**User Question (3): new requirements for vulnerability assessments**

| **Model Name** | **LLM Generated Content** |
| --- | --- |
| GPT-3.5-Turbo | **What are the new requirements for vulnerability assessments in PCI DSS version 4.0?** |
|  | In PCI DSS version 4.0, there are several new requirements for vulnerability assessments. Here are the new requirements: |
|  | - Requirement 11.3.1.1: Manage all other applicable vulnerabilities (those not ranked as high-risk or critical). |
|  | - Requirement 11.3.1.2: Internal vulnerability scans are performed via authenticated scanning. |
|  | - Requirement A3.3.1: Failures of automated log review mechanisms and automated code review tools are detected, alerted, and reported in a timely manner. |
|  | These new requirements are applicable to all entities and service providers and are effective immediately for all v4.0 assessments. |
| GPT-4 | **What are the new requirements for vulnerability assessments in the PCI DSS?** |
|  | The new requirements for vulnerability assessments in the PCI DSS v4.0 as compared to v3.2.1 are: |
|  | 1. Requirement 10.4.2.1: A targeted risk analysis is performed to determine the frequency of log reviews for all other system components. |
|  | 2. Requirement 11.3.1.1: Manage all other applicable vulnerabilities (those not ranked as high-risk or critical). |
|  | 3. Requirement 11.3.1.2: Internal vulnerability scans are performed via authenticated scanning. |
|  | 4. Requirement A1.2.3: The multi-tenant service provider implements processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities. |
|  | 5. Requirement A3.3.1: Failures of the following are detected, alerted, and reported in a timely manner: Automated log review mechanisms and Automated code review tools. |
| Llama-2-13b | **What are the new requirements for vulnerability assessments in PCI DSS version 4.0?** |
|  | According to the provided document, there are several new requirements for vulnerability assessments in PCI DSS version 4.0. These include: |
|  | \* Performing a targeted risk analysis to determine the frequency of log reviews for all other system components (10.4.2.1) |
|  | \* Detecting, alerting, and addressing failures of critical security control systems promptly (10.7.2 and 10.7.3) |
|  | \* Documenting, assigning, and understanding roles and responsibilities for performing activities in Requirement 11 (11.1.2) |
|  | \* Managing all other applicable vulnerabilities (not ranked as high-risk or critical) (11.3.1.1) |
|  | \* Performing internal vulnerability scans via authenticated scanning (11.3.1.2) |
|  | \* Supporting multi-tenant services (11.4.7) |
|  | \* Implementing processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities (A1.2.3) |
|  | \* Detecting, alerting, and reporting failures of automated log review mechanisms and automated code review tools in a timely manner (A3.3.1) |
| Llama-2-7b | **What are some of the new requirements for vulnerability assessments introduced in PCI DSS version 4.0 compared to previous versions?** |
|  | According to the provided documents, one of the new requirements for vulnerability assessments introduced in PCI DSS version 4.0 is the addition of a bullet point in requirement 6.3.1 to clarify applicability to vulnerabilities for bespoke and custom and third-party software (see page 10). Additionally, there is a new requirement for maintaining an inventory of trusted keys and certificates (see page 1), which is a best practice until March 31, 2025. |
| Orca-2-13b | **¿Cuáles son las nuevas requisitos para las evaluaciones de vulnerabilidades en la versión 4.0 de PCI DSS?** |
|  | Las nuevas requisitos para las evaluaciones de vulnerabilidades en la versión 4.0 de PCI DSS incluyen resolver vulnerabilidades con una puntuación de 4.0 o más en el CVSS, realizar rescans cuando sea necesario, y tener un método de penetration testing definido, documentado e implementado que incluye enfoques aceptados por la industria y cobertura para el perímetro del SDE y los sistemas críticos. |
| Orca-2-7b | **What are some new requirements for vulnerability assessments introduced in PCI DSS version 4.0?** |
|  | Some new requirements for vulnerability assessments introduced in PCI DSS version 4.0 include: |
|  | - Performing a targeted risk analysis to determine the frequency of log reviews for all other system components (Requirement 10.4.2.1) |
|  | - Ensuring failures of critical security control systems are detected, alerted, and addressed promptly (Requirement 10.7.2), and responded to promptly (Requirement 10.7.3) |
|  | - Documenting, assigning, and understanding roles and responsibilities for performing activities in Requirement 11 (Requirement 11.1.2) |
|  | - Managing all applicable vulnerabilities not ranked as high-risk or critical (Requirement 11.3.1.1) |
|  | - Performing internal vulnerability scans via authenticated scanning (Requirement 11.3.1.2) |