CYBERSECURITY INSTITUTE APPRENTICESHIP

THE HIDDEN GENIUS PROJECT

TABLE OF CONTENTS

PROGRAM OVERVIEW

CYBER SECURITY INSTITUTE APPRENTICESHIP

MISSION

Provide a post-immersion entry-level **IT and Cybersecurity Opportunity**, collaboratively developed with **Corporate Partners at Technology Companies**

VISION

The apprenticeship will provide hands-on experience in **Managerial Cybersecurity, Infrastructure Security, and Applications Security** to Geniuses interested in the industry

PARTNERSHIP OVERVIEW

CYBER SECURITY INSTITUTE APPRENTICESHIP

OBJECTIVE

Expanding access to *IT and Cybersecurity education and career opportunities* to some of the brightest Genius Alumni to increase equity and diversity in the field and provide a diverse pool of talent for our partners

OPPORTUNITY

Our program offers a unique opportunity for technology companies to *invest in the future workforce of the IT and cybersecurity industries* by supporting the development and delivery of a skills-training program for our Geniuses and gaining early access to a diverse pool of highly-skilled and motivated individuals

IMPACT

We invite our technology partners to join us in this endeavor, as we believe this program has the potential to make a significant impact on the future of the IT and cybersecurity industries, and on the lives of the students who participate in it.

APPRENTICE OVERVIEW

RESPONSIBILITIES & TASKS

- Conducting assessments based on provided questions and evaluating the organization's cybersecurity practices.
- Collaborating with your coach to develop recommendations for improving security measures.
- Participating in meetings and discussions to share findings and insights.
- Assisting in the development and testing of incident response plans.*

BENEFITS

- Hands-on experience in real-world cybersecurity scenarios.
- Exposure to industry-standard tools and frameworks.
- Mentorship and guidance from experienced professionals.
- Opportunities for networking and personal branding.
- Practical application of business acumen and project management skills.

HOW IT WORKS

VOLUNTEERS

- Partner organizations help plan and build the curriculum using our virtually optimized lesson plans to facilitate an easy understanding of program concepts and objectives

GENIUS ALUMNI

- Participating Geniuses will already have had **800 hours** of **Computer Science Training**, including front-end and back-end web development.

STIPENDS
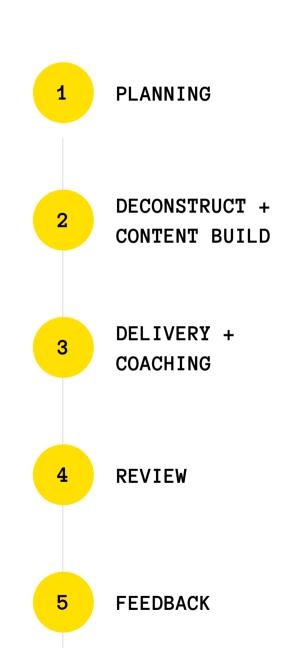
- The monthly stipend will provide an incentive for college-going or working Geniuses to participate in the program and will help to cover expenses.

MENTORING

- Mentoring calls for 2 hours per month with volunteer industry experts. Progress of the program will be tracked and reported on a quarterly basis.

FEEDBACK

- Feedback from the program will be incorporated to inform and improve the curriculum for future cohorts.

1 PLANNING

2 DECONSTRUCT + CONTENT BUILD

3 DELIVERY + COACHING

4 REVIEW

5 FEEDBACK

KEY FOCUS AREAS

- **MANAGERIAL CYBERSECURITY**

- **INFRASTRUCTURE SECURITY**
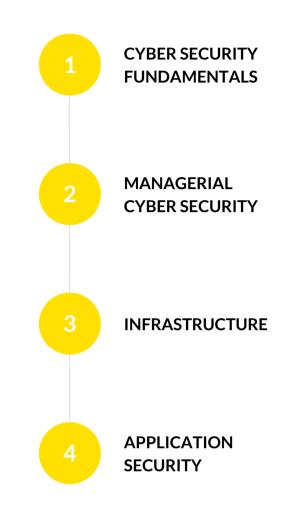
- **APPLICATIONS SECURITY**

PROGRAM TIMELINE

4 PHASES

CADENCE of the program will consist of two VIRTUAL weekly or bi-weekly sessions led by industry experts

DURATION of the program will go from January to March 2024

STRUCTURE of the program will be divided into **4 fundamental phases:**

1. CYBER SECURITY FUNDAMENTALS

2. MANAGERIAL CYBER SECURITY

3. INFRASTRUCTURE

4. APPLICATION SECURITY

CYBERSECURITY FUNDAMENTALS

January – February 2024

During this phase, Geniuses will establish a fundamental foundation in cybersecurity by exploring and learning the core principles of information security and understanding how to apply these principles to protect confidentiality, integrity, and availability.

DISCUSSION TOPICS:

- General Business Course
- Business Acumen, Time Management, Project Management
- Soft Skills / "Power Skills"
- Interview Skills, Presentation & Facilitation Skills, Networking
- Introduction to Computer Science OR Introduction to Computer Programming
- Introduction to Information Systems Security
- Hacker Techniques & Exploits (Red Team)
- Cybersecurity Defense Techniques (Blue Team)
- Computer Forensics Fundamentals (Blue Team)

KEY TAKEAWAYS:

- Define key cybersecurity terms and concepts.
- Identify and categorize common cyber threats.
- Explain the CIA triad and its significance.
- Differentiate between symmetric and asymmetric cryptography.

MANAGERIAL CYBERSECURITY

February 2024

In this phase, Geniuses will learn to develop and implement effective security policies, guidelines, and standards within an organization. Geniuses will progress their skills in risk management, including identifying potential risks, assessing their impact, and implementing mitigation strategies

DISCUSSION TOPICS:

- IT Security Strategic Planning, Policy, and Leadership
- Compliance / GRC
- Risk Assessment
- Incident Handling

KEY TAKEAWAYS:

- Draft and present a sample security policy.
- Conduct a basic risk assessment for a given scenario.
- Summarize key compliance regulations affecting the industry.
- Develop a brief security awareness training outline.

INFRASTRUCTURE

February 2024

The Infrastructure phase delves into the technical aspects of securing an organization's infrastructure. Geniuses will explore network security, learning about firewall technologies, intrusion detection and prevention systems, and virtual private networks.

DISCUSSION TOPICS:

- Systems & Network Administration
- Cloud Security Fundamentals
- In-Depth Intrusion Detection, Forensics & Troubleshooting

KEY TAKEAWAYS:

- Configure a basic network firewall for a test environment.
- Set up endpoint security measures for a sample device.
- Design a basic cloud security architecture diagram.
- Create a simple IAM role and assign permissions.

Phase 4

APPLICATIONS SECURITY

March 2024

The final phase focuses on securing applications and software development processes. Geniuses will gain insights into the **secure software development lifecycle** (SDLC), understanding how security measures are integrated at each stage of development.

DISCUSSION TOPICS:

- Secure coding in Java and Net (Security Operations?)
- Applications in Information Security (Application Security?)
- Web Application PEN Testing

KEY TAKEAWAYS:

- Outline a secure software development process.
- Identify and fix a simple web application vulnerability.
- Incorporate a security step in a sample CI/CD pipeline.
- Participate in a simulated incident response exercise.

CAPSTONE
PROJECT

ASSESSMENT & RECCOMENDATION

Apprentices will be tasked with auditing the security processes of a selected partner organization. Based on the understanding of the course material, interns will answer the provided assessment questions and make recommendations for improving the partner's cybersecurity posture.

This exercise will provide valuable experience in applying theoretical knowledge to practical scenarios and developing actionable insights.

FOR INQUIRIES,
CONTACT US

🌐 www.hiddengeniusproject.org

✉ arnold@hiddengeniusproject.org