KTest

更に上のクオリティ　更に上のサービス

問題集

1 / 3

Exam : **312-85**

Title : Certified Threat Intelligence Analyst

Version : DEMO

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
Answer: D

2.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)
Answer: B

3.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
Answer: C

4.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
Answer: A

5.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?
A. OPSEC
B. ISAC

C. OSINT
D. SIGINT
Answer: C