Eccouncil

CTIA

Certified Threat Intelligence Analyst (C|TIA)

QUESTION & ANSWERS

Question: 1

How you can deduce a great deal about adversaries' TTPs

A. Exchanges of information about new exploits and tools being developed

B. Discussions of plans and tactics on forums and social media sites

C. Purchases of tools and services

D. All of these

Answer: D

Question: 2

What does CrowdStrike Cyber Threat Intelligence Solution's Falcon product offers

A. indicators of compromise (IOCs)

B. snort/yara rules

C. All of these

D. automated investigations

Answer: C

Question: 3

What defines ThreatConnect® TC Complete

A. Security Operations and Analytics Platform

B. Threat Intelligence Platform (TIP)

C. Intelligence-Driven Orchestration

D. Intelligence Delivered with ThreatConnect

Answer: A

Question: 4

The Stuxnet worm, targeted

A. SMB

B. HTTPS

C. SCADA

D. FTP

Answer: C

Question: 5

What is not a part of the Diamond Model

A. Threat

B. Adversary

C. Infrastructure

D. Capabilities

Answer: a

Question: 6

What can be a source for observables in Yeti

A. malware trackers

B. XML feeds

C. MISP instances

D. All of these

Answer: D

Question: 7

What is not an export format for MISP

A. CSV

B. plain text

C. JSON

D. None of these

Answer: D

Question: 8

Identify the primary source of strategic CTI

A. hacker web forums, underground marketplace

B. All of these

C. Honeypot or scanner on network

D. statistical analysis of indicators

Answer: A

Question: 9

Triage for SIEM alerts by SOC analysts can be categorized as

A. All of these

B. Ignore

C. Escalate immediately to the incident response (IR) team

D. Investigate when time permits

Answer: A