EC-Council

Exam Questions 312-39

Certified SOC Analyst (CSA)

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

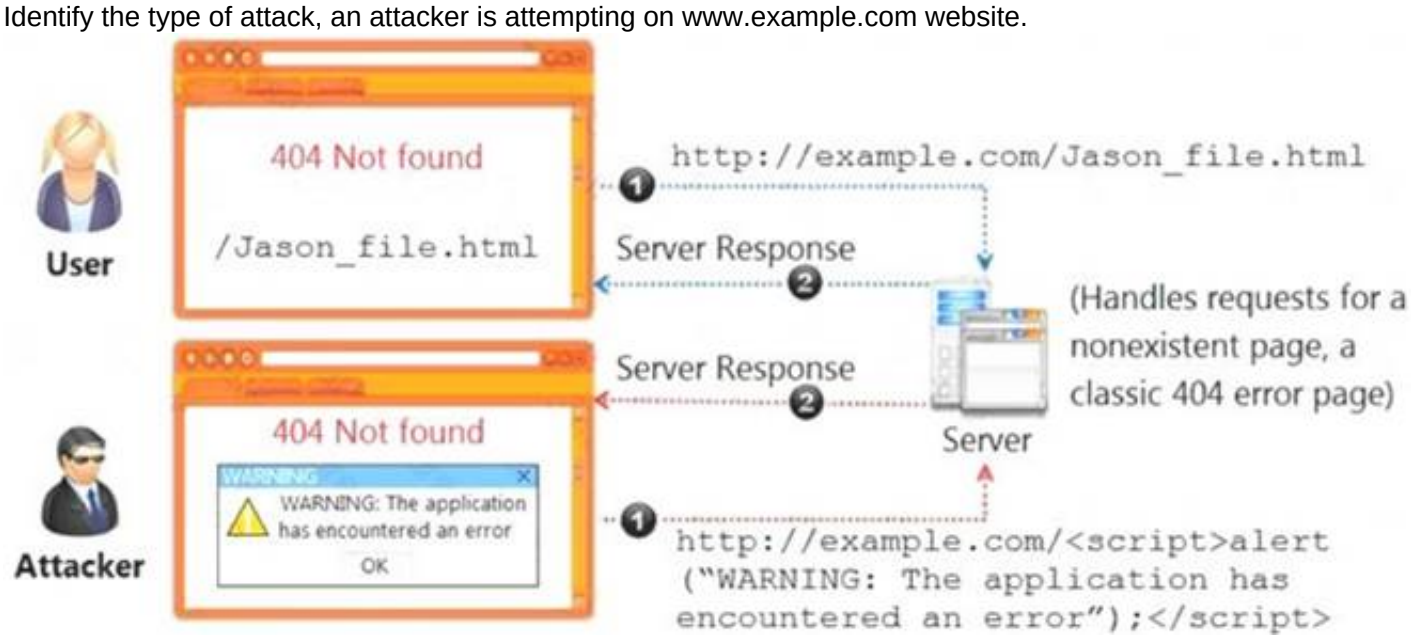
Answer: D

NEW QUESTION 2
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 3
Identify the type of attack, an attacker is attempting on www.example.com website.



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

Answer: A

NEW QUESTION 4
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 5
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 6
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 7
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 8
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 9
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 10
Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:
http://www.terabytes.com/process.php./../../../../etc/passwd

A. Directory Traversal Attack
B. SQL Injection Attack
C. Denial-of-Service Attack
D. Form Tampering Attack

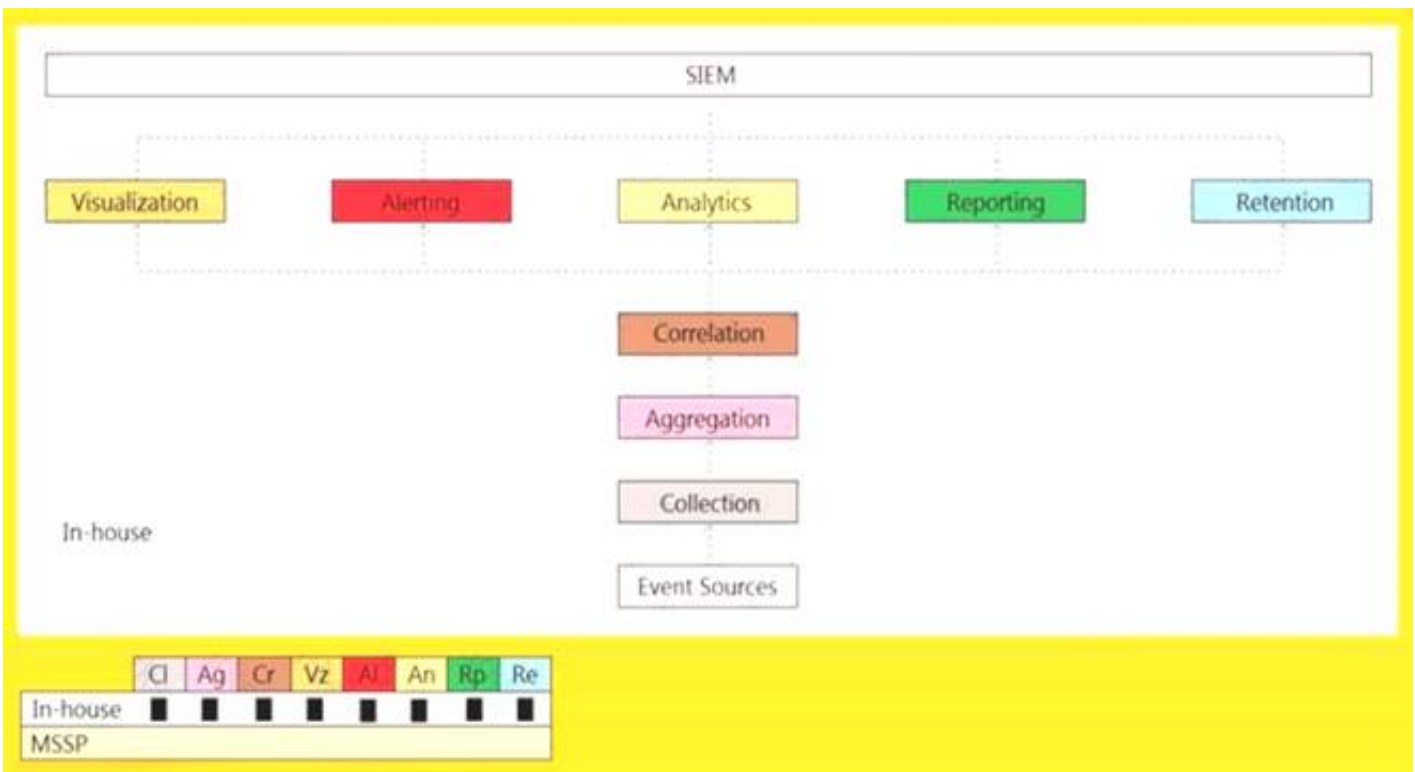
Answer: B

NEW QUESTION 10
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 12
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 14
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 16
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 21
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 25
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 30
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 32
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 34
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 38
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 43
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 45
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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