EC-Council

Exam Questions 312-39

Certified SOC Analyst (CSA)

NEW QUESTION 1
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 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
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 4
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 5
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 6
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 7
Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

A. $ tailf /var/log/sys/kern.log
B. $ tailf /var/log/kern.log
C. # tailf /var/log/messages
D. # tailf /var/log/sys/messages

Answer: B

NEW QUESTION 8
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 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
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 14
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 15
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 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 17
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 21
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 23
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 28
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 29
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 31
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

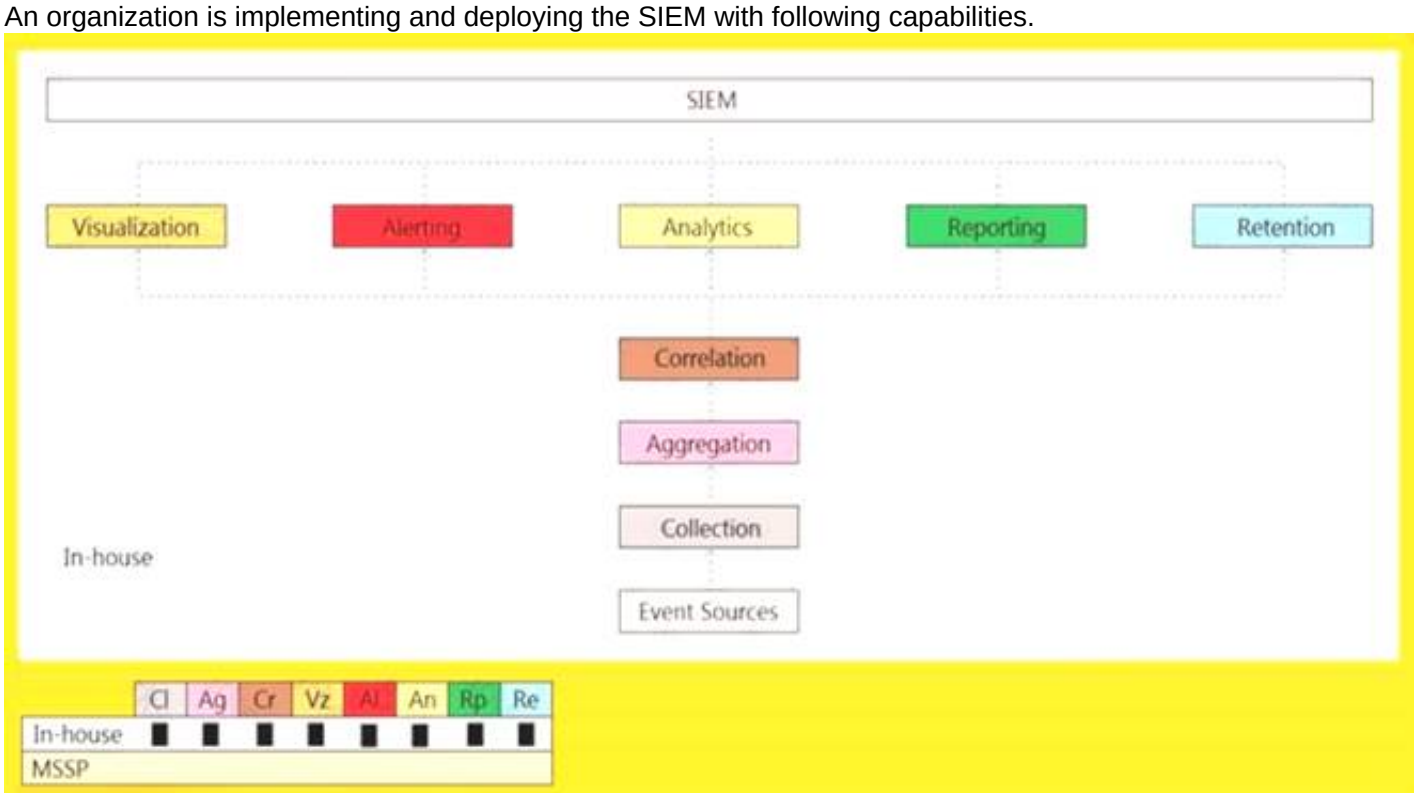
NEW QUESTION 36
Identify the HTTP status codes that represents the server error.

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

Answer: D

NEW QUESTION 41

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 42
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 46
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 49
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 53
Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.

_time	cs_uri_query
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE 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 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE 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 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE 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 56
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 57
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 60
Which of the following tool is used to recover from web application incident?

A. CrowdStrike FalconTM Orchestrator
B. Symantec Secure Web Gateway
C. Smoothwall SWG
D. Proxy Workbench

Answer: B

NEW QUESTION 64
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 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 70
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 74
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 78
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 83
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 86
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 90
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 92
Which of the following formula is used to calculate the EPS of the organization?

A. EPS = average number of correlated events / time in seconds
B. EPS = number of normalized events / time in seconds
C. EPS = number of security events / time in seconds
D. EPS = number of correlated events / time in seconds

Answer: A

NEW QUESTION 94
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 99
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 104
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 108
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 111
Which of the following is a Threat Intelligence Platform?

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

Answer: A

NEW QUESTION 115
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 119
What type of event is recorded when an application driver loads successfully in Windows?

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

Answer: D

NEW QUESTION 121
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 126
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 129
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 133
.....

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