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
What does the Security Log Event ID 4624 of Windows 10 indicate?

A. Service added to the endpoint
B. A share was assessed
C. An account was successfully logged on
D. New process executed

Answer: C

NEW QUESTION 3
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 4
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 5
Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?

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: A

NEW QUESTION 6
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 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

NEW QUESTION 8
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 9
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 10
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 10
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?

A. Broken Access Control Attacks
B. Web Services Attacks
C. XSS Attacks
D. Session Management Attacks

Answer: C

NEW QUESTION 14
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 17
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 21
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

NEW QUESTION 23

What does the HTTP status codes 1XX represents?

A. Informational message
B. Client error
C. Success
D. Redirection

Answer: A

NEW QUESTION 27
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 31
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 36
The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk. What kind of threat intelligence described above?

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

Answer: B

NEW QUESTION 40
Which encoding replaces unusual ASCII characters with "%" followed by the character’s two-digit ASCII code expressed in hexadecimal?

A. Unicode Encoding
B. UTF Encoding
C. Base64 Encoding
D. URL Encoding

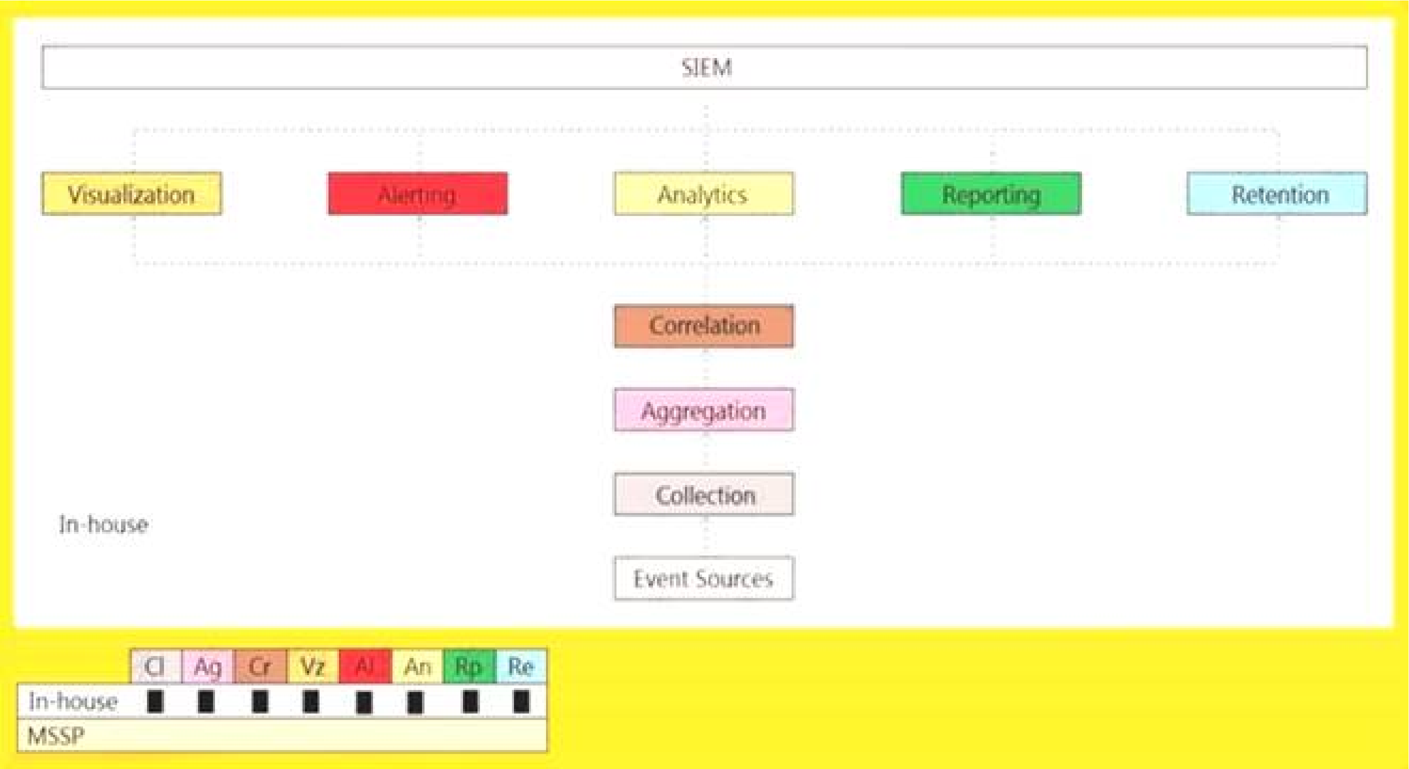
Answer: D

NEW QUESTION 42
Identify the HTTP status codes that represents the server error.

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

Answer: D

NEW QUESTION 45
An organization is implementing and deploying the SIEM with following capabilities.



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

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

Answer: A

NEW QUESTION 49
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?

A. III
B. IV
C. II
D. I

Answer: D

NEW QUESTION 52
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 57
Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)/|.
What does this event log indicate?

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

Answer: C

NEW QUESTION 58
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 62
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 64
What does HTTPS Status code 403 represents?

A. Unauthorized Error
B. Not Found Error
C. Internal Server Error
D. Forbidden Error

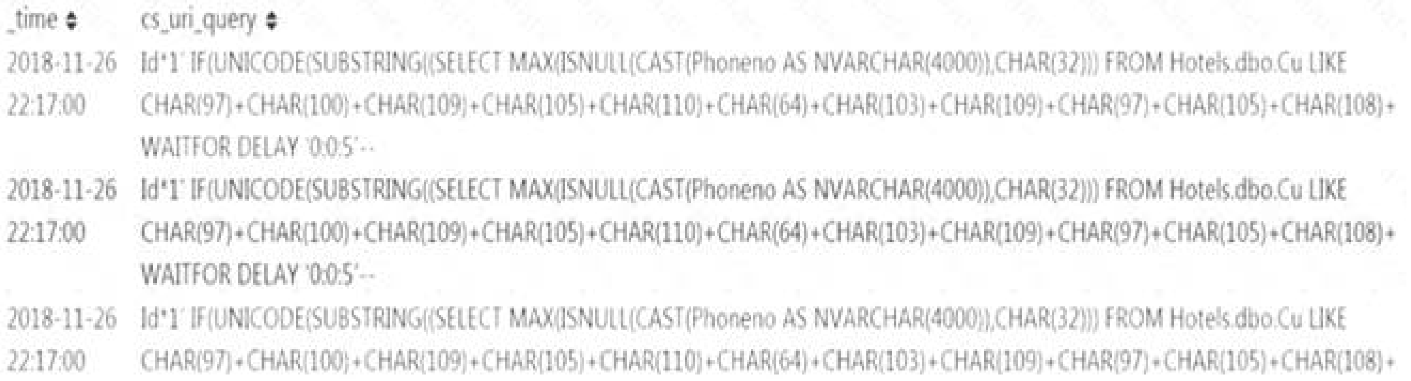
Answer: D

NEW QUESTION 67
Which of the following Windows event is logged every time when a user tries to access the "Registry" key?

A. 4656
B. 4663
C. 4660
D. 4657

Answer: D

NEW QUESTION 69
Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.



```
_time ⬍      cs_uri_query ⬍
2018-11-26   Id'1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE
22:17:00     CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+
             WAITFOR DELAY '0:0:5'--
2018-11-26   Id'1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE
22:17:00     CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+
             WAITFOR DELAY '0:0:5'--
2018-11-26   Id'1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE
22:17:00     CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+
```

What does this event log indicate?

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

Answer: A

NEW QUESTION 73
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 76
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 80
According to the Risk Matrix table, what will be the risk level when the probability of an attack is very high, and the impact of that attack is major?
NOTE: It is mandatory to answer the question before proceeding to the next one.

A. High
B. Extreme
C. Low
D. Medium

Answer: A

NEW QUESTION 82
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 87
Wesley is an incident handler in a company named Maddison Tech. One day, he was learning techniques for eradicating the insecure deserialization attacks. What among the following should Wesley avoid from considering?

A. Deserialization of trusted data must cross a trust boundary
B. Understand the security permissions given to serialization and deserialization
C. Allow serialization for security-sensitive classes
D. Validate untrusted input, which is to be serialized to ensure that serialized data contain only trusted classes

Answer: C

NEW QUESTION 89
What does Windows event ID 4740 indicate?

A. A user account was locked out.
B. A user account was disabled.
C. A user account was enabled.
D. A user account was created.

Answer: A

NEW QUESTION 92
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 94
Which of the following Windows features is used to enable Security Auditing in Windows?

A. Bitlocker
B. Windows Firewall
C. Local Group Policy Editor
D. Windows Defender

Answer: C

NEW QUESTION 97
In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

A. rule-based
B. pull-based
C. push-based
D. signature-based

Answer: A

NEW QUESTION 98
Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

A. Containment –> Incident Recording –> Incident Triage –> Preparation –> Recovery –> Eradication –> Post-Incident Activities
B. Preparation –> Incident Recording –> Incident Triage –> Containment –> Eradication –> Recovery –> Post-Incident Activities
C. Incident Triage –> Eradication –> Containment –> Incident Recording –> Preparation –> Recovery –> Post-Incident Activities
D. Incident Recording –> Preparation –> Containment –> Incident Triage –> Recovery –> Eradication –> Post-Incident Activities

Answer: B

NEW QUESTION 99
John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming.
Which of the following data source will he use to prepare the dashboard?

A. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
C. DNS/ Web Server logs with IP addresses.
D. Apache/ Web Server logs with IP addresses and Host Name.

Answer: D

NEW QUESTION 101
Which of the log storage method arranges event logs in the form of a circular buffer?

A. FIFO
B. LIFO
C. non-wrapping
D. wrapping

Answer: A

NEW QUESTION 104
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 107
......