Range42 Status Update

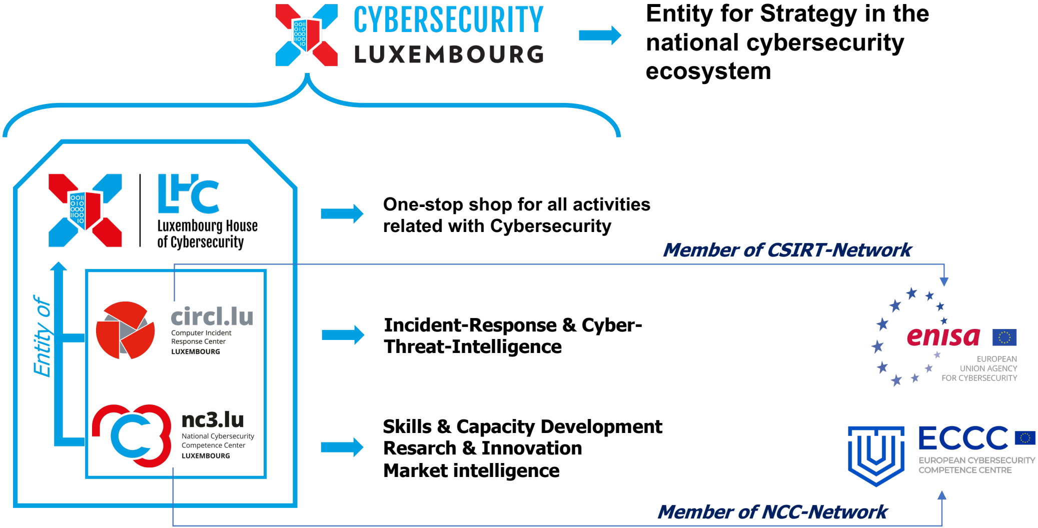
Open Cyber Range Platform for Collaborative Security Training

NC3 / Range42 Team

September 30, 2025

Proxmox Ansible Orchestration Telemetry

TLP:CLEAR – Information may be shared freely without restriction.



CYBERSECURITY LUXEMBOURG

Entity for Strategy in the national cybersecurity ecosystem

LHC Luxembourg House of Cybersecurity

One-stop shop for all activities related with Cybersecurity

Entity of

circl.lu Computer Incident Response Center LUXEMBOURG

Incident-Response & Cyber-Threat-Intelligence

nc3.lu National Cybersecurity Competence Center LUXEMBOURG

Skills & Capacity Development
Resrach & Innovation
Market intelligence

Member of CSIRT-Network

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Member of NCC-Network

Skills development

Capacity strengthening

Research & innovation

Ecosystem & industrialization

NCC coordination

ABOUT US

The mission of NC3 is to support the Luxembourg ecosystem in the development of skills and capacities in cybersecurity, thereby contributing to the development of an industrial base in cybersecurity and strengthening the strategic autonomy of the European Union.

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

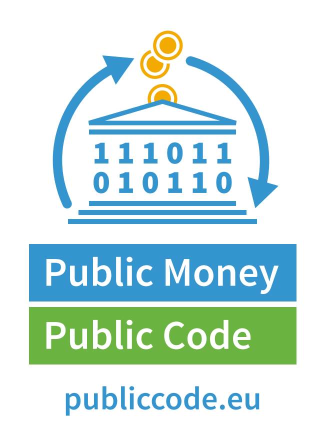
Public money, public code. Let’s go all the way, shall we?

Current Team

- Core development team of 3 contributors
- Mix of InfoSec & DevOps engineers
- Collab model with NC3 & ecosystem partners

Current Funding

- Public grant for cyber training infrastructure
- Open-source model: no licensing fees, transparent development
- Investment in reusable, community-driven tooling



Public money, public code. Let’s go all the way, shall we?

Why We Need Your Help

- Expanding scenario coverage requires diverse security expertise
- UI/UX design needs user-focused contributors
- Infrastructure automation benefits from community patterns

Join Us

- Open development: all code, docs, and issues public
- Welcoming to first-time contributors
- Apply to join the team →

Agenda

1. What Range42 is & why it matters
2. Current achievements & capabilities
3. Architecture overview
4. Development tracks: where we're heading
5. How to contribute: scenarios, automation, UI/UX
6. Lessons learned & open challenges

What is Range42?

- **Open cyber range platform** for offensive, defensive, and hybrid training
- **Reproducible Infrastructure-as-Code**: Proxmox, Ansible, Docker
- **Flexible & extensible**: supports CVE labs, misconfigurations, future malware/forensics scenarios

> ℹ Built to simulate *real-world incidents* safely, with isolation, snapshots, and telemetry.

Current Achievements ✓

What’s Working Today

- 100 CVEs & misconfigurations identified across common technologies
- 20 scenarios currently deployable for hands-on training
- **Automated provisioning** on Proxmox with networking, VPN, firewalling
- **Integrated monitoring** via Wazuh for telemetry and alerting
- **13 repositories** managing automation, content, and tooling

💡 **Key Milestone:** Platform is functional and actively used for internal training exercises.

Range42 vs. Other Cyber Ranges

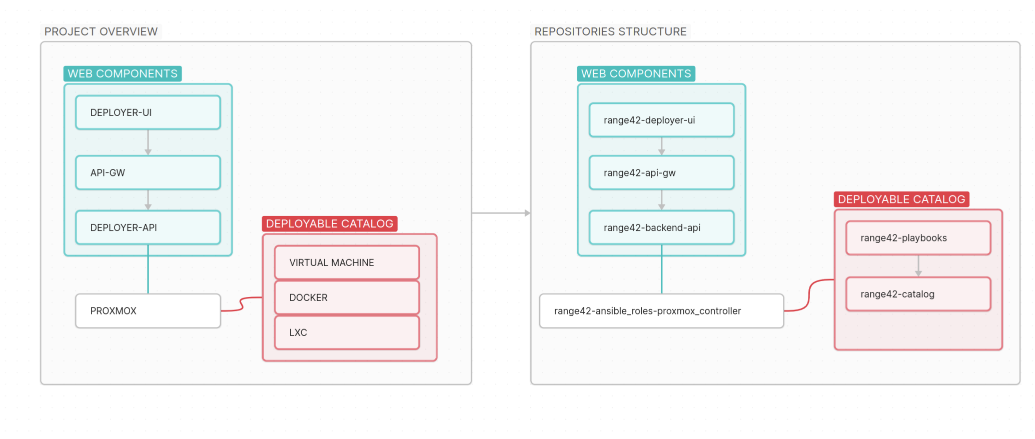
Feature	Range42	Commercial SaaS	Cloud Native	Traditional
Open Architecture	✓	×	×	×
IaC/GitOps	✓	~	✓	×
Private Deployment	✓	×	~	✓
Cost Control	✓	×	~	✓
Full Data Custody	✓	×	×	✓
API Orchestration	✓	✓	✓	×
Rapid Reset/Snapshots	✓	✓	~	~
Custom Scenarios	✓	×	~	✓

💡 **Range42's Edge:** Full control, reproducibility, and cost-effectiveness without vendor lock-in.

Architecture at a Glance

- **Hypervisor layer**: Proxmox VMs/LXCs; snapshots; network segments
- **Automation layer**: Ansible roles orchestrate lifecycle, network, firewall, images
- **Control plane**: Backend API (routes for VM/Net/Runner); Kong gateway
- **UX**: Deployer UI (visual designer), EMP mockup (exercise management)
- **Observability**: Wazuh for logs/alerts; structured telemetry

Architecture: Logical Components → Repository Mapping



Left: Logical architecture flow. **Right:** Actual GitHub repository structure.

Development Tracks

Where We're Heading: Three Development Tracks

1. **Expand Vulnerability & Misconfiguration Inventory**
   - Goal: Increase from 20 to 50+ deployable scenarios
   - Cover diverse technologies: web, network, cloud, containers
   - Community contributions welcome for CVE research and deployment automation
2. **Advance Lab Designer from PoC to Production**
   - Visual node-based infrastructure designer (VueFlow)
   - Instructor-friendly: drag-and-drop scenario composition
   - Export to Ansible playbooks for deployment
3. **Multi-Subnet Infrastructure Support**
   - Simulate complex enterprise networks (DMZ, internal, management zones)
   - Advanced firewall rules and traffic segmentation
   - Support for red team / blue team exercises

Key Repositories

Organization Overview

13 Repositories Analyzed (2 public, 11 private)

Current State

- Strong security baseline: Zero high-severity findings across all code scans
- Governance standardization in progress: LICENSE, SECURITY, CI/CD, contributor docs
- Active development: 179 commits (devkit), 125 (backend), 108 (proxmox controller)

Contribution Opportunities: Help us complete governance files, add CI pipelines, and expand scenario coverage.

range42-ansible_roles-proxmox_controller

Status: Active **Commits:** 108 **Lang:** Ansible/YAML

Purpose: Core automation for managing Proxmox nodes via API: VMs, LXC containers, networking, storage, firewall, and snapshots.

Contribution Opportunities

- Add CI pipeline with ansible-lint and Molecule idempotence tests
- Document role variables and provide example playbooks
- Extend functionality for advanced networking scenarios

range42-backend-api

Status: Active **Commits:** 125 **Lang:** Python/FastAPI

Purpose: FastAPI backend orchestrating Proxmox deployments via Ansible, with routes for VM control, networking, and bundle execution.

Contribution Opportunities

- Add unit tests and integration tests with pytest
- Improve error handling and validation

TLP:CLEAR – Information may be shared freely without restriction.

range42-deployer-ui

Status: Prototype **Commits:** 28 **Lang:** Vue/TypeScript

Purpose: VueFlow-based visual orchestrator for designing, validating, and deploying Range42 infrastructure through node-based interface.

Contribution Opportunities

- UI/UX improvements for instructor workflows
- Integration testing with backend API
- Export/import hardening for scenario sharing

range42-playbooks & range42-catalog

Status: Active **Commits:** 75 + 91 **Lang:** Ansible/YAML

Purpose: Centralized orchestration playbooks and reusable content catalog for deploying vulnerable scenarios and infrastructure bundles.

Contribution Opportunities

- Add new CVE scenarios: research, document, automate deployment
- Introduce scenario taxonomy and tagging system
- Document compatibility matrices and dependencies

How to Contribute

How to Contribute

Three Primary Contribution Paths

Scenario Design

- CVE research
- Misconfig labs
- Documentation

Infrastructure Automation

- Ansible roles/playbooks
- Backend API features
- CI/CD pipelines

UI/UX Design

- Lab designer
- Exercise mgmt
- User workflows

Get Started: Visit `github.com/range42` (public repos) or contact us for private repo access.

TLP:CLEAR – Information may be shared freely without restriction.

Getting Started: Choose & Setup

Step 1: Choose Your Path

- Browse open issues on GitHub (labeled ”good first issue” and ”help wanted”)
- Review scenario inventory to find gaps in coverage
- Check documentation for areas needing clarity

Step 2: Set Up Your Environment

- Fork repositories and clone locally
- Follow setup guides in README files
- Join our communication channels (contact us for access)

Getting Started: Contribute & Engage

Step 3: Submit Your Contribution

- Create pull request with clear description
- Ensure tests pass (where CI exists)
- Engage with code review feedback

What to Expect

- Friendly, constructive code reviews
- Response within 3-5 business days
- Recognition in contributors list and release notes

Lessons Learned

Lessons Learned 💡

What We’ve Discovered

Technical Insights

- Ansible + Proxmox API = powerful combo for IaC cyber ranges
- Snapshot/restore capabilities are critical for training resets
- Telemetry integration from day one simplifies troubleshooting

Lessons Learned 💡

Process & Collaboration

- Governance overhead is real: LICENSE, SECURITY, CI/CD take time but unlock collaboration
- Documentation maturity lags code development (common open source challenge)
- Balancing rapid prototyping with production-ready standards

🤝 **Community Benefits:** Diverse perspectives improve scenario realism and platform robustness.

Open Challenges & Opportunities ⚠

Where We Need Help

Governance & Quality

- Enable CI/CD pipelines (ansible-lint, pytest, npm audit)
- Add contributor documentation and onboarding guides

Technical Scaling

- Expand scenario coverage from 20 to 50+ deployable labs
- Support multi-subnet architectures for complex exercises

> 👥 **Your Expertise Matters:** Every contribution - code, docs, testing, design - moves the platform forward.

Range42: Today & Tomorrow

What We’ve Built

- Open, modular cyber range with 20 deployable scenarios
- Strong security baseline: zero high-severity findings
- Clear architecture with multiple contribution paths
- Active development: 13 repositories, 500+ commits

What We’re Building

- 50+ scenario coverage across diverse technologies
- Production-ready lab designer for instructors
- Multi-subnet support for advanced training exercises

Get Involved 🚀

Join the Range42 Community

Contribution Areas

- **Scenario Design**: CVE research, automation
- **Infrastructure**: Ansible roles, backend API, CI/CD
- **UI/UX**: Lab designer, EMP UI

Contact & Resources

- GitHub: `github.com/range42`
- Email: `steve.clement@nc3.lu`

Contribute

Figure 1: *

github.com/range42