RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **STR-M01**

Cyber Defense Matrix: Revolutions

Sounil Yu

CISO & Head of Research
JupiterOne
@sounilyu

Disclaimer

RSA's disclaimers

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Sounil's Disclaimers

- Vendors shown are representative only
- No usage or endorsement should be construed because they are shown here

All models are wrong, but some are useful

- George E. P. Box

Ready for a week of buzzword madness?

Phishing Awareness Interactive Application Security Testing

User & Entity Behavioral Analytics Insider Threat Secrets Management

Endpoint Protection Software Composition Analysis Cloud Access Security Broker eXtended Detection & Response

Endpoint Detection & Response Confidential Computing Data Loss Prevention

Zero Trust Network Access Secure Access Service Edge

Cloud Workload Protection Platform Cloud Infrastructure Entitlement Management

Web Application & API Protection

Identity & Access Management

Content Disarm & Reconstruction

Microsegmentation Cloud Security Posture Management

Artificial Intelligence / ML Threat Intelligence

Privileged Access Management Database Activity Monitoring

Attack Surface Management

One simple way to organize these buzzwords is by aligning them against five asset classes and the NIST CSF

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

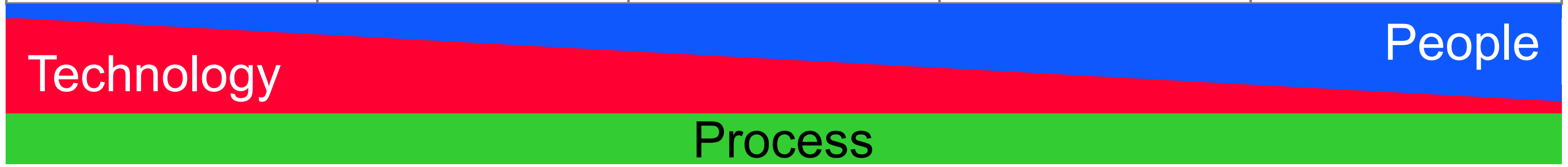
Asset Classes	
DEVICES	Workstations, servers, phones, tablets, storage, network devices, IoT infrastructure, etc.
APPS	Software, interactions, and application flows on the devices
NETWORKS	Connections and traffic flowing among devices and apps
DATA	Information at rest, in transit, or in use by the resources 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 remediation
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

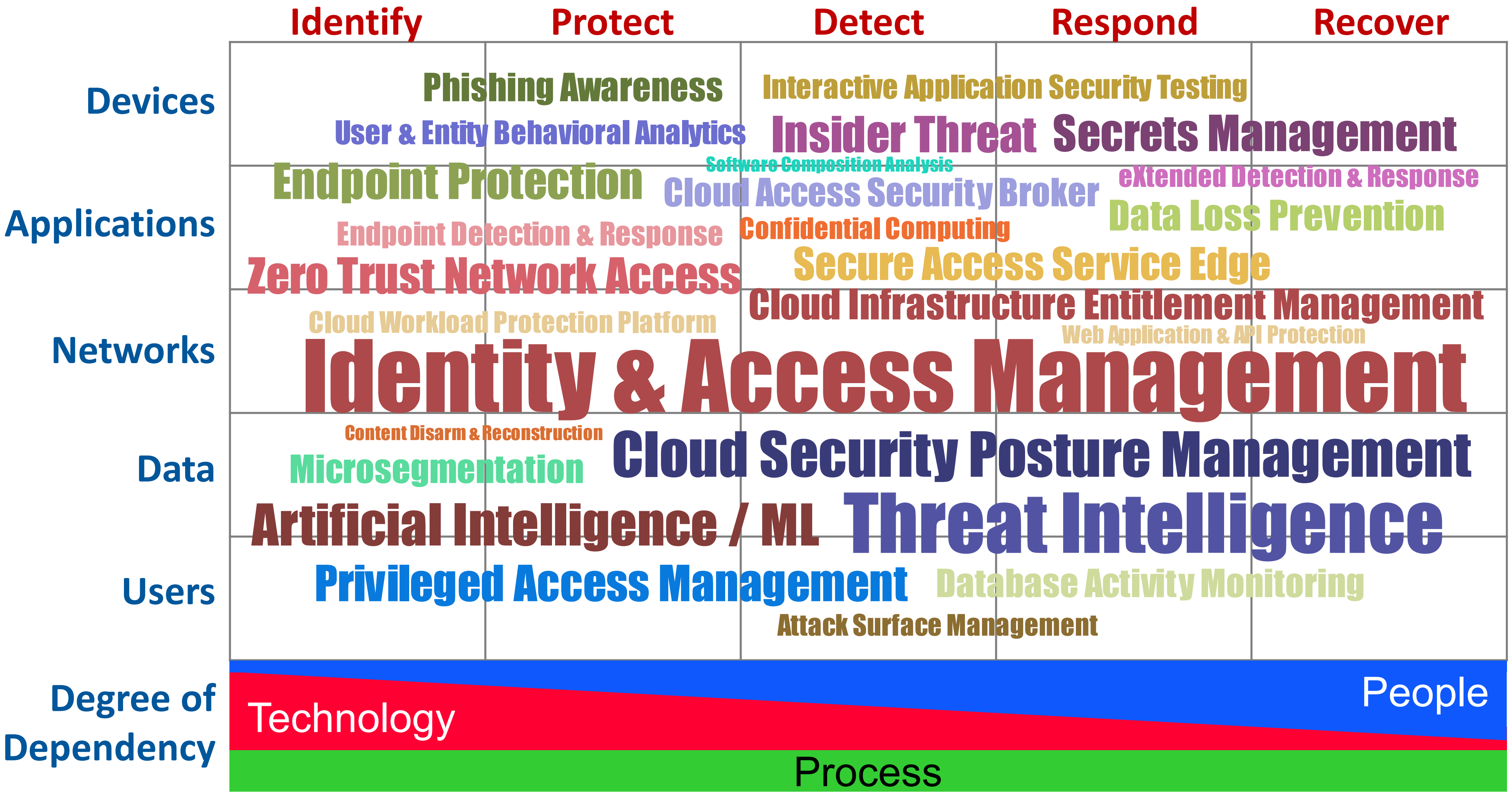
The Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

Degree of Dependency



Aligning the buzzwords against the Cyber Defense Matrix…



Identify

Protect

Detect

Respond

Recover

Devices

Applications

Networks

Data

Users

Phishing Awareness

Interactive Application Security Testing

User & Entity Behavioral Analytics

Insider Threat

Secrets Management

Software Composition Analysis

Endpoint Protection

Cloud Access Security Broker

eXtended Detection & Response

Data Loss Prevention

Endpoint Detection & Response

Confidential Computing

Zero Trust Network Access

Secure Access Service Edge

Cloud Infrastructure Entitlement Management

Cloud Workload Protection Platform

Web Application & API Protection

Identity & Access Management

Content Disarm & Reconstruction

Cloud Security Posture Management

Microsegmentation

Artificial Intelligence / ML

Threat Intelligence

Privileged Access Management

Database Activity Monitoring

Attack Surface Management

Degree of Dependency

Technology

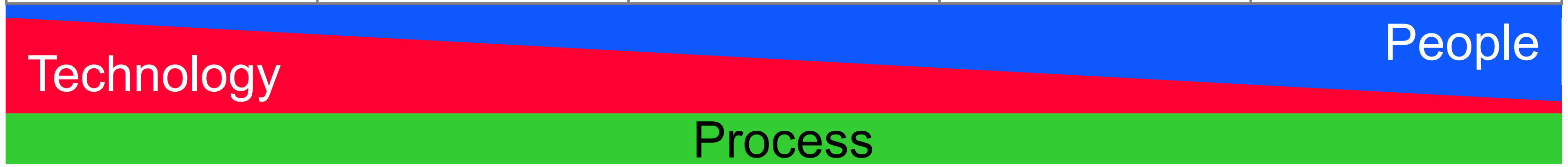
People

Process

…can help bring some order to the chaos…

	Identify	Protect	Detect	Respond	Recover
Devices	Asset Mgt, Vuln Scanning, Vuln Mgt, Certificate Mgt	AV, Anti-Malware, EPP, FIM, HIPS, Whitelisting, Patch Mgt	Endpoint Detection, UEBA, XDR	EP Response, EP Forensics	
Applications	SAST, DAST, SW Asset Mgt, Fuzzers	RASP, WAF, ZT App Access	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	
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	Security Training & Awareness	Insider Threat, User Behavior Analytics, XDR		

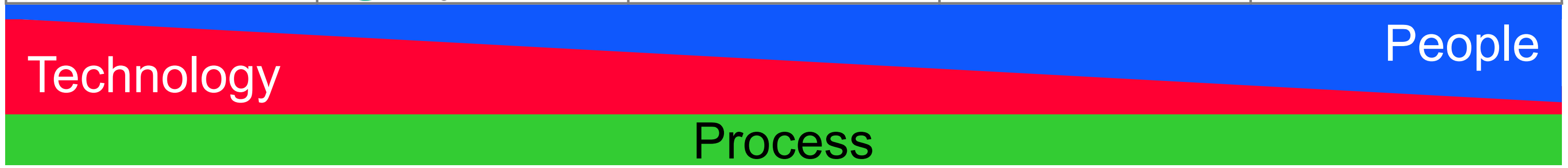
Degree of Dependency



…and help you understand what some of these vendors do! (sorry, this slide is really out of date)

	Identify	Protect	Detect	Respond	Recover
Devices	QUALYS tripwire ForeScout PACKETVIPER TANIUM orca security JupiterOne AXONIUS sysdig POLYSWARM ThreatMetrix pindrop security SECURESTACK eclypsium thred	Symantec McAfee Bromium ATOMICORP CARBON BLACK Cypherpath NTREPID HYSOLATE CYLANCE invincea TEHAMA MEDIGATE Malwarebytes VULCAN	tripwire blackpoint CARBON BLACK CROWDSTRIKE Hunters. ENDGAME. TANIUM SCYTHE Uptycs cybereason	blackpoint ENDGAME. CARBON BLACK CROWDSTRIKE TANIUM D3 SECURITY NowSecure EASYSOLUTIONS	
Applications	CodeDx CHECKMARX VERACODE insignary Signal Sciences SYNOPSYS JupiterOne skyhigh enso RISKIQ hackerone CONTRAST SECURITY bugcrowd	ArecaBay Security Compass CONTRAST SECURITY VERACODE PREVOTY CryptoMove SECURE CODE WARRIOR portshift waratek K2 Avocado Systems Karamba Security ARXAN Akamai TALA MAGNUS Signal Sciences	cycode neosec TRUEFORT		
Networks	passwordping JupiterOne LOOKINGGLASS Lancope SKYBOX SECURITY ARBOR NETWORKS FARSIGHT SECURITY corelight DOMAINTOOLS	PERCEPTION POINT CLOUDFLARE CISCO zscaler REDMARLIN Akamai f5 Meta Networks FireEye VALIMAIL paloalto zscaler algosec hp wifi wall	DARKTRACE Hunters. FORTIPHYD LOGIC Check Point SOFTWARE TECHNOLOGIES LTD. SOURCEfire	D3 SECURITY BLUE COAT RSA	
Data	boldonjames A QinetiQ Company woleet DataGravity JupiterOne SECRET DOUBLE OCTOPUS users are human TITUS VARONIS	hp Voltage security Armorblox INTRALINKS Symantec XTON technologies ixup IONIC Password satori NuID CipherCloud Trust in the Cloud SafeNet. DIGITAL GUARDIAN	IBM DARKSUM™ DECIPHER THE DARKNET DB NETWORKS pixm CYBERHAVEN	BREACHRX	VERITAS CODE42 DELL EMC NeuShield
Users	BehavioSec COFENSE BIOCATCH Less Friction. Less Fraud. JupiterOne ARMOR Scientific KnowBe4 Human error. Conquered.	COFENSE KnowBe4 Human error. Conquered. wombat security technologies HABITU8 Basil Security AUTHENTIFY Elevate Security inky	ZEROFOX exabeam Dtex systems SECURONIX observe it Hunters. FORCEPOINT GURUCUL REDOWL Bay Dynamics INTERSET		

Degree of Dependency



Use Cases of the Cyber Defense Matrix…

RSAConference2016

San Francisco | February 29–March 4 | Moscone Center

Connect to Protect

SESSION ID: PDIL-W02F

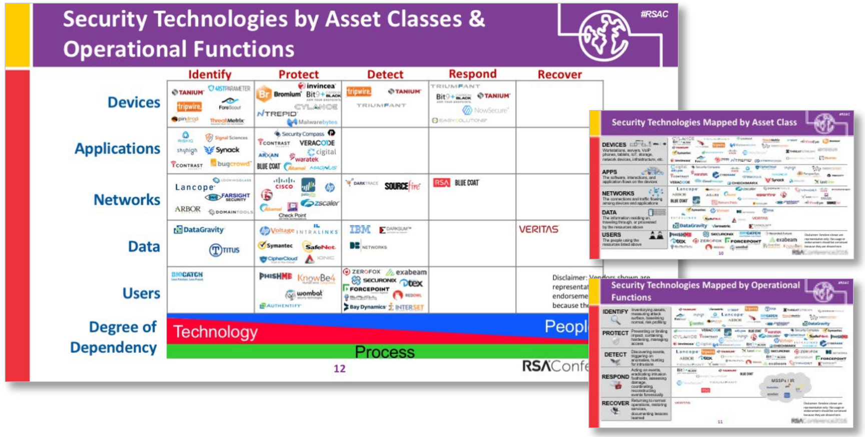
Understanding the Security Vendor Landscape Using the Cyber Defense Matrix

Sounil Yu
sounil@gmail.com
@sounilyu

#RSAC

https://bit.ly/cyberdefensematrix

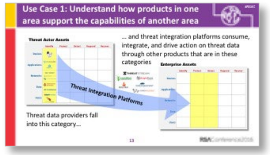
Primary Use Case: Vendor Mapping



Security Technologies by Asset Classes & Operational Functions

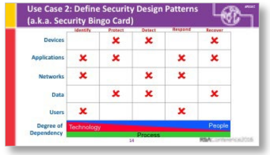
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

#RSAC
Degree of Dependency
Technology
People
Process
12
RSAConfe
Security Technologies Mapped by Asset Class
Security Technologies Mapped by Operational Functions
Disclaimer: Vendors shown are representative only…



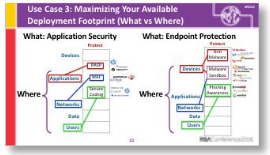
Use Case 1: Understand how products in one area support the capabilities of another area

Differentiating Primary & Supporting Capabilities



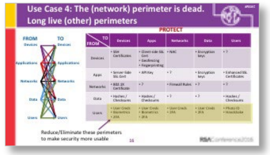
Use Case 2: Define Security Design Patterns (a.k.a. Security Bingo Card)

Defining Security Design Patterns



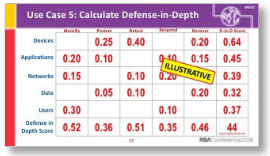
Use Case 3: Maximizing Your Available Deployment Footprint (What vs Where)

Maximizing Deployment Footprint



Use Case 4: The (network) perimeter is dead. Long live (other) perimeters

Understanding the New Perimeter

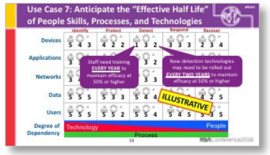


Use Case 5: Calculate Defense-in-Depth

Calculating Defense-in-Breadth

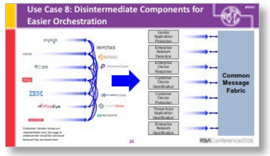
Use Case 6: Understand how to balance your portfolio without breaking the bank

Balancing Your Portfolio Budget



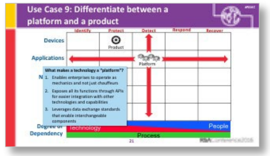
Use Case 7: Anticipate the "Effective Half Life" of People Skills, Processes, and Technologies

Planning for Obsolescence



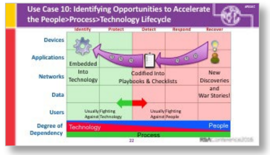
Use Case 8: Disintermediate Components for Easier Orchestration

Disintermediating Security Components



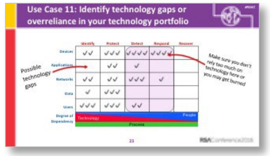
Use Case 9: Differentiate between a platform and a product

Comparing Point Products vs Platforms



Use Case 10: Identifying Opportunities to Accelerate the People>Process>Technology Lifecycle

Finding Opportunities for Automation



Use Case 11: Identify technology gaps or overreliance in your technology portfolio

Identifying Gaps in People, Process, Tech

Other Use Cases of the Cyber Defense Matrix…

RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

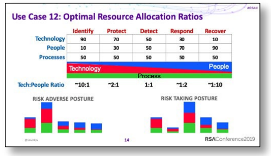
SESSION ID: STR-T09

The BETTER Cyber Defense Matrix, Reloaded

Sounil Yu
@sounilyu

#RSAC

https://bit.ly/cyberdefensematrixreloaded

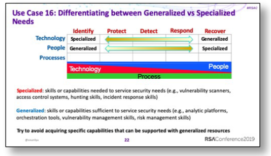


Use Case 12: Optimal Resource Allocation Ratios

	Identify	Protect	Detect	Respond	Recover
Technology	90	70	50	30	10
People	10	30	50	70	90
Processes	50	50	50	50	50
Tech:People Ratio	~10:1	~2:1	1:1	~1:2	~1:10

@sounilyu 14 RSAConference2019

Optimizing Budgets and Resource Allocation



Use Case 16: Differentiating between Generalized vs Specialized Needs

	Identify	Protect	Detect	Respond	Recover
Technology	Specialized				Generalized
People	Generalized				Specialized
Processes					

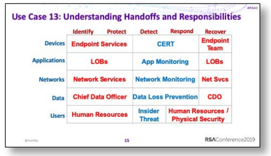
Specialized: skills or capabilities needed to service security needs (e.g., vulnerability scanners, access control systems, hunting skills, incident response skills)

Generalized: skills or capabilities sufficient to service security needs (e.g., analytic platforms, orchestration tools, vulnerability management skills, risk management skills)

Try to avoid acquiring specific capabilities that can be supported with generalized resources

@sounilyu 22 RSAConference2019

Aligning Generalized vs Specialized Needs

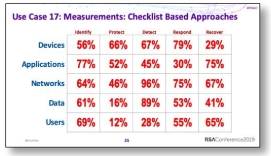


Use Case 13: Understanding Handoffs and Responsibilities

	Identify	Protect	Detect	Respond	Recover
Devices	Endpoint Services		CERT		Endpoint Team
Applications	LOBs		App Monitoring		LOBs
Networks	Network Services		Network Monitoring		Net Svcs
Data	Chief Data Officer		Data Loss Prevention		CDO
Users	Human Resources		Insider Threat	Human Resources / Physical Security	

@sounilyu 15 RSAConference2019

Mapping Organizational Handoffs

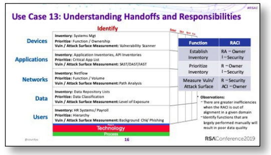


Use Case 17: Measurements: Checklist Based Approaches

	Identify	Protect	Detect	Respond	Recover
Devices	56%	66%	67%	79%	29%
Applications	77%	52%	45%	30%	75%
Networks	64%	46%	96%	75%	67%
Data	61%	16%	89%	53%	41%
Users	69%	12%	28%	55%	65%

@sounilyu 25 RSAConference2019

Measurements and Metrics



Use Case 13: Understanding Handoffs and Responsibilities

Identify

	Identify
Devices	**Inventory**: Systems Mgt **Prioritize**: Function / Ownership **Vuln / Attack Surface Measurement:** Vulnerability Scanner
Applications	**Inventory**: Application Inventories, API Inventories **Prioritize**: Critical App List **Vuln / Attack Surface Measurement:** SAST/DAST/IAST
Networks	**Inventory:** Netflow **Prioritize:** Function / Volume **Vuln / Attack Surface Measurement:** Path Analysis
Data	**Inventory:** Data Repository Lists **Prioritize:** Data Classification **Vuln / Attack Surface Measurement:** Level of Exposure
Users	**Inventory:** HR Systems / Payroll **Prioritize:** Hierarchy **Vuln / Attack Surface Measurement:** Background Chk/ Phishing

Function	RACI
Establish Inventory	RA – Owner I – Security
Prioritize Inventory	R – Owner I – Security
Measure Vuln/ Attack Surface	R – Security ACI – Owner

- Observations:
  - There are greater inefficiencies when the RACI is out of alignment in a given domain
  - Identify functions that are largely performed manually will result in poor data quality

@sounilyu 16 RSAConference2019

Aligning Roles and Responsibilities

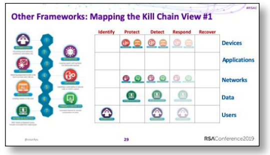
Use Case 18: Applying Security Design Patterns to Fit Business Constraints

ILLUSTRATIVE
Max Possible Security Posture = 100
Min Required Security Posture > 70
(Due to inherent risks and risk tolerance)
DAY EXTENDERS
BRANCH OFFICE
= 80
OFFICE WORKERS
CALL CENTERS
General
Who Are You ?
Specialized
ROAD WARRIORS
DEVELOPERS / DATA ANALYSTS
SENIOR EXECUTIVES
COMMODITY TRADERS
= 56
Max Possible Security Posture = 50
Min Required Security Posture > 55
(Due to inherent risks and risk tolerance)

Going above maximum possible security posture results in a business impact and forces a conscious tradeoff between business impact and security posture

@sounilyu 26 RSAConference2019

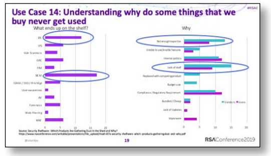
Business Aligned Security Patterns



Other Frameworks: Mapping the Kill Chain View #1

@sounilyu 29 RSAConference2019

Mapping to the Kill Chain

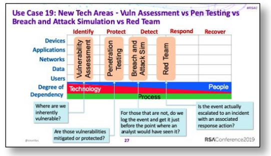


Use Case 14: Understanding why do some things that we buy never get used

Source: Security Shelfware : Which Products Are Gathering Dust In the Shed and Why?
https://www.rsaconference.com/writable/presentations/file_upload/mash-f07a-security-shelfware-which-products-gathering-dust-and-why.pdf

@sounilyu 19 RSAConference2019

Understanding Why Products are Not Used



Use Case 19: New Tech Areas - Vuln Assessment vs Pen Testing vs Breach and Attack Simulation vs Red Team

Where are we inherently vulnerable?

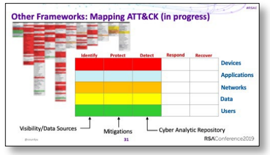
Are those vulnerabilities mitigated or protected?

For those that are not, do we log the event and get it just before the point where an analyst would have seen it?

Is the event actually escalated to an incident with an associated response action?

@sounilyu 27 RSAConference2019

Vuln Scan vs PenTest vs BAS vs Red Team



Other Frameworks: Mapping ATT&CK (in progress)

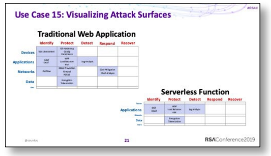
Visibility/Data Sources

Mitigations

Cyber Analytic Repository

@sounilyu 31 RSAConference2019

Mapping to MITRE ATT&CK



Use Case 15: Visualizing Attack Surfaces

Traditional Web Application

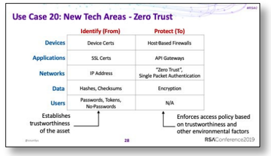
	Identify	Protect	Detect	Respond	Recover
Devices	Vuln. Assessment	OS Hardening Config Compliance			
Applications	SAST DAST	WAF Load Balancer [illegible]	Log Analysis		
Networks	Netflow	DDoS Prevention Firewall [illegible]		DDoS Mitigation PCAP Analysis	
Data		Encryption Tokenization			

Serverless Function

	Identify	Protect	Detect	Respond	Recover
Applications	SAST DAST	WAF Load Balancer [illegible]	Log Analysis		
Data		Encryption Tokenization			

@sounilyu 21 RSAConference2019

Visualizing Attack Surfaces



Use Case 20: New Tech Areas - Zero Trust

	Identify (From)	Protect (To)
Devices	Device Certs	Host-Based Firewalls
Applications	SSL Certs	API Gateways
Networks	IP Address	"Zero Trust", Single Packet Authentication
Data	Hashes, Checksums	Encryption
Users	Passwords, Tokens, No-Passwords	N/A

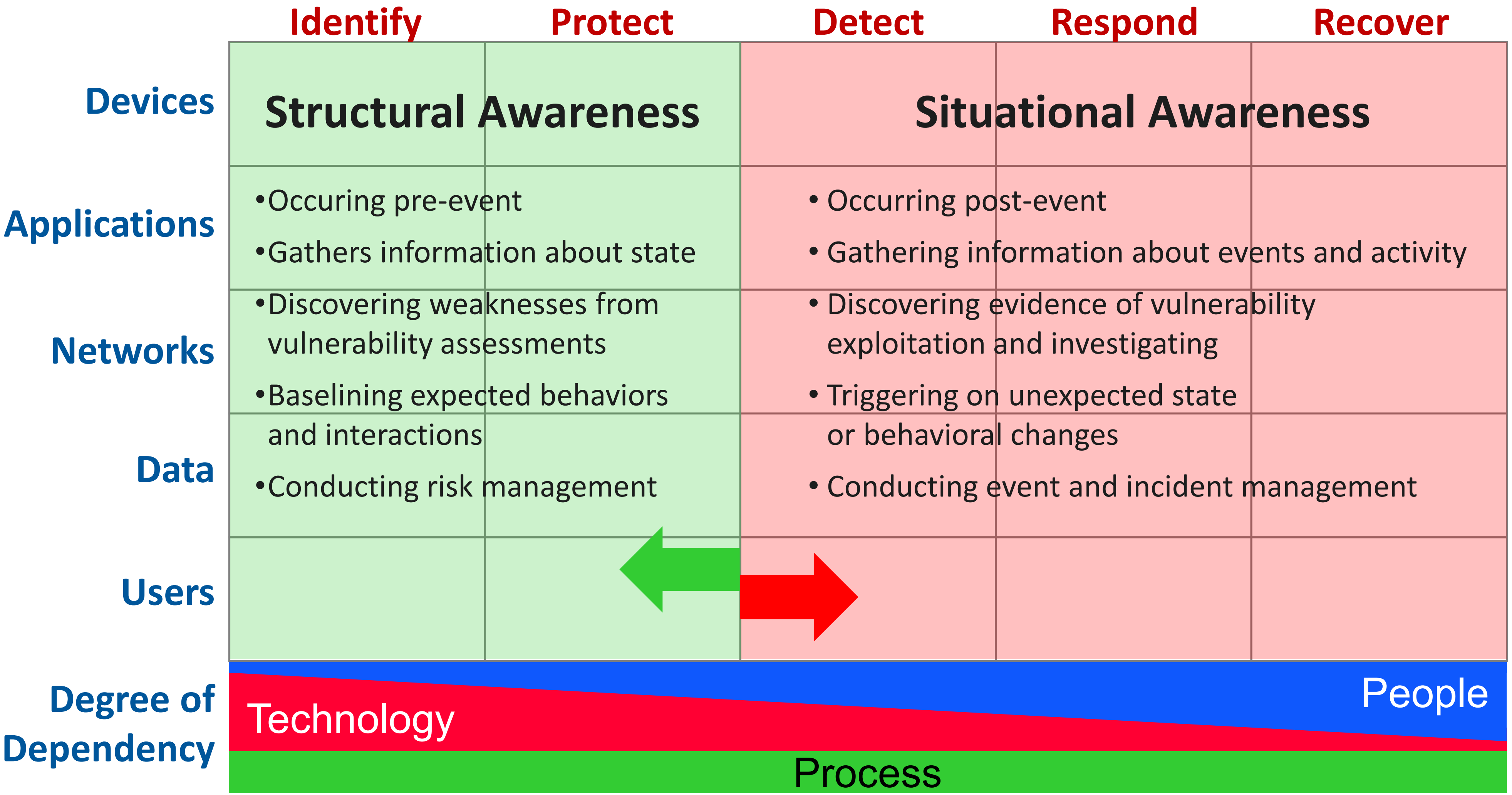
Establishes trustworthiness of the asset

Enforces access policy based on trustworthiness and other environmental factors

@sounilyu 28 RSAConference2019

Mapping Zero Trust Capabilities

Remember Left and Right of Boom



Structural Awareness

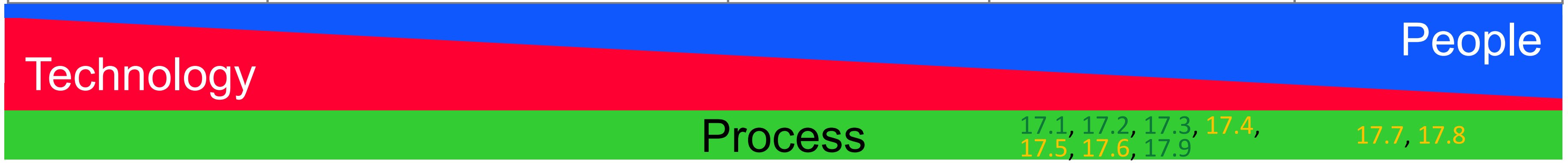
- Occuring pre-event
- Gathers information about state
- Discovering weaknesses from vulnerability assessments
- Baselining expected behaviors and interactions
- Conducting risk management

Situational Awareness

- Occurring post-event
- Gathering information about events and activity
- Discovering evidence of vulnerability exploitation and investigating
- Triggering on unexpected state or behavioral changes
- Conducting event and incident management

Use Case 21: Prioritization Using CIS Critical Security Controls

	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				17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.9	17.7, 17.8



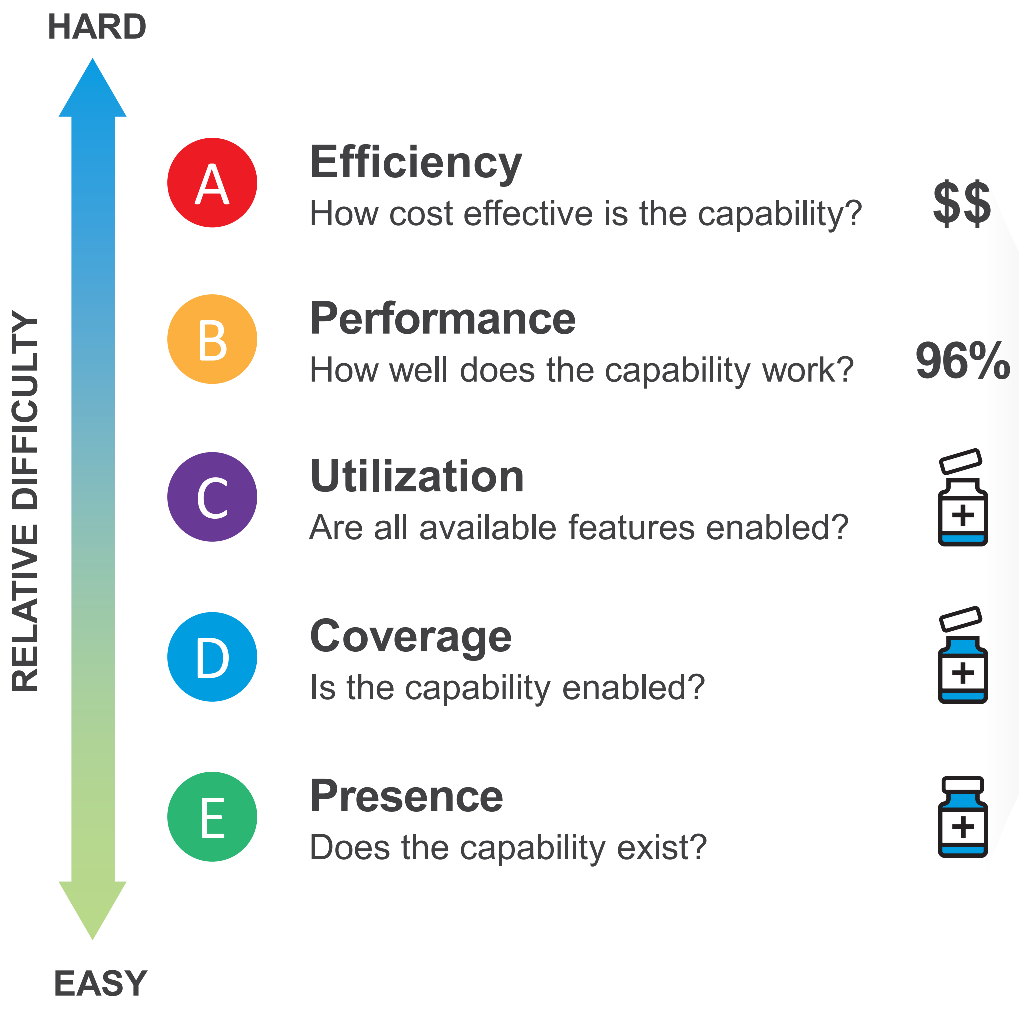
🟩 Implementation Group 1 🟨 Implementation Group 2 🟥 Implementation Group 3

Use Case 5: Calculating Defense-in-Breadth Using CIS' Control Assessment Specification

(https://controls-assessment-specification.readthedocs.io)

	Identify	Protect	Detect	Respond	Recover	Total
Devices	15 (8 / 7 / 0)	84 (30 / 36 / 18)	26 (0 / 21 / 5)	9 (5 / 4 / 0)	0	134 (43 / 68 / 23)
Applications	56 (18 / 34 / 4)	125 (33 / 72 / 20)	5 (0 / 5 / 0)	11 (7 / 4 / 0)	0	197 (58 / 115 / 24)
Networks	14 (0 / 10 / 4)	94 (21 / 53 / 20)	32 (3 / 28 / 1)	0	0	140 (24 / 91 / 25)
Data	22 (9 / 13 / 0)	67 (32 / 21 / 14)	12 (0 / 0 / 12)	0	17 (13 / 4 / 0)	118 (54 / 38 / 26)
Users	24 (9 / 15 / 0)	90 (84 / 6 / 0)	0 (0 / 0 / 0)	6 (6 / 0 / 0)	0	120 (99 / 21 / 0)
Total	134 (44 / 79 / 8)	460 (200 / 188 / 72)	75 (3 / 54 / 18)	26 (18 / 8 / 0)	17 (13 / 4 / 0)	709 (278 / 333 / 98)

Use Case 22: Measurement Health



A **Efficiency**
How cost effective is the capability? $$

B **Performance**
How well does the capability work? 96%

C **Utilization**
Are all available features enabled?

D **Coverage**
Is the capability enabled?

E **Presence**
Does the capability exist?

	Identify	Protect	Detect	Respond	Recover
Devices	E	B	D	E	F
Apps	C	B	B	E	F
Networks	A	A	E	F	E
Data	E	B	B	F	E
Users	D	C	F	E	F

	Identify	Protect	Detect	Respond	Recover
Devices		0.25	0.40		0.20
Apps	0.20	0.10		0.10	0.15
Networks	0.15		0.10	0.20	
Data		0.05	0.10		0.20
Users	0.30			0.10	

	Identify	Protect	Detect	Respond	Recover
Devices		$50	$100		$50
Apps	$50	$100		$50	$100
Networks	$100		$100	$50	
Data		$50	$50		$50
Users	$50			$50	

Use Case 23: Developing a roadmap

Foundation

Cyber Defense Matrix

Layer 1: Recipes

Proven Practices, Frameworks, Reference Architectures

Layer 2: Pantry

Current State Capabilities

Layer 3: Market

Commercial Options, Art of the Possible

Layer 4: Allergies

Allergies and Dietary Restrictions

Business/Mission/Technology Constraints, Exceptions

Layer 5: Nutritional Needs

Nutritional and Dietary Needs

Risks, Attack Surfaces, Threat Environment

The “Stack”

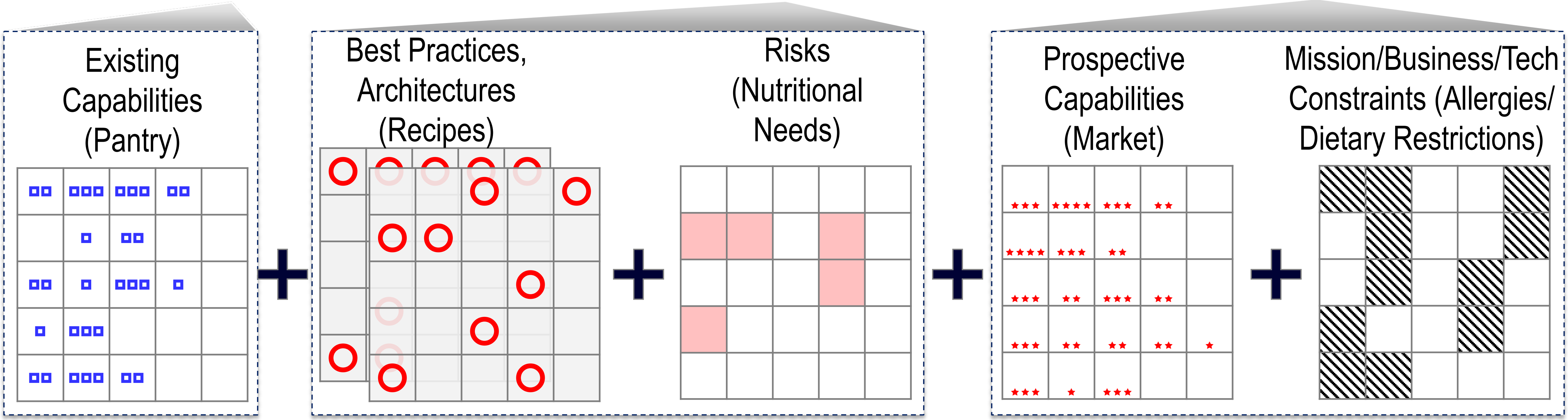
Combined Matrices

Use Case 23: Constructing a roadmap

How secure am I?

How secure should I be?

How do I get there?



Existing Capabilities (Pantry)

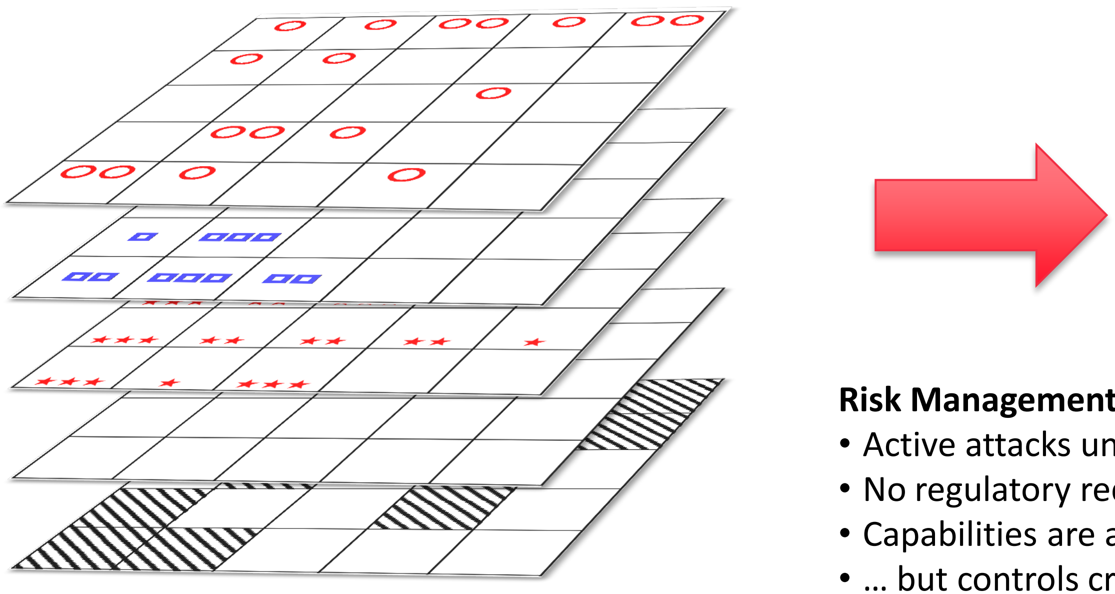
Best Practices, Architectures (Recipes)

Risks (Nutritional Needs)

Prospective Capabilities (Market)

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

Use Case 23: Interpreting the roadmap



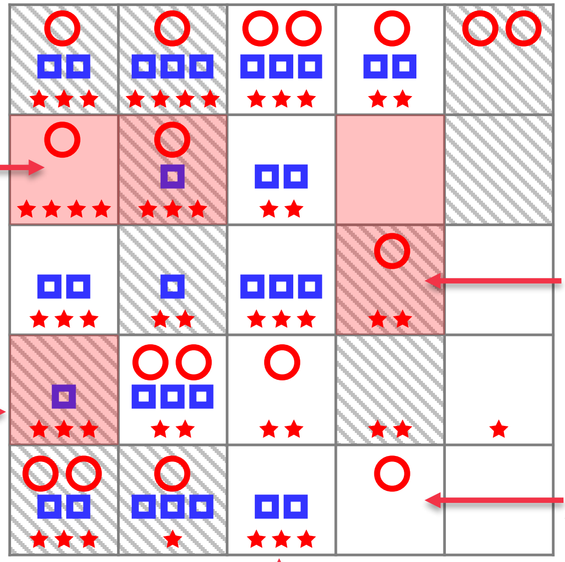


Table stakes / Just do it

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

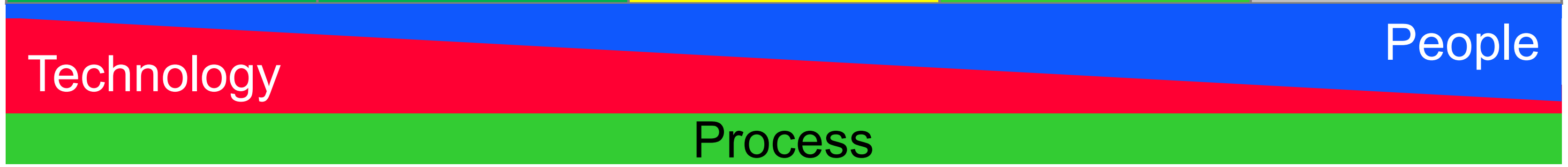
🟥 Attack Surfaces

▨ Business/Mission Constraints

Use Case 24: Board Level View

	Identify	Protect	Detect	Respond	Recover
Devices	🟩	🟩	🟨	🟨	⬜
Applications	🟩	🟨	🟥	🟨	🟨
Networks	⬜	⬜	⬜	⬜	⬜
Data	🟩	🟩	🟨	🟥	🟩
Users	🟩	🟩	🟨	🟩	⬜

Degree of Dependency

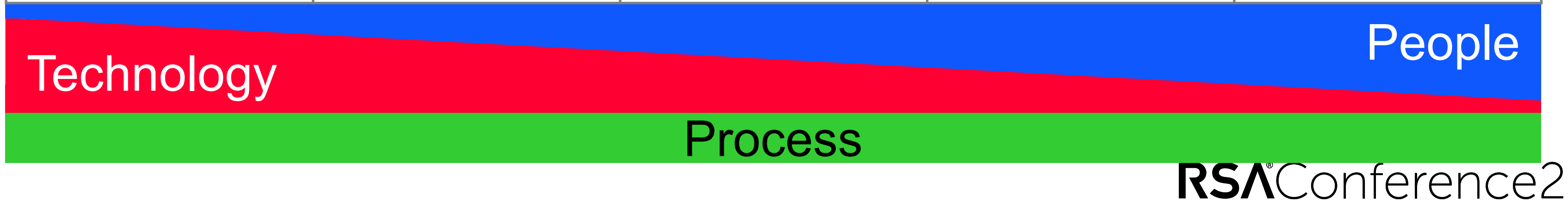


🟩	Sufficient Controls
🟨	Initiatives Underway
🟥	Additional Effort Required
⬜	No Attack Surface

Use Case 25: Seeing gaps and opportunities

	Identify	Protect	Detect	Respond	Recover
Devices	A – – C – D –	F – G – H – I – J	K – L – M – –	P – – R – S – T	– V – – X – –
Applications	A – B – C – – E	F – – H – I –	– L – M – N –	– – – S – T	– – W – – – Z
Networks	A – – C – D – E	– G – – I – J	– L – M – –	P – – R – – T	U – – – – Y –
Data	A – B – C – D –	F – – H – I –	– – M – – O	P – – – S –	– V – W – X – – Z
Users	– – C – – E	– G – H – – J	– – M – N – O	– – – –	U – V – – X – Y –

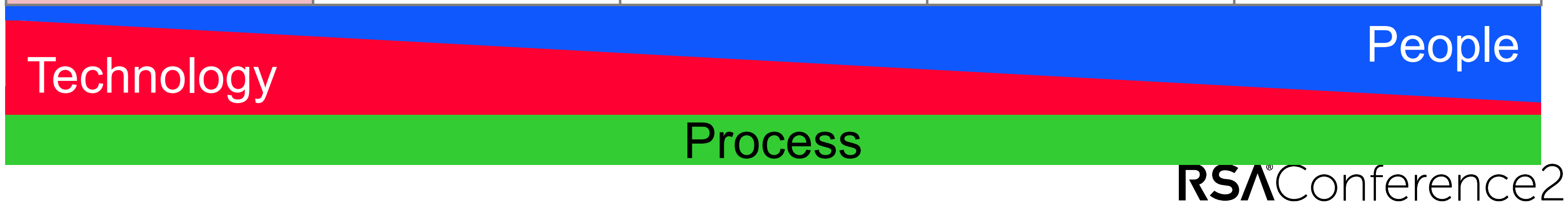
Degree of Dependency



Use Case 25: Seeing gaps and opportunities

	Identify	Protect	Detect	Respond	Recover
Devices	A – B – C – D – E	F – G – H – I – J	K – L – M – –	P – – R – S – T	– V – – X – –
Applications	A – B – C – D – E	F – – H – I –	– L – M – N –	– – – S – T	– – W – – – Z
Networks	A – B – C – D – E	– G – – I – J	– L – M – –	P – – R – – T	U – – – – Y –
Data	A – B – C – D – E	F – – H – I –	– – M – – O	P – – – S –	– V – W – X – – Z
Users	A – B – C – D – E	– G – H – – J	– – M – N – O	– – – –	U – V – – X – Y –

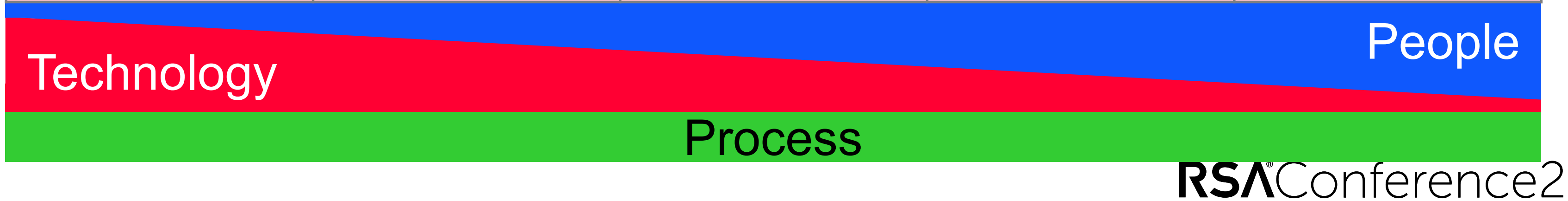
Degree of Dependency



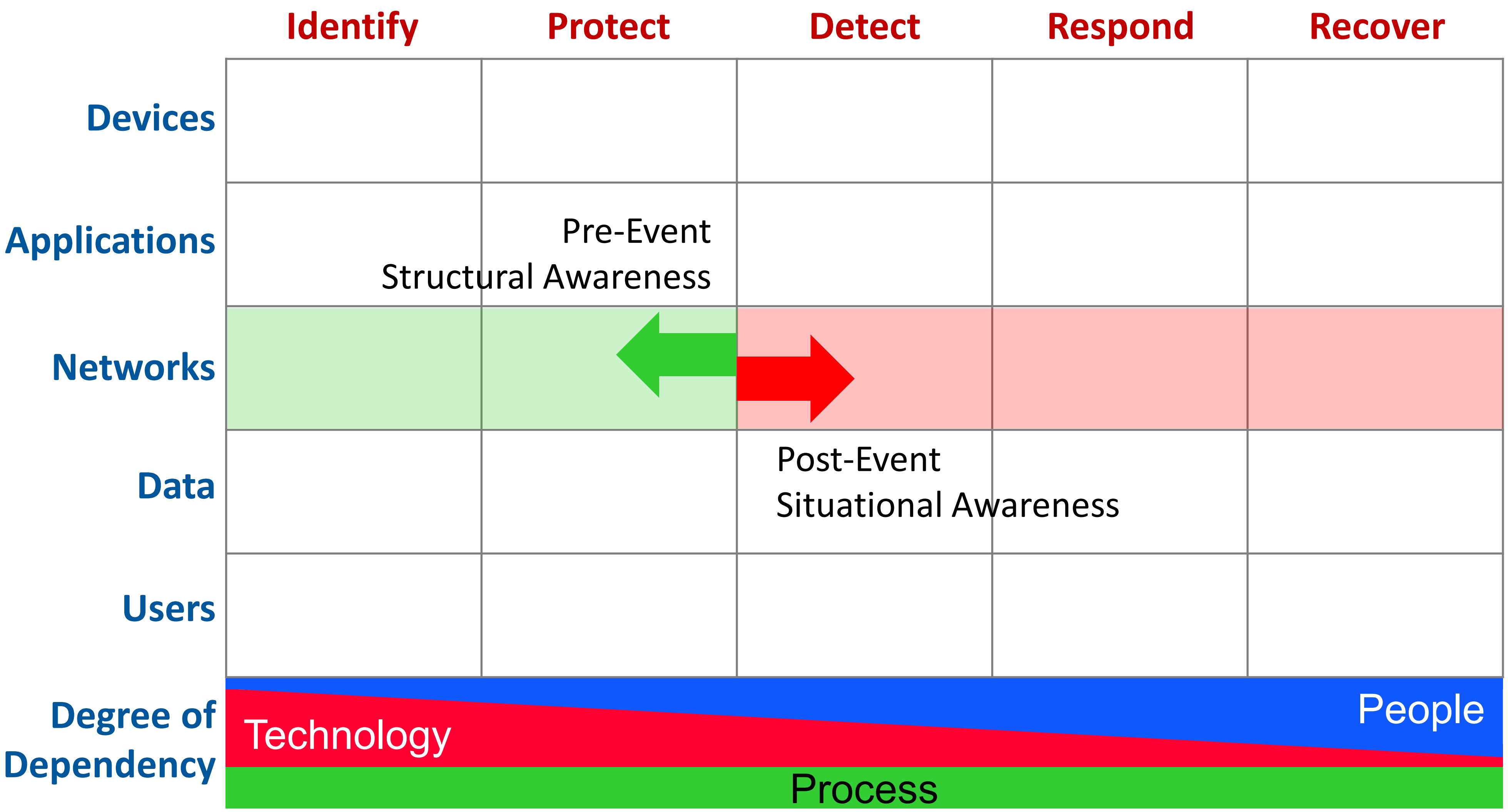
Use Case 25: Seeing gaps and opportunities

	Identify	Protect	Detect	Respond	Recover
Devices	A – B – C – D – E	F – G – H – I – J	K – L – M – N – O	P – Q – R – S – T	U – V – W – X – Y – Z
Applications	A – B – C – D – E	F – G – H – I – J	K – L – M – N – O	P – Q – R – S – T	U – V – W – X – Y – Z
Networks	A – B – C – D – E	F – G – H – I – J	K – L – M – N – O	P – Q – R – S – T	U – V – W – X – Y – Z
Data	A – B – C – D – E	F – G – H – I – J	K – L – M – N – O	P – Q – R – S – T	U – V – W – X – Y – Z
Users	A – B – C – D – E	F – G – H – I – J	K – L – M – N – O	P – Q – R – S – T	U – V – W – X – Y – Z

Degree of Dependency



Use Case 26: Improving Situational Awareness



Identify

Protect

Detect

Respond

Recover

Devices

Applications

Networks

Data

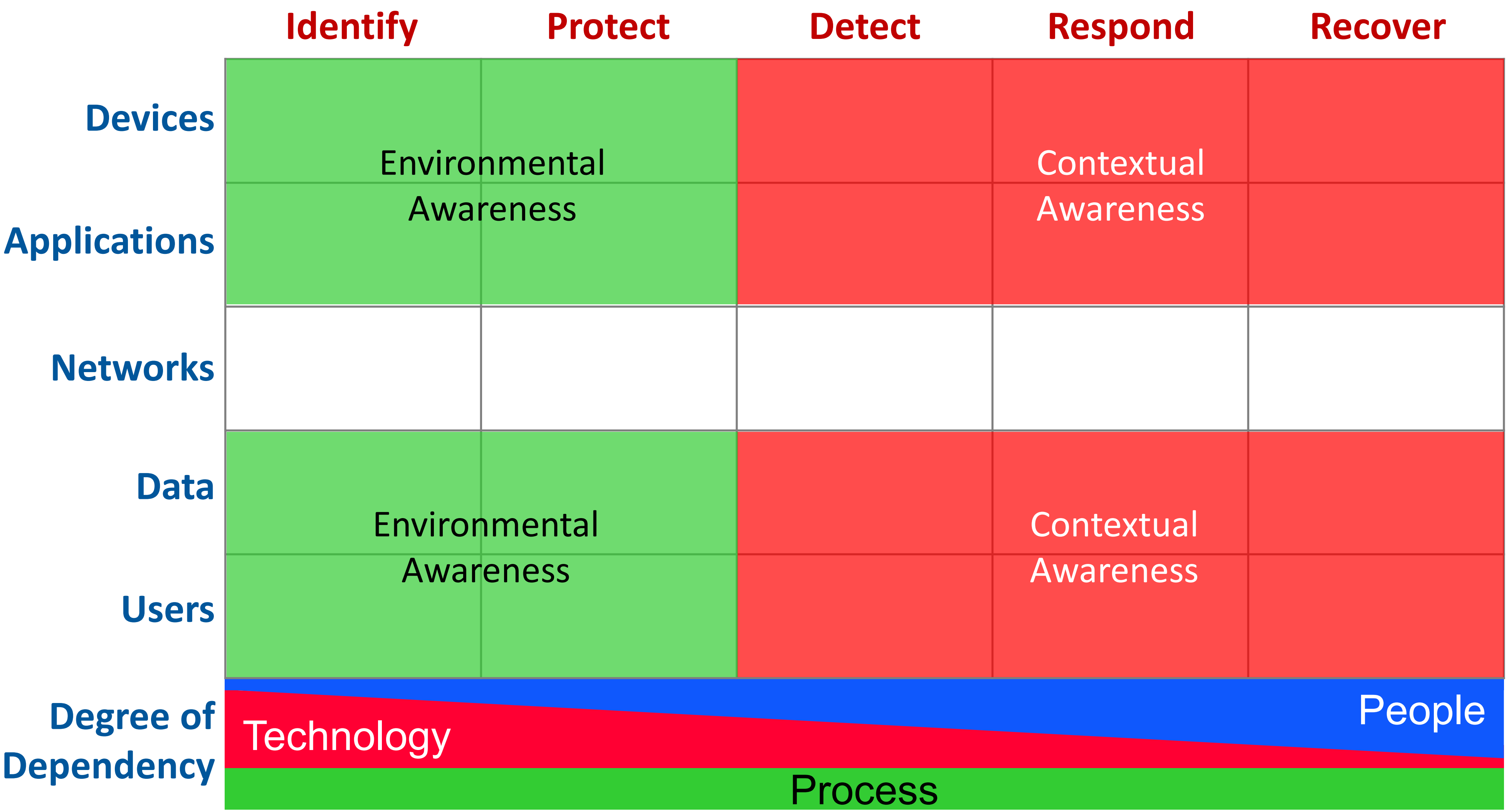
Users

Degree of Dependency

Pre-Event
Structural Awareness

Post-Event
Situational Awareness

Use Case 26: Improving Situational Awareness



Identify

Protect

Detect

Respond

Recover

Devices

Applications

Networks

Data

Users

Degree of Dependency

Environmental Awareness

Contextual Awareness

Environmental Awareness

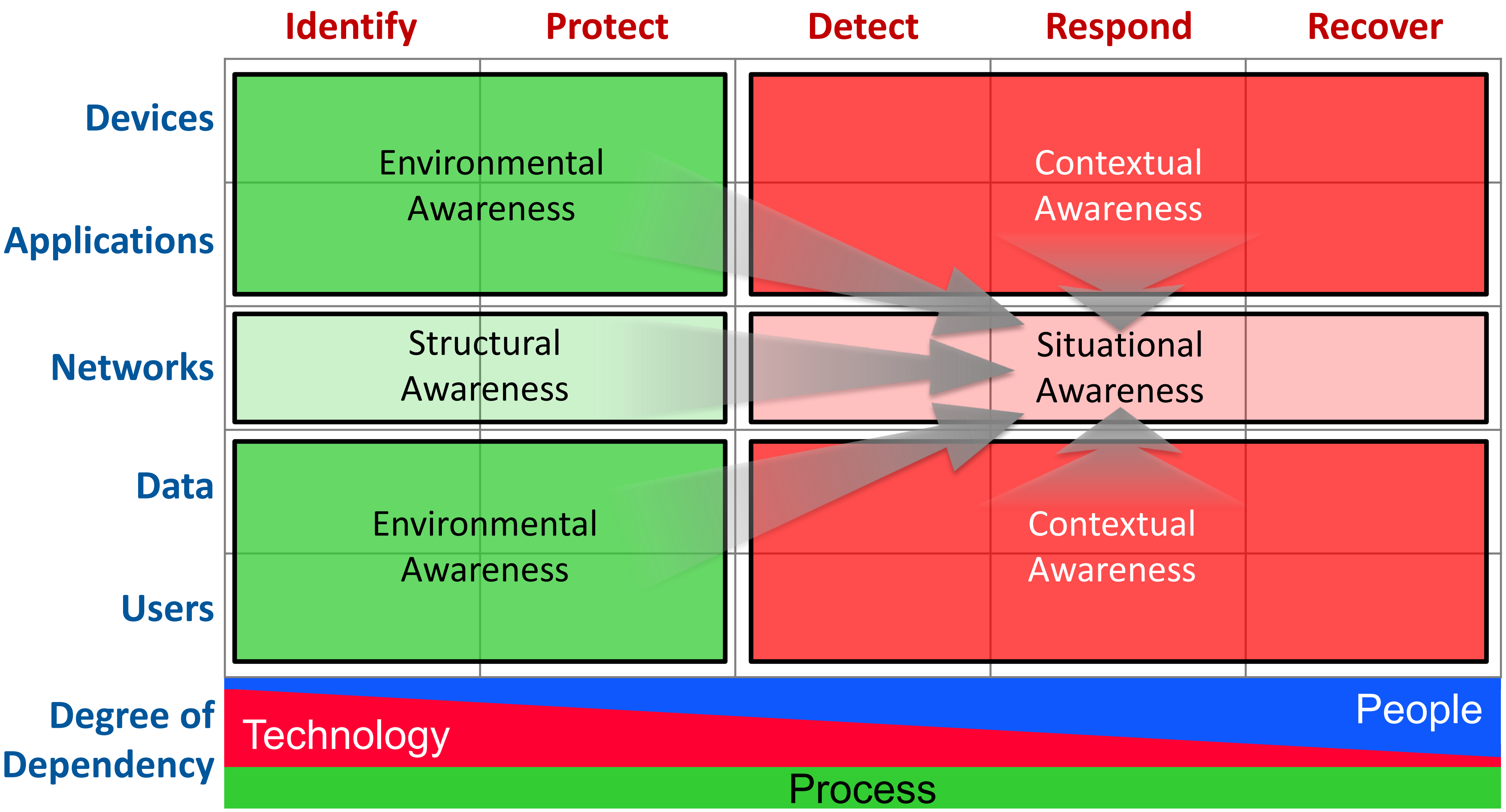
Contextual Awareness

Technology

People

Process

Use Case 26: Improving Situational Awareness



Identify Protect Detect Respond Recover

Devices

Applications

Networks

Data

Users

Environmental Awareness

Structural Awareness

Environmental Awareness

Contextual Awareness

Situational Awareness

Contextual Awareness

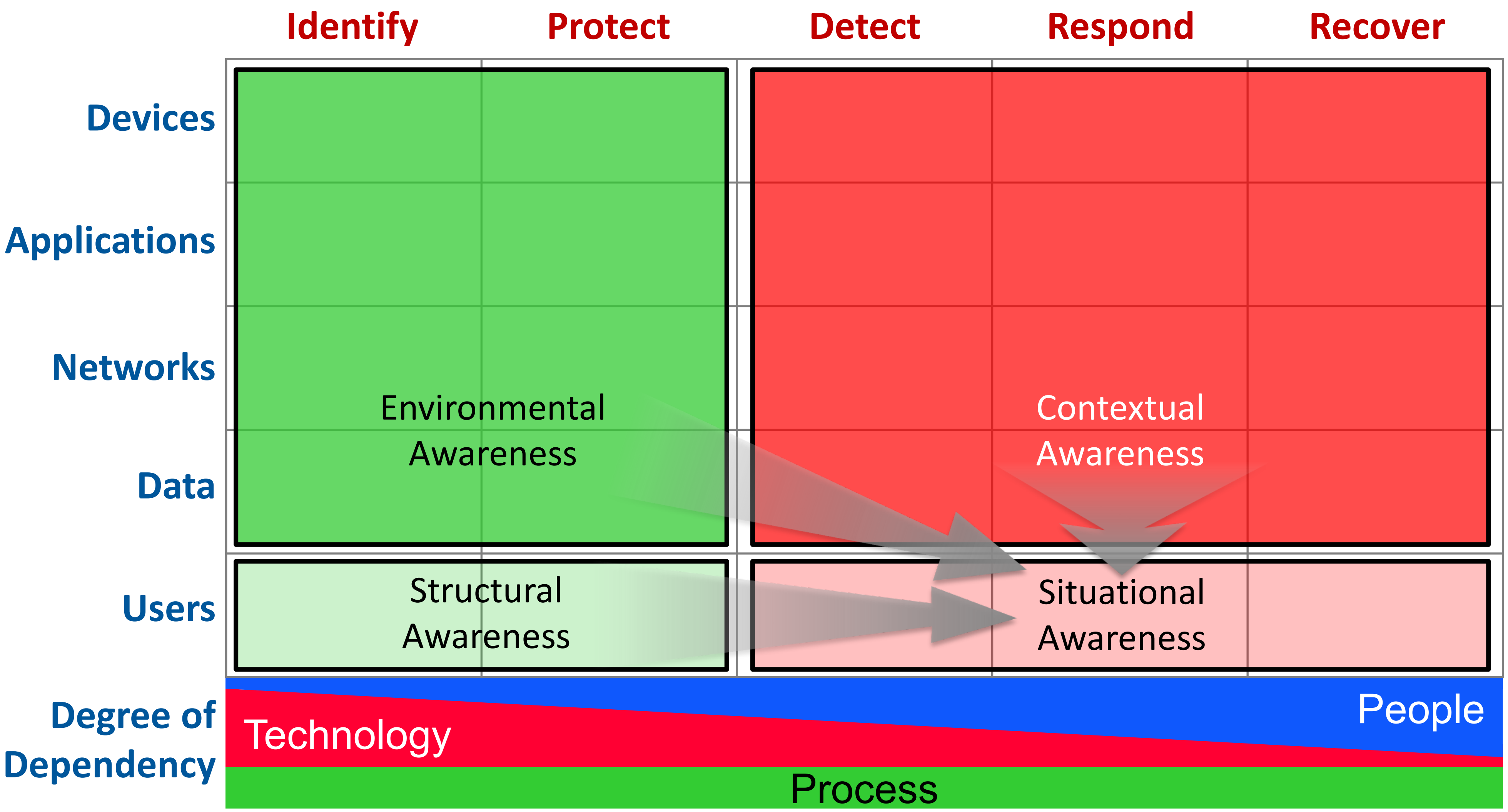
Degree of Dependency

Technology

People

Process

Use Case 26: Improving Situational Awareness



Identify

Protect

Detect

Respond

Recover

Devices

Applications

Networks

Data

Users

Environmental Awareness

Contextual Awareness

Structural Awareness

Situational Awareness

Degree of Dependency

Technology

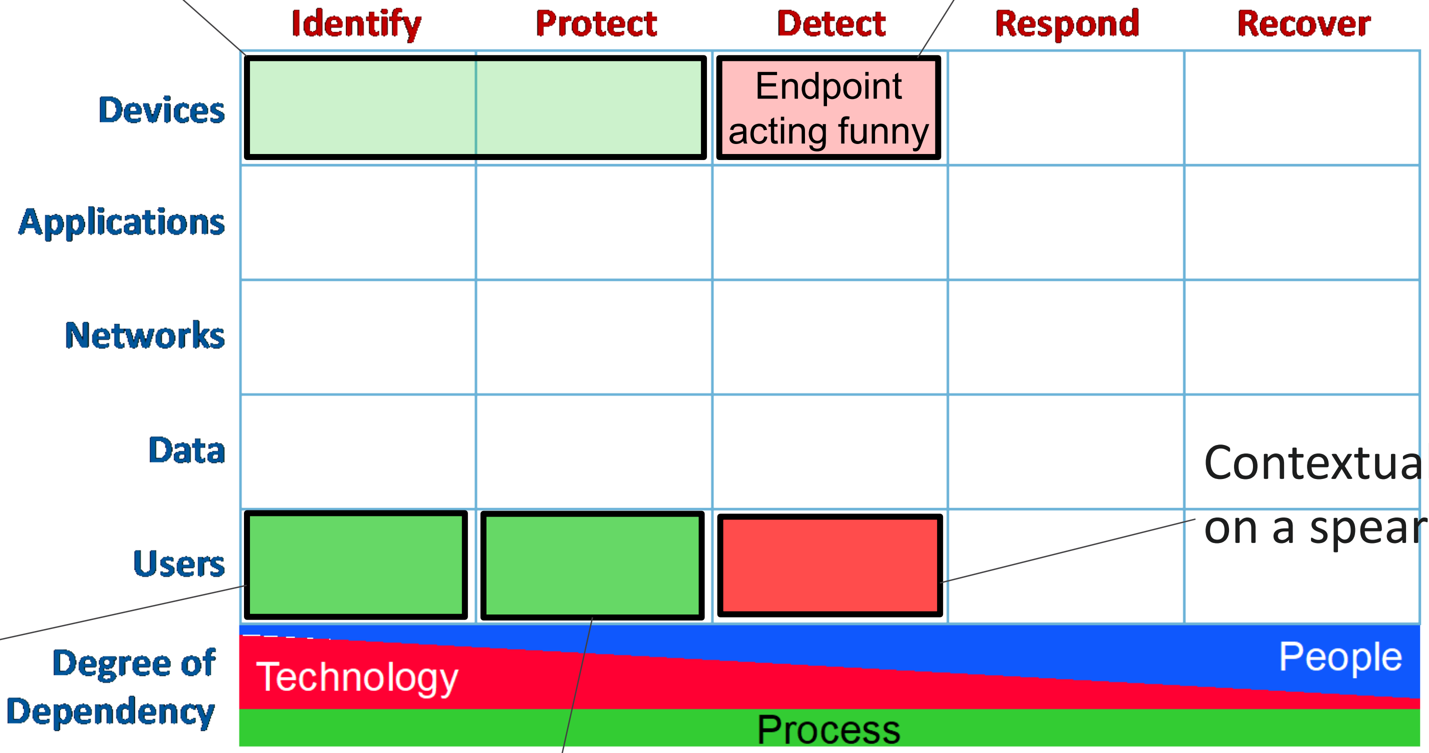
People

Process

Use Case 26: Improving Situational Awareness

Structural: Fully patched, locked down endpoint, 2FA enabled

Situational: Machine compromised due to malware installed through client-side attack



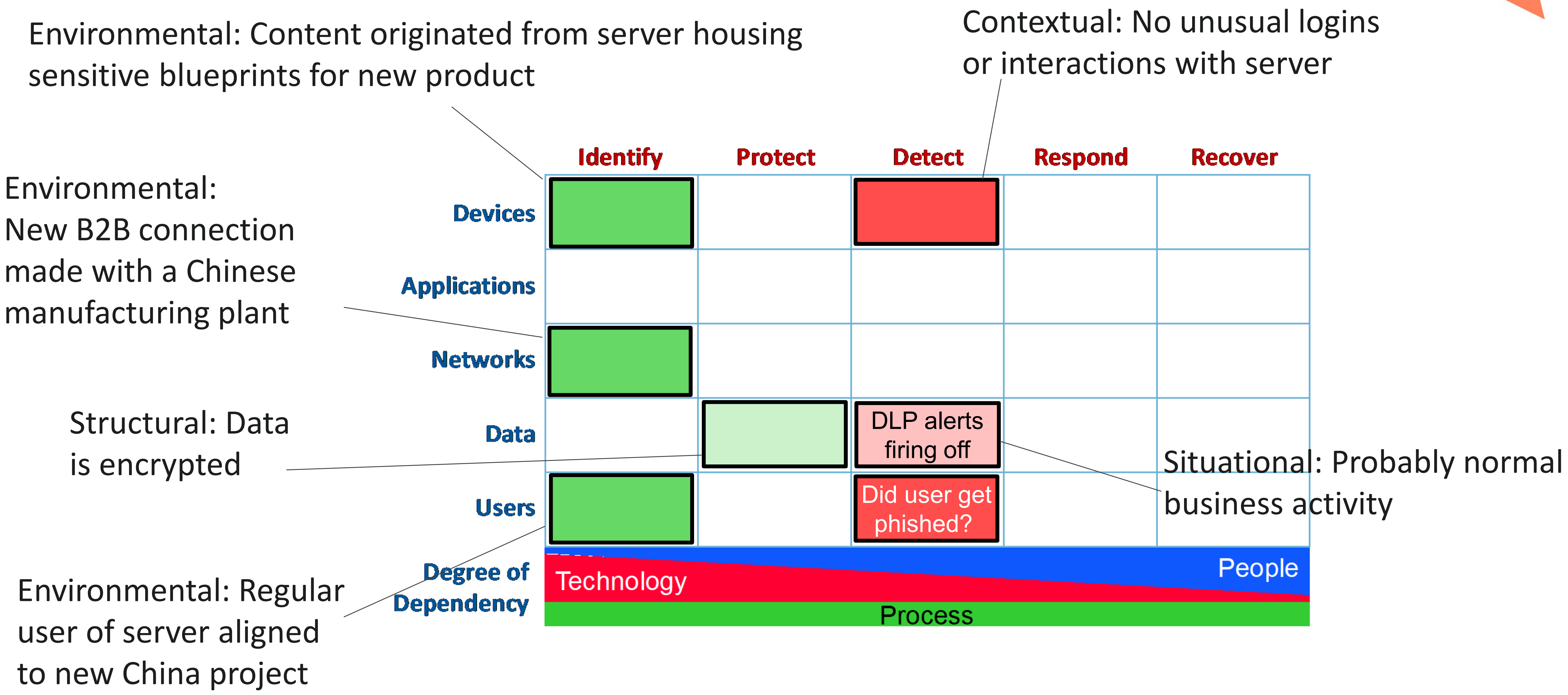
	Identify	Protect	Detect	Respond	Recover
Devices	🟩	🟩	🟥 Endpoint acting funny		
Applications					
Networks					
Data					
Users	🟩	🟩	🟥		

Contextual: User clicked on a spear phishing email

Environmental: User of endpoint failed last phishing simulation test

Environmental: Training and awareness not complete

Use Case 26: Improving Situational Awareness



Environmental: Content originated from server housing sensitive blueprints for new product

Contextual: No unusual logins or interactions with server

Environmental: New B2B connection made with a Chinese manufacturing plant

Structural: Data is encrypted

Situational: Probably normal business activity

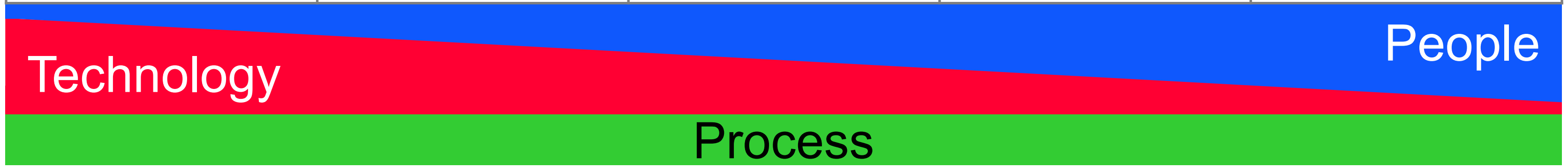
Environmental: Regular user of server aligned to new China project

	Identify	Protect	Detect	Respond	Recover
Devices	🟩		🟥		
Applications					
Networks	🟩				
Data		🟩	DLP alerts firing off		
Users	🟩		Did user get phished?		

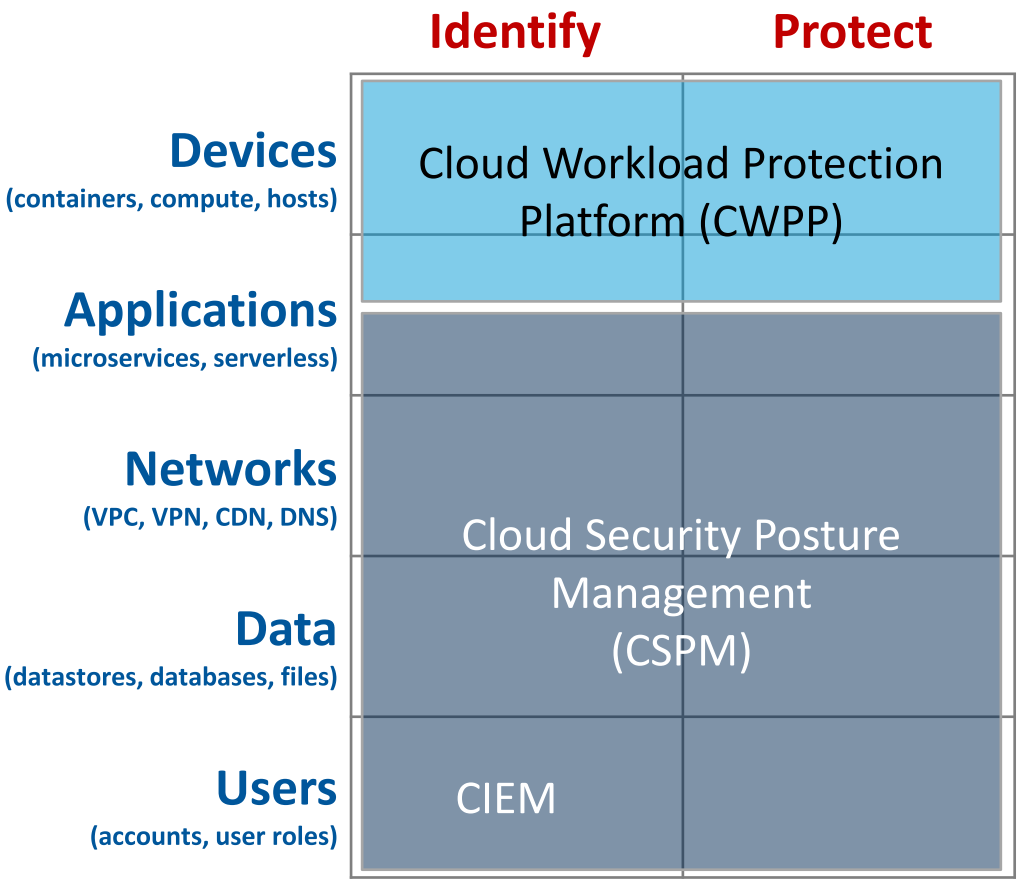
Use Case 27: Mapping Training

	Identify	Protect	Detect	Respond	Recover
Devices	**SEC460**: Enterprise Threat and Vulnerability Assessment **SEC504:** Hacker Tools, Techniques, Exploits, and Incident Handling	**SEC505:** Securing Windows and PowerShell Automation **SEC506**: Securing Linux/Unix **SEC530:** Defensible Security Architecture and Engineering	**SEC599**: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses **SEC450:** Blue Team Fundamentals: Security Operations and Analysis	**FOR500**: Windows Forensic Analysis	
Applications	**SEC504:** Hacker Tools, Techniques, Exploits, and Incident Handling	**DEV543**: Secure C/C++ Coding **SEC534:** Secure DevOps: A Practical Introduction **SEC542**: Web App Penetration Testing and Ethical Hacking			
Networks	**SEC460**: Enterprise Threat and Vulnerability Assessment **SEC504:** Hacker Tools, Techniques, Exploits, and Incident Handling	**SEC617**: Wireless Penetration Testing and Ethical Hacking **SEC530:** Defensible Security Architecture and Engineering	**SEC503**: Intrusion Detection In-Depth **SEC450:** Blue Team Fundamentals: Security Operations and Analysis	**FOR572**: Advanced Network Forensics: Threat Hunting, Analysis & Incident Response	
Data		**SEC530:** Defensible Security Architecture and Engineering			
Users	**SEC567**: Social Engineering for Penetration Testers		**SEC504:** Hacker Tools, Techniques, Exploits, and Incident Handling		

Degree of Dependency



Use Case 28: Mapping Cloud (IaaS/PaaS) Security



Identify

Protect

Devices (containers, compute, hosts)

Applications (microservices, serverless)

Networks (VPC, VPN, CDN, DNS)

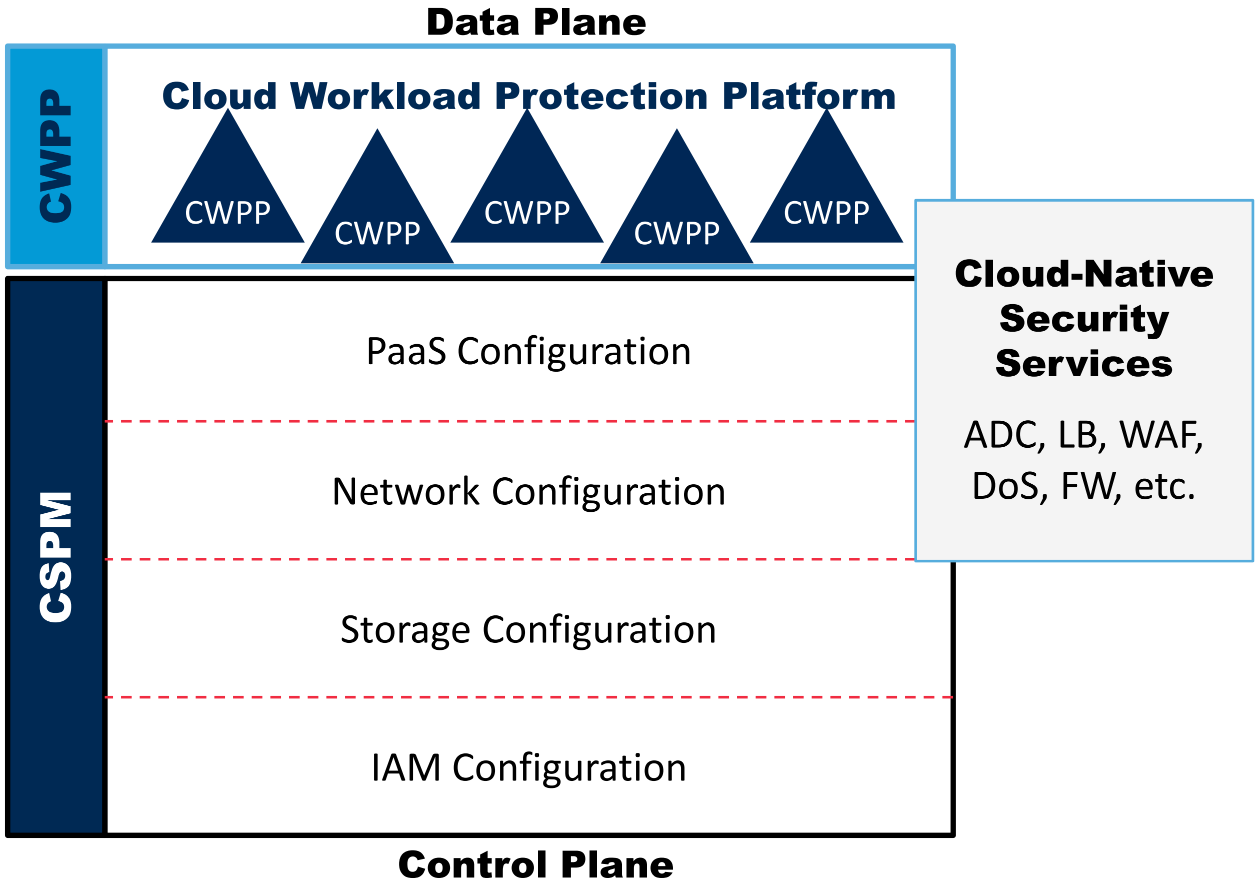
Data (datastores, databases, files)

Users (accounts, user roles)

Cloud Workload Protection Platform (CWPP)

Cloud Security Posture Management (CSPM)

CIEM



Data Plane

CWPP

Cloud Workload Protection Platform

CWPP

CWPP

CWPP

CWPP

CWPP

CSPM

PaaS Configuration

Network Configuration

Storage Configuration

IAM Configuration

Cloud-Native Security Services

ADC, LB, WAF, DoS, FW, etc.

Control Plane

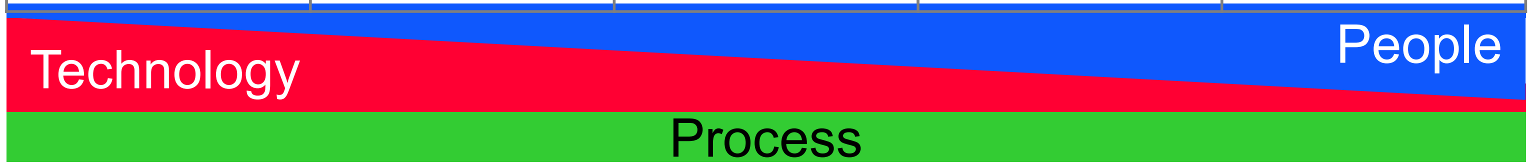
Source: Gartner Market Guide for Cloud Workload Protection Platforms, 2020 (slightly modified)

Use Case 29: Mapping Control Failures

Courtesy of Adrian Sanabria (@sawaba)

	Identify	Protect	Detect	Respond	Recover
Devices	1, 12	26, 28	29		
Applications	2, 8, 21, 23	26	3, 9, 13, 14		
Networks		4, 5, 6, 7, 16	10, 11, 20		
Data	15, 23	16, 17, 19	17, 18, 20		
Users					

Degree of Dependency

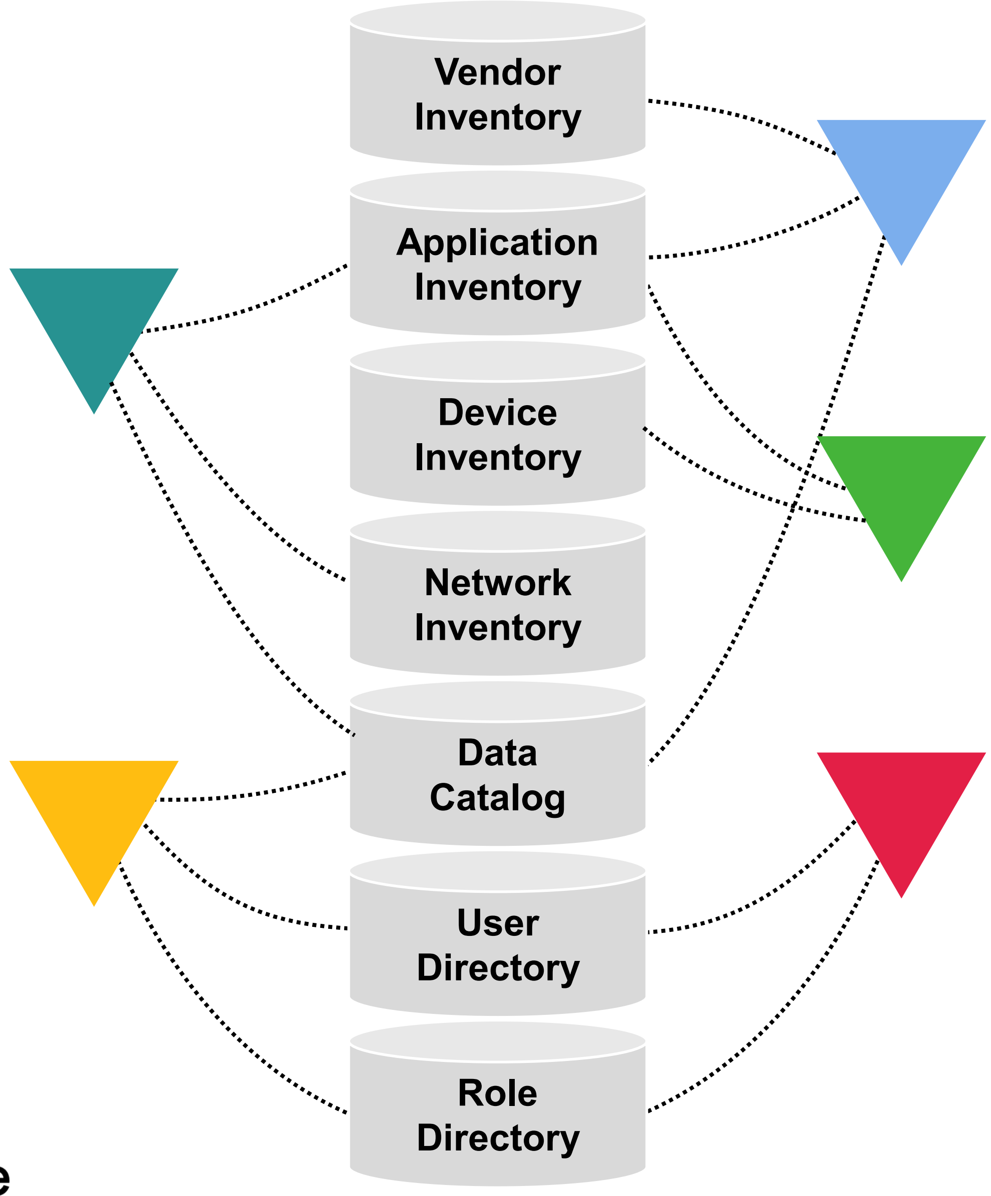


Tech Oriented Control Failure

People Oriented Control Failure

Process Oriented Control Failure

Use Case 30: Reconciling Inventories



All data associated with Internet facing applications must be classified/ tagged

Data owners must formally hold that role and be part of the organization accountable for that data

Authorized data sources can only go to approved vendors from approved applications

Applications must run on known systems or be contained in authorized container registries

All employees must have a direct manager

- Enable inventory reconciliation using a multi-domain approach using the five asset classes of the Cyber Defense Matrix
- Drive better data quality by creating “fast lanes” for security approvals if inventories are up-to-date

With modifications from original source: https://www.philvenables.com/post/taking-inventories-to-the-next-level-reconciliation-and-triangulation

“Apply” Slide

- Map your security organization to the Cyber Defense Matrix
- Try out the use cases described here, in the previous briefings, and in the Cyber Defense Matrix book
- Develop a new use case for the Cyber Defense Matrix
- Share the new use case with the community!

Want to learn more?

CYBER DEFENSE MATRIX
The Essential Guide to Navigating the Cybersecurity Landscape
By Sounil Yu
Forewords by Dan Geer and Wendy Nather

Come to the Learning Lab (LAB2-R01)
Thursday, June 9 @ 8:30a-10:30a

Come even if registration is full! If you get denied entry, I'll give you a free signed copy of the book!

Grab a free signed copy at:

- fastly Booth (Tuesday, June 7, 12:45-1:15)
- JupiterOne Booth (Wednesday, June 8, 11:30-12:30)

Questions?

@sounilyu

@cyberdefmatrix

sounil@cyberdefensematrix.com

https://cyberdefensematrix.com

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

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