EXECUTIVE ADVISORY

Defense Assessments

Understand What Matters Most Before Deciding What to Fix First

Organizations do not need another assessment that produces a longer list of findings. They need to understand where they are exposed, what matters most to the business, and what to do first.

01 — THE CHALLENGE

Security leaders are presented with maturity assessments, posture assessments, operational readiness reviews, crown-jewel exercises, and dozens of variations. Most answer only part of the question.

Traditional assessments often evaluate controls without fully understanding business consequence. The result is a prioritized list based on technical severity rather than a clear view of what hurts if a system goes down, what happens if data is stolen, and where hidden dependencies concentrate risk.

02 — WHY ARCTIQ

Defense Assessments consolidate security assessment into a single, scalable engagement that adjusts to the client's environment and maturity. The engagement can range from a focused crown-jewel and business-impact exercise to a full enterprise security posture assessment.

Arctiq works directly with executive stakeholders and process owners to identify what matters to the business, then maps those priorities to technology, identity, data, and infrastructure dependencies.

> Graph-based dependency analysis helps surface relationships that are difficult to identify manually, including privileged legacy accounts, undocumented SaaS integrations, concentrated blast radius, and hidden dependencies across hybrid environments.

03 — ADVISORY CAPABILITIES

- Enterprise security posture assessment
- Crown-jewel identification and prioritization
- Business-impact analysis
- Workshop-driven data classification
- NIST CSF 2.0 and CIS Controls v8 maturity analysis
- Identity dependency mapping across Entra ID, Okta, and Active Directory
- Infrastructure analysis across AWS, Azure, GCP, and on-premises environments
- Data dependency analysis across Snowflake, Databricks, M365, and Google Workspace
- Attack path, lateral movement, and blast-radius analysis
- Sequenced security improvement planning

ENVIRONMENTS ANALYZED

NIST CSF 2.0 | CIS Controls v8 | Entra ID | Okta | AWS | Azure | GCP | M365

04 — BUSINESS OUTCOMES

Organizations gain:

- ✓ A business-prioritized view of cyber risk
- ✓ Clear identification of critical systems and data
- ✓ Greater visibility into hidden technology and identity dependencies
- ✓ A defensible, sequenced action plan
- ✓ Better prioritization of security investment
- ✓ A foundation for CTEM, segmentation, DLP, zero trust, and resilience initiatives

05 — WHY IT MATTERS

Security investments are most effective when they protect what matters most. Arctiq helps organizations connect business consequence to technical risk and build a practical action plan based on real priorities.

Book a Defense Assessment →

www.arctiq.com