CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

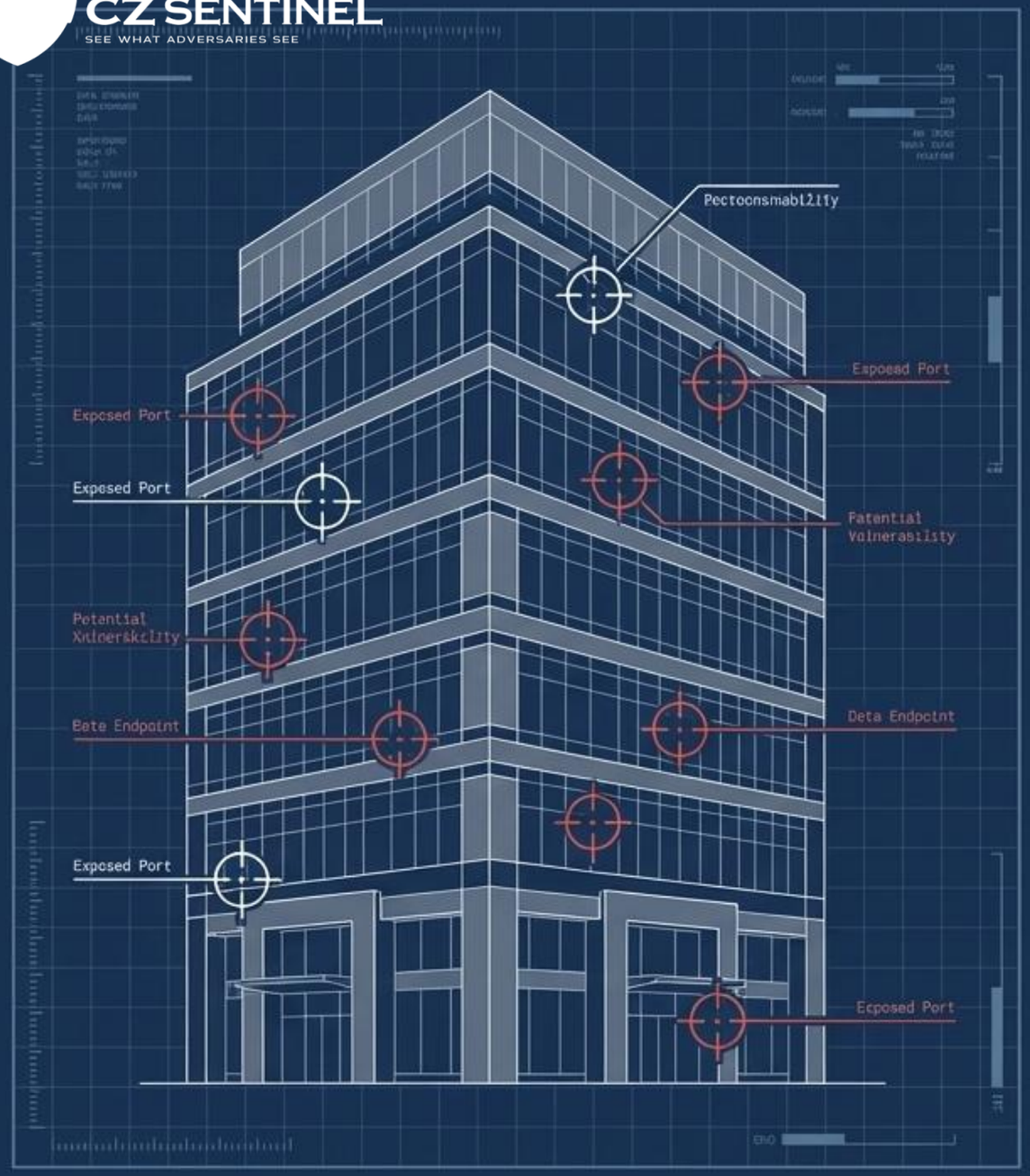
CZ SENTINEL

See What Adversaries See

Digital Exposure Intelligence and External Attack Surface Management Platform

CYBER ZONES
Innovation & Research Division

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE



Why Do Organizations Need Sentinel?

Most cyberattacks do not start with direct exploitation... they start with Reconnaissance.

- Unmanaged or forgotten assets.
- Exposed configurations made unintentionally.
- Publicly available information ripe for exploitation.
- Digital footprints inadvertently exposing the IT infrastructure.

The Problem: Organizations rarely realize the true scale of their public exposure until after an exploitation occurs.

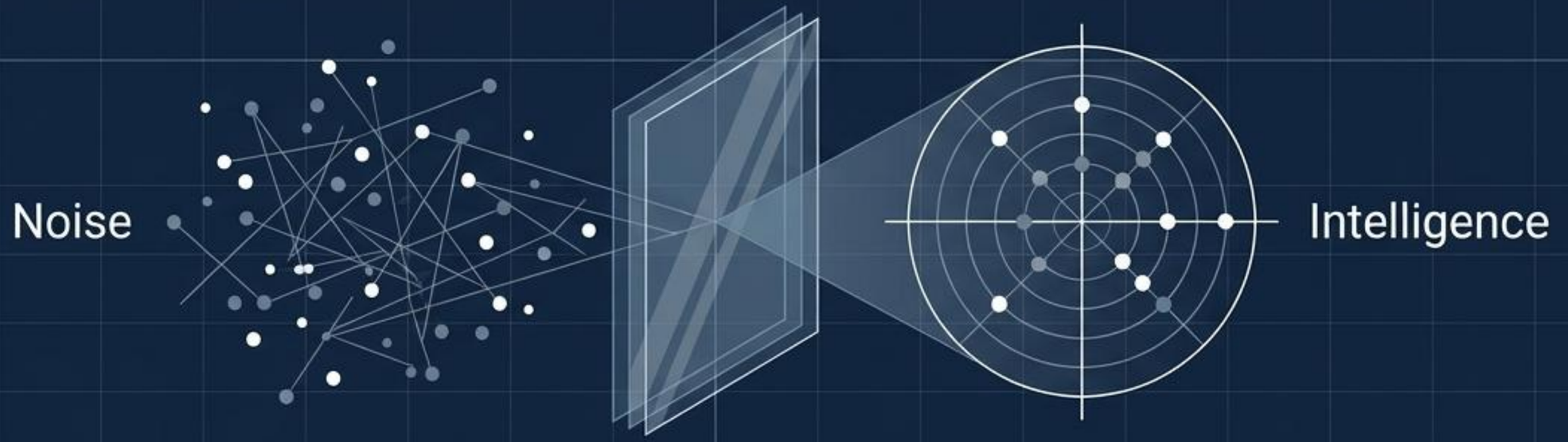
CYBER ZONES
Innovation & Research Division

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

What is Sentinel Exactly?

Sentinel is not a traditional penetration testing tool, and it is not an internal vulnerability scanner.

It is an Attack Surface Exposure Intelligence Platform that focuses on what is publicly visible, transforming raw data into manageable risk visibility.



It focuses entirely on understanding and analyzing the external attack surface from the attacker's perspective.

CYBER ZONES
Innovation & Research Division

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

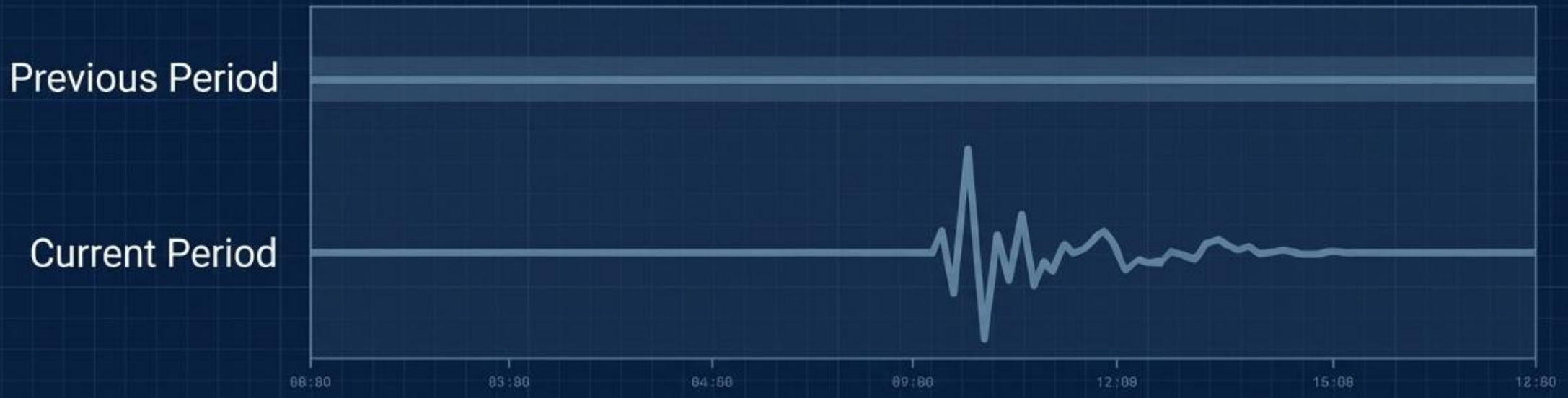
1. External Attack Surface Discovery

- **Asset Mapping**
  Identify all domains and digital assets linked to the organization.
- **Service Analysis**
  Analyze and footprint public-facing services.
- **Uncover Shadow IT**
  Discover operational assets operating outside formal IT governance (Shadow IT).
- **Attacker's Lens**
  Reveal the true digital infrastructure from an independent, external perspective.

CYBER ZONES
Innovation & Research Division

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

2. Continuous Exposure Monitoring



Generating Delta Intelligence by analyzing the variance between time periods.

- Continuously track changes in the organization's digital presence.
- Detect the immediate emergence of new, unapproved assets.
- Identify configuration shifts that elevate the overall risk level.

What changed?

Instantly highlights new assets, recent exposures, and fluctuations in risk posture.

CYBER ZONES
Innovation & Research Division

3. OSINT-Driven Risk Intelligence

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

Open Data
(Analyzing publicly available information).

Data Analysis
(Linking findings directly to business risk context).

Exposure Classification
(Categorizing the severity of the exposure).

Contextual Intelligence
(Supporting security decision-making based on independent external visibility).

4. Preventive Security Posture

Preempt Exploitation:

Address digital exposure before threat actors can exploit it.

Target Hardening:

Drastically reduce the likelihood of the organization becoming a crime-of-opportunity target.

Visibility Control:

Improve internal management and governance of previously invisible digital assets.

Mechanism of Action: From Collection to Analysis

Collect:
Gather data on publicly visible infrastructure.

Classify:
Categorize and score the level of exposure.

Record:
Store results within a historical ledger to enable chronological comparison.

Scenario: If a new subdomain unlinked to the organization suddenly appears, Sentinel detects it, runs a chronological comparison against previous baseline results, and logs it as a new environmental change—flagging a potential exposure point long before exploitation occurs.

How Does Sentinel Differ from Traditional Security?

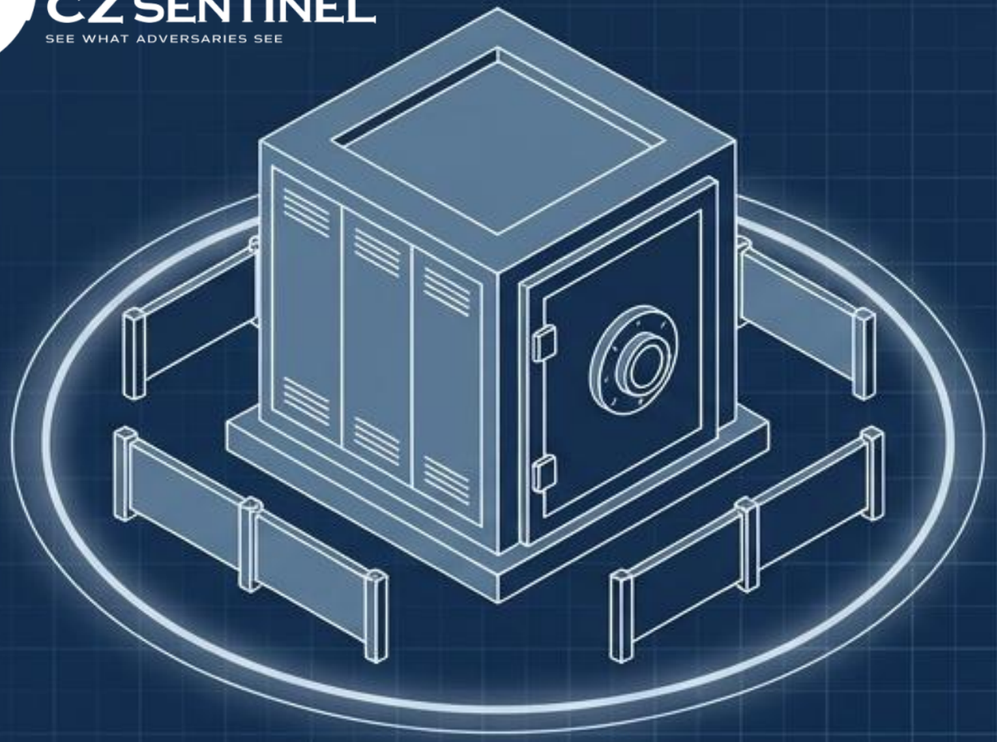
Traditional Tools	CYBER ZONES CZ SENTINEL SEE WHAT ADVERSARIES SEE
Internal network focus	Focuses on external risks
Requires internal system access	Zero internal access required
Discovers direct technical vulnerabilities	Discovers exposure and business context
Often operates post-breach	Addresses the pre-attack phase
Limited perspective	The attacker's perspective is fundamental by design

Sentinel does not replace your traditional security tools; it complements them by bridging the critical external visibility gap.

Built on Operational Expertise

Sentinel is an intelligence platform built from the ground up on deep consulting experience and practical expertise in analyzing complex enterprise exposure.

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE



Data Sovereignty and On-Premise Deployment

Total Control:

Grants the organization complete control over its intelligence data without relying on external cloud platforms.

Contextual Analysis:

Does not rely merely on third-party, ready-made intelligence feeds. It actively re-analyzes exposure specifically within the unique context of the organization.

Executive Ready:

Generates professional, highly polished reporting designed directly for sharing at the executive and board levels.

CYBER ZONES
Innovation & Research Division

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

The Sentinel Advantage (Summary)

- **Comprehensive digital exposure intelligence** and external attack surface management.
- **Developed internally** by Cyber Zones through rigorous R&D initiatives.
- **Focuses exclusively** on the critical pre-attack phase.
- **Transforms** chaotic open data into operational risk visibility.
- Grants the enterprise the attacker's perspective... before the attack begins.

CYBER ZONES
Innovation & Research Division

CYBER ZONES
CZ SENTINEL
SEE WHAT ADVERSARIES SEE

Start Seeing What Adversaries See.

We invite enterprise organizations and security leaders to experience the platform.

CYBER ZONES
DIGITAL ZONES CONSULTING

CYBER ZONES | Digital Zones Consulting
Email: info@cyber-zones.com
Web: https://cyber-zones.com/research-division

CYBER ZONES
Innovation & Research Division