In-Depth Value Assessment

ACTIVECYBER | Strategy₿

info@activecyber.com | activecyber.com

ACTIVECYBER | Strategy

In-Depth Value Assessment

Value Assessment Brochure

THE OVERVIEW

Is your business getting the most value from your analytics stack? Some companies purchase third-party software and develop complex and integrated solutions, then leave them for years to become stale and under-utilized.

Others develop solutions that utilize only a fraction of the full capabilities of the product, leaving opportunity on the table. To make sure you get the best value for your investment, this assessment analyzes your implementation end-to-end to ensure your company is getting the full value of the product.

THE BREAKDOWN

This is a follow-up to Active Cyber's "Doctor Assessment" offerings, which are a high-level look into the health of a current software implementation. This assessment goes deeper, analyzing not only your implementation, but all surrounding mechanisms and use cases to produce short, medium, and long-term plans to uplift and expand your current capabilities.

THE PHASES

1

Discovery

Understand current capabilities and desired future state from key personnel.
Critical focus areas: People, Process, Technology, and Data.

2

Analysis

Create tailored analysis on technology enhancements, training needs, and strategic initiatives.

3

Readout

Ensure successful adoption and scalability by highlighting critical focus areas, current and future state vision, and a phased transition project plan.

THE SUBJECT AREAS

1

Software Capabilities

Observing current use cases and implementations while evaluating potential expansion and modernization opportunities specifically catered to your use cases.

2

Data Structure and Performance

Evaluating current data structure for areas of improvement and suggesting newer modern methods for better performance, maintainability and flexibility/extensibility.

3

Custom Integrations

Finding modernization opportunities of any customized processes or legacy code while analyzing potential mechanisms to benefit the current implementation.

4

Security

Analyzing current security for potential new attack vectors and overall improvements for better maintenance and scalability.