Enhancing Workforce Cyber Resilience: Bridging the Gap in ICS Protection

Abdullah Jawad

Noah Quesenberry

Husnu S. Narman

Paulus Wahjudi

Department of Computer Sciences and Electrical Engineering

Marshall University

March 2025

Outline

Introduction

Problem and Objective

CyberHive Simulation

Results

Conclusion

Introduction

- Critical Infrastructure: Growing cyber threats
- Industrial Control Systems (ICS): Vulnerable
- Skills Gap: Operational and IT/Cybersecurity Specialists
- How to address this gap to improve cyber resilience

Problem

- ICS Engineers: Lack cybersecurity training

- IT/Cyber Specialists: Lack ICS knowledge
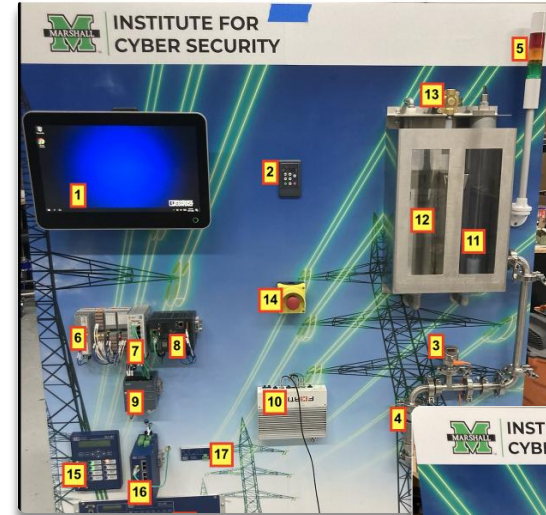
- Impact: Greater risk of cyber-attacks

Objective

- Review exiting strategies

- Measure the effectiveness

Existing Solutions

- Traditional classroom training

- Simulation

- Gamification

CyberHive

- SCADA system simulation for ICS security training

- Training Modules: ICS Basics, vulnerability analysis

- Process: Training and capture the flag challenge

Methodology

- Participants: Undergraduate students
- Process: Training with/without CyberHive
- Test: National Cyber League (NCL)
- Metrics: Scores and Completion and Accuracy Rates

CyberHive: Training and CTF

Category	Number of Challenges
1 - ICS Basics	13
2 - PLC Programming	9
3 - Modbus Basics	6
4 - Modbus Analysis	5
5 - ENIP/CIP Basics	6
6 - Attack Surface Identification	10
7 - Static Analysis	5
8 - Dynamic Analysis	6
9 - Endpoint Manipulation	2

CyberHive CTF: Team Performance

User Teams	Score	Completion Percentage
Team 1	2525	100%
Team 2	2525	100%
Team 3	1755	69.50&
Team 4	1715	67.92%
Team 5	1677	66.42%

CyberHive CTF: Challenge Performance

Category	Submission Rate
1 - ICS Basics	100%
2 - PLC Programming	95.5%
3 - Modbus Basics	100%
4 - Modbus Analysis	96%
5 - ENIP/CIP Basics	96.7%
6 - Attack Surface Identification	72%
7 - Static Analysis	100%
8 - Dynamic Analysis	100%
9 - Endpoint Manipulation	70%

National Cyber League Scores with CyberHive

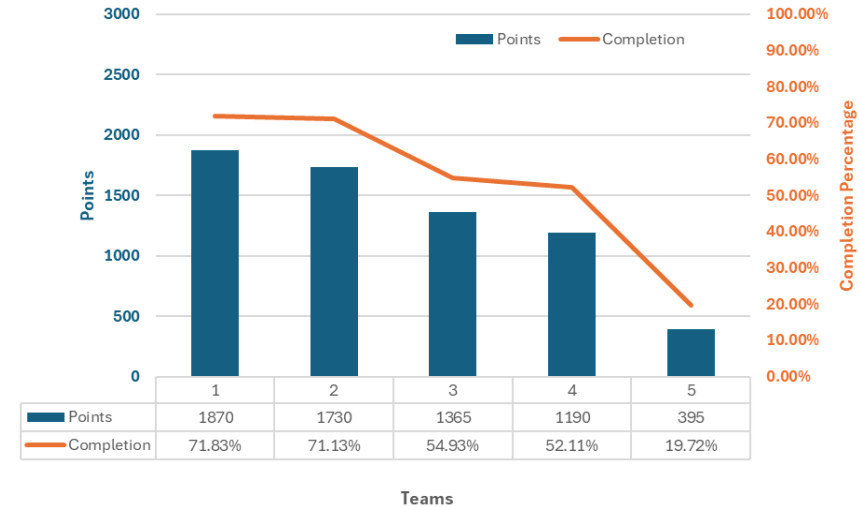

Points / Completion of CTF per Team (For NCL Spring 2024)

	1	2	3	4	5	6	7	8	9	10	11
Points	2730	1990	1925	1360	1195	1175	1140	830	545	530	475
Completion	91.60%	73.11%	65.55%	52.94%	49.58%	41.18%	45.38%	31.09%	26.89%	17.65%	15.13%

Teams
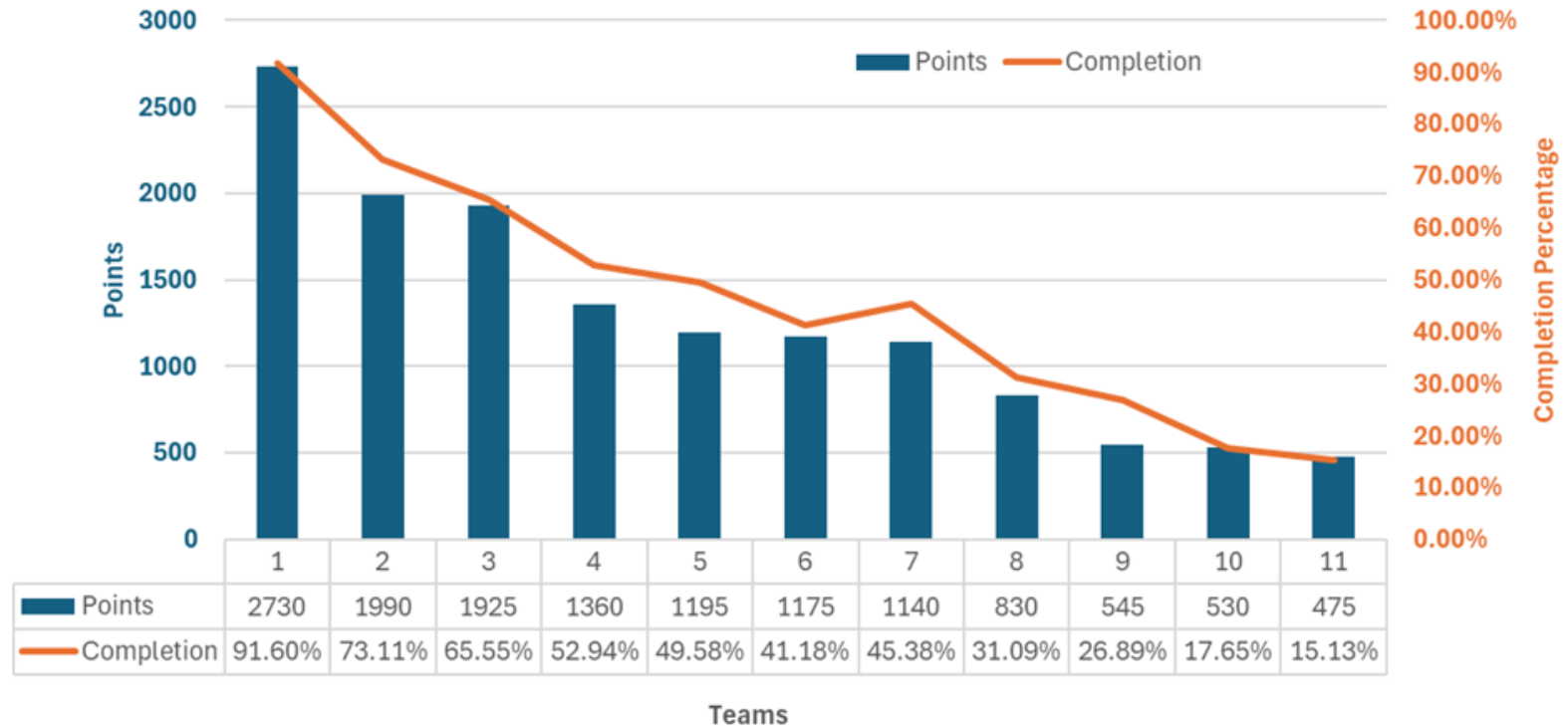
National Cyber League Scores without CyberHive

Points / Completion of CTF per Team (For NCL Spring 2023)

	1	2	3
Points	2250	1635	1475
Completion	86.49%	70.27%	62.16%

Teams

Points / Completion of CTF per Team (For NCL Spring 2022)

	1	2	3	4	5
Points	1870	1730	1365	1190	395
Completion	71.83%	71.13%	54.93%	52.11%	19.72%

Teams
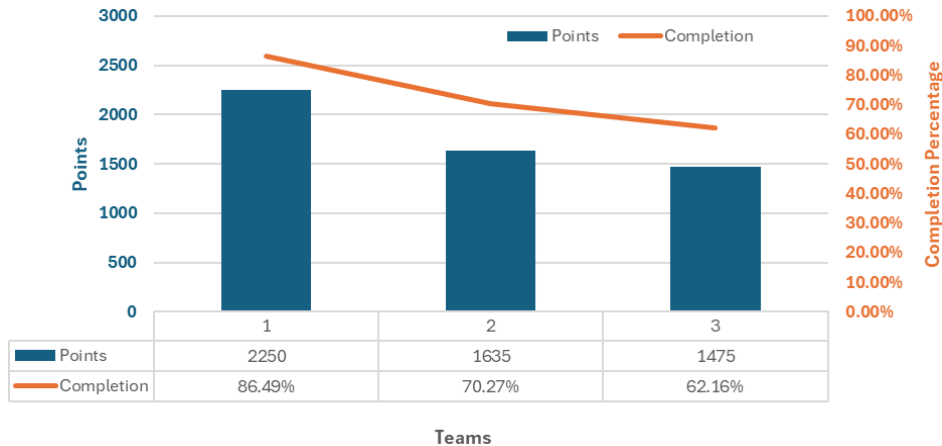
National Cyber League Scores: Findings

- Accuracy rates improved

- Completion rates varied

- Mock CTF training led to more participation in NCL

Conclusion

Training through CyberHive simulation enhances cybersecurity preparedness

Bridging the IT/OT Gap: Cross-disciplinary training enhances skills

Practical training fosters collaboration between ICS & Cybersecurity teams