CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

.govCAR

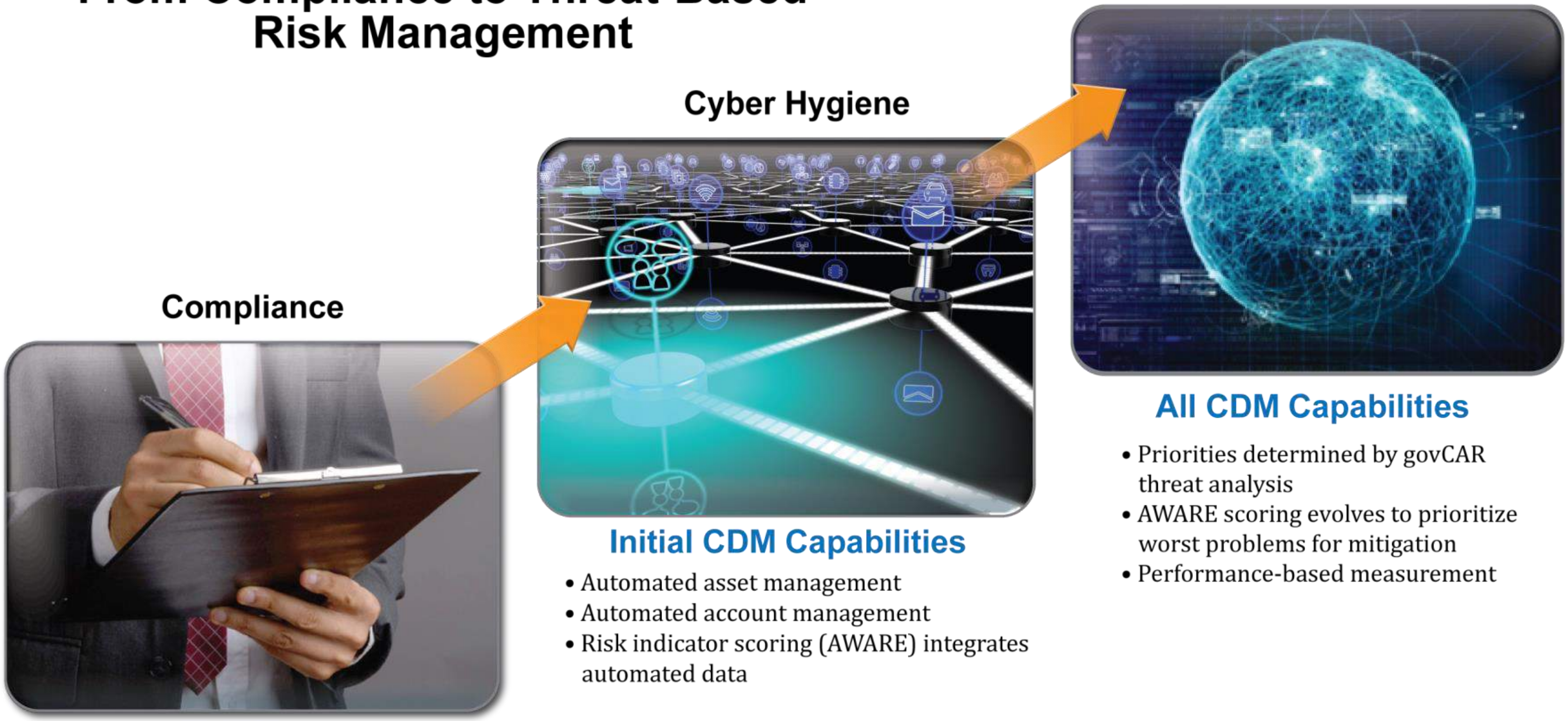
THINK LIKE THE ADVERSARY

CISA
CYBER+INFRASTRUCTURE

Greg Bastien & Branko Bokan, May 16, 2019

Move to Stronger Risk Management

From Compliance to Threat-Based Risk Management



Compliance

Cyber Hygiene

Threat-Based Approach

Pre-CDM

- Manual FISMA compliance
- Yes/no responses are simplistic
- Risk determination based on checklist

Initial CDM Capabilities

- Automated asset management
- Automated account management
- Risk indicator scoring (AWARE) integrates automated data

All CDM Capabilities

- Priorities determined by govCAR threat analysis
- AWARE scoring evolves to prioritize worst problems for mitigation
- Performance-based measurement

Risk = Consequence x Vulnerability x Threat

About

- .govCAR methodology provides threat-based assessment of cyber capabilities
- looks at the problem of cyber security the way an adversary does
- directly identifies where mitigations can be applied for the best defense against all phases of a cyber-attack.
- designed to enhance cybersecurity by analyzing capabilities against the current cyber threats to highlight gaps, and identify and prioritize areas for future investments.
- parallels DoD project known as DoDCAR (previously NSCSAR), which introduced the concept of a threat-based, end-to-end analysis of large, enterprise cybersecurity architectures and is used to provide direction and justification for cybersecurity

Why .govCAR?

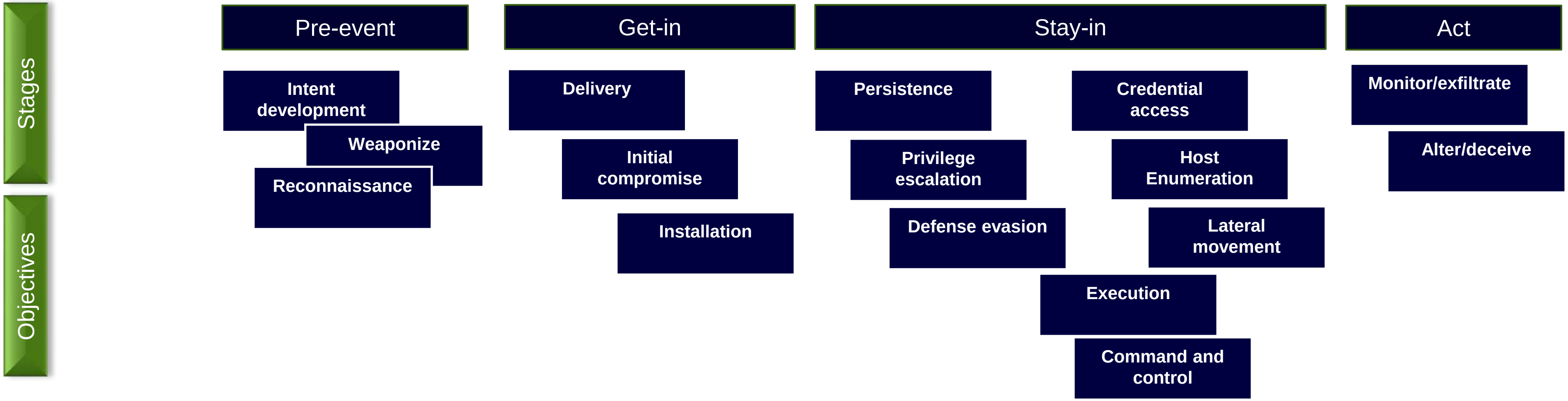
- Evaluate architectures of architectures (layered architecture)
- Are my current cyber security capabilities protecting me against threats? If not, where are the gaps?
- Support investment direction and decisions especially at the portfolio level. Am I investing my cyber security budget wisely? What should my next investment be?
- Is there unwanted duplication of security functionality?
- Can evaluate people, policy and process capabilities, but has been primarily used for technology (materiel) evaluation

Anatomy of a cyber attack

Stages

Pre-event | Get-in | Stay-in | Act

Stages and objectives



Stages

Objectives

Pre-event

- Intent development
- Weaponize
- Reconnaissance

Get-in

- Delivery
- Initial compromise
- Installation

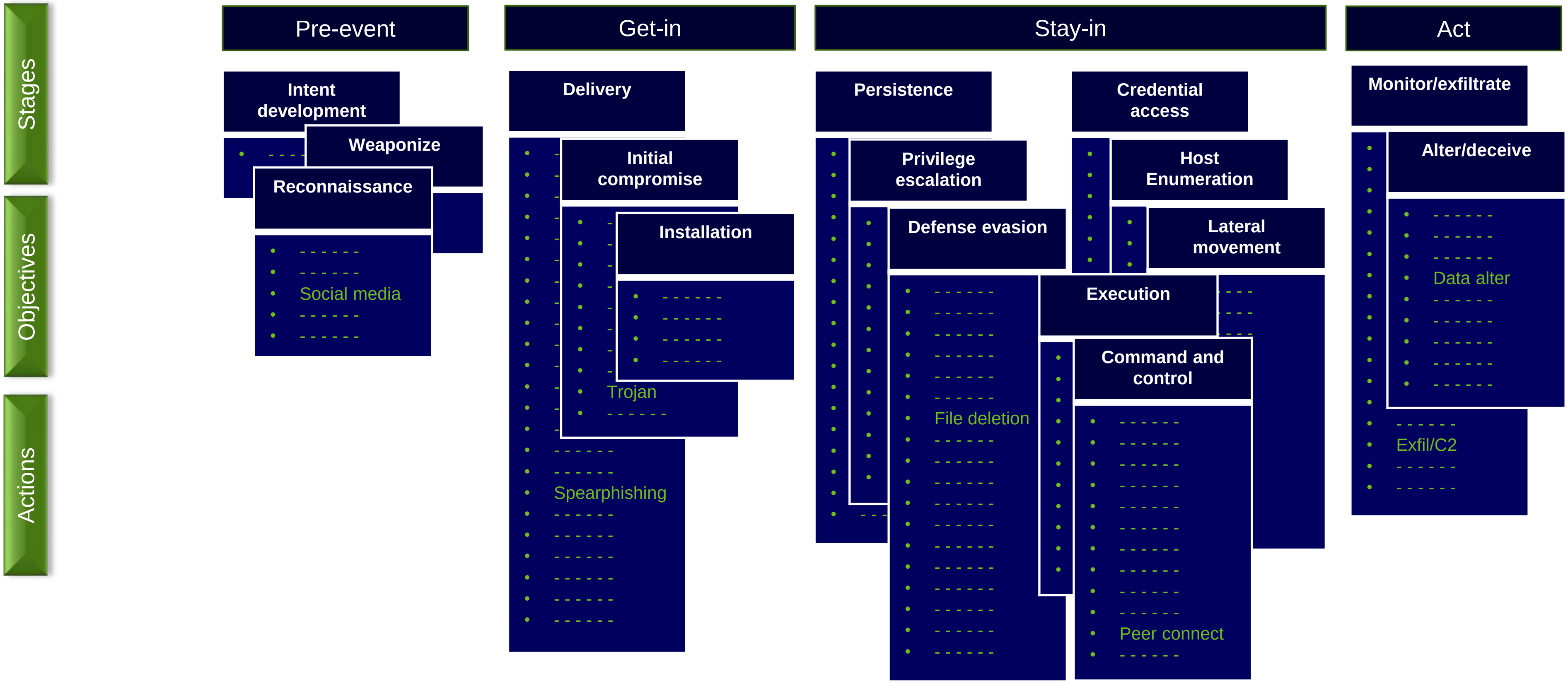
Stay-in

- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Host Enumeration
- Lateral movement
- Execution
- Command and control

Act

- Monitor/exfiltrate
- Alter/deceive

Threat actions



Stages

Objectives

Actions

Pre-event

Get-in

Stay-in

Act

Intent development

Weaponize

Reconnaissance

- Social media

Delivery

- Spearphishing

Initial compromise

- Trojan

Installation

Persistence

Privilege escalation

Defense evasion

- File deletion

Execution

Command and control

- Peer connect

Credential access

Host Enumeration

Lateral movement

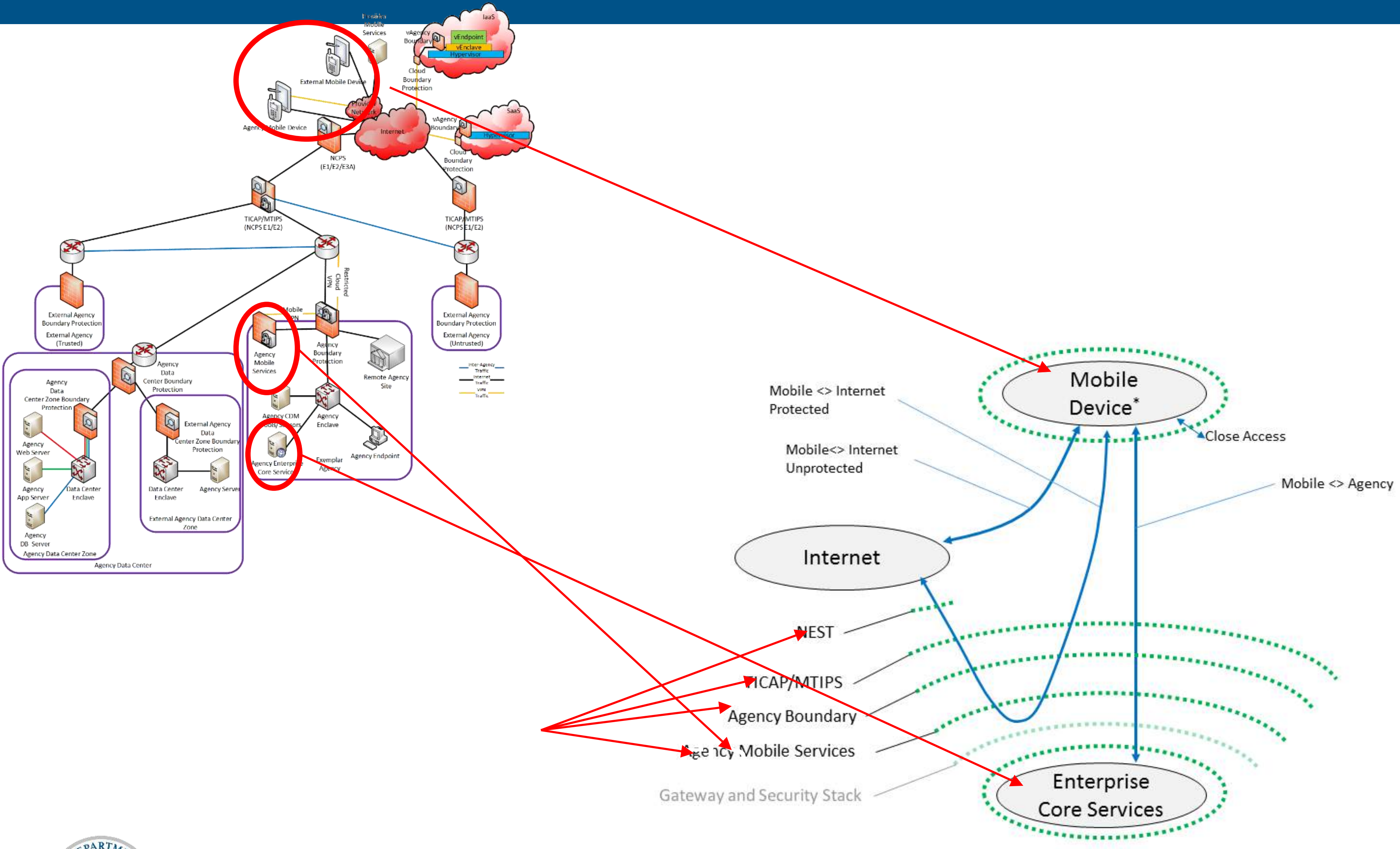
Monitor/exfiltrate

- Exfil/C2

Alter/deceive

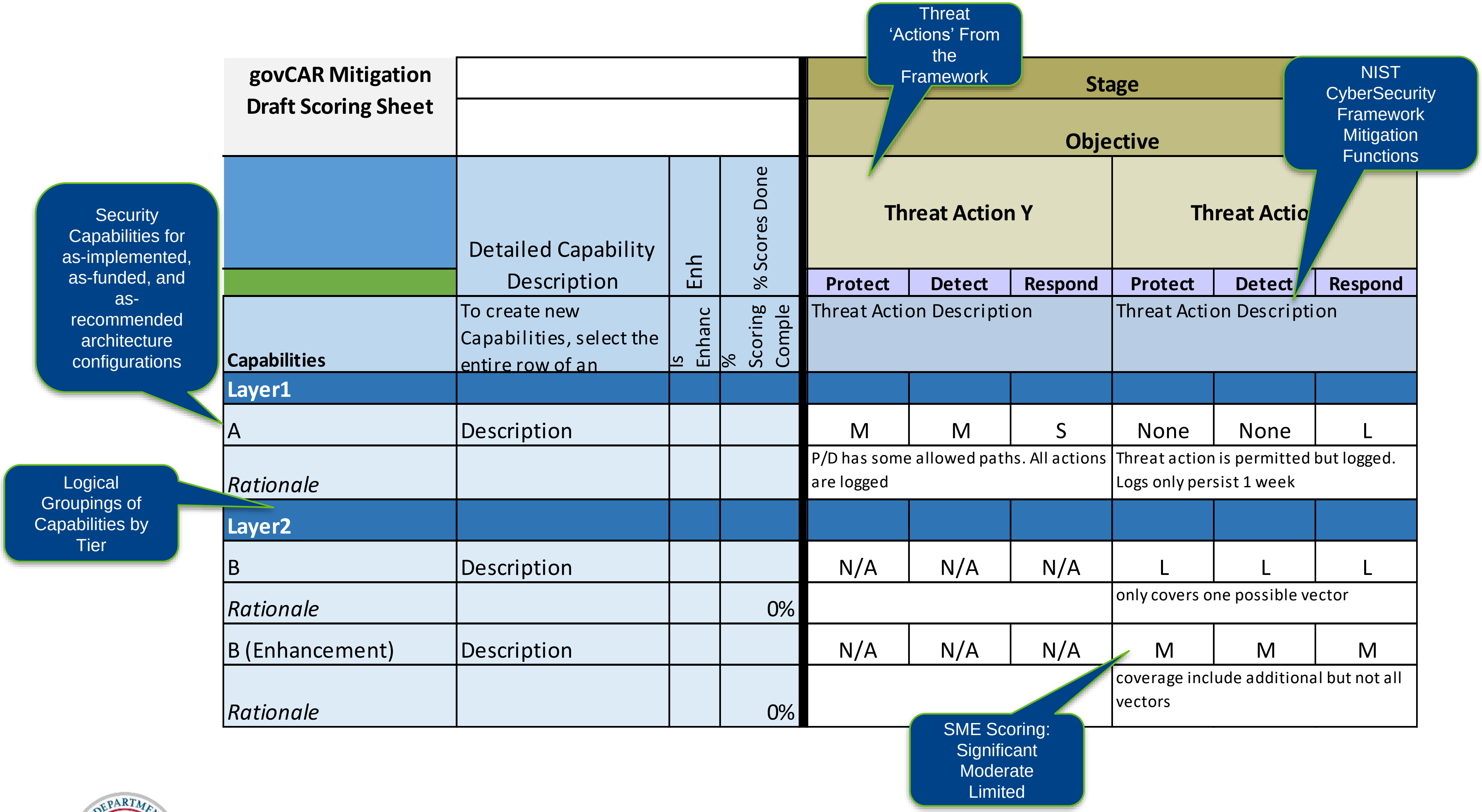
- Data alter

Architectures and Flows



*Mobile Device includes Unmanaged and Agency Managed Devices

Scoring



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		

Threat 'Actions' From the Framework

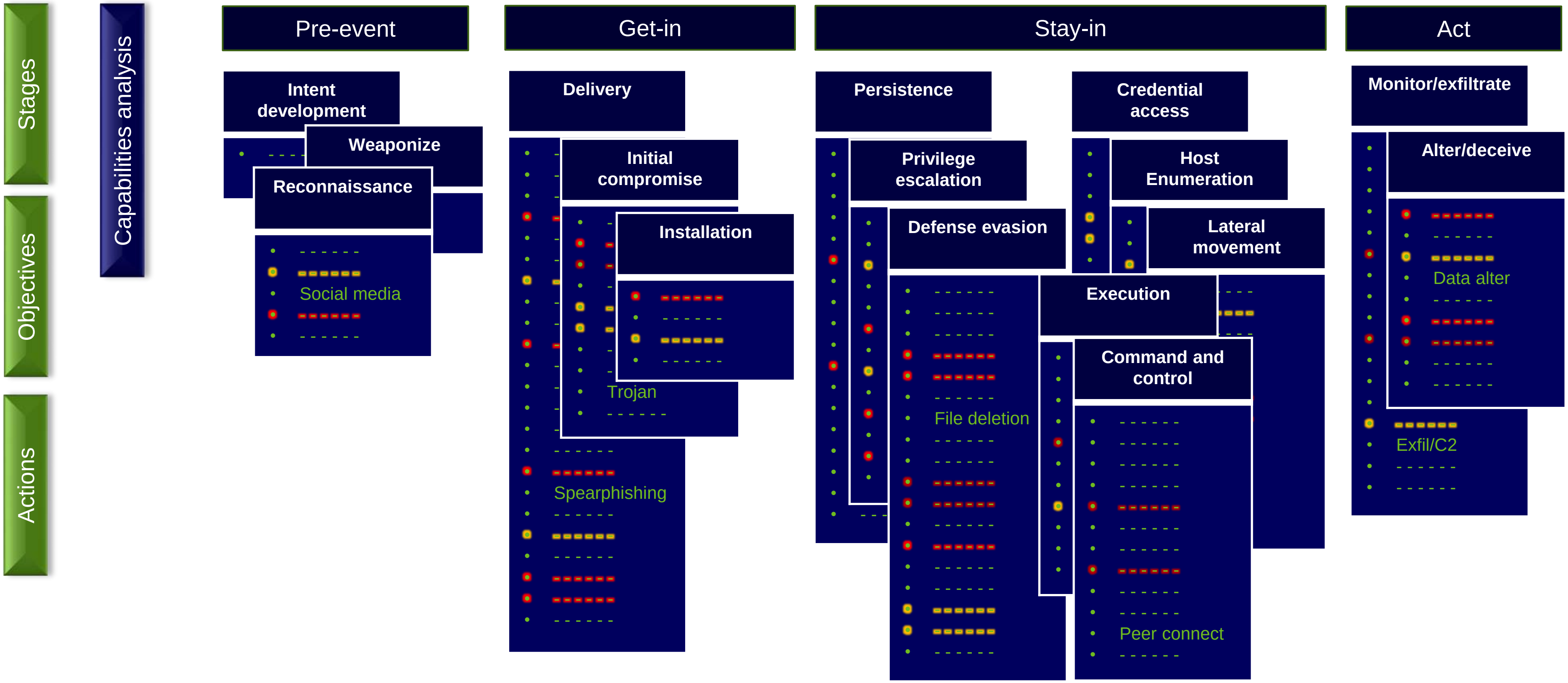
NIST CyberSecurity Framework Mitigation Functions

Security Capabilities for as-implemented, as-funded, and as-recommended architecture configurations

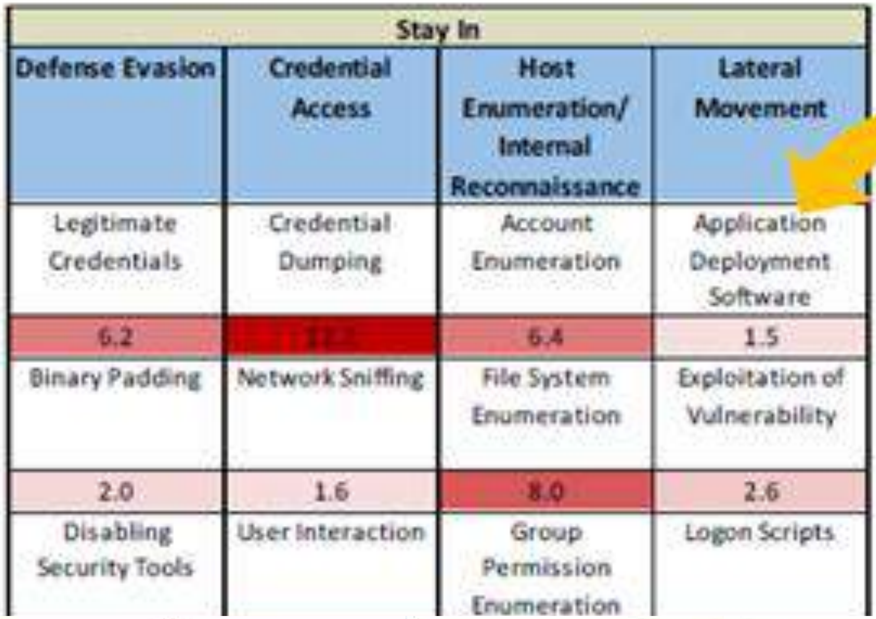
Logical Groupings of Capabilities by Tier

SME Scoring: Significant Moderate Limited

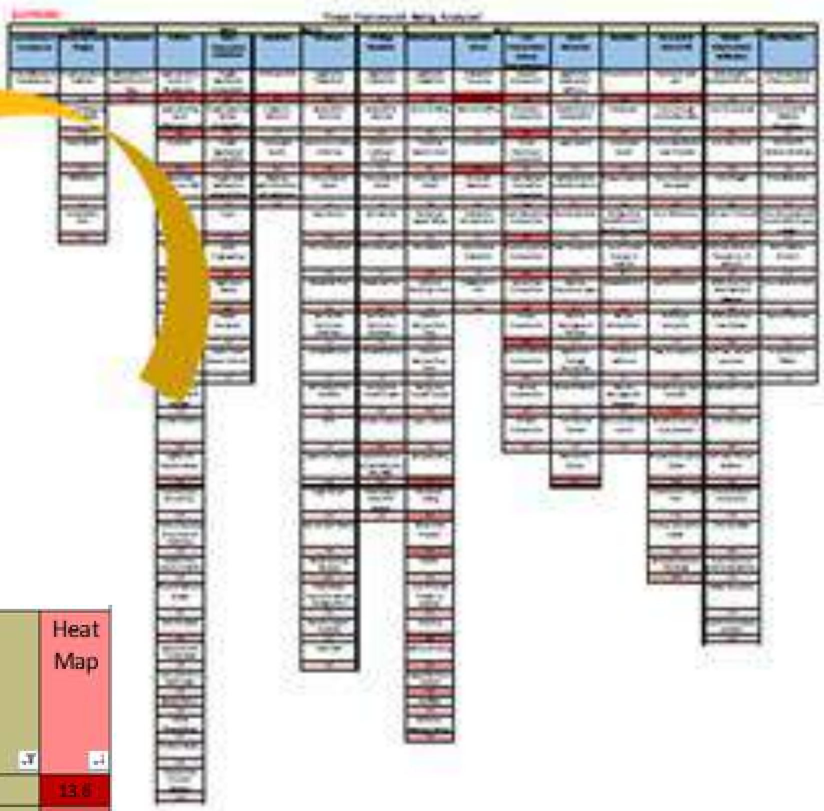
Coverage mapping

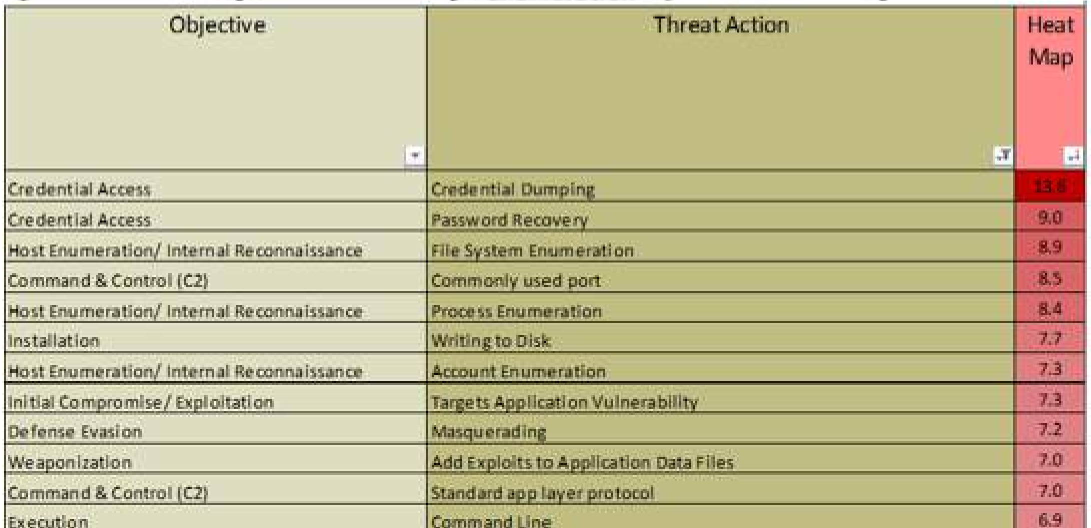


Threat heat mapping



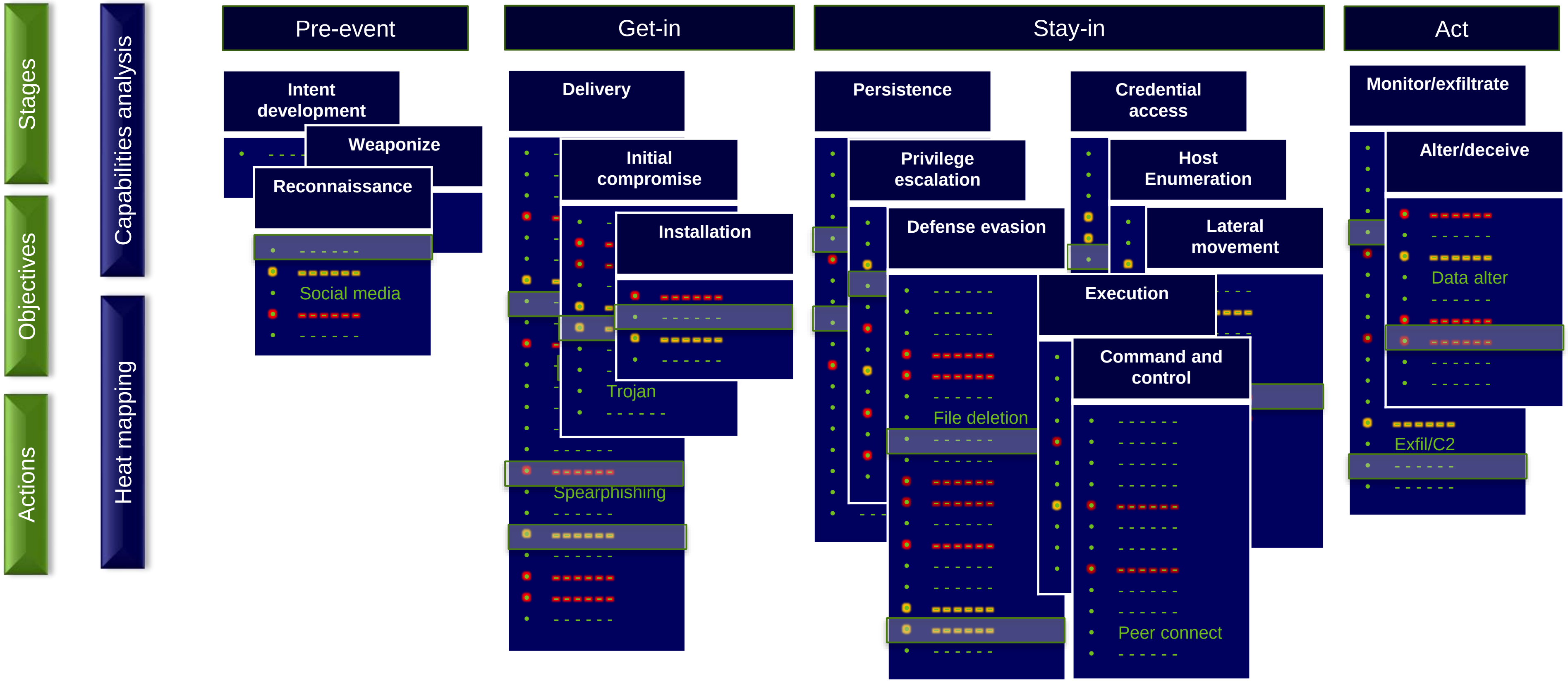
Stay In			
Defense Evasion	Credential Access	Host Enumeration/ Internal Reconnaissance	Lateral Movement
Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software
6.2	[illegible]	6.4	1.5
Binary Padding	Network Sniffing	File System Enumeration	Exploitation of Vulnerability
2.0	1.6	8.0	2.6
Disabling Security Tools	User Interaction	Group Permission Enumeration	Logon Scripts





Objective	Threat Action	Heat Map
Credential Access	Credential Dumping	13.6
Credential Access	Password Recovery	9.0
Host Enumeration/ Internal Reconnaissance	File System Enumeration	8.9
Command & Control (C2)	Commonly used port	8.5
Host Enumeration/ Internal Reconnaissance	Process Enumeration	8.4
Installation	Writing to Disk	7.7
Host Enumeration/ Internal Reconnaissance	Account Enumeration	7.3
Initial Compromise/ Exploitation	Targets Application Vulnerability	7.3
Defense Evasion	Masquerading	7.2
Weaponization	Add Exploits to Application Data Files	7.0
Command & Control (C2)	Standard app layer protocol	7.0
Execution	Command Line	6.9

Threat heat mapping



Stages

Objectives

Actions

Capabilities analysis

Heat mapping

Pre-event

Intent development

Weaponize

Reconnaissance

Social media

Get-in

Delivery

Initial compromise

Installation

Trojan

Spearphishing

Stay-in

Persistence

Privilege escalation

Defense evasion

File deletion

Credential access

Host Enumeration

Lateral movement

Execution

Command and control

Peer connect

Act

Monitor/exfiltrate

Alter/deceive

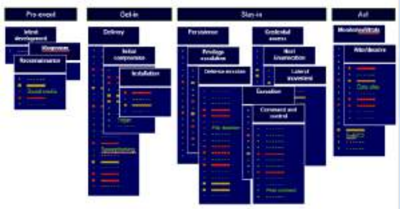
Data alter

Exfil/C2

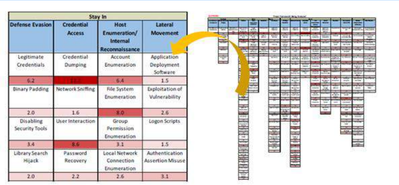
Methodology - recap

Threat Focus

Framework

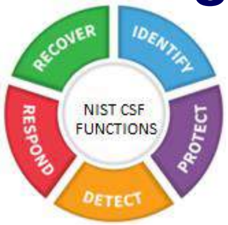


Heat_Map



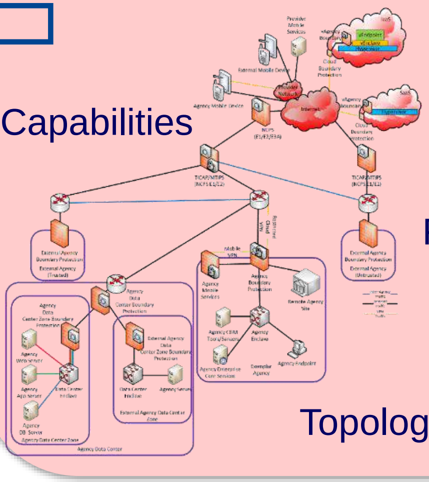
Stay In			
Defense Evasion	Credential Access	Host Enumeration/ Internal Reconnaissance	Lateral Movement
Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software
6.2	[illegible]	6.4	1.5
Binary Padding	Network Sniffing	File System Enumeration	Exploitation of Vulnerability
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

Scoring



Analysis

Architecture Focus



Recommendations
Affirmations
Observations

Notes

- Capabilities are deployed and used as intended. Scores to 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 agency.
- Threat actions are not linear.
- Vendor agnostic
- Does not provide impact analysis
- Does not delineate detailed implementation tradeoffs

Analysis to date

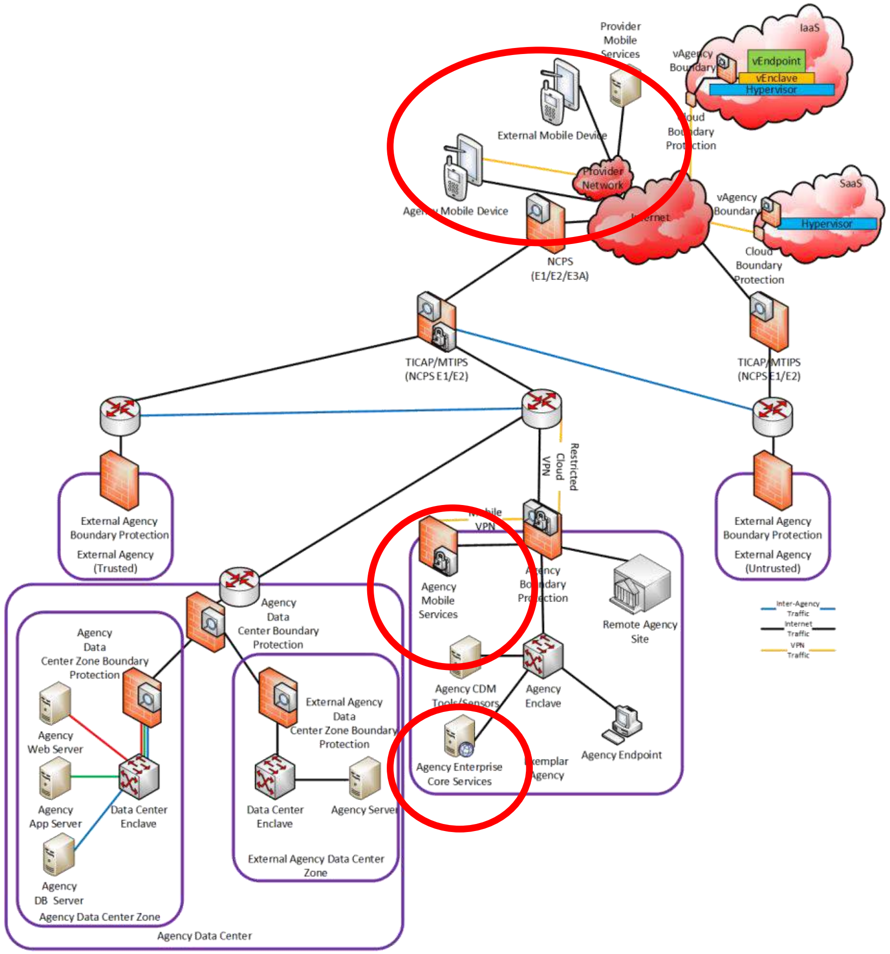
SPIN 1 - Score DHS provided cybersecurity services in the context of a typical large agency environment (NCPS and TIC).

SPIN 2 - Exemplar agency protections at boundary and endpoint

SPIN 3 – Cloud basic structures exemplar D/A protections for virtual data center (IaaS and SaaS)

SPIN 4 – Exemplar Agency Data Center

SPIN 5 – Mobile architecture



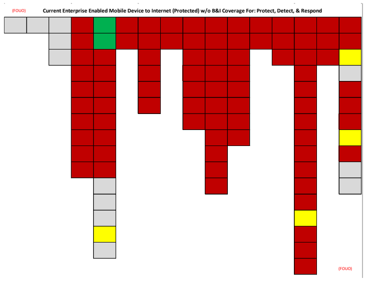
Worked Example - Mobile EE

Materiel

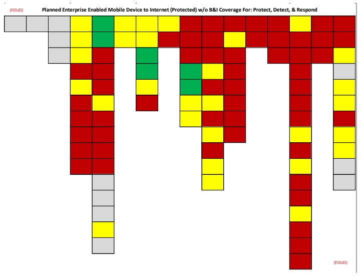
N/A
None
Limited
Moderate
Significant

Part 2

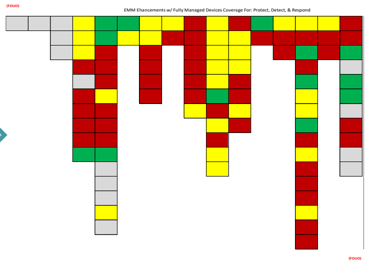
Current EE



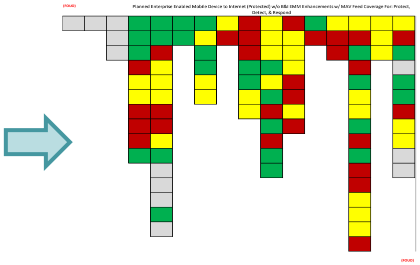
Planned EE



Planned EE Fully Managed



Planned EE w/ Integrated MAV



Configuration Control from EMM Provides Limited Mitigation

- MDM
- MAM with application blacklist
- MIM

Controlling apps via Enterprise App Store improves posture

- MDM
- MAM Enhancements with application blacklist
- MIM
- MAV
- MTD
- MDSE

Supervising device improves quality of Configuration Control

- MDM
- MAM Enhancements with application whitelist
- MIM / MAV/ MTD
- Fully Managed device

Tight integration with MAV improves quality of App Whitelisting Mitigations

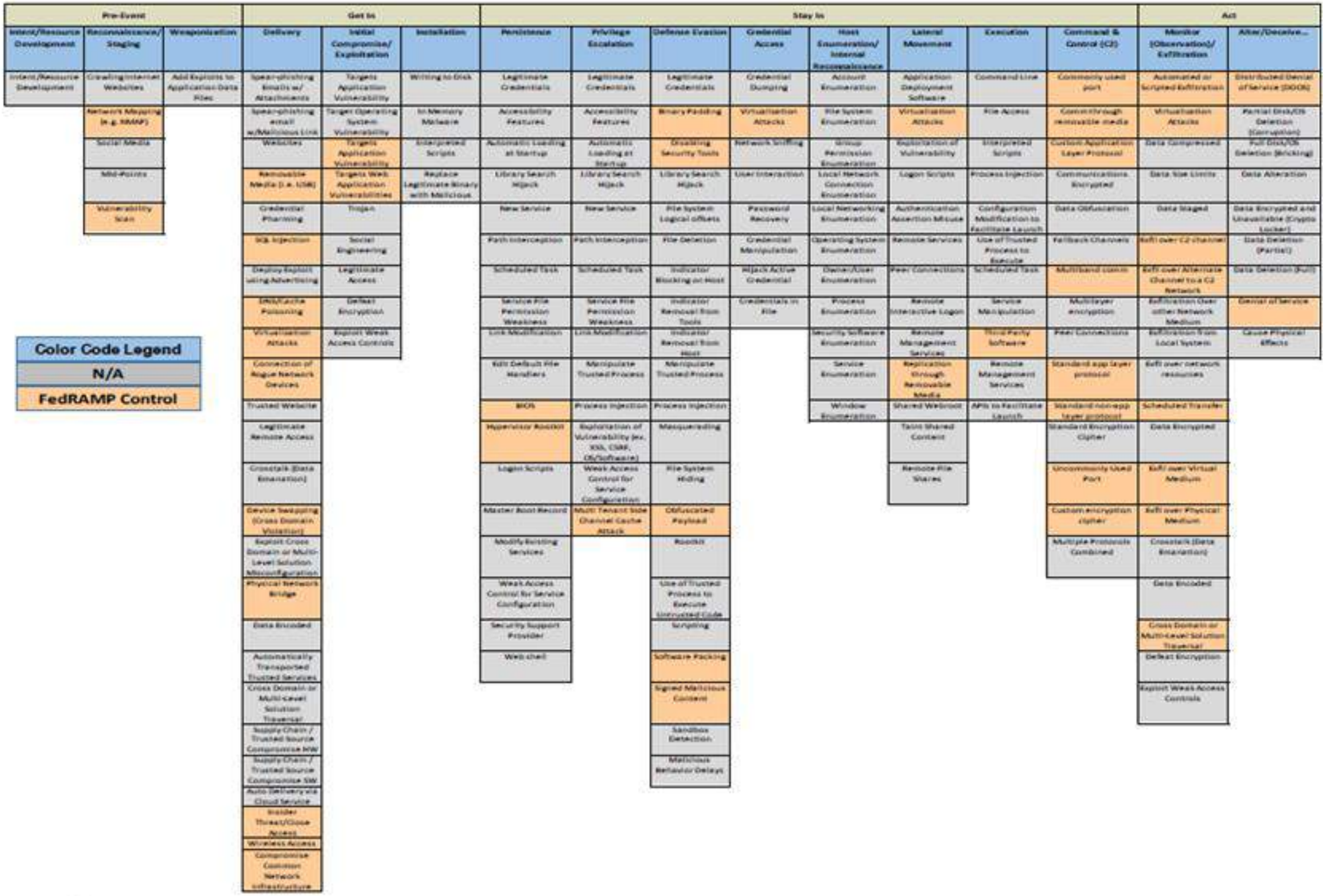
- MDM
- MAM Enhancements with application whitelist
- MIM
- MAV integrated with EMM

CISA
CYBER+INFRASTRUCTURE

Worked example – FedRAMP IaaS

Functional

Current Agency/Internet to IaaS UCLoud/RCloud CSP-Provided IaaS Only Coverage For: Protect, Detect, & Respond



Pre-Event			Get In		
Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/ Exploitation	Installation
Intent/Resource Development	Crawling Internet Websites	Add Exploits to Application Data Files	Spear-phishing Emails w/ Attachments	Targets Application Vulnerability	Writing to Disk
	🟧 Network Mapping (e.g. NMAP)		Spear-phishing email w/Malicious Link	Target Operating System Vulnerability	In Memory Malware
	Social Media		Websites	🟧 Targets Application Vulnerability	Interpreted Scripts
	Mid-Points		🟧 Removable Media (i.e. USB)	🟧 Targets Web Application Vulnerabilities	Replace Legitimate Binary with Malicious
	🟧 Vulnerability Scan		Credential Pharming	Trojan	
			🟧 SQL Injection	Social Engineering	
			Deploy Exploit using Advertising	Legitimate Access	
			🟧 DNS/Cache Poisoning	Default Encryption	
			🟧 Virtualization Attacks	Exploit Weak Access Controls	
			🟧 Connection of Rogue Network Devices		
			Trusted Website		
			Legitimate Remote Access		
			Crosstalk (Data Emanation)		
			🟧 Device Swapping (Cross Domain Violation)		
			Exploit Cross Domain or Multi-Level Solution Misconfiguration		
			🟧 Physical Network Bridge		
			Data Encoded		
			Automatically Transported Trusted Services		
			Cross Domain or Multi-Level Solution Traversal		
			Supply Chain / Trusted Source Compromise HW		
			Supply Chain / Trusted Source Compromise SW		
			Auto Delivery via Cloud Service		
			🟧 Insider Threat/Close Access		
			🟧 Wireless Access		
			🟧 Compromise Common Network Infrastructure		

Stay In			
Persistence	Privilege Escalation	Defense Evasion	Credential Access
Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping
Accessibility Features	Accessibility Features	🟧 Binary Padding	🟧 Virtualization Attacks
Automatic Loading at Startup	Automatic Loading at Startup	🟧 Disabling Security Tools	Network Sniffing
Library Search Hijack	Library Search Hijack	Library Search Hijack	User Interaction
New Service	New Service	File System Logical offsets	Password Recovery
Path Interception	Path Interception	File Deletion	Credential Manipulation
Scheduled Task	Scheduled Task	Indicator Blocking on Host	Hijack Active Credential
Service File Permission Weakness	Service File Permission Weakness	Indicator Removal from Tools	Credentials in File
Link Modification	Link Modification	Indicator Removal from Host	
Edit Default File Handlers	Manipulate Trusted Process	Manipulate Trusted Process	
🟧 BIOS	Process Injection	Process Injection	
🟧 Hypervisor Rootkit	Exploitation of Vulnerability (ex. XSS, CSRF, OS/Software)	Masquerading	
Login Scripts	Weak Access Control for Service Configuration	File System Hiding	
Master Boot Record	🟧 Multi Tenant Side Channel Cache Attack	🟧 Obfuscated Payload	
Modify Existing Services		Rootkit	
Weak Access Control for Service Configuration		Use of Trusted Process to Execute Untrusted Code	
Security Support Provider		Scripting	
Web shell		🟧 Software Packing	
		🟧 Signed Malicious Content	
		Sandbox Detection	
		Malicious Behavior Delays	

Stay In			
Host Enumeration/ Internal Reconnaissance	Lateral Movement	Execution	Command & Control (C2)
Account Enumeration	Application Deployment Software	Command Line	🟧 Commonly used port
File System Enumeration	🟧 Virtualization Attacks	File Access	🟧 Comm through removable media
Group Permission Enumeration	Exploitation of Vulnerability	Interpreted Scripts	🟧 Custom Application Layer Protocol
Local Network Connection Enumeration	Logon Scripts	Process Injection	Communications Encrypted
Local Networking Enumeration	Authentication Assertion Misuse	Configuration Modification to Facilitate Launch	Data Obfuscation
Operating System Enumeration	Remote Services	Use of Trusted Process to Execute	Fallback Channels
Owner/User Enumeration	Peer Connections	Scheduled Task	🟧 Multiband comm
Process Enumeration	Remote Interactive Logon	Service Manipulation	Multilayer encryption
Security Software Enumeration	Remote Management Services	🟧 Third Party Software	Peer Connections
Service Enumeration	🟧 Replication through Removable Media	Remote Management Services	🟧 Standard app layer protocol
Window Enumeration	Shared Webroot	APIs to Facilitate Launch	🟧 Standard non-app layer protocol
	Taint Shared Content		Standard Encryption Cipher
	Remote File Shares		🟧 Uncommonly Used Port
			🟧 Custom encryption cipher
			Multiple Protocols Combined

Act	
Monitor (Observation)/ Exfiltration	Alter/Deceive...
🟧 Automated or Scripted Exfiltration	🟧 Distributed Denial of Service (DDOS)
🟧 Virtualization Attacks	Partial Disk/OS Deletion (Corruption)
Data Compressed	Full Disk/OS Deletion (Bricking)
Data Size Limits	Data Alteration
Data Staged	Data Encrypted and Unavailable (Crypto Locker)
🟧 Exfil over C2 channel	Data Deletion (Partial)
🟧 Exfil over Alternate Channel to a C2 Network	Data Deletion (Full)
Exfiltration Over other Network Medium	🟧 Denial of Service
Exfiltration from Local System	Cause Physical Effects
Exfil over network resources	
🟧 Scheduled Transfer	
Data Encrypted	
🟧 Exfil over Virtual Medium	
🟧 Exfil over Physical Medium	
Crosstalk (Data Emanation)	
Data Encoded	
🟧 Cross Domain or Multi-Level Solution Traversal	
Defeat Encryption	
Exploit Weak Access Controls	

Color Code Legend
N/A
🟧 FedRAMP Control

Best from Spin 1-4

A value weighted by the strength and breadth of the capability with the threat importance is created. These individual values are combined across threat actions. Capabilities with the highest weighted value are considered best.

	Current	Future
1	Device Health Check Remediation	Auto Device Health Check Remediation
2	Application Whitelisting	Application Whitelisting
3	Device Health Check	NAC Enhancements
4	WAF/RWP w/ B&I	Device Health Check

.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

.govCAR and CDM

- Under the same management structure with a strong relationship:
- .govCAR provides operational recommendations for the CDM Program requirements
- CDM program uses .govCAR analysis in support of threat based mitigation approach.

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE