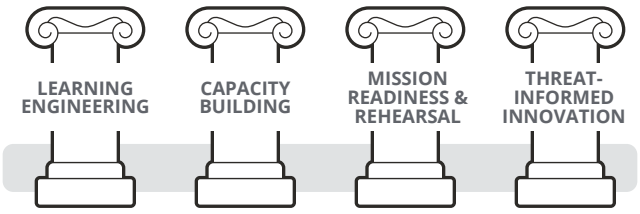
Carnegie Mellon University
Software Engineering Institute
CERT Division

Crucible Cyber Platform

An Open-Source Application Framework for Cyber Capacity Building, Experimentation, and Rehearsals

OUR MISSION: To promote and foster a comprehensive cyber-readiness ecosystem built on an open source learning and mission rehearsal platform. Leveraging SEI's Crucible framework, guided by open standards (TLA, cmi5, xAPI), and competency models (DCWF/NICE), we empower training managers, instructors, and mission partners to deliver tailored, data-driven learning experiences. We help individuals and teams achieve proficiency, certification readiness, mission qualification, and operational lethality across current and emerging cyber work roles.

Pillars



Learning Engineering

Measure what matters. Improve what matters.

We apply evidence-based learning science, open standards, and performance analytics to understand how individuals and teams learn, practice, and improve. Standards-aligned telemetry (xAPI, cmi5, TLA) transforms learner activity into actionable insight, enabling objective assessment, targeted intervention, and continuous improvement.

Capacity Building

Build durable capability, not one-off training.

We develop mature, resilient, and sustainable organic capability across people, teams, processes, and technology. Performance data reveals strengths and gaps, informs targeted development, and accelerates progression from participation to qualification, creating enduring organizational capacity.

Mission Readiness & Rehearsal

Validate readiness before it matters most.

We enable individuals and teams to rehearse real missions, validate workflows, and demonstrate operational excellence. Readiness is assessed holistically, combining technical execution with team coordination, communication, and decision-making under realistic conditions.

Threat-Informed Innovation

Stay aligned with the adversary, not yesterday's assumptions.

Capabilities evolve alongside the threat landscape through intelligence-informed scenario design, continuous experimentation, and AI-enabled concepts. This ensures mission rehearsals reflect the adversary's most current tactics, techniques, and procedures, maintaining relevance in rapidly changing environments.

Platform Outcomes

- Strengthening organizational capability across technical and non-technical domains
- Preparing leaders and teams for complex, high-consequence environments
- Driving measurable performance improvements using science, data, and standards
- Creating a pipeline of mission-ready talent aligned to competency frameworks
- Ensuring individuals and teams are fully prepared to execute mission tasks

Core Values

- **Open:** open source, open standards, open frameworks
- **Interoperable:** across learning systems, mission rehearsal platforms, and operational tools
- **Traceable:** learner behavior connected to competency via "task → measure → outcome → readiness"
- **Scalable:** from one learner to cyber units
- **Adaptable:** to evolving mission environments and requirements
- **Repeatable:** built on sharable, version-controlled content and reusable artifacts
- **Evidence-based:** backed by learning analytics and activity data

KEY PLATFORM FEATURES

- Open source built on Angular and .NET Core
- Modular, API-driven architecture for extensibility
- Customizable, browser-based, immersive UI
- Integrates with third-party open-source tools
- Automation for rapid deployment and repeatability
- Interoperability via open standards (xAPI, cmi5, TLA)
- Supports scenario-based missions, rehearsals, and challenges
- Build cyber terrain: model topologies, simulate activity, and script events
- Flexible terrain-building options:
  - Infrastructure-as-Code for scale and reuse
  - Form-based configuration for fast setup

Open-Source Platform Integrations

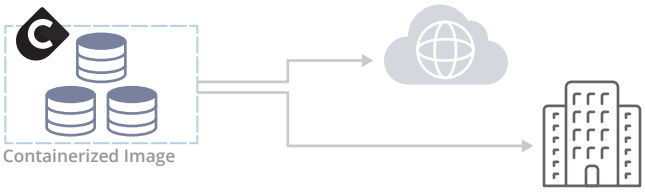
Keycloak: An open-source identity authentication service that implements the OpenID Connect authentication protocol.

Moodle: An interactive learning management system, enables embedding interactive quiz content and recording user experience data to a learning record store using the Experience API (xAPI).

MISP: A threat information sharing platform for sharing, storing and correlating Indicators of Compromise.

NextCloud Hub: A self-hosted solution that integrates file storage, chat/talk, email, calendar, office and more in one federated content collaboration platform.

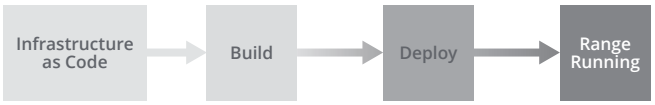
Flexible Hosting Options



Crucible applications are released as Docker images and can be easily deployed in the cloud or on-premises:

- **Cloud:** Crucible platforms have been deployed in AWS and Azure.
- **On-Premises:** Crucible platforms have been used to deploy cyber ranges onto VMware and Proxmox hypervisors.

Automated Deployment



New platforms can be deployed quickly through infrastructure as code technologies.

Content Curation

- Align content to work-role competencies: Knowledge, Skills, Abilities, Tasks (KSATs)
- Map learning activities to work-role development plans
- Integrate content from vendors, universities, and military schoolhouses
- Support easy content import and export

Use Cases

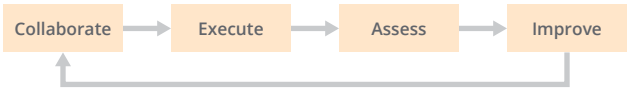
- All-hazards tabletop exercises
- Cyber wargaming
- Capture the flag competitions
- Fully online, self-paced learning
- Hybrid and facilitated learning

ENGINEERING THE FUTURE OF TRAINING

Track learner experiences to infer work role readiness

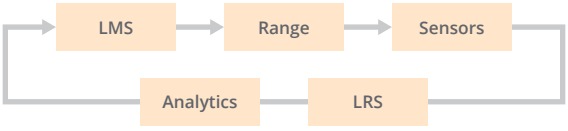
- Use xAPI telemetry + competency models to map learner behaviors to relevant KSAs and Tasks.
- Build readiness scores and profiles to demonstrate learner progression from Novice/Intermediate/Advanced to Ready-Trained, all the way to Ready-Qualified
- Identify micro-skills using machine-coded rules and AI pattern detection
- Provide adaptive feedback interventions, recommending next steps, labs, or practice scenarios based on observed performance gaps

Track team performance to infer team readiness



- Capture collaboration telemetry: communication patterns, task handoffs, decision timelines, and coordination efficiency
- Analyze team behaviors with data models to evaluate team roles
- Produce team readiness dashboards highlighting strengths, breakdowns, and mission-task coverage
- Evaluate teams/units across repeated scenarios to measure growth, cohesion, and resilience

Assess cyber performance with xAPI and TLA



- Automatically generate performance assessments built on standard verbs, objects, and profiles using event-to-KSA mapping
- Produce machine-scoreable assessment artifacts
- Enable “follow the thread” analysis: tie learner actions to scenario events to mission outcomes
- Develop cross-system interoperability for performance data flows from learning management system (LMS) → range → SIEM/sensor → assessment engine → readiness dashboard

AI-enhanced scenario design

- Integrate AI to translate threat intelligence into runnable training scenarios.
- Integrate AI to dynamically adjust scenario difficulty: inject noise, modify the adversary timeline, vary complexity of artifacts
- Generate dynamic narrative arcs guiding learners through multi-stage attacks with branching opportunities

AI-enhanced cyber range topologies

- Personalized Learning Engines for Cyber
- Individualized learning pathways informed by telemetry, prior experience, and work role requirements
- Learners receive training arcs, reorganizing content into optimized sequences for their pace and skill gaps
- Training managers get predictive dashboards showing which learners are likely to achieve advancement

Join Us

We invite you to partner with us to advance an open, interoperable, innovative, standards-aligned cyber readiness ecosystem.

Get Involved

- Explore Crucible and contact us about integrating it into your training workflows
- Collaborate with us on new learning activities, datasets, or threat-informed mission rehearsals
- Adopt open standards for performance tracking and learner data interoperability
- Engage with our community to shape the future of cyber workforce development

Together, we can build a more capable, resilient, adaptable, and mission-ready cyber force.

About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

This material is based upon work funded and supported by the Department of War under Air Force Contract Nos. FA8702-15-D-0002, and FA870225DB003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM26-0061