CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

.govCAR TRAINING

CISA
CYBER+INFRASTRUCTURE

Unclassified//For Official Use Only

Feb 27, 2019

Agenda

08:30	Check In
09:00	Welcome -- Goals and Intent
09:10	.govCAR Introduction
09:30	.govCAR Architecture Under Analysis
10:00	.govCAR Threat Methodology
10:30	*Break*
10:45	.govCAR Scoring
11:15	.govCAR Analysis Overview
11:45	*Questions*
12:00	Lunch
1:00	Capability Scoring for Protect/Detect/Respond
2:00	Analysis
2:45	*Break*
3:00	Continue Analysis
3:30	Breakouts: Architecture, Threat, Facilitating a scoring session

CISA
CYBER+INFRASTRUCTURE

Introductions

- Introduce yourself
  - Company/Department/Agency
  - Role
  - Interest in .govCAR
- What is your goal for today?

CISA
CYBER+INFRASTRUCTURE

Goals for this Morning's Training

- Provide insight and knowledge to prepare the audience to read, understand and derive maximum value from the .govCAR Technical Annex
- Deeper technical and methodology training than the standard 30 minute overview

CISA
CYBER+INFRASTRUCTURE

.govCAR goals

- Inform DHS's approach to assisting Departments and Agencies with insight and knowledge to make prioritized cybersecurity investment decisions across the .gov environment
  - Create a threat-based security architecture review that provides an end-to-end holistic assessment that is composed of capabilities provided by DHS or the individual Departments and Agencies.
  - Create a common framework to discuss and assess cybersecurity architectural choices:
    - For a shared Federal IT Infrastructure
    - To inform DHS's approach for its capabilities
    - To enable Departments and Agencies to make threat-based risk decisions
- Be transparent and traceable

CISA
CYBER+INFRASTRUCTURE

.govCAR: Move to Stronger Risk Management

.govCAR

Compliance

Risk determination based on checklist

Cyber Hygiene

Risk determination based on automated asset and account management

Threat-based Approach

Risk determination based on performance-based measures

CISA
CYBER+INFRASTRUCTURE

Relationship to DoDCAR

- The Department of Defense Cybersecurity Analysis and Review (DoDCAR) was created by the DoD CIO, NSA, and DISA in June of 2015 to analyze the existing architecture and proposed changes and make recommendations
- Developed a threat-based methodology that provided a single evaluation framework across the full scope (holistic) of the DoD Architecture, including the DoD boundary and individual services and agencies
- Architectural recommendations used to drive budget (POM) and programmatic changes
- .govCAR began in April 2017 and leverages the same methodology and is part of the DoDCAR community
- OMB "Federal Cybersecurity Risk Determination Report and Action Plan", May 2018 – implement the Cyber Threat Framework to prioritize efforts and manage cybersecurity risks.

CISA
CYBER+INFRASTRUCTURE

Why .govCAR?

- Are my current cyber security capabilities protecting me against threats?
- If not, where are the gaps?
- Am I investing my cyber security budget wisely?
- Is there unwanted duplication of security functionality?
- What should my next investment be?

CISA
CYBER+INFRASTRUCTURE

How to use .govCAR

- Evaluate architectures of architectures (layered architecture)
- Evaluate enterprise architectures and capabilities (vendor independent descriptions of building blocks, e.g., firewall)
- Evaluate security stack architectures and capabilities
- Support investment direction and decisions
- Can evaluate people, policy and process capabilities, but has been primarily used for technology (materiel) evaluation

CISA
CYBER+INFRASTRUCTURE

How NOT to use .govCAR

- Does not evaluate vendor implementations of a capability
- Does not provide mission-based/cyber key terrain-based analysis (no impact analysis)
- Does not provide implementation choices

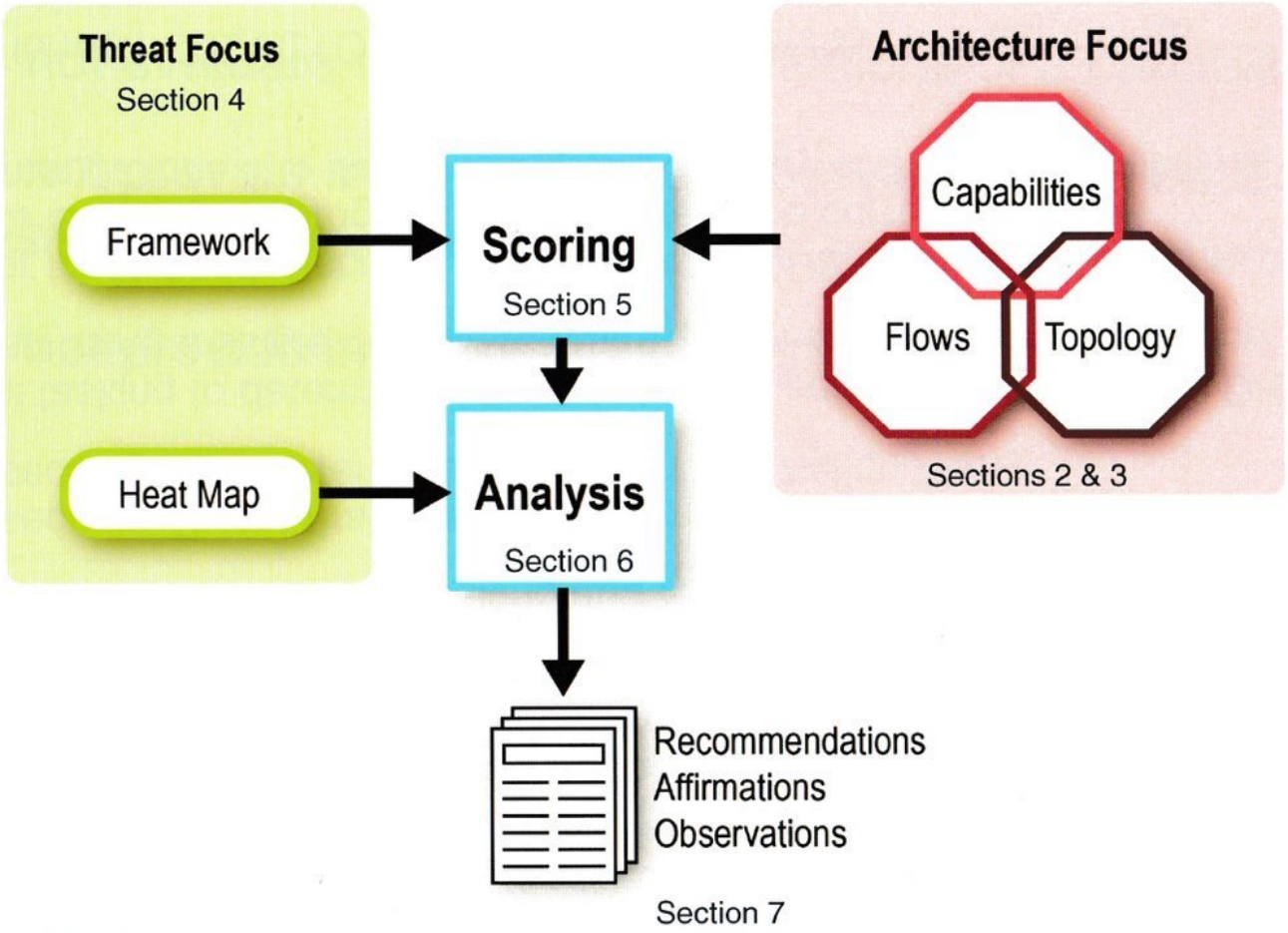
CISA
CYBER+INFRASTRUCTURE

Impact of .govCAR

- Have provided actionable recommendations, backed by extensive data and analysis, for targeting cybersecurity investments on department and agency networks, and for DHS services
- Provided input for decision-making and revectoring on CDM Phase 3, TIC RA v3.
- Cybersecurity Threat Framework mentioned in OMB report: Federal Cybersecurity Risk Determination Report and Action Plan
- Special tasking to determine if there is a clear security distinction for DHS between using a single or multi-tenant deployment model for MS Office 365
- Director for Network Security Deployment at DHS, signed out a memo directing the NCPS and CDM program to incorporate the current .govCAR recommendations into the planning and delivery of evolving capabilities (August 2018)
- Newly formed CISA CTO using .govCAR results to drive technology investigations

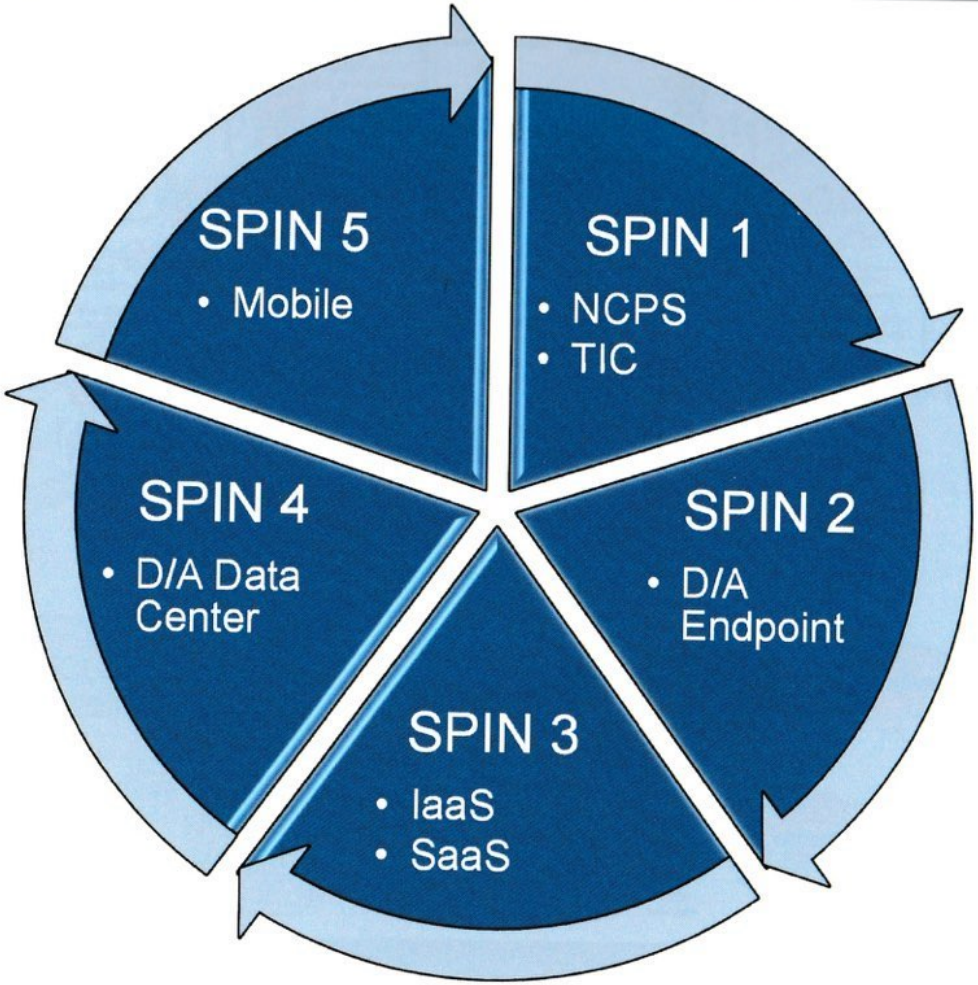
CISA
CYBER+INFRASTRUCTURE

.govCAR Methodology



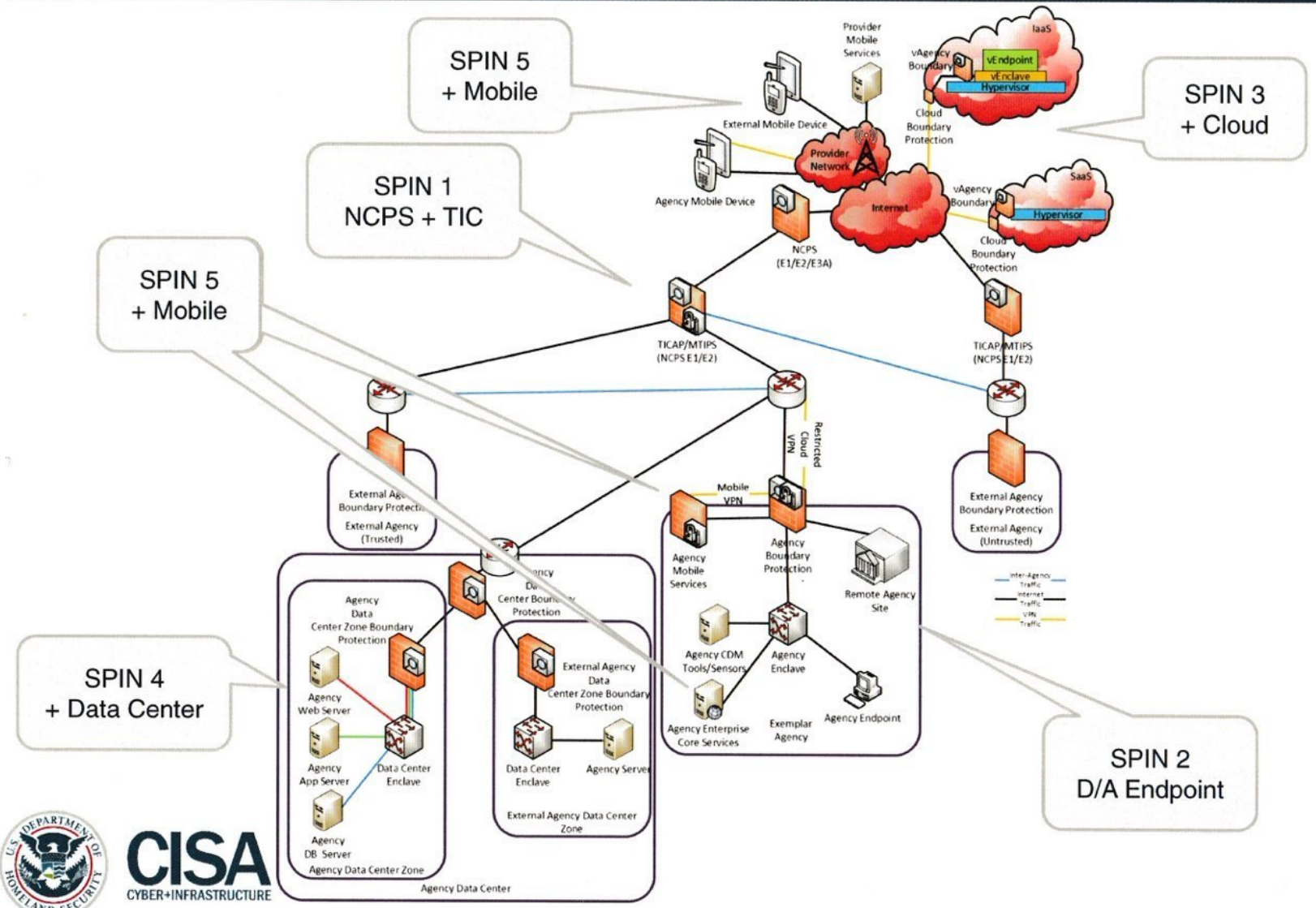
CISA
CYBER+INFRASTRUCTURE

SPINs to date



CISA
CYBER+INFRASTRUCTURE

Spin 1-5 Architecture View



CISA
CYBER+INFRASTRUCTURE

Core Assumptions

- Capabilities are deployed and used as intended. Scores do not reflect the impact of partial, incomplete, or incorrect deployment of a capability.
- A generic architecture is used for scoring and analysis; current results do not represent a particular D/A.

CISA
CYBER+INFRASTRUCTURE

Deliverables

.gov Cybersecurity Architecture Review (.govCAR)

Technical Annex

Version 5.0

December 19, 2018

For Official Use Only

Not to be Published

CISA
CYBER+INFRASTRUCTURE

.gov Cybersecurity Architecture Review (.govCAR)

Spin 5 Summary and Findings

December 19, 2018

Version 1.0

For Official Use Only

CISA
CYBER+INFRASTR

.govCAR
Spin 5 Preliminary Results
11/27/2018
V 1.2

CISA
CYBER+INFRASTRUCTURE

Homeland Security FOUO

Additional Materials

- Methodology Document
- Slick Sheets
- Fact Sheets

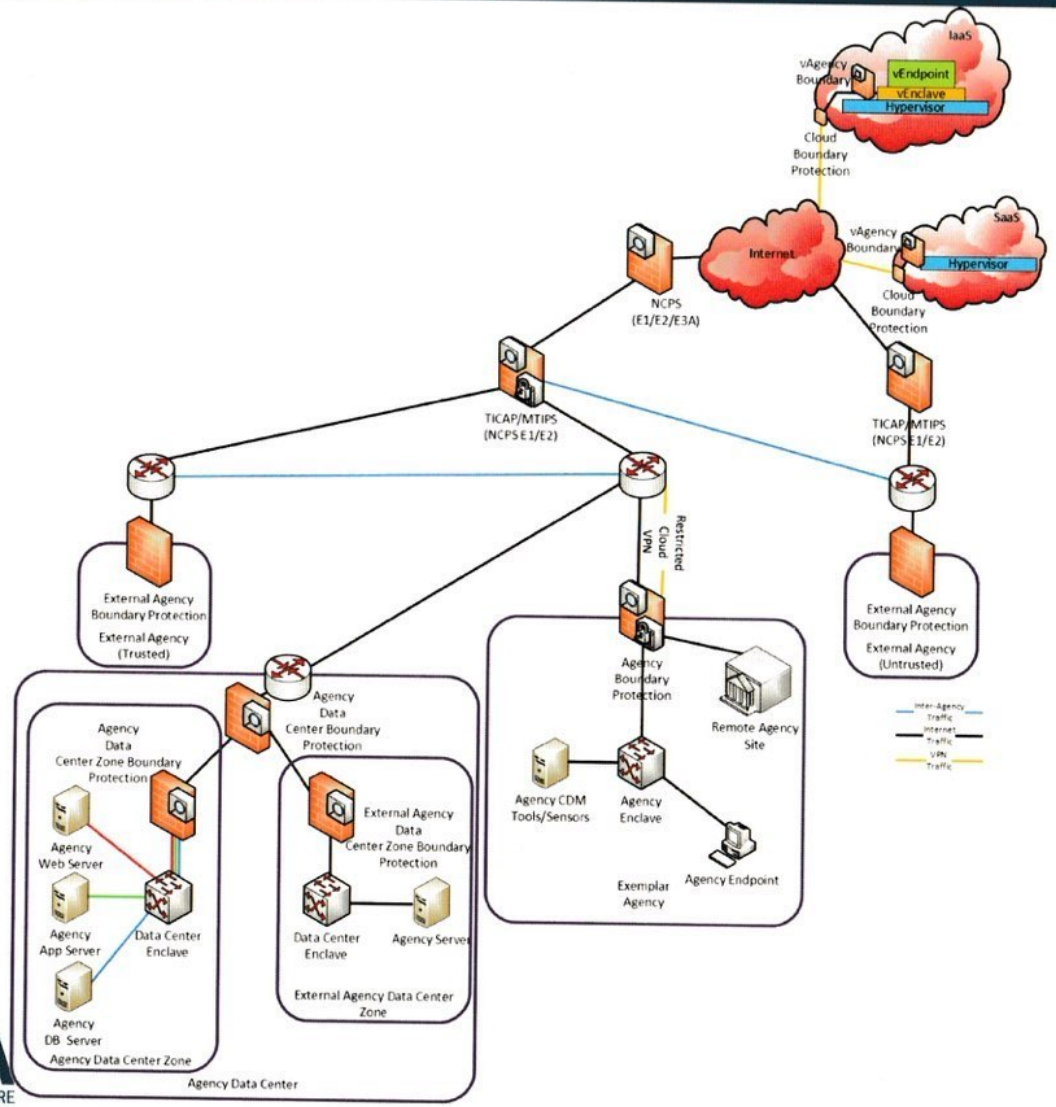
CISA
CYBER+INFRASTRUCTURE

ARCHITECTURE UNDER ANALYSIS

Kurt

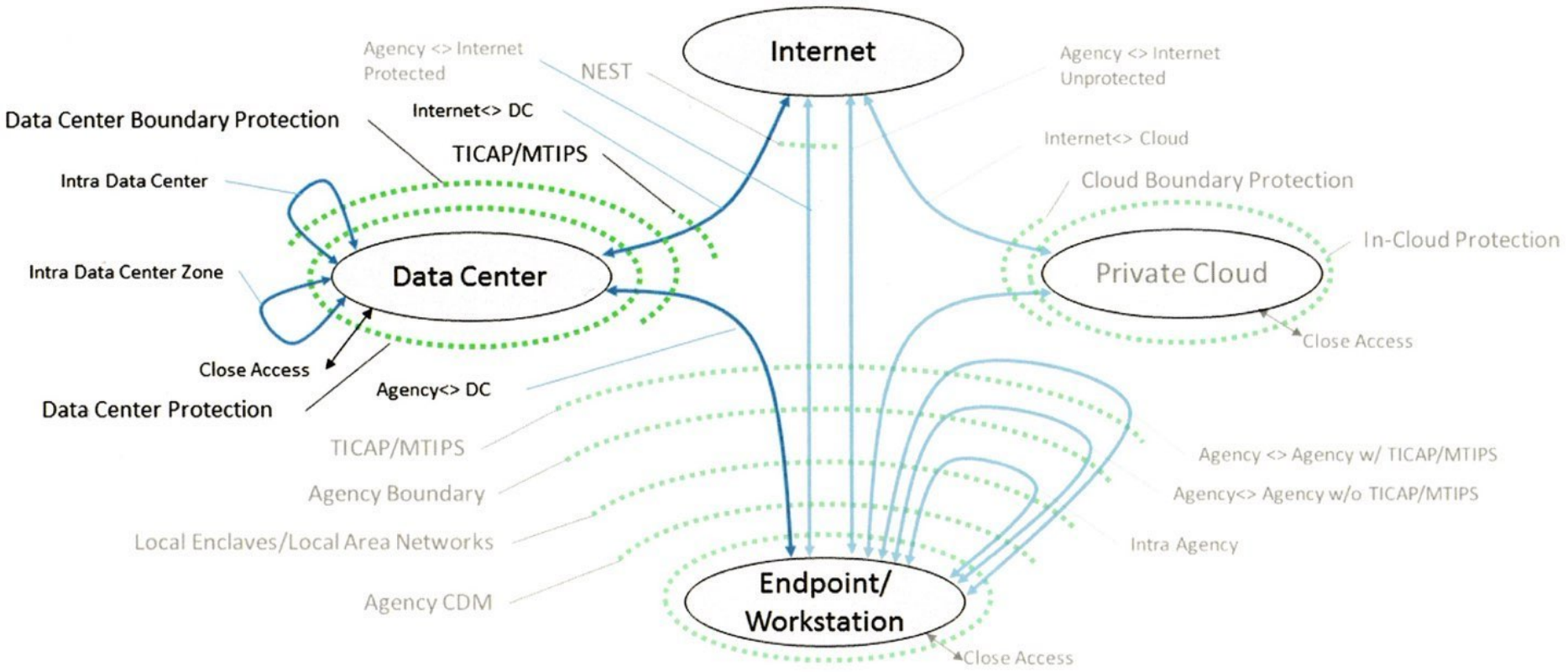
CISA
CYBER+INFRASTRUCTURE

Representative Architecture (Section 2)



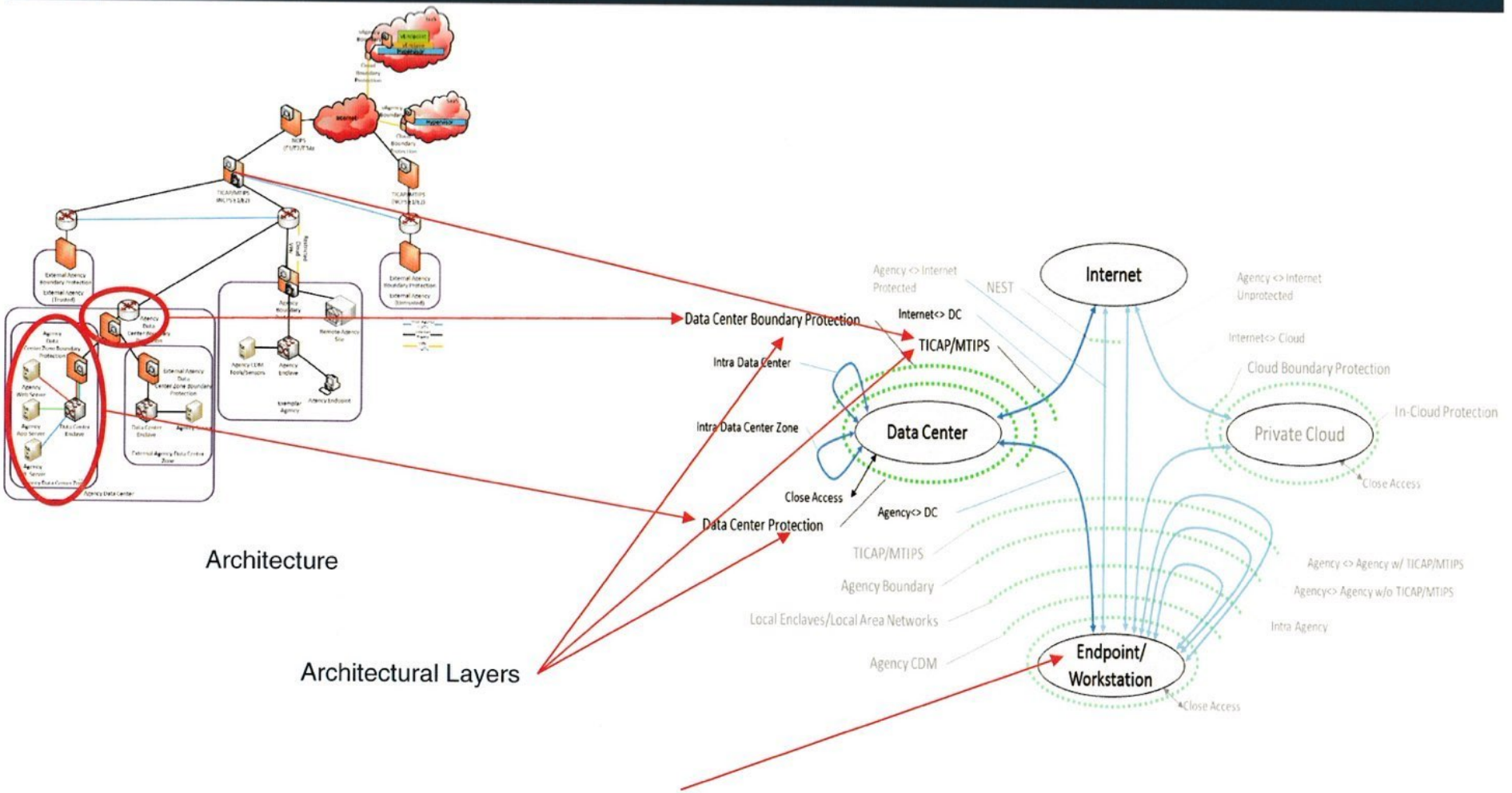
CISA
CYBER+INFRASTRUCTURE

Data Center Data Flows (Section 3)



CISA
CYBER+INFRASTRUCTURE

Spin 4 Architecture and Flows Relationship



Considered to be untrusted – no credit for endpoint/enclave protections

CISA
CYBER+INFRASTRUCTURE

Capabilities (Section 3 and Appendix C)

TICAP/MTIPS	Spin	Description	Assumptions
Firewall TICAP/MTIPS	1,3	Deep Packet Inspection (DPI) firewall	Scored without access to clear text traffic payload data
Firewall TICAP/MTIPS Enhancements	1,3	Adds QoS and file reputation	Scored without access to clear text traffic payload data
Firewall TICAP/MTIPS w/ Break & Inspect (B&I)	1,3		Scored with access to clear text traffic payload data
Firewall TICAP/MTIPS Enhancements w/ B&I	1,3	Adds QoS and file reputation	Scored with access to clear text traffic payload data

Section 3 – List of capabilities in an architectural layer with an abbreviated capability description

Architectural Layer → TICAP/MTIPS Capabilities

Architectural Layer Capabilities → Table C-1.8 – TICAP/MTIPS - Firewall Features

Appendix C – Detailed list and description of the features of the architectural layer capabilities

"Future" and "Enhancements" are part of the "Planned" architecture

Feature	Description
GeoIP Blocking source/dest IP	The source/destination IP address is checked against a vendor supplied GeoIP database and is filtered according to rules in the NGFW/IPS. Supports custom IP assignment into GeoIP groups.
Application Filtering	Deep Packet Inspection is used to identify the application (e.g., Skype) being used in a session and supports filtering by application. Supports custom application identification. Supports blocking functions w/in applications (e.g., file transfer w/in instant messaging).
Protocol Port Enforcement	Using Application Identification enforce that ports are only being used for the intended application.

Architecture layer capabilities have one or more features that are described in a generic nature (i.e., not a specific product, but generally included in products in that category) and in sufficient detail to allow scoring for P/D/R against threat actions

CISA CYBER+INFRASTRUCTURE

Spin 4 Architectural Layers & Capabilities

TICAP/MTIPS:
Firewall
Passive Sensor

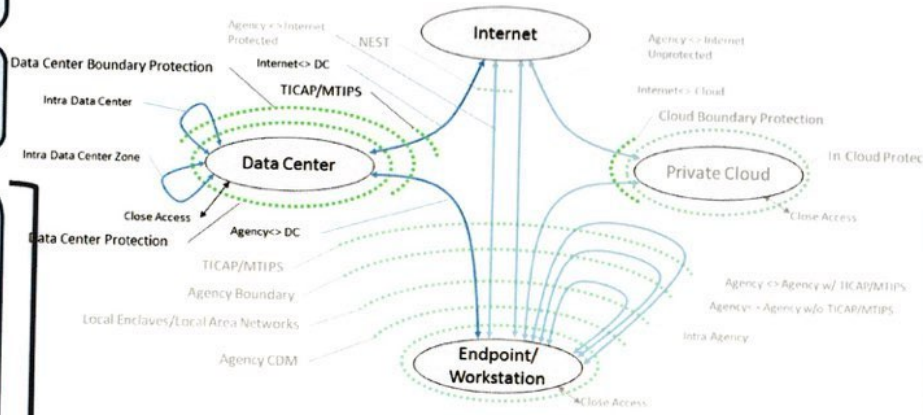
Data Center Boundary:
IP Blacklist
DDoS Mitigation

Data Center Zone Boundary:
NGFW
Passive Sensor
WAF/RWP
ID Federation/RBAC/MFA
DBFW
DBAM

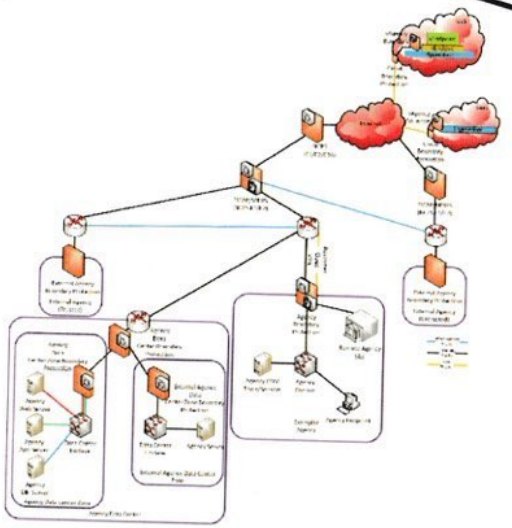
Data Center Enclave:
Network Segmentation
NAC

Agency Server:
Host IPS/FW
Device Control
File Integrity
DHC
DHC-R
Application Whitelisting

Current



Data Center Protection



Planned

TICAP/MTIPS:
Firewall Enhancements
Passive Sensor

Data Center Boundary:
IP Blacklist
DDoS Mitigation

Data Center Zone Boundary:
NGFW
Passive Sensor
WAF/RWP Enhancements
ID Federation/RBAC/MFA
DBFW
DBAM

Data Center Enclave:
ANDB
Network Segmentation
NAC Enhancements

Agency Server:
Host IPS/FW
Device Control
File Integrity
DHC
Auto DHC-R
Application Whitelisting
Reputation

CISA
CYBER+INFRASTRUCTURE

Meaning of with and without B&I

- ~75% of traffic to/from D/As is encrypted (mostly HTTPS)
- Need to show the effect of widely-used encryption on ability to mitigate threats
- Notation:
  - "without B&I" - govCAR scoring assumes 100% of traffic is encrypted (except DNS)
  - "with B&I" – govCAR scoring assumes that in some manner clear text traffic payload is available to the component being scored
- Not intended to imply or endorse the ***method*** (e.g., Break & Inspect) of decryption – just a shorthand notation for access to clear text traffic payload

CISA
CYBER+INFRASTRUCTURE

THREAT METHODOLOGY

Ingrid

CISA
CYBER+INFRASTRUCTURE

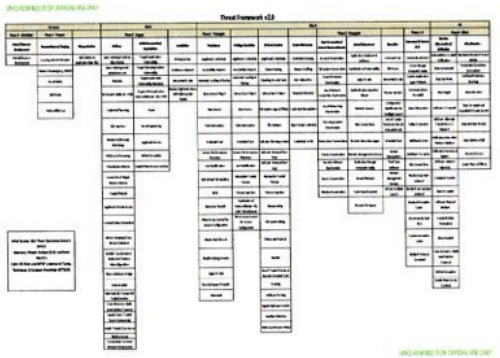
Cyber Threat Framework

STAGES
The progression of cyber threats over time to achieve objectives

OBJECTIVES
The purpose of conducting an action or series of actions

ACTIONS
Actions and associated resources used by a threat actor to satisfy an objective

Pre-Event	Get-In	Stay-In	Act
Intent/Resource Development 1	Delivery 23	Persistence 18	Monitor / Exfiltration 17
Reconnaissance/ Staging 5	Initial Compromise/ Exploitation 9	Privilege Escalation 13	Alter/Deceive 9
Weaponize 1	Installation 4	Defense Evasion 21	
		Credential Access 7	
		Host Enumeration/ Internal Recon 11	
		Lateral Movement 12	
		Execution 11	
		Command & Control 15	



Set of threat actions requiring counteraction by Protect / Detect / Respond

CISA
CYBER+INFRASTRUCTURE

NSA Adversary Lifecycle Threat Framework v2.0

Pre-Event			Get In			Stay In								Act	
Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/ Exploitation	Installation	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration/ Internal Reconnaissance	Lateral Movement	Execution	Command & Control (C2)	Monitor (Observation)/ Exfiltration	Alter/Deceive...
Intent/Resource Development	Crawling Internet Websites	Add Exploits to Application Data Files	Spear-phishing Emails w/ Attachments	Targets Application Vulnerability	Writing to Disk	Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software	Command Line	Commonly used port	Automated or Scripted Exfiltration	Distributed Denial of Service (DDOS)
	Network Mapping (e.g. NMAP)		Spear-phishing email w/Malicious Link	Target Operating System Vulnerability	In Memory Malware	Accessibility Features	Accessibility Features	Binary Padding	Virtualization Attacks	File System Enumeration	Virtualization Attacks	File Access	Comm through removable media	Virtualization Attacks	Partial disk/OS deletion (corruption)
	Social Media		Websites	Targets Application Vulnerability Remotely	Interpreted Scripts	Automatic Loading at Startup	Automatic Loading at Startup	Disabling Security Tools	Network Sniffing	Group Permission Enumeration	Exploitation of Vulnerability	Interpreted Scripts	Custom Application layer Protocol	Data Compressed	Full disk/OS deletion (bricking)
	Mid-Points		Removable Media (i.e. USB)	~~Targets Web Application Vulnerabilities (ex: XSS, CSRF, SQL)~~	Replace legitimate binary with Malicious (ex: Haven)	Library Search Hijack	Library Search Hijack	Library Search Hijack	User Interaction	Local Network Connection Enumeration	Logon Scripts	Process Injection	Communications Encrypted	Data Size limits	Data Alteration
	Vulnerability Scan		Credential Pharming	Trojan		New Service	New Service	File System Logical Offsets	Password Recovery	Local Networking Enumeration	Authentication Assertion Misuse	Configuration Modification to Facilitate Launch	Data Obfuscation	Data Staged	Data Encrypted and Unavailable (Crypto Locker)
			~~SQL Injection~~	Social Engineering		Path Interception	Path Interception	File Deletion	Credential Manipulation	Local Network Enumeration	Remote Services	Use of Trusted Process to Execute Untrusted Code	Fallback Channels	Exfil over C2 channel	Data Deletion (Partial)
			Application or Operating System Exploit over the Network	Legitimate Access		Scheduled Task	Scheduled Task	Indicator Blocking on Host	Hijack Active Credential	Operating System Enumeration	Peer Connections	Scheduled Task	Multiband comm	Exfil over Alternate Channel to a C2 Network	Data Deletion (full)
			Web Application Exploit over the Network	Defeat Encryption		Service File Permission Weakness	Service File Permission Weakness	Indicator Removal from Tools	Credentials in File	Owner/User Enumeration	Remote Interactive Logon	Service Manipulation	Multilayer Encryption	Exfiltration Over other Network Medium	Denial of Service
			Deploy Exploit using Advertising	Exploit Weak Access Controls		Link Modification	Link Modification	Indicator Removal from Host		Process Enumeration	Remote Management Services	Third Party Software	Peer Connections	Exfiltration from Local System	Cause Physical Effects
			DNS/Cache Poisoning			Edit Default File Handlers	Manipulate Trusted Process	Manipulate Trusted Process		Security Software Enumeration	Replication through removable media	Remote Management Services	Standard app layer protocol	Exfil over network resources	
			Virtualization Attacks			BIOS	Process Injection	Process Injection		Service Enumeration	Shared Webroot	APIs to Facilitate Launch	Standard non-app layer protocol	Scheduled Transfer	
			Connection of Rogue Network Devices			Install Hypervisor Rootkit	Exploitation of Vulnerability (ex. XSS, CSRF, OS/Software)	Masquerading		Window Enumeration	Taint Shared Content		Standard Encryption Cipher	Data Encrypted	
			Trusted Website			Modify Service Configuration	Weak Access Control for Service Configuration	File System Hiding			Remote File Shares		Uncommonly Used Port	Exfil over Virtual Medium	
			Legitimate Remote Access			Master Boot Record	Multi Tenant Side Channel Cache Attack	Obfuscated Payload					Custom encryption cipher	Exfil over Physical Medium	
			Crosstalk (Data Emanation)			Modify Existing Services		Rootkit					Multiple Protocols Combined	Crosstalk (Data Emanation)	
			Device Swapping (Cross Domain Violation)			Logon Scripts		Use of Trusted Process to Execute Untrusted Code					C2 via Cloud Service	Data Encoded	
			Exploit Cross Domain or Multi-Level Solution Misconfiguration			Security Support Provider		Scripting						Cross Domain or Multi-Level Solution Traversal	
			Physical Network Bridge			Web Shell		Software Packing						Defeat Encryption	
			Data Encoded					Signed Malicious Content						Exploit Weak Access Controls	
			Automatically Transported Trusted Services					Sandbox Detection						Exfil via Cloud Service	
			Cross Domain or Multi-Level Solution Traversal					Malicious Behavior Delays							
			Supply Chain / Trusted Source Compromise (Hardware)												
			Supply Chain / Trusted Source Compromise (Software)												
			Auto Delivery via Cloud Service												
			Insider Threat/Close Access												
			Wireless Access												
			Compromise Common Network Infrastructure												
			Defeat Encryption												

Legend:	
	Deprecated in govCAR Spin 4
	govCAR spin 4 modifications

Initial Sources:
* **NSA Threat Operations Center's (NTOC) Adversary Lifecycle Analysis (ALA)**
* **Lockheed Martin's Cyber Kill Chain**
* **MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)**

CISA
CYBER+INFRASTRUCTURE

Reading a threat description

- Think like the adversary

Initial Compromise/ Exploitation	Trojan	The process of executing malicious code (trojans) on a victim computer within a victim's network to gain personal information. Adversaries infect victim computers with malware (trojans) via remote access trojans (RATs).	http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/3/

- Attacks are broken apart across the framework…

Intent/Resource Development : Intent/Resource Development

Weaponization : Add Exploits to Application Data Files

Delivery : Spear-phishing Emails w/ Attachments

Initial Compromise/ Exploitation : Trojan

Sample 'trojan' compromise*

Command & Control (C2) : Commonly used port

Lateral Movement : Remote File Shares

Defense Evasion : Indicator Removal from Host

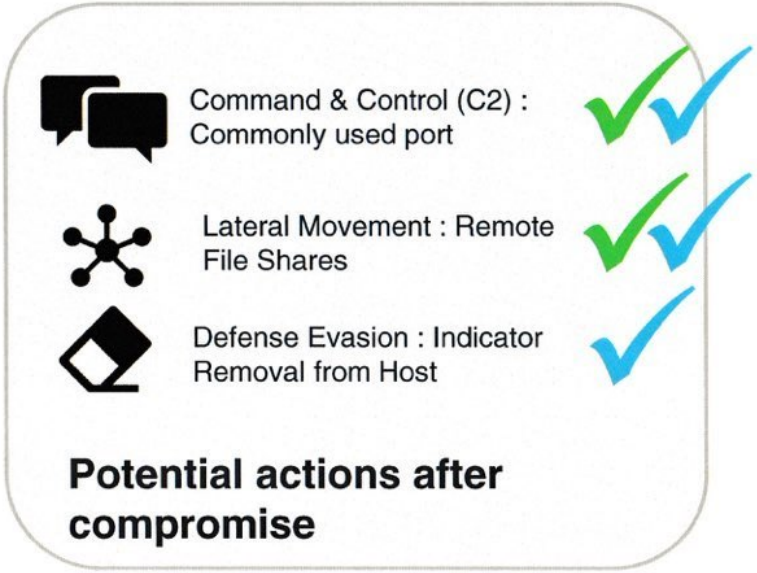
Potential actions after compromise

CISA CYBER+INFRASTRUCTURE

* May not represent all steps in actual compromise

Endpoint v Network

- Network observables sometimes occur in earlier phases or are covered under command and control
- Being observable on the network does not mean all points in the network (lateral movement may only be observable on a local segment)
- Endpoint observables include strictly host-based activity



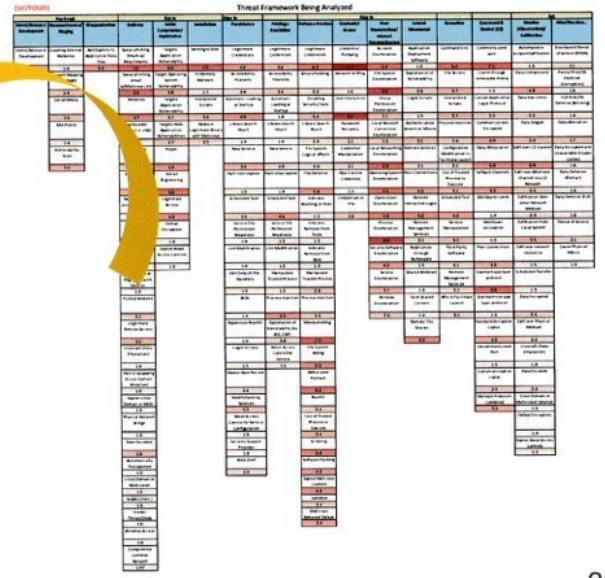
Not observable on network or endpoint Network Observable Endpoint Observable

CISA CYBER+INFRASTRUCTURE

Threat Heat map

- Heat map reflects prevalence (number of actors) & maneuverability (number of threat actions available in the objective) of adversary action
- Based on open source reporting with data on 63 different threat actor groups
  - Full list in Appendix B
- Documented threat actions map to 143 out of 188 threat actions
- Manual process to review reports and map to the threat framework

Stay In			
Defense Evasion	**Credential Access**	**Host Enumeration/ Internal Reconnaissance**	**Lateral Movement**
Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software
6.2	12.2	6.4	1.5
Binary Padding	Network Sniffing	File System Enumeration	Exploitation of Vulnerability
2.0	1.6	8.0	2.6
Disabling Security Tools	User Interaction	Group Permission Enumeration	Logon Scripts
3.4	8.6	3.1	1.5
Library Search Hijack	Password Recovery	Local Network Connection Enumeration	Authentication Assertion Misuse
2.0	2.2	2.6	3.1



CISA
CYBER+INFRASTRUCTURE

SCORING

Pete

CISA
CYBER+INFRASTRUCTURE

Scoring Team Members

- Architecture / Analysis WG member
  - Knows capability & scoring procedure; performs initial normalization; documents mitigation capability
- Threat WG member
  - Knows threat framework; assists in helping team to understand the threat actions
- Capability SME
  - From organization that owns capability; knows the details of the capability for determining mitigation; sets score
- Communications WG member
  - Develops understanding of capability and rationale for scoring in preparation for documenting
- Facilitator
  - Runs the process during a scoring meeting; responsible for overall adherence to methodology

CISA
CYBER+INFRASTRUCTURE

Scoring Approach

NIST Framework for Improving Critical Infrastructure Core Functions

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- **Protect** – Preventative measures with or without detection; near immediate effect
- **Detect** – Passive; identifies use of a given action/technique, results in event data in cyber relevant time
- **Respond** – Response after actions/techniques successful
  - Can be detection
  - Can be analysis
  - Can be changing configuration
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capability or services that were impaired due to a cybersecurity event. (Not scored in this analysis.)

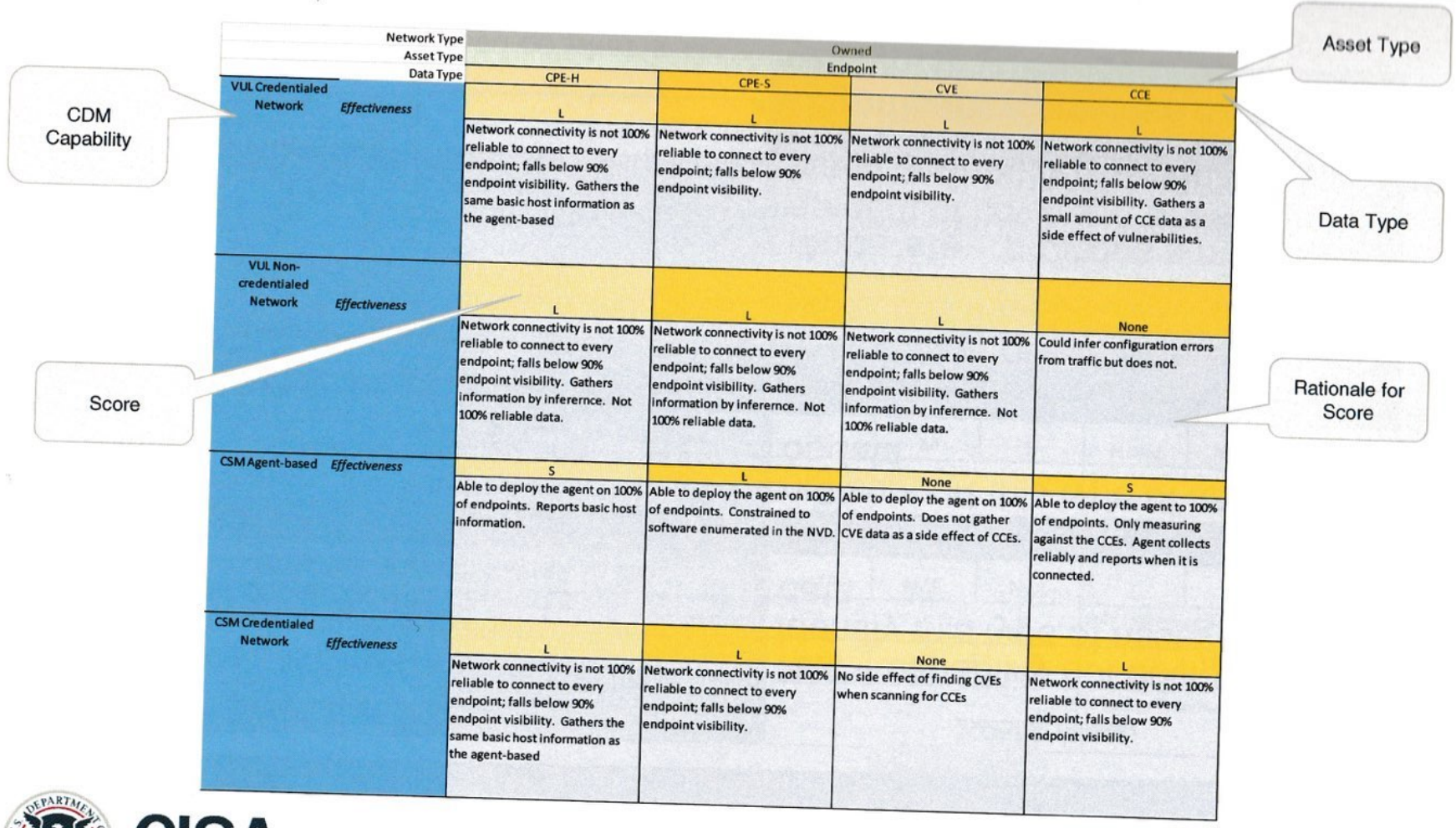
CISA
CYBER+INFRASTRUCTURE

Identify –Additional Details

- Identify capabilities provide *data to develop the organizational understanding* to manage cybersecurity risk to systems, assets, data and capabilities.
- Identify capabilities may not provide the ability to protect, detect, or respond to a threat action but *enable other capabilities* that do.
- Identify capabilities *enumerate* the security capabilities, process, policy and assets under protection.

CISA
CYBER+INFRASTRUCTURE

Identify Scoring Spreadsheet



Network Type	Owned			
Asset Type	Endpoint			
Data Type	CPE-H	CPE-S	CVE	CCE
VUL Credentialed Network *Effectiveness*	L	L	L	L
	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility. Gathers the same basic host information as the agent-based	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility.	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility.	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility. Gathers a small amount of CCE data as a side effect of vulnerabilities.
VUL Non-credentialed Network *Effectiveness*	L	L	L	None
	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility. Gathers information by inferernce. Not 100% reliable data.	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility. Gathers information by inferernce. Not 100% reliable data.	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility. Gathers information by inferernce. Not 100% reliable data.	Could infer configuration errors from traffic but does not.
CSM Agent-based *Effectiveness*	S	L	None	S
	Able to deploy the agent on 100% of endpoints. Reports basic host information.	Able to deploy the agent on 100% of endpoints. Constrained to software enumerated in the NVD.	Able to deploy the agent on 100% of endpoints. Does not gather CVE data as a side effect of CCEs.	Able to deploy the agent to 100% of endpoints. Only measuring against the CCEs. Agent collects reliably and reports when it is connected.
CSM Credentialed Network *Effectiveness*	L	L	None	L
	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility. Gathers the same basic host information as the agent-based	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility.	No side effect of finding CVEs when scanning for CCEs	Network connectivity is not 100% reliable to connect to every endpoint; falls below 90% endpoint visibility.

CISA
CYBER+INFRASTRUCTURE

Identify Scoring Rubric

Identify Data Types

- **CPE-H** - Basic Information concerning the physical device and its existence, presence or connection to networks (platform - hardware and OS – has to be IP addressable)
- **CPE-S** - Presence and versioning information of software installed and enabled on hardware (any software over/above the OS)
- **CVE** - Understanding of known vulnerabilities within that Hardware and the Software it is currently running
- **CCE** - Understanding of the security-related configuration settings for Software installed on Hardware

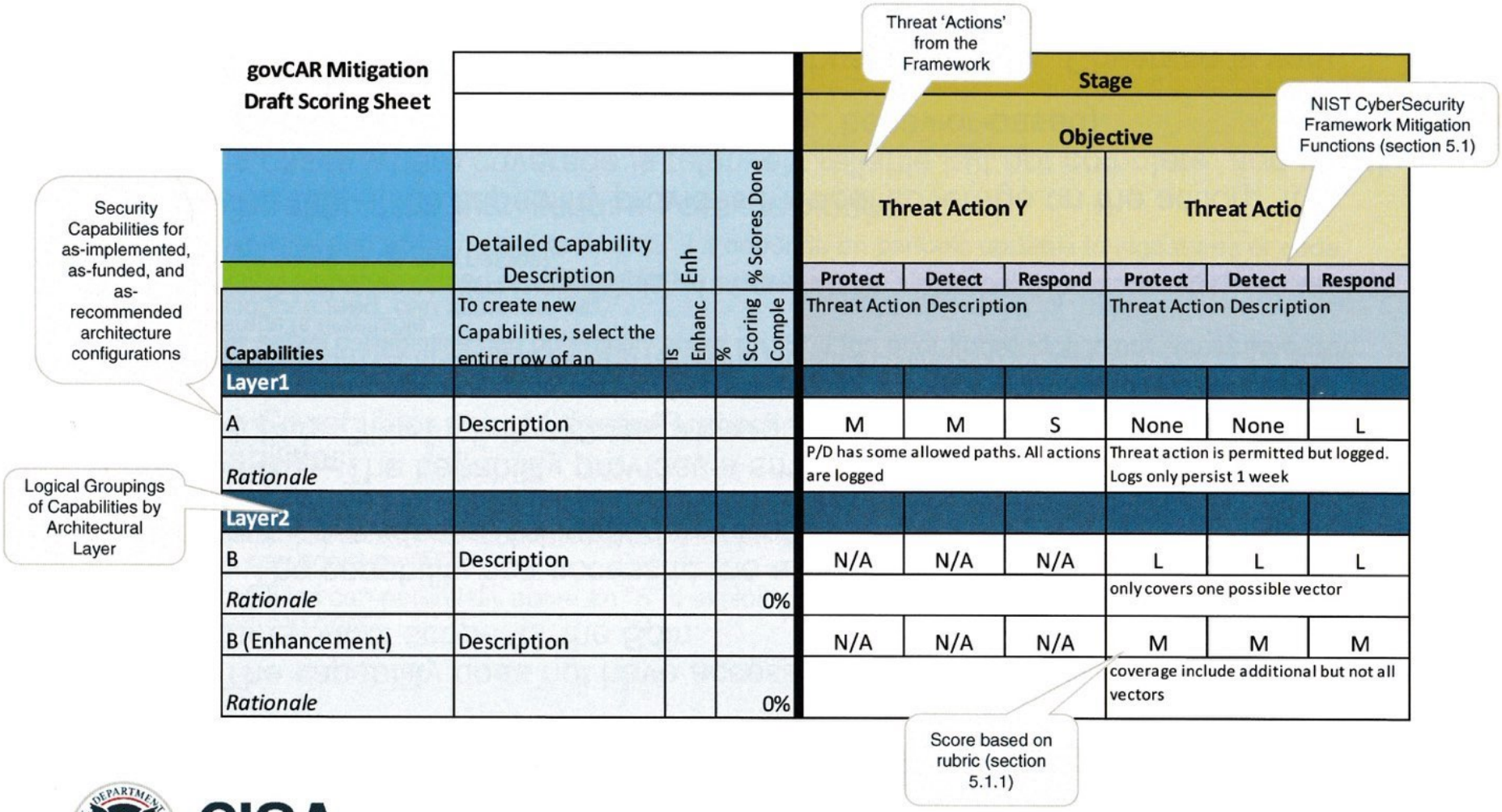
Assumption: Scoring CCE based on what is available to be configured.

Scoring Values

- **N/A** – capability not designed to identify this type of asset/entity or data
- **None** – could, but currently does not support this type of asset/entity or data
- **Limited** – provides a small amount of coverage of asset/entity types or data; less than 90%
- **Moderate** – provides a moderate amount of coverage of asset/entity types or data; 90% to 98%
- **Significant** – provides a significant amount of coverage of asset/entity types or data; greater than 98%

CISA
CYBER+INFRASTRUCTURE

Protect, Detect, Respond (PDR) Scoring Spreadsheet



govCAR Mitigation Draft Scoring Sheet				Stage					
				Objective					
	Detailed Capability Description	Enh	% Scores Done	Threat Action Y			Threat Actio		
				Protect	Detect	Respond	Protect	Detect	Respond
Capabilities	To create new Capabilities, select the entire row of an	Is Enhanc	% Scoring Comple	Threat Action Description			Threat Action Description		
Layer1									
A	Description			M	M	S	None	None	L
Rationale				P/D has some allowed paths. All actions are logged			Threat action is permitted but logged. Logs only persist 1 week		
Layer2									
B	Description			N/A	N/A	N/A	L	L	L
Rationale			0%				only covers one possible vector		
B (Enhancement)	Description			N/A	N/A	N/A	M	M	M
Rationale			0%				coverage include additional but not all vectors		

CISA
CYBER+INFRASTRUCTURE

Protect / Detect / Respond Scoring Values

- **N/A** – The capability does not have access to artifacts associated with the threat action or is out of scope for the Spin.
- **None** – The capability has access to the artifacts associated with the threat action but it provides no mitigation coverage
- **Limited (L)** – The capability provides a small amount of coverage to the given threat action. This includes cases where
  - A capability can mitigate an action, but only for a small subset of the possible execution methods for that action; the P/D/R score will be reduced to reflect the pro-rated contribution for total mitigation of the action.
  - Coverage is unreliable.
  - Protect/Detect relies on exact foreknowledge of adversary tools, protocols or infrastructure (e.g., adversary IP address space or domain names)
- **Moderate (M)** – The capability provides modest coverage on the action. It includes cases where coverage is relatively reliable but not complete, and mostly not dependent on exact foreknowledge (e.g., behavior-based).
- **Significant (S)** – The capability provides robust coverage. Coverage is very reliable, almost complete, and not dependent on foreknowledge.

PDR Scoring Intricacies

- Cyber Relevant Time
  - Applies to Protect and Detect
  - Can score 'none' for Detect, but have scores for Protect and Respond.
- Scoring Capabilities that Require Foreknowledge
  - Capabilities can score no higher than "L" if it depends on periodic updates to signatures or code.
  - A similar signature-based capability that is updated essentially in real-time, such as from a threat intelligence feed, can score an "M".
  - A few select capabilities can potentially score an "S" if the prior knowledge is not signature-based, perhaps utilizing machine learning to generate algorithms for static analysis.
- Scoring Capabilities that Mitigate/Remediate Misconfigurations or Open Vulnerabilities
  - A capability can score no higher than "L" if it depends on ad-hoc application of fixes.
  - A similar capability that is updated and can apply patches or restore configurations essentially in real-time, can score an "M".
  - Capabilities can potentially score an "S" if exploiting the vulnerability is not able to affect the underlying host.

Non-Materiel Mapping

- For non-materiel capabilities (e.g. people, processes, policy), a modified scoring approach is used.
- The mapping process requires making extrapolations and assumptions about the possible implementations of a non-materiel capability to provide potential mitigation for a threat action.
- We interpret the non-materiel capabilities in a broad manner, representing non-materiel capabilities with the largest potential applicability to threats
- The mapping process also assumes that the non-materiel capabilities have been implemented for more than just compliance, but can be measured for proper implementation in support of Ongoing Assessment (as defined in the CDM Program).

CISA
CYBER+INFRASTRUCTURE

Protect / Detect / Respond Mapping Values for Non-Materiel

- **N/A** – No part of the non-materiel capability has been identified that could mitigate the threat action.
- **Applicable** – The non-materiel capability could be implemented to provide some level of mitigation of the threat action.

FedRAMP to Threat Relationship Example

Threat: Connection of Rogue Network Devices

The insertion and/or use of existing rogue interfaces to authorized network devices (e.g. extra network interface cards (NICs), embedded infrared, Bluetooth, Wi-Fi, or cellular modems)

Control: AC-4 Information Flow Enforcement | Physical / Logical Separation of Information Flows

The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

Relationship: Protection

Assumes organization-defined policy **covers network devices** and organization-defined separations **prevent rogue network devices from communicating** if connected to virtual machine.

- Mapping Requires Assumptions and Interpretations of the Controls and Possible Implementations

CISA
CYBER+INFRASTRUCTURE

Scoring Assumptions

- Assumptions frame and focus scoring and analysis.
- Assumptions are sorted into one of the following groups:
  - Data Center Architecture, Data Center Capability, Threat Framework, Threat Heat Map, Analysis, Non-Material Capability Mapping
- Examples:
  - Capabilities that achieve any level of mitigation with respect to Protect, Detect, or Respond are given at least a score of Limited.
  - For this spin, the asset being protected in Figure 3 is the Agency Server in the Data Center (a physical server; virtualization is not used – virtualized Data Centers are covered by the Spin 3 IaaS analysis)
  - It is assumed that technical controls are in place to constrain administrator interaction with the internet (e.g. no recreational use or office automation tasks). As such, 9 threat actions were scored "N/A".

ANALYSIS OVERVIEW

Laurie

CISA
CYBER+INFRASTRUCTURE

How Analysis Uses Capability Scores

- Understand Threat coverage:
  - What is the net effect of moving from a government or contractor-owned/operated environment to the cloud?
  - What is the net effect of all capabilities combined?
  - What is the difference between capabilities at network boundaries and the endpoint?
  - What are the effects of the individual layers in the architecture?
  - What is the effect of the planned future upgrades?
  - Where are the gaps in the comprehensive view?
- Comparison of capability sets
- Future: Cost vs. threat coverage

CISA
CYBER+INFRASTRUCTURE

PDR Analysis: Capability Sets

TIC	Current Internet to Data Center w/o B&I	Current Agency to Data Center w/o B&I	Current Intra-Data Center Zone w/o B&I	Current Agency Data Center Enclave & Server w/o B&I	Current Agency Server w/o B&I	Planned Internet to Data Center w/o B&I	Planned Agency to Data Center w/o B&I	Planned Intra-Data Center Zone w/o B&I	Planned Agency Data Center Enclave & Server w/o B&I	Planned Agency Server w/o B&I
DC:Firewall current TICAP	✓									
DC:Firewall Enhancements TICAP						✓				
DC:Passive Sensor	✓					✓				
Data Center Boundary										
DC:IP Blacklist	✓	✓				✓	✓			
DC:DDoS Mitigation	✓	✓				✓	✓			
DC:ACLs	✓	✓				✓	✓			
Data Center Zone Boundary										
DC:Next GenFirewall w/o B&I	✓	✓	✓			✓	✓	✓		
DC:Passive Sensor	✓	✓				✓	✓			
DC:DLP in Motion w/ B&I	✓	✓				✓	✓			
DC:WAF/RWP w/ B&I	✓	✓								
DC:WAF/RWP w/ [illegible] Enhancements						✓	✓			
DC:ID Federation/RBAC/MFA	✓	✓				✓	✓			
DC:DBFW w/B&I			✓					✓		
DC:DBAM w/B&I			✓					✓		
Data Center Enclave										
DC:Anomalous Net Behavior Detection (future)						✓	✓	✓	✓	
DC:Network Segmentation	✓	✓	✓	✓		✓	✓	✓	✓	
DC:Network Access Control (NAC)	✓	✓	✓	✓						
DC:NAC Enhancements Combined						✓	✓	✓	✓	
Agency Server										
DC:Device Control (CSM)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DC:File Integrity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DC:Device Health Check	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DC:Device Health Check Remediation	✓	✓	✓	✓	✓					
DC:Auto Dev Health Check Remed (Future)						✓	✓	✓	✓	✓
DC:Reputation (future)						✓	✓	✓	✓	✓
DC:Whitelisting (SWAM)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DC:Host IPS/FW	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

- Enables comparison of threat coverage changes between sets and evaluation of threat coverage on a data flow
  - "Current" and "Planned", with and without B&I
- Create new sets as needed using previously defined capabilities or new capabilities

TIC	Current Internet to Data Center w/o B&I	Current Agency to Data Center w/o B&I	Current Intra-Data Center Zone w/o B&I	Current Agency Data Center Enclave & Server w/o B&I	Current Agency Server w/o B&I	Planned Internet to Data Center w/o B&I	Planned Agency to Data Center w/o B&I	Planned Intra-Data Center Zone w/o B&I	Planned Agency Data Center Enclave & Server w/o B&I	Planned Agency Server w/o B&I
DC:Firewall current TICAP	✓									
DC:Firewall Enhancements TICAP						✓				
DC:Passive Sensor	✓					✓				
Data Center Boundary										
DC:IP Blacklist	✓	✓				✓	✓			
DC:DDoS Mitigation	✓	✓				✓	✓			
DC:ACLs	✓	✓				✓	✓			
Data Center Zone Boundary										
DC:Next GenFirewall w/o B&I	✓	✓	✓			✓	✓	✓		
DC:Passive Sensor	✓	✓				✓	✓			
DC:DLP in Motion w/ B&I	✓	✓				✓	✓			
DC:WAF/RWP w/ B&I	✓	✓								

CISA
CYBER+INFRASTRUCTURE

PDR Score Roll-Up Calculation

.govCAR Mitigation Draft Scoring Sheet		Stage					
		Objective					
		Threat Action Y			Threat Action Z		
	Capabilities	Protect	Detect	Respond	Protect	Detect	Respond
		Threat Action Description			Threat Action Description		
Set	Layer 1						
1	A	L	N/A	L	M	None	M
1	B	L	None	L	L	None	L
	Layer 2						
1	C	L	None	S	S	L	S
1	D	N/A	N/A	N/A	N/A	N/A	N/A
1	E	None	None	M	None	None	M
All Capabilities Set 1		L	None	S	S	L	S
P/D/R RollUp		S			S		

Maximum score for Protect is Limited (L)

Maximum score for Protect, Detect and Respond is Significant (S)

CISA
CYBER+INFRASTRUCTURE

PDR Analysis: Aggregating the Scores - Threat Coverage Roll-Up

Title of set and list of PDR functions

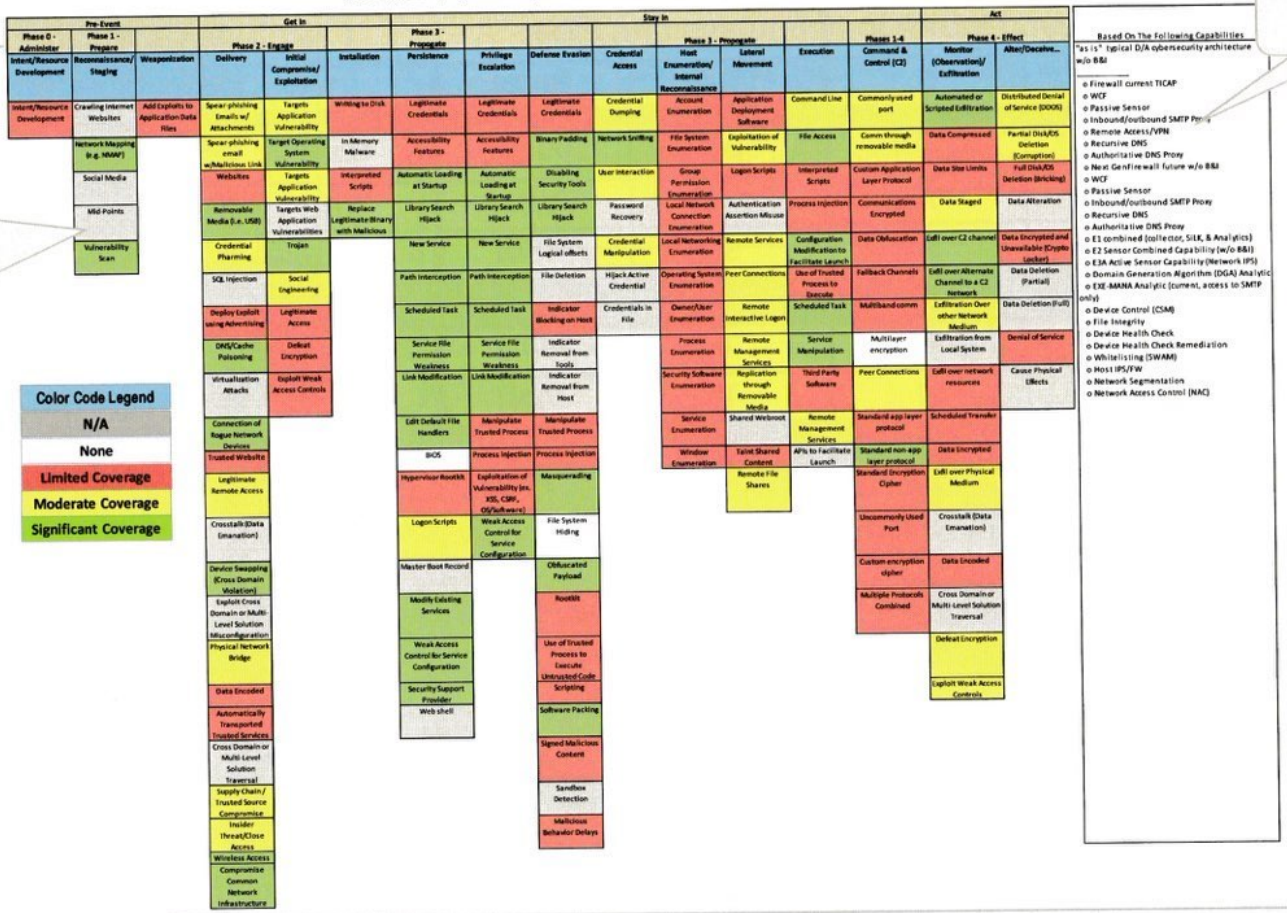
Threat Objective from the Framework

Threat Actions from the Framework.

Color is from Legend and indicates highest level of PDR coverage across all capabilities in the set.

Capabilities in the set

"as is" typical D/A cybersecurity architecture w/o B&I Coverage For: Protect, Detect, & Respond



Color Code Legend

- N/A
- None
- Limited Coverage
- Moderate Coverage
- Significant Coverage

Illustrates highest level of PDR coverage across all capabilities in the set.

Goal is not to turn it all green, but to identify opportunities for improvement.

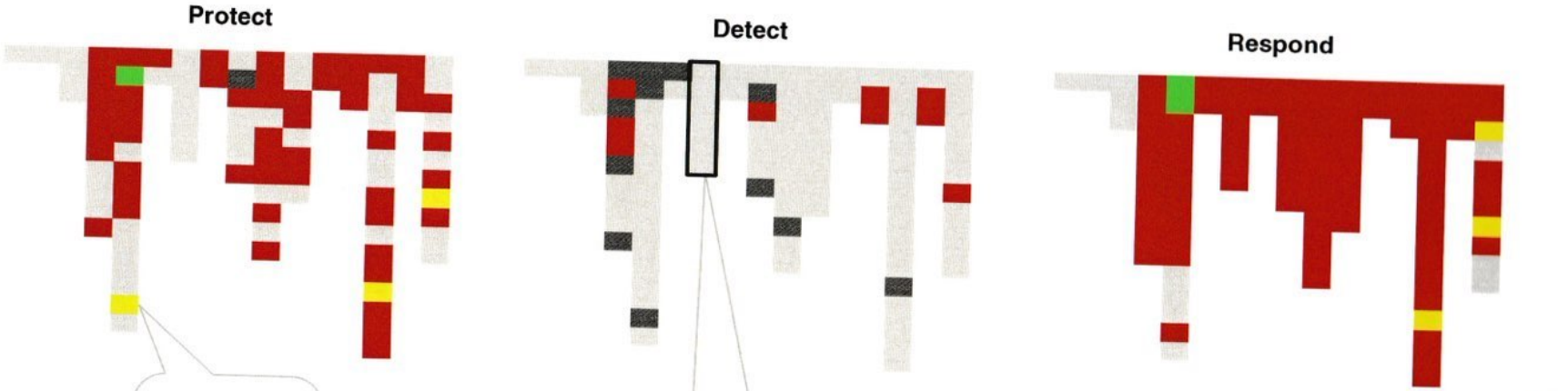
Mitigation by Protect, Detect and Respond

CSF Function

Title of set

(FOUO)

Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I



(FOUO)

Threat Actions from the Framework.

Color is from Legend and indicates highest level of PDR coverage across all capabilities in the set.

Each column represents one Threat Objective from the Framework

N/A
None
Limited
Moderate
Significant

CISA
CYBER+INFRASTRUCTURE

Resilience in Maximum Mitigation

No Coverage | Unique | Increasing Depth

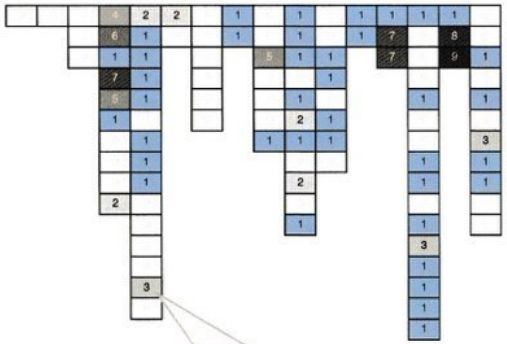
CSF Function

Title of set

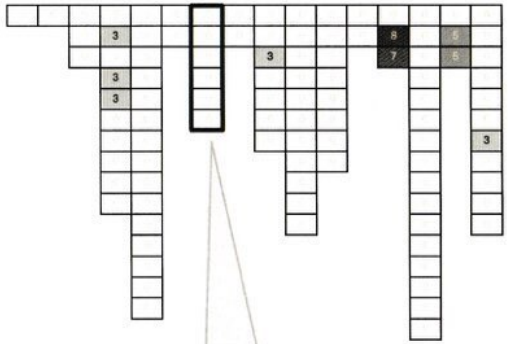
(FOUO)

Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I

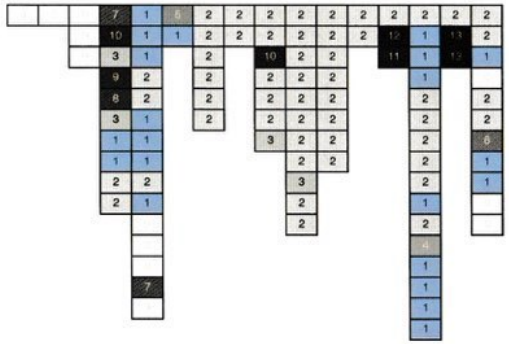
Depth - Protect



Depth - Detect



Depth - Respond



(FOUO)

Threat Actions from the Framework.

Color is from Legend and indicates amount of resilience in Protect, Detect or Respond coverage across all capabilities in the set.

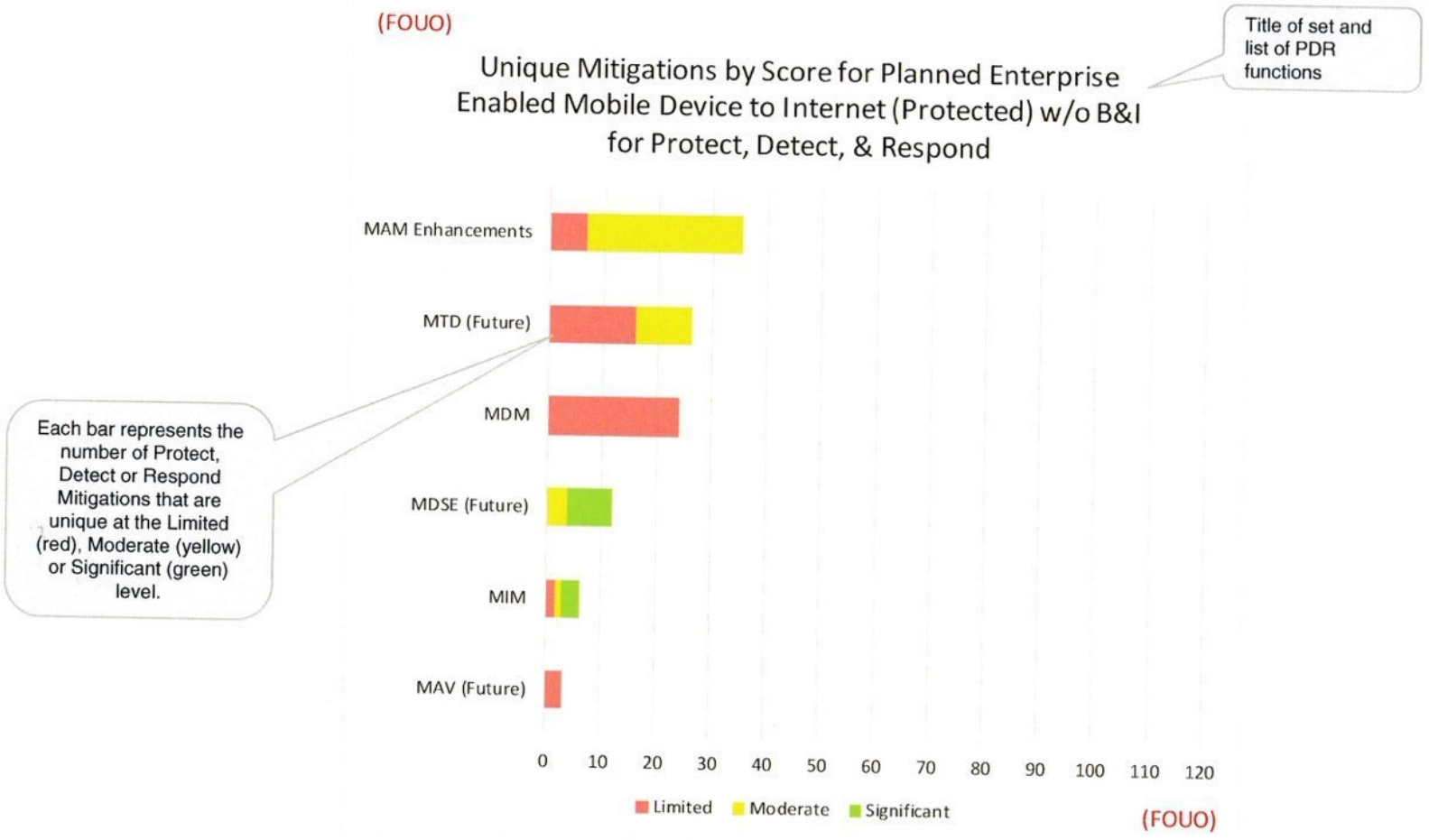
In this case, there are 3 capabilities which provide the maximum score.

Each column represents one Threat Objective from the Framework

CISA
CYBER+INFRASTRUCTURE

Unique Bar Chart

(FOUO)

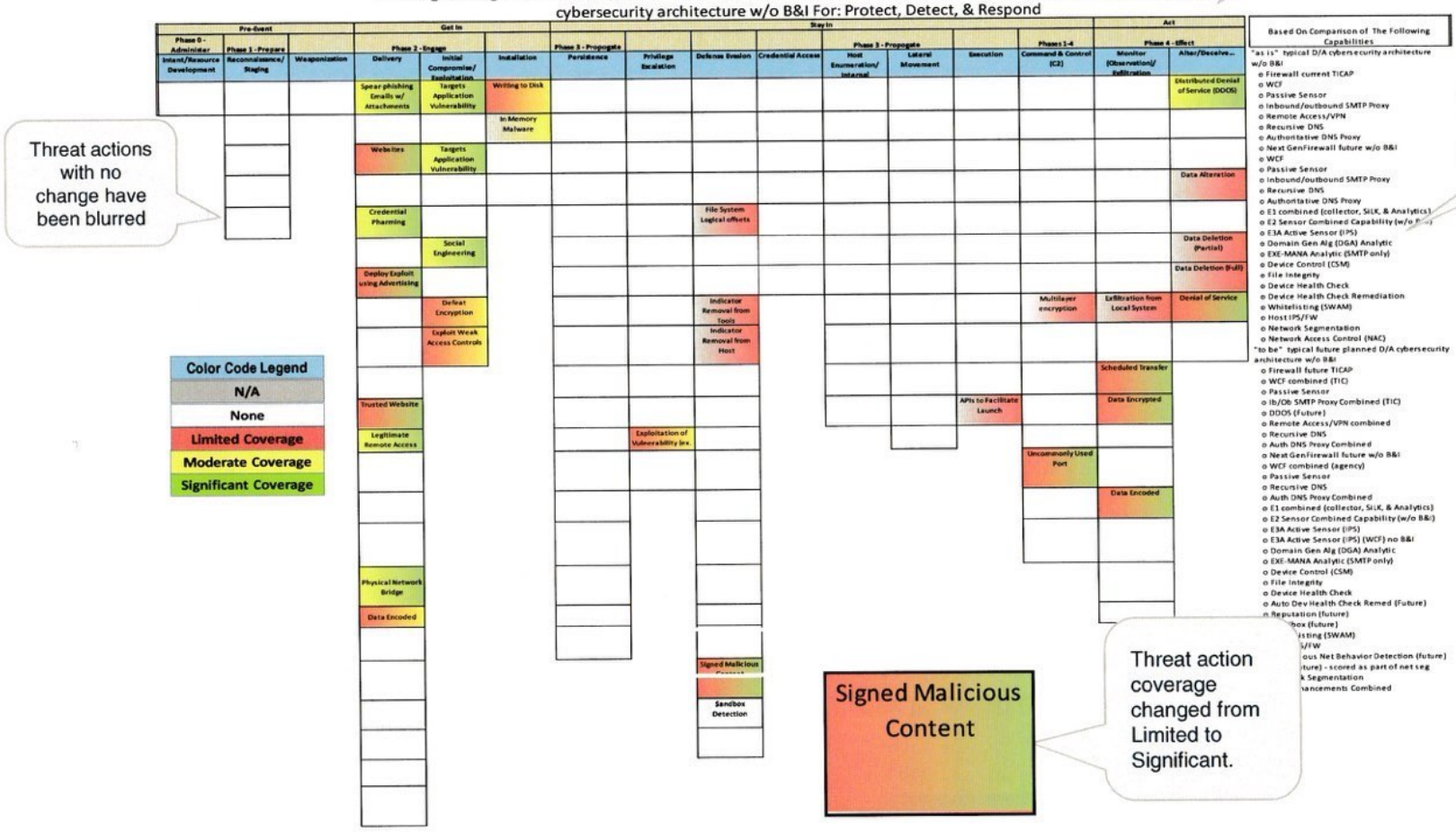


CISA
CYBER+INFRASTRUCTURE

PDR Analysis: Comparing Sets with Coverage Map

Capability sets being compared with PDR functions listed

Coverage Change from "as is" typical D/A cybersecurity architecture w/o B&I to "to be" typical future planned D/A cybersecurity architecture w/o B&I For: Protect, Detect, & Respond

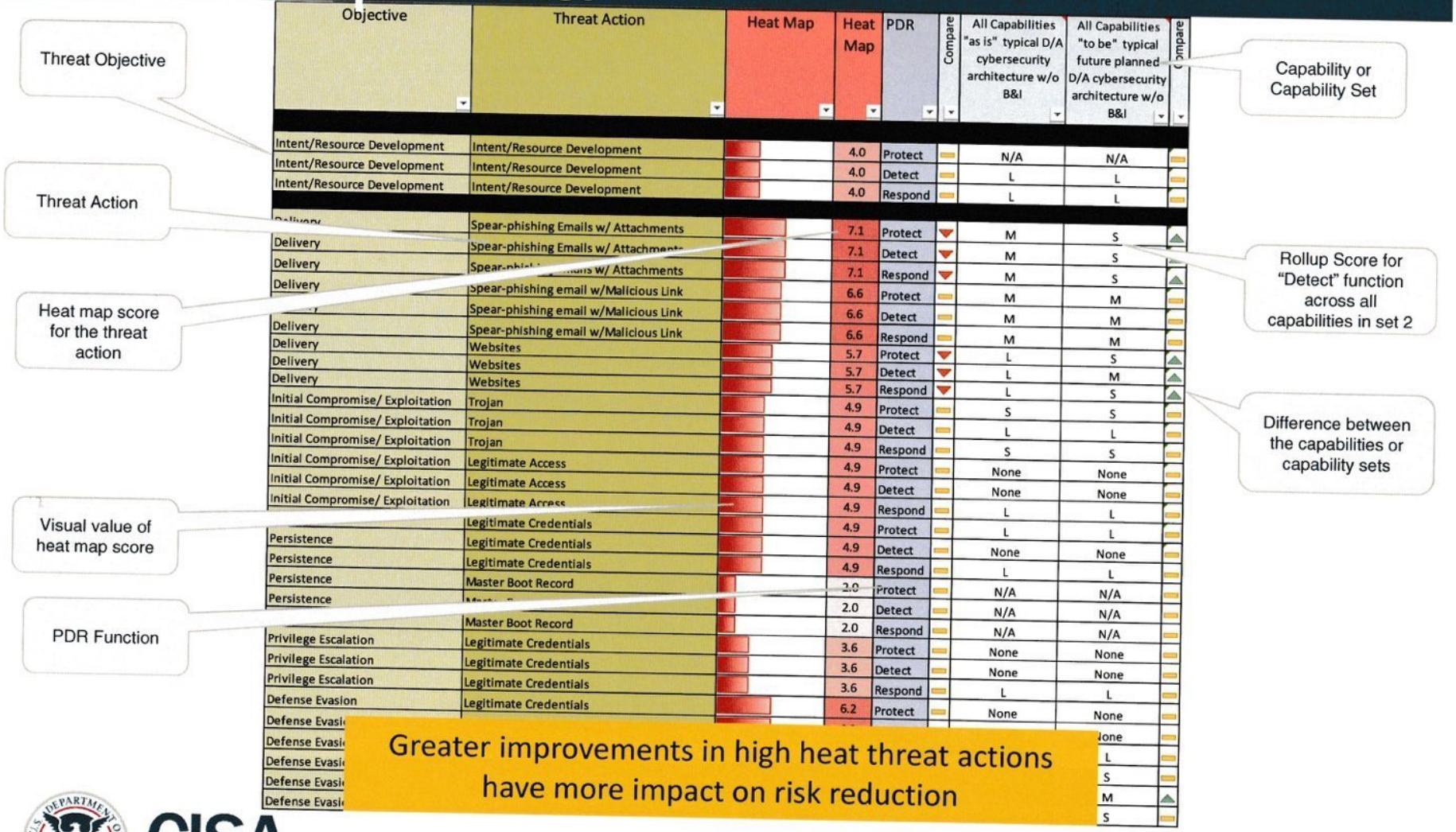


Threat actions with no change have been blurred

Capabilities in the sets

Threat action coverage changed from Limited to Significant.

PDR Analysis: Incorporating Threat Heat Map Data



Objective	Threat Action	Heat Map	Heat Map	PDR	Compare	All Capabilities "as is" typical D/A cybersecurity architecture w/o B&I	All Capabilities "to be" typical future planned D/A cybersecurity architecture w/o B&I	Compare
Intent/Resource Development	Intent/Resource Development		4.0	Protect		N/A	N/A	
Intent/Resource Development	Intent/Resource Development		4.0	Detect		L	L	
Intent/Resource Development	Intent/Resource Development		4.0	Respond		L	L	
	Spear-phishing Emails w/ Attachments		7.1	Protect		M	S	
Delivery	Spear-phishing Emails w/ Attachments		7.1	Detect		M	S	
Delivery	Spear-phishing Emails w/ Attachments		7.1	Respond		M	S	
Delivery	Spear-phishing email w/Malicious Link		6.6	Protect		M	M	
	Spear-phishing email w/Malicious Link		6.6	Detect		M	M	
Delivery	Spear-phishing email w/Malicious Link		6.6	Respond		M	M	
Delivery	Websites		5.7	Protect		L	S	
Delivery	Websites		5.7	Detect		L	M	
Delivery	Websites		5.7	Respond		L	S	
Initial Compromise/ Exploitation	Trojan		4.9	Protect		S	S	
Initial Compromise/ Exploitation	Trojan		4.9	Detect		L	L	
Initial Compromise/ Exploitation	Trojan		4.9	Respond		S	S	
Initial Compromise/ Exploitation	Legitimate Access		4.9	Protect		None	None	
Initial Compromise/ Exploitation	Legitimate Access		4.9	Detect		None	None	
Initial Compromise/ Exploitation	Legitimate Access		4.9	Respond		L	L	
	Legitimate Credentials		4.9	Protect		L	L	
Persistence	Legitimate Credentials		4.9	Detect		None	None	
Persistence	Legitimate Credentials		4.9	Respond		L	L	
Persistence	Master Boot Record		2.0	Protect		N/A	N/A	
Persistence			2.0	Detect		N/A	N/A	
	Master Boot Record		2.0	Respond		N/A	N/A	
Privilege Escalation	Legitimate Credentials		3.6	Protect		None	None	
Privilege Escalation	Legitimate Credentials		3.6	Detect		None	None	
Privilege Escalation	Legitimate Credentials		3.6	Respond		L	L	
Defense Evasion	Legitimate Credentials		6.2	Protect		None	None	
Defense Evasi							None	
Defense Evasi							L	
Defense Evasi							S	
Defense Evasi							M	
Defense Evasi							S	

Greater improvements in high heat threat actions have more impact on risk reduction

CISA
CYBER+INFRASTRUCTURE

PDR Analysis: Top Threat Actions

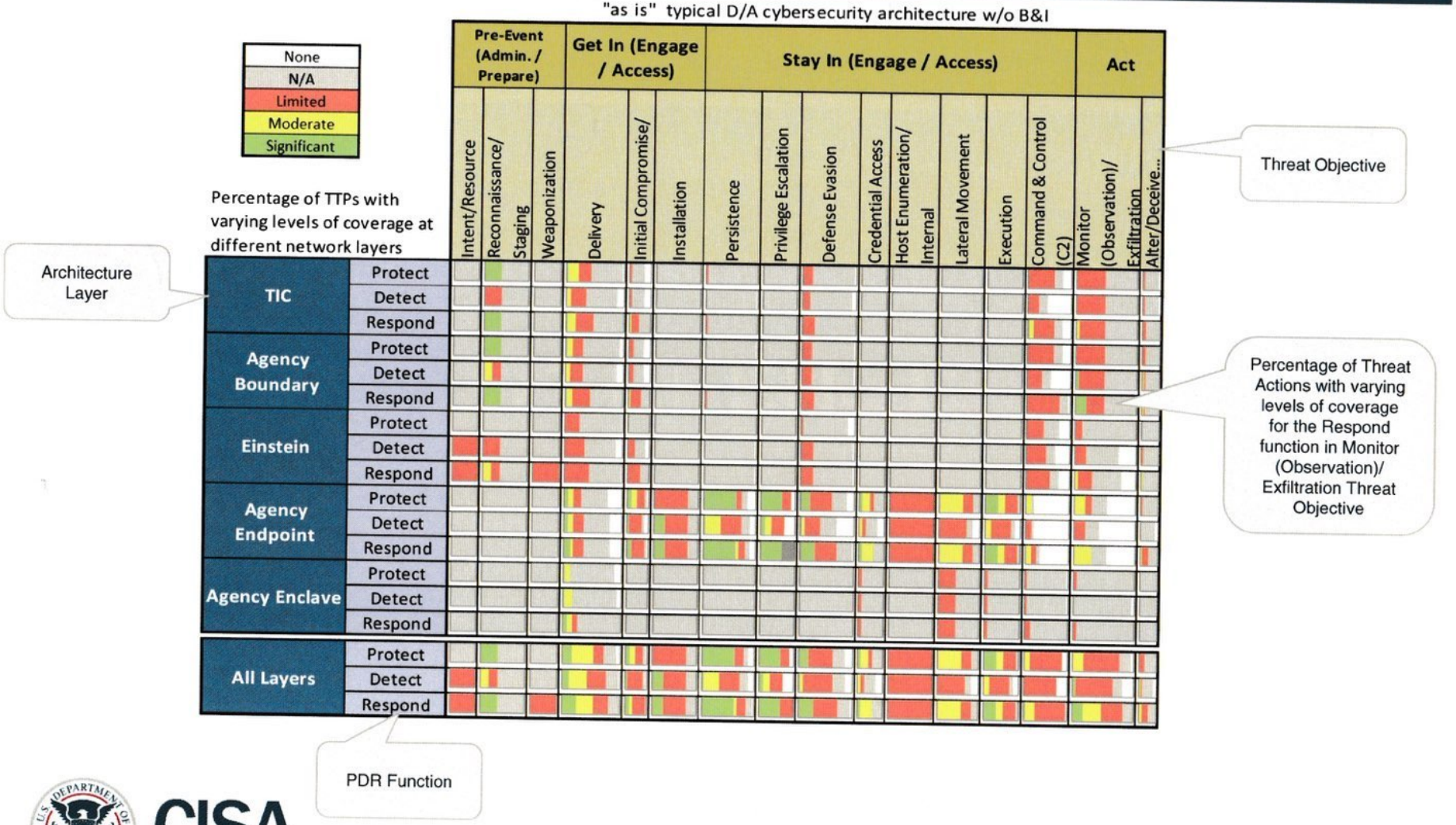
(FOUO)

Objective	Threat Action	Heat Map	Capability 1 All Capabilities Current Internet to Data Center	Capability 2 All Capabilities Planned Internet to Data Center w/o B&I	
Credential Access	Credential Dumping	11.6	M	M	
Credential Access	Password Recovery	9.0	N/A	N/A	
Host Enumeration/ Internal Reconnaissance	File System Enumeration	8.9	L	L	
Command & Control (C2)	Commonly used port	8.5	S	S	
Host Enumeration/ Internal Reconnaissance	Process Enumeration	8.4	L	L	
Installation	Writing to Disk	7.7	L	L	
Host Enumeration/ Internal Reconnaissance	Account Enumeration	7.3	L	L	
Initial Compromise/ Exploitation	Targets Application Vulnerability	7.3	L	L	
Defense Evasion	Masquerading	7.2	S	S	Respond Only
Weaponization	Add Exploits to Application Data Files	7.0	N/A	L	Rep & WAF/RWP Enh
Command & Control (C2)	Standard app layer protocol	7.0	M	M	
Execution	Command Line	6.9	M	M	
Host Enumeration/ Internal Reconnaissance	Operating System Enumeration	6.8	L	L	
Defense Evasion	Legitimate Credentials	6.7	L	L	
Defense Evasion	Obfuscated Payload	6.7	S	S	
Initial Compromise/ Exploitation	Trojan	6.7	S	S	
Persistence	Legitimate Credentials	6.4	S	S	
Host Enumeration/ Internal Reconnaissance	Local Network Configuration Enumeration	6.3	L	L	
Host Enumeration/ Internal Reconnaissance	Local Network Enumeration	6.3	M	M	
Delivery	Web Application Exploit over the Network	6.0	S	S	
Intent/Resource Development	Intent/Resource Development	6.0	N/A	L	Rep & WAF/RWP Enh
Defense Evasion	Scripting	5.8	L	L	
Host Enumeration/ Internal Reconnaissance	Owner/User Enumeration	5.7	L	L	
Lateral Movement	Remote Interactive Logon	5.7	M	M	
Lateral Movement	Remote File Shares	5.7	L	M	Rep & Auto DHC-R
Command & Control (C2)	Communications Encrypted	5.5	M	M	
Reconnaissance/ Staging	Social Media	5.4	N/A	N/A	
Persistence	Automatic Loading at Startup	5.4	S	S	
Monitor (Observation)/ Exfiltration	Exfil over C2 channel	5.3	L	L	
Defense Evasion	File Deletion	5.3	N/A	N/A	
Privilege Escalation	Scheduled Task	5.1	S	S	
Initial Compromise/ Exploitation	Legitimate Access	5.0	S	S	
Command & Control (C2)	Data Obfuscation	5.0	M	M	
Command & Control (C2)	Fallback Channels	5.0	M	M	
Defense Evasion	Signed Malicious Content	4.8	S	S	
Reconnaissance/ Staging	Vulnerability Scan	4.8	S	S	
Privilege Escalation	Legitimate Credentials	4.6	L	L	
Privilege Escalation	Multi Tenant Side Channel Cache Attack	4.6	N/A	N/A	
Defense Evasion	Software Packing	4.3	S	S	
Execution	Scheduled Task	4.2	S	S	
Host Enumeration/ Internal Reconnaissance	Security Software Enumeration	4.2	L	L	

Sorted by Heat Map Value

CISA
CYBER+INFRASTRUCTURE

PDR Analysis: Impact of Layers



CISA
CYBER+INFRASTRUCTURE

Unclassified//For Official Use Only

LUNCH BREAK

Anyone leaving now see Branko before you leave.

CISA
CYBER+INFRASTRUCTURE

.GOVCAR HANDS-ON WORKSHOP

CISA
CYBER+INFRASTRUCTURE

Workshop Agenda

1:00 Capability Scoring for Protect/Detect/Respond

2:00 Analysis

2:45 *Break*

3:00 Continue Analysis

3:30 Breakouts: Architecture, Threat, Facilitating a scoring session

CISA
CYBER+INFRASTRUCTURE

Goals for the Workshop

- Scoring: Apply Rubric, Understand Capability and Threat pairing
- Analysis: Interpreting the analysis views; Lines of investigation; Creating Recommendations, Affirmations, Observations
- Break out Sessions:
  - Architecture: Architecture decomposition, Capabilities and capability decomposition, Datasets and Flows
  - Threat: Reading a threat report, Heatmap Generation
  - Facilitating a Scoring Session: Scoring Philosophy, Modified Delphi Method

CISA
CYBER+INFRASTRUCTURE

CAPABILITY SCORING FOR PROTECT/DETECT/RESPOND

Pete

CISA
CYBER+INFRASTRUCTURE

Practice Scoring

- Apply Rubric
- Understand Capability and Threat pairing
- Hands-on Practice

CISA
CYBER+INFRASTRUCTURE

PDR Scoring Rubric

Cybersecurity Framework Core Functions

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities (Not scored by this analysis)

Protect – Preventative measures with or without detection; near immediate effect

Detect – Passive; identifies use of a given action/technique, results in event data in cyber relevant time

Respond – Response after actions/techniques successful

- Can be detection
- Can be analysis
- Can be changing configuration

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capability or services that were impaired due to a cybersecurity event. (Not scored in this analysis.)

Scoring Values

N/A – The capability does not have access to artifacts associated with the threat action

None – The capability has access to the artifacts associated with the threat action but it provides no mitigation coverage

Limited (L) – The capability provides a small amount of coverage to the given threat action. This includes cases where

- A capability can mitigate an action, but only for a small subset of the possible "delivery" methods for that action; the PDR score will be reduced to reflect the pro-rated contribution for total mitigation of the action.
- Coverage is unreliable
- Protection/Detection relies on exact foreknowledge of adversary tools, protocols or infrastructure (e.g., adversary IP address space or domain names)

Moderate (M) – The capability provides modest coverage on the action. It includes cases where coverage is relatively reliable but not complete, and mostly not dependent on exact foreknowledge (e.g., behavior-based).

Significant (S) – The capability provides robust coverage. Coverage is very reliable, almost complete, and not dependent on foreknowledge.

CISA
CYBER+INFRASTRUCTURE

NextGen Firewall

Feature	Description
GeoIP Blocking source/dest IP	The source/destination IP address is checked against a vendor supplied GeoIP database and is filtered according to rules in the Firewall/IPS. Supports custom IP assignment into GeoIP groups.
Application Filtering	Deep Packet Inspection is used to identify the application (e.g., Skype) being used in a session and supports filtering by application. Supports custom application identification. Supports blocking functions w/in applications (e.g., file transfer w/in instant messaging).
Protocol Port Enforcement	Using Application Identification, enforces that ports are only being used for the intended application.
A/V	Signature-based anti-malware
IPS	Signature based blocking of malicious traffic
Rate Limiting/QoS	Up to NN different rate limiting/QoS policies can be applied based on packet DSCP.
Custom Traffic Filtering	Filtering rules can use IP address, BGP ASN, VLAN, DSCP tag to apply rulesets.
File Reputation Check	File hash is checked against vendor supplied file reputation databases. Custom hashes/reputation can be added. Known bad files are blocked.
File Type Filtering	The file type is identified and used in filtering rules.
DLP (limited)	Data Loss Prevention is performed via pattern-based (e.g. REGEX) content in applications and files.

CISA
CYBER+INFRASTRUCTURE

File Integrity & Application Whitelisting

Capability	Description
File Integrity	Performs File Integrity Checking by performing a checksum analysis to establish a baseline for each file and generates events associated with deltas. Performed against a subset of security-relevant files (not all files)
Application Whitelisting	Monitors SW inventory to identify known "good" applications. Denies all, and allows only specified applications. Protection is limited since some high-risk applications must be allowed.

CISA
CYBER+INFRASTRUCTURE

ANALYSIS

Laurie

CISA
CYBER+INFRASTRUCTURE

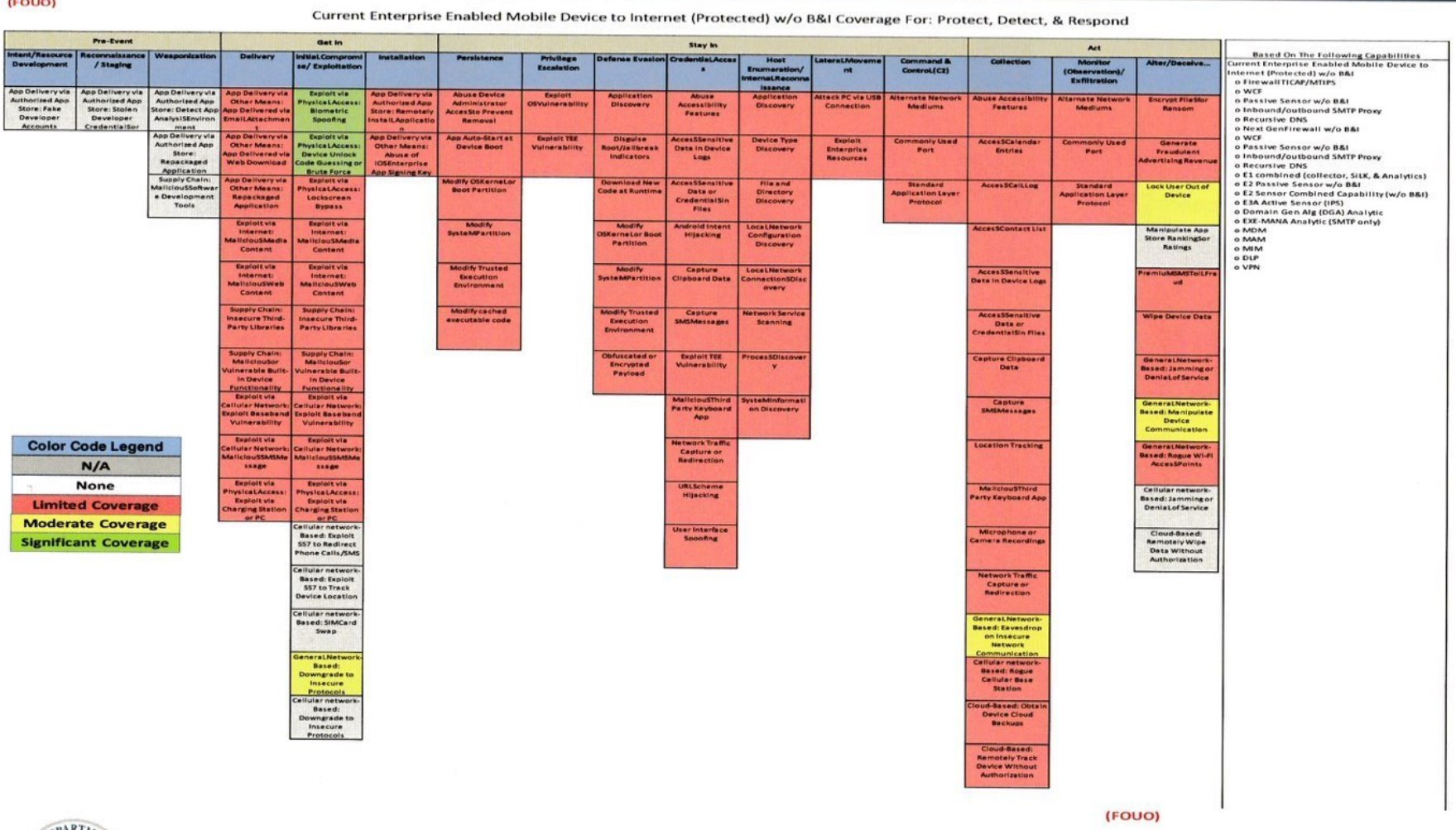
Analysis

- Interpreting the analysis views
- Lines of investigation
- Creating Recommendations, Affirmations, Observations

CISA
CYBER+INFRASTRUCTURE

Current Enterprise-Enabled Mobile Device to Internet (Protected)

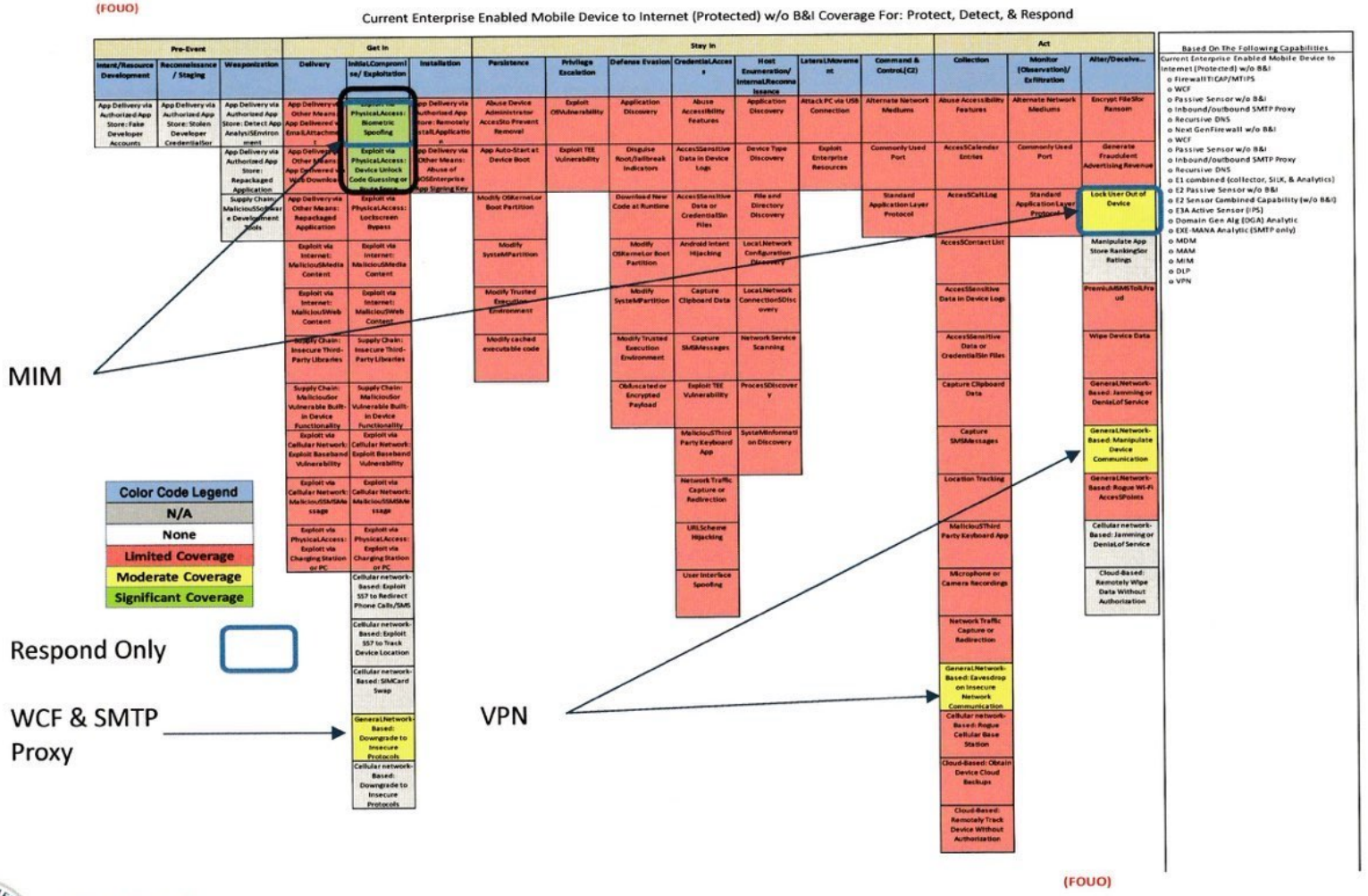
(FOUO)



(FOUO)

CISA
CYBER+INFRASTRUCTURE

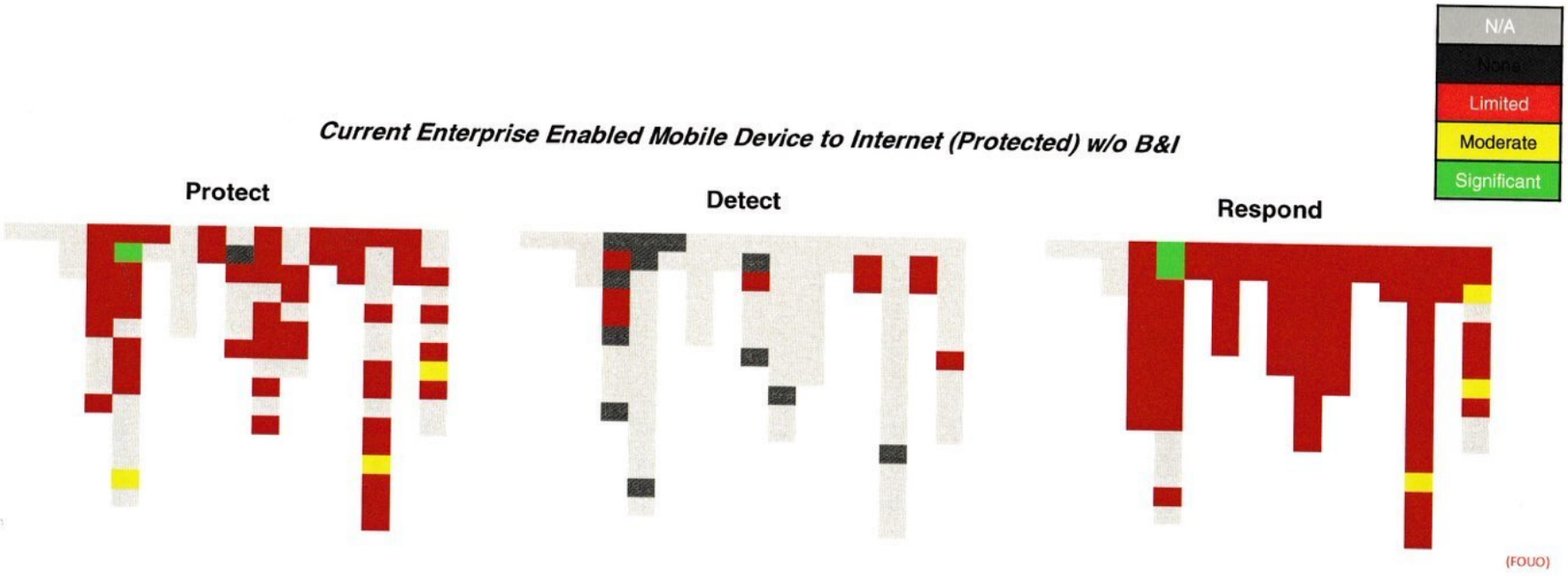
Current Enterprise-Enabled Mobile Device to Internet (Protected)



Mitigation by Protect, Detect, Respond for Current Enterpris-Enabled Mobile Device to Internet (Protected)

(FOUO)

Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I



(FOUO)

CISA
CYBER+INFRASTRUCTURE

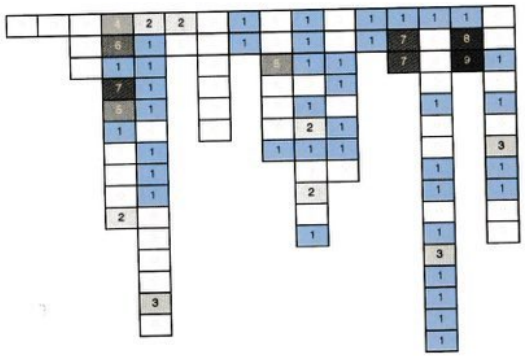
Resilience in Maximum Mitigation Current Enterpris- Enabled Mobile Device to Internet (Protected)

No Coverage | Unique | Increasing Depth

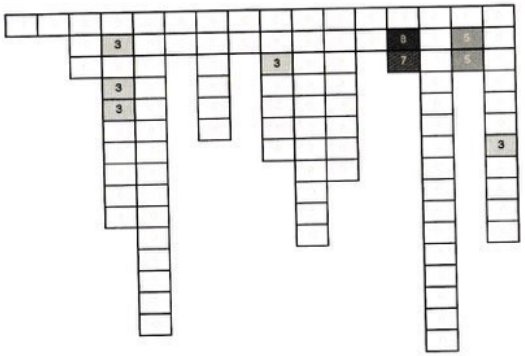
(FOUO)

Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I

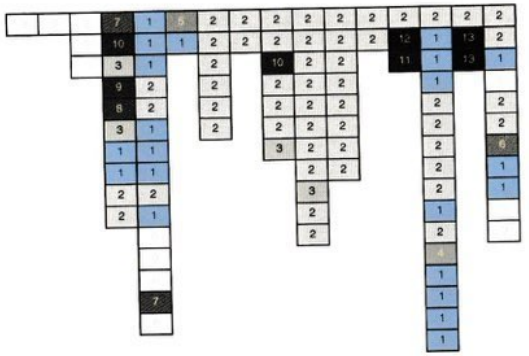
Depth - Protect



Depth - Detect



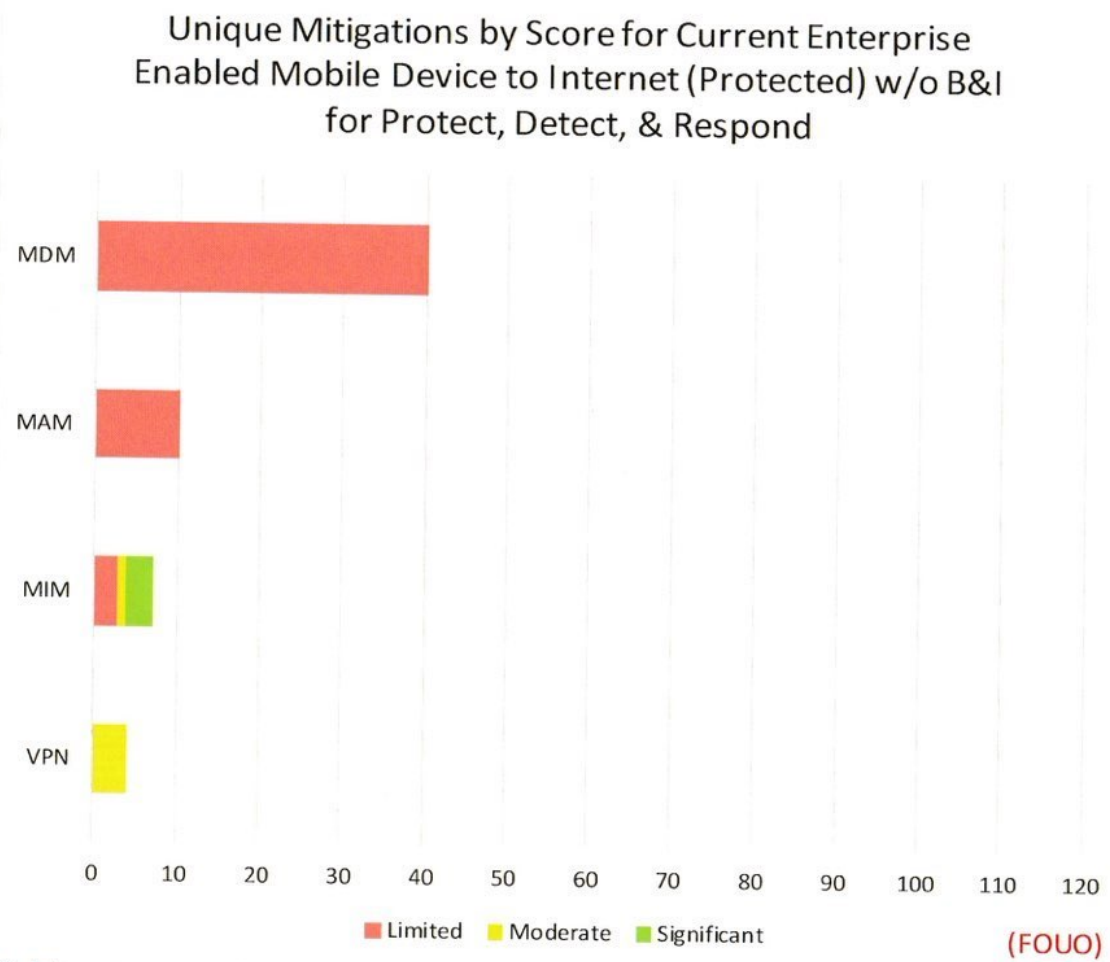
Depth - Respond



(FOUO)

Unique Mitigations for Current Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

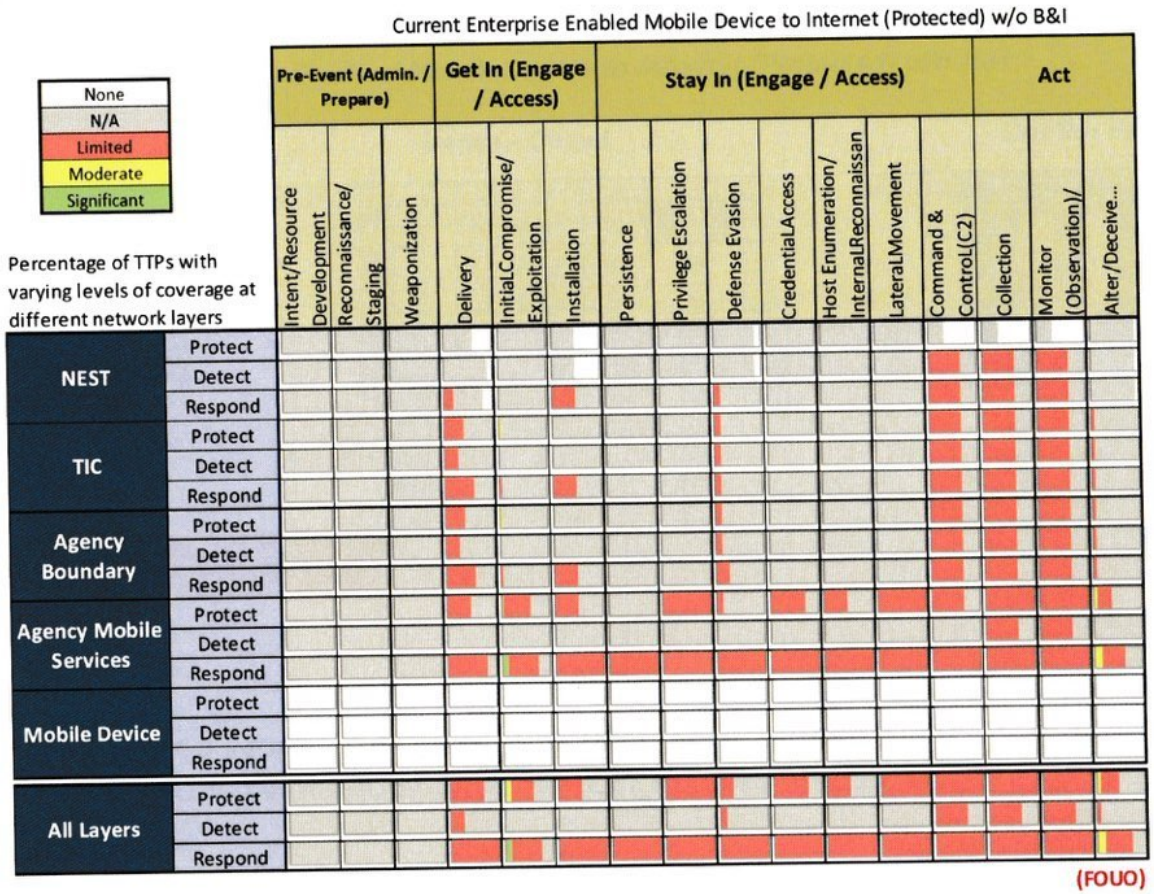


(FOUO)

CISA
CYBER+INFRASTRUCTURE

Layer Coverage for Current Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

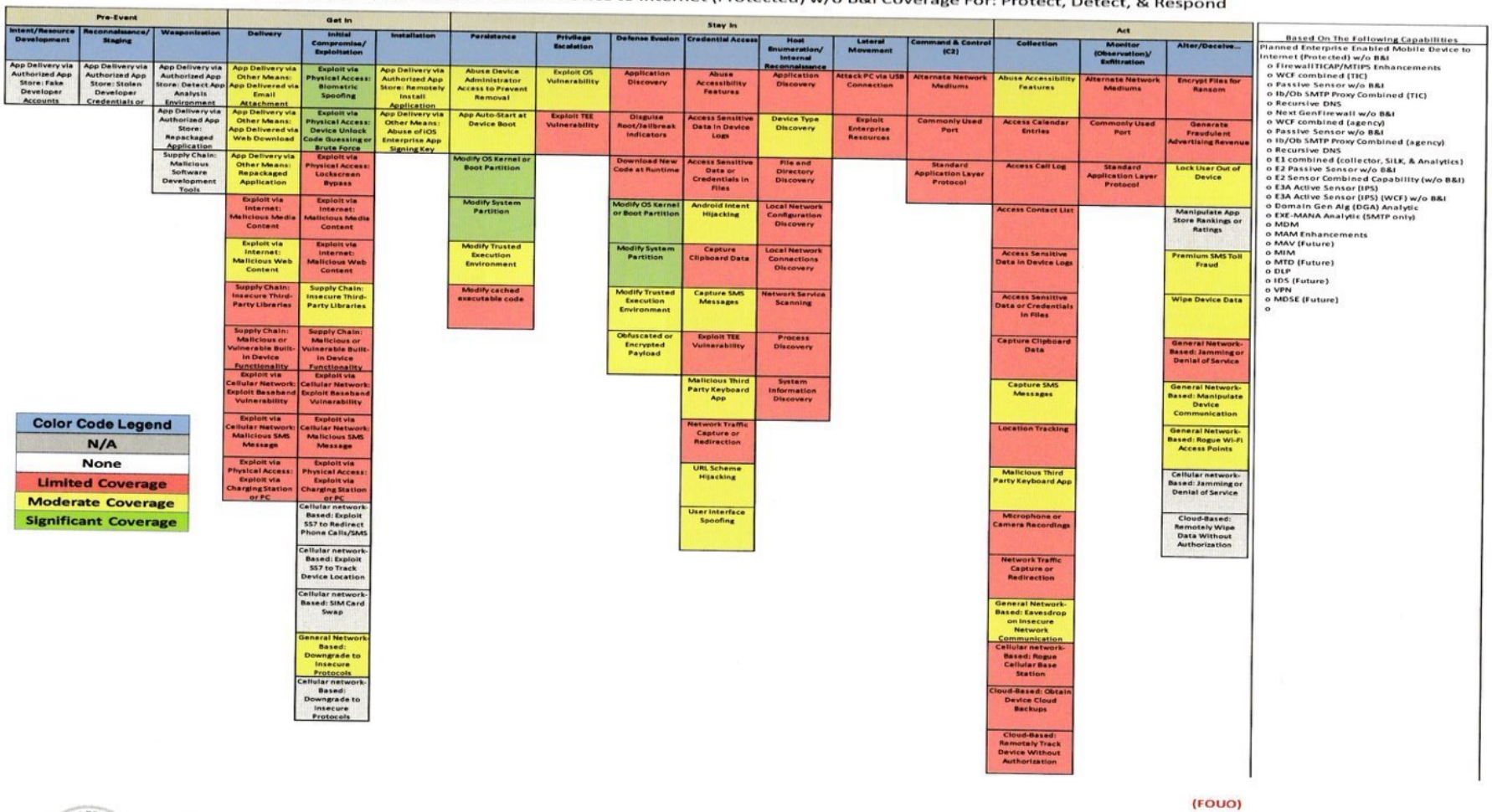


(FOUO)

Planned Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I Coverage For: Protect, Detect, & Respond



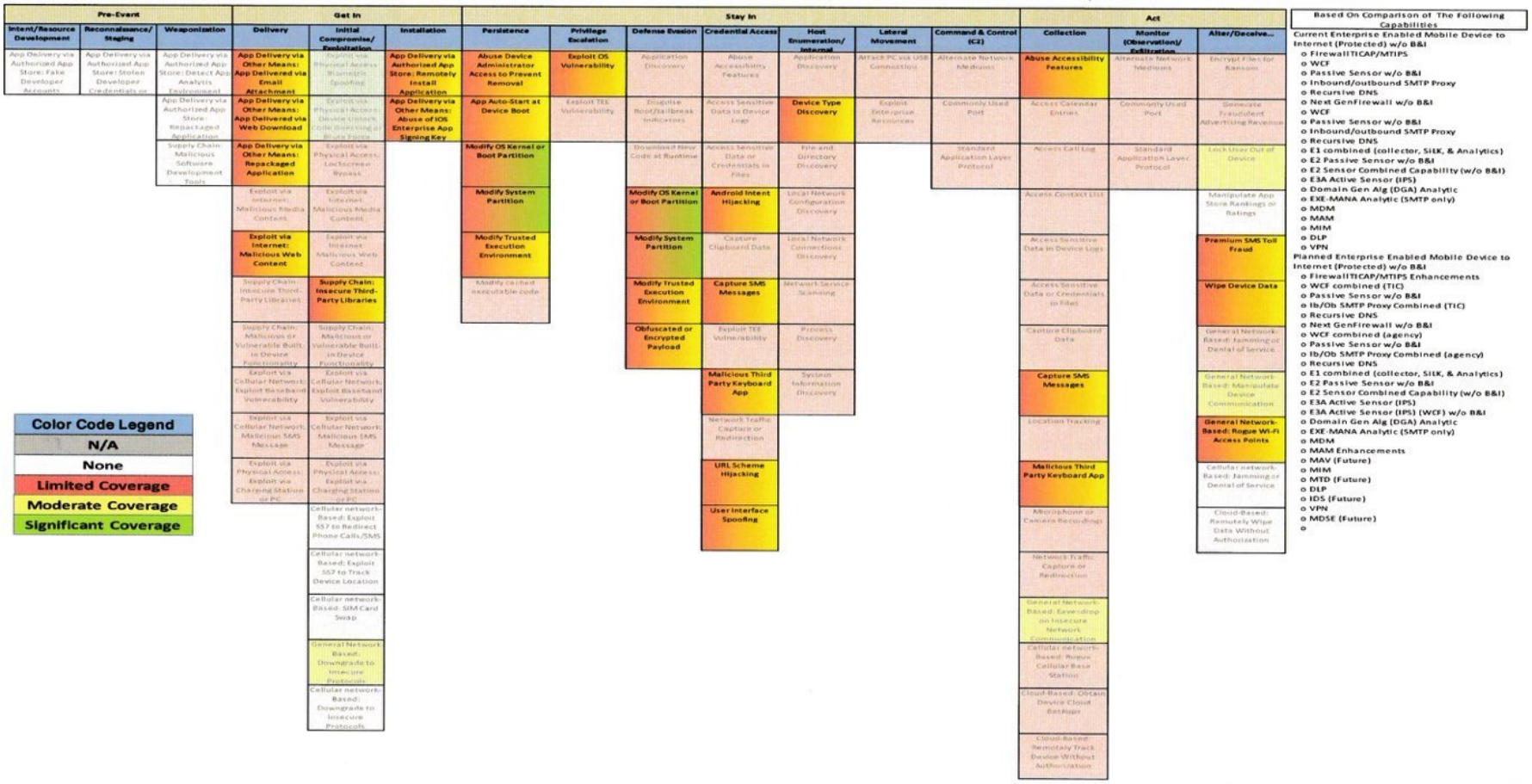
(FOUO)

CISA
CYBER+INFRASTRUCTURE

Coverage Change Current to Planned Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

Coverage Change from Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I to Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I For: Protect, Detect, & Respond



Based On Comparison of The Following Capabilities

Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I
- o FirewallTICAP/MTIPS
- o WCF
- o Passive Sensor w/o B&I
- o Inbound/outbound SMTP Proxy
- o Recursive DNS
- o Next GenFirewall w/o B&I
- o WCF
- o Passive Sensor w/o B&I
- o Inbound/outbound SMTP Proxy
- o Recursive DNS
- o E1 combined (collector, SiLK, & Analytics)
- o E2 Passive Sensor w/o B&I
- o E2 Sensor Combined Capability (w/o B&I)
- o E3A Active Sensor (IPS)
- o Domain Gen Alg (DGA) Analytic
- o EXE-MANA Analytic (SMTP only)
- o MDM
- o MAM
- o MIM
- o DLP
- o VPN

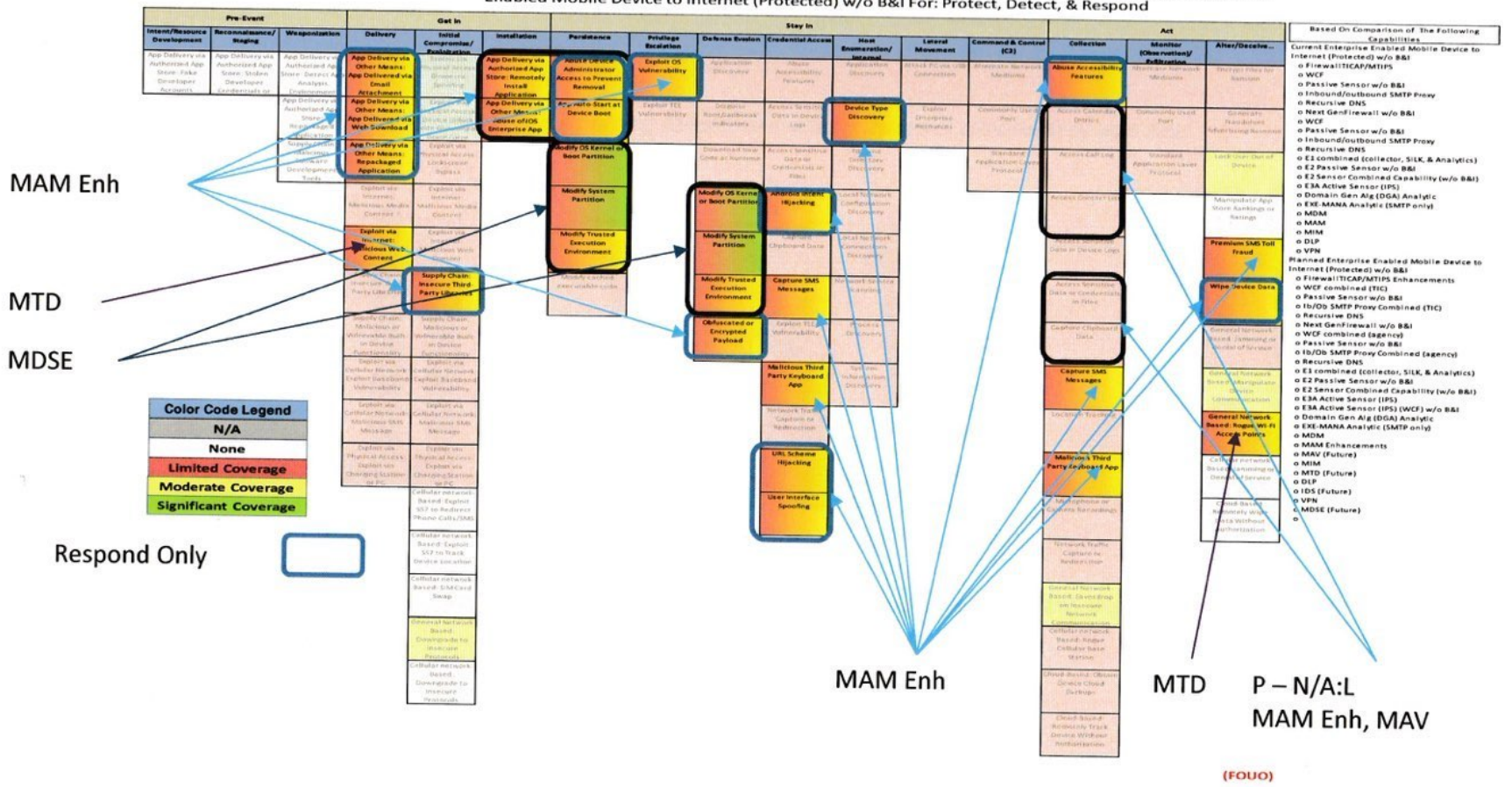
Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I
- o FirewallTICAP/MTIPS Enhancements
- o WCF combined (TIC)
- o Passive Sensor w/o B&I
- o Ib/Ob SMTP Proxy Combined (TIC)
- o Recursive DNS
- o Next GenFirewall w/o B&I
- o WCF combined (agency)
- o Passive Sensor w/o B&I
- o Ib/Ob SMTP Proxy Combined (agency)
- o Recursive DNS
- o E1 combined (collector, SiLK, & Analytics)
- o E2 Passive Sensor w/o B&I
- o E2 Sensor Combined Capability (w/o B&I)
- o E3A Active Sensor (IPS)
- o E3A Active Sensor (IPS) (WCF) w/o B&I
- o Domain Gen Alg (DGA) Analytic
- o EXE-MANA Analytic (SMTP only)
- o MDM
- o MAM Enhancements
- o MAV (Future)
- o MIM
- o MTD (Future)
- o DLP
- o IDS (Future)
- o VPN
- o MDSE (Future)
- o

(FOUO)

Coverage Change Current to Planned Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

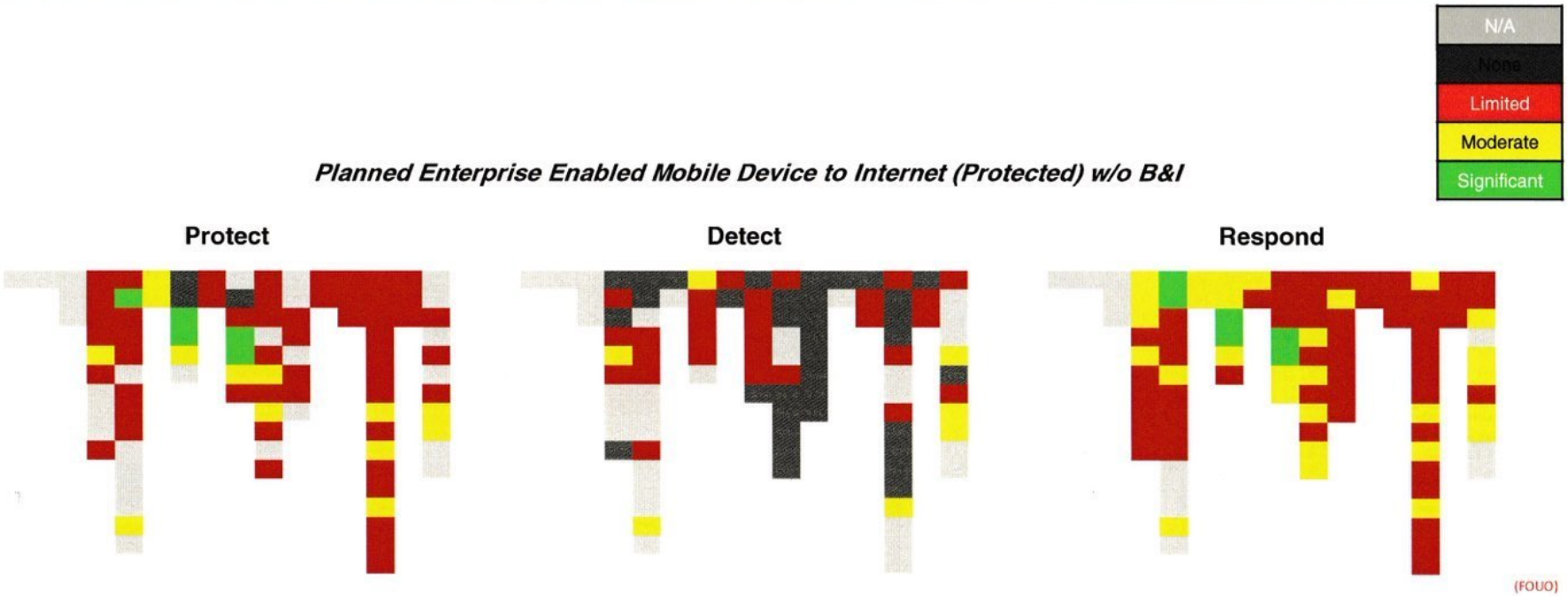
Coverage Change from Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I to Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I For: Protect, Detect, & Respond



Mitigation by Protect, Detect, Respond for Planned Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I



(FOUO)

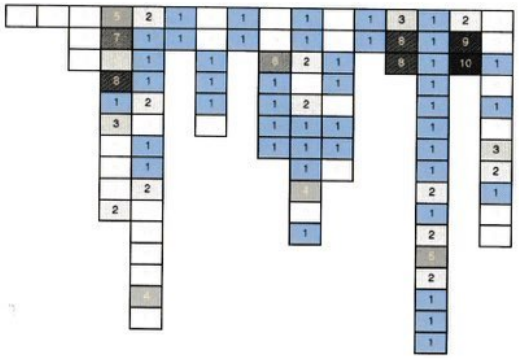
Resilience in Maximum Mitigation Planned Enterprise-Enabled Mobile Device to Internet (Protected)

No Coverage | Unique | Increasing Depth

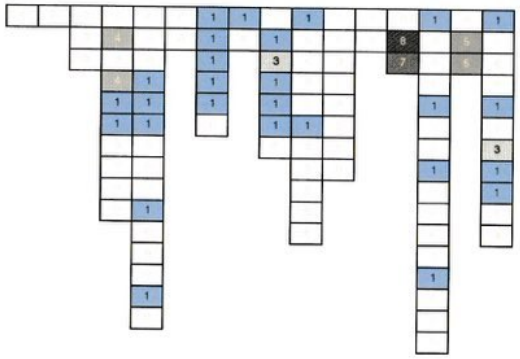
(FOUO)

Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I

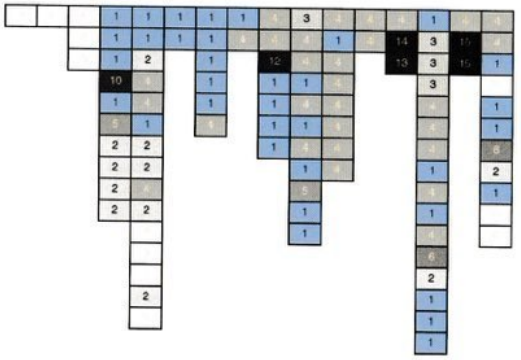
Depth - Protect



Depth - Detect



Depth - Respond

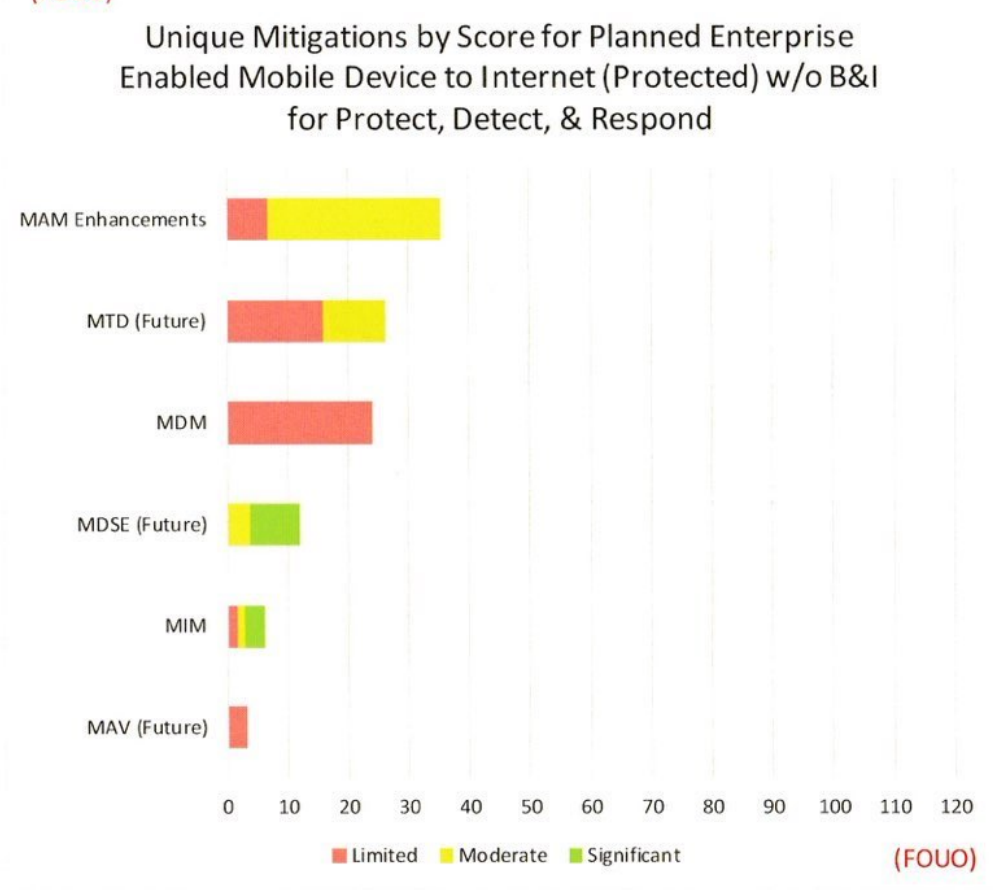


(FOUO)

CISA
CYBER+INFRASTRUCTURE

Unique Mitigations for Planned Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)



CISA CYBER+INFRASTRUCTURE

Percentage Difference by Layer: Current to Planned Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

Difference From Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I to Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I

Difference in Percentage of Adversary Tactics Covered (Significant, Moderate, or Limited) At Layers of the Network (Between Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I and Planned Enterprise		Pre-Event (Administer / Prepare)			Get In (Engage / Access)			Stay In (Engage / Access)							Act		
		Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	InitialCompromise/ Exploitation	Installation	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Host Enumeration/ InternalReconnaissan	LateralMovement	Command & ControL(C2)	Collection	Monitor (Observation)/	Alter/Deceive...
NEST	Protect																
	Detect																
	Respond																
TIC	Protect																
	Detect																
	Respond																
Agency Boundary	Protect																
	Detect																
	Respond																
Agency Mobile Services	Protect																
	Detect																
	Respond																
Mobile Device	Protect																
	Detect																
	Respond																
All Layers	Protect																
	Detect																
	Respond																

(FOUO)

CISA
CYBER+INFRASTRUCTURE

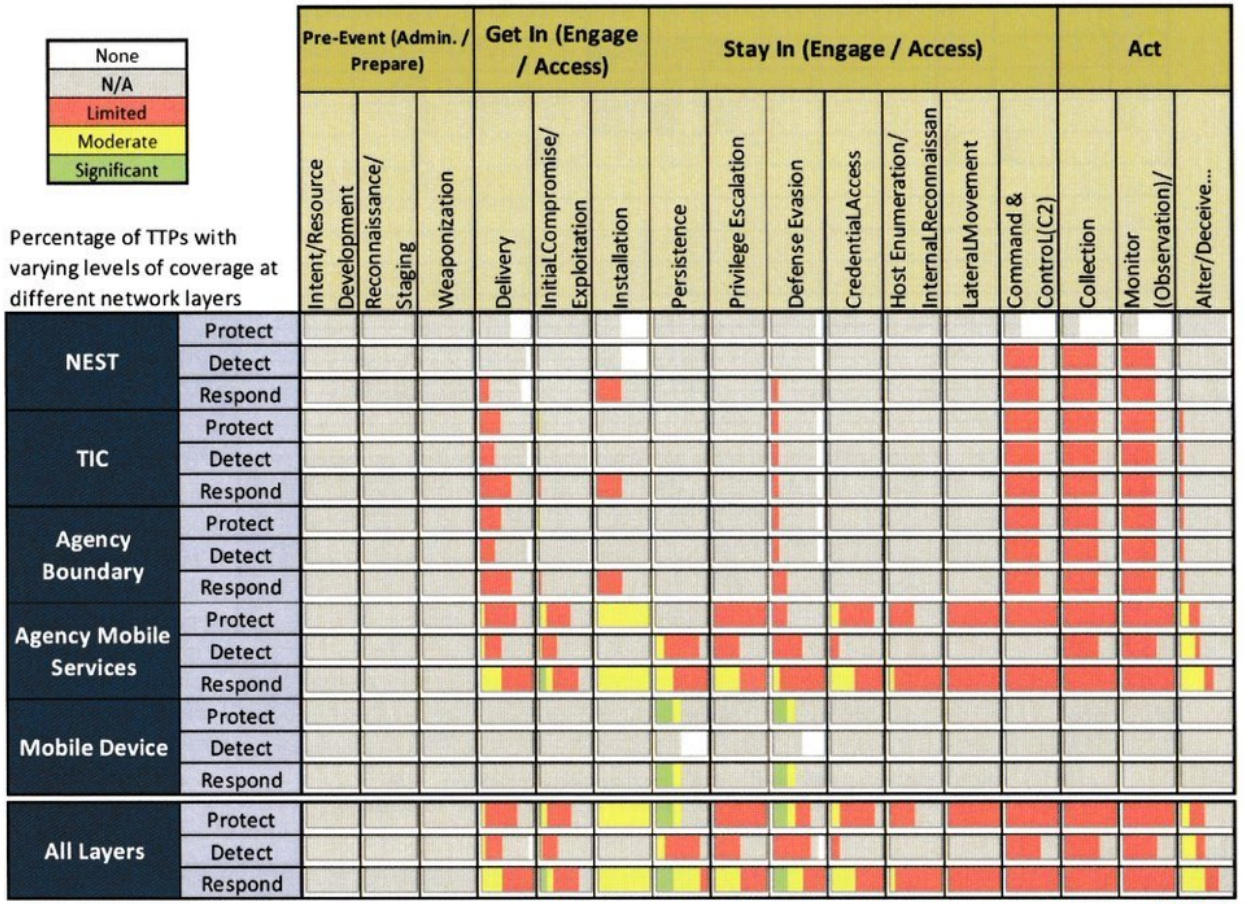
Layer Coverage for Planned Enterprise-Enabled Mobile Device to Internet (Protected)

(FOUO)

Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I

None
N/A
Limited
Moderate
Significant

Percentage of TTPs with varying levels of coverage at different network layers



(FOUO)

Best Calculation

.govCAR Mitigation Draft Scoring Sheet		Stage					
		Objective					
		Threat Action Y			Threat Action Z		
		Protect	Detect	Respond	Protect	Detect	Respond
	Capabilities	Threat Action Description			Threat Action Description		
Set	Layer 1						
1	A	L	N/A	L	M	None	M
1	B	L	None	L	L	None	L
	Layer 2						
1	C	L	None	S	S	L	S
1	D	N/A	N/A	N/A	N/A	N/A	N/A
1	E	None	None	M	None	None	M
All Capabilities Set 1		L	None	S	S	L	S
P/D/R RollUp		S			S		

Weights

Significant – 0.9
Moderate – 0.6
Limited – 0.3
None & N/A - 0

Protect – 0.4
Detect – 0.3
Respond – 0.3

Protect Weighted Coverage:

- For each Threat action, calculate Score * ScoreWeight * HeatMapValue
- Sum all the values for all threat actions

Repeat for Detect & Respond

Combined PDR Weighted Coverage:

(Protect Weighted Coverage * Protect Weight) +
(Detect Weighted Coverage * Detect Weight) +
(Respond Weighted Coverage * Respond Weight)

CISA
CYBER+INFRASTRUCTURE

Best calculation

(FOUO)

Sum of all Protect scores * ScoreWeight * HeatMapValue

Capability Mitigation Rollup	Layers	Sets	Weighted Coverage (All Enabled TTPs)			PDR Weighted
			Protect	Detect	Respond	PDR Combined
DC:Device Health Check Remediation	Agency Server	Current Internet to Data Center w/o B&I	99.4	25.4	124.0	84.6
DC:Whitelisting (SWAM)	Agency Server	Both	94.0	3.5	94.0	66.8
DC:Device Health Check	Agency Server	Both	0.0	96.5	113.5	63.0
DC:WAF/RWP w/ B&I	Data Center Zone Boundary	Current Internet to Data Center w/o B&I	60.9	22.8	58.2	48.7

Combined PDR Weighted Coverage:

(Protect Weighted Coverage * Protect Weight) +
(Detect Weighted Coverage * Detect Weight) +
(Respond Weighted Coverage * Respond Weight)

Combined PDR Weighted Coverage:

99.4 * 0.4 +
25.4 * 0.3 +
124.0 * 0.3
= 84.58

CISA CYBER+INFRASTRUCTURE

Top Threat Actions

(FOUO)

Objective	Threat Action	Heat Map	Capability 1 All Capabilities Current Internet to Data Center w/o B&I	Capability 2 All Capabilities Planned Internet to Data Center w/o B&I	
Credential Access	Credential Dumping	13.6	M	M	
Credential Access	Password Recovery	9.0	N/A	N/A	
Host Enumeration/ Internal Reconnaissance	File System Enumeration	8.9	L	L	
Command & Control (C2)	Commonly used port	8.5	S	S	
Host Enumeration/ Internal Reconnaissance	Process Enumeration	8.4	L	L	
Installation	Writing to Disk	7.7	L	L	
Host Enumeration/ Internal Reconnaissance	Account Enumeration	7.3	L	L	
Initial Compromise/ Exploitation	Targets Application Vulnerability	7.3	L	L	
Defense Evasion	Masquerading	7.2	S	S	Respond Only
Weaponization	Add Exploits to Application Data Files	7.0	N/A	L	Rep & WAF/RWP Enh
Command & Control (C2)	Standard app layer protocol	7.0	M	M	
Execution	Command Line	6.9	M	M	
Host Enumeration/ Internal Reconnaissance	Operating System Enumeration	6.8	L	L	
Defense Evasion	Legitimate Credentials	6.7	L	L	
Defense Evasion	Obfuscated Payload	6.7	S	S	
Initial Compromise/ Exploitation	Trojan	6.7	S	S	
Persistence	Legitimate Credentials	6.4	S	S	
Host Enumeration/ Internal Reconnaissance	Local Network Configuration Enumeration	6.3	L	L	
Host Enumeration/ Internal Reconnaissance	Local Network Enumeration	6.3	M	M	
Delivery	Web Application Exploit over the Network	6.0	S	S	
Intent/Resource Development	Intent/Resource Development	6.0	N/A	L	Rep & WAF/RWP Enh
Defense Evasion	Scripting	5.8	L	L	
Host Enumeration/ Internal Reconnaissance	Owner/User Enumeration	5.7	L	L	
Lateral Movement	Remote Interactive Logon	5.7	M	M	
Lateral Movement	Remote File Shares	5.7	L	M	Rep & Auto DHC-R
Command & Control (C2)	Communications Encrypted	5.5	M	M	
Reconnaissance/ Staging	Social Media	5.4	N/A	N/A	
Persistence	Automatic Loading at Startup	5.4	S	S	
Monitor (Observation)/ Exfiltration	Exfil over C2 channel	5.3	L	L	
Defense Evasion	File Deletion	5.3	N/A	N/A	
Privilege Escalation	Scheduled Task	5.1	S	S	
Initial Compromise/ Exploitation	Legitimate Access	5.0	S	S	
Command & Control (C2)	Data Obfuscation	5.0	M	M	
Command & Control (C2)	Fallback Channels	5.0	M	M	
Defense Evasion	Signed Malicious Content	4.8	S	S	
Reconnaissance/ Staging	Vulnerability Scan	4.8	S	S	
Privilege Escalation	Legitimate Credentials	4.6	L	L	
Privilege Escalation	Multi Tenant Side Channel Cache Attack	4.6	N/A	N/A	
Defense Evasion	Software Packing	4.3	S	S	
Execution	Scheduled Task	4.2	S	S	
Host Enumeration/ Internal Reconnaissance	Security Software Enumeration	4.2	L	L	

Recommendations, Affirmations, Observations

- Recommendations are suggested changes to the architecture based on the data analysis.
- Affirmations are not suggested changes, but strong statements showing where the architecture and its capabilities are providing the intended mitigations and may not need investment.
- Observations are areas where the data indicates issues, but the conclusions are not strong enough for a Recommendation or Affirmation. Further analysis in those areas is warranted.

CISA
CYBER+INFRASTRUCTURE

RAO Development

- Each analyst keeps notes on what they see
  - Application Whitelisting provides Moderate to Significant coverage for High Heat Map threat actions
  - The bulk of current threat coverage for Persistence and Privilege Escalation is mitigated by Application Whitelisting capability
- Looking across all analysis for themes
- Deciding on the messaging:
  - Have the above as Affirmations, or
  - Recommendation: Implement Application Whitelisting in the environment to prevent unknown applications from running.
- Recommendations should be actionable and have clear impact
  - It can help to present finding along with the recommendation

CISA
CYBER+INFRASTRUCTURE

ROA's from Today

CISA
CYBER+INFRASTRUCTURE

Tool Needs Discussion

CISA
CYBER+INFRASTRUCTURE

Mini Breakouts

	Architecture	Threat	Facilitating a Scoring Session
Facilitator	Kurt	Ingrid	Laurie
Topics	• Architecture decomposition • Capabilities and capability decomposition • Datasets and Flows	• Reading a threat report • Heatmap Generation	• Scoring Philosophy • Modified Delphi Method

CISA
CYBER+INFRASTRUCTURE

ARCHITECTURE

CISA
CYBER+INFRASTRUCTURE

Architecture - Composition

- Decide what you want to protect/assess
  - E.g., protect endpoints, protect data center servers
- Identify the use cases/interactions of the protected element with network source/destination points (e.g., Internet)
  - Include the network source/destination points in the architecture composition
- Establish logical groupings (Architectural Layers) where capabilities would be deployed in the Architecture
  - E.g., Agency Boundary, Agency Endpoint

CISA
CYBER+INFRASTRUCTURE

Architecture - Capabilities

- For each Architectural Layer, identify the Capabilities (things providing cybersecurity) that will contribute to providing mitigations for the protected element
  - Include Current and Planned (and Prospective?)
  - Consider "directionality" – is the protected element the initiator (source) or receptor (destination) for a network session?
  - Capabilities may be grouped if they only work in conjunction with each other
- Determine the features (cybersecurity functions) for each capability
  - Describe in sufficient detail to remove ambiguity and support scoring
  - Granularity based on ability to "turn on/off" or configure

CISA
CYBER+INFRASTRUCTURE

Architecture – Flows/Capability Sets

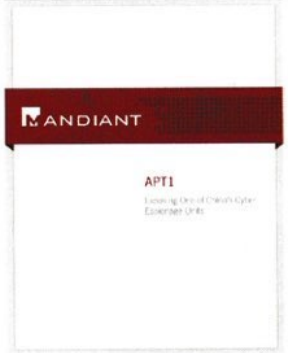
- Flows are the path through the Architectural Layers between network source/destination points
  - Establishes the baseline Capability Sets (Current/Planned) based on the capabilities in the Architectural Layers traversed
- Baseline Capability Sets are modified to do layer analysis
  - Remove capabilities one Architectural Layer at a time
- Create additional Capability Sets to add/remove capabilities for layer or "what if" analysis
  - May include only a few capabilities to show overlap/complementary nature

CISA
CYBER+INFRASTRUCTURE

THREAT

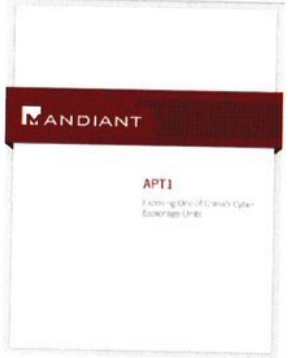
CISA
CYBER+INFRASTRUCTURE

Parsing a threat report (Example)



- "The Initial Compromise represents the methods intruders use to first penetrate a target organization's network. As with most other APT groups, spear phishing is APT1's most commonly used technique. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file." (p. 28)
- "The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples' names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel — and uses these accounts to send the emails."
- "If anyone had clicked on the link that day (which no one did, thankfully), their computer would have downloaded a malicious ZIP file named "Internal_ Discussion_Press_Release_In_Next_Week8.zip". This file contained a malicious executable that installs a custom APT1 backdoor that we call WEBC2-TABLE." (p. 28)
- "APT1's beachhead backdoors are usually what we call WEBC2 backdoors. WEBC2 backdoors are probably the most well-known kind of APT1 backdoor, and are the reason why some security companies refer to APT1 as the "Comment Crew." A WEBC2 backdoor is designed to retrieve a webpage from a C2 server. It expects the webpage to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The standard, non-WEBC2 APT1 backdoor typically communicates using the HTTP protocol (to blend in with legitimate web traffic) or a custom protocol that the malware authors designed themselves." (p. 31)

Parsing a threat report (Example)



- "The Initial Compromise represents the methods intruders use to first penetrate a target organization's network. As with most other APT groups, **spear phishing** is APT1's most commonly used technique. The spear phishing emails contain either a (1) **malicious attachment** or a (2) **hyperlink to a malicious file**." (p. 28)
  - (1) [Spear-phishing with Attachments] / (2) [Spear-phishing with Malicious Link]
- "The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates (3) **webmail accounts using real peoples' names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel** — and uses these accounts to send the emails."
  - (3) [Intent/Resource Development]
- "If anyone had clicked on the link that day (which no one did, thankfully), (4) **their computer would have downloaded a malicious ZIP file named "Internal Discussion_Press_Release_In_Next_Week8.zip".** (5) (6)**This file contained a malicious executable that installs a custom APT1 backdoor that we call WEBC2-TABLE." (p. 28)**
  - (4) [Weaponization: Add Exploits to Application Data Files],
  - (5) [Delivery:data encoded] (6) [Trojan]
  - More information needed regarding communication methods.
- "APT1's beachhead backdoors are usually what we call WEBC2 backdoors. WEBC2 backdoors are probably the most well-known kind of APT1 backdoor, and are the reason why some security companies refer to APT1 as the "Comment Crew." A WEBC2 backdoor is designed to retrieve a webpage from a C2 server. It expects the webpage to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The standard, non-WEBC2 (7) (8) **APT1 backdoor typically communicates using the HTTP protocol** (to blend in with legitimate web traffic) (9) **or a custom protocol** that the malware authors designed themselves." (p. 31)
  - (7) [C2:commonly used port], (8) [C2: Standard App Layer protocol]
  - (9) [C2:Custom Application Layer Protocol]

CISA
CYBER+INFRASTRUCTURE

Heat Map Generation

- Applicability –
  - Based on whether the use of that action produces artifacts that can be observed in the cybersecurity architecture. That is, whether the architecture can defend against the action. Actions that are not observable by the architecture are given lower applicability scores. (Currently all are 1)
- Maneuverability
  - Based on the number of actions/techniques identified for achieving a particular objective/tactic. (Log 16 of Threat Actions in Objective + 1)
- Prevalence Count
  - Based on the number of threat actors that used the action/technique.
- Heat Map Formula:

$$\frac{Applicability * Prevalence}{Maneuverability} + 1$$

CISA
CYBER+INFRASTRUCTURE

FACILITATING A SCORING SESSION

CISA
CYBER+INFRASTRUCTURE

Facilitating a Scoring Session: Philosophy

- We are interested in big muscle movements, not configuration details.
- The Scoring Moderator guides the team through the processes keeping the team focused on the capability definition, threat action definition, scoring rubric, and CSF Function definition to guard against scope creep.

CISA
CYBER+INFRASTRUCTURE

Facilitating a Scoring Session: Delphi Method (modified)

- Introduce problem
  - Understanding of threat action and capability
- Some discussion, with no positing of scores
  - Examples of good discussion include:
    - How reliable is the anomalous behavior detection?
    - Is the capability only signature based?
    - What are the facets of this threat?
- Everyone silently arrives at a scoring value
- Around the room to collect scoring value only.
- Summarize and discuss rationales
- Arrive at consensus

CISA
CYBER+INFRASTRUCTURE

Facilitating a Scoring Session: Art of Leading the meeting

- The moderator should guide through the process in a way that avoids anchoring.
- Get the score and rationale individually, then allow discussions, then guide to consensus.
- Don't start with your opinion. Err on not having one unless information is missing.
- Don't auto-N/A. Sometimes there are artifacts that are seen.
- We advocate, not argue. To advocate you have to have a position and rationale.
- Listen for "facts not in evidence" e.g. someone trying to attribute a function to a capability (over-exaggerated example – making a passive sensor have a protect capability)

CISA
CYBER+INFRASTRUCTURE

Running a Scoring Session: Art of Leading the meeting

- Approaches - list all scores individually; get a sense of the room. Help focus discussion.
- Delphi is not a voting or averaging mechanism. It is a focusing mechanism and a forcing mechanism to provide info that may not have been in the room
- There's an art to letting everyone be heard, and then if needed, SME tiebreak. Caveat- SME thinks everything is wonderful.
- Develop a sense of the scores against a particular threat action or from a capability in a broad sense to be aware if there's a major deviation going on
  - Host v network
  - Suddenly giving protect scores
  - Giving unusually high or low score
- Learn team – who needs to be prompted; recognize if someone is spoken over and then doesn't speak up again (around the room helps but is time consuming)

CISA
CYBER+INFRASTRUCTURE

Running a Scoring Session: Time Management

- Leading the witness:
  - Select a score as a prompt.
  - Judgement call as to when to use – make sure everyone has spoken
  - Use as a way to wrap up discussion
- When you come to similar threat action – allow air time for concurrence/disagreements. If they disagree, don't disagree with the disagreement. (that poisons the water)
- Tactical and Strategic time management
  - Figure out when its time to finalize score
  - Know how much needs to get done today, and where you are in meeting that
- Don't be afraid to park an issue in order to keep moving.

CISA
CYBER+INFRASTRUCTURE

Running a Scoring Session: Discussion Management

- When it feels like you are getting pushback/arguments (and not advocacy) –
  - Sometimes you just have to offer a score - are you ok with this? What they may be trying to get at is something in the rationale.
  - Do you have a specific recommendation / rationale
- Silent room? Call on people

CISA
CYBER+INFRASTRUCTURE

Running a Scoring Session: Potential traps/rabbit holes

Trap / Rabbit hole	Exit Approach
Google has the answers	Stay true to the defined / agreed upon capability features and threat definition /interpretation
I know the product	Stay true to the defined / agreed upon capability features and threat definition /interpretation
Extreme corner cases	It's ok not to consider an extreme corner case
Valid examples seriously deflating score	A valid counter example may reduce the score, but often that doesn't mean the capability provides nothing.

CISA
CYBER+INFRASTRUCTURE

WRAP UP

CISA
CYBER+INFRASTRUCTURE

Wrap Up

- Thank you
- Electronic versions of the slides will be sent to you.
- Please fill out the survey on this training.
- Please protect this information:
  - It is CUI
  - Encrypt for transmission
  - No further dissemination
- Contact CyberLiaison@hq.dhs.gov for further questions

CISA
CYBER+INFRASTRUCTURE

Technical Annex Requests

- Request in writing to CyberLiaison@hq.dhs.gov
  - Description of interest and intent
  - Expected users
  - Use and potential benefit to agency
- Requests adjudicated by DHS leadership
- Once distributed
  - Protect information
  - Limit access to requested users
  - No further dissemination
  - Allow DHS review of derived work

CISA
CYBER+INFRASTRUCTURE

Topics for Discussion

- D/A volunteers to participate in Spin 6?
- What can D/As do today?
- D/A Suggested future Spin topics?

CISA
CYBER+INFRASTRUCTURE

QUESTIONS?

CISA
CYBER+INFRASTRUCTURE

Comments/Questions

- Lessons learned from applying .govCAR
- Data Architectures

CISA
CYBER+INFRASTRUCTURE

BACKUP

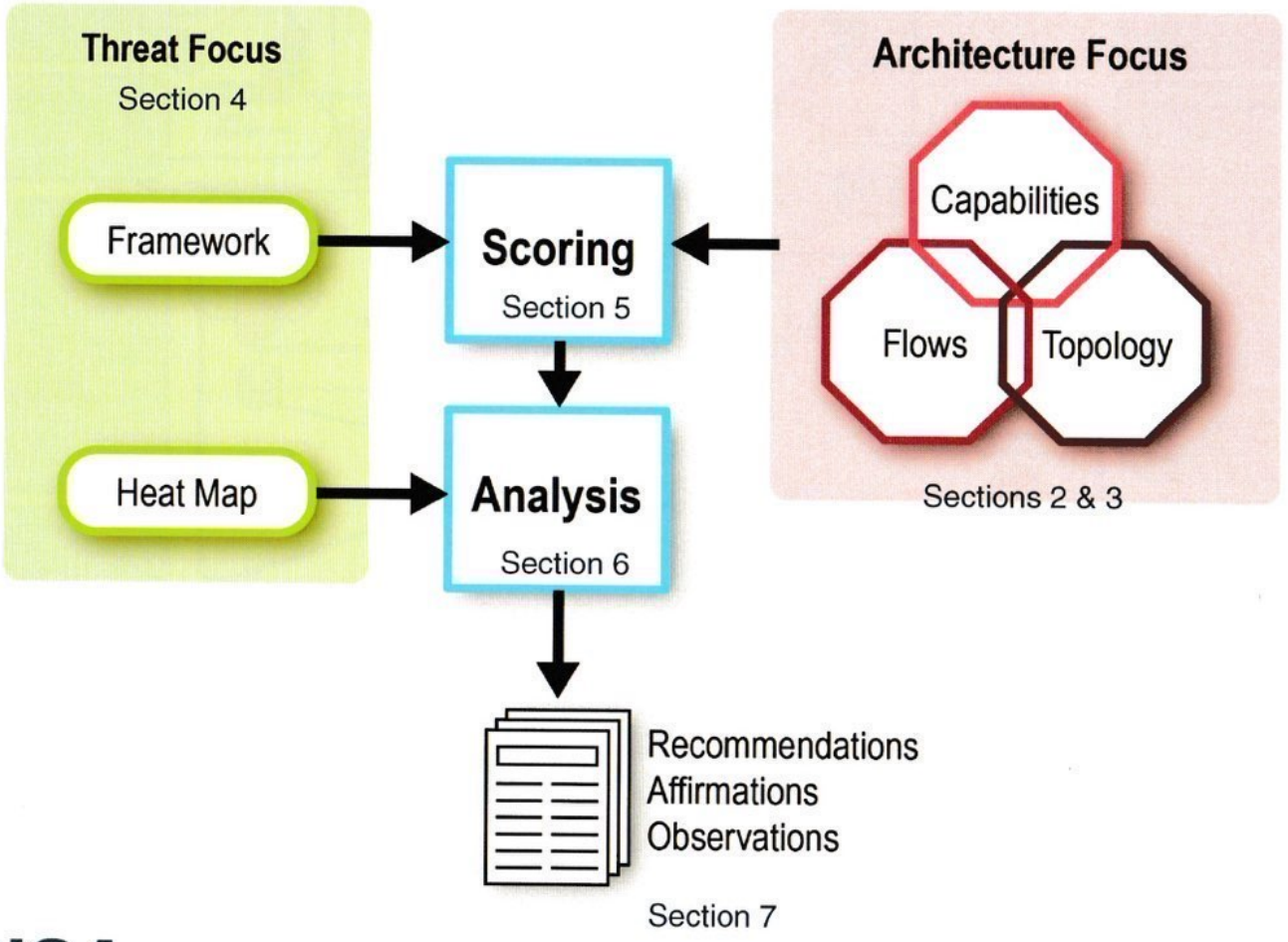
CISA
CYBER+INFRASTRUCTURE

Agenda

08:30	Check In
09:00	Welcome -- Goals and Intent
09:10	.govCAR Introduction
09:30	.govCAR Architecture Under Analysis
10:00	.govCAR Threat Methodology
10:30	*Break*
10:45	.govCAR Scoring
11:15	.govCAR Analysis Overview
11:45	*Questions*
12:00	Lunch
1:00	Capability Scoring for Protect/Detect/Respond
2:00	Analysis
2:45	*Break*
3:00	Continue Analysis
3:30	Breakouts: Architecture, Threat, Facilitating a scoring session

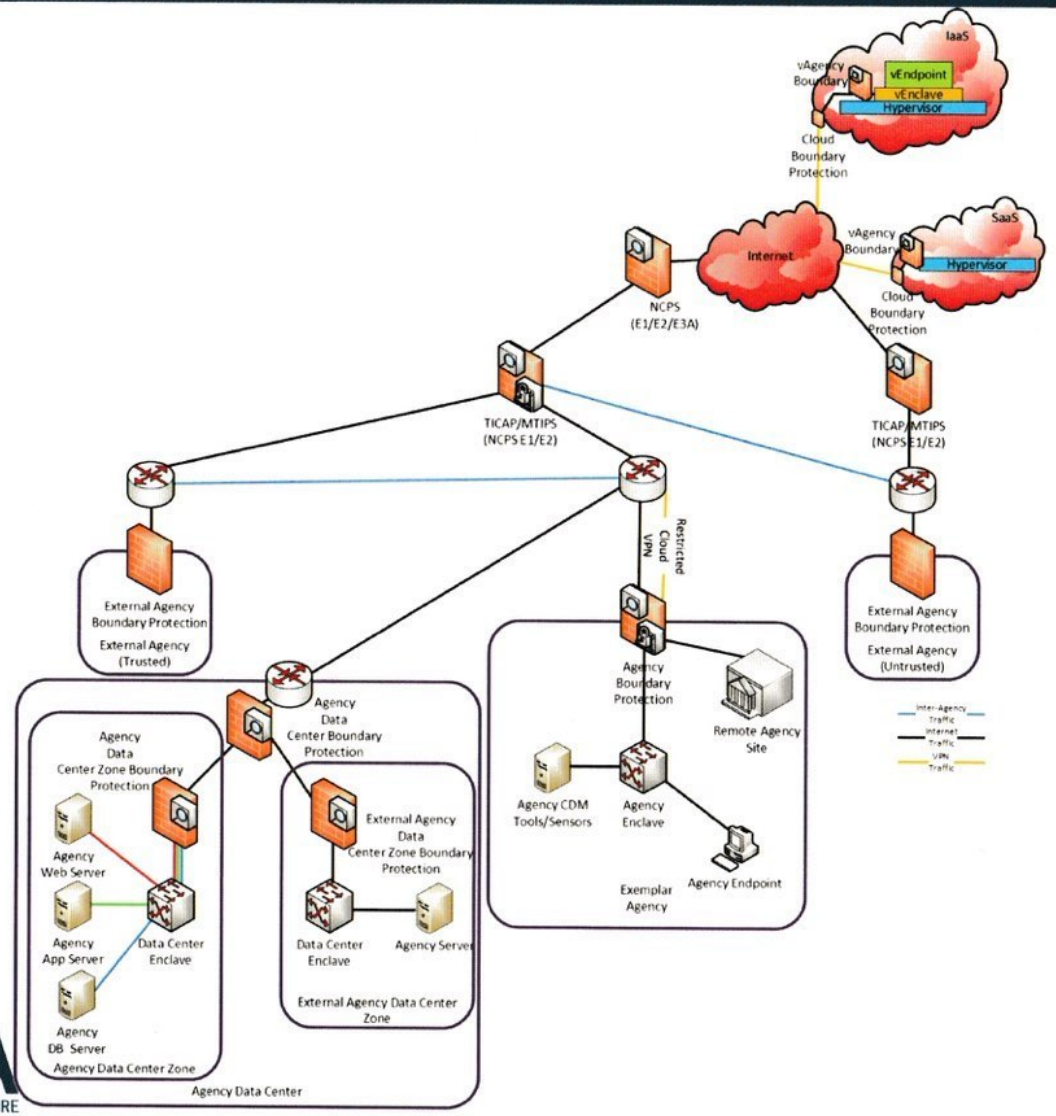
CISA
CYBER+INFRASTRUCTURE

.govCAR Methodology



CISA
CYBER+INFRASTRUCTURE

Representative Architecture (Section 2)



CISA
CYBER+INFRASTRUCTURE

Spin 4 Architectural Layers & Elements

TICAP/MTIPS:
Firewall
Passive Sensor

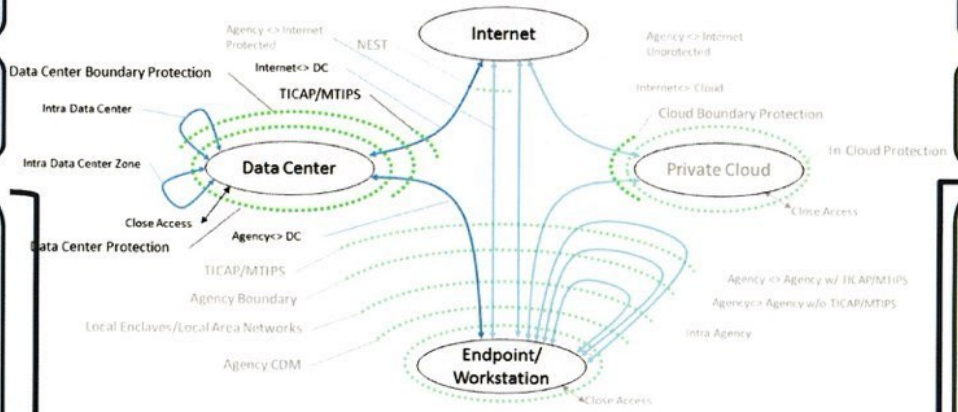
Data Center Boundary:
IP Blacklist
DDoS Mitigation

Data Center Zone Boundary:
NGFW
Passive Sensor
WAF/RWP
ID Federation/RBAC/MFA
DBFW
DBAM

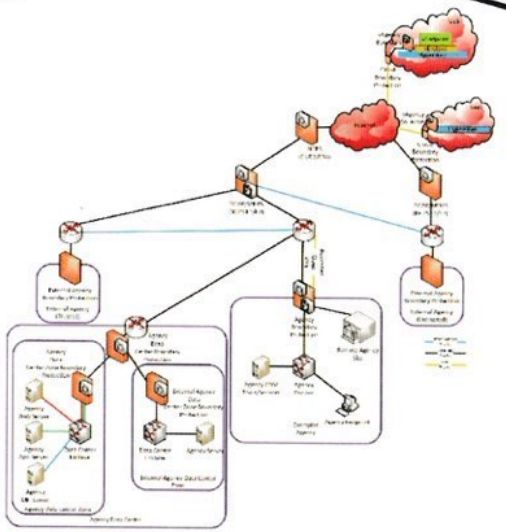
Data Center Enclave:
Network Segmentation
NAC

Agency Server:
Host IPS/FW
Device Control
File Integrity
DHC
DHC-R
Application Whitelisting

Current



Data Center Protection



Planned

TICAP/MTIPS:
Firewall Enhancements
Passive Sensor

Data Center Boundary:
IP Blacklist
DDoS Mitigation

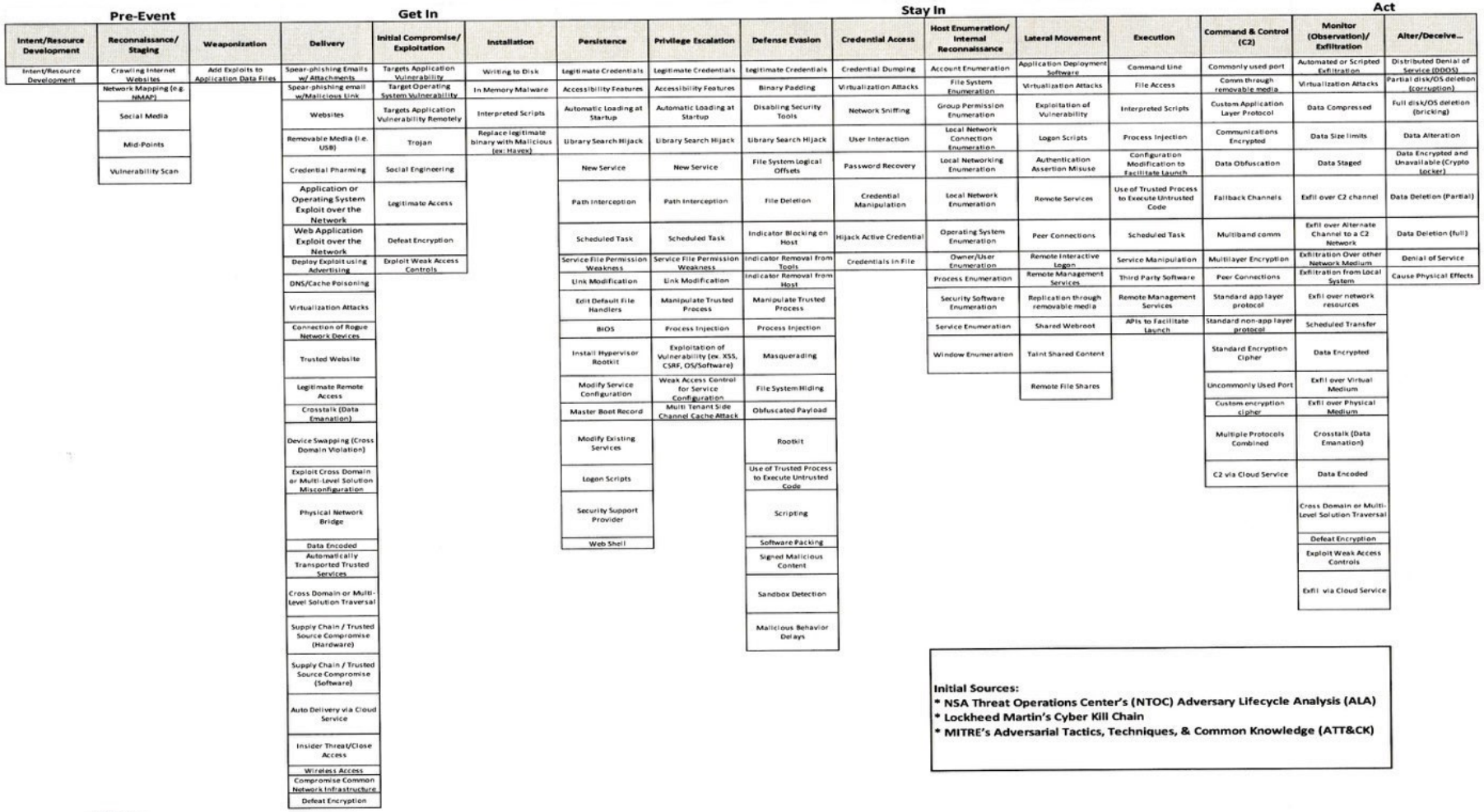
Data Center Zone Boundary:
NGFW
Passive Sensor
WAF/RWP Enhancements
ID Federation/RBAC/MFA
DBFW
DBAM

Data Center Enclave:
ANDB
Network Segmentation
NAC Enhancements

Agency Server:
Host IPS/FW
Device Control
File Integrity
DHC
Auto DHC-R
Application Whitelisting
Reputation

CISA
CYBER+INFRASTRUCTURE

NSA Adversary Lifecycle Threat Framework v2.0

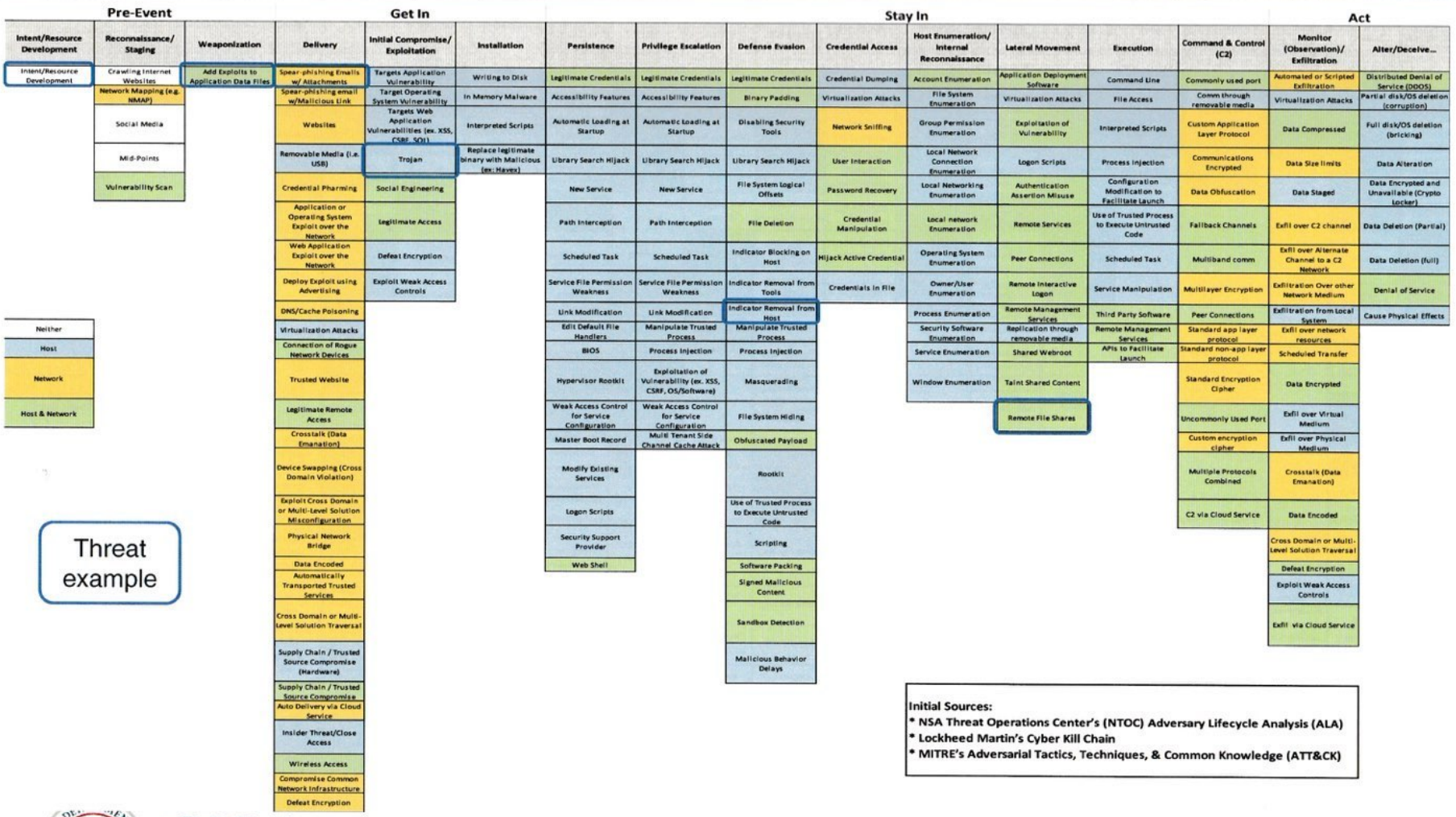


Pre-Event			Get In		Stay In								Act	
Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/ Exploitation	Installation	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration/ Internal Reconnaissance	Lateral Movement	Execution	Command & Control (C2)	Monitor (Observation)/ Exfiltration	Alter/Deceive...
Intent/Resource Development	Crawling Internet Websites	Add Exploits to Application Data Files	Spear-phishing Emails w/ Attachments	Targets Application Vulnerability	Writing to Disk	Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software	Command Line	Commonly used port	Automated or Scripted Exfiltration	Distributed Denial of Service (DDOS)
	Network Mapping (e.g. NMAP)		Spear-phishing email w/Malicious Link	Target Operating System Vulnerability	In Memory Malware	Accessibility Features	Accessibility Features	Binary Padding	Virtualization Attacks	File System Enumeration	Virtualization Attacks	File Access	Comm through removable media	Virtualization Attacks	Partial disk/OS deletion (corruption)
	Social Media		Websites	Targets Application Vulnerability Remotely	Interpreted Scripts	Automatic Loading at Startup	Automatic Loading at Startup	Disabling Security Tools	Network Sniffing	Group Permission Enumeration	Exploitation of Vulnerability	Interpreted Scripts	Custom Application Layer Protocol	Data Compressed	Full disk/OS deletion (bricking)
	Mid-Points		Removable Media (i.e. USB)	Trojan	Replace legitimate binary with Malicious (ex: Havex)	Library Search Hijack	Library Search Hijack	Library Search Hijack	User Interaction	Local Network Connection Enumeration	Logon Scripts	Process Injection	Communications Encrypted	Data Size limits	Data Alteration
	Vulnerability Scan		Credential Pharming	Social Engineering		New Service	New Service	File System Logical Offsets	Password Recovery	Local Networking Enumeration	Authentication Assertion Misuse	Configuration Modification to Facilitate Launch	Data Obfuscation	Data Staged	Data Encrypted and Unavailable (Crypto locker)
			Application or Operating System Exploit over the Network	Legitimate Access		Path Interception	Path Interception	File Deletion	Credential Manipulation	Local Network Enumeration	Remote Services	Use of Trusted Process to Execute Untrusted Code	Fallback Channels	Exfil over C2 channel	Data Deletion (Partial)
			Web Application Exploit over the Network	Defeat Encryption		Scheduled Task	Scheduled Task	Indicator Blocking on Host	Hijack Active Credential	Operating System Enumeration	Peer Connections	Scheduled Task	Multiband comm	Exfil over Alternate Channel to a C2 Network	Data Deletion (full)
			Deploy Exploit using Advertising	Exploit Weak Access Controls		Service File Permission Weakness	Service File Permission Weakness	Indicator Removal from Tools	Credentials in File	Owner/User Enumeration	Remote Interactive Logon	Service Manipulation	Multilayer Encryption	Exfiltration Over other Network Medium	Denial of Service
			DNS/Cache Poisoning			Link Modification	Link Modification	Indicator Removal from Host		Process Enumeration	Remote Management Services	Third Party Software	Peer Connections	Exfiltration from Local System	Cause Physical Effects
			Virtualization Attacks			Edit Default File Handlers	Manipulate Trusted Process	Manipulate Trusted Process		Security Software Enumeration	Replication through removable media	Remote Management Services	Standard app layer protocol	Exfil over network resources	
			Connection of Rogue Network Devices			BIOS	Process Injection	Process Injection		Service Enumeration	Shared Webroot	APIs to Facilitate Launch	Standard non-app layer protocol	Scheduled Transfer	
			Trusted Website			Install Hypervisor Rootkit	Exploitation of Vulnerability (ex. XSS, CSRF, OS/Software)	Masquerading		Window Enumeration	Taint Shared Content		Standard Encryption Cipher	Data Encrypted	
			Legitimate Remote Access			Modify Service Configuration	Weak Access Control for Service Configuration	File System Hiding			Remote File Shares		Uncommonly Used Port	Exfil over Virtual Medium	
			Crosstalk (Data Emanation)			Master Boot Record	Multi Tenant Side Channel Cache Attack	Obfuscated Payload					Custom encryption cipher	Exfil over Physical Medium	
			Device Swapping (Cross Domain Violation)			Modify Existing Services		Rootkit					Multiple Protocols Combined	Crosstalk (Data Emanation)	
			Exploit Cross Domain or Multi-Level Solution Misconfiguration			Logon Scripts		Use of Trusted Process to Execute Untrusted Code					C2 via Cloud Service	Data Encoded	
			Physical Network Bridge			Security Support Provider		Scripting						Cross Domain or Multi-Level Solution Traversal	
			Data Encoded			Web Shell		Software Packing						Defeat Encryption	
			Automatically Transported Trusted Services					Signed Malicious Content						Exploit Weak Access Controls	
			Cross Domain or Multi-Level Solution Traversal					Sandbox Detection						Exfil via Cloud Service	
			Supply Chain / Trusted Source Compromise (Hardware)					Malicious Behavior Delays							
			Supply Chain / Trusted Source Compromise (Software)												
			Auto Delivery via Cloud Service												
			Insider Threat/Close Access												
			Wireless Access												
			Compromise Common Network Infrastructure												
			Defeat Encryption												

Initial Sources:
* **NSA Threat Operations Center's (NTOC) Adversary Lifecycle Analysis (ALA)**
* **Lockheed Martin's Cyber Kill Chain**
* **MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)**

CISA
CYBER+INFRASTRUCTURE

Threat Framework Host vs. Network



CISA
CYBER+INFRASTRUCTURE

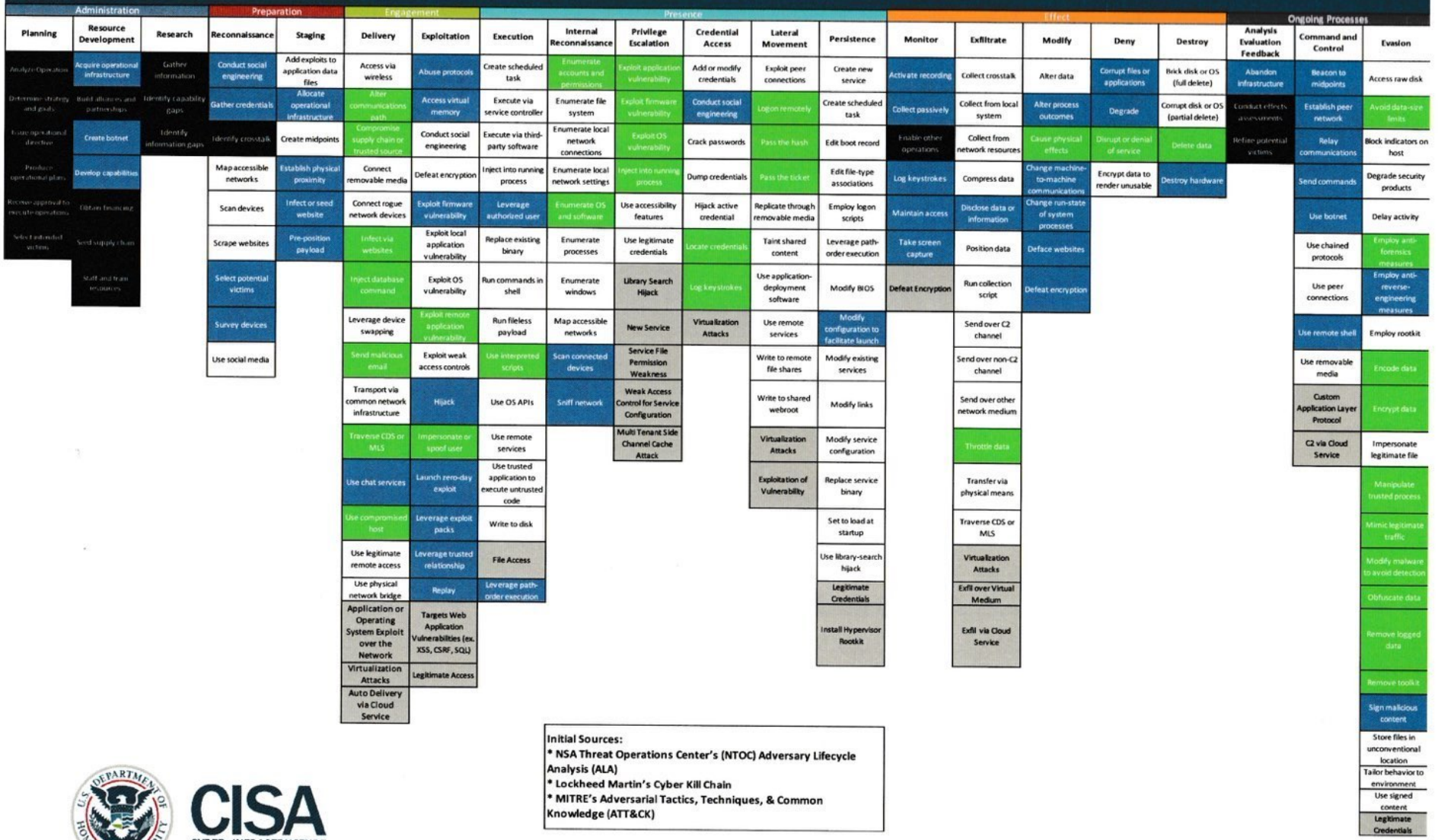
NTCTF 2.0

Administration			Preparation		Engagement		Presence						Effect					Ongoing Processes		
Planning	**Resource Development**	**Research**	**Reconnaissance**	**Staging**	**Delivery**	**Exploitation**	**Execution**	**Internal Reconnaissance**	**Privilege Escalation**	**Credential Access**	**Lateral Movement**	**Persistence**	**Monitor**	**Exfiltrate**	**Modify**	**Deny**	**Destroy**	**Analysis Evaluation Feedback**	**Command and Control**	**Evasion**
Analyze Operation	Acquire operational infrastructure	Gather information	Conduct social engineering	Add exploits to application data files	Access via wireless	Abuse protocols	Create scheduled task	Enumerate accounts and permissions	Exploit application vulnerability	Add or modify credentials	Exploit peer connections	Create new service	Activate recording	Collect crosstalk	Alter data	Corrupt files or applications	Brick disk or OS (full delete)	Abandon infrastructure	Beacon to midpoints	Access raw disk
Determine strategy and goals	Build alliances and partnerships	Identify capability gaps	Gather credentials	Allocate operational infrastructure	Alter communication s path	Access virtual memory	Execute via service controller	Enumerate file system	Exploit firmware vulnerability	Conduct social engineering	Logon remotely	Create scheduled task	Collect passively	Collect from local system	Alter process outcomes	Degrade	Corrupt disk or OS (partial delete)	Conduct effects assessments	Establish peer network	Avoid data-size limits
Issue operational directive	Create botnet	Identify information gaps	Identify crosstalk	Create midpoints	Compromise supply chain or trusted source	Conduct social engineering	Execute via third-party software	Enumerate local network connections	Exploit OS vulnerability	Crack passwords	Pass the hash	Edit boot record	Enable other operations	Collect from network resources	Cause physical effects	Disrupt or denial of service	Delete data	Refine potential victims	Relay communication s	Block indicators on host
Produce operational plans	Develop capabilities		Map accessible networks	Establish physical proximity	Connect removable media	Defeat encryption	Inject into running process	Enumerate local network settings	Inject into running process	Dump credentials	Pass the ticket	Edit file-type associations	Log keystrokes	Compress data	Change machine-to-machine communication s	Encrypt data to render unusable	Destroy hardware		Send commands	Degrade security products
Receive approval to execute operations	Obtain financing		Scan devices	Infect or seed website	Connect rogue network devices	Exploit firmware vulnerability	Leverage authorized user	Enumerate OS and software	Use accessibility features	Hijack active credential	Replicate through removable media	Employ logon scripts	Maintain access	Disclose data or information	Change run-state of system processes				Use botnet	Delay activity
Select intended victims	Seed supply chain		Scrape websites	Pre-position payload	Infect via websites	Exploit local application vulnerability	Replace existing binary	Enumerate processes	Use legitimate credentials	Locate credentials	Taint shared content	Leverage path-order execution	Take screen capture	Position data	Deface websites				Use chained protocols	Employ anti-forensics measures
	Staff and train resources		Select potential victims		Inject database command	Exploit OS vulnerability	Run commands in shell	Enumerate windows		Log keystrokes	Use application-deployment software	Modify BIOS		Run collection script	Defeat encryption				Use peer connections	Employ anti-reverse-engineering measures
			Survey devices		Leverage device swapping	Exploit remote application vulnerability	Run fileless payload	Map accessible networks			Use remote services	Modify configuration to facilitate launch		Send over C2 channel					Use remote shell	Employ rootkit
			Use social media		Send malicious email	Exploit weak access controls	Use interpreted scripts	Scan connected devices			Write to remote file shares	Modify existing services		Send over non-C2 channel					Use removable media	Encode data
					Transport via common network infrastructure	Hijack	Use OS APIs	Sniff network			Write to shared webroot	Modify links		Send over other network medium						Encrypt data
					Traverse CDS or MLS	Impersonate or spoof user	Use remote services					Modify service configuration		Throttle data						Impersonate legitimate file
					Use chat services	Launch zero-day exploit	Use trusted application to execute untrusted code					Replace service binary		Transfer via physical means						Manipulate trusted process
					Use compromised host	Leverage exploit packs	Write to disk					Set to load at startup		Traverse CDS or MLS						Mimic legitimate traffic
					Use legitimate remote access	Leverage trusted relationship						Use library-search hijack								Modify malware to avoid detection
					Use physical network bridge	Replay														Obfuscate data
																				Remove logged data
																				Remove toolkit
																				Sign malicious content
																				Store files in unconventional location
																				Tailor behavior to environment
																				Use signed content

Initial Sources:
*** NSA Threat Operations Center's (NTOC) Adversary Lifecycle Analysis (ALA)**
*** Lockheed Martin's Cyber Kill Chain**
*** MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)**

CISA
CYBER+INFRASTRUCTURE

NTCTF 2.0



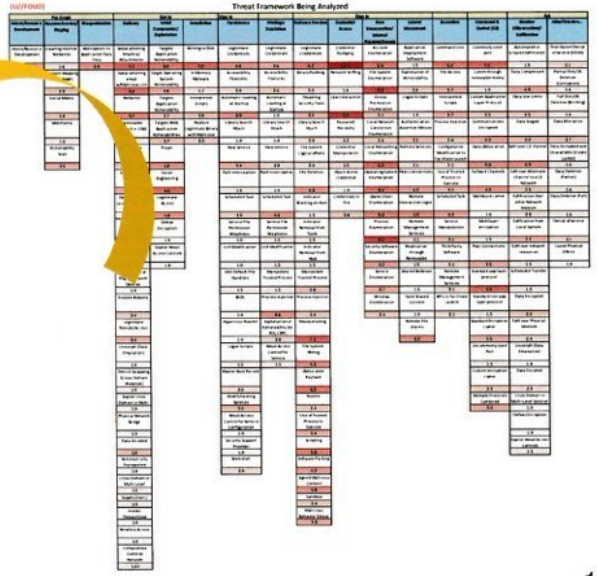
Initial Sources:
* **NSA Threat Operations Center's (NTOC) Adversary Lifecycle Analysis (ALA)**
* **Lockheed Martin's Cyber Kill Chain**
* **MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)**

CISA
CYBER+INFRASTRUCTURE

Threat Heat map

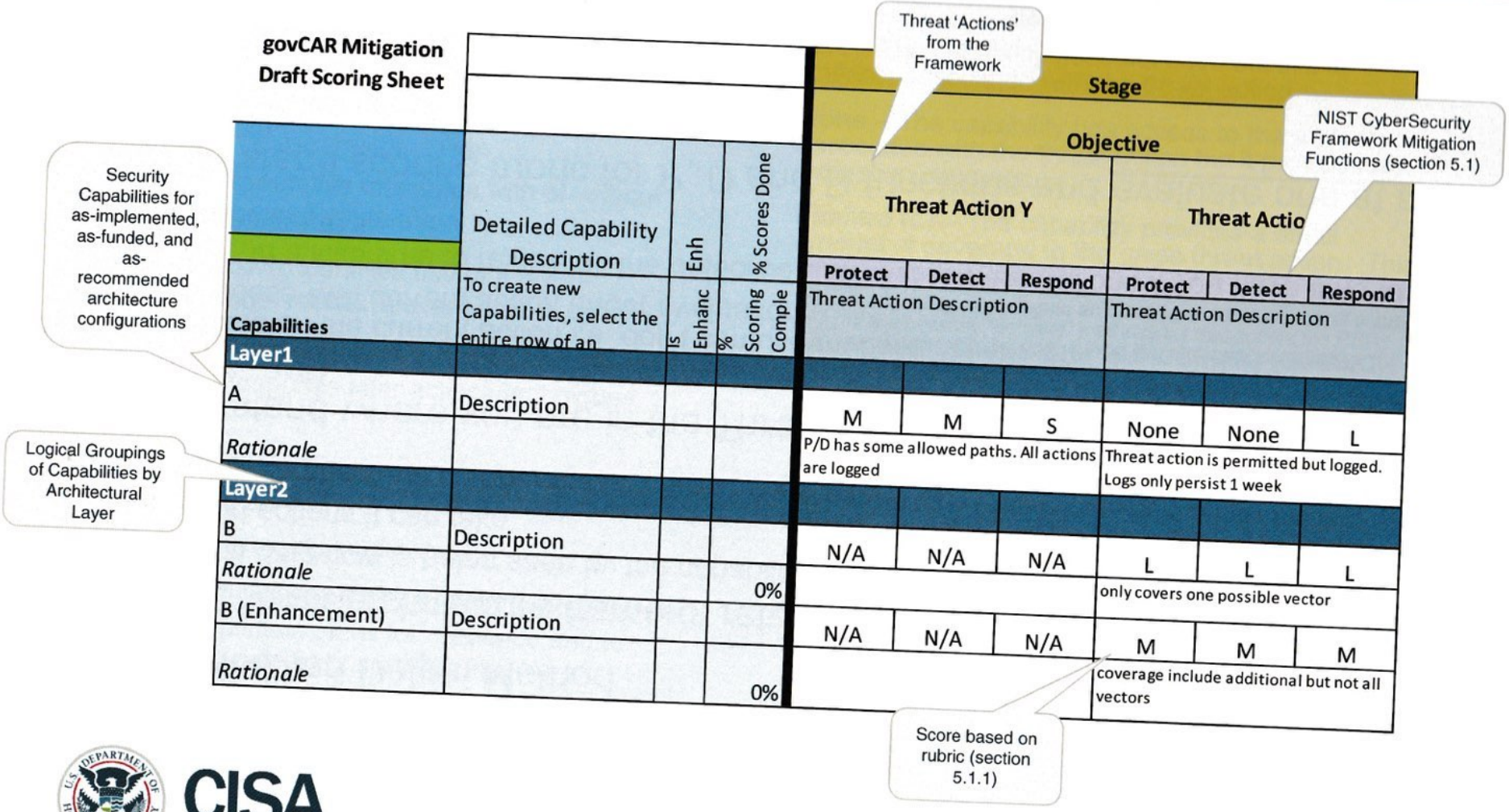
- Based on open source reporting
- Includes data on 63 different threat actor groups
  - Full list in Appendix B
- Documented threat actions map to 143 out of 188 Heat map reflects prevalence/ maneuverability of adversary action
- Manual process to review reports and map to the threat framework

Stay In			
Defense Evasion	**Credential Access**	**Host Enumeration/ Internal Reconnaissance**	**Lateral Movement**
Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software
6.2	12.2	6.4	1.5
Binary Padding	Network Sniffing	File System Enumeration	Exploitation of Vulnerability
2.0	1.6	8.0	2.6
Disabling Security Tools	User Interaction	Group Permission Enumeration	Logon Scripts
3.4	8.6	3.1	1.5
Library Search Hijack	Password Recovery	Local Network Connection Enumeration	Authentication Assertion Misuse
2.0	2.2	2.6	3.1



CISA
CYBER+INFRASTRUCTURE

Protect, Detect, Respond (PDR) Scoring Spreadsheet



CISA
CYBER+INFRASTRUCTURE

Key Tenets of Scoring

- Use Modified Delphi Method
- Establish an architecture frame of reference for the capability
  - What data flow is being seen by the capability
  - What actions it can take
  - What architectural component is it protecting
- Understand where you are in the Threat Framework (prepare, get in, stay in, act).
  - Focus on the current action i.e. don't confuse multiple actions that are needed for actor success with current action under evaluation.
  - Spend a little time to review all the objectives at least. Threat Actions if you have time to help with this
- Understand scoring rubric for P, D and R functions and evaluate one at a time.
  - Completeness
  - Reliability
  - Foreknowledge
  - Cyber relevant time – capability "functions" (PDR) before threat actor

CISA
CYBER+INFRASTRUCTURE

PDR Scoring Rubric

Cybersecurity Framework Core Functions

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities (Not scored by this analysis)

Protect – Preventative measures with or without detection; near immediate effect

Detect – Passive; identifies use of a given action/technique, results in event data in cyber relevant time

Respond – Response after actions/techniques successful

- Can be detection
- Can be analysis
- Can be changing configuration

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capability or services that were impaired due to a cybersecurity event. (Not scored in this analysis.)

Scoring Values

N/A – The capability does not have access to artifacts associated with the threat action

None – The capability has access to the artifacts associated with the threat action but it provides no mitigation coverage

Limited (L) – The capability provides a small amount of coverage to the given threat action. This includes cases where

- A capability can mitigate an action, but only for a small subset of the possible "delivery" methods for that action; the PDR score will be reduced to reflect the pro-rated contribution for total mitigation of the action.
- Coverage is unreliable
- Protection/Detection relies on exact foreknowledge of adversary tools, protocols or infrastructure (e.g., adversary IP address space or domain names)

Moderate (M) – The capability provides modest coverage on the action. It includes cases where coverage is relatively reliable but not complete, and mostly not dependent on exact foreknowledge (e.g., behavior-based).

Significant (S) – The capability provides robust coverage. Coverage is very reliable, almost complete, and not dependent on foreknowledge.

CISA
CYBER+INFRASTRUCTURE

PDR Analysis: Aggregating the Scores - Threat Coverage Roll-Up

Title of set and list of PDR functions

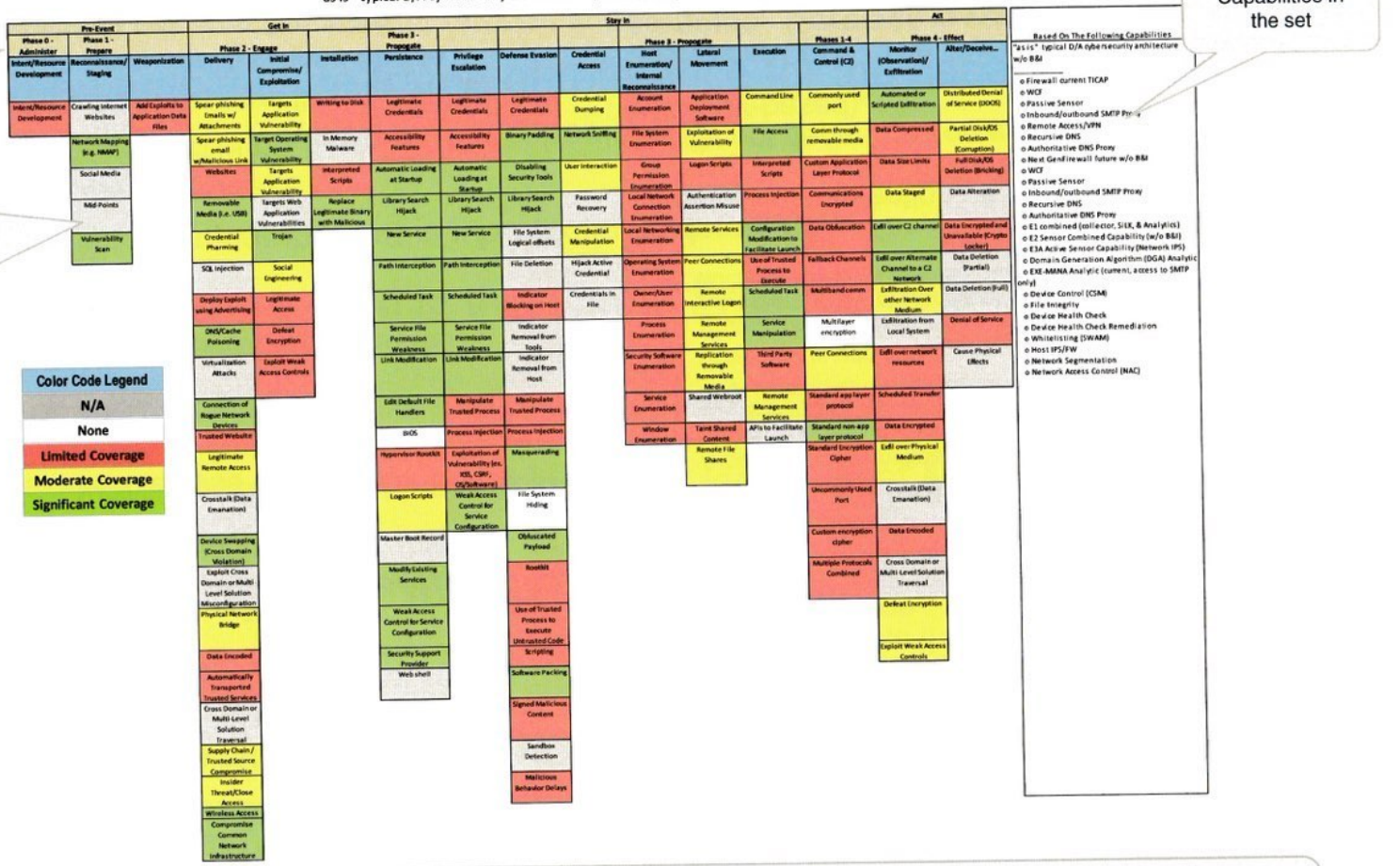
Capabilities in the set

Threat Objective from the Framework

Threat Actions from the Framework.

Color is from Legend and indicates highest level of PDR coverage across all capabilities in the set.

"as is" typical D/A cybersecurity architecture w/o B&I Coverage For: Protect, Detect, & Respond



Illustrates highest level of PDR coverage across all capabilities in the set.

Goal is not to turn it all green, but to identify opportunities for improvement.

CISA CYBER+INFRASTRUCTURE

References

- NIST Framework for Improving Critical Infrastructure Core Functions
  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Federal Cybersecurity Risk Determination Report and Action Plan https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf
- NTCTF 2.0 https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf

CISA
CYBER+INFRASTRUCTURE

CISA

CYBER+INFRASTRUCTURE