Question #1 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D
As per Module 02 Page 92 of CTIA Courseware
upvoted 3 times

Question #2 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

3bc35a7 3 months, 2 weeks ago

Now pg. 403

upvoted 1 times

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answere is D

As per Module 04 Page 314 of CTIA Courseware

upvoted 2 times

Anzk 1 year, 3 months ago

ANSWER IS D

PG 314

upvoted 2 times

Question #3 *Topic 1*

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

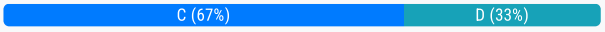
B. White

C. Green

D. Amber

Suggested Answer: *D*

Community vote distribution



3bc35a7 3 months, 2 weeks ago
I think sensitive and particular community is key here and would lead you to answer Amber. If data is sensitive, you wouldn't share with a partner community as noted with Green.
upvoted 2 times

Pragdeashwar 7 months, 3 weeks ago
Selected Answer: C
Answer is C as per CTIA (page 584)
upvoted 3 times

fmerlone 9 months, 2 weeks ago
green for community ; amber for organization
upvoted 3 times

azera_exl 9 months, 3 weeks ago
Selected Answer: D
Has anyone confirmed the answer is actually C? As it mentions 'sensitive information', I am inclined to agree with emoram, even though it mentions 'community'. TLP GREEN is for awareness only, with no 'risk to privacy, reputation, or operations if shared outside of the organization[s] involved'.
upvoted 2 times

MascaCri 11 months ago
Answer is C as per CTIA (page 584)
upvoted 1 times

BionicBeaver 1 year, 3 months ago
Selected Answer: C
Answer is C
As per Module 06 Page 584 of CTIA Courseware
upvoted 1 times

emoram 1 year, 8 months ago
I think the key part here is the sensitive data explicitly mentioned on the question, and therefore it is amber due to the implicit risk it represents on sharing that information with the wrong audience. Green is for awareness. Pag 584 in ECC material
upvoted 2 times

jojo2k 2 years, 1 month ago
Its actually green. if you read the definition of TLP green it mentions that "limited disclosure, Restricted to community only"
upvoted 4 times

emoram 1 year, 8 months ago
I think the key part here is the sensitive data explicitly mentioned on the question, and therefore it is amber due to the implicit risk it represents on sharing that information with the wrong audience. Green is for awareness. Pag 584 in ECC material
upvoted 1 times

pinguin666 2 years ago

Correct GREEN. Amber is for only org, clients or customers. page 584 in EC material BTW

upvoted 2 times

Question #4 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: A

Answer is A

As per Module 04 Page 282 of CTIA Courseware

upvoted 2 times

Alapo 1 year, 5 months ago

A is correct because the question requested for similar websites

upvoted 2 times

Question #5 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: C

Answer is C
As per Module 05 Page 420 of CTIA Courseware
upvoted 2 times

Question #6 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: B

Answer is B

As per Module 04 Page 387 of CTIA Courseware

upvoted 2 times

Question #7 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: B

Answer is B

As per Module 06 Page 516 of CTIA Courseware

upvoted 2 times

Anzk 1 year, 3 months ago

answer is B

pg 516

upvoted 2 times

Question #8 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: C

Answer is C

As per Module 01 Page 15 of CTIA Courseware

upvoted 2 times

Anzk 1 year, 3 months ago

correct answer is c

pg 15

upvoted 1 times

Question #9 *Topic 1*

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)

Suggested Answer: *B*

Community vote distribution

A (100%)

pinguin666 Highly Voted 2 years ago

Selected Answer: A

Method described is PASSIVE DNS monitoring page 335 module 4

upvoted 5 times

3bc35a7 Most Recent 3 months, 2 weeks ago

PASSIVE DNS monitoring, now page 426.

upvoted 1 times

AbdallaAli 5 months, 1 week ago

Selected Answer: A

It is a passive DNS as described in the Book

upvoted 2 times

BionicBeaver 1 year, 3 months ago

Selected Answer: A

Answer is A

As per Module 04 Page 335 of CTIA Courseware

upvoted 2 times

keloki2020 1 year, 4 months ago

It is Passive DNS Monitoring.

"Passive DNS monitoring is a cyber counterintelligence mechanism where a recursive DNS server is employed to perform inter-server DNS communication.

"

upvoted 1 times

LordXander 1 year, 7 months ago

Selected Answer: A

Passive DNS monitoring is a counterintelligence mechanism

upvoted 2 times

jojo2k 2 years, 1 month ago

Passive DNS monitoring is a counterintelligence mechanism where a recursive DNS server is
employed to perform inter-server DNS communication. When a request is generated from any name server to the recursive DNS server, the recursive DNS server logs the responses that are received. Then it replicates the logged data and stores the data in the central database.

upvoted 3 times

Question #10 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

sunce12 5 months ago
C correct ECC page 102
upvoted 1 times

BionicBeaver 1 year, 3 months ago
Selected Answer: C
Answer is C
As per Module 02 Page 102 of CTIA Courseware
upvoted 2 times

Alapo 1 year, 4 months ago
C correct ECC page 102
upvoted 1 times

Question #11 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: C

Answer is C
As per Module 02 Page 116 of CTIA Courseware

upvoted 1 times

emoram 1 year, 8 months ago

Asper the ECC material the right answer is C, however this question could be appealable as in real life data can be stolen/exfiltrated through CnC servers and DNS tunneling which could be detected/mitigated by some sort of DNS solution checking on DNS queries integrity and suspicious domains. As stated by answer B.

upvoted 1 times

Question #12 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D

As per Module 06 Page 566 of CTIA Courseware

upvoted 1 times

Boats 1 year, 6 months ago

http://fismapedia.org/index.php/NIST_SP_800-39_Appendix_G

upvoted 1 times

Question #13 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

sunce12 5 months ago

Answer is C

As per Module 01 Page 8 of CTIA Courseware

upvoted 1 times

BionicBeaver 1 year, 3 months ago

Selected Answer: C

Answer is C

As per Module 01 Page 8 of CTIA Courseware

upvoted 2 times

Anzk 1 year, 3 months ago

answer is c

pf 8

upvoted 1 times

Question #14 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: C

Answer is C

As per Module 02 Page 106 of CTIA Courseware

upvoted 1 times

Anzk 1 year, 3 months ago

answer is c

pg 106

upvoted 1 times

Question #15 *Topic 1*

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

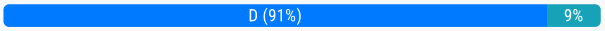
B. Unexpected patching of systems

C. Unusual activity through privileged user account

D. Geographical anomalies

Suggested Answer: *C*

Community vote distribution



Bigbear246 Highly Voted 2 years, 1 month ago

The correct answer is D - Geographical Anomalies:
• Geographical anomalies: Analyst monitor the network access and collect the data related to access requests from unidentified and unusual geographical locations. The unusual login or access request from the geographical locations where the organization has no usual business to carry out indicates compromise in the network.

upvoted 5 times

BionicBeaver Most Recent 1 year, 3 months ago

Selected Answer: D

Answer is D
As per Module 04 Page 355 of CTIA Courseware

upvoted 1 times

[Removed] 1 year, 3 months ago

Selected Answer: D

Answer is D.
As per Module 02 Page 126 of ECC Courseware

upvoted 2 times

Anzk 1 year, 3 months ago

Answer is D. reference on page 126 EC Council courseware.

upvoted 2 times

keloki2020 1 year, 4 months ago

Answer is D: Geographical Anomalies
"Geographical Anomalies
Irregular login patterns can be used as evidence of compromise. Login attempts from locations where the organization does not have business relations resemble that confidential information being stolen. Analyzing multiple logins from different locations in a short time span tagged with the location may reveal evidence of compromise.
"

upvoted 1 times

LordXander 1 year, 7 months ago

Selected Answer: C

No mention of a privileged accpint

upvoted 1 times

Art007 1 year, 9 months ago

Selected Answer: D

Would also have to go with Geographical anomalies as there is no mention of privileged accounts in the question and the logins come from multiple geographical locations.

upvoted 3 times

pinguin666 2 years ago

Selected Answer: D

Geographical anomalies as it comes from multiple countries and loacations. Nothing mentioned about PRIVILEGED account either.

upvoted 4 times

Question #16 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: C

Answer is C

As per Module 02 Page 99 of CTIA Courseware

upvoted 1 times

ech 1 year, 4 months ago

EC-Council Material reference for attack origination points

They refer to numerous attempts done to gain entry to the target's network. This point of entry can be used to gain access to the network and launch further attacks. To succeed in gaining initial access, the attacker needs to perform exhaustive research to identify the vulnerabilities and gatekeeper functions in the target network.

Numbers Involved in the Attack It is defined as a number of host systems that are involved in the attack. APT attacks are usually carried out by a crime group or crime organization.

upvoted 1 times

Boats 1 year, 6 months ago

Selected Answer: C

https://www.cimcor.com/blog/14-telltale-characteristics-of-an-advanced-persistent-threat

Attack Origination Points

Multiple attempts at gaining a point of entry may be launched to gain an initial presence within a network, though first attempts are typically sufficiently well-researched to be successful. Months of research can culminate in the full knowledge of your network's vulnerabilities as well as the human gatekeepers within your organization.

upvoted 2 times

Question #17 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: C

Answer is C
As per Module 05 Page 460 of CTIA Courseware
upvoted 1 times

Anzk 1 year, 3 months ago

ec council ref page 460. Octave is the right answer
upvoted 1 times

Question #18 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: B

Answer is B

As per Module 05 Page 489 of CTIA Courseware

upvoted 2 times

Alapo 1 year, 4 months ago

B correct check page 489 ECC council material

upvoted 1 times

Boats 1 year, 6 months ago

Selected Answer: B

https://info-savvy.com/what-is-threat-assessment/

Discussed below are different types of attributions:

– Group Attribution: It deals with attributing based on the common group or association of multiple malicious actors and their attack methodologies.

– Campaign Attribution: It deals with attributing based on the malware or the campaign strategy of specific malware.

– Intrusion-set Attribution: It deals with attributing the attacker based on the intrusion patterns.

– True Attribution: it deals with the identification of a specific person, society, or country sponsored g a well-planned and executed intrusion or attack over its target.

– Nation-state Attribution: It deals with the attribution of attacks that are sponsored by any nation against another nation

upvoted 3 times

Question #19 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

A (100%)

emoram Highly Voted 1 year, 8 months ago

The right answer is A) Game Theory. The description is on pag 474 on the ECC material

upvoted 6 times

BionicBeaver Most Recent 1 year, 3 months ago

Selected Answer: A

Answer is A

As per Module 05 Page 474 of CTIA Courseware

upvoted 1 times

[Removed] 1 year, 3 months ago

Selected Answer: A

Answer is A

As per Module 05 Page 474 of ECC Courseware

upvoted 2 times

kelie 1 year, 3 months ago

Selected Answer: A

Right Answer is A

upvoted 2 times

Alapo 1 year, 4 months ago

A correct

upvoted 1 times

Question #20 *Topic 1*

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

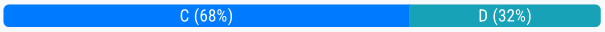
B. Planning and direction

C. Processing and exploitation

D. Analysis and production

Suggested Answer: *A*

Community vote distribution



pinguin666 Highly Voted 2 years ago

Selected Answer: C

page 48: Processing and Exploitation
 Process raw data for exploitation Convert processed data into usable format for data analysis
upvoted 11 times

Bigbear246 Highly Voted 2 years, 1 month ago

The correct answer is C - Processing and Exploitation
Data processing and exploitation are key tasks of an analyst where he/she has to reduce the collected data into useful and reliable information that can be further used in threat analysis.
Data processing and exploitation deal with the following tasks:
• Structuring/normalization of collected data
• Storing and data visualization
• Sharing the threat information
upvoted 8 times

vikask13 Most Recent 8 months, 1 week ago

Answer: D - Analysis and Production (Page 48) COnverting raw data in to information with machine learning and statistical methods
upvoted 1 times

azera_exl 9 months, 3 weeks ago

Selected Answer: C

The analysts are 'converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods'. Page 48 states 'Processing and Exploitation' processes raw data and converts processed data into a usable format.
upvoted 1 times

upichi 11 months, 1 week ago

D. Analysis and production | Page 49
Keywords: machine-based techniques, and statistical methods.
upvoted 1 times

Kezuko 11 months, 1 week ago

Selected Answer: C

C, cause just started
upvoted 1 times

cybercypher 11 months, 3 weeks ago

Answer is D
upvoted 1 times

joaquinemege 1 year, 2 months ago

Selected Answer: C

at the phrase " the analysts started converting", "Started" is the key word, beacause they have not finished the activity yet

upvoted 2 times

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D

As per Module 01 Page 49 Certified Threat of CTIA Courseware

upvoted 2 times

[Removed] 1 year, 3 months ago

Selected Answer: D

Answer is D

As per Module 01 Page 49 of ECC Courseware

upvoted 3 times

[Removed] 1 year, 3 months ago

Selected Answer: C

Answer is C

As per Module 01 Page 48 of ECC Courseware

upvoted 2 times

Night_Hawk 1 year, 3 months ago

Selected Answer: D

Answer is D, ref page 48

upvoted 3 times

Anzk 1 year, 3 months ago

answer is D

page 48

upvoted 4 times

Question #21 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

D (100%)

clouddemohk Highly Voted 1 year, 12 months ago

D.Proactive surveillance feeds

Proactive surveillance feeds include information that is acquired using the real-time assessment of system activities and events. It enables appropriate defensive measures and immediate response to such activities. These feeds also enable the security teams to build defensive strategies in advance keeping in mind the possible intrusion attempts and securing the vulnerabilities visible in the system.
These sources include the following: o Honeynets o Malware forensics o Brand monitoring o P2P monitoring o DNS monitoring o Watchlist monitoring o Infrastructure and application logs

upvoted 9 times

rj8yy_8 Highly Voted 1 year, 8 months ago

The Correct answer is D Proactive Surveillance Feeds. in the ECC doc. Pg. 265 clouddemohk is correct

upvoted 5 times

Ernest123 Most Recent 11 months, 1 week ago

Selected Answer: D

D as per ECC materials

upvoted 2 times

defleppard89 1 year, 1 month ago

i agree with D

upvoted 1 times

TttPik 1 year, 1 month ago

D from pg. 265

upvoted 1 times

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D
As per Module 04 Page 266 of CTIA Courseware

upvoted 2 times

[Removed] 1 year, 3 months ago

Selected Answer: D

Answer is D
As per Module 04 Page 265 of Courseware

upvoted 2 times

Anzk 1 year, 3 months ago

answer is D

upvoted 2 times

Question #22 *Topic 1*

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)

Suggested Answer: *B*

Community vote distribution

B (100%)

TttPik 1 year, 1 month ago

B Page 144

upvoted 1 times

BionicBeaver 1 year, 3 months ago

Selected Answer: B

Answer is B

As per Module 03 Page 144 of CTIA Courseware

upvoted 3 times

Rch0 1 year, 3 months ago

B is correct

upvoted 1 times

Anzk 1 year, 3 months ago

answer is B

upvoted 1 times

Question #23 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: A

Answer is A

As per Module 03 Page 182 of CTIA Courseware

upvoted 1 times

[Removed] 1 year, 3 months ago

Selected Answer: A

Answare is A

As per Module 03 Page 182 of ECC Courseware

upvoted 2 times

Question #24 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

hoamee 7 months, 2 weeks ago
Cuckoo Sandbox: Malware data collection
OmniPeek: Network protocol analyzer
PortDroid network analysis
Blueliv: Threat intelligence provider
upvoted 1 times

TttPik 1 year, 1 month ago
Answer is D pg. 597
upvoted 1 times

BionicBeaver 1 year, 3 months ago
Selected Answer: D
Answer is D
As per Module 06 Page 597 of CTIA Courseware
upvoted 2 times

Rch0 1 year, 3 months ago
D blueliv
upvoted 2 times

Question #25 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D

As per Module 05 Page 434 of CTIA Courseware

upvoted 1 times

Anzk 1 year, 3 months ago

answer D

pg 434

upvoted 1 times

Question #26 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D

As per Module 03 Page 190 of CTIA Courseware

upvoted 3 times

Anzk 1 year, 3 months ago

correct answer d

page 190

upvoted 2 times

Question #27 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: A

Answer is A
As per Module 05 Page 421 of CTIA Courseware
upvoted 1 times

Anzk 1 year, 3 months ago

answer is A
upvoted 1 times

Alapo 1 year, 4 months ago

A correct check page 424 ECC material
upvoted 1 times

Question #28 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D
As per Module 04 Page 298 of CTIA Courseware
upvoted 2 times

Question #29 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: D

Answer is D
As per Module 03 Page 234 of CTIA Courseware
upvoted 1 times

Anzk 1 year, 3 months ago

answer D
Page 234
upvoted 1 times

Question #30 *Topic 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

Suggested Answer: *B*

Community vote distribution

B (100%)

BionicBeaver 1 year, 3 months ago

Selected Answer: B

Answer is B

As per Module 06 Page 524 of CTIA Courseware

upvoted 1 times

Alapo 1 year, 4 months ago

B correct check page 524 ECC material

upvoted 1 times