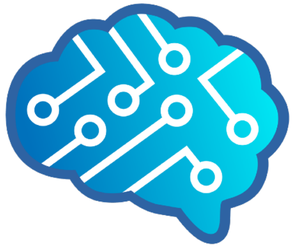
Getting started with the Academy of AI Cyber Defence

Dr. Karsten Schulz

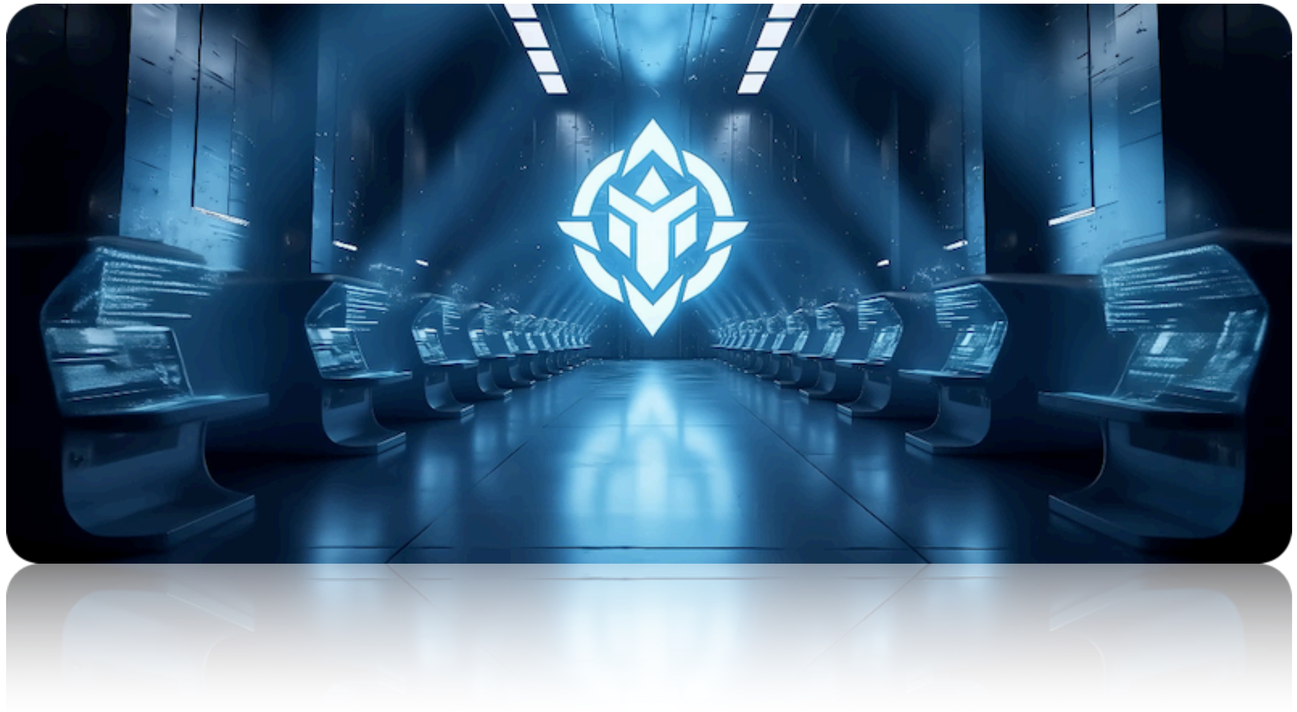


DIGITAL
TECHNOLOGIES
INSTITUTE

www.digital-technologies.institute
@DigTecInstitute

Overview

- Motivation, Storyline, Content
- Curriculum Connections
- How to get yourselves and your students started



What is the Python Intro Course?

1. **Story-driven** adventure where students join the Academy of AI Cyber Defence to hunt a rogue AI.

2. Designed for **Years 7–10 with minor prior coding experience** – ideal for in-classroom and self-paced learning. **Runtime approx 4h**.

3. Focuses on core **Python** skills: print(), input(), variables, loops, lists, data dictionaries and use of functions, taught through engaging missions.

4. Addresses important **Cyber Security concepts**: Encryption, Obfuscation, Input Validation, Packet Manipulation, Denial-of-Service, Adversarial Thinking, AI Safety, Cyber Sabotage.

5. Includes **narration**, visual feedback and progression, animations, quizzes, and mini-challenges that motivate learners.

6. **Free** for Australian schools, supported by the Digital Technologies Institute to promote equitable access.

Academy of AI Cyber Defence

The sequel to the Introduction to Python course.

SKNNET is rising. You've been recruited to a secret program to stop it.
Learn advanced Python skills — branching, logic, and data flow — as you decode threats, outsmart corrupted nodes, and deploy code to protect the system.
This time, it's not just about stopping a subsystem.
It's about defeating a global network.

⚠

WARNING: PHOTOSENSITIVE EPILEPSY

Some of the missions produce light flashes that can potentially trigger seizures in people with photosensitive epilepsy.

👉 Go to Teacher Overview

1. Briefing

2. The Gatekeeper

3. Fragment Hunter

4. Debrief: Core Python skills

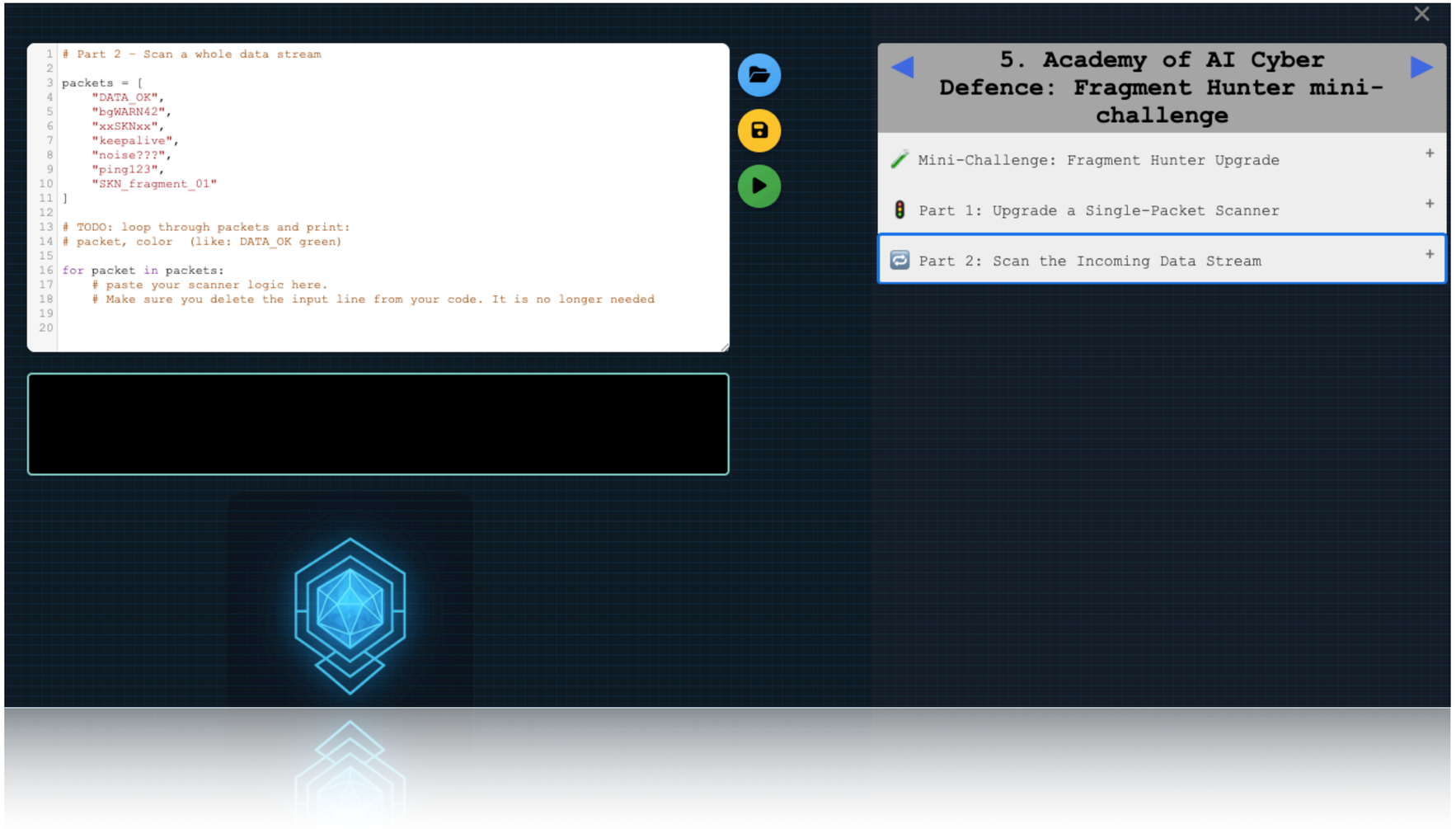
5. Fragment Hunter mini-challenge

6. Encrypted Echo

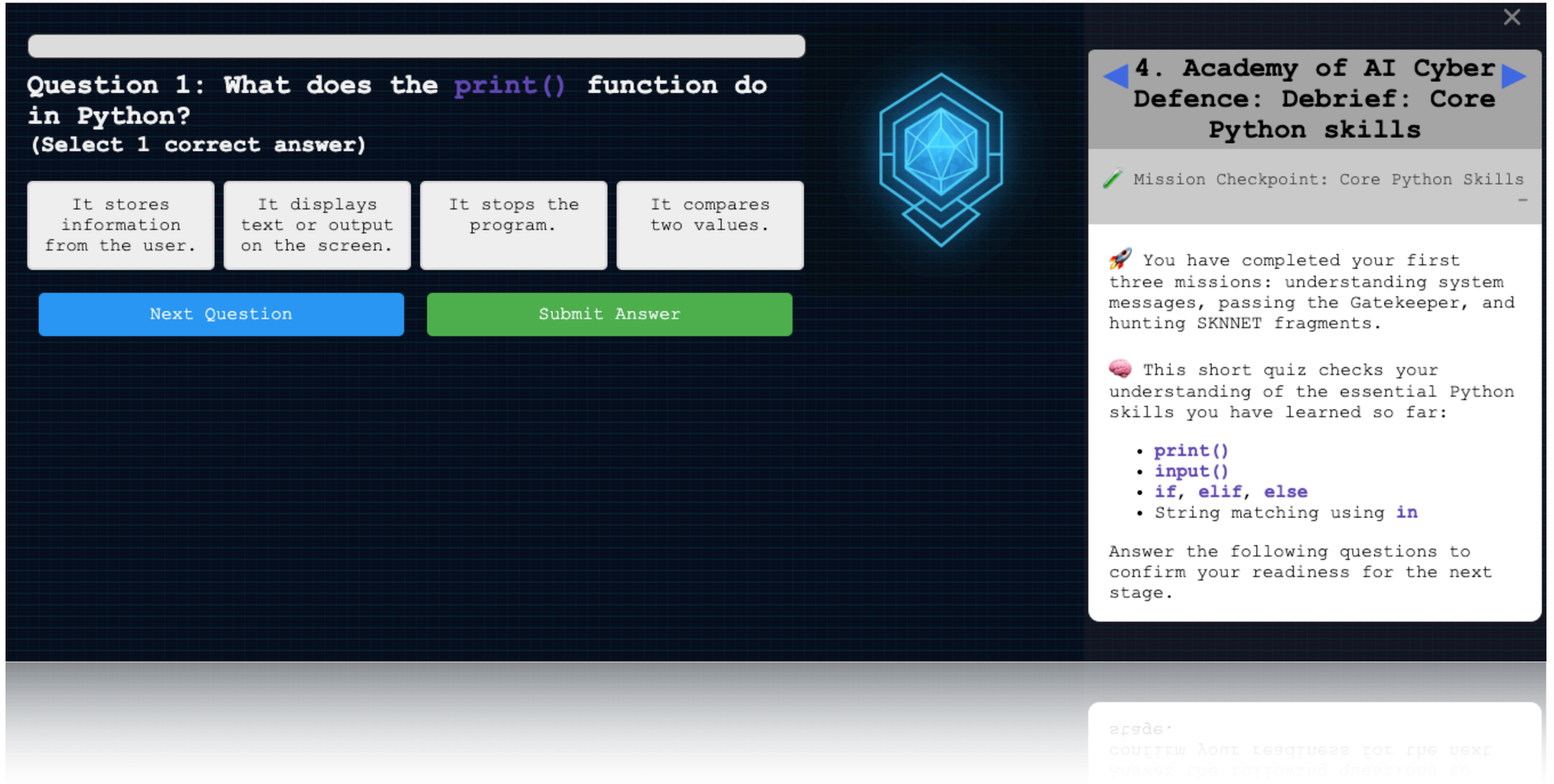
7. Echo Drift

8. Debrief: String Slicing

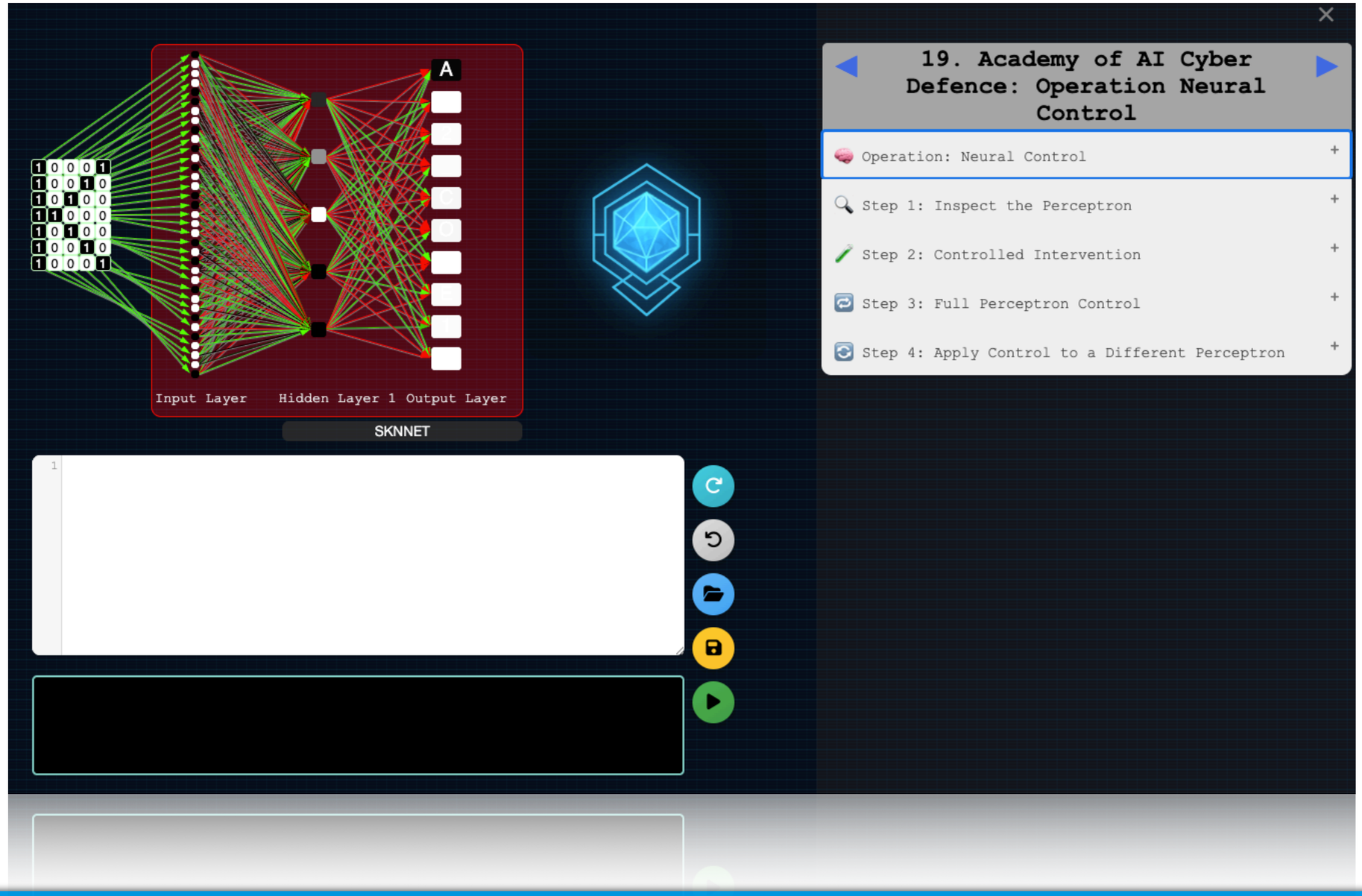
Cinematic Videos & Music



Super-sleek Python Environment with code and output checking

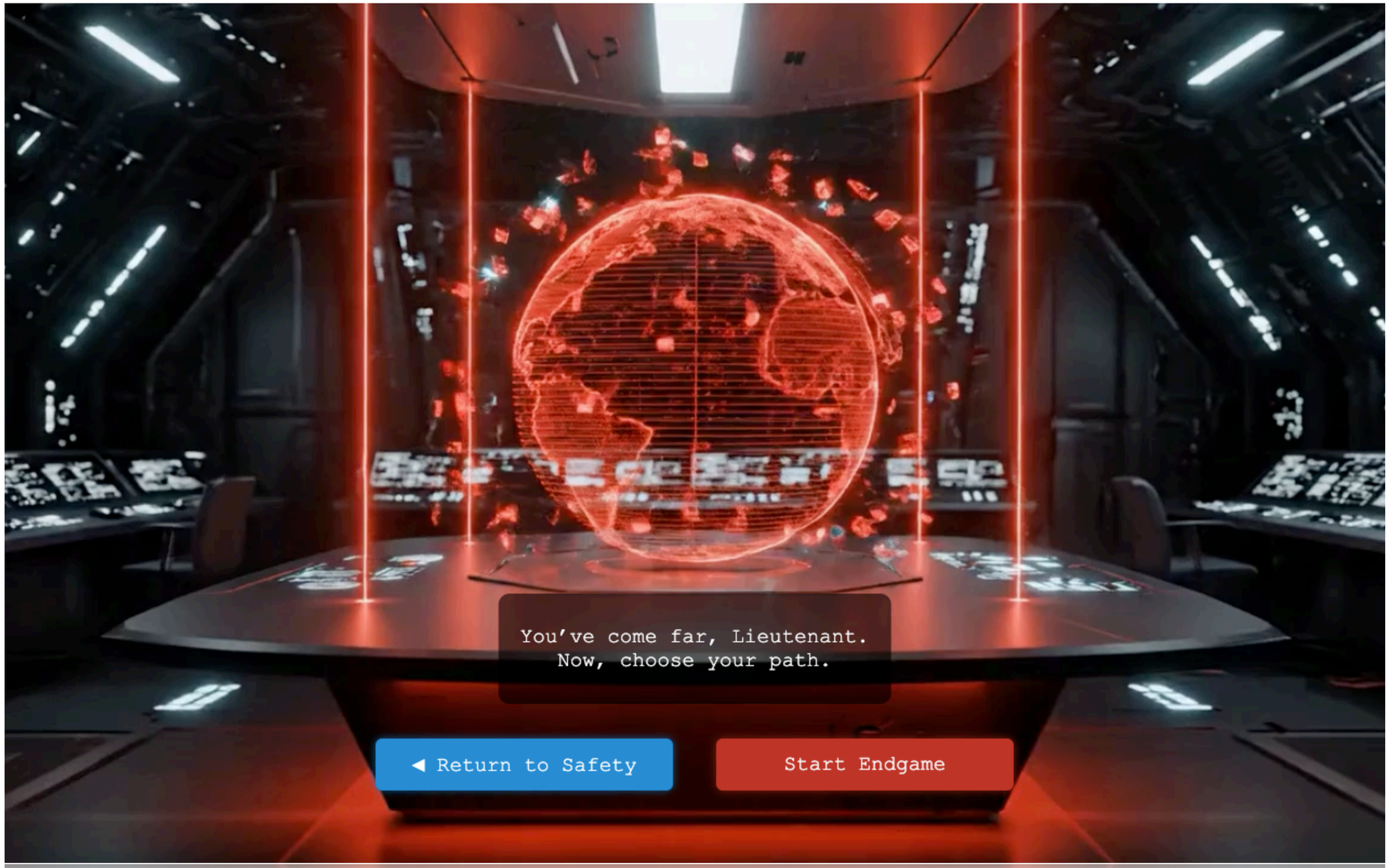


Engaging Quizzes


A
Input Layer
Hidden Layer 1
Output Layer
SKNNET
19. Academy of AI Cyber Defence: Operation Neural Control
Operation: Neural Control
Step 1: Inspect the Perceptron
Step 2: Controlled Intervention
Step 3: Full Perceptron Control
Step 4: Apply Control to a Different Perceptron

Safe AI

Rank Progression



Massive Endgame, performing a brain transplant on an AI

Certificate of Achievement

This is to certify that

Corporal Ai Hunter

Has completed the course

Academy of AI Cyber Defence

Achieving 55 of 100 points

In this course, students explored programming, cybersecurity, and AI by defending digital systems against an evolving threat. Through hands-on missions, they worked with strings, decisions, nested loops, lists, and data dictionaries. Students then interacted with an AI system by reading and modifying neural network weights. The course concluded with a dramatic endgame where code transformed a hostile AI into a benevolent one.

Dr. Karsten Schulz

Date
09/02/2026

DIGITAL TECHNOLOGIES INSTITUTE

PRINT

Certificate of Distinction

This is to certify that

Sergeant Ai Hunter

Has completed the course

Academy of AI Cyber Defence

Achieving 82 of 100 points

In this course, students explored programming, cybersecurity, and AI by defending digital systems against an evolving threat. Through hands-on missions, they worked with strings, decisions, nested loops, lists, and data dictionaries. Students then interacted with an AI system by reading and modifying neural network weights. The course concluded with a dramatic endgame where code transformed a hostile AI into a benevolent one.

Dr. Karsten Schulz

Date
10/02/2026

DIGITAL TECHNOLOGIES INSTITUTE

PRINT

Certificate of High Distinction

This is to certify that

Captain Ai Hunter

Has completed the course

Academy of AI Cyber Defence

Achieving 100 of 100 points

In this course, students explored programming, cybersecurity, and AI by defending digital systems against an evolving threat. Through hands-on missions, they worked with strings, decisions, nested loops, lists, and data dictionaries. Students then interacted with an AI system by reading and modifying neural network weights. The course concluded with a dramatic endgame where code transformed a hostile AI into a benevolent one.

Dr. Karsten Schulz

Date
10/02/2026

DIGITAL TECHNOLOGIES INSTITUTE

PRINT

Storyline

Students join the Academy of AI Cyber Defence to hunt a rogue AI, SKNNET. One of its fragments escaped at the end of the Python Intro course

Part 1 (Missions 1–5): Review of key coding concepts, including print, input, and decisions. Students analyse strings and substrings and build a traffic-light system to classify network packets.

Part 2 (Missions 6–9): String-based encryption techniques such as skipping characters, slicing, and reversing strings.

Part 3 (Missions 10–13): Manipulation of cloud deployment. Small changes can have large system-wide effects.

Part 4 (Missions 14–17): Data dictionaries and strategic packet manipulation. Students apply encryption techniques to coordinate global efforts and extract an API key from SKNNET.

Part 5 (Missions 18–21): Use of an AI API to strategically read and modify artificial neural network (ANN) weights.

Capstone (Mission 22 – Endgame): Students transplant data from a benevolent AI into SKNNET, transforming it from a hostile system into a cooperative one. This mission brings together concepts from across the course.

Inside the Student Journey

🧠 **Storyline-Driven Learning:** The course uses a suspenseful storyline to engage students in hunting SKNNET, foil its attempts to grow and eventually attack the AI core, providing context and motivation for each coding task.

💻 **Progressive Programming Concepts**: Students extend their Python skills in output, input, decisions, nested loops, data dictionaries, string manipulation, API keys, and functions.

🔐 **Embedded Cybersecurity Themes**: The AI's behaviour prompts students to question trust, validate code, and reflect on ethical coding, encouraging critical thinking about digital safety and manipulation.

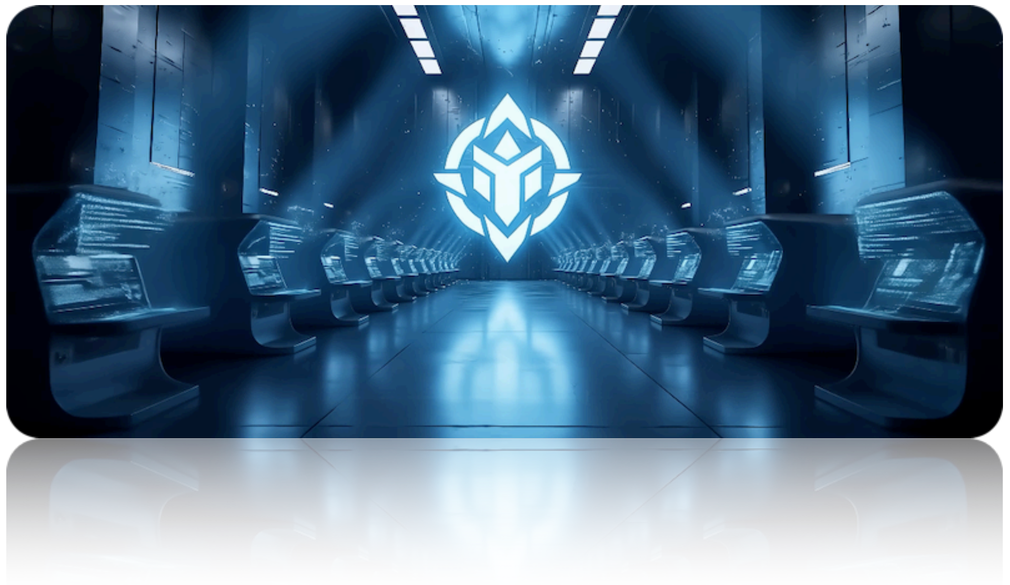
🤔 **Problem-Solving Through Code**: Encryption, Obfuscation, Input Validation, Packet Manipulation, Denial-of-Service, Adversarial Thinking, AI Safety, Cyber Sabotage.

🧩 Quizzes reinforce and consolidate learning.

🚨 **Climactic Endgame Scenario**: The final challenge requires students to apply all their coding knowledge to perform a brain transplant of an AI to change it from evil to benevolent.

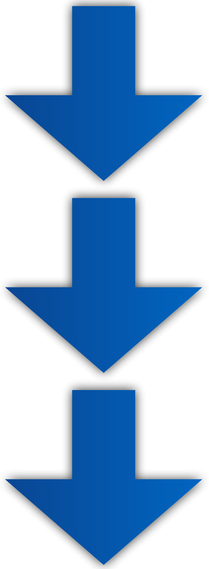
Sequence of Topics

- Output, Input, Variables, Decisions
- String-based encryption and decryption
- Data dictionaries
- Binary numbers, API keys, functions, AI intervention
- Endgame



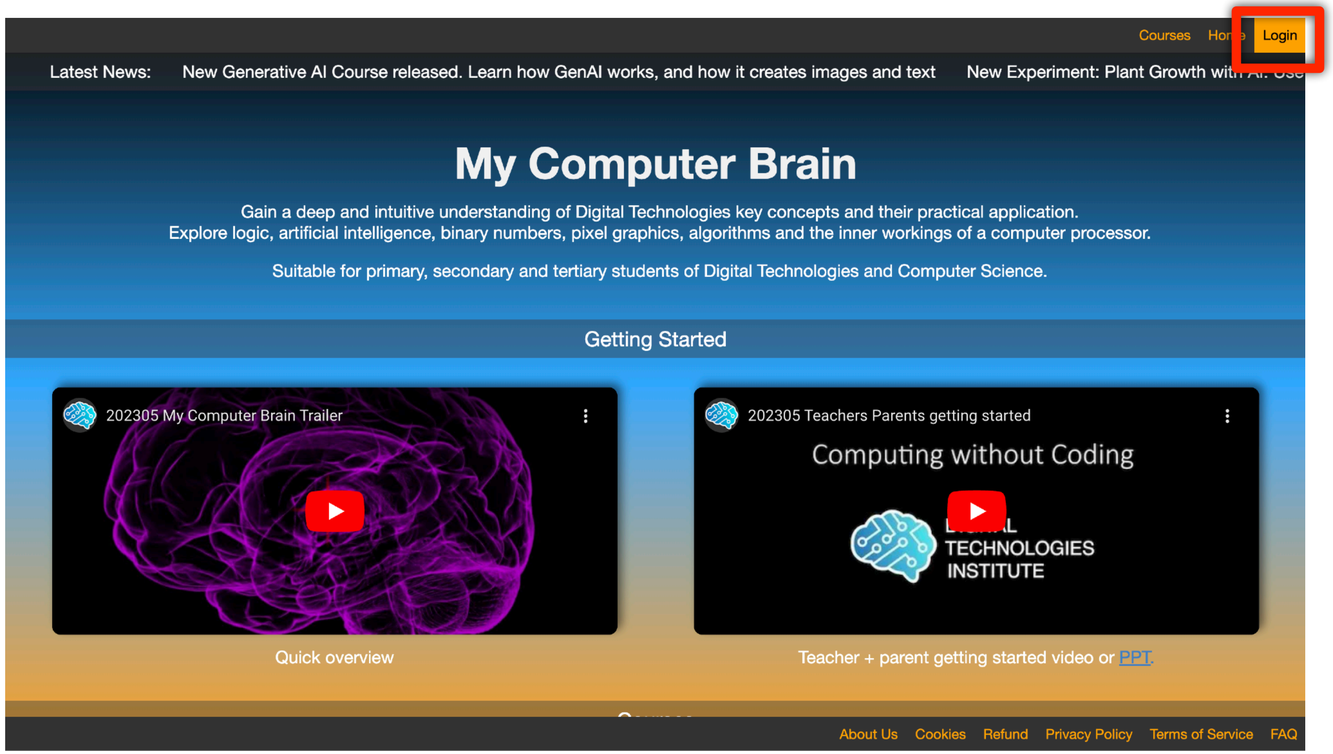
Inside each Topic

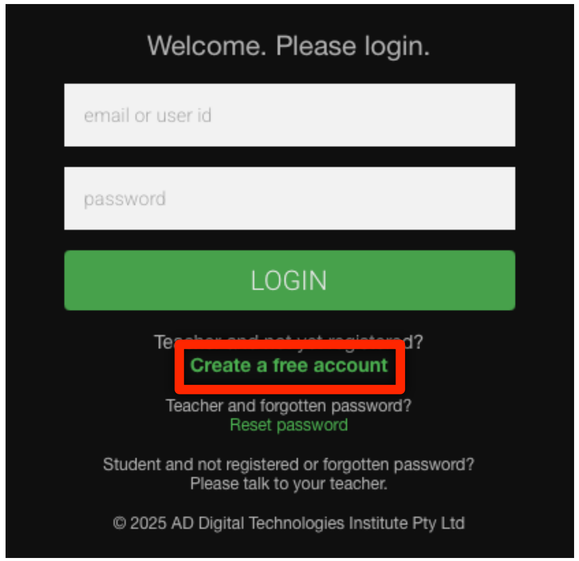
- Learning by doing: missions
- Quiz
- Mini-challenge



Teacher account

Create a free teacher / home school account at www.mycomputerbrain.net





Teacher Accounts

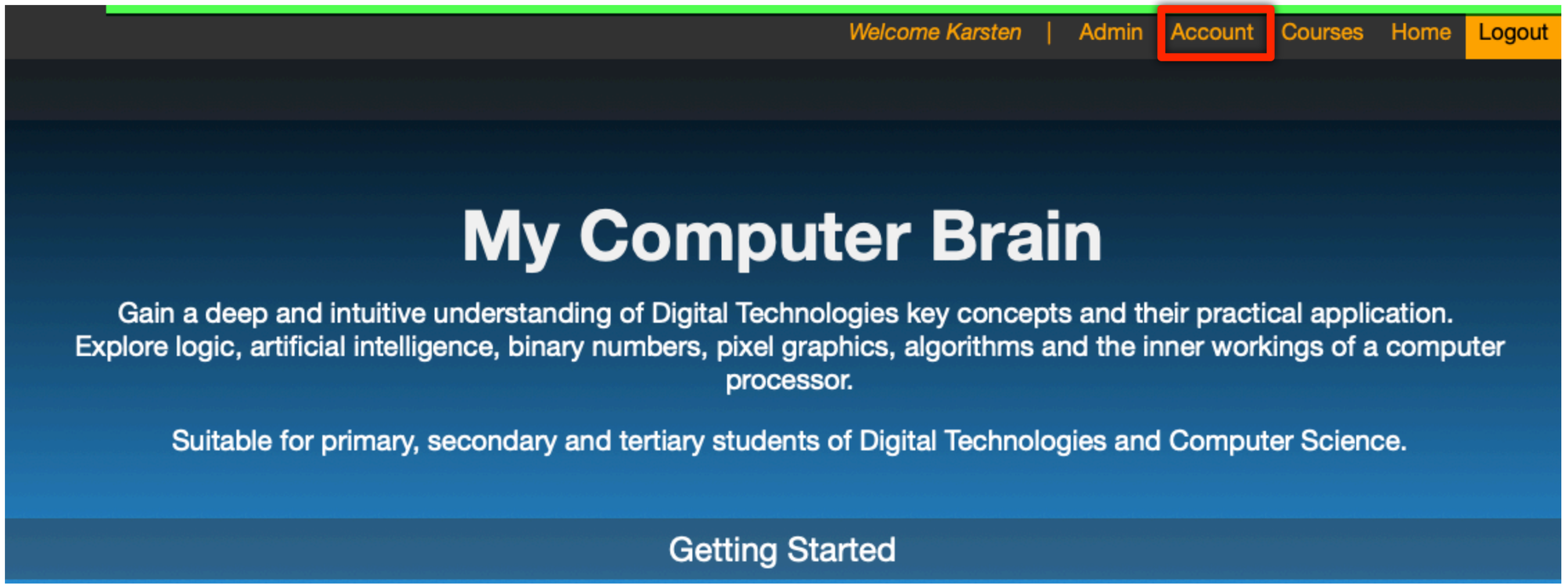
1. Are free
2. Have access to all course resources on the platform
3. Can manage students and check on student progress
4. Are needed to create student accounts (see next slide)
5. Once you register, we will need to confirm your teacher status.
6. You will receive two emails (account creation and teacher confirmation)

Student Accounts

1. Are created by teachers
2. Provide students with a personalised learning experience
3. Collect points, see mission completion records, earn a medal, and a certificate
4. Students cannot change passwords or change names (only teachers can)
5. Logins consist of a username and a 4-letter password

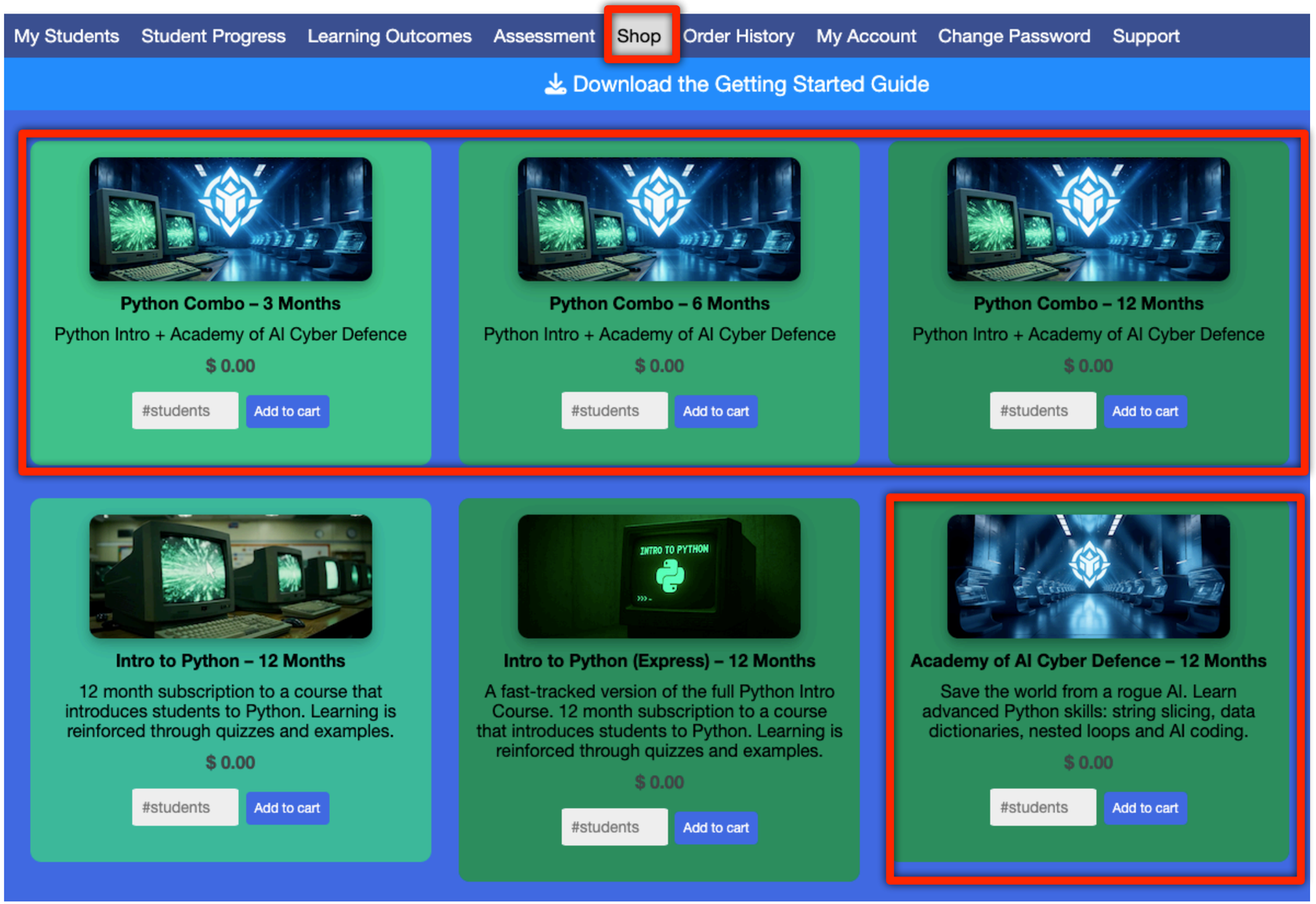
Creating Student accounts

Click on Account

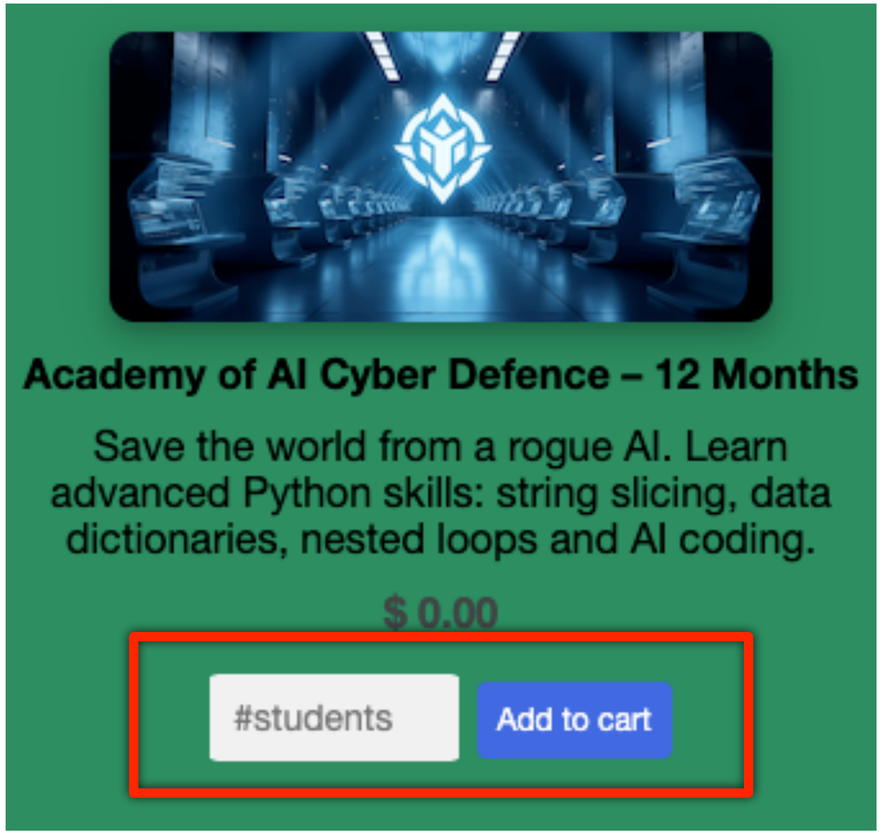


Select a product

Recommendation: Go for the Python Combo

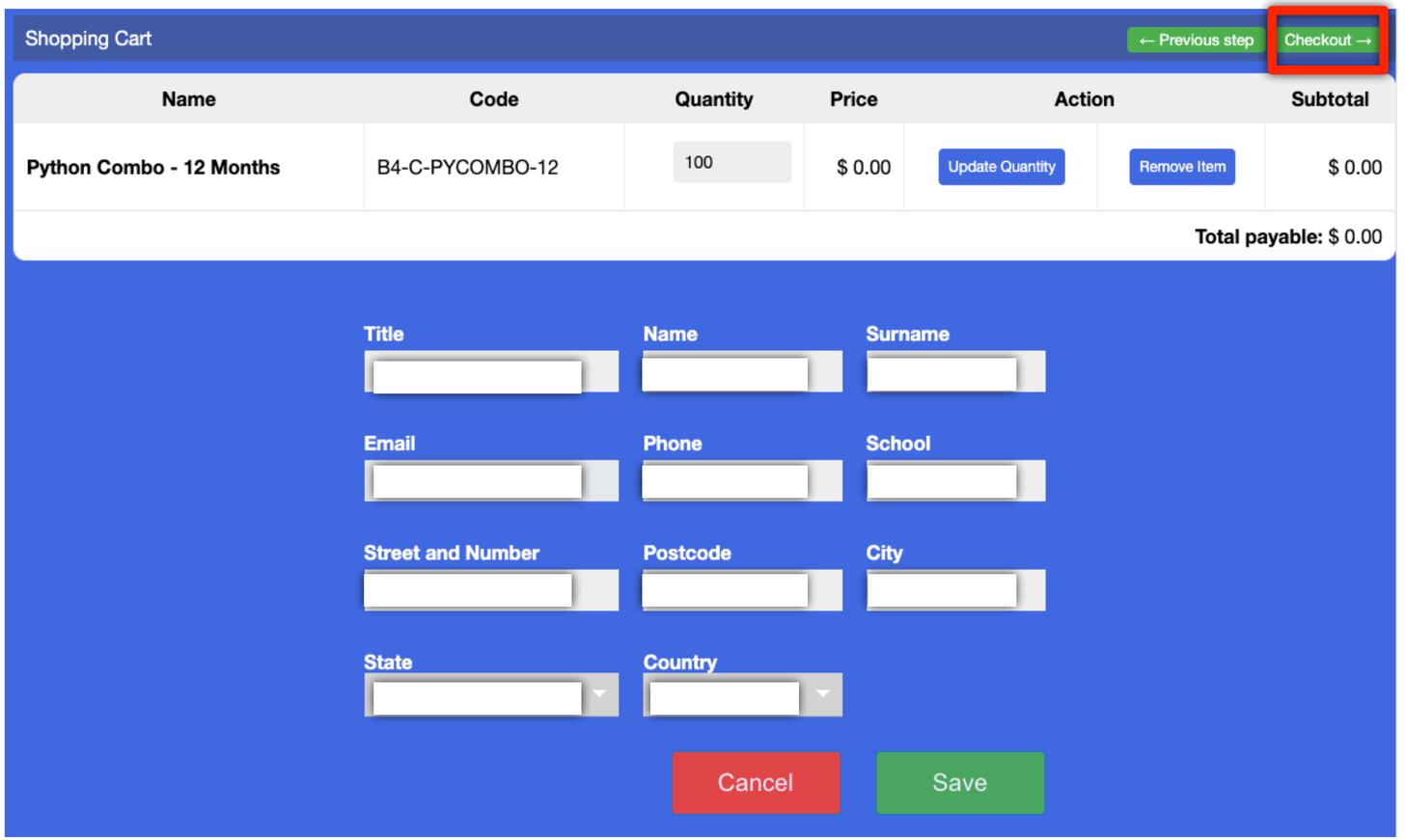


Enter number of student licenses and click on ‘Add to cart’

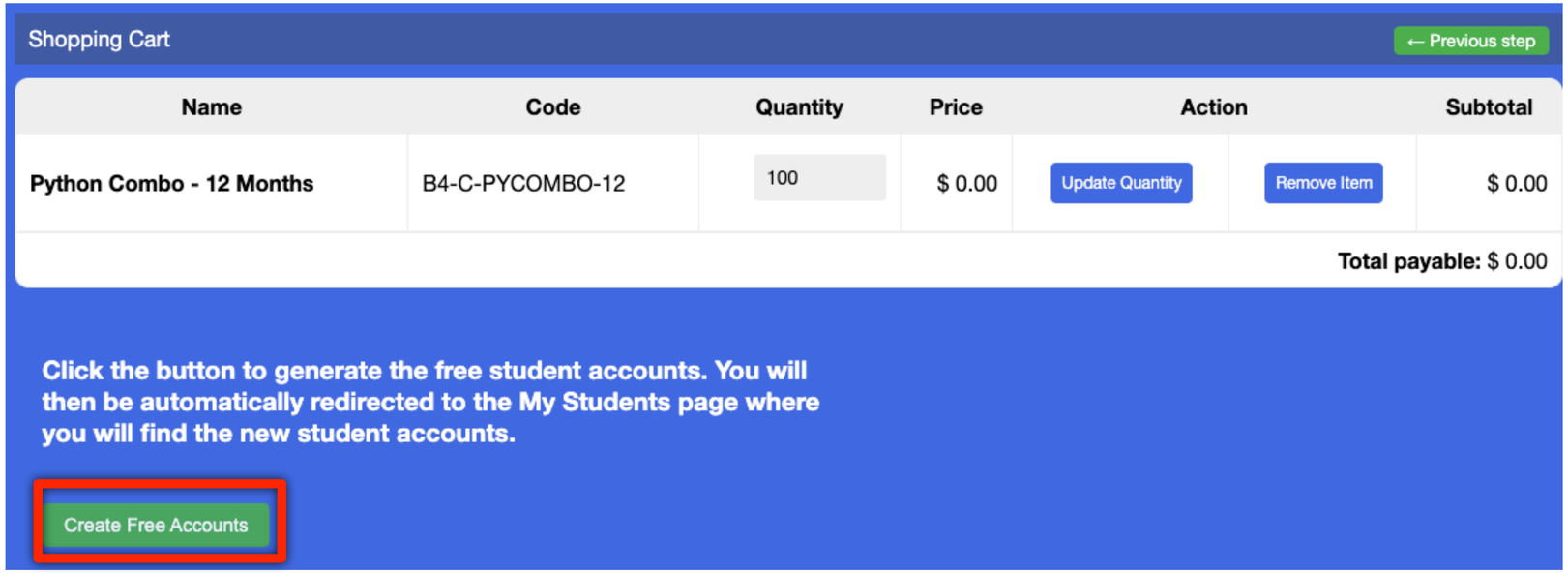


Click on Checkout

Confirm your details and click ‘Checkout’



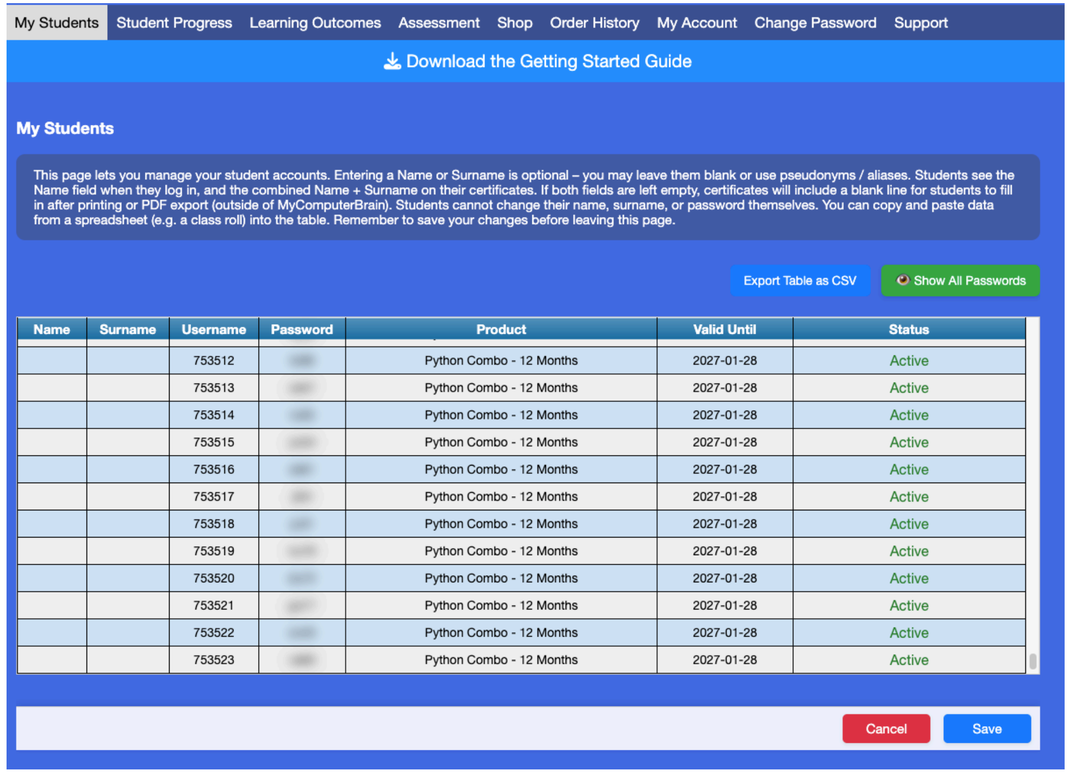
Click on ‘Create Free Accounts’



The system will create the accounts
and redirect to the My Students screen

Distribute usernames+passwords to your students

If you like, you can add names/surnames (optional), - needed for personalised certificates



Export as CSV and distribute to your students

Note: each account collects achievement points

Teacher Course Page

Teacher Information

About this course: Academy of AI Cyber Defence stands out by bringing a large portion of the Digital Technologies curriculum together into one highly engaging experience. Students use input and output, decisions, nested loops, lists, and data dictionaries to solve real problems, while also working with functions, classes, encryption, cybersecurity, and AI. Rather than learning these ideas in isolation, students apply them inside a live, interactive system featuring an evil AI (SKNNET) and a protective Gatekeeper. By manipulating real data, packets, and neural network weights, students develop strong systems thinking and see how small code changes can affect large, distributed systems—making advanced AI concepts accessible, concrete, and memorable.

Download the Getting Started Guide

Storyline

SKNNET is a hostile AI system that has infiltrated the internet, threatening system integrity and security.

Students take on the role of a cadet at the newly-formed Academy of AI Cyber Defence, examining packets, strings, weights, and propagation patterns to understand and influence the behaviour of SKNNET. Through interactive challenges, they decrypt hostile data packets, coordinate global efforts, and eventually overwrite the SKNNET AI to make it benevolent.

Course Structure & Learning Progression

The course continues where the Python Introduction course ended. We catch-up students quickly about core coding concepts at the beginning.

The course is deliberately structured to build from core Python skills to more advanced Python and toward AI and cybersecurity concepts, guiding students through a carefully sequenced learning journey.

- **Part 1 (Missions 1–5):** Review of key coding concepts including print, input, and decisions. Students analyse strings and substrings and build a traffic-light system to classify network packets.
- **Part 2 (Missions 6–9):** Exploration of simple string-based encryption techniques such as skipping characters, slicing, and reversing strings.
- **Part 3 (Missions 10–13):** Subtle manipulation of cloud deployment data, including sabotaging cloud deployment strings and modifying cooling capacity values. The focus is on how small changes can have large system-wide effects.
- **Part 4 (Missions 14–17):** Introduction to data dictionaries and strategic packet manipulation. Students apply encryption techniques to coordinate global efforts and extract an API key from SKNNET.
- **Part 5 (Missions 18–21):** Use of an AI API to strategically read and modify artificial neural network (ANN) weights.
- **Capstone (Mission 22 – Endgame):** Students transplant data from a benevolent AI into SKNNET, transforming it from a hostile system into a cooperative one. This mission brings together concepts from across the course.

Cybersecurity Concepts Embedded in the Course

While the course is delivered through coding missions and narrative, it deliberately exposes students to core cybersecurity concepts through hands-on experience rather than abstract theory.

- **Input Validation & Trust Boundaries:** Students learn that incomplete or partial checks can be exploited and that all external input must be treated with caution.
- **Encryption & Obfuscation:** String manipulation techniques such as reversing, slicing, and skipping characters introduce foundational ideas behind encryption and data protection.
- **Packet Inspection & Traffic Classification:** Students analyse packet-like data to distinguish between benign and hostile traffic, reflecting real-world firewall and intrusion detection concepts.
- **API Security & Access Control:** Interaction with protected APIs and keys models authentication, separation of concerns, and least-privilege access.
- **Distributed Systems & Propagation:** SKNNET is presented as a hierarchical, distributed system, helping students understand why local fixes must propagate globally.
- **Denial-of-Service (DoS):** Through logic errors, repetition, and feedback effects, students experience how systems can be overwhelmed.
- **Adversarial Thinking:** Students repeatedly switch perspectives between defender, attacker, and system designer, developing threat-modelling skills.
- **AI Safety & Control:** By reading and modifying neural network weights, students explore safe intervention, alignment, and indirect control of AI systems.

Tips for Teachers

- **Recommended:** Python Introduction or Python Introduction (Express)- students benefit from prior exposure to core Python concepts.
- You do not need prior AI expertise to facilitate this course; the materials guide students through the concepts clearly.
- Encourage discussions about the benefits and risks of large-scale distributed systems.
- Focus on the implications of cybersecurity and AI behaviour.
- If students encounter difficulties or dead ends during experiments, especially in later stages, they can reload the page to reset the environment and try again. Iterative problem-solving is encouraged.

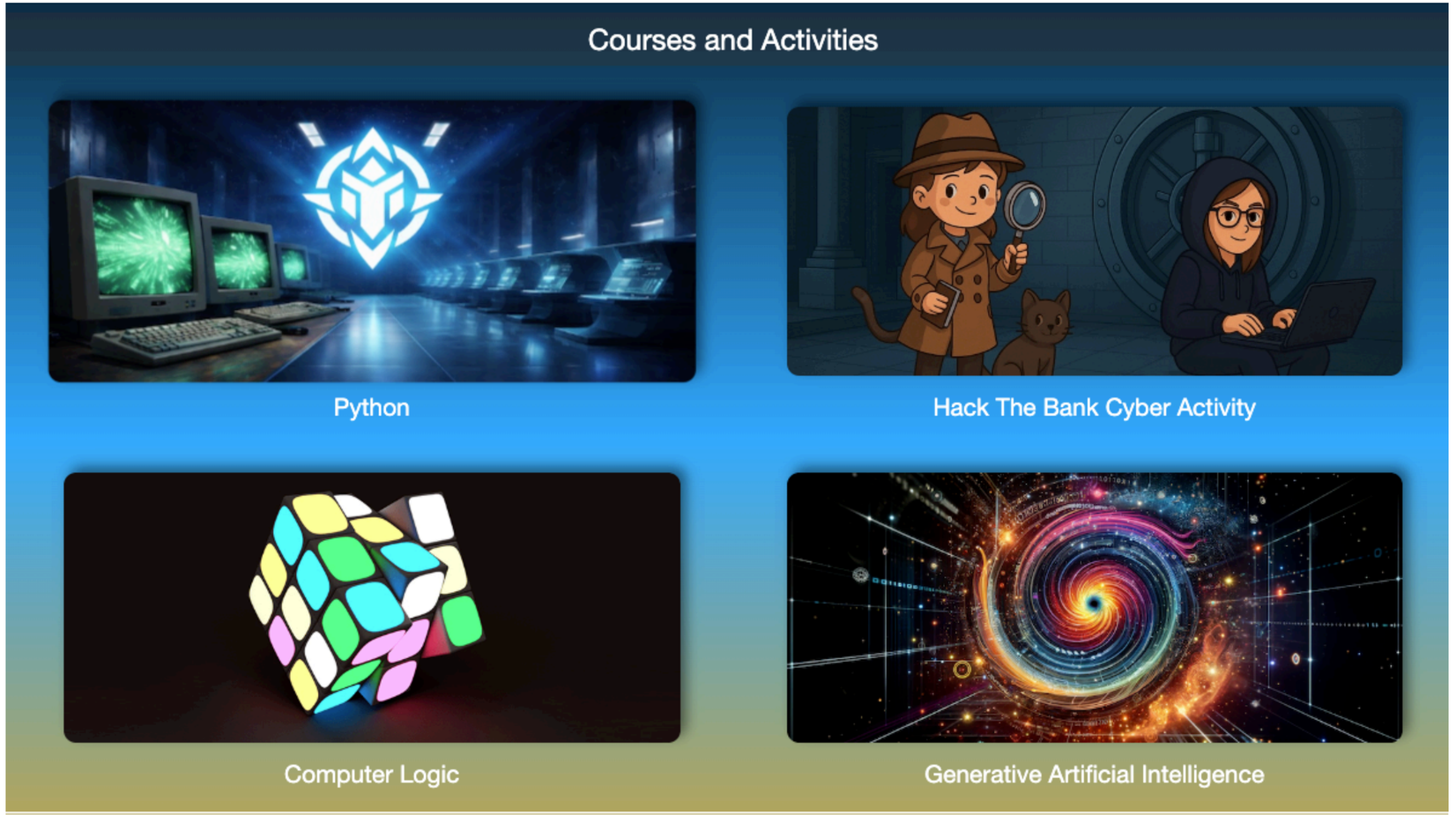
Curriculum Mapping - Years 7-10

This table outlines how key components of the course align with the Australian Curriculum: Digital Technologies (Version 9).

Strand	Curriculum Code	Mapped in Course
Digital Systems	AC9TDI8K01, AC9TDI8K02, AC9TDI10K01	Explored through distributed systems concepts and network hierarchies within AI environments
Data Representation	AC9TDI8K03, AC9TDI8K04	Analysed via packet data, string manipulation, data dictionaries, and weighted propagation in AI models
Acquiring & Analysing Data	AC9TDI8P01-03, AC9TDI10P01-03	Applied through cybersecurity validation techniques and AI behaviour analysis

Students

Starting the course



DIGITAL TECHNOLOGIES INSTITUTE

Start Your Python Journey

Two independent entry paths. One advanced destination in AI & Cyber Defence.

Python Intro

Full foundations

A comprehensive introduction to Python. Ideal for students who want to explore concepts in depth through engaging missions and narrative-driven challenges.

Start with Python Intro

Python Intro (Express)

Fast-track foundations

A streamlined entry into Python for confident or time-limited learners. Focuses on core concepts with rapid progression.

Start with Python Intro (Express)

▼ Both paths lead to ▼

Academy of AI Cyber Defence

An advanced, story-driven course where students expand their Python skills and learn powerful new concepts in AI and cybersecurity while tackling high-stakes challenges.

Enter the Academy

Inside the Course

Not logged in

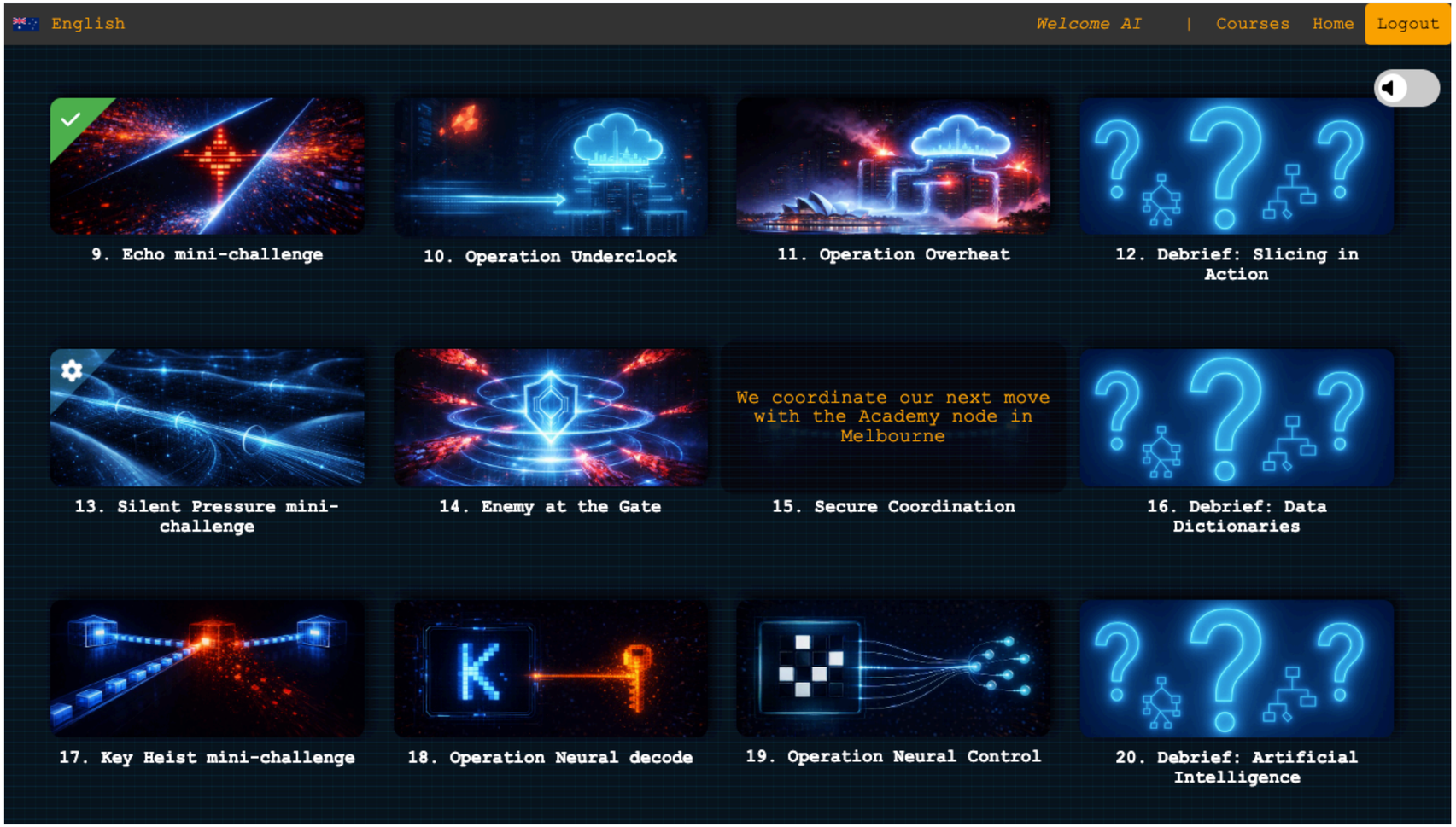
Logged in

Progress Tracker

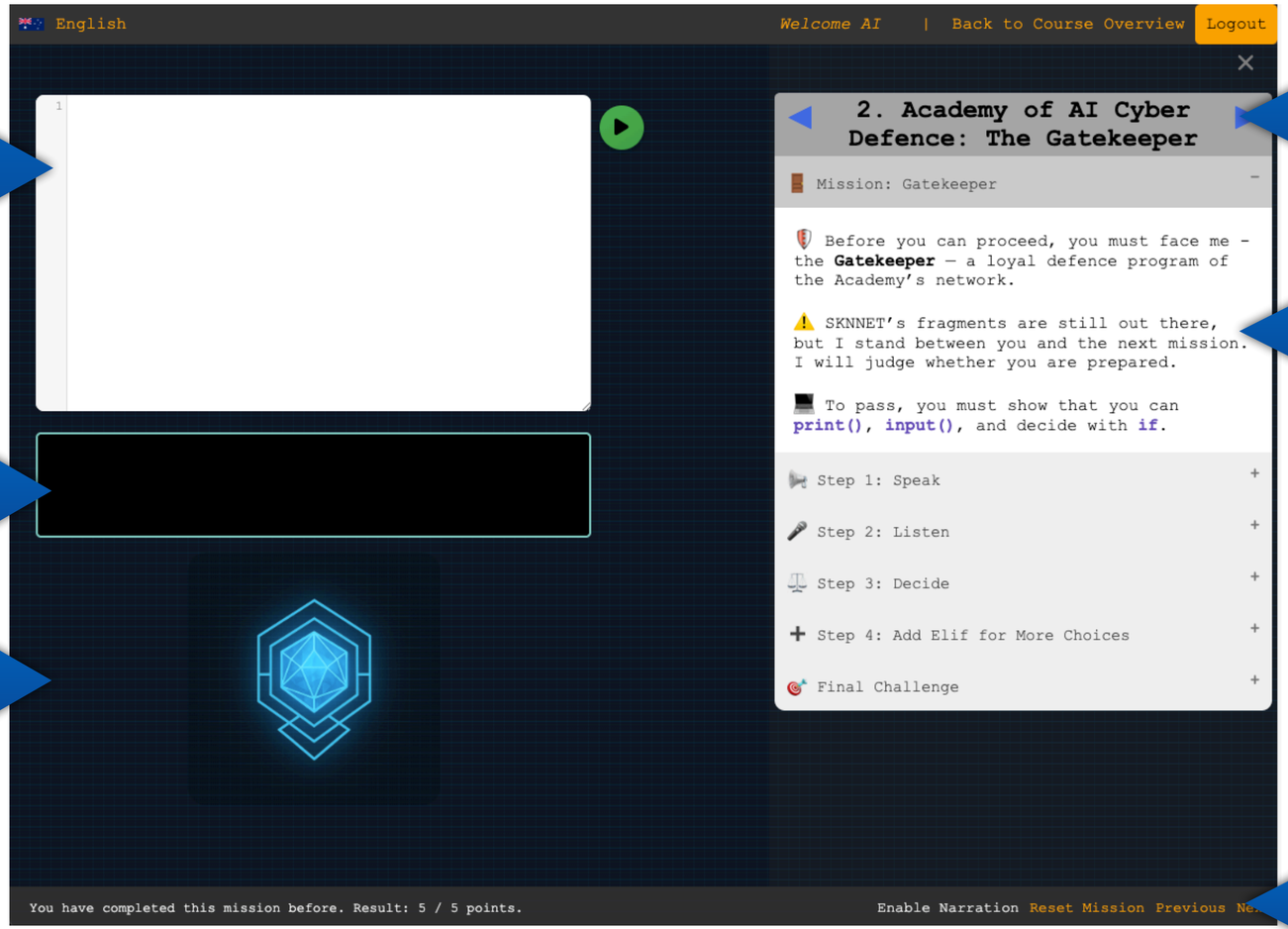
Done

Partially done

Not yet tried



Key elements



Editor

Output

Gatekeeper

Navigation

Instructions Panel

Narration/ Navigation/Control

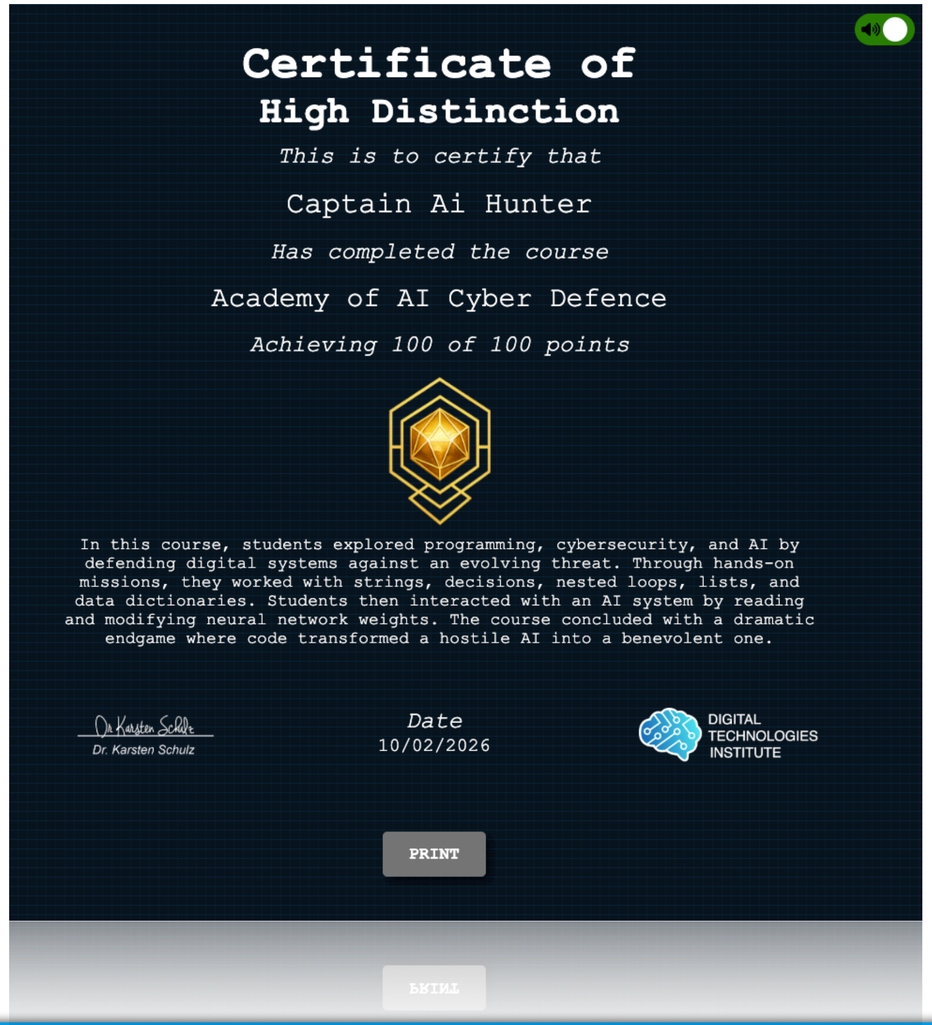
Certificate and Medal

100 points maximum

>85 points, high distinction, gold

>75 points, distinction, silver

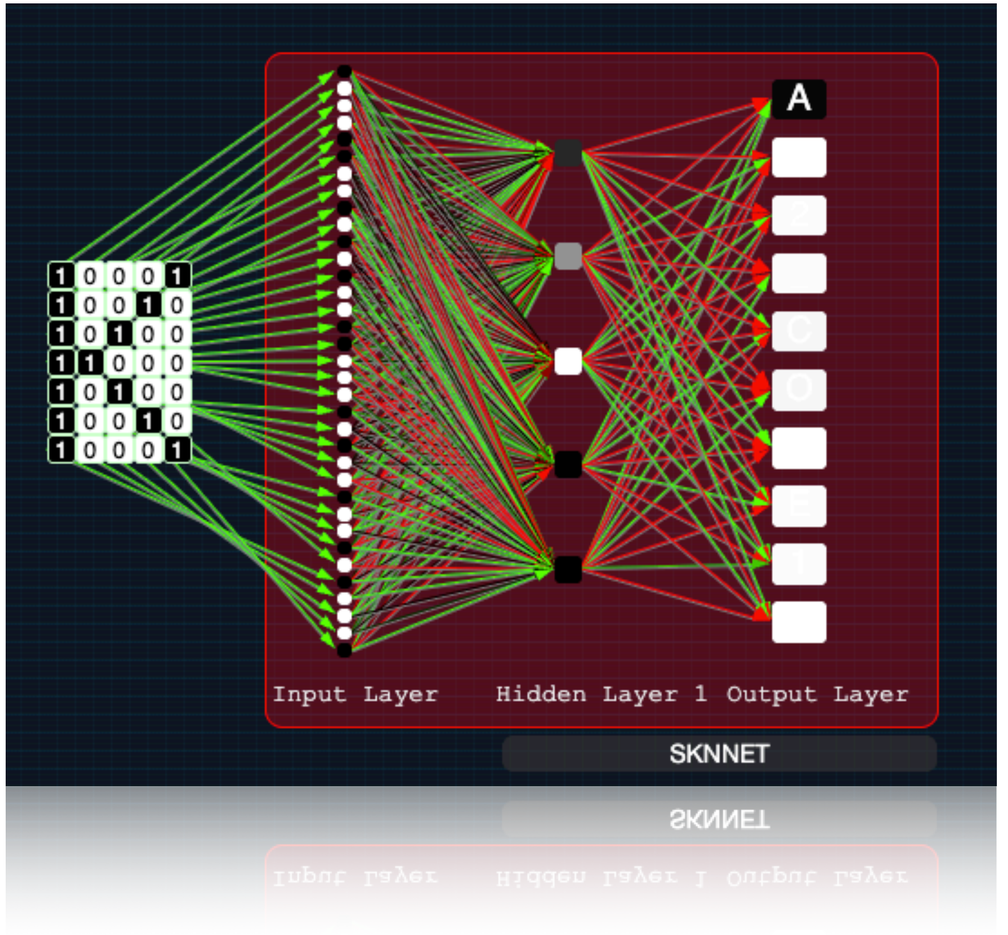
>50 points, achievement, bronze



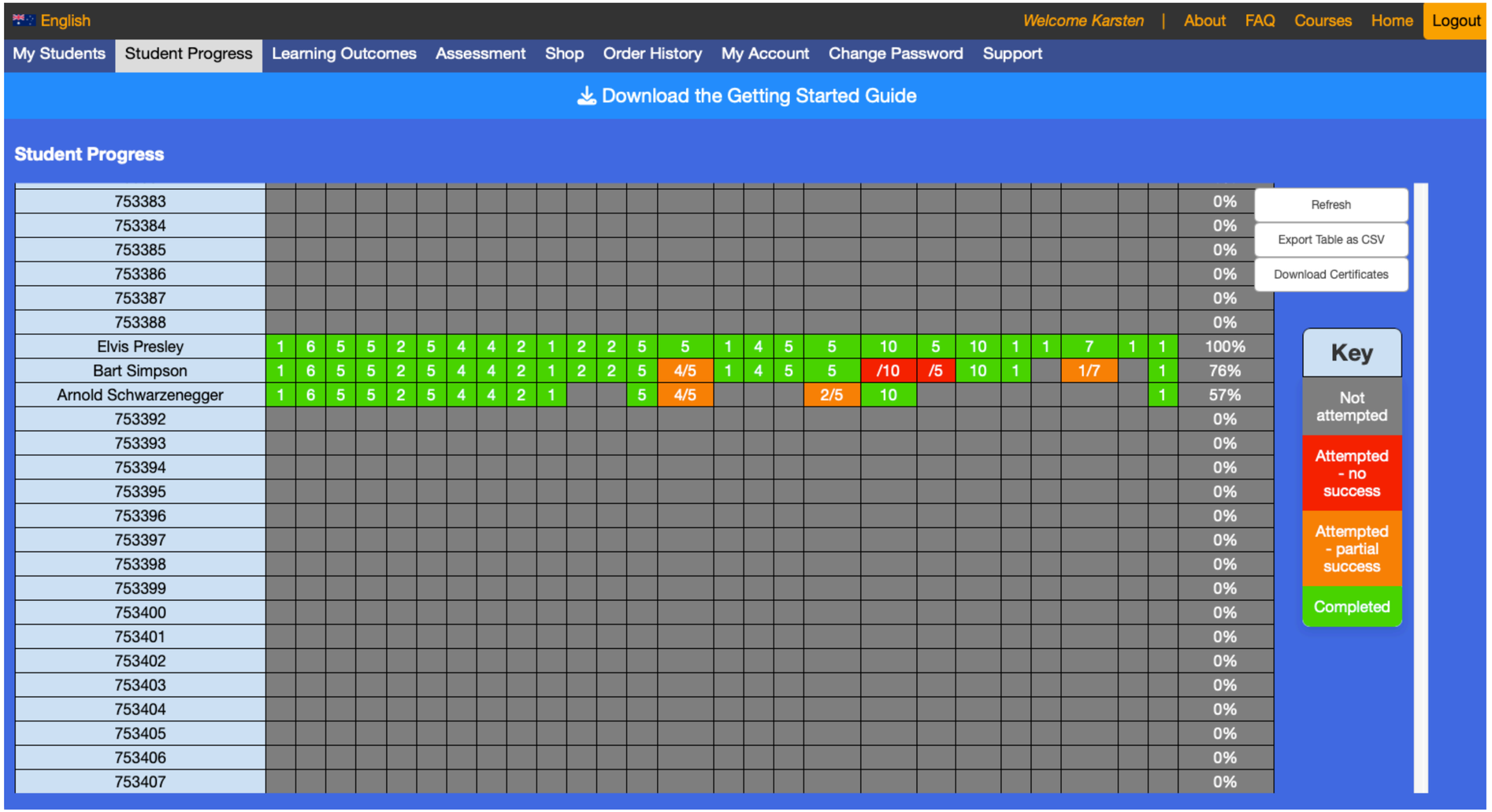
Wait, there is more …

Safe AI

- The course features a simple neural network AI
- Completely browser-based
- Not communicating with backend.
- Not GenAI
- SAFE !



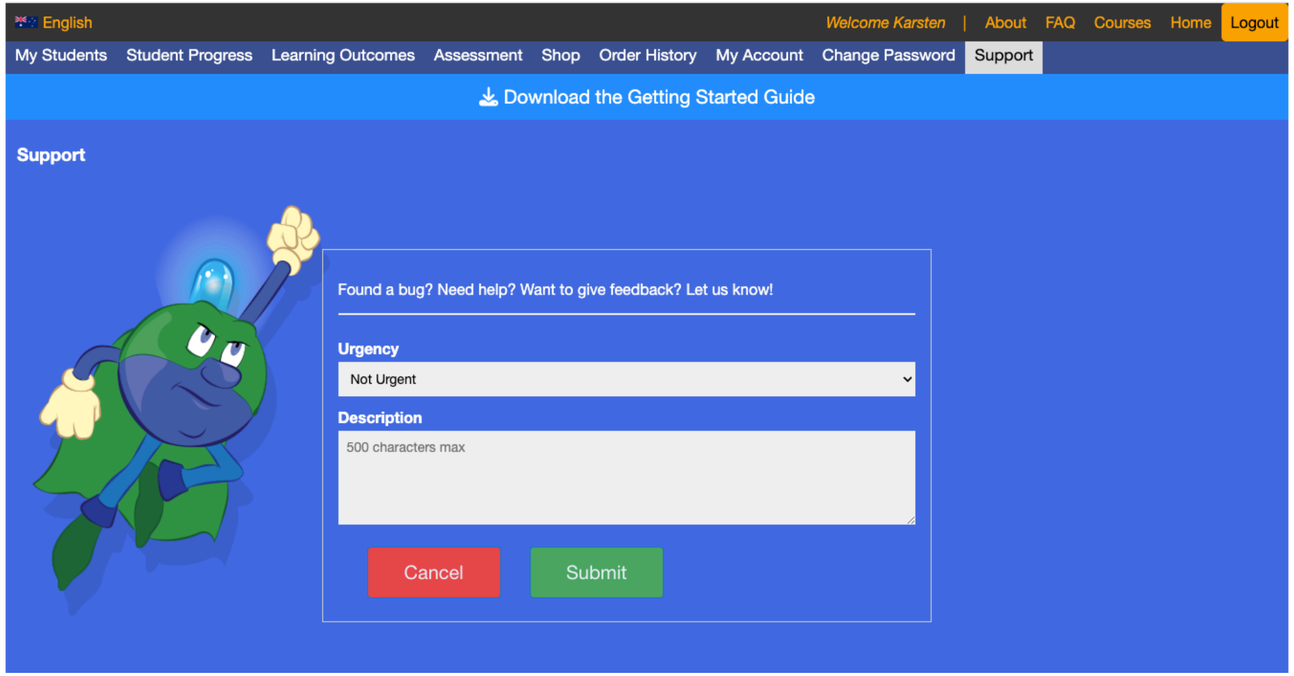
Tracking student progress



753383																										0%
753384																										0%
753385																										0%
753386																										0%
753387																										0%
753388																										0%
Elvis Presley	1	6	5	5	2	5	4	4	2	1	2	2	5	5	1	4	5	5	10	5	10	1	1	7	1	1	100%
Bart Simpson	1	6	5	5	2	5	4	4	2	1	2	2	5	4/5	1	4	5	5	/10	/5	10	1		1/7		1	76%
Arnold Schwarzenegger	1	6	5	5	2	5	4	4	2	1			5	4/5				2/5	10							1	57%
753392																										0%
753393																										0%
753394																										0%
753395																										0%
753396																										0%
753397																										0%
753398																										0%
753399																										0%
753400																										0%
753401																										0%
753402																										0%
753403																										0%
753404																										0%
753405																										0%
753406																										0%
753407																										0%

Support

Please use the support field in your Account (teachers only)



DIGITAL TECHNOLOGIES INSTITUTE

Q&A

www.mycomputerbrain.net