Tales from the Trenches

Cybersecurity Incidents & the Imperative for Zero Trust in Healthcare

Hi, I'm Todd Sorg

- Chief Operations Officer/CISO

Tales from the Trenches:

Cybersecurity Incidents & the Imperative for Zero Trust in Healthcare

Takeaways:

1. Understanding of Cybersecurity Incidents
2. Lessons Learned
3. The Need for Adopting a Zero Trust Mentality

Understanding Adversaries

Type of Threat Actor	Motives
State Sponsored	Espionage, theft, or furthers other national interests
Organized Crime	Financial gain
Hacktivists	Exposing secrets, disrupting service to those with differing morals
Insiders	Bypassing controls, further self-interests
Script Kiddies	Vandalism, Curiosity

Key Terminology

Security Incident

A security event that compromises an asset's integrity, confidentiality, or availability

Security Breach

An incident that results in the confirmed disclosure of data to an unauthorized party

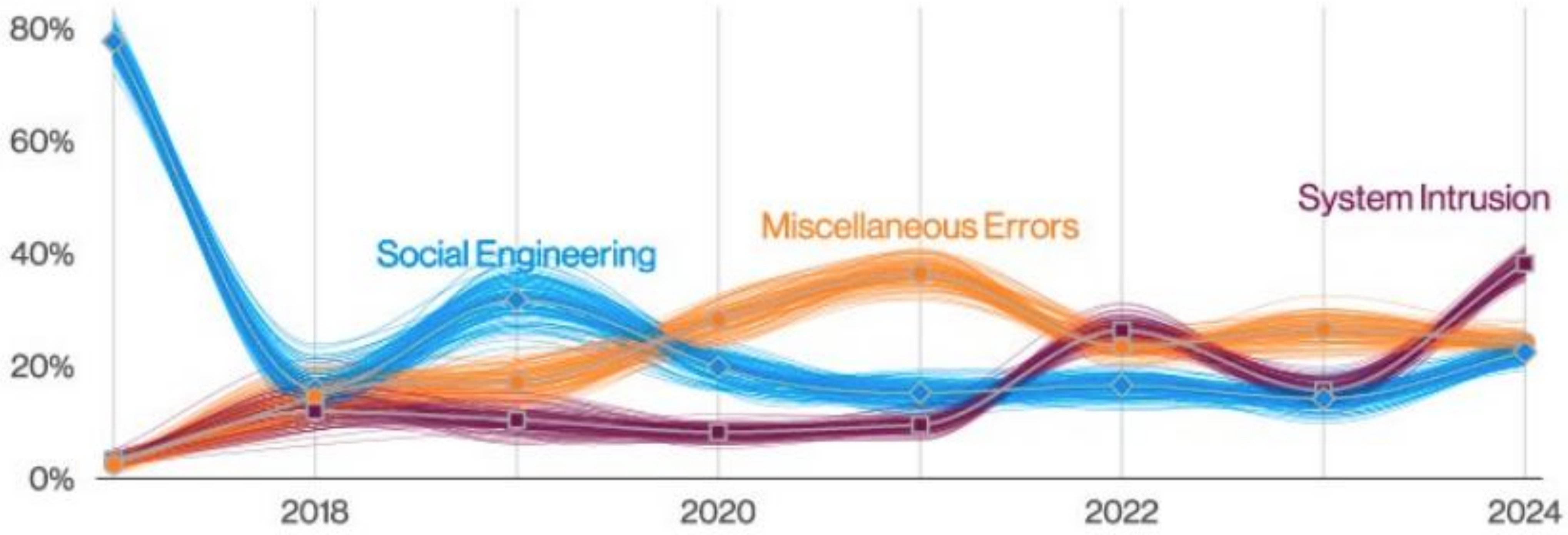


Figure 60. Top patterns in Financial and Insurance industry breaches

Credit: 2024 Verizon DBIR

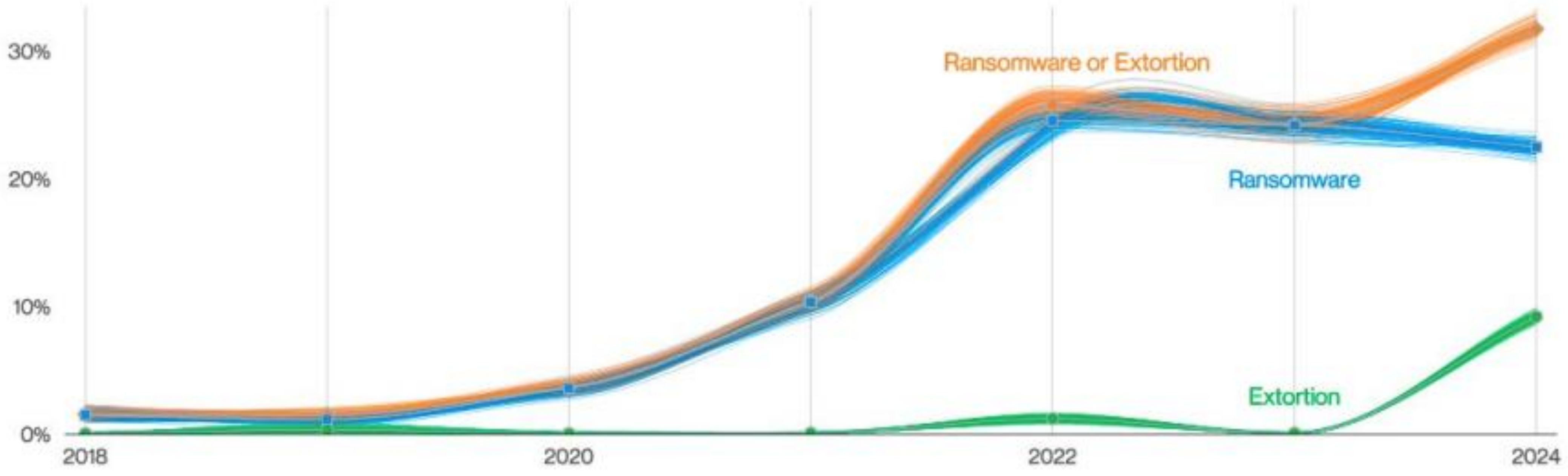
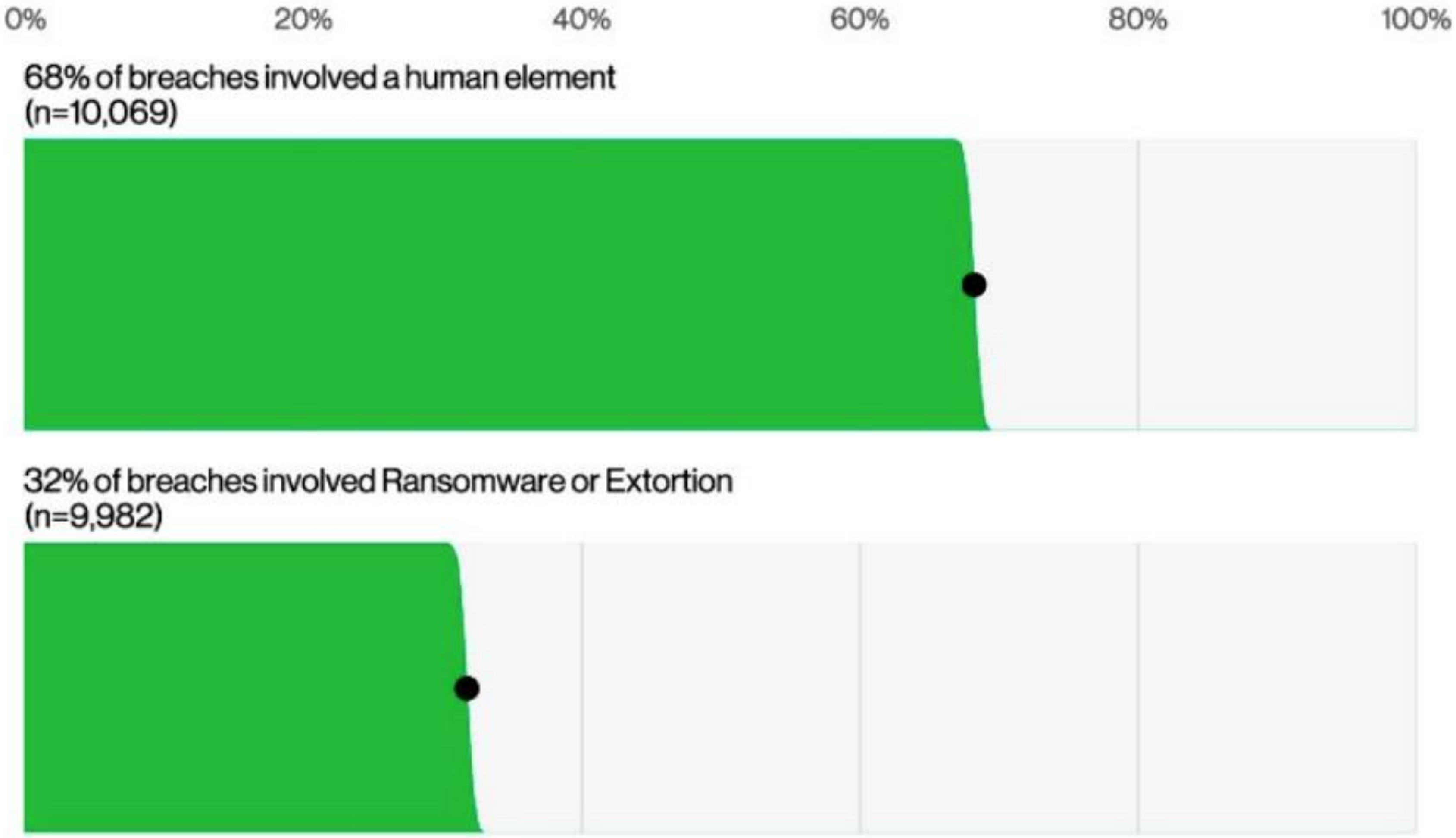


Figure 2. Ransomware and Extortion breaches over time

Credit: 2024 Verizon DBIR



68% of breaches involved a human element (n=10,069)

32% of breaches involved Ransomware or Extortion (n=9,982)

Credit: 2024 Verizon DBIR

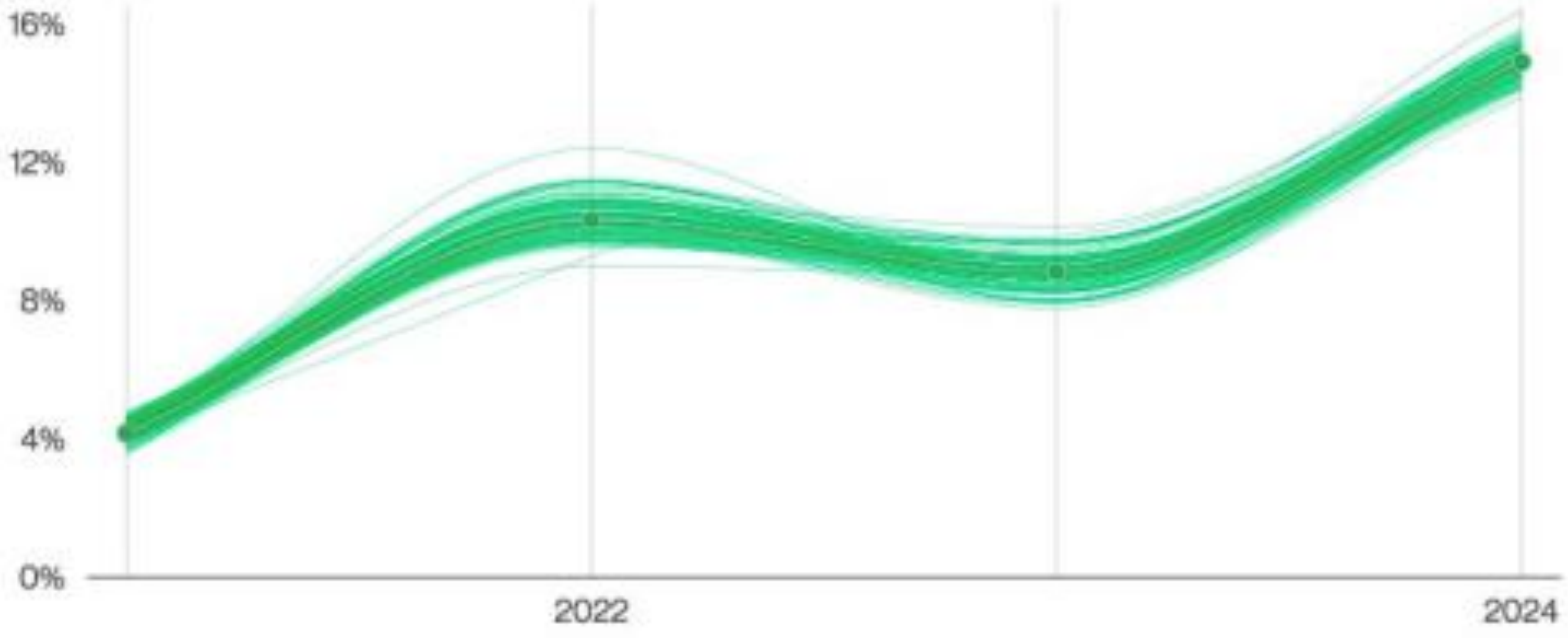
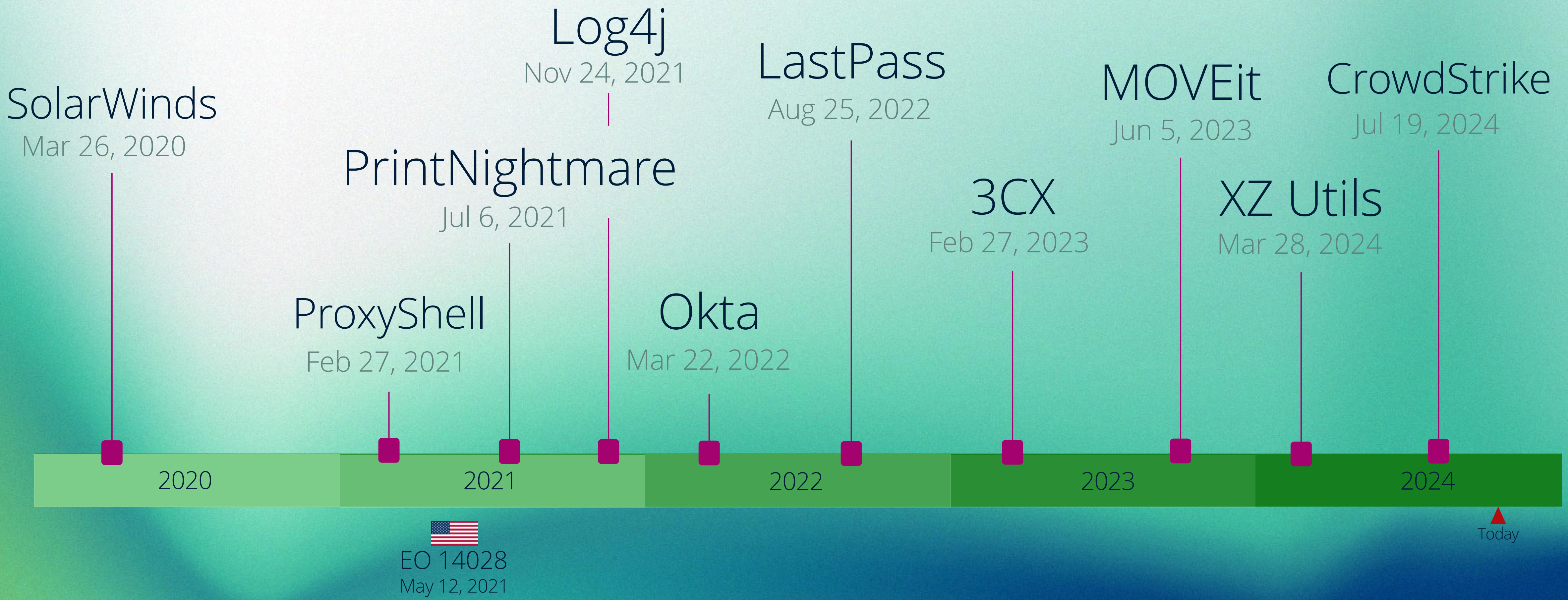


Figure 9. Supply chain interconnection in breaches over time

Credit: 2024 Verizon DBIR

Notable Supply Chain Events



SolarWinds
Mar 26, 2020

ProxyShell
Feb 27, 2021

EO 14028
May 12, 2021

PrintNightmare
Jul 6, 2021

Log4j
Nov 24, 2021

Okta
Mar 22, 2022

LastPass
Aug 25, 2022

3CX
Feb 27, 2023

MOVEit
Jun 5, 2023

XZ Utils
Mar 28, 2024

CrowdStrike
Jul 19, 2024

Incident #1: Persistence Pays Off

- Employee received a “remittance” email
- Scanned image was blurry, employee clicked to view
- Entered Office 365 credentials
- Did not report incident to IT
- Began receiving frequent phone calls
- Accepted MFA prompt on phone
- Began sending thousands of emails

Incident #1: Lessons Learned

Implement frequent security and awareness training

Never accept an MFA prompt unless actively logging in

Implement phishing resistant MFA

Consider incorporating device evaluation into access policies

Perform audits on critical controls to identify misconfigurations

Incident #2: The Perfect Storm

- SIEM alerted on unusual VPN activity over the weekend
- IT staff unreachable
- All servers encrypted
- Slow insurance engagement
- Effective backups, poor continuity
- Poor inventory management
- Lack of BCDR planning
- Storing PII in plain text
- Paid ransom, failed decryption
- EOL VPN appliance

Incident #2: Lessons Learned

- Inventory all systems on network
- Document RTO/RPO of critical business systems
- Ensure availability of key personnel or alternatives
- Practice your incident response plan
- Implement application allowlisting and ZTNA

Incident #3: The Family Business

- Business owner calls into support
- $800,000 wire transfer
- Contacted IC3
- Started with email compromise
- Communicated with “vendor” to initiate wire transfer
- Shut down the family business

Incident #3: Lessons Learned

Implement frequent security and awareness training

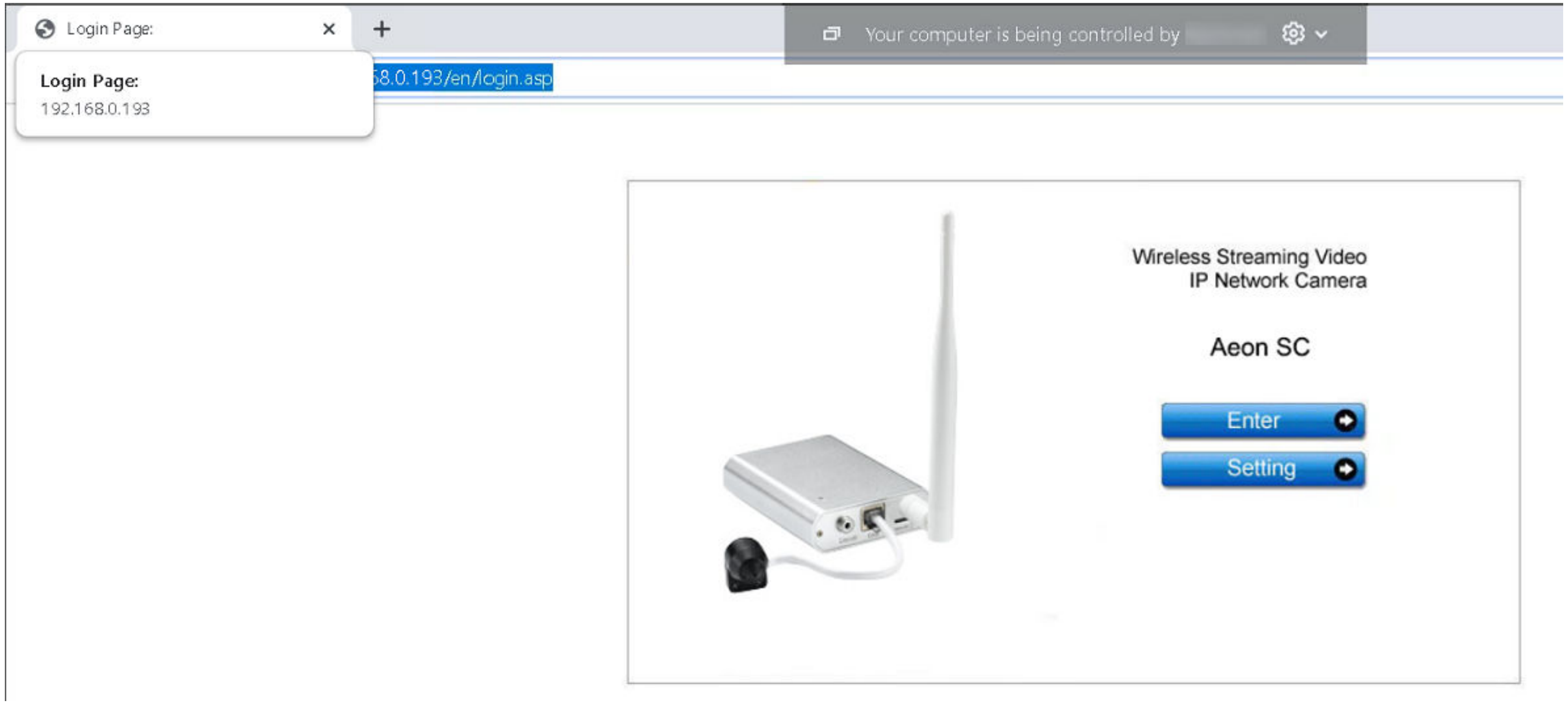
Implement MFA on all critical applications – Phishing resistant preferred

Implement dual approvals for payment transfers

Review cyber insurance policies

Incident #3: Swimming Lessons

- Customer was evaluating new security tool
- Identified a device making unusual network connections



Login Page:

Your computer is being controlled by [redacted]

Login Page:
192.168.0.193

68.0.193/en/login.asp

Wireless Streaming Video
IP Network Camera

Aeon SC

Incident #4: Lessons Learned

Implement solutions that inventory devices on the network

Isolate unauthorized devices on the network

Incident #5: Verkada's Response

- https://www.verkada.com/security-update/report/

Incident #5: Lessons Learned

Develop solid communication plan

Honest communications

Address concerns promptly

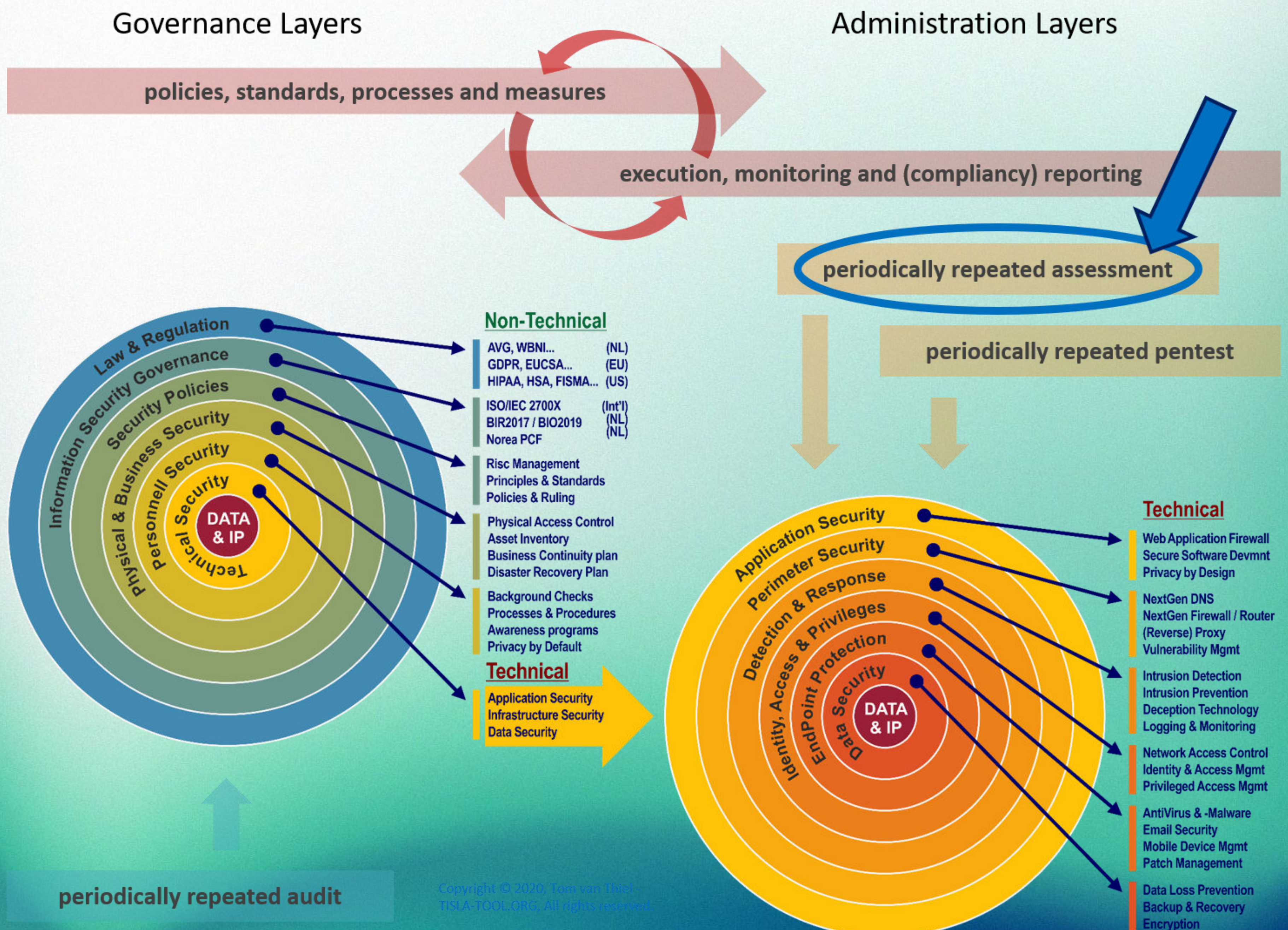
Continue providing updates until resolution

Introduction to Zero Trust

IS	IS NOT
A mentality/framework	A single product or technology
Data-focused	Perimeter-based security
Proactive	One-size-fits-all
Identity-centric	Easy to implement
Dynamic	A silver bullet to eliminate risk

Zero Trust Tenets

1. All resources must be considered
2. Location should be considered irrelevant
3. Access is granted on a per-session basis
4. Access is determined by dynamic evaluation
5. Authentication and authorization is evaluated BEFORE access is allowed
6. Monitor integrity and security posture of all devices
7. Develop baseline of network to further improvements



Governance Layers

Administration Layers

policies, standards, processes and measures

execution, monitoring and (compliancy) reporting

periodically repeated assessment

periodically repeated pentest

periodically repeated audit

Non-Technical

AVG, WBNI...	(NL)
GDPR, EUCSA...	(EU)
HIPAA, HSA, FISMA...	(US)
ISO/IEC 2700X	(Int'l)
BIR2017 / BIO2019	(NL)
Norea PCF	(NL)

Risc Management
Principles & Standards
Policies & Ruling

Physical Access Control
Asset Inventory
Business Continuity plan
Disaster Recovery Plan

Background Checks
Processes & Procedures
Awareness programs
Privacy by Default

Technical

Application Security
Infrastructure Security
Data Security

Technical

Web Application Firewall
Secure Software Devmnt
Privacy by Design

NextGen DNS
NextGen Firewall / Router
(Reverse) Proxy
Vulnerability Mgmt

Intrusion Detection
Intrusion Prevention
Deception Technology
Logging & Monitoring

Network Access Control
Identity & Access Mgmt
Privileged Access Mgmt

AntiVirus & -Malware
Email Security
Mobile Device Mgmt
Patch Management

Data Loss Prevention
Backup & Recovery
Encryption

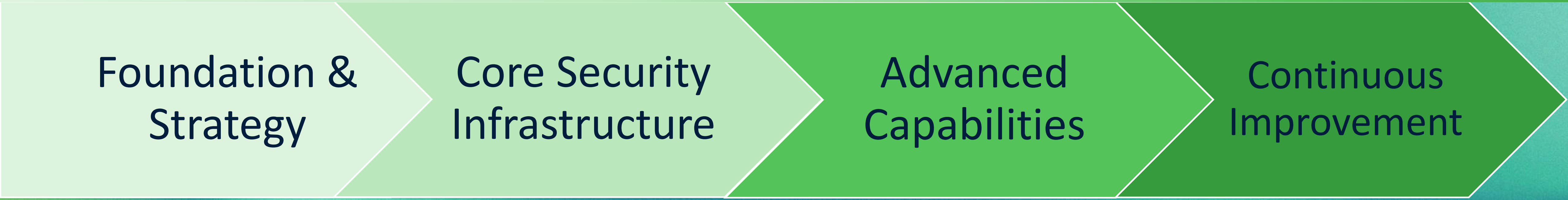
Implementation Plan

1. Define Strategy
2. Inventory Resources
3. Define Scope

4. Enhance Device Security
5. Network Segmentation
6. Implement IAM

7. Implement SIEM
8. Deploy DLP
9. Automate Processes

10. Monitor & Adapt



Foundation & Strategy

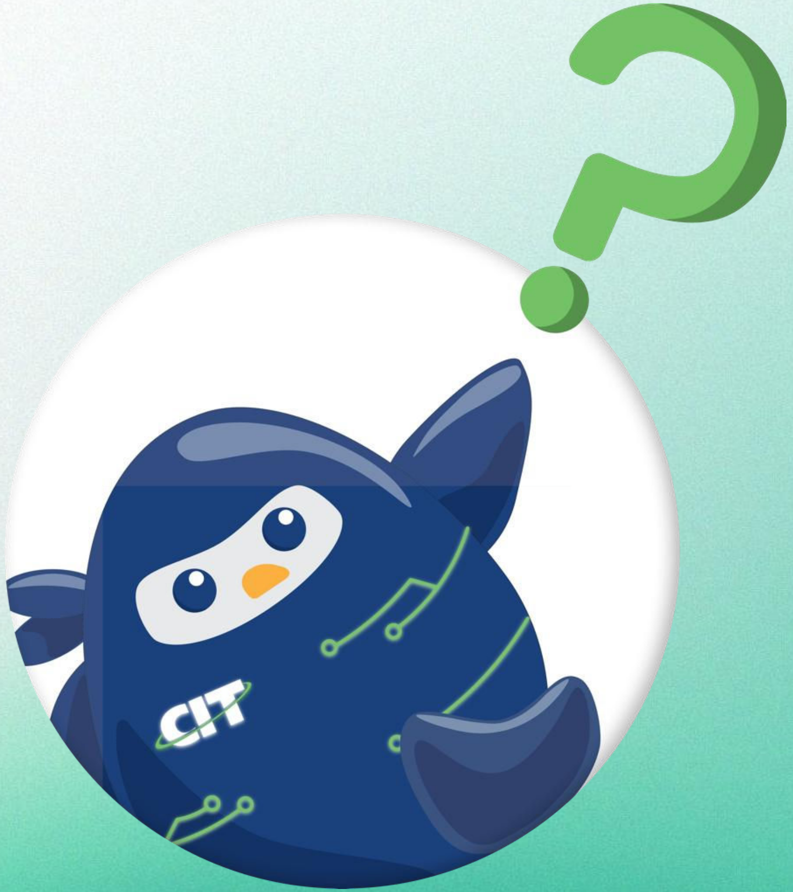
Core Security Infrastructure

Advanced Capabilities

Continuous Improvement

Core Recommendations

- Phishing Resistant MFA
- Endpoint Detection & Response (EDR)
- Application Allowlisting
- Privileged Access Management
- Zero Trust Network Access (ZTNA)
- Network Access Control (NAC)
- Security Awareness Training
- BCDR Review



CIT

MAKING TECHNOLOGY WORK FOR BUSINESS