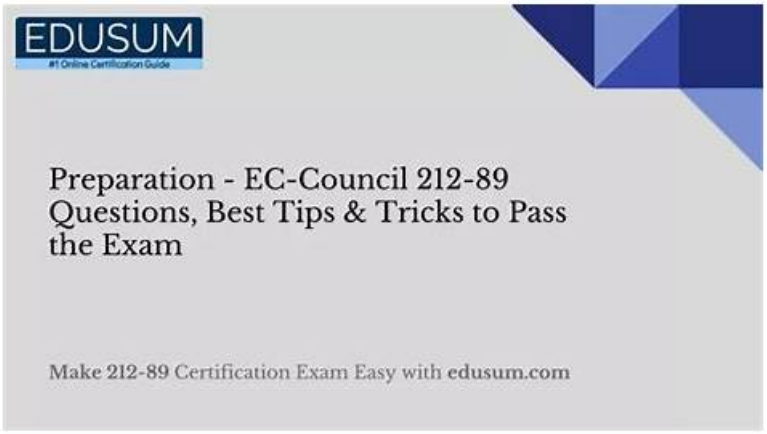
212-89시험패스가능공부자료 & 212-89시험대비덤프공부자료



BONUS!!! ExamPassdump 212-89 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1PaKhMFbox1nmzYcY0TwNsoRblzTGVucY

ExamPassdump 에서EC-COUNCIL 212-89 덤프를 구매하시면 일년무료 업데이트서비스를 받을수 있습니다.일년무료 업데이트서비스란 구매일로부터 1년동안 구매한 덤프가 업데이트될때마다 구매시 사용한 메일주소로 가장 최신버전을 보내드리는것을 의미합니다. EC-COUNCIL 212-89덤프에는 가장 최신시험문제의 기출문제가 포함되어 있어 높은 적주율을 자랑하고 있습니다.

EC-COUNCIL 212-89 시험은 보안 전문가, 사고 대응 담당자, IT 매니저, 네트워크 관리자 및 사고 처리 및 대응 분야에서 지식과 기술을 향상 시키기를 원하는 모든 사람들에게 이상적입니다. 이 자격증은 특히 조직 내 보안 사고를 관리하고 대응하는 책임이 있는 사람들에게 유용합니다.

EC-COUNCIL 212-89 (EC Council Certified Incident Handler (ECIH v2)) 시험은 사고 처리와 응답 분야 전문가들에게 유용한 인증서입니다. 이 시험은 다양한 주제를 다루며 후보자의 보안 사고를 효과적으로 식별, 대응 및 해결할 수 있는 능력을 검증합니다. 이 인증서는 전 세계적으로 인정되며 벤더 중립적이어서 다양한 산업과 조직에 적용할 수 있는 다재다능한 자격증입니다.

>> 212-89시험패스 가능 공부자료 <<

212-89시험패스 가능 공부자료 100% 합격 보장 가능한 덤프공부자료

EC-COUNCIL인증 212-89시험은 멋진 IT전문가로 거듭나는 길에서 반드시 넘어야할 높은 산입니다. EC-COUNCIL인증 212-89시험문제패스가 어렵다한들ExamPassdump덤프만 있으면 패스도 간단한 일로 변경됩니다. ExamPassdump의EC-COUNCIL인증 212-89덤프는 100%시험패스율을 보장합니다. EC-COUNCIL인증 212-89시험문제가 업데이트되면EC-COUNCIL인증 212-89덤프도 바로 업데이트하여 무료 업데이트서비스를 제공해드리기에 덤프유효기간을 연장해는것으로 됩니다.

최신 ECIH Certification 212-89 무료샘플문제 (Q25-Q30):

질문 # 25
A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

- A. adware (spelled all lower case)
- B. Worm
- C. Virus
- D. Trojan
- E. RootKit

정답： A

질문 # 26
Which of the following is NOT a network forensic tool?

- A. Advanced NTFS Journaling Parser
- B. Wire shark
- C. Tcpdump
- D. Caps a Network Analyzer

정답：A

질문 # 27
Which of the following methods help incident responders to reduce the false-positive alert rates and further provide benefits of focusing on topmost priority issues reducing potential risk and corporate liabilities?

- A. Threat profiling
- B. Threat attribution
- C. Threat correlation
- D. Threat contextualization

정답：C

설명：
Threat correlation is a method used by incident responders to analyze and associate various indicators of compromise (IoCs) and alerts to identify genuine threats. By correlating data from multiple sources and applying intelligence to distinguish between unrelated events and coordinated attack patterns, responders can significantly reduce the rate of false-positive alerts. This enables teams to prioritize their efforts on the most critical and likely threats, thereby reducing potential risks and corporate liabilities. Effective threat correlation involves the use of sophisticated security information and event management (SIEM) systems, threat intelligence platforms, and analytical techniques to identify relationships between seemingly disparate security events and alerts.
References:The role of threat correlation in improving the efficiency of incident response activities by reducing false positives and focusing on high-priority issues is outlined in various cybersecurity frameworks and incident response guides, including those related to the ECIH v3 certification. These resources emphasize the importance of applying context and intelligence to security alerts to accurately identify and respond to genuine threats.

질문 # 28
Your company sells SaaS, and your company itself is hosted in the cloud (using it as a PaaS). In case of a malware incident in your customer's database, who is responsible for eradicating the malicious software?

- A. The customer
- B. Building management
- C. The PaaS provider
- D. Your company

정답：D

설명：
In the scenario where your company sells Software as a Service (SaaS) and is hosted on the cloud using it as a Platform as a Service (PaaS), your company is responsible for eradicating malware in your customer's database. This is because, as the SaaS provider, your company manages the software and is responsible for its security and maintenance, including the databases that store customer data. While the PaaS provider is responsible for the underlying infrastructure, platform, and possibly some middleware security aspects, the application layer security, including data and application management, falls to the SaaS provider. Building management would not be involved in digital security matters, and while customers are responsible for their data, the actual software maintenance and security in a SaaS model are the provider's responsibility.References:Incident Handler (ECIH v3) certification materials often discuss cloud service models (IaaS, PaaS, SaaS) and their associated security responsibilities, highlighting the importance of understanding who is responsible for what in cloud environments.

질문 # 29

Michael is a part of the computer incident response team of a company. One of his responsibilities is to handle email incidents. The company receives an email from an unknown source, and one of the steps that he needs to take is to check the validity of the email. Which of the following tools should he use?

- A. Yes ware
- B. Zendio
- C. Email Dossier
- D. G Suite Toolbox

정답：C

질문 # 30

.....