最受歡迎的312-39考古題更新，免費下載312-39學習資料幫助妳通過312-39考試

BONUS!!! 免費下載PDFExamDumps 312-39考試題庫的完整版：https://drive.google.com/open?id=1To7t7DgJ8tEWTTHtBuh9MB1D22do_kwW

你還在為通過EC-COUNCIL 312-39認證考試難度大而煩惱嗎？你還在為了通過EC-COUNCIL 312-39認證考試廢寢忘食的努力復習嗎？想更快的通過EC-COUNCIL 312-39認證考試嗎？快快選擇我們PDFExamDumps吧！有了他可以迅速的完成你的夢想。

EC-Council 312-39（認證的SOC分析師（CSA））認證考試是一個絕佳的選擇，並且網絡安全專業人員希望通過在SOC分析中證明自己的技能和知識來促進職業生涯。該認證適用於SOC分析師，事件響應者，安全專業人員和網絡管理員。獲得認證可以幫助專業人員在職業生涯中脫穎而出並提高收入潛力。

為了準備考試，候選人可以參加EC-COUNCIL的認證SOC分析師（CSA）培訓計劃。該計劃旨在為候選人提供SOC運營實踐經驗，並涵蓋考試中將被測試的各種主題。該計劃還包括實踐練習、案例研究和模擬，以幫助候選人開發作為SOC分析師所需的技能。總的來說，EC-COUNCIL 312-39（認證SOC分析師（CSA））考試是尋求在網絡安全行業，特別是在SOC運營方面建立職業生涯的人士的優秀認證計劃。

>> 312-39考古題更新 <<

312-39認證題庫 - 312-39最新題庫資源

PDFExamDumps的產品不僅可以幫你順利通過EC-COUNCIL 312-39 認證考試，而且還可以享用一年的免費線上更新服務，把我們研究出來的最新產品第一時間推送給客戶，方便客戶對考試做好充分的準備。如果你考試失敗，我們會全額退款給你。

EC-COUNCIL 312-39: 認證 SOC 分析師 (CSA) 考試是專業安全人員願意展示他們在 SOC 分析方面的專業知識的有價值的認證。這項認證涵蓋了與 SOC 分析相關的各種主題，並受到領先的網絡安全行業組織的認可。隨著對熟練的 SOC 分析師的需求不斷增長，CSA 認證是尋求在這一領域提高職業前景的專業人士的有價值的資格證書。

最新的 EC-COUNCIL CSA 312-39 免費考試真題 (Q146-Q151):

問題 #146
A mid-sized healthcare organization is facing frequent phishing and ransomware attacks. They lack an internal SOC and want proactive threat detection and response capabilities. Compliance with HIPAA regulations is essential. The organization seeks a solution that includes both monitoring and rapid response to incidents. Which service best meets their needs?

- A. MDR with proactive threat hunting and incident containment
- B. Cloud-based SIEM with MSSP-managed services
- C. Self-hosted SIEM with in-house SOC analysts
- D. MSSP with 24/7 log monitoring and incident escalation

答案：A

解題說明：

Managed Detection and Response (MDR) best fits because it typically includes proactive threat hunting, continuous monitoring, and direct incident containment actions-exactly what an organization without an internal SOC needs when facing active phishing and ransomware threats. MDR providers usually operate with EDR/XDR-style telemetry, enabling rapid endpoint isolation, malicious process containment, and guided remediation, which is critical for ransomware where time-to-containment determines impact. An MSSP focused on log monitoring and escalation may provide visibility and alerting but often stops at notifying or ticketing rather than performing containment actions, which can slow response. A self-hosted SIEM with in- house analysts contradicts the constraint "lack an internal SOC" and requires significant staffing and engineering to be effective. A cloud SIEM with MSSP-managed services can be viable, but the question emphasizes proactive detection and response; MDR is the most directly aligned service model for hands-on containment and active hunting. For HIPAA, MDR also supports incident documentation, monitoring evidence, and response coordination, which helps meet regulatory expectations for safeguarding and incident handling.

問題 #147
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=3688 NOT (Account_Name=*$) .. .. ..
- B. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
- C. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...
- D. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..

答案：D

解題說明：
)ComprehensiveDetailedStepbyStepExplanation:InWindowssecurityeventlogs, EventCode4688signifiesaprocesscreationevent.TheSplunkquery'index=windowsLogName=SecurityEventCode =4688NOT(AccountName=)is used to fetch logs related to process creation activities. This query filters the logs to only show events where a new process has been created, which is indicated by EventCode 4688. The NOT (Account_Name=$)` part of the query excludes any events where the account name ends with a dollar sign, which typically represents a machine or service account. References: The EC-Council's Certified SOC Analyst (CSA) program provides detailed knowledge on security operation center (SOC) operations, including log management and correlation, SIEM deployment, advanced incident detection, and incident response. The CSA course materials and study guides cover the use of Splunk for monitoring and analyzing security events, which would include the creation of such queries for process creation monitoring1

問題 #148
The threat intelligence, which will help you, understand adversary intent and make informed decision to ensure appropriate security in alignment with risk.
What kind of threat intelligence described above?

- A. Tactical Threat Intelligence
- B. Operational Threat Intelligence
- C. Functional Threat Intelligence
- D. Strategic Threat Intelligence

答案：D

問題 #149
A financial services company implements a SIEM solution to enhance cybersecurity. Despite deployment, it fails to detect known attacks or suspicious activities. Although reports are generated, the team struggles to interpret them. Investigation shows that critical logs from firewalls, IDS, and endpoint devices are not reaching the SIEM. What is the reason the SIEM is not functioning as expected?

- A. Improper configuration or design of the SIEM deployment architecture
- B. Difficulty handling the volume of collected log data
- C. Delays in log collection and analysis due to system performance issues
- D. Lack of understanding of SIEM features and capabilities

答案：A

解題說明：
If critical logs are not reaching the SIEM, the most direct root cause is an architectural or configuration failure in the SIEM deployment. A SIEM's detection capability depends on ingesting the right telemetry from key control points (network, endpoint, identity, cloud). Missing firewall, IDS, and endpoint logs creates blind spots that will prevent detections from firing, even for well-known attacks, because the SIEM simply lacks the required evidence. This commonly happens due to misconfigured collectors/agents, incorrect forwarding rules, blocked network paths, wrong ports/protocols, parsing failures, certificate/auth issues, or incomplete onboarding of data sources. While lack of SIEM knowledge can affect tuning and interpretation, it does not explain missing log delivery. Volume-handling issues typically show up as ingestion throttling, dropped events, or delayed indexing after logs are onboarded-not as a complete absence of critical sources.
Performance delays can degrade detection timeliness, but again the scenario states the logs are not reaching the SIEM at all. From a SOC engineering standpoint, the first troubleshooting steps are data pipeline validation (connectivity, agent health, message counts), ingestion dashboards, and source-side forwarding verification. Therefore, improper configuration or deployment architecture is the correct reason.

問題 #150
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=3688 NOT (Account_Name=*$) .. .. ..
- B. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
- C. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...
- D. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..

答案：D

問題 #151
.....