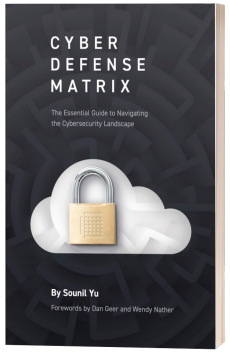
Simplifying QBRs with the Cyber Defense Matrix

Grab a free copy in the back courtesy of Connectwise (so that I don’t have to take it home!)



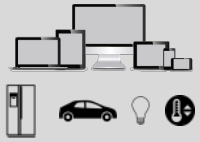
Sounil Yu
@sounilyu

The cybersecurity industry is full of jargon terms that make it difficult to communicate the value of the capabilities you offer to your customers and clients

One simple way to make cybersecurity more approachable is by aligning capabilities against five asset classes (nouns) and the NIST CSF (verbs)

Asset Classes

DEVICES



Workstations, servers, phones, tablets, storage, network devices, IoT, infrastructure, etc.

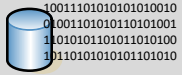
APPS

Software, APIs, webapps, microservices, and app flows on the devices

NETWORKS

Connections and traffic flowing among devices and apps

DATA



Information at rest, in transit, or in use by the resources above

USERS

The people using the resources listed above

Operational Functions

IDENTIFY

Inventorying assets and vulns, measuring attack surface, prioritizing, baselining normal, threat modeling, risk assessment

PROTECT

Preventing or limiting impact, patching, containing, isolating, hardening, managing access, vuln mitigation

DETECT

Discovering events, triggering on anomalies, hunting for intrusions, security analytics

RESPOND

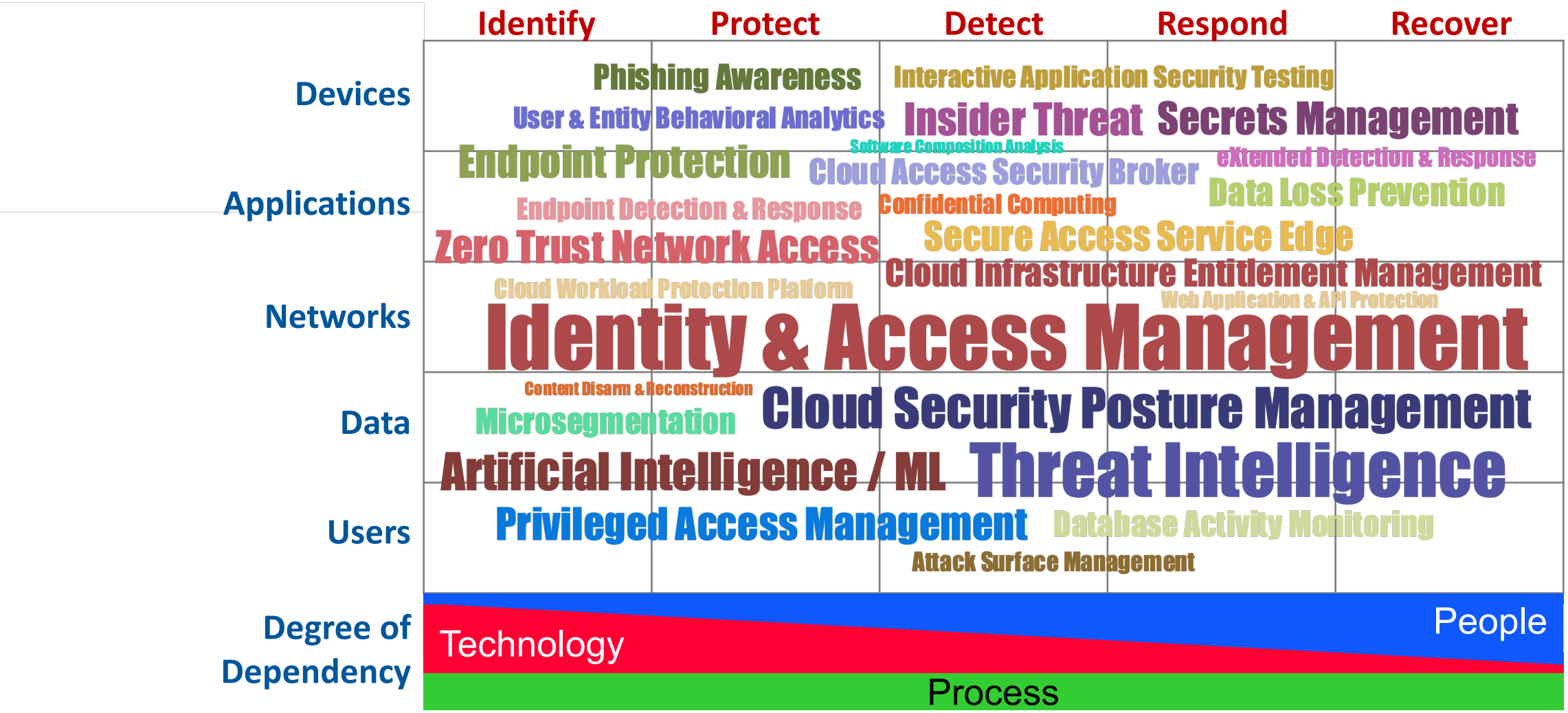
Acting on events, eradicating intrusion, assessing damage, forensic reconstruction

RECOVER

Returning to normal operations, restoring services, documenting lessons learned, resiliency

Introducing the Cyber Defense Matrix

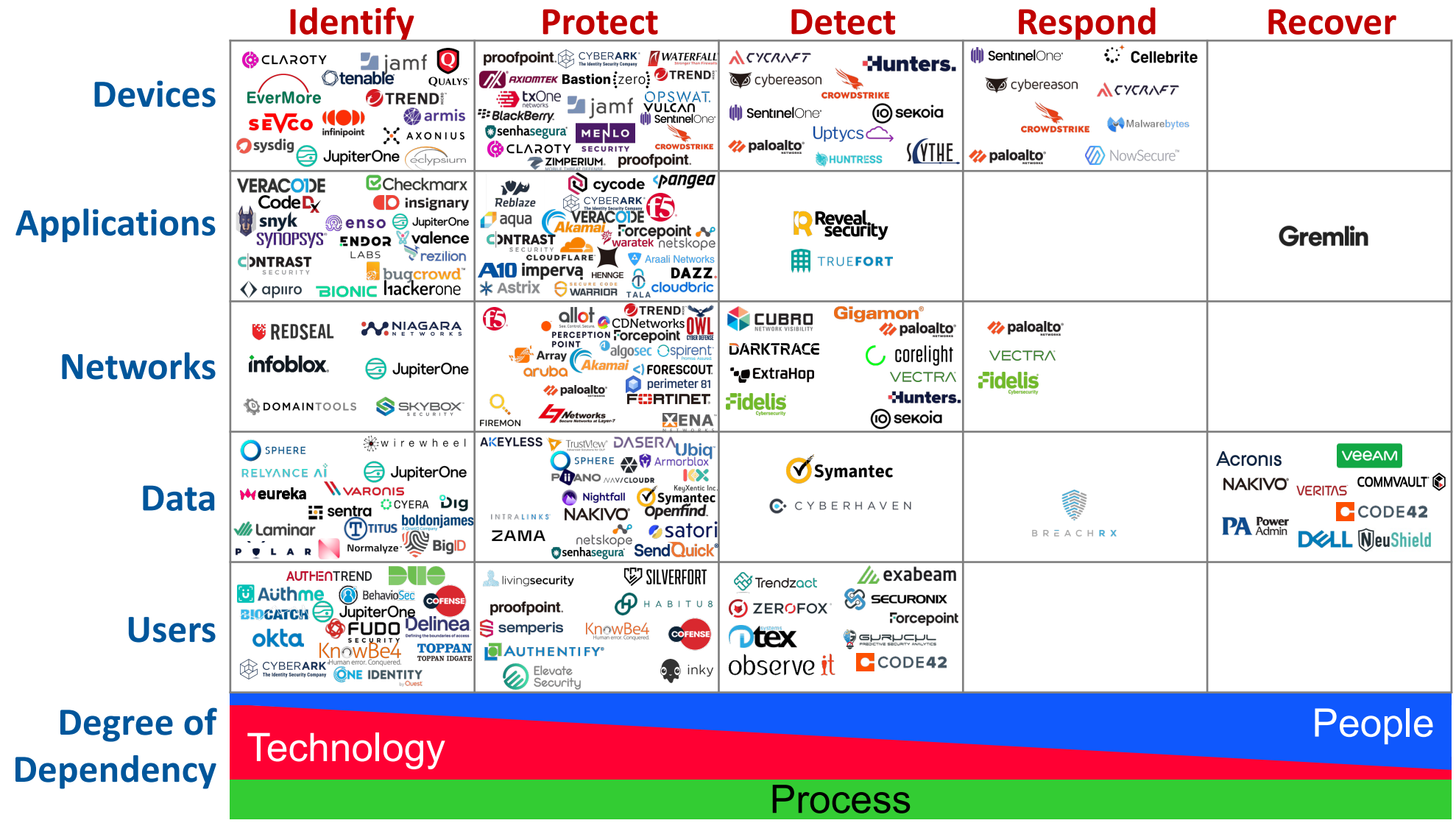
Testing the Cyber Defense Matrix against the marketing buzzwords…



… reveals how various cybersecurity capabilities align to problems being solved

	Identify	Protect	Detect	Respond	Recover
Devices	Asset Mgt, Vuln Scanning, Vuln Mgt, Certificate Mgt	AV, Anti-Malware, EPP, FIM, HIPS, Vuln Mitigation, Allowlisting	Endpoint Detection, UEBA, XDR	EP Response, EP Forensics, SOAR	
Applications	SAST, DAST, SW Asset Mgt, Fuzzers, Bug Bounty	RASP, WAF, ASOC, ZT App Access, API Security	Source Code Compromise, Logic Bomb Discovery, App IDS, XDR		
Networks	Netflow, Network Vuln Scanner	FW, IPS/IDS, Microseg, ESG, SWG, ZTNA	DDoS Detection, Net Traf Analysis, UEBA, XDR	DDoS Response, NW Forensics, SOAR	
Data	Data Audit, Discovery, Classification	Encryption, Tokenization, DLP, DRM, DBAM, DB Access Proxy	Deep Web, Data Behavior Analytics, FBI, Brian Krebs, XDR	DRM, Breach Response	Backup
Users	Phishing Sim, Background Chk, MFA, Human Risk Mgt	Sec Awareness & Training, Adaptive People Protection	Insider Threat, User Behavior Analytics, XDR, Human Det & Resp		
Degree of Dependency	People / Technology / Process				

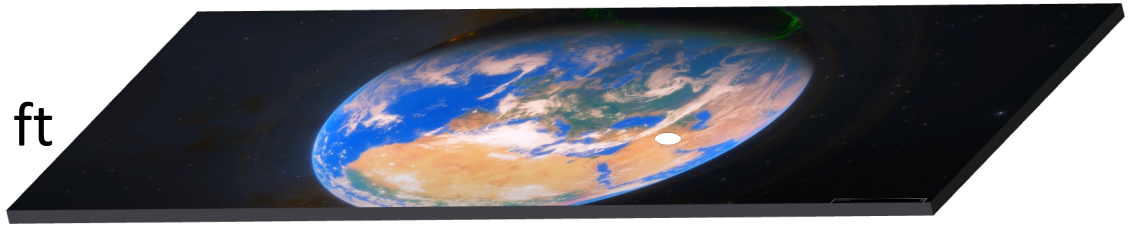
Example mapping of various vendors to the Cyber Defense Matrix



We need to choose the right map to communicate clearly

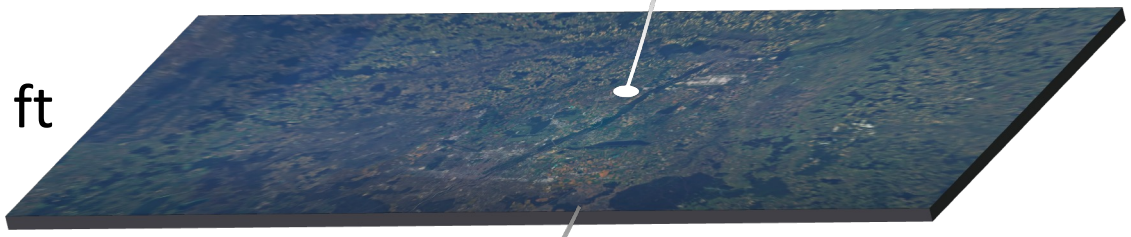
Strategic

50,000 ft



25,000 ft

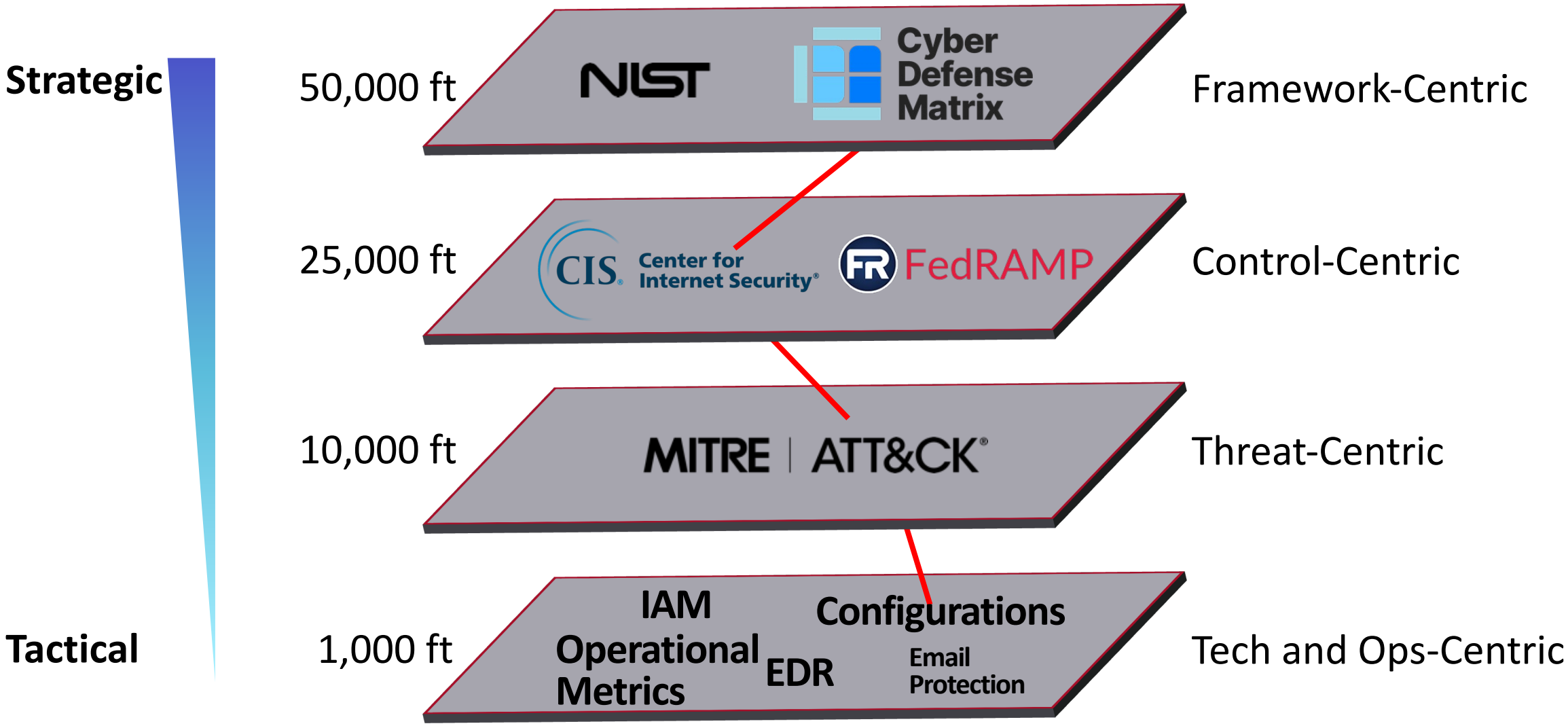
10,000 ft



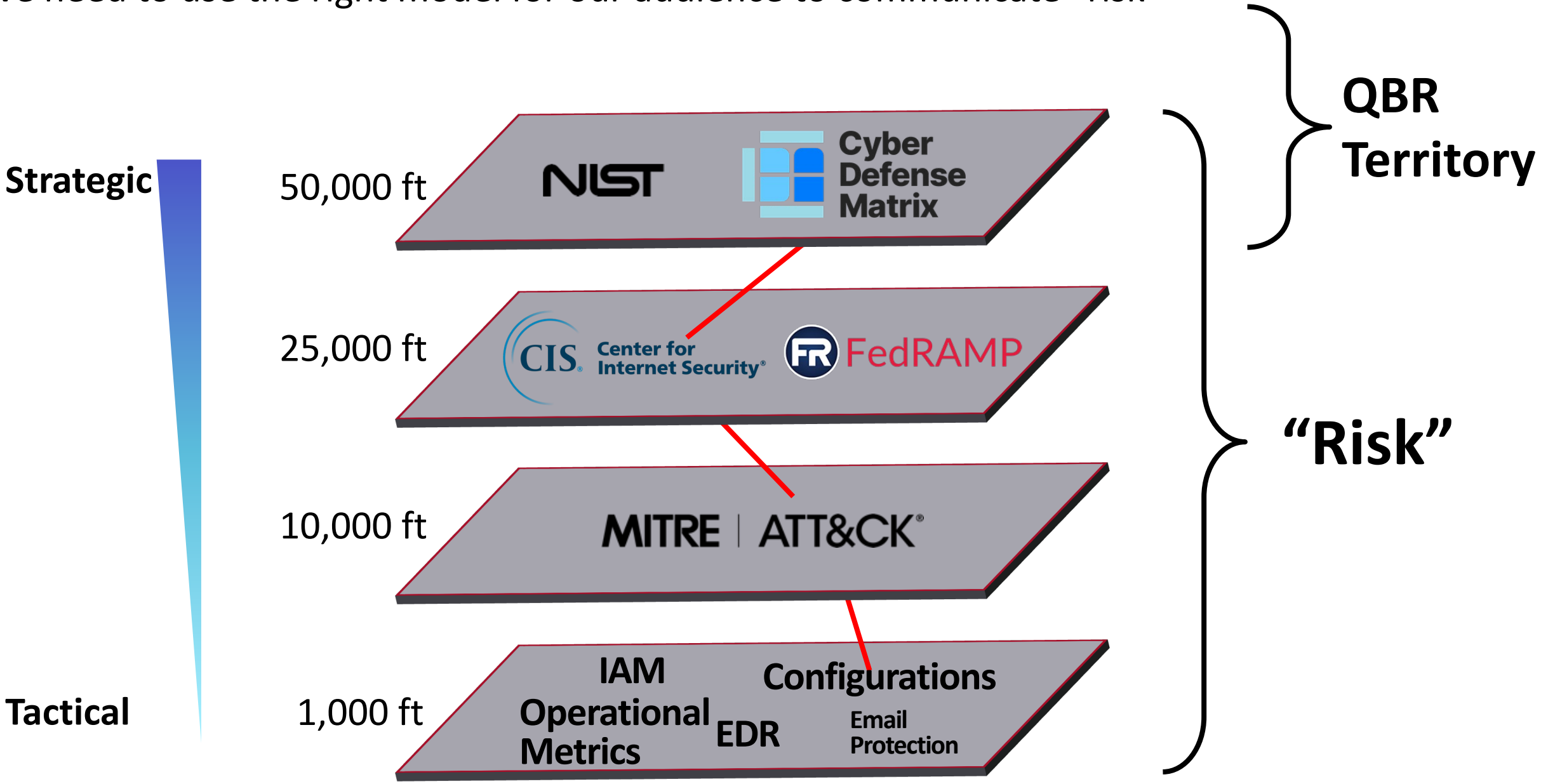
1,000 ft

Tactical

Cybersecurity has similar maps



We need to use the right model for our audience to communicate “risk”

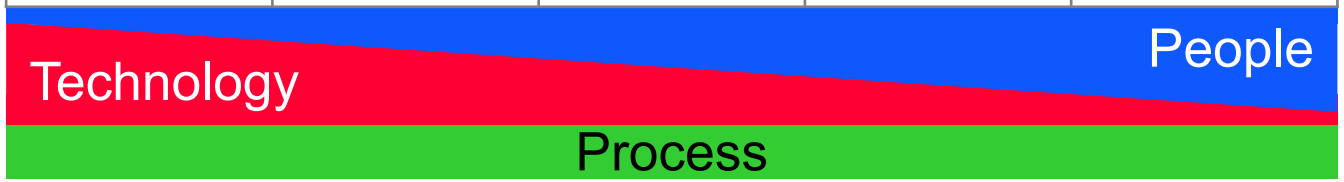


Playing Security Bingo… don’t play blackout!

What are the minimum effective tools and expertise needed to declare bingo?

	Identify	Protect	Detect	Respond	Recover
Devices		X	X		X
Applications	X	X		X	X
Networks	X		X	X	
Data		X	X		X
Users	X			X	

Degree of Dependency



Different layers of the Cyber Defense Matrix can help you profile and organize information related to your customer's specific needs

Foundation

Cyber Defense Matrix

Layer 1: Recipes

Proven Practices, Frameworks, Reference Architectures

Layer 2: Pantry

Current State Capabilities

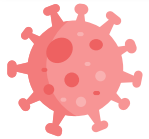
Layer 3: Market

Commercial Options

Layer 4: Allergies

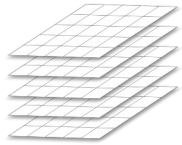
Business/Mission/Technology Constraints, Exceptions

Layer 5: Nutritional Needs



Risks, Attack Surfaces, Threat Environment

The "Stack"



Combined Matrices

Recipe Example: CIS Critical Security Controls

Implementation Group 1
Implementation Group 2
Implementation Group 3

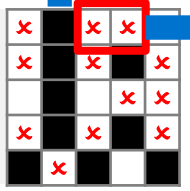
	Identify	Protect	Detect	Respond	Recover
Devices	1.1, 1.4	3.6, 4.4, 4.5, 4.8, 4.9, 4.11, 4.12, 10.1, 10.2, 10.3, 10.5, 10.6, 12.7, 12.8, 13.5, 13.7, 13.9	1.3, 1.5, 8.8, 10.4, 10.7, 13.2	1.2, 4.10	
Applications	2.1, 2.2, 7.5, 7.6, 15.1, 15.2, 15.3, 15.5, 18.6, 18.7, 18.8	2.5, 2.6, 2.7, 4.1, 7.1, 7.3, 7.4, 9.1, 9.4, 15.4, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13, 16.14, 18.9, 18.10	2.4	2.3, 7.2, 7.7	
Networks	12.4, 18.1, 18.2, 18.5	3.12, 4.2, 4.6, 8.1, 8.3, 8.4, 8.10, 9.2, 9.3, 9.5, 9.6, 9.7, 12.1, 12.2, 12.3, 12.5, 12.6, 13.4, 13.8, 13.10, 18.3, 18.4	8.2, 8.5, 8.6, 8.7, 8.9, 8.11, 13.1, 13.3, 13.6, 13.11		
Data	3.1, 3.2, 3.7, 3.8	3.3, 3.4, 3.5, 3.9, 3.10, 3.11, 3.13, 6.8, 11.3, 14.6, 15.7, 18.11	3.14, 8.12, 15.6		11.1, 11.2, 11.4, 11.5
Users	5.1, 5.5, 6.6	4.3, 4.7, 5.2, 5.4, 5.6, 6.1, 6.2, 6.3, 6.4, 6.5, 6.7, 14.1, 14.2, 14.3, 14.4, 14.5, 14.7, 14.8, 14.9		5.3	
Degree of Dependency	Technology				People
	Process			17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.9	17.7, 17.8

Allergy Example: Capturing Exceptions and Business Impacts

ILLUSTRATIVE

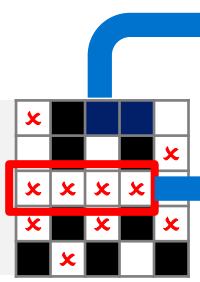
Allergy Example: Business and Technological Constraints

DEVELOPERS / DATA ANALYSTS



- Local Admin Rights Restriction as a protective control
- EDR as a less impactful, compensating, detective control

ICS / OT / MED ENVIRONMENTS



- No ability to modify or instrument the devices
- Network based controls as an alternative

Nutritional Needs: Threats and Safeguards Matrix (TaSM) by Ross Young

https://owasp.org/www-project-threat-and-safeguard-matrix/

Threats and Safeguards Matrix (TaSM)

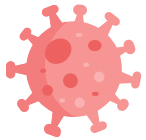
-An action-oriented view to safeguard and enable the business (Ross Young)

Threats	Functions & Safeguards				
	Identify	Protect	Detect	Respond	Recover
Phishing	Identity & Access Mgt - Active Directory User Info - Identify High Profile Accts - Role Based Email Privs	Awareness Training Email Security MFA Email Security Phishing Simulations Proxy Server	Deception Technology EDR Email Security Outlook Plugins User Reports	EDR Forensics Investigation Isolate / Quarantine Wipe Machine	Additional Training Post-Mortem (Blameless)
Ransomware	Audit Admin Accounts Identify Critical Systems - PCI / HIPAA / ... Resiliency Requirements Tabletop Exercises	AV / Endpoint protection Email Security Least Privilege Accounts Offline Backups Password Complexity Reqs	Deception Technology EDR Intrusion Detection Logging/Monitoring User Reports	Contact Law Enforcement EDR Forensics Investigation Identify Infection Vector Patching / Refreshing	Backups Business Continuity Plans Disaster Recovery Tests Public Disclosures
Web App Attacks	API Gateway Asset Management CMDB Digital Footprint Monitoring	AppSec Testing Bug Bounty Programs Pentesting / Red Teams Secure Configs / Patching WAF / RASP	IDS / SIEM Logging / Monitoring - App logs - Network - WAF / RASP	Block IP addresses Disable Connectivity Enable DLP Responses Fix Vulnerabilities Forensics Investigation	Audit/Evaluate Controls - WAF / RASP Enhance - Logging / Monitoring
Vendor & Partner Data Loss	Risk Assessments - Example CAIQ / SIG - ISO 27001 / SOC2 Type 2 Supply Chain Risk Mgt	Access Control Contract Agreements Vendor Monitoring	Cyber Threat Intel Vendor Self Reporting	Disable Connectivity Remove Data	Investigation Report Modify Contract Language

Nutritional Needs: Community Defense Model for Ransomware

Implementation Group 1
Implementation Group 2
Implementation Group 3

	Identify	Protect	Detect	Respond	Recover
Devices		4.4, 4.5, 10.1, 10.2, 10.3			
Applications	2.1, 2.2	4.1, 7.1, 7.3, 7.4, 9.1		2.3, 7.2	
Networks		4.2, 4.6, 8.1, 8.3, 9.2, 12.1	8.2		
Data	3.1, 3.2	3.3, 3.4, 11.3, 14.6			11.1, 11.2, 11.4
Users	5.1	4.7, 5.2, 5.4, 6.1, 6.2, 6.3, 6.4, 6.5, 14.1, 14.2, 14.3, 14.4, 14.5		5.3	
Degree of Dependency	Technology				People
	Process				



Nutritional Needs: Community Defense Model for Ransomware

Implementation Group 1
Implementation Group 2
Implementation Group 3

	Identify	Protect	Detect	Respond	Recover
Devices		4.4, 4.5, 10.1, 10.2, 10.3			
Applications	2.1, 2.2	4.1, 7.1, 7.3, 7.4, 9.1		2.3, 7.2	
Networks		4.2, 4.6, 8.1, 8.3, 9.2, 12.1	8.2		
Data	3.1, 3.2	3.3, 3.4, 11.3, 14.6			11.1, 11.2, 11.4
Users	5.1	4.7, 5.2, 5.4, 6.1, 6.2, 6.3, 6.4, 6.5, 14.1, 14.2, 14.3, 14.4, 14.5		5.3	

Degree of Dependency

People

Technology

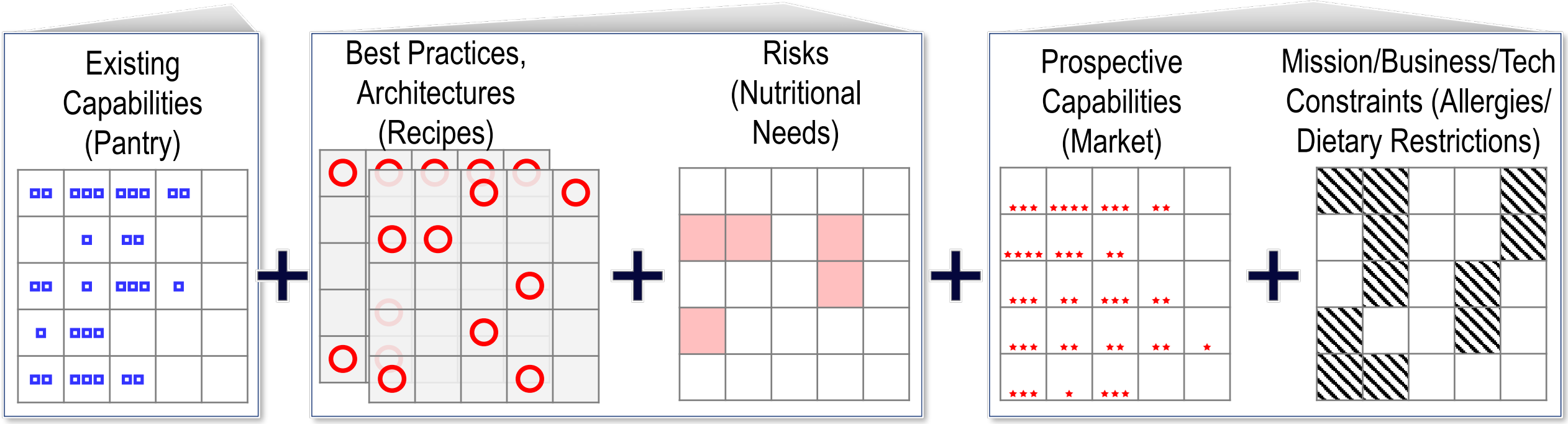
Process

The combination of the layers help us quickly understand our current security posture and the options for improving it

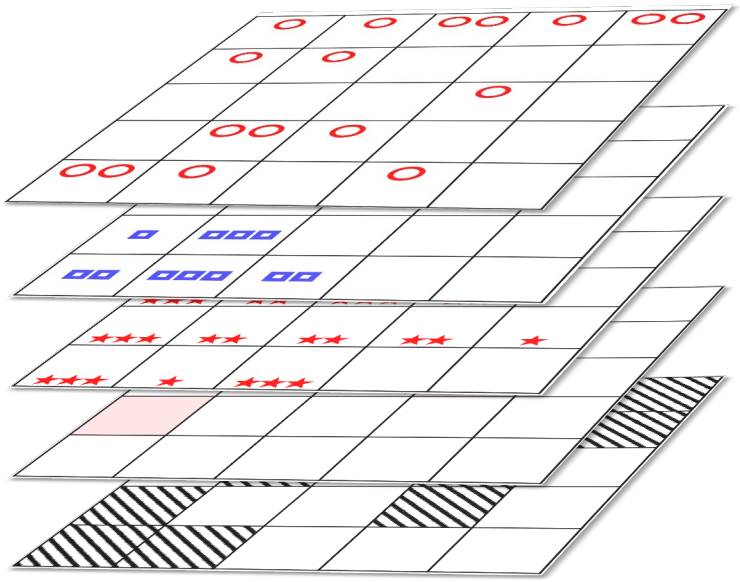
How secure am I?

How secure should I be?

How do I get there?



A combined view of all the layers provides a way to understand the decision space and the range of risk management options



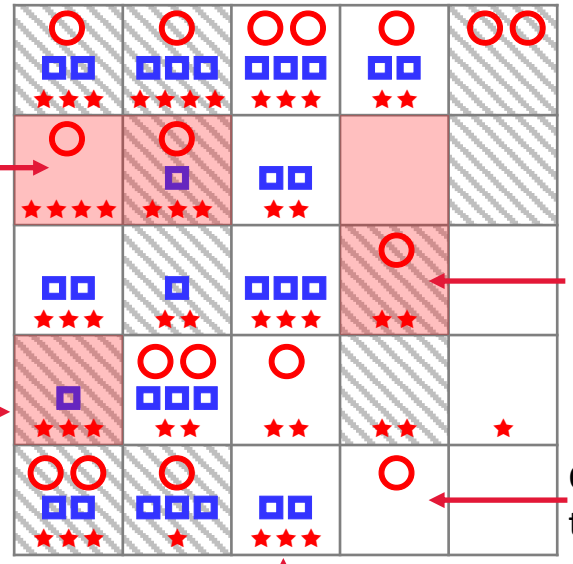


Table stakes /
Just do it

Risk Management Discussion:
- Active attacks underway
- Regulatory requirement
- Capabilities are available...
- … but controls create major mission impact

Risk Management Discussion:
- Active attacks underway
- No regulatory requirement
- Capabilities are available...
- … but controls create minor mission impact

Opportunities
to innovate

Opportunities
to deprecate
or capture
best practice

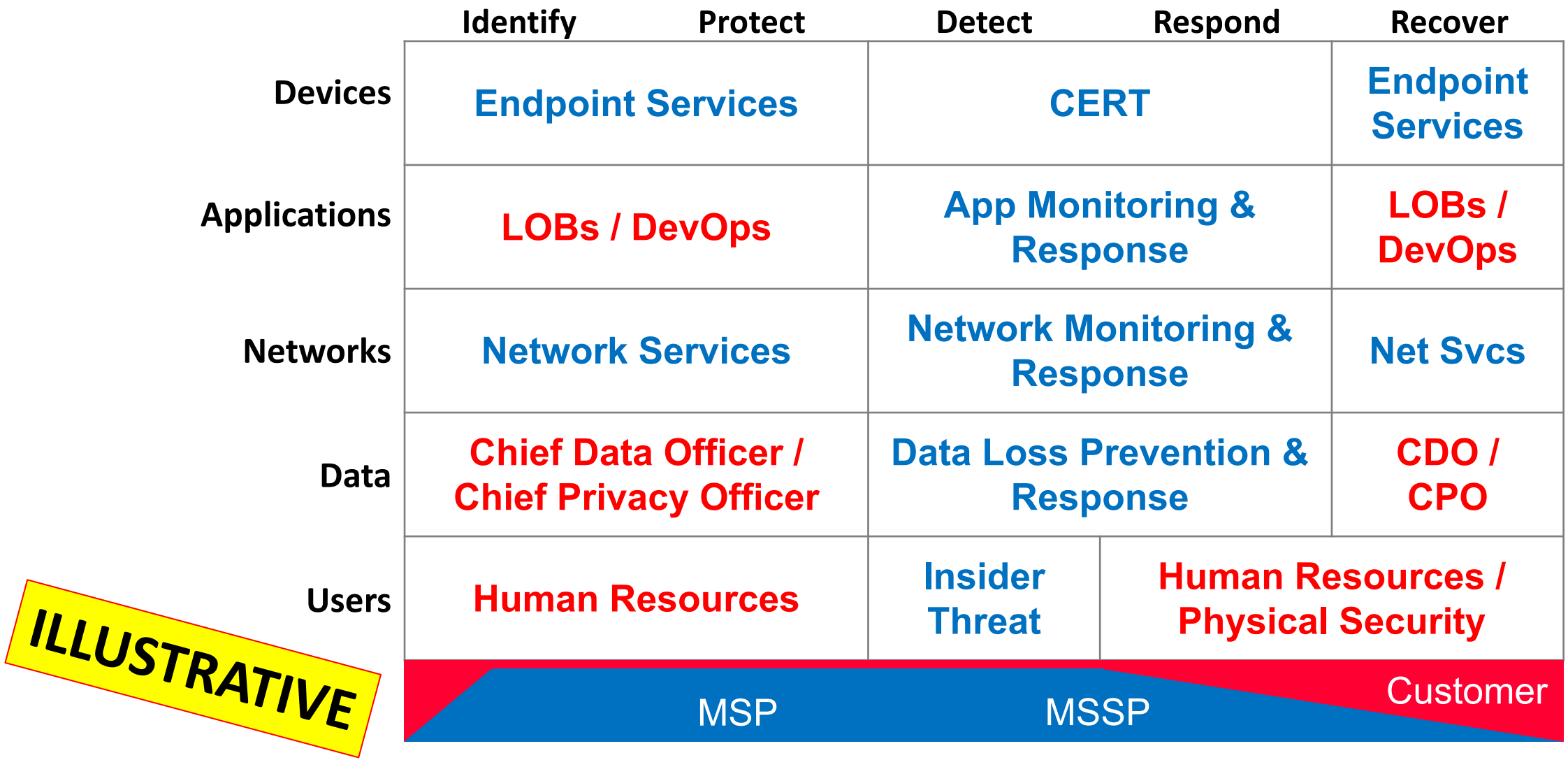
Architectural Requirements
Existing Capabilities
Commercial Capabilities
Attack Surfaces
Business/Mission Constraints

Other Use Cases: Understand how to balance your portfolio without breaking the bank

	Identify	Protect	Detect	Respond	Recover	Total
Devices		$50	$100		$50	$200
Applications	$50	$100		$50	$100	$300
Networks	$100		$100	$50		$250
Data		$50	$50		$50	$150
Users	$50			$50		$100
Total	$200	$200	$250	$150	$200	$1000

ILLUSTRATIVE

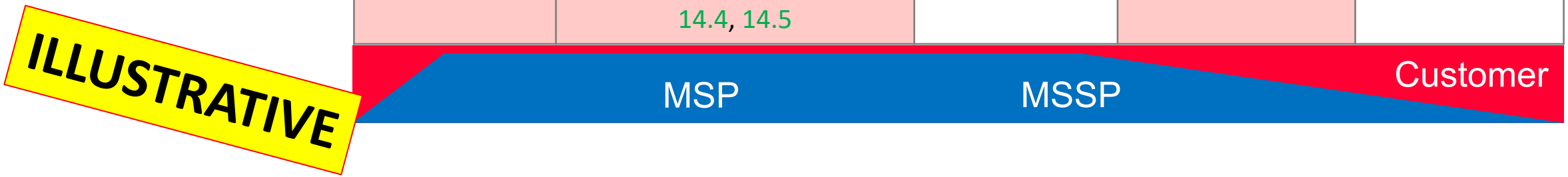
Other Use Cases: MSP Handoffs and Responsibilities



Dividing Responsibilities with the Customer in Ransomware Protection (Not correct, purely illustrative)

MSP Responsibility
Customer Responsibility
Shared Responsibility w/MSP Lead
Shared Responsibility w/Customer Lead

	Identify	Protect	Detect	Respond	Recover
Devices		4.4, 4.5, 10.1, 10.2, 10.3			
Applications	2.1, 2.2	4.1, 7.1, 7.3, 7.4, 9.1		2.3, 7.2	
Networks		4.2, 4.6, 8.1, 8.3, 9.2, 12.1	8.2		
Data	3.1, 3.2	3.3, 3.4, 11.3, 14.6			11.1, 11.2, 11.4
Users	5.1	4.7, 5.2, 5.4, 6.1, 6.2, 6.3, 6.4, 6.5, 14.1, 14.2, 14.3, 14.4, 14.5		5.3	



ILLUSTRATIVE

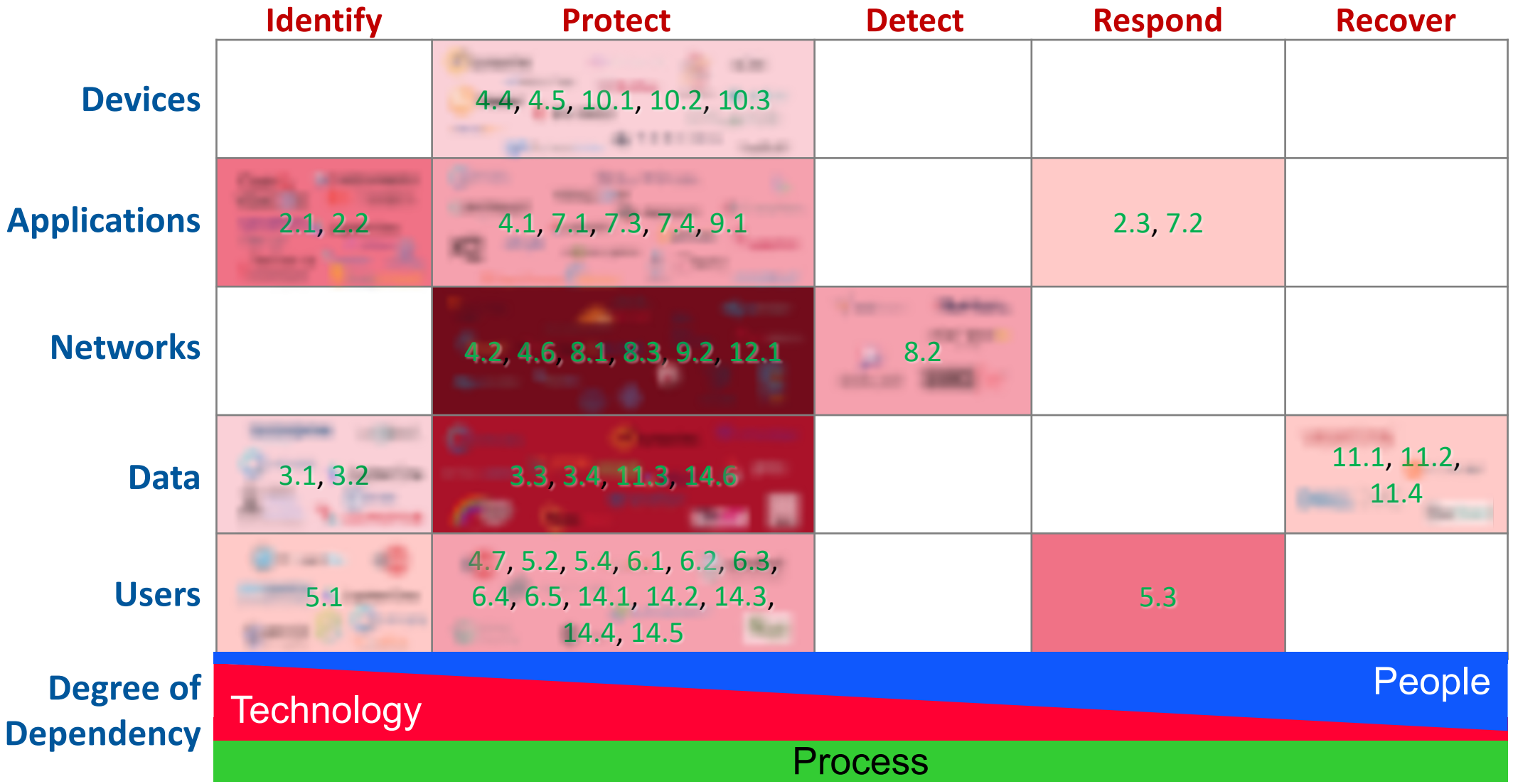
Client XYZ Cyber Defense Matrix
(by Andrew Szokoly at Proda Technology, https://prodatechnology.com)

	Identify $ Asset Management	Protect $$ Defense Against Threats	Detect $$$ Security Incident	Respond $$$$ Security Incident Response	Recover $$$$$ Restore After Incident
Devices	• RMM Automated Asset Discovery • Continuous Vulnerability Scanning • Group Policy Discovery / Hardening Policies • Documentation Automation • Mobile Device Management • Annual Risk Review / Assessment	• RMM Patching / Healing / Alerting • Endpoint Ransomware Protection • Asset Lifecycle Management • Endpoint DNS Filtering • AV / Centralized Management • Spam Filtering • Group Policy Discovery / Hardening Policies • Advanced Email Security (Advanced Threat Protection) • AI Based AV with 7x24 Security Operations Center • Privileged Access Management (& Device MFA) • Radius Wireless • Privilege Elevation Management (Request to Install) • Mobile Device Management	• AV / Centralized Management • RMM Patching / Healing / Alerting • Endpoint Ransomware Protection • Endpoint DNS Filtering • AI Based AV with 7x24 Security Operations Center • SIEM with 7x24 SOC (Logging and Detection)	• Endpoint Ransomware Protection • AI Based AV with 7x24 Security Operations Center • SIEM with 7x24 SOC (Logging and Detection) • Centralized Change Reporting • Cyberinsurance / Ransomware Insurance	• Centralized Change Reporting • Segregated Server and Workstation Backups • Server Cloud Replication (DR Hot Site) • Cyberinsurance / Ransomware Insurance • Disaster Recovery Plan
Apps	• Automated Asset Discovery • Continuous Vulnerability Scanning • Continuous Security Auditing / Management • Business Impact Analysis • Privilege Elevation Management (Request to Install) • Annual Risk Review / Assessment	• Application Single Sign On (SSO) • Domain DNS Protection • Password Management • Mobile Application Management		• Cyberinsurance / Ransomware Insurance	• Cyberinsurance / Ransomware Insurance • Disaster Recovery Plan
Networks	• Continuous Vulnerability Scanning • Documentation Automation • Annual Risk Review / Assessment	• RMM Patching / Healing / Alerting • Asset Lifecycle Management • Next Generation Firewall with Service Agreement • SIEM with 7x24 SOC (Logging and Detection) • Endpoint DNS Filtering • Privileged Access Management (& Device MFA) • Radius Wireless • Domain DNS Protection	• Endpoint DNS Filtering • SIEM with 7x24 SOC (Logging and Detection) • Domain DNS Protection • Bandwidth Monitoring • Network Management	• SIEM with 7x24 SOC (Logging and Detection) • Centralized Change Reporting • AI Based AV with 7x24 Security Operations Center • Cyberinsurance / Ransomware Insurance	• Centralized Change Reporting • Network Management • Disaster Recovery Plan
Data	• DataLoss Prevention (DLP) in M365 • Continuous Vulnerability Scanning • Documentation Automation • Automated Identification of M365 Groups • Annual Risk Review / Assessment	• Group Policy Discovery / Hardening Policies • Endpoint DNS Filtering • Application Single Sign On (SSO) • Privileged Access Management (& Device MFA) • Domain DNS Protection • DataLoss Prevention (DLP) in M365 • AI Based AV with 7x24 Security Operations Center • Email Encryption • Mobile Device Management	• Darkweb Scanning (For Stolen Credentials) • Email Encryption • Bandwidth Monitoring • Mobile Device Management	• Cyberinsurance / Ransomware Insurance	• Segregated Server and Workstation Backups • Server Cloud Replication (DR Hot Site) • Disaster Recovery Plan
Users	• Darkweb Scanning (For Stolen Credentials) • Continuous Security Auditing / Management • Documentation Automation • Annual Risk Review / Assessment	• Spam Filtering • Security Awareness Training • Phishing Simulation • Self Service Password Reset (Identity Verification) • Privileged Access Management (& Device MFA) • Password Management • Radius Wireless • Advanced Email Security (Advanced Threat Protection) • Privilege Elevation Management (Request to Install) • Mobile Device Management		• Cyberinsurance / Ransomware Insurance • Incident Response Plan	

In Place Today

Available Services and Projects

Emerging threats change priorities



Combining Emerging Threats with Andrew's version of the Cyber Defense Matrix

	Identify $ Asset Management	Protect $$ Defense Against Threats	Detect $$$ Security Incident	Respond $$$$ Security Incident Response	Recover $$$$$ Restore After Incident
Devices	• RMM Automated Asset Discovery • Continuous Vulnerability Scanning • Group Policy Discovery / Hardening Policies • Documentation Automation • Mobile Device Management • Annual Risk Review / Assessment	• RMM Patching / Healing / Alerting • Endpoint Ransomware Protection • Asset Lifecycle Management • Endpoint DNS Filtering • AV / Centralized Management • Spam Filtering • Group Policy Discovery / Hardening Policies • Advanced Email Security (Advanced Threat Protection) • AI Based AV with 7x24 Security Operations Center • Privileged Access Management (& Device MFA) • Radius Wireless • Privilege Elevation Management (Request to Install) • Mobile Device Management	• AV / Centralized Management • RMM Patching / Healing / Alerting • Endpoint Ransomware Protection • Endpoint DNS Filtering • AI Based AV with 7x24 Security Operations Center • SIEM with 7x24 SOC (Logging and Detection)	• Endpoint Ransomware Protection • AI Based AV with 7x24 Security Operations Center • SIEM with 7x24 SOC (Logging and Detection) • Centralized Change Reporting • Cyberinsurance / Ransomware Insurance	• Centralized Change Reporting • Segregated Server and Workstation Backups • Server Cloud Replication (DR Hot Site) • Cyberinsurance / Ransomware Insurance • Disaster Recovery Plan
Apps	• Automated Asset Discovery • Continuous Vulnerability Scanning • Continuous Security Auditing / Management • Business Impact Analysis • Privilege Elevation Management (Request to Install) • Annual Risk Review / Assessment	• Application Single Sign On (SSO) • Domain DNS Protection • Password Management • Mobile Application Management		• Cyberinsurance / Ransomware Insurance	• Cyberinsurance / Ransomware Insurance • Disaster Recovery Plan
Networks	• Continuous Vulnerability Scanning • Documentation Automation • Annual Risk Review / Assessment	• RMM Patching / Healing / Alerting • Asset Lifecycle Management • Next Generation Firewall with Service Agreement • SIEM with 7x24 SOC (Logging and Detection) • Endpoint DNS Filtering • Privileged Access Management (& Device MFA) • Radius Wireless • Domain DNS Protection	• Endpoint DNS Filtering • SIEM with 7x24 SOC (Logging and Detection) • Domain DNS Protection • Bandwidth Monitoring • Network Management	• SIEM with 7x24 SOC (Logging and Detection) • Centralized Change Reporting • AI Based AV with 7x24 Security Operations Center • Cyberinsurance / Ransomware Insurance	• Centralized Change Reporting • Network Management • Disaster Recovery Plan
Data	• DataLoss Prevention (DLP) in M365 • Continuous Vulnerability Scanning • Documentation Automation • Automated Identification of M365 Groups • Annual Risk Review / Assessment	• Group Policy Discovery / Hardening Policies • Endpoint DNS Filtering • Application Single Sign On (SSO) • Privileged Access Management (& Device MFA) • Domain DNS Protection • DataLoss Prevention (DLP) in M365 • AI Based AV with 7x24 Security Operations Center • Email Encryption • Mobile Device Management	• Darkweb Scanning (For Stolen Credentials) • Email Encryption • Bandwidth Monitoring • Mobile Device Management	• Cyberinsurance / Ransomware Insurance	• Segregated Server and Workstation Backups • Server Cloud Replication (DR Hot Site) • Disaster Recovery Plan
Users	• Darkweb Scanning (For Stolen Credentials) • Continuous Security Auditing / Management • Documentation Automation • Annual Risk Review / Assessment	• Spam Filtering • Security Awareness Training • Phishing Simulation • Self Service Password Reset (Identity Verification) • Privileged Access Management (& Device MFA) • Password Management • Radius Wireless • Advanced Email Security (Advanced Threat Protection) • Privilege Elevation Management (Request to Install) • Mobile Device Management		• Cyberinsurance / Ransomware Insurance • Incident Response Plan	

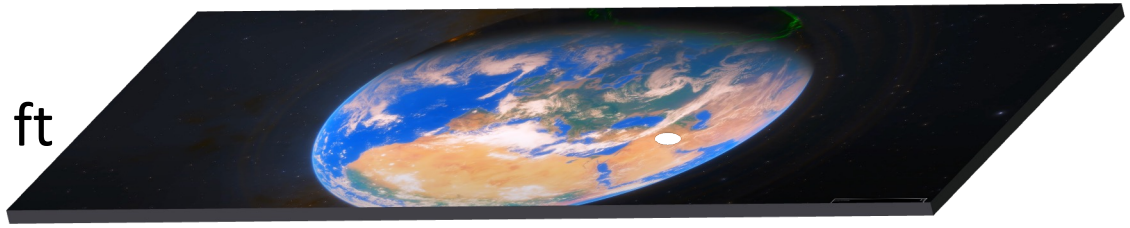
In Place Today

Available Services and Projects

Remember to choose the right map to communicate clearly

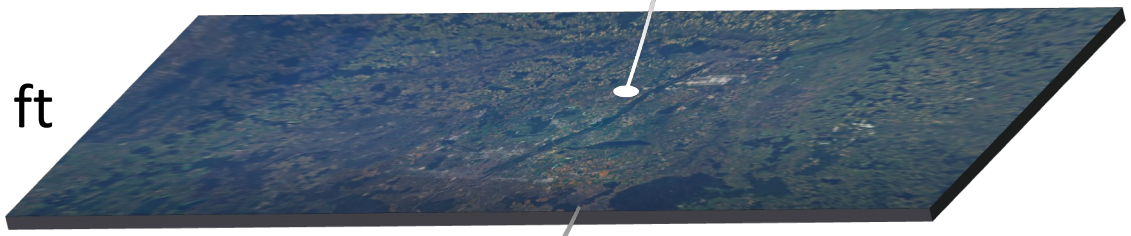
Strategic

50,000 ft



25,000 ft

10,000 ft



1,000 ft

Tactical

Cyber Defense Matrix

Questions?

 @sounilyu

 @cyberdefmatrix

 sounil@cyberdefensematrix.com

 https://cyberdefensematrix.com

 https://www.linkedin.com/in/sounil

 https://www.slideshare.net/sounilyu/presentations