Free Questions for 312-39 by certscare

Shared by Sheppard on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

Options:

A- Windows Event Log

B- Web Server Logs

C- Router Logs

D- Switch Logs

Answer:

B

Question 2

Question Type: MultipleChoice

Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs.

What does these TTPs refer to?

Options:

A- Tactics, Techniques, and Procedures

B- Tactics, Threats, and Procedures

C- Targets, Threats, and Process

D- Tactics, Targets, and Process

Answer:

A

Question 3

Question Type: **MultipleChoice**

Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.

1. Strategic threat intelligence

2. Tactical threat intelligence

3. Operational threat intelligence

4. Technical threat intelligence

Options:

A- 2 and 3

B- 1 and 3

C- 3 and 4

D- 1 and 2

Answer:

A

Question 4

Question Type: **MultipleChoice**

Chloe, a SOC analyst with Jake Tech, is checking Linux systems logs. She is investigating files at /var/log/ wtmp.

What Chloe is looking at?

Options:

A- Error log

B- System boot log

C- General message and system-related stuff

D- Login records

Answer:

D

Question 5

Question Type: **MultipleChoice**

A type of threat intelligent that find out the information about the attacker by misleading them is known as

.

Options:

A- Threat trending Intelligence

B- Detection Threat Intelligence

C- Operational Intelligence

D- Counter Intelligence

Answer:

D

Question 6

Question Type: **MultipleChoice**

Which of the following is a Threat Intelligence Platform?

Options:

A- SolarWinds MS

B- TC Complete

C- Keepnote

D- Apility.io

Answer:

B