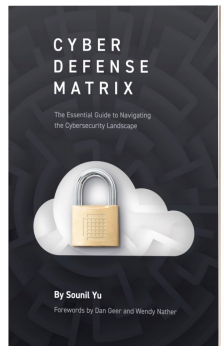


Simplifying QBRs with the Cyber Defense Matrix

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

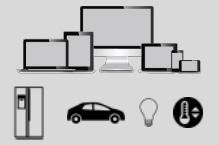
Phishing Awareness **Interactive Application Security Testing**
User & Entity Behavioral Analytics **Insider Threat** **Secrets Management**
Endpoint Protection **Software Composition Analysis** **eXtended Detection & Response**
Cloud Access Security Broker **Data Loss Prevention**
Endpoint Detection & Response **Confidential Computing**
Zero Trust Network Access **Secure Access Service Edge**
Cloud Workload Protection Platform **Cloud Infrastructure Entitlement Management**
Identity & Access Management **Web Application & API Protection**
Content Disarm & Reconstruction **Cloud Security Posture Management**
Microsegmentation **Artificial Intelligence / ML** **Threat Intelligence**
Privileged Access Management **Database Activity Monitoring**
Attack Surface Management

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

Phishing Awareness Interactive Application Security Testing
 User & Entity Behavioral Analytics Insider Threat Secrets Management
 Endpoint Protection Cloud Access Security Broker Automated Detection & Response
 Endpoint Detection & Response Confidential Computing Data Loss Prevention
 Zero Trust Network Access Secure Access Service Edge
 Cloud Infrastructure Entitlement Management
 Identity & Access Management
 Microsegmentation Cloud Security Posture Management
 Artificial Intelligence / ML Threat Intelligence
 Privileged Access Management Database Activity Monitoring
 Attack Surface Management

Asset Classes

DEVICES



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

APPS



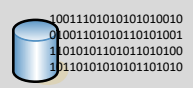
Software, APIs, webapps, microservices, and app flows on the devices

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



Inventorizing 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



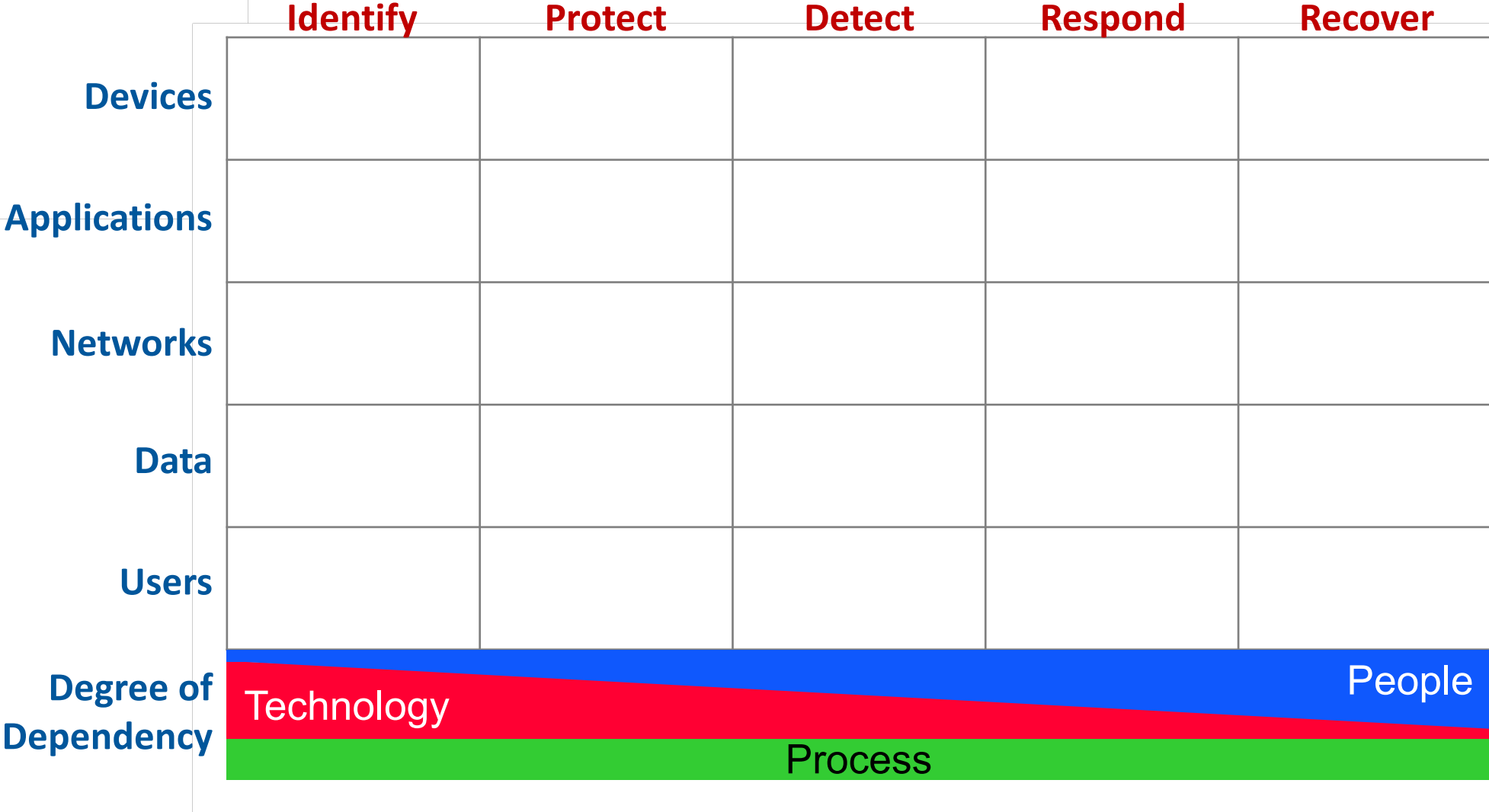
Acting on events, eradicating intrusion, assessing damage, forensic reconstruction

RECOVER



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

Introducing the Cyber Defense Matrix



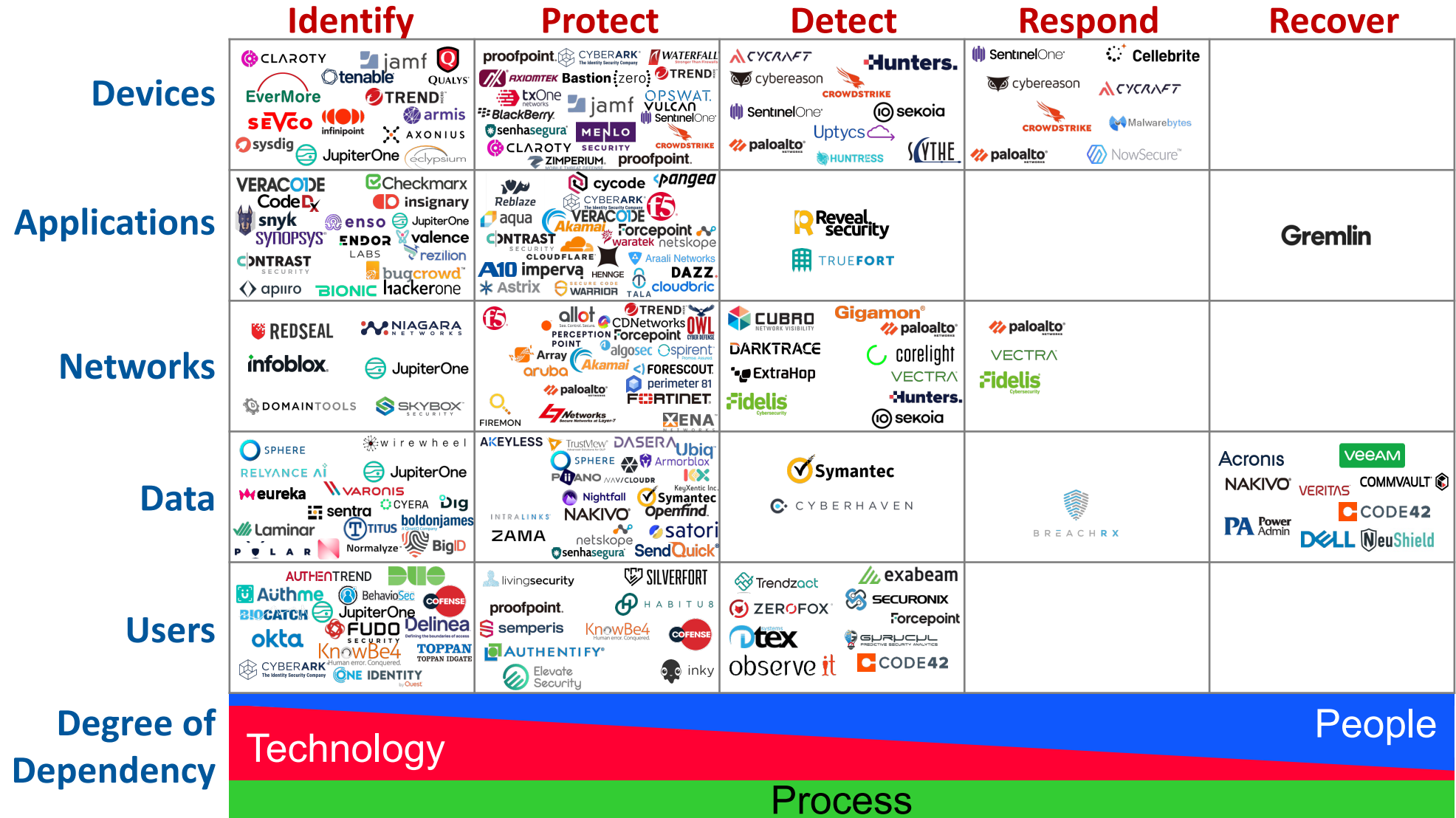
Testing the Cyber Defense Matrix against the marketing buzzwords...



... 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 | Technology | | | | People |
| | Process | | | | |

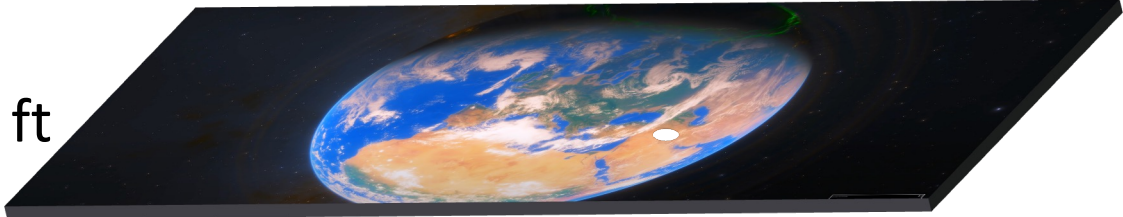
Example mapping of various vendors to the Cyber Defense Matrix



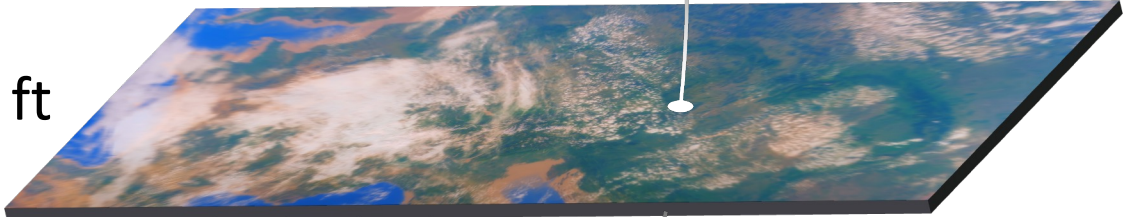
We need to choose the right map to communicate clearly

Strategic

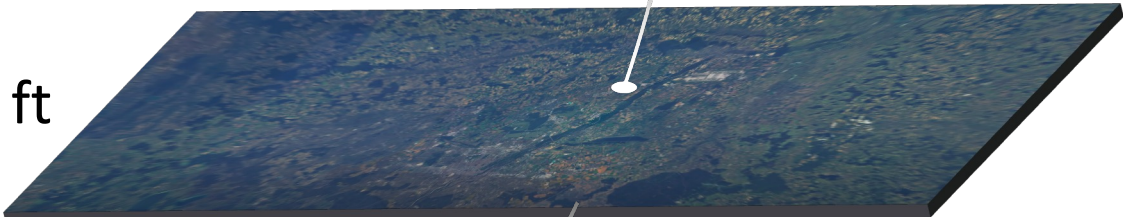
50,000 ft



25,000 ft



10,000 ft

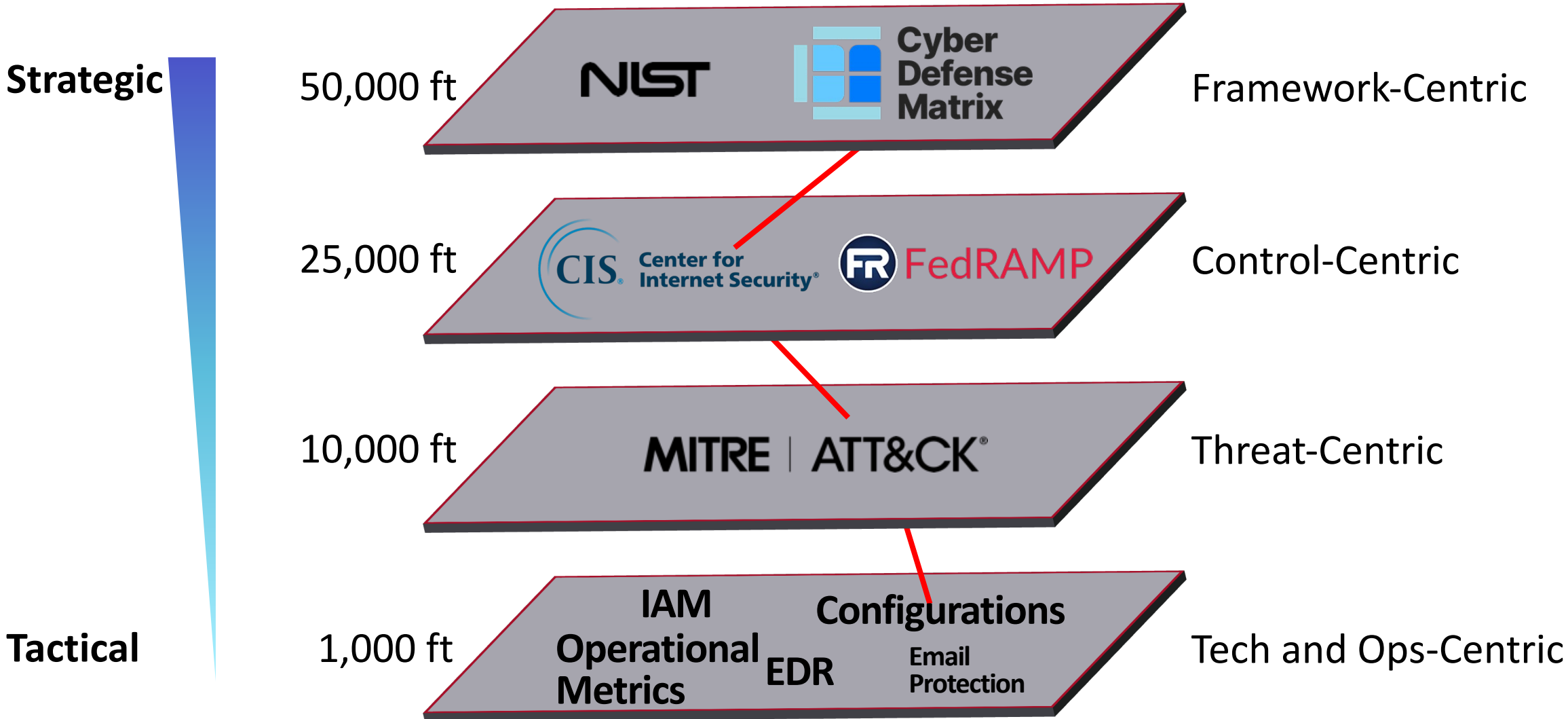


Tactical

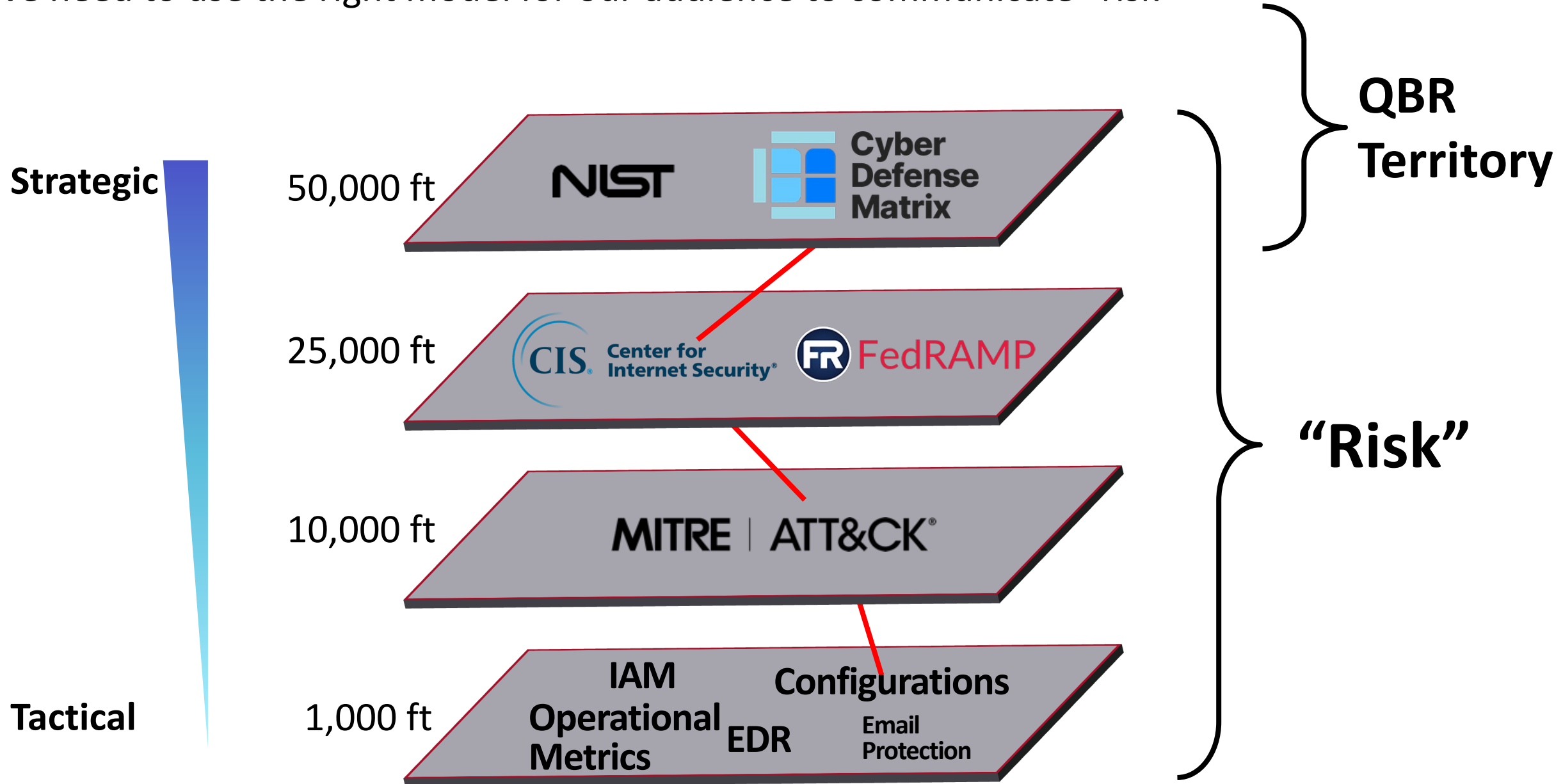
1,000 ft



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?

UP. DOWN. DIAGONAL. ACROSS!

Visit Invent Solution partners for stamps. Complete two rows, three rows or get a blackout. Then fill out ALL the info on the front of the card, and you're eligible to win. Submit your completed card to the Marketplace section in the ConnectWise Booth before the close of IT Nation.

+ GOOD LUCK!

| | | | | | | | |
|----------------------------|-------------------------|---------------------------|------------------------------------|---------------------------|------------------------------|---------------------------|--------------------------|
| SaaS Alerts Booth 108 | ZORUS Booth 134 | VONAH! IT Booth 17 | STRATEGY OVERVIEW Booth 4 | FREE SPACE | PC Matic Booth 229 | Insperty Booth 114 | getKambium Booth 19 |
| VISIONARY Booth 1010 | FREE SPACE | E.T.N Booth 912 | cynet Booth 213 | Bitdefender Booth 227 | ADAPTIVE CATALOG Booth 13 | auvik Booth 940 | Quickpass Booth 421 |
| Dropsuite Booth 533 | CyberFox Booth 809 | opentext Booth 420 | BlackBerry CYLANCE Booth 908 | tribu Booth 12 | STACK Booth 910 | arcserve Booth 535/537 | FREE SPACE |
| CLIP TRAINING Booth 900 | FREE SPACE | GreatAmerica Booth 838 | FREE SPACE | ANUN Booth 505 | chatgenie Booth 100 | TRACESSIO Booth 15 | SentinelOne Booth 326 |
| erception Booth 231 | Third Wall Booth 531 | FREE SPACE | Avalara Booth 136 | CentralCase Booth 104 | INKY Booth 920 | INTERMEDIA Booth 1000 | FREE SPACE |
| AvePoint Booth 904 | AlertOps Booth 18 | MSPCFO Booth 824 | BINDX Booth 16 | perimeter 81 Booth 626 | eset Booth 936 | FREE SPACE | CRUSH-BANK Booth 740 |
| FREE SPACE | MindMatrix Booth 812 | EXIUM Booth 332 | FREE SPACE | Acronis Booth 314 | CLEARBENCH Booth 14 | H Booth 20 | FREE SPACE |
| FREE SPACE | GlassHive Booth 650 | FREE SPACE | proofpoint Booth 324 | TimeZest Booth 804 | FREE SPACE | evo Booth 632 | IronVest Booth 10 |

THE FANTASTIC PRIZES!

TWO ROWS:
You're eligible to win one of three \$100 Amazon Gift Cards.

THREE ROWS:
You're eligible to win a pair of Bose Earbuds.

BLACKOUT (ALL SQUARES):
You're eligible to win an Electric Scooter or Solo Stove Bonfire.

Devices

Applications

Networks

Data

Users

Degree of Dependency

| | 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 | |
| Technology | People | | | | |
| Process | | | | | |

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



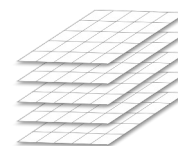
Business/Mission/Technology
Constraints, Exceptions

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**

| | | |
|---|---|---|
| x | x | x |
| x | x | x |
| | | x |
| x | x | x |
| | x | |

Local Admin Rights Restriction as a protective control

EDR as a less impactful, compensating, detective control

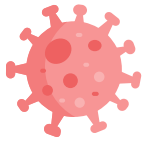


**ICS / OT / MED
ENVIRONMENTS**

| | | | |
|---|---|---|---|
| x | | | |
| x | x | x | x |
| x | x | x | x |
| | x | | |

No ability to modify or instrument the devices

Network based controls as an alternative



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

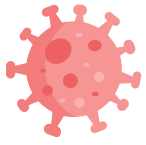
<https://owasp.org/www-project-threat-and-safeguard-matrix/>

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 |

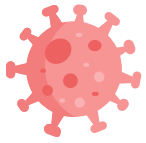


Nutritional Needs: Community Defense Model for Ransomware

- 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 | Technology | | | | People |
| | 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?

Existing Capabilities (Pantry)

| | | | | |
|----|-----|-----|----|--|
| □□ | □□□ | □□□ | □□ | |
| | □ | □□ | | |
| □□ | □ | □□□ | □ | |
| □ | □□□ | | | |
| □□ | □□□ | □□ | | |



Best Practices, Architectures (Recipes)

| | | | | | |
|---|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ | ○ |
| | ○ | ○ | | | |
| | | | ○ | | |
| | ○ | | | | |
| | | | | | |
| ○ | ○ | | ○ | | |

Risks (Nutritional Needs)

| | | | | | |
|---|---|--|---|--|--|
| | | | | | |
| ■ | ■ | | ■ | | |
| | | | ■ | | |
| ■ | | | | | |
| | | | | | |



Prospective Capabilities (Market)

| | | | | | |
|---|---|---|---|---|---|
| ★ | ★ | ★ | ★ | ★ | |
| ★ | ★ | ★ | ★ | | |
| ★ | ★ | ★ | ★ | ★ | |
| ★ | ★ | ★ | ★ | ★ | ★ |
| ★ | ★ | ★ | ★ | | |
| ★ | ★ | ★ | | | |

Mission/Business/Tech Constraints (Allergies/Dietary Restrictions)

| | | | | | |
|---|---|--|--|---|--|
| ▨ | ▨ | | | ▨ | |
| | ▨ | | | | |
| | | | | ▨ | |
| | ▨ | | | | |
| ▨ | | | | | |
| ▨ | ▨ | | | | |



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

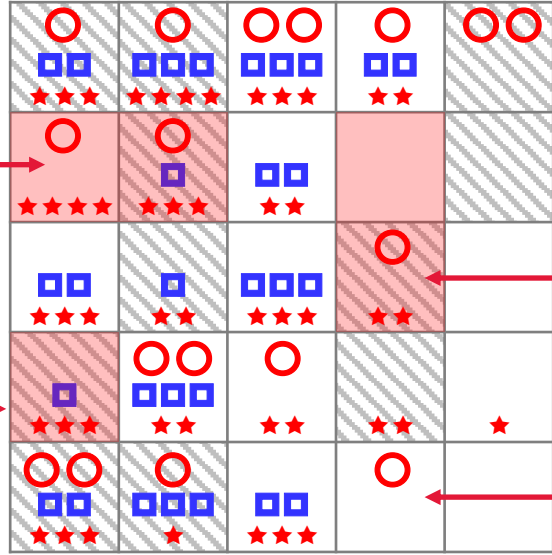
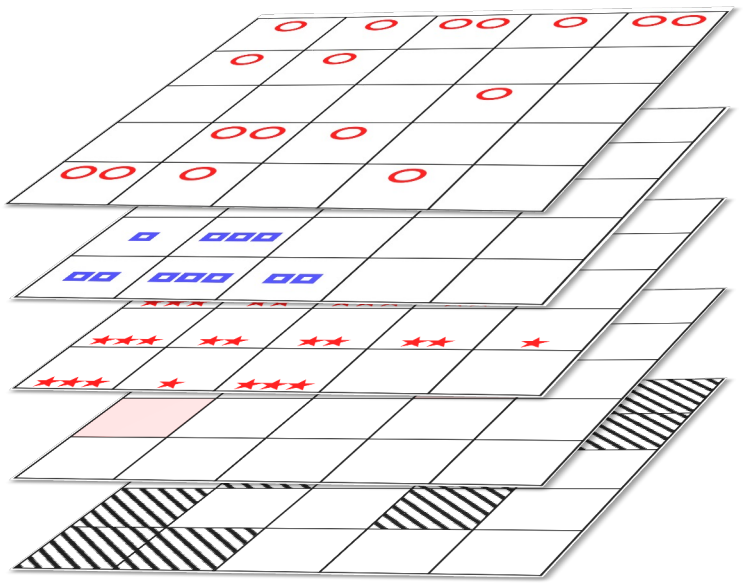


Table stakes /
Just do it

Risk Management Discussion:

- Active attacks underway
- No regulatory requirement
- Capabilities are available...
- ... but controls create minor mission impact

Risk Management Discussion:

- Active attacks underway
- Regulatory requirement
- Capabilities are available...
- ... but controls create major 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

| | Identify | Protect | Detect | Respond | Recover |
|--------------|--|---------|---------------------------------|-------------------------------------|-------------------|
| Devices | Endpoint Services | | CERT | | Endpoint Services |
| Applications | LOBs / DevOps | | App Monitoring & Response | | LOBs / DevOps |
| Networks | Network Services | | Network Monitoring & Response | | Net Svcs |
| Data | Chief Data Officer / Chief Privacy Officer | | Data Loss Prevention & Response | | CDO / CPO |
| Users | Human Resources | | Insider Threat | Human Resources / Physical Security | |
| | MSP | | MSSP | | Customer |

ILLUSTRATIVE

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 | |
| | | MSP | | MSSP | |
| | | | | | Customer |

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 | <ul style="list-style-type: none"> RMM Automated Asset Discovery Continuous Vulnerability Scanning Group Policy Discovery / Hardening Policies Documentation Automation Mobile Device Management Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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) | <ul style="list-style-type: none"> Endpoint Ransomware Protection AI Based AV with 7x24 Security Operations Center SIEM with 7x24 SOC (Logging and Detection) Centralized Change Reporting Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Centralized Change Reporting Segregated Server and Workstation Backups Server Cloud Replication (DR Hot Site) Cyberinsurance / Ransomware Insurance Disaster Recovery Plan |
| Apps | <ul style="list-style-type: none"> Automated Asset Discovery Continuous Vulnerability Scanning Continuous Security Auditing / Management Business Impact Analysis Privilege Elevation Management (Request to Install) Annual Risk Review / Assessment | <ul style="list-style-type: none"> Application Single Sign On (SSO) Domain DNS Protection Password Management Mobile Application Management | | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance Disaster Recovery Plan |
| Networks | <ul style="list-style-type: none"> Continuous Vulnerability Scanning Documentation Automation Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> Endpoint DNS Filtering SIEM with 7x24 SOC (Logging and Detection) Domain DNS Protection Bandwidth Monitoring Network Management | <ul style="list-style-type: none"> SIEM with 7x24 SOC (Logging and Detection) Centralized Change Reporting AI Based AV with 7x24 Security Operations Center Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Centralized Change Reporting Network Management Disaster Recovery Plan |
| Data | <ul style="list-style-type: none"> DataLoss Prevention (DLP) in M365 Continuous Vulnerability Scanning Documentation Automation Automated Identification of M365 Groups Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> Darkweb Scanning (For Stolen Credentials) Email Encryption Bandwidth Monitoring Mobile Device Management | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Segregated Server and Workstation Backups Server Cloud Replication (DR Hot Site) Disaster Recovery Plan |
| Users | <ul style="list-style-type: none"> Darkweb Scanning (For Stolen Credentials) Continuous Security Auditing / Management Documentation Automation Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance Incident Response Plan | |

In Place Today

Available Services and Projects

Emerging threats change priorities

| | 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 | | | | |

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 | <ul style="list-style-type: none"> RMM Automated Asset Discovery Continuous Vulnerability Scanning Group Policy Discovery / Hardening Policies Documentation Automation Mobile Device Management Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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) | <ul style="list-style-type: none"> Endpoint Ransomware Protection AI Based AV with 7x24 Security Operations Center SIEM with 7x24 SOC (Logging and Detection) Centralized Change Reporting Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Centralized Change Reporting Segregated Server and Workstation Backups Server Cloud Replication (DR Hot Site) Cyberinsurance / Ransomware Insurance Disaster Recovery Plan |
| Apps | <ul style="list-style-type: none"> Automated Asset Discovery Continuous Vulnerability Scanning Continuous Security Auditing / Management Business Impact Analysis Privilege Elevation Management (Request to Install) Annual Risk Review / Assessment | <ul style="list-style-type: none"> Application Single Sign On (SSO) Domain DNS Protection Password Management Mobile Application Management | | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance Disaster Recovery Plan |
| Networks | <ul style="list-style-type: none"> Continuous Vulnerability Scanning Documentation Automation Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> Endpoint DNS Filtering SIEM with 7x24 SOC (Logging and Detection) Domain DNS Protection Bandwidth Monitoring Network Management | <ul style="list-style-type: none"> SIEM with 7x24 SOC (Logging and Detection) Centralized Change Reporting AI Based AV with 7x24 Security Operations Center Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Centralized Change Reporting Network Management Disaster Recovery Plan |
| Data | <ul style="list-style-type: none"> DataLoss Prevention (DLP) in M365 Continuous Vulnerability Scanning Documentation Automation Automated Identification of M365 Groups Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> Darkweb Scanning (For Stolen Credentials) Email Encryption Bandwidth Monitoring Mobile Device Management | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance | <ul style="list-style-type: none"> Segregated Server and Workstation Backups Server Cloud Replication (DR Hot Site) Disaster Recovery Plan |
| Users | <ul style="list-style-type: none"> Darkweb Scanning (For Stolen Credentials) Continuous Security Auditing / Management Documentation Automation Annual Risk Review / Assessment | <ul style="list-style-type: none"> 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 | | <ul style="list-style-type: none"> Cyberinsurance / Ransomware Insurance Incident Response Plan | |

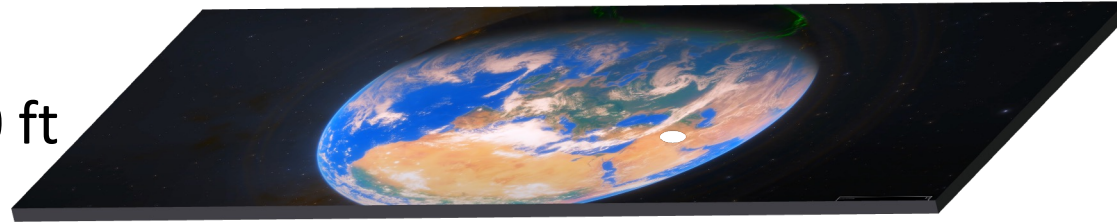
In Place Today

Available Services and Projects

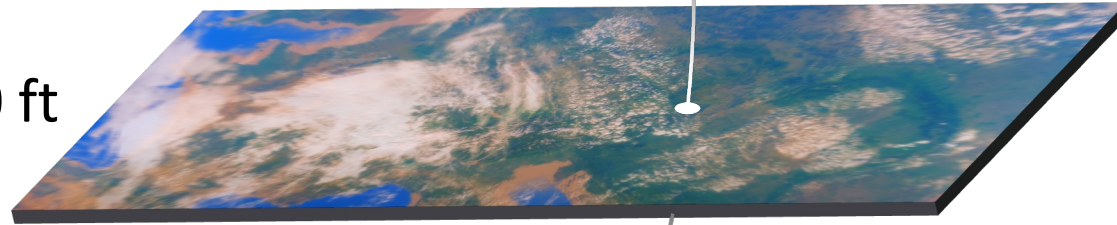
Remember to choose the right map to communicate clearly

Strategic

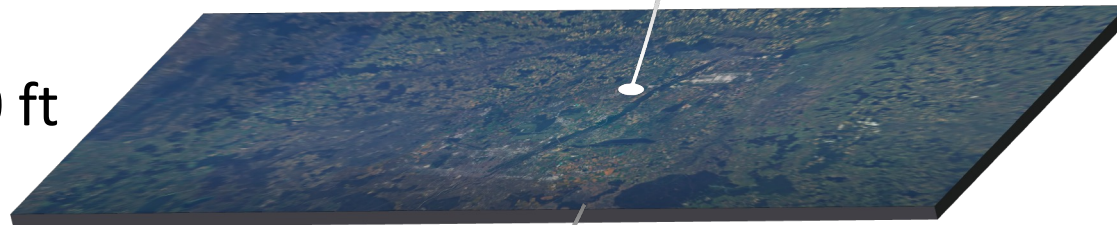
50,000 ft



25,000 ft



10,000 ft



Tactical

1,000 ft



Questions?



@sounilyu



@cyberdefmatrix



sounil@cyberdefensematrix.com



<https://cyberdefensematrix.com>



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



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