Utilizing Security Frameworks Effectively

J.C. Checco

J.C. Checco

C|CISO, CISSP, CSSLP, CCSK,
Boardroom Certified QTE

Proofpoint:

- Resident CISO, Financial Services

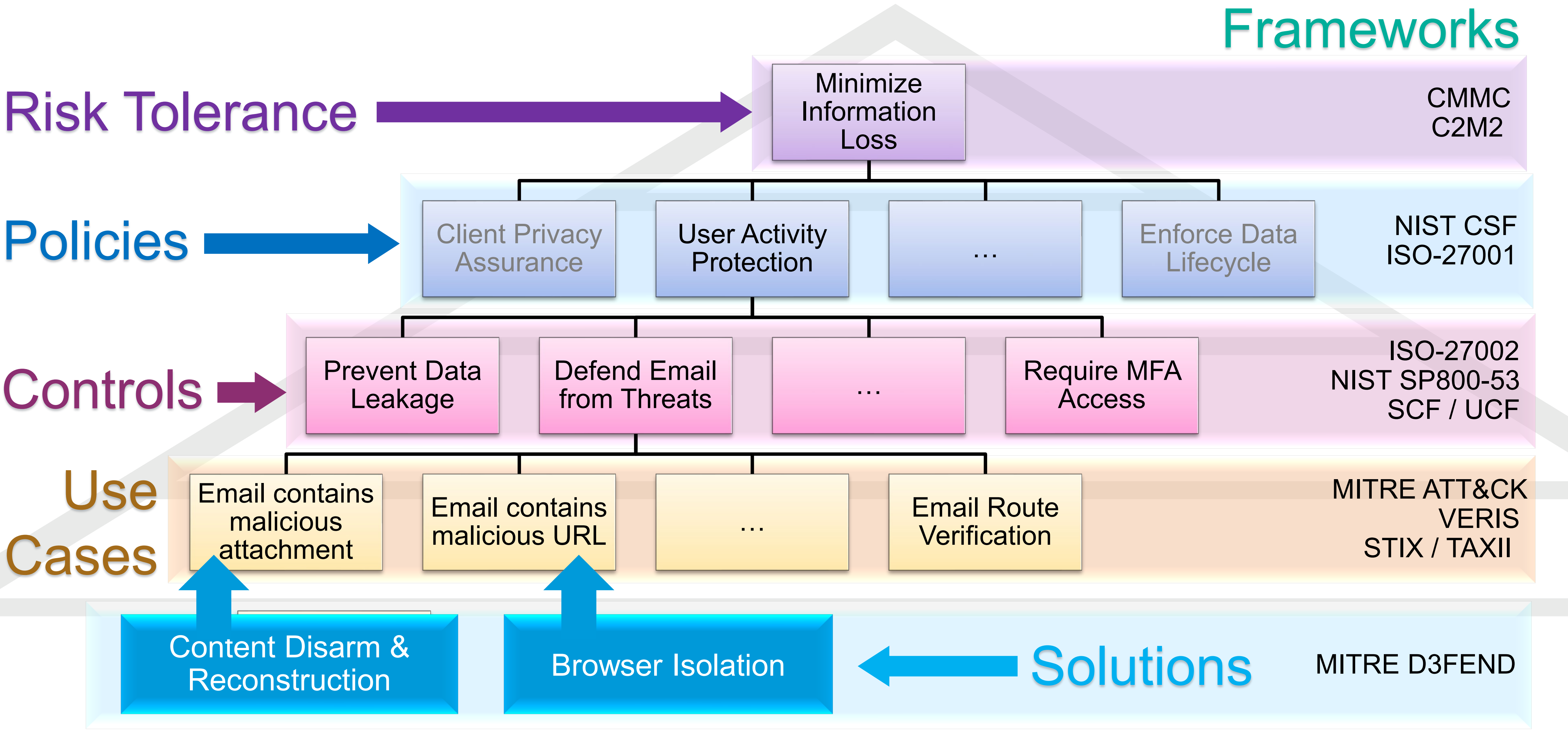
Bank of America:

- Lead, Zero-Trust Strategy & Architecture
- SVP, Security Innovation Team
- Head of Security Technology Assessment Team
- BISO, Global Markets (Merrill Lynch)

Bloomberg:

- CISO for BloombergBlack (Personal Wealth)
- Senior Security & Risk Advisor

TL;DR



Frameworks

Risk Tolerance

Minimize Information Loss

CMMC
C2M2

Policies

Client Privacy Assurance

User Activity Protection

…

Enforce Data Lifecycle

NIST CSF
ISO-27001

Controls

Prevent Data Leakage

Defend Email from Threats

…

Require MFA Access

ISO-27002
NIST SP800-53
SCF / UCF

Use Cases

Email contains malicious attachment

Email contains malicious URL

…

Email Route Verification

MITRE ATT&CK
VERIS
STIX / TAXII

Content Disarm & Reconstruction

Browser Isolation

Solutions

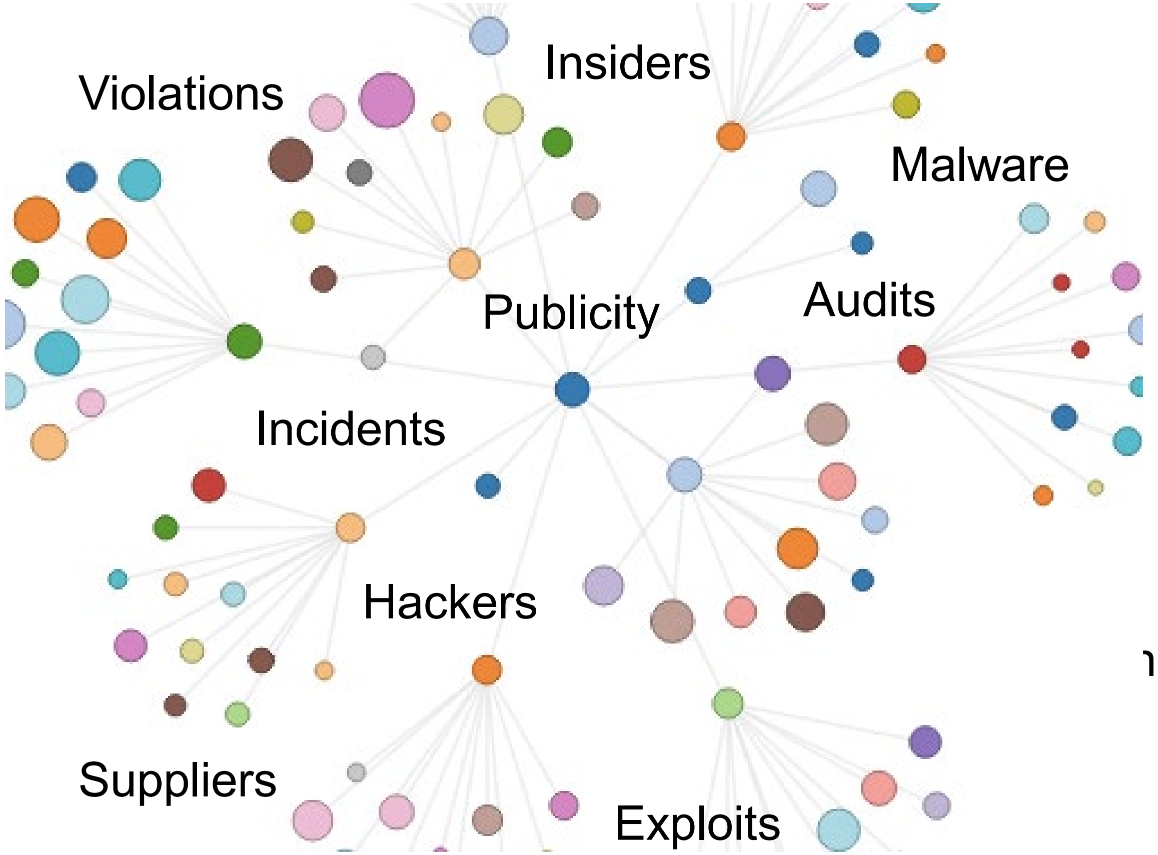
MITRE D3FEND

The Need for Frameworks

CISO / C-Level Security Reporting

Squirrel-Based Management

Our Reality

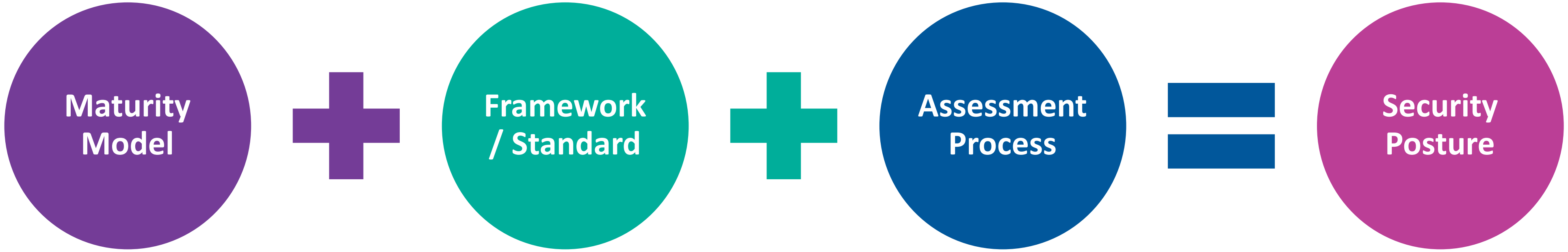


ng

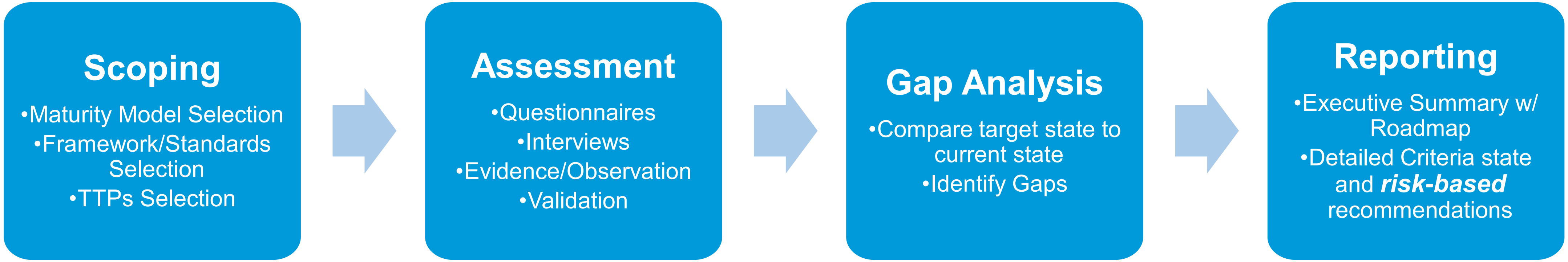
The Plan

Cyber Security Management	• Policies, GRC, 3rd party risk
Cyber Security Operations / Defense	• SOC, Threat Intel, Red Teams
Cyber Security Technology	• DLP, CASB, Endpoint Security
Cyber Security Outreach	• Education, Notifications
Cyber Security Reporting	• Audit, Compliance, Legal Counsel, Board

Defining Security Posture



Maturity Model + Framework / Standard + Assessment Process = Security Posture



Scoping

- Maturity Model Selection
- Framework/Standards Selection
- TTPs Selection

Assessment

- Questionnaires
- Interviews
- Evidence/Observation
- Validation

Gap Analysis

- Compare target state to current state
- Identify Gaps

Reporting

- Executive Summary w/ Roadmap
- Detailed Criteria state and ***risk-based*** recommendations

Sidebar→ Service Organization Control (SOC) reports

AICPA audits to verify data center operational and security excellence

SOC1

- Focus: **Governance and Procedures**
- Validating ISMS (i.e. ISO-27001)
- Proper Documentation
- Oversight of the organization
- Internal corporate governance and risk management processes

SOC2

- Focus: **Process Execution and Control Effectiveness**
- Validating Security Controls (i.e. ISO-27002)
- Vendor management
- Regulatory oversight
- Details gaps and vulnerabilities

SOC3

- Focus: **Assurance of Operational Excellence**
- Attestation of SOC1 and/or SOC2 examination without disclosing details

Maturity Models, Frameworks & Standards

Maturity Models

- Maturity models represent theories of stage-based evolution of self-improvement.
- As-is assessments of the current capabilities with respect to given criteria.

Assessment Goals

How mature are our security processes?
Where are our strategic gaps?

Model	Description	Focus
Capability Maturity Model (CMMI)	Process level improvement training and appraisal program.	Universal
Portfolio, Programme and Project Management Maturity Model (P3M3)	Evaluates how it delivers its projects, programmes and portfolio(s).	Project Management
Quality Management Maturity Grid (QMMG)	Benchmark with respect to service or product quality management.	Quality
Capability Maturity Model (CMM)	Measure the degree of formality and optimization of software development processes.	Software Development
Cybersecurity Maturity Model Certification (CMMC)	US Department of Defense standard for measuring effectiveness based on process and reporting.	Technology & Processes
Cybersecurity Capability Maturity Model (C2M2)	US Department of Energy standard for measuring effectiveness based on relevancy and impact.	Technology, Processes & People

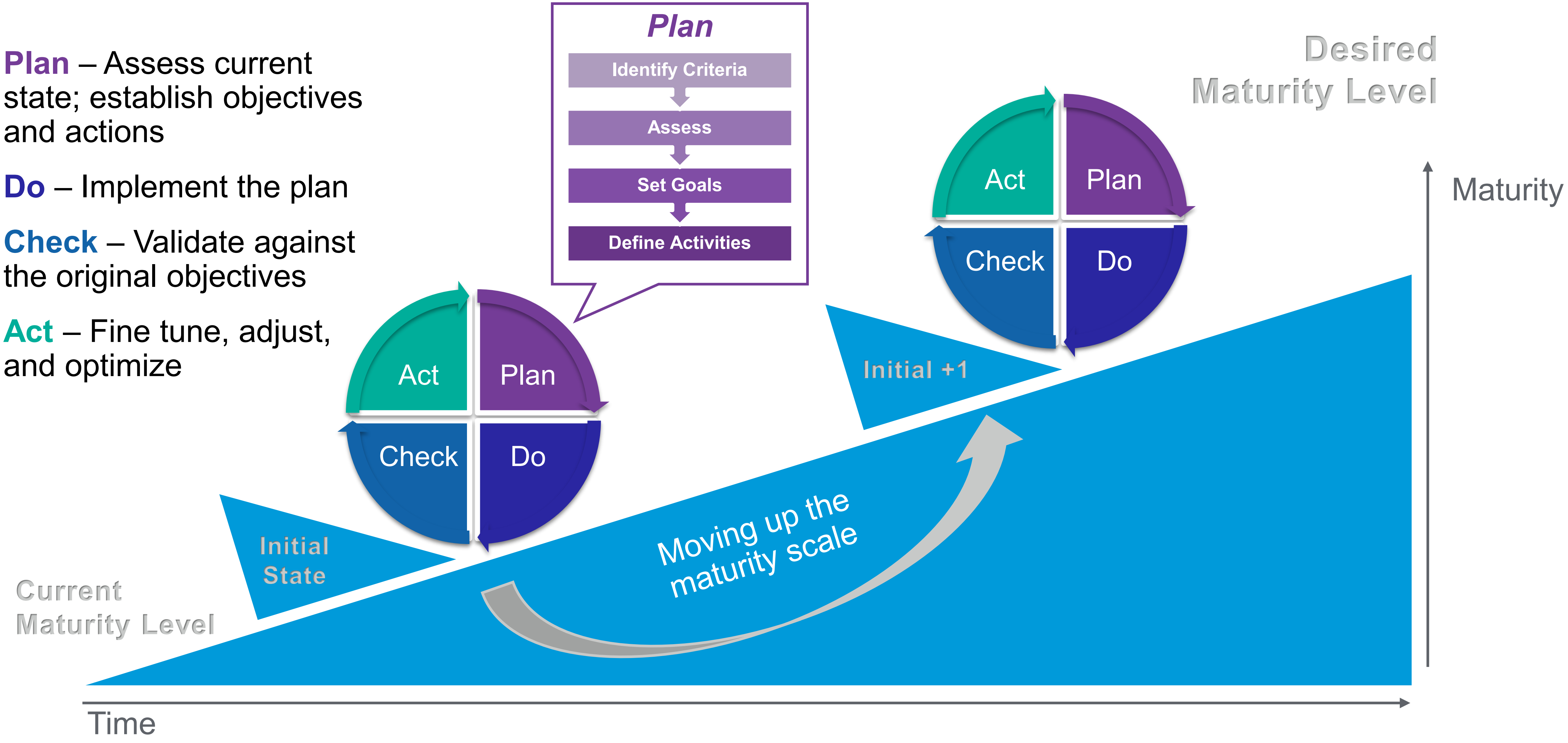
Maturation Process

Plan – Assess current state; establish objectives and actions

Do – Implement the plan

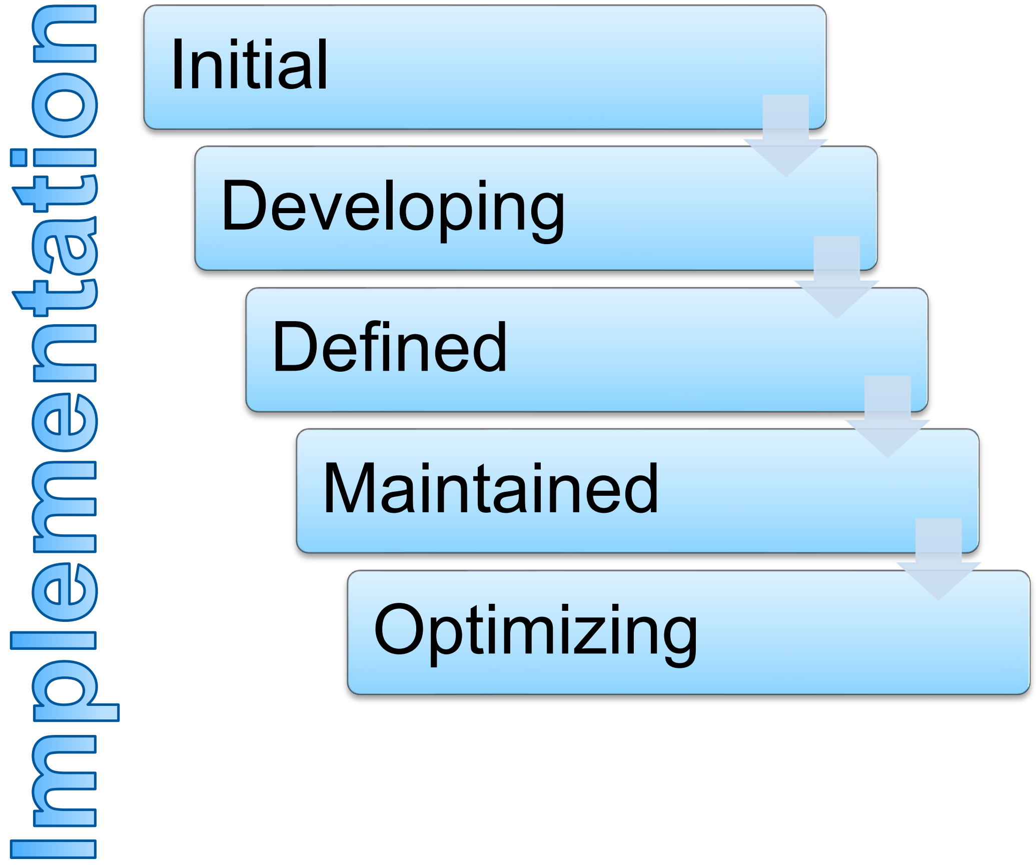
Check – Validate against the original objectives

Act – Fine tune, adjust, and optimize



Sidebar→ CMMC & C2M2

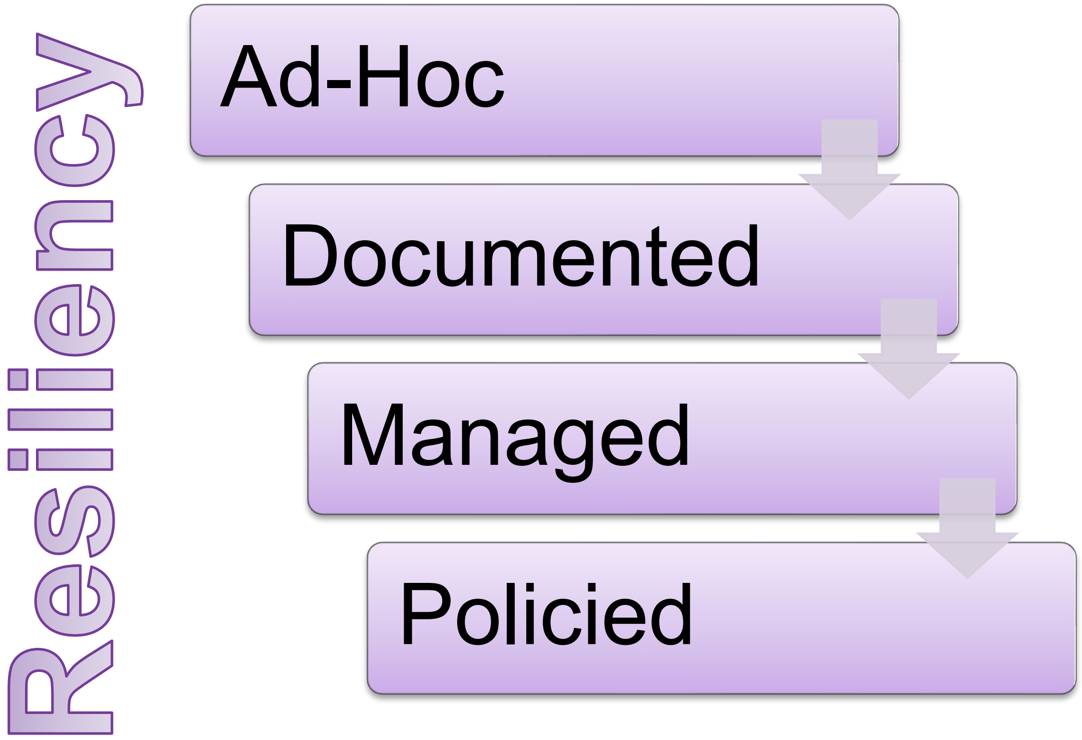
CMMC



Implementation

- Initial
- Developing
- Defined
- Maintained
- Optimizing

C2M2



Resiliency

- Ad-Hoc
- Documented
- Managed
- Policied

Frameworks and Standards

- Cybersecurity frameworks and standards represent compliance-based criteria for control implementation.
- Target criteria, usually with risk-based specificity configuration options to facilitate meeting legal and regulatory requirements.

Implementation Goals

How relevant is our framework to our threats?
Are we in compliance?

Model	Description	Focus
NIST Cyber Security Framework (CSF)	Security threat and response categories.	Security Management
NIST Special Publication 800-53	Security controls and associated assessment procedures.	Federal Systems Security Controls
Payment Card Industry Data Security Standard (PCI DSS)	Information security for organizations that handle branded credit cards from the major card schemes.	Credit Cart & Payment Systems
North American Electrical Reliability Corporation (NERC CIP)	Reliability standards for energy sector in North America.	Critical Infrastructure Protection (CIP)
ISO/IEC Information Security Management (ISO 27001)	Requirements for an information security management system (ISMS).	Security Management & Processes
ISO/IEC Information Security Controls (ISO 27002)	Reference for security controls within the process of implementing an Information Security Management System.	Security Controls
Security Controls Framework (SCF)	Generic reference for security controls, non-industry specific.	Security Controls
Unified Controls Framework (UCF)	Globally harmonized security controls, with cross references to international regulations and other standards.	International Security Controls
Cloud Controls Matrix (CCM)	Cloud-specific reference for security controls.	Cloud Security Controls

IOCs (Indicators of Compromise) & TTPs (Tactics, Techniques, and Procedures)

- Tactical vocabulary for offensive and defensive cybersecurity activities
  - Lack specificity to preventative detection and mitigation
  - Lack of comprehensive inclusion of human vectors, detection and mitigation.
  - Risk-based application reliant on mature organizational risk modeling framework being applied in tandem

Protection Goals

Do we address/defend against TTPs?
How well are we protected?

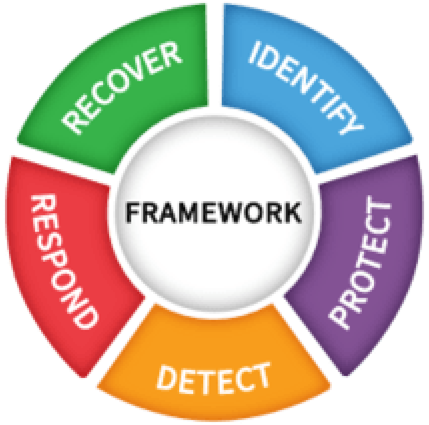
Model	Description	Focus
MITRE ATT&CK (Adversarial Tactics Techniques & Common Knowledge)	ATT&CK was created out of a need to systematically categorize adversary behavior as part of conducting structured adversary emulation exercises against endpoints.	Threat Tactics Categorizations
MITRE D3FEND	D3FEND estimates operational applicability, identifies strengths and weaknesses, and supports development of enterprise solutions comprising multiple capabilities.	Defensive Tactics Categorizations
Veris	Vocabulary for event recording and incident sharing. Extends ATT&CK TTPs – used for developing the annual DBIR	Incident Vocabulary
STIX (Structured Threat Information Expression)	Language and serialization format used to exchange cyber threat intelligence, complemented by the TAXII (Trusted Automated eXchange of Intelligence Information) protocol.	Threat Intelligence Vocabulary, Exchange Format and Protocol.

Inter-Framework Relationships

NIST CSF, MITRE ATT&CK, and D3FEND

NIST CSF v1.1

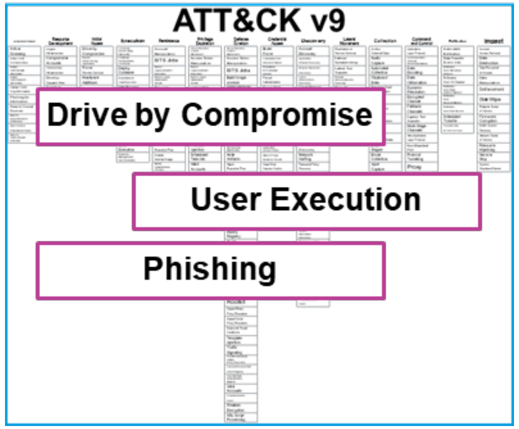
- Common language for understanding, managing, and expressing cybersecurity risk
- Identify and prioritize actions for reducing risk
- Tool for aligning policy, business, and technology



MITRE ATT&CK v9

- Knowledge base of offensive/adversary IOCs & TTPs.
- Foundation for the development of specific threat models methodologies.

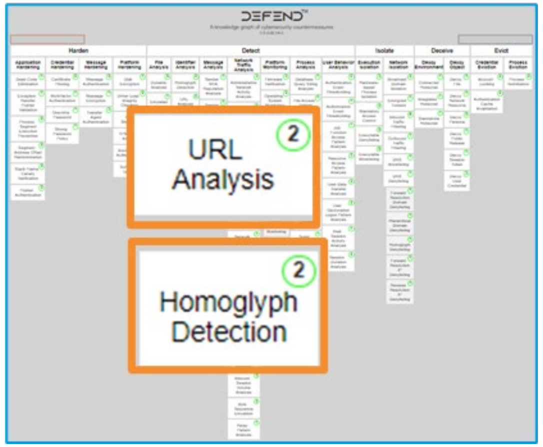
Offensive Model



MITRE D3FEND v0.9.3-BETA-1

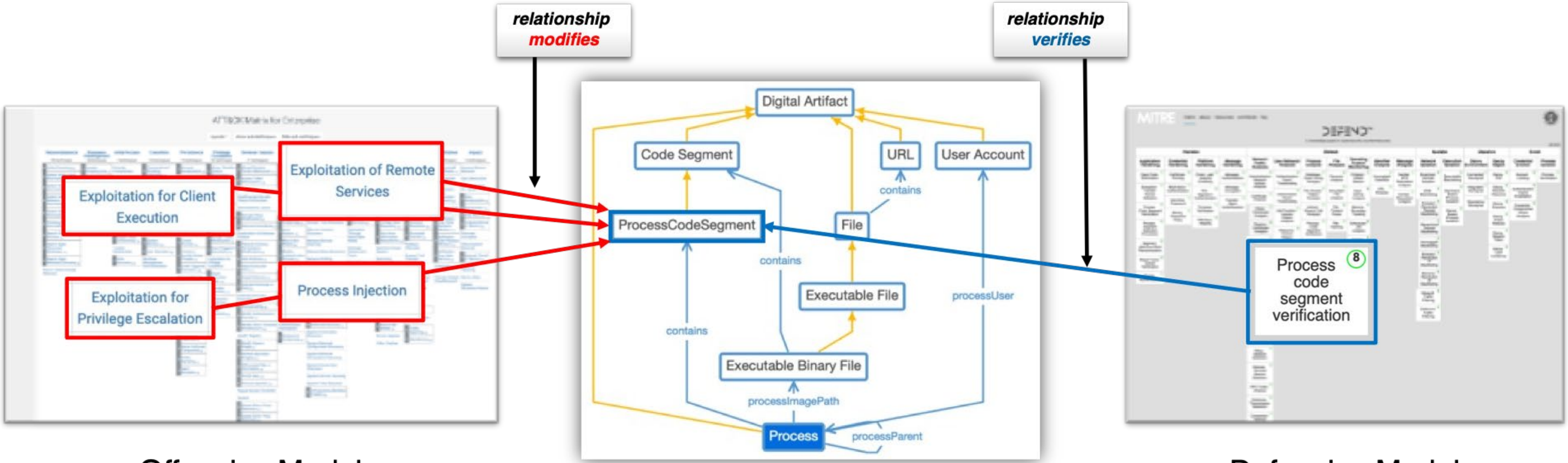
- Knowledge base of cybersecurity countermeasure techniques.
- Catalog of defensive cybersecurity techniques/relationships to ATT&CK.

Defensive Model



Focus on *endpoint* protection

MITRE ATT&CK / D3FEND Digital Artifact Ontology

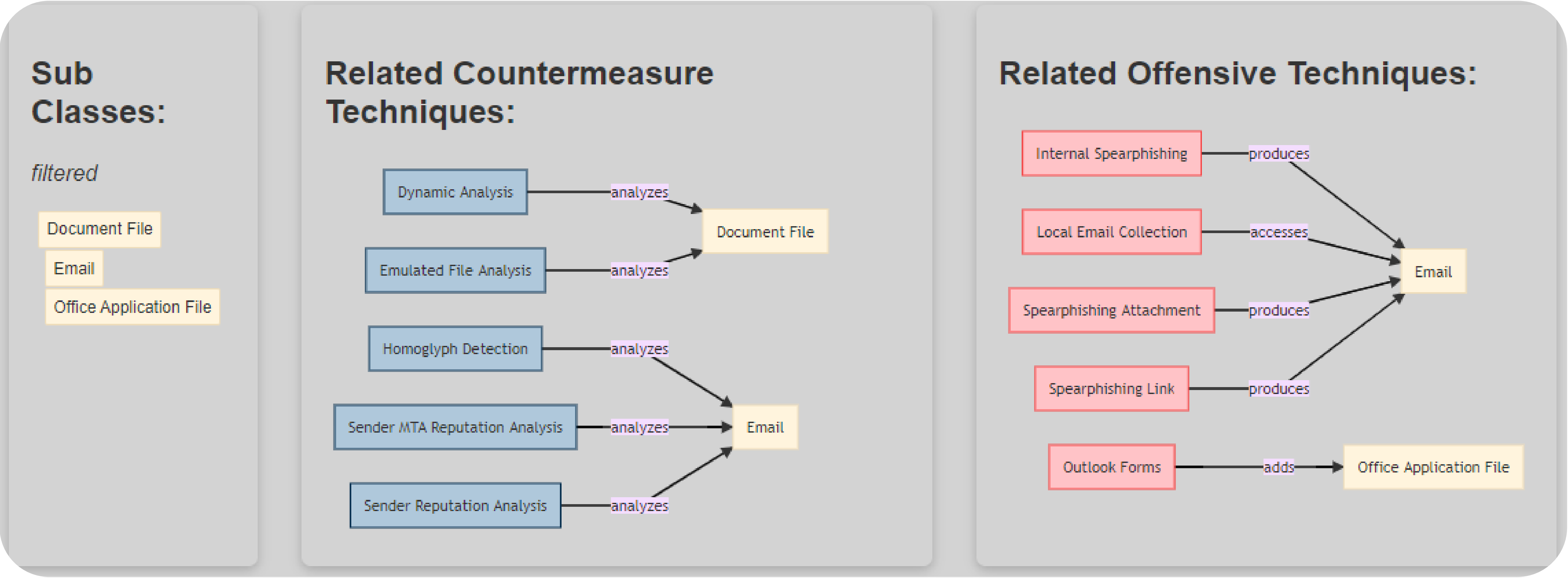


Offensive Model

Digital Artifact Ontology
(simplified)

Defensive Model

Example: MITRE Digital Artifact Ontology



Sub Classes:

filtered

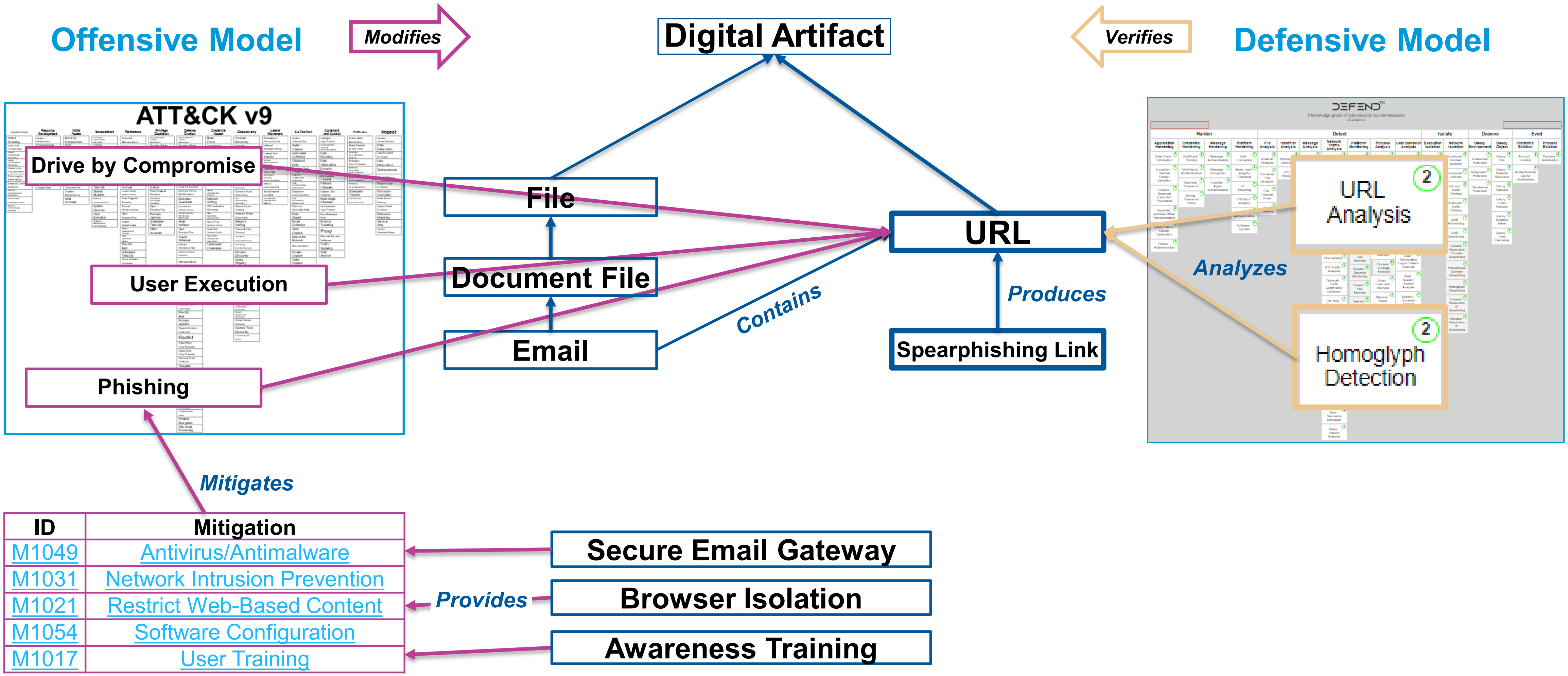
- Document File
- Email
- Office Application File

Related Countermeasure Techniques:

Related Offensive Techniques:

Reality: ATT&CK and D3FEND Framework Relationships

Digital Artifact Ontology



ID	Mitigation
M1049	Antivirus/Antimalware
M1031	Network Intrusion Prevention
M1021	Restrict Web-Based Content
M1054	Software Configuration
M1017	User Training

Frameworks & Assessment Methodologies

Assessment Functions

Governance, Risk, and Compliance

- Align Security Maturity targets to Business Objectives
- Establish and Maintain Policies
- Sponsor and Fund Security Initiatives
- Manage Capabilities and Portfolio

- Risk is aligned to ERM
- Risk management is proactively used for decision making
- KRIs and predictive risk analytics proactively used to identify & act
- Compliance and oversight assesses and enforces policies

People

- Leadership messaging aligns with culture
- People Centric Mindset
- People Centric threats are understood by the workforce
- Awareness and Training program are proactively implemented

Process

- Formal process exists and is documented.
- Detailed metrics of the process are captured and reported.
- Minimal target for metrics has been established and continually improving.
- Less than 1% of process exceptions occur.

Technology

- Fully integrated systems aligned to security strategy
- KPIs and KRIs are proactively used to identify and mitigate technology risk.
- Less than 1% of technology exceptions occur.

Assessment Functions and NIST CSF

To further support the management of risks associated with security-related events, organizations may choose to use Detect, Respond, and Recover Functions from the Cybersecurity Framework.

Function Unique Identifier	Function	Category Unique Identifier	Category
GR	Governance, Risk & Compliance	GR.BE	Business Environment
		GR.CO	Compliance and Oversight
		GR.GP	Governance Policies
		GR.IM	Inventory and Mapping
		GR.OE	Organizational Ecosystem Risk
		GR.RA	Risk Assessment
		GR.RM	Risk Management Strategy

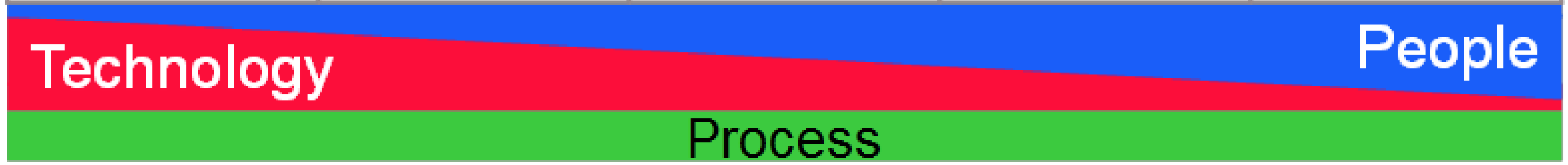
Function Unique Identifier	Function	Category Unique Identifier	Category
PL	People	PL.AT	Awareness and Training
		PL.RR	Roles and Responsibilities
PR	Process	PR.GP	Governance Processes and Procedures
		PR.AC	Identity Management, Authentication, and Access Control
		PR.AP	Associated Processing
		PR.DS	User Activity Data Security
		PR.MA	Maintenance
IT	Technology	IT.PM	PCS Management
		IT.PT	Protective Technology

Function Unique Identifier	Function	Category Unique Identifier	Category
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Assessment Functions and Cyber Defense Matrix

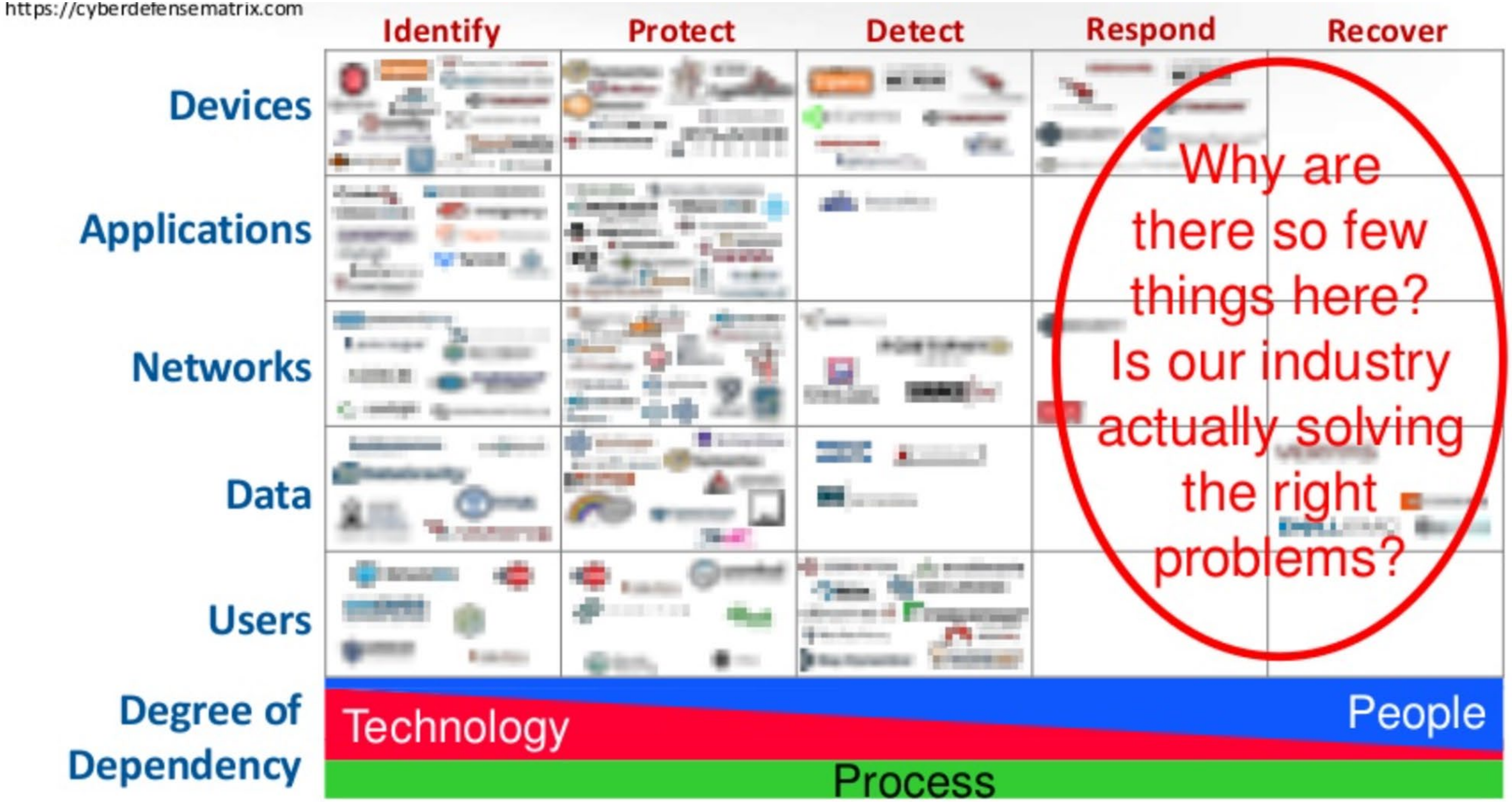
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

Degree of Dependency



Source: *Sounil Yu, RSA 2016*

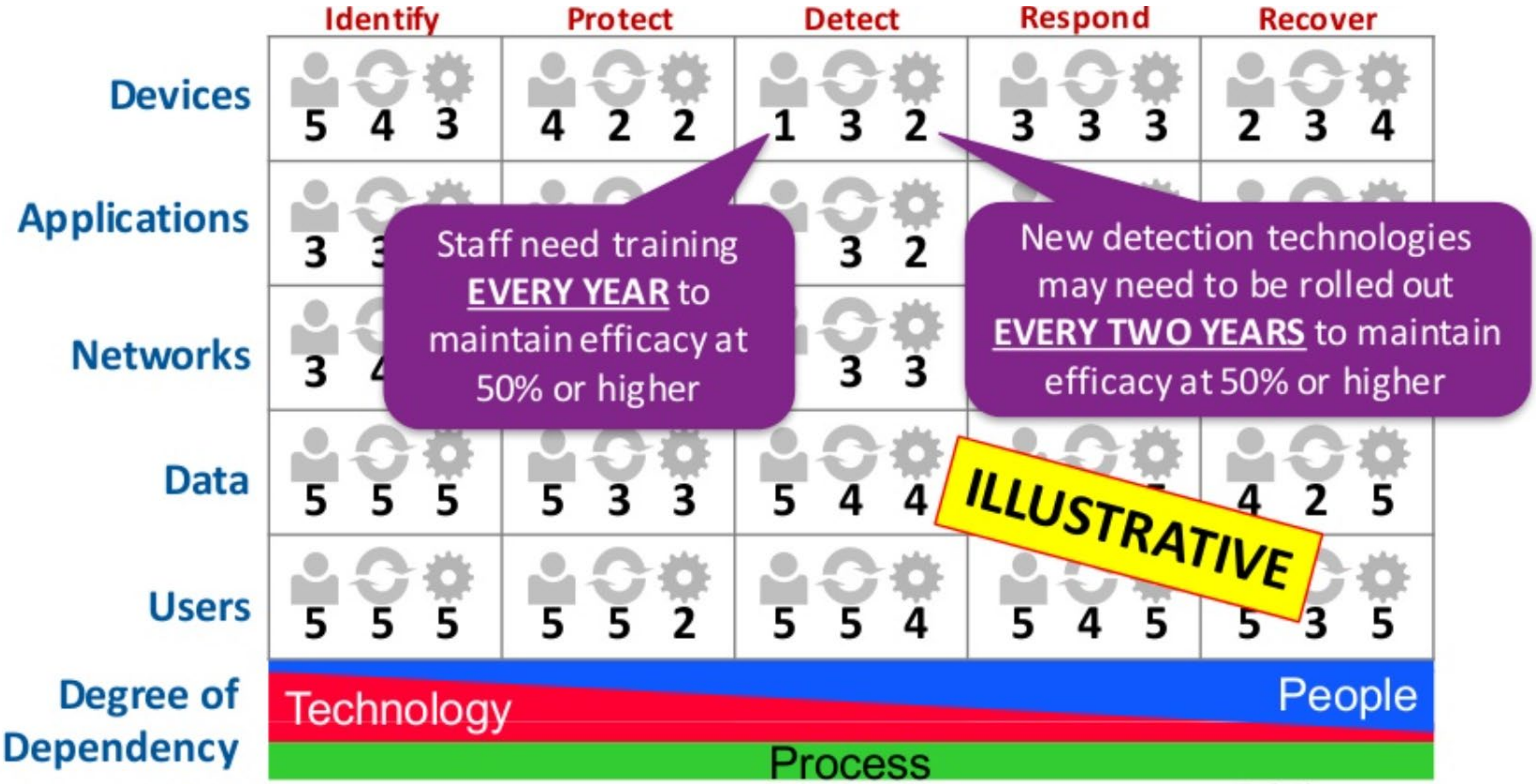
Cyber Defense Matrix – Security Solution Mapping



Why are there so few things here? Is our industry actually solving the right problems?

Source: *Sounil Yu, RSA 2016*

Cyber Defense Matrix: Resource Weighting Overlay



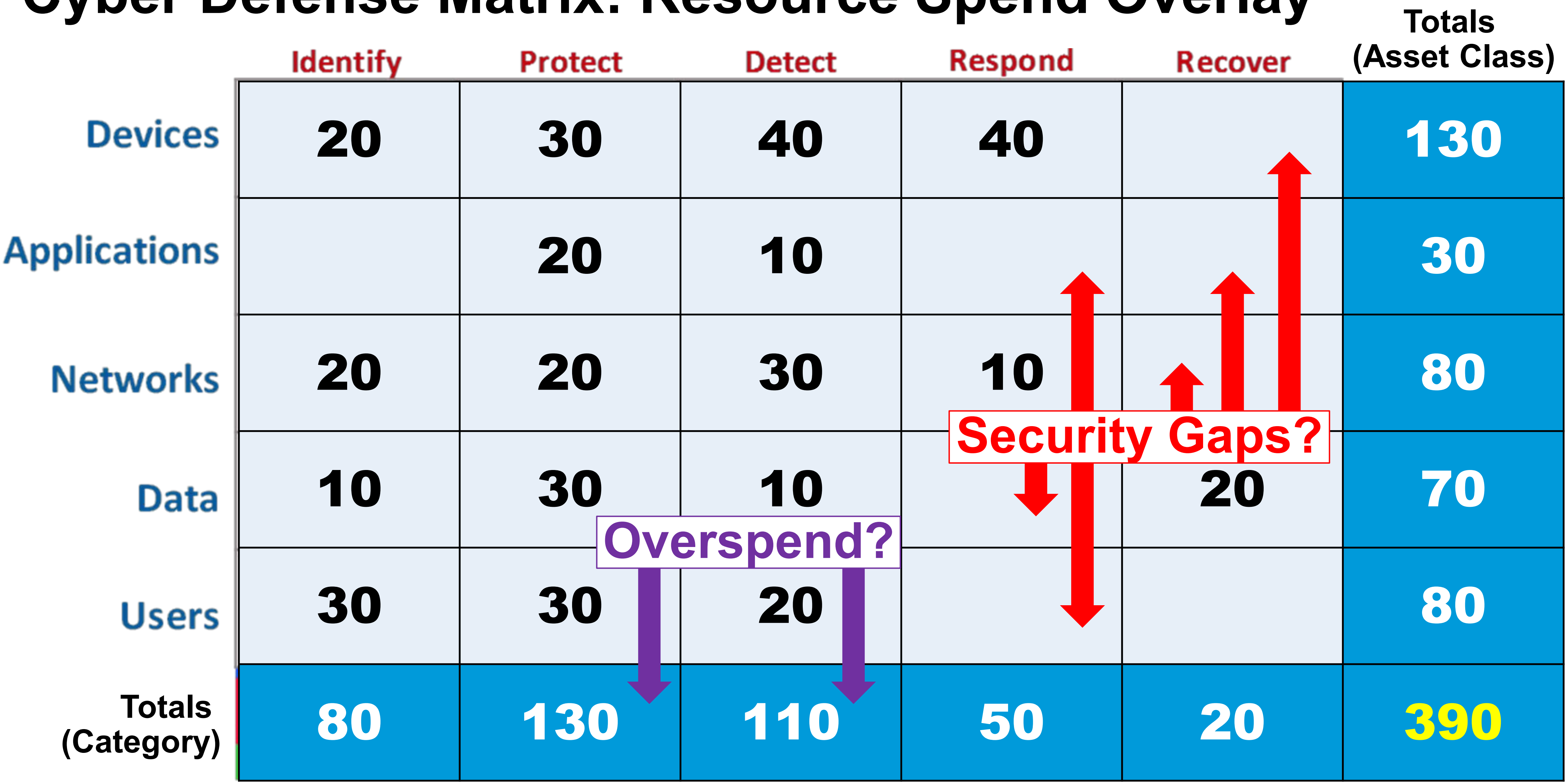
	Identify	Protect	Detect	Respond	Recover
Devices	5 4 3	4 2 2	1 3 2	3 3 3	2 3 4
Applications	3 3		3 2		
Networks	3 4		3 3		
Data	5 5 5	5 3 3	5 4 4		4 2 5
Users	5 5 5	5 5 2	5 5 4	5 4 5	5 3 5

Staff need training **EVERY YEAR** to maintain efficacy at 50% or higher

New detection technologies may need to be rolled out **EVERY TWO YEARS** to maintain efficacy at 50% or higher

Source: *Sounil Yu, RSA 2016*

Cyber Defense Matrix: Resource Spend Overlay



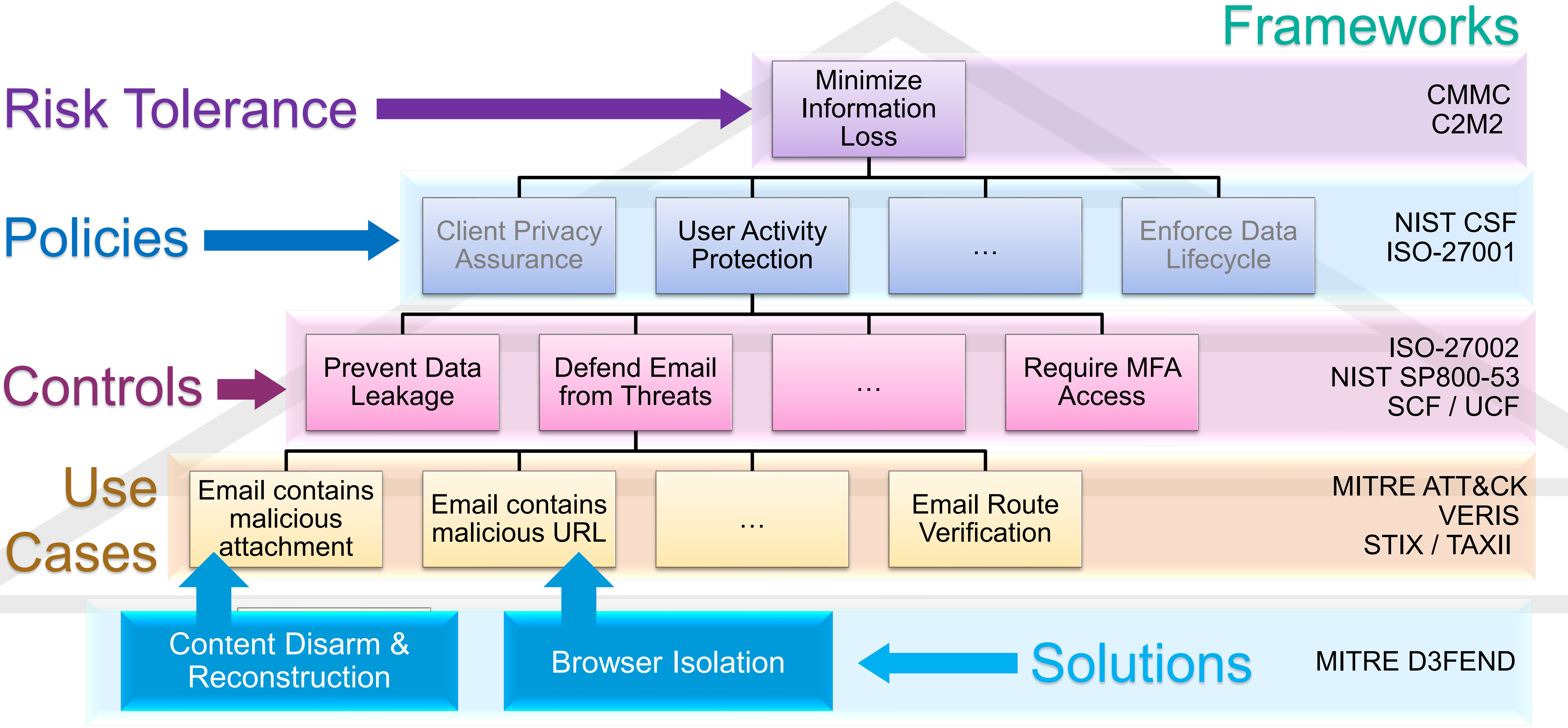
	Identify	Protect	Detect	Respond	Recover	Totals (Asset Class)
Devices	20	30	40	40		130
Applications		20	10			30
Networks	20	20	30	10		80
Data	10	30	10		20	70
Users	30	30	20			80
Totals (Category)	80	130	110	50	20	390

Security Gaps?

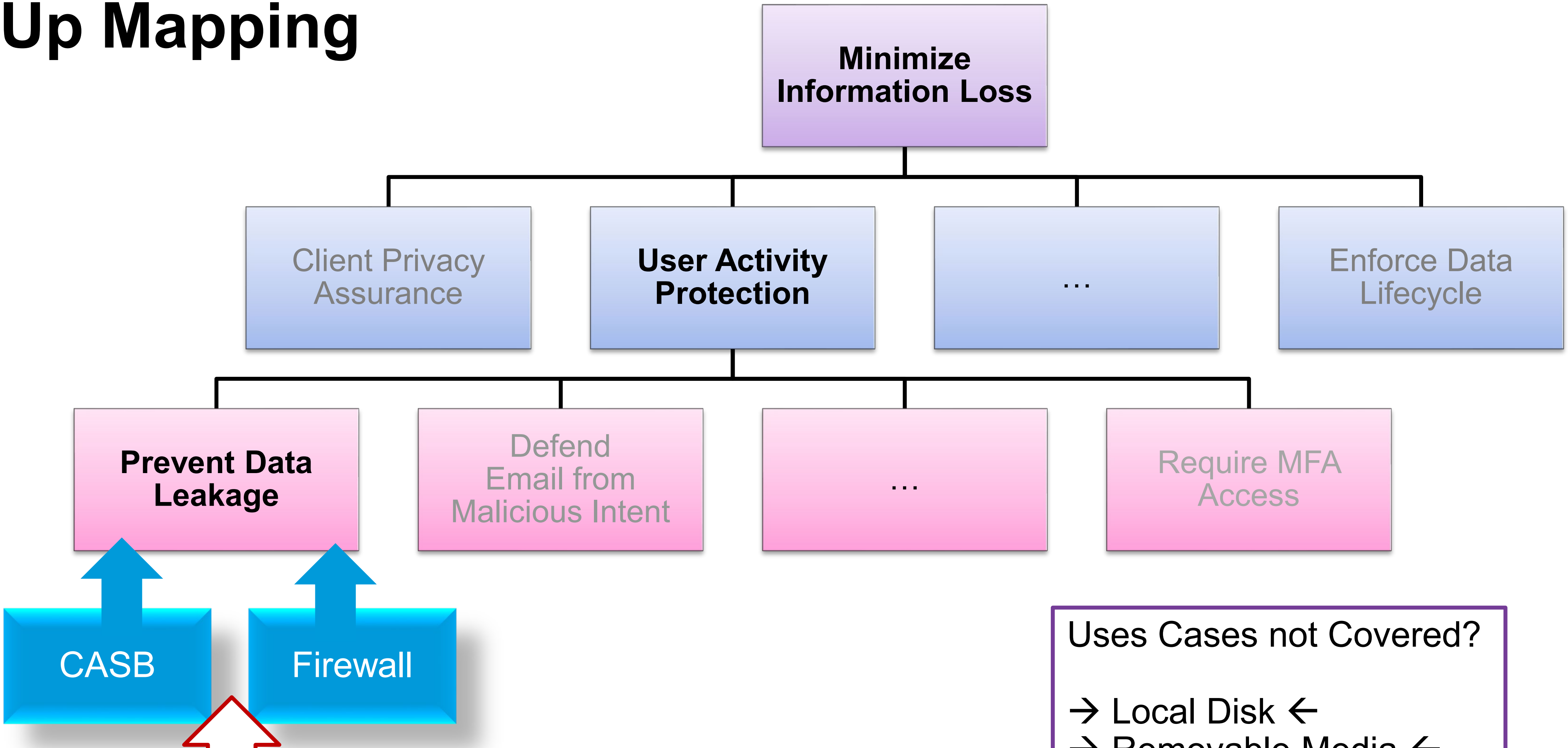
Overspend?

Mapping Organizational Risks using Frameworks

Mapping Risks – Tower of Babel & Threat Modeling



Bottom-Up Mapping

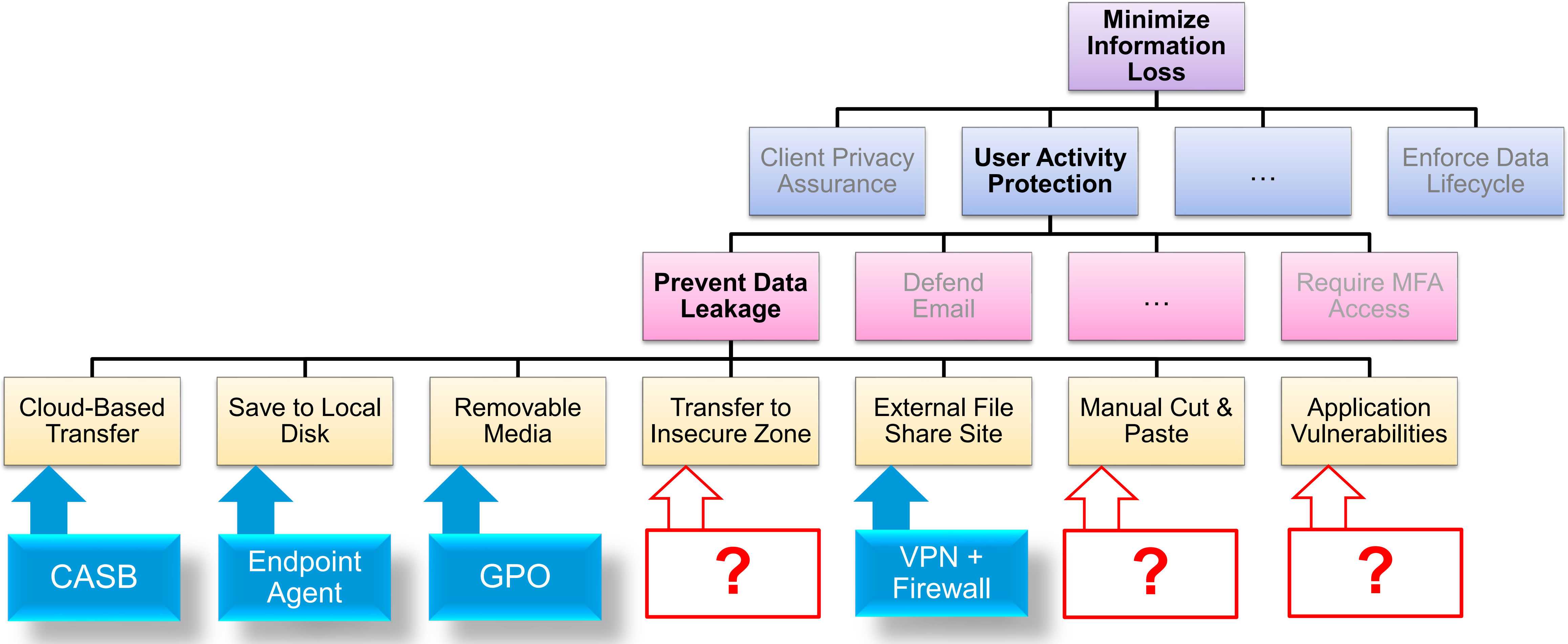


Even Multiple Solutions Only Cover a Partial Set of Use Cases

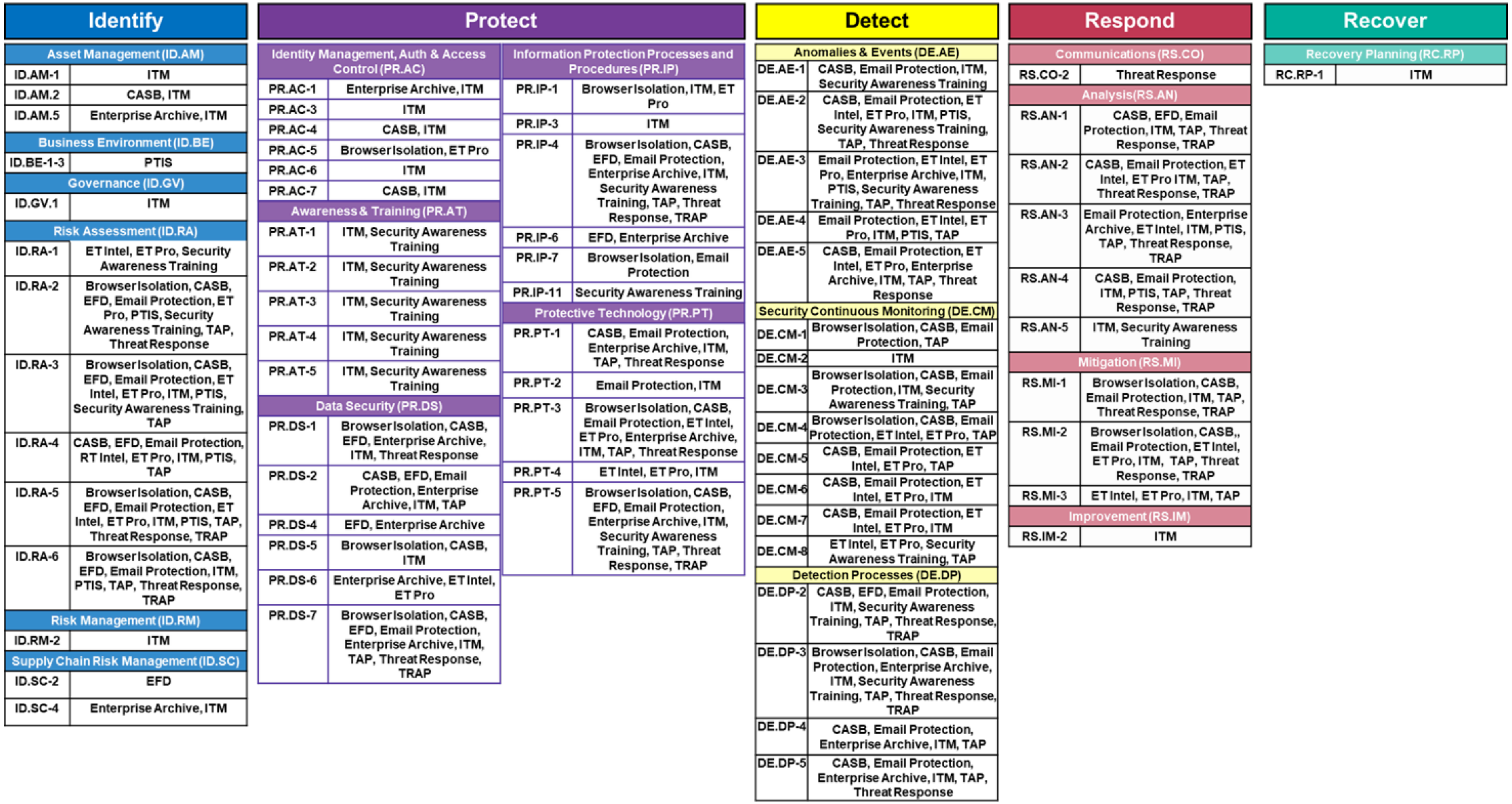
Uses Cases not Covered?

→ Local Disk ←
→ Removable Media ←
→ Internal File share ←
→ External File share ←

Top-Down Mapping



Mapping Risks – NIST CSF



Identify	
Asset Management (ID.AM)	
ID.AM-1	ITM
ID.AM.2	CASB, ITM
ID.AM.5	Enterprise Archive, ITM
Business Environment (ID.BE)	
ID.BE-1-3	PTIS
Governance (ID.GV)	
ID.GV.1	ITM
Risk Assessment (ID.RA)	
ID.RA-1	ET Intel, ET Pro, Security Awareness Training
ID.RA-2	Browser Isolation, CASB, EFD, Email Protection, ET Pro, PTIS, Security Awareness Training, TAP, Threat Response
ID.RA-3	Browser Isolation, CASB, EFD, Email Protection, ET Intel, ET Pro, ITM, PTIS, Security Awareness Training, TAP
ID.RA-4	CASB, EFD, Email Protection, RT Intel, ET Pro, ITM, PTIS, TAP
ID.RA-5	Browser Isolation, CASB, EFD, Email Protection, ET Intel, ET Pro, ITM, PTIS, TAP, Threat Response, TRAP
ID.RA-6	Browser Isolation, CASB, EFD, Email Protection, ITM, PTIS, TAP, Threat Response, TRAP
Risk Management (ID.RM)	
ID.RM-2	ITM
Supply Chain Risk Management (ID.SC)	
ID.SC-2	EFD
ID.SC-4	Enterprise Archive, ITM

Protect			
Identity Management, Auth & Access Control (PR.AC)		Information Protection Processes and Procedures (PR.IP)	
PR.AC-1	Enterprise Archive, ITM	PR.IP-1	Browser Isolation, ITM, ET Pro
PR.AC-3	ITM	PR.IP-3	ITM
PR.AC-4	CASB, ITM	PR.IP-4	Browser Isolation, CASB, EFD, Email Protection, Enterprise Archive, ITM, Security Awareness Training, TAP, Threat Response, TRAP
PR.AC-5	Browser Isolation, ET Pro	PR.IP-6	EFD, Enterprise Archive
PR.AC-6	ITM	PR.IP-7	Browser Isolation, Email Protection
PR.AC-7	CASB, ITM	PR.IP-11	Security Awareness Training
Awareness & Training (PR.AT)		Protective Technology (PR.PT)	
PR.AT-1	ITM, Security Awareness Training	PR.PT-1	CASB, Email Protection, Enterprise Archive, ITM, TAP, Threat Response
PR.AT-2	ITM, Security Awareness Training	PR.PT-2	Email Protection, ITM
PR.AT-3	ITM, Security Awareness Training	PR.PT-3	Browser Isolation, CASB, Email Protection, ET Intel, ET Pro, Enterprise Archive, ITM, TAP, Threat Response
PR.AT-4	ITM, Security Awareness Training	PR.PT-4	ET Intel, ET Pro, ITM
PR.AT-5	ITM, Security Awareness Training	PR.PT-5	Browser Isolation, CASB, EFD, Email Protection, Enterprise Archive, ITM, Security Awareness Training, TAP, Threat Response, TRAP
Data Security (PR.DS)			
PR.DS-1	Browser Isolation, CASB, EFD, Enterprise Archive, ITM, Threat Response		
PR.DS-2	CASB, EFD, Email Protection, Enterprise Archive, ITM, TAP		
PR.DS-4	EFD, Enterprise Archive		
PR.DS-5	Browser Isolation, CASB, ITM		
PR.DS-6	Enterprise Archive, ET Intel, ET Pro		
PR.DS-7	Browser Isolation, CASB, EFD, Email Protection, Enterprise Archive, ITM, TAP, Threat Response, TRAP		

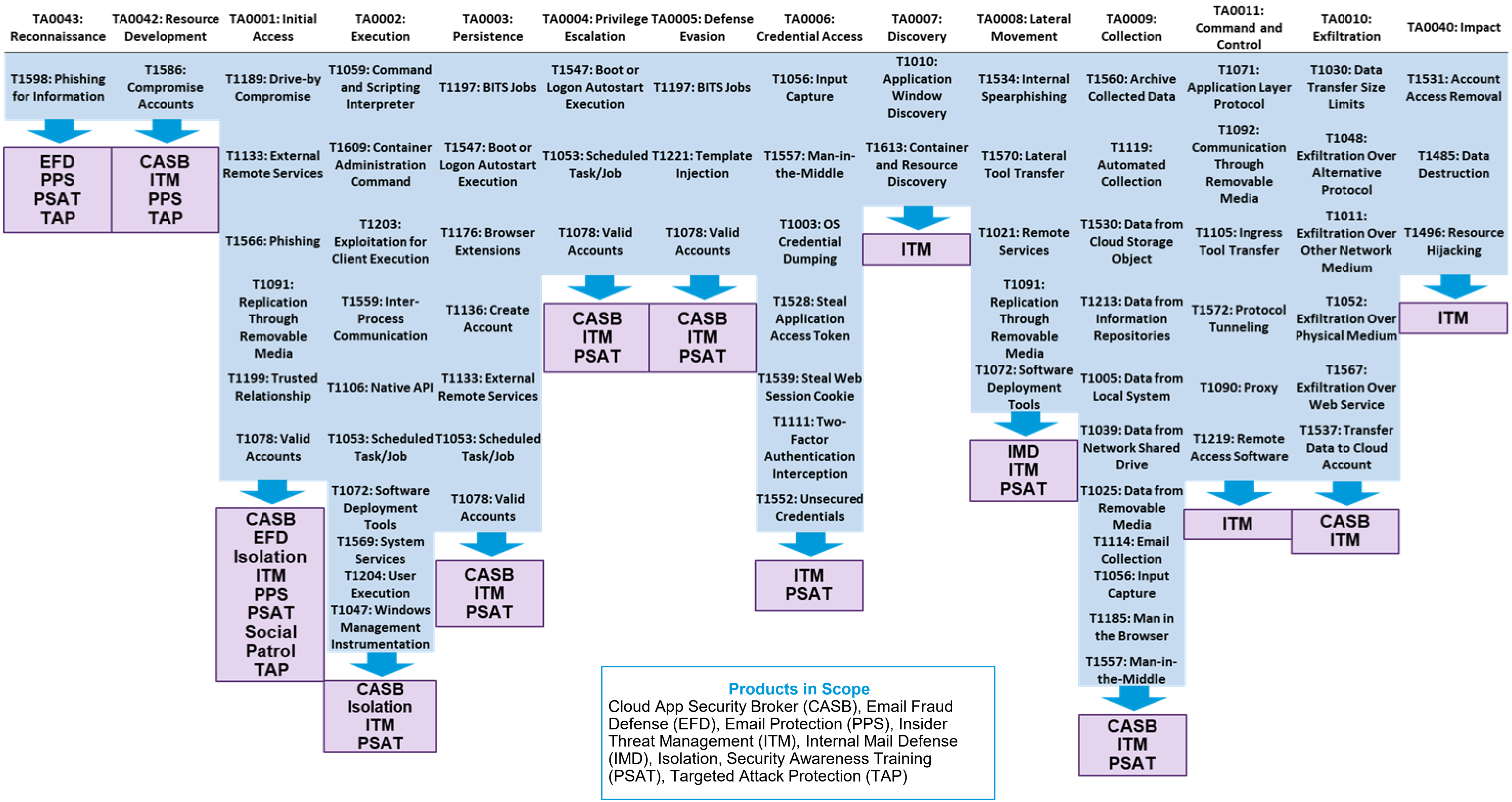
Detect	
Anomalies & Events (DE.AE)	
DE.AE-1	CASB, Email Protection, ITM, Security Awareness Training
DE.AE-2	CASB, Email Protection, ET Intel, ET Pro, ITM, PTIS, Security Awareness Training, TAP, Threat Response
DE.AE-3	Email Protection, ET Intel, ET Pro, Enterprise Archive, ITM, PTIS, Security Awareness Training, TAP, Threat Response
DE.AE-4	Email Protection, ET Intel, ET Pro, ITM, PTIS, TAP
DE.AE-5	CASB, Email Protection, ET Intel, ET Pro, Enterprise Archive, ITM, TAP, Threat Response
Security Continuous Monitoring (DE.CM)	
DE.CM-1	Browser Isolation, CASB, Email Protection, TAP
DE.CM-2	ITM
DE.CM-3	Browser Isolation, CASB, Email Protection, ITM, Security Awareness Training, TAP
DE.CM-4	Browser Isolation, CASB, Email Protection, ET Intel, ET Pro, TAP
DE.CM-5	CASB, Email Protection, ET Intel, ET Pro, TAP
DE.CM-6	CASB, Email Protection, ET Intel, ET Pro, ITM
DE.CM-7	CASB, Email Protection, ET Intel, ET Pro, ITM
DE.CM-8	ET Intel, ET Pro, Security Awareness Training, TAP
Detection Processes (DE.DP)	
DE.DP-2	CASB, EFD, Email Protection, ITM, Security Awareness Training, TAP, Threat Response, TRAP
DE.DP-3	Browser Isolation, CASB, Email Protection, Enterprise Archive, ITM, Security Awareness Training, TAP, Threat Response, TRAP
DE.DP-4	CASB, Email Protection, Enterprise Archive, ITM, TAP
DE.DP-5	CASB, Email Protection, Enterprise Archive, ITM, TAP, Threat Response

Respond	
Communications (RS.CO)	
RS.CO-2	Threat Response
Analysis(RS.AN)	
RS.AN-1	CASB, EFD, Email Protection, ITM, TAP, Threat Response, TRAP
RS.AN-2	CASB, Email Protection, ET Intel, ET Pro ITM, TAP, Threat Response, TRAP
RS.AN-3	Email Protection, Enterprise Archive, ET Intel, ITM, PTIS, TAP, Threat Response, TRAP
RS.AN-4	CASB, Email Protection, ITM, PTIS, TAP, Threat Response, TRAP
RS.AN-5	ITM, Security Awareness Training
Mitigation (RS.MI)	
RS.MI-1	Browser Isolation, CASB, Email Protection, ITM, TAP, Threat Response, TRAP
RS.MI-2	Browser Isolation, CASB,, Email Protection, ET Intel, ET Pro, ITM, TAP, Threat Response, TRAP
RS.MI-3	ET Intel, ET Pro, ITM, TAP
Improvement (RS.IM)	
RS.IM-2	ITM

Recover	
Recovery Planning (RC.RP)	
RC.RP-1	ITM

Products in Scope:
Browser Isolation, Cloud App Security Broker (CASB), Email Encryption, Email Protection, Enterprise Archive, ET Intel, ET Pro, Insider Threat, Premium Threat Information Service (PTIS), Phishing Simulation Awareness Training (PSAT), Targeted Attack Protection (TAP), Threat Response, Threat Response Auto-Pull (TRAP), Unified DLP (U-DLP)

Mapping Risks – MITRE ATT&CK



TA0043: Reconnaissance

- T1598: Phishing for Information

EFD
PPS
PSAT
TAP

TA0042: Resource Development

- T1586: Compromise Accounts

CASB
ITM
PPS
TAP

TA0001: Initial Access

- T1189: Drive-by Compromise
- T1133: External Remote Services
- T1566: Phishing
- T1091: Replication Through Removable Media
- T1199: Trusted Relationship
- T1078: Valid Accounts

CASB
EFD
Isolation
ITM
PPS
PSAT
Social Patrol
TAP

TA0002: Execution

- T1059: Command and Scripting Interpreter
- T1609: Container Administration Command
- T1203: Exploitation for Client Execution
- T1559: Inter-Process Communication
- T1106: Native API
- T1053: Scheduled Task/Job
- T1072: Software Deployment Tools
- T1569: System Services
- T1204: User Execution
- T1047: Windows Management Instrumentation

CASB
Isolation
ITM
PSAT

TA0003: Persistence

- T1197: BITS Jobs
- T1547: Boot or Logon Autostart Execution
- T1176: Browser Extensions
- T1136: Create Account
- T1133: External Remote Services
- T1053: Scheduled Task/Job
- T1078: Valid Accounts

CASB
ITM
PSAT

TA0004: Privilege Escalation

- T1547: Boot or Logon Autostart Execution
- T1053: Scheduled Task/Job
- T1078: Valid Accounts

CASB
ITM
PSAT

TA0005: Defense Evasion

- T1197: BITS Jobs
- T1221: Template Injection
- T1078: Valid Accounts

CASB
ITM
PSAT

TA0006: Credential Access

- T1056: Input Capture
- T1557: Man-in-the-Middle
- T1003: OS Credential Dumping
- T1528: Steal Application Access Token
- T1539: Steal Web Session Cookie
- T1111: Two-Factor Authentication Interception
- T1552: Unsecured Credentials

ITM
PSAT

TA0007: Discovery

- T1010: Application Window Discovery
- T1613: Container and Resource Discovery

ITM

TA0008: Lateral Movement

- T1534: Internal Spearphishing
- T1570: Lateral Tool Transfer
- T1021: Remote Services
- T1091: Replication Through Removable Media
- T1072: Software Deployment Tools

IMD
ITM
PSAT

TA0009: Collection

- T1560: Archive Collected Data
- T1119: Automated Collection
- T1530: Data from Cloud Storage Object
- T1213: Data from Information Repositories
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1025: Data from Removable Media
- T1114: Email Collection
- T1056: Input Capture
- T1185: Man in the Browser
- T1557: Man-in-the-Middle

CASB
ITM
PSAT

TA0011: Command and Control

- T1071: Application Layer Protocol
- T1092: Communication Through Removable Media
- T1105: Ingress Tool Transfer
- T1572: Protocol Tunneling
- T1090: Proxy
- T1219: Remote Access Software

ITM

TA0010: Exfiltration

- T1030: Data Transfer Size Limits
- T1048: Exfiltration Over Alternative Protocol
- T1011: Exfiltration Over Other Network Medium
- T1052: Exfiltration Over Physical Medium
- T1567: Exfiltration Over Web Service
- T1537: Transfer Data to Cloud Account

CASB
ITM

TA0040: Impact

- T1531: Account Access Removal
- T1485: Data Destruction
- T1496: Resource Hijacking

ITM

Products in Scope

Cloud App Security Broker (CASB), Email Fraud Defense (EFD), Email Protection (PPS), Insider Threat Management (ITM), Internal Mail Defense (IMD), Isolation, Security Awareness Training (PSAT), Targeted Attack Protection (TAP)

Mapping Risks – MITRE D3FEND v0.9.3-BETA-1

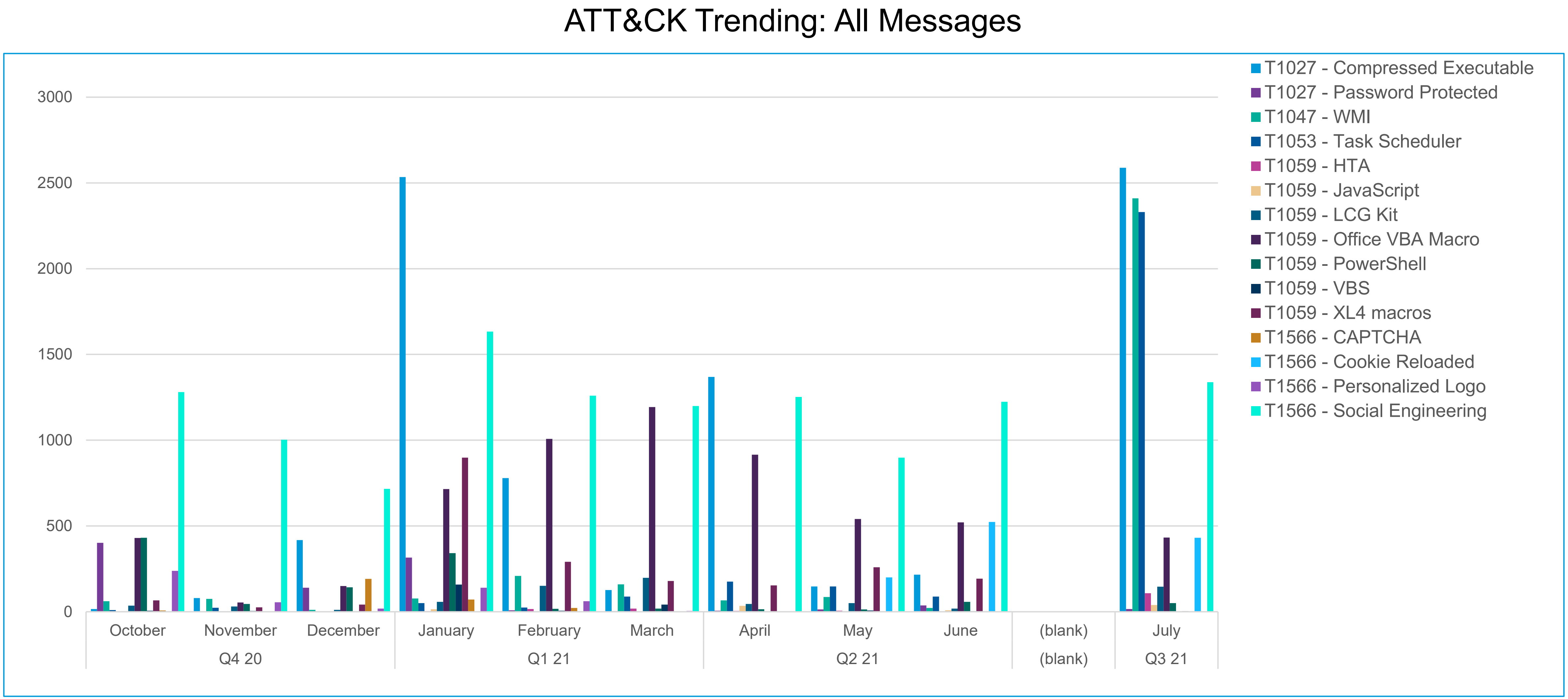
Harden	Detect	Isolate	Deceive	Evict
Application	**File Analysis**	**Execution Isolation**	Decoy Environment	**Credential Eviction**
Credential	**Identifier Analysis**	**Network Isolation**	Decoy Object	**Process Eviction**
Message	**Message Analysis**	↓		↓
Platform	**Network Traffic Analysis**	**ET** **Isolation** **ITM**		**CASB** **ITM**
↓	Platform Monitoring			
CASB **EFD** **Email Encryption** **PPS**	**Process Analysis**			
	User Behavior Analysis			
	↓			
	ET **ITM** **PPS** **TAP** **uDLP**			

Products in Scope

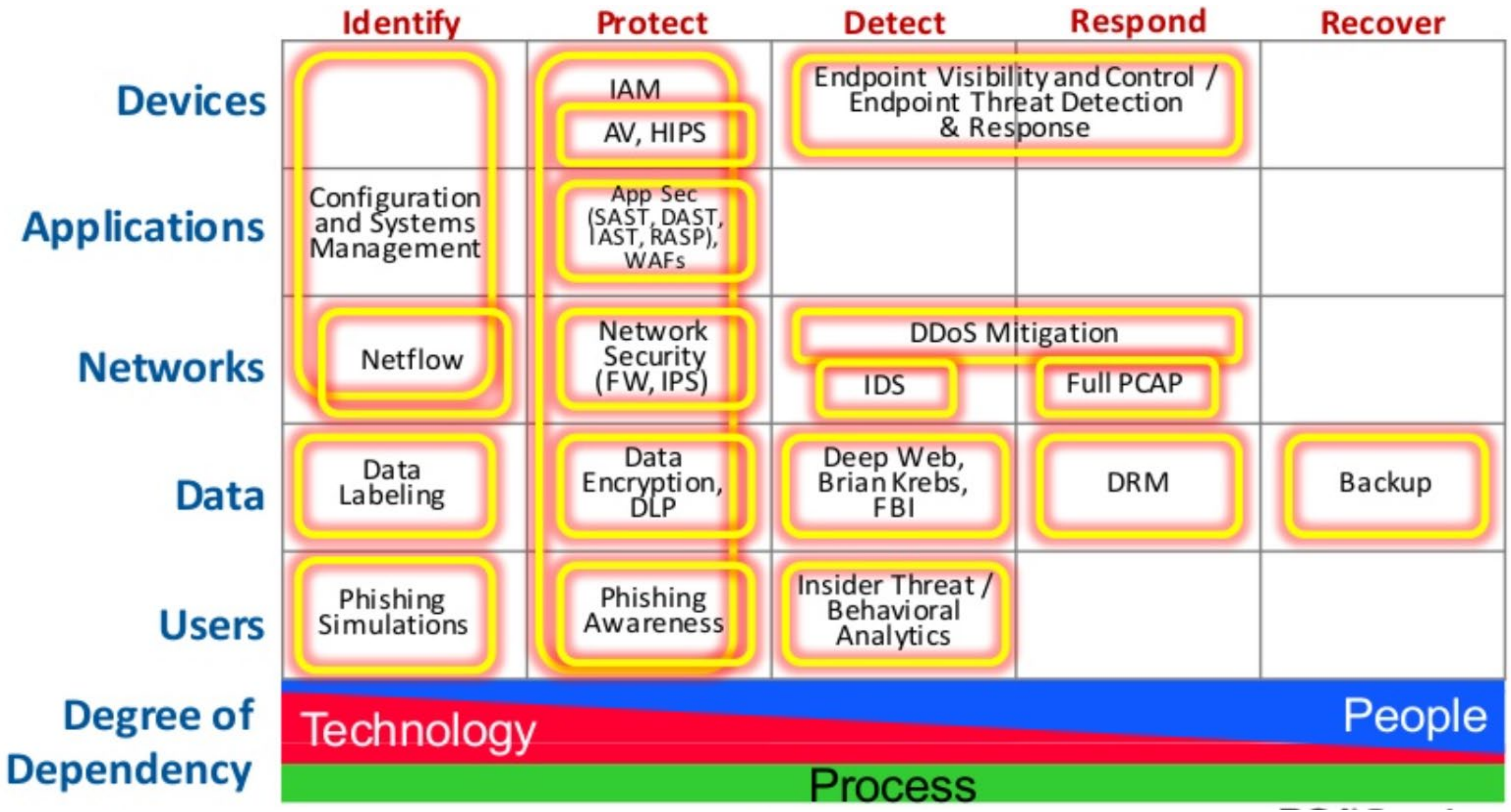
Cloud App Security Broker (CASB), Email Fraud Defense (EFD), Email Protection (PPS), Emerging Threats (ET), Insider Threat Management (ITM), Internal Mail Defense (IMD), Isolation, Targeted Attack Protection (TAP), Unified DLP for CASB, Email, Endpoint (uDLP)

Where mapping to ATT&CK makes sense

Trending



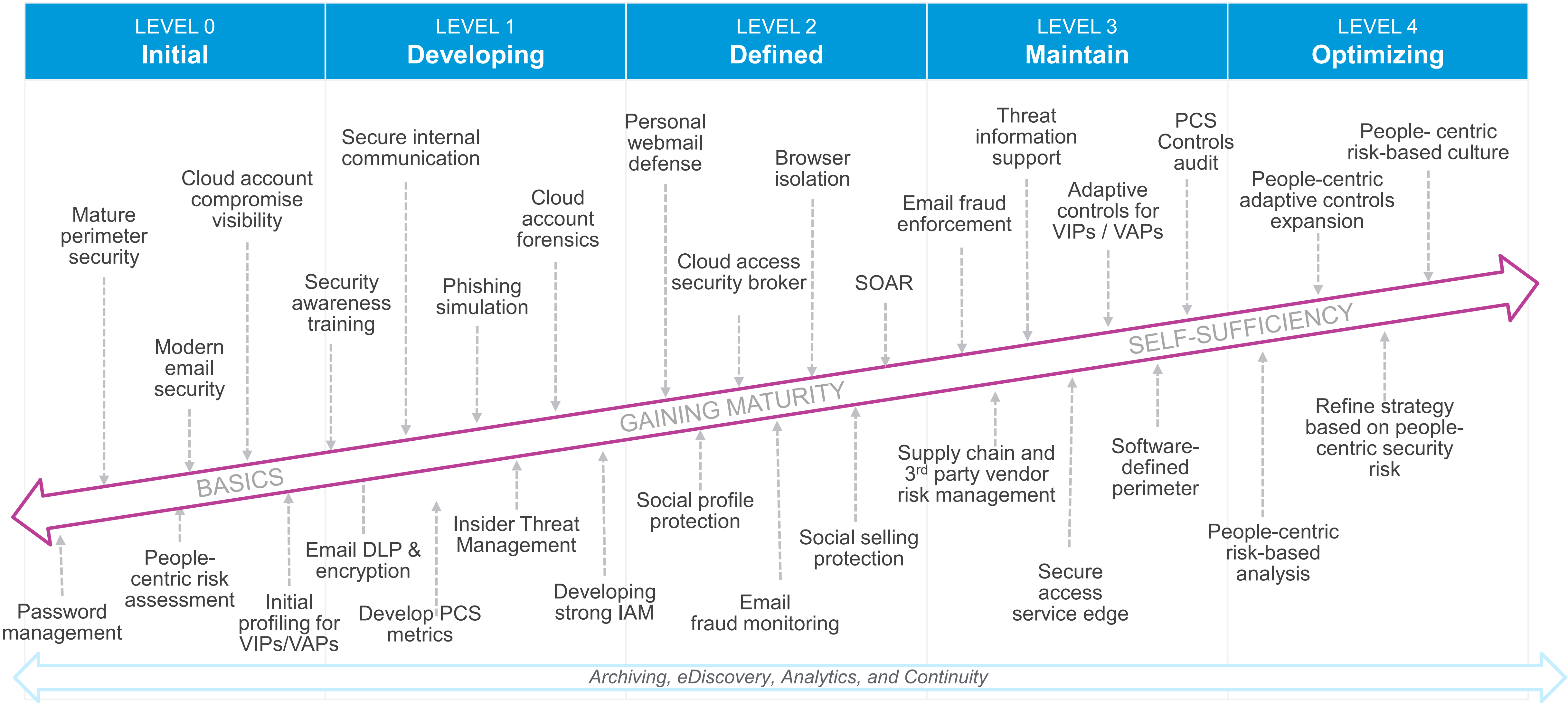
Mapping Risks – Cyber Defense Matrix



	Identify	Protect	Detect	Respond	Recover
Devices		IAM AV, HIPS	Endpoint Visibility and Control / Endpoint Threat Detection & Response		
Applications	Configuration and Systems Management	App Sec (SAST, DAST, IAST, RASP), WAFs			
Networks	Netflow	Network Security (FW, IPS)	DDoS Mitigation IDS	Full PCAP	
Data	Data Labeling	Data Encryption, DLP	Deep Web, Brian Krebs, FBI	DRM	Backup
Users	Phishing Simulations	Phishing Awareness	Insider Threat / Behavioral Analytics		

Source: *Sounil Yu, RSA 2016*

Mapping Risks – Maturity Modeling



LEVEL 0
Initial

LEVEL 1
Developing

LEVEL 2
Defined

LEVEL 3
Maintain

LEVEL 4
Optimizing

Mature perimeter security

Cloud account compromise visibility

Modern email security

Password management

People-centric risk assessment

Initial profiling for VIPs/VAPs

BASICS

Security awareness training

Secure internal communication

Phishing simulation

Cloud account forensics

Email DLP & encryption

Develop PCS metrics

Insider Threat Management

Developing strong IAM

Personal webmail defense

Cloud access security broker

Browser isolation

SOAR

GAINING MATURITY

Social profile protection

Email fraud monitoring

Social selling protection

Email fraud enforcement

Threat information support

Adaptive controls for VIPs / VAPs

PCS Controls audit

Supply chain and 3rd party vendor risk management

Secure access service edge

Software-defined perimeter

People-centric adaptive controls expansion

People- centric risk-based culture

SELF-SUFFICIENCY

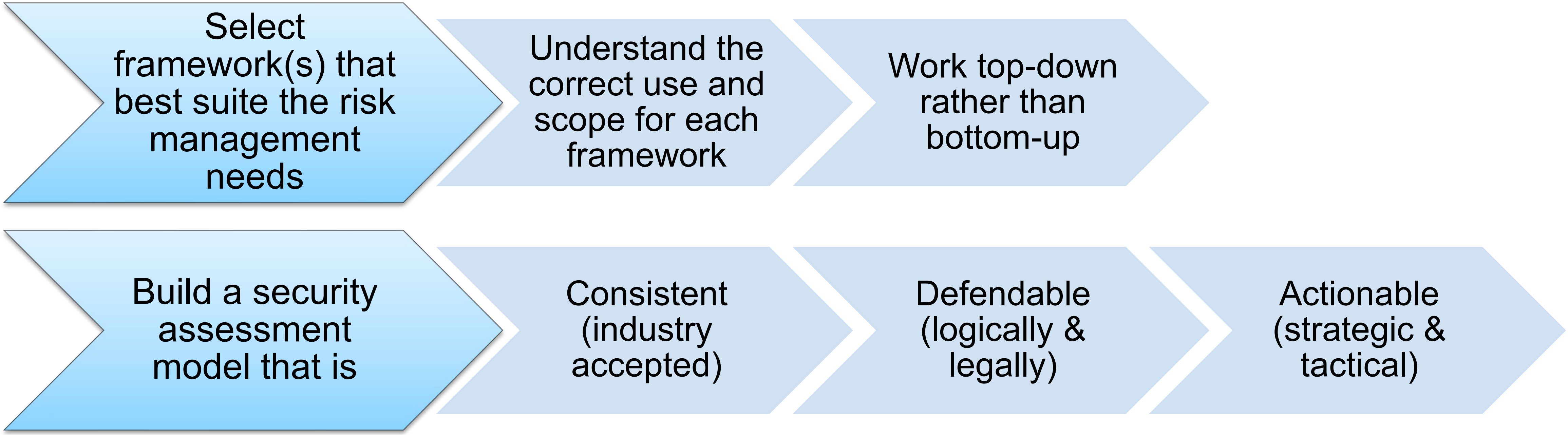
People-centric risk-based analysis

Refine strategy based on people-centric security risk

Archiving, eDiscovery, Analytics, and Continuity

Key Takeaways

Key Takeaways



Select framework(s) that best suite the risk management needs

Understand the correct use and scope for each framework

Work top-down rather than bottom-up

Build a security assessment model that is

Consistent (industry accepted)

Defendable (logically & legally)

Actionable (strategic & tactical)