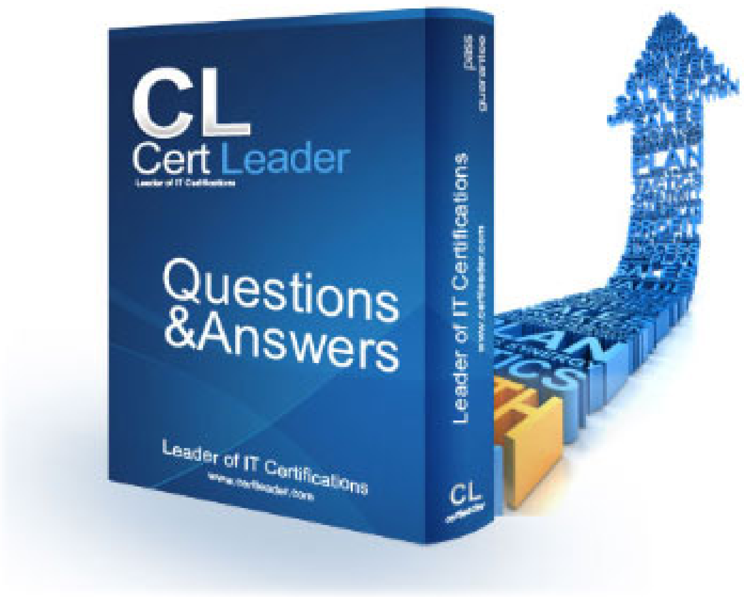
312-39 Dumps

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
John, a threat analyst at GreenTech Solutions, wants to gather information about specific threats against the organization. He started collecting information from various sources, such as humans, social media, chat room, and so on, and created a report that contains malicious activity.
Which of the following types of threat intelligence did he use?

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

Answer: D

NEW QUESTION 3
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 4
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 5
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 6
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 7
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 8

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 9
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 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 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 13
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 17
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 19
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

Which of the following formula represents the risk levels?

A. Level of risk = Consequence × Severity
B. Level of risk = Consequence × Impact
C. Level of risk = Consequence × Likelihood
D. Level of risk = Consequence × Asset Value

Answer: B

NEW QUESTION 25
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 29
Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

A. Windows Event Log
B. Web Server Logs
C. Router Logs
D. Switch Logs

Answer: B

NEW QUESTION 32
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 35
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

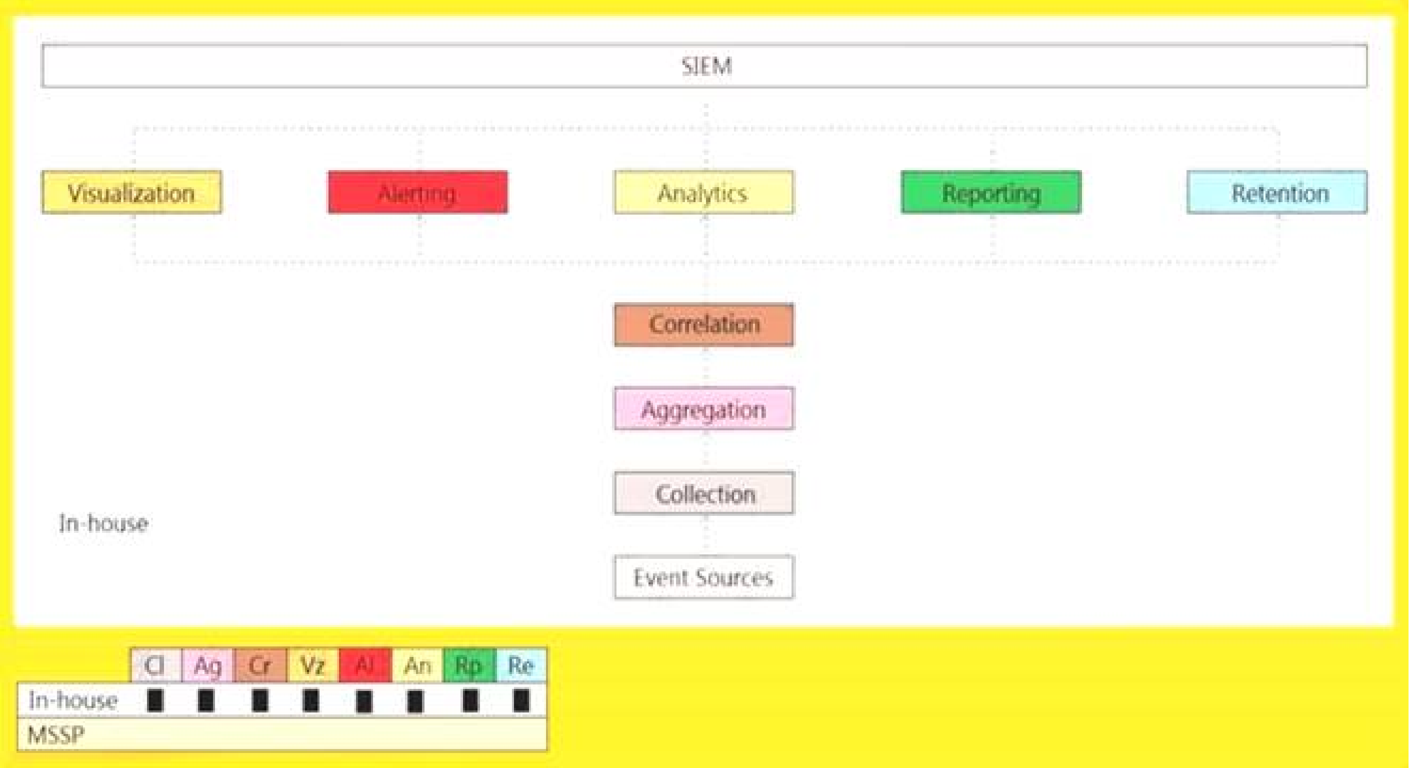
Answer: D

NEW QUESTION 36
Identify the HTTP status codes that represents the server error.

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

Answer: D

NEW QUESTION 39
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 43
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 45
Which of the following tool can be used to filter web requests associated with the SQL Injection attack?

A. Nmap
B. UrlScan
C. ZAP proxy
D. Hydra

Answer: B

NEW QUESTION 48
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 51
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 55
Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.

A. Slow DoS Attack
B. DHCP Starvation

C. Zero-Day Attack
D. DNS Poisoning Attack

Answer: C

NEW QUESTION 58
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 61
Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

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

Answer: B

NEW QUESTION 62
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 64
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 67
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 71
Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads. What does this indicate?

A. Concurrent VPN Connections Attempt
B. DNS Exfiltration Attempt
C. Covering Tracks Attempt
D. DHCP Starvation Attempt

Answer: B

NEW QUESTION 76
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 80
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 81
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 82
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 83
......