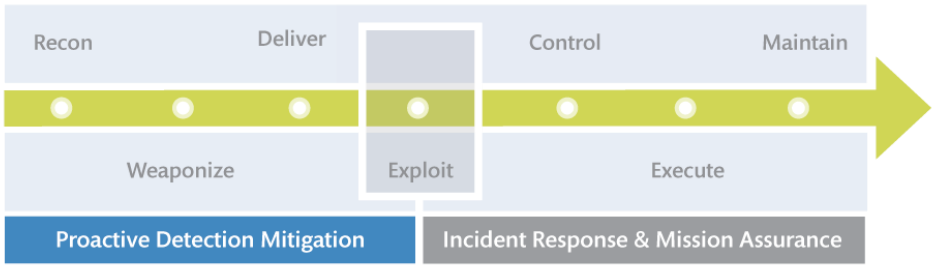
Overview of How Cyber Resiliency Affects the Cyber Attack Lifecycle

The Big Idea

By using the cyber attack lifecycle as a framework for employing cyber resiliency techniques (summarized in Cyber Resiliency: Key Concepts & Terms), organizations can more optimally make and balance investment decisions to prepare and plan for an attack and recover and reconstitute their assets in the aftermath.

Cyber Attack Lifecycle



The cyber attack lifecycle, first articulated by Lockheed Martin as the "kill chain," depicts the phases of a cyber attack: **Recon**—the adversary develops a target; **Weaponize**—the attack is put in a form to be executed on the victim's computer/network; **Deliver**—the means by which the vulnerability is weaponized; **Exploit**—the initial attack on target is executed; **Control**—mechanisms are employed to manage the initial victims; **Execute**—leveraging numerous techniques, the adversary executes the plan; and **Maintain**—long-term access is achieved.

A threat-based defense leverages the cyber attack lifecycle to provide defenders more opportunity to discover and respond to an attack. By mapping an organization's defensive tools and capabilities across the cyber attack lifecycle, opportunity gaps are revealed as investment needs.

Defender Actions & Effects on Adversaries

The table below provides an overview of how defender actions can affect a cyber adversary across the cyber attack lifecycle.

Defender Actions	Effect on Adversary
Divert the adversary's efforts	
Deter	The adversary ceases or suspends activities, or redirects activities toward different targets.
Misdirect	The adversary reveals capabilities, intent, targeting, TTPs, or strategy, w/o achieving intended effects.
Preclude the adversary's specific efforts from having an effect	
Negate	The adversary's efforts or resources cannot be applied or are wasted.

Preempt	The adversary's resources cannot be applied and/or the adversary cannot perform activities.
Impede the adversary so that only by investing more resources or taking additional actions can they achieve their goals	
Degrade	The adversary achieves some but not all of the intended effects, or achieves all intended effects but only after taking additional actions.
Delay	The adversary achieves the intended effects, but may not achieve them within the intended time period.
Detect the adversary's activities so that the adversary's ability to act stealthily is removed	
Limit the adversary's effectiveness	
Contain	The value of the activity to the adversary, in terms of achieving the adversary's goals, is reduced.
Curtail	The time period during which the adversary's activities have their intended effects is limited.
Recover	The adversary fails to retain mission impairment due to recovery of the capability to perform key mission operations.
Expunge	The adversary loses a capability for some period of time.
Expose the adversary so that they lose the advantage, as defenders are better prepared	
Analyze	The adversary loses the advantages of uncertainty, confusion, and doubt; the defender can recognize adversary tactics, techniques, and procedures (TTPs).
Publicize	The adversary loses the advantage of surprise; the adversary's ability to compromise one organization's systems to attack another organization is impeded.

Defender Actions across the Cyber Attack Lifecycle Enabled by Resiliency

The figure below illustrates a mapping of defender actions (taken from the table above) across the cyber attack lifecycle that are enabled by the cyber resiliency technique of Diversity. If an organization extended this mapping to include all their resiliency techniques, gaps in their opportunities to better defend and recover from a cyber attack would be revealed. Those gaps would represent resiliency investment needs. Further extending this mapping to include all the tools and capabilities in their cyber defense suite (including subject matter expertise) would provide the basis for an investment roadmap for the organization.