FRENOS

FRENOS.IO
INFO@FRENOS.IO

CASE STUDY — S4X26 POC PAVILION

42 MINUTES. 154,000 SIMULATIONS. 18 VALIDATED ATTACK PATHS.

Completed a simulated OT penetration test — live, on stage, on a laptop — at the industry's most demanding proof-of-concept event.

11m 42s	154,000	18	17m 7s
INSTALL TO DIGITAL TWIN	*ATTACK PATH SIMULATIONS*	*VALIDATED ATTACK PATHS*	*TOTAL ASSESSMENT TIME*

THE CHALLENGE

Dale Peterson and the Booz Allen Hamilton team build a highly realistic automotive environment — MES, SCADA, HMI, and PLC layers running Inductive Automation, Rockwell, and Siemens — then hand eight vendors a live network and tell them to prove their products work. No canned demos. No safety net.You either show real capability on an environment you've never seen before, or get kicked out of the PoC Pavillion.

THE APPROACH — FOUR DAYS, ONE LAPTOP

DAY 1

INSTALL

- *Install on a fresh laptop ->* 11m 42s
- *Firewall configs arrived 12:41 PM.*
- *Digital twin built by 12:47 PM*
- *No hardware, sensors, agents, or SPAN ports required*

DAY 2

SIMULATE

- *Overnight firewall/topology changes ingested in minutes.*
- *Ingested asset and vuln data from Claroty and Dragos*
- *SAIRA ran* 154,000 simulations in 17m 7s *across 2 assumed-breach networks (iDMZ, Enterprise).*

DAY 3

INTEGRATE

- *Built brand-new Cisco Cyber Vision parser* in under 3 hours.
- *Normalized 63,928 flow records and 193 vulns*
- *55 of 56 assets auto-matched to the Frenos model.*

DAY 4

DELIVER

- *Completed simlated OT penetration test in 17 mins 7 secs*
- *42 mins total from install to completion*
- *Completed live demo for S4x26 attendees*

THE RESULT

From 154,000 Paths to the 18 That Matter

Frenos' Simulated AI-powered Adversarial Reasoning Agent (SAIRA) modeled every feasible path an attacker could take given the actual firewall rules, routing, and configurations in the environment. Out of 154,000 simulated paths, SAIRA validated 18 exploitable routes into the critical Rockwell and Siemens zone. Not theoretical CVSS findings, paths confirmed against real controls in the digital twin.

By the numbers

- *11m 42s install → live digital twin*
- *154,000 attack path simulations executed*
- *17m 7s total SAIRA simulation runtime*
- *86% asset coverage / 41% fully enriched*
- *63,928 Cyber Vision flows normalized into asset model*
- *42 min end-to-end — install → twin → simulate → validate*
- *Ran entire simulation on a MacBook Pro; zero touching of OT network, software, or devices.*

WHY IT MATTERS

For a decade, OT security has focused on visibility and vulnerability collection, necessary foundational work. But visibility alone doesn't answer the question every asset owner is asking: what can an adversary actually do in my environment right now and what mitigations should I focus on?

Frenos answers that in minutes, not months, using data the environment already produces safely, inside a consequence-free digital twin.

> ***"We completed a simulated OT penetration test, from installation to validated attack paths, in just 42 total minutes on a laptop. Let that sink in for a second."***
>
> — BRIAN PROCTOR & HARRY THOMAS, FOUNDERS, FRENOS

BUILD YOUR RESILIENCE ▸ FRENOS.IO