Cyber Ranges as the Validation Layer of Cyber Resilience

A CYBER RANGES perspective on Gartner's Hype Cycle for Security Operations, 2026

STAFFORD, VA, UNITED STATES, June 18, 2026 /EINPresswire.com/ -- Gartner's 2026 security operations research is useful to CYBER RANGES as a vendor not because it offers a recognition to display, but because it captures a larger market correction. Security operations are being pushed away from static assurance and towards continuous validation. In that frame, cyber ranges belong in the same conversation as CTEM, adversarial exposure validation, RTaaS and PTaaS: not as a training theatre, but as the environment where exposure data, controls, playbooks and human decisions are tested together.

The signal in the Gartner paper

The relevant point in Gartner's Hype Cycle for Security Operations, 2026 is not simply that Cyber Range appears as a category, or that CYBER RANGES is listed among the Sample Vendors. The more important point is the architecture of Gartner's argument. Security operations is being described as a market undergoing structural correction: traditional reactive models are under pressure, CTEM is moving from concept to operating priority, and security leaders are being pushed to separate operational reality from vendor noise.

That is where CYBER RANGES' vendor role becomes clear. The paper places cyber ranges near a set of adjacent movements - continuous threat exposure management, adversarial exposure validation, red teaming-as-a-service, penetration-testing-as-a-service, incident response management and AI-assisted SecOps. These are not random categories. They all express the same customer frustration: security teams have more information than ever, but they still struggle to prove what will actually happen when a real attack path meets their environment, controls, processes and people.
For years, many organizations bought security in fragments. A scanner here, a SIEM there, an

EDR platform, a tabletop exercise, a red team, a report, a course, a playbook. The fragments were not useless; they were necessary. But Gartner's analysis reflects something that practitioners already feel: the value now comes from connecting those fragments into measurable operational outcomes. Cyber ranges become strategically relevant when they provide the place where that connection is tested.

The training label is now too small

The most common mistake in cyber range positioning is to begin with training. Training is a real use case, but it is too narrow to carry the category now. Once a cyber range is presented as a training product, the buying discussion collapses into seats, courses, content libraries, certifications and learner throughput. Those metrics may matter to a learning department. They do not describe the problem that Gartner is highlighting.

The serious buyer is asking something harder: can we validate that our SOC, incident response process, crisis structure, detection content, recovery assumptions and technical controls will perform against the attack paths we are worried about? Such a question cannot be answered by classroom learning, a static lab or an annual tabletop exercise. It requires a realistic execution environment where the technical sequence of an attack and the organizational response can be observed together.

This changes the category from capability development to capability proof. It also changes the buyer. The conversation moves from learning and awareness budgets to CISOs, SOC leaders, incident response leads, cyber defence & resilience teams and, in critical infrastructure, operational and safety stakeholders. They are not buying generic learning anymore, but instead reduced uncertainty.

Where CYBER RANGES fits

CYBER RANGES sits in the part of the Gartner narrative where validation becomes operational. Exposure management identifies and contextualizes what actually matters. AEV tests which paths are executable. RTaaS brings continuous adversarial pressure. PTaaS improves the cadence and workflow of testing. The cyber range is where all of this can be translated into a controlled, observable, measurable exercise of people, process, technology and decision-making.

The value is therefore not simply that CYBER RANGES can replicate networks, identities and traffic (as digital twins or cousins) although such technical capability is essential. The more strategic point is that CYBER RANGES turns threat-led assumptions into operational evidence. It can show whether detections fire, whether analysts understand the context, whether escalation thresholds are clear, whether playbooks are usable, whether containment decisions are owned, whether crisis teams receive the right information, and whether recovery assumptions survive contact with reality.

This is especially important because many security failures are no longer caused by a single missing tool. They occur in the seams between tools, teams and decisions. A realistic cyber-physical range exercise can expose that a ransomware playbook depends on an identity team that is not in the escalation chain, that legal notification assumptions do not match the technical evidence available in the first hours, or that an OT containment action proposed by the SOC is unacceptable to plant operations. These are not training gaps in the traditional sense. They are validation gaps.

AI, IT/OT and cloud delivery make the case stronger

Gartner's cyber range drivers are useful because they move the conversation beyond generic skills development. Ransomware, AI-driven attacks, cloud adoption, IT/OT convergence, skills pressure and the need to progress beyond tabletop maturity all point in the same direction. Organizations need safe environments to test what they cannot responsibly test in production.

AI strengthens the argument rather than weakening it. AI assistants, autonomous claims and agentic security workflows need disciplined validation before they are trusted in live operations. A generated detection may look plausible and still fail against realistic telemetry. An AI-supported investigation may accelerate triage and still create false confidence. The range gives teams a safe place to evaluate these behaviours without confusing a demo with operational proof.

The same is true for IT/OT convergence. In critical infrastructure and industrial environments, the relevant question is not only whether an attack can be detected, but whether the response is compatible with safety, production continuity and engineering constraints. A cyber-physical range gives IT, security and operations teams a shared environment to work through those trade-offs before the incident makes them urgent.

What serious buyers should now ask

As more vendors attach themselves to the validation story, CYBER RANGES approaches this market by helping buyers ask better questions. The market does not need another generic claim about simulation. It needs a clearer distinction between training throughput and resilience evidence.

Technical realism:

- Can the environment represent our estate, integrate with our tools and support current threat-led scenarios?
- Number of labs or courses

Operational validation:

- Can it test detection, triage, escalation, playbooks and cross-team decisions end to end?
- Completion rates or learner satisfaction

Resilience economics

- Can it produce evidence that improves prioritisation, readiness and recovery decisions?
- Cost per learner or certification count

Content relevance

- Are scenarios refreshed from current threat intelligence and mapped to the attack paths we actually care about?
- Size of the content catalogue

The short version: if a buyer measures a cyber range like an LMS, they are probably buying it for the wrong reason.

“Most organizations do not have a training problem. They have a proof problem. They cannot yet demonstrate, with enough precision, that their controls, teams and incident structures will perform under real attack pressure.”

Conclusion: proof has become the product

The useful way to read Gartner's recognition is not as an award and not as a discovery moment. It is external confirmation that the market is moving towards a problem CYBER RANGES was built to address: proving cyber-physical capability under very realistic conditions.

The discussion should not start with category education or platform mechanics. Mature buyers are already surrounded by tooling, pressured by AI-driven threat acceleration, expected to show measurable resilience and increasingly unconvinced by periodic assessment alone. They do not need another platform story. They need a way to prove that their security programme works when the scenario becomes operational.

That is the point we believe highly matters now: cyber ranges should no longer be bought as training platforms and then expected to deliver resilience outcomes. They are becoming the validation layer of cyber resilience, i.e. the place where CTEM decisions, controls, SOC operations, incident response and crisis assumptions are tested before an adversary tests them instead.

Source notes

1. Gartner source and article framing. This article draws exclusively on Gartner, Hype Cycle for

Security Operations, 2026, 5 June 2026, ID G00846365, by Darren Livingstone and Jonathan Nunez. The framing relies on Gartner's description of a market shifting from reactive models towards proactive, continuous validation; the increasing priority of CTEM; the need to separate hype from operational reality; and the requirement for measurable, objective-aligned resilience.
2. CTEM, exposure management and validation. The article's positioning of cyber ranges as part of the validation layer in resilience and CTEM programmes is grounded in Gartner's discussion of threat exposure management moving beyond point-in-time discovery towards continuous, threat-led validation, and in the report's treatment of AEV, RTaaS and PTaaS as related validation-oriented capabilities.
3. Cyber Range category and CYBER RANGES. The article refers to Gartner's Cyber Range entry, including its definition of cyber ranges as technology-enabled virtual simulation environments that replicate IT/OT networks, systems, identities and traffic, support live-fire training, skills assessment, technology testing and incident response playbook validation, and identify CYBER RANGES among sample vendors.
4. Customer outcomes and buyer criteria. The buyer criteria reflect Gartner's cyber range business impact and recommendations, including risk reduction, operational resilience, content freshness, SaaS/cloud delivery, use-case alignment and integration with existing operational security tooling such as SIEM and EDR.
5. Use of Gartner name. Gartner is a registered trademark of Gartner, Inc. and/or its affiliates. This article is an independent CYBER RANGES market commentary based on the cited Gartner research. Gartner does not endorse any vendor, product or service depicted in its research publications.

Anthony Munns
CYBER RANGES LTD
+357 99 211223
email us here
