



Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1

Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

Answer: C

NEW QUESTION 2

What is the difference between deep packet inspection and stateful inspection?

- A. Deep packet inspection is more secure than stateful inspection on Layer 4
- B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
- C. Stateful inspection is more secure than deep packet inspection on Layer 7
- D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

Answer: D

NEW QUESTION 3

You have identified a malicious file in a sandbox analysis tool. Which piece of file information from the analysis is needed to search for additional downloads of this file by other hosts?

- A. file name
- B. file hash value
- C. file type
- D. file size

Answer: B

NEW QUESTION 4

What is a benefit of agent-based protection when compared to agentless protection?

- A. It lowers maintenance costs
- B. It provides a centralized platform
- C. It collects and detects all traffic locally
- D. It manages numerous devices simultaneously

Answer: B

NEW QUESTION 5

Which type of evidence supports a theory or an assumption that results from initial evidence?

- A. probabilistic
- B. indirect
- C. best
- D. corroborative

Answer: D

NEW QUESTION 6

Drag and drop the technology on the left onto the data type the technology provides on the right.

tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

NEW QUESTION 7

Refer to the exhibit.

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

- A. /var/log/authorization.log
- B. /var/log/dmesg
- C. var/log/var.log
- D. /var/log/auth.log

Answer: D

NEW QUESTION 8

Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 9

Which incidence response step includes identifying all hosts affected by an attack'?

- A. post-incident activity
- B. detection and analysis
- C. containment eradication and recovery
- D. preparation

Answer: A

NEW QUESTION 10

What does an attacker use to determine which network ports are listening on a potential target device?

- A. man-in-the-middle
- B. port scanning
- C. SQL injection
- D. ping sweep

Answer: B

NEW QUESTION 10

What is a difference between inline traffic interrogation and traffic mirroring?

- A. Inline inspection acts on the original traffic data flow
- B. Traffic mirroring passes live traffic to a tool for blocking
- C. Traffic mirroring inspects live traffic for analysis and mitigation
- D. Inline traffic copies packets for analysis and security

Answer: B

NEW QUESTION 11

What is the practice of giving an employee access to only the resources needed to accomplish their job?

- A. principle of least privilege
- B. organizational separation
- C. separation of duties
- D. need to know principle

Answer: A

NEW QUESTION 15

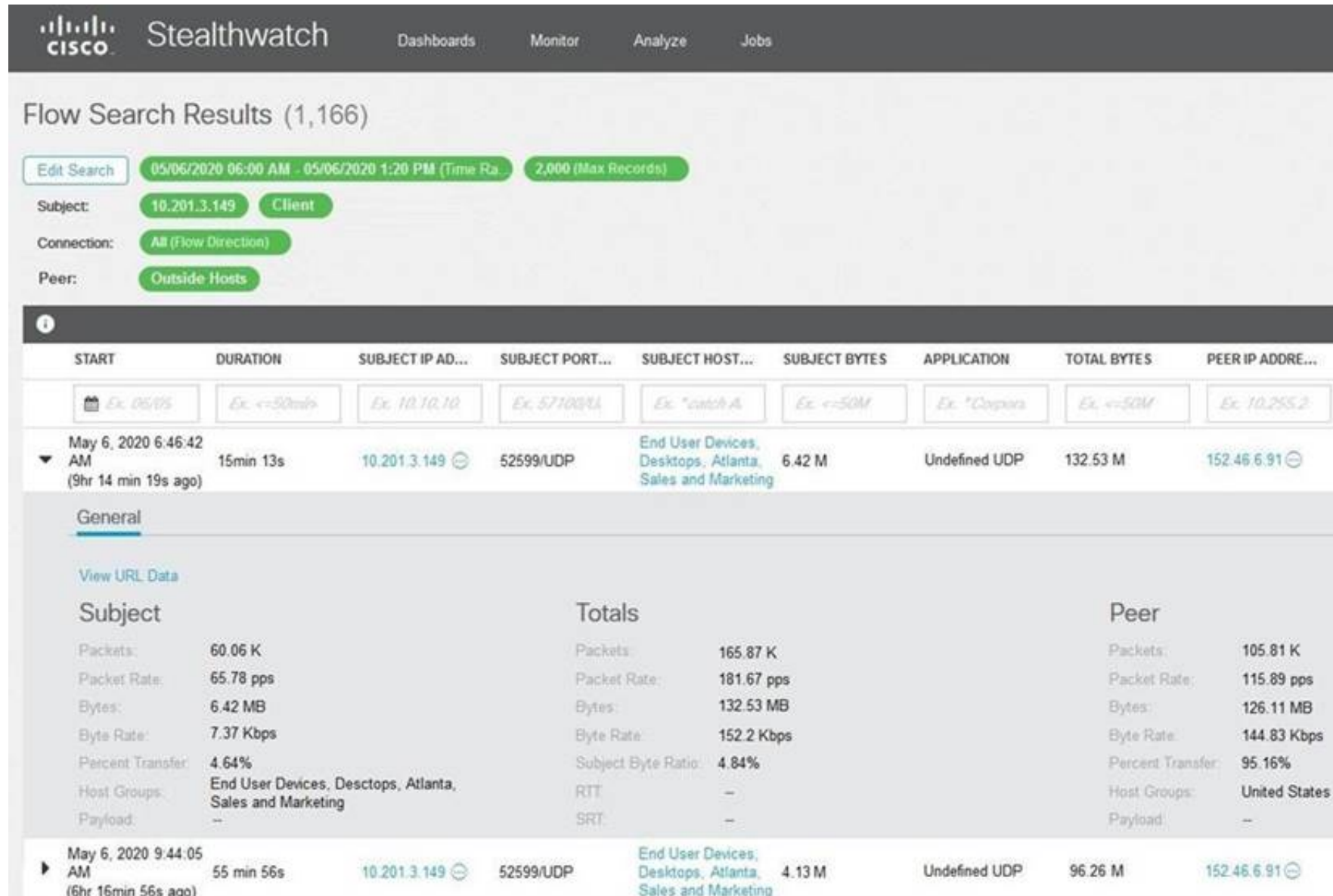
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

- A. Tapping interrogation replicates signals to a separate port for analyzing traffic
- B. Tapping interrogations detect and block malicious traffic
- C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
- D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A

NEW QUESTION 20

Refer to the exhibit.



The screenshot shows the Cisco Stealthwatch interface. At the top, there's a navigation bar with 'Dashboards', 'Monitor', 'Analyze', and 'Jobs'. Below this, the 'Flow Search Results' section shows 1,166 results. The search filters are: Subject: 10.201.3.149 (Client), Connection: All (Flow Direction), Peer: Outside Hosts. The search criteria bar shows: 05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Range), 2,000 (Max Records).

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...
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's a 'General' tab with 'View URL Data'. It shows details for the selected flow:

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: 4.64%	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: --

At the bottom, another flow is shown: 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

NEW QUESTION 21

What is rule-based detection when compared to statistical detection?

- A. proof of a user's identity
- B. proof of a user's action
- C. likelihood of user's action
- D. falsification of a user's identity

Answer: B

NEW QUESTION 24

An analyst discovers that a legitimate security alert has been dismissed. Which signature caused this impact on network traffic?

- A. true negative
- B. false negative
- C. false positive
- D. true positive

Answer: B

NEW QUESTION 29

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

- A. integrity
- B. confidentiality
- C. availability
- D. scope

Answer: A

NEW QUESTION 34

A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.

Which type of evidence is this?

- A. best evidence
- B. prima facie evidence
- C. indirect evidence
- D. physical evidence

Answer: C

NEW QUESTION 35

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the link launched, it infected machines and the intruder was able to access the corporate network.

Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating

Answer: A

NEW QUESTION 38

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

- A. encapsulation
- B. TOR
- C. tunneling
- D. NAT

Answer: D

NEW QUESTION 39

Which artifact is used to uniquely identify a detected file?

- A. file timestamp
- B. file extension
- C. file size
- D. file hash

Answer: D

NEW QUESTION 44

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

NEW QUESTION 47

How does an SSL certificate impact security between the client and the server?

- A. by enabling an authenticated channel between the client and the server
- B. by creating an integrated channel between the client and the server
- C. by enabling an authorized channel between the client and the server
- D. by creating an encrypted channel between the client and the server

Answer: D

NEW QUESTION 48

Which system monitors local system operation and local network access for violations of a security policy?

- A. host-based intrusion detection
- B. systems-based sandboxing
- C. host-based firewall
- D. antivirus

Answer: C

NEW QUESTION 50

What makes HTTPS traffic difficult to monitor?

- A. SSL interception
- B. packet header size
- C. signature detection time
- D. encryption

Answer: D

NEW QUESTION 54

Refer to the exhibit.

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

Which type of log is displayed?

- A. IDS
- B. proxy
- C. NetFlow
- D. sys

Answer: D

NEW QUESTION 58

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

Answer: AD

NEW QUESTION 60

An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise. Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

Answer: B

NEW QUESTION 63

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

Answer: CD

NEW QUESTION 68

Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

- A. NetScout
- B. tcpdump
- C. SolarWinds
- D. netsh

Answer: B

NEW QUESTION 72

An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

- A. data from a CD copied using Mac-based system
- B. data from a CD copied using Linux system
- C. data from a DVD copied using Windows system
- D. data from a CD copied using Windows

Answer: B

NEW QUESTION 76

When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

- A. fragmentation
- B. pivoting
- C. encryption
- D. stenography

Answer: D

NEW QUESTION 79

Refer to the exhibit.

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp     Postfix smtpd
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
Service Info: Host: 172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

What does the output indicate about the server with the IP address 172.18.104.139?

- A. open ports of a web server
- B. open port of an FTP server
- C. open ports of an email server
- D. running processes of the server

Answer: C

NEW QUESTION 84

Which two elements are used for profiling a network? (Choose two.)

- A. total throughout
- B. session duration
- C. running processes
- D. OS fingerprint
- E. listening ports

Answer: DE

NEW QUESTION 88

Which utility blocks a host portscan?

- A. HIDS
- B. sandboxing
- C. host-based firewall
- D. antimalware

Answer: C

NEW QUESTION 93

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

- A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
- B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Answer: C

NEW QUESTION 98

Which security technology allows only a set of pre-approved applications to run on a system?

- A. application-level blacklisting
- B. host-based IPS
- C. application-level whitelisting
- D. antivirus

Answer: C

NEW QUESTION 99

A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

- A. the intellectual property that was stolen
- B. the defense contractor who stored the intellectual property
- C. the method used to conduct the attack
- D. the foreign government that conducted the attack

Answer: D

NEW QUESTION 104

An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

- A. sequence numbers
- B. IP identifier
- C. 5-tuple
- D. timestamps

Answer: C

NEW QUESTION 107

Which event artifact is used to identify HTTP GET requests for a specific file?

- A. destination IP address
- B. URI
- C. HTTP status code
- D. TCP ACK

Answer: B

NEW QUESTION 109

Which access control model does SELinux use?

- A. RBAC
- B. DAC
- C. MAC
- D. ABAC

Answer: C

NEW QUESTION 111

An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

- A. The computer has a HIPS installed on it.
- B. The computer has a NIPS installed on it.
- C. The computer has a HIDS installed on it.
- D. The computer has a NIDS installed on it.

Answer: C

NEW QUESTION 112

What is a difference between SOAR and SIEM?

- A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not
- B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
- C. SOAR receives information from a single platform and delivers it to a SIEM
- D. SIEM receives information from a single platform and delivers it to a SOAR

Answer: A

NEW QUESTION 114

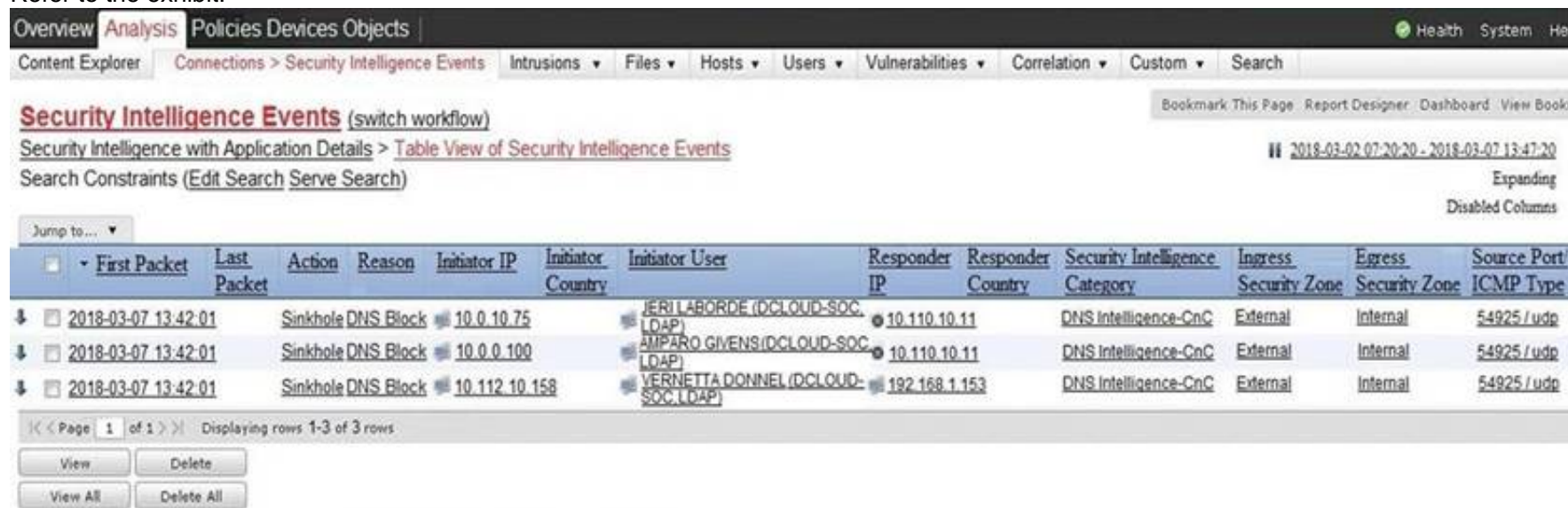
Which action prevents buffer overflow attacks?

- A. variable randomization
- B. using web based applications
- C. input sanitization
- D. using a Linux operating system

Answer: C

NEW QUESTION 119

Refer to the exhibit.



First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ICMP Type
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.10.75		JERI LABORDE (DCLOUD-SOC LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (DCLOUD-SOC LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01		Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

Which two elements in the table are parts of the 5-tuple? (Choose two.)

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port
- E. Initiator IP

Answer: DE

NEW QUESTION 121

Why is encryption challenging to security monitoring?

- A. Encryption analysis is used by attackers to monitor VPN tunnels.
- B. Encryption is used by threat actors as a method of evasion and obfuscation.
- C. Encryption introduces additional processing requirements by the CPU.
- D. Encryption introduces larger packet sizes to analyze and store.

Answer: B

NEW QUESTION 124

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

Answer: D

NEW QUESTION 125

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

200-201 Practice Exam Features:

- * 200-201 Questions and Answers Updated Frequently
- * 200-201 Practice Questions Verified by Expert Senior Certified Staff
- * 200-201 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 200-201 Practice Test Here](#)