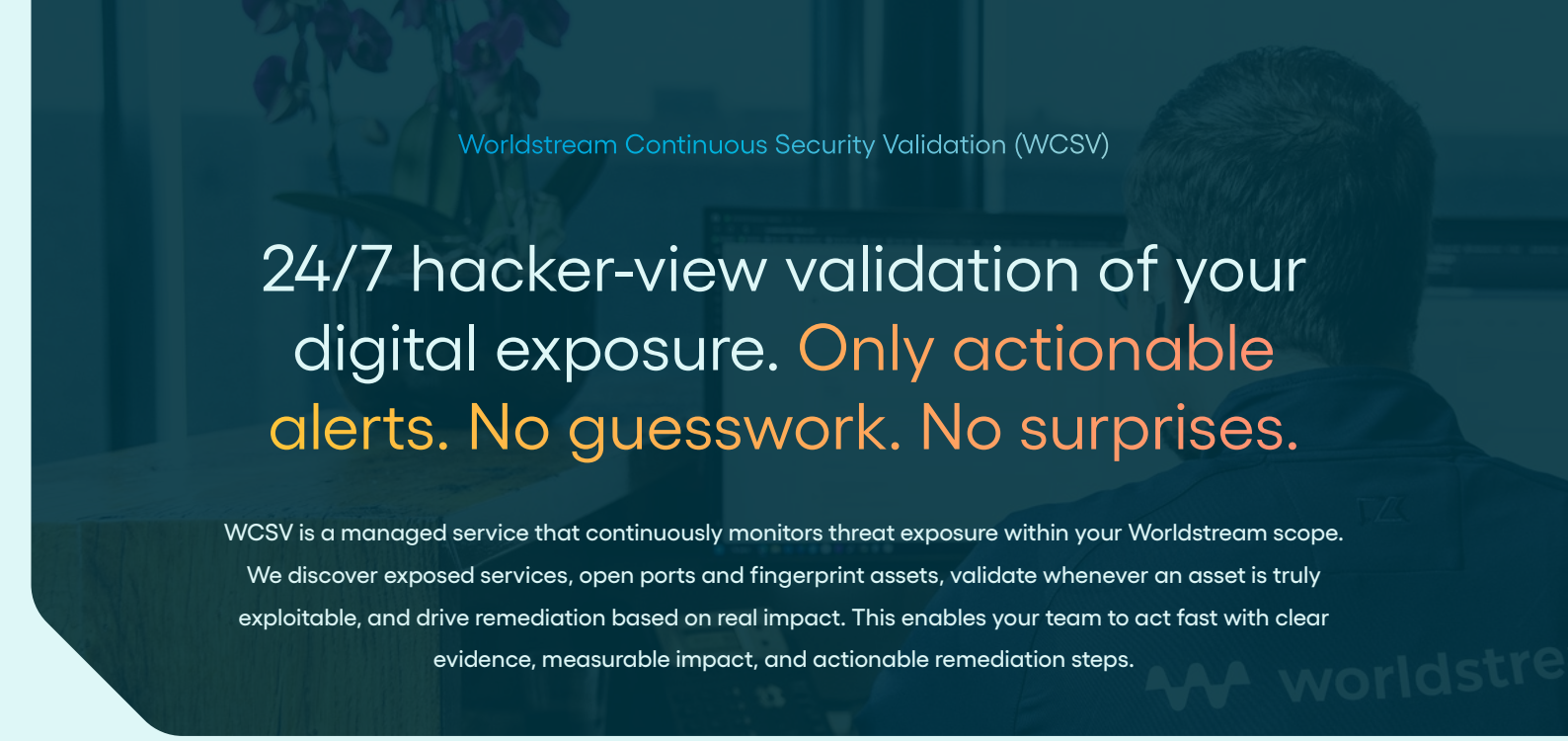

Worldstream Continuous Security Validation (WCSV)

24/7 hacker-view validation of your digital exposure. Only actionable alerts. No guesswork. No surprises.

WCSV is a managed service that continuously monitors threat exposure within your Worldstream scope. We discover exposed services, open ports and fingerprint assets, validate whenever an asset is truly exploitable, and drive remediation based on real impact. This enables your team to act fast with clear evidence, measurable impact, and actionable remediation steps.

Common challenges

Even with traditional vulnerability scanning, teams still find it hard to consistently turn exposure into action.

- **Disconnected signals:** asset data, vulnerabilities, misconfigurations, and threat intelligence don't converge into one clear priority list
- **Limited validation:** "critical" doesn't always mean exploitable in your environment
- **Constant change:** new assets, deployments, and configuration drift create new exposure every day
- **Remediation bottlenecks:** ownership, evidence, and clear fix steps are missing. The same risks keep resurfacing.

Business impact

Here's what those challenges translate to at a business level: higher risk, slower remediation, more operational load, and more friction in governance and audits.

- **Higher incident likelihood** when external exposure isn't continuously managed
- **Longer time-to-remediate** due to noise and missing context
- **More operational pressure** from manual investigation and follow-up
- **More audit friction** without consistent reporting and evidence

The Solution?

Worldstream Continuous Security Validation

WCSV gives you a continuous, attacker-led view of your threat exposure, so you can stay ahead of risks and changes instead of chasing scan results. We separate what's theoretical from what's proven — and surface the real attacker openings in your environment, backed by evidence, impact, and clear remediation guidance. No noise. Just Solid IT.

"By 2026, organizations prioritizing their security investments based on a continuous exposure management program will be three times less likely to suffer a breach." — Gartner

worldstream

How it works

1	Define scope	Worldstream-hosted IPs/domains, notification channels and reporting cadence.
2	Continuous discovery	Keep your external exposure inventory current as it changes.
3	Continuous testing	Identify vulnerabilities, misconfigurations, and exposure risks.
4	Threat exposure validation	Confirm what is truly exploitable and provide evidence and context, including how an attacker could chain the weakness.
5	Alerts, reporting & fix verification	Proactive, low-noise alerts with high-value insights, monthly reporting, and post-fix verification to confirm the risk is removed.

What you get (deliverables)

- **Always-on monitoring** of in-scope Worldstream-hosted assets
- **Actionable alerts** on proven exploitable risks (severity, impact, evidence, remediation steps)
- **Monthly executive & technical reports** (useful for governance, cyber hygiene and audit/compliance processes
- **Fix verification** after remediation (regression testing)

Outcomes

- **Less noise. Faster fixes.** (exploitability-first)
- **Continuous coverage** (no gaps between assessments)
- **Reduced triage effort** through validation and risk-based prioritization
- **Measurable posture improvement** with clear reporting and trends over time

Pricing overview

Pay-per-use.
You pay per monitored IP, per month. No setup fees. No retainers.

Amount of IPs	Price per IP / Month
1 - 5	€ 25,00
6 - 50	€ 21,00
51 - 100	€ 18,00
100+	€ 15,00

All prices excl. VAT. Volume discounts apply automatically based on the total number of monitored IPs.

Monitoring a larger scope or need a custom setup? Contact us for a tailored quote.

Use cases

Continuous Attack Surface Management (ASM)	Continuously discover and track everything that is internet-exposed in scope, including newly appearing assets.
Exploitability validation & prioritised remediation	Validate what's actually exploitable (not theoretical) and focus fixes on the highest-impact attacker openings first.
Continuous testing	Keep validating real attacker paths continuously instead of relying on point-in-time pentest windows.
Cloud / internet-facing configuration exposure control	Spot and validate public-facing misconfigurations and exposures as cloud environments change.
Change-driven exposure monitoring (release / migration / new environments)	Automatically catch new attacker openings introduced by deployments, migrations, or new services.
Attack Exposure Validation (AEV)	Continues validation on how your defenses help you protect against known adversary techniques, tactics, and procedures.

Get started

Want no surprises in your external exposure?

Book a 20-minute WCSV scope walkthrough. We'll show exactly what we monitor in your Worldstream environment and what output you can expect.

sales@worldstream.com

+31 (0)174 712 117

www.worldstream.com

worldstream