

# DIGITAL TWINS FOR AI CYBERSECURITY

## THE POWER OF AUTONOMOUS OT SECURITY ASSESSMENTS

In an increasingly interconnected world, the security of critical infrastructure—from utility grids to transportation networks—is paramount. Traditional cybersecurity assessment methods often fall short in addressing the complex and dynamic nature of operational technology (OT) environments. A revolutionary approach is emerging, combining digital network twins with AI reasoning agents to provide autonomous, rapid, and proactive vulnerability identification. This ground-breaking platform utilizes carefully selected technologies to enhance security in mission-critical environments.

### Revolutionizing Critical Infrastructure Security

The world's first Autonomous OT Security Assessment Platform, developed by Frenos, is transforming how critical infrastructure teams assess their cybersecurity posture. Founded in 2023, Frenos has quickly gained recognition—notably winning the prestigious DataTribe Challenge in 2024, securing \$3.88 million in financing by outperforming hundreds of cybersecurity and data science startups.

Frenos's innovative platform assesses, prioritizes, and defends mission-critical environments, addressing the unique security challenges across all sixteen critical infrastructure sectors. This is achieved by simulating the physical and network environments of a utility company, replicating them virtually, and then deploying AI agents to identify vulnerabilities that could lead to physical breaches or cyber attacks, with potentially catastrophic consequences like grid outages.

### The Technical Foundation: Building a Robust Cybersecurity Platform

Our team provides comprehensive software development services to Frenos, encompassing the full lifecycle of their platform. This includes the development and maintenance of APIs, management of the database, and oversight of the platform infrastructure. We are responsible for handling code repositories, implementing deployment methods using Docker, and managing the release infrastructure, which includes Google Cloud Platform (GCP) configurations and Replicated services. Furthermore, our responsibilities extend to developing UI features, performing ongoing maintenance across the application, and responding to the evolving needs of new clients onboarded to the platform

- **Languages:** Go, Golang
- **Libraries:** React
- **Services:** ArangoDB, Kubernetes
- **Tools:** Docker



## Strategic Technology Selections and Their Advantages

The selection of our technology stack was driven by the demanding requirements of a continuous cybersecurity assessment platform for critical infrastructure. Each component plays a crucial role in enabling the platform's robust functionality, scalability, and security.

- **Go (Golang):** As a modern, compiled programming language, Go is ideally suited for developing high-performance, concurrent, and scalable backend services. In the context of a cybersecurity AI platform that continuously performs security assessments, Go's efficiency and excellent concurrency primitives are invaluable. It allows for the rapid processing of complex data, efficient API development, and the handling of numerous simultaneous operations—essential for simulating large-scale network environments and running multiple AI agents concurrently. Its strong typing and robust standard library also contribute to building reliable and maintainable code, critical for a platform dealing with sensitive security information.
- **React:** For the user interface (UI), React was chosen for its component-based architecture and efficiency in building dynamic and responsive web applications. For a platform that onboards new clients and requires intuitive visualization of complex cybersecurity data and assessment results, React's ability to create interactive and user-friendly interfaces is paramount. Its vast ecosystem and community support also facilitate rapid development and ongoing maintenance of UI features, ensuring a seamless experience for critical infrastructure teams.
- **ArangoDB:** This multi-model NoSQL database is a strategic choice for managing the diverse and often complex data generated by an AI-powered cybersecurity platform. ArangoDB's ability to handle document, graph, and key-value data models within a single database system is particularly advantageous for representing intricate network topologies, vulnerability relationships, and AI agent findings. Its flexibility allows for efficient storage and retrieval of vast amounts of assessment data, crucial for both real-time analysis and historical trend identification.
- **Kubernetes:** For orchestrating containerized applications, Kubernetes provides a powerful and scalable solution. In the context of simulating diverse physical and network environments and deploying AI agents for continuous assessments, Kubernetes enables efficient resource management, automated scaling, and high availability. It allows the platform to dynamically spin up and tear down virtual environments, isolate assessment processes, and ensure that the AI agents have the necessary computational resources without manual intervention. This is vital for a platform that must perform assessments across various critical infrastructure sectors with varying complexities.
- **Docker:** Docker is fundamental to our deployment strategy, providing a standardized way to package and run the platform's components, including the AI agents and supporting services. By containerizing applications, Docker ensures consistency across development, testing, and production environments, reducing compatibility issues and streamlining the deployment process. This is particularly beneficial for a cybersecurity platform where reliability and repeatable deployments are key, especially when replicating complex virtual environments for vulnerability assessment.

## AI Cybersecurity Twins - Conclusion

The development work for Frenos's Autonomous OT Security Assessment Platform exemplifies the power of strategic technology selection and robust software engineering in addressing critical cybersecurity challenges. By leveraging Go, React, ArangoDB, Kubernetes, and Docker, we have built a highly performant, scalable, and secure platform capable of continuously assessing and defending mission-critical environments. This work is not just about code; it's about safeguarding the essential services that underpin our modern world.

---



## A CATALYST FOR STARTUPS

If you have a product concept and are seeking capital for its development, consider First Factory's nearshore development team for expert design, development, and product ideation services. Our comprehensive software solutions, cloud infrastructure expertise, and product development services are designed to help you succeed. We pride ourselves on quickly understanding your business goals and adapting to your specific needs, rather than simply completing tasks.

[CONTACT US](#)

---