nagomi

Operationalizing Continuous Threat Exposure Management

CTEM Implementation Roadmap

CTEM only works if you can execute. Most teams already have the tools, what's missing is a connected, accurate view of assets, exposures, and control coverage, along with a plan to close the right gaps in the right order. This roadmap turns CTEM from theory into action by using what you already have to deliver impact from day one.

PHASE 1: INTEGRATE

- Establish a single, connected view across systems
- Connect to core systems (EDR, IAM, cloud, SaaS, CMDB)
- Pull asset and control telemetry through APIs — no agents or scans
- Begin real-time assessment of control health and coverage

OUTCOME: Unified asset inventory, live control data, and the foundation for exposure tracking.

PHASE 2: BASELINE

- Define where you stand and where you fall short
- Identify orphaned assets, stale tooling, shadow IT, and toxic exposure chains
- Map compensating controls to top threats and critical assets
- Benchmark effectiveness across business units or subsidiaries

OUTCOME: Verified coverage baseline and exposure footprint, including pre/post M&A visibility.

PHASE 3: OPERATIONALIZE

- Shift from activity to action
- Correlate vulnerabilities, misconfigurations, and threat intel into prioritized breach paths
- Launch focused remediation campaigns tied to business risk
- Route ownership, track closure, and measure progress

OUTCOME: Clear prioritization, faster fixes, and exposure reduction that's visible across teams.

PHASE 4: EXPAND

- Scale across the business and bring stakeholders with you
- Align teams on a single data set, from SecOps to the board
- Track control improvements and exposure trends over time
- Report by business unit, geography, or framework (MITRE, NIST, CIS, ISO)

OUTCOME: Strategic visibility for executive reporting and program accountability.