SimSpace

SOLUTION BRIEF

THE AI PROVING GROUNDS

Cyber Simulation Infrastructure to Preempt the Next Attack

As autonomous adversarial AI accelerates the speed, scale, and sophistication of attacks, security teams can't wait for an attack to strike before building defenses against it. But how can organizations build a defense for an attack they haven't seen?

Security teams need to move from proactive to preemptive AI-powered defense.

The **SimSpace Cyber Simulation Infrastructure** provides a digital replica of an organization's production environment. SimSpace empowers teams to build the environment, simulate active nation-state campaigns, and validate detection simultaneously—before an attack ever hits.

Built on this foundation of preemptive cyber simulation, **the SimSpace AI Proving Grounds** is where next-generation, AI-driven capabilities are built, stress-tested, and hardened. Here, organizations train, test, and operationalize autonomous AI agents alongside human operators against real attack traffic, ensuring human-AI teams can withstand attacks fueled by modern LLMs like Mythos and Daybreak.

AI Proving Grounds: Build, Validate, and Operationalize AI Agents

The SimSpace AI Proving Grounds is a dedicated infrastructure for building, stress-testing, and operationalizing next-generation agentic AI capabilities alongside human analysts.

Build AI Agents

Data science and product engineering teams generate hyper-synthetic, precision-labeled, multi-vector log data from simulated active environments, replacing static datasets to eliminate model drift and fragile logic.

Validate AI Agents

Continuously stress-test internal and third-party AI agents in a zero-risk range against modern zero-day attacks and LLM threat engines like Mythos and Daybreak. Evaluation maps decision accuracy, policy boundaries, collateral damage, and vulnerability to prompt injection, data tampering, and model poisoning.

Operationalize AI Agents & Human Operators

Converge human operators and tactical AI agents into a single, coordinated defensive unit. Teams refine escalation handshakes, optimize automation playbooks, and confirm operational handoffs under live threat conditions.

Testing Security Teams and Tools: Stack Tuning & Interoperability

SimSpace offers a risk-free environment to validate, measure, and optimize an organization's entire security stack—including EDR, SIEM, SOAR, firewalls, OT/cloud controls, and AI security

Automated Security Tool Evaluation

Compare vendors, test side-by-side stack options, and automate tool evaluations under realistic background noise and active threat traffic.

Stack Interoperability & Misconfiguration Testing

Test compatibility, latency, signal prioritization, and policy orchestration across the full security stack to surface misconfigurations before production deployment.

Automated Attack Variation Loops

Run permutations of active nation-state campaigns and living-off-the-land (LoTL) tactics to evaluate detection coverage and accelerate detection engineering.

Training Teams and Individuals: Continuous Human & AI Readiness

SimSpace provides individual and team training across SOC analysts, cyber defense teams, incident response units, and specialized cyber mission forces.

Live-Fire Cyber Exercises

Defenders engage in immersive live-fire exercises inside enterprise-mirrored, high-fidelity network environments.

Role-Based Content & Upskilling

Custom learning paths and skills assessments support onboarding, continuous upskilling, and objective readiness verification.

Human + AI SOC Training

Operators practice monitoring, supervising, and collaborating with autonomous AI agents across simulated SOC workflows.

Benchmark & Rehearse Response

Organizations rehearse complex incident response scenarios and benchmark operational performance to build human intuition alongside machine speed.

Measurable Value

Accelerate Cyber Readiness & Resilience: Prepare teams, tools, and processes to outsmart modern AI-fueled threats before the fight begins.

Optimize Any Tool Against Any Threat: Graduate from static, individual testing to continuous, multi-vector stack and threat validation.

Consolidate Cyber Spend: Rationalize security tools and maximize SecOps ROI without compromising posture.

Ready to Preempt the Future?

Schedule a discovery call with the SimSpace team today.

SimSpace.com