CYBER WAR CENTER

ISAUNITED SIMULATOR

DEFENSIBLE CAPABILITY SCORE REPORT

CYBER CAPSTONE EVALUATION AND SCORING REPORT

ISAUNITED CYBER WAR CENTER SIMULATOR

ROLE TRACK	SCENARIO	REPORT ID

SAMPLE REPORT

ISAUnited Cyber War Center

Defensible Capability Score Report

Sample Public Report | Fictional Data

Cyber Capstone Evaluation and Scoring Report

Student or Practitioner	Sample Practitioner	TOTAL TECHNICAL SCORE
Role Track	Security by Design	**84%**
Organization	Orion Digital Services	**Rating: Green**
Scenario	ICC-SbD-06 Launch Shield	**Outcome: Pass**
Review Date	November 29, 2025	
Report ID	2026-SAMPLE-001	

Rating Legend

Green	Yellow	Yellow	Red
80 to 100% Pass	70 to 79% Conditional Pass	60 to 69% Remediation Required	0 to 59% Fail

1. Report Purpose

This sample report shows how a completed Cyber Capstone submission is converted into an evidence based Defensible Capability Score. The score reflects artifact quality, defensible reasoning, and demonstrated practitioner capability.

The Technical Artifact Evaluation determines the official score and outcome. The Professional Capability Profile is scored separately to show skills, knowledge, abilities, judgment, communication, and evidence discipline. This sample uses fictional data.

2. Scoring Formula Summary

Formula Area	Calculation	Notes
Technical score	Sum of the five weighted category scores	Maximum technical score is 100 points.
Technical percent	Technical score divided by 100	The percent drives the color rating and formal outcome.
Capability score	Average of Skill, Knowledge, and Ability for each capability dimension, rounded to one decimal place	This does not replace the technical score.
Overall capability profile	Average of all capability scores, rounded to one decimal place	1.0 to 1.4 Foundation, 1.5 to 2.4 Proficient, 2.5 to 3.0 Advanced.

3. Cyber Capstone Artifacts Reviewed

Artifact ID	Artifact Title	Evidence Reviewed
Artifact 1	Executive Summary	Problem framing, business context, assumptions, and recommended direction.
Artifact 2	Threat and Risk Threat Model Snapshot	Threat vectors, exposure conditions, impact paths, and risk priorities.
Artifact 3	Design and Control Strategy	Core principles, security controls, standards alignment, requirements, and rationale.
Artifact 4	Key Cybersecurity Design Model Architecture Diagram	Trust boundaries, defensive mechanism placement, architecture fit, and control placement.
Artifact 5	Project Team Presentation Deck	Clear communication of the defensible plan, major decisions, tradeoffs, and readiness recommendation.

4. Technical Artifact Evaluation

This section scores the submitted Cyber Capstone artifacts using five weighted categories. Scores must reference specific artifacts, sections, figures, tables, diagrams, or presentation slides. This section determines the official technical score and capstone outcome.

Scoring Category	Weight	What the Category Measures	Primary Evidence	Score	Rating
Threat Reasoning and Risk Judgment	20	Quality of inferred threat vectors, exposure conditions, threat tools, risk prioritization, and scenario specific judgment.	Artifacts 2, 3, 4	17 / 20	Proficient
Design and Control Strategy	25	Quality, relevance, and practicality of Security by Design decisions, control direction, requirements, and tradeoffs.	Artifacts 1, 3, 4	21 / 25	Proficient
Standards and Control Alignment	20	Use of Defensible 10 Standards, Cybersecurity Core Principles, control intent, and traceability recommendations.	Artifacts 3, 4	17 / 20	Proficient
Architecture Reasoning and Defense Model	20	Ability to interpret the system, trust boundaries, dependencies, data flows, defensive placement, and architecture fit.	Artifacts 2, 4	17 / 20	Proficient
Communication and Defensibility	15	Clarity of assumptions, rationale, presentation quality, decision defense, and ability to brief a project team.	Artifacts 1, 5	12 / 15	Proficient
Total Technical Score	100	Total weighted score across all categories.	All artifacts	**84 / 100**	**Green**

5. Technical Scoring Rubric

Category	Foundation Range	Proficient Range	Advanced Range
Threat Reasoning and Risk Judgment	Identifies general threats but misses scenario specific exposure conditions, impact paths, or risk priorities.	Identifies credible threat vectors, exposure conditions, and risk priorities that fit the scenario.	Anticipates adversary behavior, failure modes, trust dependencies, and business impact with clear prioritization.
Design and Control Strategy	Provides generic controls or principles with limited fit to scenarios.	Provides practical Security by Design decisions with clear rationale and tradeoffs.	Builds an integrated design strategy that balances risk, operations, launch constraints, and sustainment.
Standards and Control Alignment	Mentions standards or controls without strong traceability.	Connects recommendations to Defensible 10 Standards, principles, and control intent.	Uses standards and control intent to create a traceable, defensible, and evidence ready design position.
Architecture Reasoning and Defense Model	Describes the diagram but does not fully reason through dependencies or boundaries.	Interprets components, data flows, trust boundaries, and defensive placement credibly.	Shows strong system reasoning with control placement that fits architecture, operations, and likely misuse conditions.
Communication and Defensibility	The submission is difficult to follow and lacks clear assumptions and rationale.	Communicates the plan clearly with reasonable assumptions, evidence, and decision logic.	Presents a strong professional argument that a technical project team or leader can act on.

6. Defensible Loop Evidence Coverage

This section does not replace the official technical score. It maps submitted evidence to the Defensible Loop, enabling the evaluator to show where the candidate demonstrated lifecycle coverage across Define, Design, Deploy, Detect, Defend, and Demonstrate outcomes.

Phase	Evidence Expected	Artifact Sources	Coverage	Evaluator Notes
Define	Scope, business requirements, constraints, assumptions, and design problem framing.	Artifacts 1, 3	**Complete**	Scope and launch constraints are clear.
Design	Threat informed design direction, control intent, standards alignment, and risk based security decisions.	Artifacts 2, 3, 4	**Complete**	Threat informed design choices are traceable.
Deploy	Defensive mechanism placement, architecture fit, implementation intent, and configuration direction.	Artifact 4	**Complete**	Placement of key mechanisms is shown.
Detect	Monitoring, logging, alerting, telemetry, and detection considerations.	Artifacts 3, 4	**Partial**	Detection intent is present; telemetry detail needs expansion.
Defend	Resilience, containment, response readiness, residual risk, and operational protection.	Artifacts 3, 4, 5	**Complete**	Residual risk and response posture are addressed.
Demonstrate	Evidence, rationale, presentation quality, decision defense, and stakeholder communication.	Artifacts 1, 5	**Complete**	Presentation supports the recommendation.

7. Professional Capability Profile

This section evaluates the practitioner's skills, knowledge, and abilities as demonstrated through the submitted artifacts. It is scored separately from the Technical Artifact Evaluation and measures disciplined practice, the quality of reasoning, and the defensibility of professional judgment.

1 Foundation	2 Proficient	3 Advanced

Skill means execution and technique. Knowledge means understanding and correctness. Ability means judgment and application under constraints. Capability Score is the average of Skill, Knowledge, and Ability for each capability dimension, rounded to one decimal place.

Capability Dimension	Skill	Knowledge	Ability	CP	Evidence References	Evaluator Notes
Engineering Discipline	2	3	2	**2.3**	Artifacts 3 and 4	Structured and practical.
Systems Reasoning	2	3	3	**2.7**	Artifact 4, Figure 1	Strong boundary reasoning.
Threat and Risk Judgment	2	2	2	**2.0**	Artifact 2, Section 2	Credible threat priority.
Defensive Design Quality	3	3	2	**2.7**	Artifact 3, Section 4	Well aligned controls.
Verification and Evidence Mindset	2	2	2	**2.0**	Artifacts 3 and 5	Evidence is usable.
Operational Readiness	2	2	2	**2.0**	Artifact 5, Slide 8	Clear readiness path.
Clarity and Communication	3	2	3	**2.7**	Artifact 1 and Slide 3	Concise executive brief.
Overall Capability Profile	**2.3**	**2.4**	**2.3**	**2.3**	All artifacts	Overall profile is Proficient.

8. Capability Profile Summary

Executive Summary	The sample practitioner demonstrated a strong Security by Design posture with credible threat reasoning, practical control selection, and clear architecture rationale. The work is ready to advance, with additional telemetry detail recommended before production launch.
Key Strengths	1. Clear threat vector prioritization 2. Practical defensive mechanism placement 3. Strong executive communication
Priority Development Areas	1. Expand detection telemetry requirements 2. Strengthen residual risk evidence 3. Add stronger verification criteria
Recommended Next Step	Advance to the next capstone tier
Evaluator Recommendation	This sample result supports advancement. A team lead should use the development areas as coaching points before assigning higher complexity scenarios.
Evidence Citation Format	Example: Artifact 2, Section 3.2; Artifact 4, Figure 1; Artifact 5, Slide 8.

9. Evaluator Attestation

The evaluator attests that the score is based on submitted Cyber Capstone evidence, the applicable rubric version, and the role track expectations assigned to the scenario. The evaluation reflects the submitted work and does not certify independent job performance outside the capstone unless separately authorized by the ISAUnited program policy.

Reviewer	Sample Evaluator
Title	Cyber Capstone Evaluator
Rubric Version	v1.0 - Sample Rubric
Signature and Date	Sample Signature November 29, 2025