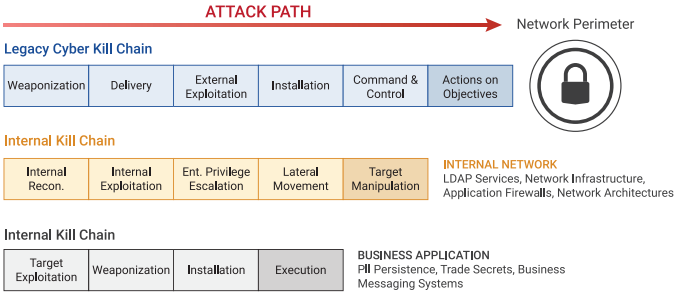
FRACTAL INDUSTRIES

Advanced Cyber Decision Platform™ (ACDP)

Use Case: Anomalous Behavior Analytics

A fully informed understanding of your network infrastructure is a fundamental requisite in modern network security. To most organizations, that means asset and inventory management, configuration management, and enumeration of controls. To declare victory there, however, is to leave a pivotal gap in your awareness of your network. Understanding people, the services they consume, and their logical and physical connectedness to the network is key to a truly comprehensive understanding of your entire security posture.



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 manner of escalating privileges to acquire access to the target.

People are simultaneously an enterprise's greatest strength and its biggest vulnerability. That vulnerability spans a spectrum of intent, from well-meaning human error, to careless or negligent activity, to a sophisticated bad actor intent on doing crippling damage to the business. The variety of risks exposed by human behavior makes these vulnerabilities exceedingly difficult to identify, isolate, and mitigate. Understanding the discrete patterns that users display is critical to reliably detecting behavioral anomalies that could pose a serious threat to the enterprise.

A user's day-to-day activities should provide all the necessary ingredients to establish a benchmark of what constitutes "normal" behavior. Over time, these activities will fall into identifiable patterns that provide a deeper understanding of the potential impact a user can have on network health. However, "point" solutions that only capture a singular dimension of user activity cannot provide a contextualized outlook of how that behavior might compromise network resilience.

ACDP™ provides a better alternative. We deploy purpose-built machine learning algorithms to leverage open, unstructured data extracted from both internal and external sources to provide context to all telemetry data collected from your network. In other words, constantly updated

Internal Kill Chain

Internal Recon.	Internal Exploitation	Ent. Privilege Escalation	Lateral Movement	Target Manipulation

Utilizing ACDPs Anomalous User detection capability, we catch internal exploitation of user accounts, thwarting escalation of privileges, catching misconfigurations, and identifying potential threats before exploits are realized.

vulnerability data from external sources is correlated with real-time analysis of internal data such as user and network activity, server logs, HR data, deployment documentation, etc. This provides a dynamic and comprehensive understanding of the full impact (or, Blast Radius™) associated with any given user's behavior, as it's taking place. Information about people, places, devices, and services—including the ever-changing relationships between them over time—is aggregated and rendered in a highly intuitive and interactive map called the Cyber-Physical Graph (CPG). Its dynamic enrichment allows CPG to scale actively to your entire infrastructure, across all domains and deployment vectors.

As more explicit data is collected over time, additional machine learning algorithms perform pattern matching and trend analysis to establish relevant and precise benchmarks for every user's normal behavior. These benchmarks are refined through advanced simulation models that utilize self-improving machine learning techniques to recognize and correct for model bias—continually maximizing the accuracy and effectiveness of those models over time. The result is a contextualized understanding of user behavior that immediately detects abnormalities such as:

- Anomalous Login Times
- Anomalous Web Browsing
- Anomalous Data Exfiltration
- Unlikely Login Locations
- Unusual Domain Requests
- New Endpoint Hashes
- New Machine Access Attempts

ACDP is the first application that uses a data science approach to detecting these vulnerabilities—not by simply alerting when a baseline is breached, but by delivering the context of the behavior in consideration of activity across the rest of the system. As the nucleus of your cybersecurity framework, ACDP enables fully informed decision-making in response to the unpredictability of human behavior.