CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

CYBER ZONES
Innovation & Research Division

Continuously monitors an organisation's external digital footprint — domains, email infrastructure, leaked credentials and dark-web exposure — to reveal real-world risk before attackers find it first.

24	0-100	24/7	3
Intelligence Modules	Unified Risk Score	Continuous Monitoring	AI Deployment Modes

Full Attack Surface Discovery

Maps an organisation's domains, subdomains and DNS infrastructure, surfacing assets security teams didn't know existed.

Email Security & Phishing Exposure

Audits email authentication posture and flags harvestable employee and company details attackers use for phishing and BEC.

Breach & Credential Exposure

Checks corporate and employee credentials against known data breaches and infostealer malware logs.

Leaked Secrets & Dark-Web Monitoring

Scans paste sites, exposed databases and public code repositories for leaked API keys and confidential data.

Threat & Reputation Intelligence

Cross-references the organisation's IPs and domains against global threat-intel feeds for malicious activity and reputation risk.

Ransomware & Supply-Chain Watch

Detects look-alike phishing domains, ransomware-group disclosures naming the organisation, and third-party exposure.

Continuous Monitoring & Risk Scoring

Findings are deduplicated, correlated and weighted by asset criticality into one risk score, with scheduled rescans and alerts on risk increases.

Flexible, Privacy-First AI Engine

Choose fully offline on-device AI, a local server, or cloud AI — analysis adapts to the customer's data-control requirements.

RISK CLASSIFICATION LOW | MEDIUM | HIGH | CRITICAL

Built for CISOs, SOC/threat-intel teams and MSSPs needing continuous, attacker's-eye visibility across monitored brands.

info@cyber-zones.com