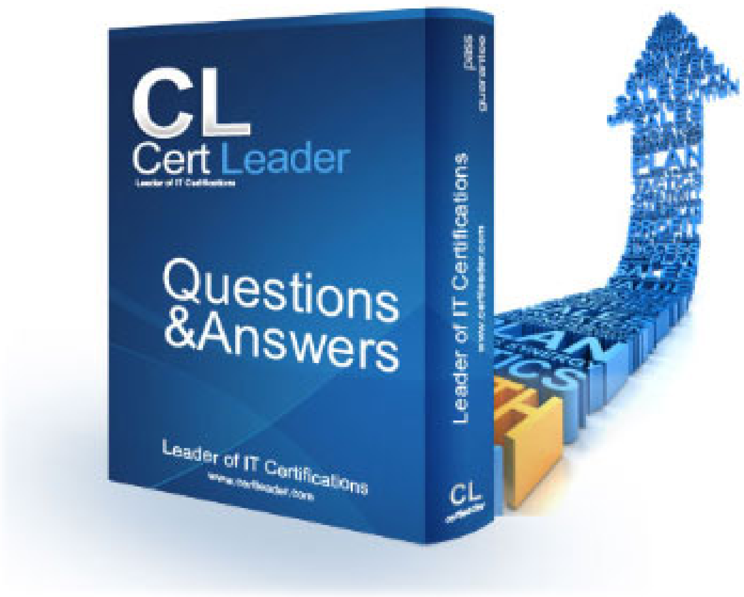
312-39 Dumps

Certified SOC Analyst (CSA)

https://www.certleader.com/312-39-dumps.html



NEW QUESTION 1
What is the correct sequence of SOC Workflow?

A. Collect, Ingest, Validate, Document, Report, Respond
B. Collect, Ingest, Document, Validate, Report, Respond
C. Collect, Respond, Validate, Ingest, Report, Document
D. Collect, Ingest, Validate, Report, Respond, Document

Answer: A

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
Which of the following is a default directory in a Mac OS X that stores security-related logs?

A. /private/var/log
B. /Library/Logs/Sync
C. /var/log/cups/access_log
D. ~/Library/Logs

Answer: D

NEW QUESTION 4
Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs. What does these TTPs refer to?

A. Tactics, Techniques, and Procedures
B. Tactics, Threats, and Procedures
C. Targets, Threats, and Process
D. Tactics, Targets, and Process

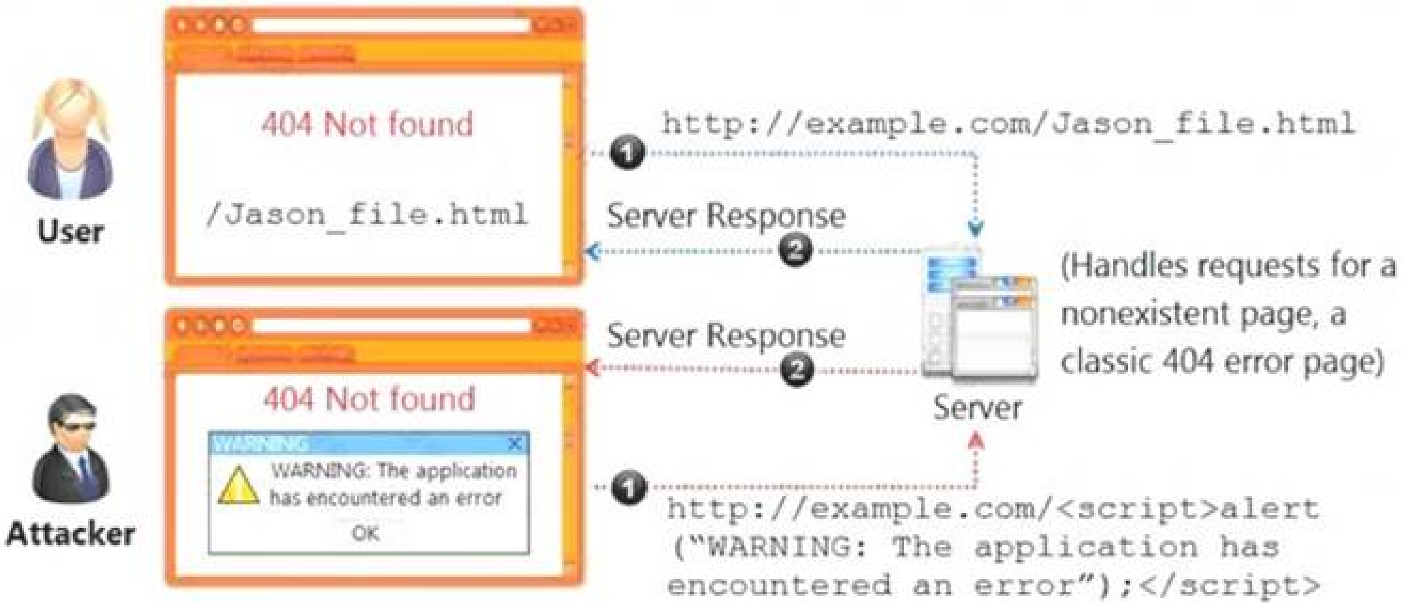
Answer: A

NEW QUESTION 5
Which of the following fields in Windows logs defines the type of event occurred, such as Correlation Hint, Response Time, SQM, WDI Context, and so on?

A. Keywords
B. Task Category
C. Level
D. Source

Answer: A

NEW QUESTION 6
Identify the type of attack, an attacker is attempting on www.example.com website.



```
http://example.com/Jason_file.html
```

WARNING: The application has encountered an error

```
http://example.com/<script>alert
("WARNING: The application has
encountered an error");</script>
```

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

D. SQL Injection Attack

Answer: A

NEW QUESTION 7
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 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
Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.
What is Ray and his team doing?

A. Blocking the Attacks
B. Diverting the Traffic
C. Degrading the services
D. Absorbing the Attack

Answer: D

NEW QUESTION 10
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 11
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 14
What does the HTTP status codes 1XX represents?

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

Answer: A

NEW QUESTION 15
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 18
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

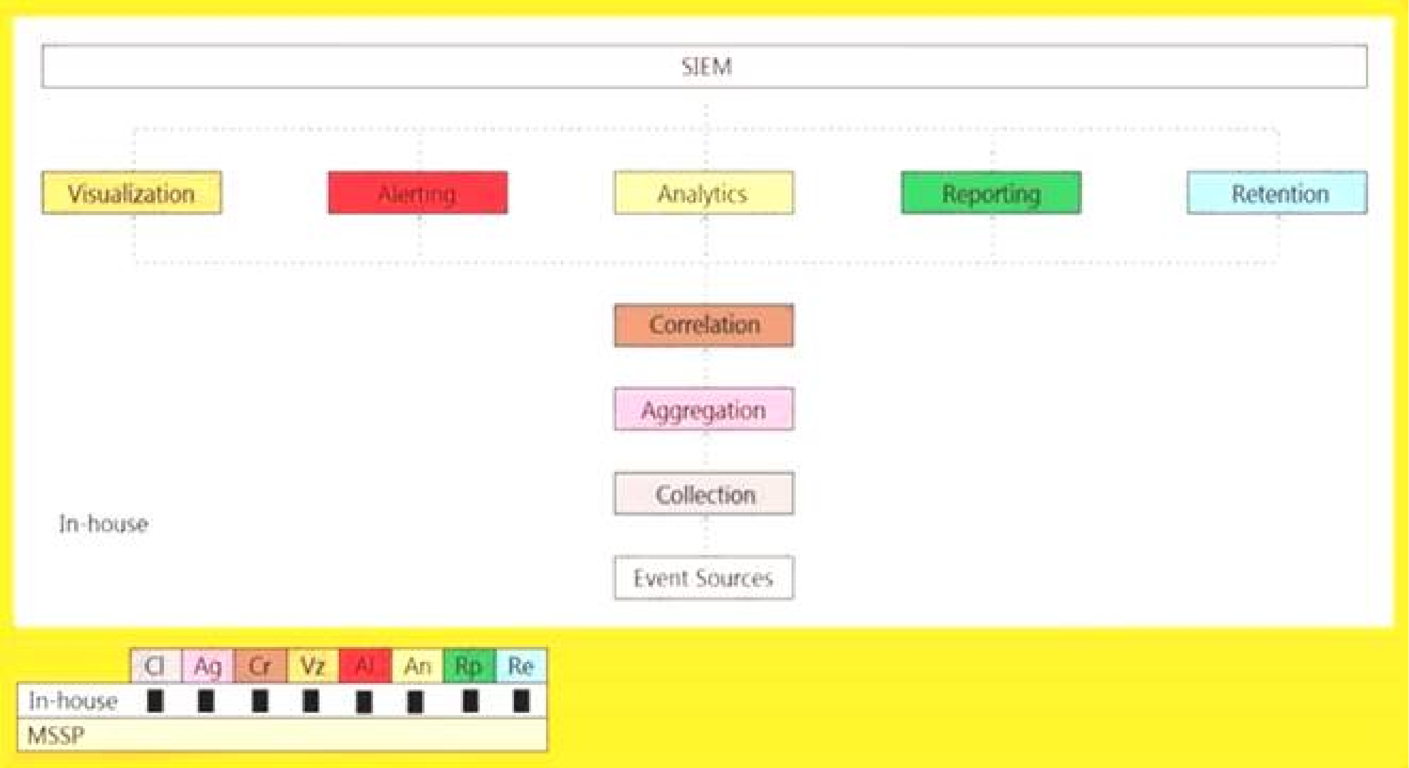
Answer: B

NEW QUESTION 19
Identify the HTTP status codes that represents the server error.

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

Answer: D

NEW QUESTION 20
An organization is implementing and deploying the SIEM with following capabilities.



	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house	■	■	■	■	■	■	■	■
MSSP								

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 24
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

NEW QUESTION 25
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 28
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 29
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 33
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 36
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?

A. Incident Response Intelligence
B. Incident Response Mission
C. Incident Response Vision
D. Incident Response Resources

Answer: D

NEW QUESTION 41
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 45
John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regex
/(\.|(%|%25)2E)(\.|(%|%25)2E)(\/|(%|%25)2F|\\|(%|%25)5C)/i.
What does this event log indicate?

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

Answer: A

NEW QUESTION 49
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

NEW QUESTION 50
Which of the following attack can be eradicated by filtering improper XML syntax?

A. CAPTCHA Attacks
B. SQL Injection Attacks
C. Insufficient Logging and Monitoring Attacks
D. Web Services Attacks

Answer: B

NEW QUESTION 53
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 56
Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex
/\\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix.
What does this event log indicate?

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

Answer: A

NEW QUESTION 59
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 61
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 64
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 65
Which of the following is a Threat Intelligence Platform?

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

Answer: A

NEW QUESTION 67
Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file?

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

Answer: B

NEW QUESTION 71
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 76
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 78
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 80
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 83
......