

[Q53-Q75 Sep-2023 Realistic 312-39 Accurate & Verified Answers As Experienced in the Actual Test!



[Q53-Q75] Sep-2023 Realistic 312-39 Accurate & Verified Answers As Experienced in the Actual Test!

Sep-2023 Realistic 312-39 Accurate & Verified Answers As Experienced in the Actual Test!

Latest EC-COUNCIL 312-39 Practice Test Questions, Certified SOC Analyst (CSA) Exam Dumps

EC-COUNCIL 312-39 certification exam is a valuable credential for individuals who are looking to advance their career in the security field and demonstrate their expertise in the area of SOC analysis. With the right preparation and dedication, candidates can successfully pass the exam and take their career to the next level.

QUESTION 53

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?

- * She should immediately escalate this issue to the management
- * She should immediately contact the network administrator to solve the problem

- * She should communicate this incident to the media immediately
- * She should formally raise a ticket and forward it to the IRT

QUESTION 54

The Syslog message severity levels are labelled from level 0 to level 7.

What does level 0 indicate?

- * Alert
- * Notification
- * Emergency
- * Debugging

Severity Levels of Cisco Router Logs

Log messages in Cisco routers are categorized into eight severity levels ranging from 0 to 7. Each severity level determined a number and its corresponding name and UNIX syslog definitions. The lower severity number represents the high severity, and higher severity number represents the least severity.

| Level | Level name | Syslog definition | Description |
|-------|-------------|-------------------|-------------------------|
| 0 | Emergencies | LOG_EMERG | System unusable |
| 1 | Alerts | LOG_ALERT | Immediate action needed |
| 2 | Critical | LOG_CRIT | Critical conditions |
| 3 | Errors | LOG_ERR | Error conditions |
| 4 | Warnings | LOG_WARNING | Warning conditions |

QUESTION 55

Which of the following formula represents the risk levels?

- * Level of risk = Consequence * Severity
- * Level of risk = Consequence * Impact
- * Level of risk = Consequence * Likelihood
- * Level of risk = Consequence * Asset Value

Risk/Impact Assessment

The risk level is an assessment of the resulted impact on the network. Various methods exist to differentiate risk levels depending on the risk frequency and severity. One of the common methods used to classify risks is to develop a two-dimensional matrix.

To analyze risks, you need to work out the frequency or probability of an incident happening (likelihood) and the consequences it would have. This is referred to as the level of risk. Incident responders can represent and calculate the risk levels using the following formula:

Level of risk = consequence × likelihood

There are three risk levels: Very High (VH)/High (H), Medium (M), and Low (L)/Very Low (VL). Remember that control measures decrease the level of risk, but do not always eliminate them.

QUESTION 56

Which of the following formula is used to calculate the EPS of the organization?

- * EPS = average number of correlated events / time in seconds
- * EPS = number of normalized events / time in seconds
- * EPS = number of security events / time in seconds
- * EPS = number of correlated events / time in seconds

EPS, Volume, and Hardware Requirements



- Based on the scope, the SIEM size is decided
- SIEM size depends upon majority **three** factors:

1. Event Per Second (EPS)

- The SIEM sizing depends upon **how fast a security device generates events** and **how fast a SIEM product can correlate events** from those devices
- This ratio is referred to as SIEM Velocity. It is measured in terms of Events Per Second (EPS)
- EPS = number of security events / time in seconds
- EPS helps organizations to correlate the capacity of IT infrastructure and plan and choose best-suited SIEM solution for them

QUESTION 57

Which of the following formula represents the risk levels?

- * Level of risk = Consequence * Severity
- * Level of risk = Consequence * Impact
- * Level of risk = Consequence * Likelihood
- * Level of risk = Consequence * Asset Value

QUESTION 58

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?

- * Directory Traversal Attack
- * XSS Attack
- * SQL Injection Attack
- * Parameter Tampering Attack

QUESTION 59

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?

- * DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
- * IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
- * DNS/ Web Server logs with IP addresses.
- * Apache/ Web Server logs with IP addresses and Host Name.

Detect Attempt of Communicating over Private Network (TOR Network)



Users can use private network such as TOR Network to hide their malicious intent

If you found outside host is TOR Network, then this can be **indication of an attack or reconnaissance event**

If you found user from inside corporate network is using TOR Network, this is an **indication of malicious insider**

| | |
|--------------------|---|
| Data Source | DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution |
| Anomaly/Signatures | Identify source IP address that are attempting to connect to TOR IP address |

QUESTION 60

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.

- * Security Analyst – L1
- * Chief Information Security Officer (CISO)
- * Security Engineer
- * Security Analyst – L2

QUESTION 61

Which of the following contains the performance measures, and proper project and time management details?

- * Incident Response Policy
- * Incident Response Tactics
- * Incident Response Process
- * Incident Response Procedures

Develop IR Policy



Policy is a set of guidelines used to **achieve goals and objectives of incident response** initiative set by the IR plan

- IR policies contain:
- 1 Statement of **management commitment** to IR plan
 - 2 **Purpose and Objectives** of the policy
 - 3 **Scope** of the policy
 - 4 Definition of **security incidents** and their consequences within the context of the organization
 - 5 Organizational structure and **delineation of roles, responsibilities, and levels of authority**
 - 6 Guidelines for **prioritization** or assigning severity levels
 - 7 Performance **measures** and proper **project management and time management** details
 - 8 Reporting guidelines
 - 9 Guidelines for **communication** within and outside of the organization

QUESTION 62

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.

- * High
- * Extreme
- * Low
- * Medium

QUESTION 63

Which of the log storage method arranges event logs in the form of a circular buffer?

- * FIFO
- * LIFO
- * non-wrapping
- * wrapping

QUESTION 64

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?

- * Parameter Tampering Attack
- * XSS Attack
- * Directory Traversal Attack
- * SQL Injection Attack

QUESTION 65

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?

- * SystemDrive%inetpublogsLogFilesW3SVCN
- * SystemDrive%LogFilesinetpublogsW3SVCN

- * %SystemDrive%LogFileslogsW3SVCN
- * SystemDrive% inetpubLogFileslogsW3SVCN

Internet Information Services (IIS) Logs



Internet Information Services (IIS) is a **web server for Windows** server that hosts anything on the Web.

IIS consists of many log files. Log file formats provide different information like **IP address**, different sites visited by the user with **date and time**.

IIS log file provides useful information regarding person who visited your site, what information is viewed and when it is viewed, the activity of various web applications, etc.

Proper analysis of IIS log files will also provide **demographic information** and the **usage of IIS server**.

The log files are located by default at:

- IIS 6.0
%system32%\LogFiles\W3SVCN
- IIS 7.0
%SystemDrive%\inetpub\logs\LogFiles\W3SVCN
- IIS 8.0
%SystemDrive%\inetpub\logs\LogFiles
- IIS 10.0
%SystemDrive%\inetpub\logs\LogFiles

QUESTION 66

Which of the following attack can be eradicated by disabling of allow_url_fopen and allow_url_include in the php.ini file?

- * File Injection Attacks
- * URL Injection Attacks
- * LDAP Injection Attacks
- * Command Injection Attacks

QUESTION 67

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

- * Reconnaissance
- * Delivery
- * Weaponization
- * Exploitation

QUESTION 68

John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regexp `/(.|%25)2E)(.|%25)2E)/(|%25)2F|(|%25)5C)/i`.

What does this event log indicate?

- * XSS Attack
- * SQL injection Attack
- * Directory Traversal Attack
- * Parameter Tampering Attack

QUESTION 69

Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash

values to crack the password.

- * Dictionary Attack
- * Rainbow Table Attack
- * Bruteforce Attack
- * Syllable Attack

QUESTION 70

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?

- * Complaint to police in a formal way regarding the incident
- * Turn off the infected machine
- * Leave it to the network administrators to handle
- * Call the legal department in the organization and inform about the incident

QUESTION 71

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.
- * 1 and 2
 - * 2 and 3
 - * 1 and 4
 - * 3 and 1

QUESTION 72

Which of the following factors determine the choice of SIEM architecture?

- * SMTP Configuration
- * DHCP Configuration
- * DNS Configuration
- * Network Topology

QUESTION 73

Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?

- * `$ tailf /var/log/sys/kern.log`
- * `$ tailf /var/log/kern.log`
- * `# tailf /var/log/messages`
- * `# tailf /var/log/sys/messages`

QUESTION 74

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?

- * Error log
- * System boot log
- * General message and system-related stuff
- * Login records

QUESTION 75

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?

- * SQL Injection Attack
- * Parameter Tampering Attack
- * XSS Attack
- * Directory Traversal Attack

EC-COUNCIL 312-39 certification exam, also known as the Certified SOC Analyst (CSA) exam, is designed for individuals who want to validate their skills and knowledge in the field of security operations center (SOC) analysis. 312-39 exam covers various topics related to SOC operations, including threat detection and response, incident management, and vulnerability management. Certified SOC Analyst (CSA) certification is recognized globally and is highly sought after by employers looking for skilled SOC analysts.

Free 312-39 Exam Files Downloaded Instantly 100% Dumps & Practice Exam:

<https://www.exams4sures.com/EC-COUNCIL/312-39-practice-exam-dumps.html>