HORIZON3

The CTEM Operating Loop Must Run Across Every Attack Surface

Identify what matters. Fix it. Prove it is fixed. *Repeat.*

Visibility alone does not reduce risk. Most CTEM programs discover more, prioritize differently, and report more frequently, but still struggle to answer: What can an attacker actually do? Which exposures create real business risk? Did remediation change anything meaningful?

Horizon3 CTEM Loop

DISCOVER EXPOSURE

Build complete visibility across vulnerabilities, misconfigurations, identity risks, & exposed assets.

VALIDATE WHAT IS EXPLOITABLE

Determine which weaknesses can be exploited, chained, and used to reach critical systems or data.

PRIORITIZE BASED ON IMPACT

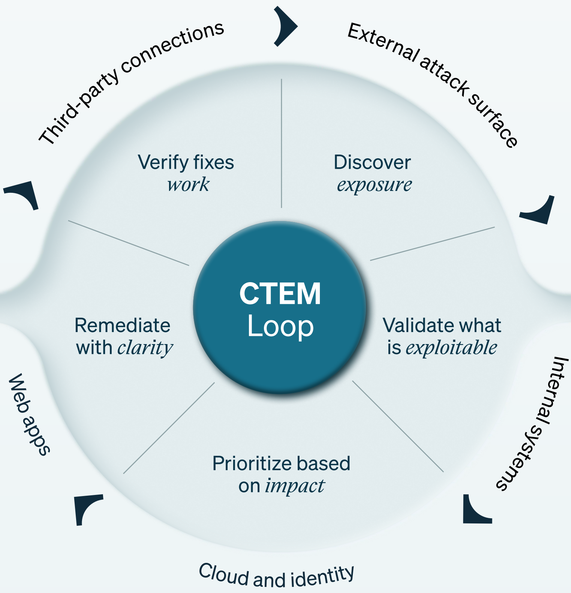
Focus remediation on proven attacker opportunity and potential business consequence

REMEDIATE WITH CLARITY

Give the right owners clear evidence of what must be fixed and why it matters.

VERIFY FIXES WORK

Retest to prove the exposure & associated attack path have been eliminated.



Without the CTEM Loop	*With* the CTEM Loop
More findings	Validated risk
More scores	Clear priorities
More reports	Verified remediation
More assumptions	Proven exposure reduction

Metrics that *matter*

- Reduction in exploitable attack paths
- Reduction in blast radius
- Decrease in high-impact exposures
- Percentage of remediated exposures verified
- Time required to validate and eliminate risk

CTEM is *not* another layer of insight.
It is a repeatable operating model for reducing attacker opportunity.

Operationalize CTEM ›