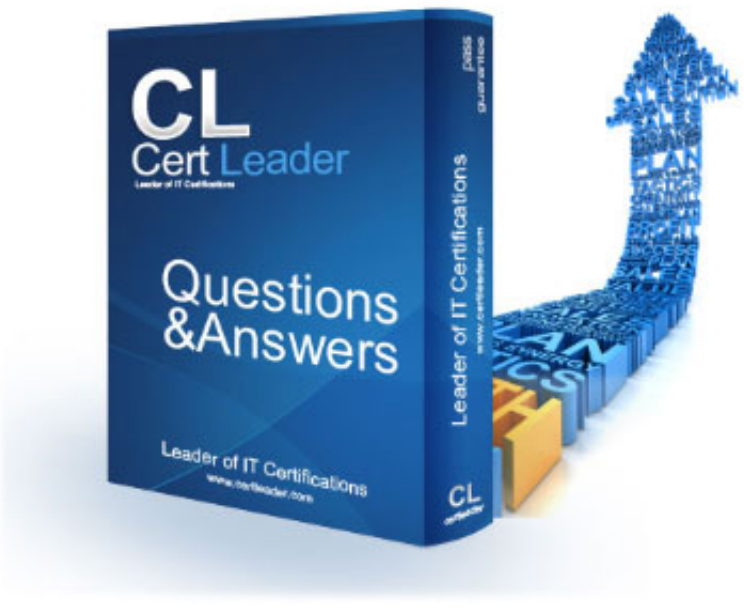
312-39 Dumps

Certified SOC Analyst (CSA)

https://www.certleader.com/312-39-dumps.html



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

A. Incident Response Policy
B. Incident Response Tactics
C. Incident Response Process
D. Incident Response Procedures

Answer: D

NEW QUESTION 5
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 6
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 7
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 8

What does the HTTP status codes 1XX represents?

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

Answer: A

NEW QUESTION 9
A type of threat intelligent that find out the information about the attacker by misleading them is known as.

A. Threat trending Intelligence
B. Detection Threat Intelligence
C. Operational Intelligence
D. Counter Intelligence

Answer: C

NEW QUESTION 10
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 10
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 13
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 16
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 17
John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regex
/(\.|(%|%25)2E)(\.|(%|%25)2E)(\/|(%|%25)2F|\\|(%|%25)5C)/i.
What does this event log indicate?

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

Answer: A

NEW QUESTION 20
What is the process of monitoring and capturing all data packets passing through a given network using different tools?

A. Network Scanning
B. DNS Footprinting
C. Network Sniffing
D. Port Scanning

Answer: C

NEW QUESTION 25
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 29
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 34
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?

A. Evidence Gathering
B. Evidence Handling
C. Eradication
D. Systems Recovery

Answer: A

NEW QUESTION 37
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 42
Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A. Hybrid Attack
B. Bruteforce Attack
C. Rainbow Table Attack
D. Birthday Attack

Answer: B

NEW QUESTION 46
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-39 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-39-dumps.html