Actual exam question from ECCouncil's 312-85

Question #: 1

Topic #: 1

[All 312-85 Questions]

Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.

Daniel comes under which of the following types of threat actor.

A. Industrial spies

B. State-sponsored hackers

C. Insider threat

D. Organized hackers

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 2

Topic #: 1

[All 312-85 Questions]

An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.

Which of the following technique is used by the attacker?

A. DNS zone transfer

B. Dynamic DNS

C. DNS interrogation

D. Fast-Flux DNS

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 3

Topic #: 1

[All 312-85 Questions]

Kathy wants to ensure that she shares threat intelligence containing sensitive information with the appropriate audience. Hence, she used traffic light protocol (TLP). Which TLP color would you signify that information should be shared only within a particular community?

A. Red

B. White

C. Green

D. Amber

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 4

Topic #: 1

[All 312-85 Questions]

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 organization'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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 5

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 6

Topic #: 1

[All 312-85 Questions]

Miley, an analyst, wants to reduce the amount of collected data and make the storing and sharing process easy. She uses filtering, tagging, and queuing technique to sort out the relevant and structured data from the large amounts of unstructured data.

Which of the following techniques was employed by Miley?

A. Sandboxing

B. Normalization

C. Data visualization

D. Convenience sampling

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 7

Topic #: 1

[All 312-85 Questions]

Bob, a threat analyst, works in an organization named TechTop. He was asked to collect intelligence to fulfil the needs and requirements of the Red Tam present within the organization.

Which of the following are the needs of a RedTeam?

A. Intelligence related to increased attacks targeting a particular software or operating system vulnerability

B. Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)

C. Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs

D. Intelligence that reveals risks related to various strategic business decisions

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 8

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 9

Topic #: 1

[All 312-85 Questions]

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?

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)

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 10
Topic #: 1
[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 11

Topic #: 1

[All 312-85 Questions]

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.

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 12
Topic #: 1
[All 312-85 Questions]

Andrews and Sons Corp. has decided to share threat information among sharing partners. Garry, a threat analyst, working in Andrews and Sons Corp., has asked to follow a trust model necessary to establish trust between sharing partners. In the trust model used by him, the first organization makes use of a body of evidence in a second organization, and the level of trust between two organizations depends on the degree and quality of evidence provided by the first organization.
Which of the following types of trust model is used by Garry to establish the trust?

A. Mediated trust
B. Mandated trust
C. Direct historical trust
D. Validated trust

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 13

Topic #: 1

[All 312-85 Questions]

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

C. Distributed Denial-of-Service (DDoS) attack

D. Bandwidth attack

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 14

Topic #: 1

[All 312-85 Questions]

Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.

Which of the following phases of cyber kill chain methodology is Jame executing?

A. Reconnaissance

B. Installation

C. Weaponization

D. Exploitation

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 15
Topic #: 1
[All 312-85 Questions]

Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.
Which of the following key indicators of compromise does this scenario present?

A. Unusual outbound network traffic

B. Unexpected patching of systems

C. Unusual activity through privileged user account

D. Geographical anomalies

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 16

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 17

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 18

Topic #: 1

[All 312-85 Questions]

Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

A. Nation-state attribution

B. True attribution

C. Campaign attribution

D. Intrusion-set attribution

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 19
Topic #: 1
[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 20

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 21

Topic #: 1

[All 312-85 Questions]

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. Internal intelligence feeds

B. External intelligence feeds

C. CSV data feeds

D. Proactive surveillance feeds

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 22

Topic #: 1

[All 312-85 Questions]

Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?

A. Repeater

B. Gateway

C. Hub

D. Network interface card (NIC)

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 23

Topic #: 1

[All 312-85 Questions]

What is the correct sequence of steps involved in scheduling a threat intelligence program?

1. Review the project charter
2. Identify all deliverables
3. Identify the sequence of activities
4. Identify task dependencies
5. Develop the final schedule
6. Estimate duration of each activity
7. Identify and estimate resources for all activities
8. Define all activities
9. Build a work breakdown structure (WBS)

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 24

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 25
Topic #: 1
[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 26

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 27
Topic #: 1
[All 312-85 Questions]

Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.
What stage of ACH is Bob currently in?

A. Diagnostics
B. Evidence
C. Inconsistency
D. Refinement

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 28
Topic #: 1
[All 312-85 Questions]

Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header.
Connection status and content type
Accept-ranges and last-modified information

X-powered-by information -
Web server in use and its version
Which of the following tools should the Tyrion use to view header content?

A. Hydra

B. AutoShun

C. Vanguard enforcer

D. Burp suite

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 29

Topic #: 1

[All 312-85 Questions]

Joe works as a threat intelligence analyst with Xsecurity Inc. He is assessing the TI program by comparing the project results with the original objectives by reviewing project charter. He is also reviewing the list of expected deliverables to ensure that each of those is delivered to an acceptable level of quality.
Identify the activity that Joe is performing to assess a TI program's success or failure.

A. Determining the fulfillment of stakeholders

B. Identifying areas of further improvement

C. Determining the costs and benefits associated with the program

D. Conducting a gap analysis

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 30

Topic #: 1

[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85
Question #: 31
Topic #: 1
[All 312-85 Questions]

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

Show Suggested Answer

Actual exam question from ECCouncil's 312-85

Question #: 32

Topic #: 1

[All 312-85 Questions]

An organization suffered many major attacks and lost critical information, such as employee records, and financial information. Therefore, the management decides to hire a threat analyst to extract the strategic threat intelligence that provides high-level information regarding current cyber-security posture, threats, details on the financial impact of various cyber-activities, and so on.

Which of the following sources will help the analyst to collect the required intelligence?

A. Active campaigns, attacks on other organizations, data feeds from external third parties

B. OSINT, CTI vendors, ISAO/ISACs

C. Campaign reports, malware, incident reports, attack group reports, human intelligence

D. Human, social media, chat rooms

Show Suggested Answer