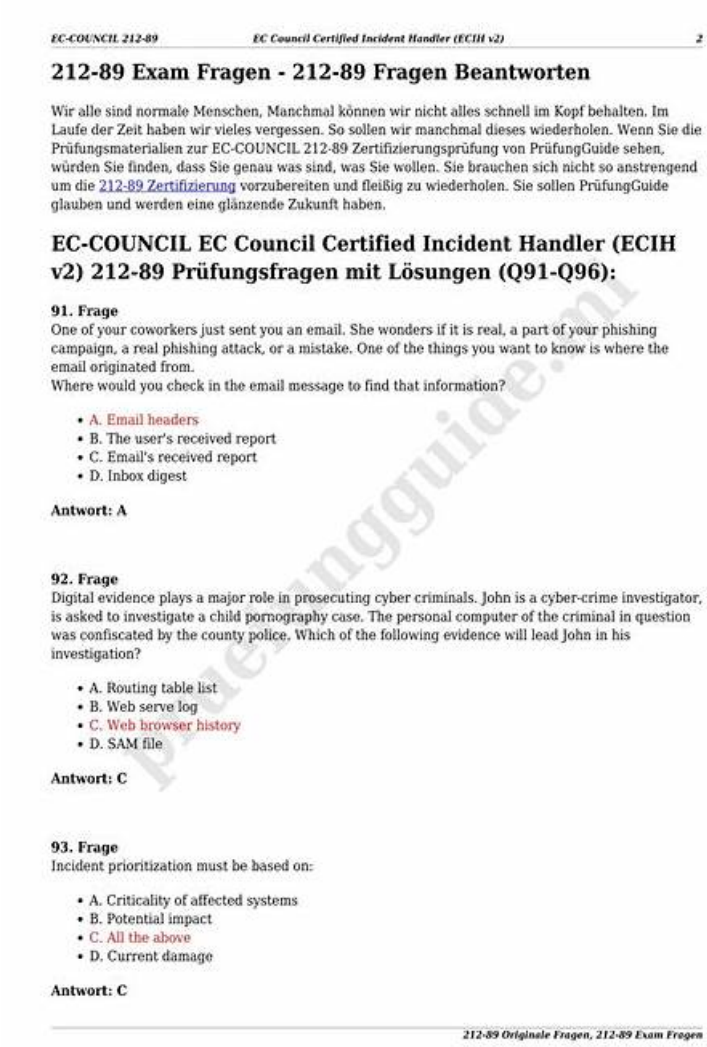
212-89 Prüfung, 212-89 Fragen Antworten



212-89 Exam Fragen - 212-89 Fragen Beantworten

Wir alle sind normale Menschen, Manchmal können wir nicht alles schnell im Kopf behalten. Im Laufe der Zeit haben wir vieles vergessen. So sollen wir manchmal dieses wiederholen. Wenn Sie die Prüfungsmaterialien zur EC-COUNCIL 212-89 Zertifizierungsprüfung von PrüfungGuide sehen, würden Sie finden, dass Sie genau was sind, was Sie wollen. Sie brauchen sich nicht so anstrengend um die 212-89 Zertifizierung vorzubereiten und fleißig zu wiederholen. Sie sollen PrüfungGuide glauben und werden eine glänzende Zukunft haben.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v2) 212-89 Prüfungsfragen mit Lösungen (Q91-Q96):

91. Frage
One of your coworkers just sent you an email. She wonders if it is real, a part of your phishing campaign, a real phishing attack, or a mistake. One of the things you want to know is where the email originated from.
Where would you check in the email message to find that information?

- A. Email headers
- B. The user's received report
- C. Email's received report
- D. Inbox digest

Antwort: A

92. Frage
Digital evidence plays a major role in prosecuting cyber criminals. John is a cyber-crime investigator, is asked to investigate a child pornography case. The personal computer of the criminal in question was confiscated by the county police. Which of the following evidence will lead John in his investigation?

- A. Routing table list
- B. Web serve log
- C. Web browser history
- D. SAM file

Antwort: C

93. Frage
Incident prioritization must be based on:

- A. Criticality of affected systems
- B. Potential impact
- C. All the above
- D. Current damage

Antwort: C

Übrigens, Sie können die vollständige Version der It-Pruefung 212-89 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=14UhrEwTzj-gJxZQxpov6xi4-2LFRut5d

Haben Sie gedacht, wie EC-COUNCIL 212-89 Zertifizierungsprüfung leicht bestehen? Haben Sie die Geräte finden? Wenn nein, erkläre ich zu Ihnen. Es gibt viele Methoden, die 212-89 Prüfung zu bestehen. Sehr fleißig die entsprechenden Bücher zu lesen, ist eine Methode. Machen Sie jetzt das? Aber diese Methode kostet dich viel Zeit und kann den Erfolg vielleicht nicht erreichen. Und Gibt es nicht genug Zeit für Sie, wenn Sie sich mit der Arbeit sehr beschäftigt sind? Lassen Sie EC-COUNCIL 212-89 Dumps probieren. Diese Unterlagen können den Erfolg erreichen, woran Sie nicht glauben könnten.

Die V2-Prüfung des EC-Rates Certified Incident Handler (ECIH) ist eine branchenbezogene Zertifizierung, die die Fähigkeiten und Kenntnisse von Fachleuten validiert, die verschiedene Cybersicherheitsvorfälle effektiv bearbeiten und darauf reagieren können. Dieses Zertifizierungsprogramm soll den Teilnehmern praktische Fähigkeiten bieten, die in realen Szenarien angewendet werden können, sodass sie Risiken mindern, Datenverletzungen verhindern und ihre Systeme vor Cyber-Angriffen schützen können.

Die ECIH V2 -Prüfung deckt verschiedene Themen im Zusammenhang mit der Behandlung und Reaktion in der Vorfälle ab, einschließlich Vorfälle, Vorfälle, Vorfälleanalysen und Incident -Reaktionstechniken. Die Prüfung deckt auch verschiedene Tools und Techniken ab, die bei der Behandlung von Vorfällen verwendet werden, z. B. die Netzwerküberwachung, die Protokollanalyse und die forensische Analyse. Es umfasst auch praktische Labors und Simulationen, um praktische Erfahrungen beim Umgang mit verschiedenen Arten von Vorfällen zu bieten.

>> 212-89 Prüfung <<

212-89 Fragen Antworten & 212-89 Online Prüfungen

It-Pruefung ist eine Website, die Bedürfnisse der Kunden abdecken kann. Diejenigen, die unsere Simulationssoftware zur EC-COUNCIL 212-89 IT-Zertifizierungsprüfung benutzt und die Prüfung betanden haben, sind unsere Stammgäste geworden. It-Pruefung stellt Ihnen die fortschrittliche Ausbildungstechnik zur Verfügung, die Ihnen beim Bestehen der EC-COUNCIL 212-89 Zertifizierungsprüfung hilft.

Die EC-COUNCIL 212-89-Zertifizierungsprüfung ist eine weltweit anerkannte Referenz, die vom International Council of E-Commerce Consultants (EC-Council) angeboten wird. Die Zertifizierung soll das Wissen und die Fähigkeiten von Cybersicherheitsfachleuten in Bezug auf Vorfallbearbeitung und -reaktion validieren. Die EC-Council Certified Incident Handler (ECIH v2)-Zertifizierung ist ideal für Fachleute, die für das Verwalten und Reagieren auf Sicherheitsvorfälle in einer Organisation verantwortlich sind.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) 212-89 Prüfungsfragen mit Lösungen (Q85-Q90):

85. Frage
Following a spear-phishing campaign targeting executive-level employees, a mid-sized financial firm experienced unauthorized access to internal systems, leading to widespread disruption of customer-facing applications. Although the technical issues were resolved within days, the breach triggered legal scrutiny and negative press coverage. Several major customers expressed concern about the firm's risk posture and began transitioning to competitors. Investor confidence was impacted as the stock value dipped, and senior leadership initiated a damage control campaign. Which of the following best categorizes the broader consequences experienced by the organization?

- A. Measurable loss from hardware failure and direct asset compromise.
- B. Recovery complications caused by delayed asset inventory synchronization.
- C. Intangible business effects involving stakeholder defection and public image decline.
- D. Tangible operational costs including the deployment of response infrastructure.

Antwort: C

Begründung:
Comprehensive and Detailed Explanation (ECIH-aligned):
The scenario describes consequences extending beyond technical remediation into reputational, financial, and stakeholder trust impacts. According to ECIH risk assessment and post-incident analysis guidance, these outcomes are classified as intangible business effects.
Option C is correct because customer loss, investor confidence decline, and reputational damage cannot be easily quantified yet often exceed direct incident response costs. ECIH emphasizes that post-incident reviews must consider both tangible and intangible impacts to accurately assess business risk.
Options A, B, and D describe operational or technical impacts, which were resolved quickly in this scenario.
The lasting damage occurred at the business and market perception level.
Understanding intangible impacts is critical for executive reporting, risk management, and long-term resilience planning, making Option C correct.

86. Frage
Which of the following is an Inappropriate usage incident?

- A. Access-control attack
- B. Reconnaissance attack
- C. Insider threat
- D. Denial-of-service attack

Antwort: C

Begründung:
An Inappropriate Usage incident refers to instances where computing resources are misused or abused, often violating organizational policies or laws. While access-control attacks, reconnaissance attacks, and denial-of-service (DoS) attacks represent different types of external threats or methods of attack, an Insider Threat is an example of inappropriate usage. Insider threats come from individuals within the organization, such as employees or contractors, who misuse their access to harm the organization's interests. This can include stealing confidential information, intentionally disrupting systems, or other malicious activities that leverage their

legitimate access to the organization's resources.References:EC-Council's Incident Handler (ECIH v3) materials often discuss various typesof security incidents, including inappropriate usage, and emphasize the importance of recognizing and preparing for insider threats as a critical component of an organization's incident response strategy.

87. Frage
Jason is an incident handler dealing with malware incidents. He was asked to perform memory dump analysis in order to collect the information about the basic functionality of any program. As a part of his assignment, he needs to perform string search analysis to search for the malicious stringthat could determine harmful actions that a program can perform. Which of the following string-searching tools Jason needs to use to do the intended task?

- A. BinText
- B. Dependency Walker
- C. PEView
- D. Process Explorer

Antwort: A

Begründung:
BinText is a lightweight text extraction tool that can be used to perform string search analysis within binary files. This functionality is crucial for incident handlers like Jason, who are tasked with analyzing memory dumps for malicious activity or indicators of compromise. By searching for specific strings or patterns that are known to be associated with malware, BinText helps in identifying potentially harmful actions that a program could perform, thus aiding in the investigation of malware incidents.
References:Memory dump analysis and string search techniques are important skills covered in the ECIH v3 curriculum, emphasizing the use of tools like BinText to aid in the forensic analysis of malware-infected systems.

88. Frage
Joseph is an incident handling and response (IH&R) team lead in Toro Network Solutions Company. As a part of IH&R process, Joseph alerted the service providers, developers, and manufacturers about the affected resources.
Identify the stage of IH&R process Joseph is currently in.

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

Antwort: D

Begründung:
When Joseph, the IH&R team lead, alerted service providers, developers, and manufacturers about the affected resources, he was engaged in the Containment stage of the Incident Handling and Response (IH&R) process. Containment involves taking steps to limit the spread or impact of an incident and to isolate affected systems to prevent further damage. Alerting relevant stakeholders, including service providers and developers, is part of containment efforts to ensure that the threat does not escalate and that measures are taken to protect unaffected resources. This stage precedes eradication and recovery, focusing on immediate response actions to secure the environment.
References:The ECIH v3 certification program outlines the IH&R process stages, explaining the roles and actions involved in containment, including communication with external and internal stakeholders to manage and mitigate the incident's effects.

89. Frage
Which of the following is not called volatile data?

- A. The dale a no Lime of the system
- B. Creation dates of files
- C. State of the network interface
- D. Open sockets er open ports

Antwort: B

Begründung:

Volatile data refers to information that is stored temporarily and is lost when a computer is turned off or restarted, such as RAM contents, including open sockets and open ports, the date and time of the system, and the state of the network interface. The creation dates of files, however, are considered non-volatile data because they are preserved on the hard drive and remain available after the system is restarted or turned off.
Non-volatile data is stored on persistent storage mediums like hard drives, SSDs, and magnetic tapes, where it remains until it is deleted or overwritten.References:The Incident Handler (ECIH v3) certification emphasizes the distinction between volatile and non-volatile data in the context of digital forensics and incident response, highlighting the importance of understanding what data may be lost upon system shutdown and what data persists.

90. Frage
.....

212-89 Fragen Antworten: https://www.it-pruefung.com/212-89.html

- 212-89 PDF Demo □ 212-89 Online Prüfungen □ 212-89 Ausbildungsressourcen □ Öffnen Sie die Website ▹ www.deutschpruefung.com ◃ Suchen Sie □ 212-89 □ Kostenloser Download □212-89 Fragenkatalog
- 212-89 Lerntipps □ 212-89 Lerntipps □ 212-89 Kostenlos Downloden □ Öffnen Sie die Webseite □ www.itzert.com □ und suchen Sie nach kostenloser Download von 【 212-89 】 □212-89 Übungsmaterialien
- Zertifizierung der 212-89 mit umfassenden Garantien zu bestehen □ Sie müssen nur zu 「 www.zertpruefung.de 」 gehen um nach kostenloser Download von 《 212-89 》 zu suchen □212-89 Online Prüfungen
- 212-89 Prüfungsguide: EC Council Certified Incident Handler (ECIH v3) - 212-89 echter Test - 212-89 sicherlich-zu-bestehen □ Suchen Sie auf [www.itzert.com] nach kostenlosem Download von 《 212-89 》 □212-89 Online Praxisprüfung
- 212-89 Ausbildungsressourcen □ 212-89 Zertifikatsfragen □ 212-89 Online Praxisprüfung □ Suchen Sie auf □ www.examfragen.de □ nach kostenlosem Download von ➤ 212-89 □ □212-89 Online Prüfungen
- 212-89 Neuesten und qualitativ hochwertige Prüfungsmaterialien bietet - quizfragen und antworten □ Sie müssen nur zu " www.itzert.com " gehen um nach kostenloser Download von ✔ 212-89 □✔□ zu suchen □212-89 Online Praxisprüfung
- 212-89 Dumps Deutsch □ 212-89 Ausbildungsressourcen □ 212-89 Demotesten □ Suchen Sie jetzt auf { www.zertpruefung.ch } nach ➠ 212-89 □ und laden Sie es kostenlos herunter □212-89 German
- 212-89 Testking ▸ 212-89 Testengine □ 212-89 Zertifizierungsantworten ⧗ Suchen Sie auf □ www.itzert.com □ nach 「 212-89 」 und erhalten Sie den kostenlosen Download mühelos □212-89 Kostenlos Downloden
- 212-89 Prüfungsunterlagen □ 212-89 Prüfungsmaterialien □ 212-89 Kostenlos Downloden □ Suchen Sie einfach auf " www.zertpruefung.de " nach kostenloser Download von □ 212-89 □ □212-89 Testking
- 212-89 Kostenlos Downloden □ 212-89 Zertifikatsfragen □ 212-89 Testking □ Suchen Sie auf □ www.itzert.com □ nach kostenlosem Download von [212-89] ☣212-89 Übungsmaterialien
- Neueste EC Council Certified Incident Handler (ECIH v3) Prüfung pdf - 212-89 Prüfung Torrent □ Geben Sie ▹ www.zertpruefung.ch ◃ ein und suchen Sie nach kostenloser Download von ➠ 212-89 □ □212-89 Unterlage
- 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, 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, 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 212-89 Prüfungsfragen sind auf Google Drive freigegeben von It-Pruefung verfügbar: https://drive.google.com/open?id=14UhrEwTzj-gJxZQxpov6xi4-2LFRut5d