Exam Questions 312-39

Certified SOC Analyst (CSA)

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

NEW QUESTION 1
Robin, a SOC engineer in a multinational company, is planning to implement a SIEM. He realized that his organization is capable of performing only Correlation, Analytics, Reporting, Retention, Alerting, and Visualization required for the SIEM implementation and has to take collection and aggregation services from a Managed Security Services Provider (MSSP).
What kind of SIEM is Robin planning to implement?

A. Self-hosted, Self-Managed
B. Self-hosted, MSSP Managed
C. Hybrid Model, Jointly Managed
D. Cloud, Self-Managed

Answer: B

NEW QUESTION 2
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 3
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 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
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 6
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 7
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 8
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 9
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 10
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 10
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 12
Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.

A. Post-Incident Activities
B. Incident Recording and Assignment
C. Incident Triage
D. Incident Disclosure

Answer: B

NEW QUESTION 13
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 19
Which of the following service provides phishing protection and content filtering to manage the Internet experience on and off your network with the acceptable use or compliance policies?

A. Apility.io
B. Malstrom
C. OpenDNS
D. I-Blocklist

Answer: C

NEW QUESTION 22
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 23
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 24
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 26
What does the HTTP status codes 1XX represents?

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

Answer: A

NEW QUESTION 28
Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?

A. De-Militarized Zone (DMZ)
B. Firewall
C. Honeypot
D. Intrusion Detection System

Answer: C

NEW QUESTION 32
Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

A. Windows Event Log
B. Web Server Logs
C. Router Logs
D. Switch Logs

Answer: B

NEW QUESTION 34
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 36
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 38
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 43
Which encoding replaces unusual ASCII characters with "%" followed by the character’s two-digit ASCII code expressed in hexadecimal?

A. Unicode Encoding
B. UTF Encoding
C. Base64 Encoding
D. URL Encoding

Answer: D

NEW QUESTION 47
Identify the HTTP status codes that represents the server error.

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

Answer: D

NEW QUESTION 50
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 54
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 58
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 59
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 61
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 62
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 66
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 69
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

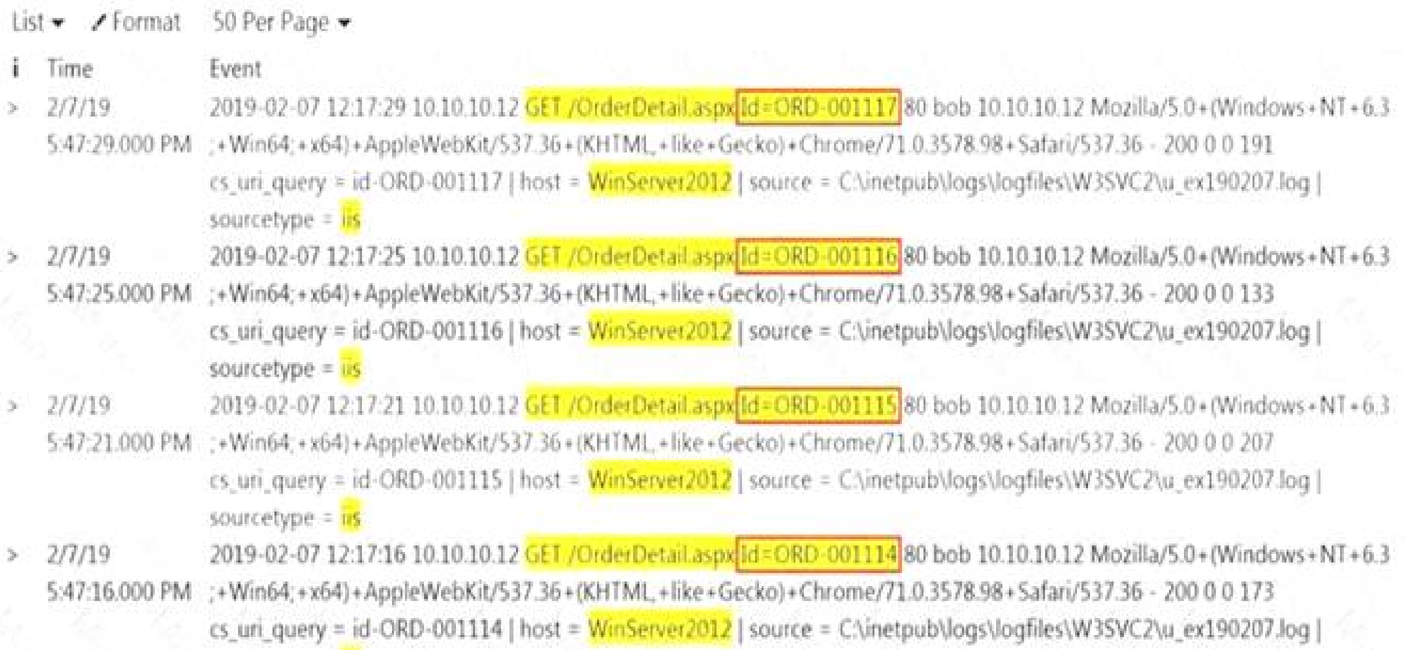
Answer: B

NEW QUESTION 74
Which of the following 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 76
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.



```
i  Time              Event
>  2/7/19            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
   5:47:29.000 PM    ;+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            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
   5:47:25.000 PM    ;+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            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
   5:47:21.000 PM    ;+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            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
   5:47:16.000 PM    ;+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 80
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 81
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.

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

Answer: A

NEW QUESTION 82
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 84
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 87
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 89
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 90
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 95
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 98
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 102
......