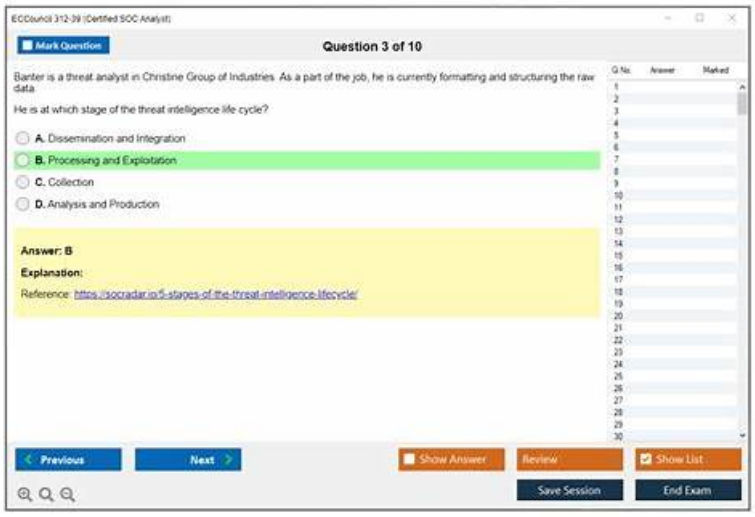
312-39 Testing Engine - 312-39 Prüfungen



P.S. Kostenlose und neue 312-39 Prüfungsfragen sind auf Google Drive freigegeben von Fast2test verfügbar: https://drive.google.com/open?id=1AXTLkt3HWtYVJ0kq_YvBldLE-s02cAX-

Fast2test hat die spezielle Schulungsunterlagen zur EC-COUNCIL 312-39 Zertifizierungsprüfung. Sie können mit wenig Zeit und Geld Ihre IT-Fachkenntnisse in kurzer Zeit verbessern und somit Ihre Fachkenntnisse und Technik in der IT-Branche beweisen. Die Kurse von Fast2test werden von den Experten nach ihren Kenntnissen und Erfahrungen für die EC-COUNCIL 312-39 Zertifizierungsprüfung bearbeitet

Die Zertifizierungsprüfung der EC-Council 312-39, auch als Certified SoC Analyst (CSA) -Prüfung bekannt, soll das Wissen und die Fähigkeiten einer Person im Sicherheitsvorgang (SOC) -Management (SOC), Netzwerksicherheit, Bedrohung intelligenz und Vorfallreaktion testen. Diese Zertifizierung ist ideal für Fachkräfte, die an einer Karriere in der Cybersicherheit interessiert sind oder in ihrer aktuellen Cybersicherheit aufsteigen möchten.

Kandidaten, die die CSA-Prüfung bestehen, können ihre Fähigkeit demonstrieren, Aufgaben wie das Analysieren von Sicherheitsereignissen, das Identifizieren von Sicherheitsvorfällen und das Verwalten von Sicherheitsvorfällen bis zur Lösung durchzuführen. Sie können auch ihr Wissen über verschiedene Sicherheitsrahmenwerke und -vorschriften wie NIST, CIS Critical Security Controls und GDPR demonstrieren. Insgesamt bietet diese Zertifizierung den Kandidaten die Fähigkeiten und Kenntnisse, die erforderlich sind, um ein erfolgreicher SOC-Analyst zu werden und wesentliche Beiträge zur Sicherheitslage einer Organisation zu leisten.

>> 312-39 Testing Engine <<

EC-COUNCIL 312-39 Prüfungen - 312-39 Testfagen

Sind Sie neugierig, warum so viele Menschen die schwierige EC-COUNCIL 312-39 Prüfung bestehen können? Ich können Sie beantworten. Der Kunstgriff ist, dass Sie haben die Prüfungsunterlagen der EC-COUNCIL 312-39 von unsere Fast2test benutzt. Wir bieten Ihnen: reichliche Prüfungsaufgaben, professionelle Untersuchung und einjährige kostenlose Aktualisierung nach dem Kauf. Mit Hilfe der EC-COUNCIL 312-39 Prüfungsunterlagen können Sie wirklich die Erhöhung Ihrer Fähigkeit empfinden. Sie können auch das echte Zertifikat der EC-COUNCIL 312-39 erwerben!

Die Zertifizierungsprüfung der EC-Council 312-39 (Certified SoC Analyst (CSA)) ist eine global anerkannte Zertifizierung, die die Fähigkeit des Kandidaten zeigt, Cybersicherheitsvorfälle effektiv zu bewältigen. Die Zertifizierung eignet sich für IT und Cybersecurity -Fachkräfte, die ihre Karriere in der SOC -Analyse vorantreiben möchten. Das Bestehen der Prüfung erfordert gründliche Kenntnisse und Fähigkeiten in verschiedenen Bereichen, einschließlich Netzwerksicherheit, Vorfälle und Computer -Forensik.

EC-COUNCIL Certified SOC Analyst (CSA) 312-39 Prüfungsfragen mit Lösungen (Q154-Q159):

154. Frage
A security team is configuring a newly deployed SIEM system. With limited resources, they must prioritize monitoring scenarios that provide the greatest security benefit. The team understands an effective SIEM relies on well-defined use cases tailored to the organization's environment. Which factor should guide their selection of use cases?

- A. Prioritize use cases that address zero-day attacks
- B. Implement as many use cases as the SIEM supports to cover all threats
- C. Select use cases based on the availability and quality of data from existing data sources
- D. Focus on use cases required to meet industry compliance standards

Antwort: C

Begründung:
Use cases should be selected based on the availability and quality of data because detections cannot work without reliable telemetry. In SOC engineering, the first constraint is data: what sources exist, how complete they are, how quickly they arrive, and whether fields are parsable and consistent. Choosing use cases that your environment can actually support produces faster time-to-value, fewer false positives, and fewer blind spots.
Prioritizing "zero-day" use cases is too vague and often unrealistic, because zero-days vary widely and require strong behavioral telemetry and baselines. Implementing as many use cases as possible spreads resources thin and increases noise, creating alert fatigue. Compliance-driven use cases are important, but if the underlying data is missing or poor quality, compliance rules will still fail operationally and can create a false sense of security. A mature approach is: start with high-value, high-feasibility detections that match available data (identity compromise, suspicious admin actions, endpoint malware, critical network anomalies), then expand as data coverage improves. Therefore, data availability and quality should guide initial use case selection.

155. Frage
Which of the following formula represents the risk levels?

- A. Level of risk = Consequence * Severity
- B. Level of risk = Consequence * Asset Value
- C. Level of risk = Consequence * Likelihood
- D. Level of risk = Consequence * Impact

Antwort: C

Begründung:

156. Frage
Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?

- A. Netstat Data
- B. DHCP Data
- C. IIS Data
- D. DNS Data

Antwort: A

157. Frage
TechSolutions, a software development firm, discovered a potential data leak after an external security researcher reported finding sensitive customer data on a public code repository. Level 1 SOC analysts confirmed the presence of the data and escalated the issue. Level 2 analysts traced the source of the leak to an internal network account. The incident response team has been alerted, and the CISO demands a comprehensive analysis of the incident, including the extent of the data breach and the timeline of events. The SOC manager must decide whom to assign to the in-depth investigation. To accurately determine the timeline, extent, and root cause of the data leak, which SOC role is critical in gathering and analyzing digital evidence?

- A. Threat Intelligence Analyst
- B. Subject Matter Expert
- C. Forensic Analyst
- D. SOC Manager

Antwort: C

Begründung:
A forensic analyst is the role best suited to perform in-depth evidence gathering and analysis required to reconstruct timelines, determine scope, and establish root cause for a data leak. This work includes preserving evidence (ensuring integrity), collecting endpoint and server artifacts, reviewing authentication and repository access logs, correlating commit history with identity and device telemetry, and building a defensible chain of events for leadership and potential legal/regulatory review. The SOC manager coordinates resources and priorities but typically does not perform hands-on forensic reconstruction. A subject matter expert may provide domain expertise (e.g., on Git workflows, cloud platforms, or database systems), but forensic rigor and evidence handling are the core requirement here. A threat intelligence analyst focuses on external adversary information, campaigns, and indicators; they can assist with context but are not the primary role for internal evidence reconstruction. Because the CISO needs timeline, extent, and root cause-deliverables that depend on digital evidence handling and forensic methodology-the forensic analyst is the critical assignment.

158. Frage
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. push-based
- C. pull-based
- D. signature-based

Antwort: B

Begründung:
In a push-based log collection mechanism, the system or application actively sends (or "pushes") log records to a designatedstorage location, which can be either on the local disk or over a network to a remote server.
This is in contrast to a pull-based mechanism, where the log records are retrieved (or "pulled") by the management server from the devices.
The push-based mechanism is often used for real-time monitoring and alerting because it allows for immediate transfer of log data as events occur. This method ensures that log records are consistently and reliably sent to a central repository without the need for a third-party service to request or retrieve them.
References: The EC-Council's Certified SOC Analyst (CSA) program includes the study of various log collection mechanisms as part of its curriculum. The CSA study materials provide detailed explanations of push-based and other log collection mechanisms, emphasizing their role in effective security operations center (SOC) monitoring and incident response. For further information, please refer to the official EC-Council CSA study guides and related course materials.

159. Frage
.....

- Die seit kurzem aktuellsten Certified SOC Analyst (CSA) Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der EC-COUNCIL 312-39 Prüfungen! □ Öffnen Sie ➽ www.examfragen.de □ geben Sie □ 312-39 □ ein und erhalten Sie den kostenlosen Download □312-39 Online Praxisprüfung
- 312-39 Aktuelle Prüfung - 312-39 Prüfungsguide - 312-39 Praxisprüfung □ Suchen Sie auf ➤ www.itzert.com □ nach kostenlosem Download von （ 312-39 ） □312-39 Fragenkatalog
- 312-39 PrüfungGuide, EC-COUNCIL 312-39 Zertifikat - Certified SOC Analyst (CSA) □ Öffnen Sie die Webseite { www.deutschpruefung.com } und suchen Sie nach kostenloser Download von ➠ 312-39 □ □312-39 Lernhilfe
- www.stes.tyc.edu.tw, bbs.t-firefly.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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, Disposable vapes

P.S. Kostenlose und neue 312-39 Prüfungsfragen sind auf Google Drive freigegeben von Fast2test verfügbar: https://drive.google.com/open?id=1AXTLkt3HWtYVJ0kq_YvBldLE-s02cAX-