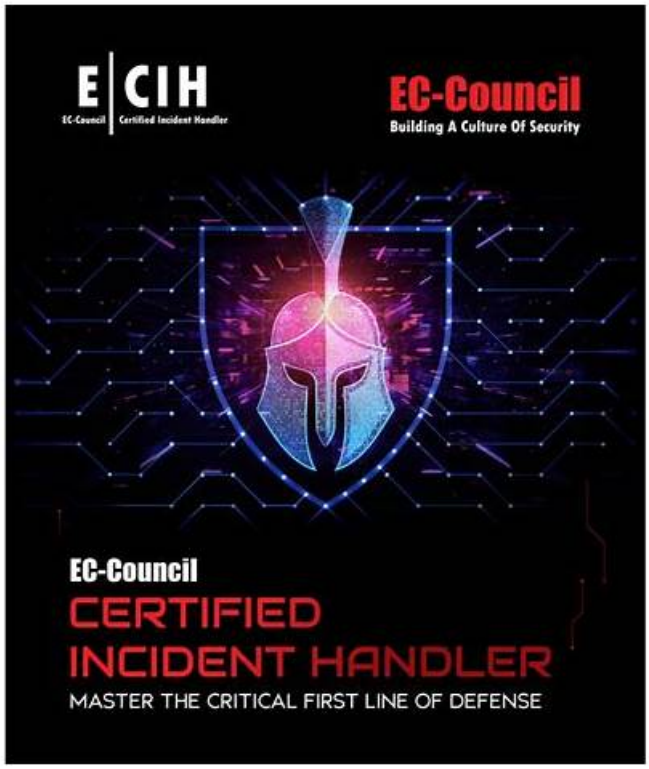
212-89 Übungstest: EC Council Certified Incident Handler (ECIH v3) & 212-89 Braindumps Prüfung



BONUS!!! Laden Sie die vollständige Version der Fast2test 212-89 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1cS94wO-Od-6BviYTX0IF0-anwQt-plIZ

Um Sie beim Kauf der EC-COUNCIL 212-89 Prüfungssoftware beruhigt zu lassen, wenden wir die gesicherteste Zahlungsmittel an. Paypal ist das größte internationale Zahlungssystem. Und wir bewahren sorgfältig Ihre persönliche Informationen. Wenn Sie Fragen über die EC-COUNCIL 212-89 Prüfungsunterlagen oder Interesse an anderen Prüfungssoftwaren haben, könnten Sie diret mit uns online kontaktieren oder uns E-Mail schicken. Wir tun unser Bestes, um Ihnen bei der EC-COUNCIL 212-89 Prüfung zu helfen.

Die Zertifizierungsprüfung EC-COUNCIL 212-89 (EC Council Certified Incident Handler (ECIH v2)) ist eine professionelle Zertifizierung, die entwickelt wurde, um die Fähigkeiten und Kenntnisse von Kandidaten im Bereich Incident Handling und Response zu testen und zu validieren. Die Zertifizierung wird von der EC-Council angeboten, einer führenden Organisation für Cybersecurity-Education und -Training, und wird weltweit von Arbeitgebern und Fachleuten anerkannt.

Die EC-COUNCIL 212-89 Zertifizierungsprüfung ist speziell für Cybersicherheitsfachleute konzipiert, die Incident-Handler, Mitglieder des Incident Response-Teams oder Computer-Forensik-Experten werden möchten. Diese IT-Sicherheitspraktiker arbeiten daran, Unternehmen, Regierungsorganisationen und andere große Institutionen zu schützen und sind in der Regel dafür verantwortlich, Sicherheitsvorfälle zu identifizieren, zu untersuchen und zu lösen. Diese Fachleute benötigen spezifische Fähigkeiten und Kenntnisse, um in ihrer Arbeit erfolgreich zu sein, daher ist der Prüfungsinhalt darauf ausgerichtet, die relevantesten und aktuellsten Themen abzudecken.

>> 212-89 Prüfungsvorbereitung <<

212-89 Trainingsmaterialien: EC Council Certified Incident Handler (ECIH v3) & 212-89 Lernmittel & EC-COUNCIL 212-89 Quiz

Bevor Sie sich für Fast2test entscheiden, können Sie die EC-COUNCIL 212-89 Examensfragen-und antworten teilweise als Probe kostenlos herunterladen. So können Sie die Glaubwürdigkeit vom Fast2test testen. Der Fast2test ist die beste Wahl für Sie, wenn Sie die EC-COUNCIL 212-89 Zertifizierungsprüfung unter Garantie bestehen wollen. Wenn Sie sich für den Fast2test entscheiden,

wird der Erfolg auf Sie zukommen.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) 212-89 Prüfungsfragen mit Lösungen (Q34-Q39):

34. Frage
An incident handler is analyzing email headers to find out suspicious emails.
Which of the following tools he/she must use in order to accomplish the task?

- A. Gophish
- B. Barracuda Email Security Gateway
- C. SPAMfighter

Antwort: B

Begründung:
The Barracuda Email Security Gateway is designed to manage and filter inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. As an incident handler analyzing email headers to find out suspicious emails, using a tool like the Barracuda Email Security Gateway would be appropriate. This tool can help identify and block spam, phishing, malware, and other malicious email threats, making it easier to focus on analyzing potentially harmful emails more closely.

35. Frage
Which of the following is NOT one of the techniques used to respond to insider threats:

- A. Placing malicious users in quarantine network, so that attack cannot be spread
- B. Blocking malicious user accounts
- C. Preventing malicious users from accessing unclassified information
- D. Disabling the computer systems from network connection

Antwort: C

36. Frage
An adversary attacks the information resources to gain undue advantage is called:

- A. Electronic Warfare
- B. Offensive Information Warfare
- C. Defensive Information Warfare
- D. Conventional Warfare

Antwort: B

37. Frage
Alice is an incident handler and she has been informed by her lead that the data on affected systems must be backed up so that it can be retrieved if it is damaged during the incident response process. She was also told that the system backup can also be used for further investigation of the incident. In which of the following stages of the incident handling and response (IH&R) process does Alice need to do a complete backup of the infected system?

- A. Incident recording
- B. Incident triage
- C. Eradication
- D. Containment

Antwort: D

Begründung:
In the incident handling and response (IH&R) process, backing up the data on affected systems is a critical step that usually falls under the Containment phase. The Containment phase is crucial for limiting the scope and severity of an incident, ensuring that it

does not spread further or affect additional systems. Backing up affected systems during containment is essential for several reasons: it preserves a snapshot of the system in its current state for forensic analysis, ensures that data is not lost if the system needs to be wiped or altered during the response process, and helps in the recovery process if data is corrupted or lost.
By performing a complete backup of the infected system during the Containment phase, Alice ensures that there is a reliable copy of all data and system states before any major actions, such as eradication or deeper forensic analysis, are taken. This step is also preparatory for the potential use of the backup in analyzing how the incident occurred and in restoring system functionality after the incident is resolved.
References:EC-Council's Certified Incident Handler (ECIH v3) courses and study guides highlight the importance of the Containment phase in the IH&R process, including the practice of backing up affected systems to prevent data loss and to aid in the investigation and recovery processes.

38. Frage
Identify a standard national process which establishes a set of activities, general tasks and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.

- A. NIASAP
- B. NIPACP
- C. NIAAAP
- D. NIACAP

Antwort: D

39. Frage
.....

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, 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, 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

Laden Sie die neuesten Fast2test 212-89 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1cS94wO-Od-6BviYTX0IF0-anwQt-pllZ