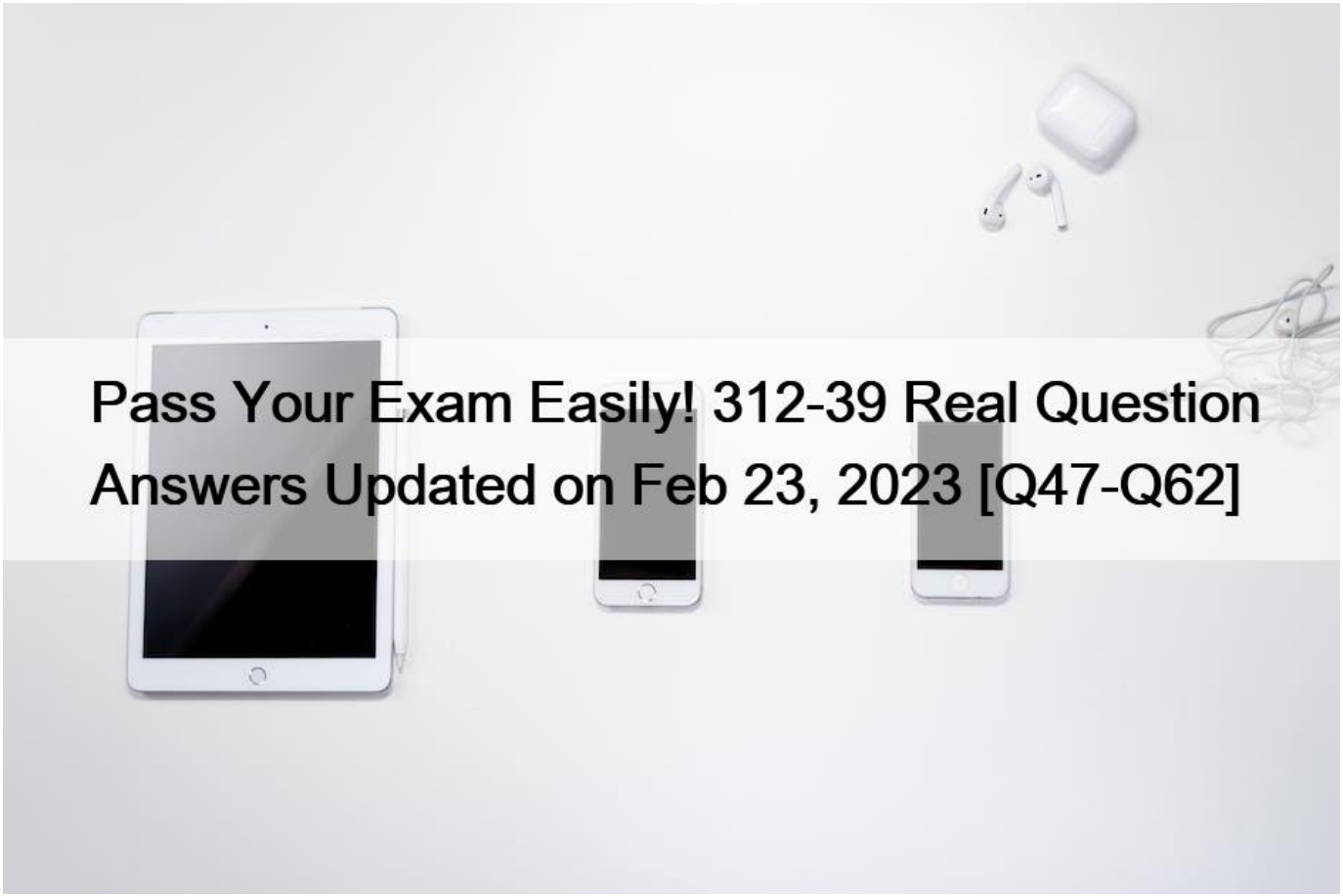
Pass Your Exam Easily! 312-39 Real Question Answers Updated on Feb 23, 2023 [Q47-Q62



Pass Your Exam Easily! 312-39 Real Question Answers Updated on Feb 23, 2023 Actual Questions Answers Pass With Real 312-39 Exam Dumps NO.47 If the SIEM generates the following four alerts at the same time:

I.Firewall blocking traffic from getting into the network alerts

II.SQL injection attempt alerts

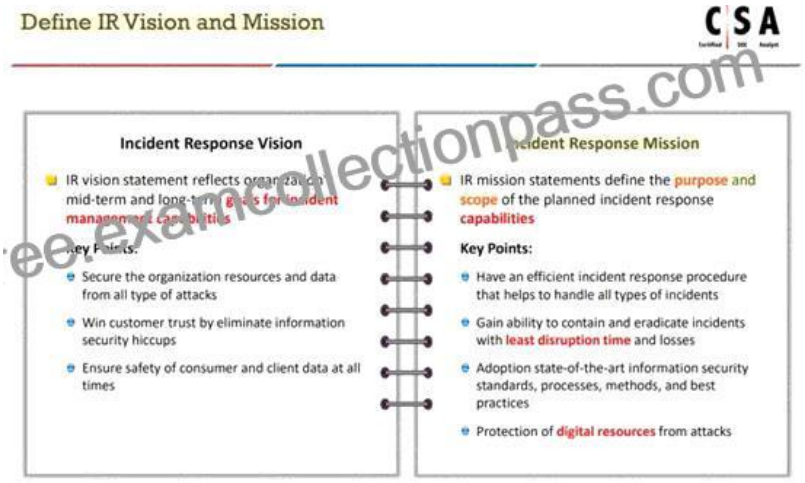
III.Data deletion attempt alerts

IV.Brute-force attempt alerts

Which alert should be given least priority as per effective alert triaging?
* III
* IV
* II
* I

NO.48 Daniel is a member of an IRT, which was started recently in a company named Mesh Tech. He wanted to find the purpose and scope of the planned incident response capabilities.

What is he looking for?
* Incident Response Intelligence
* Incident Response Mission
* Incident Response Vision
* Incident Response Resources



NO.49 Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?
* Windows Event Log
* Web Server Logs
* Router Logs
* Switch Logs

NO.50 Which of the following is a Threat Intelligence Platform?
* SolarWinds MS
* TC Complete
* Keepnote
* Apility.io

NO.51 An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP.

Which SIEM deployment architecture will the organization adopt?
* Cloud, MSSP Managed
* Self-hosted, Jointly Managed
* Self-hosted, MSSP Managed
* Self-hosted, Self-Managed

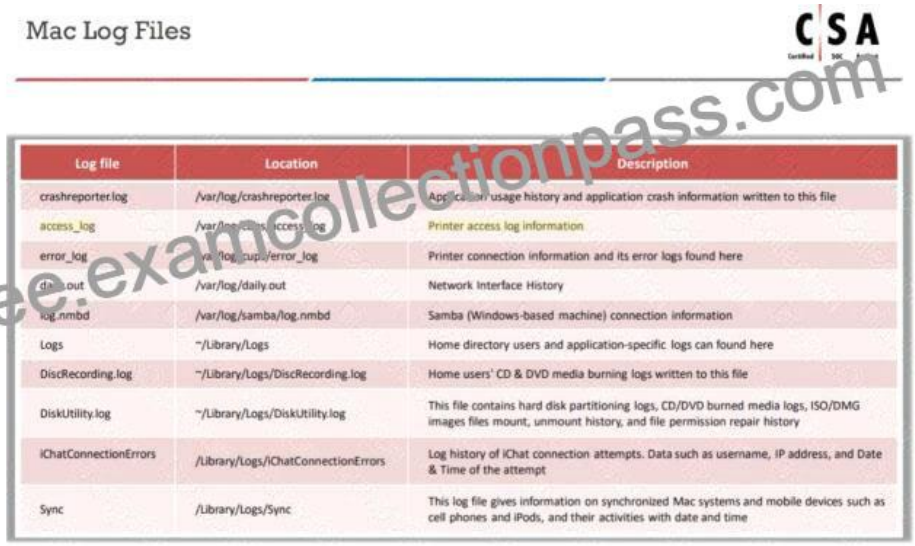
NO.52 Which of the following process refers to the discarding of the packets at the routing level without informing the source that the data did not reach its intended recipient?
* Load Balancing
* Rate Limiting
* Black Hole Filtering

* Drop Requests

NO.53 Which of the following directory will contain logs related to printer access?
* /var/log/cups/Printer_log file
* /var/log/cups/access_log file
* /var/log/cups/accesslog file
* /var/log/cups/Printeraccess_log file

Explanation

Graphical user interface Description automatically generated with low confidence



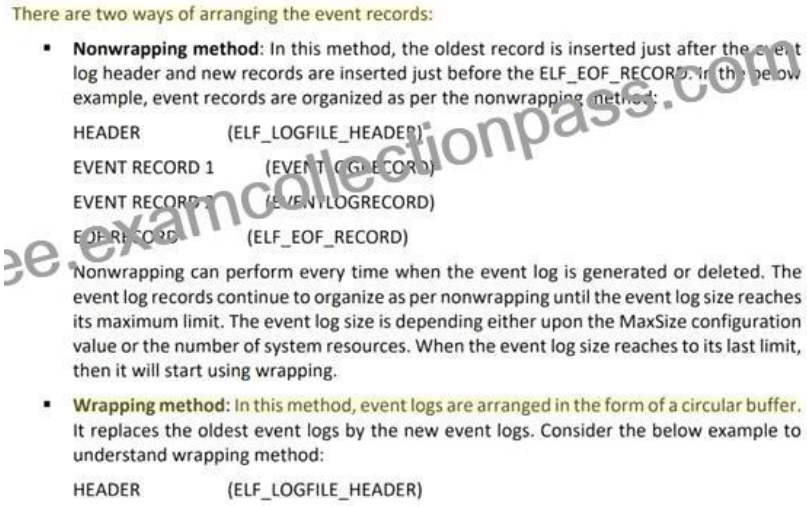
NO.54 Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.
* Dictionary Attack
* Rainbow Table Attack
* Bruteforce Attack
* Syllable Attack

NO.55 Which of the following formula represents the risk levels?
* Level of risk = Consequence * Severity
* Level of risk = Consequence * Impact
* Level of risk = Consequence * Likelihood
* Level of risk = Consequence * Asset Value

NO.56 Which of the following attack can be eradicated by converting all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums?
* Broken Access Control Attacks
* Web Services Attacks
* XSS Attacks
* Session Management Attacks

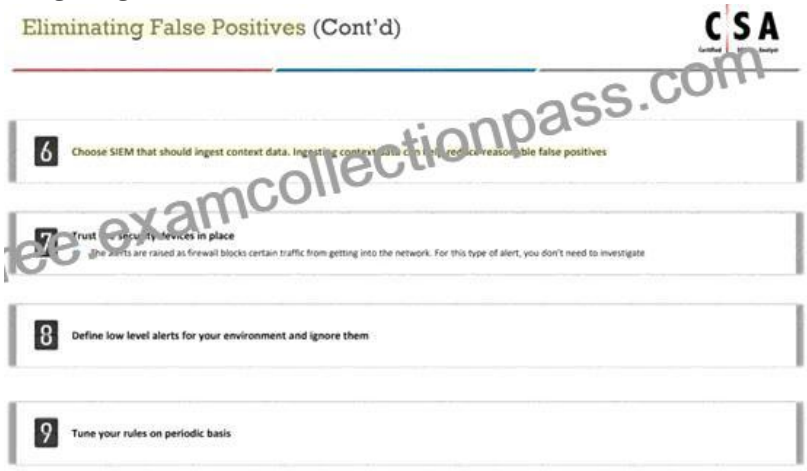
NO.57 Which of the log storage method arranges event logs in the form of a circular buffer?

* FIFO
* LIFO
* non-wrapping
* wrapping



NO.58 Which of the following can help you eliminate the burden of investigating false positives?

* Keeping default rules
* Not trusting the security devices
* Treating every alert as high level
* Ingesting the context data



NO.59 Robin, a SOC engineer in a multinational company, is planning to implement a SIEM. He realized that his organization is capable of performing only Correlation, Analytics, Reporting, Retention, Alerting, and Visualization required for the SIEM implementation and has to take collection and aggregation services from a Managed Security Services Provider (MSSP).

What kind of SIEM is Robin planning to implement?

* Self-hosted, Self-Managed
* Self-hosted, MSSP Managed
* Hybrid Model, Jointly Managed

* Cloud, Self-Managed

NO.60 Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.

What does this event log indicate?
* Directory Traversal Attack
* XSS Attack
* SQL Injection Attack
* Parameter Tampering Attack

NO.61 What does [-n] in the following checkpoint firewall log syntax represents?

fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]
* Display both the date and the time for each log record
* Speed up the process by not performing IP addresses DNS resolution in the Log files
* Display account log records only
* Display detailed log chains (all the log segments a log record consists of)

NO.62 Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?
* Containment -> Incident Recording -> Incident Triage -> Preparation -> Recovery -> Eradication -> Post-Incident Activities
* Preparation -> Incident Recording -> Incident Triage -> Containment -> Eradication -> Recovery -> Post-Incident Activities
* Incident Triage -> Eradication -> Containment -> Incident Recording -> Preparation -> Recovery -> Post-Incident Activities
* Incident Recording -> Preparation -> Containment -> Incident Triage -> Recovery -> Eradication -> Post-Incident Activities

Career Prospects

Those candidates who achieve the passing score in the certification exam are entitled to earn the CSA certification as well as membership privileges. The certified individuals are in high demand with numerous job openings that they can explore. Without a doubt, this EC-Council certificate is a highly rewarding option that allows the professionals to take up different job roles. Some career paths that they can explore include a Security & Network Administrator, a Network Defense Analyst, a Security & Network Engineer, a Network Security Specialist, a Network Defense Technician, a Network Security Operator, and a Cybersecurity Analyst, among others.

New 312-39 Dumps - Real EC-COUNCIL Exam Questions:
https://www.examcollectionpass.com/EC-COUNCIL/312-39-practice-exam-dumps.html]