EXECUTIVE ADVISORY

CTEM-Aligned Exposure & Resilience Advisory

Move Beyond CVSS and Prioritize the Exposures That Threaten the Business

Continuous Threat Exposure Management was never intended to be vulnerability management with a new name. Effective exposure management connects attack paths, business consequence, and remediation.

01 — THE CHALLENGE

Many organizations have extensive vulnerability data, scan reports, and remediation backlogs that grow faster than teams can address them. What they often lack is a continuous, business-prioritized view of which exposures create real paths to critical systems and data.

CVSS scores alone cannot answer which exposures matter most to the business.

02 — WHY ARCTIQ

Arctiq anchors exposure prioritization to crown jewels, business consequence, and validated attack paths. Rather than producing another vulnerability spreadsheet, we help clients build a ranked exposure landscape that reflects how an adversary could reach systems that matter.

We operationalize CTEM across scoping, discovery, prioritization, validation, and mobilization. The engagement includes the operating model, tooling strategy, cross-functional workflow, and governance cadence required to sustain the program.

> Our approach is tooling agnostic and works with the technologies clients already use.

03 — ADVISORY CAPABILITIES

- CTEM operating model design
- Crown-jewel and business-impact alignment
- Exposure discovery and prioritization
- Attack path analysis
- Identity attack path validation
- Cloud and network reachability analysis
- Exploitability and exposure validation
- Tenable, Qualys, Wiz, Rapid7, and Microsoft Defender for Cloud alignment
- BAS integration with platforms such as AttackIQ and SafeBreach
- Integration with vulnerability, change, and detection engineering workflows

TOOLING (AGNOSTIC) Tenable · Qualys · Wiz · Rapid7 · Defender for Cloud · AttackIQ · SafeBreach

04 — BUSINESS OUTCOMES

Organizations gain:

- ✓ Exposure prioritization based on business consequence
- ✓ Greater visibility into real attack paths
- ✓ Reduced reliance on CVSS scores in isolation
- ✓ A repeatable CTEM operating model
- ✓ Better alignment between security, infrastructure, and application teams
- ✓ A direct path from exposure discovery to remediation

05 — WHY IT MATTERS

Organizations cannot remediate every vulnerability at the same speed. Arctiq helps security teams focus resources on the exposures most likely to create meaningful business impact.

Book a CTEM consultation →

www.arctiq.com