AXE55 Technologies

The Assured Discovery and Intelligence Ontology

Executives today aren't just defending networks, they are defending ownership structures, insider exposure, and hidden code dependencies that traditional audits never reveal. Assured Discovery and Intelligence (ADI) is an intelligence-grade assessment framework that exposes blind spots before they explode into liability, brand damage, or shareholder fallout. We map who really controls your suppliers, which insiders could be leveraged, and what exploitable code exists in your environment—delivering a risk map you can act on immediately. The choice is simple: wait until a regulator, journalist, or adversary finds it first, or uncover it now—on your terms.

In today's environment, waiting to act means handing your adversaries the first move. The ADI process transforms hidden exposures into decisive intelligence, turning uncertainty into action, and risk into opportunity.

Resilience is built through action not reaction

Contact us for pricing, a demonstration, or contract details.

Warren Holston, Founder
wholston@axe55tech.com
813-375-2166
AXE55TECH.com

The process of moving from a company or client profile to a comprehensive assessment package is achieved through a structured, intelligence-driven methodology designed to uncover vulnerabilities across every layer of an organization. It begins with defining the entity—mapping its digital infrastructure, ownership, people, and logistics—and then systematically identifying weaknesses within each domain. The result is a complete assessment that not only identifies vulnerabilities but contextualizes them within business, mission, and strategic consequences.

The Ontology

Entity Map – Who Really Controls Your Ecosystem

The Entity Map uncovers the true ownership, equity chains, and operational control behind critical infrastructure. By mapping beneficial owners, shell structures, and upstream/downstream affiliates, the Entity Map eliminates uncertainty about who exerts influence.

Risk Profile – Exposure Rating Across All Domains

The Risk Profile aggregates vulnerabilities from digital systems, equity chains, human insiders, and code dependencies into a single, weighted exposure rating. Each risk is measured by likelihood, severity, and potential impact on operations, enabling organizations to prioritize with precision.

Exploit Paths – Adversary Playbook Before It Runs

The Exploit Paths output reconstructs the methods adversaries would use to penetrate the ecosystem. By analyzing open-source code contributions, patch delays, insider vulnerabilities, and vendor weaknesses, ADI anticipates the precise pivot points attackers will exploit. This adversary simulation reveals leverage that most monitoring tools miss: abandoned domains, reused credentials, foreign-authored code commits, and unpatched third- or fourth-tier dependencies.

Recommended Actions – Mitigation and Offensive Options

The final stage delivers Recommended Actions that range from defensive remediation to offensive countermeasures.

- Mitigation options: patching code dependencies, segmenting networks, resetting compromised credentials, or offboarding high-risk vendors.
- Offensive options: exploit prioritization, infiltration sequencing, or maintaining persistence against adversary-aligned assets.