Cyber Battle Royale

"Defend. Attack. Adapt. Become the Ultimate Cyber Champion."

Part of the Cyber School 6-Year Pathway

Target Audience: Grade 9 Students and Above (Ages 14+). Designed for students who want to test their cybersecurity skills in **real-world scenarios** and **competitive challenges**. **Course Duration:** 38 Core Sessions (1 hour each) + 10 Optional Sessions **Course Format:** Fully Online, Hands-On Learning with CTF Tournaments, Attack/Defense Simulations, and Real-World Cybersecurity Labs

This immersive program takes students beyond theoretical knowledge into the high-stakes world of practical cybersecurity. Participants will develop critical offensive and defensive skills through engaging challenges that simulate actual cyber threats.

Key Benefits:

- Master ethical hacking techniques and penetration testing methodologies
- Develop defensive strategies to protect systems and networks from sophisticated attacks
- Build problem-solving skills through time-pressured challenges and team competitions
- Learn from industry experts with real-world cybersecurity experience
- Earn recognized certifications that enhance college applications and future career opportunities

Program Highlights:

The Cyber Battle Royale culminates in a high-intensity competition where students demonstrate their abilities in a controlled but realistic environment. Throughout the course, participants will face increasingly complex challenges, from basic CTF (Capture The Flag) exercises to advanced attack/defense simulations against other student teams.

Prerequisites: Basic understanding of networking concepts and programming fundamentals is recommended but not required. The course begins with foundational skills and progressively builds to advanced techniques, making it accessible to motivated beginners while challenging for experienced students.

Join us to experience the thrill of cybersecurity competitions while developing practical skills that are in high demand across industries worldwide.

About the Cyber School 6-Year Pathway

The **Cyber Battle Royale** is the **final level** of the Cyber School 6-Year Pathway. After building foundational skills in computers, coding, AI, ethical hacking, and Python security, students are now ready to enter the **real-world arena**—where the stakes are high, the challenges are intense, and the skills they've learned will be put to the ultimate test.

The 6 Courses in the Pathway:

1. 1. Cyber Kids (Grade 4+)

   Computer literacy, internet safety, and Scratch coding.

2. 2. Programming Through Games (Minecraft) (Grade 5+)

   Problem-solving through Minecraft coding.

3. 3. AI Explorer (Grade 6+)

   Build AI models and explore data science.

4. 4. Cyber Rangers (Grade 7+)

   Ethical hacking, forensics, and CTF challenges.

5. 5. Python Security (Grade 8+)

   Python programming and secure coding practices.

6. 6. Cyber Battle Royale (Grade 9+)

   Attack and defense simulations, CTF tournaments, and real-world cyber scenarios.

Start Anytime, Learn at Your Own Pace:

- Though courses are designed to be taken chronologically, **Cyber Battle Royale is open to any student** with solid cybersecurity knowledge and Python skills.

About This Course: Cyber Battle Royale

This is where students go **from learning to leading**. In this course, students will:

- Engage in **real-world cybersecurity scenarios** (ransomware attacks, network breaches, and social engineering).
- Participate in **Capture The Flag (CTF)** challenges in cryptography, forensics, web exploitation, and reverse engineering.
- Experience **attack vs. defense games**—hacking systems while defending their own.
- Work in teams, mimicking real **Security Operations Center (SOC)** roles.
- Build a **final project**: a multi-layered CTF challenge for their peers.

Key Themes:

Critical Thinking & Strategy

Plan, adapt, and outsmart your opponents.

Ethical Hacking in Practice

Explore the hacker mindset while adhering to legal frameworks.

Real-World Simulations

Engage in scenarios drawn from actual cyberattacks.

Competitive Cybersecurity

Work solo, in teams, or in red vs. blue competitions.

Module 1: The Arena – CTF Training (Sessions 1-10)

Students dive into the world of CTF competitions and learn the strategies used by real-world cyber defenders and attackers.

1 1. Welcome to Cyber Battle Royale

What is a CTF? How do ethical hackers train?

Types of CTFs: **Jeopardy-Style**, **Attack-Defense**, and **King of the Hill**.

Lab: Set up your own virtual machine (Kali Linux) for ethical hacking.

2 2. Tools of the Trade: Mastering the Hacker's Toolkit

Nmap, Burp Suite, Wireshark, John the Ripper, Metasploit

Lab: Complete a scavenger hunt using common cybersecurity tools.

3 3. Cryptography: Cracking the Code

Encryption basics, ciphers, and cracking techniques.

Lab: Solve classic cryptography puzzles and decode secret messages.

4 4. Web Exploitation: Finding Weak Spots

XSS, SQL Injection, and other web vulnerabilities.

Lab: Hack a vulnerable website in a sandboxed environment.

5 5. Forensics: Digging Through Digital Evidence

File carving, log analysis, and metadata extraction.

Lab: Recover hidden files and trace digital footprints.

6 6. Reverse Engineering: Taking Things Apart

Analyze compiled code to find hidden vulnerabilities.

Lab: Decompile a program and modify its behavior.

7 7. Steganography: Hiding in Plain Sight

Conceal information in images, audio, and documents.

Lab: Hide and retrieve secret messages from images.

8 8. Social Engineering: Manipulating the Human Element

Phishing, baiting, and pretexting techniques.

Lab: Simulate a phishing attack in a controlled environment.

9 9. CTF Mini-Tournament

Students compete in a mini CTF to apply their skills.

Lab: Earn flags across multiple challenge categories.

10 10. Debrief: Building Better Defenses

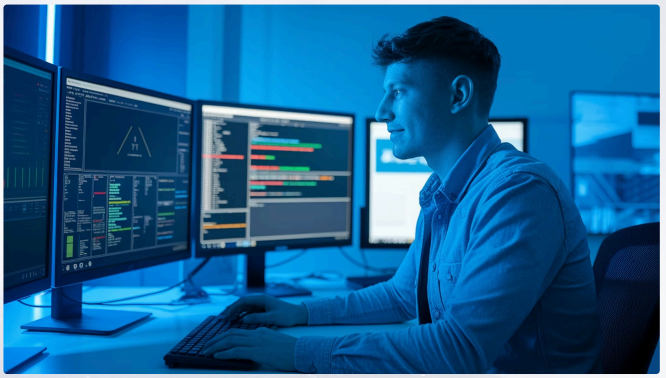
Analyze the CTF and learn from common mistakes.

Lab: Fix vulnerabilities in pre-built systems.

Module 2: Attack & Defense (Sessions 11-24)

Red Team (Attackers) vs. Blue Team (Defenders):

Students rotate between the **Red Team** (offense) and **Blue Team** (defense) to gain perspective from both sides.



Red Team Operations

- **Offensive Tactics: Red Team Strategies** - Penetration testing, reconnaissance, and exploiting weaknesses.
- **Phishing Simulation: Building Traps** - Red Team creates phishing emails; Blue Team builds defenses.
- **Lab:** Perform a vulnerability scan and exploit weak systems.

Blue Team Operations

- **Network Defense: Blue Team Basics** - Firewalls, intrusion detection systems, and traffic monitoring.
- **Advanced Threat Hunting: Blue Team Forensics** - Analyzing logs, tracing intrusions, and stopping attackers.
- **Lab:** Set up a firewall and block simulated attacks.

Module 2: Attack & Defense (Sessions 11-24)

11. Red vs. Blue: The First Showdown (Part 1)

Capture the Flag–style attack and defense battle.

12. Red vs. Blue: The First Showdown (Part 2)

Lab: Teams score points by hacking or defending systems.

13. Web App Security: Defending the Digital Frontline

Strengthening web apps against common exploits.

14. Web App Security: Applied Defense

Lab: Secure a vulnerable website from SQL Injection attacks.

15. Malware Analysis: Unpacking the Bad Stuff

Identify, analyze, and neutralize malicious software.

16. Malware Analysis: Practical Exercise

Lab: Dissect malware in a controlled sandbox.

17. Ransomware Crisis: Understanding the Threat

Blue Team recovers encrypted files; Red Team spreading tactics.

18. Ransomware Crisis: Response Strategies

Lab: Live simulation of a ransomware attack.

19. AI-Powered Attacks: Offensive Capabilities

How AI can be weaponized in cyber attacks.

20. AI-Powered Defense: Protective Measures

Using AI as a shield against cyber threats.

21. AI Security Lab

Lab: Train an AI tool to detect cyber threats.

22. Zero-Day Exploits: The Race Against Time

Responding to unknown vulnerabilities.

23. Zero-Day Response Lab

Lab: Simulate a zero-day attack and scramble to patch it.

24. CTF Tournament: Intermediate Level

Complex challenges across all categories.

Lab: Students compete for top hacker honors.

Module 3: Real-World Scenarios (Sessions 25-34)

Students take on challenges based on real cyberattacks.

25-26. The Corporate Data Breach

Defend a virtual company from insider threats and external attacks.

Lab: Secure sensitive data before it's stolen.

27-28. Power Grid Under Attack

Red Team attempts to disrupt the power grid; Blue Team fights to stop them.

Lab: Use SCADA simulations to control infrastructure.

29-30. Bank Heist 2.0

A digital heist scenario inspired by real-world breaches.

Lab: Blue Team defends, Red Team attacks a simulated bank.

31-32. Critical Infrastructure Defense

Protect a city's water supply, transport systems, and energy grid.

Lab: Monitor networks for intrusion attempts.

33-34. Nation-State Cyberwarfare Simulation

Advanced Persistent Threats (APTs) and long-term infiltration tactics.

Lab: Defend government networks from stealthy attackers.

Module 4: The Cyber Battle Royale (Sessions 35-38)

The ultimate CTF competition to crown the Cyber Champion.

35-37. Mega CTF Tournament

A multi-day Capture the Flag event covering all skills learned.

Students form teams, solve complex challenges, and climb the leaderboard.

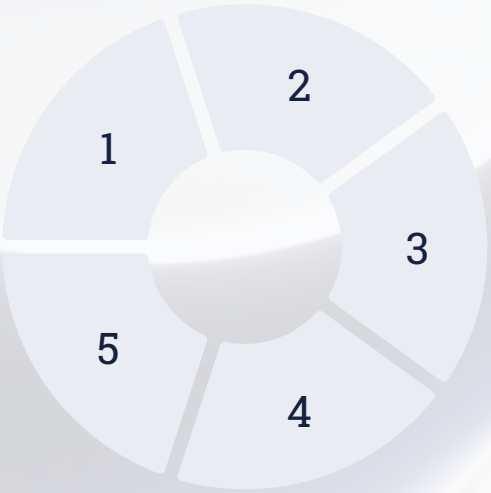
Categories:

Cryptography

Breaking codes and deciphering encrypted messages

Web Exploitation

Finding and exploiting vulnerabilities in web applications



Forensics

Recovering and analyzing digital evidence

OSINT

Open-Source Intelligence gathering and analysis

Reverse Engineering

Analyzing and modifying compiled code

38. Cyber Battle Royale Awards & Graduation

Announce winners, hand out digital badges, and celebrate success.

Students receive feedback and explore future cybersecurity pathways.

Optional Content & Enrichment (10 Extra Sessions)

1. 1. Hacking Smart Homes

   IoT security challenges.

2. 2. AI vs. Hackers

   Train AI to defend against cyberattacks.

3. 3. Bug Bounty Basics

   How to legally hack and get paid.

4. 4. Advanced OSINT Investigations

   Find digital breadcrumbs.

5. 5. Quantum Cryptography

   The future of encryption.

1. 6. Deep Web vs. Dark Web

   Exploring hidden parts of the internet.

2. 7. Malware Creation & Defense

   Build malware (safely) and learn to stop it.

3. 8. Ethical Hacking Career Paths

   How to land jobs in cybersecurity.

4. 9. Personal Branding for Ethical Hackers

   Build a hacker portfolio.

5. 10. Family & Friends Cybersecurity Challenge

   Host a CTF for parents and peers.