FRENOS

The Continuous Attack Surface Mitigation Platform

Introduction

The Frenos Platform helps enterprises understand their most probable attack paths while highlighting the most effective risk mitigations to deter and defend against today's adversaries. This innovative approach empowers security teams to focus on the most relevant and risk-reducing activities, saving time, money, and resources. Developed with design partners from five critical infrastructure sectors including finance, healthcare, energy, and manufacturing, the Frenos Platform is tailored to meet the unique challenges of securing all sixteen critical infrastructure sectors.

What is the Frenos Platform?

The Frenos Platform is an AI-driven adversarial attack path simulation platform focused on identifying the most probable successful adversary tactics, techniques, and procedures for the purpose of helping cybersecurity teams prioritize proactive risk mitigation activities.

Why the Frenos Platform?

Digital Twin + AI-Driven Adversarial Thinking:

- **Digital Network Twin: C**reates a digital twin of your network to simulate attack scenarios, offering a comprehensive view of possible threats without impacting live systems
- **AI Adversarial Intelligence:** The Frenos Platform employs trained AI within the digital twin to think like sophisticated adversaries, providing more accurate and realistic simulations of potential threats.

Dynamic Attack Path Analysis:

- **Prioritization of Threats:** Focuses on identifying and prioritizing the most likely attack paths and steps, ensuring security teams address the most critical first.
- **Comprehensive Insight:** By providing individual attack step techniques, tactics, or procedures that can be leveraged in sequence, the Frenos Platform provides a holistic view of potential attack scenarios.
- **Continuous Adaptive Environment Analysis:** Integrates with your existing security tools and technologies, adjusting the likelihood of attack success based on your current defenses.

Proactive Risk Mitigation:

- **Actionable Insights:** Delivers prioritized, actionable recommendations for mitigating risks, allowing for efficient allocation of security resources.
- **Strategic Focus:** Empowers security teams to take a proactive approach, staying ahead of potential threats rather than reacting to incidents

KEY BENEFITS

Enhanced Security Posture
Significantly improve your organization's defenses with intelligent, prioritized attack path analysis.

Efficient Resource Allocation
Optimize your security efforts by focusing on the most critical vulnerabilities, and attack paths.

Cost Savings
Reduce costs associated with manual penetration testing and reactive incident response by leveraging continuous, AI-driven analysis.

Time Efficiency
Save time with automated, real-time simulations and prioritized action plans, allowing security teams to focus on strategic tasks.

Future-Proof Defense
Stay ahead of evolving threats with an AI that continuously learns and adapts.