.govCAR TRAINING



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



Introductions

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



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

1999999999999999999999999



.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: Move to Stronger Risk Management

.govCAR

Cyber Hygiene

Compliance







Risk determination based on automated asset and account management

Threat-based Approach



Risk determination based on performance-based measures

Risk determination based on checklist



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.



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?



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



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

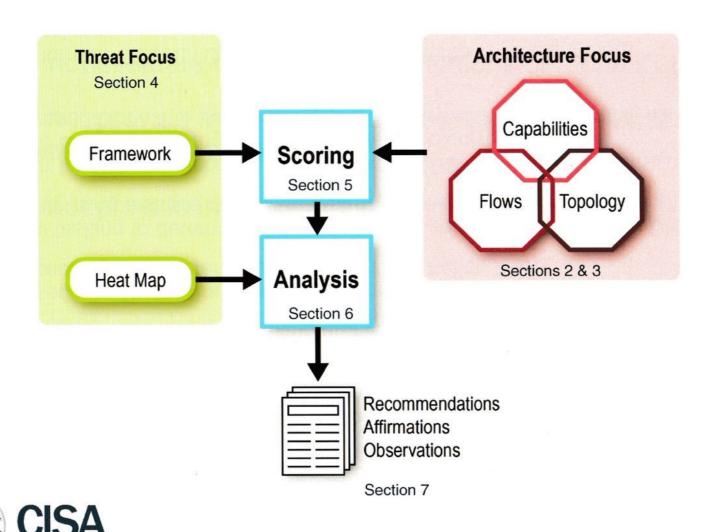


Impact of .govCAR

- 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

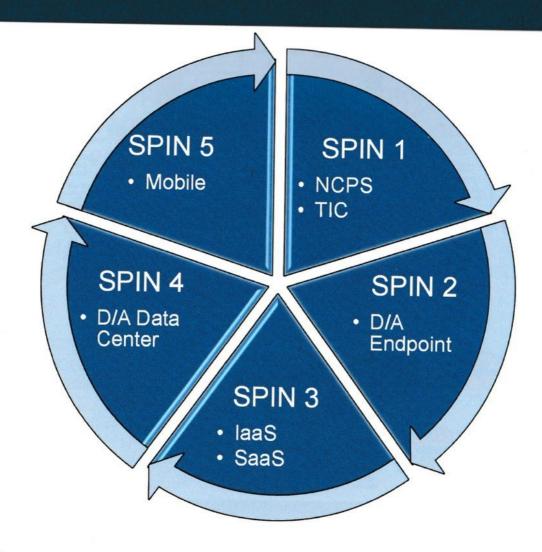


.govCAR Methodology



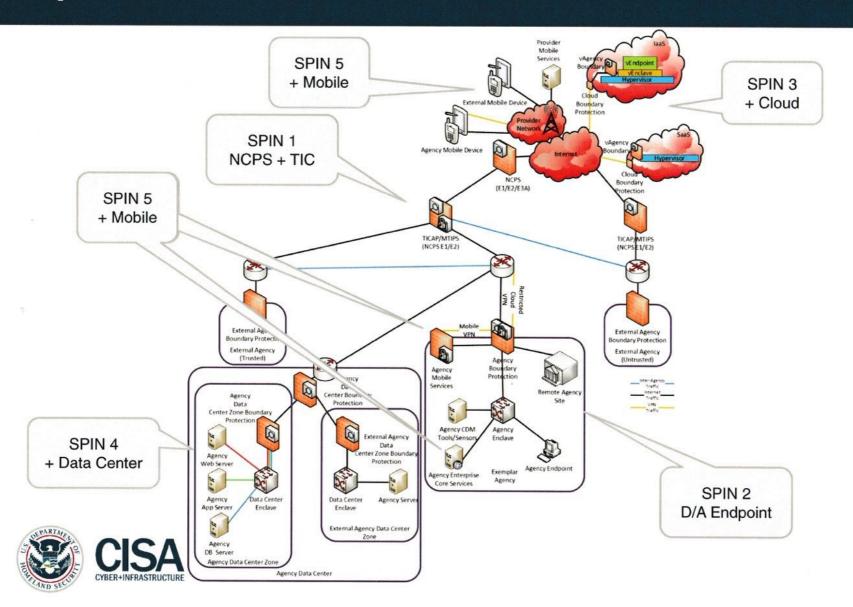


SPINs to date





Spin 1-5 Architecture View



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.



Deliverables

.gov Cybersecurity Architecture

Review (.govCAR)

Technical Annex

Version 5.0

December 19, 2018

For Official Use Only

Not to be Published





.gov Cybersecurity Architecture Review (.govCAR)

Spin 5 Summary and Findings

December 19, 2018

Version 1.0

For Official Use Only







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



FOLIO



Additional Materials

- Methodology Document
- Slick Sheets
- Fact Sheets

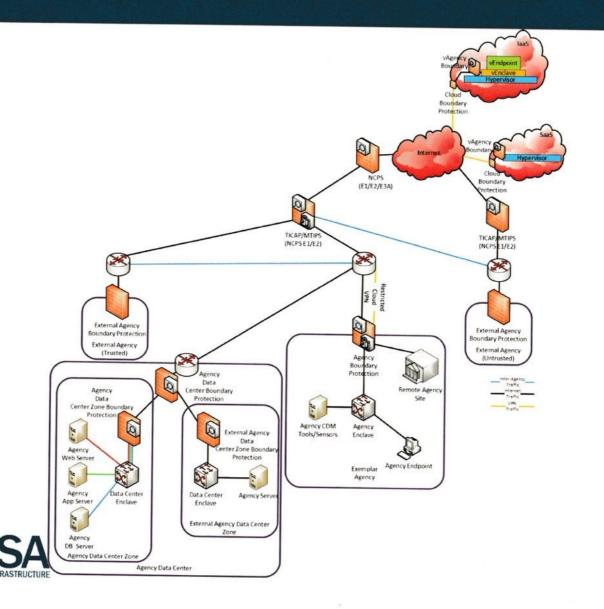


ARCHITECTURE UNDER ANALYSIS

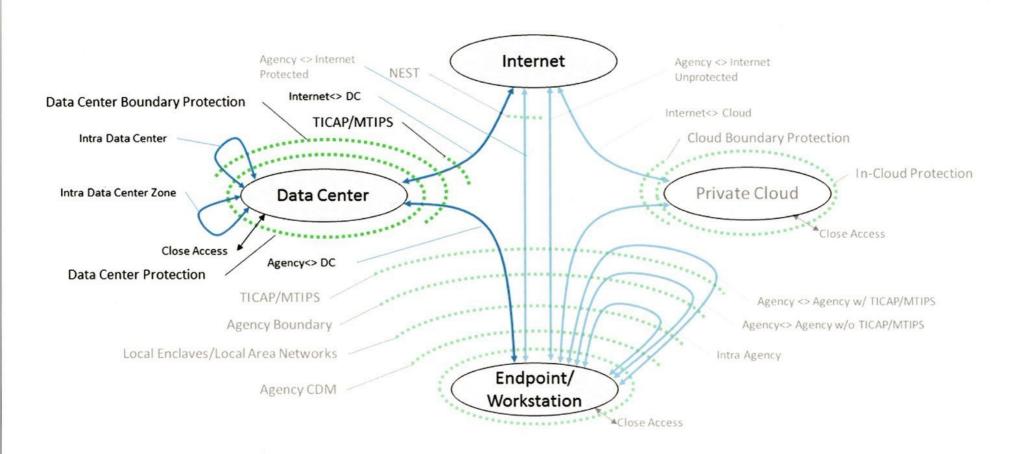
Kurt



Representative Architecture (Section 2)

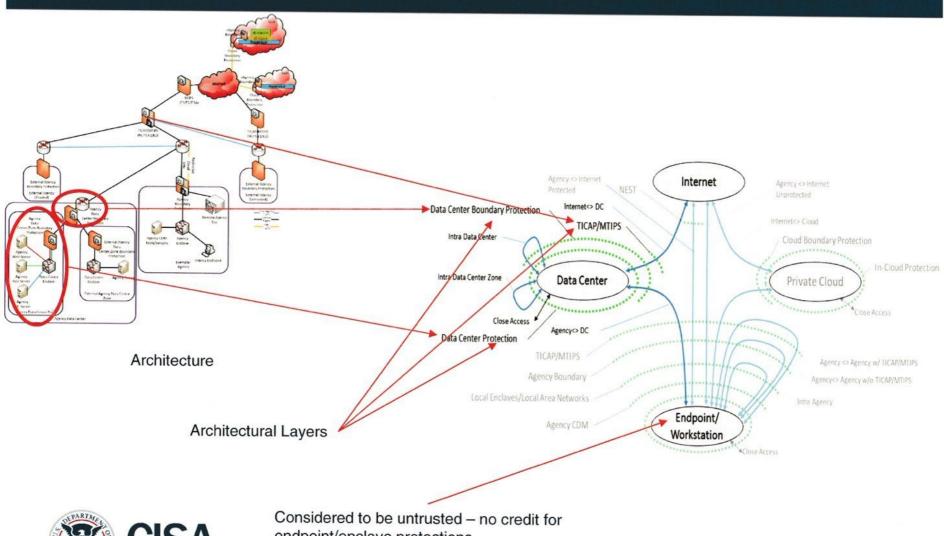


Data Center Data Flows (Section 3)





Spin 4 Architecture and Flows Relationship





endpoint/enclave protections

Capabilities (Section 3 and Appendix C)

TICAP/MTIPS	Spin	Description	n	Assu	mptions							
1												
Firewall TICAP/MTIPS 1,3 Deep Packet					t access to clear		Section 3 – List of capabilities in					
1		Inspection (DPI)		text traffic pay	load data	-	an architectural layer with an					
Firewall TICAP/MTIPS	Firewall TICAP/MTIPS 1,3 Adds QoS and fil				t access to clear	1	abbreviated capability description					
Enhancements	1225.06	reputation		text traffic pay	rload data							
Firewall TICAP/MTIPS w/ Break &	1,3			Scored with a	ccess to clear							
	Inspect (B&I)					*						
Firewall TICAP/MTIPS	e	Scored with a	cess to clear									
Enhancements w/ B&I		reputation		text traffic pay	load data							
Architectural Layer			TICAP,	/MTIPS Capabi		ICAP/MTIPS	Firewall Features					
Capabilities			Featur	e	Description							
			GeoIP	Blocking			dress is checked against a vendor supplied					
Appendix C – Detailed list and		_	901/09/03/05/05/05	/dest IP	Parameter district and the second second		d according to rules in the NGFW/IPS.					
description of the features of th	е						ent into GeoIP groups.					
architectural layer capabilities			Deep Packet Inspection is used to identify the application (e.g., Sky									
•	Applica	ation Filtering	being used in a session and supports filtering by application. Supports									
"Future" and "Enhancements" a	re par	t		2 7 1			ation. Supports blocking functions w/in					
of the "Planned" architecture	- 1				applications (e.g., file transfer w/in instant messaging).							
and the district and th		-		ol Port	TOWNS AND ADDRESS OF THE PARTY	Using Application Identification enforce that ports are only being used for						
			Enforc	ement	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

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



CISA CYBER+INFRASTRUCTUR

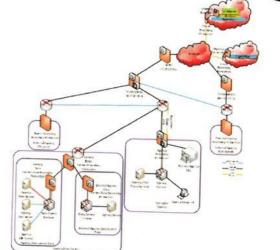
Current

Data Center Boundary Protection
Internet De Data Center Boundary Protection
Intra Data Center Zone
Intra Data Center Zone
Data Center Zone
Data Center Data Center Zone
Data Center Data Center Data Center Data Center
Data Center Data Center Zone
Data Center Data Center Data Center Data Center
Data Center D

Endpoint/

Workstation

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

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



THREAT METHODOLOGY

Ingrid



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

Weaponize Installation

Pre-Event

Intent/Resource

Development /

Reconnaissance/

Staging

Get-In

Delivery

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

ACTIONS

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



Stay-In Act Monitor / Persistence Exfiltration Privilege Initial Compromise/ Alter/Deceive Escalation Exploitation Defense Evasion Credential Access Host Enumeration/ Internal Recon Lateral Movement Execution Command & Control

NSA Adversary Lifecycle Threat Framework v2.0

eco Bankaran	Pre-Event	Proceedings of the Control of the Co		Get In			La Company								
Intent/Resource Reconnaissance/				Residence of the Control of the Cont	DESCRIPTION OF THE PARTY OF THE	The same of the same of	1	Ste	ay In						
Development Intent/Resource	Staging Crawling Internet	Wesponization	Delivery	Initial Compromise/ Exploitation	Installation	Persistence	Privilege Escalation	Orferes Evasion	Credential Access	Heat Enumeration/	Lateral Movement	fraculton	Command & Control	Monttor	Act
Development	Websites	Add Exploits to Application Data Files	Spear-phishing Emails w/ Attachments		Writing to Disk		Sample of the State of State o	R SINGSPINGS CONCESSION		Reconnelsance			(C2)	(Observation)/	Aher/Deceive
	Network Mapping (e.g.		Spear-phishing email	Vulnerability Target Operating		Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deploymen				
	NMAP)	1	w/Malicious Link	System Vulnerability	In Memory Malware	Accessibility Features	Accessibility Features	Binary Padding	Virtualization Attacks		Software	Command Line	Commonly used port	Automated or Scriptor Exfiltration	d Distributed Denial : Service (DDOS)
	Social Media		Websites	Targets Application	2220 9394290	Automatic Loading at			THE PERSON ASSESSED.	Enumeration	Virtualization Attacks	file Access	Comm through removable media	Virtualization Attacks	
				Vulnerability Remotely	Interpreted Scripts	Startup	Automatic Loading at Startup	Disabling Security Tools	Network Sniffing	Group Permission	Exploitation of		- 1000000000000000000000000000000000000		(corruption)
	Mid-Points		Removable Media (i.e.	Forgote Web-	Replace legitimate					Enumeration	Vulnerability	Interpreted Scripts	Custom Application Layer Protocol	Data Compressed	Full disk/OS delette
	27.045.050.050		USB)	Vulnorabilities (on XFE, CSRF, EQL)	binary with Malicious (ex: Havex)	Library Search Hijack	Ubrary Search Hijack	Library Search Hijack	User Interaction	Local Network Connection Enumeration	Logon Scripts	Process Injection	Communications Encrypted	Data Size limits	(bricking)
	Vulnerability Scan		Credential Pharming	Trojan		New Service		File System Logical				1000000	Encrypted	0.0000000000000000000000000000000000000	Data Autoration
			ECL Injection	Social Engineering		Path interception	New Service	Offsets	Password Recovery	Local Networking Enumeration	Authentication Assertion Misuse	Configuration Modification to Facilitate Launch	Data Obfuscation	Data Staged	Data Encrypted and Unavailable (Crypte
			Application or Operating System			rain interception	Path interception	File Deletion	Credential Manipulation	Local Network Enumeration	Remote Services	Use of Trusted Process to Execute Untrusted Code	Fallback Channels	Exfit over C2 channel	Locker) Data Deletion (Partie
			Exploit over the Network Web Application	Logitimate 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)
			Exploit over the Network Deploy Exploit using	Defeat Encryption Exploit Weak Access		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	Denial of Service
		1	Advertising	Controls		Unk Modification	Unk Modification	Indicator Removal from Host		Process Enumeration	Remote Management			Network Medium	Cental of Service
			DNS/Cache Poisoning			Edit Default File	Manipulate Trusted	Manipulate Trusted	1	Security Software	Services	Third Party Software	Peer Connections	Exfiltration from Local System	Cause Physical Effect
Lage	nd:	1	Virtualization Attacks			Handlers	Process	Process		Enumeration	Replication through removable media	Remote Management Services	Standard app layer	Exfil over network	
910000000000000000000000000000000000000		-	Total Strong Actacks		\ \	BIOS	Process Injection	Process Injection	1	Service Enumeration			protocol	resources	
	Deprecated in govCAR Spin 4		Connection of Rogue		1		Exploitation of			strice thumeration	Shared Webroot	APIS to Facilitate Launch	Standard non-app layer protocol	Scheduled Transfer	
	govCAR spin 4	-	Network Devices			Install Hypervisor Rootkit	Vulnerability (ex. XSS, CSRF, OS/Software)	Masquerading		Window Enumeration	Taint Shared Content		Standard Encryption Cipher	Data Encrypted	
	modifications	-	Trusted Website Legitimate Remote			Modify Service Configuration	Weak Access Control for Service Configuration	File System Hiding	,		Remote File Shares		Uncommonly Used Port	Exfli over Virtual	
			Access			Master Boot Record	Multi Tenant Side Channel Cache Attack	Obfuscated Payload						Medium	1
		- 1	Crosstalk (Data				Committee Cache Actack						Custom encryption cipher	Exfil over Physical	į .
			Emanation)			Modify Existing Services		Rootkit					Cipian	Medium	i
		ŀ	Device Swapping (Cross Domain Violation)					Use of Trusted Process					Multiple Protocols Combined	Crosstalk (Data Emanation)	
13			ixploit Cross Domain or			Logon Scripts		to Execute Untrusted Code					C2 via Cloud Service	Data Encoded	
			Multi-Level Solution Misconfiguration		1	Security Support		40.0							
	P	hysical Network Bridge			Provider		Scripting						Cross Domain or Multi- Level Solution Traversal		
	- F			L	Web Shell		Software Packing					1			
		-	Data Encoded				1	Signed Malicious					1	Defeat Encryption	
		- 1	Automatically				-	Content					1	Exploit Weak Access	
			Transported Trusted Services				- 1	Sandbox Detection					ŀ	Controls	
		-	341744				- 1	Juneoux Detection						Exfit via Cloud Service	
		c	ross Domain or Multi-				ł						1	via Ciona Sechice	
		16	evel Solution Traversal				- 1	Malicious Behavior					L		
	-	upply Chain / Trusted					Delays								



- * 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)

Reading a threat description

Think like the adversary

Initial Compromise/	Troian	victim computer within a victim's network to gain personal	
Exploitation		victim computer within a victim's network to gain personal policy/2011/02/a	speaks-the-inside-story-of-the-
Zaprorudon		malware (trojans) via remote access trojans (RATs).	hbgary-hack/3/

Attacks are broken apart across the framework...



Intent/Resource Development : Intent/Resource Development



Weaponization : Add Exploits to Application Data Files



Delivery : Spearphishing Emails w/ Attachments



Initial Compromise/ Exploitation : Trojan



Command & Control (C2): Commonly used port

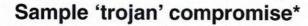


Lateral Movement : Remote File Shares



Defense Evasion : Indicator Removal from Host

Potential actions after compromise



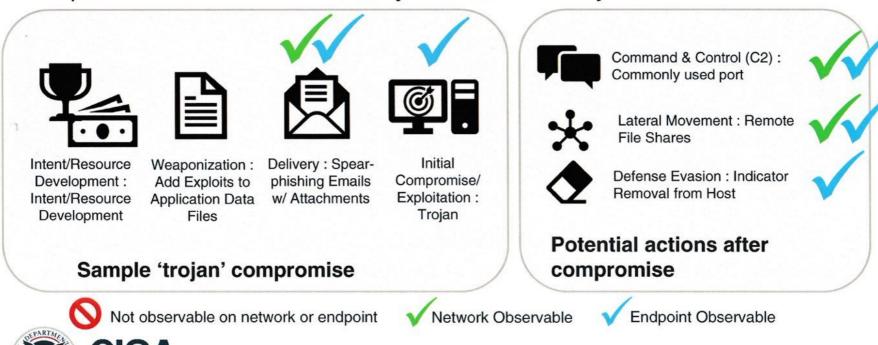


CISA

* 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



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

用版图2 图10 0字	(u//rout	9					Threat	Framewor	k Being An	alyzed									
		y In	Lateral	Section 2	Park Indian	1	-	=		-	==		=	=	=	-	Consult Consult	-	-
Defense Evasion	Credential	Host		Territoria	Sapley Horse Waltering	APPENDENCE Appropriate two	Spenyshalog Study of Analysis	Appropriate and the second sec	wenterin	- represent	(mprops	(agricult	Comment Company	Brast Succession	April 100 to 100	interpretation of the last of	Generally and	Arrest -	Parties of
	Access	Enumeration/	Movement	Contract of the last of the la	-	-	-	Terger dervering	Statement .	R modern, registers	Average (and the same	********	Parameter Street	Barren or a	******	- Committee	Tara Compression	Aphyrib face Samp
		Internal			in grown	1	-	Agent aller Schoolste	territo.	alteria	Antonios Caetinge Voltage	Britania Printerior	ARTHURN	Automore Statements	1 de puer	6-91	Total Property	Seatta men.	terms 8
		Reconnaissance			Mercen		T-100	Spinor Spinor	****	Mari .	Object Storm	(April back	April 1	Indiana.		-	To take	Territogra 8.0	No. Bo
Legitimate	Credential	Account	Application		18 September September		1	-				Helyson Light there	Signature Margaritation	Trumpiers		indports management management	-	Ball ner II rame	Paris Server Insurance Lands
Credentials	Dumping	Enumeration	Deployment		14	3	-	Marine Na	1			Alta Serianna	-	Service of the last	11	Use of Females American	What Denni	Carlot Service Characteristic	Tele-bill Parts
			Software				3	- Marrier		Patricks pro	Parties per	****	Combuman on Ann	Own to a		District Co.	William Inc.	Intrace in one black	fore leaves
6.2	12.2	6.4	1.5				ī	To years	1	Andrews	AL STATE OF THE PARTY OF THE PA	- 13 - 10 de - 10 de - 10 de	- 10	- MA	-			Manufacture Language	
SHALL BEET THE SEASON BLOW								Topics Rope British Street	1			11		Townson	-	No.	Ann Carrie State	Office of the last	(marks
Binary Padding	Network Sniffing	File System	Exploitation of			4	1	18	4	18 1817/mb/cf file Spiders	- LE - Taranta - Taranta	15		- 13 - 10-10 - 10-10-10	12	-	Tentral services	Literatur Novelo	- 18
		Enumeration	Vulnerability				20 m			83.	Faces having			- U	ton Bass Great	en unturina lamb	10		
		DISTRIBUTE ON THE DESCRIPTION OF THE PERSON					Lagranian Service Scine			-	Santana o Santana o Santana o Santana o	-		- 14	Samuel Villa Vision	1		let are There	
2.0	1.6	8.0	2.6				Therefore			Light School	Secretary Secretary	Title Lateral Maring			Mark Charles			(Partier)	
Disabling	User Interaction	Group	Logon Scripts				10 00 - 00 00 - 00 00 00 - 00 00 - 00	-		15	- 15	Marian Terran					15	- Next - see	
Security Tools		Permission					ine and			Maritime of Maritime (Maritime)		-					Security Common	On house of	
400.0000.0000.0000000000000000000000000		Enumeration						1		Gertament Gertament		Sales of Persons Sales of Sales of Sales of Sales of						father for salter	
3.4	8.6	3.1	1.5				44			SE SENTENCE OF THE PROPERTY OF		84						ietos.	
Library Search	Password	Local Network	Authentication				Library Company of the Company of th	-		11	1	Egrani State on (parameter and the state of the state of the state of							
Hijack	Recovery	Connection	Assertion Misuse				Andreita 13	-				Marine Marine							
•		Enumeration										33							
2.0	2.2	2.6	3.1				Companies Comman Mercant												



SCORING

Pete



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



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.)

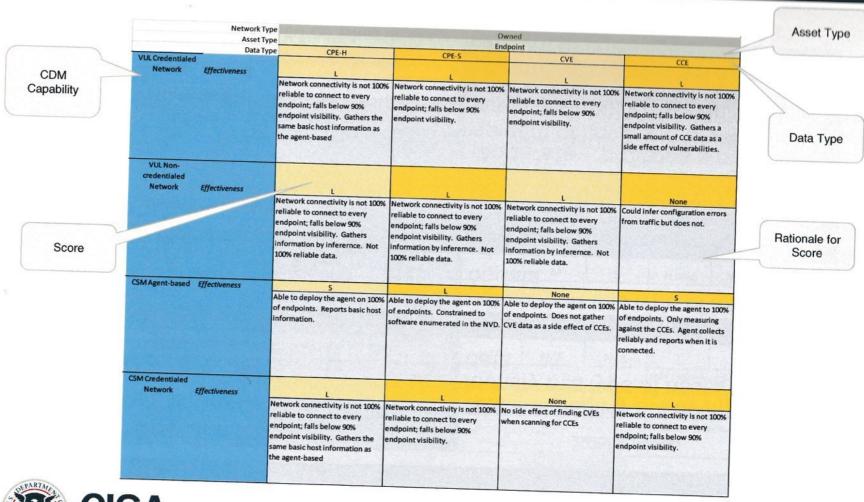


Identify -Additional Details

- 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.



Identify Scoring Spreadsheet





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 securityrelated 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%



Protect, Detect, Respond (PDR) Scoring Spreadsheet

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

Logical Groupings of Capabilities by Architectural Layer

govCAR Mitigation					from the Framework	Tonas dad	age		26. 化自然温度	
Draft Scoring Sheet					6-14		ective		NIST CyberSe Framework Mit Functions (sect	tigati
	Detailed Capability	% Scores Done	Th	reat Actio	n Y	Threat Actio				
THE EXECUTION OF STREET	Description	Enh	The second second	Protect	Detect	Respond	Protect	Detect	Respond	
Capabilities	To create new Capabilities, select the entire row of an	Is Enhanc	% Scoring Comple	Threat Acti	on Descript	ion	Threat Acti	on Descrip	otion	
Layer1						4.77				
A	Description		Codes (A)	М	М	S	None	None	L	
Rationale	Estreti Didag			P/D has some are logged	e allowed pat	hs. All actions	Threat action Logs only per		d but logged.	
Layer2						Same to				
В	Description			N/A	N/A	N/A	L	L	L	
Rationale	Managera an 15		0%		in .	*	only covers o	ne possible	vector	
B (Enhancement)	Description			N/A	N/A	N/A	М	М	М	
Rationale	000000000000000000000000000000000000000		0%			//	coverage inc vectors	lude additio	nal but not all	
					Soore bo	. 7				



Score based on rubric (section 5.1.1)

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 nonmateriel 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).



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



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 laaS 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



How Analysis Uses Capability Scores

- Understand Threat coverage:
 - What is the net effect of moving from a government or contractorowned/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



PDR Analysis: Capability Sets

	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		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		
	3	W/0	W/W	clav		3	3	3	clay	_	l
	ğ	re.	auc	E	Current Agency Server w/o B&I	ter	ter	ou o	ü	Planned Agency Server w/o B&I	ı
	ő	5	ž	ter	0	ő	Le C	r Z	ter	0/1	ı
	3	3	nte	ő	3	ats	ţ	at c	ő	5	ı
	å	å	S	ata	2	0	ä	ů	ata	ž	ı
	#	1 8	ata	ě.	s v	f 5	, tc	at a	٥_	y 8	ı
	Ĕ	i i	9-6	B&I	in in	Ę	ou a	ě	enc B&	ou o	ı
	할	A	12	Current Agency Server w/o B&I	Age	12	Ag	2	Planned Agency Server w/o B&I	Ag	l
	ž	ig i	2	2 2	a t	pac	pec	Pac	por s	pac	ı
	Ę	1 5	Ę	F 5	E	È	è	č	a v	an a	١
	ŭ	ŭ	ŭ	บีดี	ű	ā	ā	ā	P S	ā	ı
											ı
TIC											1
DC:Firewall current TICAP	1								- 8		1
DC:Firewall Enhancements TICAP						1					1
DC:Passive Sensor	1					1					1
Data Center Boundary					100		13		1		1
DC:IP Blacklist	1	1				1	1				1
DC:DDoS Mitigation	1	1		-		1	1		\vdash		1
DCACLs	1	1		\vdash		1	1				1
Data Center Zone Boundary					100			18.00			d
DC:Next GenFirewall w/o B&I	1	1	1			1	1	1			١
DCPassive Sensor	1	1	Y			1	1	-			1
DCDLP in Motion w/ B&I	1	1				1	1				1
DC. AF/RWP w/ B&I	1	1									Ŕ
DCWAF/RWF Wy was consenses the control		H			_		-				1
DCID Federation/RBAC/MFA	1	1				1	1				1
DC:DBFW w/B&I			1		-			1			1
DC:DBAM w/B&I			1					1			
Data Center Enclave			22				187		1026		I
DC:Anomalous Net Behavior Detection (future)	г					1	1	1	1		1
DC:Network Segmentation	1	1	1	1		1	1	1	1		1
DC:Network Access Control (NAC)	1	1	1	1				1			1
DC:NAC Enhancements Combined						1	1	1	1		1
Agency Server							1000				
DC:Device Control (CSM)	1	1	1	1	1	1	1	1	1	1	٦
DC:File Integrity	1	1	1	1	1	1	1	1	1	1	1
DC:Device Health Check	1	1	1	1	1	1	1	1	1	1	1
DC:Device Health Check Remediation	1	1	1	1	1						
DC:Auto Dev Health Check Remed (Future)						1	1	1	1	1	1
DC:Reputation (future)						1	1	1	1	1	1
DC:Whitelisting (SWAM)	1	1	1	1	1	1	1	1	1	1	
DC:Host IPS/FW	1	1	1	1	1	1	1	1	1	1	1



- 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

	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&l	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
TIC										
DC:Firewall current TICAP	1		2000					guiran		
DC:Firewall Enhancements TICAP					- Vallage	1				
DC:Passive Sensor	1					1				
Data Center Boundary					486					
DC:IP Blacklist	1	1				1	1			
DC:DDoS Mitigation	1	1	-			1	1			
DC:ACLs	1	1				1	1			
Data Center Zone Boundary			18/9	NAME OF						
DC:Next GenFirewall w/o B&I	1	1	1			1	1	1	January 1	
DC:Passive Sensor	1	1				1	1		Contract of the Contract of th	This see
DC:DLP in Motion w/ B&I	1	1			100	1	1			
DC:WAF/RWP w/ B&I	1	1								

PDR Score Roll-Up Calculation

	AR Mitigation Draft Scoring Sheet			Wo Street Pool State of Company of the Street	age ective						
		TI	hreat Actio	n Y	Threat Action Z						
		Protect	Detect	Respond	Protect	Detect	Respond				
	Capabilities	Threa	Action Descr	ription	Threa	at Action Descr	iption				
Set	Layer 1										
1	A	L	N/A	L	М	None	NA				
1	В	L	None	L	1	None	M				
	Layer 2					None	L				
1	С	L	None	S	S		S				
1	D	N/A	N/A	N/A	N/A	N/A					
1	E	None	None	М	None	None	N/A M				
	Capabilities Set 1	L	None	S	S	L	S				
	P/D/R RollUp		S			S					

Maximum score for Protect is Limited (L)

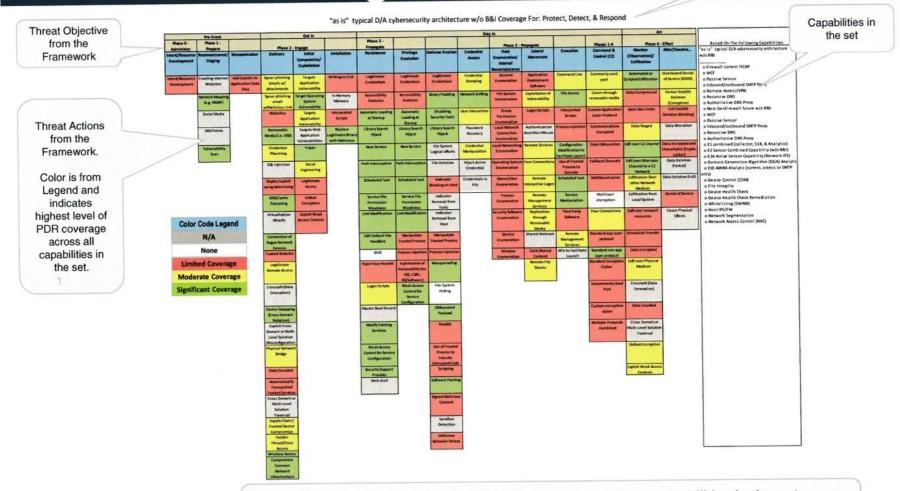
Maximum score for Protect, Detect and Respond is Significant (S)



PDR Analysis: Aggregating the Scores -

Threat Coverage Roll-Up

Title of set and list of PDR functions





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

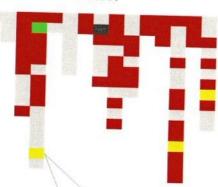
Goal is not to turn it all green, but to identify opportunities for improvement.

Unclassified//For Official Use Only

Mitigation by Protect, Detect and Respond

CSF Function Title of set (FOUO) Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I

Protect



Threat Actions from the Framework.

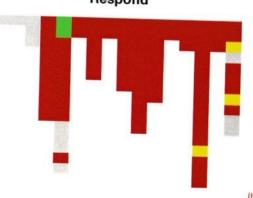
Color is from Legend and indicates highest level of PDR coverage across all capabilities in the set.

Detect



Each column represents one Threat Objective from the Framework

Respond

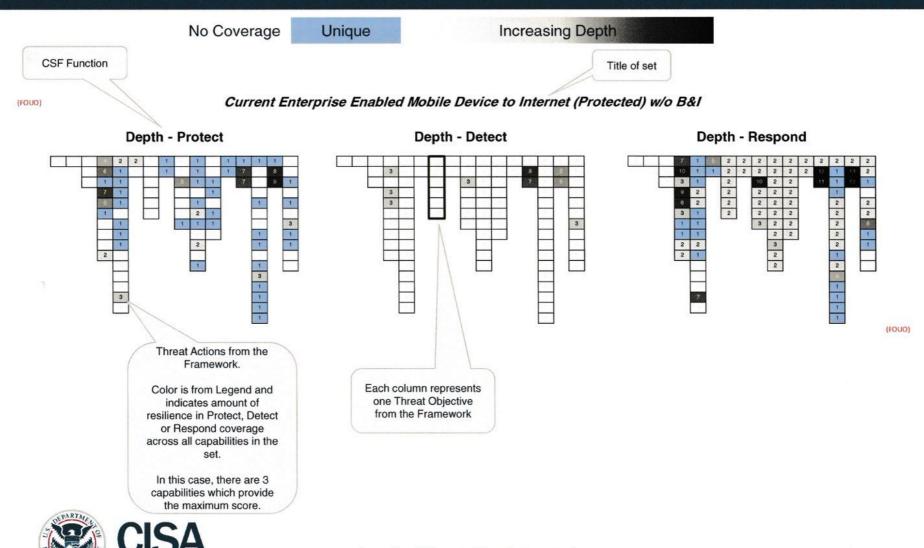


(FOUO)

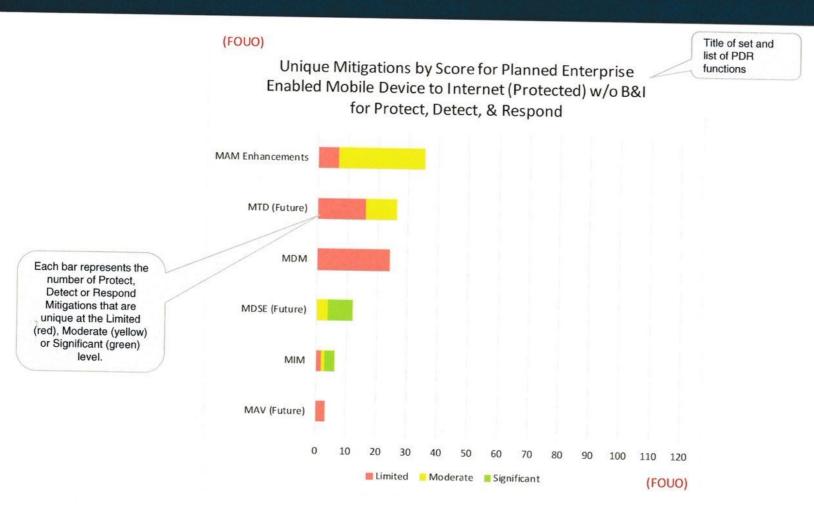
Limited Moderate Significant

Unclassified//For Official Use Only

Resilience in Maximum Mitigation



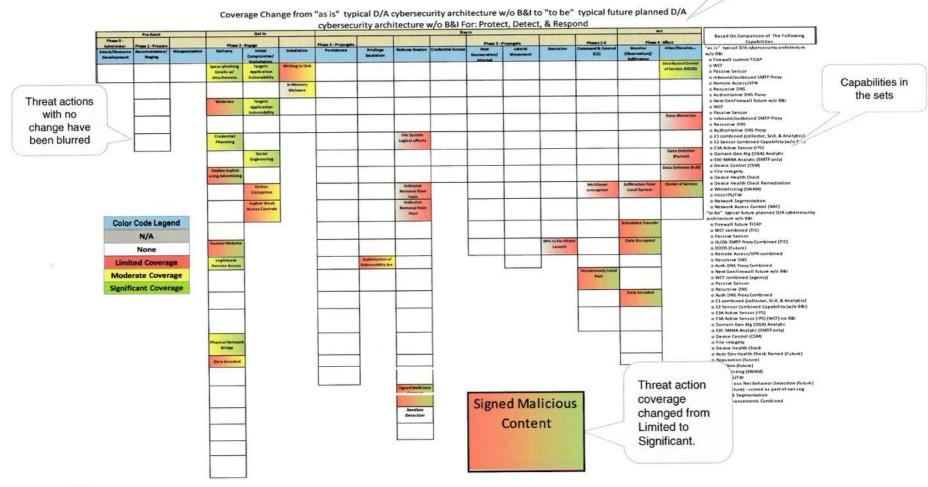
Unique Bar Chart





PDR Analysis: Comparing Sets with Coverage Map

Capability sets being compared with PDR functions listed





aaaaaaaaaaaaaaaaaaaaa

PDR Analysis: Incorporating Threat Heat Map Data

Threat Objective	Objective	Threat Action	Heat Map	Heat Map	The state of the s	Compare	All Capabilities "as is" typical D/A cybersecurity architecture w/o B&I	All Capabilities "to be" typical future planned D/A cybersecurit architecture w/c B&I	d mc	Capability or Capability Set
	Intent/Resource Development	Intent/Resource Development		40						
	Intent/Resource Development	Intent/Resource Development		4.0	Protect	-	N/A	N/A		
Chunch A. H.	Intent/Resource Development	Intent/Resource Development		4.0	Detect Respond		L	L		
Threat Action	Dalisons	Space phighing Frontier (Ass.)								
	Delivery	Spear-phishing Emails w/ Attachments	0.0000000000000000000000000000000000000	7.1	Protect	~	М	S		
	Delivery	Spear-phishing Emails w/ Attachments		7.1	Detect	~	М	S	P	Rollup Score fo
	Delivery	Spear-phisis W/ Attachments		7.1	Respond	~	М	S	A	"Detect" function
	Delivery	Spear-phishing email w/Malicious Link		6.6	Protect	-	м	м	_	across all
Heat map score	I	Spear-phishing email w/Malicious Link	Secretary of the second	6.6	Detect		м	М		capabilities in set
for the threat	Delivery Delivery	Spear-phishing email w/Malicious Link		6.6	Respond		м	M		oupabilities ill se
action	Delivery	Websites		5.7	Protect	~	L	S		
	Delivery	Websites		5.7	Detect	~	L	М	<u></u>	
	Initial Compromise/ Exploitation	Websites		5.7	Respond	~	L	S	A	
	Initial Compromise/ Exploitation	Trojan		4.9	Protect	000	S	S	-	D:"
	ALCOHOLOGICAL CONTRACTOR CONTRACT	Trojan	3000	4.9	Detect		L	L		Difference between
	Initial Compromise/ Exploitation	Trojan		4.9	Respond		S	S		the capabilities of
	Initial Compromise/ Exploitation	Legitimate Access		4.9	Protect		None	None		capability sets
	Initial Compromise/ Exploitation	Legitimate Access		4.9	Detect		None	None		
	Initial Compromise/ Exploitation	Legitimate Arress		4.9	Respond		L	1		
Visual value of		Legitimate Credentials	CONTRACTOR OF THE PARTY OF THE	4.9	Protect		1	L		
neat map score	Persistence	Legitimate Credentials		4.9	Detect		None	None		
	Persistence	Legitimate Credentials		and the second	Respond		I	L		
	Persistence	Master Boot Record		100201	Protect		N/A	N/A		
	Persistence	Marian T			Detect		N/A			
DDD =		Master Boot Record			Respond		N/A	N/A		
PDR Function	Privilege Escalation	Legitimate Credentials		The state of the s	Protect		None	N/A		
	Privilege Escalation	Legitimate Credentials			Detect			None		
	Privilege Escalation	Legitimate Credentials		12000	Respond		None	None		
	Defense Evasion	Legitimate Credentials		CONTRACTOR OF THE PARTY OF THE	Discussion of the last of the		L	L	G	
	Defense Evasion		Name of Street, or other Desires.		Protect		None	None	-	
	Defense Evasio Great	or improvements :	a latala la					lone		
	Defense Evasio	er improvements in	n nigh he	at t	nrea	it.	actions	L		
	Defense Evasio	have more in-						S		
DARTA	Defense Evasion	have more impac	t on risk	red	uctio	n		м	<u> </u>	

PDR Analysis: Top Threat Actions

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	
			m/a 001		Sorted by Heat Map Value
Credential Access	Crédential Dumping	13.5	M	M	
redential Access	Password Recovery	9.0	N/A	N/A	1
ost Enumeration/Internal Reconnaissance	File System Enumeration	8.9	L	L	1
ommand & Control (C2)	Commonly used port	8.5	S	s	
ost Enumeration/Internal Reconnaissance	Process Enumeration	8.4	L	L	1
stallation	Writing to Disk	7.7	L	L	1
ost Enumeration/Internal Reconnaissance	Account Enumeration	7.3	L	L	1
itial Compromise/ Exploitation	Targets Application Vulnerability	7.3	ı	i	1
efense Evasion	Masquereding	74	3	S	Respond Only
/eaponization	Add Exploits to Application Data Files	7.0	N/A	1 1	Rep & WAF/RWP Enh
ommand & Control (C2)	Standard app layer protocol	7.0	M	м	THE CONTRACT CITE
xecution	Command Line	8.5	м	M	
lost Enumeration/Internal Reconnaissance	Operating System Enumeration	6.8	ı	L	1
efense Evasion	Legitimate Credentials	6.7	i	ì	1
efense Evasion	Obfuscated Payload	693	•	•	
itial Compromise/ Exploitation	Trojan	6.7	5		
ersistence	Legitimate Credentials	6.4	******************************	5	
ost Enumeration / Internal Reconnaissance		6.3	5	5	1
lost Enumeration/ Internal Reconnaissance	Local Network Configuration Enumeration	6.3	L	L	
TALL CONTROL OF THE TOTAL TO SELECT THE TOTAL TO SELECT THE TOTAL	Local Network Enumeration	\$00000000	М	M	
elivery	Web Application Exploit over the Network	6,0	5	S	
tent/Resource Development	Intent/Resource Development	6.0	N/A	ı	Rep & WAF/RWP Enh
efense Evasion	Scripting	5.8	L	L	50
ost Enumeration/Internal Reconnaissance	Owner/User Enumeration	5.7	L	L	l .
steral Movement	Remote Interactive Logon	5.7	М	M	
iteral Movement	Remote File Shares	5.7	L	M	Rep & Auto DHC-R
ommand & Control (C2)	Communications Encrypted	53	M	M	
econnaissance/ Staging	Social Media	5.4	N/A	N/A	
ersistence	Automatic Loading at Startup	5.4	\$	5	
onitor (Observation) / Exfiltration	Exfil over C2 channel	5.3	L	L	
efense Evasion	File Deletion	5.3	N/A	N/A	
ivilege Escalation	Scheduled Task	3.4	5	S	
itial Compromise/Exploitation	Lugitimate Access	5.0	S	s	
ommand & Control (C2)	Data Obfuscation	5.0	м	м	
ommand & Control (C2)	Fallback Channels	5.0	м	M	
efense Evesion	Signed Malicious Content	4.8	5	5	
econnaissance/ Staging	Vulnerability Scan	4.8	5	9	
rivilege Escalation	Legitimate Credentials	4.6	L	L	1
rivilege Escalation	Multi Tenant Side Channel Cache Attack	4.6	N/A	N/A	
efense Evasion	Software Packing	4.3	\$	N/A	
ecution	Scheduled Task	4.2			
ost Enumeration/Internal Reconnaissance	Security Software Enumeration	4.2	. 5 L	S.	



PDR Analysis: Impact of Layers

"as is" typical D/A cybersecurity architecture w/o B&I **Pre-Event** Get In (Engage (Admin. / None Stay In (Engage / Access) Act / Access) N/A Prepare) Limited Moderate Command & Control nitial Compromise/ Privilege Escalation Host Enumeration/ ateral Movement Significant Reconnaissance/ Intent/Resource Credential Access Defense Evasion Neaponization (Observation)/ nstallation Persistence Percentage of TTPs with Delivery Staging Internal varying levels of coverage at different network layers Protect TIC Detect Respond Protect Agency Detect **Boundary** Respond Protect Einstein Detect Respond Protect Agency Detect Endpoint Respond Protect **Agency Enclave** Detect Respond Protect **All Layers** Detect Respond

Threat Objective

Percentage of Threat Actions with varying levels of coverage for the Respond function in Monitor (Observation)/ Exfiltration Threat Objective



Architecture Layer

PDR Function

Unclassified//For Official Use Only

LUNCH BREAK

Anyone leaving now see Branko before you leave.



GOVCAR HANDS-ON WORKSHOP



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



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



CAPABILITY SCORING FOR PROTECT/DETECT/RESPOND

Pete



Practice Scoring

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



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.

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.



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
Application Trintensuing	applications. Protection is limited since some high-risk applications must be allowed.



ANALYSIS

Laurie



Analysis

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



Current Enterprise-Enabled Mobile Device to Internet (Protected)

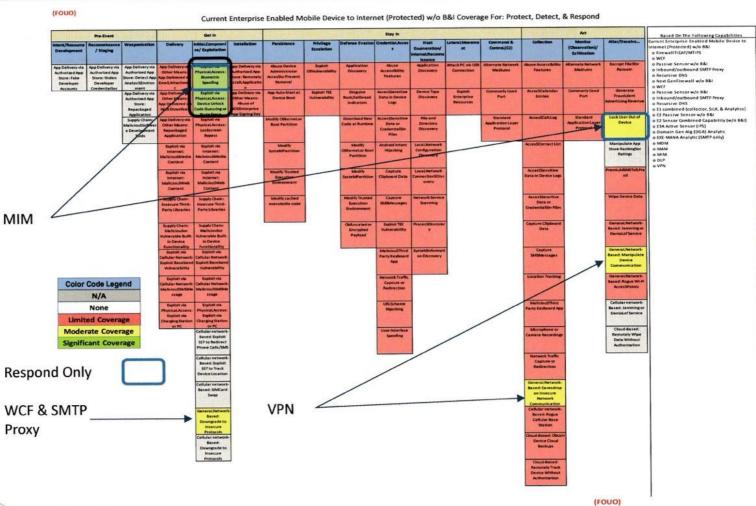
(FOUO)

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

nt/Resource	Reconnaissance	Weaponization	Delivery	Initial Compromi	Installation	Persistence	Privilege	Defense Evasion	Stay in Credential Acces	Host	Lateral Moveme	Command &	Collection	Act	T	Based On The Following Capabilities
Deliveryvia	/ Staging App Delivery via			se/ Exploitation			Escalation			Enumeration/ Internal.Reconna issance	nt	Control(C2)	Collection	(Observation)/ Exfiltration	Alter/Deceive	Current Enterprise Enabled Mobile Device Internet (Protected) w/o B&I o FirewallTICAP/MTIPS o WCF
horized App tore: Fake Developer Accounts	Authorized App Store: Stolen Developer CredentialSor	App Delivery via Authorized App Store: Detect App Analysi SEnviron ment	Other Means: App Delivered via Email.Attachmen	Exploit via Physics LAccessi Biometric Spoofing	App Delivery via Authorized App Store: Remotely Install.Application	Abuse Device Administrator Accessto Prevent Removal	Exploit OSVuinerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection	Alternate Network Mediums	Abuse Accessibility Features	Alternate Network Mediums	Encrypt FileSfor Rensom	o Passive Sensor w/o B&I o Inbound/outbound SMTP Proxy o Recursive DNS o Next GenFirewall w/o B&I
		App Delivery via Authorized App Store: Repackaged Application	App Delivery via Other Means: App Delivered via Web Download	Exploit via Physica LAccess: Device Unlock Code Guessing or Brute Force	App Delivery via Other Means; Abuse of IOSEnterprise App Signing Key	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jelibreak Indicators	AccesSensitive Date in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Commonly Used Part	AccesSCalendar Entries	Commonly Used Port	Generate Fraudulent Advertising Revenue	o WCF o Passive Sensor w/o B&I o Inbound/outbound SMTP Proxy o Recursive DNS o E1 combined (collector, SiLK, & Analytic
		Supply Chain: MaliciouSSoftwar e Development Tools	App Delivery via Other Means: Repackaged Application	Exploit via Physical Access: Lockscreen Bypass		Medify OSKernetor Boot Partition		Download New Code at Runtime	AccesSensitive Date or CredentialSin Files	File and Directory Discovery		Standard Application Layer Protocol	AccesSCelLlog	Standard Application Layer Protocol	Lock User Out of Device	o E2 Passive Sensor w/o B&I o E2 Sensor Combined Capability (w/o B o E3A Active Sensor (IPS) o Domain Gen Alg (DGA) Analytic
			Exploit via Interneti MaliciousMedia Content	Exploit via Internet: MaliciousMedia Content		Modify SysteMPartition		Modify OSKerneLor Boot Pertition	Androld Intent Hijacking	Local Network Configuration Discovery			AccesSContact List		Manipulate App Store RankingSor Ratings	o EXE-MANA Analytic (SMTP only) o MDM o NAM o MIM o DIP
			Exploit via Internet: MaliciousWeb Content	Exploit via Internet: MaliciouSWeb Content		Modify Trusted Execution Environment		Modify SysteMPartition	Capture Clipboard Data	Local Network ConnectionSDIsc every			AccesSSensitive Date in Device Logs		PremiuMSMSTolLFre ud	o VPN
			Supply Chain: Insecure Third- Party Libraries	Supply Chain: Insecure Third- Party Libraries		Modify cached executable code		Modify Trusted Execution Environment	Capture SMSMessages	Network Service Scanning			AccesSensitive Data or CredentialSin Files		Wipe Device Data	
			Supply Chain: MaliclouSor Vulnerable Bullt- in Device Functionality	Supply Chain: Maliciousor Vuinerable Built- In Device Functionality				Obfuscated or Encrypted Payload	Exploit TEE Vulnerability	ProcesSDiscover V			Capture Clipboard Data		General Network- Based: Jamming or Denial of Service	
			Exploit via Cellular Network: Exploit Baseband Vulnerability	Exploit via Cellular Networks Exploit Baseband Vulnerability					MaliciouSThird Party Keyboard App	SysteMinformati on Discovery			Capture SMSMessages		GeneralNetwork- Basedi Manipulate Device Communication	
A STATE OF THE PARTY OF THE PAR	ode Leger	nd	Exploit via Celluler Network: MaliciouSSMSMe ssage	Exploit via Cellular Network: Malicioussmisme saage					Network Traffic Capture or Redirection				Location Tracking		General Network- Based: Rogue Wi-Fi AccessPoints	
Limite	None d Coverag	A CONTRACTOR OF THE PARTY OF TH	Exploit via Physical Access; Exploit via Charging Station or PC	Exploit via Physica LAccess: Exploit via Charging Stetion or PC					URLScheme Hijacking				MaliciouSThird Party Keyboard App		Cellular network- Based: Jamming or DeniaLof Service	
	nt Covera	-		Cellular network- Based: Exploit SS7 to Redirect Phone Calls/SMS					User Interface Spoofing				Microphone or Camera Recordings		Cloud-Based: Remotely Wipe Data Without Authorization	
				Cellular network- Based: Exploit SS7 to Track Device Location				'					Network Traffic Capture or Redirection			
				Cellular network- Based: SIMCard Swap									General Network- Based: Eavesdrop on Insecure Network			
				GeneralNetwork- Based: Downgrade to Insecure									Communication Cellular network- Based: Rogue Cellular Base Station			
				Protocols Cellular network- Based: Downgrade to Insecure Protocols									Cloud-Based: Obtain Device Cloud Backups			
													Cloud-Based: Remotely Track Device Without Authorization			
														(FO	110)	



Current Enterprise-Enabled Mobile Device to Internet (Protected)





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

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

Protect

Detect

Respond



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

No Coverage

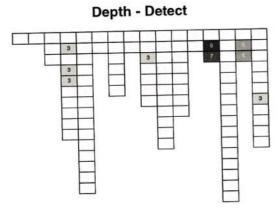
Unique

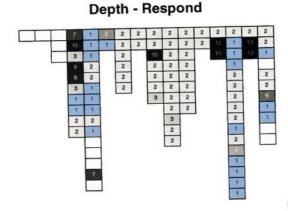
Increasing Depth

(FOUO)

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

Depth - Protect

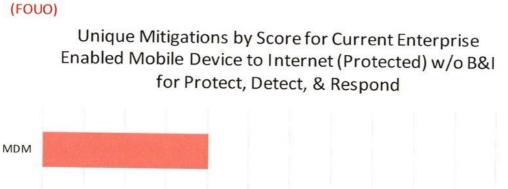


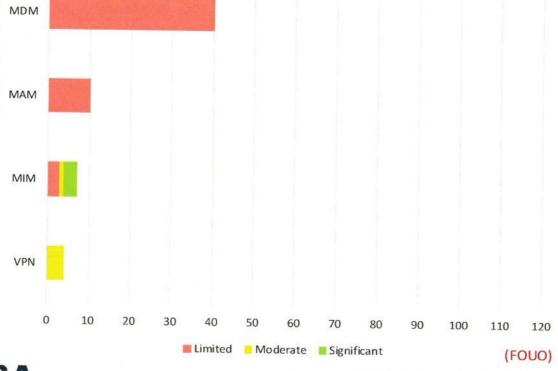


(FOUO)



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







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

(FOUO

None		Pre-		nt (Ad	THE PERSON NAMED IN		In (Eng Access			Stay	In (E	ngage	/ Acc	ess)			Act	
N/A Limited Moderate Significant Percentage of TTPs rarying levels of co	verage at	Intent/Resource	Development	Reconnaissance/ Staging	Weaponization	Delivery	InitialCompromise/ Exploitation	Installation	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Host Enumeration/ InternalReconnaissan	LateraLMovement	Control (C2)	Collection	Monitor (Observation)/	Alter/Deceive
	Protect					Wit												10000
NEST	Detect																- Contract	
	Respond										Piggs	E Base						-
тіс	Protect																	-
	Detect												Line of			100		
	Respond								LIBERT .	0.55						Sec.		
and the	Protect				PART.			BALL										
Agency	Detect															Sept.	- Control	
Boundary	Respond														1000			-
A Nachila	Protect									No.				ERIO SE				
Agency Mobile Services	Detect						No.	1									- Emilian	
Services	Respond							200				Sin		lane.	la Linia		0	
	Protect									-	_	-	-		-	+	+	+
Mobile Device	Detect								-			-	-	-	-	+	+	+
	Respond														-	_		+
	Protect											1810		Militar				
All Layers	Detect											-			C Report	No.	E STATE OF	
	Respond											4		1				(FOU



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

Intent/Resource Reconnelssance/ Wespenisston			Delivery	Get In					Stay In					Act		
Development op Delivery via	Staging App Delivery via	App Delivery via	App Delivery via	Compromise/ Exploitation	App Delivery via	Persistence Abuse Device	Privilege Escalation Exploit OS		Credential Access	Host Enumeration/ Internal Reconnelssance	Lateral Movement	Command & Control (C2)	Collection	Monitor (Observation)/ Exfitration	Alter/Deceive	Based On The Following Capabilities Planned Enterprise Enabled Mobile Device Internet (Protected) w/o B&I o firewallTICAP/MTIPS Enhancements
thorized App Store: Fake Developer Accounts	Authorized App Store: Stolen Developer Credentials or	Authorized App Store: Detect App Analysis Environment App Delivery via	Other Means: App Delivered via Email Attachment App Delivery via	Physical Access: Blometric Spoofing Exploit via	Authorized App Store: Remotely Install Application	Administrator Access to Prevent Removal	Vulnerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection	Alternate Network Mediums	Abuse Accessibility Features	Alternate Network Mediuma	Encrypt Files for Rensom	o WCF combined (TIC) o Fassiev Sensor w/o B&I o Ib/Ob SMTP Proxy Combined (TIC) o Recursive DNS o Next GenFirewall w/o B&I
		Authorized App Store: Repackaged Application Supply Chain:	Other Means: App Delivered via Web Download App Delivery via	Physical Access: Device Unlock Code Guessing or Brute Force	App Delivery via Other Means: Abuse of iOS Enterprise App Signing Key	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jellbreak Indicators	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Commonly Used Port	Access Calendar Entries	Commonly Used Port	Generate Fraudulent Advertising Revenue	o WCF combined (agency) o Passive Sensor w/o B&I o Ib/Ob SMTP Proxy Combined (agency) o Recursive DNS
		Malicious Software Development Tools	Repackaged Application	Exploit via Physical Access Lockscreen Bypass		Modify OS Kernel or Boot Partition		Download New Code at Runtime	Access Sensitive Data or Credentiels in Files	Pile and Directory Discovery		Standard Application Layer Protocol	Access Call Log	Standard Application Layer Protocol	Lock User Out of Device	o EL combined (collector, SILK, & Analytic o E2 Passive Sensor w/o B&I o E2 Sensor Combined Capability (w/o B/ o E3A Active Sensor (IPS) o E3A Active Sensor (IPS) (WCF) w/o B&I
			Exploit via Internet: Melicious Media Content	Exploit via Internet; Malicious Media Content		Modify System Partition		Modify OS Kernel or Boot Partition	Android Intent Hijacking	Local Network Configuration Discovery			Access Contact List		Manipulate App Store Rankings or Ratings	o Domain Gen Alg (DGA) Analytic o EXE-MANA Analytic (SMTP only) o MDM o MAM Enhancements
			Exploit via Internet: Malicious Web Content	Exploit via Internet: Malicious Web Content		Modify Trusted Execution Environment		Modify System Partition	Capture Clipboard Data	Local Network Connections Discovery			Access Sensitive Data in Device Logs		Premium SMS Toll Fraud	o MAV (Future) o MIM o MTO (Future) o DLP o IDS (Future)
			Supply Chain: Insecure Third- Party Libraries	Supply Chain: Insecure Third- Party Libraries		Modify cached executable code		Modify Trusted Execution Environment	Capture SMS Messages	Natwork Service Scanning			Access Sensitive Data or Credentials In Files		Wipe Device Data	o VPN o MDSE (Future)
			Supply Chain: Malicious or Vulnerable Built- in Device Functionality	Supply Chain: Melicious or Vuinerable Built- in Device Functionality				Obfuscated or Encrypted Payload	Exploit TEE Vulnerability	Process Discovery			Capture Clipboard Data		General Network- Based: Jamming or Denial of Service	
			Exploit via Cellular Network: Exploit Besebend Vulnerability	Exploit via Cellular Network: Exploit Baseband Vulnerability					Malicious Third Party Keyboard App	System Information Discovery			Capture SMS Messages		General Network- Based: Manipulate Device Communication	
AT SEP	N/A	end	Exploit via Cellular Natwork: Malicious SMS Message	Exploit via Cellular Network: Malicious SMS Massage					Network Traffic Capture or Redirection				Location Tracking		General Network- Based: Rogue Wi-Fi Access Points	
Limite	None d Covera	The second second	Exploit via Physical Access: Exploit via Charging Station or PC	Exploit via Physical Access: Exploit via Charging Station or PC					URL Scheme Hijacking				Malicious Third Party Keyboard App		Cellular network- Based: Jamming or Denial of Service	
	ant Cover			Cellular network- Based: Exploit 557 to Redirect Phone Cells/SMS					User Interface Spoofing				Microphone or Camera Recordings		Cloud-Based: Remotely Wipe Data Without Authorization	
				Cellular network- Based: Exploit \$57 to Track Device Location									Network Traffic Capture or Redirection	ı		
				Cellular network- Based: SIM Card Swap									General Network- Based: Eavesdrop on Insecure Network			
				General Network- Based: Downgrade to Insecure Protocols									Communication Cellular network- Based: Rogue Cellular Base Station			
				Cellular network- Based: Downgrade to Insecure Protocels								C	loud-Based: Obtain Device Cloud Backups			
													Cloud-Based: Remotely Track Device Without Authorization			



(FOUO)

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

(FOUO)

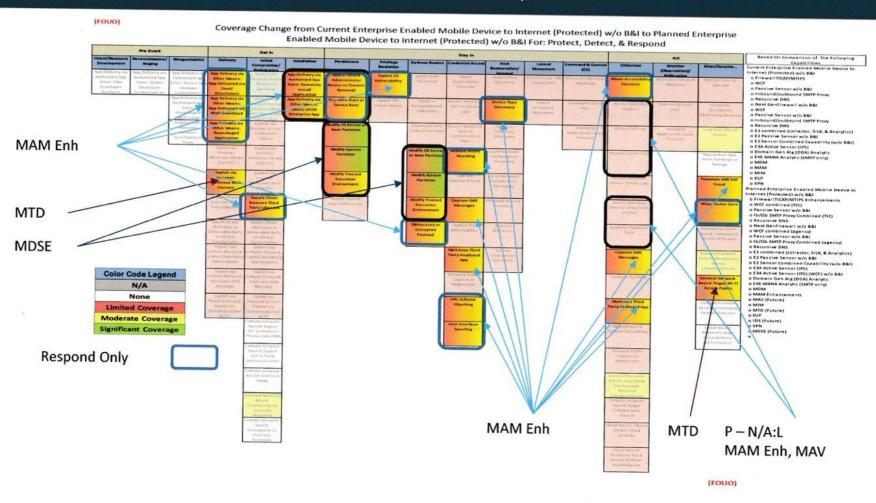
Coverage Change from Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I to Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I For: Protect, Detect, & Respond

	Pre-Event			Get In			ACCESSED IN		Stay In				K STOLEN	Act		Based On Comparison of The Following
ntent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/	Installation	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration/	Lateral Movement	Command & Control (C2)	Collection	Monitor (Observation)/	Alter/Deceive	Capabilities Current Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I
App Delivery via Authorized App Store: Fake Developer	App Delivery via Authorized App Store: Stolen Developer	App Delivery via Authorized App Store: Detect Aps Analytis	App Delivery via Other Means: App Delivered via Email Attachment	Experie via Dispersi Access Mismetric Speeding	App Delivery via Authorized App Store: Remotely Install Application	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application (Hardwary	Abuse Accessibility Features	Application Dissevery	Arrack PC via USE Connection	Alternate Network Nedowa	Abuse Accessibility Features	Altertion Alternate Network Neclines	Encrypt Files for flamous	o FirewallTiCAP/MTIPS o WCF o Passive Sensor w/o B&I o Inbound/outbound 5MTP Proxy o Recursive DNS
•		App Delivery via Authorized App Store: Empackaged Application	App Delivery via Other Means: App Delivered via Web Download	Exploit via Physica i Acces o Davida United Edde Greek uniq p Dista Porce	App Delivery via Other Means: Abuse of IOS Enterprise App Signing Key	App Auto-Start at Device Boot	Espirit TEE Vulnerability	Disputse Root/tailbreak Indicators	Access Sensitive Data in Device Legs	Device Type Olscovery	Exploit Enterprise Resources	Commonly Used Port	Access Calendar Entrees	Commanly Used Port	Governce Fractistent Astvertiking Revenue	o Next Genfirewall w/o B&I o WCF o Passive Sensor w/o B&I o Inbound/outbound SMTP Proxy o Recursive DNS
		Supply Chain Malicipus Software Development Tools	App Delivery via Other Means: Repackaged Application	Exploit via Physical Access. Lockscreen Bygiass		Modify OS Kernel or Boot Partition		Downland New Code at Runtinse	Access Sensitive Data or Credentials in Files	Bile and Directory Discovery		Standard Application Layer Protecol	Access Call Log	Standard Application Layer Protocol	Lock User Out of Onvice	o E1 combined (collector, Sitk, & Analytics) o E2 Passive Sensor w/o B&I o E2 Sensor Combined Capability (w/o B&I) o E3A Active Sensor (IPS)
			Exploit via (externet) Malicious Media Contest	Exploit via fote med Malicious Media Content		Modify System Partition		Modify OS Kernel or Boot Partition	Android Intent Hijacking	Lincal Network Configuration Discovery			Access Contact List		Manipulate App Store Rankings or Ratings	o Domain Gen Alg (DGA) Analytic o EXE-MANA Analytic (SMTP only) o MDM o MAM o MIM
			Exploit via Internet: Malicious Web Content	Exploit wa Internet Maticious Web- Content		Modify Trusted Execution Environment		Modify System Partition	Capture Clipboard Data	Local Network Connections Discovery			Access Synstone Data in Device Logs		Premium SMS Toll Fraud	o DLP o VPN Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I o FirewallTiCAP/MTIPS Enhancements
			Supply Chain interview Third- Party Libraries	Supply Chain: Insecure Third- Party Libraries		Modify carned executable code		Modify Trusted Execution Environment	Capture SMS Messages	Hetwork Service Schneing			Access tensitive Data or Credentials in Files		Wipe Device Data	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
			Supply Chain, Mahuigas or Vulnerable Built- in Drivice Functionality	Supply Chain, Madicious or Valorrable Built- in Device Functionality				Obfuscated or Encrypted Payload	Explor TEE Vulnerability	Principal Discovery			Capture Clipboard Data		General Networks Based: Jamening or Denial of Service	o WCF combined (agency) o Passive Sensor w/o B&I o Ib/Ob SMTP Proxy Combined (agency) o Recursive DNS
			Exploit via Cellular Network Exploit these band Volmerability	Exploit via Cellular Network Exploit Baseband Volnerability					Malicious Third Party Kayboard App	System teformation Discovery			Capture SMS Messages		General Network- Based: Manipulate Device Communication	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)
Color	N/A	end	Exploit via Ceffular Network Malicinus SMS Massage	Exploit via Cellular Network Malicious SMS Message					Network Traffic Capture or Environtion				Location Tracking		General Network- Based: Rogue Wi-Fi Access Points	o Domain Gen Alg (DGA) Analytic o EXE-MANA Analytic (SMTP only) o MDM o MAM Enhancements o MAY (Future)
Limite	None d Coverage ate Coverage	Total Control of the last of t	Exploit via Physical Access Exploit via Charging Station or PC	Exploit via Physical Access Exploit wa Charging Station or PC					URL Scheme Hijacking				Malicious Third Party Keyboard App		Cellular network Based: Jamming or Denial of Service	o MIM o MTD (Future) o DLP o IDS (Future)
	ant Cover			Cellular network- Based: Exploit 557 to Redirect Phone Calls/SMS					User Interface Spoofing				Meroshone or Camera Recordings		Cloud-Based: Remotely Wipe Data Without Authorization	o VPN o MDSE (Future) o
				Cellular network Based: Exploit 557 to Track Device Location									Network Traffic Capture or Reclinication			
				Cellular network Based, SIM Card Swap									General Network Based: Eavesdrop on Insecure Network Communication			
				General Network Based: Downgrade to Imecure Protocols									Cellular networks Based Ropes Cellular Base Station			
				Cellular network- Based: Downgrade to Insecure Protocols									Cloud-Based Obtain Davice Cloud Backups			
													Remotely Track Device Without Authorization			



(FOUO)

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

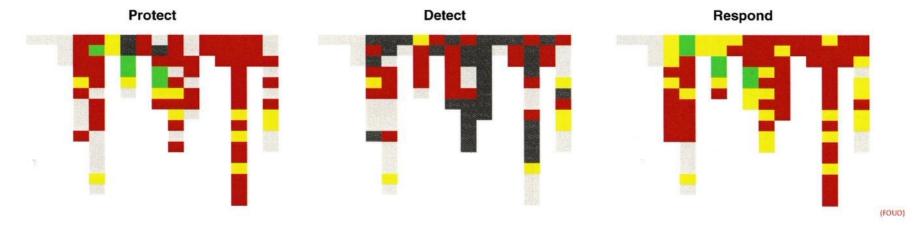




Mitigation by Protect, Detect, Respond for Planned Enterprise-Enabled Mobile Device to Internet (Protected)

N/A
None
Limited
Moderate
Significant

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





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

No Coverage

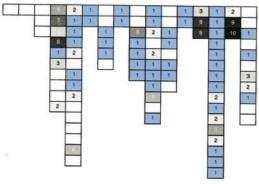
Unique

Increasing Depth

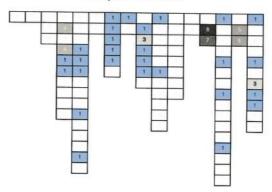
(FOUO)

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

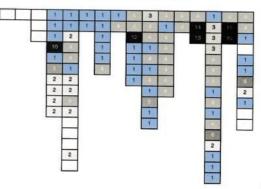
Depth - Protect



Depth - Detect



Depth - Respond



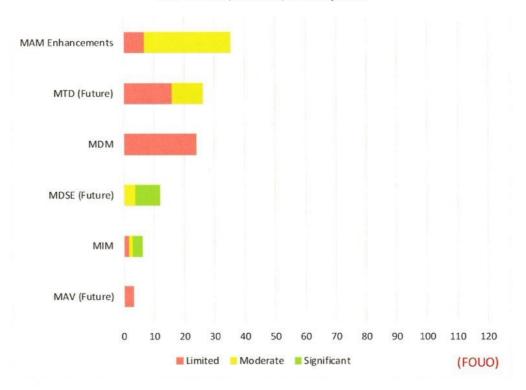
(FOUO)



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



Unique Mitigations by Score for Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I for Protect, Detect, & Respond





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			Adı	re-Eve minist repare	ter/		In (E	ngage	1515					Acce) w/o B	S.I	Act	
		92	Development	Reconnaissance/ Staging	Weaponization	Delivery	InitialCompromise/	Exploitation		Persistence	Privilege Escalation	Defense Evasion	CredentiaLAccess	Host Enumeration/ Internal Reconnaissan	ateraLMovement	Command &	Collection	Monitor (Observation)/	Alter/Deceive
Planned En	THE RESERVE THE PARTY NAMED IN	<u>=</u>	<u> </u>	St.	3	Ğ	<u>-</u>	E E	\perp	Pel	Pri	Def	S	Inte	Late	5 5	3	§ 6	Afte
NECT	Protect		1														- J		
NEST	Detect		1																
	Respond		1																
	Protect		1						\perp			-							
TIC	Detect		4																
	Respond		1																
Agency	Protect		4																
Boundary	Detect		4						1										
	Respond		1																
Agency	Protect	_	1										0						
Mobile	Detect		1														ī		
Services	Respond		1														_		
Mobile	Protect		1																
Device	Detect		1	_															
	Respond																		
	Protect																		
All Layers	Detect												n I						
	Respond								f			_	_						





(FOUO)

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

(FOUO)

Planned Enterprise Enabled Mobile Device to Internet (Protected) w/o B&I Get In (Engage Pre-Event (Admin., Stay In (Engage / Access) Act None Prepare) / Access) N/A Limited nternalReconnaissa Moderate nitialCompromise/ lost Enumeration, ateralMovement Significant Veaponization Observation)/ Command & ersistence nstallation Percentage of TTPs with Staging varying levels of coverage at different network layers Protect NEST Detect Respond Protect TIC Detect Respond Protect Agency Detect Boundary Respond Protect **Agency Mobile** Detect Services Respond Protect **Mobile Device** Detect Respond Protect **All Layers** Detect Respond



(FOUO)

Best Calculation

govCAR Mitigation Draft Scoring Sheet		Stage											
		Th	reat Action	Obje n Y	CONTRACTOR OF CONTRACTOR	reat Action	n 7						
		Protect	Detect	Respond	Protect	Detect	Respond						
Capabilities		Threa	t Action Descr	iption	Threat Action Description								
Set	Layer 1	Marin Land		0.000									
1	A	L	N/A	L	M	None	M						
1	В	L	None	L	1	None	IVI						
	Layer 2	10000		TO THE RESIDENCE OF THE PARTY O		None							
1	C	L	None	S	S	1	S						
1	D	N/A	N/A	N/A	N/A	N/A	N/A						
1	E	None	None	М	None	None	M						
All Capabilities Set 1 P/D/R RollUp		L	None	S	S		s						
			S		S								

Weights

Significant -0.9 Protect -0.4 Moderate -0.6 Detect -0.3 Limited -0.3 Respond -0.3 None & N/A -0

Protect Weighted Coverage:

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

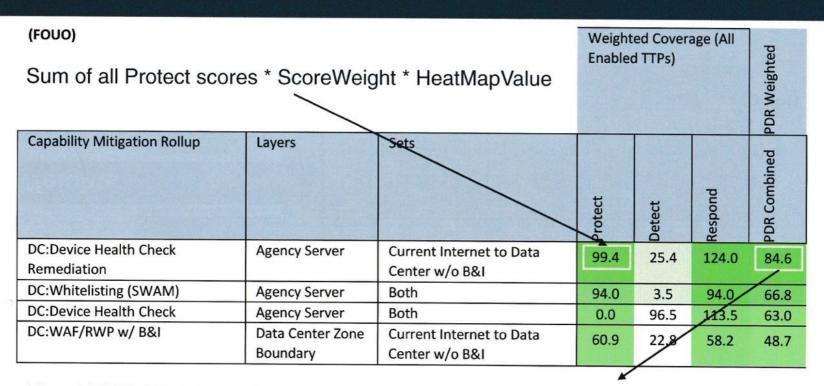
Repeat for Detect & Respond

Combined PDR Weighted Coverage:

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



Best calculation



Combined PDR Weighted Coverage:

Combined PDR Weighted Coverage:

(Protect Weighted Coverage * Protect Weight) +

99.4 * 0.4 +

(Detect Weighted Coverage * Detect Weight) +

25.4 * 0.3 +

(Respond Weighted Coverage * Respond Weight)

124.0 * 0.3

= 84.58



Top Threat Actions

(FOUO)			Capability 1	Capability 2	
Objective	Threat Action	Heat Map	All Capabilities Current Internet to Data Center w/o B&I	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	1
Command & Control (C2)	Commonly used port	881	· ·	5	
Host Enumeration/Internal Reconnaissance	Process Enumeration	8.4	L	L	1
Installation	Writing to Disk	7.7	L	L	1
Host Enumeration/Internal Reconnaissance	Account Enumeration	7.3	L	L	
Initial Compromise/ Exploitation	Targets Application Vulnerability	7.3	L	ı	
Defense Evesion	Masquerading	72	5	5	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	MCP & WAITH EIII
Execution	Command Line	6.9	м	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	5	s	
Initial Compromise/ Exploitation	Trojan	6.7	5	s	
Persistence	Legitimate Credentials	6.4	5	s	
Host Enumeration/Internal Reconnaissance	Local Network Configuration Enumeration	6.3	L	L	
Host Enumeration / Internal Reconnaissance	Local Network Enumeration	6.3	M	M	
Defivery	Web Application Exploit over the Network	6.0	5	S	
Intent/Resource Development	Intent/Resource Development	6.0	N/A		Rep & WAF/RWP Enh
Defense Evasion	Scripting	5.8	ι	L	HEP & WAITKWF LIIII
Host Enumeration/Internal Reconnaissance	Owner/User Enumeration	5.7	L	L	
Lateral Movement	Remote interactive Logon	3.7	M	M	
Lateral Movement	Remote File Shares	5.7	L	M	Rep & Auto DHC-R
Command & Control (C2)	Communications Encrypted	5.5	M	M	nep a rate brie-it
Reconnaissance/ Staging	Social Media	5.4	N/A	N/A	
Persistence	Automatic Loading at Startup	5.4		5	
Monitor (Observation) / Exfiltration	Exfil over C2 channel	5.3	L	L	
Defense Evasion	File Deletion	5.3	N/A	N/A	
Privilege Escalation	Scheduled Tesk	3.1	5	\$	
Initial Compromise/ Exploitation	Legitimate Access	5.0	5	S	
Command & Control (C2)	Data Obfuscation	5,0	M	M	
Command & Control (C2)	Fallback Channels	5,0	M	M	
Defense Evesion	Signed Malicious Content	4.8	5	5	
Reconnaissance/ Staging	Vulnerability Scan	4.8	5	5	
Privilege Escalation	Legitimate Credentials	4.6	t	L	
Privilege Escalation	Multi Tenant Side Channel Cache Attack	4.6	N/A	N/A	
Defense Evasion	Software Packing	4.3	8	5	
Execution	Scheduled Task	4.2	5	5	
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.



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



ROA's from Today



Tool Needs Discussion



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 PhilosophyModified Delphi Method



ARCHITECTURE



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

CELETETETETETETETETETETE

E.g., Agency Boundary, Agency Endpoint



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



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



THREAT



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]



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:

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



FACILITATING A SCORING SESSION



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.



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



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)



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)



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.



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



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.



WRAP UP



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



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



Topics for Discussion

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



QUESTIONS?



Comments/Questions

- Lessons learned from applying .govCAR
- Data Architectures



BACKUP

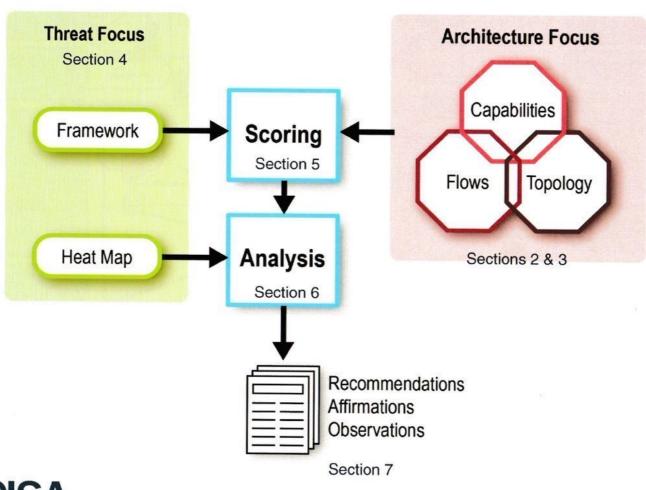


Agenda

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

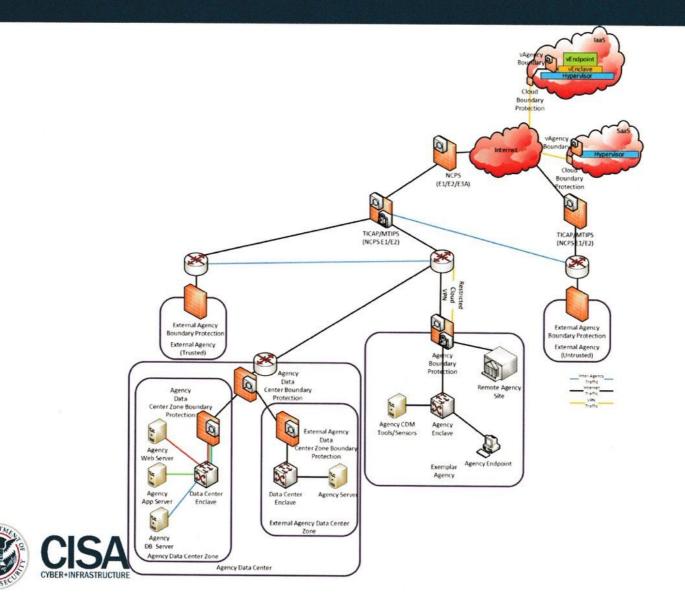


.govCAR Methodology





Representative Architecture (Section 2)



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



CISA CYBER+INFRASTRUCTURE

Current

ta Center Protection

Data Center Boundary Protection

Internet

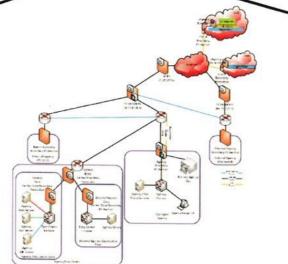
Internet

Agency -> Internet
Unprotected
Unprot

Endpoint/

Workstation

Data Center Protection



TICAP/MTIPS:

Planned

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

NSA Adversary Lifecycle Threat Framework v2.0

	Pre-Event			Get In					Sta	y In				A	ct
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	Crawling Internet	Add Exploits to	Spear-phishing Emails	Targets Application	Writing to Disk	Legiti mate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software	Command Line	Commonly used port	Automated or Scripted Exfiltration	Distributed Denial Service (DDOS)
Development	Websites Network Mapping (e.g.	Application Data Files	w/ Attachments Spear-phishing email	Vulnerability Target Operating	In Memory Malware	Accessibility Features	Accessibility Features	Binary Padding	Virtualization Attacks	File System	Virtualization Attacks	File Access	Comm through removable media	Virtualization Attacks	Partial disk/OS delet (corruption)
	NMAP) Social Media		w/Malicious Link Websites	System Vulnerability Targets Application	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 deletio (bricking)
	Mid-Points		Removable Media (i.e.	Vulnerability Remotely Trojan	Replace legitimate binary with Malicious	Ubrary Search Hijack	Library Search Hijack	Library Search Hijack	User Interaction	Local Network Connection	Logon Scripts	Process Injection	Communications Encrypted	Data Size limits	Data Alteration
	Vulnerability Scan		USB) Credential Pharming	Social Engineering	(ex: Havex)	New Service	New Service	File System Logical Offsets	Password Recovery	Enumeration Local Networking Enumeration	Authentication Assertion Misuse	Configuration Modification to Escilitate Launch	Data Obfuscation	Data Staged	Data Encrypted an Unavailable (Crypt Locker)
		I	Application or Operating System Exploit over the	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	Exfit over C2 channel	Data Deletion (Part
			Web Application Exploit over the	Defeat Encryption		Scheduled Task	Scheduled Yask	Indicator Blocking on Host	Hijack Active Credentia	Operating System Enumeration	Peer Connections	Scheduled Task	Multiband comm	Exfit over Alternate Channel to a C2 Network	Data Deletion (ful
			Network Deploy Exploit using	Exploit Weak Access	-	Service File Permission	Service File Permission	Indicator Removal from	Credentials in File	Owner/User	Remote Interactive	Service Manipulation	Multilayer Encryption	Exfiltration Over other Network Medium	Denial of Service
			Advertising	Controls	J	Weakness Unk Modification	Weakness Link Modification	Tools Indicator Removal from		Process Enumeration	Remote Management	Third Party Software	Peer Connections	Exfiitration from Local System	Cause Physical Effe
			DNS/Cache Poisoning 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	1
			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	File System Hiding			Remote File Shares		Uncommonly Used Port	Exfit over Virtual Medium	
			Crosstalk (Data Emanation)			Master Boot Record	Configuration Multi Tenant Side Channel Cache Attack	Obfuscated Payload				_	Custom encryption cipher	Exfil over Physical Medium	-
1.100			Device Swapping (Cross Domain Violation)			Modify Existing Services		Rootkit					Multiple Protocels 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 Traversa	
				1		Web Shell	4	Software Packing	+					Defeat Encryption	1
			Pata Encoded Automatically Transported Trusted			Web sales	_	Signed Malicious Content						Exploit Weak Access Controls	
			Cross Domain or Multi Level Solution Traversa					Sandbox Detection						Exfil via Cloud Service	
			Supply Chain / Trusted Source Compromise (Hardware)	1				Malicious Behavior Delays							-
			Supply Chain / Truster Source Compromise (Software)							Initial Sources	:				
			Auto Delivery via Clou Service	d						* Lockheed M	artin's Cyber Kil	er's (NTOC) Adv I Chain Techniques, & C			
			Insider Threat/Close Access Wireless Access							WITTE S AUV	cisana ractica,				



Threat Framework Host vs. Network

	Pre-Event	Television and the second		Get In					Sta	y In				A	ct
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 delet (corruption)
	Social Media		Websites	Targets Web Application Vulnerabilities (ex. XSS, CSBF, SQ1)	Interpreted Scripts	Automatic Loading at Startup	Automatic Loading at Startup	Disabiling Security Tools	Network Sniffing	Group Permission Enumeration	Exploitation of Vulnerability	Interpreted Scripts	Custom Application Layer Protocol	Data Compressed	Full disk/OS defetion (bricking)
	Mid-Points		Removable Media (i.e. USB)	Trojan	Replace legitimate binary with Malicious (ex: Havex)	Ubrary 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 an Unavailable (Crypt Locker)
			Application or Operating System Exploit over the Network	Legitimate Access		Path Interception	Path Interception	File Deletion	Credential Manipulation	tocal network Enumeration	Remote Services	Use of Trusted Process to Execute Untrusted Code	Fallback Channels	Exfil over C2 channel	Data Deletion (Parti
			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
	1		DNS/Cache Poisoning			Unk Modification	Unk Modification	Indicator Removal from Host		Process Enumeration	Remote Management Services	Third Party Software	Peer Connections	Exfiltration from Local System	Cause Physical Effe
Neither			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	
Host			Connection of Rogue Network Devices			BIOS	Process Injection	Process Injection	1	Service Enumeration	Shared Webroot	APIS to Facilitate Launch	Standard non-app layer protocol	resources Scheduled Transfer	
Network			Trusted Website			Hypervisor Rootkit	Exploitation of Vulnerability (ex. XSS, CSRF, OS/Software)	Masquerading		Window Enumeration	Taint Shared Content		Standard Encryption Cipher	Data Encrypted	
Host & Network			Legitimate Remote Access			Weak Access Control for Service Configuration	Weak Access Control for Service Configuration	File System Hiding	1		Remote File Shares	1	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	
- 5			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	
TI	hreat		Physical Network Bridge			Security Support Provider		Scripting						Cross Domain or Multi- Level Solution Traversal	
OV	ample		Data Encoded Automatically			Web Shell	l _a	Software Packing						Defeat Encryption	
ex	ample		Transported Trusted Services					Signed Malicious Content						Exploit Weak Access Controls	
			Cross Domain or Multi- Level Solution Traversal					Sandbox Detection						Exfit via Cloud Service	
			Supply Chain / Trusted Source Compromise (Hardware)					Malicious Behavior Delays							
			Supply Chain / Trusted						J					Maria	ı
			Auto Delivery via Cloud							Initial Sources:					
			Service							* NSA Threat O	perations Cente	r's (NTOC) Adve	rsary Lifecycle A	Analysis (ALA)	
			Insider Threat/Close Access							* Lockheed Ma	rtin's Cyber Kill (ersarial Tactics, To	Chain			
			Wireless Access									comques, & Co	Annion Knowled	Se (MIIOCK)	
			Compromise Common Network Infrastructure												

NTCTF 2.0

	Administration		Prepa	ration	Engagement Presence							A CONTRACTOR	Effect						Ongoing Processes		
Planning	Resource Development	Research	Reconnaissan ce	Staging	Delivery	Exploitation	Execution	Internal Reconnaissan ce	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		Mapaccessible 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	
elect 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		Mi			Use remote shell	Employ rootkit	
	1		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 Use trusted					Modify service configuration		Throttle data						Impersonate legitimate file	
					Use chat services	Launch zero- day exploit	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									at Operation	ns Center's (NTOC) Adve	ersary		Obfuscate data	
															ialysis (ALA) Martin's Cy	her Kill Cha	in			Remove logged data	
															Adversarial 1			ommon		Remove toolkit Sign malicious	
														Knowledge		deties, reen	inques, a c			content	
																				Store files in	



location Tailor behavior to environmen Use signed

NTCTF 2.0

	Administration	HEAT STATE	Prepa	ration	Engag	ement				ence	MINISTER AND ADDRESS OF THE PARTY OF THE PAR				Effect				ongoing Process	ø
Planning	Development	Research	Reconnaissance	i i i i i i i i i i i i i i i i i i i	Delivery	Exploitation	Execution	Internal Reconnalssance	Privilege Escalation	Credential Access	Lateral Movement	Persistence	Monitor	Exflitrate	Modify	Deny	Destroy	Analysis Evaluation Feedback	Command and Control	
Analyzi-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	Alterdata	Corrupt files or applications	Brick disk or OS (full delete)	Abandon infrastructure	Beacon to midpoints	١
Determine strategy and goals	Build alliances and partnerships	Intentify capability gaps	Gather credentials	Allocate operational infrastructure	Alter communications path	Access virtual memory	Execute via service controller	Enumerate file system	Exploit firmware vulnerability	Conduct social engineering	Logion 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	ı
Loue 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	Defete data	Refine potential victims	Relay communications	ı
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 communications	Encrypt data to render unusable	Destroy hardware		Send commands	ı
Receive approval to execute operations			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	İ
Select infunded victims	Seed supply clean		Scrape websites	Pre-position payload	Infectivia 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	١
	Staff and fram responses		Select potential victims		Inject database command	Exploit OS vulnerability	Run commands in shell	Enumerate windows	Ubrary Search Hijack	Log keystrokes	Use application- deployment software	Modify BIOS	Defeat Encryption	Run collection script	Defeat encryption				Use peer connections	ı
			Survey devices		Leverage device swapping	Exploit remote application vulnerability	Run fileless payload	Map accessible networks	New Service	Virtualization Attacks	Use remote services	Modify configuration to facilitate launch		Send over C2 channel					Use remote shell	ı
			Use social media		Send malicious email	Exploit weak access controls	Use interpreted scripts	Scan connected devices	Service File Permission Weakness		Write to remote file shares	Modify existing services		Send over non-C2 channel					Use removable media	Ì
					Transport via common network infrastructure	Hjack	Use OS APIs	Sniff network	Weak Access Control for Service Configuration		Write to shared webroot	Modify links		Send over other network medium					Custom Application Layer Protocol	
					Traverse CDS or MLS	Impersonate or spoof user	Use remote services		Multi Tenant Side Channel Cache Attack		Virtualization Attacks	Modify service configuration		Throttle data					C2 via Cloud Service	ľ
					Use chat services	Launch zero-day exploit	Use trusted application to execute untrusted code				Exploitation of Vulnerability	Replace service binary		Transfer via physical means				9.5		
					Use compromised host	Leverage exploit packs	Write to disk					Set to load at startup		Traverse CDS or MLS						
	22				Use legitimate remote access	Leverage trusted relationship	File Access					Use library-search hijack		Virtualization Attacks						ı
					Use physical network bridge Application or	Replay	Leverage path- order execution					Legitimate Credentials		Exfil over Virtual Medium						
					Operating System Exploit over the Network	Targets Web Application Vulnerabilities (ex. XSS, CSRF, SQL)						Install Hypervisor Rootkit		Exfil via Cloud Service						
					Virtualization Attacks	Legitimate Access														
					Auto Delivery via Cloud Service															



nitial 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) Store files in unconventional

Block indicators on host Degrade security

Delay activity

Impersonate legitimate file

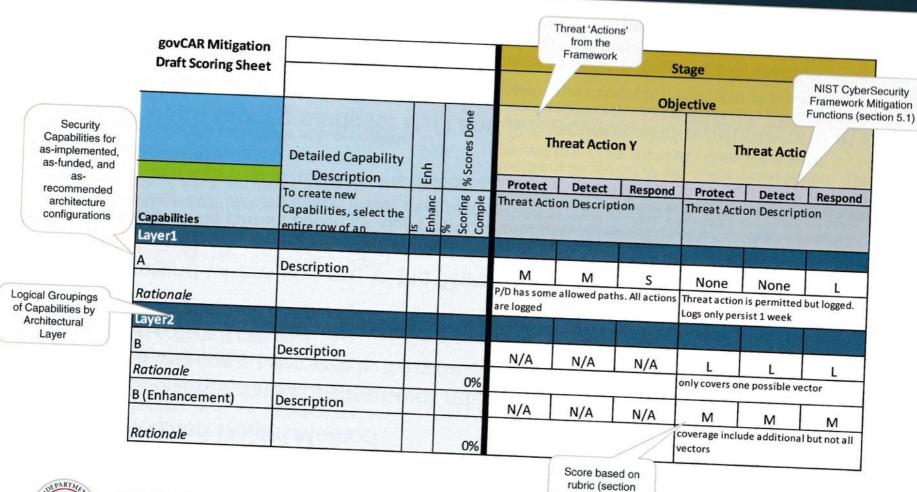
Threat Heat map

- 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

	Sta	y 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



Protect, Detect, Respond (PDR) Scoring Spreadsheet



5.1.1)

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



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.

PDR Analysis: Aggregating the Scores -Threat Coverage Roll-Up Title of set and list of PDR

functions





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.

Unclassified//For Official Use Only

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