Exam Questions 312-39

Certified SOC Analyst (CSA)

https://www.2passeasy.com/dumps/312-39/

NEW QUESTION 1
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

NEW QUESTION 2
Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:
May 06 2018 21:27:27 asa 1: %ASA -5 – 11008: User 'enable_15' executed the 'configure term' command What does the security level in the above log indicates?

A. Warning condition message
B. Critical condition message
C. Normal but significant message
D. Informational message

Answer: A

NEW QUESTION 3
The Syslog message severity levels are labelled from level 0 to level 7. What does level 0 indicate?

A. Alert
B. Notification
C. Emergency
D. Debugging

Answer: B

NEW QUESTION 4
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?

A. Load Balancing
B. Rate Limiting
C. Black Hole Filtering
D. Drop Requests

Answer: C

NEW QUESTION 5
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?

A. Cloud, MSSP Managed
B. Self-hosted, Jointly Managed
C. Self-hosted, MSSP Managed
D. Self-hosted, Self-Managed

Answer: C

NEW QUESTION 6
Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

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

NEW QUESTION 7
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]

A. Speed up the process by not performing IP addresses DNS resolution in the Log files
B. Display both the date and the time for each log record
C. Display account log records only
D. Display detailed log chains (all the log segments a log record consists of)

Answer:

A

NEW QUESTION 8
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?

A. Egress Filtering
B. Throttling
C. Rate Limiting
D. Ingress Filtering

Answer: A

NEW QUESTION 9
Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

A. Rule-based detection
B. Heuristic-based detection
C. Anomaly-based detection
D. Signature-based detection

Answer: C

NEW QUESTION 10
Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.

A. Post-Incident Activities
B. Incident Recording and Assignment
C. Incident Triage
D. Incident Disclosure

Answer: B

NEW QUESTION 10
Which of the following can help you eliminate the burden of investigating false positives?

A. Keeping default rules
B. Not trusting the security devices
C. Treating every alert as high level
D. Ingesting the context data

Answer: A

NEW QUESTION 11
An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company's URL as follows: http://technosoft.com.com/<script>alert("WARNING: The application has encountered an error");</script>. Identify the attack demonstrated in the above scenario.

A. Cross-site Scripting Attack
B. SQL Injection Attack
C. Denial-of-Service Attack
D. Session Attack

Answer: D

NEW QUESTION 15
Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?

A. Command Injection Attacks
B. SQL Injection Attacks
C. File Injection Attacks
D. LDAP Injection Attacks

Answer: B

NEW QUESTION 18
Which of the following service provides phishing protection and content filtering to manage the Internet experience on and off your network with the acceptable use or compliance policies?

A. Apility.io
B. Malstrom
C. OpenDNS
D. I-Blocklist

Answer: C

NEW QUESTION 21
Which of the following directory will contain logs related to printer access?

A. /var/log/cups/Printer_log file
B. /var/log/cups/access_log file
C. /var/log/cups/accesslog file
D. /var/log/cups/Printeraccess_log file

Answer: A

NEW QUESTION 25
Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?

A. Rate Limiting
B. Egress Filtering
C. Ingress Filtering
D. Throttling

Answer: C

NEW QUESTION 29
A type of threat intelligent that find out the information about the attacker by misleading them is known as.

A. Threat trending Intelligence
B. Detection Threat Intelligence
C. Operational Intelligence
D. Counter Intelligence

Answer: C

NEW QUESTION 30
Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

A. De-Militarized Zone (DMZ)
B. Firewall
C. Honeypot
D. Intrusion Detection System

Answer: C

NEW QUESTION 32
Which of the following formula represents the risk?

A. Risk = Likelihood × Severity × Asset Value
B. Risk = Likelihood × Consequence × Severity
C. Risk = Likelihood × Impact × Severity
D. Risk = Likelihood × Impact × Asset Value

Answer: B

NEW QUESTION 36
Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?

A. Containment
B. Data Collection
C. Eradication
D. Identification

Answer: A

NEW QUESTION 41
Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

A. DoS Attack
B. Man-In-Middle Attack
C. Ransomware Attack
D. Reconnaissance Attack

Answer: D

NEW QUESTION 43
Identify the HTTP status codes that represents the server error.

A. 2XX
B. 4XX
C. 1XX
D. 5XX

Answer: D

NEW QUESTION 45
Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?

A. Analytical Threat Intelligence
B. Operational Threat Intelligence
C. Strategic Threat Intelligence
D. Tactical Threat Intelligence

Answer: D

NEW QUESTION 50
An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.
Original
URL: http://www.buyonline.com/product.aspx?profile=12
&debit=100
Modified URL: http://www.buyonline.com/product.aspx?profile=12
&debit=10
Identify the attack depicted in the above scenario.

A. Denial-of-Service Attack
B. SQL Injection Attack
C. Parameter Tampering Attack
D. Session Fixation Attack

Answer: D

NEW QUESTION 52
Bonney's system has been compromised by a gruesome malware.
What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

A. Complaint to police in a formal way regarding the incident
B. Turn off the infected machine
C. Leave it to the network administrators to handle
D. Call the legal department in the organization and inform about the incident

Answer: B

NEW QUESTION 55
Which one of the following is the correct flow for Setting Up a Computer Forensics Lab?

A. Planning and budgeting –> Physical location and structural design considerations –> Work area considerations –> Human resource considerations –> Physical security recommendations –> Forensics lab licensing
B. Planning and budgeting –> Physical location and structural design considerations–> Forensics lab licensing –> Human resource considerations –> Work area considerations –> Physical security recommendations
C. Planning and budgeting –> Forensics lab licensing –> Physical location and structural design considerations –> Work area considerations –> Physical security recommendations –> Human resource considerations
D. Planning and budgeting –> Physical location and structural design considerations –> Forensics lab licensing –>Work area considerations –> Human resource considerations –> Physical securityrecommendations

Answer: A

NEW QUESTION 57
Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

A. Dictionary Attack
B. Rainbow Table Attack
C. Bruteforce Attack
D. Syllable Attack

Answer: A

NEW QUESTION 59
Which of the following tool is used to recover from web application incident?

A. CrowdStrike FalconTM Orchestrator
B. Symantec Secure Web Gateway
C. Smoothwall SWG

D. Proxy Workbench

Answer: B

NEW QUESTION 62
Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?

A. Netstat Data
B. DNS Data
C. IIS Data
D. DHCP Data

Answer: A

NEW QUESTION 66
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?

A. threat_note
B. MagicTree
C. IntelMQ
D. Malstrom

Answer: C

NEW QUESTION 67
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

NEW QUESTION 68
Peter, a SOC analyst with Spade Systems, is monitoring and analyzing the router logs of the company and wanted to check the logs that are generated by access control list numbered 210.
What filter should Peter add to the 'show logging' command to get the required output?

A. show logging | access 210
B. show logging | forward 210
C. show logging | include 210
D. show logging | route 210

Answer: C

NEW QUESTION 72
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.

What does this event log indicate?

A. Directory Traversal Attack
B. XSS Attack
C. SQL Injection Attack
D. Parameter Tampering Attack

Answer: D

NEW QUESTION 74

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

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: A

NEW QUESTION 76
Which of the following are the responsibilities of SIEM Agents?
* 1. Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
* 2. Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.
* 3. Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
* 4. Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.

A. 1 and 2
B. 2 and 3
C. 1 and 4
D. 3 and 1

Answer: C

NEW QUESTION 78
Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.
What would be her next action according to the SOC workflow?

A. She should immediately escalate this issue to the management
B. She should immediately contact the network administrator to solve the problem
C. She should communicate this incident to the media immediately
D. She should formally raise a ticket and forward it to the IRT

Answer: B

NEW QUESTION 79
Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?

A. Ransomware Attack
B. DoS Attack
C. DHCP starvation Attack
D. File Injection Attack

Answer: A

NEW QUESTION 82
In which phase of Lockheed Martin's – Cyber Kill Chain Methodology, adversary creates a deliverable malicious payload using an exploit and a backdoor?

A. Reconnaissance
B. Delivery
C. Weaponization
D. Exploitation

Answer: B

NEW QUESTION 84
Which of the following is a Threat Intelligence Platform?

A. SolarWinds MS
B. TC Complete
C. Keepnote
D. Apility.io

Answer: A

NEW QUESTION 85
Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

A. FISMA
B. HIPAA
C. PCI-DSS
D. DARPA

Answer: C

NEW QUESTION 89
What type of event is recorded when an application driver loads successfully in Windows?

A. Error
B. Success Audit
C. Warning
D. Information

Answer: D

NEW QUESTION 94
Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.
What is the first step that the IRT will do to the incident escalated by Emmanuel?

A. Incident Analysis and Validation
B. Incident Recording
C. Incident Classification
D. Incident Prioritization

Answer: C

NEW QUESTION 99
John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints.
Which of following Splunk query will help him to fetch related logs associated with process creation?

A. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
C. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. .. ..
D. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...

Answer: B

NEW QUESTION 100
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-39 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-39 Product From:

https://www.2passeasy.com/dumps/312-39/

Money Back Guarantee

312-39 Practice Exam Features:

* 312-39 Questions and Answers Updated Frequently

* 312-39 Practice Questions Verified by Expert Senior Certified Staff

* 312-39 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-39 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year