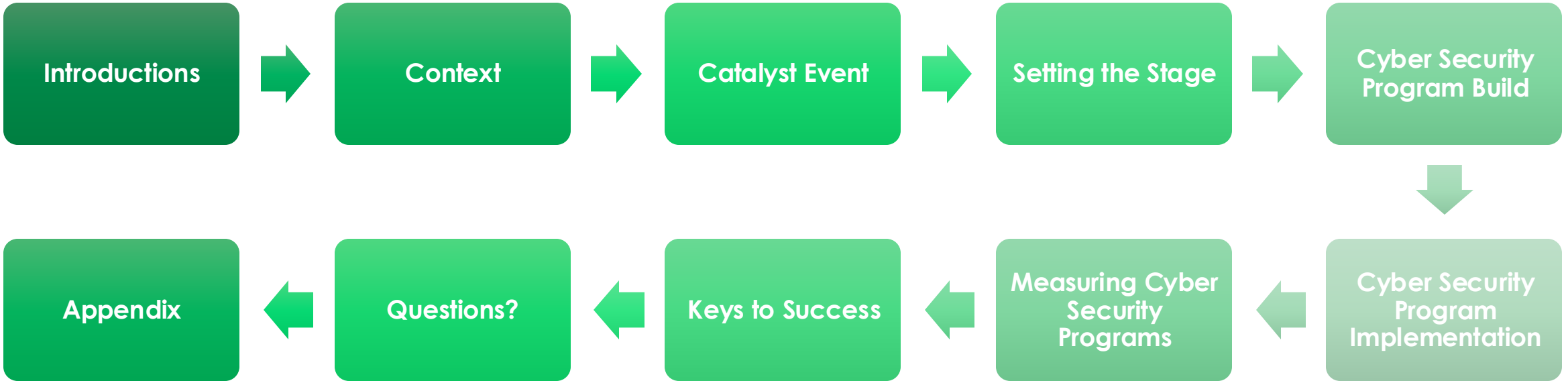
Defending Justice

Building Cybersecurity Strategies for the Modern Court

CTC KANSAS CITY 2025

HOSTED BY NCSC National Center for State Courts

Agenda and Flow



David Slayton

Executive Officer/Clerk of Court

Mike Baliel

CIO

Ofer Amrami

Deputy CIO Cyber Security (CISO)

The Context

The Justice System Role

- In every society/culture/organization, to maintain order, there is a system:
  - In Democracies – The System includes law enforcement and the Courts
  - In Corporations – The system includes HR, Legal and Unions
  - In tribal societies – The system includes the Elders Council
  - Even in criminal organizations – The systems includes an Arbitrator
- For a system to be effective and successful, the majority, if not all, must trust it.
- Trust, in the courts' case, does not mean I always win, it means I believe the process was fair and transparent.

CA Judicial Branch and LA Court Mission and Goals

- Fair, impartial and effective access to justice
- Protection of rights and liberties
- Independence and accountability
- Contributes to public safety and strengthen the rule of law
- Stewardship of resources

Trust – The Court's Currency

"The Court's only armor is the cloak of public trust"

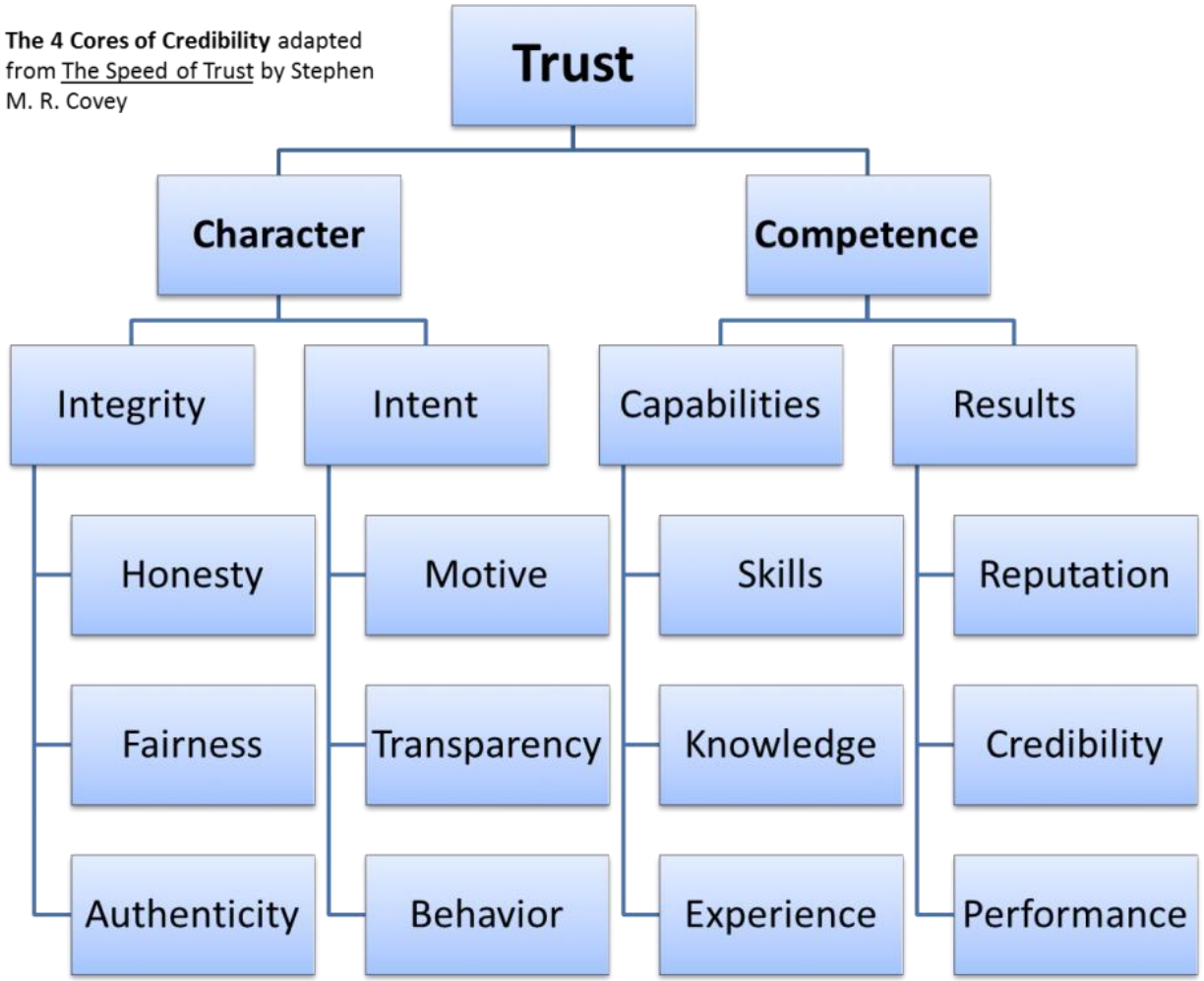
- Irving R. Kaufman

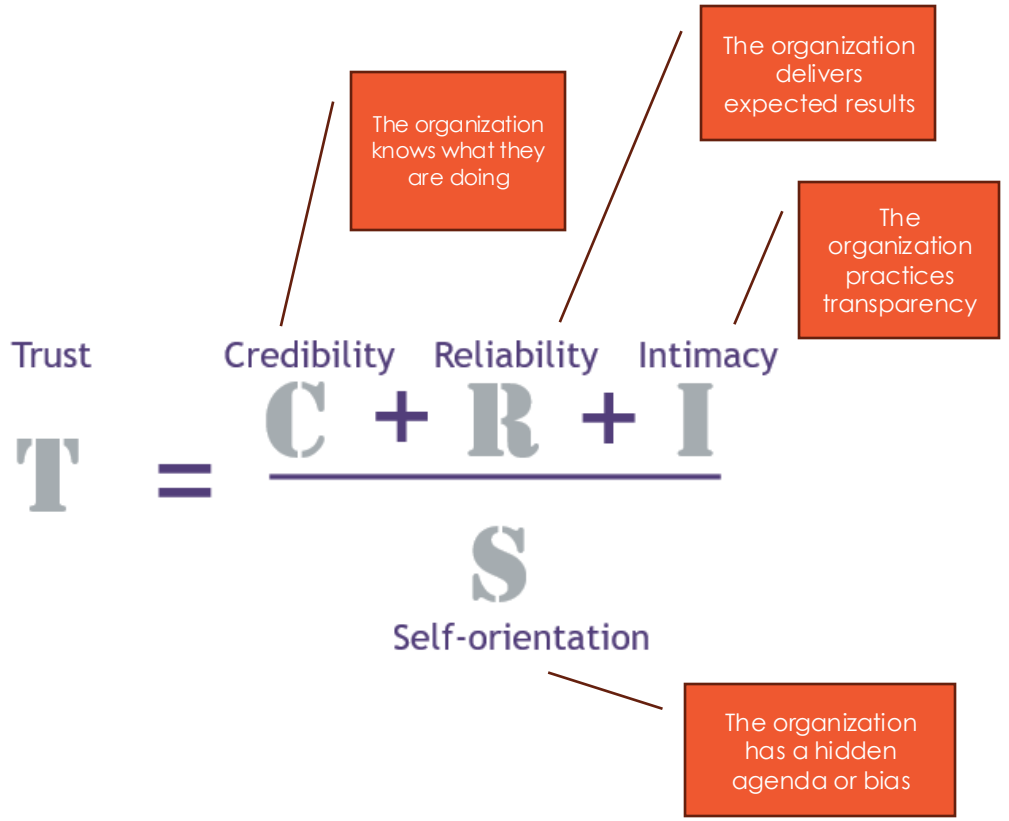
"Trust takes years to build, seconds to break and forever to repair"

-Dhar Mann

What is Trust?

The 4 Cores of Credibility adapted from The Speed of Trust by Stephen M. R. Covey





Cyber Security Goals and Objectives Cascade

- Maintaining Public's Trust:
  - Ensure the availability, integrity and reliability of technological systems and technology reliant business processes
  - Ensure a demonstrable, robust and transparent control environment to:
    - Safeguarding constituent's information
    - Preventing fraud and abuse
    - Ensuring privacy and security by design
  - Responsible use of public resource
  - Information sharing
  - Contribute to legislation and regulation

The Catalyst

May 30th to July 19th 2024

May 30th
Court hires its first security leader

June 28th
Gap analysis is completed

July 2nd
Charter, initial strategy and operating plan drafted

July 3rd
First operational decisions made, and work started

July 17th
Leadership approved program to launch, initial budget allocated

AND THEN Came July 19….

News Report

Incident Timeline

- On July 19th 2024, 6:15 am, during the world-wide Crowdstrike Outage, the Court investigated an alert about a ransomware process detected on one of the Court's laptops
- At 7 am the security team observed multiple encryption processes in progress across our environment
- Around that same time, we received the first report of a ransom note left on a few of our laptops
- Around 7:15 am the Court activated its incident response retainer and plan
- The attack was contained around 4:30 pm on Friday and eradication and recovery efforts began shortly after.
- Around that time, we concluded the initial investigation and attributed the attack to Blacksuit, a ransomware operator out of Russia.
- The group's tactics, techniques, and procedures were identified and mapped over the weekend, at which point, information was shared with partner agencies.
- In total, around 2000 Court devices were impacted, including all of the Court's server environment

What contributed to the attack?

- The attack began with a stolen credential obtained from a credential broker in the dark web. Those credentials were obtained in a separate event that went unnoticed a few months earlier and through a critical known zero-day vulnerability on one of the Court's edge devices.
- Strong authentication was not yet in full use
- The Court was in the beginning phases of replacing its endpoint protection tool with a modern tool: Crowdstrike
- The attack occurred at the same time as a significant security tool outage worldwide
- Limited visibility for internal movement and indicator of attack/compromise

What went right?

- The Court had a strong backup in place
- Decision making of the leadership team:
  - Disconnect all network access to the court (including VPNs)
  - Prioritize forensic examinations and build a strong containment and eradication plan
  - Re-image and restore based on a priority list dictated by court leadership
- The Court leveraged pre-established partnerships with an incident response provider and various support vendors as well as relationships with law enforcement agencies and partner agencies
- Communication, internal and external, and information sharing
- Court employees and leadership cooperation
- The attack occurred on a Friday allowing the Court 2 full days of no public pressures

Results

- The attack was contained within 10 hours, the attackers and their tools were eradicated from all systems within 72 hours.
- The Court mission critical operations were back online within 5 days and fully within a 10 days. The Court was closed to the public for only 2 business days.
- Recovery tasks to resolve damages resulting from the attack continued through August
- No data was exfiltrated and financial\reputational damages were kept low in consideration to the size of the attack
- Cyber Security Program build accelerated

Setting The Stage

Or “What do I need to consider?”

Let's Start by Acknowledging and Accepting

- Budgets are tight and resources are limited
- Skills shortage
- Cyber Arms Race in progress - AI is supercharging attacks
- Regulation is lagging behind
- Cyber Security is often viewed as a necessary evil or a pure cost of doing business
- Court data is mostly public data (…or is it?)
- **We will be hacked and/or breached**
- Human Nature is a powerful thing
  - "It is human nature to think wisely and act in an absurd fashion" (Anatole France)
  - "Human action can be modified to some extent, but human nature cannot be changed" (Abraham Lincoln)

Human Nature

Questions to Ask Yourself and Your Leaders

What is Cyber Security's role in achieving the Court's mission, goals and objectives? Is Cyber Security a cost center or a Court enabler?

Is Cyber Security a technology function only or a Court wide function?

Is it enough to just check the regulatory box?

What is an effective defense strategy? Is risk transfer an effective strategy?

Are we looking far enough into the future of justice and technology intersection? Legislative and regulatory?

How do we impact real change to human nature? Organization Culture?

Program Development and Build

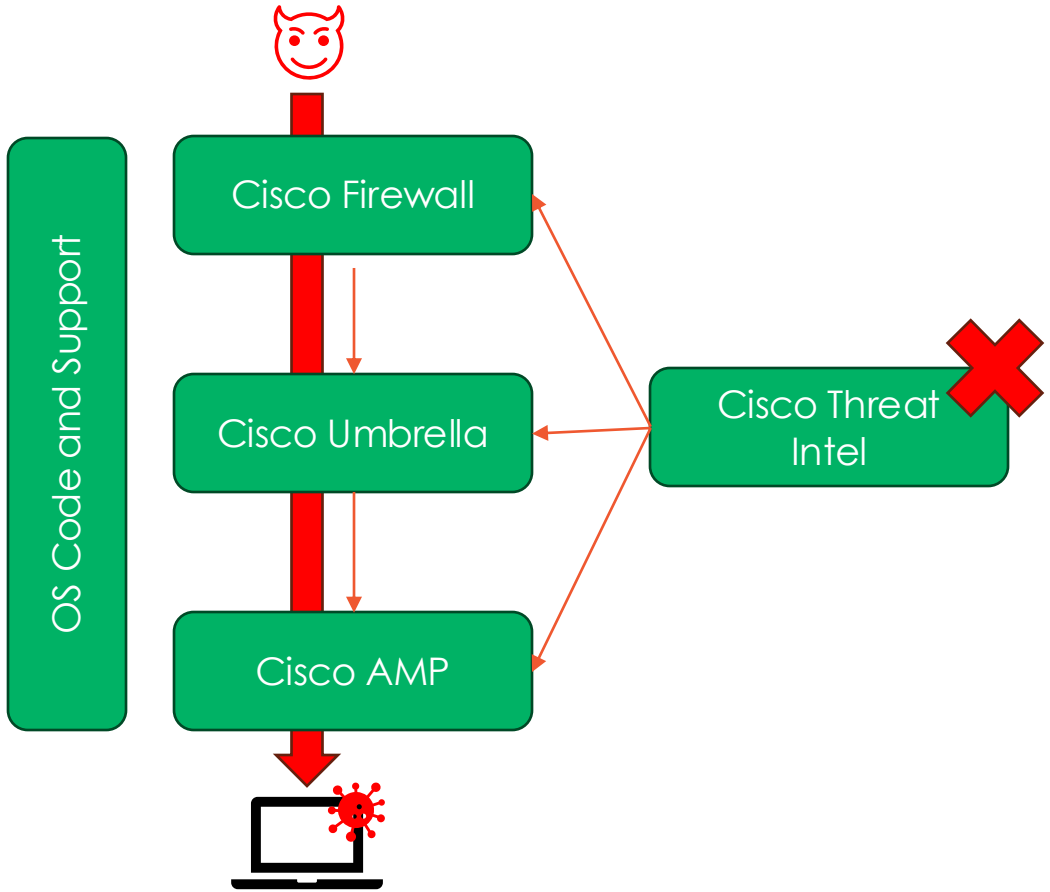
Or “How do I never have to go through this incident again?”

Approach to building a program

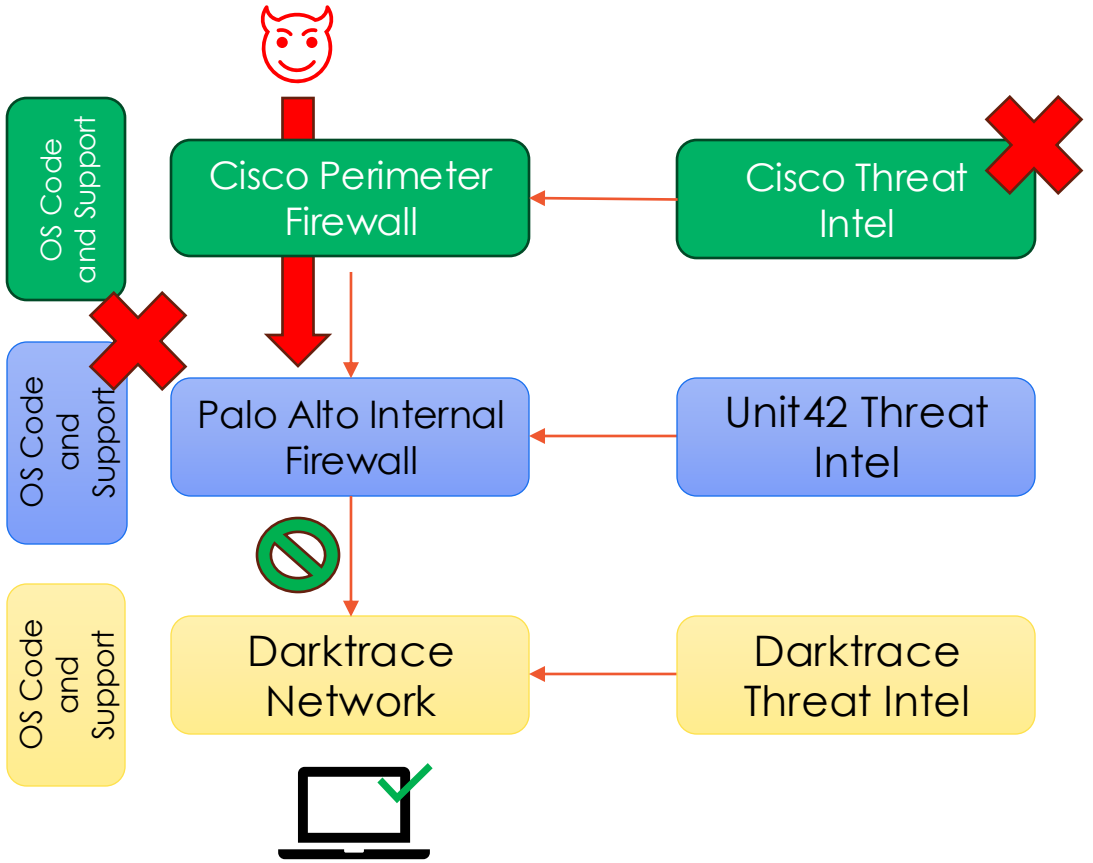
- Building a program is a multi-year process
- Simplification is crucial
  - Leaders and staff do not support what they do not understand – make sure you understand it first
  - Avoid buzz words, fear and fud
  - Governance and transparency facilitates simplification
- Build a program based on a strong foundation
  - While technology changes fast, a good foundation will ensure agility and scalability
- Ensure layered defense and diversity of tools – Platform vs Best of Breed
  - Eliminate single provider failure point
  - Different technologies, approaches and intel sources
- Look for the "Free" and Reliable
  - There are plenty of no/low-cost services from government agencies as well as grants
  - Use existing skills and resources in your organization – many IT staff love to add security tasks to their roles (but check with labor relations….)
- Awareness is key – Leadership, Judicial Officers, Court staff and IT
  - Start by learning the operations – understand the possible risks each area is facing
  - Outreach and educate often
- Visibility is King
  - You cannot protect what you cannot see or do not know about
  - You also cannot protect what you do not control - Eliminate Shadow IT
  - Visibility is not only in tools and devices, but also in processes
- Consider impact to others
  - A balanced program works for all
  - Programs that are too tight will be circumvented
  - Ask "how can I enable this" instead of "how do I block this?"

Platform vs Diverse – Network Security Example

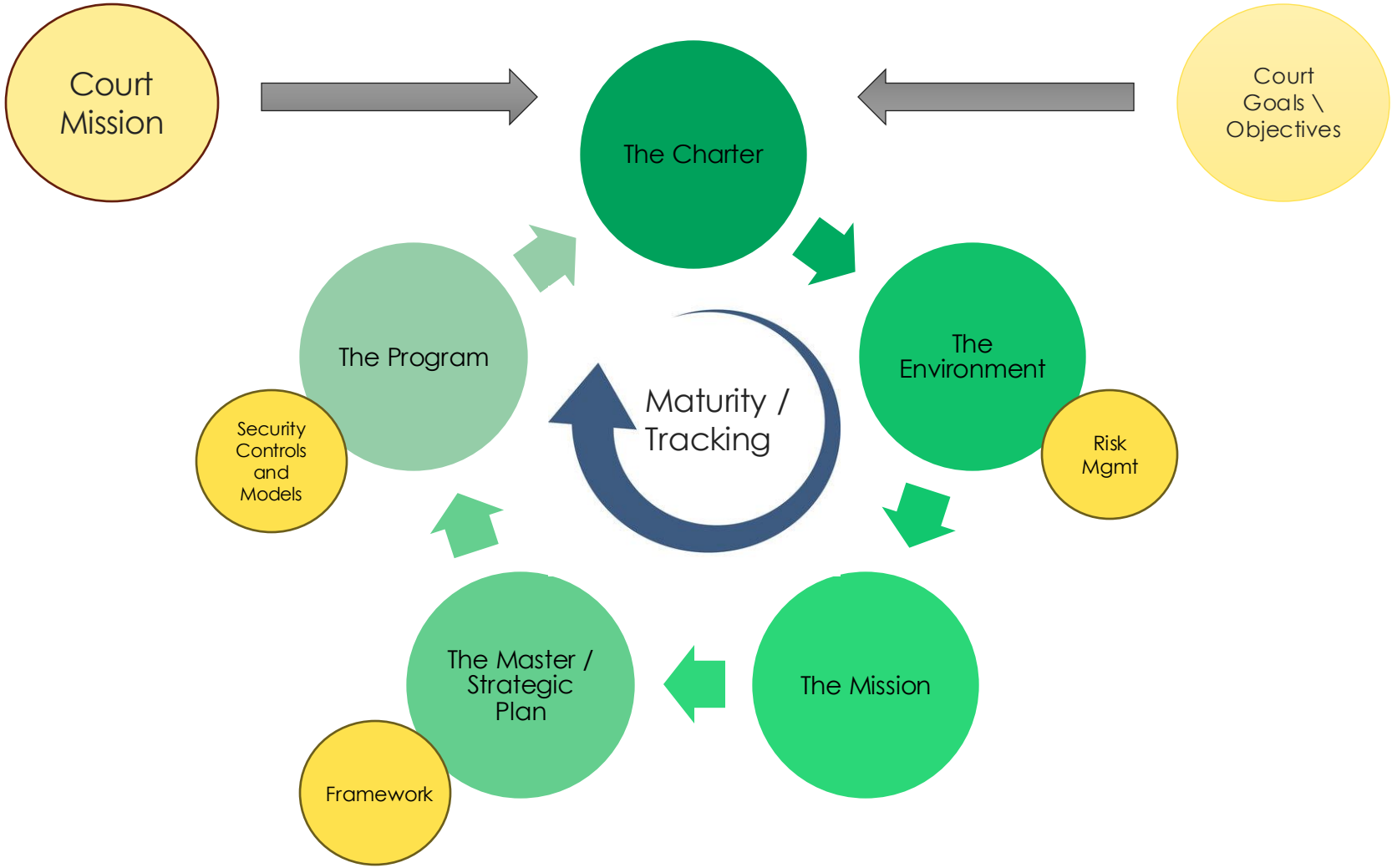
Platform Approach – Before Attack



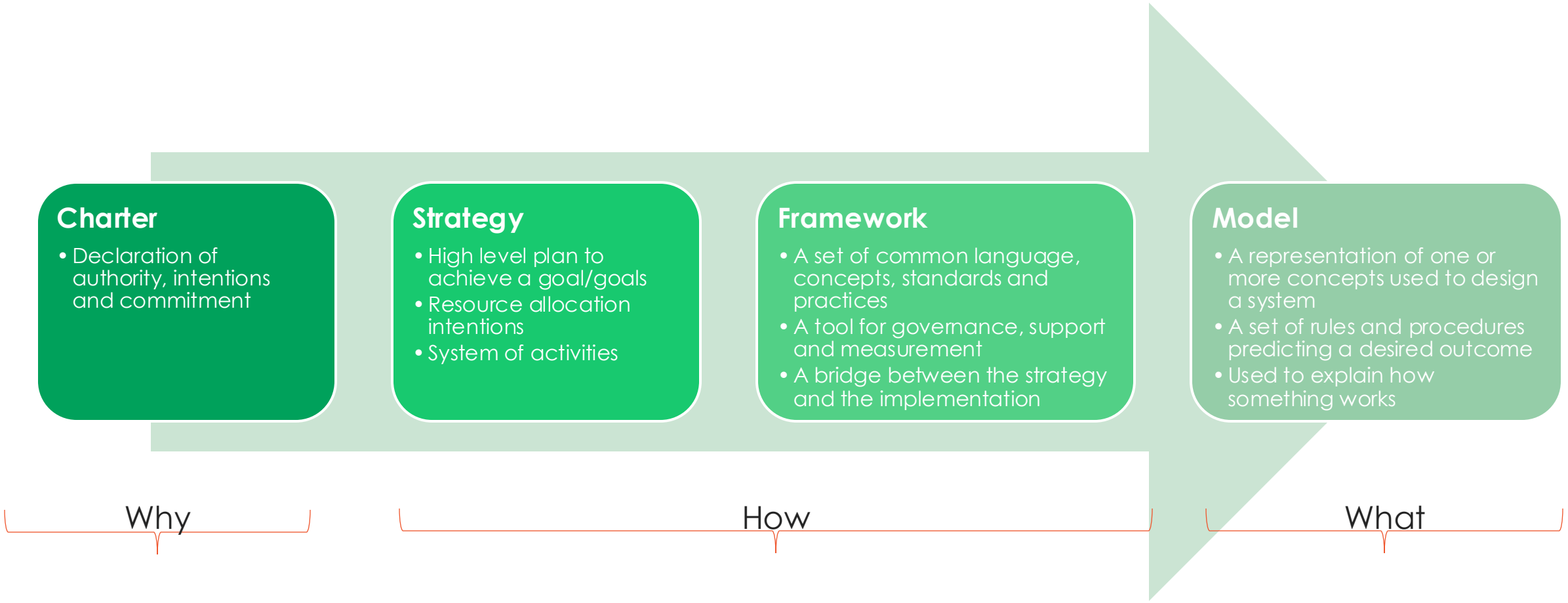
Diversified Approach – Post Attack



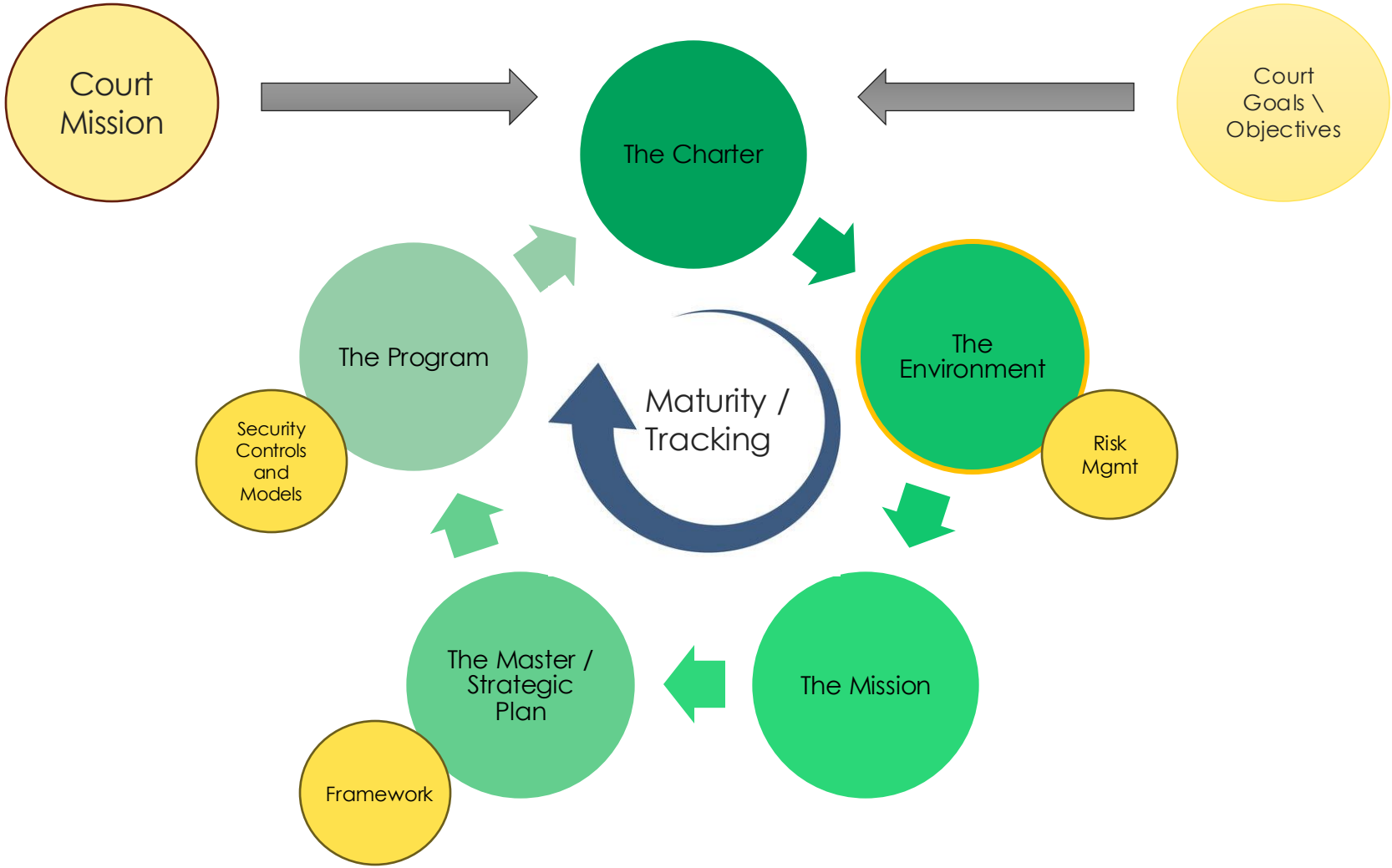
Cyber Security Strategy and Program Build



Charter, Strategy, Framework and Models



Cyber Security Strategy and Program Build



The Environment – 4 Key Pillars

01

Know what is important

- Crown Jewels
- Risk Appetite and Tolerance
- Mission, Critical Goals and Objectives
- Operating Environment:
  - Mandates and Directives
  - Regulations
  - Policies and Procedures

02

Know what you have

- Assets and business processes
- Criticality – Processes and data
- Skills
- Security Tool Stack

03

Know what you are up against

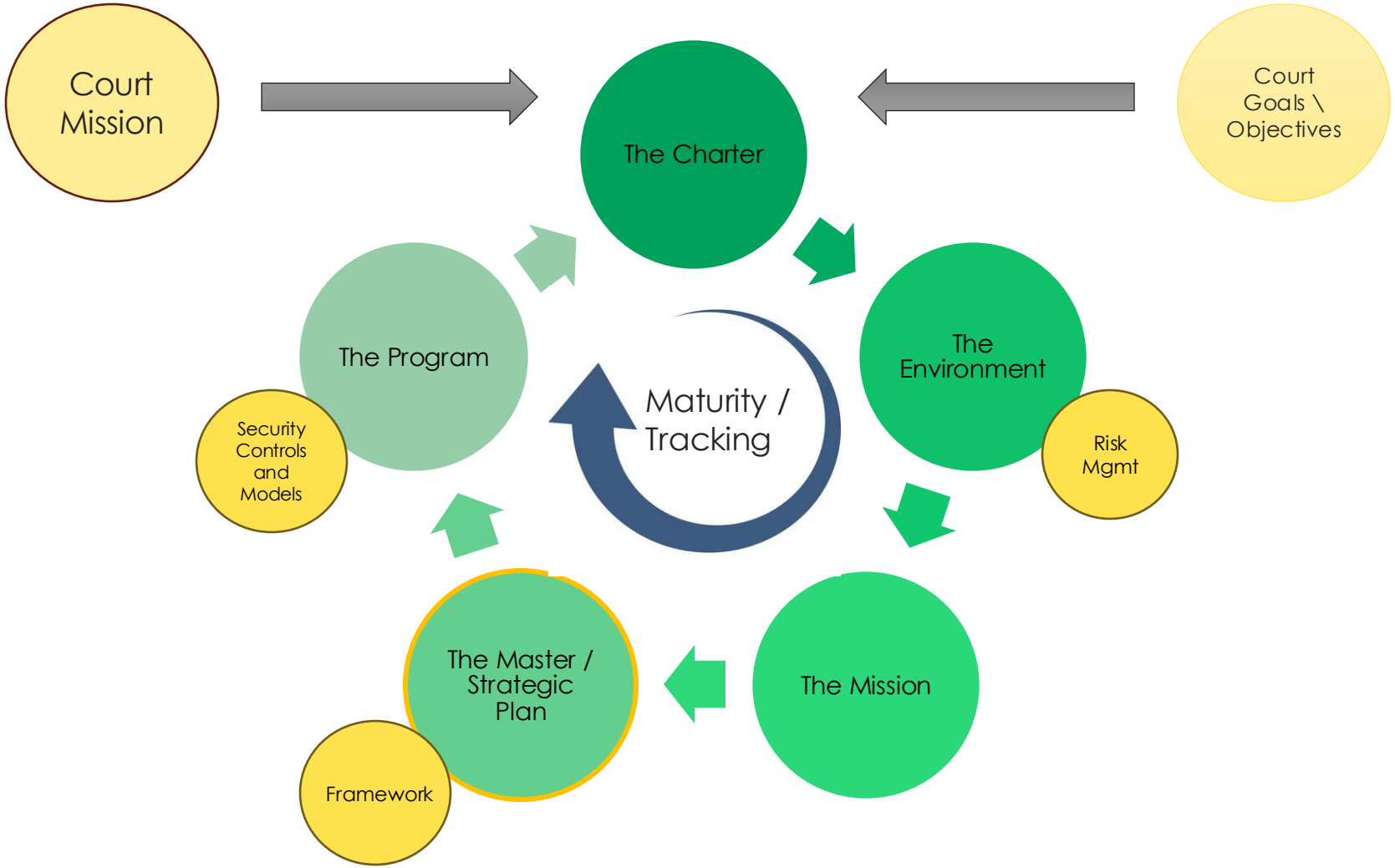
- Adversaries' Intentions
- Adversaries' TTPs – Tactics, Techniques and Procedures
- Geolpolitical environment

04

Know your weaknesses

- Vulnerabilities and exploits - Real vs Perceived – Systems and Processes
- Blind Spots
- Impact Analysis - Recovery and business continuity

Cyber Security Strategy and Program Build



Master/Strategic Plan

Key Goals – 2-3 long term intentions that support the goals of the Court

Key Strategic Objectives – Focus on 4-5 broad themes supporting the goals

Key initiatives – High level project areas within each objective realm

Example of Strategic Objective and Initiative

Proactive Risk Management

Initiatives that support this objective will allow data owners and administrators to be aware of the security risks that their information assets are vulnerable to, identify controls to reduce those risks, and understand what risks remain after any identified controls have been implemented.

Strategic Objective

Cyber intelligence

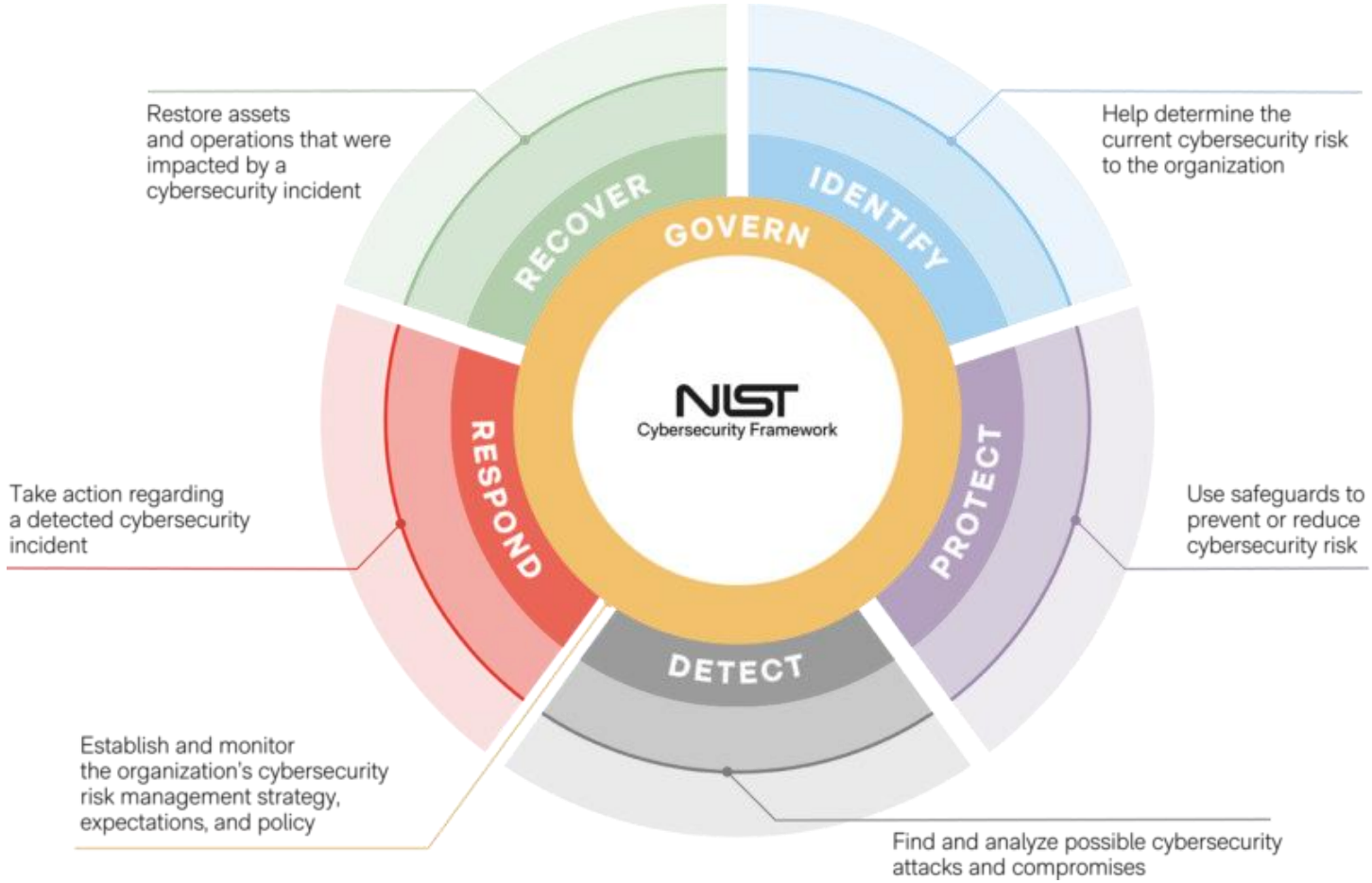
The objective of a Cyber intelligence program is to generate actionable information used to better assess Los Angeles Superior Court and its officers' security posture and improve controls to protect against current and emerging threats. Data collected will be analyzed and disseminated when and where applicable and developed into changes and improvements to existing controls or contribute to the introduction of new controls.

Employee Information Security Awareness

The objective of the employee awareness program is to extend information security task and responsibility to every member of the Los Angeles Superior Court team. All employees will be trained on current information security risks and threats as well as information security best practices. Training will be provided on a bi-annual basis as well as ad-hoc communications covering recent events in the information security field will serve as a reminder and refresher. Management will evaluate the effectiveness of the awareness efforts utilizing a quarterly security simulation including phishing and various social engineering techniques.

Strategic Initiatives in support of the Objective

NIST Cyber Security Framework 2.0



6 Core Functions

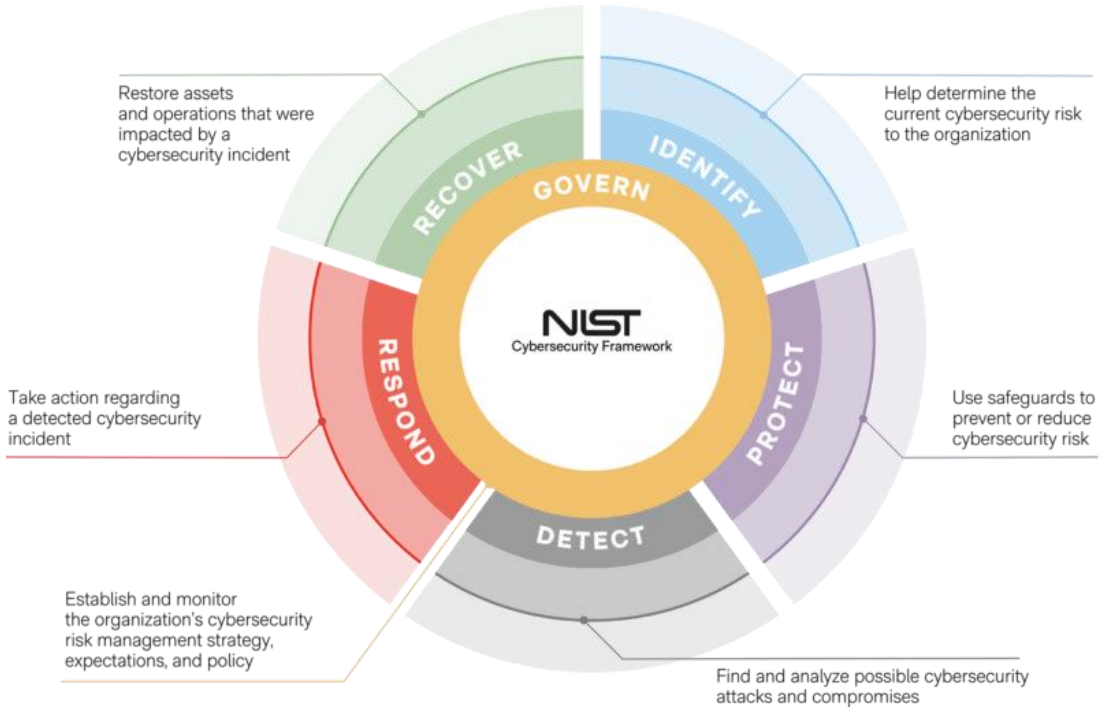
22 Categories

107 Controls

Gap Analysis/Risk Assessment

- Where you are vs. where you want to be
- Interviews:
  - Not just technology
  - Not just leadership
  - Not just employees
- Data Collection:
  - Policies and Procedures
  - Diagrams
  - Technology and Business Process Documents
    - If there is an informal process, document it
  - Past assessments
  - Tool reports – Capabilities, Coverage, Configuration
  - Logs and Alerts
- Maturity Assessment
  - Select a framework that fits your organization (NIST, ISO, CIS, etc.)
  - Select a maturity model (CMMI, PEMM, etc.)
  - Define your desired end point

Technology General Controls



89 CTS General Controls (LASC TS GCE)

The controls are comprised of policies and procedures the Court will need to implement to manage risk and align with National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA) security frameworks.

Controls are categorized into groups called **Control Types**. Each control will have one Control Type:
Entity Level – foundation controls that other controls are built on to ensure goals and objectives are met.
Logging and Monitoring – controls designed for visibility, troubleshooting and compliance.
Logical Access – regulate user access to systems, networks, and applications.
Change Management - manages and oversees changes made to the environment to ensure they are implemented effectively, without introducing security risks and with minimal disruption.
Data Security and Privacy – protects sensitive information from unauthorized access, use, disclosure, disruption, modification or destruction.
Operations - procedures, safeguards, and countermeasures implemented to protect information systems.

Deliverables

Mission Statement

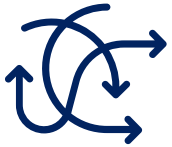
Why and How does cyber security contributes to the Court's mission?

Strategic Objectives

How does cyber security contributes to the Court's Goals and Objectives?

Cyber Security Modified Framework/Control Environment

How does cyber security track and measure development, progress and maturity?



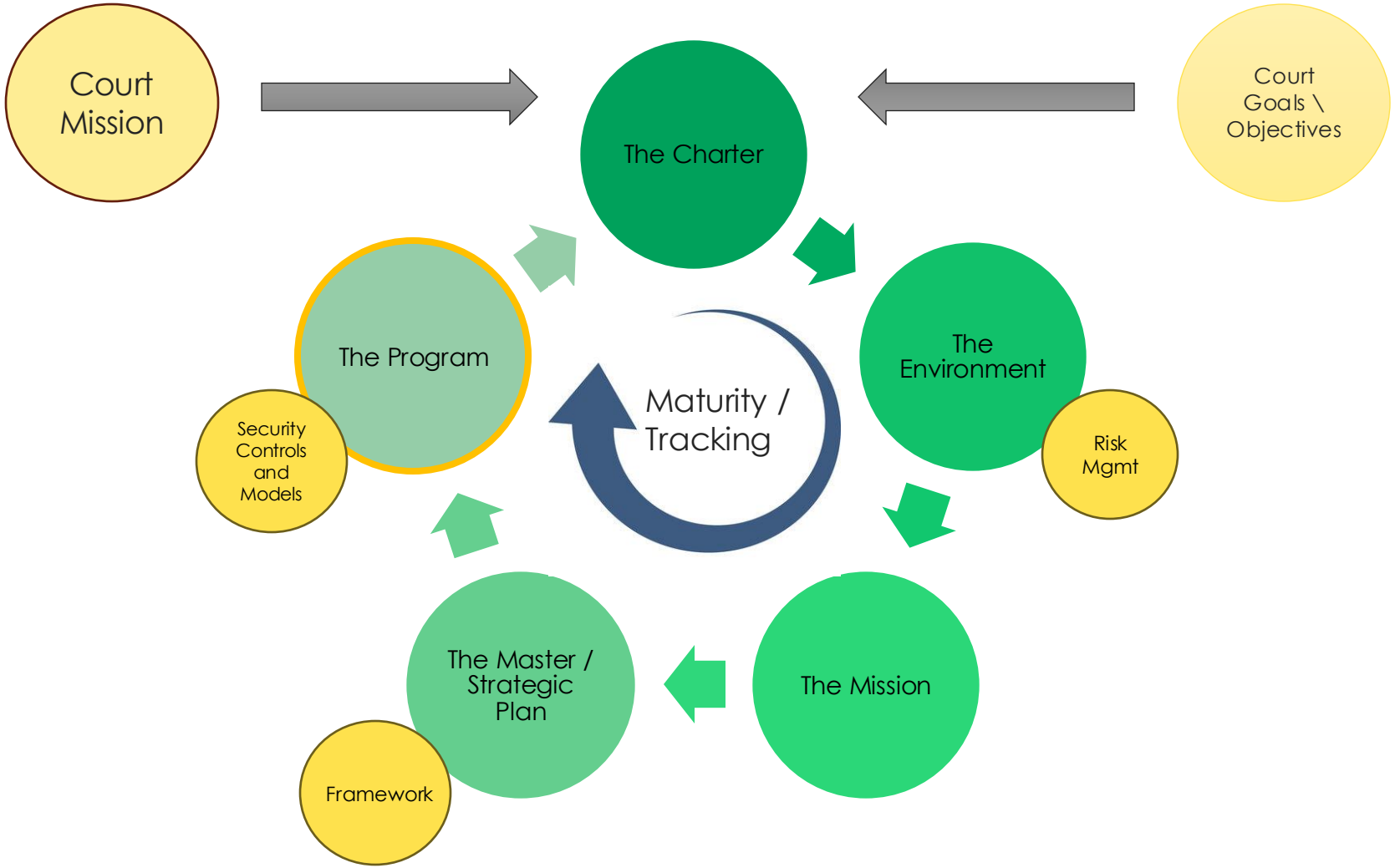
Gap Analysis

Where does cybersecurity want to be at the end of the program build and beyond?

Security Program Plan

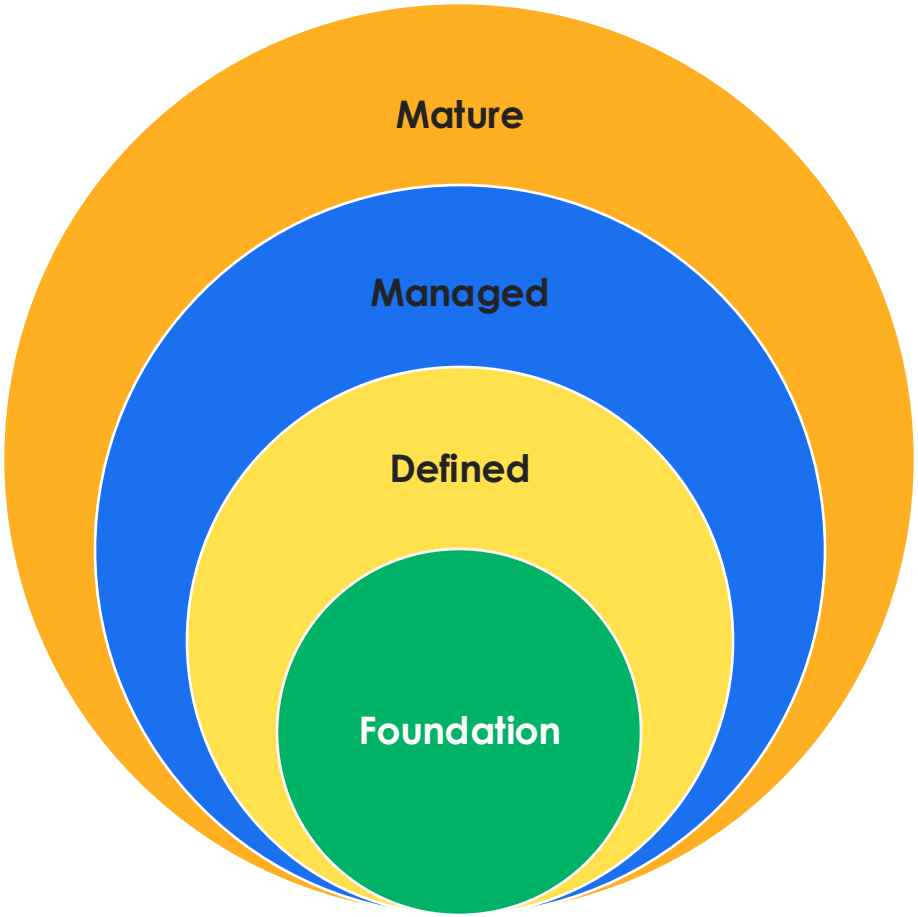
Remediation Plan/Project Plan/Budget Plan – Tactical list of programs to be built, projects to be initiated and budgets/resources needs

Cyber Security Strategy and Program Build



Cyber Security Program Development

Each level is not exclusive, work across levels

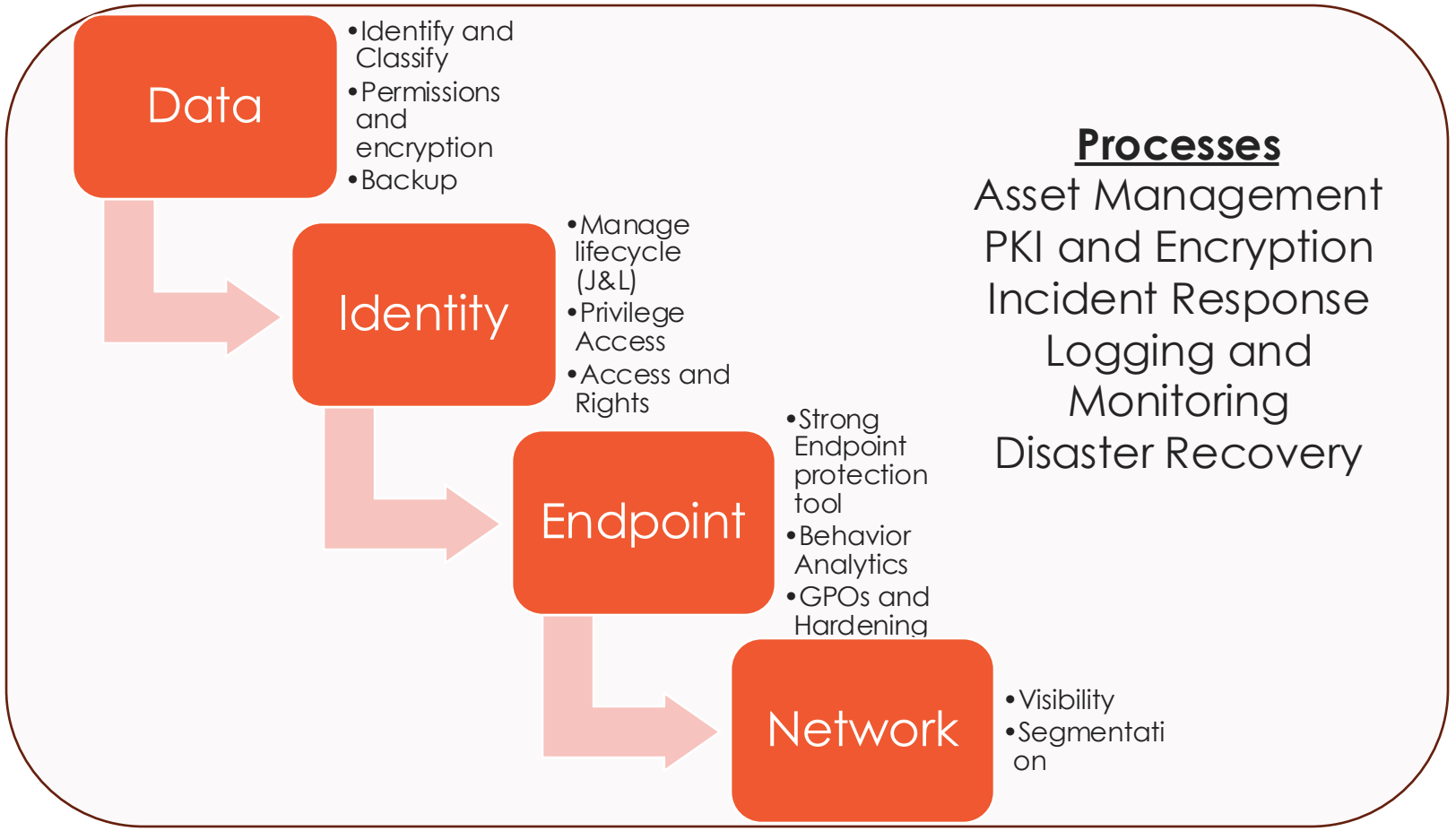


Not all areas must get to mature level

Foundation – Cyber Hygiene

- Visibility - Asset Management, Classification, Detection, Logging and Monitoring
- Identity and Authentication - Password/Passwordless, MFA and Privilege Control
- Appropriate basic tools – Endpoint protection, next-gen firewalls, etc.
- Initial Network Segmentation
- Basic Incident Response and Recovery
- PKI and Encryption Capabilities

The Foundation Processes and Tools



Defined Cyber Security Program

- Framework Controls and Models Adjustment
- Targeted Risk Assessment and Prioritization
- Incident Management
- Awareness for leadership
- Identity Management and Access

Managed Cyber Security Program

- Governance – Policies, Processes, Standards
- KPI definitions
- Awareness for All
- Data Segmentation and control
- Identity Governance - Access, Authentication and Authorization

Mature Cyber Security Program

- Embed Security in Business Processes – Security and Privacy by Default and by Design
- Compliance and Audit
- Vendor Control
- Actionable Cyber Intelligence
- Reporting
- Continuous Improvement
- Capability Development

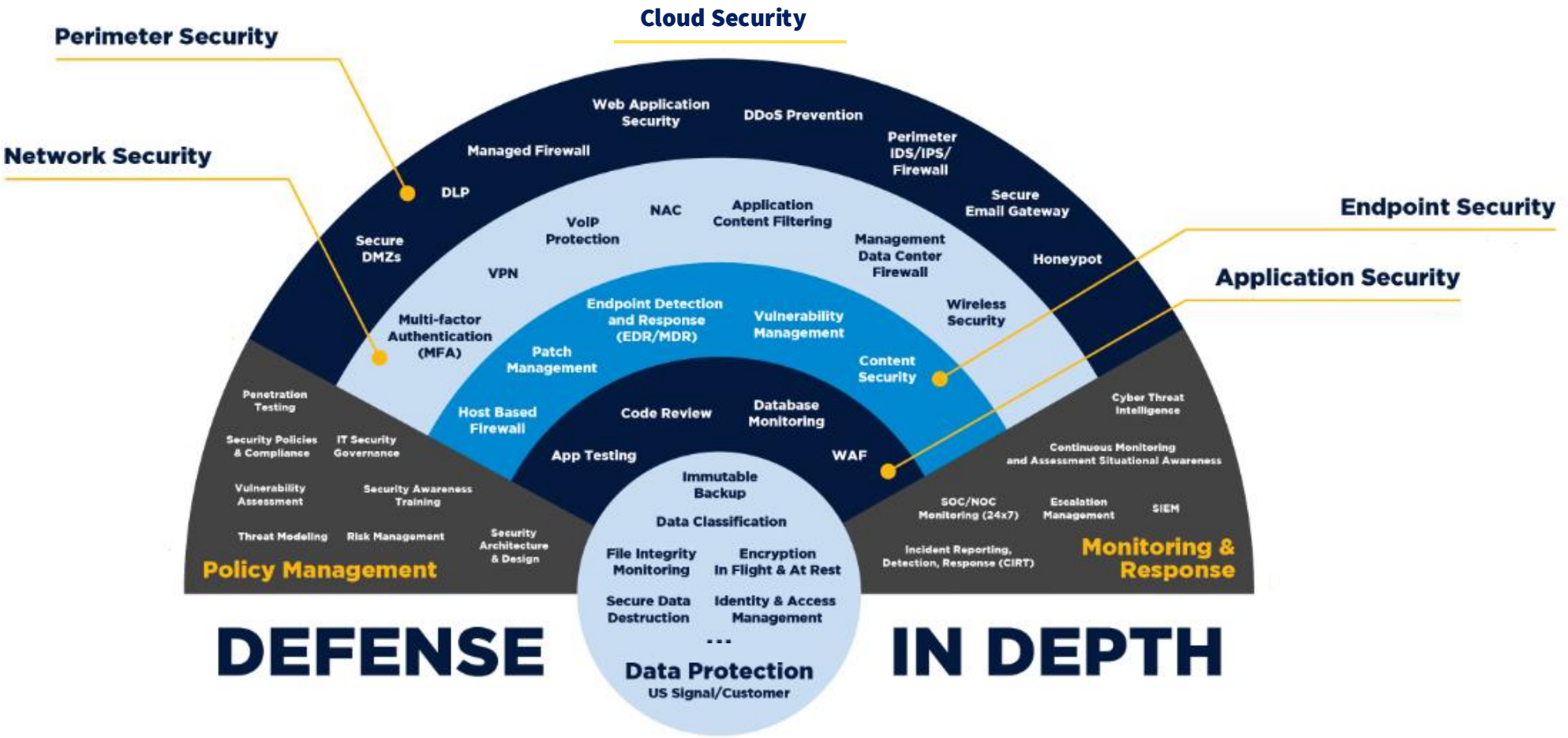
Security Models Implementation

Or “How do I communicate what we do?”

Defense in Depth Key Objectives

A Solution at each layer	Make it difficult to defeat multiple security processes and tools
Product Diversity	Eliminate a single point of failure by choosing best of breed from different vendors. Focus on integrations.
Ease of Management/ Use	Bring solutions in each layer to a single management layer and single pane of glass view. Reduce alert redundancy

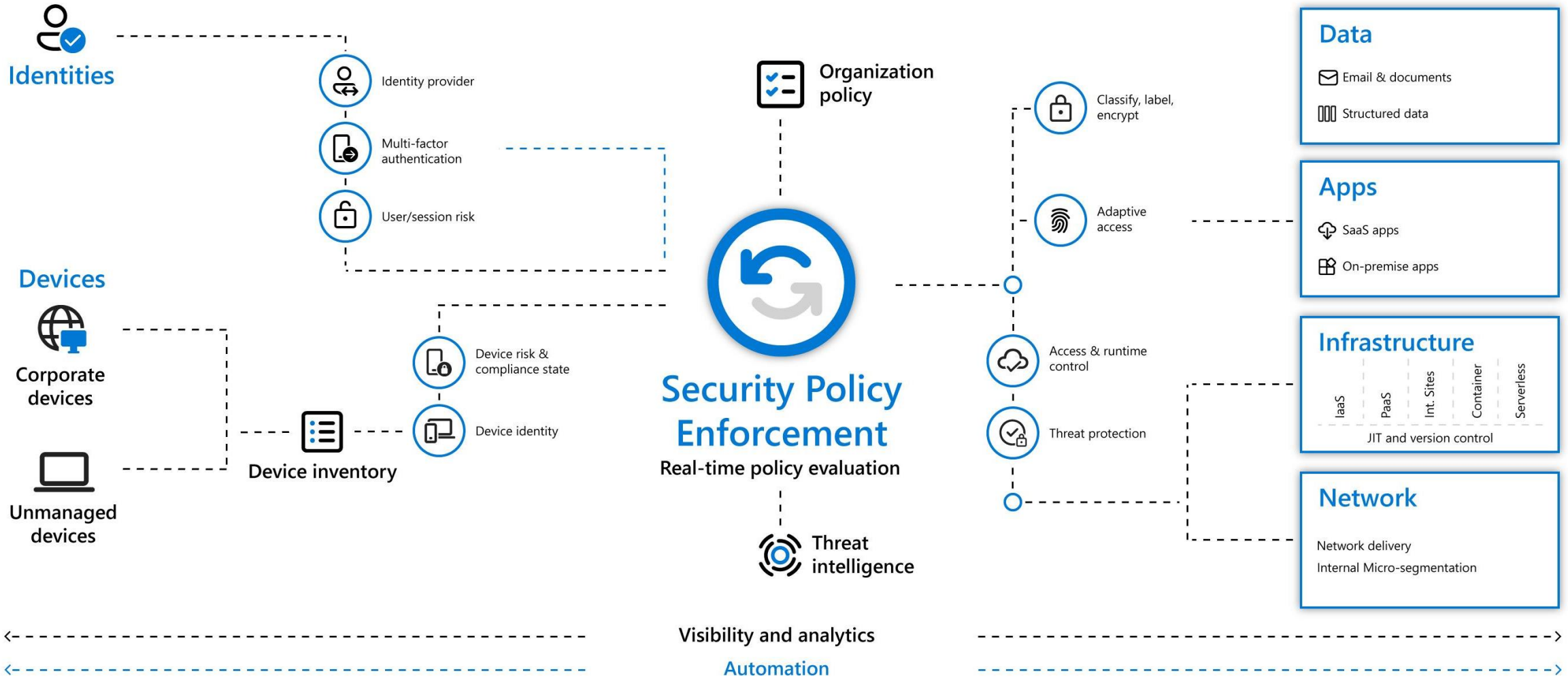
Defense in Depth Model



Zero Trust Key Objectives

Verify Explicitly	Always authenticate and authorize **based on all available data points**, including user identity, location, device health, service or workload, data classification, and anomalies.
Least Privilege Access	Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.
Assume Breach	Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

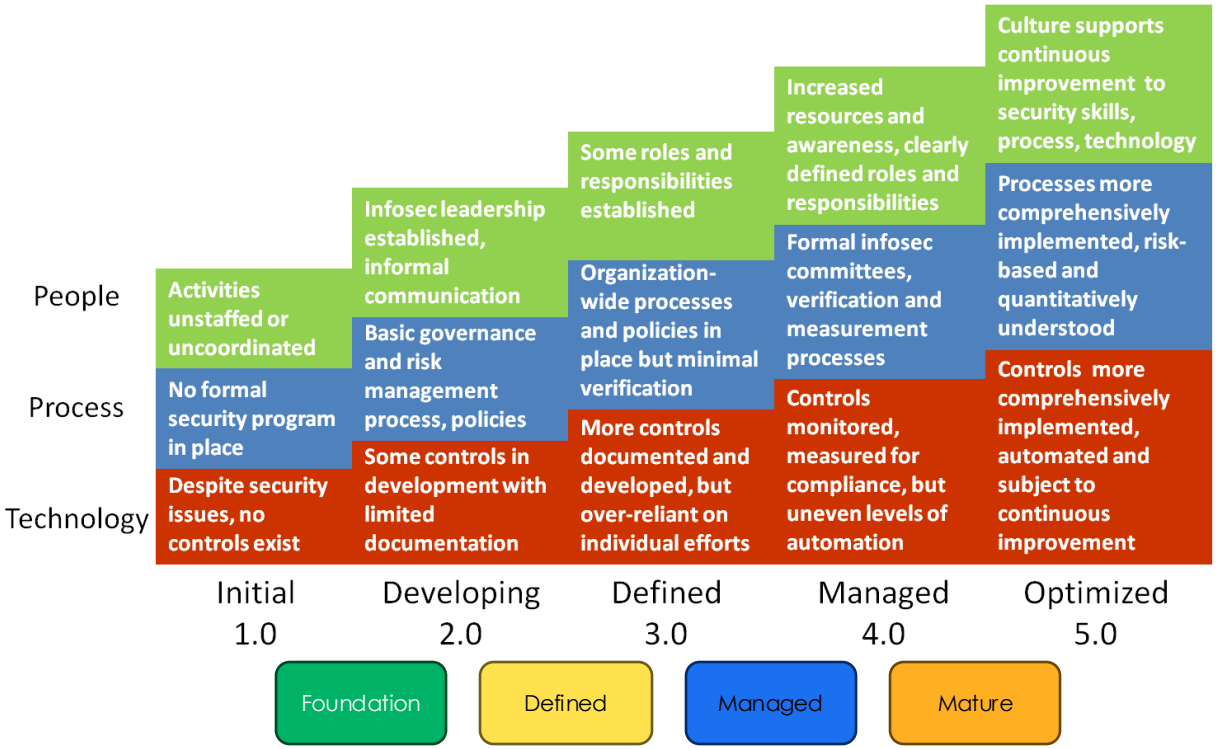
Zero Trust Model

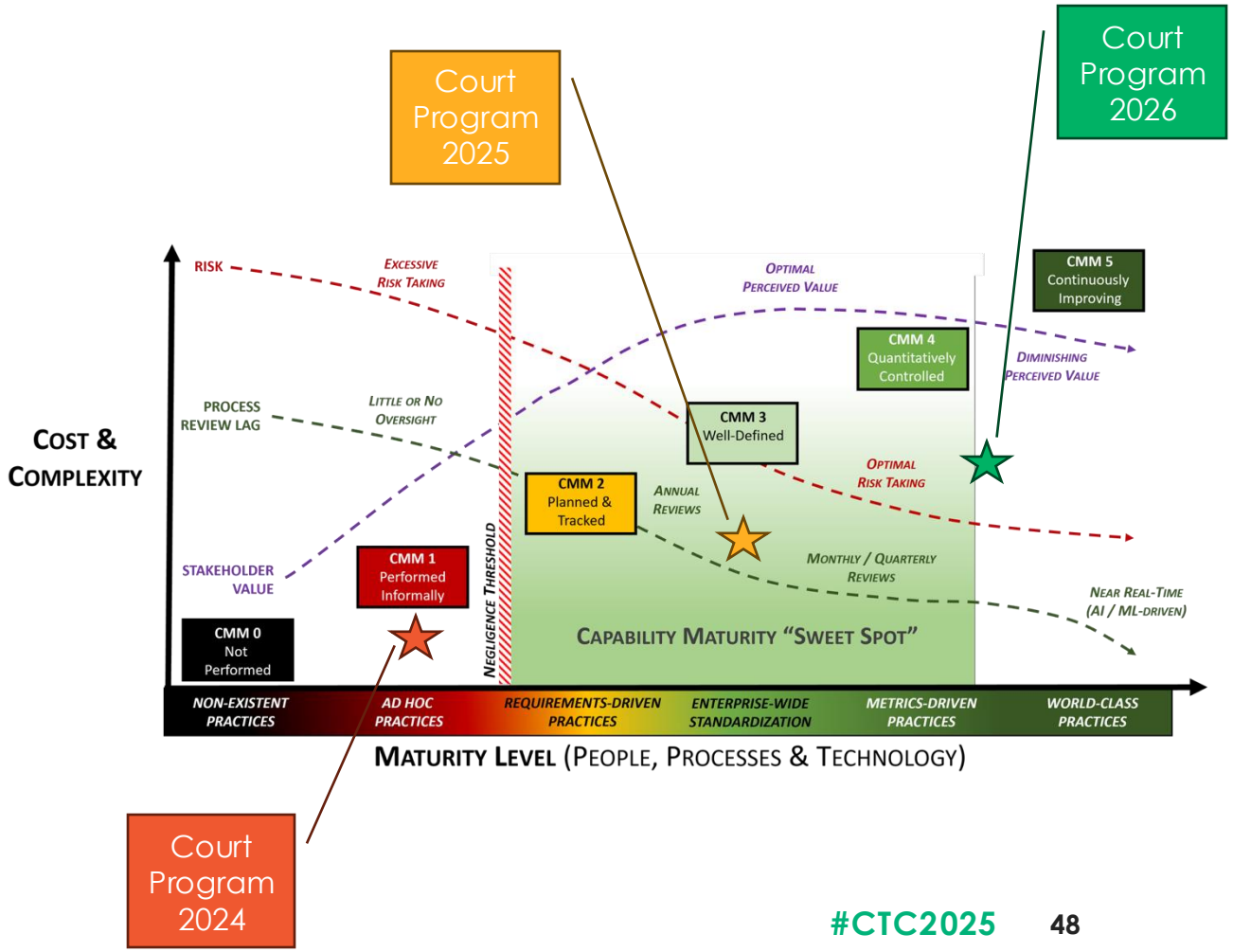


Measuring a Program

Or “How do I show progress and where we are?”

Maturity Levels - CMMI







Keys to Success

Keys to Success – CEO View

Invest in protection, but…

Prepare as when, not if

Don’t let convenience trump security

Communication

Stay calm

Keys to Success – CIO View

Preparation: Build Defenses Before the Attack Hits

- Develop and Test a Comprehensive Incident Response Plan (IRP)
- Implement Robust Prevention Measures (Tools and Policies)
- Assemble a Response Team and Forensic Capabilities (Dedicated Cyber Security Staff)

Response: Act Swiftly to Contain the Threat

- Isolate and Assess Immediately
- Communicate Transparently and Strategically

Recovery: Restore and Learn to Strengthen Resilience

- Eradicate, Rebuild, and Restore
- Conduct Post-Incident Review and Adapt

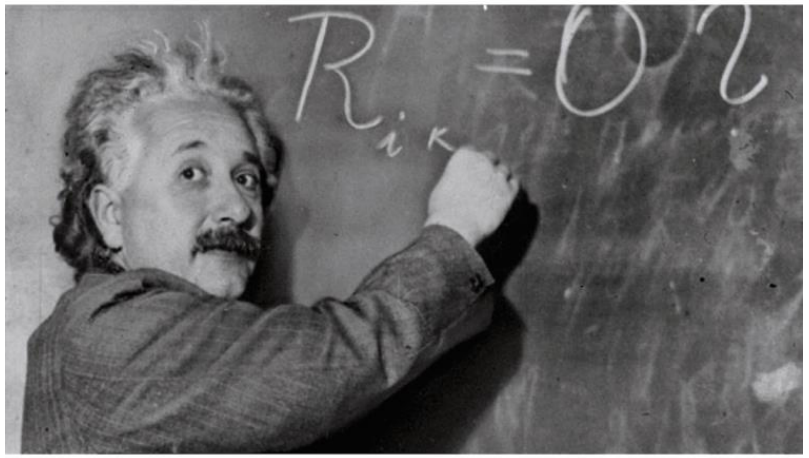
Keys to Success – CISO View

Create a journey focused on facts and risks

Be clear and concise

Talk about internal AND external

How I think I look explaining cyber risk to the board



How I actually look

Keys to Success

Be realistic about your resources

Look for the most bang for buck

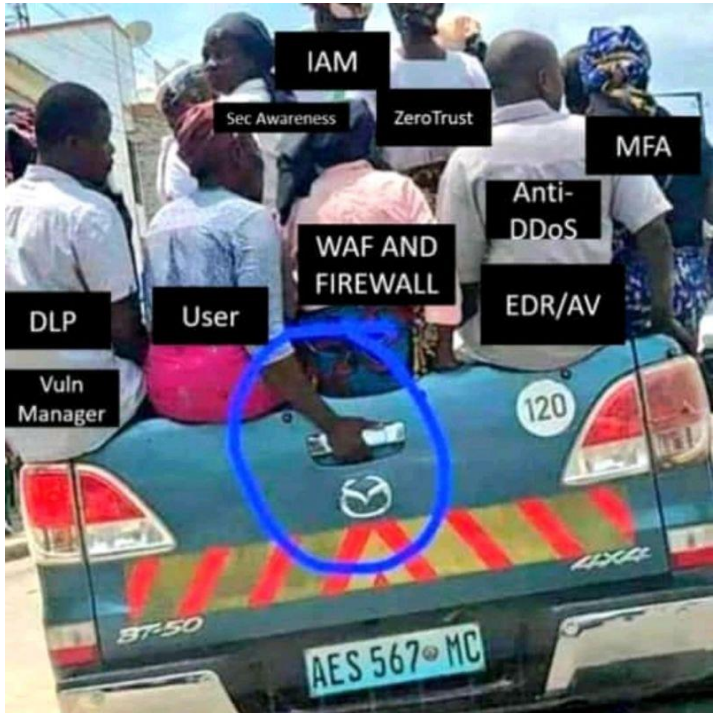
Define your “non-negotiables”

Build for purpose (ROI)

Keys to Success

Remember the human element:

Never underestimate what one user can do – unintentionally or intentionally



Keys to Success

Measure and demonstrate progress and efficacy

Document everything

Test, test and test again

Keys to Success

Solve the Skills Shortage with education and training, with services, or with AI

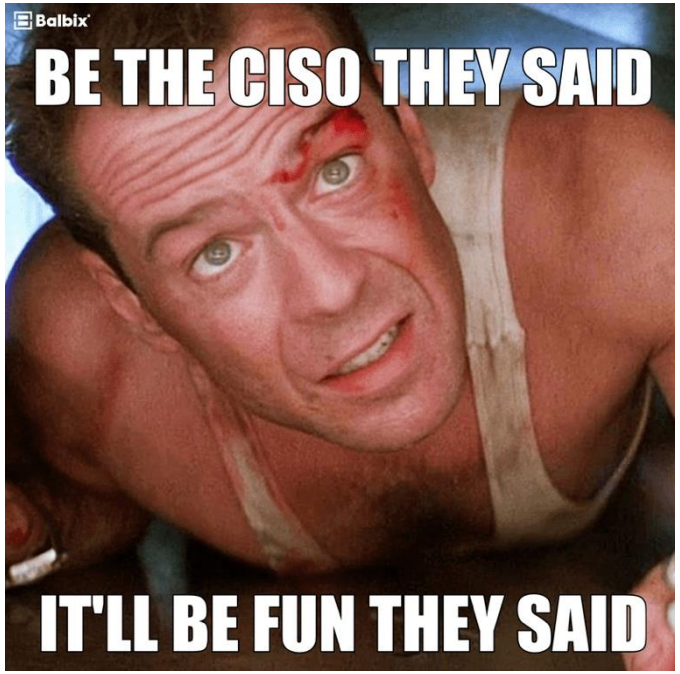
Look for personality attributes and attitudes (how fast can you learn)

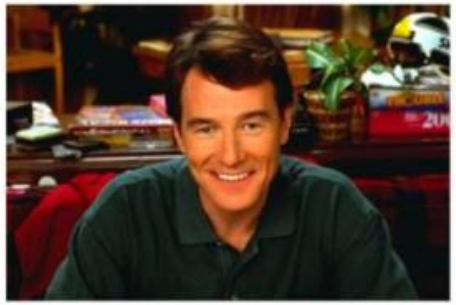
Exercise your staff regularly

In-House vs. Outsourced vs. AI

Final Thought

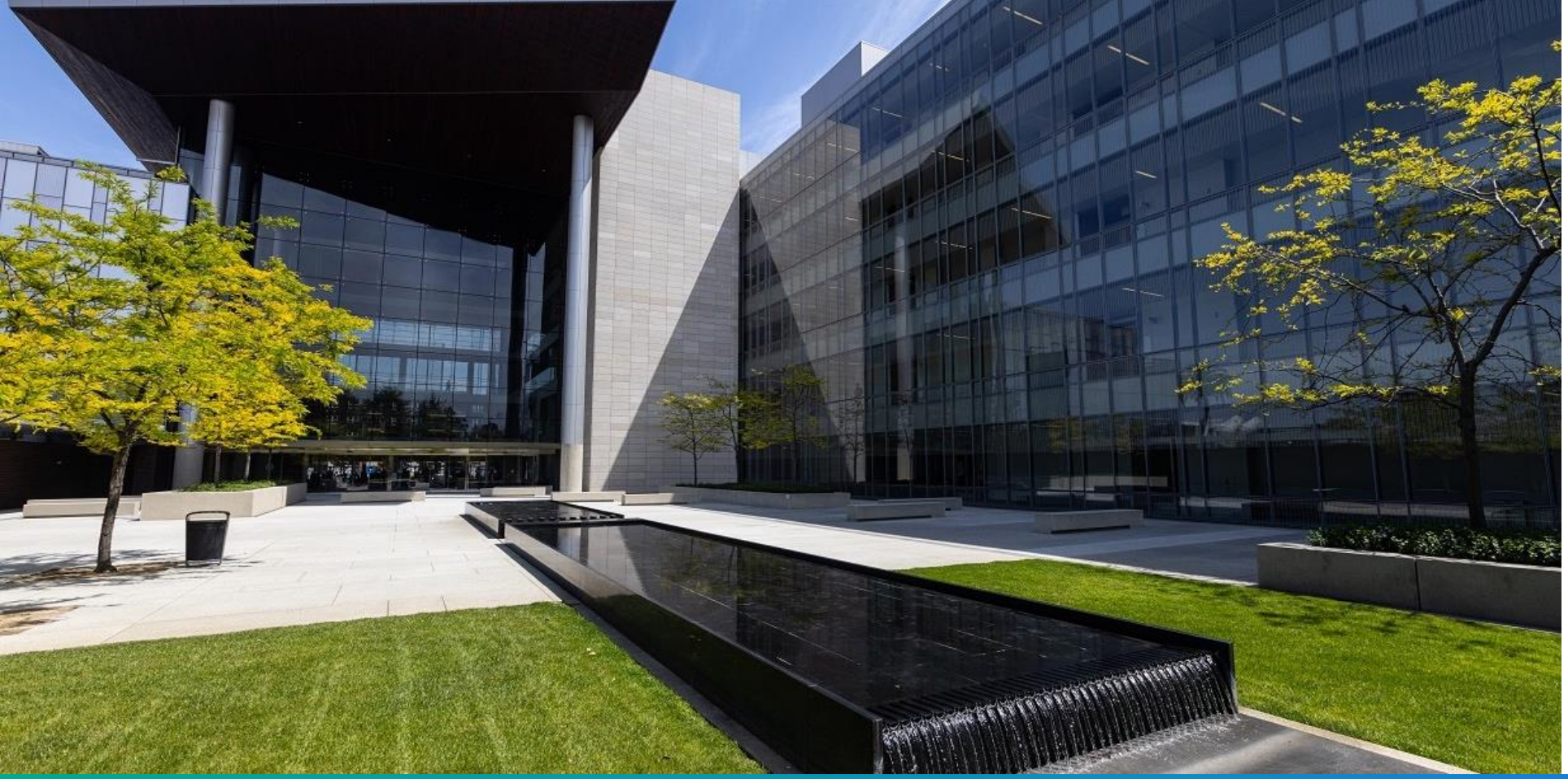
- Running Cyber is not easy, it is not meant to be. It is a state of mind, a culture and a commitment
- You will hit walls, sometimes more than once. Find your way around it or an alternate road to keep moving forward
- Be creative and resilient
- For non-cyber leaders, show your cyber team some love…





First day as a CISO

One year later



Ofer Amrami

Email: oamrami@lacourt.org

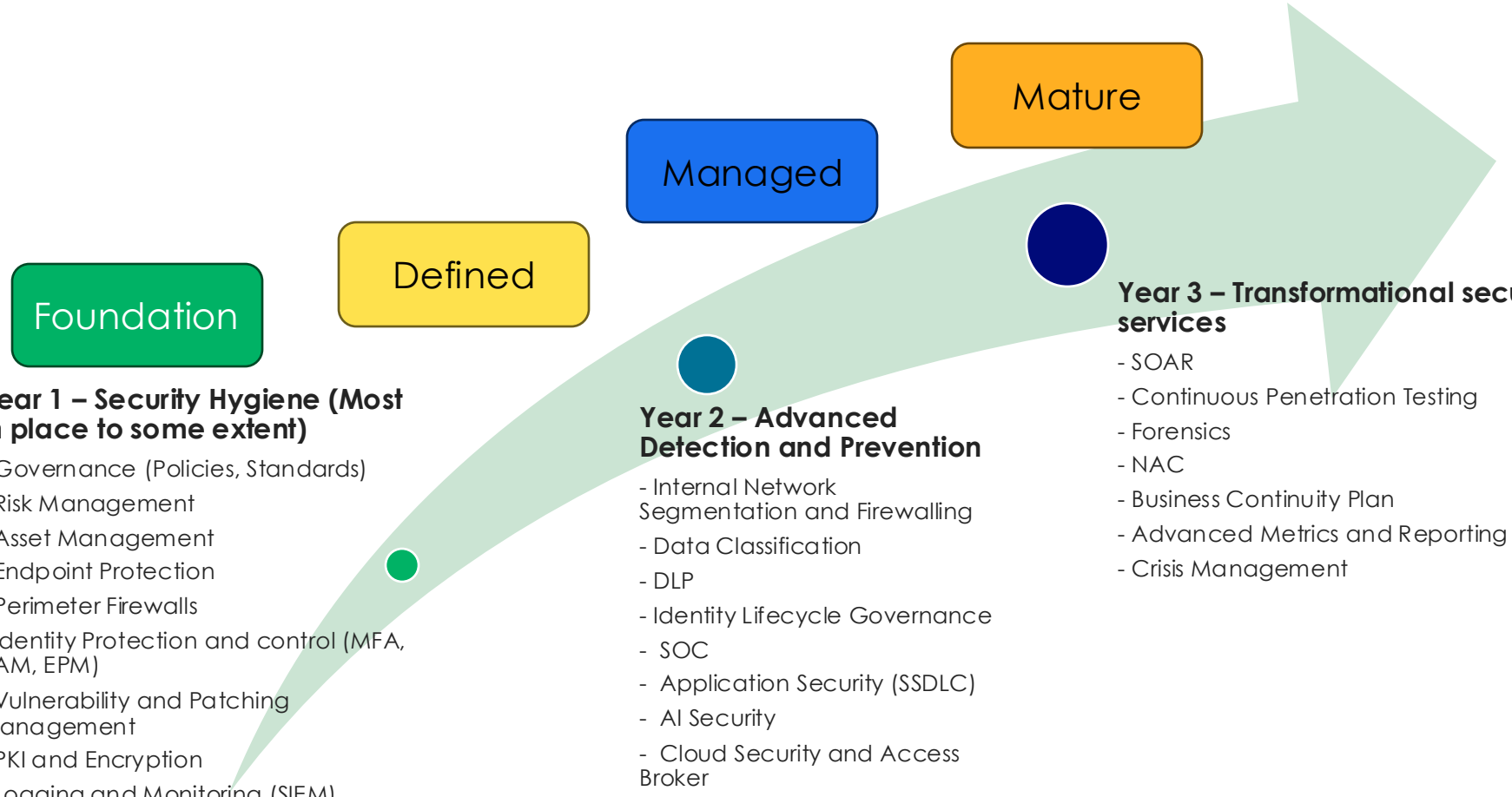
Office: 213-830-0288

QUESTIONS?

Appendix

Sample 3-Year Implementation

3-year model implementation



Year 1 – Security Hygiene (Most in place to some extent)

- Governance (Policies, Standards)
- Risk Management
- Asset Management
- Endpoint Protection
- Perimeter Firewalls
- Identity Protection and control (MFA, PAM, EPM)
- Vulnerability and Patching Management
- PKI and Encryption
- Logging and Monitoring (SIEM)
- Awareness Program
- Backup and Disaster Recovery
- Incident Response Plan

Year 2 – Advanced Detection and Prevention

- Internal Network Segmentation and Firewalling
- Data Classification
- DLP
- Identity Lifecycle Governance
- SOC
- Application Security (SSDLC)
- AI Security
- Cloud Security and Access Broker
- Dashboard and Reporting
- Tabletop exercises

Year 3 – Transformational security services

- SOAR
- Continuous Penetration Testing
- Forensics
- NAC
- Business Continuity Plan
- Advanced Metrics and Reporting
- Crisis Management

NIST Based Defense Model Implementation

Defense Model and Tool Stack

NIST Function	Stack Purpose	Components and Processes	Layer	Tool Family	Example of Tools
Govern	1. Strategy and expectations communicated and monitored	1. Risk Management 2. Policies, Processes and Procedures 3. Supply Change Risk Management	N/A	1.Enterprise Risk Management System 2.Enterprise Compliance System 3. Vendor/3rd Party Risk Management System	1.MetricStream, Workiva, Archer, **eRamba** 2.ServiceNow, SAP GRC, OneTrust, **eRamba** 3.UpGuard, ServiceNow, Archer, **Excel**
Identify	1. Cyber security risks are understood 2. Organization assets are understood -Assets include: hardware, software, data, systems, facilities, services, people and identities	1. Asset Management 2. Risk Assessments	Identity	1.Directory Services 2.Identity Discovery	1.MS Azure, Cisco DUO, OKTA 2.CyberArk, BeyondTrust, Delinea
			Data	1.Data Classification and Labeling	1.MS Purview, Cyera, Varonis, Fortra, Secuvy
			Application	1.Application Inventory/License tracking system 2.SAST/DAST 3.Vulnerability Management 4.Penetration Testing	1.ServiceNow, BMC, Ivanti, **OCS, Snipe-IT** 2.VeraCode, Checkmarx, SonarQube, Miggo, **GitHub, Aikido** 3.DDI, Qualys, Rapid7, **OpenVAS** 4.Fortra CoreImpact, Rapid7 Metasploit, Pentera, **Kali**
			Endpoint	1.Asset Management System 2.Vulneratbility Management 3.Penetration Testing	1.ServiceNow, BMC, Ivanti, **OCS, Snipe-IT** 2.DDI, Qualys, Rapid7, **OpenVAS** 3.Fortra CoreImpact, Rapid7 Metasploit, **Kali**
			Network	1.Asset Management System 2.Vulneratbility Management 3.Penetration Testing	1.ServiceNow, BMC, Ivanti, **OCS, Snipe-IT** 2.DDI, Qualys, Rapid7, **OpenVAS** 3.Fortra CoreImpact, Rapid7 Metasploit, **Kali**
			Perimeter	1.Asset Management System 2.Vulneratbility Management 3.Penetration Testing	1.ServiceNow, BMC, Ivanti, **OCS, Snipe-IT** 2.DDI, Qualys, Rapid7, **OpenVAS** 3.Fortra CoreImpact, Rapid7 Metasploit, **Kali**
			Cloud	1.Cloud Access Broker System	1.MS Cloud App Security, Cisco, Palo Alto Networks

Defense Model and Tool Stack

NIST Function	Stack Purpose	Components and Processes	Layer	Tool Family	Example of Tools
Protect	1. Secure assets to prevent or lower the likelihood and/or impact of adverse events	1. Identity Management 2. Data Security 3. Platform Security 4. Resilience 5. Awareness and Training	Identity	1.Identity Threat Detection and Response (ITDR) 2.Privilege Access Management 3.LMS/Phish Sim	1.MS Defender for Identity, Crowdstrike Identity Protection, SentineOne Singularity for Identity 2.CyberArk, BeyondTrust, Delinea 3.KnowB4, Proofpoint, **Gophish**
			Data	1.Enterprise Information Protection 2.Message Security/Data Loss Prevention	1.MS IRM, MS SQL Encryption, Varonis, Fortra 2.MS Defender for Collaboration, Forcepoint, Proofpoint, Darktrace
			Application	1.Web Application Firewall 2.Threat Modeling	1.Azure WAF, Palo Alto, Fortinet, Imperva, **Coraza WAF** 2.**MS Threat Modeling, OWASP Threat Dragon, IriusRisk**
			Endpoint	1.Endpoint Protection 2.Endpoint Privilege Management 3.Patch Management	1.CrowdStrike, SentinelOne, MS Defender 2.BeyondTrust, CyberArk 3.MS InTune, PatchMyPC, ManageEngine
			Network	1.Network Access Control 2.Network Intrusion Detection/Prevention 4.DNS Security	1.CISCO ISE, Forescout, Fortinet, **PacketFence** 2.Darktrace, Cisco, Palo Alto, Trelix, **Snort, Suricata** 3.Cisco Umbrella, zScaler, Palo Alto
			Perimeter	1.Firewall 2.VPN/Remote Access	1.Palo Alto, Cisco, Fortinet, **PFSense** 2.Palo Alto GlobalProtect, Cisco Secure Client, CyberArk Vendor PAM, BeyondTrust Secure Remote Access
			Cloud	1.Cloud Access Broker System 2. Cloud Posture Management	1.MS Cloud App Security, Cisco, Palo Alto Networks 2. MS Cloud App Security, Cisco, Palo Alto Networks
Detect	1. Enable the timely discovery and analysis of anomalies, indicators of compromise/attack and other potentially adverse events	1. Continuous Monitoring 2. Adverse Event Analysis	Identity	1.Identity Threat Detection and Response (ITDR) 2.Security Event and Incident Management (SEIM)	1.MS Defender for Identity, Crowdstrike Identity Protection, SentineOne Singularity for Identity 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh**
			Data	1.Enterprise Information Protection 2.Data Loss Prevention	1.MS IRM, MS SQL Encryption, Varonis, Fortra 2.MS Defender for Collaboration, Forcepoint, Proofpoint
			Application	1.Web Application Firewall 2.SEIM	1.Azure WAF, Palo Alto, Fortinet, Imperva, **Coraza WAF** 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh**
			Endpoint	1.Endpoint Protection 2.SEIM	1.CrowdStrike, SentinelOne, MS Defender 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh**
			Network	1.Network Access Control 2.Network Intrusion Detection/Prevention 3.SEIM	1.CISCO ISE, Forescout, Fortinet 2.Darktrace, Cisco, Palo Alto, Trelix, **Snort, Suricata** 3.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh**
			Perimeter	1.Firewall 2.SEIM	1. Palo Alto, Cisco, Fortinet, **PFSense** 2.Digital Hands, MS Sentinel, Splunk
			Cloud	1.Cloud Access Broker System 2.SEIM	1.MS Cloud App Security, Cisco, Palo Alto Networks 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh**

Defense Model and Tool Stack

NIST Function	Stack Purpose	Components and Processes	Layer	Tool Family	Example of Tools
Respond	1. Contain the effects of cybersecurity incidents	1. Incidenet Mitigation 2. Incident Management 3. Incident Analysis 4. Response Reporting	Identity	1.Identity Threat Detection and Response (ITDR) 2.SEIM 3.Security Orchestration and Automated Response (SOAR) 4.Incident Management and Reporting	1.MS Defender for Identity, Crowdstrike Identity Protection, SentineOne Singularity for Identity 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh** 3.Palo Alto Cortex, ServiceNow SecOps, **Ansible, Shuffle** 4.ServiceNow SecOps, CyberCPR, **TheHive, IRIS**
			Data	1.Backup 2.DR Replication 3.Incident Management and Reporting	1.Rubrik, Cohesity 2.VMWare, Azure Site Recovery, HP Simplivity 3.ServiceNow SecOps, CyberCPR, **TheHive, IRIS**
			Application	1.Web Application Firewall 2.SEIM 3.Incident Management and Reporting	1.Azure WAF, Palo Alto, Fortinet, Imperva, **Coraza WAF** 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh** 3.ServiceNow SecOps, CyberCPR, **TheHive, IRIS**
			Endpoint	1.Endpoint Protection 2.SEIM 3.SOAR 4.Forensics 5.Incident Management and Reporting	1.CrowdStrike, SentinelOne, MS Defender 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh** 3.Palo Alto Cortex, ServiceNow SecOps, **Ansible, Shuffle** 4.EnCase, Fortra FTK, CrowdStrike Sandbox, Hex-Rays IDA Pro, **Wireshark, ProcMon, Autopsy, Colatility** 5.ServiceNow SecOps, CyberCPR, **TheHive, IRIS**
			Network	1.Network Access Control 2.Network Intrusion Detection/Prevention 3.SEIM 4.SOAR 5.Incident Management and Reporting	1.CISCO ISE, Forescout, Fortinet, **PFSense** 2.Darktrace, Cisco, Palo Alto, Trelix, **Snort, Suricata** 3.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh** 4.Palo Alto Cortex, ServiceNow SecOps, **Ansible, Shuffle** 5.ServiceNow SecOps, CyberCPR, **TheHive, IRIS**
			Perimeter	1.Firewall 2.SEIM 3.SOAR 4.Incident Management and Reporting	1.Palo Alto, Cisco, Fortinet, **PFSense** 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh** 3.Palo Alto Cortex, ServiceNow SecOps, **Ansible, Shuffle** 4.ServiceNow SecOps, CyberCPR, **TheHive, IRIS**
			Cloud	1.Cloud Access Broker System 2.SEIM 3.Incident Management and Reporting	1.MS Cloud App Security, Cisco, Palo Alto Networks 2.Digital Hands, MS Sentinel, Splunk, **UTMStack, Wazuh** 3.ServiceNow SecOps, CyberCPR, **TheHive, IRIS**
Recover	1. Timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable communication during recovery efforts	1. Recovery Plan Execution 2. Recovery Communication	Identity	1.Backup 2.DR Replication 3.Crisis Notification System	1.Rubrik, Cohesity 2.VMWare, Azure Site Recovery, HP Simplivity 3.Blackberry AtHoc, Everbridge, OnSolve
			Data	1.Backup 2.DR Replication	1.Rubrik, Cohesity 2.VMWare, Azure Site Recovery, HP Simplivity
			Application	1.Backup 2.DR Replication	1.Rubrik, Cohesity 2.VMWare, Azure Site Recovery, HP Simplivity
			Endpoint	1.Backup 2.DR Replication	1.MS Images/InTune, MS OneDrive, Crashplan 2.VMWare, Azure Site Recovery, HP Simplivity
			Network	1.Backup 2.DR Replication	1.SolarWinds, Dynatrace 2.VMWare, Azure Site Recovery, HP Simplivity
			Perimeter	1.Backup 2.DR Replication	1.SolarWinds, Dynatrace 2.VMWare, Azure Site Recovery, HP Simplivity
			Cloud	1.Backup 2.DR Replication	1.Rubrik, Cohesity 2.VMWare, Azure Site Recovery, HP Simplivity