CS0-002$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

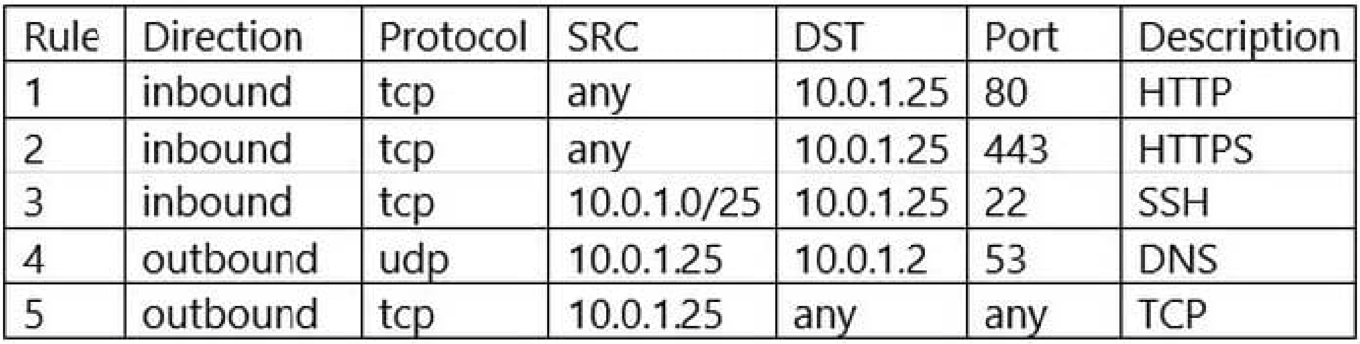
Pass CompTIA CS0-002 Exam with 100% Guarantee

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

QUESTION 1

A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.

The network rules for the instance are the following:



Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

Which of the following is the BEST way to isolate and triage the host?

A. Remove rules 1.2. and 3.

B. Remove rules 1.2. 4. and 5.

C. Remove rules 1.2. 3.4. and 5.

D. Remove rules 1.2. and 5.

E. Remove rules 1.4. and 5.

F. Remove rules 4 and 5

Correct Answer: D

QUESTION 2

A security analyst with an international response team is working to isolate a worldwide distribution of ransomware. The analyst is working with international governing bodies to distribute advanced intrusion detection routines for this variant of ransomware. Which of the following is the MOST important step with which the security analyst should comply?

A. Security operations privacy law

B. Export restrictions

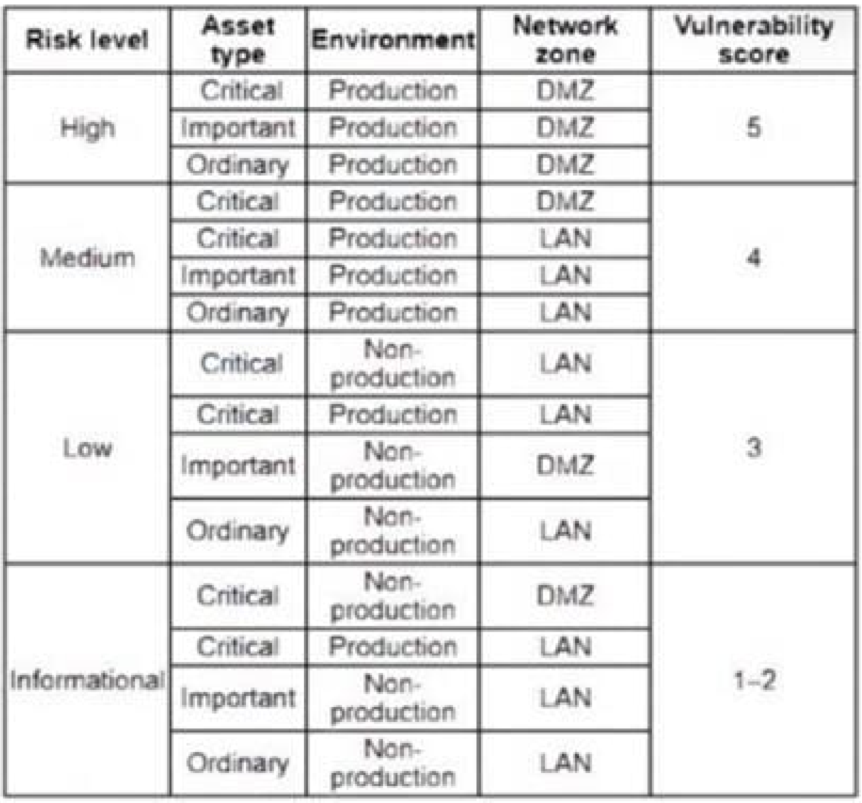
C. Non-disclosure agreements

D. Incident response forms

Correct Answer: D

QUESTION 3

A cybersecurity analyst is working with a SIEM tool and reviewing the following table:



Risk level	Asset type	Environment	Network zone	Vulnerability score
High	Critical	Production	DMZ	5
	Important	Production	DMZ	
	Ordinary	Production	DMZ	
Medium	Critical	Production	DMZ	4
	Critical	Production	LAN	
	Important	Production	LAN	
	Ordinary	Production	LAN	
Low	Critical	Non-production	LAN	3
	Critical	Production	LAN	
	Important	Non-production	DMZ	
	Ordinary	Non-production	LAN	
Informational	Critical	Non-production	DMZ	1-2
	Critical	Production	LAN	
	Important	Non-production	LAN	
	Ordinary	Non-production	LAN	

When creating a rule in the company\\'s SIEM, which of the following would be the BEST approach for the analyst to use to assess the risk level of each vulnerability that is discovered by the vulnerability assessment tool?

A. Create a trend with the table and join the trend with the desired rule to be able to extract the risk level of each vulnerability

B. Use Boolean filters in the SIEM rule to take advantage of real-time processing and RAM to store the table dynamically, generate the results faster, and be able to display the table in a dashboard or export it as a report

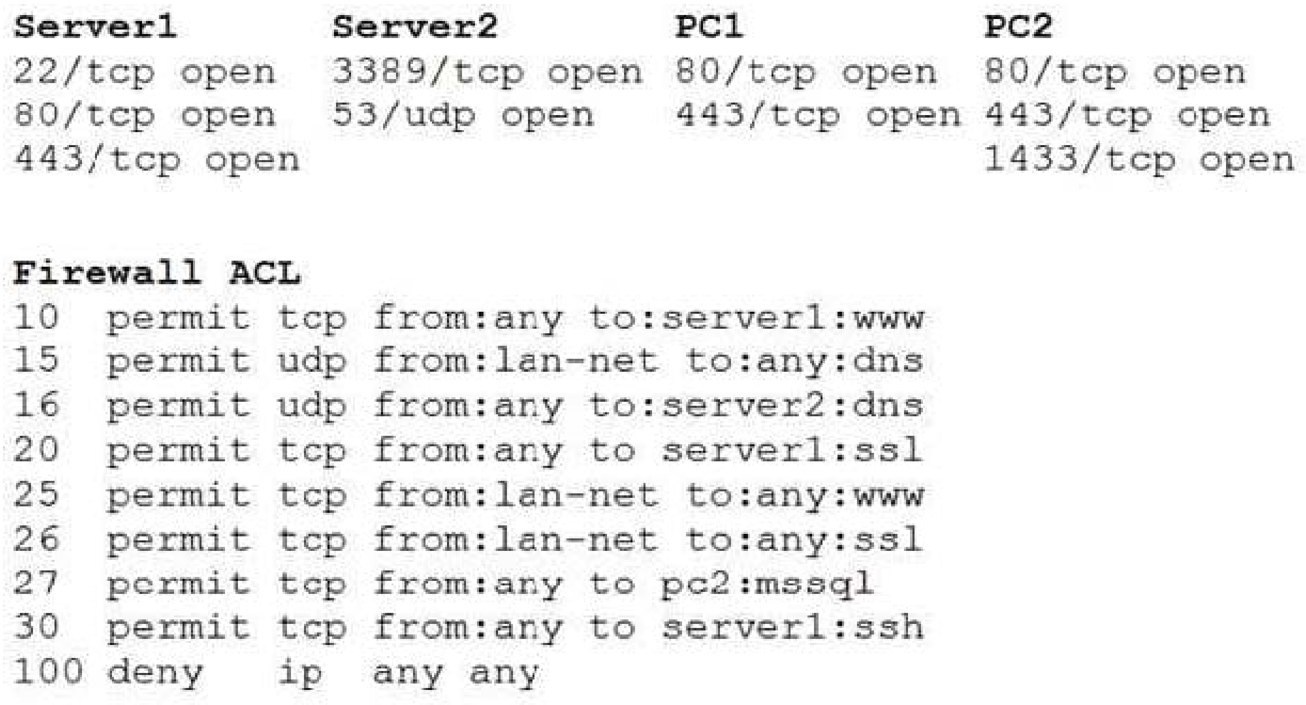
C. Use a static table stored on the disk of the SIEM system to correlate its data with the data ingested by the vulnerability scanner data collector

D. Use the table as a new index or database for the SIEM to be able to use multisearch and then summarize the results as output

Correct Answer: B

QUESTION 4

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:



```
Server1        Server2        PC1            PC2
22/tcp open    3389/tcp open  80/tcp open    80/tcp open
80/tcp open    53/udp open    443/tcp open   443/tcp open
443/tcp open                                 1433/tcp open

Firewall ACL
10  permit tcp from:any to:server1:www
15  permit udp from:lan-net to:any:dns
16  permit udp from:any to:server2:dns
20  permit tcp from:any to server1:ssl
25  permit tcp from:lan-net to:any:www
26  permit tcp from:lan-net to:any:ssl
27  permit tcp from:any to pc2:mssql
30  permit tcp from:any to server1:ssh
100 deny   ip  any any
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

A. PC1

B. PC2

C. Server1

D. Server2

E. Firewall

Correct Answer: E

QUESTION 5

Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?

A. There is a longer period of time to assess the environment.

B. The testing is outside the contractual scope

C. There is a shorter period of time to assess the environment

D. No status reports are included with the assessment.

Correct Answer: B