Eccouncil 312-85 Practice Questions

Shared by Dillon on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.

Which of the following sources of intelligence did the analyst use to collect information?

Options:

A- OPSEC
B- ISAC
C- OSINT
D- SIGINT

Answer:

C

Explanation:

The analyst used Open Source Intelligence (OSINT) to gather information from publicly available sources. OSINT involves collecting and analyzing information from publicly accessible sources to produce actionable intelligence. This can include media reports, public government data, professional and academic publications, and information available on the internet. OSINT is widely used for national security, law enforcement, and business intelligence purposes, providing a rich source of information for making informed decisions and understanding the threat landscape. Reference:

'Open Source Intelligence (OSINT) Tools and Techniques,' by SANS Institute

'The Role of OSINT in Cybersecurity and Threat Intelligence,' by Recorded Future

Question 2

Question Type: MultipleChoice

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?

Options:

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

Answer:

D

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 3

Question Type: MultipleChoice

H&P, Inc. is a small-scale organization that has decided to outsource the network security monitoring due to lack of resources in the organization. They are looking for the options where they can directly incorporate threat intelligence into their existing network defense solutions.

Which option best is the most cost-effective methods the organization can employ?

Options:

A- Recruit the right talent
B- Look for an individual within the organization
C- Recruit data management solution provider
D- Recruit managed security service providers (MSSP)

Answer:

D

Explanation:

For H&P, Inc., a small-scale organization looking to outsource network security monitoring and incorporate threat intelligence into their network defenses cost-effectively, recruiting a Managed Security Service Provider (MSSP) would be the most suitable option. MSSPs offer a range of services including network security monitoring, threat intelligence, incident response, and compliance management, often at a lower cost than maintaining an in-house security team. This allows organizations to benefit from expert services and advanced security technologies without the need for significant resource investment. Reference:

'The Benefits of Managed Security Services,' by Gartner

'How to Choose a Managed Security Service Provider (MSSP),' by CSO Online

Question 4

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

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 5

Question Type: MultipleChoice

Sam works as an analyst in an organization named InfoTech Security. He was asked to collect information from various threat intelligence sources. In meeting the deadline, he forgot to verify the threat intelligence sources and used data from an open-source data provider, who offered it at a very low cost. Through it was beneficial at the initial stage but relying on such data providers can produce unreliable data and noise putting the organization network into risk.

What mistake Sam did that led to this situation?

Options:

A- Sam used unreliable intelligence sources.
B- Sam used data without context.
C- Sam did not use the proper standardization formats for representing threat data.
D- Sam did not use the proper technology to use or consume the information.

Answer:

A

Explanation:

Sam's mistake was using threat intelligence from sources that he did not verify for reliability. Relying on intelligence from unverified or unreliable sources can lead to the incorporation of inaccurate, outdated, or irrelevant information into the organization's threat intelligence program. This can result in 'noise,' which refers to irrelevant or false information that can distract from real threats, and potentially put the organization's network at risk. Verifying the credibility and reliability of intelligence sources is crucial to ensure that the data used for making security decisions is accurate and actionable. Reference:

'Best Practices for Threat Intelligence Sharing,' by FIRST (Forum of Incident Response and Security Teams)

'Evaluating Cyber Threat Intelligence Sources,' by Jon DiMaggio, SANS Institute InfoSec Reading Room

Question 6

Question Type: MultipleChoice

A threat analyst wants to incorporate a requirement in the threat knowledge repository that provides an ability to modify or delete past or irrelevant threat data.

Which option best requirement must he include in the threat knowledge repository to fulfil his needs?

Options:

A- Protection ranking
B- Evaluating performance
C- Data management
D- Searchable functionality

Answer:

C

Explanation:

Incorporating a data management requirement in the threat knowledge repository is essential to provide the ability to modify or delete past or irrelevant threat data. Effective data management practices ensure that the repository remains accurate, relevant, and up-to-date by

allowing for the adjustment and curation of stored information. This includes removing outdated intelligence, correcting inaccuracies, and updating information as new insights become available. A well-managed repository supports the ongoing relevance and utility of the threat intelligence, aiding in informed decision-making and threat mitigation strategies. Reference:

'Building and Maintaining a Threat Intelligence Library,' by Recorded Future

'Best Practices for Creating a Threat Intelligence Policy, and How to Use It,' by SANS Institute

Question 7

Question Type: MultipleChoice

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?

Options:

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 and urgency 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.

Question 8

Question Type: MultipleChoice

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?

Options:

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. Reference:

'Understanding Zero-Day Exploits,' by MITRE

'Zero-Day Threats: What They Are and How to Protect Against Them,' by Symantec

Question 9

Question Type: MultipleChoice

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 option best categories of threat intelligence feed was acquired by Jian?

Options:

A- Internal intelligence feeds
B- External intelligence feeds
C- CSV data feeds
D- Proactive surveillance feeds

Answer:

A

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 10

Question Type: MultipleChoice

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?

Options:

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)

Answer:

A

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 11

Question Type: MultipleChoice

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.

Options:

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:

B

Explanation:

ABC cyber-security company, which has implemented automation for tasks such as data enrichment and indicator aggregation and has joined various communities to increase knowledge about emerging threats, is demonstrating characteristics of a Level 3 maturity in the threat intelligence maturity model. At this level, organizations have a formal Cyber Threat Intelligence (CTI) program in place, with processes and tools implemented to collect, analyze, and integrate threat intelligence into their security operations. Although they may still be reactive in detecting and preventing threats, the existence of structured CTI capabilities indicates a more developed stage of threat intelligence maturity. Reference:

'Building a Threat Intelligence Program,' by Recorded Future

'The Threat Intelligence Handbook,' by Chris Pace, Cybersecurity Evangelist at Recorded Future

Question 12

Question Type: MultipleChoice

Which option best characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

Options:

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

Answer:

D

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