Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Free - Reliable ISO-IEC-27035-Lead-Incident-Manager Dumps

P.S. Free & New ISO-IEC-27035-Lead-Incident-Manager dumps are available on Google Drive shared by Getcertkey: https://drive.google.com/open?id=1b8I9U_BMAFj5RswiBmlHdcoO4BYOF1fg

If you are still unsure whether to pursue PECB ISO-IEC-27035-Lead-Incident-Manager exam questions for PECB PECB Certified ISO/IEC 27035 Lead Incident Manager exam preparation, you are losing the game at the first stage in a fiercely competitive marketplace. PECB ISO-IEC-27035-Lead-Incident-Manager Questions are the best option for becoming PECB PECB Certified ISO/IEC 27035 Lead Incident Manager.

PECB ISO-IEC-27035-Lead-Incident-Manager Exam Syllabus Topics:

Topic	Details
Topic 1	• Fundamental principles and concepts of information security incident management: This section of the exam measures skills of Information Security Analysts and covers the core ideas behind incident management, including understanding what constitutes a security incident, why timely responses matter, and how to identify the early signs of potential threats.
Topic 2	• Improving the incident management processes and activities: This section of the exam measures skills of Incident Response Managers and covers the review and enhancement of existing incident management processes. It involves post-incident reviews, learning from past events, and refining tools, training, and techniques to improve future response efforts.
Topic 3	• Implementing incident management processes and managing information security incidents: This section of the exam measures skills of Information Security Analysts and covers the practical implementation of incident management strategies. It looks at ongoing incident tracking, communication during crises, and ensuring incidents are resolved in accordance with established protocols.
Topic 4	• Information security incident management process based on ISO • IEC 27035: This section of the exam measures skills of Incident Response Managers and covers the standardized steps and processes outlined in ISO • IEC 27035. It emphasizes how organizations should structure their incident response lifecycle from detection to closure in a consistent and effective manner.

>> Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Free <<

Reliable ISO-IEC-27035-Lead-Incident-Manager Dumps & Study ISO-IEC-27035-Lead-Incident-Manager Demo

Getcertkey online digital PECB ISO-IEC-27035-Lead-Incident-Manager exam questions are the best way to prepare. Using our PECB ISO-IEC-27035-Lead-Incident-Manager exam dumps, you will not have to worry about whatever topics you need to master. To practice for a PECB ISO-IEC-27035-Lead-Incident-Manager Certification Exam in the software (free test), you should perform a self-assessment.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q74-Q79):

NEW QUESTION # 74
Based on the categorization of information security incidents, incidents such as abuse of rights, denial of actions, and misoperations are categorized as:

- A. Breach of rule incident
- B. Compromise of information incident
- C. Compromise of functions incident

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1 classifies incidents into several categories based on the nature of their impact. Incidents involving the abuse of user rights, denial of authorized activities, or improper system use are considered violations of internal policies or rules. These fall under the category of "Breach of Rule" incidents.
This category emphasizes that while data or functionality may not be directly compromised, internal governance, permissions, or acceptable use policies have been violated. These incidents are crucial to detect as they often indicate insider threats or misconfigured permissions.
Reference:
ISO/IEC 27035-1:2016, Annex A.2.3: "Breach of Rule" incidents include abuse of privileges, unauthorized activities, and actions violating organizational policies.
Correct answer: C
-

NEW QUESTION # 75
During an ongoing cybersecurity incident investigation, the Incident Management Team (IMT) at a cybersecurity company identifies a pattern similar to recent attacks on other organizations. According to best practices, what actions should the IMT take?

- A. Proactively exchange technical information and incident insights with trusted Incident Response Teams (IRTs) from similar organizations while adhering to predefined information-sharing protocols to improve collective security postures
- B. Delay any external communication until a thorough internal review is conducted, and the impact of the incident is fully understood to prevent any premature information leakage that could affect ongoing mitigation efforts
- C. Focus on internal containment and eradication processes, consulting external experts strictly for legal and public relations management

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035 strongly encourages information sharing among trusted parties to enhance collective incident response capabilities and reduce the broader impact of cyber threats. Clause 6.5.6 in ISO/IEC 27035-1 highlights the importance of cooperation and communication with external parties, including industry-specific information-sharing forums, CERTs/CSIRTs, and trusted partners.
The practice of proactive information exchange allows organizations to:
Detect coordinated or widespread attacks
Accelerate response through shared indicators of compromise (IOCs)

Benefit from collective intelligence and incident analysis
Build sector-wide resilience
However, such exchanges must occur within well-defined protocols that preserve confidentiality, legal compliance, and operational integrity.
Option B and C reflect overly cautious or siloed approaches that may delay response or reduce the effectiveness of collaborative efforts.
Reference Extracts:
ISO/IEC 27035-1:2016, Clause 6.5.6: "Incident management should consider the importance of trusted collaboration, sharing of incident information, and threat intelligence between relevant entities." ENISA and FIRST.org also support this collaborative approach in their best practices.
Correct answer: A
-

NEW QUESTION # 76
Scenario 4: ORingo is a company based in Krakow, Poland, specializing in developing and distributing electronic products for health monitoring and heart rate measurement applications. With a strong emphasis on innovation and technological advancement, ORingo has established itself as a trusted provider of high-quality, reliable devices that enhance the well being and healthcare capabilities of individuals and healthcare professionals alike.
As part of its commitment to maintaining the highest standards of information security, ORingo has established an information security incident management process This process aims to ensure that any potential threats are swiftly identified, assessed, and addressed to protect systems and information. However, despite these measures, an incident response team member at ORingo recently detected a suspicious state in their systems operational data, leading to the decision to shut down the company-wide system until the anomaly could be thoroughly investigated Upon detecting the threat, the company promptly established an incident response team to respond to the incident effectively. The team's responsibilities encompassed identifying root causes, uncovering hidden vulnerabilities, and implementing timely resolutions to mitigate the impact of the incident on ORingo's operations and customer trust.
In response to the threat detected across its cloud environments. ORingo employed a sophisticated security tool that broadened the scope of incident detection and mitigation This tool covers network traffic, doud environments, and potential attack vectors beyond traditional endpoints, enabling ORingo to proactively defend against evolving cybersecurity threats During a routine check, the IT manager at ORingo discovered that multiple employees lacked awareness of proper procedures following the detection of a phishing email. In response, immediate training sessions on information security policies and incident response were scheduled for all employees, emphasizing the importance of vigilance and adherence to established protocols in safeguarding ORingo's sensitive data and assets.
As part of the training initiative. ORingo conducted a simulated phishing attack exercise to assess employee response and knowledge. However, an employee inadvertently informed an external partner about the 'attack" during the exercise, highlighting the importance of ongoing education and reinforcement of security awareness principles within the organization.
Through its proactive approach to incident management and commitment to fostering a culture of security awareness and readiness. ORingo reaffirms its dedication to safeguarding the integrity and confidentiality of its electronic products and ensuring the trust and confidence of its customers and stakeholders worldwide.
In scenario 4, during a routine check, the IT manager discovered that multiple employees were unaware of the proper procedures following the detection of a phishing email and scheduled immediate training for all employees on information security policies and incident response. Is this recommended?

- A. No, the IT manager should handle the incident without involving other employees
- B. No, providing training is unnecessary; the employees' ignorance of proper procedures regarding phishing emails is a minor issue
- C. Yes, it is recommended that immediate training on these topics be provided to ensure employees know how to respond correctly to phishing emails

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
Phishing is one of the most common entry points for cybersecurity incidents. ISO/IEC 27035 and ISO/IEC
27002 both recommend security awareness training as a key preventive control. When users do not understand proper response procedures, the risk of successful attacks increases significantly.
Providing immediate training, especially following the identification of a knowledge gap, is considered best practice. This aligns with ISO/IEC 27001:2022 Annex A.6.3 and A.5.36, which emphasize the need for education and continuous awareness on security topics, including how to handle phishing attempts.
Reference:
ISO/IEC 27035-1:2016, Clause 6.1 - "Preparation includes awareness training to reduce the likelihood and impact of incidents."

ISO/IEC 27002:2022, Control A.6.3 - "Personnel should receive appropriate awareness education and training to carry out their information security responsibilities." Therefore, the correct answer is A.

NEW QUESTION # 77
Scenario 3: L&K Associates is a graphic design firm headquartered in Johannesburg, South Africa. It specializes in providing innovative and creative design solutions to clients across various industries. With offices in multiple parts of the country, they effectively serve clients, delivering design solutions that meet their unique needs and preferences.
In its commitment to maintaining information security, L&K Associates is implementing an information security incident management process guided by ISO/IEC 27035-1 and ISO/IEC 27035-2. Leona, the designated leader overseeing the implementation of the incident management process, customized the scope of incident management to align with the organization's unique requirements. This involved specifying the IT systems, services, and personnel involved in the incident management process while excluding potential incident sources beyond those directly related to IT systems and services.
Based on the scenario above, answer the following question:
Is the incident management scope correctly determined at L&K Associates?

- A. No, the incident management scope is overly restrictive, excluding potential incident sources beyond those directly related to IT systems and services
- B. No, the incident management scope is too broad, encompassing all IT systems regardless of relevance
- C. Yes, the incident management scope is customized to align with the organization's unique needs

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 encourages organizations to define the scope of incident management based on their own risk environment, business model, and available resources. This scope should be tailored to focus on the systems, services, and personnel that are most critical and relevant to the organization's operations.
In this scenario, Leona appropriately aligned the scope with L&K Associates' specific IT infrastructure and business processes, deliberately including relevant IT systems and associated personnel while excluding unrelated sources. This customization is consistent with best practices and ensures that the incident management process remains focused, efficient, and manageable.
ISO/IEC 27035-2, Clause 4.2, emphasizes that "the scope of incident management should be defined in a way that it supports the organization's objectives and risk environment." Therefore, the correct answer is A: Yes, the incident management scope is customized to align with the organization's unique needs.
-

NEW QUESTION # 78
Scenario 6: EastCyber has established itself as a premier cyber security company that offers threat detection, vulnerability assessment, and penetration testing tailored to protect organizations from emerging cyber threats. The company effectively utilizes ISO/IEC 27035*1 and 27035-2 standards, enhancing its capability to manage information security incidents.
EastCyber appointed an information security management team led by Mike Despite limited resources, Mike and the team implemented advanced monitoring protocols to ensure that every device within the company's purview is under constant surveillance This monitoring approach is crucial for covering everything thoroughly, enabling the information security and cyber management team to proactively detect and respond to any sign of unauthorized access, modifications, or malicious activity within its systems and networks.
In addition, they focused on establishing an advanced network traffic monitoring system This system carefully monitors network activity, quickly spotting and alerting the security team to unauthorized actions This vigilance is pivotal in maintaining the integrity of EastCyber's digital infrastructure and ensuring the confidentiality, availability, and integrity of the data it protects.
Furthermore, the team focused on documentation management. They meticulously crafted a procedure to ensure thorough documentation of information security events. Based on this procedure, the company would document only the events that escalate into high-severity incidents and the subsequent actions. This documentation strategy streamlines the incident management process, enabling the team to allocate resources more effectively and focus on incidents that pose the greatest threat.
A recent incident involving unauthorized access to company phones highlighted the critical nature of incident management. Nate, the incident coordinator, quickly prepared an exhaustive incident report. His report detailed an analysis of the situation, identifying the problem and its cause. However, it became evident that assessing the seriousness and the urgency of a response was inadvertently overlooked.
In response to the incident, EastCyber addressed the exploited vulnerabilities. This action started the eradication phase, aimed at systematically eliminating the elements of the incident. This approach addresses the immediate concerns and strengthens EastCyber's defenses against similar threats in the future.

According to scenario 6, what mechanisms for detecting security incidents did EastCyber implement?

- A. Intrusion detection systems
- B. Intrusion prevention systems
- C. Security information and event management systems

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the scenario, EastCyber implemented an "advanced network traffic monitoring system" that "spots and alerts the security team to unauthorized actions." This aligns closely with the functional characteristics of an Intrusion Detection System (IDS), which monitors traffic or systems for malicious activities and policy violations and sends alerts for review.
While Security Information and Event Management (SIEM) tools and Intrusion Prevention Systems (IPS) offer valuable detection and response capabilities, the scenario specifically describes a system focused on monitoring and alerting-not automatically blocking traffic, which would indicate an IPS.
SIEM platforms correlate and analyze logs from various sources, which wasn't described. Therefore, IDS is the most accurate interpretation.
Reference:
ISO/IEC 27035-2:2016, Clause 7.4.2: "Detection mechanisms can include intrusion detection systems, log analysis tools, and traffic monitoring systems to detect potential security events." Correct answer: B
-

NEW QUESTION # 79
.....

Our company is a professional certification exam materials provider, we have occupied in the field for more than ten years, and therefore we have rich experiences. In addition, ISO-IEC-27035-Lead-Incident-Manager Exam Materials have free demo, and you can have a try before buying, so that you can have a deeper understanding for ISO-IEC-27035-Lead-Incident-Manager exam dumps. We are pass guarantee and money back guarantee, and if you fail to pass the exam, we will give you full refund. You can receive your download link and password within ten minutes, so that you can start your learning as quickly as possible. We have online and offline chat service, if you have any questions for the exam, you can consult us.

Reliable ISO-IEC-27035-Lead-Incident-Manager Dumps: https://www.getcertkey.com/ISO-IEC-27035-Lead-Incident-Manager_braindumps.html

- ISO-IEC-27035-Lead-Incident-Manager Latest Braindumps Free □ ISO-IEC-27035-Lead-Incident-Manager Pdf Torrent □ Sample ISO-IEC-27035-Lead-Incident-Manager Questions Answers □ Search for { ISO-IEC-27035-Lead-Incident-Manager } and download it for free on ▹ www.getvalidtest.com ◃ website □ISO-IEC-27035-Lead-Incident-Manager New Test Camp
- Right Q-A in PECB ISO-IEC-27035-Lead-Incident-Manager Exam Questions ↖ Easily obtain " ISO-IEC-27035-Lead-Incident-Manager " for free download through □ www.pdfvce.com □ □ISO-IEC-27035-Lead-Incident-Manager Quiz
- Pass Guaranteed PECB - ISO-IEC-27035-Lead-Incident-Manager Perfect Valid Dumps Free □ Search for ➥ ISO-IEC-27035-Lead-Incident-Manager □ and download it for free immediately on 【 www.testkingpdf.com 】 □ISO-IEC-27035-Lead-Incident-Manager Quiz
- Sample ISO-IEC-27035-Lead-Incident-Manager Questions Answers □ Sample ISO-IEC-27035-Lead-Incident-Manager Questions Pdf □ ISO-IEC-27035-Lead-Incident-Manager Study Test □ Search for □ ISO-IEC-27035-Lead-Incident-Manager □ and obtain a free download on 【 www.pdfvce.com 】 □Real ISO-IEC-27035-Lead-Incident-Manager Testing Environment
- Valid Test ISO-IEC-27035-Lead-Incident-Manager Format □ Valid ISO-IEC-27035-Lead-Incident-Manager Exam Papers □ ISO-IEC-27035-Lead-Incident-Manager Latest Braindumps Free □ Easily obtain free download of ✔ ISO-IEC-27035-Lead-Incident-Manager □✔□ by searching on [www.testsimulate.com] □Real ISO-IEC-27035-Lead-Incident-Manager Testing Environment
- The Best Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Free Offers Candidates Perfect Actual PECB PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Products □ Search for （ ISO-IEC-27035-Lead-Incident-Manager ） and download exam materials for free through □ www.pdfvce.com □ □ISO-IEC-27035-Lead-Incident-Manager Reliable Braindumps
- ISO-IEC-27035-Lead-Incident-Manager Pdf Torrent □ ISO-IEC-27035-Lead-Incident-Manager Valid Exam Review □ □ Best ISO-IEC-27035-Lead-Incident-Manager Vce □ Download □ ISO-IEC-27035-Lead-Incident-Manager □ for free by simply entering [www.testsimulate.com] website □Real ISO-IEC-27035-Lead-Incident-Manager Testing

Environment

- ISO-IEC-27035-Lead-Incident-Manager Valid Exam Review □ Test ISO-IEC-27035-Lead-Incident-Manager Simulator Fee □ ISO-IEC-27035-Lead-Incident-Manager Reliable Braindumps □ Easily obtain free download of ▸ ISO-IEC-27035-Lead-Incident-Manager ◂ by searching on [www.pdfvce.com] □Exam ISO-IEC-27035-Lead-Incident-Manager Exercise
- The Best Valid Dumps ISO-IEC-27035-Lead-Incident-Manager Free Offers Candidates Perfect Actual PECB PECB Certified ISO/IEC 27035 Lead Incident Manager Exam Products ➡ Open 《 www.examsreviews.com 》 enter ☀ ISO-IEC-27035-Lead-Incident-Manager □☀□ and obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Latest Braindumps Free
- ISO-IEC-27035-Lead-Incident-Manager Exam Quiz 🈵 Sample ISO-IEC-27035-Lead-Incident-Manager Questions Pdf □ Hot ISO-IEC-27035-Lead-Incident-Manager Questions □ Search for ➥ ISO-IEC-27035-Lead-Incident-Manager □ and download exam materials for free through ▸ www.pdfvce.com ◂ □ISO-IEC-27035-Lead-Incident-Manager Exam Blueprint
- Real ISO-IEC-27035-Lead-Incident-Manager Testing Environment □ ISO-IEC-27035-Lead-Incident-Manager Latest Braindumps Free □ ISO-IEC-27035-Lead-Incident-Manager New Test Camp □ Download ➽ ISO-IEC-27035-Lead-Incident-Manager □ for free by simply searching on ✔ www.examcollectionpass.com □✔□ □New ISO-IEC-27035-Lead-Incident-Manager Test Camp
- edumente.me, 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, sdbagroup.com, tomfox883.ampblogs.com, digilearn.co.zw, www.myaniway.com, alisadosdanys.top, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New ISO-IEC-27035-Lead-Incident-Manager dumps are available on Google Drive shared by Getcertkey: https://drive.google.com/open?id=1b8I9U_BMAFj5RswiBmlHdcoO4BYOF1fg