AI Validation Range™

Test AI models. Train AI agents. Secure AI before deployment.

As organizations accelerate the use of autonomous and agentic AI in security operations, most lack a safe, realistic way to evaluate how those systems behave before they influence live production environments.

Cloud Range's AI Validation Range enables organizations to operationalize AI with confidence.

Validate, Train, and Prove AI Readiness

AI Validation Range provides organizations with a safe, realistic way to examine how AI models and agents behave before they affect real systems or decisions. With Cloud Range's controlled, production-safe, virtual cyber range platform, organizations can:

- **Test AI models before deployment** to verify reliability, decision logic, and failure modes
- **Train agentic AI on real systems** across SOC and security workflows, including detection, triage, investigation, and response
- **Red team AI models** to probe hallucinations, unsafe outputs, policy failures, and misuse scenarios
- **Evaluate AI behavior under realistic conditions**, including enterprise infrastructure, security tools, network segments, and IT and OT/ICS environments
- **Assess AI performance under adversarial pressure** using real-world attack simulations, particularly for agentic workflows
- **Test for sensitive data leakage**, including PII and restricted responses
- **Reduce false positives** by validating triage and decision logic
- **Evaluate AI reliability** when signals are incomplete, contradictory, or intentionally deceptive
- **Compare performance across models, agents, and human teams** using the same scenarios and conditions

Together, these insights give organizations clear visibility into how AI behaves before it is trusted with real decisions or actions.

AI Research & Adversary Lab

Find out what your model does under pressure

Agentic AI Training Range

Train agents on real systems — not toy datasets

AI Model Validation Range

Evaluate and prove the model is safe enough to trust

AI Validation Range connects to customer AI models and agents via secure API, allowing organizations to evaluate behavior, decisions, and outcomes in a controlled environment before deployment. Organizations gain clear evidence of where AI accelerates detection and response, where human judgment must remain in the loop, and whether systems are ready to be trusted with real operational responsibility.

Ensure your AI is ready before it influences real systems.

Contact us for more information at info@cloudrangecyber.com.

Operationalize AI with Confidence with AI Validation Range

Once AI systems move beyond pilots, organizations face harder questions than "Does it work?" They need to know how AI behaves in context, how it changes decision-making, and what changes once AI is trusted with real responsibility. They also need to know how it performs alongside people in a high-pressure situation.

AI Validation Range is designed to answer those questions by placing AI into realistic operational conditions and observing outcomes that matter.

HUMAN AND AI PERFORMANCE, SIDE BY SIDE

As AI is integrated into security operations, success depends on more than model performance. Teams need to understand how AI behaves, how to supervise it, and how to secure it.

AI Validation Range enables organizations to train AI agents and human security teams in the **same environments, using the same tools and conditions,** with Cloud Range's library of live-fire attack simulations.

This comparison allows organizations to:

- Measure differences in speed, accuracy, coverage, and decision quality
- Reveal how AI and humans interpret and act on the same signals
- Expose gaps, tradeoffs, and handoff points between automation and human decision-making
- Track performance trends over time using consistent scenarios and metrics

This allows AI to be developed and applied deliberately as a force multiplier to augment detection, triage, and response, while making it clear where human judgment and oversight remain essential.

Why AI Validation Matters

AI changes how security work gets done, but responsibility remains with the organization. By validating AI behavior before deployment, organizations gain clarity on risk, readiness, and reliability, enabling informed decisions about how AI is used in operational workflows.

Contact us to learn more about AI Validation Range and how organizations use it to evaluate AI models, train AI agents, and assess readiness in a controlled environment.

info@cloudrangecyber.com.