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.

ADI Targeting Matrix Example

Most risk analysis stop at surface-level signals. ADI is designed to reconstruct the picture from independent evidence, prioritize what matters, and identify what still needs to be collected before leaders make a decision. The Targeting and Collection Matrix is a focused distillation of prioritized risk areas identified in the ADI Comprehensive Intelligence Report, linking each attack surface to its operational impact and the specific intelligence required to validate, exploit, or mitigate exposure. All information is sourced to ensure provenance and verifiability.

Targeting and Collection Matrix

Priority	Target	Category / Attack Surface	Risk Identified	Why It Matters (Operational Impact)	Next Collection Requirements	Source
1	js.zohocdn.com css.zohocdn.com static.zohocdn.com	CDN / Infrastructure	Unknown provider identity; no certifications; foreign infrastructure	Unattributed data path; potential for **content manipulation, script**	Identify ownership, jurisdiction, certifications, data flow	§6.0, §17.0
2	Huawei Relationship	Supply Chain	Verified partnership claim with regulatory sensitivity	Potential **hardware manipulation prior to delivery**; compliance and procurement disqualification risk	Validate partner status, sourcing chain, distribution routes, target markets	§7.0, §1.1
3	Beneficial Ownership (UBOs)	Governance / Control	No ownership or control disclosures	Unknown entity control → **insider threat, foreign influence, non-attributable decision-making**	Obtain corporate filings, operating agreement, ownership %, control rights	§4.0, §3.0
4	Sandeep Kumar (CEO)	Leadership / Insider Risk	Insufficient verification of leadership role	Unclear authority over **systems, vendors, and financial decisions**; potential proxy leadership risk	Validate identity, role, authority, prior affiliations, control over accounts	§16.0, §1.1
5	Cisco Relationship	Supply Chain / Governance	Conflicting affiliation claims	**Misrepresentation risk**; unclear support, warranty, and authorized sourcing channels	Validate Cisco partner status, authorization level, sourcing pathways	§4.0, §7.0
6	Google Tag Manager (and tag containers)	Runtime / Application Layer	Dynamic script injection capability	Centralized **on-glass attack vector**; enables persistent script injection without code changes	Identify admins, enforce MFA, review audit logs, inventory loaded scripts	§5.0, §7.0
7	India (Noida) & UAE (Dubai) Personnel	Operational / Insider Threat	Offshore development and logistics footprint	Cross-border access → **data exposure, insider threat, jurisdictional risk**	Map system access, privileges, vendor dependencies, data access levels	§16.0, §1.0
8	campaign.netmatriks.com	Network / Subdomain	Separate campaign/marketing surface	Potential **shadow environment** with weaker controls and third-party integrations	Identify hosting, security headers, scripts, external connections	§7.0
9	Cloudflare / Azure CDN (scripts.clarity.ms)	Infrastructure / Control Plane	Critical delivery and edge control points	Misconfig = **traffic manipulation, logging exposure, or availability disruption**	Validate services used (WAF/CDN/DNS), access control, logging, IR procedures	§6.0, §17.0

AXE55 Technologies ADI Operational Use Cases

Defensive/Blue Team

Supply Chain Exposure Response (Commercial)

A Fortune 1000 company identifies potential compromise in a third-party SaaS provider and uses ADI to map enterprise-wide exposure, while APL rapidly sources and deploys a trusted alternative without operational disruption.

Critical Infrastructure Defense (Government)

A critical infrastructure operator uses ADI to identify foreign-owned dependencies and runtime vulnerabilities across its network, while APL enables secure replacement and procurement of compliant technologies.

Due Diligence

Acquisition Risk (Defense Contractor)

A defense contractor pursuing an acquisition uses ADI to uncover hidden ownership, contract exposure, and supply chain risk, while APL enables discreet validation and secure engagement without signaling intent.

Vendor Vetting (Commercial / PE / VC)

A private equity firm evaluates a target using ADI to expose leadership ties, digital dependencies, and latent risk, while APL supports secure onboarding and controlled vendor engagement.

Offensive/Red Team

Adversary Pathway Emulation (Enterprise / Defense)

A red team uses ADI to identify real-world infiltration paths through third-party services and exposed infrastructure, while APL enables acquisition of mission-required access and tooling without attribution.

Operational Preparation of the Environment

A USG element uses ADI to map target networks, digital supply chains, and key personas, while APL enables procurement of infrastructure, devices, and access required to operate with cover and persistence.