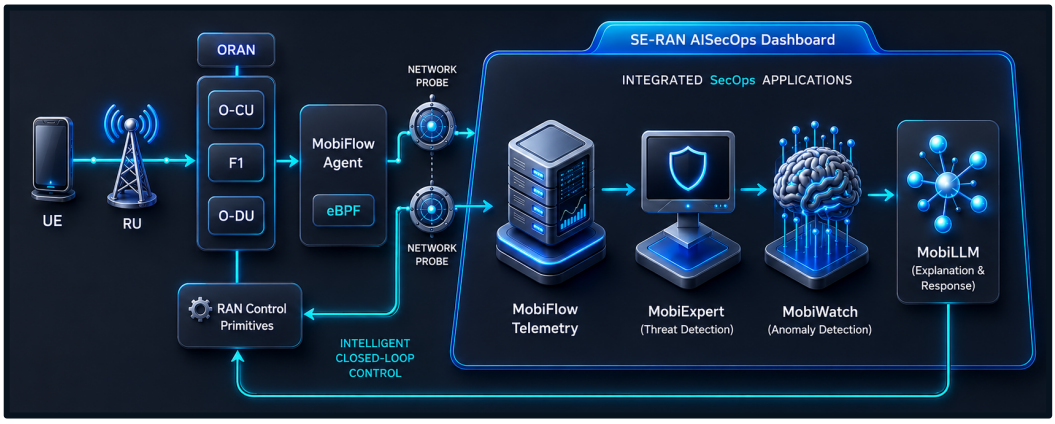
SE-RAN.AI – AI-SECOPS FOR AI-RANS



SE-RAN's AISecOps framework design. The figure illustrates our closed-loop interaction framework that introduces (1) The AISecOps Monitor using security-focused telemetry collection through the MobiFlow eBPF Agent, (2) AI-driven detection and diagnostic services including MobieXpert and MobiWatch, (3) A MobiLLM agentic AI Operator that automates closed-loop response to run-time threats and anomalies.

Our Mission: SE-RAN.ai seeks to secure and stabilize AI-driven 5G/6G radio access networks (RANs) by providing a runtime assurance layer for O-RAN and AI-RAN environments. It applies high-fidelity telemetry, protocol-aware analytics, and AI models to detect, explain, and mitigate control-plane threats and anomalous behavior in real time. Its AI Security Operations (AISecOps) platform seamlessly integrates with 3GPP- and O-RAN-compliant architectures to enable closed-loop, autonomous security operations across distributed, GPU-accelerated infrastructure, reducing risk from model compromise, telemetry poisoning, privilege abuse, and multi-tenant interference. This architecture aligns directly with the AI-RAN model, where AI increasingly drives network optimization, autonomous operations, fault diagnosis, and service orchestration.

Market Relevance: SE-RAN's architecture aligns strategically with the technology direction of NVIDIA, Samsung, SoftBank, Ericsson, Nokia, Red Hat, Rakuten Group, and the AI-RAN alliance, all advancing AI-native telecom platforms. Beyond security, SE-RAN reduces operational burden by automating continuous monitoring, anomaly triage, policy validation, and remediation workflows, enabling mobile network operators and Mobile Virtual Network Operators (MVNOs) to manage autonomous infrastructure with leaner teams and lower operational expense (OpEx). For private 5G deployments, where compliance, security assurance, and liability management often slow adoption, SE-RAN lowers deployment barriers through automated runtime assurance and security validation, making private-network operations economically practical at scale. For strategic investors, SE-RAN represents an IP-rich startup opportunity positioned at the intersection of AI-RAN, autonomous network operations, O-RAN security, and private-5G assurance.

Customer Benefits: SE-RAN.ai delivers a self-healing, self-defending network framework that slashes operational risk and infrastructure Total Cost of Ownership (TCO). By replacing legacy manual workflows with real-time AI analytics, automated causality testing, and machine-readable configuration fixes, the platform collapses Mean Time to Resolution (MTTR) while reducing infrastructure OpEx. SE-RAN.ai eliminates critical cellular-edge blind spots by detecting and autonomously mitigating sophisticated control-plane faults and threats completely missed by traditional enterprise firewalls—including signaling storms, false base station attacks, and handover manipulation. Built on native 3GPP and O-RAN compliant architectures (SMO, RICs, E2, A1), the vendor-agnostic solution seamlessly integrates into modern, multi-vendor cloud environments, completely neutralizing vendor lock-in and future-proofing mission-critical telecom infrastructure.

Our Solution: SE-RAN's AISecOps is designed through a modular approach, separated into three synergistic packages:

The SE-RAN Observability Platform establishes a foundation for intelligent AI-RAN network trust by capturing high-fidelity MobiFlow telemetry that extends far beyond standard RAN logging limitations. Operating natively within the system kernel via eBPF, the vendor-agnostic MobiFlow agent extracts real-time, non-invasive protocol telemetry and cross-layer KPIs without requiring modification to the underlying RAN software stack. This fine-grained telemetry stream seamlessly drives AI-driven proactive threat detection and automated network optimization.

The SE-RAN AI Analyzer drives dual-track diagnostic intelligence through two complementary engines: MobiWatch and MobieXpert. MobiWatch utilizes our high-fidelity MobiFlow data stream to isolate complex faults and security incidents via unsupervised deep learning architectures that can detect zero-day anomalies and stealthy attack patterns deviated from normal operations. This pipeline is complemented by MobieXpert, a specialized cellular Expert System that processes real-time telemetry against deterministic protocol rules, delivering high-performance, low-latency detection for advanced runtime faults and cellular threat vectors.

The SE-RAN Agentic AI Operator closes the operational loop by transforming raw security intelligence into autonomous, real-time mitigation. MobiLLM delivers reliable, automated causality analysis that classifies anomalies and identifies root causes. Leveraging this localized context, it automatically formulates and orchestrates optimal course-of-action playbooks, such as RAN parameter tuning and localized policy adjustments. By seamlessly managing response orchestration between the AI platform and network operators, it proactively eliminates manual troubleshooting bottlenecks to securely resolve faults, misconfigurations, and active security incidents.

The Company. Founded in the heart of Silicon Valley by researchers from SRI International and The Ohio State University, SE-RAN.ai is committed to delivering seamless integration of our advanced Edge-to-Core Security Posture Management into legacy and next-generation O-RAN infrastructures, setting a new benchmark for secure, reliable, and cost-effective AI-RAN operations. Our vision is to lead the industry in the next generation of 5G/6G AISecOps services, uniquely capable of identifying and responding to diverse cellular protocol anomalies, sophisticated cellular attacks, and critical device-to-base station faults and misconfigurations.