ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

The Cyber War Center: Cyber Threat Simulations for Defensible Design and Engineering Teams.

Institute of Security Architecture United
Art Chavez

Divisions of Technical Excellence

ISAUnited is organized into specialized divisions that advance technical rigor, applied education, and disciplined inquiry in cybersecurity architecture and engineering. Each division concentrates expertise in a defined domain and strengthens system design, development, and defense through standards development, research, and verification-focused work. Together, these divisions also form the technical backbone of the ISAUnited Cyber War Center by shaping scenario realism, defining defensible design expectations, mapping mechanisms and controls to architectural decisions, and supporting evidence-based evaluation of Skills, Knowledge, and Abilities, which reinforces both the Center's defensive mission and its credibility.

ISAUnited Cyber War Center

Executive Summary

Executive Summary

Cybersecurity is a performance profession. Reading, watching videos, and passing quizzes do not automatically translate into the ability to design and build systems that withstand real threats.

The ISAUnited Cyber War Center (CWC) is a simulation and evaluation capability built to close that gap for defensive designers and builders. It helps learners put what they know into practice by working through realistic threat conditions, adopting an attacker mindset at the level of intent and observable effects, and producing defensible engineering artifacts.

The Cyber War Center supports two audiences:

- Students and career entrants who need a structured bridge between learning and doing.
- Enterprise teams that need annual cyber threat simulations and skills validation with evidence-based Skills, Knowledge, and Abilities (SKA) reporting for leadership.

Operational support for the Cyber War Center is provided through the ISAUnited School of Engineering Cyber Defense. That partnership ensures scenario quality, defensible grading, and consistent engineering expectations across both academic capstones and industry training.

1. Introduction

Cybersecurity has become a daily operational concern for every organization that depends on connected systems. New applications, cloud platforms, branch networks, and internet-connected devices create opportunity, but they also create exposure. When a system is built without clear boundaries, controlled pathways, and measurable safeguards, a threat event becomes a business event.

In most professions where safety, reliability, and continuity matter, simulation is not optional. It is the method used to keep skills current, build confidence under pressure, and expose gaps before they cause harm. Cybersecurity deserves the same discipline, especially for the people responsible for designing and building the systems that others depend on.

Workforce guidance from the National Initiative for Cybersecurity Education describes cyber ranges as interactive, simulated representations of networks, systems, tools, and applications. It emphasizes that these environments provide a safe and legal way to build hands-on skills and to test security posture. [1] The Cyber Range Guide expands that rationale by highlighting performance-based learning and assessment, teamwork and coordination, real-time feedback, on-the-job experience, and an environment where new ideas can be tested and refined. [2]

National Institute of Standards and Technology guidance on test, training, and exercise programs reinforces the value of structured practice to validate plans and capabilities. [3] Incident response guidance similarly stresses preparation and repeatable exercises as part of readiness. [4] Industry exercise guidance aligns with this view: rehearsal and evaluation expose weaknesses that policies and diagrams alone will not reveal. [5]

The ISAUnited Cyber War Center is built to meet this need with defensive intent. It is a simulation and evaluation center for cyber threat scenarios that require defensible architecture and engineering decisions. The operational support function for the Cyber War Center is provided by the ISAUnited School of Engineering Cyber Defense, ensuring consistent expectations, evaluator discipline, and academic alignment for capstones and workforce programs.

Participants learn to think like an attacker without glamorizing offense. The opposing force perspective is limited to intent, pathways, and observable effects, so designers and builders can anticipate pressure and engineer controls that hold. Each simulation guides participants through a structured sequence of modules, scenario injects, and decision points, leading to concrete outputs such as diagrams, control strategies

mapped to the Defensible 10 Standards, measurable acceptance criteria, and an evidence index.

For prospective students, the Cyber War Center is where knowledge becomes capability and where skill can be demonstrated through defensible artifacts. For managers, it is a repeatable approach to simulation-based training and validation that produces Skills, Knowledge, and Abilities reporting, highlights improvement priorities, and strengthens the quality of systems delivered to the business.

2. The problem: knowledge without capability

Cyber teams are often trained with content that is easy to deliver but hard to operationalize. Learners can describe threats and controls but struggle to apply them under time pressure, with incomplete information, and in real-world contexts.

The NICE community has highlighted a persistent gap: cybersecurity education and workforce development often lack realistic simulation environments comparable to those in other professional fields. Cyber range concepts help address challenges in realism, legality, accessibility, and scalability. [2]

In practice, this gap shows up in predictable ways:

- Design decisions are made without clear system boundaries, trust zones, or data flow understanding.
- Controls are selected as checklists instead of mechanisms tied to specific threats and measurable acceptance criteria.
- Teams cannot demonstrate whether a design is defensible because evidence and validation were never planned.

The Cyber War Center exists to turn learning into defensible practice: threat-informed architecture, engineering decisions, and proof.

3. Why simulation-based training and why now

Simulation is widely used to build performance in high-stakes professions. In cybersecurity, simulation environments are valued because they provide a safe, legal space to build hands-on skills and validate procedures and plans. [1] [2]
NIST NICE describes cyber ranges as interactive simulated representations of networks, systems, tools, and applications that enable hands-on skill development in a controlled environment. [1]

Simulation training improves outcomes because it can:

- Provide performance-based learning, assessment, and real-time feedback. [1] [2]
- Simulate on-the-job experience and team coordination. [1] [2]
- Support skills validation for hiring, promotions, and readiness planning. [2]
- Validate the viability of response, continuity, and communication plans through structured exercises. [3] [5]

Tabletop exercises are often cost-effective tools for validating plans and ensuring they are viable and implementable in an emergency. [3]

4. What the Cyber War Center is and what it is not

The Cyber War Center is a defensive simulation and assessment environment for people who design and build systems. It strengthens the capability to make sound security decisions before systems go live and as threats evolve.

What it is:

- A structured simulation that produces defensible architecture and engineering artifacts.
- A capstone administration capability for ISAUnited academic programs and Certified Professional License pathways.
- A workforce readiness service for organizations that need annual training and evidence-based evaluation.
- A bridge between knowing and doing through controlled adversary intent and realistic injects.

What it is not:

- Not a Security Operations Center school or alert triage training program.
- Not a platform that teaches intrusion steps, exploit development, or offensive tooling.
- Not a one-time discussion exercise without evidence capture and scoring.

The adversary perspective is used to build defensive clarity: objectives, constraints, likely paths, and expected observable effects. Participants learn to think like an attacker so they can design and build defenses that hold up, without being trained in offensive execution.

5. The CWC experience: modules, artifacts, and evidence

Each simulation is delivered in a modular sequence. Participants receive scenario context and timed injects, then produce artifacts that demonstrate defensible decisions. Short adversary diary videos may be used to introduce limited intent-based clues to increase realism while keeping the exercise defensively oriented.

CWC exercise flow (Phase 1: LMS plus artifacts; Phase 2: hybrid or live fire):

1. Brief: scope and system
2. Map: attack surface
3. Design: controls and criteria
4. Validate: defend plan
5. Demonstrate: evidence and report

Core participant outputs (portfolio ready):

- System scope and boundary diagram, including trust zones and critical assets.
- Attack surface and risk snapshot tied to the scenario.
- Defensible control strategy mapped to engineering standards and measurable acceptance criteria.
- Updated architecture diagrams using ISAUnited stencils and a mechanism catalog for consistent control placement.
- Evidence index: what proof would demonstrate detection, containment, and prevention in this design?
- Management-ready summary describing decisions, trade-offs, and residual risk.

For enterprise teams, these outputs also become improvement inputs: design backlog items, control gaps, engineering standards updates, and targeted training recommendations.

6. SKA profiling: what learners and managers receive

The Cyber War Center produces Skills, Knowledge, and Abilities (SKA) profiles based on observable work products and documented decisions. This supports both learner growth and organizational readiness planning.

Individual SKA Profile (for the participant):

- Strengths and gaps across Knowledge, Skills, and Abilities.
- Evidence-based notes tied to submitted artifacts.
- Role-aligned development plan: what to learn next and what to practice next.

Team and Management Readiness Report (for leadership):

- Aggregated heat maps across role groups and skill dimensions.
- Recurring design and engineering gap themes such as trust boundaries, identity plane design, and logging requirements.
- Training priorities and recommended engineering standard updates.
- Optional retest plan to measure improvement over time.

Exercise guidance emphasizes running simulations regularly so teams understand roles, priorities, coordination, and what is missing from plans. [5] CWC reporting is designed to make that rhythm measurable and defensible.

7. Program lanes: students and enterprises

Lane A: School of Engineering Cyber Defense

Students complete capstone simulations administered through the Cyber War Center. The School of Engineering Cyber Defense provides curriculum alignment, quality standards for scenarios, and capstone governance. The Center provides delivery operations, evaluation, and SKA reporting.

Lane B: Industry Training and Skills Validation

Organizations enroll builders such as platform teams, infrastructure teams, cloud teams, application teams, and Security by Design practitioners. Exercises can be used to meet annual training requirements, support onboarding, assess promotion readiness, or target capability improvement.

- Annual readiness simulations and validation
- Role-based tracks for architecture and engineering teams
- Scenario rotation to reduce coaching bias
- Optional customization to match technology stacks and delivery models

8. Governance, Safety, and Defensive Intent

The Cyber War Center is designed to strengthen defense. It uses an opposing force narrative to create realism, not to glamorize or teach offense.

CWC governance principles:

- Defensive only content: adversary materials focus on objectives, constraints, and observable effects.

- Evidence-based scoring: evaluations are based on artifacts and documented reasoning, not personality or theatrics.
- Separation of roles: an internal adversary cell drives injects; participants operate as defenders and designers.
- Professional discipline: exercises strengthen plans, roles, and communications, consistent with exercise guidance from standards bodies. [3] [5]

This approach makes the experience safe for education, appropriate for enterprise adoption, and aligned with responsible security practice.

9. In Summary

The ISAUnited Cyber War Center exists to close the gap between knowing cybersecurity and practicing it with discipline. In every organization, security outcomes are shaped long before an incident, through the way systems are designed, integrated, and operated. Simulation brings that reality into focus by forcing real decisions under time pressure, exposing weak assumptions, and turning abstract guidance into defensible architecture and engineering choices that can be measured and improved.

This Center is built with a defensive intent and a commitment to professional responsibility. It trains designers and builders to anticipate threats without glamorizing offense, and it evaluates capability through structured artifacts that demonstrate clear reasoning, control strategy, and evidence of outcomes. The operational support function is provided by the ISAUnited School of Engineering Cyber Defense, ensuring consistent standards, evaluator discipline, and a reliable pathway for both Certified Professional License capstones and workforce readiness programs.

For prospective students, the Cyber War Center is where a career begins with proof, not promises. For managers, it is a repeatable method for strengthening teams, validating readiness, and improving the quality of systems delivered to the business. If you are ready to move from intention to defensible execution, the Cyber War Center provides the scenarios, structure, and accountability to make that shift real.

References and next steps

[1] National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology. Cyber Ranges. One-page brief (February 2018).

[2] NICE Community Coordinating Council. The Cyber Range: A Guide. Guidance document for use cases, features, and types of cyber ranges (September 2023).

[3] Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., and Good, T. NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (September 2006).

[4] Nelson, A., Rekhi, S., Souppaya, M., and Scarfone, K. NIST Special Publication 800-61 Revision 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management (April 2025).

[5] Wlosinski, L. G. Cybersecurity Incident Response Exercise Guidance. ISACA Journal, Volume 1 (January 2022).

Next steps

- Prospective students: ask about the School of Engineering Cyber Defense pathway and when capstones are administered through the Cyber War Center.
- Managers: schedule an intake to select a scenario track, define the annual training cadence, and choose SKA reporting options.

Contact:
info@isaunited.org
isaunited.org

End of Document
IO.