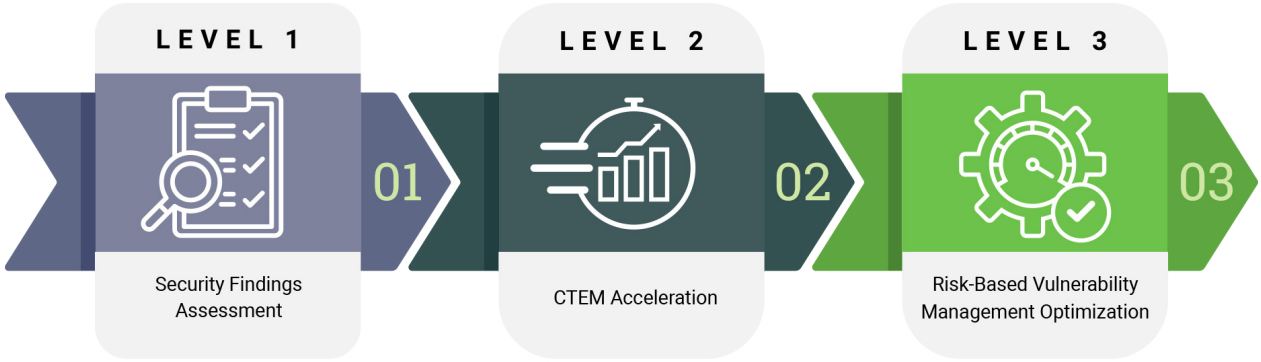
TEVORA™

Continuous Threat Exposure Management (CTEM) Services

As attack surfaces continue to expand across cloud environments, applications, identities, endpoints, and third-party technologies, many organizations are finding that traditional vulnerability management programs can no longer keep pace with modern threat exposure.

Our Continuous Threat Exposure Management (CTEM) offering helps organizations transition from a reactive, vulnerability-focused approach to a proactive, risk-based security strategy. The result is a more mature, integrated, and operationalized exposure management program that enables security teams to focus on reducing real risk.

Service Levels



Level 1: Security Findings Assessment
We assess your current security tooling and exposure data, identify key visibility and prioritization gaps, and consolidate findings into a structured, risk-based remediation backlog that enables clear, actionable prioritization of security efforts.

Level 2: CTEM Acceleration
Implementing risk-based prioritization and integrating workflows across security tools to ensure exposures are consistently evaluated, enriched with context, and seamlessly routed or automated remediation processes.

Level 3: Risk-Based Vulnerability Management Program Optimization
Ongoing quarterly optimization and acceleration of exposure management program, including continuous tracking of key metrics to measure improvement, validate prioritization effectiveness, and drive sustained reduction in security risk over time as new threats are discovered.

"Continuous Threat Exposure Management (CTEM) isn't just about discovering exposures. It's about applying expert insight to identify what matters most and continuously reduce real-world risk."

Mark Broghammer
VP, Security Architecture

Key Outcomes:

- Improved visibility across internal, external, cloud, and application attack surfaces
- Operationalizing and tuning of vulnerability-focused operations to risk-based exposure management
- Better utilization and optimization of existing security tooling investments
- Streamlined remediation workflows and operational efficiencies
- Improved integration and data sharing across security technologies
- Increased exposure management maturity and program scalability
- Greater alignment between security operations and business risk priorities
- Faster identification and reduction of critical exposures
- More actionable insights for security leadership and operational teams

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's organizations, people, and assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and—year after year—apply our cumulative learnings to continually strengthen the company's digital defenses.

ACHIEVED ACCREDITATIONS

ISO 27001 · ISO 27017 Certified · A2LA ACCREDITED CERT #5062.01 · CREST PEN TEST

ACHIEVED ASSESSOR

PCI Security Standards Council — PCI DSS QSA, PCI PA-DSS QSA, 3DS ASSESSOR · AICPA SOC · ISO Audit · HITRUST Authorized CSF Assessor · FedRAMP · TPN Trusted Partner Network · GovRAMP