It’s Time to Upgrade: Is Your Security Solution Ready for PCI DSS v4.0?

Posted on May 17, 2024

For organizations handling cardholder data, security is a constant battle, with cybercriminals devising new tactics and exploits to steal sensitive information left and right. That is why the Payment Card Industry Data Security Standard (PCI DSS) has been crucial as the gold standard for safeguarding payment-related data. And just as threats evolve, so too must the standards protecting financial information.

Recognizing this need, the PCI Security Standards Council introduced PCI DSS v4.0, effectively retiring PCI DSS v3.2.1 on 31 March 2024. Let’s explore what this new version brings to the table and how it can help organizations better protect cardholder data.

What Is PCI DSS?

PCI DSS refers to a set of security requirements designed to ensure organizations that handle credit card data maintain a secure environment.

Compliance with PCI DSS isn’t optional. It is enforced by major credit card brands like Visa, Mastercard, and American Express. So, any business that accepts, stores, or transmits credit card information needs to comply with PCI DSS.

By adhering to PCI DSS, businesses not only safeguard sensitive customer data but also avoid monetary penalties and reputational damages associated with noncompliance.

What Is New in PCI DSS v4.0?

PCI DSS v4.0 introduces several new requirements alongside an overall shift toward a more risk-

based and outcome-oriented approach. Here's a breakdown of the shift in focus of the updated version.

- **Outcomes over checklists:** PCI DSS v4.0 focuses on security outcomes rather than simply following a checklist of controls, allowing organizations to tailor their security posture to their unique needs.

- **Prioritization approach:** Recognizing that implementing all controls at once may not be feasible, the new version allows organizations to prioritize the most critical controls first. This strategy makes compliance more achievable, especially for smaller businesses.

Aside from these general changes, PCI DSS v4.0 also introduces new requirements. Below are a few of them.

- **Stronger authentication:** Multifactor authentication (MFA) has become mandatory for administrative access to the cardholder data environment (CDE) and all remote access means to an organization's network that can impact the CDE.

- **Enhanced password security:** The minimum password complexity requirements increased, making brute-forcing and similar attacks significantly more difficult. PCI DSS v4.0 requires passwords to be at least 12 characters long and contain alphanumeric characters.

- **Strict account management:** Shared, group, and generic accounts can only access the CDE when necessary (e.g., for emergency use when all other authentication methods have failed). Organizations must ensure individual accounts have unique and strong login credentials.

- **Accountability and traceability:** Each PCI DSS requirement now mandates clearly defined roles and responsibilities. That helps ensure everyone within an organization understands who is responsible for implementing and maintaining specific security requirements.

- **Targeted risk analysis:** In addition to recommending enterprise-wide risk assessment, PCI DSS v4.0 requires targeted risk analysis for each requirement. The risk analysis must identify all assets that need protection, the threats the requirement addresses, the likelihood and impact of a threat, and how frequently the requirement must be performed.

- **Web application security:** An automated solution is required to detect and prevent web-based attacks continually for public-facing web applications. This new requirement also mandates that all vulnerabilities are ranked and addressed.

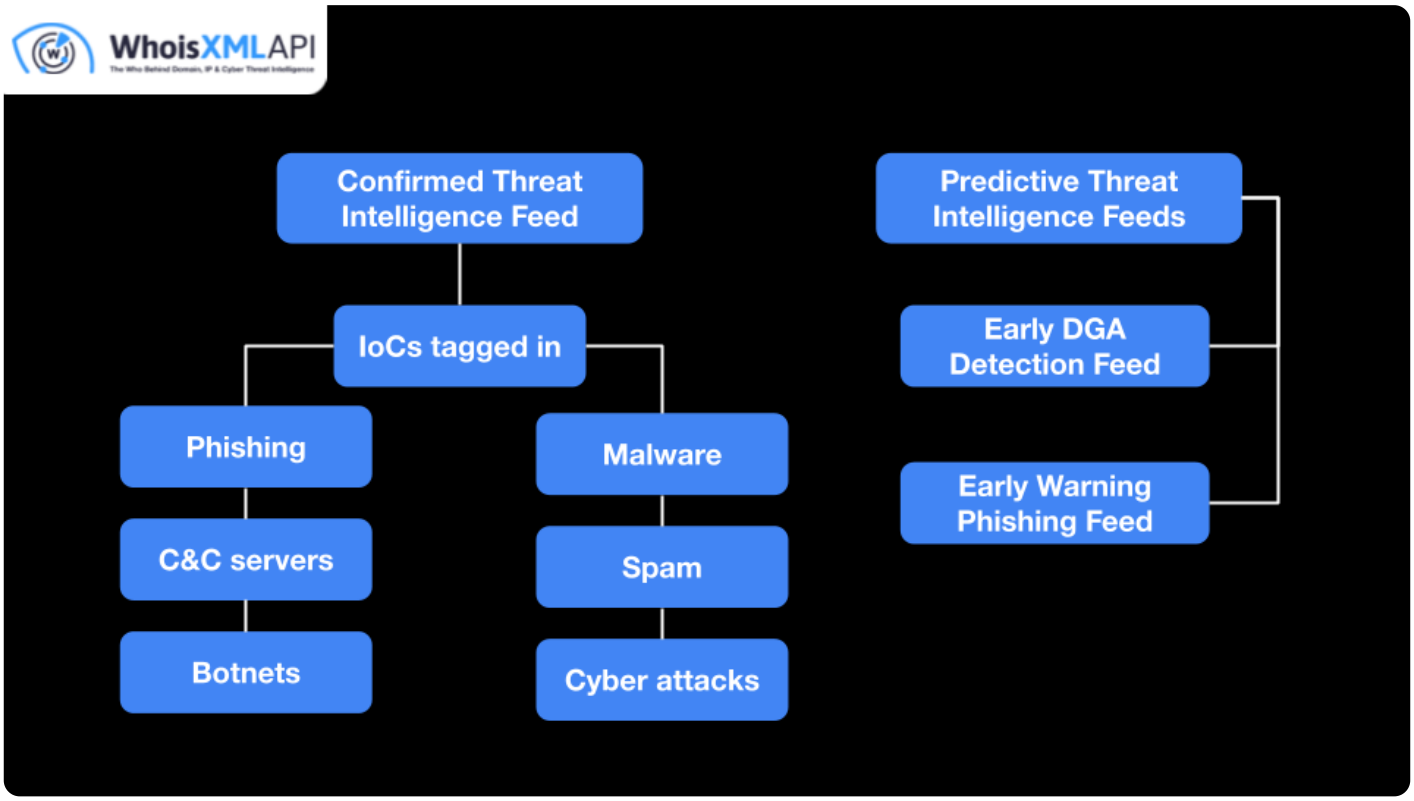
- **Cloud security:** The standard now explicitly addresses cloud environments, providing guidance on implementing security measures from selecting a cloud service provider to decommissioning cloud resources.

How Can WhoisXML API Intelligence Help with PCI DSS v4.0 Compliance?

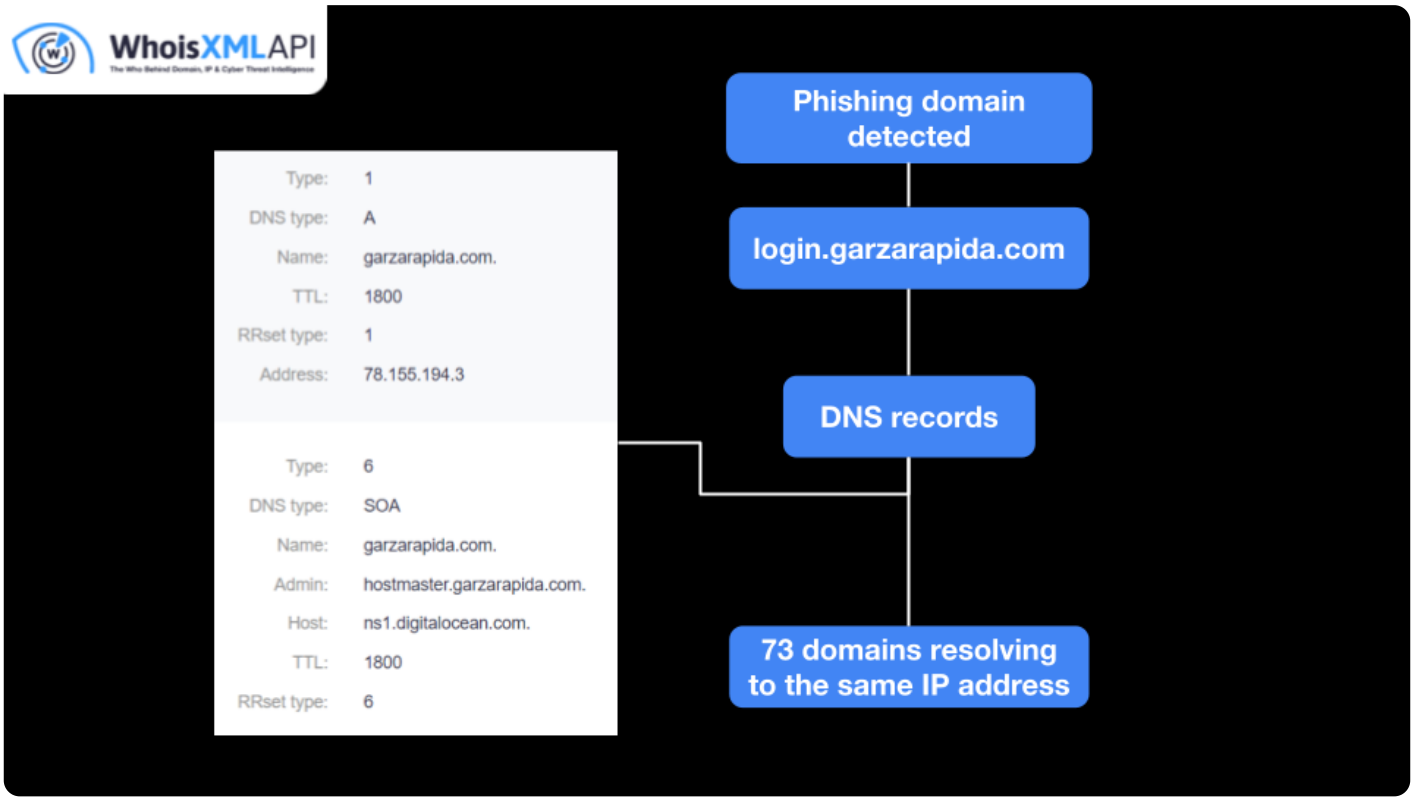
Organizations handling customer payment data need all the support they can get. With PCI DSS raising the bar for security, they are seeking tools and solutions to help with compliance. But are security solution providers ready to take on the PCI DSS v4.0 requirements?

Here's where WhoisXML API intelligence can help security solutions tackle vital aspects of PCI DSS v4.0.

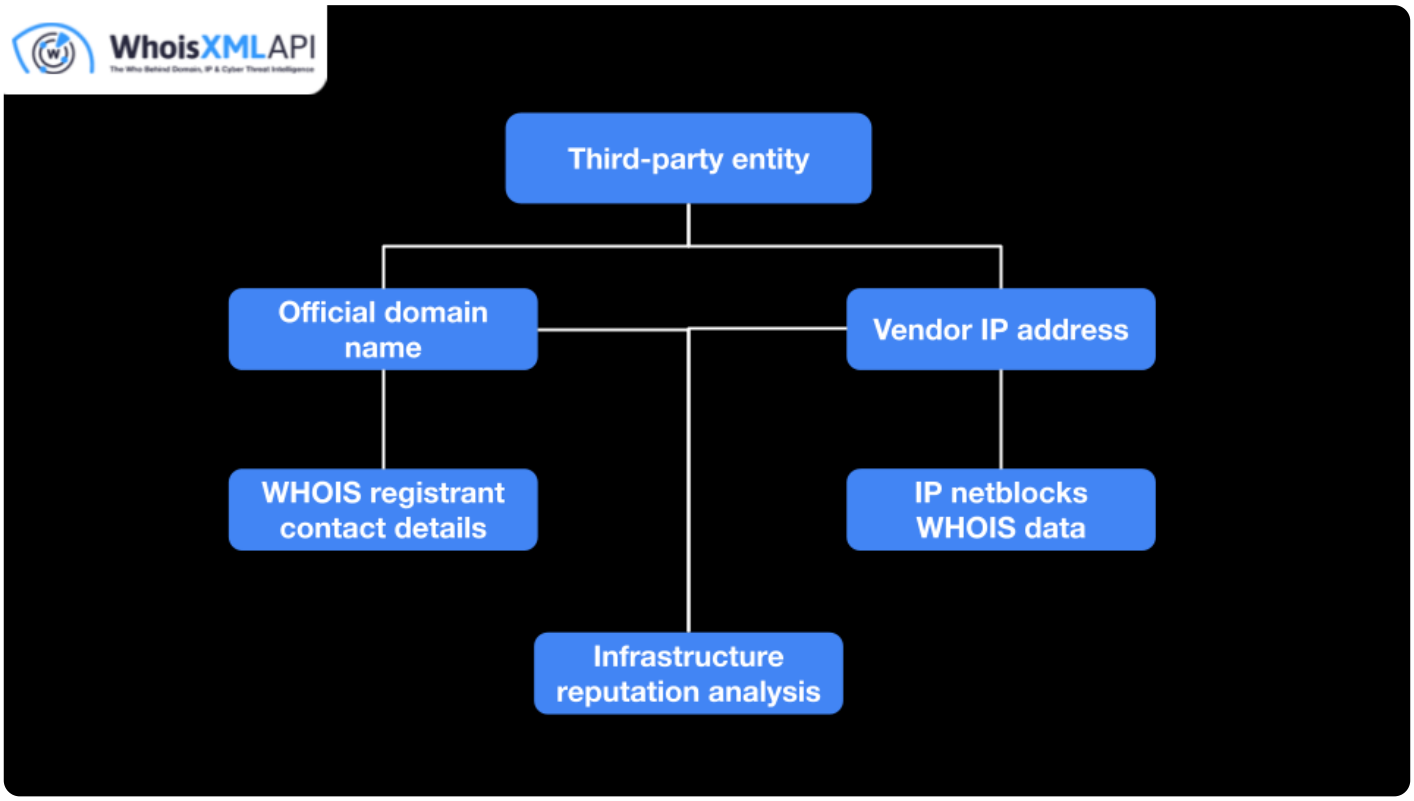
- **Threat detection and prevention:** Confirmed threat intelligence feeds can help intrusion detection systems/intrusion prevention systems (IDSs/IPSs) and other security controls identify and filter known malicious resources. These security solutions can also be fed with Early Warning Phishing Feeds and Early DGA Detection Feeds to monitor cybersquatting and algorithmically created newly registered domains (NRDs) likely to figure in phishing (and other) attacks.



- **Enhanced incident response:** During a security incident, tools powered by DNS intelligence can help learn more about the source of an attack and track its spread. That is crucial since Requirement 12.10 of PCI DSS v4.0 mandates that “Suspected and confirmed security incidents that could impact the CDE are responded to immediately.” Therefore, organizations must have a thorough incident response plan, which includes monitoring, responding to, and investigating alerts from security monitoring systems. The image below shows an example of how the DNS infrastructure of a detected phishing domain can be traced.



- **Improved vendor risk assessment:** Throughout the updated standard, requirements for handling vendor accounts are specified. Some of them dictate certain approaches for when significant changes (e.g., any change to critical third-party vendors and service providers) occur. As part of due diligence, third-party risk management solutions can leverage IP and WHOIS data to verify ownership and check the reputation of IP addresses and domains associated with potential vendors.



- **User account management:** IP intelligence can help identify suspicious login attempts originating from known malicious IP addresses. This information can be used to flag such attempts for further investigation or even trigger additional verification steps for high-risk logins. Such capability helps organizations comply with the strict account management requirements of the standard.

Conclusion

The continued proliferation of Magecart, online card skimming attacks, and other threats shows that financial information is still highly targeted by threat actors. In response to existing and emerging threats, the PCI Security Standards Council updated PCI DSS, and we may see regular updates in the future.

Security solutions must also step up and utilize deep cyber intelligence that can help improve their

processes, assist them in complying with standards, and, most importantly, prevent threats.

Learn how WhoisXML API intelligence can support PCI DSS 4.0 compliance. Contact us now .