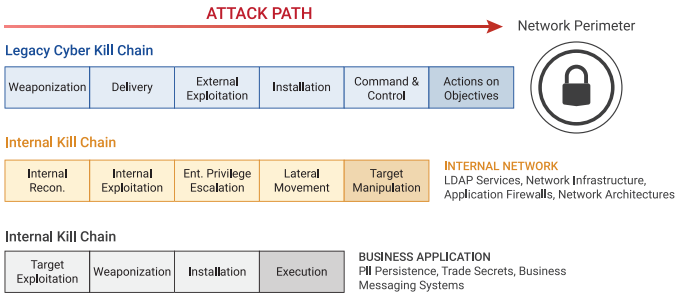
FRACTAL INDUSTRIES

Advanced Cyber Decision Platform™ (ACDP)

Use Case: Privilege Oversight

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 through their access privileges 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 go 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.

Network credentials are typically defined as either user accounts with individual permissions, or service accounts used by applications or services to log on to a device to make changes to its configuration or the operating system. Effective and secure systems administration emphasizes the need to restrict user and service account permissions so that these accounts can access only those services or devices which support a legitimate business requirement.

However, in modern and complex environments, permissions for user and service accounts are often over- or mis-allocated and rarely audited to identify improper or out-dated access.

Because of the variety of access levels that exist on the typical network, the risks exposed by these vulnerabilities can reach every segment of your infrastructure. Unnecessary access that is tied to a role that has changed or to a one-time need that has expired, for example, opens the door to potential exploits that can be exceedingly difficult to detect and mitigate because attacker activity often appears to be legitimate traffic. As the number of overall users grows, the risk exposure is exacerbated.

ACDP™ provides an 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 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. Contextualized 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.

Internal Kill Chain

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

Utilizing ACDPs Anomalous User detection capability, we catch over-allocation of access and close the gaps before attackers discover and exploit them.

The CPG provides a dynamic and comprehensive understanding of the full impact (or, Blast Radius™) associated with any given user or service account's behavior, as it's taking place.

Coupled with the behavior analytics and simulation modeling capabilities of Fractal | OS™, ACDP administrators can automate reports that routinely assess the proper allocation of permissions based on metrics such as frequency-of-use benchmarks and the sensitivity of accessible data.

For example, ACDP can provide a list of account-related events daily, which includes a review of the previous 30 days' updates. This report will be prioritized by impact and will deliver the name of the user, account permissions, systems they have accessed, systems they can but have not accessed, and a recommendation for optimal user account privilege allocation according a workflow such as the following:

1. Each privileged user is scored based on type(s) of privileges they have, number of systems they touch, and the business requirements of their operational role
2. The more "connected" the user and/or the more permissions allocated, the higher their "ranking," or risk score
3. When a user has not authenticated using admin or higher permissions in the previous 30 days, an event is generated for review
4. Based on the risk score of the user, an appropriate weight is applied to the 30-day group for event prioritization
5. ACDP provides an over-allocation report daily

This type of workflow enables the speedy auditing and revocation of privileges when necessary, based on actual risk and use. With its end-to-end data management and simulation modeling capabilities, ACDP legitimately recognizes improper or inefficient user and server account access from a truly holistic view. The result is unmatched visibility into the genuine vulnerability of your network, and the ability to make fully informed decisions about the allocation of permissions across your entire infrastructure.