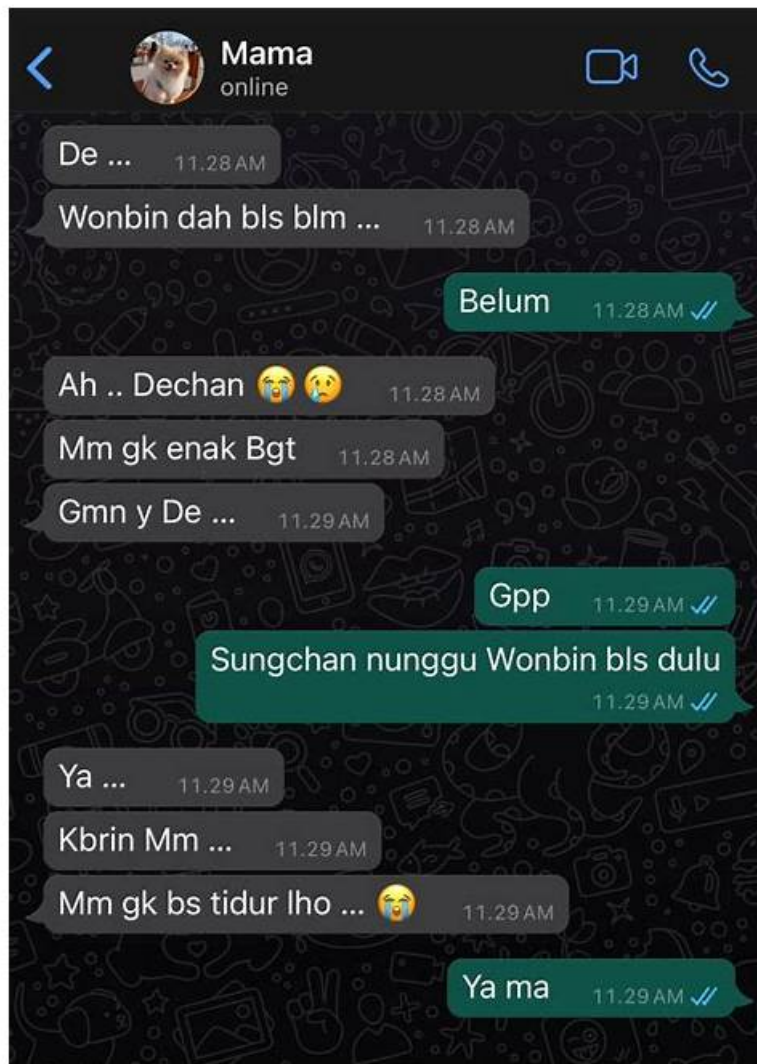


# New 312-39 Dumps Questions | 312-39 Latest Dumps Pdf



BTW, DOWNLOAD part of Free4Torrent 312-39 dumps from Cloud Storage: [https://drive.google.com/open?id=1OtD3\\_ooAnxBihpvFrqQQ9rgMZ7wWPeTy](https://drive.google.com/open?id=1OtD3_ooAnxBihpvFrqQQ9rgMZ7wWPeTy)

Do you want to pass your Certified SOC Analyst (CSA) exam? If so, Free4Torrent is the ideal place to begin. Free4Torrent provides comprehensive 312-39 exam questions preparation in two simple formats: a pdf file format and an EC-COUNCIL 312-39 online practice test engine. If you fail your Certified SOC Analyst (CSA) (312-39) Exam, you can obtain a full refund and a 20% discount! Continue reading to discover more about the essential aspects of these excellent 312-39 exam questions.

EC-COUNCIL 312-39 (Certified SOC Analyst (CSA)) Certification Exam is designed for professionals who wish to demonstrate their expertise in the field of Security Operations Center (SOC) analysis. Certified SOC Analyst (CSA) certification is aimed at individuals who have experience working with security protocols, incident response, and threat detection. 312-39 exam is designed to test a candidate's knowledge and skills in these areas, and upon successful completion, the candidate is awarded the CSA certification.

## EC-COUNCIL 312-39 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• Understand the architecture, implementation and fine-tuning of SIEM solutions</li><li>• Gain Knowledge of SOC processes, procedures, technologies, and workflows</li></ul>

Topic 2	<ul style="list-style-type: none"> <li>• Gain experience and extensive knowledge of Security Information and Event Management</li> <li>• Able to monitor emerging threat patterns and perform security threat analysis</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• Learn use cases that are widely used across the SIEM deployment</li> <li>• Gain knowledge of Incident Response Process</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• Able to escalate incidents to appropriate teams for additional assistance</li> <li>• Able to make use of varied, disparate, constantly changing threat information</li> </ul>
Topic 5	<ul style="list-style-type: none"> <li>• Able to develop threat cases (correlation rules), create reports</li> <li>• Gain a basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities</li> </ul>
Topic 6	<ul style="list-style-type: none"> <li>• Able to perform Security events and log collection, monitoring, and analysis</li> <li>• Gain knowledge of administering SIEM solutions</li> </ul>
Topic 7	<ul style="list-style-type: none"> <li>• Gain knowledge of integrating threat intelligence into SIEM</li> <li>• Able to recognize attacker tools, tactics, and procedures</li> </ul>
Topic 8	<ul style="list-style-type: none"> <li>• Gain understating of SOC and IRT collaboration for better incident response</li> <li>• Gain knowledge of the Centralized Log Management (CLM) process</li> </ul>

The EC-Council Certified SOC Analyst (CSA) certification is a comprehensive program that tests the skills and knowledge required to effectively monitor, detect, and respond to security incidents in real-time. The CSA certification covers the essential skills required to work in a Security Operations Center (SOC) and is designed for professionals who want to enhance their knowledge of security operations, incident response, and threat intelligence.

>> New 312-39 Dumps Questions <<

## 312-39 Latest Dumps Pdf & 312-39 Test Question

Even some one can job-hop to this international company. Opportunities are reserved for those who are prepared. Only if you pass the exam can you get a better promotion. And if you want to pass it more efficiently, we must be the best partner for you. Because we are professional 312-39 question torrent provider, we are worth trusting; because we make great efforts, we do better. Here are many reasons to choose us.

### EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q84-Q89):

#### NEW QUESTION # 84

Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex `/((\%3C)|<)(\%69)|i(\%49))(\%6D)|m(\%4D))(\%67)|g(\%47))`

BONUS!!! Download part of Free4Torrent 312-39 dumps for free: [https://drive.google.com/open?id=1OtD3\\_ooAnxBihpvFrqQQ9rgMZ7wWPeTy](https://drive.google.com/open?id=1OtD3_ooAnxBihpvFrqQQ9rgMZ7wWPeTy)