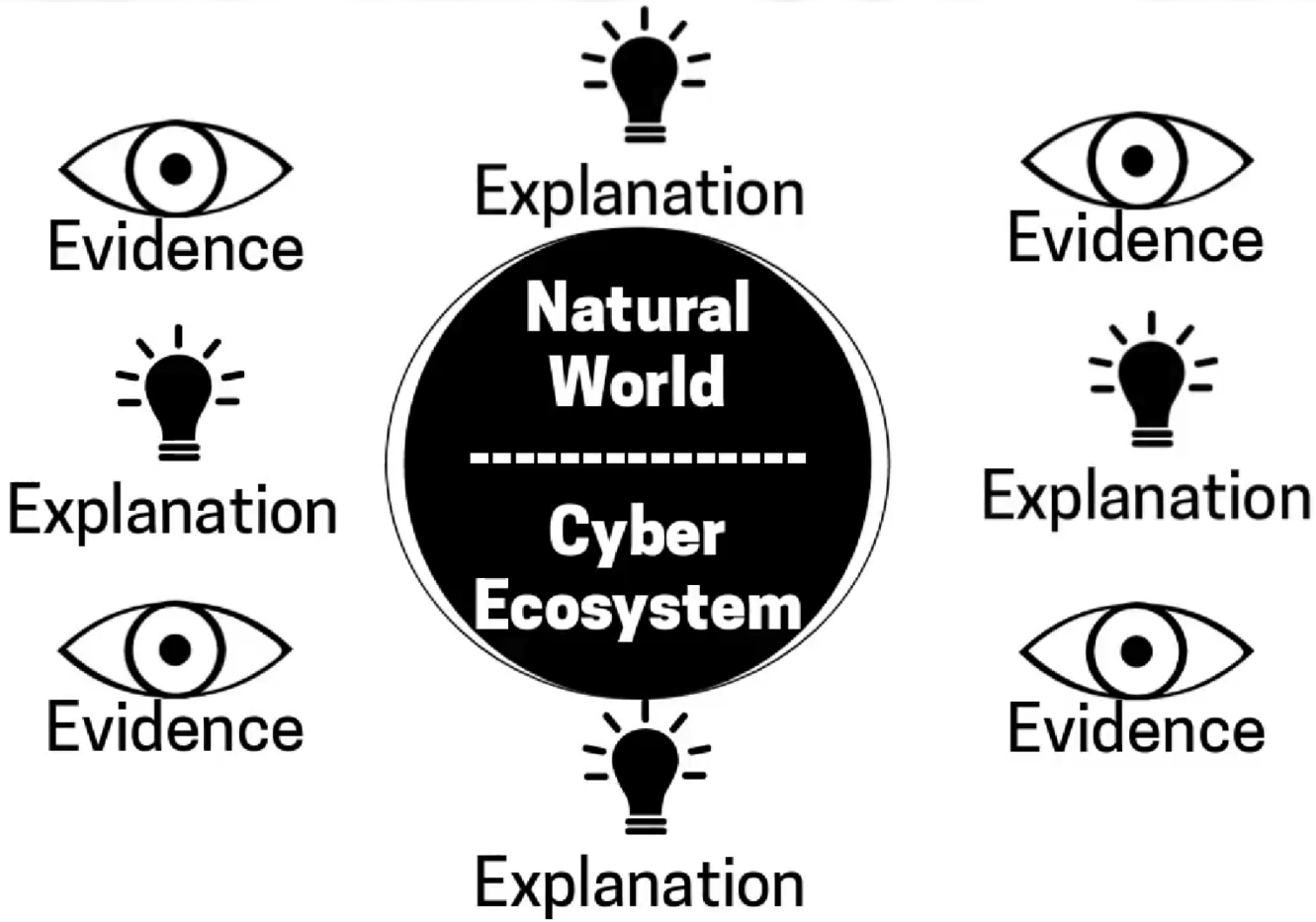
Understanding Resiliency Effects On Adversary Behavior

By

Shawn Riley, CDO & CISO, DarkLight, Inc.

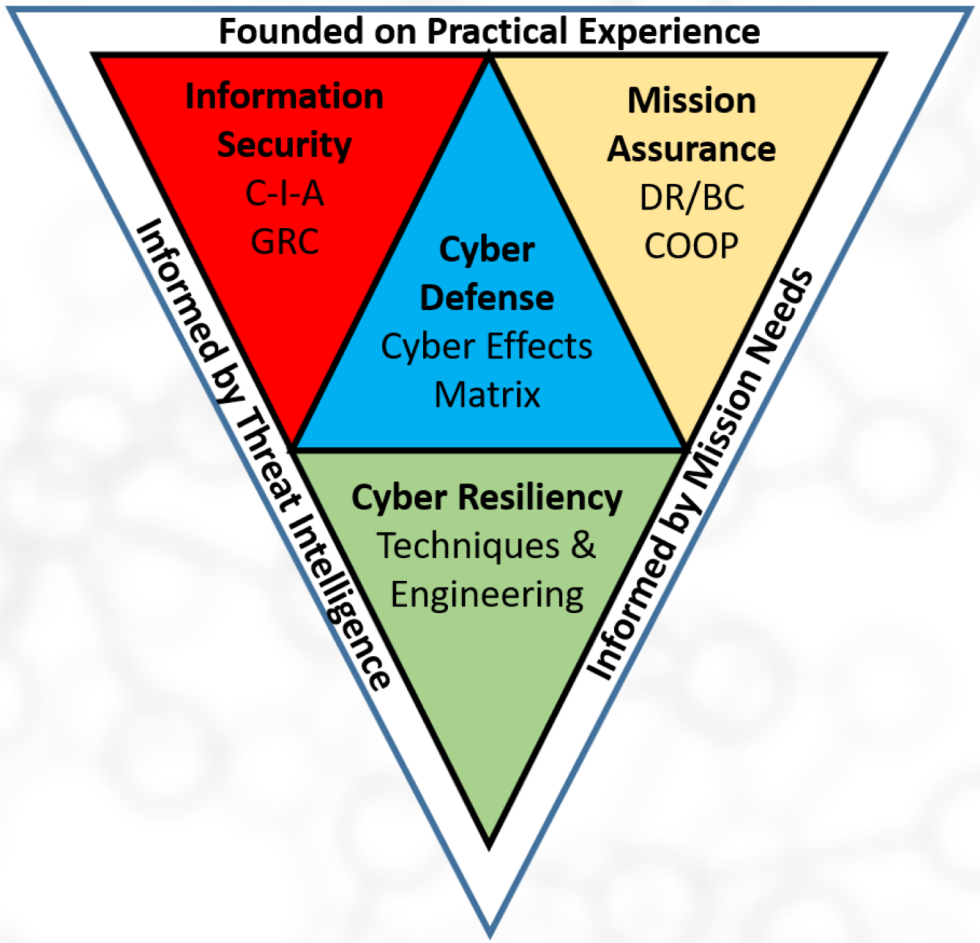
Science is about making sense of the evidence



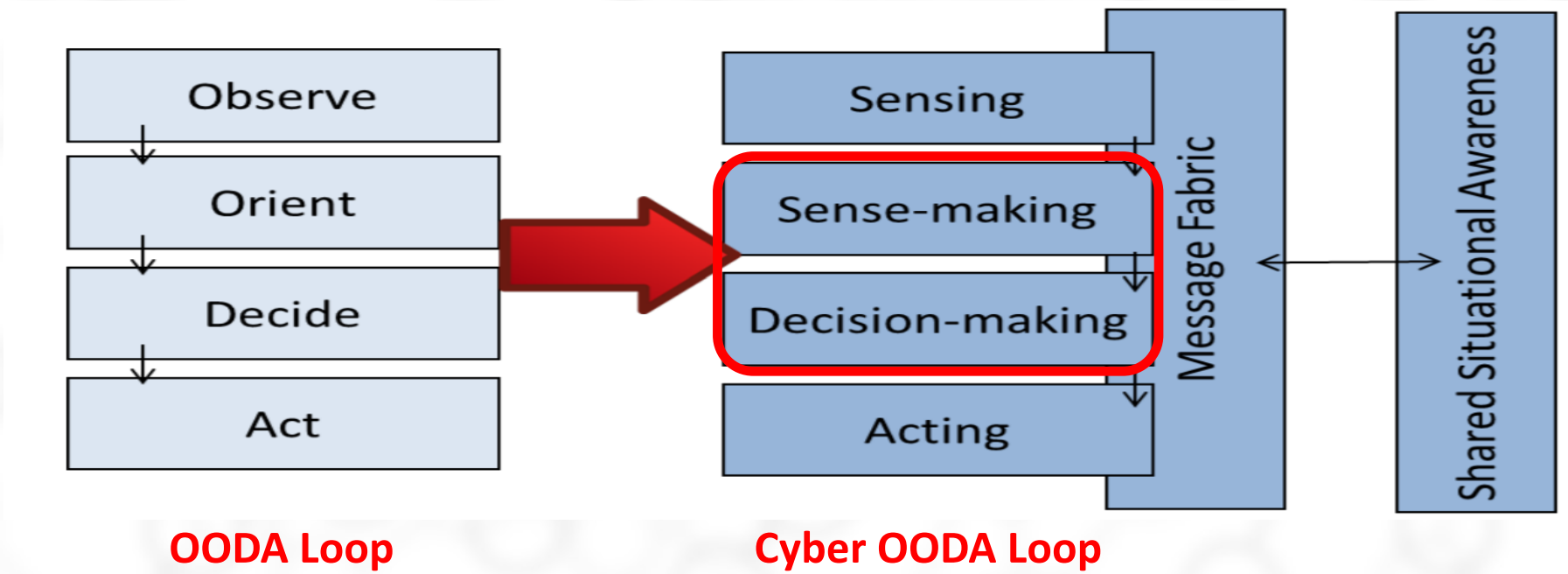
What is Cybersecurity Science?

- Security science is taken to mean **a body of knowledge containing laws, axioms and provable theories** relating to some aspect of cyber security. Security science should provide an understanding of what is possible in the security domain, by **providing objective and qualitative or quantifiable descriptions of security properties and behaviors**. The notions embodied in security science should have broad applicability - **transcending specific systems, attacks, and defensive mechanisms**.
- There are a set of 7 core themes that together form the foundational basis for security science discipline. The themes are strongly interrelated, and mutually inform and benefit each other. They are: **Common Language, Core Principles, Attack Analysis, Measurable Security, Risk, Agility,** and **Human Factors.**

Operational Cyber Defense Knowledge



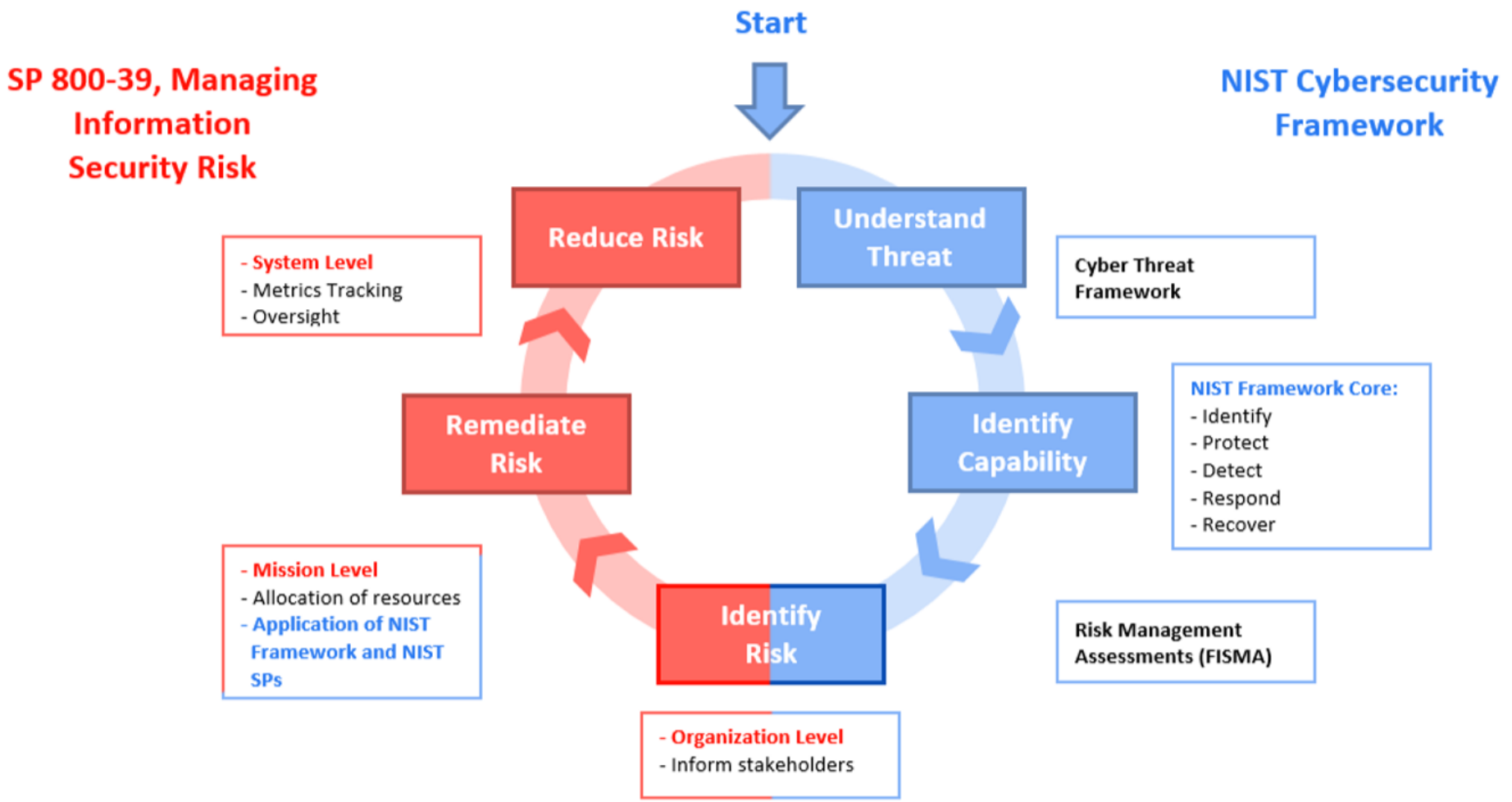
The Cyber OODA Loop



Federal Cybersecurity Risk Determination Report and Action Plan

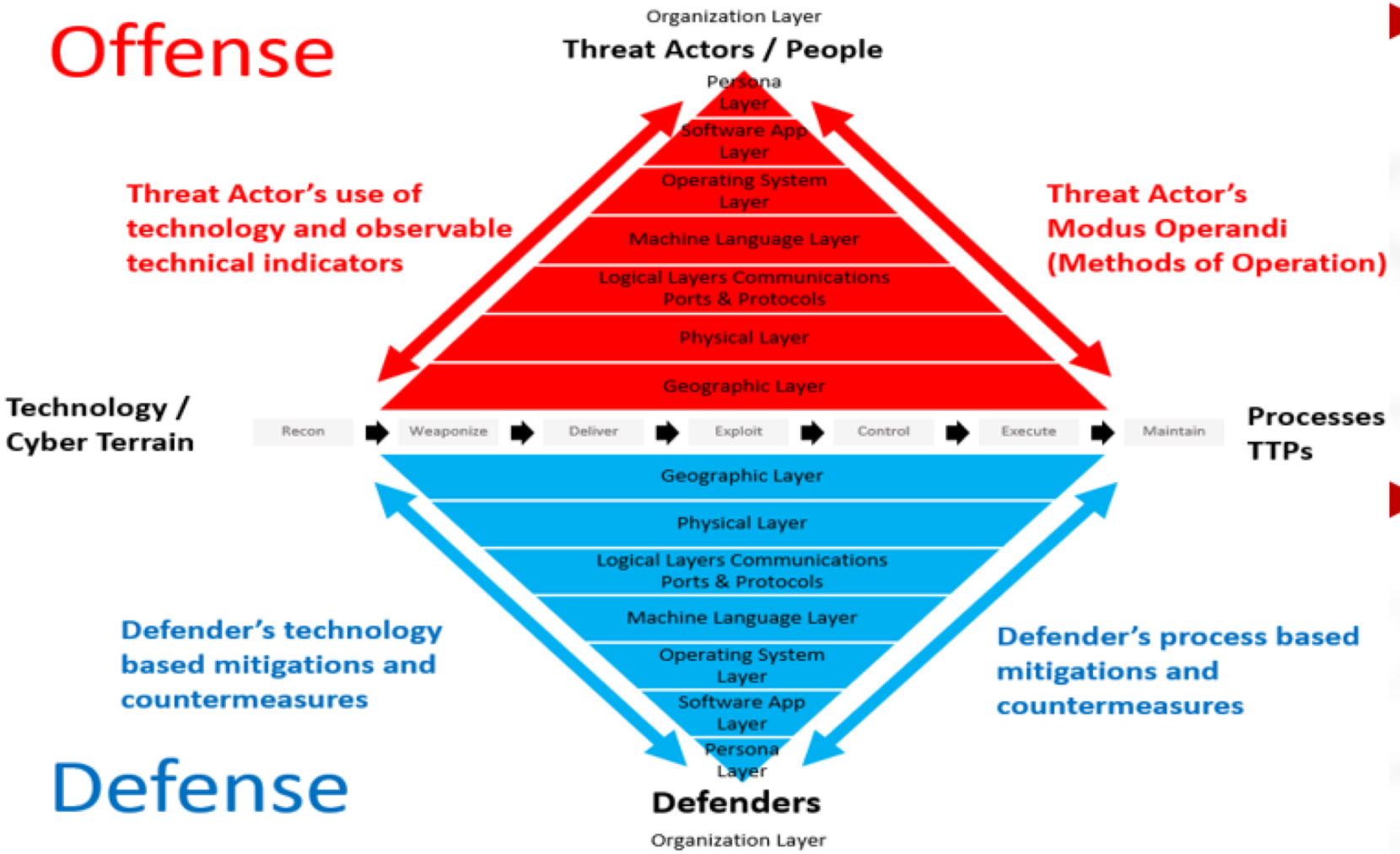
OMB
May 2018

Figure 1: Cyber Risk Management Lifecycle Management



Adversary Attack Goals vs Defender Resiliency Goals

Offense

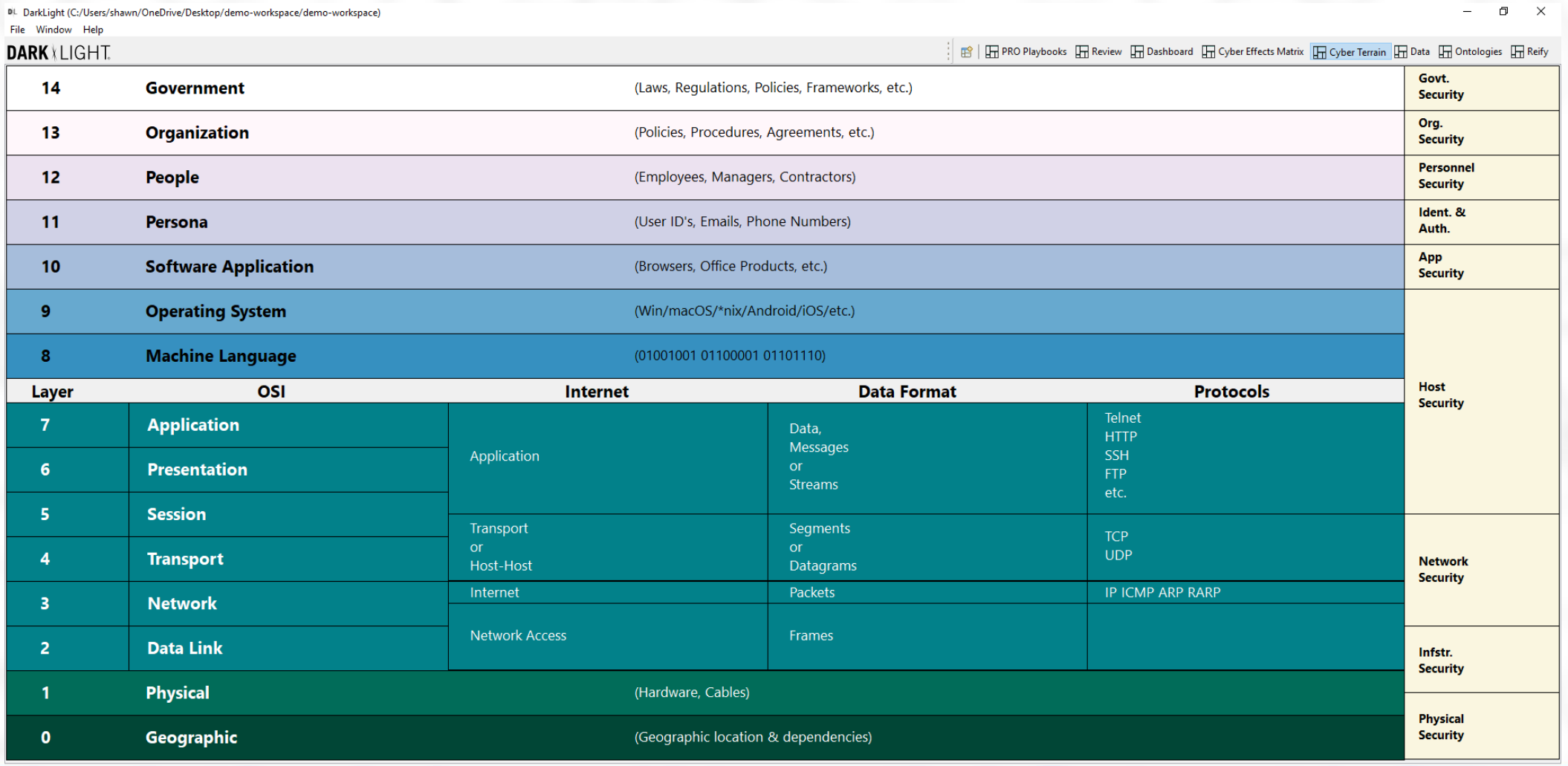


Defense

- Stages / Goal
  - Tactics / Objective
    - Techniques / Activity
      - Procedures / Recipe (Indicators)
        - Tools (Indicators)
          - Host and/or Network Artifacts (Indicators)
- Goals
  - Objectives
    - Techniques
      - Approaches
        - Countermeasures, Mitigations, and Courses of Action
          - Effects

DARK LIGHT

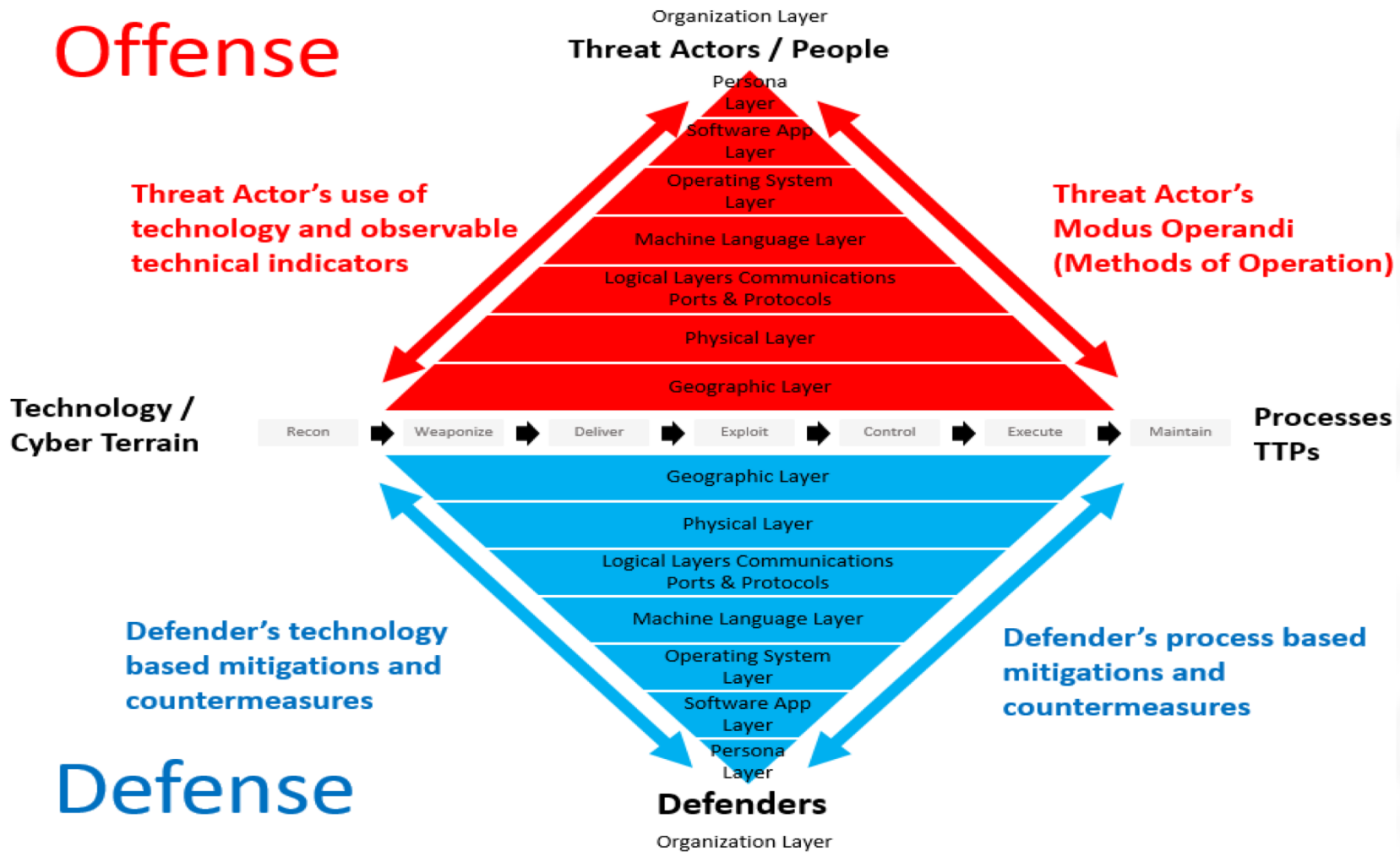
Cyber Environment w/Terrain Layers



14	**Government**	(Laws, Regulations, Policies, Frameworks, etc.)			**Govt. Security**
13	**Organization**	(Policies, Procedures, Agreements, etc.)			**Org. Security**
12	**People**	(Employees, Managers, Contractors)			**Personnel Security**
11	**Persona**	(User ID's, Emails, Phone Numbers)			**Ident. & Auth.**
10	**Software Application**	(Browsers, Office Products, etc.)			**App Security**
9	**Operating System**	(Win/macOS/*nix/Android/iOS/etc.)			**Host Security**
8	**Machine Language**	(01001001 01100001 01101110)			
Layer	**OSI**	**Internet**	**Data Format**	**Protocols**	
7	**Application**	Application	Data, Messages or Streams	Telnet HTTP SSH FTP etc.	
6	**Presentation**				
5	**Session**				
4	**Transport**	Transport or Host-Host	Segments or Datagrams	TCP UDP	**Network Security**
3	**Network**	Internet	Packets	IP ICMP ARP RARP	
2	**Data Link**	Network Access	Frames		**Infstr. Security**
1	**Physical**	(Hardware, Cables)			**Physical Security**
0	**Geographic**	(Geographic location & dependencies)			

DARK LIGHT™

Adversary & Defender Knowledge



"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

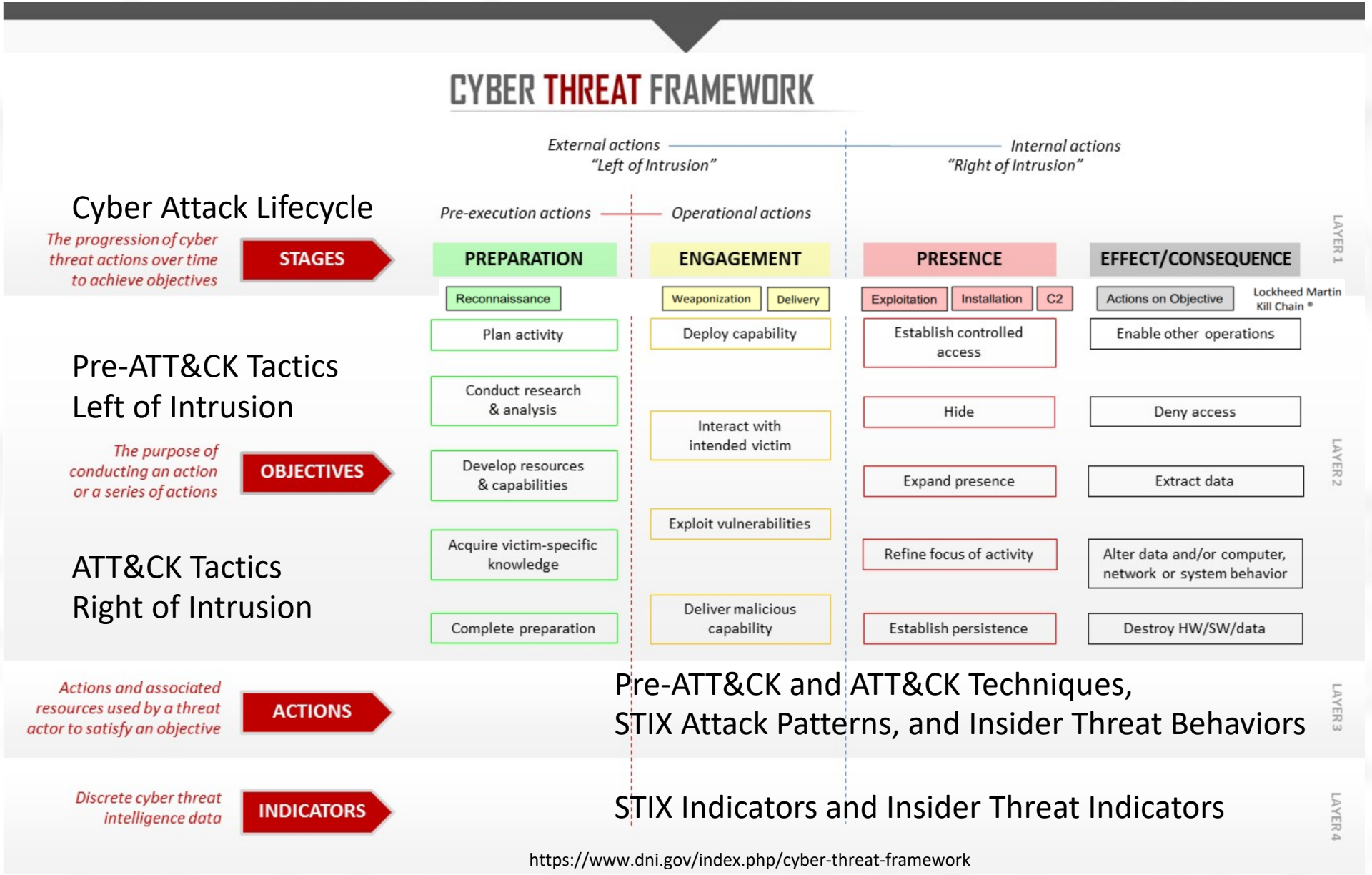
— **Sun Tzu**, **The Art of War**

DARK LIGHT

Deriving a 'Best of Breed' Common Framework

	Preparation	Engagement	Presence	Effect/Consequence
NSA	Intent, Resource development, Reconnaissance, Staging	Target ID, Delivery, Exploitation	Maintain/expand Target access, Establish/modify Network infrastructure, Detection avoidance, C2	Deny Access, Extract Data, Manipulate
STIX™	Intent, Development, Reconnaissance, Staging	Engagement	Maneuver, Configure, C2	Effect
NSA 10 Step	Intent, Reconnaissance, Development, Staging	Delivery	Configure, Maneuver, Exploitation, C2	Effect
ALA	Administer, Prepare	Engage	Propagate	Effect
CNE	Administration	Targeting	Compromise, Propagation	Effects
Lockheed Martin Kill Chain ®	Reconnaissance	Weaponization, Delivery	Exploitation, Installation, C2	Actions on Objective
VERIS Categories of Threat Actions	Malware, Hacking, Social	Environmental threat	Physical threat, Misuse, Error	
JCAC Exploitation	Foot printing, Scanning, Enumeration	Gain access (exploitation)	Privilege escalation, Situational awareness, Covering tracks	Creating Backdoors

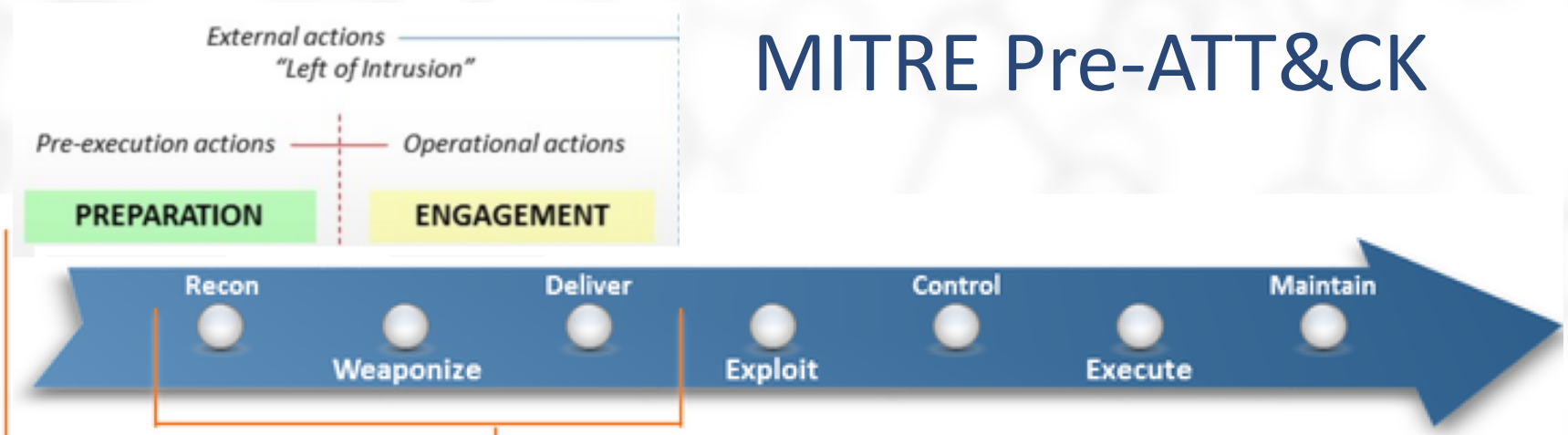
DARK LIGHT™



https://www.dni.gov/index.php/cyber-threat-framework

DARK LIGHT™

MITRE Pre-ATT&CK



Priority Definition
- Planning, Direction

Target Selection

Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec

Establish & Maintain Infrastructure

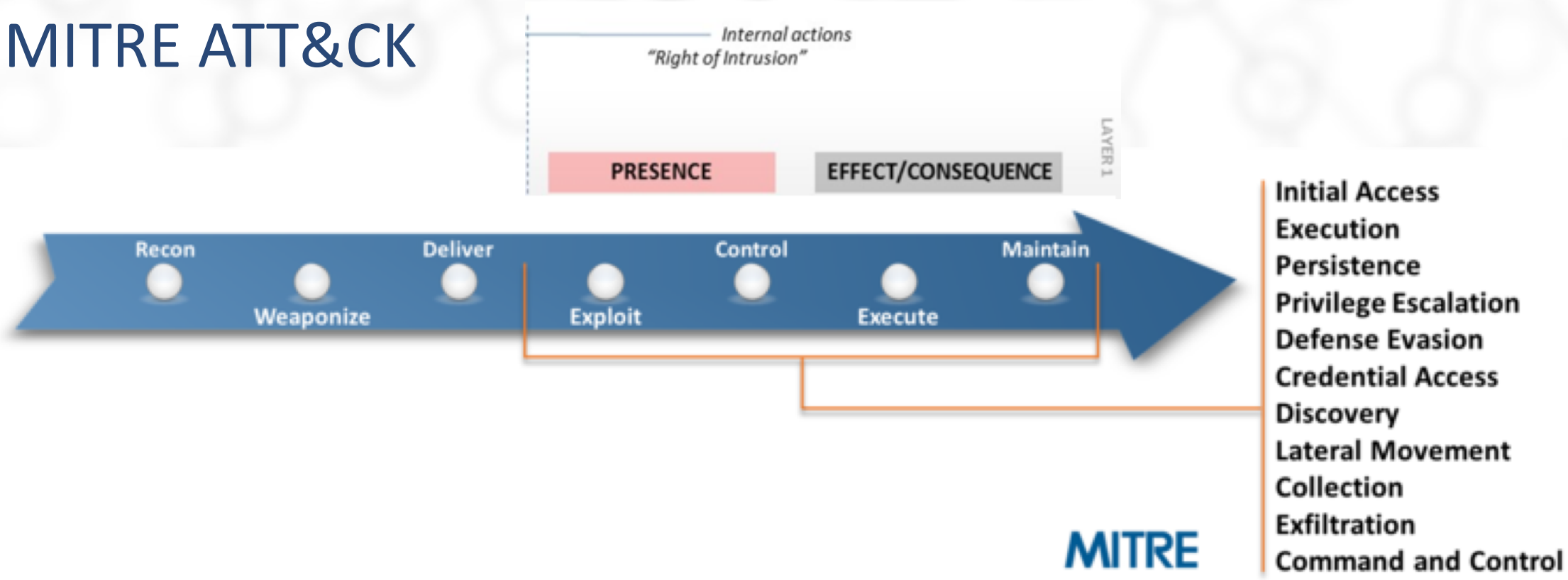
Persona Development

Build Capabilities

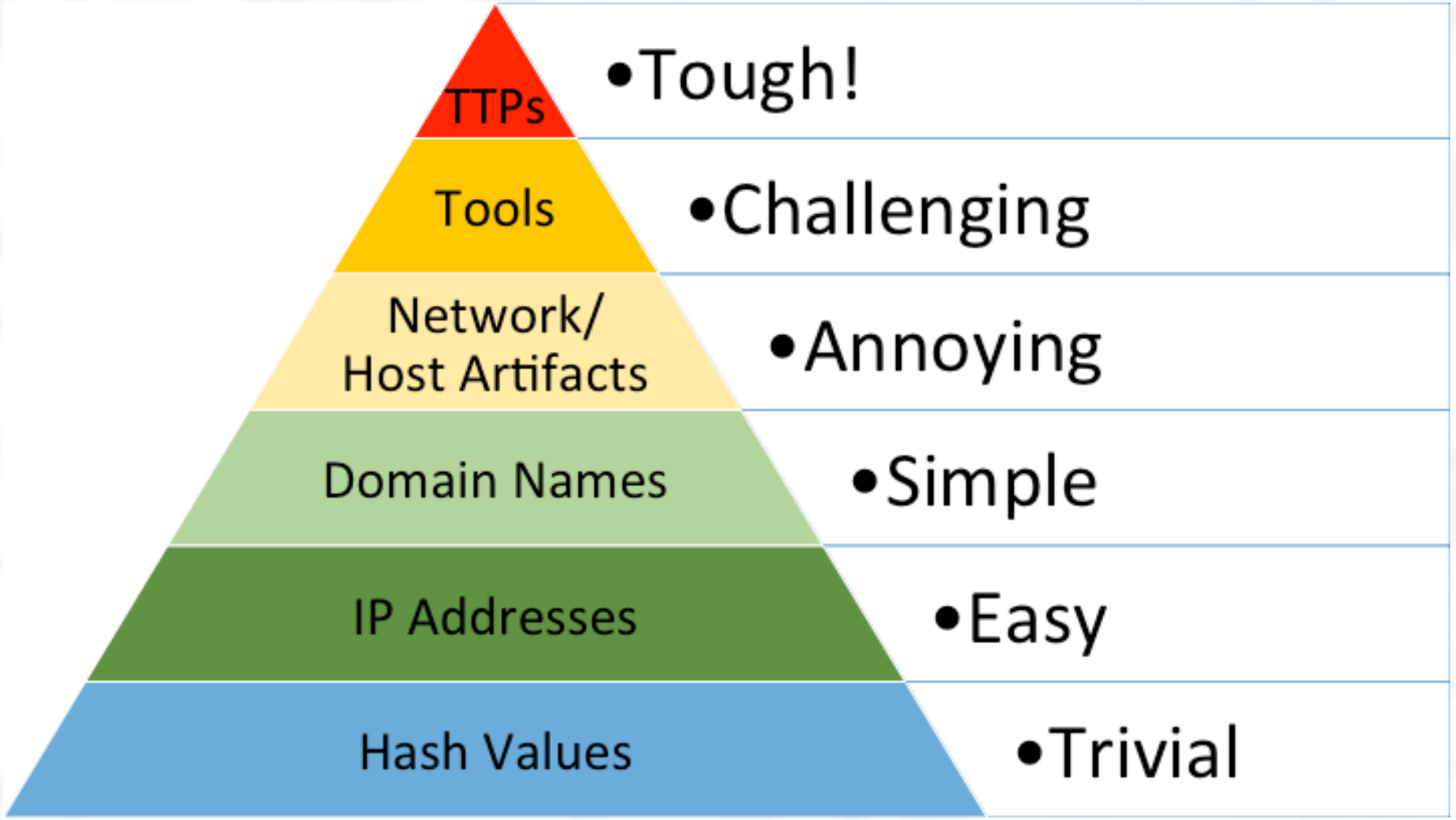
Test Capabilities

Stage Capabilities

MITRE ATT&CK


Internal actions
"Right of Intrusion"
PRESENCE
EFFECT/CONSEQUENCE
LAYER 1
Recon
Weaponize
Deliver
Exploit
Control
Execute
Maintain
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
MITRE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Securityd Memory	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Two-Factor Authentication Interception	System Time Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	SID-History Injection	Gatekeeper Bypass						Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Scheduled Task	HISTCONTROL						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	Hidden Files and Directories						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Setuid and Setgid	Hidden Users						
	Source	LSASS Driver	Startup Items	Hidden Window						
	Space after Filename	Launch Agent	Sudo	Image File Execution Options Injection						
	Third-party Software	Launch Daemon	Sudo Caching	Indicator Blocking						
	Trap	Launchctl	Valid Accounts	Indicator Removal from Tools						
	Trusted Developer Utilities	Local Job Scheduling	Web Shell	Indicator Removal on Host						
	User Execution	Login Item		Indirect Command Execution						
	Windows Management Instrumentation	Logon Scripts		Install Root Certificate						
	Windows Remote Management	Modify Existing Service		InstallUtil						
		Netsh Helper DLL		LC_MAIN Hijacking						
		New Service		Launchctl						
		Office Application Startup		Masquerading						
		Path Interception		Modify Registry						
		Plist Modification		Mshta						
		Port Knocking		NTFS File Attributes						
		Port Monitors		Network Share Connection Removal						
		Rc.common		Obfuscated Files or Information						
		Re-opened Applications		Plist Modification						
		Redundant Access		Port Knocking						
		Registry Run Keys / Start Folder		Process Doppelgänging						
		SIP and Trust Provider Hijacking		Process Hollowing						
		Scheduled Task		Process Injection						
		Screensaver		Redundant Access						
		Security Support Provider		Regsvcs/Regasm						
		Service Registry Permissions Weakness		Regsvr32						
		Shortcut Modification		Rootkit						
		Startup Items		Rundll32						
		System Firmware		SIP and Trust Provider Hijacking						
		Time Providers		Scripting						
		Trap		Signed Binary Proxy Execution						
		Valid Accounts		Signed Script Proxy Execution						
		Web Shell		Software Packing						
		Windows Management Instrumentation Event Subscription		Space after Filename						
		Winlogon Helper DLL		Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						


TTPs
•Tough!
Tools
•Challenging
Network/
Host Artifacts
•Annoying
Domain Names
•Simple
IP Addresses
•Easy
Hash Values
•Trivial

Identify Capability - NIST Cybersecurity Framework

Left and Right of "Boom"

#RSAC

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications		Pre-Event Structural Awareness			
Networks					
Data			Post-Event Situational Awareness		
Users					
Degree of Dependency	Technology / Process	Technology / Process	Technology / People / Process	People / Process	People / Process

@sounilyu from RSAC 2016

RSAConference2016

DARK LIGHT

NIST 800-160 Vol 2 Cyber Resiliency Engineering Framework

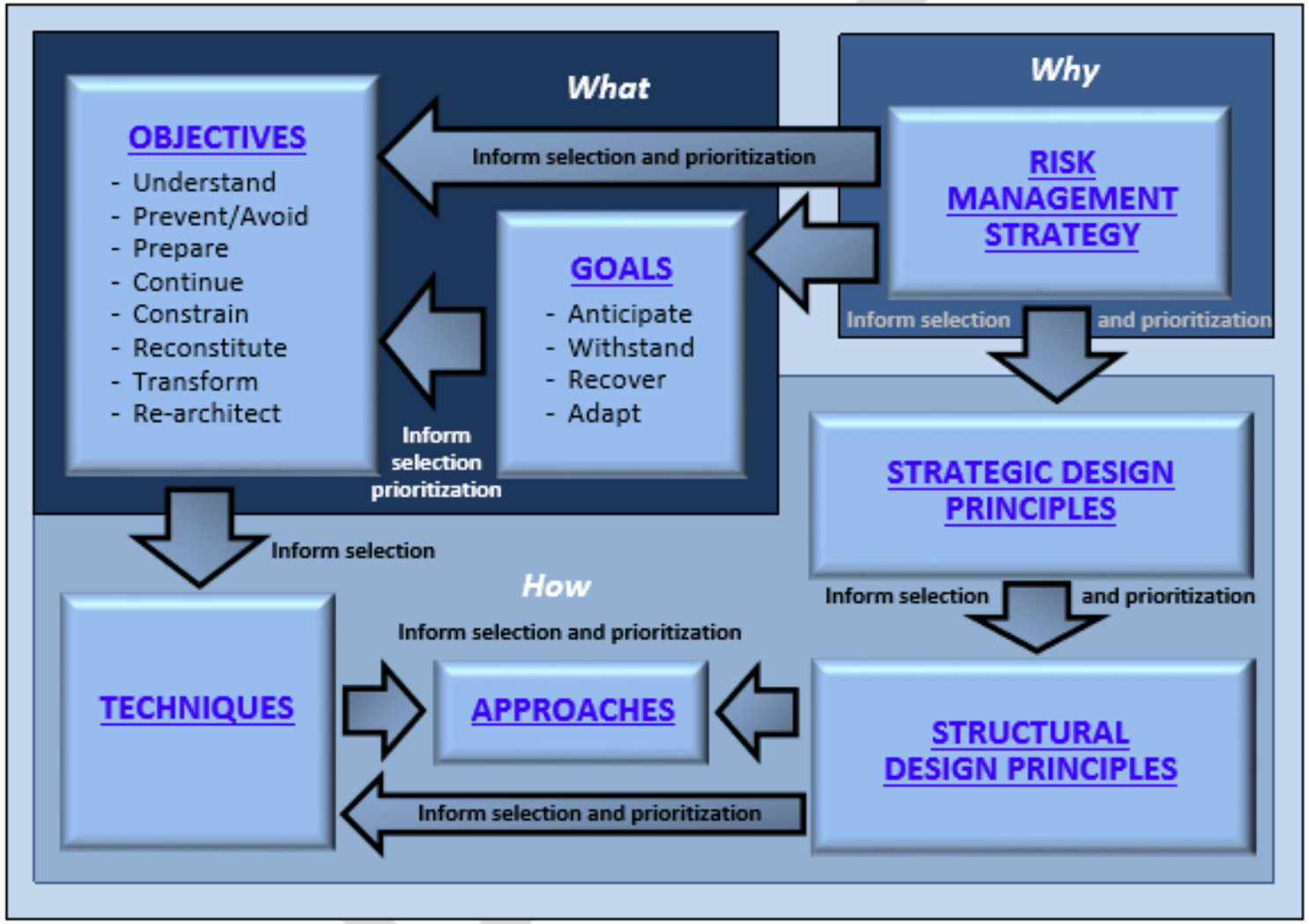


FIGURE 1: RELATIONSHIPS AMONG CYBER RESILIENCY CONSTRUCTS

DARK LIGHT

TECHNIQUES	APPROACHES	EXAMPLES
Adaptive Response Implement nimble cyber courses of action to manage risks.	**Dynamic Reconfiguration** Make changes to individual systems, system elements, components, or sets of cyber resources to change functionality or behavior without interrupting service.	• Dynamically change router rules, access control lists, intrusion detection and prevention system parameters, and filter rules for firewalls and gateways.
	Dynamic Resource Allocation Change the allocation of resources to tasks or functions without terminating critical functions or processes.	• Employ dynamic provisioning. • Reprioritize messages or services. • Implement load balancing. • Provide emergency shutoff capabilities. • Pre-empt communications.
	Adaptive Management Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment.	• Disable access dynamically. • Implement adaptive authentication. • Provide for automatic disabling of the system. • Provide dynamic deployment of new or replacement resources or capabilities.
Analytic Monitoring Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.	**Monitoring and Damage Assessment** Monitor and analyze behavior and characteristics of components and resources to look for indicators of	• Employ Continuous Diagnostics and Mitigation (CDM) or other vulnerability scanning tools. • Deploy Intrusion Detection Systems (IDSs) and other monitoring tools.
	adversary activity, and to detect and assess damage from adversity.	• Use Insider Threat monitoring tools. • Perform telemetry analysis. • Detect malware beaconing. • Monitor open source information for indicators of disclosure or compromise.
	Sensor Fusion and Analysis Fuse and analyze monitoring data and analysis results from different components, together with externally provided threat intelligence.	• Enable organization-wide situational awareness. • Implement cross-organizational auditing. • Correlate data from different tools. • Fuse data from physical access control systems and information systems.
	Malware and Forensic Analysis Analyze malware and other artifacts left behind by adverse events.	• Deploy an integrated team of forensic and malware analysts, developers, and operations personnel. • Use reverse engineering and other
Coordinated Protection Ensure that protection mechanisms operate in a coordinated and effective manner.	**Calibrated Defense-in-Depth** Provide complementary protective mechanisms at different architectural layers or in different locations, calibrating the strength and number of mechanisms to resource value.	• Design for defense-in-depth. • Employ multiple, distinct authentication challenges over the course of a session to confirm identity. • Combine network and host-based intrusion detection. • Provide increasing levels of protection to access more sensitive or critical resources. • Conduct sensitivity and criticality analyses.
	Consistency Analysis Determine whether and how protections can be applied in a coordinated, consistent way that minimizes interference, potential cascading failures, or coverage gaps.	• Employ unified IdAM administration tools. • Analyze mission/business process flows and threads. • Employ privilege analysis tools to support an ongoing review of whether user privileges are assigned consistently. • Interpret attributes consistently. • Coordinate the planning, training, and testing of incident response, contingency planning, etc. • Design for facilitating coordination and mutual support among safeguards.
	Orchestration Coordinate the ongoing behavior of mechanisms and processes at	• Coordinate incident handling with mission/business process continuity
	different layers, in different locations, or implemented for different aspects of trustworthiness to avoid causing cascading failures, interference, or coverage gaps.	of operations and organizational processes. • Conduct coverage planning and management for sensors. • Use cyber playbooks.
	Self-Challenge Affect mission/business processes or system elements adversely in a controlled manner, to validate the effectiveness of protections and to enable proactive response and improvement.	• Conduct role-based training exercises. • Conduct penetration testing and Red Team exercises. • Test automated incident response. • Employ fault injection. • Conduct tabletop exercises.

NIST 800-160 Vol 2 Cont.

TABLE G-1: NIST 800-53 CONTROLS SUPPORTING CYBER RESILIENCY AND RELEVANT TECHNIQUES

CONTROL NO.	CONTROL OR CONTROL ENHANCEMENT NAME	RESILIENCY TECHNIQUE
Access Control		
AC-2 (6)	ACCOUNT MANAGEMENT | *DYNAMIC PRIVILEGE MANAGEMENT*	Privilege Restriction Adaptive Response
AC-2 (12)	ACCOUNT MANAGEMENT | *ACCOUNT MONITORING / ATYPICAL USAGE*	Analytic Monitoring
AC-3 (2)	ACCESS ENFORCEMENT | *DUAL AUTHORIZATION*	Privilege Restriction
AC-3 (9)	ACCESS ENFORCEMENT | *CONTROLLED RELEASE*	Privilege Restriction
AC-4 (2)	INFORMATION FLOW ENFORCEMENT | *PROCESSING DOMAINS*	Segmentation
AC-4 (3)	INFORMATION FLOW ENFORCEMENT | *DYNAMIC INFORMATION FLOW CONTROL*	Adaptive Response
AC-4 (8)	INFORMATION FLOW ENFORCEMENT | *SECURITY POLICY FILTERS*	Substantiated Integrity
AC-4 (21)	INFORMATION FLOW ENFORCEMENT | *PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*	Segmentation
AC-6	LEAST PRIVILEGE	Privilege Restriction
AC-6 (1)	LEAST PRIVILEGE | *AUTHORIZE ACCESS TO SECURITY FUNCTIONS*	Privilege Restriction
AC-6 (2)	LEAST PRIVILEGE | *NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS*	Privilege Restriction
AC-6 (3)	LEAST PRIVILEGE | *NETWORK ACCESS TO PRIVILEGED COMMANDS*	Privilege Restriction
AC-6 (4)	LEAST PRIVILEGE | *SEPARATE PROCESSING DOMAINS*	Privilege Restriction

TABLE H-1: CYBER RESILIENCY OBJECTIVES SUPPORT CYBER RESILIENCY GOALS

Objectives \ Goals	ANTICIPATE	WITHSTAND	RECOVER	ADAPT
Prevent/Avoid	X	X		
Prepare	X	X	X	X
Continue		X	X	
Constrain		X	X	
Reconstitute			X	
Understand	X	X	X	X
Transform			X	X
Re-Architect			X	X

TABLE H-2: TECHNIQUES AND IMPLEMENTATION APPROACHES TO ACHIEVE OBJECTIVES

Techniques/Approaches \ Objectives	Prevent Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
Adaptive Response	X	X	X	X	X	X		
Dynamic Reconfiguration	X		X	X	X	X		
Dynamic Resource Allocation	X		X	X	X			
Adaptive Management	X	X	X	X	X	X		
Analytic Monitoring		X	X	X	X	X		
Monitoring and Damage Assessment			X	X	X	X		
Sensor Fusion and Analysis						X		
Malware and Forensic Analysis						X		
Coordinated Protection	X	X	X		X	X	X	X
Calibrated Defense-in-Depth	X	X			X			
Consistency Analysis	X	X			X	X	X	X
Orchestration	X	X	X		X	X	X	X

Cyber Resiliency Effects on Adversary Activities

- Deter, divert, and deceive in support of redirect;
- Prevent, preempt, and expunge in support of preclude;
- Contain, degrade and delay in support of impede;
- Shorten and recover in support of limit; and
- Detect, reveal, and scrutinize in support of expose

- NIST 800-160 vol 2 DRAFT

Effects of Cyber Resiliency Techniqueso n Adversary Threat Events

TABLE I-1: EFFECTS OF CYBER RESILIENCY TECHNIQUES ON ADVERSARIAL THREAT EVENTS

INTENDED EFFECT	EFFECT ON RISK	EXPECTED RESULT
Redirect (includes deter, divert, and deceive): Direct adversary activities away from defender-chosen targets.	Reduce likelihood of occurrence and, (to a lesser extent) reduce likelihood of impact.	• The adversary's efforts cease, or become misinformed. • The adversary targets incorrectly.
Deter: Discourage the adversary from undertaking further activities, by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve intended effects (e.g., that targets exist).	Reduce likelihood of occurrence.	• The adversary ceases or suspends activities. **Example**: The defender uses disinformation to make it appear that the organization is better able to detect attacks than it is, and is willing to launch major counter strikes. The result is that the adversary chooses to not launch attack due to fear of detection and reprisal.
Divert: Lead the adversary to direct activities away from defender-chosen targets.	Reduce likelihood of occurrence.	• The adversary refocuses activities on different targets (e.g., other organizations, defender-chosen alternate targets). • The adversary's efforts are wasted. **Example**: The defender uses selectively planted false information (disinformation) and honeynets (misdirection) to cause an adversary to focus its malware at virtual sandboxes, while at the same time employing obfuscation to hide the actual resources. The result is that the adversary's attacks are directed away from critical resources.
Deceive: Lead the adversary to believe false information about defended systems, missions, or organizations, or about defender capabilities or TTPs.	Reduce likelihood of occurrence and/or reduce likelihood of impact.	• The adversary's efforts are wasted, as the assumptions on which the adversary bases attacks are false. **Example:** The defender strategically places false information (disinformation) about the cybersecurity investments that it plans to make. As a result, the adversary's malware development is wasted by being focused on countering nonexistent cybersecurity protections.
Preclude (includes expunge, preempt, and prevent): Ensure that specific threat events do not have an effect.	Reduce likelihood of occurrence and/or reduce likelihood of impact.	• The adversary's efforts or resources cannot be applied or are wasted.
Expunge: Remove unsafe, incorrect, or corrupted resources that could cause damage.	Reduce likelihood of impact of subsequent events in the same threat scenario.	• The adversary loses a capability for some period, as adversary-directed threat mechanisms (e.g., malicious code) are removed. • Adversary-controlled resources are so badly damaged that they cannot perform any function or be restored to a usable condition without being entirely rebuilt. **Example:** The defender uses virtualization to refresh critical software (*non-persistent* services) at random intervals (temporal unpredictability). As a result, the adversary's malware that is implanted in the software is expunged.
Preempt: Forestall or avoid conditions under which the threat event could occur or result in an effect.	Reduce likelihood of occurrence and/or reduce likelihood of impact.	• The adversary's resources cannot be applied and/or the adversary cannot perform activities (e.g., because resources are destroyed or made inaccessible). **Example:** Critical software is not assembled (adaptive management) or activated (non-persistent services) until it is needed. The adversary, therefore, cannot perform reconnaissance on, and tailor malware targeted to, the software.
Prevent: Create conditions under which the threat event cannot be expected to result in an effect.	Reduce likelihood of impact.	• The adversary's efforts are wasted, as the assumptions on which the adversary based its attack are no longer valid and as a result, the intended effects cannot be achieved. **Example:** Subtle variations in critical software are implemented (synthetic diversity), with the result that the adversary's malware is no longer able to compromise the targeted software.
Impede (includes contain, degrade and delay): Make it more difficult for threat events to cause adverse impacts or consequences.	Reduce likelihood of impact and reduce level of impact.	• To achieve the intended effects, the adversary should invest more resources or undertake additional activities.
Contain: Restrict the effects of the threat event to a limited set of resources.	Reduce level of impact.	• The value of the activity to the adversary, in terms of achieving the adversary's goals, is reduced. **Example:** The defender organization makes changes to a combination of internal firewalls and logically separated networks (dynamic segmentation) to isolate enclaves in response to detection of malware, with the result that the

DARK LIGHT™

INTENDED EFFECT	EFFECT ON RISK	EXPECTED RESULT
		effects of the malware is limited to just initially infected enclaves.
Degrade: Decrease the likelihood that a given threat event will have a given level of effectiveness or impact.	Reduce likelihood of impact and reduce level of impact.	• The adversary achieves some but not all intended effects. • The adversary achieves all intended effects but only after taking additional actions. **Example**: The defender uses multiple browsers and operating systems (architectural diversity) on both end user systems and some critical servers. The result is that malware that is targeted at specific software can only compromise a subset of the targeted systems; a sufficient number continue to operate to keep mission going, although in degraded mode.
Delay: Increase the amount of time needed for a threat event to result in adverse impacts.	Reduce likelihood of impact and reduce level of impact.	• The adversary achieves the intended effects, but may not achieve them within the intended period. • The adversary's activities may, therefore, be exposed to greater risk of detection and analysis. **Example**: The protection measures (e.g., access controls, encryption) allocated to resources increase in number and strength based on resource criticality (calibrated defense-in-depth). The frequency of authentication challenges varies randomly (temporal unpredictability) and with increased frequency for more critical resources. The result is that it takes the attacker more time to successfully compromise the targeted resources.
Limit (includes shorten and recover): Restrict the consequences of threat events by limiting the damage or effects they cause in terms of time, system resources, and/or mission or business impacts.	Reduce level of impact and reduce likelihood of impact of subsequent events in the same threat scenario.	• The adversary's effectiveness is limited.
Shorten: Limit the duration of a threat event or the conditions caused by a threat event.	Reduce level of impact.	• The time period during which the adversary's activities have their intended effects is limited. **Example**: The defender employs a diverse set of suppliers (supply chain diversity) for time-critical components. As a result, when an adversary's attack on one supplier causes it to shut down, the defender can increase its use of the other suppliers, thus shortening the time when it is without the critical components.
Recover: Roll back the consequences of a threat event, particularly with respect to mission or business impairment.	Reduce level of impact.	• The adversary fails to retain mission or business impairment due to recovery of the capability to perform key missions or business operations. **Example**: Resources determined to be corrupted or suspect (integrity checks, behavior validation) are restored from a clean copy (protected backup and restore).
Expose (includes detect, scrutinize and reveal): Reduce risk due to ignorance of threat events and possible replicated or similar threat events in the same or similar environments.	Reduce likelihood of impact.	• The adversary loses the advantage of stealth, as defenders are better prepared by developing and sharing threat intelligence.
Detect: Identify threat events or their effects by discovering or discerning the fact that an event is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur.	Reduce likelihood of impact and reduce level of impact (depending on responses).	• The adversary's activities become susceptible to defensive responses. **Example**: The defender continually moves its sensors (functional relocation of sensors), often at random times (temporal unpredictability), to common points of egress from the organization. They combine this with the use of beacon traps (tainting). The result is that the defender can quickly detect efforts by the adversary to exfiltrate sensitive information.
Scrutinize: Analyze threat events and artifacts associated with threat events, particularly with respect to patterns of exploiting vulnerabilities, predisposing conditions, and weaknesses, to inform more effective detection and risk response.	Reduce likelihood of impact.	• The adversary loses the advantages of uncertainty, confusion, and doubt. • The defender understands the adversary better, based on analysis of adversary activities, including the artifacts (e.g., malicious code) and effects associated with those activities and on correlation of activity-specific observations with other activities (as feasible), and thus can recognize adversary TTPs. **Example**: The defender deploys honeynets (misdirection), inviting attacks by the defender, allowing the defender to apply their TTPs in a safe environment. The defender then analyzes (malware and forensic analysis) the malware captured in the honeynet to determine the nature of the attacker's TTPs, allowing it to develop appropriate defenses.
Reveal: Increase awareness of risk factors and relative effectiveness of remediation approaches across the stakeholder community, to support common, joint, or coordinated risk response.	Reduce likelihood of impact, particularly in the future.	• The adversary loses the advantage of surprise and possible deniability. • The adversary's ability to compromise one organization's systems to attack another organization is impaired, as awareness of adversary characteristics and behavior across the stakeholder community (e.g., across all computer security incident response teams that support a given sector, which might be expected to be attacked by the same actor or actors) is increased. **Example**: The defender participates in threat information sharing, and uses dynamically updated threat intelligence data feeds (dynamic threat modeling) to inform actions (adaptive management).

Effects on Adversary Threats & Effects on Risk Factors

TABLE I-2: EFFECTS OF CYBER RESILIENCY TECHNIQUES AND APPROACHES ON ADVERSARIAL THREATS

TECHNIQUES AND APPROACHES	EFFECTS ON ADVERSARIAL THREATS
Adaptive Response	Contain, Degrade, Delay, Prevent, Recover, Reveal, Shorten
Dynamic Reconfiguration	Degrade, Delay, Prevent, Reveal, Shorten, Recover
Dynamic Resource Allocation	Degrade, Delay, Prevent, Reveal, Shorten, Recover
Adaptive Management	Contain, Degrade, Delay, Prevent, Reveal, Shorten, Recover
Analytic Monitoring	Detect, Scrutinize
Monitoring and Damage Assessment	Detect, Scrutinize
Sensor Fusion and Analysis	Detect
Malware and Forensic Analysis	Scrutinize
Coordinated Protection	Degrade, Delay, Detect
Calibrated Defense-in-Depth	Degrade, Delay
Consistency Analysis	Detect
Orchestration	Detect
Self-Challenge	Detect, Scrutinize
Deception	Scrutinize, Deceive, Degrade, Delay, Detect, Deter, Divert
Obfuscation	Deceive, Degrade, Delay

TABLE I-3: EFFECTS OF CYBER RESILIENCY TECHNIQUES ON RISK FACTORS

	REDUCE IMPACT	REDUCE LIKELIHOOD OF IMPACT	REDUCE LIKELIHOOD OF OCCURENCE
Adaptive Response	X	X	
Analytic Monitoring		X	
Coordinated Protection	X	X	
Deception		X	X
Diversity	X	X	
Dynamic Positioning	X	X	X
Dynamic Representation	X	X	
Non-Persistence	X	X	X
Privilege Restriction	X	X	
Realignment	X	X	X
Redundancy	X	X	
Segmentation	X	X	
Substantiated Integrity	X	X	
Unpredictability	X	X	

DARK LIGHT™

TABLE J-1: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR PERSISTENCE

PERSISTENCE	
Persistence refers to any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures.	
TECHNIQUE: Adaptive Response	
APPROACH: Dynamic Reconfiguration	Making changes to certain resources that the adversary is known to employ (e.g., configuration files) renders the adversary's knowledge of resources and configuration outdated. As a result, the adversary's actions are impeded, making it more difficult for the adversary to maintain its persistent position in the organization's infrastructure. In addition, resource reallocation may result in the removal of resources from the adversary's control that it uses to remain hidden, thus increasing the likelihood that it will be detected. In addition, reconfiguration (e.g., changing internal communications or call paths) renders the adversary's stealthy means of communication ineffective, aiding in revealing the adversary.
TECHNIQUE: Diversity	
APPROACH: Architectural Diversity	The adversary's efforts at persisting are geared toward specific operating systems and architectures (e.g., Windows vs. Linux). The efforts will not work against variant implementations as such implementations are different from the implementations the adversary anticipated (e.g., tools the adversary needs to compromise Windows-based systems are different than those tools needed to compromise Linux-based systems, and therefore adversary will need different tools than originally in its toolset). This will prevent the adversary from establishing a stealthy, persistent presence. Moreover, the failure of the adversary's techniques to achieve a foothold (because it is designed for a specific architecture) will also increase the likelihood that the adversary's presence will be detected. Any effort by the adversary to develop tools capable of compromising all of the architectural designs will cost the adversary additional time and resources, thus delaying the adversary's ability to compromise the resources in a timely manner.
TECHNIQUE: Non-Persistence	
APPROACH: Non-Persistent Services	The adversary's attempt to exploit a vulnerability to achieve a persistent foothold is impeded if the attacked service is terminated because it is no longer needed by the defender. Moreover, if re-instantiated from a clean version, the new instance of the service will not be compromised and malware will no longer exist. Any persistent foothold established by the adversary is eliminated and the adversary is effectively flushed from its foothold. Even if a foothold is not eliminated, the restart of the service could create indicators of persistence, facilitating detection.

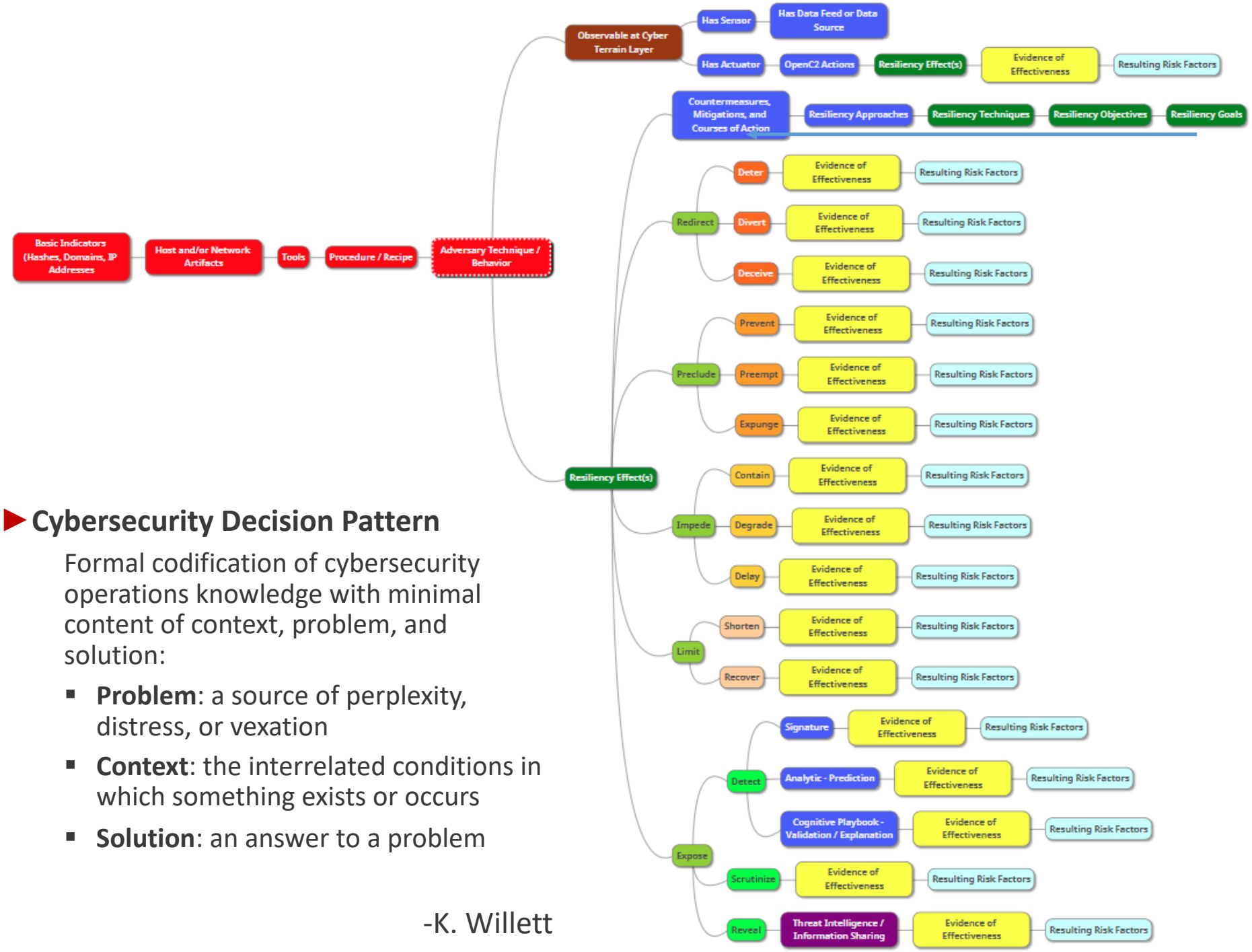
TABLE J-2: CYBER RESILIENCY TECHNIQUES AND APPROACHES FOR PRIVILEGE ESCALATION

PRIVILEGE ESCALATION	
Privilege Escalation refers to the methods that allow an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout a remote operation.	
TECHNIQUE: Analytic Monitoring	
APPROACH: Monitoring and Damage Assessment	A defender can increase probability of detection of an adversary through monitoring of privilege states, movement and integrity of access tokens, unusual privilege changes, or malfunction of privilege management actions, making the adversary's activities visible to defenders.
TECHNIQUE: Privilege Restriction	
APPROACH: Trust-Based Privilege Management	Strict management and diligence in monitoring of privileges is a fundamental method to delay, degrade, or curtail attacker-attempted privilege escalation (e.g., dividing privileges among more administrators, auditing any changes for consistency against entity roles).
APPROACH: Dynamic Privileges	This approach impedes, delays, or degrades adversary actions since the adversary must pass additional contextual tests, or take additional time to accomplish escalation given transient permissions, such as required to change configuration settings or installation of software.
TECHNIQUE: Substantiated Integrity	
APPROACH: Behavior Validation	Continuous validation of privilege change actions can lead to early detection of attacker compromises, such as noting unexpected software execution in a non-application context.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

DARK LIGHT™



Cybersecurity Decision Pattern

Formal codification of cybersecurity operations knowledge with minimal content of context, problem, and solution:

- **Problem**: a source of perplexity, distress, or vexation
- **Context**: the interrelated conditions in which something exists or occurs
- **Solution**: an answer to a problem

-K. Willett

DARK LIGHT™

Enable Filter Configure

Defender Resiliency Effects

April 2018 Update

Adversary Tactics & Techniques	Redirect			Prelude			Impede			Limit		Expose		
	Deter	Divert	Deceive	Expunge	Preempt	Prevent	Contain	Degrade	Delay	Shorten	Recover	Detect	Scrutinize	Reveal
Stage: Preparation														
Priority Definition Planning														
Priority Definition Direction														
Target Selection														
Technical Information Gathering														
People Information Gathering														
Organizational Information Gathering														
Technical Weakness Identification														
People Weakness Identification														
Organizational Weakness Identification														
Stage: Engagement														
Adversary Opsec														
Establish & Maintain Infrastructure														
Persona Development														
Build Capabilities														
Test Capabilities														
Stage Capabilities														
Stage: Presence														
Initial Access														
Execution												11		
Persistence												20		
Privilege Escalation												10		
Defense Evasion												16		
Command And Control														
Stage: Effect Consequence														
Credential Access												5		
Discovery												16		
Lateral Movement												5		
Collection												2		
Exfiltration												1		

Adversary Tactic | Mitigation | Groups | Software

Resiliency Technique: Analytic Monitoring

(Detect, Scrutinize)

Approach: Monitoring and Damage Assessment (Detect, Scrutinize)

A defender can increase probability of detection of an adversary through monitoring of privilege states, movement and integrity of access tokens, unusual privilege changes, or malfunction of privilege management actions, making the adversary's activities visible to defenders.

Example: Employ Continuous Diagnostics and Mitigation (CDM) or other vulnerability scanning tools; Deploy Intrusion Detection Systems (IDSs) and other monitoring tools; Use Insider Threat monitoring tools; Perform telemetry analysis; Detect malware beaconing; Monitor open source information for indicators of disclosure or compromise.

Resiliency Technique: Privilege Restriction

(Contain, Degrade, Delay, Prevent)

Approach: Trust-Based Privilege Management (Contain, Degrade, Delay, Prevent)

Strict management and diligence in monitoring of privileges is a fundamental method to delay, degrade, or curtail attacker-attempted privilege escalation (e.g., dividing privileges among more administrators, auditing any changes for consistency against entity roles).

Example: Implement least privilege; Employ time-based account restrictions.

Approach: Dynamic Privileges (Contain, Degrade, Delay, Prevent)

Defender Technique | Definition

Defender Tactic: Technique

Mitigation Effectiveness: None

Expose: Detect

PRO Playbooks

Add/Remove Playbooks

Windows | T1013 - Port Monitors

"Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM."
More documentation can be found here: "https://attack.mitre.org/wiki/Technique/T1013"

Windows | T1015 - Accessibility Features

"Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system."
More documentation can be found here: "https://attack.mitre.org/wiki/Technique/T1015"

Windows | T1134 - Access Token Manipulation

Windows | T1050 - Service Installation

When operating systems boot up, they can start programs or applications called services that perform background system functions. A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry.
Author: Darklight

Questions?

Thank You!

www.DarkLight.ai

DARK LIGHT™

About DarkLight

DarkLight Cyber is an Artificial Intelligence software utilizing an Expert System with contextual reasoning capabilities. The Expert System approach solves many of the challenges not addressed by the majority of current cyber AI utilizing algorithm-based solutions. Specifically, too many false positive alerts and an inability to explain why an alert occurred in the first place. These limitations reduce productivity and increase risk. DarkLight Cyber's Active Defense Expert System integrates threat, and risk information from current tools with critical contextual information, automates detection and investigation with shareable cognitive playbooks, validates the alerts, risks and predictions, and explains to the human analyst why DarkLight came to its conclusion in a transparent and understandable way. To learn more, please visit www.darklight.ai.

DARK LIGHT™