ISO-IEC-27035-Lead-Incident-Manager Reliable Braindumps Sheet & Exam ISO-IEC-27035-Lead-Incident-Manager Learning

BTW, DOWNLOAD part of DumpsReview ISO-IEC-27035-Lead-Incident-Manager dumps from Cloud Storage: https://drive.google.com/open?id=1rltFCf3ha5ORc8HPerqPPysM7fLEoP9b

At DumpsReview, we offer a ISO-IEC-27035-Lead-Incident-Manager dumps PDF, desktop PECB ISO-IEC-27035-Lead-Incident-Manager practice test software, and a web-based practice exam which is specifically designed to help you prepare for your PECB ISO-IEC-27035-Lead-Incident-Manager Certification Exam. Whether you are looking for real PECB ISO-IEC-27035-Lead-Incident-Manager dumps pdf file or practice exams to help you master the PECB ISO-IEC-27035-Lead-Incident-Manager exam, we have got you covered.

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

Topic	Details
Topic 1	• 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 2	- Designing and developing an organizational incident management process based on ISO - IEC 27035: This section of the exam measures skills of Information Security Analysts and covers how to tailor the ISO - IEC 27035 framework to the unique needs of an organization, including policy development, role definition, and establishing workflows for handling incidents.
Topic 3	- 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.

>> ISO-IEC-27035-Lead-Incident-Manager Reliable Braindumps Sheet <<

Exam PECB ISO-IEC-27035-Lead-Incident-Manager Learning | ISO-IEC-27035-Lead-Incident-Manager Reliable Dumps Book

Today is the right time to learn new and in demands skills. You can do this easily, just get registered in certification exam and start preparation with PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager exam dumps. The PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager pdf questions and practice test are ready for download. Just pay the affordable ISO-IEC-27035-Lead-Incident-Manager authentic dumps charges and click on the download button. Get the ISO-IEC-27035-Lead-Incident-Manager latest dumps and start preparing today.

PECB Certified ISO/IEC 27035 Lead Incident Manager Sample Questions (Q79-Q84):

NEW QUESTION # 79
What is the purpose of incident identification in the incident response process?

- A. To collect all data related to the incident, including information from affected systems, network logs, user accounts, and any other relevant sources
- B. To conduct a preliminary assessment of the incident
- C. To recognize incidents through various methods like intrusion detection systems and employee reports

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Incident identification is the first operational step in the incident response process. It involves detecting unusual or suspicious activity and recognizing whether it constitutes an information security incident. ISO
/IEC 27035-1:2016 describes various sources of detection, such as:
Security monitoring tools (e.g., IDS/IPS)
User reports or helpdesk notifications
Automated alerts from applications or infrastructure
The goal at this stage is not to collect detailed forensic data or conduct deep analysis, but rather to determine whether the activity warrants classification as a potential incident and to escalate accordingly.
Reference:
ISO/IEC 27035-1:2016, Clause 6.2.1: "Incident identification involves recognizing the occurrence of an event that could be an information security incident." Correct answer: C
-

NEW QUESTION # 80
Scenario 7: Located in central London, Konzolo has become a standout innovator in the cryptocurrency field.
The company faced challenges monitoring the security of its own and third-party systems. An incident involving server downtime exposed vulnerabilities in a third-party service provider's security posture, leading to unauthorized access.
In response, Konzolo launched a thorough vulnerability scan of its cryptographic wallet software and uncovered critical weaknesses

due to outdated encryption algorithms. Noah, the IT manager, documented and communicated the findings. Paulina was brought in to lead a forensic investigation, provide actionable insights, and help enhance the company's overall incident response strategy based on ISO/IEC 27035 standards.
Based on the scenario above, answer the following question:
Which of the following steps for effective security monitoring did Konzolo NOT adhere to?

- A. Monitor the outsourced services
- B. Monitor behavioral analytics
- C. Monitor security vulnerabilities

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016 emphasize the importance of monitoring not only internal systems but also third-party or outsourced services. Clause 7.3.2 of ISO/IEC 27035-2 specifically recommends that organizations establish mechanisms for the continuous monitoring of service providers and outsourced systems, particularly when such services process or store sensitive information.
In the scenario, Konzolo suffered an incident due to a failure by a third-party service provider to uphold security controls. This indicates that Konzolo had insufficient or no effective monitoring of outsourced services in place, which directly contributed to the breach and system downtime.
On the other hand:
Option A is incorrect because Konzolo did conduct a vulnerability scan, identifying and addressing cryptographic weaknesses.
Option B is also incorrect, as Paulina conducted forensic and behavioral analysis (both manual and automated) as part of the investigation process.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.3.2: "Monitoring should not be limited to internal infrastructure but should include third-party and outsourced services to ensure that they are operating within defined security parameters." ISO/IEC 27002:2022, Control 5.23: "Information security should be addressed in agreements with third parties." Correct answer: C
-

NEW QUESTION # 81
Which team has a broader cybersecurity role, including incident response, monitoring, and overseeing general operations?

- A. Computer Security Incident Response Team (CSIRT)
- B. Computer Emergency Response Team (CERT)
- C. Security Operations Center (SOC)

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035 and industry best practices, a Security Operations Center (SOC) is the central hub for an organization's cybersecurity operations. Its responsibilities go beyond pure incident response.
SOCs continuously monitor the organization's network and systems for suspicious activity and threats, providing real-time threat detection, incident response coordination, vulnerability management, and overall security infrastructure oversight.
While CSIRTs and CERTs specialize in handling and managing security incidents, their roles are generally more narrowly focused on the detection, reporting, and resolution of security events. SOCs, on the other hand, manage the broader spectrum of operations, including:
Real-time monitoring and logging
Threat hunting and intelligence
Security incident analysis and triage
Coordinating CSIRT activities
Supporting policy compliance and auditing
Integration with vulnerability management and security infrastructure
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.3.1: "Monitoring systems and activities should be established, operated and maintained to identify deviations from normal behavior." NIST SP 800-61 Revision 2 and industry alignment with ISO/IEC 27035 recognize the SOC as the broader operational environment that houses or interacts with the CSIRT/CERT.
Therefore, the correct answer is: B - Security Operations Center (SOC)

-

NEW QUESTION # 82

Scenario 8: Moneda Vivo, headquartered in Kuala Lumpur. Malaysia, is a distinguished name in the banking sector. It is renowned for its innovative approach to digital banking and unwavering commitment to information security. Moneda Vivo stands out by offering various banking services designed to meet the needs of its clients. Central to its operations is an information security incident management process that adheres to the recommendations of ISO/IEC 27035-1 and 27035-2.

Recently. Moneda Vivo experienced a phishing attack aimed at its employees Despite the bank's swift identification and containment of the attack, the incident led to temporary service outages and data access issues, underscoring the need for improved resilience The response team compiled a detailed review of the attack, offering valuable insights into the techniques and entry points used and identifying areas for enhancing their preparedness.

Shortly after the attack, the bank strengthened its defense by implementing a continuous review process to ensure its incident management procedures and systems remain effective and appropriate While monitoring the incident management process, a trend became apparent. The mean time between similar incidents decreased after a few occurrences; however, Moneda Vivo strategically ignored the trend and continued with regular operations This decision was rooted in a deep confidence in its existing security measures and incident management protocols, which had proven effective in quick detection and resolution of issues Moneda Vivo's commitment to transparency and continual improvement is exemplified by its utilization of a comprehensive dashboard. This tool provides real time insights into the progress of its information security incident management, helping control operational activities and ensure that processes stay within the targets of productivity, quality, and efficiency. However, securing its digital banking platform proved challenging.

Following a recent upgrade, which included a user interface change to its digital banking platform and a software update, Moneda Vivo recognized the need to immediately review its incident management process for accuracy and completeness. The top management postponed the review due to financial and time constraints.

Based on scenario 8, Moneda Vivo conducts continuous review of the incident management process to ensure the effectiveness of processes and procedures in place. Is this a good practice to follow?

- A. Yes, organizations should conduct continuous review of the incident management process to ensure the effectiveness of the processes and procedures in place
- B. No, organizations should regularly assess the physical security measures to ensure they align with incident management protocols
- C. No, organizations should conduct quarterly performance reviews of individual employees to ensure they follow incident management protocols

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
ISO/IEC 27035-1:2016 stresses the importance of continual review and improvement of the incident management process. Clause 7.1 specifically advises that organizations regularly evaluate their policies, procedures, and tools to ensure they remain effective in the face of evolving threats and business changes.
Moneda Vivo's continuous review aligns perfectly with this guidance, reinforcing preparedness and adaptability. Options A and C, while related to broader security or HR practices, are not directly aligned with ISO/IEC 27035's core recommendation regarding process review.
Reference:
ISO/IEC 27035-1:2016, Clause 7.1: "The organization should review the effectiveness of the information security incident management process regularly and in response to incidents and significant changes."

NEW QUESTION # 83

What is the purpose of a gap analysis?

- A. To identify the differences between current processes and company policies
- B. To assess risks associated with identified gaps in current practices compared to best practices
- C. To determine the steps to achieve a desired future state from the current state

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
Gap analysis is a structured method used to compare the current state of processes, capabilities, or systems against a desired or

required state (such as compliance with ISO standards). The main goal is to determine what needs to change to achieve that future state. While identifying gaps (A) and assessing risks (C) may occur during the process, the primary purpose is strategic planning and improvement.
Reference:
ISO/IEC 27001 Implementation Guidelines, Clause 0.3: "Gap analysis is used to evaluate the difference between current practices and ISO requirements and to define actions to meet compliance." Correct answer: B
-

NEW QUESTION # 84
......

Our PECB Certified ISO/IEC 27035 Lead Incident Manager ISO-IEC-27035-Lead-Incident-Manager questions PDF is a complete bundle of problems presenting the versatility and correlativity of questions observed in past exam papers. These questions are bundled into PECB Certified ISO/IEC 27035 Lead Incident Manager PDF questions following the official study guide. PECB ISO-IEC-27035-Lead-Incident-Manager PDF Questions are a portable, printable document that simultaneously plays on multiple devices. Our PECB ISO-IEC-27035-Lead-Incident-Manager PDF questions consists of problems in all aspects, whether theoretical, practical, or analytical.

Exam ISO-IEC-27035-Lead-Incident-Manager Learning: https://www.dumpsreview.com/ISO-IEC-27035-Lead-Incident-Manager-exam-dumps-review.html

- ISO-IEC-27035-Lead-Incident-Manager Free Download Demo - ISO-IEC-27035-Lead-Incident-Manager Latest Exam Tutorial - ISO-IEC-27035-Lead-Incident-Manager Valid Study Reviews ♣ Go to website ☀ www.prep4sures.top □☀□ open and search for ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ to download for free □ISO-IEC-27035-Lead-Incident-Manager Valid Test Cram
- ISO-IEC-27035-Lead-Incident-Manager Free Download Demo - ISO-IEC-27035-Lead-Incident-Manager Latest Exam Tutorial - ISO-IEC-27035-Lead-Incident-Manager Valid Study Reviews □ Search for { ISO-IEC-27035-Lead-Incident-Manager } and easily obtain a free download on ☀ www.pdfvce.com □☀□ □New ISO-IEC-27035-Lead-Incident-Manager Test Prep
- Is It Important To Get PECB ISO-IEC-27035-Lead-Incident-Manager Exam Material For The Exam? □ Enter 《 www.dumpsquestion.com 》 and search for ➡ ISO-IEC-27035-Lead-Incident-Manager □□□ to download for free □ □Reliable ISO-IEC-27035-Lead-Incident-Manager Cram Materials
- Quiz PECB - The Best ISO-IEC-27035-Lead-Incident-Manager Reliable Braindumps Sheet □ Easily obtain free download of ➥ ISO-IEC-27035-Lead-Incident-Manager □ by searching on { www.pdfvce.com } □ISO-IEC-27035-Lead-Incident-Manager Training Courses
- ISO-IEC-27035-Lead-Incident-Manager Valid Exam Pdf □ ISO-IEC-27035-Lead-Incident-Manager Reliable Test Duration □ New ISO-IEC-27035-Lead-Incident-Manager Exam Vce □ Enter ☀ www.prepawaypdf.com □☀□ and search for ⇛ ISO-IEC-27035-Lead-Incident-Manager ⇚ to download for free □Reliable ISO-IEC-27035-Lead-Incident-Manager Cram Materials
- Authentic PECB ISO-IEC-27035-Lead-Incident-Manager PDF Dumps - Get Outstanding Results In Exam □ Download ➥ ISO-IEC-27035-Lead-Incident-Manager □ for free by simply entering □ www.pdfvce.com □ website □ISO-IEC-27035-Lead-Incident-Manager PDF Question
- ISO-IEC-27035-Lead-Incident-Manager Exam Outline □ Free ISO-IEC-27035-Lead-Incident-Manager Dumps □ Valid ISO-IEC-27035-Lead-Incident-Manager Exam Question □ Download { ISO-IEC-27035-Lead-Incident-Manager } for free by simply searching on □ www.examcollectionpass.com □ □Valid Braindumps ISO-IEC-27035-Lead-Incident-Manager Questions
- ISO-IEC-27035-Lead-Incident-Manager Reliable Test Sims □ ISO-IEC-27035-Lead-Incident-Manager Valid Test Guide □ ISO-IEC-27035-Lead-Incident-Manager Training Courses □ Search for ▷ ISO-IEC-27035-Lead-Incident-Manager ◁ on [www.pdfvce.com] immediately to obtain a free download □ISO-IEC-27035-Lead-Incident-Manager Reliable Test Duration
- Is It Important To Get PECB ISO-IEC-27035-Lead-Incident-Manager Exam Material For The Exam? □ Open □ www.verifieddumps.com □ and search for （ ISO-IEC-27035-Lead-Incident-Manager ） to download exam materials for free □Latest ISO-IEC-27035-Lead-Incident-Manager Test Question
- ISO-IEC-27035-Lead-Incident-Manager Free Download Demo - ISO-IEC-27035-Lead-Incident-Manager Latest Exam Tutorial - ISO-IEC-27035-Lead-Incident-Manager Valid Study Reviews □ Copy URL 【 www.pdfvce.com 】 open and search for 【 ISO-IEC-27035-Lead-Incident-Manager 】 to download for free □ISO-IEC-27035-Lead-Incident-Manager Valid Test Cram
- Latest ISO-IEC-27035-Lead-Incident-Manager Exam Forum □ Reliable ISO-IEC-27035-Lead-Incident-Manager Cram Materials □ Reliable ISO-IEC-27035-Lead-Incident-Manager Cram Materials □ Search on （ www.pass4test.com ） for ➽ ISO-IEC-27035-Lead-Incident-Manager □ to obtain exam materials for free download □Latest ISO-IEC-

27035-Lead-Incident-Manager Exam Forum

- 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, lms.ait.edu.za, shortcourses.russellcollege.edu.au, exxpertscm.com, daotao.wisebusiness.edu.vn, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes