PCI Security Standards Council®

Digital Fire Doors:

The Frontline Defenders Against Ransomware and For Maintaining Secure & Resilient Operations

Ian Robinson

Chief Architect, UK, Titania Ltd

TITANIA

Jim Seaman

Director, UK, IS Centurion Consulting Ltd

INFORMATION SECURITY CENTURION

PCI Security Standards Council

Introduction

The Importance of Digital Fire Doors

- Comparing the Fire Threat to the Ransomware Threat.
  - Deliberate Vs Non-Deliberate.
- Importance of Effective Network Segmentation.
  - PCI DSS v4.0 Perspective.
    - Page 12, PCI DSS v4.0.
  - EU Digital Operational Resilience Act (EU DORA).
    - Article 9: Protection and prevention (4(b)).

PCI Security Standards Council

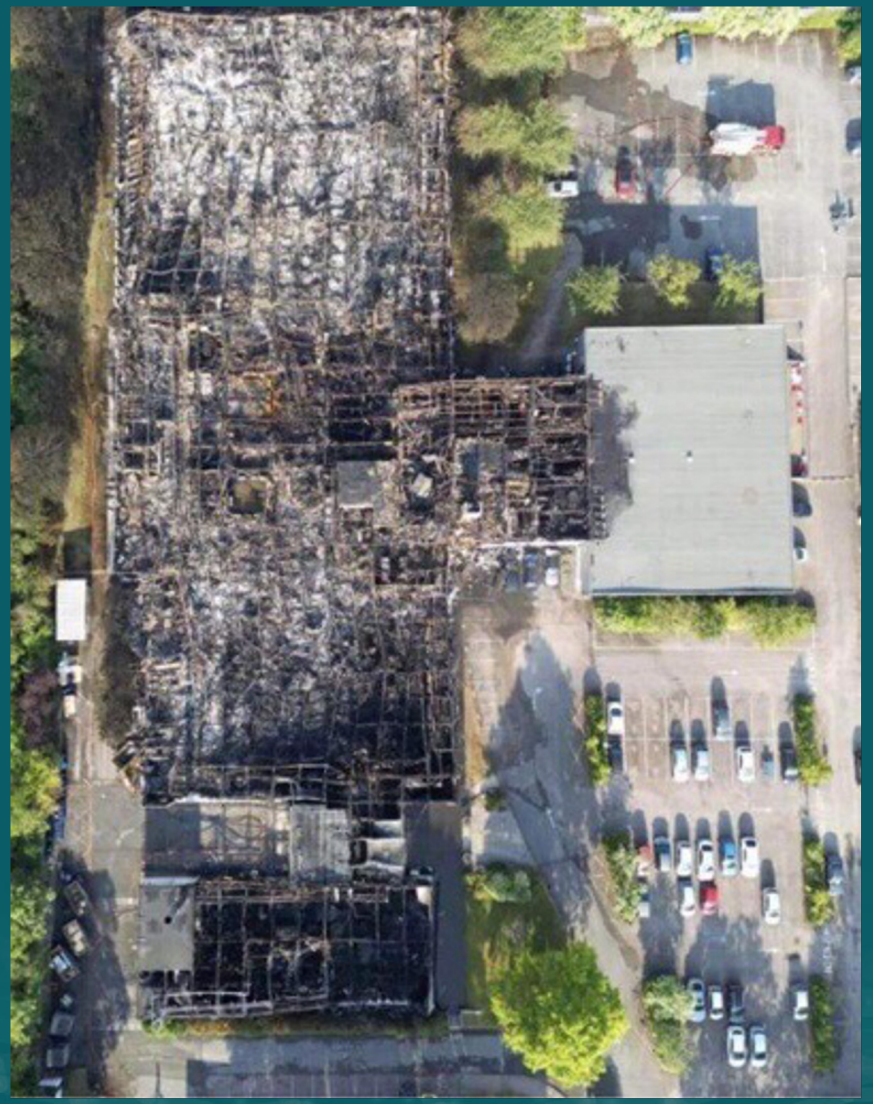
Real-Life Example:

Fire Spread Due to Ineffective Fire Doors

PCI Security Standards Council®

From This:

To This:



PCI Security Standards Council®

Analogy:

Comparison of Fire Spread with Ransomware

- *“Ransomware is a type of malware that encrypts an organization’s data and demands payment as a condition of restoring access to that data.*
- *Ransomware can also be used to steal an organization’s information and demand additional payment in return for not disclosing the information to authorities, competitors, or the public.*
- *Ransomware attacks target the organization’s data or critical infrastructure, disrupting or halting operations and posing a dilemma for management:*
  - *Pay the ransom and hope that the attackers keep their word about restoring access and not disclosing data, or*
  - *Do not pay the ransom and attempt to restore operations themselves.”*

PCI Security Standards Council

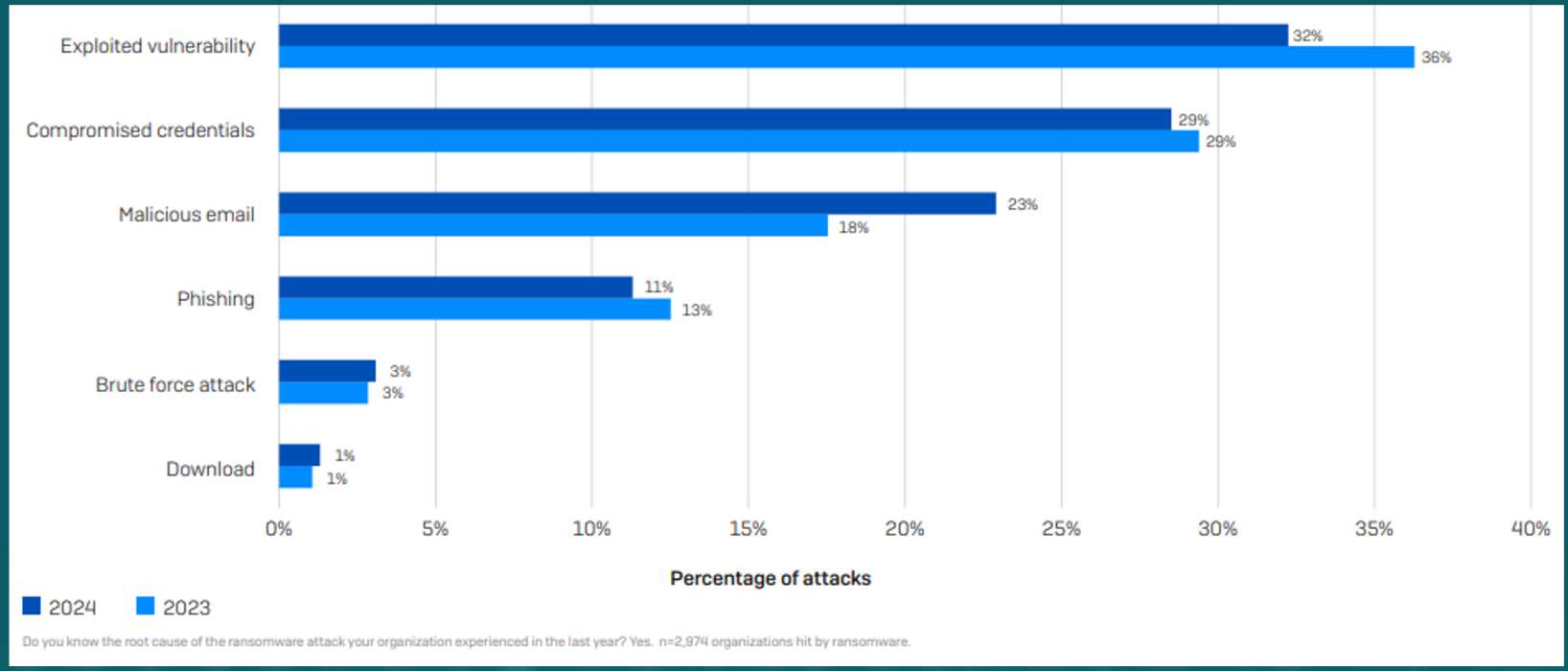
Source:
NISTIR 8374 – Ransomware Risk Management: A Cybersecurity Framework Profile

Ransomware:

Spread Mechanisms:

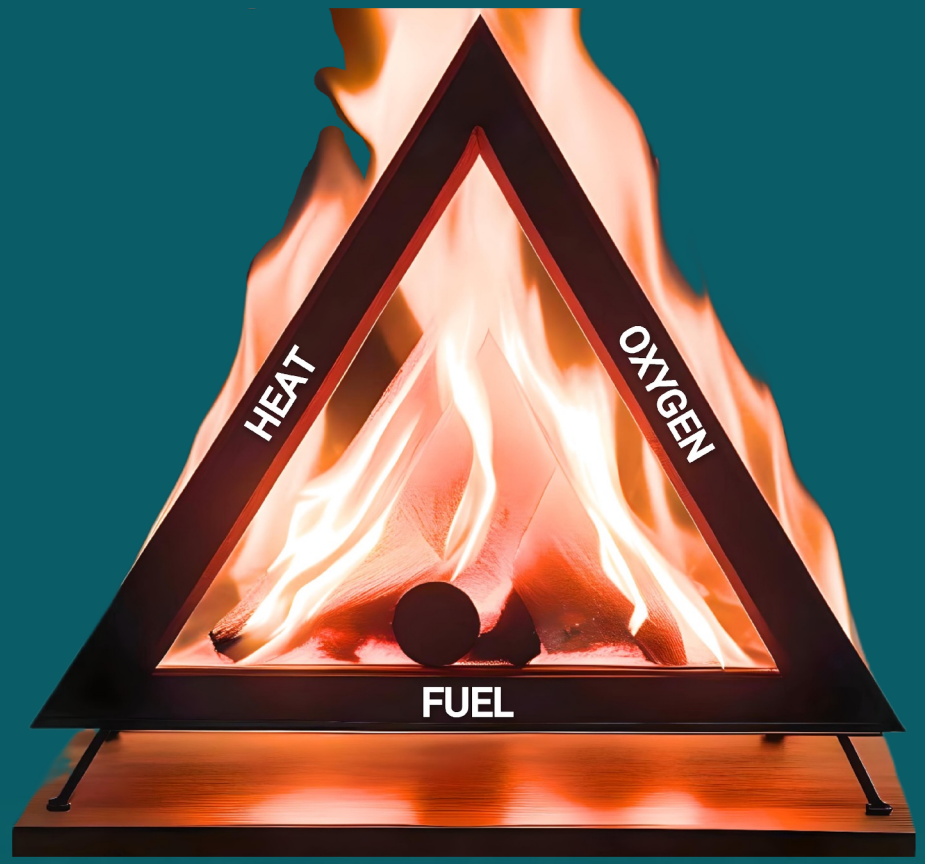
- Email attachments.
- Malicious URLs.
- Remote Desktop Protocols (RDPs).
- Removable devices.

Root Causes of Ransomware Attacks



PCI Security Standards Council®

The Triangle Models:



Fire Triangle

Ransomware Triangle

PCI Security Standards Council

Digital Fire Doors

Ransomware Triangle Mitigation Measures

Delivery Method (HEAT)

- Email Security
- Web Filtering
- Application Whitelisting

Vulnerability (FUEL)

- Asset & Definition Management
- Configuration Management
  - *Principle of 'Least Functionality'*
- Patch Management
- Risk Management

Execution (OXYGEN)

- Backup & Recovery
- Incident Response Planning
- Network Monitoring & IDS/IPS
- Endpoint Protection and Response
- Sandboxing

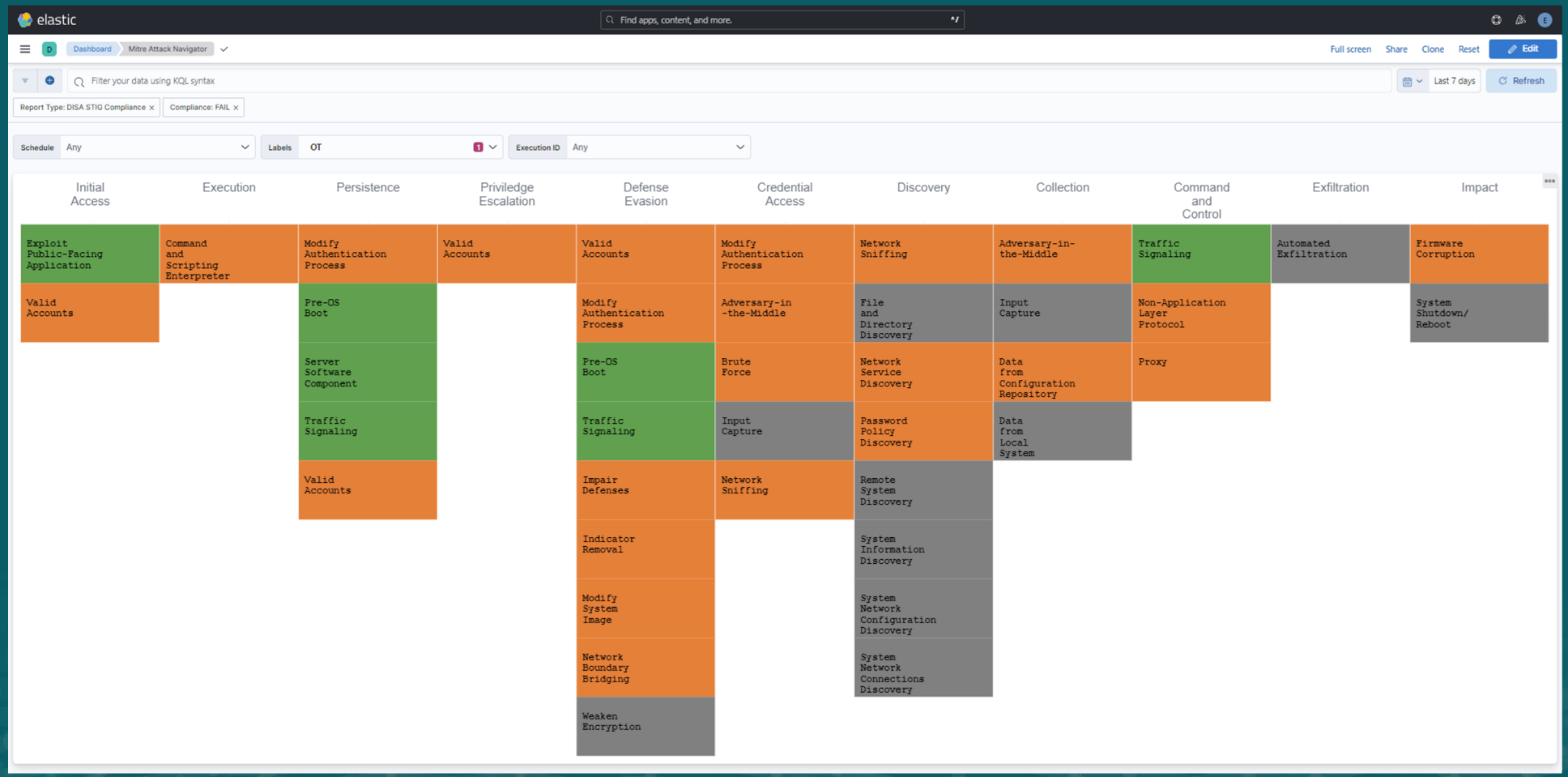
PCI Security Standards Council

Be PROACTIVE:

- **Act like you expect your network WILL BE compromised!**
- **Implement measures to LIMIT the potential damage/impact!!**

Heatmapping levels of exposure

By giving visibility of vulnerabilities to execution and delivery mechanisms

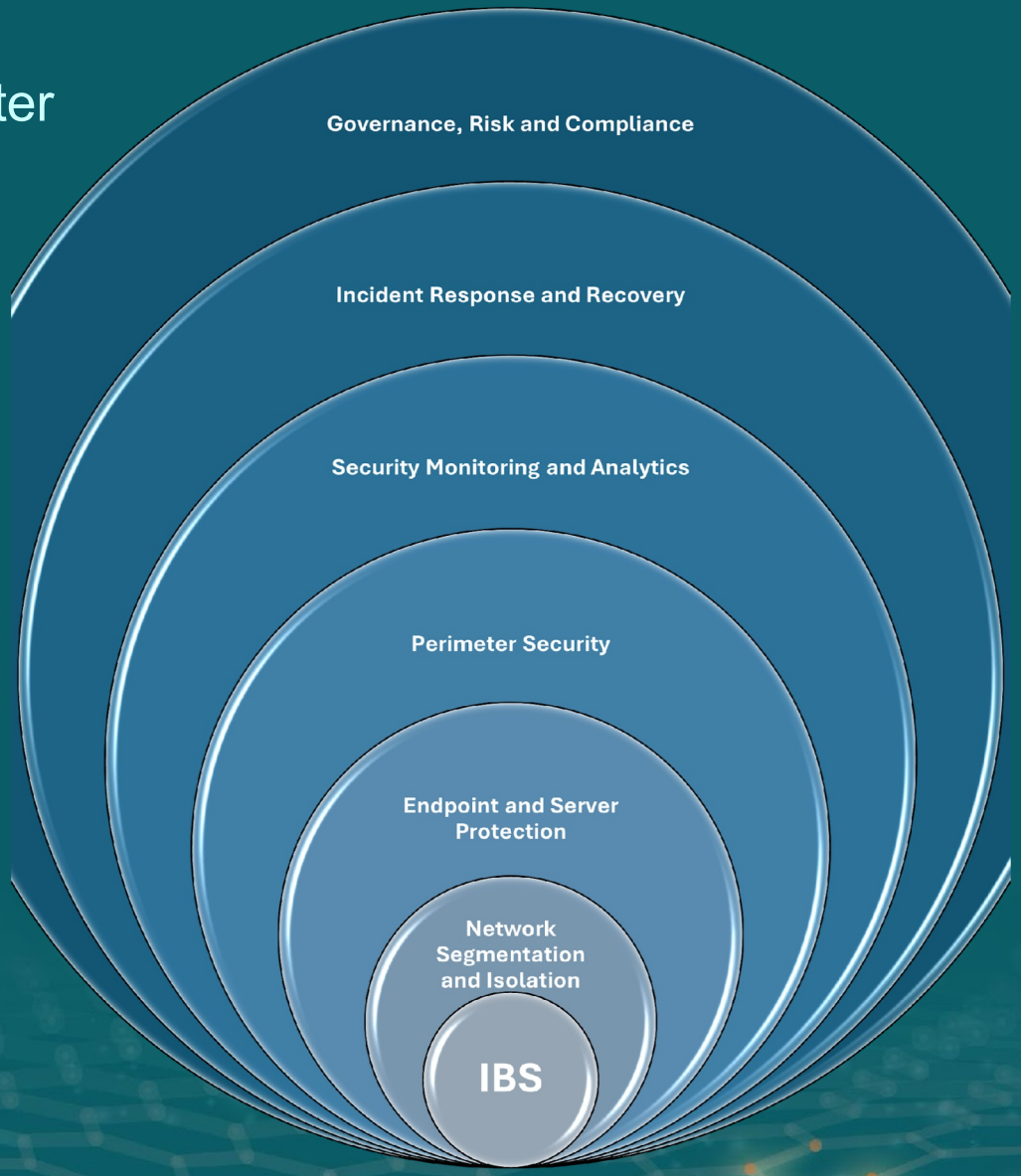


PCI Security Standards Council®

Creating Effective Defensive Layers

From the Inside Looking Outwards towards the Perimeter

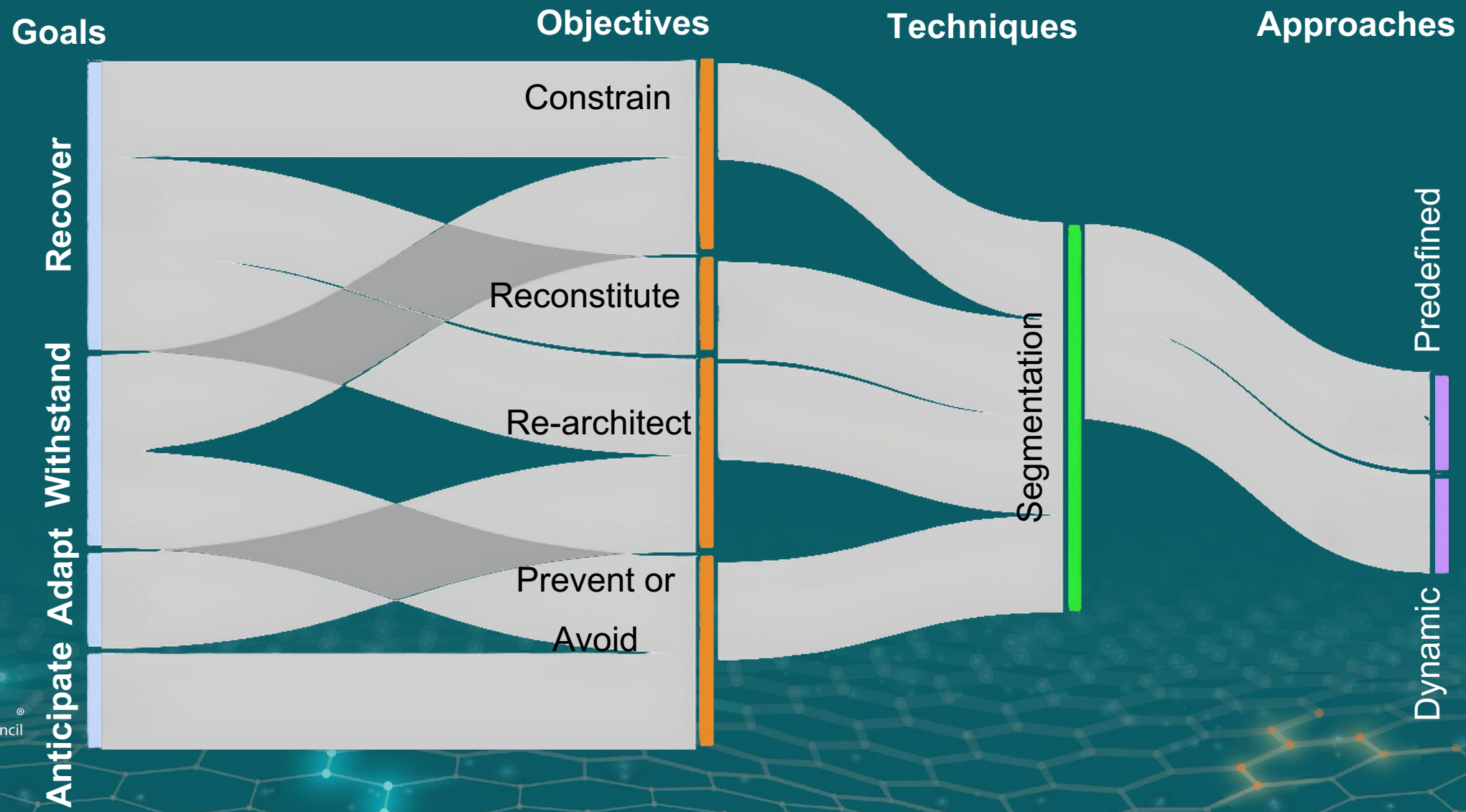
- NIST SP800-160 Volume 2, Revision 1 *(Developing Cyber-Resilient Systems: A Systems Security Engineering Approach)* advocates for a cyber resiliency strategy that:
  - Focuses on defending systems from the inside out.



PCI Security Standards Council®

Segmentation

Define and separate system elements based on criticality and trustworthiness.

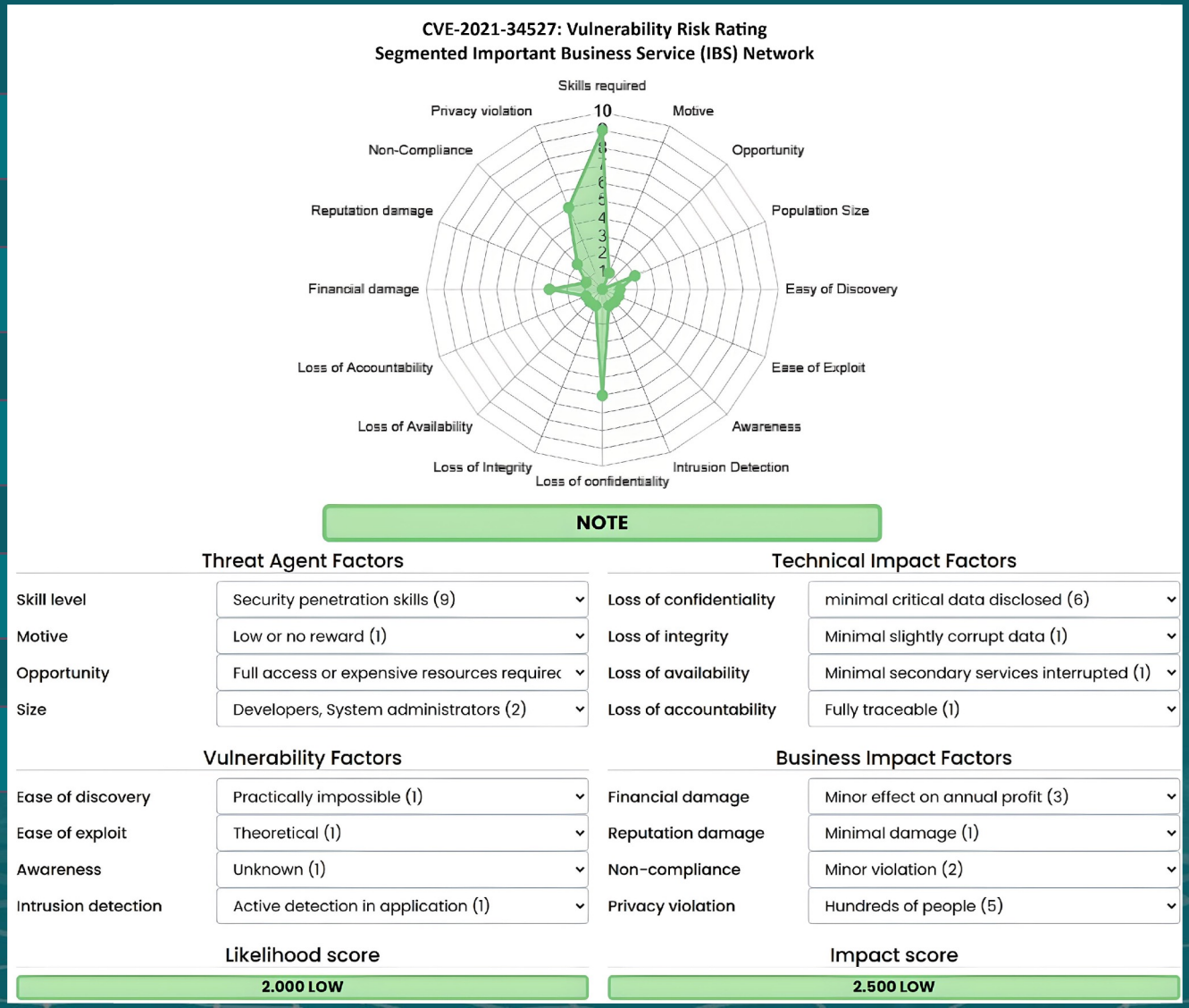


PCI Security Standards Council

Benefits of Effective Network Isolation

SMARTer Risk-Based Vulnerability Management

- **S**pecific
- **M**easurable
- **A**chievable
- **R**ealistic
- **T**imebound



PCI Security Standards Council®

Network & Information Security 2 Directive

NCSC Cyber Assurance Framework (CAF)

- **Mandatory from 18 October 2024.**
- **Applies to:**
  - **Essential Entities:**
    - Max fines – 10 Million Euros (2% of global annual revenue).
  - **Important Entities:**
    - Fines of at least 7 Million Euros (1.4% of global annual revenue).
- **CAF Objective B - Protecting against cyber attacks**
  - Building resilience against cyber attack.
- **Principle**
  - The organisation builds resilience against cyber attack into the design, implementation, operation and management of systems that support the operation of essential functions.
- **B5.b Design for Resilience**
  - You design the network and information systems supporting your essential function(s) to be resilient to cyber security incidents.
  - Systems are **appropriately** segregated and resource limitations are mitigated.

PCI Security Standards Council®

Conclusion

Maintaining Secure & Resilient Operations

Continuously check your networks for opportunities for ransomware to take hold

Extinguish one ransomware element, and remove the operational risk

Prioritize which risks are most critical, and need addressing first

Ensure that the safeguarding measures deployed have been effective in shutting the fire doors - and shutting down attacks.

PCI Security Standards Council®

Thank You!

PCI Security Standards Council®