



Executive Framework: Identify and Reduce Your Exploitable Attack Surface

Why “Attack Surface” Is an Executive Concern



Every organization has an attack surface - but only part of it is exploitable.

As environments expand through cloud adoption, third party integrations, remote access, and ongoing configuration change, exposure grows in ways that are difficult to track through point in time assessments. While most organizations maintain foundational discovery through tools like vulnerability scanning, discovery alone does not explain which weaknesses an attacker can use to reach critical systems or data.

For executive leaders, the challenge is not visibility - it is prioritization.

Continuous Threat Exposure Management (CTEM) enables leadership teams to move beyond broad awareness and focus on exploitable attack paths that represent real business risk.

From Total Attack Surface to Exploitable Exposure

Traditional approaches treat all vulnerabilities as equal inputs. In reality, attackers do not exploit issues in isolation - they chain weaknesses together, bypass controls, and target assets that matter most to the business.

CTEM reframes the attack surface by answering three leadership level questions:

1. Which weaknesses are reachable?
2. How would an attacker move through the environment?
3. Which paths lead to critical assets?

By safely simulating real world attacker behavior, CTEM filters discovery data into **validated attack paths**, transforming raw findings into prioritized risk insight.

The CTEM Driven Model for Reducing Exploitable Exposure

This framework outlines how organizations use CTEM to continuously reduce their exploitable attack surface - without disrupting operations or replacing existing tools.

1. Establish Comprehensive Discovery (Input Layer)

Foundational services such as Vulnerability Scanning provide essential visibility across internal, external, cloud, and hybrid environments. This step ensures known weaknesses are identified and nothing is overlooked. However, discovery alone does not determine impact.

2. Validate Exploitability with CTEM (Differentiator)

CTEM uses autonomous penetration testing and attack surface analysis to determine:

- Whether vulnerabilities are reachable
- How they can be chained together
- Whether existing controls block or fail to stop an attacker

This validation shifts focus from severity scores to real world exploitability.



3. De Prioritize Noise, Elevate What Matters

CTEM actively reduces alert fatigue by:

- Lowering priority on issues blocked by compensating controls
- Highlighting paths that bypass defenses
- Focusing remediation on exposures tied to business critical assets

This enables teams to reduce actual risk - not just improve metrics.

4. Guide Remediation with Proof

For validated attack paths, CTEM delivers clear, step by step remediation guidance. Internal teams retain control of execution, while OXEN validates that fixes close exposure.

5. Retest and Measure Reduction Over Time

Exposure reduction is verified through retesting. Leadership can now track whether exploitable risk is decreasing quarter over quarter, rather than relying on static reports.

What This Delivers to Executive Leadership

- Clear distinction between total risk and exploitable risk
- Better alignment of remediation effort to business impact
- Reduced operational noise for IT and security teams
- Defensible, evidence based cyber risk decisions
- Measurable reduction of exploitable exposure over time

Identify and Reduce Your Exploitable Attack Surface

Use this framework to align leadership and IT teams around what truly matters - validated exposure, prioritized action, and measurable risk reduction.

Why OXEN Technology

OXEN Technology delivers CTEM as a fully managed service that integrates into existing environments without disruption. OXEN conducts attack simulations, validation, and prioritization while internal teams retain control of remediation execution. The result is a collaborative, scalable approach to continuous risk reduction.

OXEN is an established cybersecurity and IT managed service provider founded in 1985. Teams deliver full-service infrastructure management, compliance-minded cybersecurity, and 24x7 support.

OXEN serves clients in regulated industries like finance, healthcare, manufacturing, legal, and government. OXEN teams care deeply about client satisfaction and positive outcomes.

Contact OXEN Today

 888-296-3619  hello@OXEN.tech  OXEN.tech