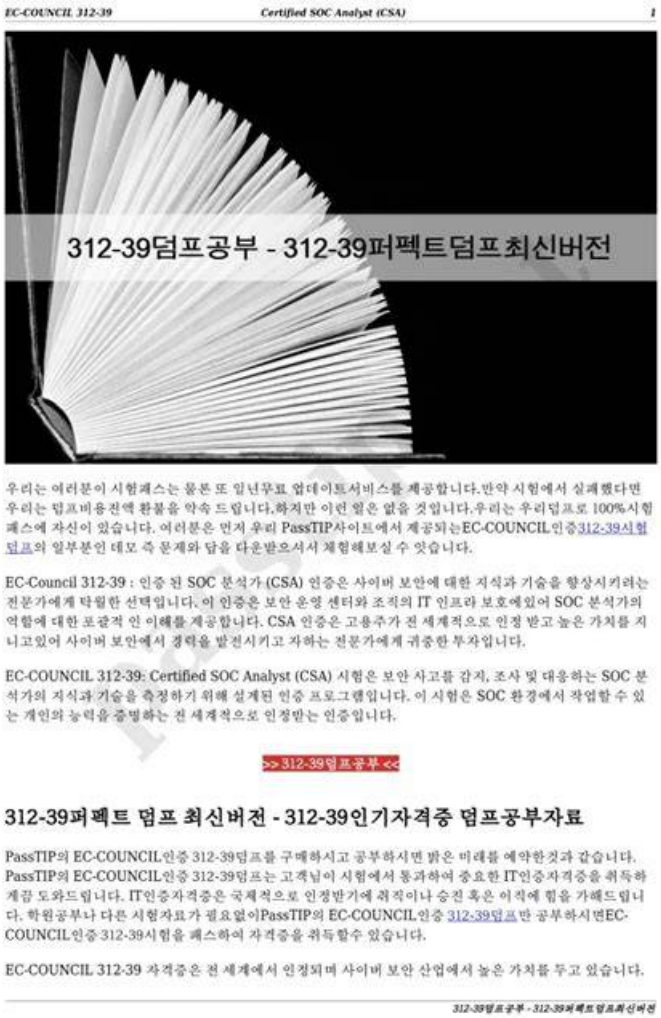
312-39시험대비최신덤프 & 312-39유효한최신덤프공부



그 외, KoreaDumps 312-39 시험 문제집 일부가 지금은 무료입니다: https://drive.google.com/open?id=1l2krpObSkjorSMQZzzDmW2FtjwyTQyTG

EC-COUNCIL 312-39 덤프는EC-COUNCIL 312-39시험문제변경에 따라 주기적으로 업데이트를 진행하여 저희 덤프가 항상 가장 최신버전이도록 보장해드립니다. 고객님들에 대한 깊은 배려의 마음으로 고품질EC-COUNCIL 312-39덤프를 제공해드리고 디테일한 서비스를 제공해드리는것이 저희의 목표입니다.

EC-COUNCIL 312-39 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Incident Detection with SIEM	25%	- Correlation rules and alert generation - SIEM architecture, components, and deployment models - SIEM dashboards and reporting - Alert triage, prioritization, and false positive reduction - Data ingestion, parsing, and normalization
Topic 2: Forensic Investigation and Malware Analysis	5%	- Digital forensics fundamentals in SOC context - IoC extraction and evidence handling - Malware types, behavior, and analysis techniques

Topic 3: Incident Response	25%	- SOAR, EDR, XDR technologies - Incident response lifecycle and frameworks - Roles and responsibilities in incident response - Documentation, reporting, and post-incident review - Containment, eradication, and recovery procedures
Topic 4: Security Operations and Management	5%	- SOC implementation and operational models - SOC fundamentals and objectives - SOC components: people, processes, technology
Topic 5: Log Management	15%	- Log normalization, correlation, and retention policies - Log sources, types, and collection methods - Events vs incidents vs logs - Centralized logging architecture
Topic 6: SOC for Cloud Environments	5%	- Cloud security monitoring challenges - Cloud threat detection and response - Cloud log collection and analysis
Topic 7: Understanding Cyber Threats, IoCs, and Attack Methodology	8%	- Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) - Types of cyber threats and threat actors - Attack frameworks and methodologies - Network, host, and application-level attacks
Topic 8: Proactive Threat Detection	12%	- Threat intelligence types and sources - UEBA and advanced detection methods - Integrating threat intelligence into SOC workflows - Threat hunting methodologies and techniques

312-39유효한 최신덤프공부, 312-39최신버전 시험덤프문제

EC-COUNCIL 312-39인증시험은 전문적인 관련지식을 테스트하는 인증시험입니다. KoreaDumps는 여러분이EC-COUNCIL 312-39인증시험을 통과할 수 잇도록 도와주는 사이트입니다. 많은 분들이 많은 시간과 돈을 들여 혹은 여러 학원 등을 다니면서EC-COUNCIL 312-39인증시험패스에 노력을 다합니다. 하지만 우리KoreaDumps에서는 20시간 좌우만 투자하면 무조건EC-COUNCIL 312-39시험을 패스할 수 있도록 도와드립니다.

최신 EC-COUNCIL CSA 312-39 무료샘플문제 (Q151-Q156):

질문 # 151
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. Operational Threat Intelligence
- B. Strategic Threat Intelligence
- C. Functional Threat Intelligence
- D. Tactical Threat Intelligence

정답：B

설명:
The type of threat intelligence that helps in understanding adversary intent and making informed decisions to ensure appropriate security in alignment with risk is known as Strategic Threat Intelligence. This form of intelligence is concerned with the broader goals and motivations of threat actors, as well as the long-term trends and implications of their activities. It provides insights into the cyber threat landscape and helps organizations shape their security strategy and policies to mitigate risks.
Strategic Threat Intelligence is used to inform decision-makers about the nature of threats, the potential impact on the organization, and the necessary steps to align security measures with business objectives. It is less technical than Tactical or Operational Threat Intelligence and does not focus on the specific details of attacks or the technical indicators of compromise. Instead, it provides a high-level view of the threats and their relevance to the organization's risk management.
References: The information provided aligns with the EC-Council's Certified Threat Intelligence Analyst (C|TIA) program, which

covers the use of threat intelligence in SOC operations and the integration of threat intelligence into risk management processes1. Additionally, the distinction between different types of threat intelligence, such as Tactical, Strategic, and Operational, is well-documented in the cybersecurity community and can be found in various threat intelligence resources23.
Reference: https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat- intelligence/what-is-threat-intelligence/

질문 # 152
Wesley is an incident handler in a company named Maddison Tech. One day, he was learning techniques for eradicating the insecure deserialization attacks.
What among the following should Wesley avoid from considering?

- A. Deserialization of trusted data must cross a trust boundary
- B. Understand the security permissions given to serialization and deserialization
- C. Allow serialization for security-sensitive classes
- D. Validate untrusted input, which is to be serialized to ensure that serialized data contain only trusted classes

정답：C

설명：
Insecure deserialization often leads to critical vulnerabilities allowing attackers to perform various attacks, such as remote code execution. To mitigate these vulnerabilities, Wesley should avoid considering the serialization of security-sensitive classes because it can expose sensitive data to untrusted sources or lead to arbitrary code execution.
Here are the steps Wesley should follow:
* Avoid Serialization of Sensitive Data: Do not serialize sensitive information. If it's essential to serialize, then ensure it's encrypted and the process is secure.
* Implement Integrity Checks: Use digital signatures or checksums to verify that the serialized data has not been tampered with before deserializing it.
* Enforce Strict Type Constraints: When deserializing, ensure that the data adheres to strict type constraints to prevent the instantiation of unexpected types.
* Logging and Monitoring: Keep detailed logs of serialization and deserialization processes to monitor for any suspicious activities.
* Security Controls Review: Regularly review and update security controls related to serialization and deserialization to ensure they are effective against emerging threats.
References:
* EC-Council's Certified SOC Analyst (CSA) program provides extensive training on how to handle various cybersecurity threats, including insecure deserialization12.
* The CSA certification emphasizes the importance of understanding the security risks associated with serialization and deserialization and implementing best practices to mitigate these risks12.
* Additional resources and study guides from EC-Council's official materials on the Certified SOC Analyst (CSA) program would provide more in-depth strategies and practices for handling insecure deserialization attacks12.

질문 # 153
During a threat intelligence briefing, a SOC analyst comes across a classified report detailing a sophisticated cybercrime syndicate targeting executives of high-profile financial institutions. These adversaries rarely leave digital footprints and seem to anticipate security measures. Several breaches began with seemingly innocent conversations: a foreign journalist requesting an interview with a CEO and a "security consultant" offering free risk assessments. Further investigation reveals attackers socially engineered employees, manipulated trust, and extracted critical security details long before launching technical attacks. The analyst decides to focus on intelligence involving deception detection and psychological profiling to uncover true intent and methods. Which type of intelligence is the analyst leveraging?

- A. Human Intelligence
- B. Threat Intelligence Feeds
- C. Open-Source Intelligence (OSINT)
- D. Technical Threat Intelligence

정답：A

설명：
Human Intelligence (HUMINT) involves information gathered from people, relationships, and human behavior rather than purely technical artifacts. The scenario describes adversaries using social engineering and pretexting-building trust through conversations

and manipulating employees to reveal sensitive information.
The analyst is focusing on deception detection and psychological profiling, which are rooted in understanding human intent, influence tactics, and interpersonal manipulation patterns. That aligns with HUMINT, where insights may come from interviews, insider reporting, investigative findings, or controlled engagements that reveal motivations and methods that logs will not show. Threat intelligence feeds and technical threat intelligence primarily provide machine-consumable indicators, malware signatures, infrastructure data, and observed TTPs; they are valuable but not the main lens here because these attackers "rarely leave digital footprints." OSINT is derived from publicly available sources, which can help identify personas or prior campaigns, but the core described intelligence method is interpreting human behavior and social manipulation. From a SOC standpoint, HUMINT-driven insights inform security awareness training, executive protection protocols, identity verification procedures, and "out-of-band" validation processes that reduce success of pretexting and business email compromise.

질문 # 154
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.

What does this event log indicate?

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

정답：C

설명:
The event log indicates a Parameter Tampering Attack. This type of attack involves the manipulation of parameters exchanged between the client and the server to alter application data, such as user credentials and permissions, product price and quantity, etc. The IDS log entries showing repeated access to the URL "/OrderDetail.aspx?id=ORDR-001117" with varying order ID values suggest that the attacker is manipulating the 'id' parameter to potentially access or modify order details unauthorizedly.
References The EC-Council's Certified SOC Analyst (CSA) course materials and study guides discuss various types of cyber attacks, including Parameter Tampering, and their characteristics. Additionally, information on this type of attack can be found in resources provided by the OWASP Foundation1.

질문 # 155
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. Medium
- B. High
- C. Extreme
- D. Low

정답：C

설명:
In a Risk Matrix, risk levels are determined by the intersection of the likelihood of an occurrence (probability) and the consequence of that occurrence (impact). When the probability of an event is very high and the impact is major, it typically falls into the 'Extreme' category. This is because the combination of a high likelihood and major impact represents a scenario where the risk is unacceptable and requires immediate attention and mitigation measures.
References: The EC-Council's Certified SOC Analyst (CSA) course materials and study guides provide detailed information on assessing risks using a Risk Matrix. The course emphasizes the importance of understanding the Risk Matrix for effective security operations center (SOC) analysis. For more in-depth information, refer to the official EC-Council CSA study materials and resources12.

질문 # 156
.....

취직을 원하시나요? 승진을 원하시나요? 연봉인상을 원하시나요? 무엇을 원하시든 국제적으로 인정받은 IT인증자격증을 취득하는것이 길입니다. EC-COUNCIL인증 312-39시험은 널리 인정받는 인기자격증의 시험과목입니다. EC-COUNCIL인증 312-39시험을 패스하여 자격증을 취득하면 소원이 이루어집니다. KoreaDumps의EC-COUNCIL인증 312-39덤프는 시험패스율이 높아EC-COUNCIL인증 312-39시험준비에 딱 좋은 공부자료입니다. KoreaDumps에서 덤프를 마련하여 자격증취득에 도전하여 인생을 바꿔보세요.

312-39유효한 최신덤프공부: https://www.koreadumps.com/312-39_exam-braindumps.html

- 최신버전 312-39시험대비 최신 덤프 인기 덤프문제 다운 □ ➽ kr.fast2test.com □에서⇛ 312-39 ⇚를 검색하고 무료 다운로드 받기312-39높은 통과율 인기 덤프자료
- 312-39시험대비 최신 덤프자료 □ 312-39최고덤프자료 □ 312-39인기자격증 시험덤프 최신자료 □ 무료로 다운로드하려면⇛ www.itdumpskr.com ⇚로 이동하여▷ 312-39 ◁를 검색하십시오312-39시험대비 최신버전 덤프
- 312-39시험대비 최신 덤프 최신 덤프문제보기 □ 오픈 웹 사이트[www.dumptop.com]검색⇛ 312-39 ⇚무료 다운로드312-39최고패스자료
- 312-39시험대비 최신 덤프 최신 덤프문제보기 □ ▸ www.itdumpskr.com ◂을 통해 쉽게➽ 312-39 □무료 다운로드 받기312-39덤프문제집
- 312-39시험대비 최신버전 덤프 □ 312-39시험대비 덤프문제 □ 312-39높은 통과율 덤프문제 □ ➥ www.dumptop.com □은□ 312-39 □무료 다운로드를 받을 수 있는 최고의 사이트입니다312-39유효한 시험자료
- 312-39덤프문제집 □ 312-39인기자격증 덤프공부자료 □ 312-39최신 시험 공부자료 □ ➤ www.itdumpskr.com □에서☀ 312-39 □☀□를 검색하고 무료로 다운로드하세요312-39최신버전 시험덤프공부
- 312-39시험대비 최신버전 덤프 □ 312-39시험대비 덤프공부 □ 312-39최신 시험 공부자료 □ 지금➥ kr.fast2test.com □을(를) 열고 무료 다운로드를 위해「 312-39 」를 검색하십시오312-39시험대비 덤프공부
- 312-39인기자격증 덤프공부자료 □ 312-39최고덤프자료 □ 312-39시험대비 덤프문제 □ [www.itdumpskr.com]에서 검색만 하면{ 312-39 }를 무료로 다운로드할 수 있습니다312-39시험대비 최신 덤프자료
- 312-39시험합격덤프 □ 312-39최신 시험 공부자료 □ 312-39시험합격덤프 □ ▸ kr.fast2test.com ◂의 무료 다운로드{ 312-39 }페이지가 지금 열립니다312-39최신버전 시험덤프공부
- 312-39시험대비 최신 덤프 최신 덤프문제보기 □ 검색만 하면▸ www.itdumpskr.com ◂에서▸ 312-39 ◂무료 다운로드312-39높은 통과율 인기 덤프자료
- 312-39시험대비 최신 덤프 시험준비에 가장 좋은 공부자료 □ 무료로 다운로드하려면【 www.pass4test.net 】로 이동하여“ 312-39 ”를 검색하십시오312-39최신버전 덤프공부문제
- 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, telegra.ph, 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, Disposable vapes

참고: KoreaDumps에서 Google Drive로 공유하는 무료, 최신 312-39 시험 문제집이 있습니다: https://drive.google.com/open?id=1l2krpObSkjorSMQZzzDmW2FtjwyTQyTG