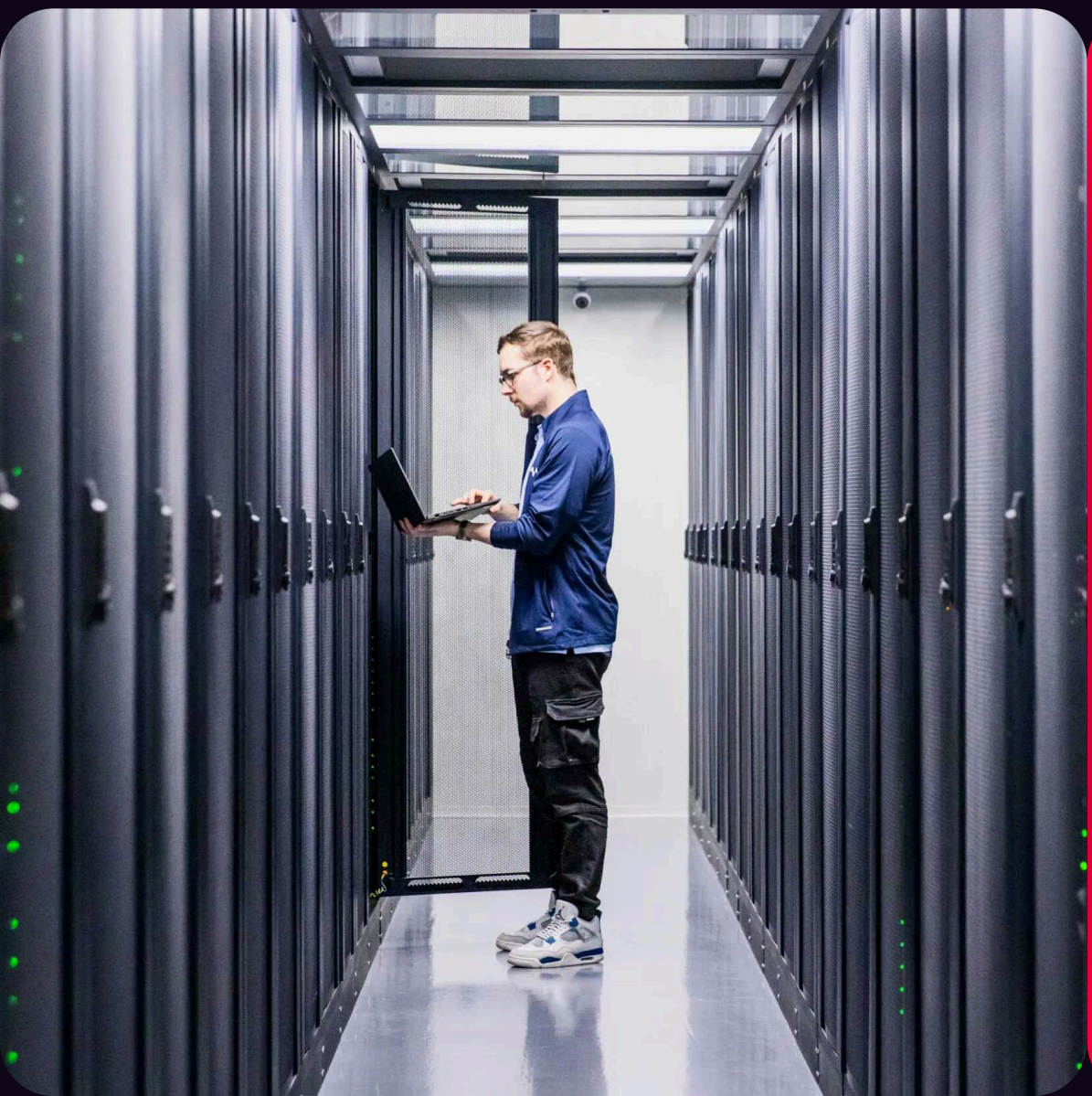
HADRIAN

WORLDSTREAM

CASE STUDY

How Worldstream operationalized continuous exposure management across a critical infrastructure environment

IT INFRASTRUCTURE, THE NETHERLANDS

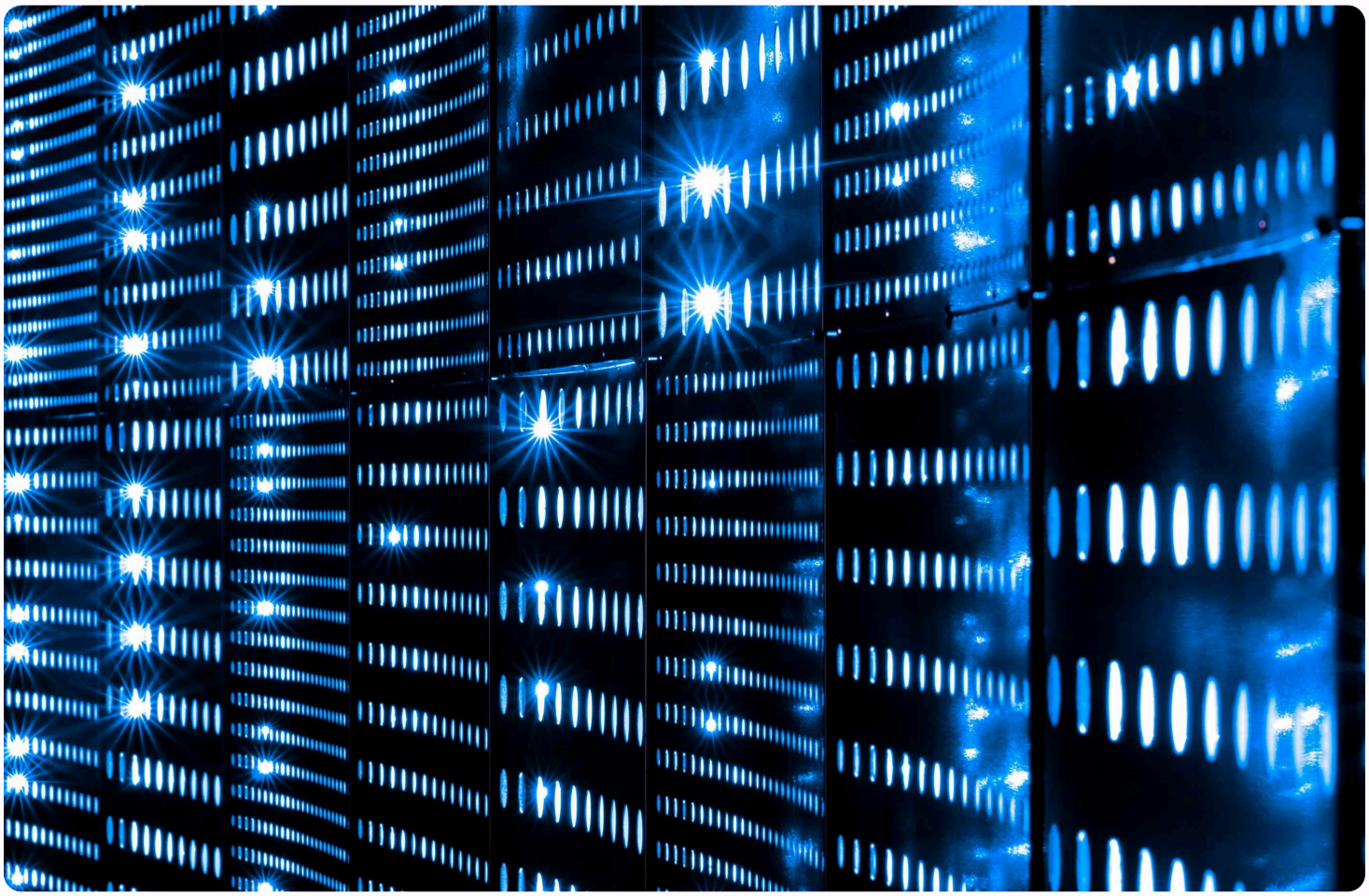


About Worldstream

Worldstream is a Dutch cloud infrastructure provider with its own data centers and its own network in Europe. Since 2006, we design, build, and manage IT infrastructure for organizations that require control, transparency and predictability.

Worldstream delivers dedicated servers, private cloud, and hybrid infrastructure solutions for mission-critical workloads. By keeping the infrastructure chain in-house, from data centers and network to hardware and 24/7 support, Worldstream provides organizations a solid, transparent, and predictable foundation for modern IT environments.

FOUNDED	PHYSICAL SERVERS	CUSTOMERS
2006	15,000+	2,500+



Challenges

01 **Maintaining continuous control over an evolving attack surface**

The organizations hosting their workloads with Worldstream expect the infrastructure to be stable and secure. Security is a core part of the value the business delivers, and maintaining real-time, always-on visibility over every externally exposed asset is what that promise requires.

02 **Modernizing from vulnerability management to exposure-led prioritization**

The team was managing a large, complex estate using traditional vulnerability management, prioritizing findings by CVSS scores.

03 **Ensuring every escalation is warranted**

Worldstream's security monitoring team continuously tracks the attack surface while a cross-disciplinary incident response team stands ready for critical findings. The goal was to ensure only confirmed, genuinely exploitable findings triggered an escalation, so expert capacity was deployed precisely where it mattered most.

Solution

✓ **Continuous outside-in visibility across the attack surface**

Worldstream's security team now has a real-time, continuously updated view of its entire external-facing infrastructure, mapped from the outside in with Hadrian. New assets and domains are surfaced the moment they appear, so the environment never outpaces what the team can see.

✓ **Exposure-led prioritization replacing volume-driven vulnerability management**

Rather than working through large volumes of findings ranked by CVSS score, Worldstream's security team now focuses on a smaller set of exposures confirmed as genuinely exploitable in their specific environment. Each finding is checked against real-world exploitability and business context before it reaches the team, turning a long list of possibilities into a short list of priorities.

✓ **Validated findings that make every escalation count**

Before a finding reaches the security monitoring team, it's confirmed as a real, exploitable risk, not a theoretical one. That gives the team confidence to escalate only what matters, and gives the incident response team everything they need to act immediately, without re-investigating from scratch. Every escalation is warranted. Every response is precise.

Outcome

Continuous visibility as a customer promise

For Worldstream, attack surface visibility is not just an internal security objective. It is part of what customers are buying when they choose to host their workloads with a critical infrastructure provider. Organizations that choose Worldstream expect infrastructure that's continuously secured, monitored, and in control of its own exposure. That's a promise periodic assessments and point-in-time snapshots can't keep.

Worldstream's security team now accounts for every exposed asset in real time, as the infrastructure evolves. New domains, new services, and changes in exposure are caught the moment they occur, not at the next scheduled review. Whether growth comes from new customer deployments, expanded services, or network changes, the team sees it immediately, and the attack surface never drifts unmonitored. That capability translates directly into the assurance Worldstream's customers expect: that the infrastructure they depend on is under continuous, active control, not just reviewed on a schedule.

> **"With Hadrian, you have a really strong partner in operationalizing continuous exposure management at scale. It requires not so much effort to set up, improves your efficiency in mitigating findings and risk reduction, and it is really easy to use, scalable, and repeatable."**
>
> Alan Lucas - CISO, Worldstream

From scoring to validated exploitability

Worldstream's security team now operates against a smaller, higher-confidence set of confirmed, exploitable exposures rather than working through large volumes of findings ranked by CVSS scores. Hadrian validates each finding against real-world exploitability and the specific context of Worldstream's environment before surfacing it, so the team acts on what actually matters rather than what a scoring model suggests might matter.
That shift also changes how the security program is measured and reported. Worldstream tracks its security score across the external attack surface, the percentage of assets under continuous scanning, and mean time to identify, contain, eradicate, and recover, all mapped to the NIST Cybersecurity Framework. That structure now runs on a live, validated foundation. For a provider operating under PCI DSS, preparing for NIS2, and serving as an ICT third-party service provider under DORA, that continuous evidence of control matters both operationally and commercially.

Outcome

An escalation model the whole team trusts

The operational impact of validation extends beyond the security monitoring team itself. Worldstream's incident response function is made up of senior experts drawn from across the organization, each bringing deep domain knowledge in their respective area, available on standby to respond to critical findings. That model only works if the findings that trigger an escalation are genuinely worth acting on.

With Hadrian confirming exploitability before a finding reaches the security monitoring team, the decision to escalate carries a level of confidence that matches the standard Worldstream holds itself to. The monitoring team knows that what they are passing on has been tested and confirmed as a real, exploitable exposure, not a theoretical risk that may or may not apply to their environment. The incident response team, in turn, receives validated findings with the full context needed to act immediately, without having to re-investigate from scratch. Each escalation is warranted, each response is precise, and the relationship between the two teams is built on signal rather than noise. That dynamic is what allows Worldstream's security function to operate at the speed and scale its infrastructure demands.