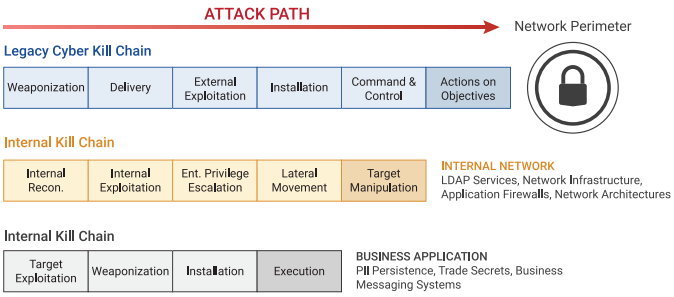
FRACTAL INDUSTRIES

Advanced Cyber Decision Platform™ (ACDP)

Use Case: Dynamic Asset Discovery

As any CISO will agree, you cannot secure what you don't know you have. Despite advancements in network discovery tools and asset management software, no enterprise can claim with certainty to know all it should know about its network infrastructure. This problem is amplified by the increasing reliance on wireless networks and mobile connectivity.



The path an attacker takes to penetrate networks is complex and spans multiple iterative phases. The attacker must penetrate your network perimeter, identify their target, and execute an exploit to steal the data. Key to this process is a quiet method of escalating privileges to acquire access to the target.

One of the more common and particularly dangerous threats that results from this lack of awareness is the presence of rogue devices on the network. Common examples of rogue devices are wireless credit card skimmers or wireless keyloggers that capture keystrokes from a compromised machine. Other examples are rogue (or, "evil") access points such as mis- or un-configured wireless printers, non-malicious employees enabling their own "hot-spots" for convenience, or a simple Wi-Fi USB card used by attackers to lure unsuspecting users to log onto a fake wireless network. These attackers typically stay connected to the network for brief periods of time and move around often, which makes them particularly difficult to detect and mitigate. More often than not, network administrators become aware of them only after it's too late.

ACDP™ provides an alternative. We deploy purpose-built machine learning algorithms to provide context to all telemetry data, including real-time analysis of user and network activity, server logs, remote queries, etc. Information about people, places, devices, services—and the dynamic relationships between them over time—are all stored in a highly intuitive and interactive map called the Cyber-Physical Graph (CPG). This dynamic enrichment allows CPG to scale to your entire infrastructure, across all domains.

Continuous monitoring of the entire network detects any changes and updates the CPG in real-time, with immediate assessments of possible vulnerabilities and their potential impact (or, Blast Radius™) represented in a single metric called the Network Resiliency score. For example, a new connection to a fileserver with sensitive data is more critical than a new connection to a web server—context matters. Rather than overwhelming operators with noisy alarms, ACDP correlates and presents event information with concise details about issues with the network (including bugs and misconfigurations as well as malicious activity), along with contextually-based, tactical recommendations for optimal response based on potential impact.

ACDP is the first application that uses a data science approach to detecting rogue devices—by customizing AI-driven analytics to the behavior of your network, with rich context in real-time.

Detecting rogue devices in real-time breaks the kill chain very early. We prevent the attacker from breaching the perimeter and thus collecting data on the internal network and target.