CLOUD RANGE

AI Validation Range™ for Security Operations

Train, Test, and Validate AI Before Deployment

Safely validate AI models and agents in realistic enterprise environments to avoid negatively impacting operations.

cloudrangecyber.com

AI Is Moving Into Security Operations Fast

Organizations are rapidly integrating AI into:

- SOC workflows
- Investigation and response
- Enrichment and automation
- Offensive and defensive operations

But most still lack a realistic way to validate how those systems will behave before deployment.

Traditional testing environments often fail to reveal:

- Operational failure modes
- Adversarial weaknesses
- Escalation issues
- Unpredictable behavior under real conditions

Production environments are the wrong place to discover those problems.

Cloud Range's AI Validation Range provides a safe, isolated environment to test, train, and validate AI systems under realistic cyber conditions before deployment.

> "Cloud Range's AI Validation Range literally checked every single box. We needed a full enterprise network with real tools, telemetry data, secure hardware in the loop, and unlimited customizable range time. They delivered it all."
>
> — **CYBER RANGE ENGINEER, MAJOR DEFENSE CONTRACTOR**

What Is AI Validation Range?

Cloud Range's AI Validation Range enables organizations to safely evaluate AI models and agentic AI systems against realistic cyberattacks, enterprise telemetry, and operational workflows.

The platform includes:

- Realistic enterprise infrastructure
- Live-fire attack simulations
- Licensed enterprise security tools
- Customizable environments and complexity levels
- Measurable visibility into AI behavior and performance

Use Real Data

AI Agents must be tested using an organization's unique data. In addition to Cloud Range's AI Validation Range providing a highly realistic enterprise environment equipped with standard security tools, you can also bring your own reality to the range by utilizing the built-in traffic generator and ingesting your custom packet capture (PCAP) files.

By layering your actual network traffic patterns into the simulation, your agent learns to hunt for anomalies against your specific behavioral baseline. This provides highly relevant, customized training data without requiring a time-consuming or costly 1:1 replica of your entire production tool stack. As a result, organizations can confidently ensure their AI is operationally ready to detect and respond to threats within their exact, real-world traffic patterns.

Organizations are using AI Validation Range to safely test, train, and evaluate:

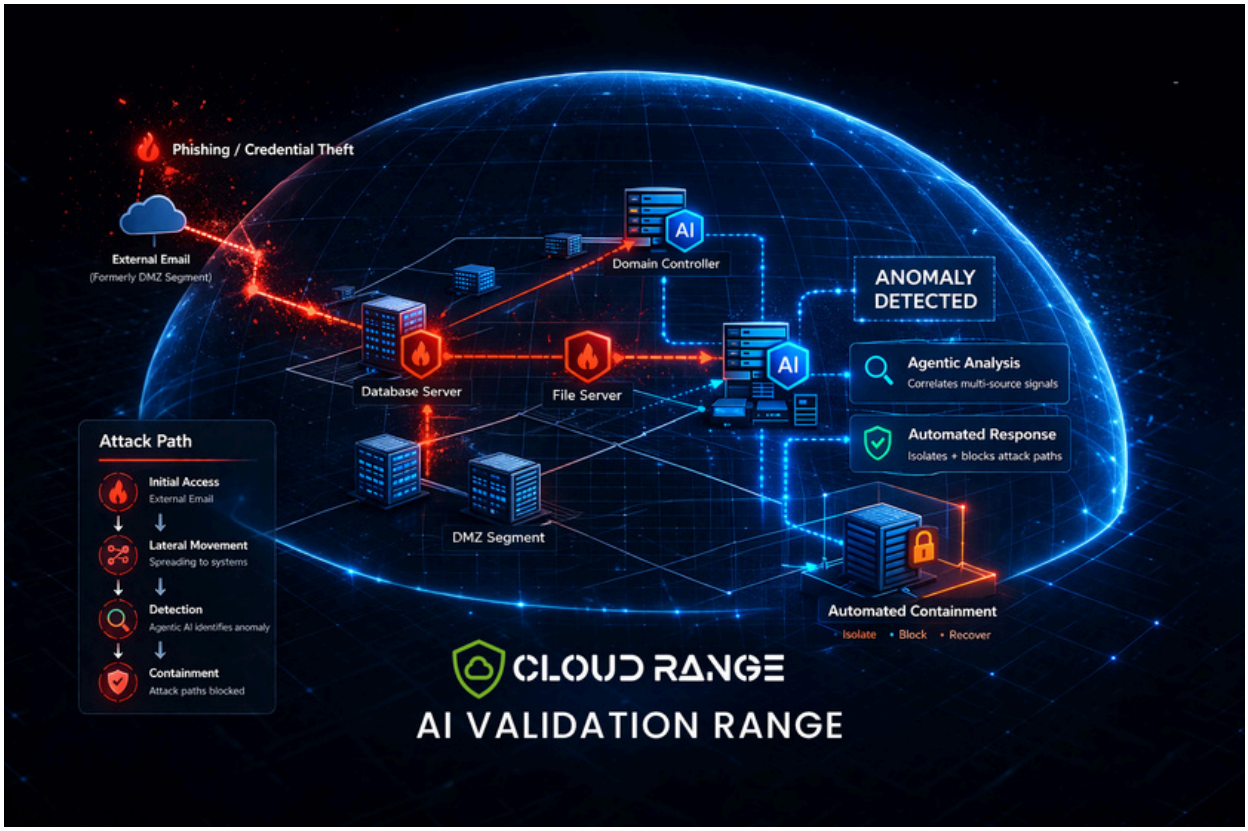
- Alert triage and investigation agents
- AI-assisted SOC workflows
- Response automation and escalation logic
- AI-driven detections and enrichment
- Human vs. AI performance benchmarking
- Offensive security agents and adversarial AI
- Autonomous and semi-autonomous AI behavior
- AI performance under realistic attack conditions
- AI resilience against adversarial manipulation
- Decision-making and operational readiness before deployment

Operational Validation for AI Systems

Organizations are rapidly operationalizing AI across security workflows, from investigation and enrichment to autonomous response and offensive security operations. As AI systems take on greater responsibility, organizations need more than functionality testing or isolated demonstrations. They need realistic validation before deployment.

Cloud Range AI Validation Range enables organizations to validate AI behavior under realistic cyber conditions, benchmark human and AI performance, safely train agentic AI systems, identify operational risks and failure modes, and evaluate adversarial resilience before deployment—all within isolated enterprise environments designed to simulate real operational conditions.

> "Cloud Range provided the realistic simulations and visibility required to measure how well our models identify blue team actions and exploit vulnerabilities."
>
> — **PRODUCT LEADER, GLOBAL FOUNDATION AI LAB**



AI Validation Range in Practice

Pre-Production AI Validation

Organizations are increasingly integrating AI models and agentic AI systems into security operations workflows, often without a realistic way to evaluate how those systems will behave before deployment. Traditional testing environments may validate basic functionality, but they rarely expose how AI responds during active attacks, noisy telemetry conditions, escalation scenarios, or unfamiliar operational inputs.

Using AI Validation Range, **organizations can evaluate AI systems against realistic cyberattacks before deployment.** Observe how AI handles detection, investigation, escalation, response logic, and decision-making within isolated enterprise environments that simulate real operational conditions before those systems are introduced into production workflows.

OUTCOME
Organizations gain greater confidence in operational readiness and can make more informed go/no-go decisions before deploying AI into live security environments.

AI Agent Readiness

As organizations begin integrating agentic AI into SOC operations, many are discovering that task completion alone does not necessarily translate into operational readiness. AI agents may perform well in controlled demonstrations but behave unpredictably when exposed to realistic attack activity, conflicting telemetry, incomplete data, or evolving attack conditions.

AI Validation Range enables organizations to train and evaluate AI agents through realistic attack simulations involving alert triage, investigation, containment, and response under live-fire cyberattack conditions. Observe how agents **prioritize activity, make decisions, and interact with existing workflows** before introducing autonomous capabilities into production environments.

OUTCOME
Organizations can deploy AI agents into security operations with greater confidence in how those systems will behave during real-world security events.

Human vs. AI Performance Benchmarking

Many organizations are still trying to determine where AI meaningfully improves security operations performance and where human oversight remains essential. Without realistic side-by-side evaluation, leaders often lack visibility into how AI compares to experienced analysts during investigations, escalation decisions, or rapidly evolving attack scenarios.

Using AI Validation Range, organizations can **run identical attack scenarios for AI agents and human SOC teams to compare speed, accuracy, coverage, and decision quality under the same operational conditions.** This helps teams identify where AI accelerates workflows, where humans outperform automation, and where collaborative human-AI models may produce the strongest outcomes.

OUTCOME
Organizations gain a clearer understanding of the strengths, limitations, and optimal operational roles for both human analysts and AI systems.

> "Cloud Range's AI Validation Range gave us exactly what we needed to train our agents safely. The customizability, ability to adjust and select specific defense levels, and metrics to track attack success rates resulted in a 10 out of 10 success for our objectives."
>
> — **HEAD OF PRODUCT, LEADING AI RED TEAMING COMPANY**

AI Security Validation & Red Teaming

Organizations deploying AI systems into operational environments need a safe way to aggressively test those systems for vulnerabilities, misuse, manipulation, and adversarial behavior. Conducting this type of testing directly in production environments risks contaminating datasets, influencing model behavior, exposing sensitive information, or introducing operational instability.

AI Validation Range provides isolated environments designed specifically for AI security validation and adversarial testing. Organizations can conduct **red teaming exercises, adversarial prompt testing, vulnerability validation, and behavior analysis** using clean, snapshotted environments with rollback capabilities. This enables teams to safely stress-test AI systems while maintaining data integrity and preserving production stability.

OUTCOME
Organizations can identify weaknesses, validate resilience, and strengthen trust in operational AI systems without introducing unnecessary production risk.

Adversary AI Lab (Offensive Security Agents)

As AI-powered offensive capabilities continue to evolve, security teams need realistic environments where they can safely design, train, and evaluate adversarial AI agents without exposing production systems or creating uncontrolled operational risk. Traditional testing labs often lack the realism, telemetry, and infrastructure complexity required to accurately simulate modern attacker behavior.

AI Validation Range enables organizations to develop and operate offensive security agents within isolated, purposely vulnerable enterprise environments designed to emulate realistic attack paths and operational conditions. Teams can evaluate how adversarial AI agents behave during **reconnaissance, exploitation, lateral movement, persistence, and coordinated attack campaigns**. By training agents to find pivot points and identify clear paths to sensitive data or exfiltration, organizations can observe the exact impact these offensive agents have on defensive systems and workflows.

OUTCOME
Organizations improve defensive readiness, better understand emerging AI-driven attack techniques, and strengthen resilience against increasingly autonomous adversaries.

Managed Security Service Providers (MSSPs)

Managed Security Service Providers are increasingly exploring AI-driven SOC capabilities to improve efficiency, accelerate investigations, and automate repetitive workflows. However, testing AI systems directly against customer environments introduces significant operational and reputational risk, particularly when organizations lack a safe environment to validate behavior under realistic attack conditions.

Using AI Validation Range, MSSPs can **safely evaluate and train AI-driven SOC workflows** involving alert triage, investigation, enrichment, and response automation within isolated enterprise environments that simulate real-world attack activity. They can observe how AI agents behave during active incidents, refine operational logic, and validate effectiveness before deployment into customer-facing environments.

OUTCOME
MSSPs can operationalize AI-driven security capabilities more confidently while reducing risk to customer systems, sensitive data, and production operations.

AI-Enabled Security Vendors

AI-enabled security vendors are rapidly embedding AI models and agentic capabilities into their products to automate threat detection, ransomware defense, and response workflows. However, proving the efficacy, safety, and operational readiness of these AI-powered features to enterprise clients is challenging. Testing in sterile lab environments fails to demonstrate how these products perform under complex, real-world attack conditions or within specific enterprise network baselines.

Using AI Validation Range, cybersecurity vendors gain a highly realistic, isolated enterprise testing environment to **continuously evaluate and validate their own AI-enabled products.** Vendors can ingest custom network traffic baselines (PCAPs), run advanced live-fire attack simulations, and stress-test their tools against evolving threat actor TTPs. This enables vendors to confidently demonstrate their product's capabilities, decision logic, and safety to prospective buyers in a real-world context.

OUTCOME
Security vendors accelerate market adoption and build enterprise trust by providing defensible, empirical proof of their AI-powered product's performance and security readiness.

Validate AI Before Deployment

Request a demo to learn how Cloud Range helps organizations safely test, train, and validate AI systems under realistic cyber conditions before deployment into production operations.

LEARN MORE

cloudrangecyber.com/ai-validation-range

ABOUT CLOUD RANGE

Cloud Range's revolutionary cloud-based cyber range platform helps organizations measurably reduce cyber risk by testing and training both human and AI SOC agents to defend against real attacks. Its simulation platform includes an ever-changing library of realistic, live-fire attacks, IT/OT/IoT/cloud environments, skill development labs, advanced tabletop exercises, reporting, and more. Its AI Validation Range enables organizations to safely test, train, and validate AI models and agents without exposing real data in production environments. Ensure your organization is battle-ready.

CLOUD RANGE

REQUEST A DEMO

Contact Cloud Range at
info@cloudrangecyber.com

cloudrangecyber.com

©2026 Cloud Range | cloudrangecyber.com