시험패스에유효한ISO-IEC-27035-Lead-Incident-Manager적중율높은인증시험덤프최신버전공부자료

참고: PassTIP에서 Google Drive로 공유하는 무료 2025 PECB ISO-IEC-27035-Lead-Incident-Manager 시험 문제집이 있습니다: https://drive.google.com/open?id=1Oo9VIeBLxSDEuPLnxkxQhS_yVFBceEAx

ISO-IEC-27035-Lead-Incident-Manager인증시험은PECB인증시험중의 하나입니다.그리고 또한 비중이 아주 큰 인증시험입니다. 그리고PECB ISO-IEC-27035-Lead-Incident-Manager인증시험 패스는 진짜 어렵다고 합니다. 우리 PassTIP에서는 여러분이ISO-IEC-27035-Lead-Incident-Manager인증시험을 편리하게 응시하도록 전문적이 연구팀에서 만들어낸 최고의ISO-IEC-27035-Lead-Incident-Manager덤프를 제공합니다, PassTIP와 만남으로 여러분은 아주 간편하게 어려운 시험을 패스하실 수 있습니다,

PassTIP를 선택함으로 여러분은 PECB 인증ISO-IEC-27035-Lead-Incident-Manager시험에 대한 부담은 사라질 것입니다.우리 PassTIP는 끊임없는 업데이트로 항상 최신버전의 PECB 인증ISO-IEC-27035-Lead-Incident-Manager시험덤프임을 보장해드립니다.만약 덤프품질을 확인하고 싶다면PassTIP 에서 무료로 제공되는PECB 인증ISO-IEC-27035-Lead-Incident-Manager덤프의 일부분 문제를 체험하시면 됩니다.PassTIP 는 100%의 보장도를 자랑하며PECB 인증ISO-IEC-27035-Lead-Incident-Manager시험을 한번에 패스하도록 도와드립니다.

>> ISO-IEC-27035-Lead-Incident-Manager적중율 높은 인증시험덤프 <<

ISO-IEC-27035-Lead-Incident-Manager인증시험자료 - ISO-IEC-27035-Lead-Incident-Manager합격보장 가능 공부자료

PassTIP의 경험이 풍부한 IT전문가들이 연구제작해낸 PECB인증 ISO-IEC-27035-Lead-Incident-Manager덤프는 시험패스율이 100%에 가까워 시험의 첫번째 도전에서 한방에 시험패스하도록 도와드립니다. PECB인증 ISO-IEC-27035-Lead-Incident-Manager덤프는PECB인증 ISO-IEC-27035-Lead-Incident-Manager최신 실제시험문제의 모든 시험문제를 커버하고 있어 덤프에 있는 내용만 공부하시면 아무런 걱정없이 시험에 도전할수 있습니다.

PECB ISO-IEC-27035-Lead-Incident-Manager 시험요강:

주제	소개
주제 1	• 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.
주제 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.

주제 3	• 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.

최신 ISO 27001 ISO-IEC-27035-Lead-Incident-Manager 무료샘플문제 (Q71-Q76):

질문 # 71
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. Security information and event management systems
- C. Intrusion prevention systems

정답：A

설명:
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
-

질문 # 72
Scenario 5: Located in Istanbul. Turkey. Alura Hospital is a leading medical institution specializing in advanced eye surgery and

vision care. Renowned for its modern facilities, cutting edge technology, and highly skilled staff, Alura Hospital is committed to delivering exceptional patient care. Additionally, Alura Hospital has implemented the ISO/IEC 27035 standards to enhance its information security incident management practices.
At Alura Hospital, the information security incident management plan is a critical component of safeguarding patient data and maintaining the integrity of its medical services This comprehensive plan includes instructions for handling vulnerabilities discovered during incident management According to this plan, when new vulnerabilities are discovered, Mehmet is appointed as the incident handler and is authorized to patch the vulnerabilities without assessing their potential impact on the current incident, prioritizing patient data security above all else Recognizing the importance of a structured approach to incident management. Alura Hospital has established four teams dedicated to various aspects of incident response The planning team focuses on implementing security processes and communicating with external organizations The monitoring team is responsible for security patches, upgrades, and security policy implementation The analysis team adjusts risk priorities and manages vulnerability reports, while the test and evaluation team organizes and performs incident response tests to ensure preparedness During an incident management training session, staff members at Alura Hospital were provided with clear roles and responsibilities. However, a technician expressed uncertainty about their role during a data integrity incident as the manager assigned them a role unrelated to their expertise. This decision was made to ensure that all staff members possess versatile skills and are prepared to handle various scenarios effectively. Additionally. Alura Hospital realized it needed to communicate better with stakeholders during security incidents. The hospital discovered it was not adequately informing stakeholders and that relevant information must be provided using formats, language, and media that meet their needs. This would enable them to participate fully in the incident response process and stay informed about potential risks and mitigation strategies.
Also, the hospital has experienced frequent network performance issues affecting critical hospital systems and increased sophisticated cyber attacks designed to bypass traditional security measures. So, it has deployed an external firewall. This action is intended to strengthen the hospital s network security by helping detect threats that have already breached the perimeter defenses. The firewall's implementation is a part of the hospital's broader strategy to maintain a robust and secure IT infrastructure, which is crucial for protecting sensitive patient data and ensuring the reliability of critical hospital systems. Alura Hospital remains committed to integrating state-of-the-art technology solutions to uphold the highest patient care and data security standards.
When vulnerabilities are discovered during incident management, Mehmet takes action to patch the vulnerabilities without assessing their potential impact on the current incident. Is this action in accordance with ISO/IEC 27035-2 recommendations?

- A. No, he should report the vulnerability to the incident coordinator, who will redirect the issue to the team responsible for the vulnerability
- B. Yes, vulnerabilities should be patched without assessing their potential impact on the current incident
- C. No, he should wait for a scheduled vulnerability assessment instead

정답：A

설명：
Comprehensive and Detailed Explanation:
According to ISO/IEC 27035-2:2016, vulnerabilities identified during incident handling must be assessed and documented before remediation. Immediate patching without evaluating its impact could compromise incident evidence, interfere with ongoing investigations, or unintentionally trigger additional issues.
ISO/IEC 27035-2 recommends that the incident coordinator (or an equivalent role) be responsible for directing how such vulnerabilities are managed and coordinated across relevant teams. This maintains process integrity and avoids uncoordinated actions.
Reference:
ISO/IEC 27035-2:2016, Clause 6.4.2: "Detected vulnerabilities should be communicated to appropriate stakeholders for evaluation. Unauthorized immediate actions could affect incident containment or recovery efforts." Correct answer: C
-

질문 # 73
What is one of the requirements for an organization's technical means in supporting information security?

- A. Quick acquisition of information security event/incident/vulnerability reports
- B. Public disclosure of contact register details for transparency
- C. Immediate deletion of all incident reports for security purposes

정답：A

설명：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27035-2:2016, one of the technical requirements to support effective incident management is the capability

to rapidly detect, collect, and process information about security events, incidents, and vulnerabilities. Timely acquisition of this data allows the organization to assess threats, determine the scope of incidents, and execute response measures quickly.
Clause 7.4.1 emphasizes the need for adequate tools and infrastructure to support the detection and acquisition of information security events and vulnerability reports. The collected data becomes the foundation for risk assessment, root cause analysis, and corrective action planning.
Option A (public disclosure of contact details) might be relevant for CERT/CSIRT public coordination but is not a core requirement in technical incident response. Option B (immediate deletion of reports) is contrary to best practices, as incident reports are critical for audits, compliance, and continuous improvement.
Reference Extracts:
ISO/IEC 27035-2:2016, Clause 7.4.1: "Organizations should ensure that technical means are in place to allow quick acquisition and analysis of information related to events, incidents, and vulnerabilities." Correct answer: C
-

질문 # 74
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.
According to scenario 4, in response to a detected threat across its cloud environments, which tool did ORingo utilize to extend its threat detection and response capabilities beyond traditional endpoints?

- A. SIEM
- B. IPS
- C. XDR

정답：C

설명：
Comprehensive and Detailed Explanation:
XDR (Extended Detection and Response) is a security solution that integrates and correlates data across multiple domains including endpoints, networks, cloud workloads, and more. In the scenario, the tool is described as capable of covering network traffic, cloud environments, and beyond-characteristics that align directly with the capabilities of XDR.
IPS (Intrusion Prevention System) focuses narrowly on network perimeter security.
SIEM (Security Information and Event Management) is primarily focused on log aggregation and analysis rather than real-time detection and automated response across multiple layers.
Reference:
NIST SP 800-207 and modern security frameworks define XDR as a centralized detection and response platform with cross-domain visibility.
Therefore, the correct answer is A: XDR
-

질문 # 75
Which of the following is NOT an example of technical control?

- A. Implementing a policy for regular password changes
- B. Implementing surveillance cameras
- C. Installing a firewall to protect the network

정답： A

설명：
Comprehensive and Detailed Explanation From Exact Extract:
According to ISO/IEC 27002:2022 (and earlier versions), information security controls can be broadly categorized into three types: technical (also called logical), physical, and administrative (or organizational) controls.
Technical controls (also known as logical controls) involve the use of software and hardware to protect assets.
Examples include:
Firewalls
Intrusion detection systems
Encryption
Access control mechanisms
Physical controls are designed to prevent physical access to IT systems and include things such as:
Surveillance cameras
Security guards
Biometric access systems
Administrative controls, also called management or procedural controls, include the policies, procedures, and guidelines that govern the organization's security practices. These include:
Security awareness training
Acceptable use policies
Password policies
Option A, "Implementing a policy for regular password changes," is an administrative control, not a technical one. It dictates user behavior through rules and policy enforcement, but does not technically enforce the change itself unless paired with technical enforcement (like system settings).
Option B, surveillance cameras, are physical controls, and option C, installing a firewall, is a classic example of a technical control.
Reference Extracts:
ISO/IEC 27002:2022, Clause 5.1 - "Information security controls can be administrative (policy-based), technical, or physical depending on their form and implementation." NIST SP 800-53, Control Families - Differentiates between management, operational, and technical controls.
Therefore, the correct answer is A: Implementing a policy for regular password changes.
-

질문 # 76
.....

- 시험준비에 가장 좋은 ISO-IEC-27035-Lead-Incident-Manager적중율 높은 인증시험덤프 최신버전 덤프샘플문제 다운로드 □ 오픈 웹 사이트▸ www.dumptop.com ◂검색➠ ISO-IEC-27035-Lead-Incident-Manager □무료 다운로드ISO-IEC-27035-Lead-Incident-Manager최신 덤프데모
- ISO-IEC-27035-Lead-Incident-Manager적중율 높은 인증시험덤프 인증덤프는 PECB Certified ISO/IEC 27035 Lead Incident Manager 시험 기출문제모음집 □ ➡ ISO-IEC-27035-Lead-Incident-Manager □□□를 무료로 다운로드하려면“ www.itdumpskr.com ”웹사이트를 입력하세요ISO-IEC-27035-Lead-Incident-Manager적중율 높은 덤프
- ISO-IEC-27035-Lead-Incident-Manager적중율 높은 인증시험덤프 인증덤프는 PECB Certified ISO/IEC 27035 Lead Incident Manager 시험 기출문제모음집 □ ➥ www.koreadumps.com □은▸ ISO-IEC-27035-Lead-Incident-Manager ◂무료 다운로드를 받을 수 있는 최고의 사이트입니다ISO-IEC-27035-Lead-Incident-Manager시험대비 공부자료
- ISO-IEC-27035-Lead-Incident-Manager적중율 높은 인증시험덤프 인증덤프는 PECB Certified ISO/IEC 27035 Lead Incident Manager 시험 기출문제모음집 □ 오픈 웹 사이트□ www.itdumpskr.com □검색✔ ISO-IEC-27035-Lead-Incident-Manager □✔□무료 다운로드ISO-IEC-27035-Lead-Incident-Manager인증덤프공부
- ISO-IEC-27035-Lead-Incident-Manager시험 □ ISO-IEC-27035-Lead-Incident-Manager적중율 높은 덤프 □ ISO-IEC-27035-Lead-Incident-Manager합격보장 가능 시험 □ ✔ www.passtip.net □✔□웹사이트를 열고{ ISO-IEC-27035-Lead-Incident-Manager }를 검색하여 무료 다운로드ISO-IEC-27035-Lead-Incident-Manager합격보장 가능 덤프공부
- ISO-IEC-27035-Lead-Incident-Manager최신 업데이트버전 공부문제 □ ISO-IEC-27035-Lead-Incident-Manager 최신버전 시험자료 □ ISO-IEC-27035-Lead-Incident-Manager유효한 공부문제 □ □ www.itdumpskr.com □에서☀ ISO-IEC-27035-Lead-Incident-Manager □☀□를 검색하고 무료로 다운로드하세요ISO-IEC-27035-Lead-Incident-Manager최고품질 덤프샘플문제 다운
- 시험준비에 가장 좋은 ISO-IEC-27035-Lead-Incident-Manager적중율 높은 인증시험덤프 최신버전 공부자료 □ 《 ISO-IEC-27035-Lead-Incident-Manager 》를 무료로 다운로드하려면▸ www.pass4test.net ◂웹사이트를 입력하세요ISO-IEC-27035-Lead-Incident-Manager최신 덤프데모
- ISO-IEC-27035-Lead-Incident-Manager덤프샘플문제 체험 □ ISO-IEC-27035-Lead-Incident-Manager덤프샘플문제 체험 □ ISO-IEC-27035-Lead-Incident-Manager인증덤프공부 □ 시험 자료를 무료로 다운로드하려면▸ www.itdumpskr.com ◂을 통해▸ ISO-IEC-27035-Lead-Incident-Manager ◂를 검색하십시오ISO-IEC-27035-Lead-Incident-Manager최신버전 시험자료
- 시험준비에 가장 좋은 ISO-IEC-27035-Lead-Incident-Manager적중율 높은 인증시험덤프 최신버전 덤프샘플문제 다운로드 □ 【 www.koreadumps.com 】을(를) 열고⇒ ISO-IEC-27035-Lead-Incident-Manager ⇐를 검색하여 시험 자료를 무료로 다운로드하십시오ISO-IEC-27035-Lead-Incident-Manager최신버전 시험자료
- www.wcs.edu.eu, www.stes.tyc.edu.tw, www.wcs.edu.eu, study.stcs.edu.np, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, easierandsofterway.com, Disposable vapes

그리고 PassTIP ISO-IEC-27035-Lead-Incident-Manager 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1Oo9VIeBLxSDEuPLnxkxQhS_yVFBceEAx