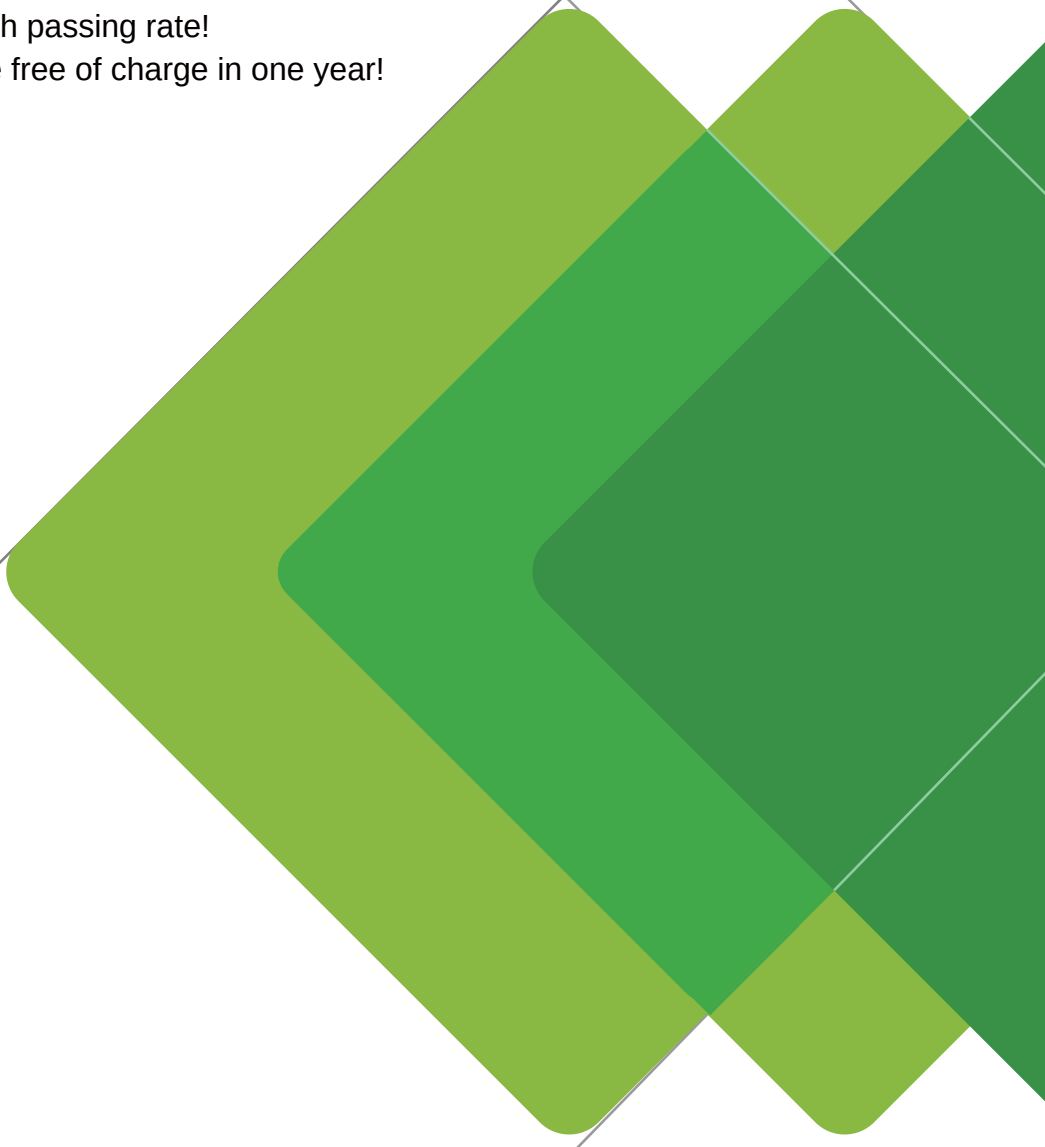
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

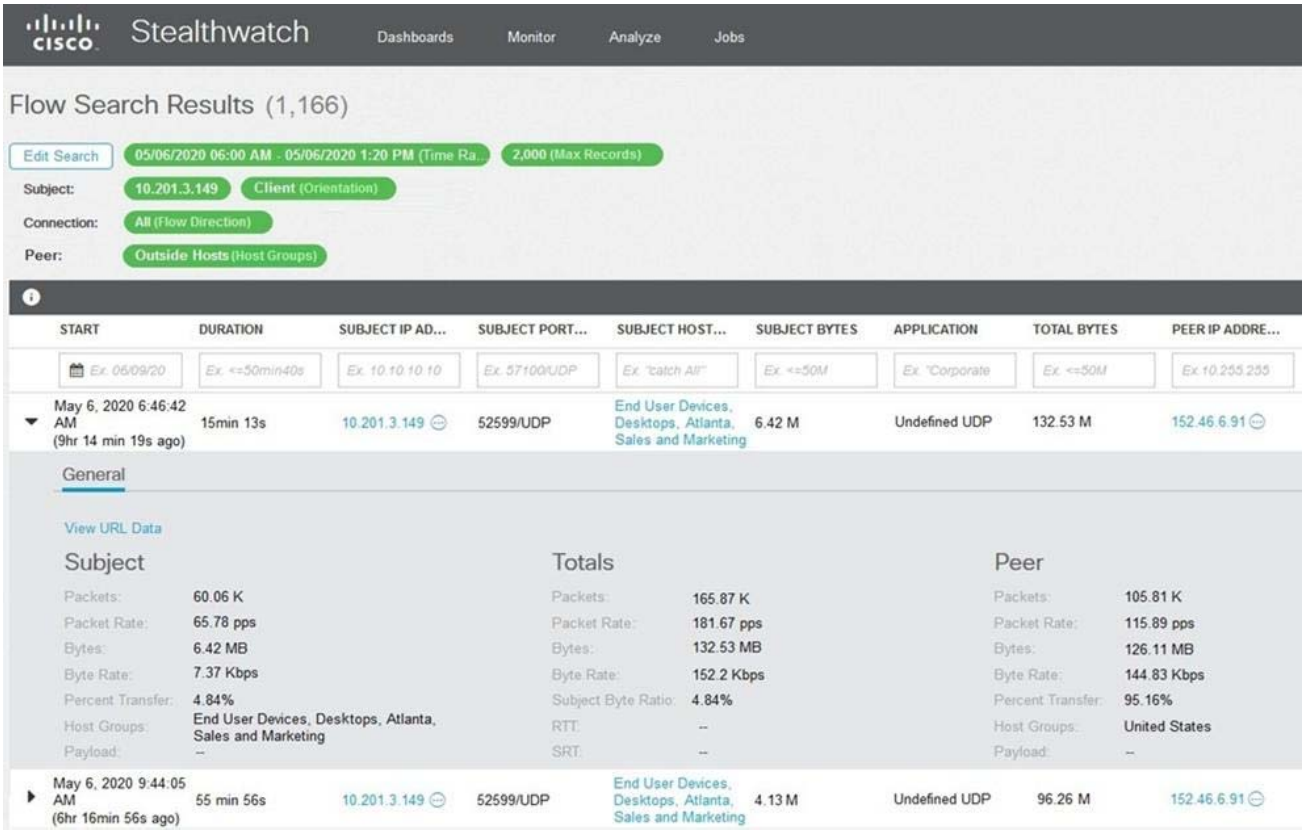


Exam : **200-201**

Title : Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Version : DEMO

1.Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?

A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.

B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.

C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.

D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

Answer: D

2.What does cyber attribution identify in an investigation?

A. cause of an attack

B. exploit of an attack

C. vulnerabilities exploited

D. threat actors of an attack

Answer: D

Explanation:

https://www.techtarget.com/searchsecurity/definition/cyber-attribution

3.Refer to the exhibit.

```
Aug 24 2020 09:02:37: %ASA-4-106023: Deny tcp src outside:209.165.200.228/51585 dst
inside:192.168.150.77/22 by access-group "OUTSIDE" [0x5063b82f, 0x0]
```

An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced.

How should this type of evidence be categorized?

A. indirect

B. circumstantial
C. corroborative
D. best
Answer: C
Explanation:
Indirect=circumstantail so there is no posibility to match A or B (only one answer is needed in this question). For suer it's not a BEST evidence - this FW data inform only of DROPPED traffic. If smth happend inside network, presented evidence could be used to support other evidences or make our narreation stronger but alone it's mean nothing.

4.What is a sandbox interprocess communication service?
A. A collection of rules within the sandbox that prevent the communication between sandboxes.
B. A collection of network services that are activated on an interface, allowing for inter-port communication.
C. A collection of interfaces that allow for coordination of activities among processes.
D. A collection of host services that allow for communication between sandboxes.
Answer: C
Explanation:
Inter-process communication (IPC) allows communication between different processes. A process is one or more threads running inside its own, isolated address space.
https://docs.legato.io/16_10/basicIPC.html

5.A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver.
Which event category is described?
A. reconnaissance
B. action on objectives
C. installation
D. exploitation
Answer: C