

# 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.

The screenshot shows the Cisco Stealthwatch interface. At the top, there are navigation tabs: Dashboards, Monitor, Analyze, and Jobs. Below this, the page title is "Flow Search Results (1,166)". There are several filters: "Edit Search", "05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Ra...)", and "2,000 (Max Records)". The search criteria are: Subject: 10.201.3.149 Client (Orientation); Connection: All (Flow Direction); Peer: Outside Hosts (Host Groups).

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...
May 6, 2020 6:46:42 AM (9hr 14 min 19s ago)	15min 13s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	6.42 M	Undefined UDP	132.53 M	152.46.6.91

Below the table, there is a "General" section with a "View URL Data" link. It shows statistics for Subject, Totals, and Peer:

Subject	Totals	Peer
Packets: 60.06 K	Packets: 165.87 K	Packets: 105.81 K
Packet Rate: 65.78 pps	Packet Rate: 181.67 pps	Packet Rate: 115.89 pps
Bytes: 6.42 MB	Bytes: 132.53 MB	Bytes: 126.11 MB
Byte Rate: 7.37 Kbps	Byte Rate: 152.2 Kbps	Byte Rate: 144.83 Kbps
Percent Transfer: 4.84%	Subject Byte Ratio: 4.84%	Percent Transfer: 95.16%
Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing	RTT: --	Host Groups: United States
Payload: --	SRT: --	Payload: --

Another flow entry is visible below:

May 6, 2020 9:44:05 AM (6hr 16min 56s ago)	55 min 56s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	4.13 M	Undefined UDP	96.26 M	152.46.6.91
--	------------	--------------	-----------	--	--------	---------------	---------	-------------

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=circumstantial so there is no possibility to match A or B (only one answer is needed in this question). For sure 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](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**