Free Questions for 312-39 by dumpssheet

Shared by Gillespie on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following Windows features is used to enable Security Auditing in Windows?

Options:

A- Bitlocker

B- Windows Firewall

C- Local Group Policy Editor

D- Windows Defender

Answer:

C

Question 2

Question Type: MultipleChoice

Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?

Options:

A- threat_note

B- MagicTree

C- IntelMQ

D- Malstrom

Answer:

C

Question 3

Question Type: **MultipleChoice**

What is the process of monitoring and capturing all data packets passing through a given network using different tools?

Options:

A- Network Scanning

B- DNS Footprinting

C- Network Sniffing

D- Port Scanning

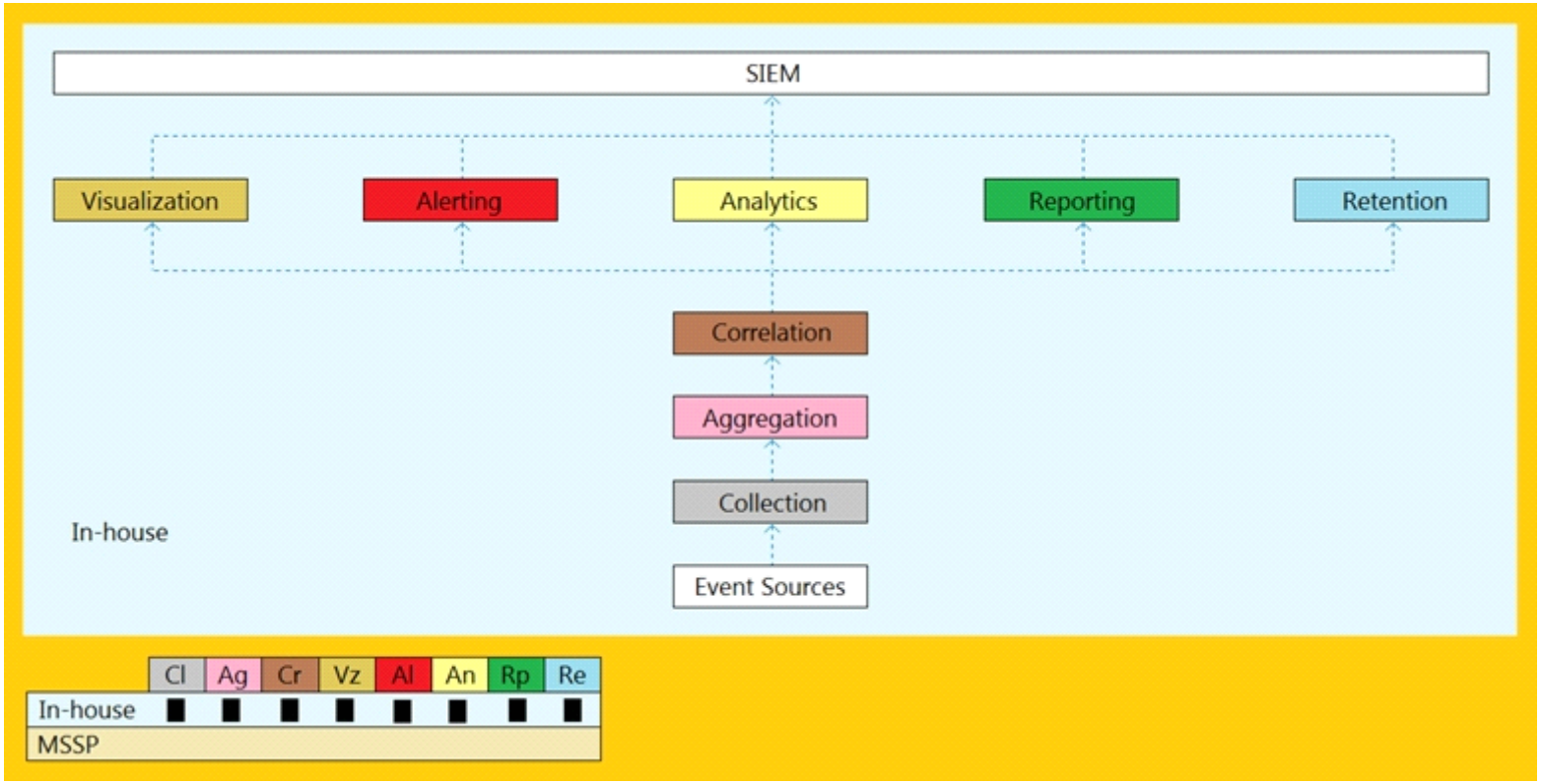
Answer:

C

Question 4

Question Type: **MultipleChoice**

An organization is implementing and deploying the SIEM with following capabilities.



What kind of SIEM deployment architecture the organization is planning to implement?

Options:

A- Cloud, MSSP Managed

B- Self-hosted, Jointly Managed

C- Self-hosted, Self-Managed

D- Self-hosted, MSSP Managed

Answer:

C

Question 5

Question Type: MultipleChoice

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

What does this indicate?

Options:

A- Concurrent VPN Connections Attempt

B- DNS Exfiltration Attempt

C- Covering Tracks Attempt

D- DHCP Starvation Attempt

Answer:

B

Explanation:

&url=https%3A%2F%2Fconf.splunk.com%2Fsession%2F2014%
2Fconf2014_FredWilmotSanfordOwings_Splunk_Security.pdf&usg=AOvVaw3ZLfzGqM-VUG7xKtze67ac

Question 6

Question Type: **MultipleChoice**

Which of the following formula is used to calculate the EPS of the organization?

Options:

A- EPS = average number of correlated events / time in seconds

B- EPS = number of normalized events / time in seconds

C- EPS = number of security events / time in seconds

D- EPS = number of correlated events / time in seconds

Answer:

C

Question 7

Question Type: MultipleChoice

Which of the following technique involves scanning the headers of IP packets leaving a network to make sure

that the unauthorized or malicious traffic never leaves the internal network?

Options:

A- Egress Filtering

B- Throttling

C- Rate Limiting

D- Ingress Filtering

Answer:

A

Question 8

Question Type: **MultipleChoice**

Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

Options:

A- $ tailf /var/log/sys/kern.log

B- $ tailf /var/log/kern.log

C- # tailf /var/log/messages

D- # tailf /var/log/sys/messages

Answer:

B

Question 9

Question Type: MultipleChoice

According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact of that attack is major?

Options:

A- High

B- Extreme

C- Low

D- Medium

Answer:

D

Question 10

Question Type: MultipleChoice

Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

Options:

A- /etc/ossim/reputation

B- /etc/ossim/siem/server/reputation/data

C- /etc/siem/ossim/server/reputation.data

D- /etc/ossim/server/reputation.data

Answer:

D

Question 11

Question Type: MultipleChoice

The Syslog message severity levels are labelled from level 0 to level 7.

What does level 0 indicate?

Options:

A- Alert

B- Notification

C- Emergency

D- Debugging

Answer:

C