Exam Questions 312-39

Certified SOC Analyst (CSA)

https://www.2passeasy.com/dumps/312-39/

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
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 3
Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website.
Where will Harley find the web server logs, if he wants to investigate them for any anomalies?

A. SystemDrive%\inetpub\logs\LogFiles\W3SVCN
B. SystemDrive%\LogFiles\inetpub\logs\W3SVCN
C. %SystemDrive%\LogFiles\logs\W3SVCN
D. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN

Answer: B

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
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 6
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 7
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 8
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 9
Which of the following stage executed after identifying the required event sources?

A. Identifying the monitoring Requirements
B. Defining Rule for the Use Case
C. Implementing and Testing the Use Case
D. Validating the event source against monitoring requirement

Answer: D

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 12
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 16
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 21
What does the HTTP status codes 1XX represents?

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

Answer: A

NEW QUESTION 26
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 31
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 35
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 38
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 42
Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.
* 1. Strategic threat intelligence
* 2.Tactical threat intelligence
* 3.Operational threat intelligence
* 4.Technical threat intelligence

A. 2 and 3
B. 1 and 3
C. 3 and 4
D. 1 and 2

Answer: A

NEW QUESTION 44
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 47
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 52
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 56
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 60
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

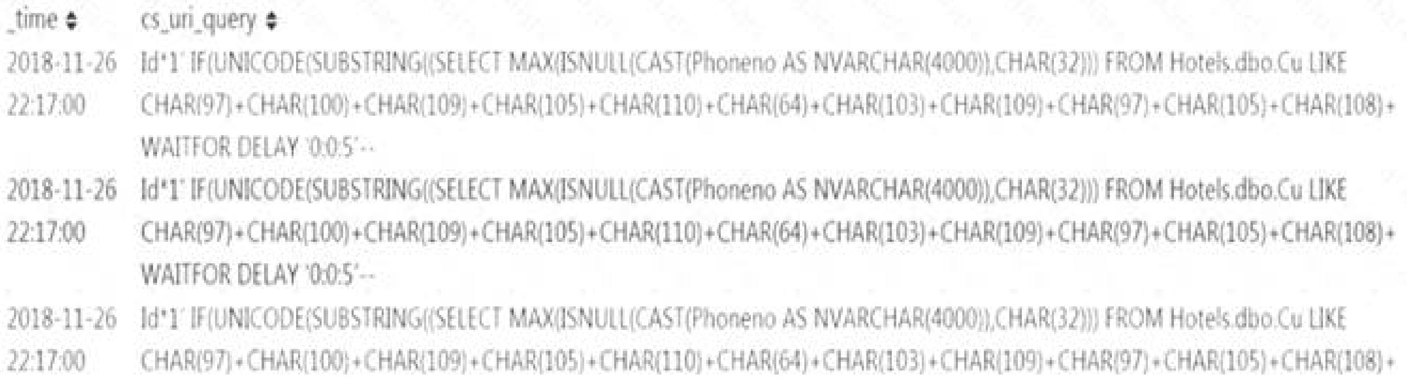
Answer: A

NEW QUESTION 61
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 62
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 67
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 72
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 77
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 82
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 86
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 91
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 92
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 97
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 102
InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.
Identify the job role of John.

A. Security Analyst – L1
B. Chief Information Security Officer (CISO)
C. Security Engineer
D. Security Analyst – L2

Answer: B

NEW QUESTION 106
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 110
In which phase of Lockheed Martin's – Cyber Kill Chain Methodology, adversary creates a deliverable malicious payload using an exploit and a backdoor?

A. Reconnaissance
B. Delivery
C. Weaponization
D. Exploitation

Answer: B

NEW QUESTION 115
Chloe, a SOC analyst with Jake Tech, is checking Linux systems logs. She is investigating files at /var/log/ wtmp.
What Chloe is looking at?

A. Error log
B. System boot log
C. General message and system-related stuff
D. Login records

Answer: D

NEW QUESTION 119
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 122
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

......