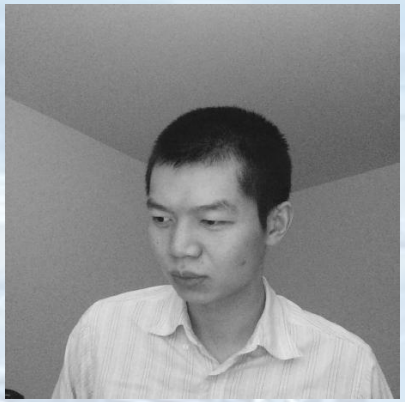
Port Sentinel

Predictive Exploitation AI for Maritime Infrastructure

Dev Team



Yingquan Li

STScI/NASA

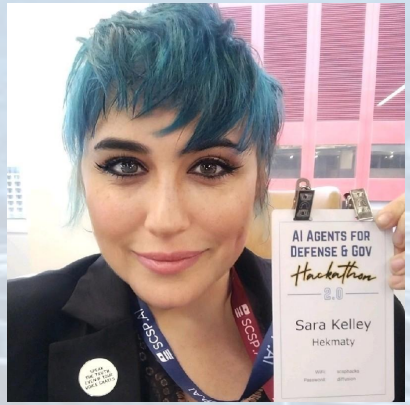
Kshitij Kumar Parashar

Carnegie Mellon Alumni

Thomas Ewing

Attorney

US Navy Reserve



Sara Hekmaty

Cayuse Government Operations

Port Sentinel

Problem Statement in Numbers

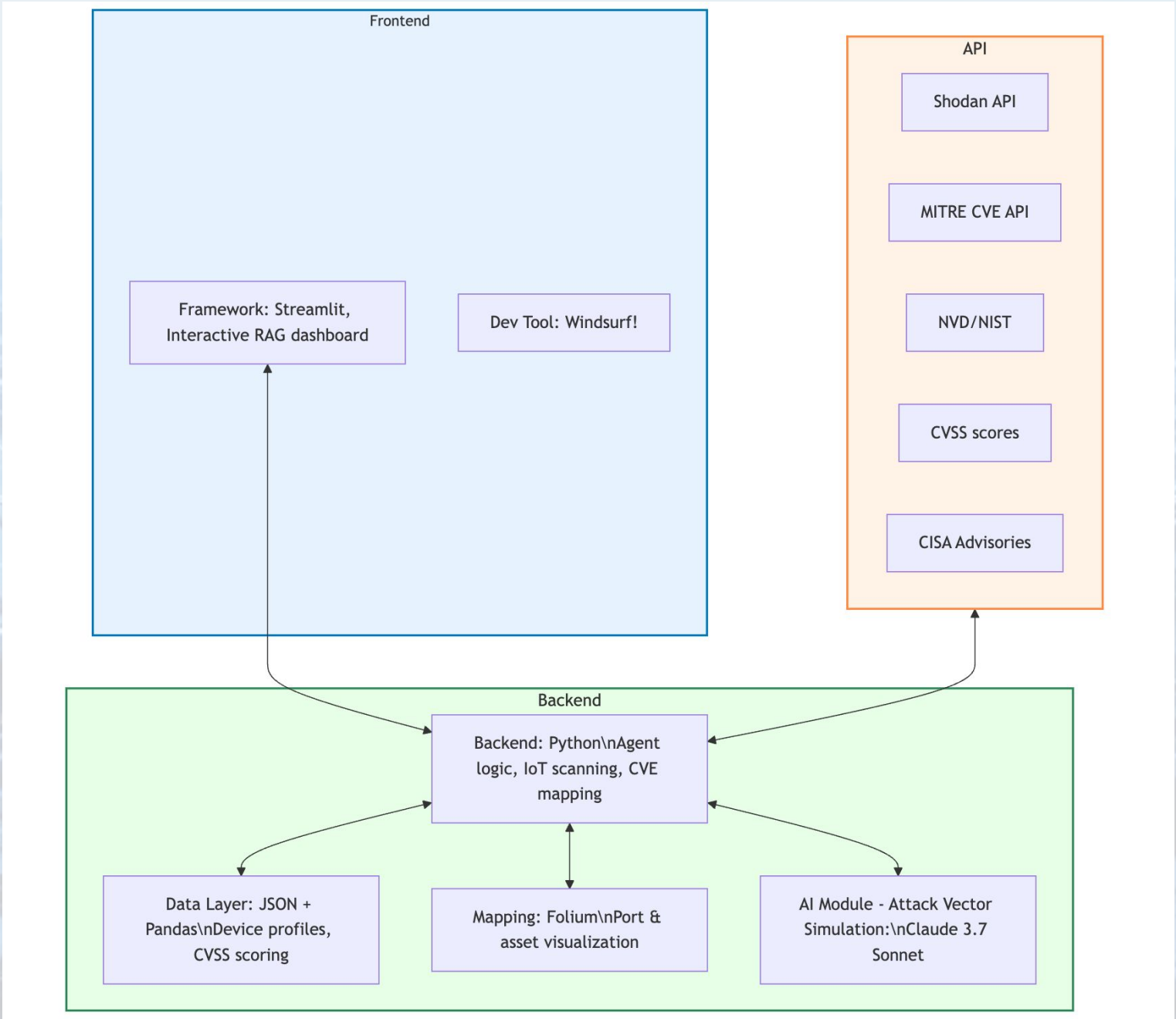
Legacy OT systems (SCADA, Modbus, RTSP) remain widely deployed and exposed across maritime infrastructure — making ports, shipyards, and logistics hubs prime cyber targets.

- A single port shutdown can cause **$1.7B** in losses per week
- The Port of Los Angeles blocks **40M+ cyber intrusion attempts** per month
- Shodan identified 110,000+ ICS devices, including **6,500+ PLCs** linked to critical infrastructure

To defend forward, we must simulate forward.

Port Sentinel lets us preempt the adversary — by using their playbook.

Port Sentinel



Architecture

Ready For Integration

- Deployable in commercial or government environments
- Complements existing cyber toolchains and assessments

Port Sentinel

Port Sentinel Workflow

1: Recon

- Scans internal + public surfaces (e.g., Shodan, local agents)
- Detects IoT/ICS/OT systems, services, firmware types

2: Analyze

- Cross-references with CVE/NVD/CISA advisories
- Scores severity, flags exploitable vectors
- Assigns Red/Amber/Green status per asset

3: Simulate

- Emulates exploit chains across devices/networks
- Visualizes lateral movement and mission impact
- Generates exploit trees and critical path maps

4: Plan Attack

- Outputs prioritized mitigation steps
- Suggests hardening actions: config fixes, segmentation, patch paths
- Provides Red Team + Blue Team summaries

Port Sentinel

DEMO

https://youtu.be/zWZdr5rvC4A

Port Sentinel

Predictive & Agentic Enhancements

Simulate the threat. Secure the mission!

Use mobile data, Ship IoT, and traffic data to predict expanded attack vectors

Group ports with similar IoT footprint to facilitate alerts

Leverage Agentic AI to quickly exploit / remediate specific risks

Port Sentinel