Range42: An Open, Automated, and Extensible Architecture for Next-Generation Cyber Ranges

Abstract

Cybersecurity training infrastructures struggle to keep pace with rapidly evolving threat landscapes, creating a critical skills gap that undermines organizational and national security postures. Traditional cyber ranges compound this problem through vendor lock-in, closed scenario repositories, and manual deployment processes that prevent scalable, collaborative defense preparation. This paper presents Range42 [1], an open cyber range platform developed by the NC3 [2] (National Cybersecurity Competence Center) under the LHC [3] (Luxembourg House of Cybersecurity) together with DIGISQUAD [4], designed to democratize access to realistic, reproducible training environments through automation and community collaboration.

This paper introduces three core contributions addressing fundamental limitations in current cyber range architectures. First, an extensible catalog of over 100 curated CVEs and misconfigurations (20 currently deployable) enabling structured reproduction of real-world attack surfaces for controlled experiments. Second, an orchestration framework deploying multi-subnet enterprise-grade networks with isolation and fidelity, eliminating manual configuration barriers. Third, a dual-layer scenario description standard (human-readable narrative + machine-ingestible JSON schema) supporting both manual authoring and LLM-assisted generation. Building on existing standards including MISP's Common EXercise Format [5], Open Cyber Range SDL [6] (Scenario Description Language), and Automating the Generation of Cyber Range Virtual Scenarios with VSDL [7], development of a proof-of-concept workflow:

prompt → validated scenario → automated deployment, enabling rapid adaptation to emerging threats.

The platform's backend achieves full operational capability in "shooting range" mode with Proxmox [8], Ansible [9], and Tailscale-based [10] connectivity, while graphical interfaces remain under development. By establishing open, standardized catalog architectures, Range42 enables shared scenario ecosystems that accelerate collective defense capabilities across organizations and nations. This approach addresses the urgent need for scalable, interoperable training infrastructures that can anticipate tomorrow's threats rather than merely replicate yesterday's incidents.

1 Introduction

Cyber threats evolve faster than training and evaluation methodologies. To secure tomorrow, cyber ranges must enable realistic, reproducible, and rapidly composed environments that reflect emerging attack surfaces and defensive strategies. Traditional cyber ranges face three critical limitations: proprietary platforms create vendor lock-in, closed scenario repositories prevent collaborative development, and manual deployment processes hinder scalability. Range42 addresses these challenges through open architecture, community-driven content catalogs, and infrastructure-as-code automation.

Range42 is an open cyber range platform emphasizing automation, flexibility, and collaboration. Our contributions are: (1) an extensible catalog of vulnerable and misconfigured systems for research-grade reproducibility; (2) an orchestration framework for deploying multi-subnet infrastructures approximating enterprise topologies; and (3) a standardized scenario description framework that blends human readability and machine ingestion, enabling consistent narrative and technical deployment definitions. The project outlines the automation pipeline and report lessons for scalability, isolation, and openness.

Exploring an experimental LLM-assisted pipeline to generate scenarios from prompts, enabling rapid scenario creation that remains current with the evolving threat landscape. Playing hundreds of generated scenarios to extract telemetry might provide valuable datasets for security analytics research, especially when paired with real-world incident data and digital twins of documented breaches.

2   Related Work

Cyber range platforms. Several academic and commercial cyber ranges address cybersecurity training needs but face limitations in openness and interoperability. KYPO Cyber Range [11] demonstrates scalable approaches using OpenStack and sandbox orchestration for hands-on cybersecurity education, achieving impressive deployment efficiency through containerization and automation. However, KYPO relies on platform-specific tooling for scenario management and lacks standardized interfaces for cross-platform scenario exchange. Commercial platforms like SimSpace [12], Immersive Labs [13], RangeForce [14], and Cyberbit [15] offer rich features including realistic enterprise environments and automated assessment, but impose vendor lock-in, lack transparent architectures, and prevent community contribution to scenario catalogs. Open-source efforts exist but often remain tightly coupled to specific infrastructure choices, limiting portability and collaborative development.

Scenario description languages. The Open Cyber Range SDL provides a YAML-based specification for defining training scenarios with infrastructure components, network topologies, and service configurations. While SDL enables declarative scenario definitions, it focuses primarily on technical infrastructure without integrated narrative layers, learning objective frameworks, or mechanisms for LLM-assisted generation. MISP's Common EXercise Format (CEXF) enables exercise information sharing across organizations through structured metadata, event timelines, and inject specifications. CEXF excels at exercise documentation and inter-organizational coordination but does not include deployment automation, orchestration primitives, or runtime scenario execution capabilities. Other domain-specific languages exist for specific platforms but lack standardization efforts enabling cross-platform compatibility. Range42 builds on these efforts by combining human-readable narratives with machine-executable schemas in a unified framework, supporting both manual authoring and automated generation while maintaining deployment platform flexibility.

Automation and orchestration. Infrastructure-as-Code (IaC) approaches using Ansible, Terraform, and Kubernetes have been successfully applied to cyber range deployment [11], enabling reproducible infrastructure provisioning and configuration management. However, existing solutions often couple scenarios tightly to specific platforms, making cross-platform scenario portability difficult. Containerization technologies like Docker [16] provide lightweight virtualization for rapid deployment but require careful orchestration for complex multi-subnet scenarios. Range42's catalog-driven architecture with extension APIs enables platform-agnostic scenario definitions while maintaining deployment flexibility through abstraction layers that map high-level scenario specifications to platform-specific orchestration logic.

LLM-assisted security training. Recent work explores using large language models for generating cybersecurity training content, automated vulnerability detection, and threat scenario synthesis. While LLMs demonstrate impressive capabilities in understanding security concepts and generating plausible training materials, concerns around hallucination, inappropriate content generation, and security risks remain significant barriers to production deployment. Range42 addresses these challenges through mandatory validation pipelines that verify technical correctness, dependency consistency, and security constraints before any LLM-generated content reaches production deployment. Human-in-the-loop approval ensures subject matter expert review, while constraint enforcement prevents generation of harmful or inappropriate scenarios. This approach balances the efficiency gains of LLM assistance with the safety requirements of operational training platforms.

Open-source community models. The MISP project [18] demonstrates successful community-driven development of cybersecurity tooling through open standards, transparent governance, and collaborative innovation. MISP's threat intelligence sharing platform achieved widespread adoption by prioritizing interoperability, providing clear contribution pathways, and fostering an inclusive community culture. Range42 adopts similar principles, aiming to build a federated ecosystem of cyber training platforms through standardized scenario formats, open catalog architectures, and community-driven content development.

3 System Architecture & Catalog Design

Range42 operates via Proxmox, Ansible, and container/VM integration. The range42-catalog is structured as a modular repository of scenario components (e.g. vulnerable hosts, network topologies, inject modules), each described with metadata (e.g. prerequisites, dependencies, scoring hooks). The project maintains extension APIs so external tools can list, validate, augment, or contribute entries. The catalog integrates seamlessly with Ansible roles to map component definitions to deployment logic.

4 Vulnerability and Misconfiguration Catalog

Curated catalog of ∼100 CVEs/misconfigurations (with ∼20 currently deployable), using build descriptors and snapshotting to balance reproducibility with support for proprietary or atypical systems. The design supports traceability, variant creation, and controlled risk exposure during exercises.

5 Scenario Description Standard

Standardized scenarios with a dual representation: (i) a human-readable layer (narrative, learning objectives, context, and both technical and non-technical injects); and (ii) a machine-ingestible schema (JSON) that encodes actors, assets, networks, triggers, dependencies, and scoring. A bidirectional mapping preserves consistency between the narrative and the structured specification.

For validation a human-readable scenario is drafted and compiled into the machine schema. Automated validators check syntax, dependency closure, resource bounds, and security constraints prior to ingestion. Rejected builds include actionable diagnostics; accepted builds become catalog entries with semantic versioning.

The standard is designed to leverage LLMs to propose both the human narrative and the machine schema from a prompt (e.g., "simulate a ransomware intrusion across three subnets"). Outputs are never trusted blindly: they pass through the same validation pipeline and require
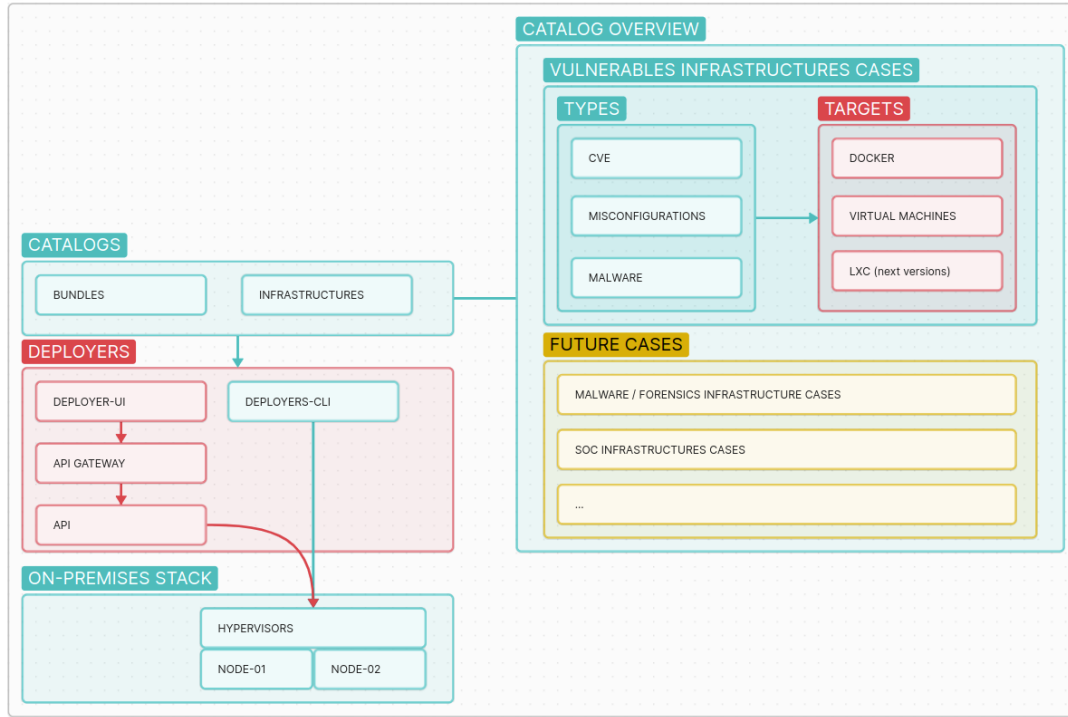
Figure 1: High-level Range42 catalog architecture.

human approval before catalog admission and deployment. Definition of a domain-specific schema (YAML / JSON hybrid tbd.) for scenario narratives. A scenario file includes sections like: background story, objectives, inject schedule, scoring rules, triggers, technical blueprint. From this human-readable form, generates canonical machine-readable JSON which Range42 ingests to deploy and run the scenario. To be included is a validation logic to catch schema errors or dependency mismatches.

6   Integration & Deployment Pipeline

From catalog + scenario schema to live lab: description of the orchestration path (Ansible playbooks, Proxmox API calls, network wiring, Tailscale connectivity). Discussions on how catalog metadata guides resource allocation, dependency resolution, and runtime coordination of injects and events.

7   LLM-Assisted Scenario Generation

Provided a proof-of-concept workflow: given a prompt (e.g., "simulate a ransomware attack in 3-subnet corporate network"), an LLM produces a draft narrative + schema. This will feed into the validation logic, correct or flag inconsistencies, then ingest it into the catalog for deployment. Preliminary results and failure modes are discussed.

8 Evaluation

Current deployment status. Range42 has achieved full operational capability in "shooting range" mode, where the complete backend infrastructure is production-ready and actively deployed. The vulnerability catalog currently encompasses approximately 100 identified CVEs and misconfigurations spanning common enterprise technologies, with approximately 20 scenarios available for immediate deployment. The backend automation stack is fully functional, providing end-to-end orchestration from infrastructure provisioning through security monitoring. A graphical user interface for scenario authoring and exercise management is currently under development to complement the operational backend.

The platform features fully automated provisioning on Proxmox infrastructure, including network segmentation, VPN connectivity via Tailscale, and firewall rule deployment. Integrated monitoring through Wazuh provides real-time telemetry collection and alerting capabilities for exercise observation and assessment. The system architecture is distributed across 14 repositories managing Ansible automation playbooks, scenario content, and supporting tooling. In shooting range mode, operators interact with the platform through command-line interfaces and declarative configuration files, enabling rapid scenario deployment for training exercises and research experiments.

Automation maturity. Core automation metrics from internal work packages indicate: hypervisor automation $\sim$80%, network topology automation $\sim$70%, and baseline catalog initialization $\sim$25%. The hypervisor and network automation components represent production-grade capabilities currently in active use, while catalog content development remains an area of ongoing expansion. The term "shooting range" reflects the platform's current operational mode: the backend orchestration, deployment, and monitoring pipelines are fully implemented and battle-tested, whereas user-facing interfaces for non-technical operators are planned enhancements.

Metrics. Report (i) ingestion success rate (schema validation pass/fail), (ii) deployment latency for typical lab topologies (VM- and container-based), and (iii) reproducibility across repeated runs. Where infrastructure constraints limit scale tests, complement with instructor/operator feedback and failure-mode analyses (e.g., image sprawl, secret handling, routing edge cases). Measure catalog ingestion success rate, scenario consistency (i.e. narrative vs deployed topology), deployment latency, and reusability across runs. Where full metrics are limited, include qualitative feedback from instructors and early users.

9 Discussion

Governance and federation: A community catalog requires contribution guidelines, schema versioning strategy, and automated QA (linting, policy checks). Ideal vision is cross-institution catalog federation where trusted peers exchange signed scenario components, enabling shared curricula and comparable experiments. (Exchange protocol needs to be decided.)

Standardization impact: A widely adopted scenario standard lowers authoring friction, enables portable exercises, and allows third-party tools (including LLM-driven assistants) to integrate safely.

Synergies with NGSOTI: The authors identified strong architectural and conceptual overlap with the Next Generation Security Operator Training Infrastructure (NGSOTI) project [17], which focuses on modular, open architectures for distributed cyber range operations. Range42 aims to cooperate with NGSOTI and re-use compatible components where feasible — particularly around orchestration pipelines, scenario interoperability, and federated data exchange. This alignment ensures that both projects contribute toward a shared European ecosystem of interoperable, open, and extensible cyber training infrastructures.

Table 1: Range42 Implementation Status and Maturity

Component	Status
Catalog & Content	
CVEs & Misconfigurations Cataloged	~100
Deployable Scenarios	~20
Backend Infrastructure (Production)	
Hypervisor Automation	80%
Network Topology Automation	70%
Orchestration Repositories	14
Backend Status	Fully Operational
User Interfaces	
CLI/API	Operational
Web GUI	In Development
Integration & Monitoring	
Wazuh Telemetry	Integrated
Tailscale VPN	Integrated
Catalog Initialization	25%

Reflections on expressivity vs. enforceable constraints, schema versioning, contribution governance, catalog federation across platforms, and operational challenges (e.g. schema drift, extension conflicts).

10 Future Work

Catalog: Expand the catalog with richer scenarios (forensics, social engineering, insider threats), build GUI editors for the standard format, integrate stronger LLM-based validation and correction, and establish federated catalogs across multiple range platforms with shared schemas. Advancing a visual lab designer; integrating malware analysis/forensics workflows; and supporting richer hybrid topologies.

Visual lab designer: While Range42's backend orchestration is fully operational in shooting range mode with command-line and API interfaces, the platform requires graphical tools to serve non-technical instructors and students. The visual lab designer will provide drag-and-drop topology composition, allowing users to construct multi-subnet networks, place vulnerable hosts, configure network segmentation, and define inject schedules through an intuitive interface. This component is currently under active development as the Exercise Management Platform (EMP) with mockups completed and frontend implementation in progress.

Exercise management interface: The EMP will extend beyond scenario authoring to provide real-time exercise orchestration, participant monitoring, and automated scoring. Instructors will track student progress, trigger dynamic injects, adjust scenario difficulty, and analyze performance metrics through unified dashboards. Integration with the scenario description standard will enable seamless transitions from design to deployment to assessment.

11 Conclusion

By combining an open catalog architecture with a standardized, dual-mode scenario description and LLM-assisted generation, Range42 demonstrates that next-generation cyber ranges must function

as ecosystems rather than isolated platforms. Following MISP's [18] successful model of community building, open standards, and collaborative innovation, Range42 establishes technical and organizational foundations for federated cyber training infrastructure.

The platform's three core contributions—extensible vulnerability catalogs, automated multi-subnet orchestration, and dual-layer scenario standards—address fundamental barriers that have prevented cyber range democratization: vendor lock-in, manual deployment overhead, and closed scenario repositories. With backend automation fully operational in shooting range mode and graphical interfaces under development, Range42 proves that research-grade reproducibility and operational accessibility need not be mutually exclusive.

The urgent cybersecurity skills gap demands training infrastructures that scale through collaboration rather than replication. Range42's open architecture enables organizations to contribute scenarios, share attack surface definitions, and collectively maintain current threat representations without rebuilding infrastructure from scratch. As cyber threats evolve daily, training platforms must anticipate emerging attack patterns through rapid scenario generation and community-driven content evolution.

Future cyber defense readiness depends on interoperable training ecosystems where scenarios, telemetry formats, and assessment frameworks cross organizational boundaries. Range42 provides both working implementation and open standards to catalyze this transition. The platform's LLM-assisted scenario generation and automated telemetry collection further enable research at scales previously impossible, generating datasets for advancing detection algorithms and defensive technologies.

Organizations seeking realistic, reproducible cyber training environments can deploy Range42 today, while researchers gain a platform for studying training effectiveness and scenario optimization at scale. By securing tomorrow's defenders through collaborative, automated, and continuously evolving training infrastructures, Range42 addresses not just technical challenges but the strategic imperative of collective defense capability development.

The authors believe this approach will help catalyze collaborative, scalable, and future-ready cyber range research and training. Automated ranges like Range42 help secure tomorrow by enabling hands-on research and training humans as well as generating data for model generation at scale.

References

[1] Range42 Cyber Range Platform: https://www.range42.lu/

[2] National Cybersecurity Competence Center Luxembourg: https://www.nc3.lu/

[3] Luxembourg House of Cybersecurity: https://www.lhc.lu/

[4] DIGISQUAD: https://www.digisquad.com/

[5] MISP Common EXercise Format: https://github.com/MISP/cexf

[6] Open Cyber Range SDL: https://documentation.opencyberrange.ee/docs/sdl/reference/

[7] G. Costa, E. Russo, and A. Armando, "Automating the Generation of Cyber Range Virtual Scenarios with VSDL," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 13, no. 1, pp. 33–52, Mar. 2022, doi: 10.22667/JOWUA.2022.03.31.0033.

[8] Proxmox VE. Available: https://www.proxmox.com/

[9] Ansible Documentation. Available: https://docs.ansible.com/

[10] Tailscale Documentation. Available: https://tailscale.com/kb/

[11] J. Vykopal, P. Čeleda, P. Seda, V. Švábenský, and D. Tovarňák, "Scalable Learning Environments for Teaching Cybersecurity Hands-on," in 2021 IEEE Frontiers in Education Conference (FIE), Lincoln, NE, USA, 2021, pp. 1–9, doi: 10.1109/FIE49875.2021.9637180.

[12] SimSpace, "Tailored Cyber Range Solutions," 2025. [Online]. Available: https://simspace.com/platform/

[13] Immersive Labs, "Immersive One Platform," 2025. [Online]. Available: https://www.immersivelabs.com/products/platform

[14] RangeForce, "Cloud-Based Cyber Range Platform," 2025. [Online]. Available: https://www.rangeforce.com/

[15] Cyberbit, "Cyber Range Platform," 2025. [Online]. Available: https://www.cyberbit.com/

[16] Docker Documentation. Available: https://docs.docker.com/

[17] D4 Project, "NGSOTI Architecture Overview: Next Generation Security Operator Training Infrastructure," 2025. [Online]. Available: https://d4-project.org/2025/06/19/NGSOTI-Architecture-Overview.html

[18] MISP Project, "MISP Threat Intelligence Sharing Platform," 2024. [Online]. Available: https://www.misp-project.org/

Use of AI tools and human oversight