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
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 3
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 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
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 8
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 9
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 10
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 10
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 14
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 15
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 17
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?

A. SQL Injection Attack
B. Parameter Tampering Attack
C. XSS Attack
D. Directory Traversal Attack

Answer: A

NEW QUESTION 18
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 22
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 25
Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads. What does this indicate?

A. Concurrent VPN Connections Attempt
B. DNS Exfiltration Attempt
C. Covering Tracks Attempt
D. DHCP Starvation Attempt

Answer: B

NEW QUESTION 28
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 30
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 34
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 37
......