NICE 2025

PRESENTATION

Cyber Kostinichi for Cyber Operations Preparedness and Education (COPE)

Jordan “Cancer” Scott

Abstract

From the legacy of the Code Talkers to the frontiers of space cybersecurity, we're bridging critical skills gaps through innovative training. Our framework combines agile methodologies with gamified learning, demonstrated through real-time space mission simulations. We'll showcase our pilot program's results, featuring Kerbal Space Program integration, and explore partnership opportunities to establish sustainable cyber education pathways in local communities.

Who We Are

Code Talkers Engineering

SPACE ISAC

cyberTAP

COPE

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Who I am

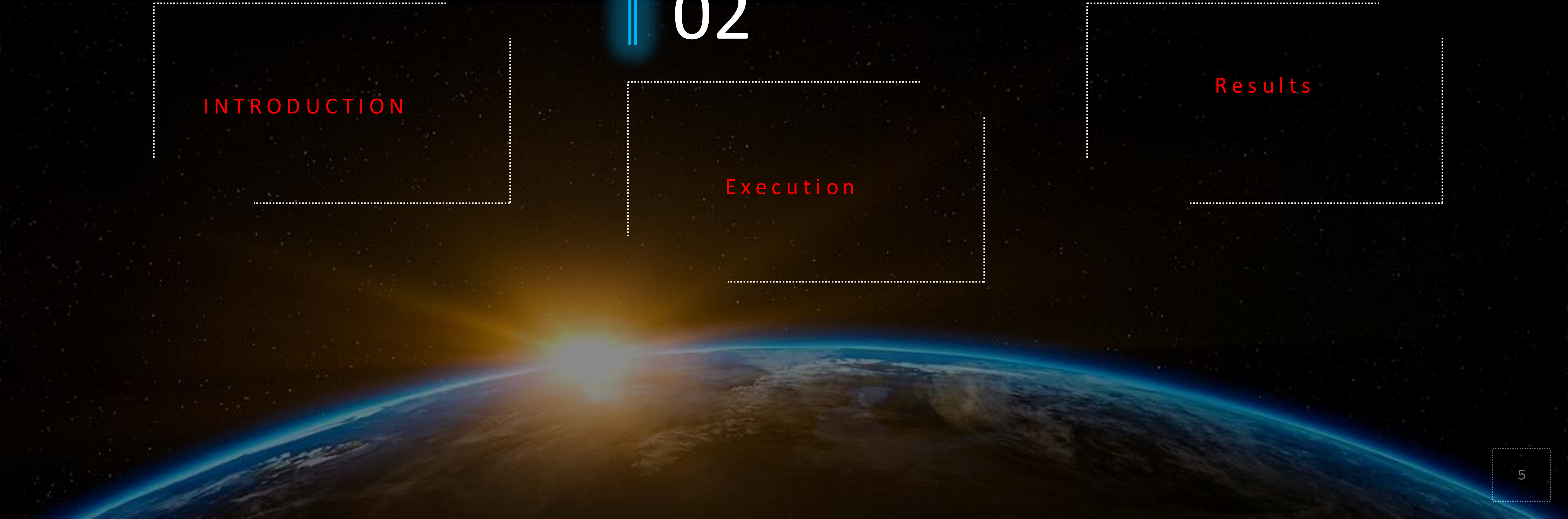
Jordan Scott

Innovation Chief @ Code Talkers Engineering

- B.S. / M.S. in Computer Engineering
- PhD in Cybersecurity (pending dissertation completion)
- CISSP, CYSA+, SEC+, SAFe Agilist/Scrum Master, CMMC RP
- Former Presidential Candidate, 2020
- Fluent in memes
- Former Army Infantry/Electronic Warfare Officer
- Has done standup comedy twice on cyber
- Creator of Cyber Attack! The Card Game

https://www.linkedin.com/in/jordan-cancer-scott/

TABLE OF CONTENTS



01

INTRODUCTION

02

Execution

03

Results

01

INTRODUCTION

What we did…

Research Questions

- How effective is an agile, gamified framework in developing Space ISSO competencies?
- Does an inverted security risk taxonomy have an impact on cybersecurity training effectiveness?
- How can domain-specific Knowledge, Skills, and Tasks (KSTs) be effectively integrated into a comprehensive cybersecurity training program?

Space ISSO

A **Space Information System Security Officer** is an individual assigned responsibility for maintaining the appropriate operational security posture for a Space (Spacecraft, Mission packages, Ground stations, Data links, Launch systems, Supporting infrastructure) information system or program. They are responsible for ensuring the confidentiality, integrity, and availability of the system or program, as well as for implementing and enforcing security policies and procedures.

Importance

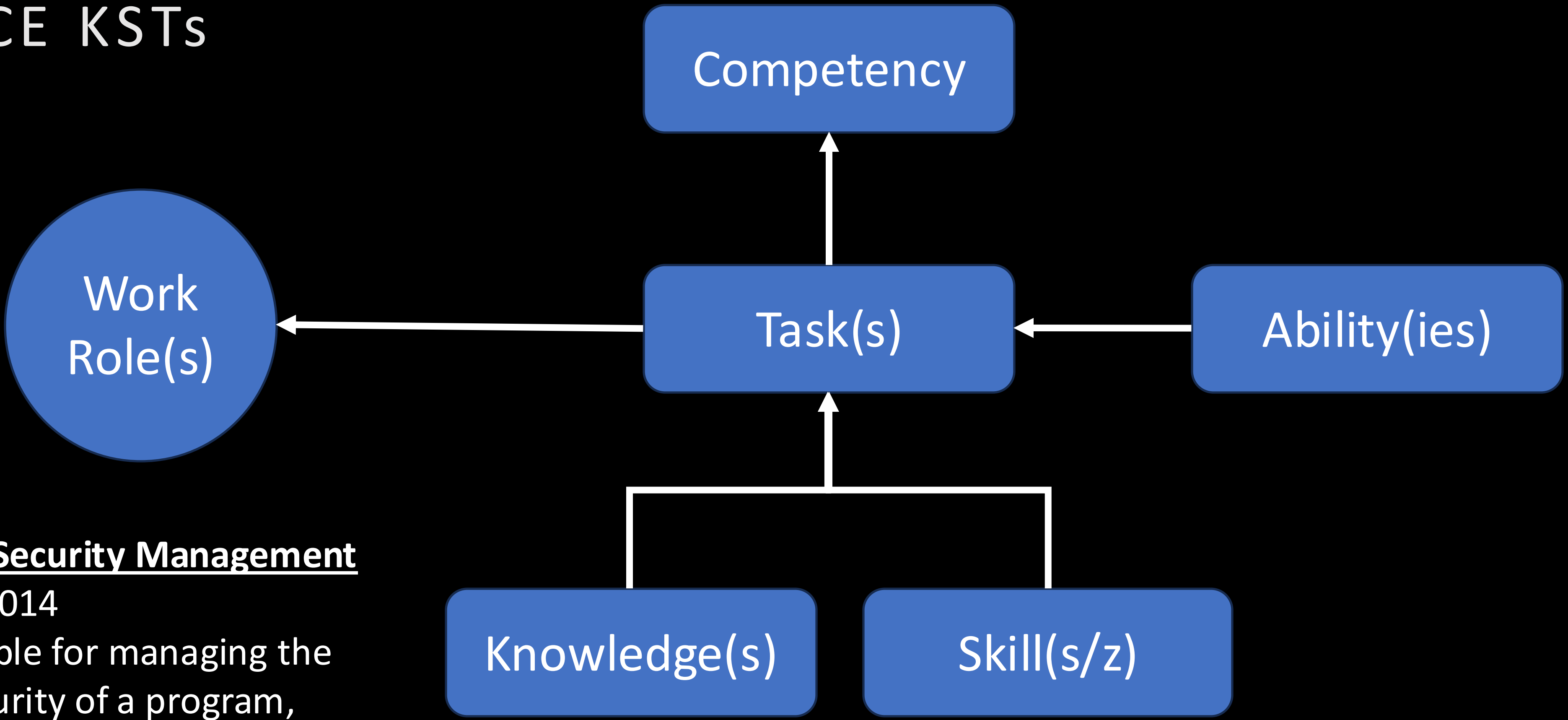
- Protection of Critical Infrastructure
- Complex and Evolving Threat Landscape
- Compliance with Regulations and Standards
- Risk Management
- Incident Response and Recovery
- Interdisciplinary Knowledge
- Innovation and Technological Advancements

NICE Workforce Framework for Cybersecurity (NICE Framework)

- Establishes a **standard approach and common language** for describing cybersecurity work and learner capabilities. The NICE Framework seeks to improve communication among stakeholders throughout the cybersecurity ecosystem about how to identify, recruit, develop, and retain talent.
- The NICE Framework includes the following components:
  - Work Role Categories (7)
  - Work Roles (52)
  - TKS Statements (2,200+)
  - Competency Areas (11)

V1.0

NICE KSTs



Systems Security Management

OG-WRL-014

Responsible for managing the cybersecurity of a program, organization, system, or enclave.

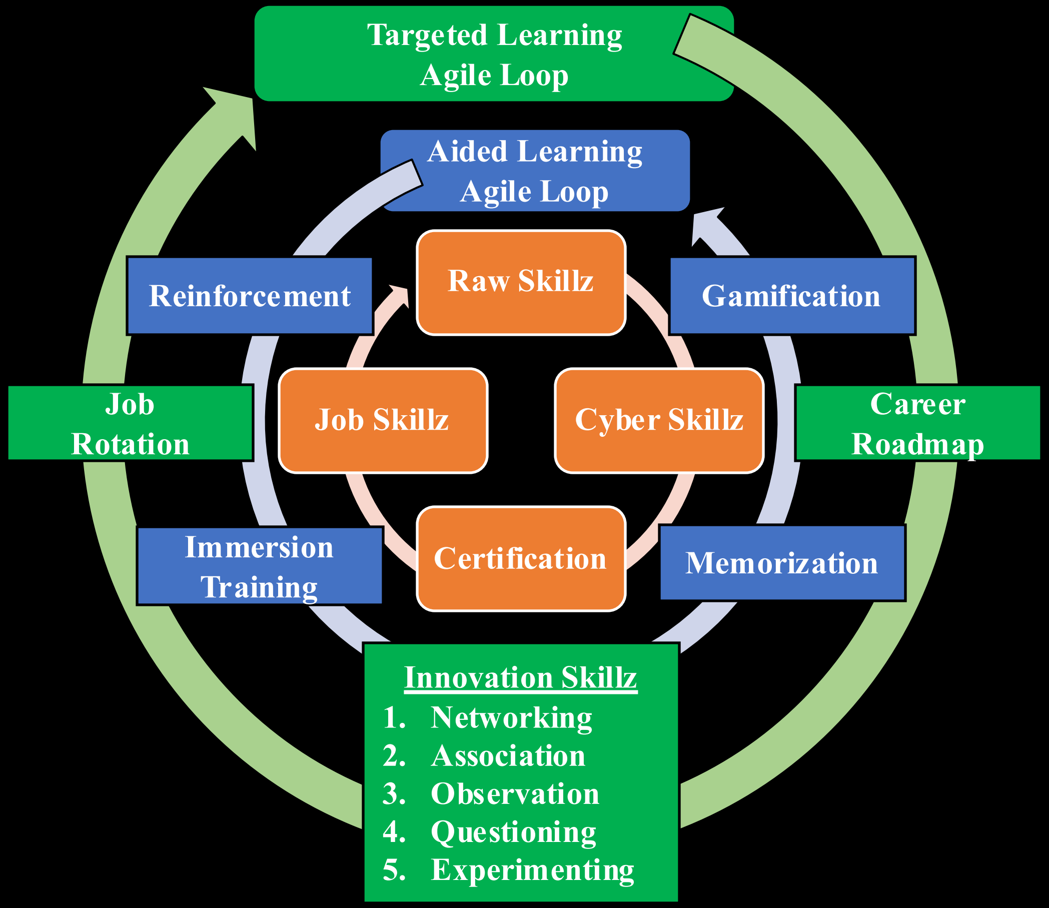
https://www.nist.gov/document/nice-framework-components-v200

V2.0

New Cyber KSTs since our course (some)…

K1288	Knowledge of OT cybersecurity compliance requirements and best practices
K1289	Knowledge of control system environment risks, threats, and vulnerabilities
K1292	Knowledge of OT cybersecurity risk tolerance levels
K1295	Knowledge of OT cybersecurity inspection and testing policies and procedures
K1297	Knowledge of OT safety systems
K1301	Knowledge of cyber incidents impacting OT
K1302	Knowledge of industry hazards
K1307	Knowledge of OT inventory principles and practices
K1308	Knowledge of OT network detection tools and techniques
K1309	Knowledge of OT protocols
S0921	Skill in performing telemetry analysis
S0942	Skill in performing system recovery for control system environments
S0946	Skill in interpreting OT network drawings
T2031	Identify gaps in OT network architecture
T2032	Assign security level targets to network zones for control systems
T2034	Design cybersecurity tools for OT systems

Agile Cybersecurity Training Loop showing learning relationships

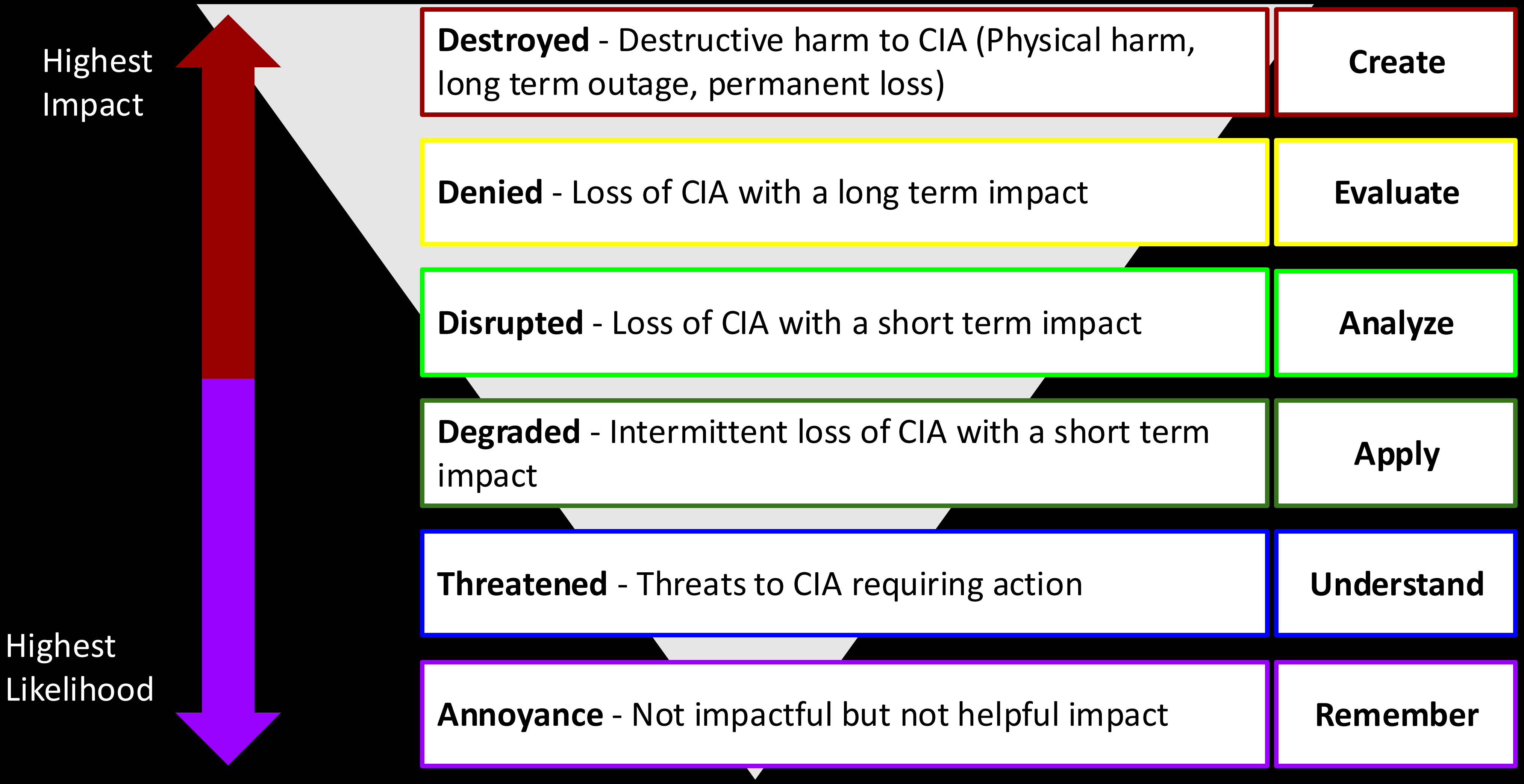


Inner Loop – Very specific, targeted aspects

Middle Loop – Learning techniques

Outer Loop – Long term planning

Inverted Security Risk Taxonomy.



Highest Impact

Destroyed - Destructive harm to CIA (Physical harm, long term outage, permanent loss)	**Create**
Denied - Loss of CIA with a long term impact	**Evaluate**
Disrupted - Loss of CIA with a short term impact	**Analyze**
Degraded - Intermittent loss of CIA with a short term impact	**Apply**
Threatened - Threats to CIA requiring action	**Understand**
Annoyance - Not impactful but not helpful impact	**Remember**

Highest Likelihood

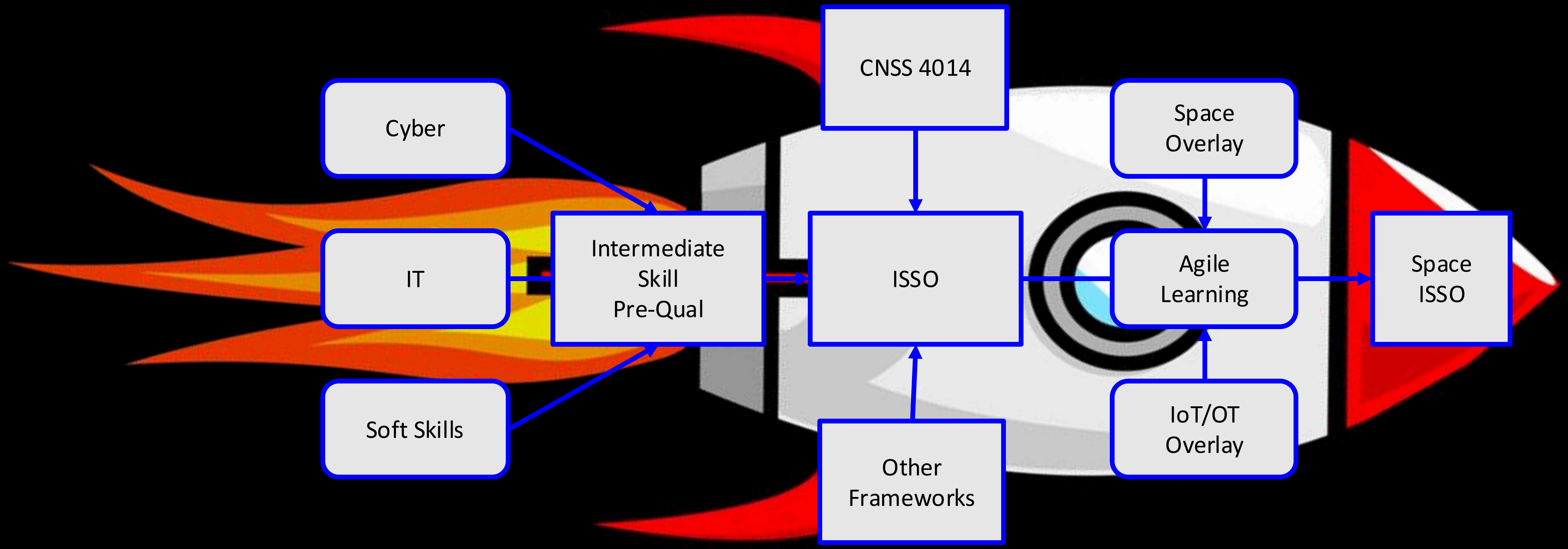
Gamification

02

Execution

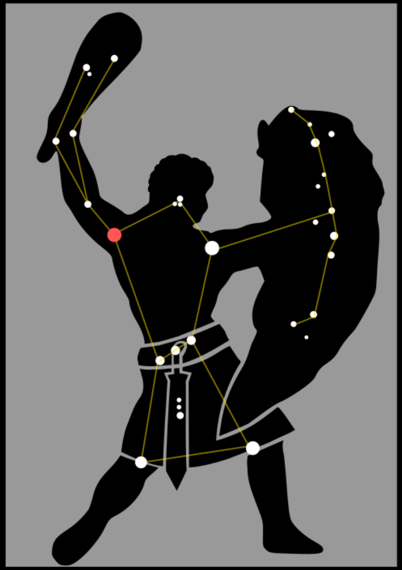
How we did it…

Space ISSO Design



Space ISSO Job Description Mapping

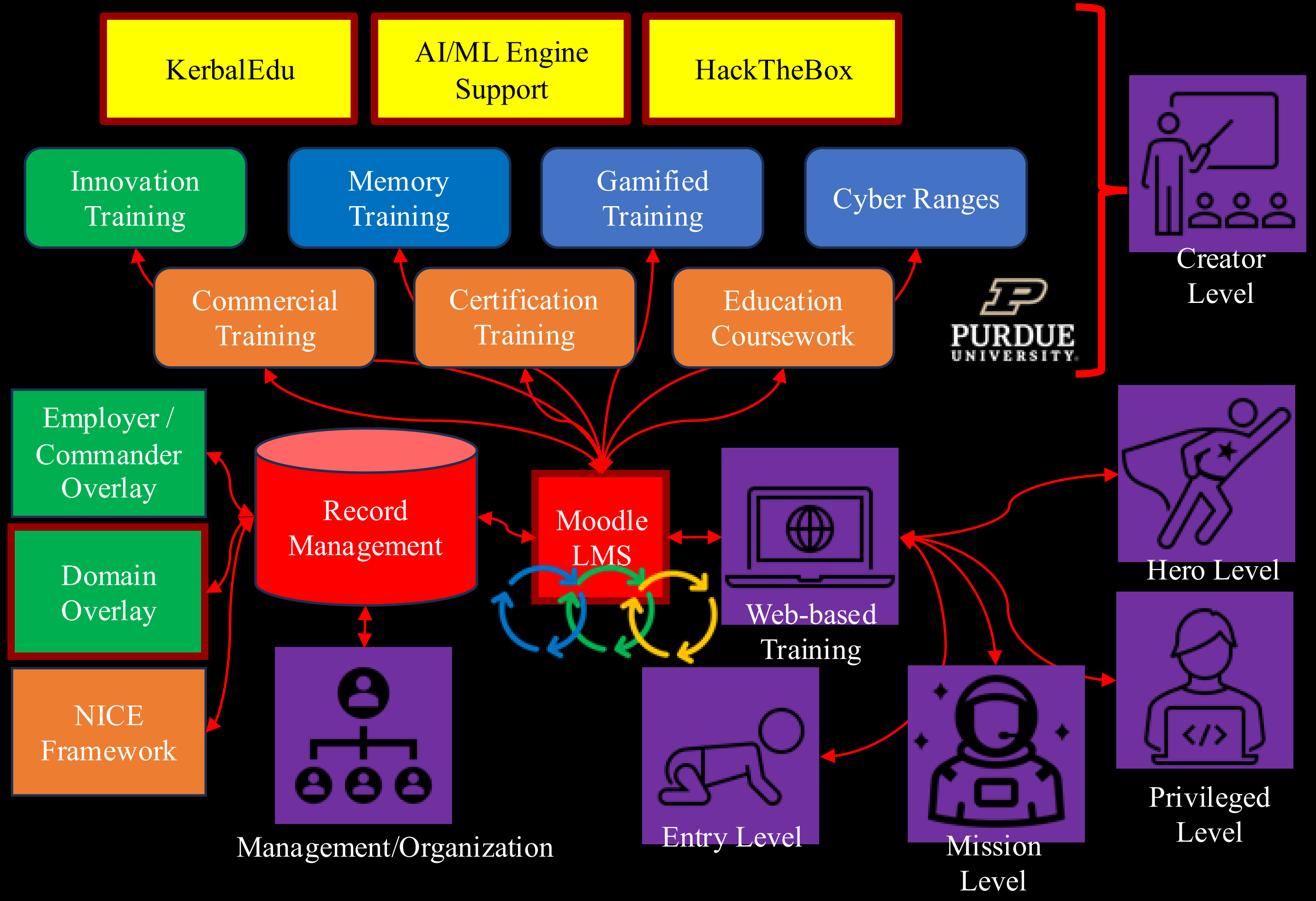
- Assist ISSM with **Incident Response actions**.
  - K0724 – Knowledge of incident response principles & practices
- Conducts independent, comprehensive management, operational, and technical **security control assessments**.
  - T1246 – Establish Security Assessment & Authorization processes
- Evaluate/Access functional areas for Risk Mitigation Strategies.
  - K1209 – Knowledge of risk mitigation principles and practices
- Good written and **interpersonal** skills.
  - ???
- **Manages** security-related **changes** to information systems and assesses the security impact of those changes.
  - ???



Space ISSO KSTs

- SpaceK0012. Familiarity with space situational awareness (SSA) principles
- SpaceS0012. TT&C system security hardening
- SpaceT0002. Develop security policies for satellite operations
- Soft K0016. Knowledge of persuasion techniques
- Soft S0025. Diplomacy
- Soft T0018. Communicate security risks to non-technical audiences
- ICS K0008: Knowledge of SCADA telemetry systems for satellite and spacecraft control
- ICS S0012: Proficiency in hardening RTOS used in spacecraft ICS
- ICS T0027: Conduct regular security audits of launch system ICS control networks

Agile, gamified learning framework showing tools that support different learning roles.



KerbalEdu

AI/ML Engine Support

HackTheBox

Innovation Training

Memory Training

Gamified Training

Cyber Ranges

Commercial Training

Certification Training

Education Coursework

PURDUE UNIVERSITY

Creator Level

Employer / Commander Overlay

Domain Overlay

NICE Framework

Record Management

Moodle LMS

Web-based Training

Hero Level

Privileged Level

Management/Organization

Entry Level

Mission Level

Schedule

Course	Day 1	Day 2	Day 3	Day 4	Day 5
Foundation	Role KSTs Agile Exam	Cyber 1 Space	Cyber 2 Soft Skills	Cyber 3 Systems Eng	Cyber 4 Intelligence Sprint Planning Sprint Demo
Intermediate	Security Architecture System Arch Exam	Config Mgmt Control Impl	Security Standards Create SSP	Risk Analysis Risk Assessment	Incident Response Sprint Planning Sprint Demo
Expert	CTF 1 Exam	CTF 2	CTF 3	CTF 4	CTF 5 Sprint Demo

Agile Learning Sprints User Stories

- Space User Story – As a Space ISSO trainee, I want to successfully launch a communication satellite into orbit using Kerbal Space Program so that I can demonstrate basic understanding of orbital mechanics and satellite deployment procedures.
- Soft Skills User Story – As a Space ISSO student in a breakout room, I want to participate in interactive security communication games so that I can improve my ability to explain technical concepts in accessible ways.
- Systems Engineering User Story – As a Space ISSO trainee, I want to analyze the ComSat Lx satellite, document its architecture, identify requirements, and implement a new capability using the Engineering V-Model so that I can demonstrate an understanding of space systems engineering processes.
- Intelligence Operations User Story – As an intelligence analyst trainee, I want to conduct rapid analysis of a current security incident and deliver a concise briefing so that I can demonstrate effective intelligence analysis and presentation skills.

CTF User Story

- CTF User Story - As A Space ISSO student I want to complete space-focused security challenges and demonstrate their relevance in KSP scenarios so that I can develop practical skills in identifying and mitigating space systems vulnerabilities.

- Students were to complete 5 Cyber Capture The Flag (CTF) challenges recommended from one of these platforms: HackTheBox, VulnHub, FITSEC Space Heroes, Ph0wn, or Hack-A-Sat. Afterward students demonstrate how the security concepts of the CTF apply to space systems by creating corresponding scenarios in Kerbal Space Program.

Exams

Exams were designed to be 2 hours long, 200 questions, and covered the breadth of KSTs.

Exams questions were multiple choice all having a single correct answer. They were not designed to be hard or for students to fail, but rather to demonstrate enough knowledge competency.

During Exam 1, a configuration error resulted in 300 questions rather than the intended 200. Despite this, participants demonstrated resilience and successfully completed the assessment without significant adverse effects. Exams were not proctored and were delivered via the MoodleCloud learning management system.

03

Results

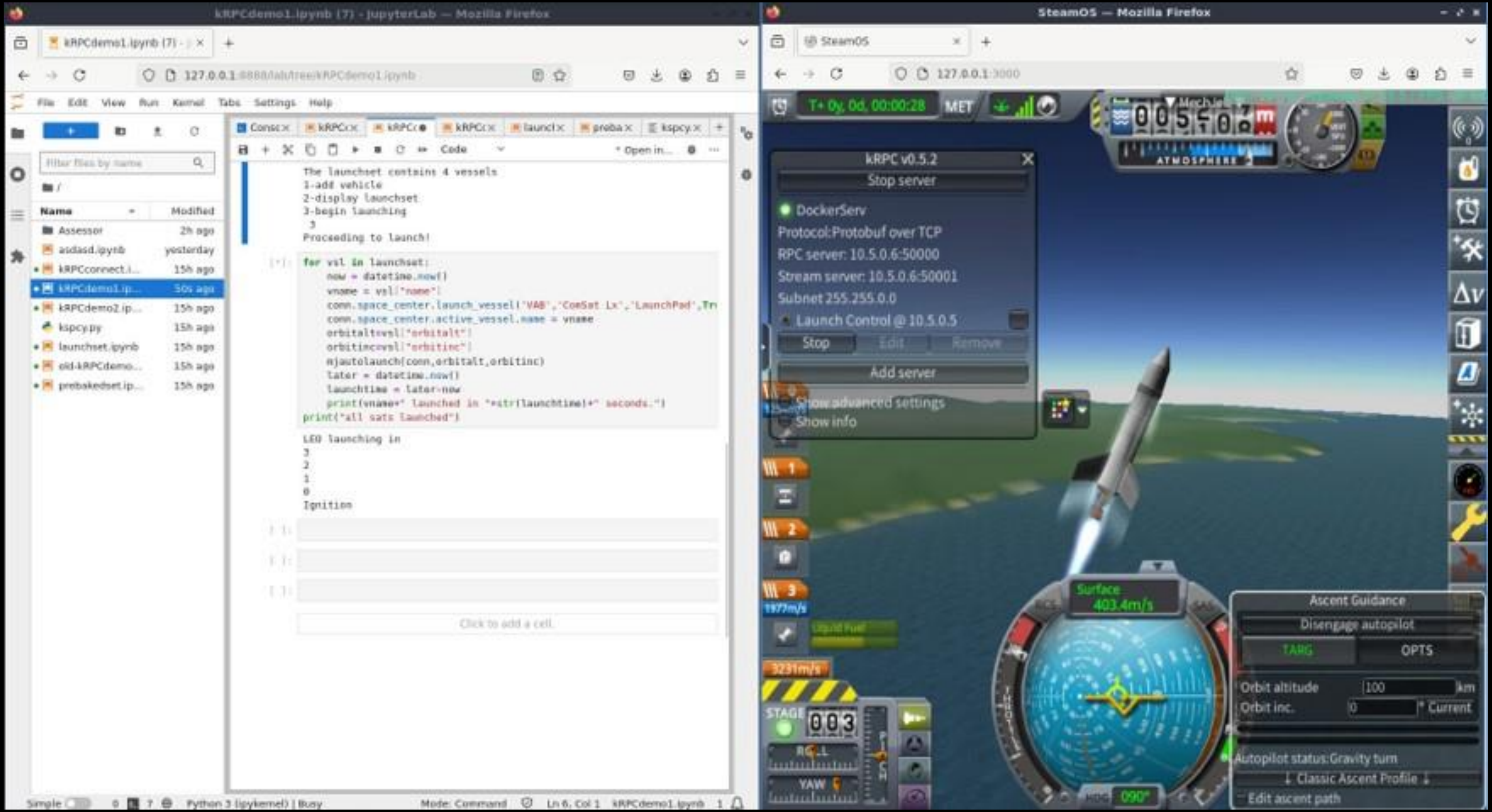
Why we did it…

QUOTE

> “It was going well until it exploded.”

Scott Manley

Student Innovation


kRPCdemo1.ipynb (7) - JupyterLab — Mozilla Firefox
127.0.0.1:8888/lab/tree/kRPCdemo1.ipynb
File Edit View Run Kernel Tabs Settings Help
Code
Open in...
SteamOS — Mozilla Firefox
127.0.0.1:3000
T+ 0y, 0d, 00:00:28
MET
ATMOSPHERE
STAGE
003
ROLL
YAW
Surface
403.4m/s
090°

Name	Modified
Assessor	2h ago
asdasd.ipynb	yesterday
kRPCconnect.i...	15h ago
kRPCdemo1.ip...	50s ago
kRPCdemo2.ip...	15h ago
kspcy.py	15h ago
launchset.ipynb	15h ago
old-kRPCdemo...	15h ago
prebakedset.ip...	15h ago

```
The launchset contains 4 vessels
1-add vehicle
2-display launchset
3-begin launching
 3
Proceeding to launch!
```

```
for vsl in launchset:
    now = datetime.now()
    vname = vsl["name"]
    conn.space_center.launch_vessel('VAB','ComSat Lx','LaunchPad',Tr
    conn.space_center.active_vessel.name = vname
    orbitalt=vsl["orbitalt"]
    orbitinc=vsl["orbitinc"]
    mjautolaunch(conn,orbitalt,orbitinc)
    later = datetime.now()
    launchtime = later-now
    print(vname+" launched in "+str(launchtime)+" seconds.")
print("all sats launched")
```

```
LEO launching in
3
2
1
0
Ignition
```

Click to add a cell.

Python 3 (ipykernel) | Busy   Mode: Command   Ln 6, Col 1   kRPCdemo1.ipynb

kRPC v0.5.2

Stop server

● DockerServ

Protocol:Protobuf over TCP

RPC server: 10.5.0.6:50000

Stream server: 10.5.0.6:50001

Subnet 255.255.0.0

Launch Control @ 10.5.0.5

Stop Edit Remove

Add server

Show advanced settings

Show info

Ascent Guidance

Disengage autopilot

TARG OPTS

Orbit altitude 100 km

Orbit inc. 0 ° Current

Autopilot status:Gravity turn

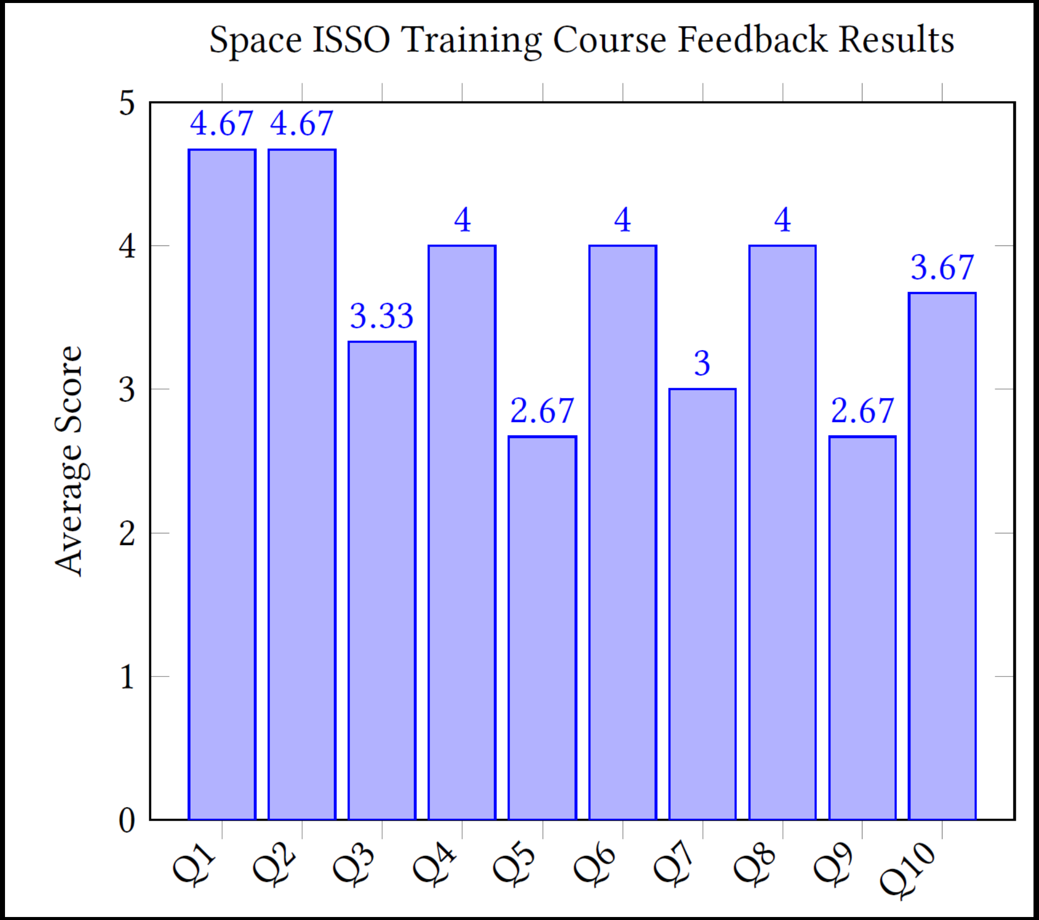
↓ Classic Ascent Profile ↓

Edit ascent path

SPACE ISSO
ESTD
2024

Qualitative and Quantitative Feedback

Q1: I would still like to play training games like this even if I am not being graded or paid.
Q2: Did you have a Significant Learning Experience?
Q3: How knowledgeable were you in the material going into the course?
Q4: How would you rate the overall effectiveness of the training?
Q5: Rate your knowledge required of Space ISSO before the course
Q6: Rate your knowledge required of Space ISSO now after the course
Q7: Rate your skills required of Space ISSO before the course
Q8: Rate your skills required of Space ISSO now after the course
Q9: Rate your ability to perform tasks required of Space ISSO before the course
Q10: Rate your ability to perform tasks required of Space ISSO now after the course



Student Feedback

What was the most valuable aspect of this cybersecurity training?

- "The integration of real world examples and fundamentals allowed for me to shape more advanced concepts into my own pre-existing mental models, accelerating my learning."

What part of this course was most helpful to your learning?

- "Opening up non-traditional forms of learning that enable students who do not benefit from traditional lecture-based learning."

Any other comments?

- "I have learned more in the last few weeks/months with project and game-oriented learning than in years of traditional learning methods, attempting to study Cybersecurity and Space topics via lecture."

Conclusion

1) test scores improving from 73.9% to 92.1% and self-reported capability ratings increased across all areas.

2) the inverted security risk taxonomy proved valuable in structuring training priorities.

3) our integration of domain-specific KSTs through the expanded NICE Framework successfully addressed the unique requirements of space cybersecurity.

Interest Form

THANK YOU

Contact Info
info@codetalkerseng.com
www.codetalkerseng.com

The look you get from the Space Force EO after making an alien joke

References

[1] 2024. Backdoors & Breaches. https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

[2] 2024. Principles behind theAgile Manifesto. https://agilemanifesto.org/principles.html

[3] 2025. The Best Cybersecurity Memes. https://www.redsentry.com/blog/thebest-cybersecurity-memes

[4] 2025. Claude AI. https://claude.ai/

[5] 2025. Hack The Box. https://www.hackthebox.com

[6] 2025. KerbalEdu. https://kerbaledu.kerbalspaceprogram.com/

[7] 2025. KerbalRPC. https://github.com/krpc/krpc original-date: 2014-02-10T23:36:25Z.

[8] 2025. KSP-RO/RealAntennas. https://github.com/KSP-RO/RealAntennasoriginal-date: 2024-05-05T11:11:40Z.

[9] 2025. MoodleCloud. https://www.moodlecloud.com/

[10] 2025. MuMech/MechJeb2. https://github.com/MuMech/MechJeb2 original-date:2013-04-03T02:51:41Z.

[11] 2025. OpenRMF - An Open Source Risk Management Framework tool. https://www.openrmf.io/

[12] 2025. When Budgets Tight, Training Often Gets Cut - But It's the Solution We Can't Afford to Lose. https://www.ifpti.org/news/when-budgets-tight-trainingoften-gets-cut-but-its-the-solution-we-cant-afford-to-lose

[13] Kimberly C. Burke. 2024. Forceful De-escalation and Organizational Inertia: Identifying Novel Justifications for Entrenched Police Violence. Critical Criminology (Sept. 2024). doi:10.1007/s10612-024-09797-x

[14] Yu-kai Chou and Erik von Mechelen. 2016. Actionable gamification: beyond points, badges, and leaderboards. Octalysis Media, Fremont, CA.

[15] CNSS. 2004. CNSSI 4014 - NATIONAL INFORMATION ASSURANCE TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY OFFICERS. https://www.cnss.gov/cnss/index.cfm

[16] CNSS. 2022. CNSSI 4009 - Committee on National Security Systems (CNSS) Glossary. https://www.cnss.gov/cnss/index.cfm

[17] Jeff Dalton. 2019. Great Big Agile: An OS for Agile Leaders. Apress, Berkeley, CA. doi:10.1007/978-1-4842-4206-3

[18] L. Dee Fink. 2013. Creating significant learning experiences: an integrated approach to designing college courses (revised and updated edition ed.). Jossey-Bass, San Francisco.

[19] Panos Fitsilis, Vyron Damasiotis, and Evangeli Boti. 2023. Agile Learning: An Innovative Curriculum for Educators. doi:10.32388/RQX9T9.3

[20] Jeff Henry. 2025. Probability Model vs Competency Model of Church Security Training.

[21] Joint Task Force Transformation Initiative. 2012. Guide for conducting risk assessments. Technical Report NIST SP 800-30r1. National Institute of Standards and Technology, Gaithersburg,MD. NIST SP 800-30r1 pages. doi:10.6028/NIST.SP.800-30r1

[22] Naurin Farooq Khan, Naveed Ikram, Hajra Murtaza, and Mehwish Javed. 2023. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. Computers & Security 125 (Feb. 2023), 103049. doi:10.1016/j.cose.2022.103049

[23] David R. Krathwohl. 1974. Taxonomy of educational objectives: the classification of educational goals. David McKay Company, New York. OCLC: 1517203.

[24] Joakim Kävrestad, Jana Rambusch, and Marcus Nohlberg. 2024. Design principles for cognitively accessible cybersecurity training. Computers & Security 137 (Feb. 2024), 103630. doi:10.1016/j.cose.2023.103630

[25] linuxgurugamer. 2023. linuxgurugamer/KerbalGPS. https://github.com/linuxgurugamer/KerbalGPS original-date: 2018-08-11T23:48:22Z.

[26] NICE. 2024. NICE Workforce Framework for Cybersecurity (NICE Framework) | NICCS. https://niccs.cisa.gov/workforce-development/nice-framework

[27] NIH. 2017. Competencies Proficiency Scale. https://hr.nih.gov/working-nih/competencies/competencies-proficiency-scale

[28] OPM. [n. d.]. Proficiency Levels for Leadership Competencies. https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/proficiency-levels-for-leadership-competencies.pdf

[29] Margarita Ortiz-Rojas, Katherine Chiluiza, and Martin Valcke. 2019. Gamification through leaderboards: An empirical study in engineering education. Computer Applications in Engineering Education 27, 4 (July 2019), 777–788. doi:10.1002/cae.12116

[30] Rodney Petersen, Danielle Santos, Matthew C. Smith, Karen A. Wetzel, and Greg Witte. 2020. Workforce Framework for Cybersecurity (NICE Framework). Technical Report. National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-181r1

[31] Carl Poole. 2021. Evolving Satellite Control Challenges: The - ProQuest. https://www.proquest.com/docview/2555180379

[32] James Prather, Paul Denny, Juho Leinonen, Brett A. Becker, Ibrahim Albluwi, Michelle Craig, Hieke Keuning, Natalie Kiesler, Tobias Kohn, Andrew Luxton-Reilly, Stephen MacNeil, Andrew Petersen, Raymond Pettit, Brent N. Reeves, and Jaromir Savelka. 2023. The Robots Are Here: Navigating the Generative AI Revolution in Computing Education. In Proceedings of the 2023 Working Group Reports on Innovation and Technology in Computer Science Education. ACM, Turku Finland, 108–159. doi:10.1145/3623762.3633499

[33] Carlos Roque, Gareth Moodley, and Sayonnha Mandal. 2024. Cybersafe: Gamifying Cybersecurity Training with a Training App. International Conference on Cyber Warfare and Security 19, 1 (March 2024), 299–307. doi:10.34190/iccws.19.1.2198

[34] KarenWetzel. 2021. NICE Framework Competencies: Moving from Concept to Implementation Workshop Report. https://www.nist.gov/system/files/documents/2021/06/09/NICE%20Framework%20Competencies%20Workshop%20Report.pdf

[35] Sierra Adare-Tasiwoopa ápi and Nathan Silva. 2023. Gamification in Higher Education: A How-To Instructional Guide. Routledge, New York. doi:10.4324/9781003444954