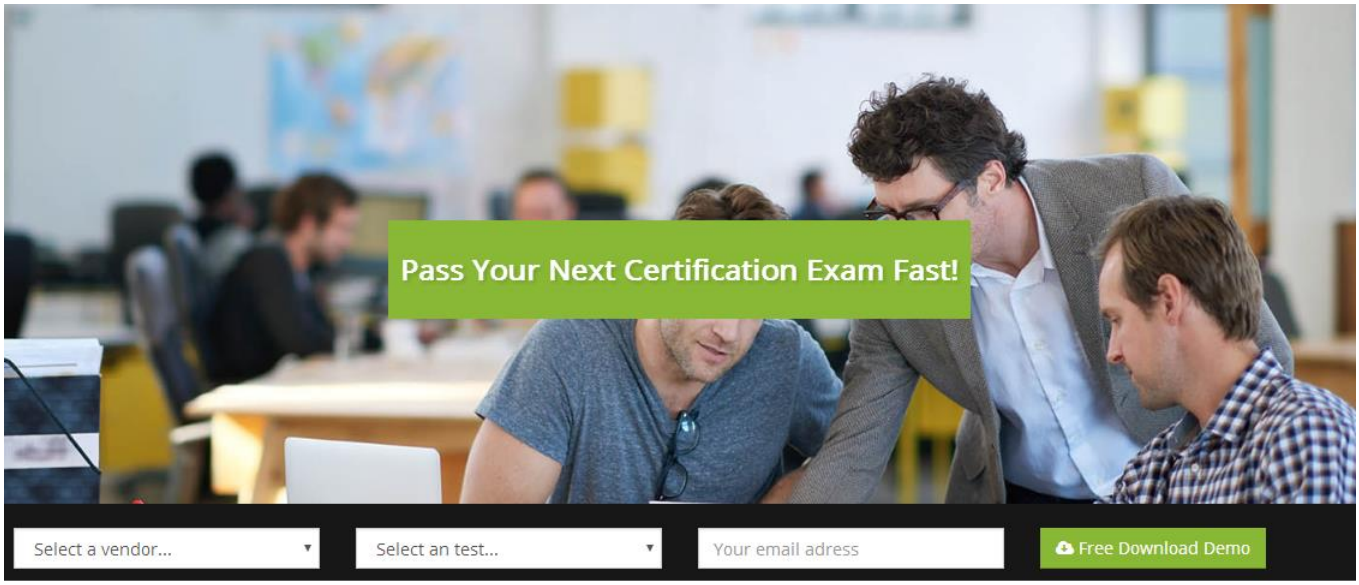
ITPassLeader



Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.itpassleader.com

High-praise Exam Dumps Questions grant you success by high pass rate - ITPassLeader

Exam : **CPTIA**

Title : CREST Practitioner Threat Intelligence Analyst

Vendor : CREST

Version : DEMO

NO.1 James is working as an incident responder at CyberSol Inc. The management instructed James to investigate a cybersecurity incident that recently happened in the company. As a part of the investigation process, James started collecting volatile information from a system running on Windows operating system.
Which of the following commands helps James in determining all the executable files for running processes?
A. cate A &. time ,/t
B. netstat -ab
C. top
D. doskey/history
Answer: B
Explanation:
Thenetstat -abcommand is useful in Windows operating systems for displaying all connections and listening ports, along with the executable involved in creating each connection or listening port. This can be particularly valuable for an incident responder like James when attempting to determine which processes are running on a system and how they are communicating over the network. This information can help identify malicious processes, unauthorized connections, or other signs of compromise on the system. Whilenetstat -ab does not exclusively list executable files for running processes, it ties processes to network activity, which is a critical part of collecting volatile information during a cybersecurity incident investigation.
References:The Certified Incident Handler (CREST CPTIA) course by EC-Council covers various commands and tools that can be used to collect volatile data from systems as part of incident response activities, highlighting the importance of understanding network connections and the processes responsible for them.

NO.2 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:
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.References:
* "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

NO.3 Which of the following risk mitigation strategies involves execution of controls to reduce the risk factor and brings it to an acceptable level or accepts the potential risk and continues operating the IT system?

A. Risk assumption

B. Risk avoidance

C. Risk planning

D. Risk transference

Answer: A

Explanation:
Risk assumption involves accepting the potential risk and continuing to operate the IT system while implementing controls to reduce the risk to an acceptable level. This strategy acknowledges that some level of risk is inevitable and focuses on managing it through mitigation measures rather than eliminating it entirely.
Risk avoidance would entail taking actions to avoid the risk entirely, risk planning involves preparing for potential risks, and risk transference shifts the risk to another party, typically through insurance or outsourcing. Risk assumption is a pragmatic approach that balances the need for operational continuity with the imperative of risk management.References:The CREST program covers various risk mitigation strategies, emphasizing the selection of the appropriate approach based on the organization's risk tolerance and the specific context of the threat.

NO.4 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

Answer: A

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.References:
* "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

NO.5 Johnson an incident handler is working on a recent web application attack faced by the organization. As part of this process, he performed data preprocessing in order to analyzing and detecting the watering hole attack. He preprocessed the outbound network traffic data collected from firewalls and proxy servers and started analyzing the user activities within a certain time period to create time-ordered domain sequences to perform further analysis on sequential patterns.
Identify the data-preprocessing step performed by Johnson.

A. Filtering invalid host names

B. Identifying unpopular domains

C. Host name normalization

D. User-specific sessionization

Answer: D

Explanation:
The data preprocessing step performed by Johnson, where he analyzes user activities within a certain time period to create time-ordered domain sequences for further analysis on sequential patterns, is known as user- specific sessionization. This process involves aggregating all user activities and requests into discrete sessions based on the individual user, allowing for a coherent analysis of user behavior over time. This is critical for identifying patterns that may indicate a watering hole attack, where attackers compromise a site frequently visited by the target group to distribute malware. User-specific sessionization helps in isolating and examining sequences of actions taken by users, making it easier to detect anomalies or patterns indicative of such an attack.References:The CREST materials discuss various data preprocessing techniques used in the analysis of cyber attacks, including the concept of sessionization to better understand user behavior and detect threats.

NO.6 Sarah is a security operations center (SOC) analyst working at JW Williams and Sons organization based in Chicago. As a part of security operations, she contacts information providers (sharing partners) for gathering information such as collections of validated and prioritized threat indicators along with a detailed technical analysis of malware samples, botnets, DDoS attack methods, and various other malicious tools. She further used the collected information at the tactical and operational levels.
Sarah obtained the required information from which of the following types of sharing partner?

A. Providers of threat data feeds

B. Providers of threat indicators

C. Providers of comprehensive cyber-threat intelligence

D. Providers of threat actors

Answer: C

Explanation:
The information Sarah is gathering, which includes collections of validated and prioritized threat indicators along with detailed technical analysis of malware samples, botnets, DDoS methods, and other malicious tools, indicates that she is obtaining this intelligence from providers of comprehensive cyber-threat intelligence.
These providers offer a holistic view of the threat landscape, combining tactical and operational threat data with in-depth analysis and context, enabling security teams to make informed decisions

and strategically enhance their defenses.References:
* "Cyber Threat Intelligence Providers: How to Choose the Right One for Your Organization," by CrowdStrike
* "The Role of Comprehensive Cyber Threat Intelligence in Effective Cybersecurity Strategies," by FireEye

NO.7 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:
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.References:
* "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

NO.8 Tracy works as a CISO in a large multinational company. She consumes threat intelligence to understand the changing trends of cyber security. She requires intelligence to understand the current business trends and make appropriate decisions regarding new technologies, security budget, improvement of processes, and staff.
The intelligence helps her in minimizing business risks and protecting the new technology and business initiatives.
Identify the type of threat intelligence consumer is Tracy.
A. Tactical users
B. Strategic users
C. Operational users
D. Technical users
Answer: B
Explanation:
Tracy, as a Chief Information Security Officer (CISO), requires intelligence that aids in understanding broader business and cybersecurity trends, making informed decisions regarding new technologies, security budgets, process improvements, and staffing. This need aligns with the role of a strategic

user of threat intelligence. Strategic users leverage intelligence to guide long-term planning and decision-making, focusing on minimizing business risks and safeguarding against emerging threats to new technology and business initiatives. This type of intelligence is less about the technical specifics of individual threats and more about understanding the overall threat landscape, regulatory environment, and industry trends to inform high-level strategy and policy.References:
* "The Role of Strategic Intelligence in Cybersecurity," Journal of Cybersecurity Education, Research and Practice
* "Cyber Threat Intelligence and the Lessons from Law Enforcement," by Robert M. Lee and David Bianco, SANS Institute Reading Room

NO.9 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:
For intelligence to be effectively disseminated and utilized by consumers, it must be presented in a manner that is concise, accurate, easily understandable, and engaging. This involves a careful balance of narrative, numerical data, tables, graphics, and potentially multimedia elements to convey the information clearly and compellingly. The right presentation takes into account the preferences and needs of the intelligence consumers, as well as the context andurgency of the information. By focusing on how the intelligence is presented, the analyst ensures that the content is not only consumed but also actionable, facilitating informed decision-making.

NO.10 Which of the following is not a countermeasure to eradicate cloud security incidents?
A. Patch the database vulnerabilities and improve the isolation mechanism
B. Remove the malware files and traces from the affected components
C. Check for data protection at both design and runtime
D. Disable security options such as two factor authentication and CAPTCHA
Answer: D
Explanation:
Disabling security options such as two-factor authentication (2FA) and CAPTCHA is not a countermeasure to eradicate cloud security incidents. In fact, it is contrary to best security practices. 2FA adds an additional layer of security by requiring two forms of verification before granting access to an account or system. CAPTCHA helps prevent automated attacks by ensuring that the entity accessing the service is human. Both are important security measures that protect against unauthorized access and automated attacks, thereby enhancing cloud security.

NO.11 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 (CSRF or XSRF) is an attack that tricks the victim's browser into executing unauthorized actions on a website where they are currently authenticated. In this scenario, the attacker exploits the trust that a site has in the user's browser, effectively forcing the browser to perform actions without the user's knowledge or consent. For example, if the user is logged into their bank's website, an attacker could craft a malicious request to transfer funds without the user's direct interaction. CSRF attacks rely on authenticated sessions and typically target state-changing requests to compromise user or application data.

References:The Certified Incident Handler (CREST CPTIA) curriculum by EC-Council discusses various web-based attacks, including CSRF, detailing their mechanisms, implications, and preventive measures to safeguard against such threats.

NO.12 Allan performed a reconnaissance attack on his corporate network as part of a red-team activity. He scanned the IP range to find live host IP addresses. What type of technique did he use to exploit the network?

A. DNS foot printing

B. Social engineering

C. Port scanning

D. Ping sweeping

Answer: D

Explanation:

Ping sweeping is a technique used in network reconnaissance to identify which IP addresses in a range are active or live. By sending ICMP echo requests ("ping") to multiple hosts and observing which ones respond, an attacker or, in this case, a red team member like Allan, can determine which systems are up and potentially vulnerable to further exploration or attack. This method is foundational for mapping the network before deploying more targeted exploits or scans.

References:EC-Council's Certified Incident Handler (CREST CPTIA) program discusses various reconnaissance techniques, including ping sweeping, as a preliminary step in network analysis and vulnerability assessment.

NO.13 In which of the following attacks does the attacker exploit vulnerabilities in a computer application before the software developer can release a patch for them?

A. Active online attack

B. Zero-day attack

C. Distributed network attack

D. Advanced persistent attack

Answer: B

Explanation:

A zero-day attack exploits vulnerabilities in software or hardware that are unknown to the vendor or for which a patch has not yet been released. These attacks are particularly dangerous because they take advantage of the window of time between the vulnerability's discovery and the availability of a fix, leaving systems exposed to potential exploitation. Zero-day attacks require a proactive and comprehensive approach to security, including the use of advanced threat detection systems and threat intelligence to identify and mitigate potential threats before they can be exploited.References:
* "Understanding Zero-Day Exploits," by MITRE
* "Zero-Day Threats: What They Are and How to Protect Against Them," by Symantec

NO.14 An incident handler is analyzing email headers to find out suspicious emails.
Which of the following tools he/she must use in order to accomplish the task?

A. Barracuda Email Security Gateway

B. Gophish

C. SPAMfighter

Answer: A

Explanation:
The Barracuda Email Security Gateway is designed to manage and filter inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. As an incident handler analyzing email headers to find out suspicious emails, using a tool like the Barracuda Email Security Gateway would be appropriate. This tool can help identify and block spam, phishing, malware, and other malicious email threats, making it easier to focus on analyzing potentially harmful emails more closely.