PCI Security Standards Council

The Future of Cyber Security from Hackers Perspective

Building a Defensible Architecture using PCI DSS

Pak Ho CHAN, Regional Head of OT/IT Cyber Defence, APAC
Queenie CHEN, Regional PCI Practice Manager, APAC

Building a Defensible Architecture using PCI DSS

- Lessons learned from the real-world hacking case studies
- PCI DSS as a practical approach to building defensible architecture
- Utilise deception technology to provide early warning of potential cyber-attacks and unauthorised activity.

PCI Security Standards Council

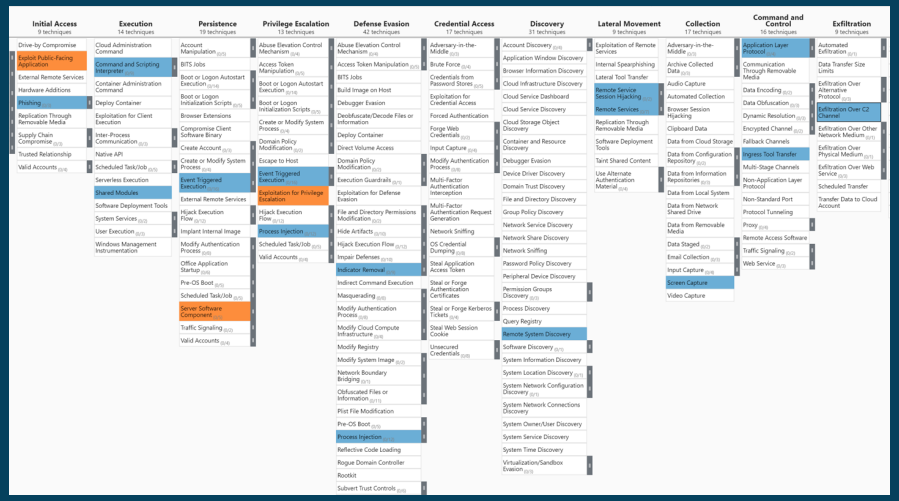
PCI Security Standards Council

Lessons Learned from the Real-world Hacking Case Studies

Case Studies

CL0P Ransomware Gang exploits CVE-2023-34362 MOVEit Vulnerability

CL0P Ransomware Gang exploited a SQL injection zero-day vulnerability CVE-2023-34362 to implant a web shell on MOVEit Transfer web applications to gain the initial access to the target environment and the latest patch was released on June 9. 2023



Threat Actors exploits Citrix CVE-2023-3519 to Implant Webshells

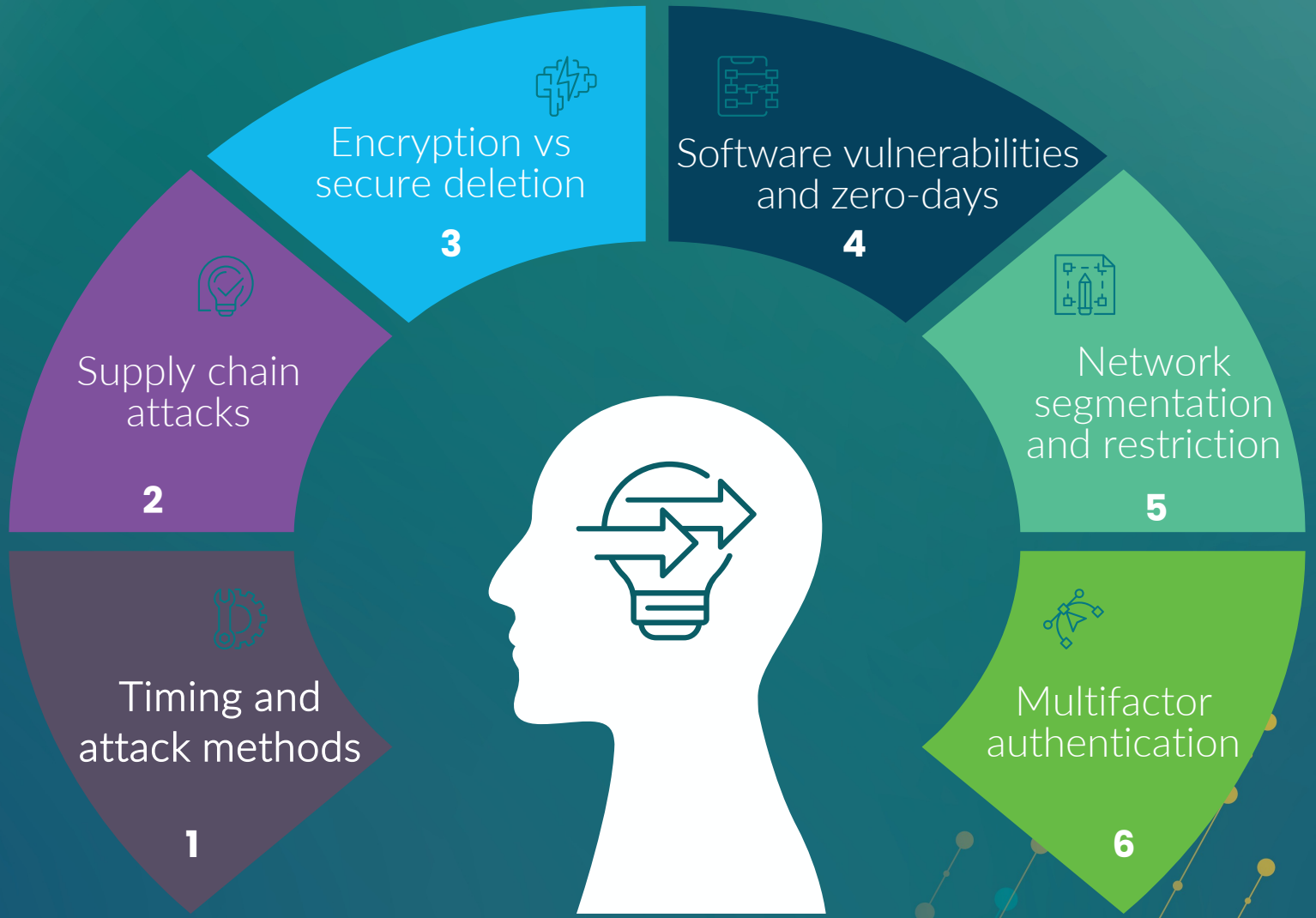
Threat Actor exploited a zero-day vulnerability CVE-2023-3519 to install a webshell on NetScaler appliance and a patch was realeased for this vulnerability on July 18, 2023.

Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/

https://attack.mitre.org/matrices/enterprise/

PCI Security Standards Council

Key Lessons Learned



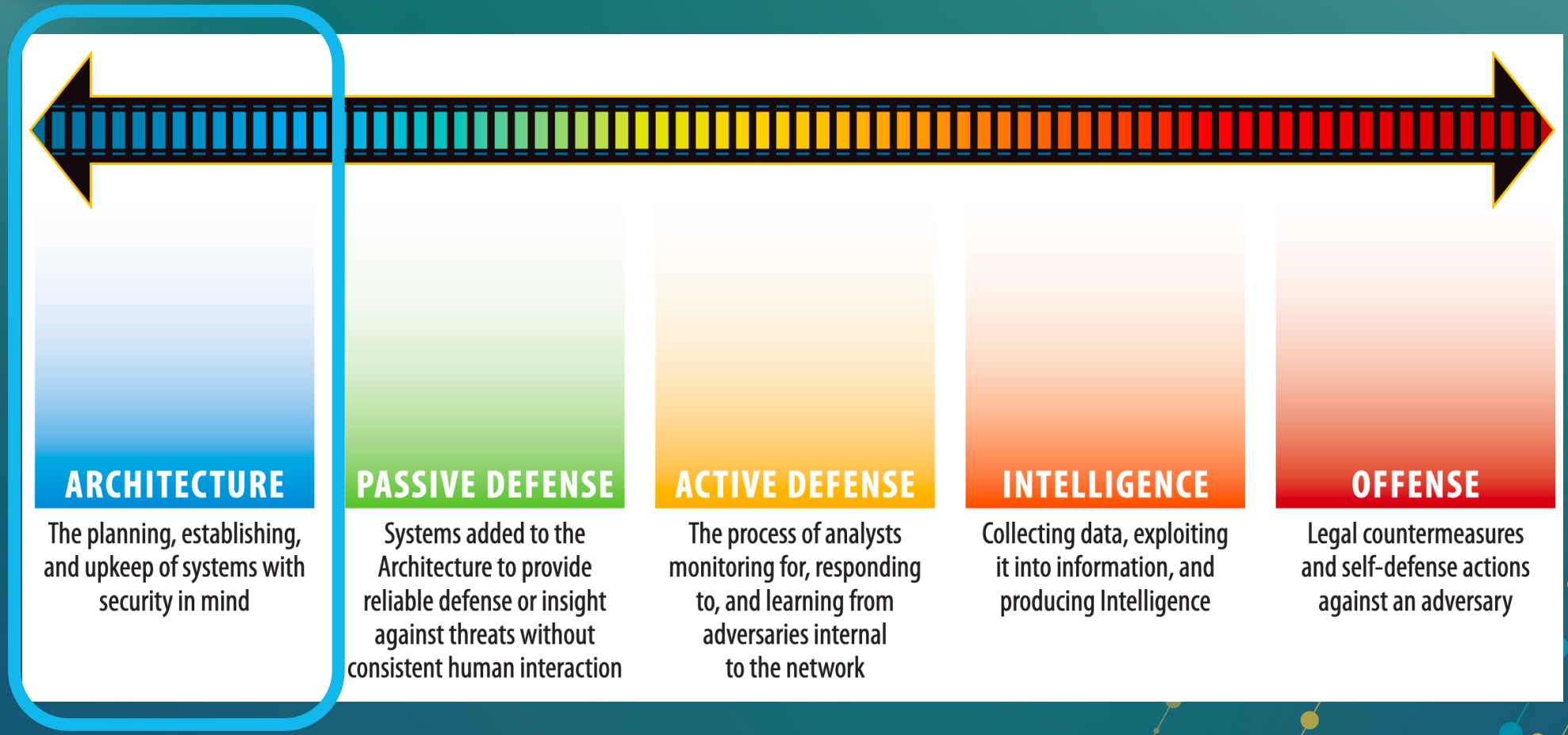
PCI Security Standards Council

PCI Security Standards Council

PCI DSS as a Practical Approach to Building Defensible Architecture

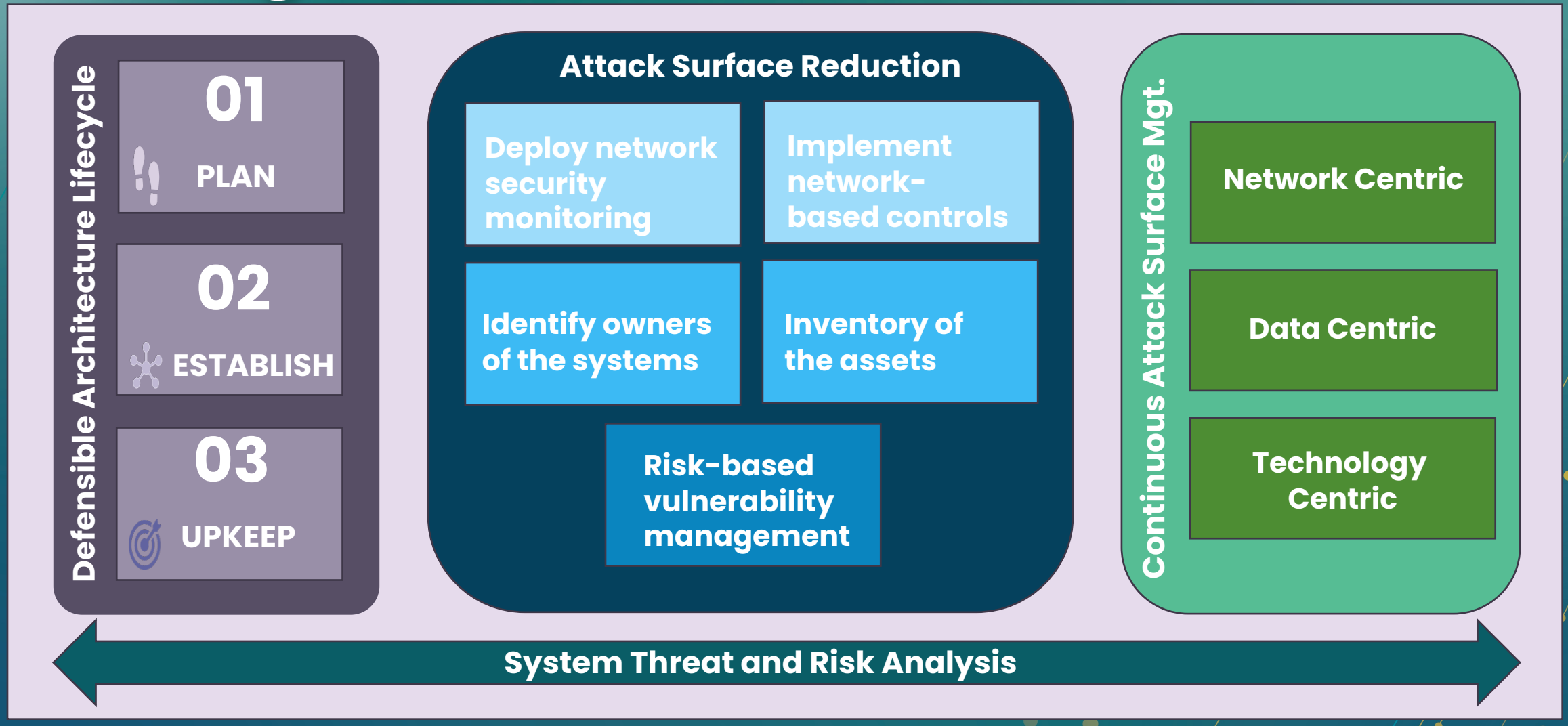
The Sliding Scale of Cybersecurity

Architecture



Ref: https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

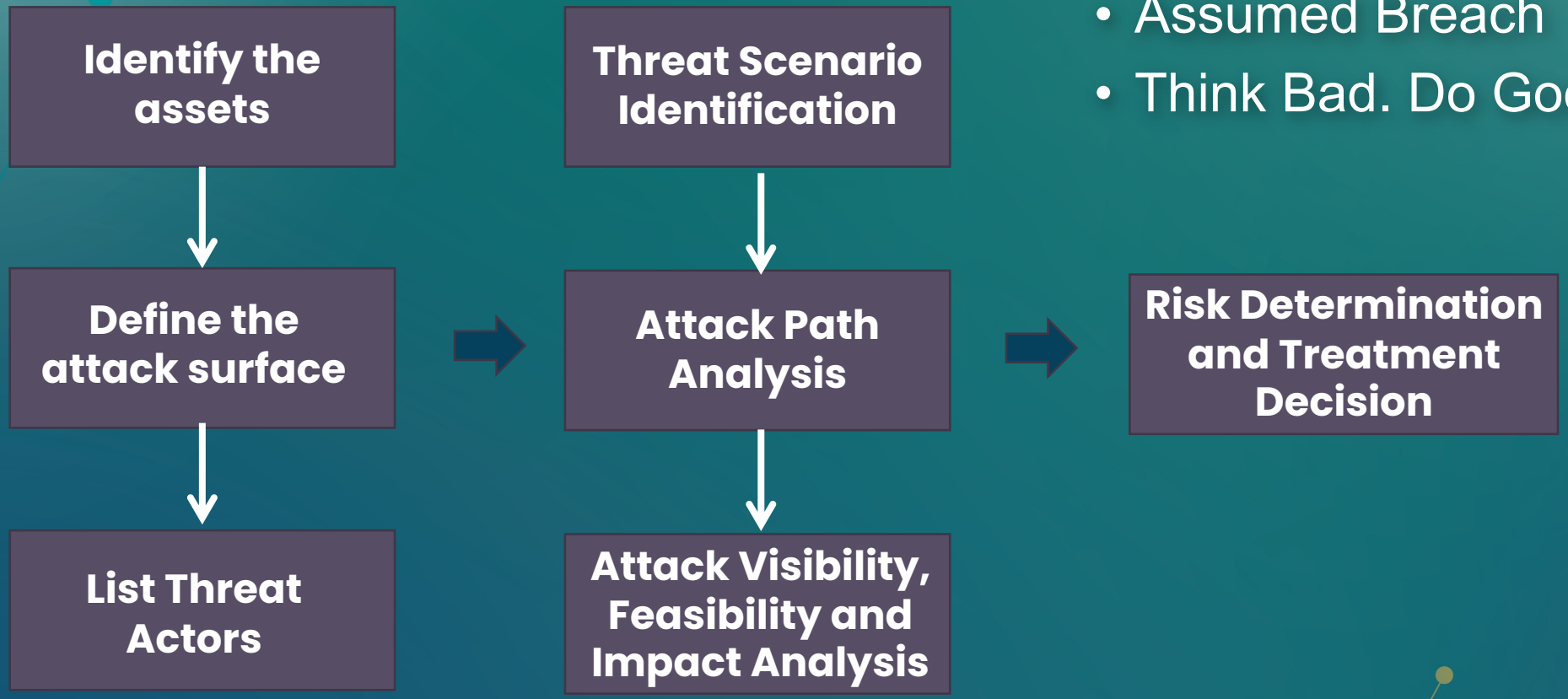
Creating Defensible Architecture



PCI Security Standards Council

Defensible Architecture

Threat and Risk Analysis



Mindset of Defensible Architecture

- Assumed Breach
- Think Bad. Do Good.

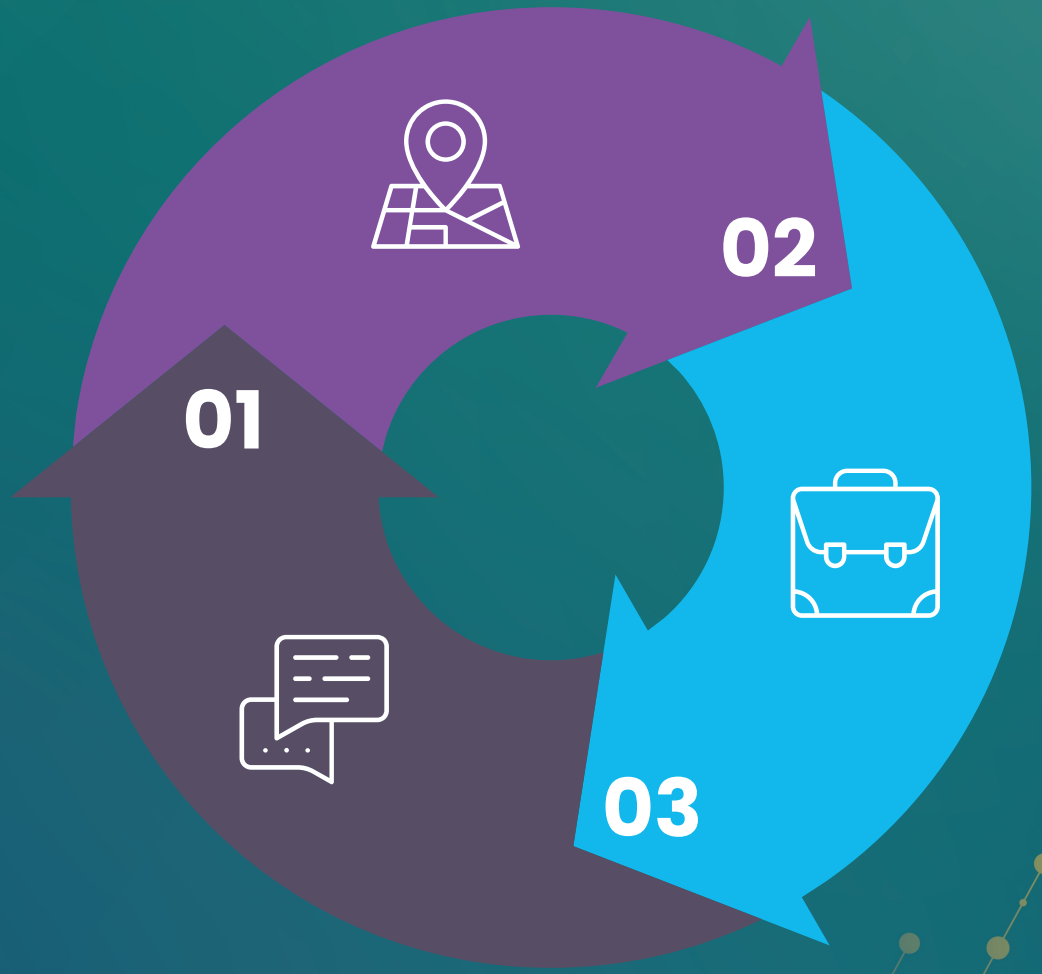
PCI Security Standards Council

Defensible Architecture

Defensible Architecture Lifecycle

ESTABLISH

Implement system functionality and security controls and validate the security controls selected during design phase.



UPKEEP

Manage the system security and sustain the security controls over time. Gain visibility into adversary activity, and detect and respond to attacks.

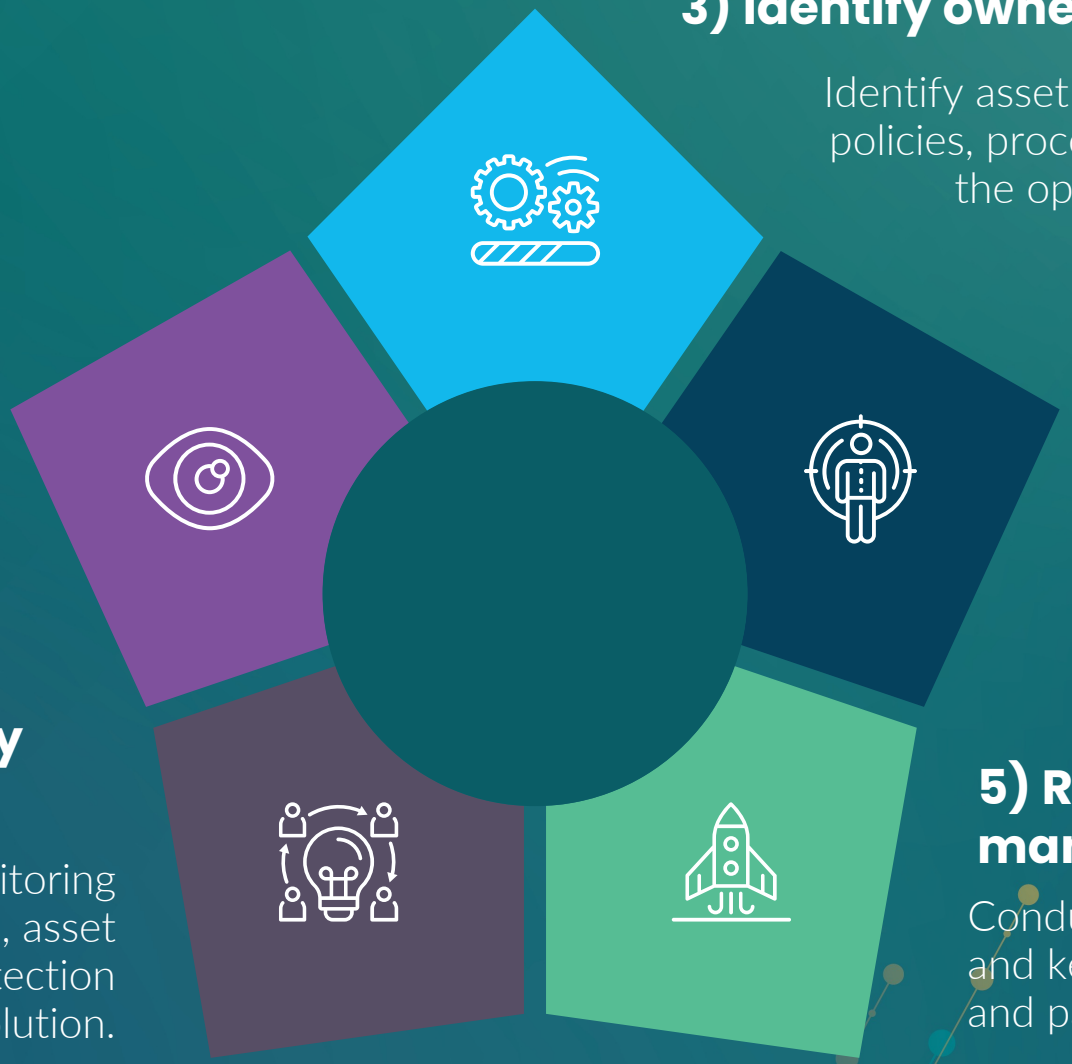
PLAN

Define the requirements and design of the system. This is to determine the fundamental security characteristics of a system.

PCI Security Standards Council

Defensible Architecture

Attack Surface Reduction



1) Deploy network security monitoring

Deploy network security monitoring sensors , for example, IDS/IPS, asset discovery and threat detection solution.

2) Implement network-based controls

For example, network segmentation, ingress/egress filtering, network admission/access control, proxy connections, hardening.

3) Identify owners of the systems

Identify asset owners and develop policies, procedures, and plans for the operation of that asset.

4) Inventory of the assets

Know everything hosted on your network.

5) Risk-based vulnerability management

Conduct vulnerability assessment and keep your assets hardened and patched.

PCI Security Standards Council

Defensible Architecture

Continuous Attack Surface Management

Network Centric

Improving prevention and detection capabilities with “Think Bad. Do Good.” and Zero Trust mindset.

Data Centric

Identify core data where they reside. Classify and prioritize security controls to protect those sensitive data.

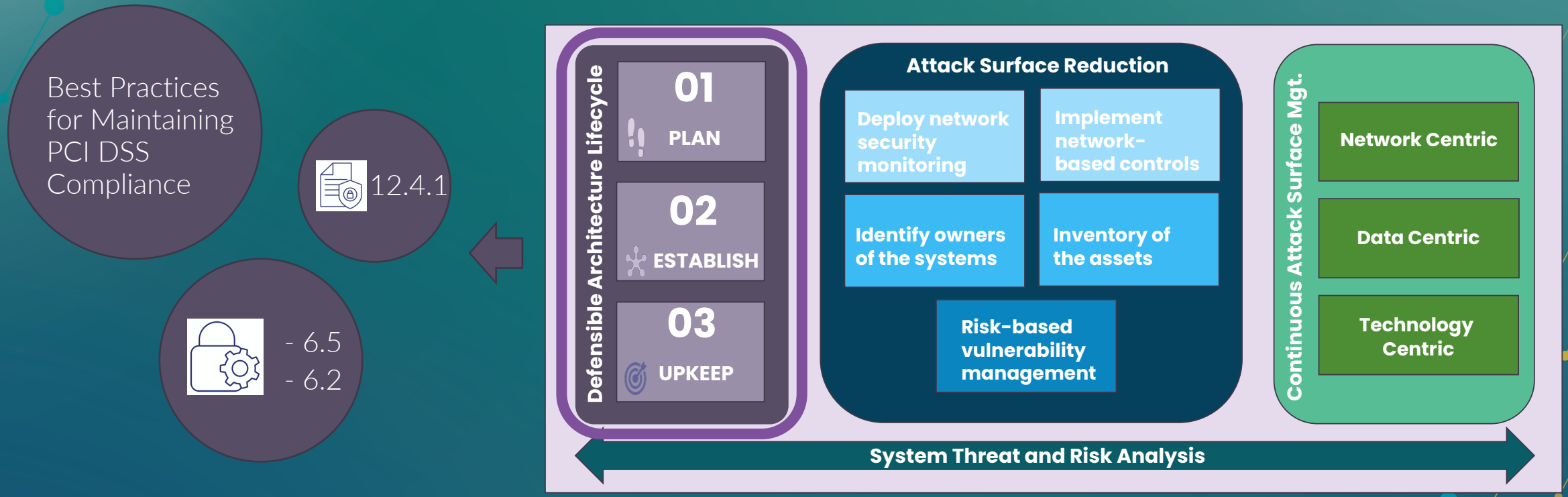
Technology Centric

Maximize the value and impact for existing security technologies to further improve an organization's security posture.

PCI Security Standards Council

Defensible Architecture

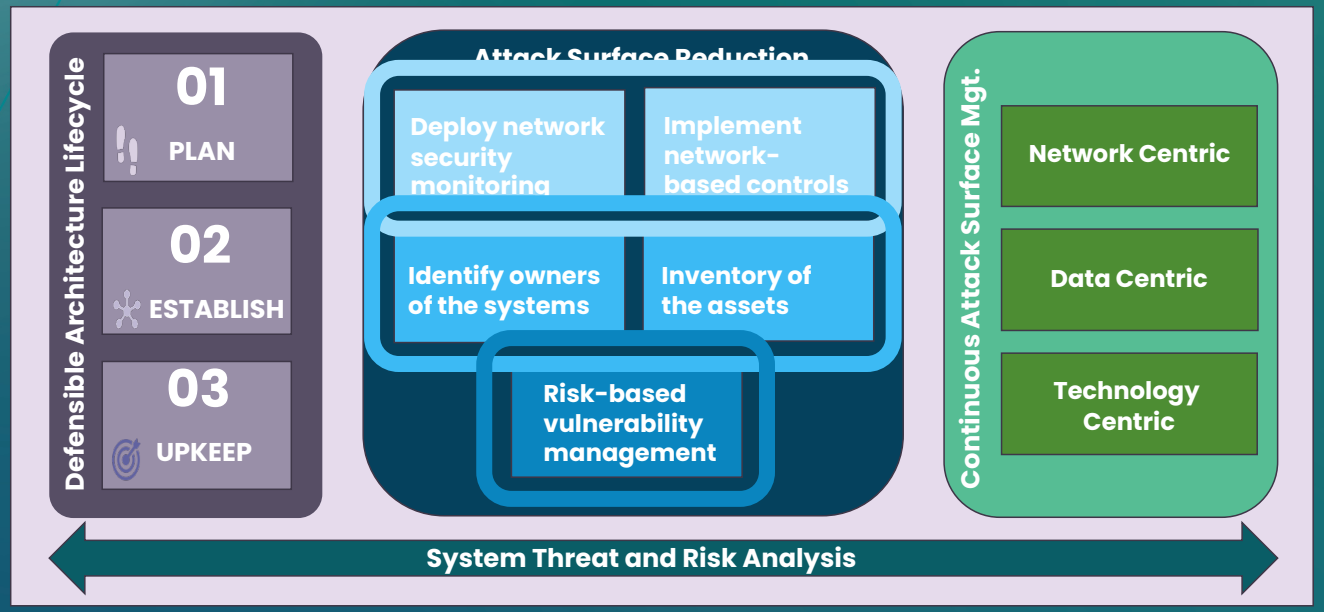
Mapping to PCI DSS requirements together - Defensible Architecture Lifecycle



PCI Security Standards Council

Defensible Architecture

Mapping to PCI DSS requirements together - Attack Surface Reduction



Scoping and Network Segmentation

- 10.2
- 10.4
- 11.5

- 1.2
- 1.3
- 1.4
- 11.2

Security policies and operational procedures for each requirements

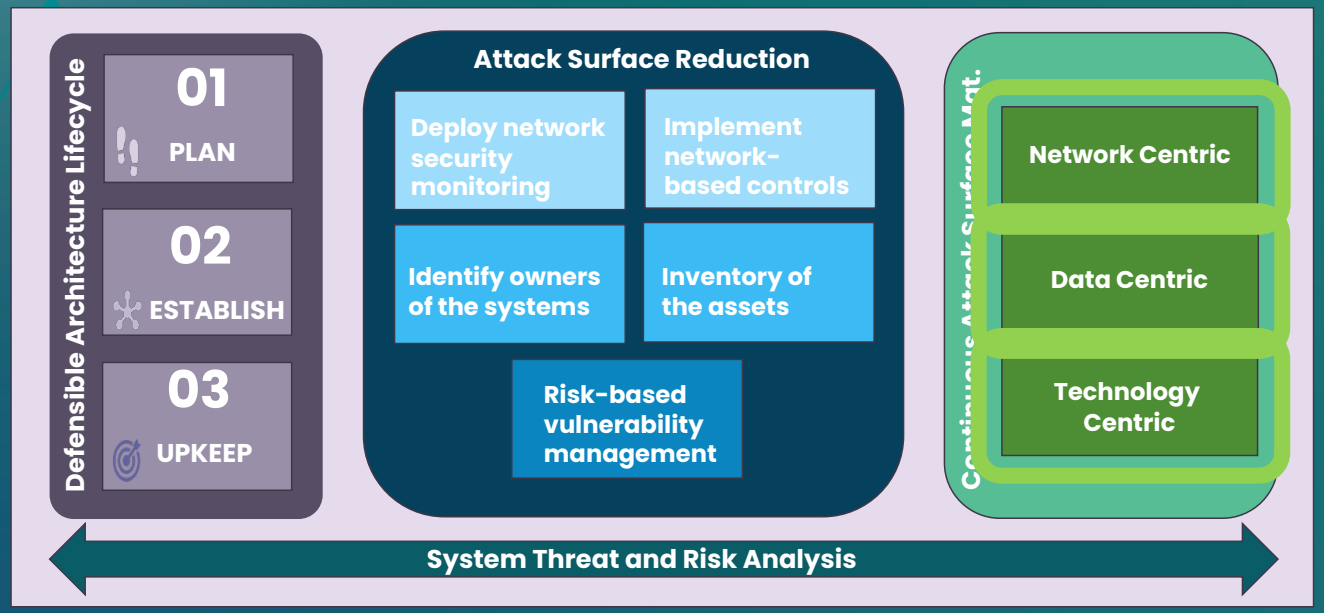
- 12.1
- 12.4.1
- 12.5

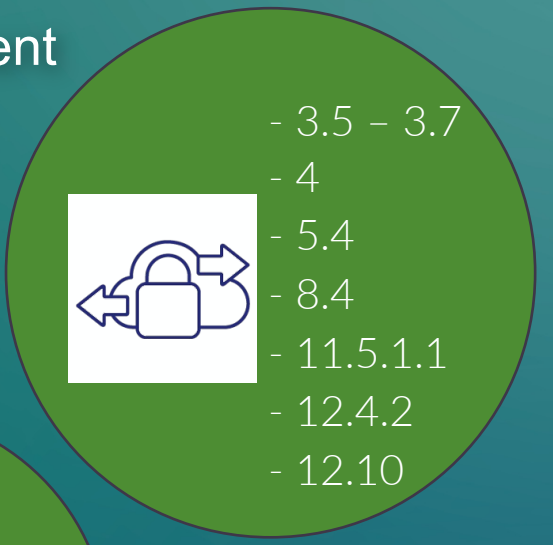
- 2.2
- 2.3
- 6.2
- 6.3
- 6.4
- 11.3
- 11.4

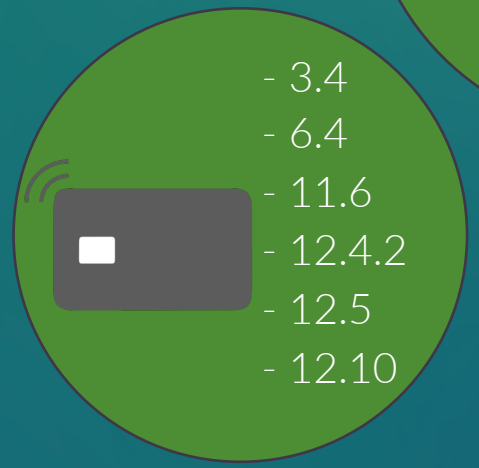
PCI Security Standards Council

Defensible Architecture

Mapping to PCI DSS together - Continuous Attack Surface Management







PCI Security Standards Council

PCI Security Standards Council

Utilize Deception Technology

Provide early warning of potential cyber-attacks and unauthorized activity.

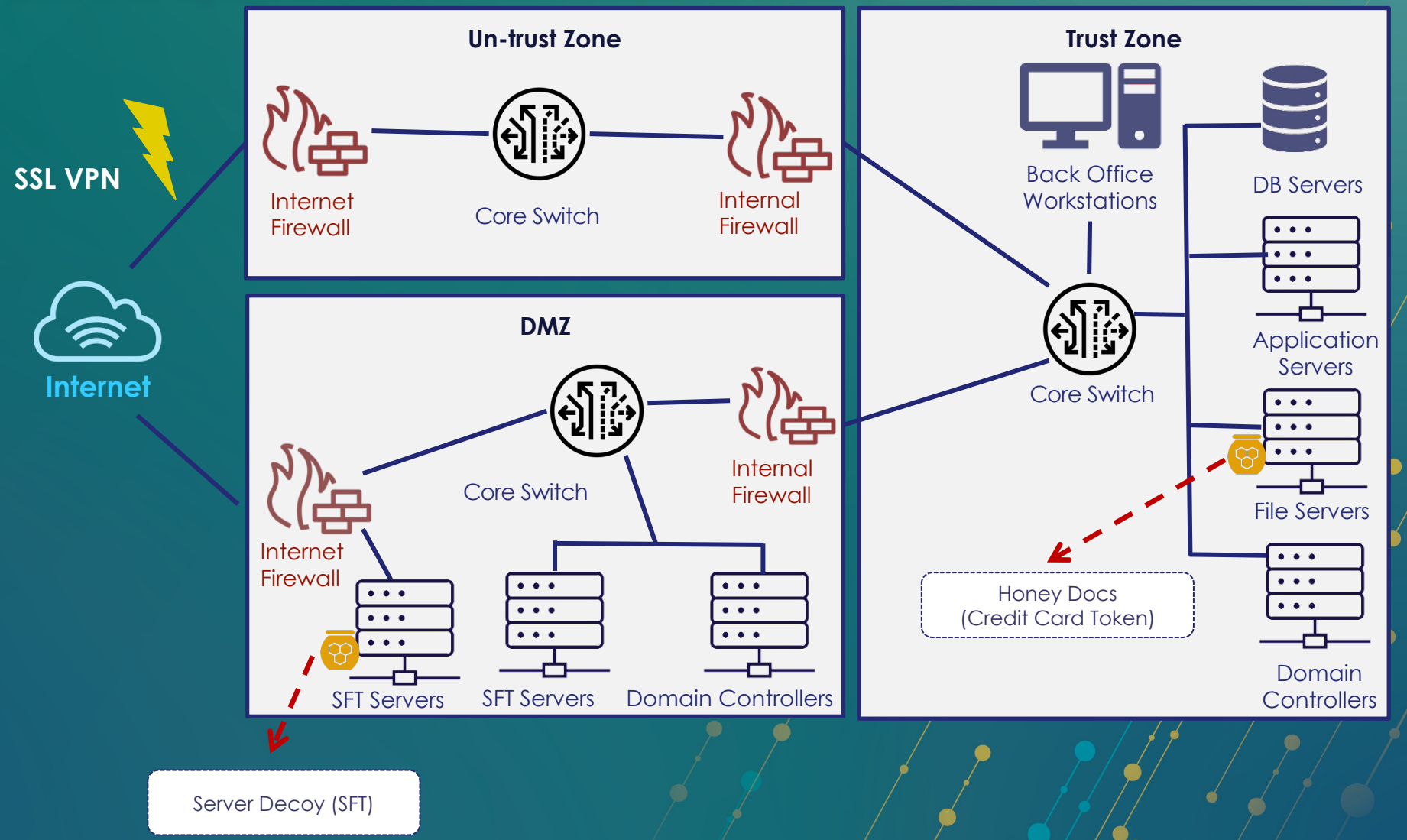
Utilize Deception Technology

Provide early warning of potential cyber-attacks and unauthorized activity.

By simulating weak and attractive IT components to lure the attackers:

- Engage threats in a controlled environment and collect valuable threat intelligence
- Minimize the threats qualification time with pre-qualified detections

Hunters become the hunted!



PCI Security Standards Council

Key Takeaways

What we have learned from the real-world hacking case studies.

Building defensible architecture using PCI DSS

Utilize deception technology to provide early warning of potential cyber-attacks

The Future of Cyber Security from Hackers Perspective:

Building a Defensible Architecture using PCI DSS

Pak Ho CHAN
Regional Head of OT/IT Cyber Defence, APAC
http://linkedin.com/in/phchan6

PCI Security Standards Council

Queenie CHEN
Regional PCI Practice Manager, APAC

Europe Community Meeting 2023

PCI Security Standards Council