EC-COUNCIL - Efficient 312-39 - Test Certified SOC Analyst (CSA) Collection Pdf

BONUS!!! Download part of ValidVCE 312-39 dumps for free: https://drive.google.com/open?id=14GPUgYgdVAc0cJXGrBetj7iyPryo4O-o

We not only do a good job before you buy our 312-39 test guides, we also do a good job of after-sales service. Because we are committed to customers who decide to choose our 312-39 study tool. We put the care of our customers in an important position. All customers can feel comfortable when they choose to buy our 312-39 study tool. We have specialized software to prevent the leakage of your information and we will never sell your personal information because trust is the foundation of cooperation between both parties. A good reputation is the driving force for our continued development. Our company has absolute credit, so you can rest assured to buy our 312-39 test guides.

EC-COUNCIL 312-39 (Certified SOC Analyst (CSA)) certification exam is designed to test the knowledge and skills of candidates in the field of security operations center (SOC) analysis. Certified SOC Analyst (CSA) certification is recognized globally and is highly valued by employers in the cybersecurity industry. 312-39 Exam is designed to test the candidate's ability to handle security incidents, detect and respond to security threats, and manage the security infrastructure of an organization.

>> Test 312-39 Collection Pdf <<

312-39 Latest Materials | Valuable 312-39 Feedback

The passing rate of our products is the highest. Many candidates can also certify for our EC-COUNCIL 312-39 study materials. As long as you are willing to trust our EC-COUNCIL 312-39 Preparation materials, you are bound to get the EC-COUNCIL 312-39 certificate. Life needs new challenge. Try to do some meaningful things.

The CSA certification exam covers a wide range of topics, including network security, threat intelligence, incident response, and compliance. It is designed to test the candidate's ability to analyze and interpret security data, identify potential security threats, and recommend appropriate responses to mitigate those threats. 312-39 Exam also assesses the candidate's understanding of security policies and procedures, as well as their ability to communicate effectively with stakeholders.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q109-Q114):

NEW QUESTION # 109
Which of the following formula is used to calculate the EPS of the organization?

- A. EPS = number of security events / time in seconds
- B. EPS = number of correlated events / time in seconds

- C. EPS = average number of correlated events / time in seconds
- D. EPS = number of normalized events / time in seconds

Answer: B

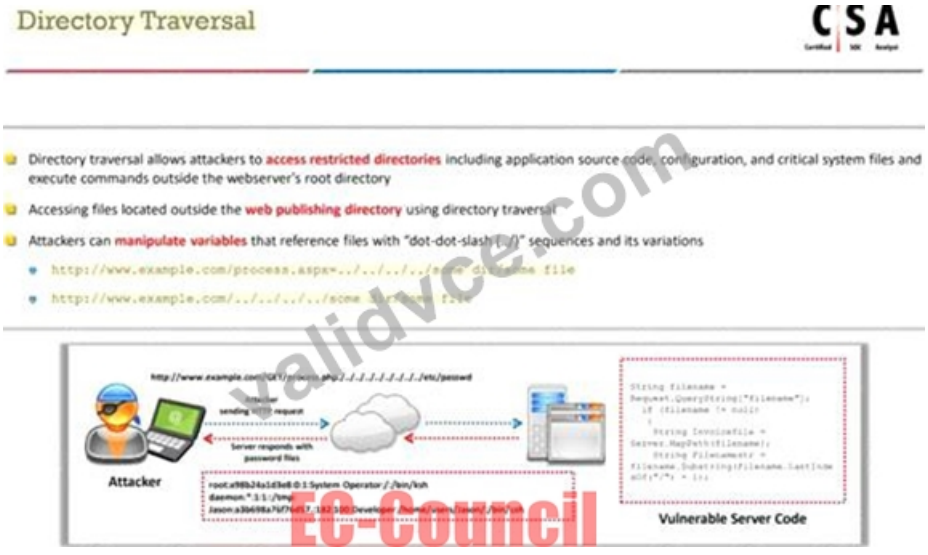
Explanation:
In the context of a Security Operations Center (SOC), EPS typically refers to "Events Per Second," which is a measure of the number of security events processed in one second. The correct formula for calculating EPS in a SOC environment is the number of correlated events divided by the time in seconds. Correlated events are those that have been analyzed and aggregated by the SOC's security information and event management (SIEM) system, indicating a potential security incident. This metric helps in understanding the operational load and performance of the SOC.
References: The information is aligned with the EC-Council's Certified SOC Analyst (CSA) course material and best practices, which emphasize the importance of understanding and managing SOC operational metrics such as EPS for effective security monitoring and incident response12.

NEW QUESTION # 110
Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:
http://www.terabytes.com/process.php./../../../../etc/passwd

- A. Form Tampering Attack
- B. Directory Traversal Attack
- C. SQL Injection Attack
- D. Denial-of-Service Attack

Answer: B

Explanation:
The attack described is a Directory Traversal Attack. This type of attack occurs when an attacker exploits vulnerabilities in a web application (or a web server's software) to gain unauthorized access to files and directories that are stored outside of the web root folder. By manipulating variables that reference files with ../ sequences (also known as dot-dot-slash), the attacker can move up the directory hierarchy and access files or directories that should be restricted. This can lead to information disclosure, such as reading sensitive files like /etc/passwd, which contains user password details in Unix-based systems.
In the given URL http://www.terabytes.com/process.php./../../../../etc/passwd, the attacker uses the ../ pattern to navigate up from the current directory where process.php resides, aiming to reach the root directory and then descend into the /etc/ directory to access the passwd file. This is a classic example of a Directory Traversal Attack.
References: The EC-Council's Certified SOC Analyst course covers various types of cyber attacks, including Directory Traversal Attacks. Specific references to this type of attack can be found in the EC-Council's official training materials for the Certified SOC Analyst (CSA) program, such as the CSA study guide and related courses that discuss web application vulnerabilities and attacks123.



NEW QUESTION # 111

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/server/reputation.data
- B. /etc/ossim/siem/server/reputation/data
- C. /etc/siem/ossim/server/reputation.data
- D. /etc/ossim/reputation

Answer: D

NEW QUESTION # 112
A security team is designing SIEM use-case logic to detect privilege escalation attempts on Windows servers.
They have already identified and validated the necessary event sources (e.g., Active Directory logs, Windows Security logs). What should be their next step in the use case logic development process?

- A. Define response actions for detected incidents before writing the rules
- B. Define correlation rules and conditions that detect specific privilege escalation patterns
- C. Implement and test the use case immediately in the production SIEM environment
- D. Collect historical security logs to confirm the use case is necessary

Answer: B

Explanation:
Once the event sources are validated, the next logical step is to define the detection logic-correlation rules and conditions that represent privilege escalation patterns. In SOC engineering, validated sources mean you have the raw ingredients; now you must specify what "bad" looks like in those logs. For privilege escalation on Windows, this might include abnormal group membership changes, creation of new privileged accounts, suspicious privilege assignment events, UAC bypass indicators, or admin logons from non-admin workstations. Defining correlation rules also includes setting time windows, selecting strong pivots (account, host, SID), and incorporating context to reduce noise (approved admin accounts, maintenance windows, known tooling). Defining response actions is important, but it should follow detection logic so you don't automate reactions to unstable or noisy detections. Testing immediately in production is risky; best practice is to test in a controlled manner or pilot mode first to avoid operational disruption and excessive false positives.
Collecting historical logs can help tune baselines, but the scenario states sources are already validated; the next step is to codify the conditions that detect the targeted behavior.

NEW QUESTION # 113
The SOC analyst at a national cybersecurity agency detected unusual system behavior on critical infrastructure servers. Initial scans flagged potential malware activity. Due to the sophisticated nature of the suspected attack, including registry modifications, process injection, and unauthorized tasks, the case was escalated to the forensic team. The forensic team suspects the malware is designed for stealthy data exfiltration. To assess the compromise, they captured system snapshots before and after suspected infection to identify unauthorized changes and anomalies. Which process are they following by capturing and comparing system snapshots to detect unauthorized changes?

- A. Host integrity monitoring
- B. Threat intelligence gathering
- C. Signature-based detection
- D. Digital forensics

Answer: A

Explanation:
Capturing and comparing system snapshots before and after suspected compromise is a core method of host integrity monitoring. The goal is to detect unauthorized changes to critical system components such as registry keys, scheduled tasks, services, binaries, configuration files, and security settings. By comparing a known-good baseline snapshot to a suspected-compromised state, analysts can identify what changed, when it changed (with supporting timestamps), and which changes are anomalous relative to expected patching or administrative activity. While this activity can occur within a broader digital forensics investigation, the specific technique described-baseline comparison to detect unauthorized modification-is integrity monitoring. Signature-based detection focuses on matching known indicators (hashes, strings, known patterns) and does not rely on before/after snapshot comparison. Threat intelligence gathering is about collecting and analyzing information on external threats, not directly comparing host states. From a SOC standpoint, integrity monitoring supports rapid scoping and eradication because it highlights persistence and tampering

mechanisms that must be removed and can reveal stealth modifications that evade signature scanners. It also supports compliance requirements by demonstrating configuration control and unauthorized- change detection capabilities.

NEW QUESTION # 114

.....

312-39 Latest Materials: https://www.validvce.com/312-39-exam-collection.html

- New Test 312-39 Collection Pdf | Valid 312-39 Latest Materials: Certified SOC Analyst (CSA) 100% Pass □ Search for ➡ 312-39 □□□ and download it for free immediately on ☀ www.troytecdumps.com □☀□ □312-39 PDF
- Valid Test 312-39 Experience □ New 312-39 Exam Name □ 312-39 Valid Test Prep □ Search for ▸ 312-39 ◂ on □ www.pdfvce.com □ immediately to obtain a free download □312-39 Latest Exam Review
- Test 312-39 Collection Pdf 100% Pass | Pass-Sure 312-39 Latest Materials: Certified SOC Analyst (CSA) □ Open 「 www.troytecdumps.com 」 enter 【 312-39 】 and obtain a free download □New 312-39 Exam Name
- Pass Guaranteed Quiz EC-COUNCIL 312-39 - Test Certified SOC Analyst (CSA) Collection Pdf □ Simply search for 【 312-39 】 for free download on ⇛ www.pdfvce.com ⇚ □312-39 Braindumps Torrent
- Pass Guaranteed Quiz EC-COUNCIL - Authoritative 312-39 - Test Certified SOC Analyst (CSA) Collection Pdf □ Open ▹ www.vce4dumps.com ◃ enter □ 312-39 □ and obtain a free download □312-39 Latest Exam Review
- Test 312-39 Collection Pdf 100% Pass | Pass-Sure 312-39 Latest Materials: Certified SOC Analyst (CSA) □ Search for （ 312-39 ） on ▸ www.pdfvce.com ◂ immediately to obtain a free download □312-39 Valid Exam Labs
- 312-39 High Quality □ Complete 312-39 Exam Dumps □ 312-39 Valid Exam Labs □ Easily obtain free download of □ 312-39 □ by searching on [www.easy4engine.com] □312-39 Braindumps Torrent
- 312-39 Latest Test Guide □ 312-39 Reliable Test Objectives □ 312-39 Reliable Test Objectives □ Search for ▸ 312-39 ◂ and download it for free on { www.pdfvce.com } website □312-39 Latest Exam Review
- EC-COUNCIL 312-39 exam study materials □ Search for ✔ 312-39 □✔□ and download it for free on ➽ www.prepawaypdf.com □ website □Test 312-39 Collection Pdf
- EC-COUNCIL 312-39 exam study materials □ Download 【 312-39 】 for free by simply entering ➽ www.pdfvce.com □ website □312-39 Related Content
- 312-39 Online Training Materials □ 312-39 Reliable Source □ 312-39 Latest Test Guide □ Search for ➽ 312-39 □ and download exam materials for free through （ www.vce4dumps.com ） □New 312-39 Exam Name
- zoeiyip184603.tokka-blog.com, advicebookmarks.com, cormaciqpk242778.wikinstructions.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, socialimarketing.com, elodiecmjm773268.wikikarts.com, bookmark-media.com, socialbraintech.com, alyshaxgnp119422.wikifiltraciones.com, Disposable vapes

BTW, DOWNLOAD part of ValidVCE 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=14GPUgYgdVAc0cJXGrBetj7iyPryo4O-o