CYBERLENCE

CYBERLENCE IN ACTION

From Cybersecurity Testing to Cyber Resilience Testing

AI is compressing the time attackers need to exploit a known vulnerability — Verizon's 2026 Data Breach Investigations Report describes the window shrinking "from months to hours." Security teams are still working on human time: the median finding takes 26 days to resolve, with roughly 84% unresolved at any given point, per Stingrai's 2026 State of Penetration Testing report.

CYBER RESILIENCE TESTING

Posture, Proven as You Execute — Not Just on a Baseline

Whether it's business as usual, a scheduled test, or a real attack, your resilience posture should answer one question: are you ready? CTEM, BAS and detection-as-code validate controls — but detection drift, alert floods, and the gap between a finding and its business impact mean a clean report doesn't guarantee readiness. Cyberlence validates posture continuously, so gaps surface the moment they appear — not after the exercise report lands.

CYBERLENCE SOLUTION

Red, Blue & Purple — Validated Live, Not Reported Later

Cyberlence treats red-team activity the same way it treats a real attacker: Detect maps every action to a live application picture, Analyze traces blast radius and business impact as the exercise unfolds, Recover routes verified findings to owners and confirms the fix, and Purple shares it all with your blue team while the exercise is still running.

CLOSE THE LOOP FASTER

Automatic retest evidence and application-aware routing mean confirmed findings get fixed and verified, not just logged and forgotten.

REPLACE MANUAL HANDOFFS

One shared, always-current picture of your resilience posture for red, blue and remediation teams — no more Slack messages, copy-pasted hashes, or emailed PDFs.

CUSTOMER BENEFIT

What Your Teams Get

Live Purple Teaming: Every red-team engagement becomes a real-time validation of blue-team detection and response.

Verified Remediation: Confirmed findings route to the right owner with full context, and retest evidence proves the fix.

Defensible Evidence: A timestamped record of red-team activity and blue-team response, ready for auditors and the board.

Security testing tells you where you're vulnerable. Cyberlence resilience testing tells you whether you're ready.

Sources: [1] Verizon, 2026 Data Breach Investigations Report. [2] Stingrai, State of Penetration Testing 2026.

© 2026 Cyberlence. All rights reserved.