Moving millions with WSO2

HTM | kom verder!

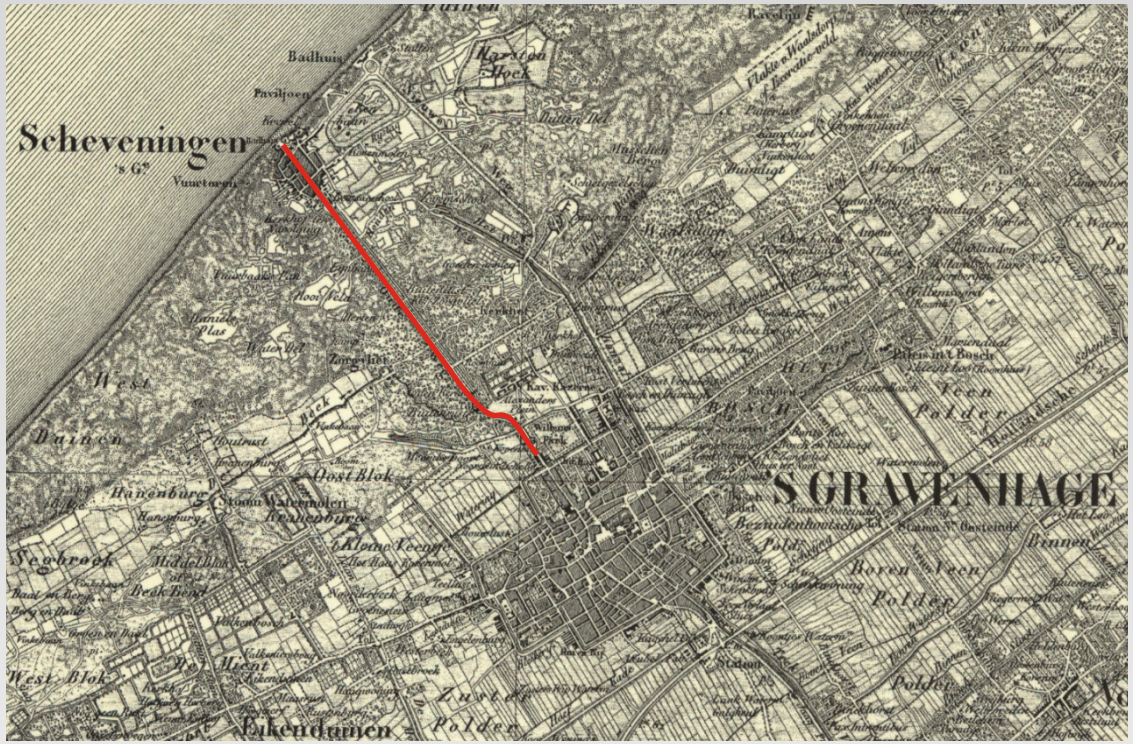
Me

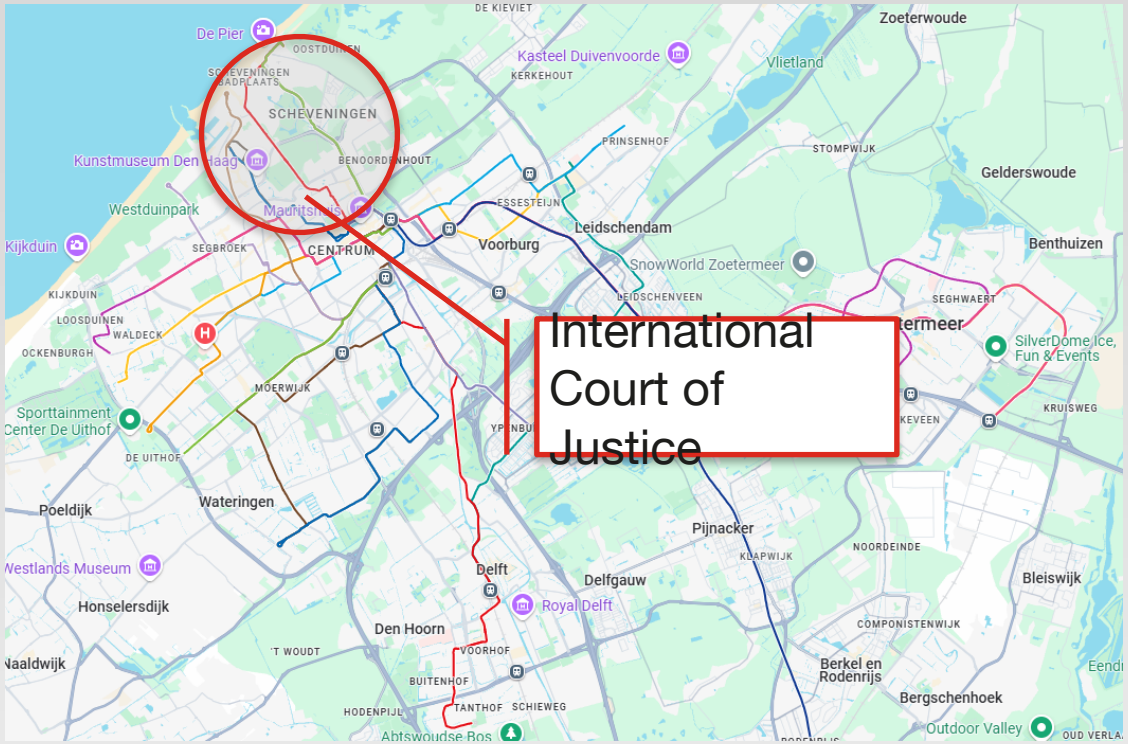
Toby van Willegen
Domain Architect, Operations & Maintenance
HTM Personenvervoer N.V. — The Hague

I draw the landscape. **I don't configure WSO2.**
So today: principles, choices, and the shape of the problem — not screenshots of admin consoles.

HTM - 160 years of moving the city

- Public transport company in the Netherlands
- Providing transport for over 160 years.





HTM | kom verder!

The fleet today

GTL-8 (x71)
From: 1981

Regio Citadis (x71)
From: 2006

Real-time vehicle data

Avenio (x60)
From: 2015

Real-time vehicle data

TINA (x62)
From: 2027

MAN (x115)
From: 2009
Fuel: CNG

VDL (x8)
From: 2018
Fuel: Electric

Real-time vehicle data

eCitaro 12m (x42)
From: 2025
Fuel: Electric

Real-time vehicle data

eCitaro 18m (x60)
From: 2025
Fuel: Electric

HTM | kom verder!

The fleet is now a data platform

YESTERDAY

Mechanical

telemetry by exception

TODAY

Streaming

telemetry continuous

TOMORROW

Connected

every vehicle, all infrastructure

Telemetry is no longer data. ***It is a decision surface.***

It is a decision surface.

It is an attack surface.

The pattern

A wave of recent breaches:

- **275 million records — education software**
- **6.2 million records — major telecom**
- **1 million records — fitness chain**
- **Undisclosed — booking platform**
- **Undisclosed — cosmetics retailer**

These are breaches *from the past 3 months, that I could fit on a slide.*

These were not caused by AI. They were caused by the foundation underneath:
exposed APIs · weak auth · missing scopes · leaked secrets · no observability

Shiny new things

WEBSITES

Pages

humans read

APIs

Contracts

machines call

AGENTS

Pages + Contracts

machines that act
like humans

The castle

The castle’s defence doesn’t stop at the wall.

1. Drawbridge: a controlled front door

One way in.

On purpose.

If you have a second front door, you have no front door.

AT HTM

WSO2 API Manager is the declared front door. Anything else is documented, or being found.

2. House keys: what, not just who

Authentication is who.
Authorisation is what.

Top API risk: broken authorisation. Not authentication.

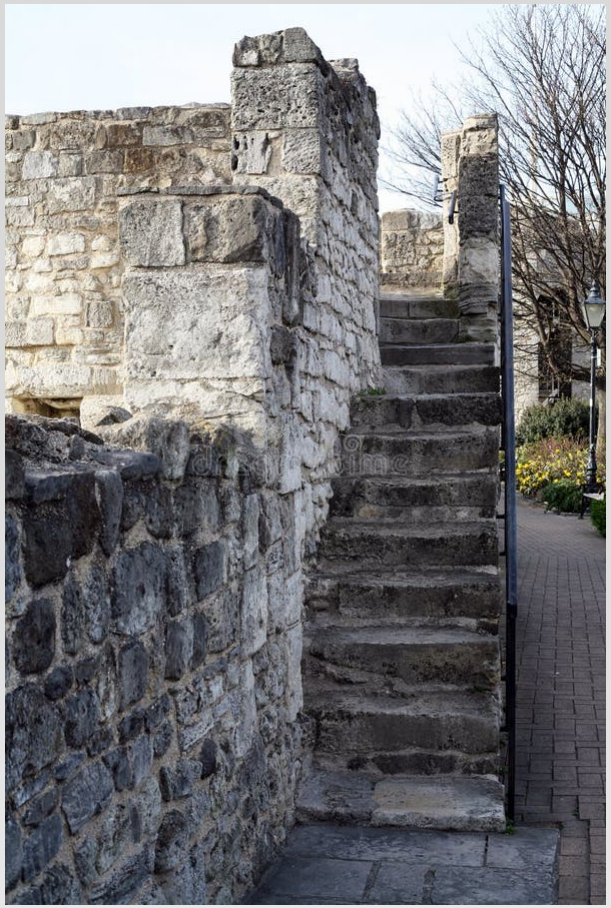
AT HTM

Identity historically sits with Entra. The gateway is WSO2 API Manager. Scoping every key to one door — that's still the work.

3. Uneven stairs: built for the defender

Designed for the defender.

Not the visitor's comfort.



Rate limits stop brute force. The agent threat hides in normal-looking traffic.

AT HTM

Broad rate limits and network anomaly detection. Message-level anomaly detection — still on the roadmap, but possible together with API Manager.

4. The high ground: see them coming, see them inside

You can’t defend what you can’t see.

And you can’t see what you didn’t build for.

Observability is not a dashboard. It’s a forensic record.

AT HTM

SIEM v1 is live. Logs flow. Correlation IDs on the calls that matter.
One integrated view is still being built.

The stone

API Manager. Micro Integrator. Entra. The SIEM.

The stones matter.
The castle matters more.

Nobody is done

Not HTM. Not most of the room.

Agents didn't break the foundation. They exposed the cracks we were already living with.

The work is the same work it always was.
The deadline just moved up.