A FIELD BRIEFING FOR MODERN DEFENDERS

THE THREATS WON'T STOP. WHAT ARE YOU DOING ABOUT IT?

Detection without action is just a feeling.

Adversaries don't wait for your quarterly scan. New CVEs land daily. Ransomware crews retool weekly. OT environments expose protocols designed before "internet" was a word. SeverityZero runs continuously against everything you own — IT, web, cloud, internal, and industrial — then prioritizes what's actually reachable, exploitable, and on a ransomware playbook today.

PLATFORM
CONTINUOUS THREAT EXPOSURE ENGINE

● LIVE
MULTI-TENANT SAAS
ZERO INSTALL FOR CLIENTS

7×	329K+	11	4-Stage
SCAN MODES FAST TO COMPREHENSIVE	EPSS-SCORED CVES SYNCED DAILY	OT/ICS PROTOCOLS READ-ONLY SAFE	VALIDATION FUNNEL DETECTED → CONFIRMED

SEE EVERYTHING. // 01

Multi-engine scanning orchestrated across seven scan modes. Edge agents reach networks behind firewalls over double-encrypted tunnels with zero inbound ports.

EXTERNAL · INTERNAL · OT/ICS · CLOUD · WEB APP · CONTINUOUS

PRIORITIZE WHAT MATTERS. // 02

EPSS exploitation probability, CISA KEV correlation, and a weighted Ransomware Exposure Index surface what attackers will actually use. Fingerprint deduplication, lifecycle tracking, and auto-close on retest kill the noise.

EPSS · CISA KEV · RANSOMWARE INDEX · MITRE ATT&CK

CATCH THEM EARLY. // 03

Edge Defense turns the scanner into a sensor — passive honeypot-like telemetry detects ping sweeps, port scans, Responder behavior, and IPv6 RA anomalies before the breach. Pre-attack discovery, mapped to MITRE ATT&CK.

RECON DETECTION · LLMNR/NBNS · PRE-ATTACK TTPS

PROVE YOUR POSTURE. // 04

Pentest readiness scoring, executive PDFs, evidence packs, SBOMs (CycloneDX 1.5), and built-in PTaaS workflow with an 8-stage engagement lifecycle — so audit, board, and customer questions all get answered the same week they're asked.

IEC 62443 · NERC CIP · NIST 800-82 · SBOM · PTAAS

INSIDE THE PLATFORM.

Built for defenders who are tired of scanner output that reads like a phone book and reports that arrive after the breach. This is what your team actually sees, day one.

EXPOSURE DASHBOARD — LIVE VIEW

DISCOVERY

Continuous Multi-Engine Scanning

Seven modes from **Fast** recon to **Ultra** sweeps, plus **Comprehensive**, **Advanced**, **Internal**, and looping **Continuous** assessments. Scheduled daily through annually with duplicate-scope detection and per-tenant admission controls.

OT / ICS

Industrial Protocol Coverage

Read-only probes for Modbus, S7comm, EtherNet/IP, BACnet, DNP3, OPC UA, FINS, Fox, CODESYS, SNMP, and more. **30+ vendor OUI fingerprints** — Siemens, Rockwell, Schneider, ABB, Honeywell, GE, Omron. Persistent device inventory tracks firmware drift over time.

RISK SCORING

Ransomware Exposure Index

Weighted score blending CVSS (30%), CISA KEV (20%), ransomware-group association (20%), reachability (15%), asset density (10%), and misconfigurations (5%). Curated knowledge base maps findings to attacker phases — initial access through credential theft.

EDGE REACH + DEFENSE

Internal Edge Scanner & Pre-Attack Sensor

One-command Docker deploy with **encrypted tunnel-bridge** — no inbound ports on the client network. Sensor mode adds passive pre-attack telemetry detecting **ping sweeps**, **port scans**, **Responder-style anomalies**, and **IPv6 RA spoofing** mapped to MITRE ATT&CK discovery techniques.

TRIAGE + VALIDATION

Lifecycle & 4-Stage Confidence Funnel

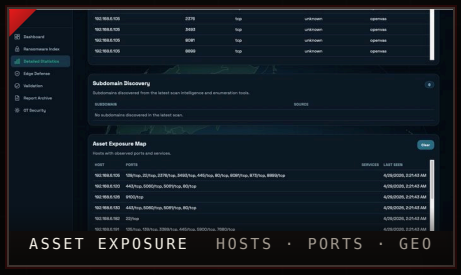
Fingerprint-based dedup flags **net-new exposures**, **reopened findings**, and **materially changed evidence**. Auto-close on retest. Confidence escalates from **Detected** → **Corroborated** → **Validated** → **Exploitability Confirmed** via per-finding re-checks.

PTAAS

Pentest-as-a-Service Workflow

Eight-stage engagement lifecycle from **Information Needed** through **Report Available**, with client-visible status, scope target management, per-engagement notes, and a full event audit trail. Pentest readiness score (0–100) shows when you're ready before you book the test.

EDGE DEFENSE — PRE-ATTACK TELEMETRY



ASSET EXPOSURE — HOSTS · PORTS · GEO

ATTACK FLOW — ENTRY → ASSET → FINDING

WHY SEVERITYZERO.

→ **IT and OT in one pane.**
Most platforms treat industrial systems as an afterthought. We probe 11 ICS protocols safely and map every finding to IEC 62443, NERC CIP, and NIST 800-82.

→ **Scanner that becomes a sensor.**
The same edge agent that reaches private networks also runs as a passive honeypot, catching reconnaissance before exploitation.

→ **PTaaS without the agency dance.**
Built-in 8-stage pentest workflow with client-visible status. Readiness scoring tells you when to book — not after a wasted engagement.

→ **Reachability over CVSS theater.**
EPSS plus CISA KEV plus ransomware-group association — we score what attackers will actually weaponize, not what looks scary in a spreadsheet.

→ **Adversary-aware by design.**
The team behind SeverityZero spent 20+ years on both sides — breaching networks and defending them. That perspective shapes every score, every detection, every workflow.

→ **Zero install for your team.**
Nothing to stand up, nothing to patch. Optional Internal Edge Scanner drops in as a single-command Docker agent — encrypted tunnel out, no inbound ports, eleven automated readiness checks before it goes live.

STOP REACTING.
START HUNTING EXPOSURE.

Book a platform walkthrough — see your real attack surface in under an hour.

SEVERITYZERO.COM
HELLO @ SEVERITYZERO.COM

● AVAILABLE NOW