The Future is Upon Us: Navigating and Complying with the New V4.0.1 Controls

PCI DSS v4.0 introduces a range of new controls and requirements. This session will tackle the challenges organizations face in meeting the new PCI DSS v4.0 controls, offering guidance on navigating the complexities and addressing common areas of confusion. Attendees will gain insights into how to interpret and implement the changes, ensuring they align their security practices with the latest standards while maintaining operational efficiency.

PCI Security Standards Council®

Marc Jackson

CISA, CISM, QSA

Compliance Manager

MEGAPLANIT

PCI Security Standards Council

Common Challenges

What we at MegaplanIT are seeing as it relates to:

- Technical Controls
- Access Control
- Software Development
- Process Improvement

Spoiler Alert:

What we will not be discussing…….

~~6.4.3~~
~~11.6~~

PCI Security Standards Council

Multi-Factor Authentication

PCI Security Standards Council

MFA

8.4.2 MFA is implemented for all non-console access into the CDE.

- Knowing your environment and where is MFA needed and how it has changed from 3.2.1
- Should you reduce CDE access to minimize MFA requirements
- FAQ #1595 and #1596
- Real world scenarios of where MFA is needed/not needed

PCI Security Standards Council

Application and System Accounts

PCI Security Standards Council

Application and System Accounts

7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows:

- What are application and system accounts?
- Do you have visibility into the list of active application and system accounts?????
- Do you have a TRA for the review frequency
- Who is reviewing and confirming that access is appropriate

PCI Security Standards Council

Software Development

PCI Security Standards Council

Software Development

6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.

- What elements are we trying to identify and why
- Is a correct inventory being kept and by whom
- How is the inventory being used to facilitate vulnerability management

Risk

Risk

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

TRAs

- Purpose of TRA
- What format must be used to document a TRA
- Who is reviewing them and how often

PCI Security Standards Council

Scope

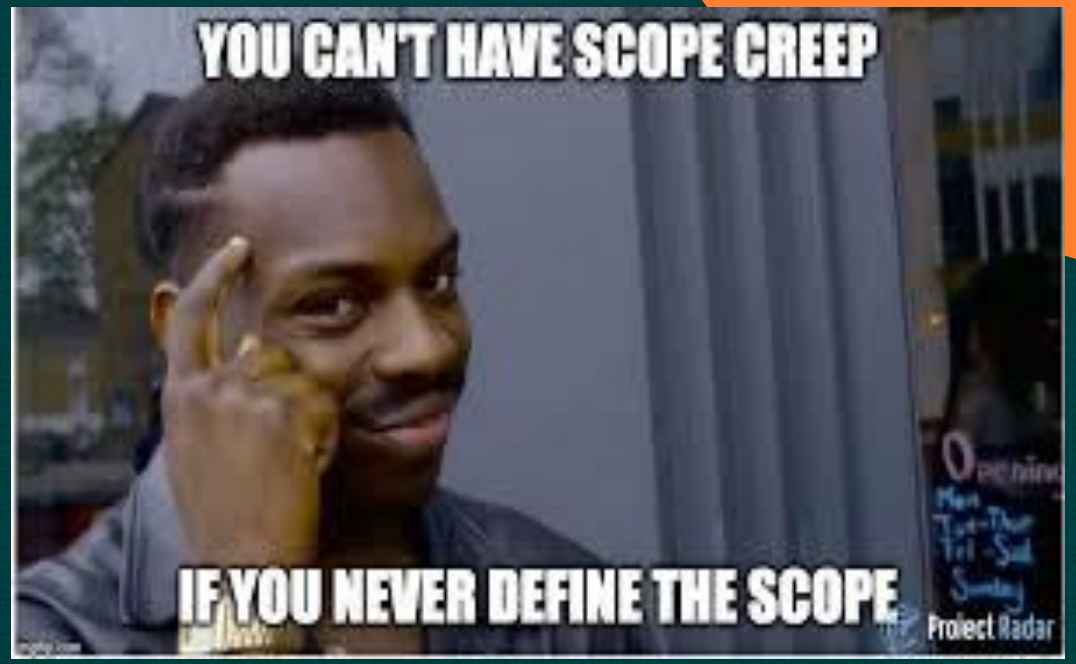
PCI Security Standards Council

Scope

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months (6 months for SP) and upon significant change to the in-scope environment.

Things to consider/think about:

- Are the right people reviewing scope for accuracy? Did everyone get invited to the party?
- What needs to be included in a scoping exercise
- What is the best way for your company to document scope



Key Takeaways

Technical Controls

MFA

- Where does it apply

Access Control

System/Application Accounts

- Interactive accounts and review

Software Development

SDLC Vulnerability Considerations

- Software component inventory

Risk & Scope

TRAs

- Which TRAs are in-scope
- What is needed in a TRA
- Review process

Scope Documentation

- Key participants
- What to include
- What documentation meets the intent of the control

MEGAPLANIT

Thank You!

Please stop by the MegaplanIT booth (44 & 45)
if you have any questions or concerns.

PCI Security Standards Council