

## 312-39 Dumps

### Certified SOC Analyst (CSA)

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



**NEW QUESTION 1**

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 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 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 5**

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 6**

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 7**

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 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**

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**

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 11**

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 16**

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 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**

According to the forensics investigation process, what is the next step carried out right after collecting the evidence?

- A. Create a Chain of Custody Document
- B. Send it to the nearby police station
- C. Set a Forensic lab
- D. Call Organizational Disciplinary Team

**Answer:** A

**NEW QUESTION 22**

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 23**

Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.

Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?

- A. Threat pivoting
- B. Threat trending
- C. Threat buy-in
- D. Threat boosting

**Answer:** C

**NEW QUESTION 26**

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 27**

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 31**

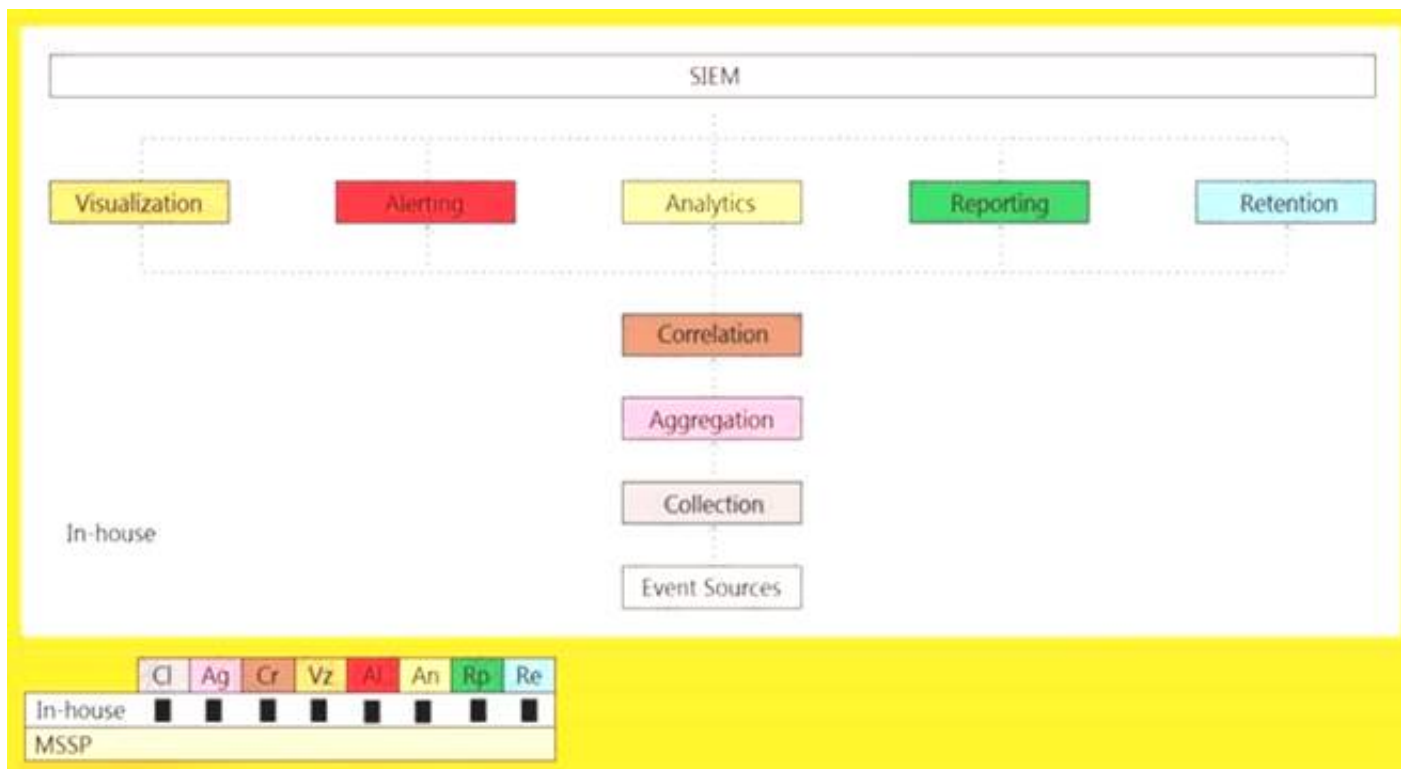
The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk. What kind of threat intelligence described above?

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

**Answer:** B

**NEW QUESTION 33**

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 35

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 40

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 44

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 47

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 50

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 security recommendations

**Answer:** A

#### NEW QUESTION 55

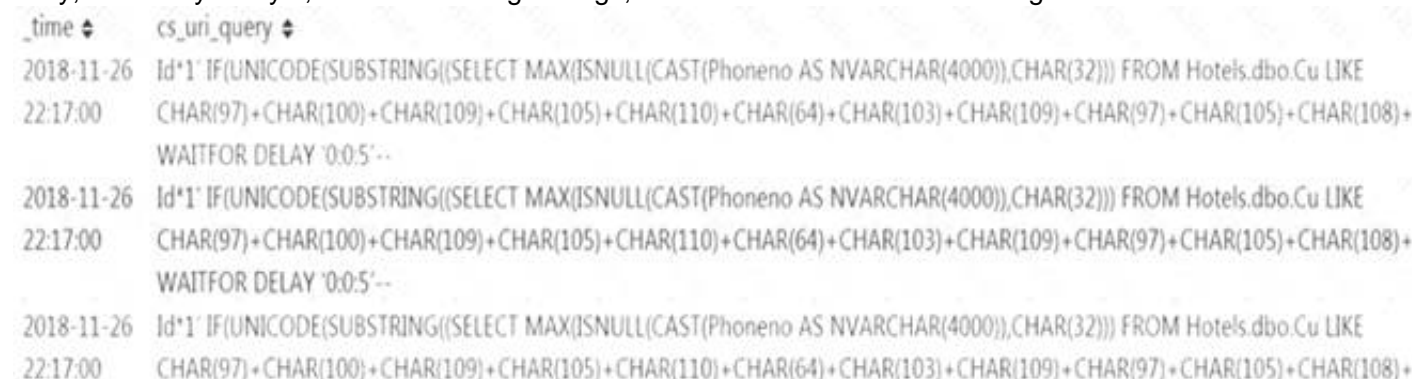
What does HTTPS Status code 403 represents?

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

**Answer:** D

#### NEW QUESTION 60

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



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 61

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

- A. CrowdStrike Falcon™ Orchestrator
- B. Symantec Secure Web Gateway
- C. Smoothwall SWG
- D. Proxy Workbench

**Answer:** B

#### NEW QUESTION 63

What is the process of monitoring and capturing all data packets passing through a given network using different tools?

- A. Network Scanning
- B. DNS Footprinting
- C. Network Sniffing
- D. Port Scanning

**Answer:** C

#### NEW QUESTION 67

Which of the following command is used to enable logging in iptables?

- A. \$ iptables -B INPUT -j LOG
- B. \$ iptables -A OUTPUT -j LOG
- C. \$ iptables -A INPUT -j LOG
- D. \$ iptables -B OUTPUT -j LOG

**Answer:** B

#### NEW QUESTION 72



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

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 77

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

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 84

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 87

According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact of that attack is major?

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

**Answer:** C

#### NEW QUESTION 88

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

List ▾	Format ▾	50 Per Page ▾
i	Time	Event
>	2/7/19 5:47:29.000 PM	2019-02-07 12:17:29 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001117 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 191 cs_uri_query = id-ORD-001117   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log   sourcetype = iis
>	2/7/19 5:47:25.000 PM	2019-02-07 12:17:25 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001116 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 133 cs_uri_query = id-ORD-001116   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log   sourcetype = iis
>	2/7/19 5:47:21.000 PM	2019-02-07 12:17:21 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001115 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 207 cs_uri_query = id-ORD-001115   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log   sourcetype = iis
>	2/7/19 5:47:16.000 PM	2019-02-07 12:17:16 10.10.10.12 GET /OrderDetail.aspx?id=ORD-001114 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 173 cs_uri_query = id-ORD-001114   host = WinServer2012   source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log

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 92

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 96

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 101

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 103

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 106

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 107

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 112

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 114

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 118

In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

- A. Evidence Gathering
- B. Evidence Handling
- C. Eradication
- D. Systems Recovery

**Answer:** A

#### NEW QUESTION 119

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 123

Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

- A. Hybrid Attack
- B. Bruteforce Attack
- C. Rainbow Table Attack
- D. Birthday Attack

**Answer:** B

#### NEW QUESTION 127

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 312-39 Exam with Our Prep Materials Via below:**

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