categorized, or converted into a common machine-readable schema. Threat-intelligence teams commonly ingest high-volume material from sources such as news reporting, technical blogs, social-media posts, malware reports, vulnerability disclosures, paste sites, and free-text incident reporting. These sources vary substantially in format, quality, language, and reliability. The value-generating step therefore occurs after collection: analysts and technical systems extract entities and indicators, assess source credibility and context, correlate observations, remove duplicates, and enrich relevant material to produce actionable intelligence. This approach supports discovery because it does not restrict collection to predefined fields or a fixed data model at the outset. NIST describes cyber-threat information sharing as involving varied threat information and emphasizes the need to process and use information in operationally meaningful ways; see NIST SP 800-150. For a practical view of converting broad threat reporting into structured intelligence objects, the OASIS STIX 2.1 overview explains a standardized representation that can be applied after information has been extracted and analyzed.

QUESTION NO: 4

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

ANSWER: C

Explanation:

OCTAVE is correct because its original approach is an asset-driven, organisation-level risk assessment methodology built around these three phases: developing asset-based threat profiles, identifying infrastructure vulnerabilities, and developing security strategy and plans. The process starts by identifying critical organisational assets and the security requirements that matter for them, such as confidentiality, integrity, and availability. It then develops threat profiles based on how those assets could be harmed and the consequences of compromise. OCTAVE next examines technical vulnerabilities in the infrastructure that supports the critical assets, allowing the organisation to understand the exposure that could enable the identified threats. Finally, the assessment results are used to determine and prioritise risks and produce a protection strategy and risk-mitigation plans. This makes OCTAVE especially appropriate where the aim is to connect business-critical assets,

threats, vulnerabilities, and planned security countermeasures rather than merely score individual technical flaws. Carnegie Mellon University's Software Engineering Institute describes the three-phase OCTAVE method and its asset-focused evaluation process in its OCTAVE Method Implementation Guide. Further background and OCTAVE resources are available from the SEI OCTAVE Allegro overview.

QUESTION NO: 5

Alison, an analyst in an XYZ organization, wants to retrieve information about a company's website from the time of its inception as well as the removed information from the target website.

What should Alison do to get the information he needs.

A. Alison should use SmartWhois to extract the required website information.

B. Alison should use https://archive.org to extract the required website information.

C. Alison should run the Web Data Extractor tool to extract the required website information.

D. Alison should recover cached pages of the website from the Google search engine cache to extract the required website information.

ANSWER: B

Explanation:

Alison should use https://archive.org to extract the required website information. The Internet Archive's Wayback Machine preserves historical snapshots of publicly accessible websites captured at different points in time. By searching for the target site's domain, an analyst can identify archived versions of pages, review how content, technologies, contact details, and organisational messaging changed over time, and potentially recover material that is no longer available on the live website. This makes it particularly useful for threat-intelligence research, OSINT investigations, attack-surface history, attribution context, and investigations requiring a time-based view of a web presence.

Archived data is not necessarily complete: capture frequency, robots directives, site availability, dynamic content, and access restrictions can affect what was retained. Nevertheless, the Wayback Machine is designed specifically to provide historical access to web content rather than merely current domain-registration data or a short-lived search-cache copy. Analysts should record the snapshot timestamp and source URL for evidential traceability, and corroborate significant findings where appropriate. The Internet Archive provides access through the Wayback Machine and documents its preservation mission at Internet Archive: About.

QUESTION NO: 6

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 delivery of intelligence; it is the process of communicating it in a form that enables the intended audience to understand, assess, and use it. Presentation determines how findings are structured and expressed, including the appropriate balance of concise narrative, quantitative evidence, tables, visualisations, and, where useful, multimedia. An analyst should tailor this format to the consumers' role, technical knowledge, decision-making needs, and the urgency of the situation. For example, senior decision-makers may need a short executive summary supported by clear visual indicators, whereas operational teams may require more detailed technical context and structured data. Effective presentation also preserves accuracy by clearly distinguishing assessed judgements, supporting evidence, confidence, and relevant limitations. This allows consumers to quickly identify what matters and make informed, actionable decisions without being overwhelmed by unnecessary detail. CREST's threat-intelligence guidance identifies reporting and communication as essential parts of delivering useful intelligence to stakeholders, while the UK National Cyber Security Centre similarly stresses communicating risk in a clear, audience-appropriate manner. See CREST and NCSC risk management guidance.

QUESTION NO: 7

A threat intelligence analyst is asked to prioritise remediation of a newly disclosed vulnerability. Public reporting indicates active exploitation, but the organisation has thousands of assets and limited patching capacity.

Which approach provides the most defensible remediation priority?

A. Patch systems solely in descending CVSS score order

B. Prioritise only systems that have generated security alerts

C. Defer remediation until a proof-of-concept exploit is tested internally

D. Prioritise assets according to operating-system age

E. Combine active-exploitation evidence with exposure, criticality, and controls

ANSWER: E

Explanation:

The correct approach is to **combine evidence of active exploitation with asset exposure, business criticality, and the availability of compensating controls**. Active exploitation materially raises the likelihood of harm, but the urgency for a particular organisation also depends on whether vulnerable assets are present, reachable by an attacker, and important to critical services.

CVSS scores are useful technical inputs but do not, by themselves, establish organisational risk. Prioritising only public attention or patching every affected system in arbitrary order can misdirect limited remediation resources away from the most exposed and consequential assets.

QUESTION NO: 8

Eric who is an incident responder is working on developing incident-handling plans and

procedures. As part of this process, he is performing analysis on the organizational

network to generate a report and to develop policies based on the acquired results.

Which of the following tools will help him in analyzing network and its related traffic?

A. FaceNiff

B. Wireshark

C. Burp Suite

D. Whois

ANSWER: B

Explanation:

Wireshark is correct because it is a packet and network-protocol analyzer designed to capture, inspect, filter, and interpret traffic traversing an organizational network. An incident responder can use it to establish normal traffic patterns, identify the protocols and services in use, examine source and destination hosts, review DNS, HTTP, TLS, and other protocol activity, and investigate anomalous communications that may indicate compromise. This evidence can be exported or documented to support a network-analysis report and to inform incident-handling procedures, such as what network telemetry should be retained, which suspicious indicators should trigger escalation, and how analysts should validate potentially malicious traffic. Wireshark supports both live capture from network interfaces and analysis of previously collected packet-capture files, making it suitable during preparation as well as active incident investigation. Its display filters also enable analysts to focus efficiently on relevant hosts, conversations, protocols, or indicators without losing the broader packet-level context needed for sound conclusions. The Wireshark project describes the tool as a network protocol analyzer that lets users capture and interactively browse network traffic; its official documentation provides guidance on capture and display filtering. See the Wireshark official website and the Wireshark User's Guide on display filters.

QUESTION NO: 9

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

ANSWER: D

Explanation:

Scoring is the appropriate feature because it enables a threat-intelligence platform to consistently rank and prioritise intelligence sources, threat actors, campaigns, indicators, attack techniques, and organisational assets according to relevance, confidence, severity, and likely business impact. This gives SecurityTech Inc. a defensible basis for directing limited analyst time, tooling spend, and defensive controls toward the threats and assets that present the greatest security risk. For example, a platform can assign higher priority where a credible actor is actively targeting a high-value internet-facing asset, while reducing attention on low-confidence or low-impact intelligence. Scoring also supports repeatable triage and makes prioritisation less dependent on individual analyst judgement alone. Effective threat intelligence is intended to support decision-making and action, rather than merely collect large volumes of data. NIST describes cyber threat information sharing as supporting improved situational awareness and more informed risk-management decisions; a scoring capability operationalises that principle by turning disparate intelligence into ranked, actionable priorities. See NIST SP 800-150: Guide to Cyber Threat Information Sharing and CISA Cyber Threats and Advisories.

QUESTION NO: 10

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

ANSWER: C

Explanation:

Expansion is the correct phase because the attacker has already achieved access to an initial endpoint and is now seeking administrative credentials to broaden that access across the organisation. In an APT lifecycle, expansion describes increasing the attacker's foothold after the initial compromise: elevating privileges, acquiring credentials, discovering accessible resources, compromising further hosts, and moving laterally. Administrative credentials are particularly valuable because they can enable access to additional systems, remote services, and higher-value network resources, allowing the operation to grow beyond the originally compromised machine.

This activity aligns with the Credential Access and Lateral Movement objectives documented in the MITRE ATT&CK knowledge base. Credential access includes techniques used to obtain account credentials, while lateral movement covers using that access to reach and control other systems. Although an attacker may establish persistence during a campaign, the described immediate objective is specifically to extend control from one system into more of the environment, which is expansion. See MITRE ATT&CK: Credential Access and MITRE ATT&CK: Lateral Movement.

QUESTION NO: 11

Eric works as a system administrator in ABC organization. He granted privileged users with unlimited permissions to access the systems. These privileged users can misuse

their rights unintentionally or maliciously or attackers can trick them to perform malicious activities.

Which of the following guidelines helps incident handlers to eradicate insider attacks by privileged users?

A. Do not use encryption methods to prevent administrators and privileged users from accessing backup tapes and sensitive information

B. Do not control the access to administrators and privileged users

C. Do not enable the default administrative accounts to ensure accountability

D. Do not allow administrators to use unique accounts during the installation process

ANSWER: C

Explanation:

Do not enable the default administrative accounts to ensure accountability is correct because privileged activity must be attributable to a specific, identifiable person. Default administrator accounts are commonly shared, have predictable names, and cannot reliably distinguish which individual performed a particular action. Disabling, renaming where appropriate, and tightly controlling such accounts reduces an attacker's ability to exploit a known privileged identity and prevents administrators from carrying out routine work through an untraceable shared account. Instead, each administrator should use a unique named account, with elevated access granted only when required and with comprehensive audit logging enabled. During incident response, these records allow handlers to establish an accurate timeline, identify the account and person associated with a change, scope potentially affected systems, and revoke or remediate compromised access quickly. This supports both containment and eradication of insider misuse, whether deliberate or accidental. NIST's account-management control requires organizations to manage system accounts and defines accountability-related attributes, while its privileged-account guidance emphasizes restricting and monitoring elevated access. See NIST SP 800-53, Account Management and CISA guidance on protecting privileged access.

QUESTION NO: 12

Employee monitoring tools are mostly used by employers to find which of the following?

A. Lost registry keys

B. Conspiracies

C. Malicious insider threats

D. Stolen credentials

ANSWER: C

Explanation:

Employee monitoring tools are primarily used to identify malicious insider threats: risks arising when people with legitimate organisational access intentionally misuse that access to steal information, disrupt operations, commit fraud, or otherwise harm the organisation. Because employees, contractors, and other trusted users may legitimately access sensitive systems and data, organisations need visibility into behaviour that departs from normal, authorised activity. Monitoring can help surface indicators such as unusual access to sensitive repositories, bulk copying or downloading of data, unauthorised use of removable media, attempts to bypass controls, access outside normal working patterns, and transmission of sensitive data to unapproved destinations.

In threat-intelligence and security operations contexts, this telemetry supports detection, investigation, and response by allowing analysts to correlate user actions with assets, identities, and known threat indicators. Effective monitoring should be risk-based, proportionate, governed by clear policy, and implemented with appropriate privacy, legal, and employment-law safeguards. CISA describes insider-threat mitigation as a process that includes identifying and detecting concerning behaviours, while NIST's insider-threat guidance highlights the value of integrating technical and behavioural indicators. See CISA Insider Threat Mitigation and NIST SP 800-53 Rev. 5.

QUESTION NO: 13

A threat intelligence team receives a request from the board asking whether a regional geopolitical development is likely to increase cyber targeting of the organisation during the next quarter, and whether additional defensive investment is justified.

How should the team classify this request?

A. Collection requirement

B. Technical indicator

C. Priority intelligence requirement

D. Request for takedown

ANSWER: C

Explanation:

Priority intelligence requirement is correct because the request is a decision-focused question from a senior stakeholder. It identifies a specific uncertainty, a time frame, and an intended business decision: whether to allocate additional defensive resources.

A collection requirement would describe the information needed to answer the question, such as reporting on relevant threat actors, targeting patterns, and capability changes. Indicators and technical observables may support collection and analysis, but they are not the executive intelligence need itself.

QUESTION NO: 14

Ren is assigned to handle a security incident of an organization. He is tasked with forensics investigation to find the evidence needed by the management. Which of the following steps falls under the investigation phase of the computer forensics investigation process?

A. Secure the evidence

B. Risk assessment

C. Setup a computer forensics lab

D. Evidence assessment

ANSWER: D

Explanation:

Evidence assessment is part of the forensic investigation phase because it turns acquired and analysed artefacts into findings that are relevant, reliable, and useful for decision-making. The investigator evaluates the evidential value of the material, including its connection to the incident, provenance, integrity, timeline relevance, and the degree to which it supports a defensible conclusion. This assessment helps establish what occurred, which systems, accounts, or data were involved, and the potential business impact. It also enables the investigator to distinguish meaningful evidence from incidental or unrelated data before presenting conclusions to management or, where necessary, to legal stakeholders. Sound assessment depends on maintaining documented handling and analysis processes so that findings can be traced back to the original evidence and independently reviewed. NIST's guidance on incident response and forensic techniques describes analysis as examining data to identify indicators, determine their significance, and support incident conclusions. Its digital-forensics guide also emphasizes preserving the integrity and chain of custody of evidence so analytical findings remain trustworthy. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 15

Racheal is an incident handler working in InceptionTech organization. Recently,

numerous employees are complaining about receiving emails from unknown senders. In

order to prevent employees against spoofing emails and keeping security in mind,

Racheal was asked to take appropriate actions in this matter. As a part of her

assignment, she needs to analyze the email headers to check the authenticity of received

emails.

Which of the following protocol/authentication standards she must check in email

header to analyze the email authenticity?

A. DKIM

B. SNMP

C. POP

D. ARP

ANSWER: A

Explanation:

DKIM is the appropriate email-authentication standard to check in a received message's headers. DomainKeys Identified Mail adds a cryptographic signature to outbound email on behalf of a sending domain. The receiving mail system can retrieve the associated public key from DNS and verify the signature. Successful verification shows that the signed portions of the message, including selected headers and body content, have not been altered after signing, and that the sender was authorized to use the signing domain represented by the `d=` value. During incident handling, the relevant evidence is commonly presented in an `Authentication-Results` header, such as `dkim=pass` or `dkim=fail`, and in the `DKIM-Signature` header itself. An analyst should correlate the signing domain with the visible From domain and other authentication results to assess spoofing risk. DKIM is therefore a key control for evaluating claimed sender-domain authenticity from message headers, although a passing result should be interpreted in context rather than as proof of an

individual sender’s identity. The DKIM protocol and signature-verification model are defined in RFC 6376. Practical guidance on how DKIM supports validation of email sent from a domain is also provided by the UK National Cyber Security Centre.