DUMPSARENA

Certified SOC Analyst

ECCouncil 312-39

Version Demo

Total Demo Questions: 10

Total Premium Questions: 102

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events.

This type of incident is categorized into _____?

A. True Positive Incidents

B. False positive Incidents

C. True Negative Incidents

D. False Negative Incidents

ANSWER: C

QUESTION NO: 2

Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

A. Failure Audit

B. Warning

C. Error

D. Information

ANSWER: B

Explanation:

Reference: https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types

QUESTION NO: 3

Which of the following Windows Event Id will help you monitors file sharing across the network?

A. 7045

B. 4625

C. 5140

D. 4624

ANSWER: C

Explanation:

Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140

QUESTION NO: 4

Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads.

What does this indicate?

A. Concurrent VPN Connections Attempt

B. DNS Exfiltration Attempt

C. Covering Tracks Attempt

D. DHCP Starvation Attempt

ANSWER: B

Explanation:

Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8gZaKq_PuAhWGi1wKHfQTC0oQFjAAegQIARAD&url=https%3A%2F%2Fconf.splunk.com%2Fsession%2F2014%2Fconf2014_FredWilmotSanfordOwings_Splunk_Security.pdf&usg=AOvVaw3ZLfzGqM-VUG7xKtze67ac

QUESTION NO: 5

Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?

A. COBIT

B. ITIL

C. SSE-CMM

D. SOC-CMM

ANSWER: C

Explanation:

Reference: https://www.iso.org/standard/44716.html

QUESTION NO: 6

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

A. Windows Event Log

B. Web Server Logs

C. Router Logs

D. Switch Logs

ANSWER: B

QUESTION NO: 7

Banter is a threat analyst in Christine Group of Industries. As a part of the job, he is currently formatting and structuring the raw data.

He is at which stage of the threat intelligence life cycle?

A. Dissemination and Integration

B. Processing and Exploitation

C. Collection

D. Analysis and Production

ANSWER: B

Explanation:

Reference: https://socradar.io/5-stages-of-the-threat-intelligence-lifecycle/

QUESTION NO: 8

Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?

A. DHCP Starvation Attacks

B. DHCP Spoofing Attack

C. DHCP Port Stealing

D. DHCP Cache Poisoning

ANSWER: A

Explanation:

Reference: https://www.cbtnuggets.com/blog/technology/networking/what-is-a-dhcp-starvation-attack

QUESTION NO: 9

Which of the following factors determine the choice of SIEM architecture?

A. SMTP Configuration

B. DHCP Configuration

C. DNS Configuration

D. Network Topology

ANSWER: C

QUESTION NO: 10

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

A. 2 and 3

B. 1 and 3

C. 3 and 4

D. 1 and 2

ANSWER: A

Explanation:

Reference: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf (38)

DUMPSARENA