equixly

Understanding COST and CTEM

A guide to Continuous Offensive Security Testing and its relationship with Continuous Threat Exposure Management.

COST: CONTINUOUS OFFENSIVE SECURITY TESTING

COST is an operating model in which offensive testing begins when something material changes in an environment, not when the calendar dictates. It uses predefined triggers to activate the right type of offensive testing at the right depth, at machine speed

CTEM: CONTINUOUS THREAT EXPOSURE MANAGEMENT

CTEM is a framework for proactively managing and mitigating threat exposure through an iterative approach that emphasizes building structured organizational processes in addition to leveraging security tools.

HOW COST WORKS

01 Target
What are we testing, and why is it worth testing right now?

02 Plan
Which method, which attacker objectives, and what depth?

03 Execute
Run the test with a mix of automation, AI, and human reasoning.

04 Report
Turn findings into actions that the right team can pick up immediately.

WHY CTEM NEEDS COST

CTEM runs continuously, while traditional penetration testing does not:

- Everything that changes between engagements - deployments, APIs, configurations - goes unvalidated.
- Each gap between tests is an unvalidated exposure window, where attackers operate.
- CVE scores and scanners cannot confirm whether an exposure is actually exploitable in your environment.

Only offensive testing can answer that question, but only if it runs at the pace environments change.

COST closes this gap, making validation as continuous as discovery and prioritization.

CTEM WITHOUT CONTINUOUS VALIDATION IS INCOMPLETE

It is simply traditional vulnerability management without continuous testing. The exposures are ranked and risk is identified, but without validation in real-time, nothing confirms whether those exposures can actually be exploited and nothing closes the window.

HOW EQUIXLY DELIVERS COST

Always On Discovery
Continuously maps the full API and application attack surface

Trigger-Driven Testing
Changes to your attack surface automatically activates testing

Agentic AI Methodology
Validates exploitability the way a real attacker would with complex testing

CTEM-Aligned Reporting
Exploit-validated findings feed into remediation workflows