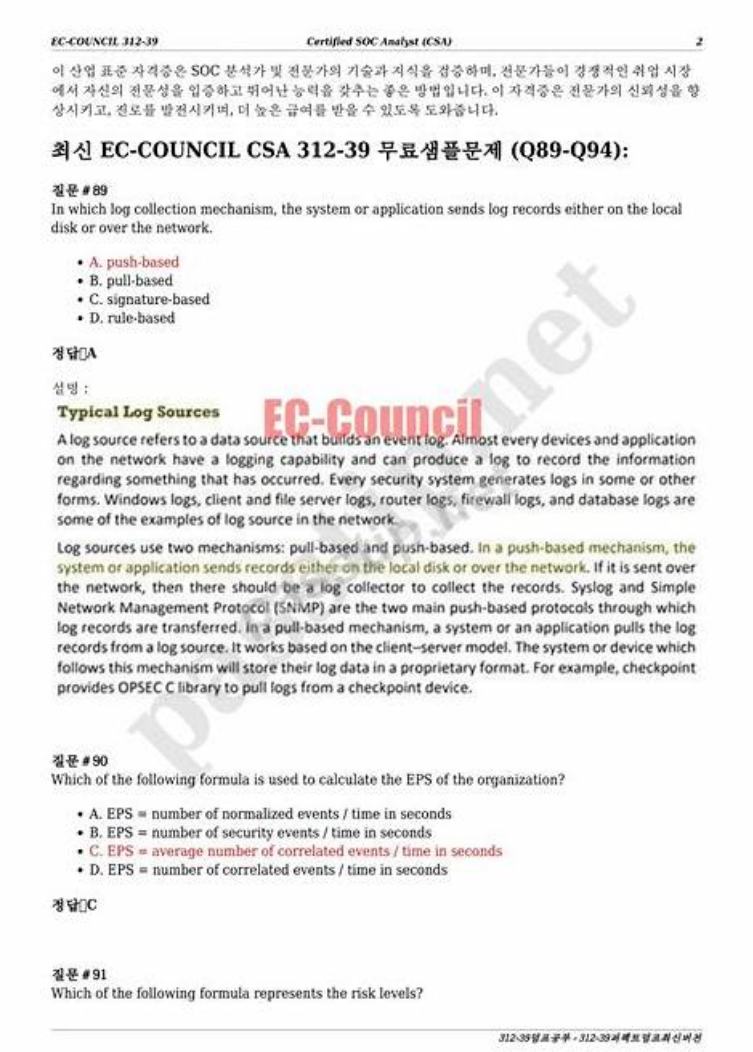
312-39시험정보, 312-39최고품질덤프문제보기



EC-COUNCIL 312-39 Certified SOC Analyst (CSA) 2

이 산업 표준 자격증은 SOC 분석가 및 전문가의 기술과 지식을 검증하며, 전문가들이 경쟁적인 취업 시장에서 자신의 전문성을 입증하고 뛰어난 능력을 갖추는 좋은 방법입니다. 이 자격증은 전문가의 신뢰성을 향상시키고, 전로를 발전시키며, 더 높은 급여를 받을 수 있도록 도와줍니다.

최신 EC-COUNCIL CSA 312-39 무료샘플문제 (Q89-Q94):

질문 # 89
In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

- A. push-based
- B. pull-based
- C. signature-based
- D. rule-based

정답□A

설명 :

Typical Log Sources

A log source refers to a data source that builds an event log. Almost every devices and application on the network have a logging capability and can produce a log to record the information regarding something that has occurred. Every security system generates logs in some or other forms. Windows logs, client and file server logs, router logs, firewall logs, and database logs are some of the examples of log source in the network.

Log sources use two mechanisms: pull-based and push-based. In a push-based mechanism, the system or application sends records either on the local disk or over the network. If it is sent over the network, then there should be a log collector to collect the records. Syslog and Simple Network Management Protocol (SNMP) are the two main push-based protocols through which log records are transferred. In a pull-based mechanism, a system or an application pulls the log records from a log source. It works based on the client–server model. The system or device which follows this mechanism will store their log data in a proprietary format. For example, checkpoint provides OPSEC C library to pull logs from a checkpoint device.

질문 # 90
Which of the following formula is used to calculate the EPS of the organization?

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

정답□C

질문 # 91
Which of the following formula represents the risk levels?

312-39덤프공부 - 312-39최신덤프최신버전

2026 ExamPassdump 최신 312-39 PDF 버전 시험 문제집과 312-39 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1qjvj95iebphvowPPWcOUGvUaWw1qWB4L

EC-COUNCIL인증 312-39시험은 IT인증시험중 가장 인기있는 시험입니다. EC-COUNCIL인증 312-39시험패스는 모든 IT인사들의 로망입니다. ExamPassdump의 완벽한 EC-COUNCIL인증 312-39덤프로 시험준비하여 고득점으로 자격증을 따보세요.

EC-COUNCIL은 교육 과정, 학습 가이드, 모의 시험을 비롯한 다양한 자원을 제공하여 CSA 자격증 시험 준비를 지원합니다. 이러한 자원들은 시험 목표를 이해하고 시험에서 예상되는 질문 유형에 대비하는 데 도움이 되도록 설계되었습니다. 또한, EC-COUNCIL은 인증 윤리 해커(CEH)와 인증 네트워크 방어자(CND)를 비롯한 다양한 사이버 보안 인증을 제공합니다.

EC-COUNCIL 312-39 (Certified SOC Analyst (CSA)) 시험은 보안 운영 센터 (SOC)와 관련된 고급 수준의 기술과 지식에 중점을 둔 세계적으로 인정받는 자격증 시험입니다. 이 자격증은 사이버 위협으로부터 기관을 보호하는 능력을 입증하고자 하는 보안 전문가들을 대상으로 설계되었습니다. 이 시험은 사고 대응, 위협 인텔리전스, 로그 관리 등 다양한 주제를 다룹니다.

>> 312-39시험정보 <<

312-39최고품질 덤프문제보기 & 312-39공부자료

EC-COUNCIL 312-39 덤프로 많은 분들께서 EC-COUNCIL 312-39시험을 패스하여 자격증을 취득하게 도와드렸지만 저희는 자만하지않고 항상 초심을 잊지않고 더욱더 퍼펙트한EC-COUNCIL 312-39덤프를 만들기 위해 모든 심여를 기울일것을 약속드립니다.

최신 EC-COUNCIL CSA 312-39 무료샘플문제 (Q144-Q149):

질문 # 144
You are working as a SOC analyst in a multinational company with multiple data centers and remote offices.
Security logs are stored locally at each site, making it difficult to correlate incidents across different locations.
Recently, an advanced persistent threat (APT) compromised multiple servers, but due to multiple sources of logs and inconsistent monitoring, the attack was detected only after significant data exfiltration. To improve visibility, streamline log analysis, and enable faster incident response, you need to implement a solution that aggregates logs from all sources into a unified system. Which solution will you implement?

- A. Local logging
- B. Event tracing
- C. Centralized logging
- D. Distributed logging

정답：C

설명:
Centralized logging is the foundation for enterprise-wide visibility and correlation. When logs remain local at each site, SOC analysts lose the ability to quickly pivot across systems, detect multi-stage attacks, and correlate signals (for example, an identity compromise at one location leading to lateral movement and exfiltration at another). Centralizing logs into a SIEM or log analytics platform standardizes ingestion, parsing, retention, and search, enabling consistent detections and faster triage. It also improves incident response by providing a single source of truth for timelines and scoping. Distributed logging and local logging keep data fragmented; even if collection exists, the lack of central correlation slows investigations and increases blind spots-exactly what the scenario describes. "Event tracing" is typically an internal diagnostic
/telemetry method (often application or OS-level tracing) and is not the overarching architectural solution for aggregating logs across multiple sites. For SOC operations, centralized logging also supports governance and compliance by enforcing retention, access controls, and audit trails, and it enables consistent alerting and reporting across the entire environment.

질문 # 145
The SOC team is investigating a phishing attack that targeted multiple employees. During the Containment Phase, they need to determine how users interacted with the malicious email: whether they opened it, clicked links, downloaded attachments, or entered credentials. This information is critical to assessing impact and preventing further compromise. Which specific activity helps the SOC team understand user interactions with the phishing email?

- A. Blocking command-and-control (C2) and email traffic
- B. User action verification
- C. Monitoring and containment validation
- D. Malware infection check

정답：B

설명:
User action verification is the activity that directly answers "what did users do with the phishing message?" In SOC containment, you need to rapidly determine exposure: who opened the email, who clicked the URL, who opened an attachment, and who submitted credentials. This drives priority actions such as password resets, session revocation, MFA re-registration, endpoint isolation, URL/domain blocking, mailbox searches for similar messages, and targeted user notifications. Monitoring/containment validation confirms whether containment actions are effective (e.g., blocks are working, incidents aren't spreading), but it does not specifically measure user interaction steps. Malware infection checks assess whether an endpoint is infected- useful if an attachment executed-but it comes after confirming interaction and is not the primary method to understand email engagement. Blocking C2 and email traffic is an active containment control, but it doesn't provide the "who clicked/opened" understanding needed to scope impacted users. SOC analysts typically use email gateway telemetry, message trace, safe links/safe attachments logs, and identity sign-in logs to verify user actions. Because the question is explicitly about understanding user interactions, "User action verification" is the best match.

질문 # 146
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. Birthday Attack
- B. Rainbow Table Attack
- C. Bruteforce Attack
- D. Hybrid Attack

정답：D

설명：

질문 # 147
Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

- A. Syllable Attack
- B. Rainbow Table Attack
- C. Dictionary Attack
- D. Bruteforce Attack

정답：C

질문 # 148
An organization is implementing and deploying the SIEM with following capabilities.
What kind of SIEM deployment architecture the organization is planning to implement?

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

정답：D

설명：

질문 # 149
.....

위해【 312-39 】를 검색하십시오312-39완벽한 시험덤프

- 312-39최신 덤프문제보기 □ 312-39인기자격증 시험대비자료 ✍ 312-39유효한 공부문제 □ ➠ www.pass4test.net □에서□ 312-39 □를 검색하고 무료로 다운로드하세요312-39유효한 공부문제
- 312-39시험대비 덤프 최신버전 □ 312-39인기자격증 시험대비자료 □ 312-39시험덤프데모 □ 지금➡ www.itdumpskr.com □□□에서➡ 312-39 □□□를 검색하고 무료로 다운로드하세요312-39인기자격증 시험덤프
- 312-39인기자격증 시험덤프 □ 312-39인증시험대비 덤프공부 □ 312-39최신버전 덤프자료 ～ 무료로 다운로드하려면✔ www.exampassdump.com □✔□로 이동하여➤ 312-39 □를 검색하십시오312-39인기자격증 시험덤프
- 312-39최고품질 시험덤프 공부자료 □ 312-39퍼펙트 덤프데모문제 다운 □ 312-39인증시험대비 덤프공부 □ 무료 다운로드를 위해 지금➤ www.itdumpskr.com □에서【 312-39 】검색312-39유효한 공부문제
- 퍼펙트한 312-39시험정보 최신버전 덤프데모 문제 □ 무료 다운로드를 위해 지금□ www.dumptop.com □에서 ☀ 312-39 □☀□검색312-39인증자료
- academy.rebdaa.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, lms.brollyacademy.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, thriveccs.org, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 ExamPassdump 최신 312-39 PDF 버전 시험 문제집과 312-39 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=1qjvj95iebphvowPPWcOUGvUaWw1qWB4L