REI by CyberZones
Risk & Exposure Intelligence Platform

REI — Risk & Exposure Intelligence

Converting Cybersecurity Risk Data Into Actionable Intelligence

A platform that discovers live hosts and exposed services on a network, then automatically assesses each one for risk — turning raw scan data into a prioritized, plain-language action list.

4-Tier	AI-Powered	MITRE ATT&CK	5
Risk Classification	Risk Narratives	Technique Mapping	SIEM Integrations

Network & Host Discovery

Automatically finds live hosts and open services across a network segment — no manual asset list required.

Exposure & Port Risk Scoring

Every exposed service is scored Low to Critical with a clear, business-readable risk narrative explaining why it matters and what to do about it.

Web & SSL/TLS Inspection

Detects expired or misconfigured certificates and weak TLS versions, and fingerprints the technology stack running on exposed web services.

Domain & Email Security Posture

Checks SPF, DKIM and DMARC so teams know whether their domain can be spoofed before attackers find out.

Brand Abuse & Look-Alike Domains

Scans for typosquatted and look-alike domains being registered against your brand — an early warning for phishing campaigns.

AI-Powered Risk Analysis

A built-in AI engine — cloud or fully offline — turns scan results into prioritized, plain-language findings and recommendations.

MITRE ATT&CK Mapping

Every finding is tied to recognised attack techniques and tactics, dropping straight into existing threat frameworks.

SIEM/SOC Integration & Reporting

One-click export to leading SIEM platforms, plus polished PDF reports with risk heatmaps for executives and auditors.

RISK CLASSIFICATION

LOW | MEDIUM | HIGH | CRITICAL

Built for SOC teams, exposure management analysts and MSSPs needing fast, prioritized attack-surface visibility.

CyberZones
Innovation & Research Division

info@cyber-zones.com