

# 200-201<sup>Q&As</sup>

Understanding Cisco Cybersecurity Operations Fundamentals  
(CBROPS)

**Pass Cisco 200-201 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/200-201.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

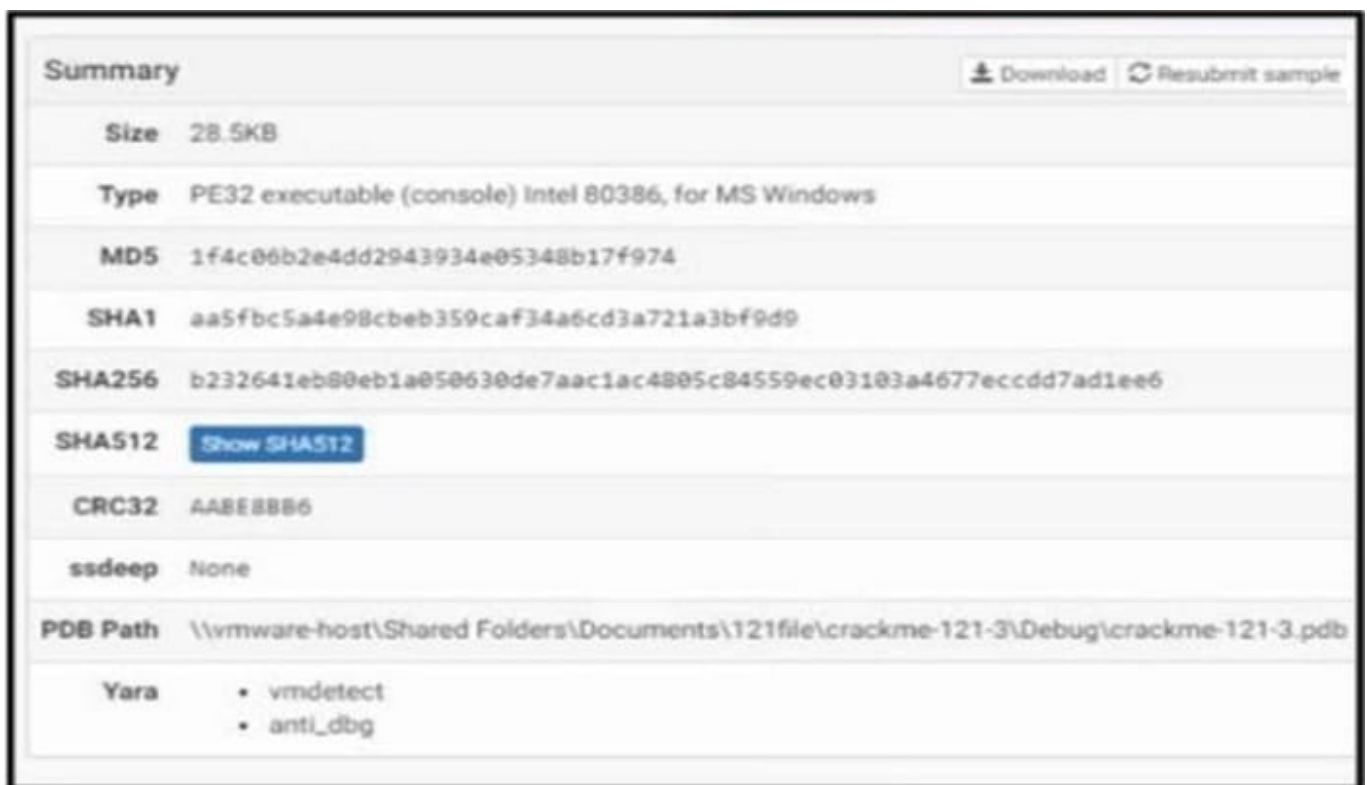
An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

- A. digital certificates
- B. static IP addresses
- C. signatures
- D. cipher suite

Correct Answer: A

**QUESTION 2**

Refer to the exhibit.



Summary		<a href="#">Download</a>	<a href="#">Resubmit sample</a>
Size	28.5KB		
Type	PE32 executable (console) Intel 80386, for MS Windows		
MD5	1f4c06b2e4dd2943934e05348b17f974		
SHA1	aa5fbc5a4e98cbeb359caf34a6cd3a721a3bf9d9		
SHA256	b232641eb80eb1a050630de7aac1ac4805c84559ec03103a4677eccdd7ad1ee6		
SHA512	<a href="#">Show SHA512</a>		
CRC32	AABE88B6		
ssdeep	None		
PDB Path	\\vmware-host\Shared Folders\Documents\121file\crackme-121-3\Debug\crackme-121-3.pdb		
Yara	<ul style="list-style-type: none"><li>• vmdetect</li><li>• anti_dbg</li></ul>		

An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

- A. The file will appear legitimate by evading signature-based detection.
- B. The file will not execute its behavior in a sandbox environment to avoid detection.
- C. The file will insert itself into an application and execute when the application is run.

D. The file will monitor user activity and send the information to an outside source.

Correct Answer: B

### QUESTION 3

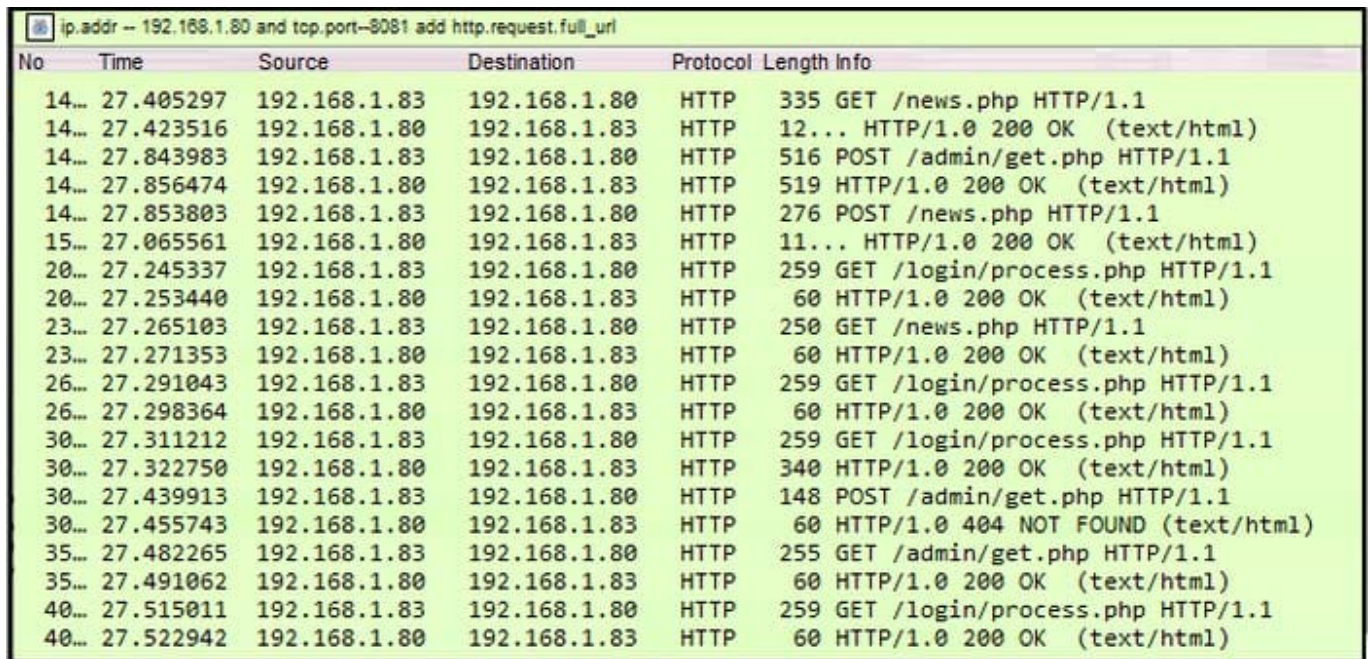
Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

- A. CSIRT
- B. PSIRT
- C. public affairs
- D. management

Correct Answer: D

### QUESTION 4

Refer to the exhibit.



No	Time	Source	Destination	Protocol	Length	Info
14...	27.405297	192.168.1.83	192.168.1.80	HTTP	335	GET /news.php HTTP/1.1
14...	27.423516	192.168.1.80	192.168.1.83	HTTP	12...	HTTP/1.0 200 OK (text/html)
14...	27.843983	192.168.1.83	192.168.1.80	HTTP	516	POST /admin/get.php HTTP/1.1
14...	27.856474	192.168.1.80	192.168.1.83	HTTP	519	HTTP/1.0 200 OK (text/html)
14...	27.853803	192.168.1.83	192.168.1.80	HTTP	276	POST /news.php HTTP/1.1
15...	27.065561	192.168.1.80	192.168.1.83	HTTP	11...	HTTP/1.0 200 OK (text/html)
20...	27.245337	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
20...	27.253440	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
23...	27.265103	192.168.1.83	192.168.1.80	HTTP	250	GET /news.php HTTP/1.1
23...	27.271353	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
26...	27.291043	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
26...	27.298364	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
30...	27.311212	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
30...	27.322750	192.168.1.80	192.168.1.83	HTTP	340	HTTP/1.0 200 OK (text/html)
30...	27.439913	192.168.1.83	192.168.1.80	HTTP	148	POST /admin/get.php HTTP/1.1
30...	27.455743	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 404 NOT FOUND (text/html)
35...	27.482265	192.168.1.83	192.168.1.80	HTTP	255	GET /admin/get.php HTTP/1.1
35...	27.491062	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
40...	27.515011	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
40...	27.522942	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)

A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of requests and data being transmitted. What is occurring?

- A. indicators of denial-of-service attack due to the frequency of requests

- B. garbage flood attack attacker is sending garbage binary data to open ports
- C. indicators of data exfiltration HTTP requests must be plain text
- D. cache bypassing attack: attacker is sending requests for noncacheable content

Correct Answer: C

---

## QUESTION 5

Which technology prevents end-device to end-device IP traceability?

- A. encryption
- B. load balancing
- C. NAT/PAT
- D. tunneling

Correct Answer: C

[200-201 PDF Dumps](#)

[200-201 VCE Dumps](#)

[200-201 Practice Test](#)