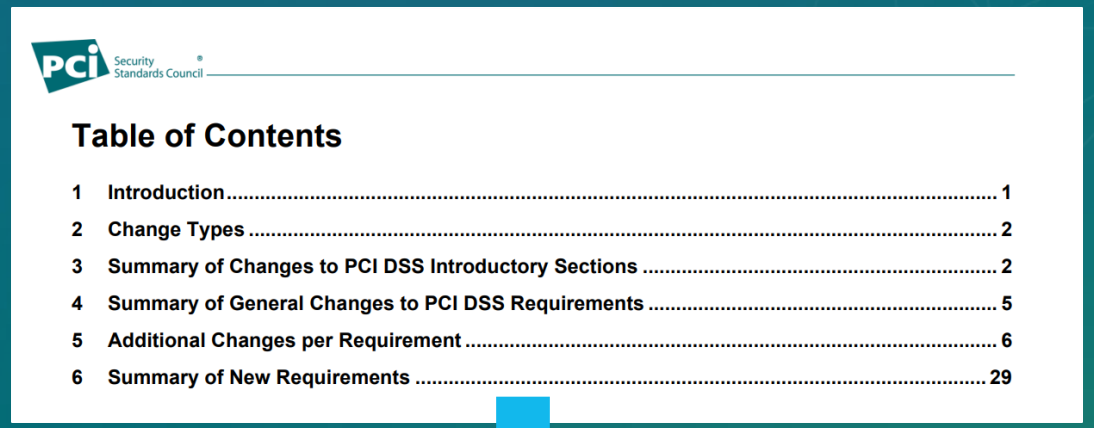
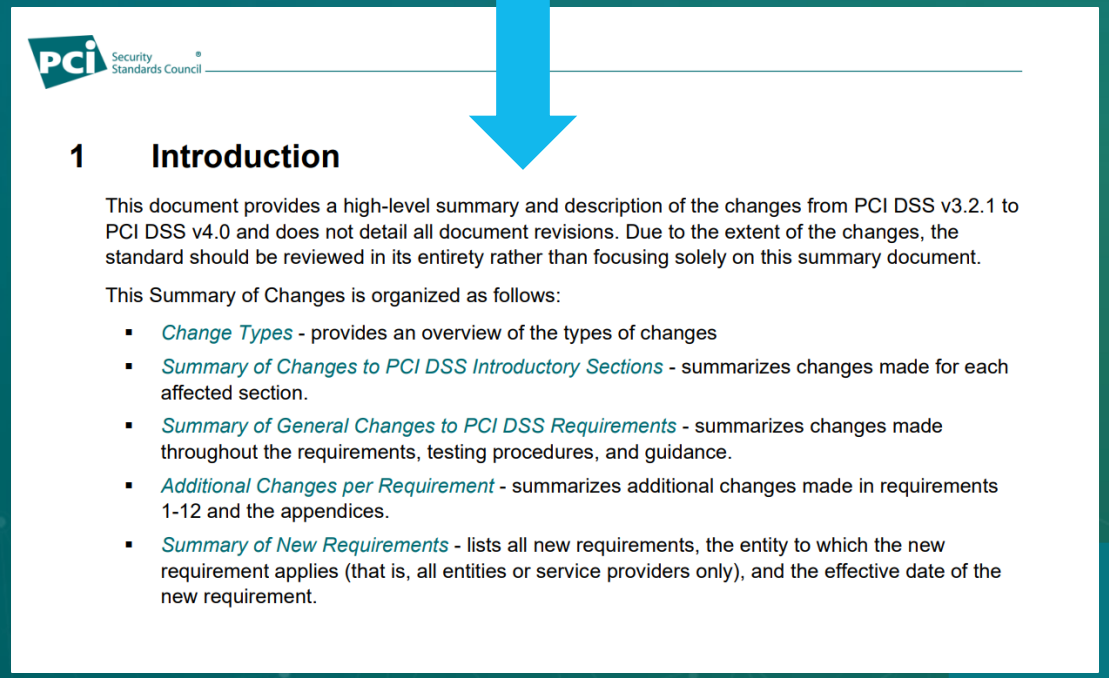
Requirements: What's New and Exciting?

Joel Weisz, Manager, Emerging Standards,
PCI Security Standards Council
Kandyce Young, Standards Manager, Data Security Standards,
PCI Security Standards Council

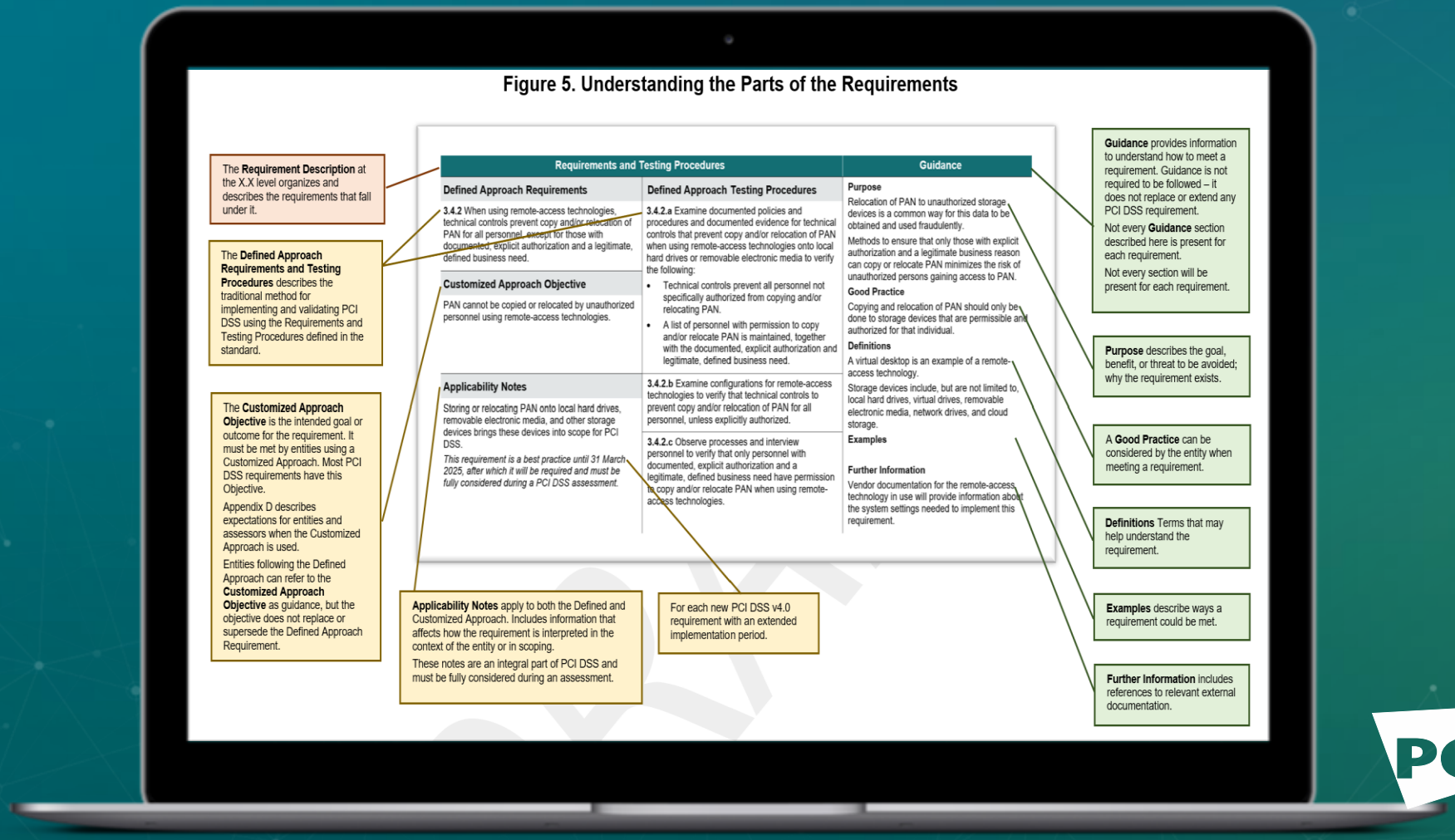
PCI Security Standards Council

Summary of Changes





New Layout for Requirements



PCI Security Standards Council®

Changes Across Requirements

Targeted Risk Analyses

- ✓ Frequency to perform activities
- ✓ Customized Approach

Roles and Responsibilities

- ✓ New in Requirements 2-11

PCI Security Standards Council®

PCI Security Standards Council®

Requirement

1

- **Networking Changes**
- **Configuration Files**
- **Network Security Controls**

PCI Security Standards Council®

TRUSTED NETWORK

Network you control or manage
& PCI DSS controls applied

VS

UNTRUSTED NETWORK

Network you can't control or manage
& PCI DSS controls not applied

PCI Security Standards Council®

Requirement

2

- **System Component Functions**

PCI Security Standards Council®

Configuration Standards

Vendor-Supplied Defaults

PCI Security Standards Council®

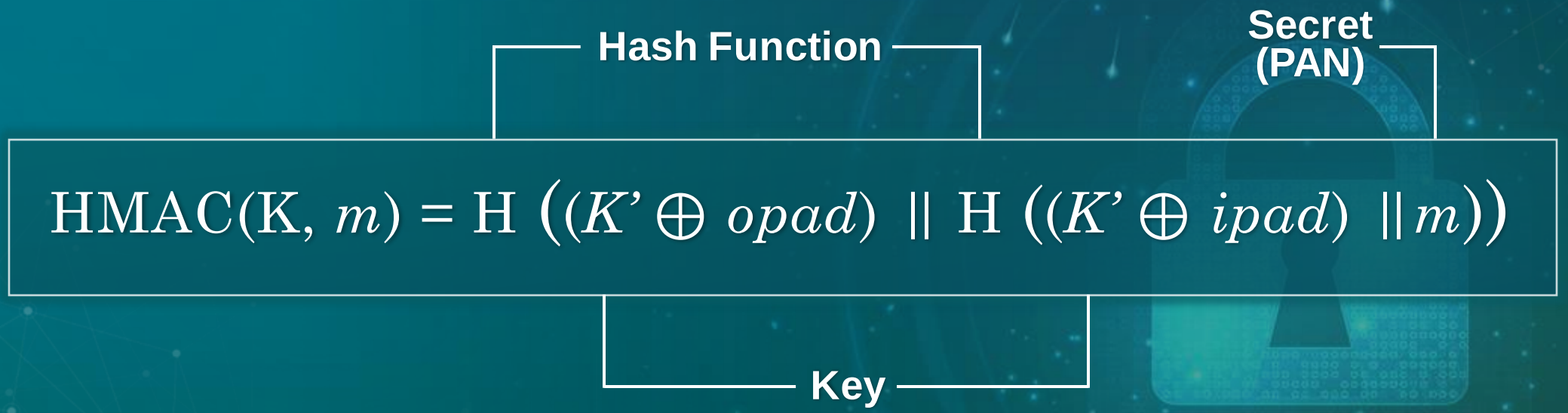
Requirement

3

- **Sensitive Authentication Data storage**
- **Copy and Paste of PAN**
- **Disk or Partition Level Encryption**
- **Cryptographic Key Use in Test and Production Networks**
- **Keyed Cryptographic Hashes**

PCI Security Standards Council®

Keyed Cryptographic Hashes



PCI Security Standards Council®

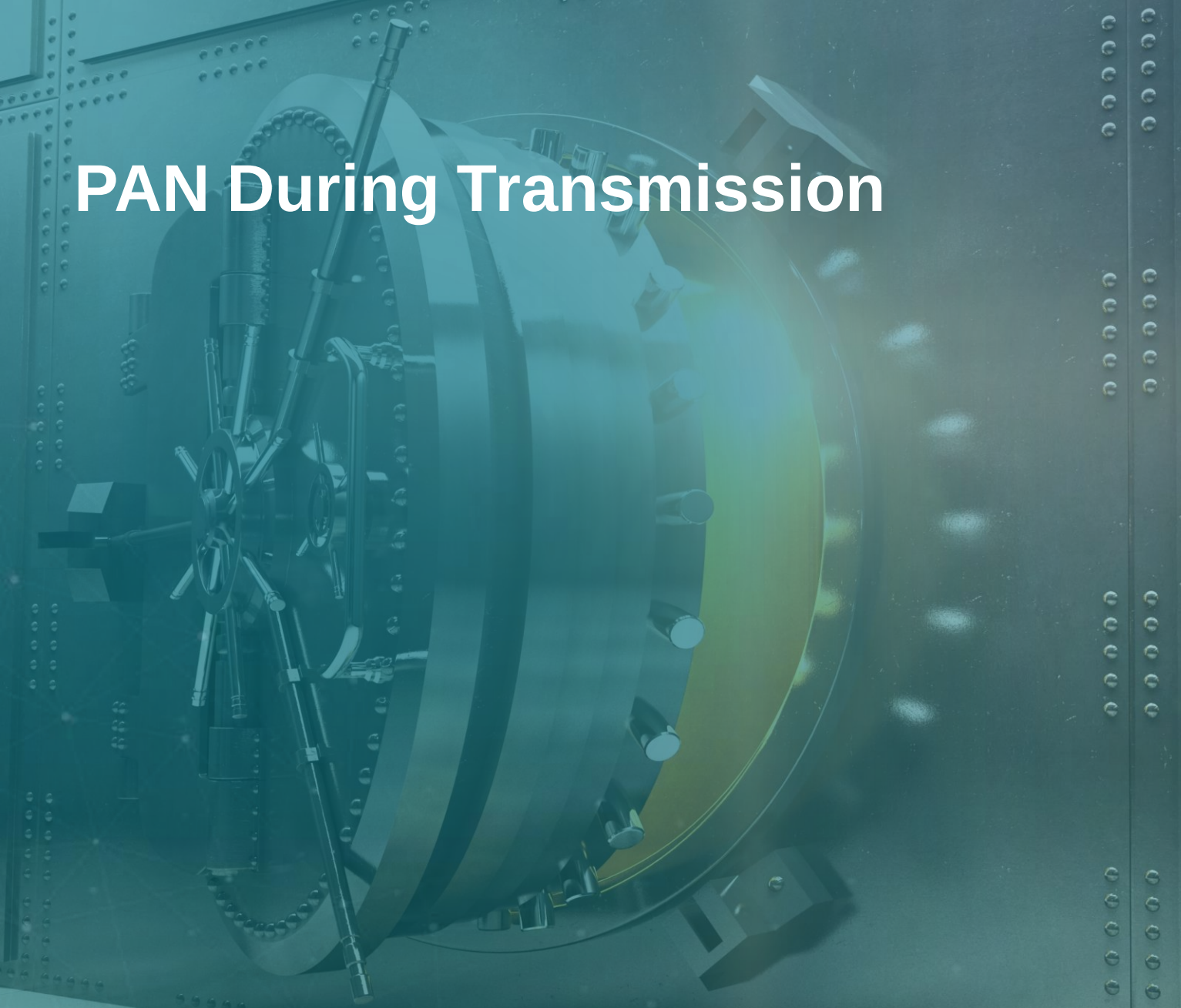
Requirement

4

- **PAN means PAN**

PCI Security Standards Council®

PAN During Transmission



Certificate Verification

Certificate and Trusted Key Inventory

PCI Security Standards Council®

Requirement

5

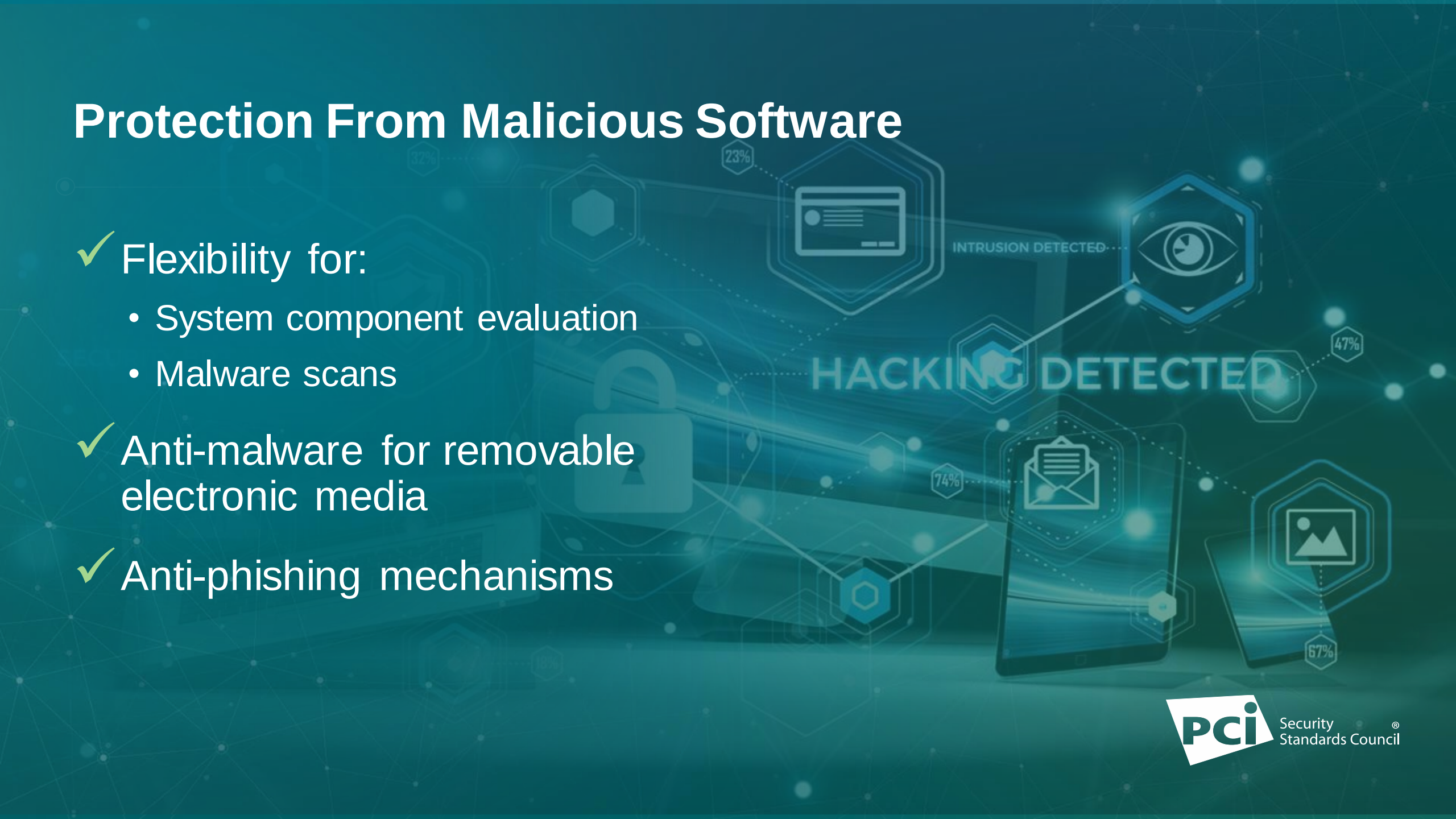
Malware Solutions

- **Behavioral Analysis**
- **Signature-Based scans**

PCI Security Standards Council®

Protection From Malicious Software

- ✓ Flexibility for:
  - System component evaluation
  - Malware scans
- ✓ Anti-malware for removable electronic media
- ✓ Anti-phishing mechanisms



PCI Security Standards Council®

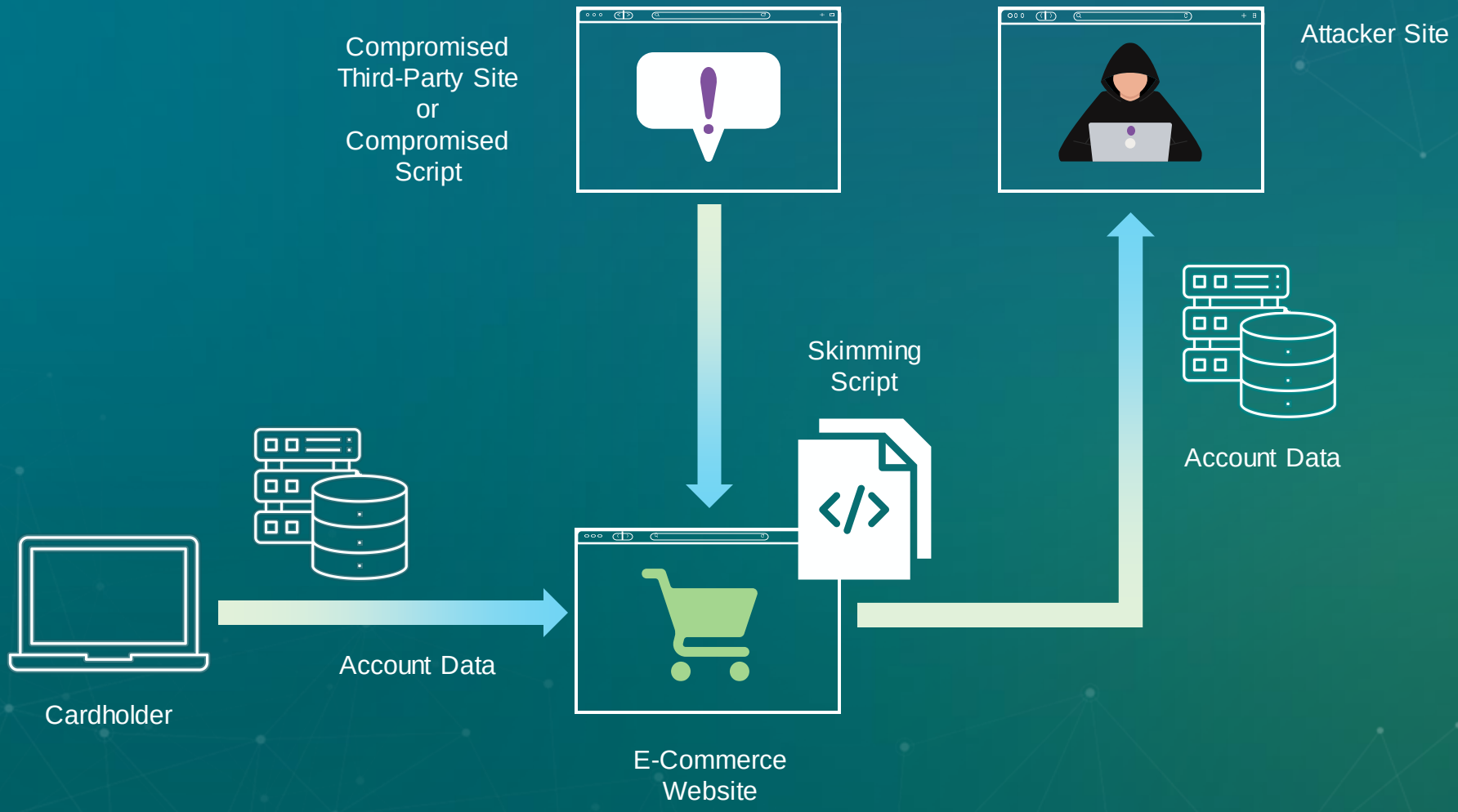
Requirement

6

- **Inventory of Bespoke and Custom Software**
- **Automated Detection and Alerting of Web-based Attacks**
- **E-commerce Skimming**

PCI Security Standards Council®

Skimming


Compromised
Third-Party Site
or
Compromised
Script
Attacker Site
Skimming
Script
Account Data
Account Data
Cardholder
E-Commerce
Website

Requirement

7

- **Access Control Model**
- **Queryable Repositories**
- **Access to All System Components**

PCI Security Standards Council®

Application and System Accounts

Accounts that execute processes or perform tasks on a computer system or in an application. These accounts usually have elevated privileges that are required to perform specialized tasks or functions and are not typically accounts used by an individual.

Also referred to as “service accounts.”

PCI Security Standards Council®

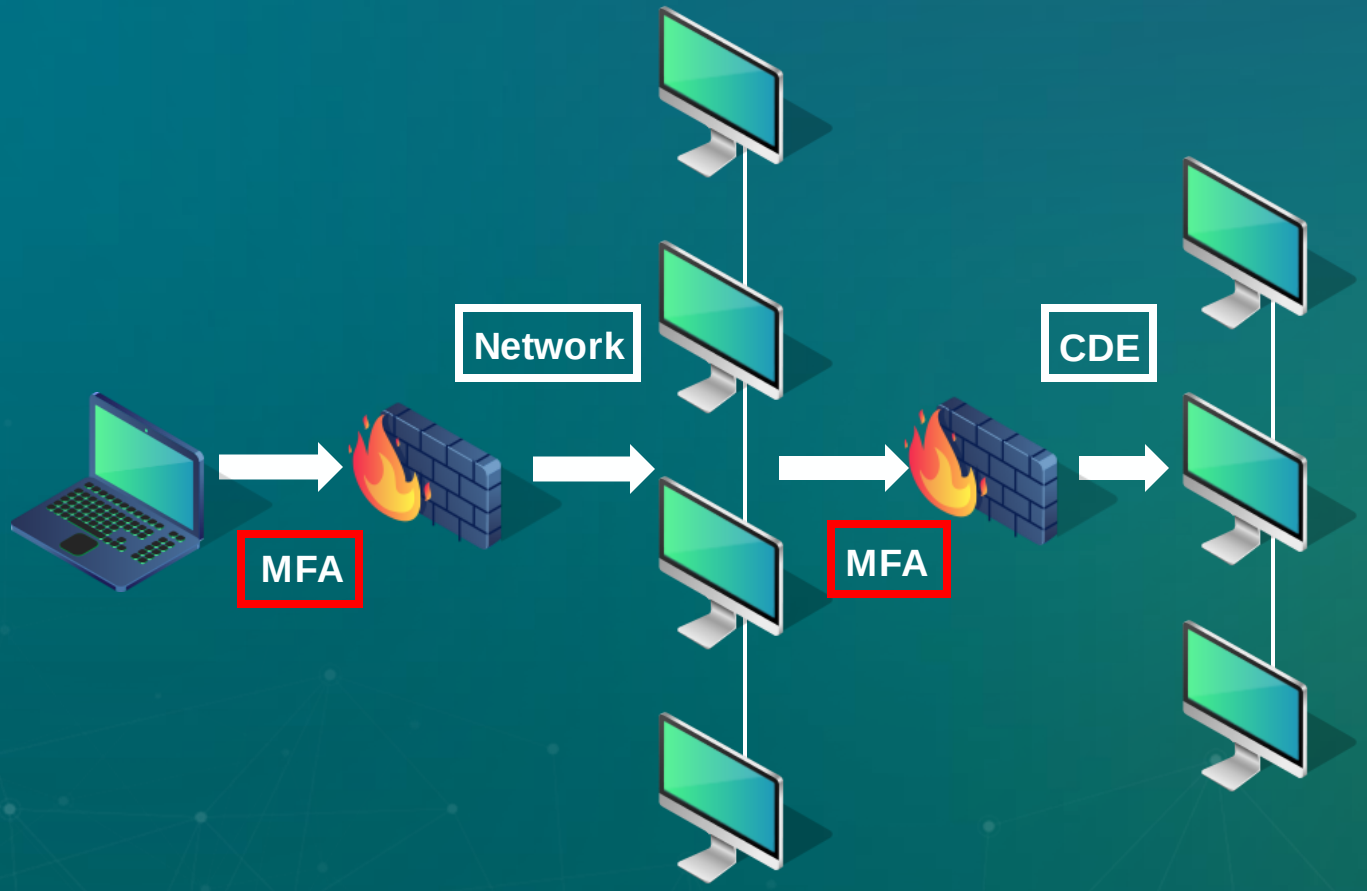
Requirement

8

- **Group, Shared, or Generic Accounts**
- **Passwords and Passphrases**
- **Dynamic Analysis**
- **Multi-factor Authentication**

PCI Security Standards Council

Regarding MFA



PCI Security Standards Council®

Dynamic Analysis

In the case of single factor authentication using a password:

- Change password at least once every 90 days

OR

- Access is determined in real-time through a dynamic analysis of the security posture of accounts

PCI Security Standards Council®

Requirement

9

- **Cardholder Data Environment (CDE)**
- **Sensitive Areas**
- **Facilities**

PCI Security Standards Council®

Requirement

10

- **Targeted Risk Analysis**
- **Critical Security Control Systems**
- **Automated Log Reviews**

PCI Security Standards Council®

Automated Log Reviews

PCI Security Standards Council®

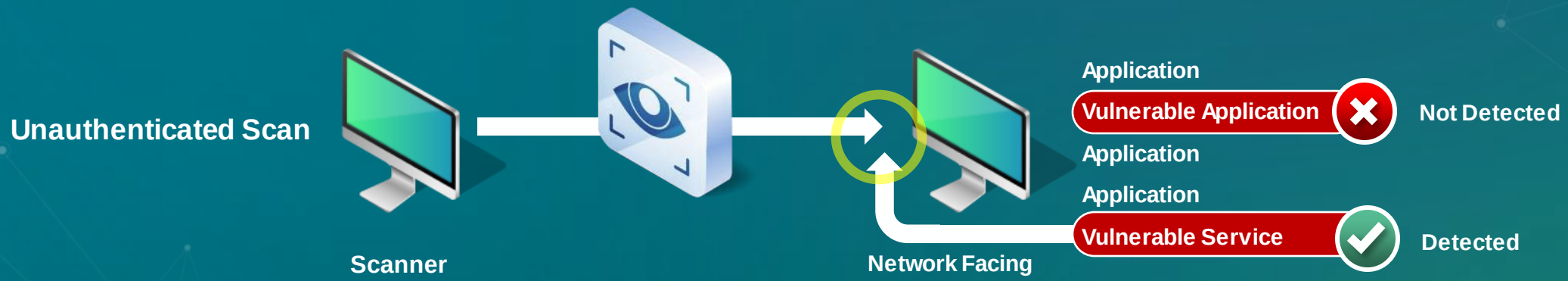
Requirement

11

- Non-high Criticality or High- Risk Findings
- Service Provider Support for Penetration Testing
- Intrusion Detection/Prevention
- E-Commerce Skimming Detection
- Credentialed Internal Vulnerability Scanning

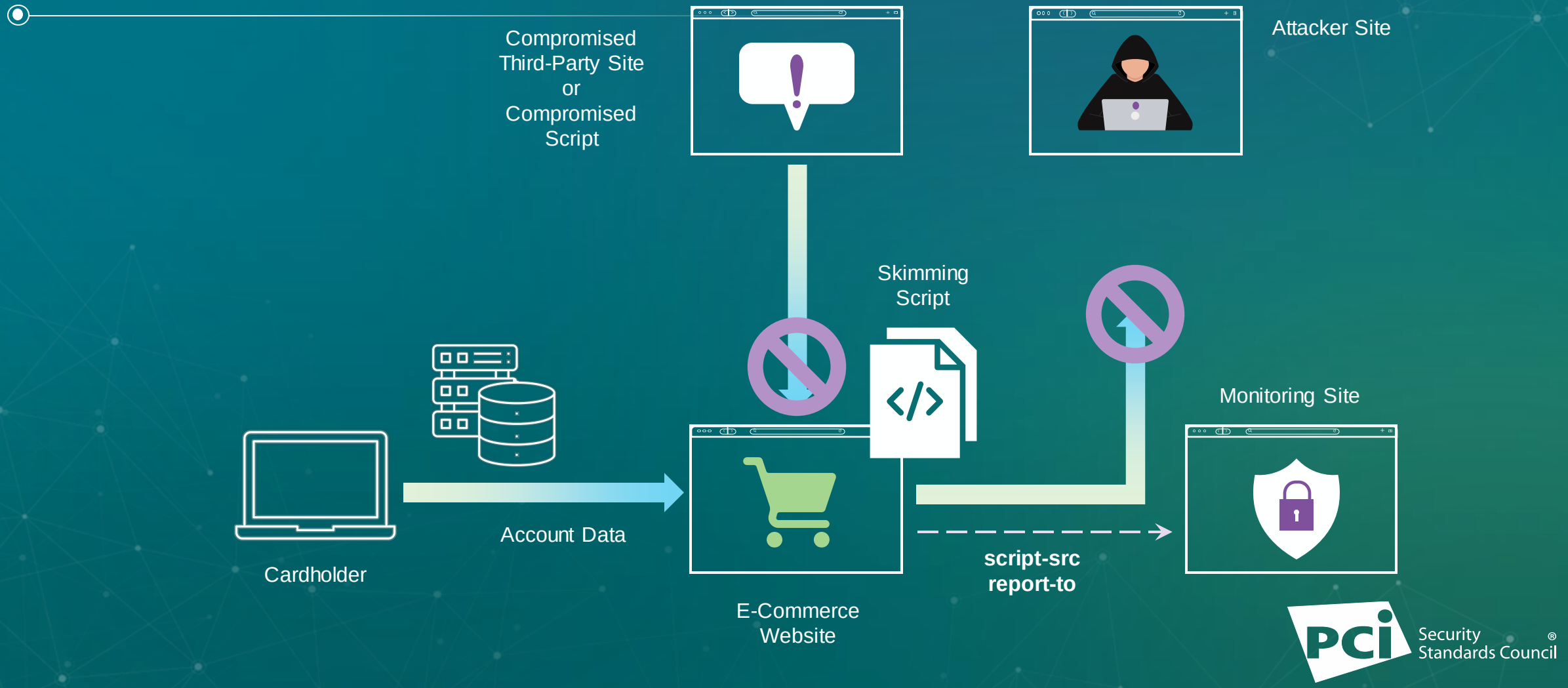
PCI Security Standards Council®

Difference Between Authenticated and Unauthenticated Scanning



PCI Security Standards Council ®

E-Commerce Skimming Detection



PCI Security Standards Council®

Requirement

12

- **Personnel Training**
- **Targeted Risk Analyses**
- **Service Provider Customer Support**
- **Cryptographic Cipher Suites and Protocols**

PCI Security Standards Council®

Scope Confirmation

- Data Flows
- System Components
- Segmentation Controls
- Locations
- Third-Party Connections

Phishing and Social Engineering

PCI Security Standards Council®

Appendix A

Multi-Tenant Service Providers

SSL/Early TLS for Card-Present POS POI

Designated Entity Supplemental Validation (DESV)

PCI Security Standards Council®

Flexibility For Implementing Security Controls and Validating Requirements

Marc Bayerkohler, Standards Trainer,
PCI Security Standards Council

Tom White, Training Content Manager,
PCI Security Standards Council

PCI Security Standards Council®