Effects on Adversary Activities:

How Cyber Resiliency Plays in the Cyber Attack Lifecycle

The BIG Idea

Because the various cyber resiliency techniques affect the cyber adversary's activities at different phases of the cyber attack lifecycle differently, a mix-and-match approach can improve resiliency.

Possible Effects

The figure illustrates effects that different cyber resiliency techniques could have on the cyber adversary throughout the cyber attack lifecycle. Each cyber resiliency technique can be applied at different architectural layers, using different approaches or providing different capabilities. Thus, a given application of a cyber resiliency technique can be expected to achieve some – but not necessarily all – of the possible effects on adversary activities identified below.

Cyber Resiliency Technique	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Adaptive Response	Contain Curtail		Curtail	Negate	Degrade Delay Contain Curtail	Negate Curtail Impede Recover	Degrade Delay Contain Curtail
Analytic Monitoring	Detect Analyze		Analyze	Analyze	Detect Analyze	Detect Analyze	Detect Analyze
Coordinated Defense		Delay		Degrade Delay	Detect Degrade Delay	Degrade Delay	Detect Degrade Delay
Deception	Degrade Delay Divert Deceive Detect Analyze	Deter Degrade Delay Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive Detect Analyze	Deter Divert Deceive Degrade Detect Analyze	Deter Deceive Detect Analyze
Diversity	Degrade, Delay	Impede	*Negate* Degrade Delay Contain *Detect*	Degrade Negate	Degrade Contain Recover	Degrade Recover	Degrade Contain Recover
Dynamic Positioning	Curtail		Negate Divert		Degrade Delay Curtail Expunge Recover	Degrade Delay Curtail Expunge Recover	Degrade Delay Curtail Expunge Recover
Dynamic Representation	Analyze				Detect Analyze	Detect *Recover*	Detect Analyze
Non-Persistence	Degrade Delay		Negate	Curtail Expunge	Curtail Expunge	Curtail	Curtail Expunge

Cyber Resiliency Technique	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Privilege Restriction	Degrade Delay			Negate Degrade Delay Contain	Negate Degrade Delay Contain	Negate Degrade Delay Contain	Negate Degrade Delay Contain
Realignment	Degrade Delay	Negate Degrade Delay	Degrade Delay	Negate Degrade Delay	Negate Degrade Delay	Negate Degrade Delay	Negate Degrade Delay
Redundancy						Degrade Curtail Recover	
Segmentation	Contain		Degrade Delay	Degrade Delay Contain	Degrade Delay Contain	Degrade Delay Contain Recover	Degrade Delay Contain
Substantiated Integrity			Negate Detect		Detect Curtail	Curtail Recover	Detect Curtail
Unpredictability	Delay	Delay	Detect	Delay Detect	Detect Delay	Delay Detect	Detect

Representative Examples

The following table provides some representative examples of how different approaches or capabilities could affect adversary activities.

Technique	Capability or Approach	Phase(s)	Effect(s)
Adaptive Response	Dynamic Reconfiguration: Make changes to an element or constituent system while it continues operating	Recon	Curtail: The adversary's knowledge of resources and configuration becomes outdated. Contain: The resources against which the adversary can conduct recon are restricted.
Analytic Monitoring	Damage Assessment: Analyze behavior, data, and system artifacts to determine the presence and extent of damage	Exploit, Execute	Detect: Damage assessment reveals the extent of the effects of adversary activities.
Coordinated Defense	Coordination and Consistency Analysis: Ensure that defenses are applied and cyber courses of action are defined and executed in a coordinated, consistent, and non-disruptive way	Control, Maintain	Detect: Inconsistencies (e.g., in configurations or in privilege assignments) provide indications of adversary activities.
Deception	Dissimulation / Disinformation: Create false target data (e.g., fabricating documents or data stores, creating false target data or simulating a non-existent application) or operational data, or provide deliberately confusing responses to adversary requests	Recon, Control, Execute, Maintain	Detect: The adversary's use of fabricated control data (e.g., configuration, network topology, or asset inventory data) serves as an indicator of adversary activity. Deceive: The adversary's knowledge about mission or defender activities is incomplete or false.
Diversity	Path Diversity: Provide multiple paths, with demonstrable degrees of independence, for information to flow between elements	Control, Execute, Maintain	Recover: Recovery from the mission effects of adversary activities is facilitated by the use of C3 paths to which the adversary lacks access (e.g., out-of-band communications among defenders).
Dynamic Positioning	Functional Relocation of Cyber Assets: Change the location of assets that provide functionality (e.g., services, applications) or information (e.g., data stores), either by moving the assets or by transferring functional responsibility	Recon, Control, Execute, Maintain	Divert: The adversary focuses activities on defender-chosen resources. Curtail: The period in which adversary activities are effective against a given location or instance of an asset is limited.

Dynamic Representation	Dynamic Mapping and Profiling: Maintain current information about resources, their status, and their connectivity	Control, Maintain	Expunge: Discovered software or components that do not fit asset policy requirements can be removed.
Non-Persistence	Non-Persistent Services: Services are refreshed periodically and/or terminated after completion of a request	Exploit, Control, Maintain	Expunge: Compromised services are terminated when no longer needed; if re-instantiated from a clean version, new instances will not be compromised.
Privilege Restriction	Privilege-Based Usage Restrictions: Define, assign, maintain, and apply usage restrictions on cyber resources based on mission criticality and other attributes (e.g., data sensitivity)	Exploit, Control, Execute, Maintain	Prevent: Privilege-based usage restrictions prevent the adversary from accessing critical or sensitive resources. Contain: Privilege-based usage restrictions limit the adversary's activities to non-critical resources, or to resources for which the false credentials the adversary has obtained allow use.
Realignment	Purposing: The mission purposes of functions, services, information, and systems are identified, to prevent uses that increase risk without any corresponding mission benefit	Deliver, Exploit	Impede: The adversary cannot take advantage of unnecessarily risky uses of resources (e.g., exposure of services to the Internet without offsetting mission benefits).
Redundancy	Replication: Information and/or functionality is replicated (reproduced exactly) in multiple locations	Execute	Degrade: The extent to which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. Recover: Recovery from the effects of adversary activities is facilitated.
Segmentation	Predefined Segmentation: Define enclaves, segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated	Control, Execute, Maintain	Delay: The adversary's ability to perform command and control is delayed, as the adversary must find ways to overcome barriers between network segments.
Substantiated Integrity	Behavior Validation: Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage)	Control, Execute, Maintain	Detect: The presence of adversary-controlled processes is detected by peer cooperating processes. Curtail: Adversary-controlled processes are isolated or terminated by peer cooperating processes.