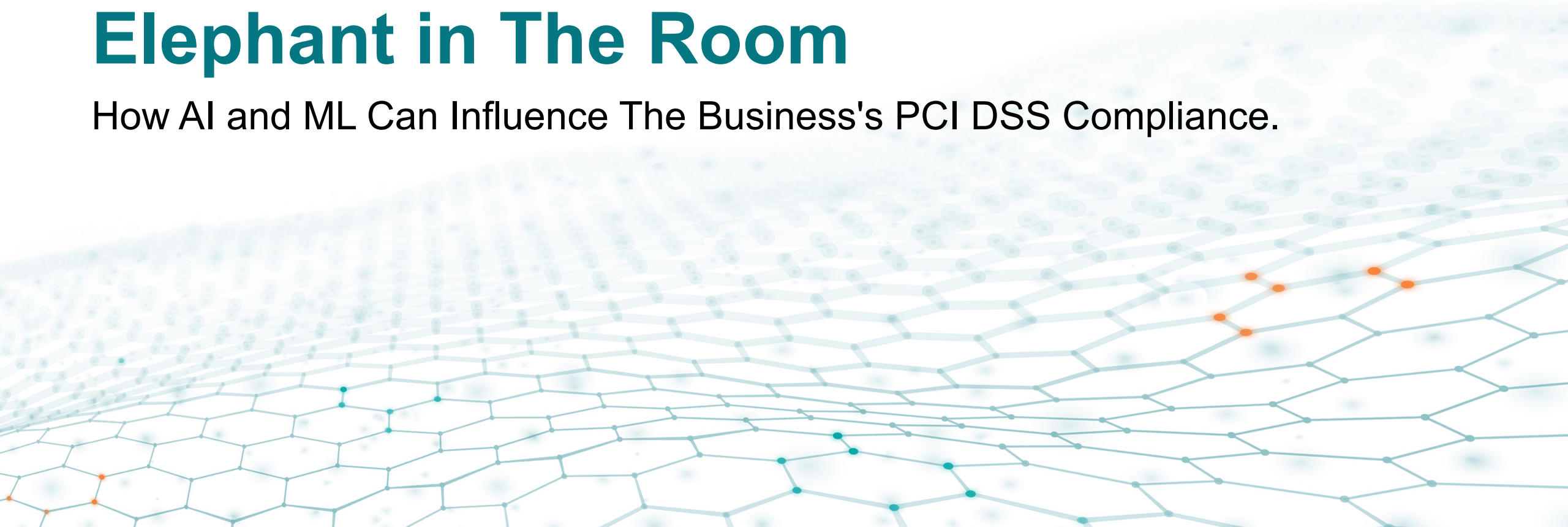
PCI Security Standards Council

Let’s Talk About That AI and ML Elephant in The Room

How AI and ML Can Influence The Business's PCI DSS Compliance.



Christopher Mawby

Oracle North America
Principal Security Architect

ORACLE

PCI Security Standards Council

Let’s Start With a Common Understanding

AI

- Artificial Intelligence frequently applied to the project of developing systems endowed with the intellectual processes which mimic humans, such as the ability to reason, discover meaning, generalize, or learn from experience.

ML

- Machine learning, in artificial intelligence discipline concerned with the implementation of computer software that can learn autonomously. This is the Learn from Experience in the AI above.

Where can AI and ML enhance our PCI DSS Compliance

1. Build and Maintain a Secure Network and Systems
2. Protect Account Data
3. Maintain a Vulnerability Management Program
4. Regularly Monitor and Test Networks

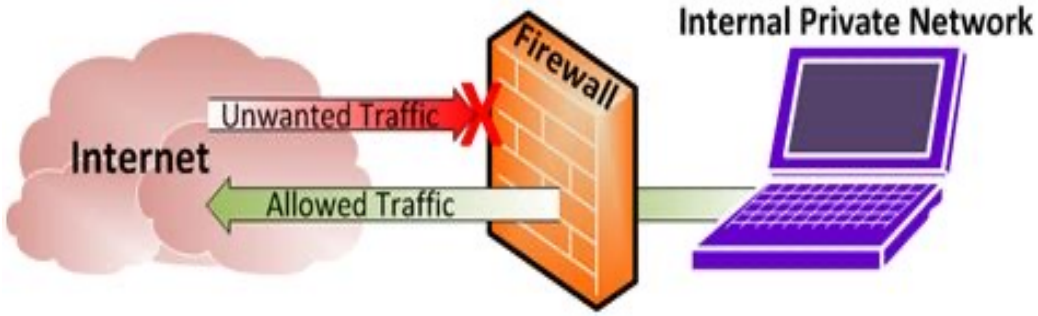
PCI Security Standards Council

Can AI and ML Build and Maintain Secure Networks and Systems?

Enhance build automation.

Collate build metrics.

Build error reduction.



Build and Maintain a Secure Network and Systems

As your posture evolves, gaps tend to emerge between the network & systems you THINK you have, vs the network & systems you ACTUALLY have. Deltas/exceptions/ad hoc changes are inevitable, and mature network maintenance often starts to hit expensive blocks because of these drifts unless they are managed proactively.

PCI Security Standards Council

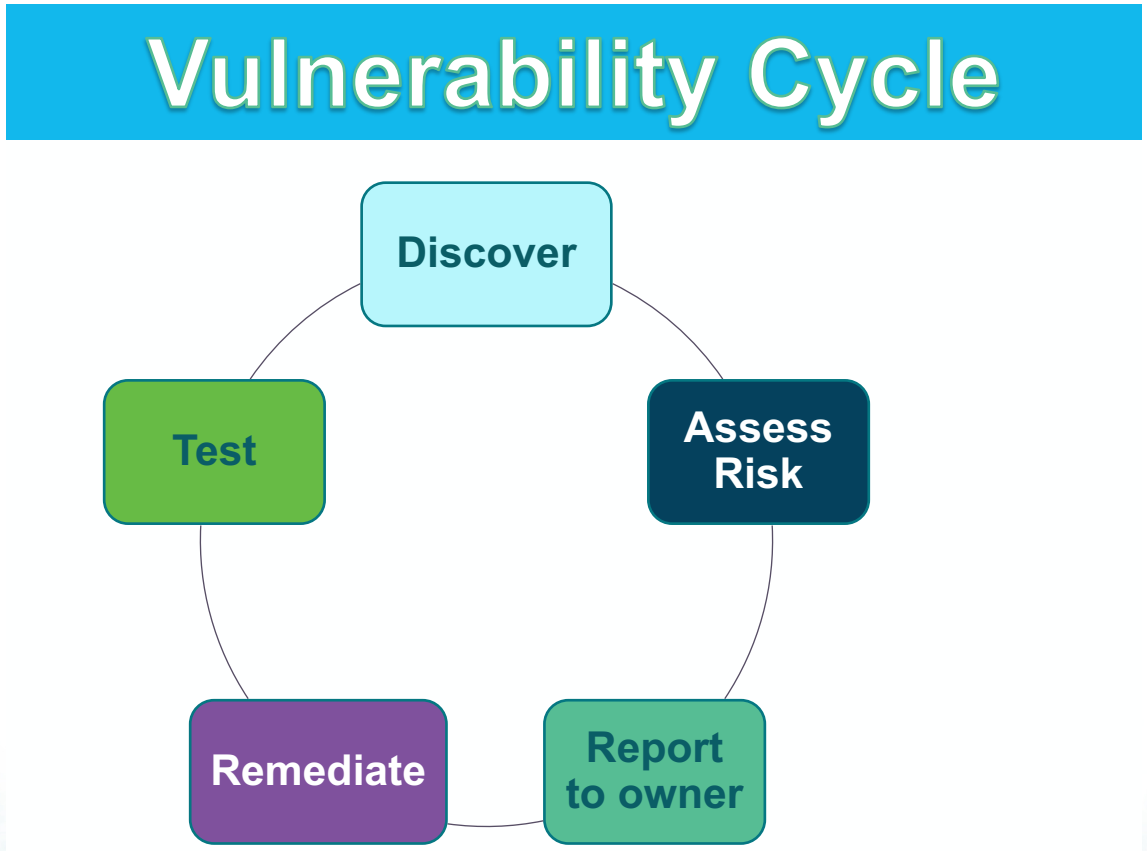
How Can AI and ML Protect Account Data?

1. Secure Development programs. Source Code Normalization.
2. Test and enhance development programs. Test code vulnerabilities. Runtime code repair.
3. Spot insecure patterns in coding and resolve to secure patterns.
4. Cryptographic controls

Not all encryption is equal. Often, we consider "encrypted" data to be a single binary state (not encrypted vs encrypted), but almost always there are necessary layers/variations possible to help improve not just security, but performance as well. Using the right type of encryption can solve multiple problems while lowering long term costs.

Can AI and ML Maintain a Vulnerability Management Program?

Vulnerabilities can get misleading and expensive. There are many high CVSS vulnerabilities that may never actually be exploitable on your system due to your specific configuration. Constantly chasing vulnerabilities just on score (or even FIFO) can become unnecessarily expensive. Prioritization can be necessary to best utilize your existing resources.



PCI Security Standards Council

AI and ML Will Regularly Monitor and Test Networks

Monitoring can quickly become exponentially expensive, not just with resources but privacy and risk. Security activities like threat sharing and segmentation can help to alleviate these costs while supporting multiple security objectives.

PCI Security Standards Council

How to Succeed in This Arms Race

CHALLENGES

- Leadership
- Cybersecurity Skills Gap
- Complacency
- Not Understanding AI & ML Risks
- Social Engineering
- Phishing
- Deep Fake Content
- Vulnerability Discovery

PCI Security Standards Council

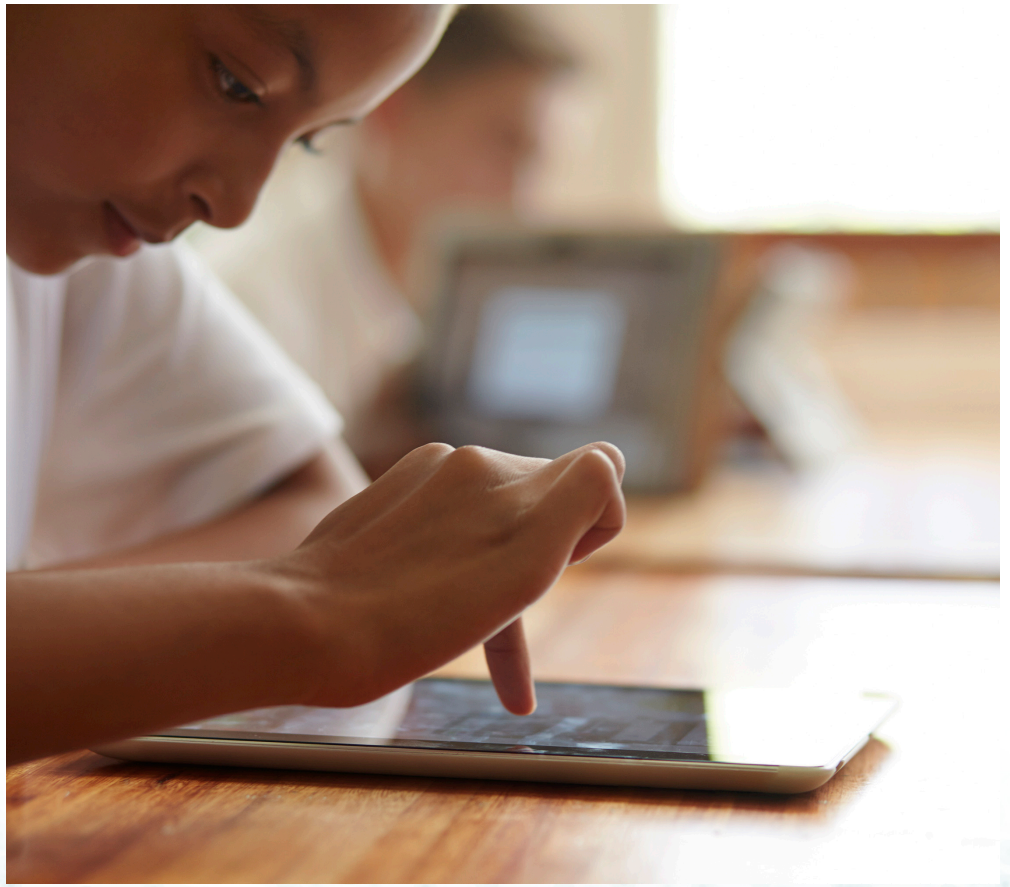
What Are the Limitations of AI Enhanced PCI DSS Controls?

Many Enhanced PCI Controls face AI limitations

None of these limitations is permanent

Today Educate yourselves and your management

Tomorrow Build responsible AI



PCI Security Standards Council