# THREAT INTELLIGENCE

Part of GoCyber Collective's (GCC) Professional Cybersecurity Upskilling Suite

# GCC's professional cybersecurity upskilling suite

GCC's upskilling suite provides trainees with the best training experience. Our offering will help Cybersecurity professionals further develop specialized skills by training them in specific advanced topics within the field.

Our courses can also cater to professional competency programs to keep them updated with the latest dynamics in the cyber environment.

## DURATION

40 Academic hours

## TARGET AUDIENCE

IT and Cyber professionals

*Dear Partners,*

*It is an honor to present you the GCC's professional cybersecurity upskilling suite. This set of upskilling courses were designed to provide you with the most updated tools and knowledge to face today's cybersecurity challenges.*

*The GCC was founded to support Ohio's cybersecurity workforce by fostering collaboration between industry leaders, educational institutions, and the state entities. Through strategic partnerships GCC aims to provide comprehensive training and development opportunities that align with the evolving demands of the cybersecurity landscape.*

*The state of Ohio plays a crucial role in this initiative, offering financial support, resources, and policy guidance to ensure the program's success and sustainability. By uniting these efforts, the GCC is poised to create a robust pipeline of skilled cybersecurity professionals who are ready to protect Ohio's digital infrastructure.*

*Sincerely,*

**Shawn Waldman**
Chairman GoCyber Collective

*Dear Students,*

*This course is intended to expand your view to beyond the horizon. The best way to defend against an enemy is to know as much as possible about them.*

*Forewarned is forearmed as we all know.*

*The intention of this course is to empower you to seek out information about potential adversaries as soon as possible. Getting to know them, understand their motivations and most of all their tactics and procedures will help in designing proactive defenses. If these fail threat intelligence will guide you to design the best detections to stop an ongoing attack in its tracks.*

*Emphasis on real world cases and extensive labs and hands on experiences will arm you with the required knowledge and experience to become a better, more proactive cyber defense professional.*

*Yours,*

**Daniel Zeldis**
Director of Cyber Services

# OVERVIEW

Cyber Threat Intelligence (CTI) covers the collection, analysis, and use of threat intelligence to defend against cyber threats. Additionally, the course delves into standards for threat intelligence sharing and methods for threat modeling and adversary emulation, providing students with the skills to combat cyber adversaries effectively.

## CATEGORY

Red Team

## TARGET AUDIENCE

This course is designed for cybersecurity professionals, IT specialists, and individuals looking to enhance their understanding of cyber threat intelligence (CTI). Ideal for those with foundational cybersecurity knowledge, it aims to equip participants with the skills to collect, analyze, and utilize threat intelligence effectively. Whether you are an aspiring CTI analyst, a security operations center (SOC) team member, or a cybersecurity manager looking to strengthen your team's defense capabilities, this course offers valuable insights into threat modeling, adversary emulation, and the standards for sharing threat intelligence.

### REQUIRED PRIOR KNOWLEDGE

- Foundational cybersecurity principles
- Basic cyber threat intelligence

### COMPUTING REQUIREMENTS

- CPU: Intel i5/i7 or AMD 5x/7x
- RAM: 16GB
- HDD: 300GB available space

**Participants who fulfill the program's criteria will be awarded a distinguished graduation certificate.**

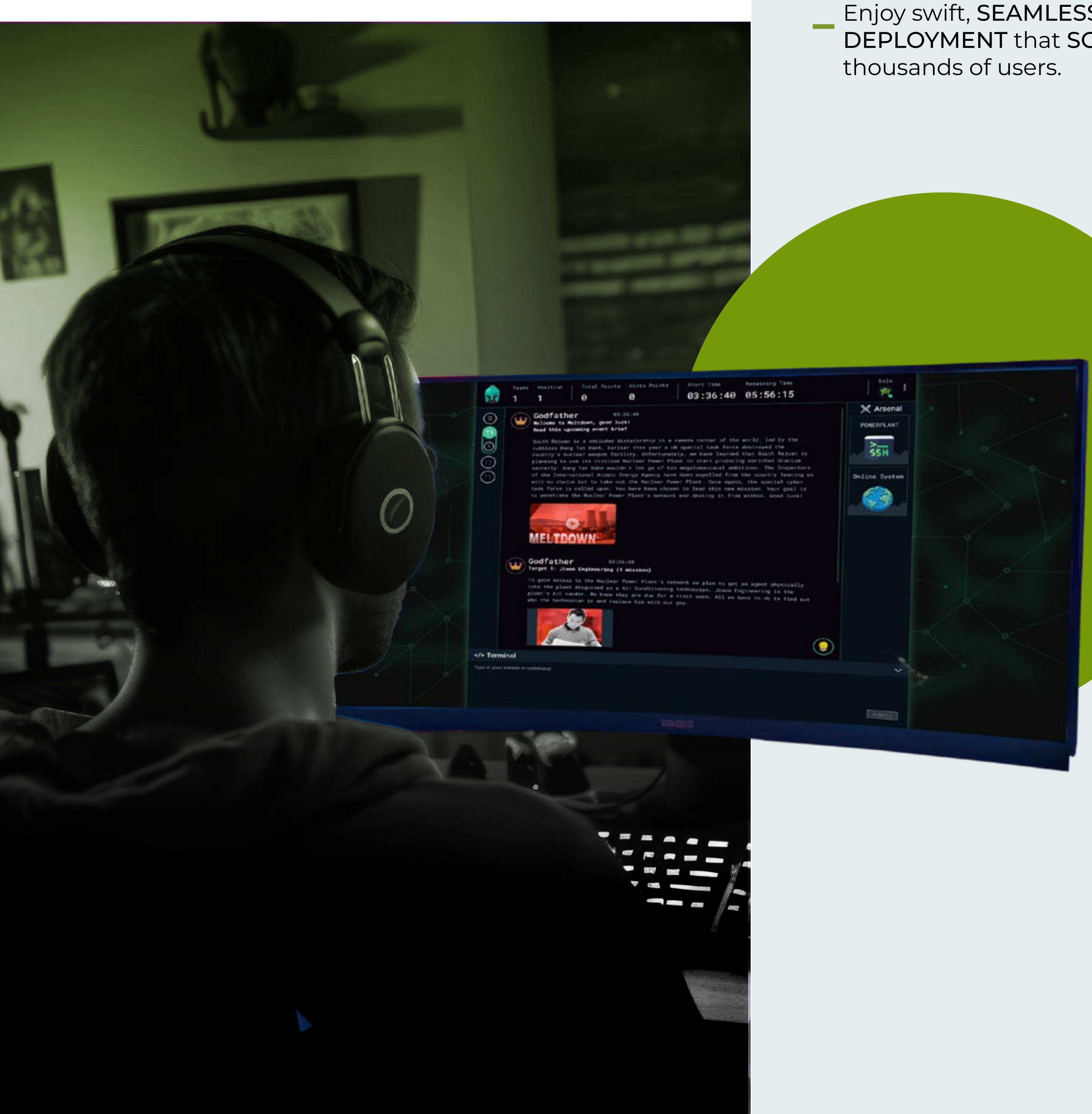
# CYWARIA

NEXT GENERATION CYBER RANGE

Cywaria is the next-generation Cyber Range: a thrilling, real-world **CYBER WARGAME ARENA** for information security professionals.

We provide an unparalleled true-to-life platform for enterprise cybersecurity teams to **TRAIN AS THEY FIGHT** and gain critical real-world experience.

- Use **REAL-LIFE CYBER TOOLS** to defend critical assets from lifelike cyber-attacks.
- Leverage our **GAMIFIED ENVIRONMENT** to boost engagement and strengthen learning.
- Choose from our range of **RED, BLUE, AND PURPLE TEAM SCENARIOS** for specialized training.
- Train **ANYTIME, ANYWHERE,** with just a laptop and an internet connection.
- Access in-depth data and metrics to **TRACK PERFORMANCE** and **ASSESS READINESS.**
- Enjoy swift, **SEAMLESS DEPLOYMENT** that **SCALES** to thousands of users.



Godfather 03:36:40
Welcome to Meltdown, good luck!
Read this upcoming event brief

South Rajuan is a secluded dictatorship in a remote corner of the world, led by the ruthless Dang Tat Danh. Earlier this year a UN special task force destroyed the country's nuclear weapon facility. Unfortunately, we have learned that South Rajuan is planning to use its civilian Nuclear Power Plant to start producing enriched Uranium secretly. Dang Tat Danh wouldn't let go of his megalomaniacal ambitions. The Inspectors of the International Atomic Energy Agency have been expelled from the country leaving us with no choice but to take out the Nuclear Power Plant. Once again, the special cyber task force is called upon. You have been chosen to lead this new mission. Your goal is to penetrate the Nuclear Power Plant's network and destroy it from within. Good luck!

Godfather 03:36:40
Target 1: Jiwon Engineering (1 mission)

To gain access to the Nuclear Power Plant's network we plan to get an agent physically into the plant disguised as a Air Conditioning technician. Jiwon Engineering is the plant's A/C vendor. We know they are due for a visit soon. All we have to do is find out who the technician is and replace him with our guy.

# COURSE SYLLABUS

## Introduction to CTI

- What is threat intelligence
- Types of threat intelligence and use cases
- Strategic threat intelligence
- Operational threat intelligence
- Threat actors, threat vectors and APT
- Motivation of threat actors
- Intelligence requirements, terms of reference
- The diamond model
- The MITRE ATT&CK framework

## The threat intelligence cycle

- What is the CTI cycle
- Translating intelligence requirements to action
- The 5 phases
- The roles in every step

## The Cyber Kill chain

- The different phases
- Analysis of attack vectors
- How to break the kill chain

## Direction

- The elements of the direction phase
- Differences between IRs, PIRs and RFIs
- Identifying intelligence gaps

## Collection

- What is collection
- Sources of CTI
- Open and closed sources
- The Dark Net
- The three grading systems for intelligence

## Analysis

- What is a hypothesis
- Testing hypotheses
- Using analytical techniques to identify critical information

## Dissemination

- What is dissemination
- Ways to present intelligence
- Reporting

## Legal and ethical

- Identifying legal and ethical practices
- How to handle classified information

### TUITION

Total Cost: $4,200
*Including digital study materials*

### STUDENTS

Min. number of students in class: 10
Max. number of students in class: 16
*The course will not open unless the minimum number of students is met. In such a case, a full refund will be issued.*

### CANCELLATION POLICY

**1.** All cancellation requests must be submitted to the GCC at training@gocybercollective.org in writing.

**2.** Refund Eligibility:

**2.1.** 90% Refund: Participants can cancel up to 14 days before the course start date and receive a 90% refund of the course fee.
**2.2.** 50% Refund: Cancellations made between 7-14 days before the start date will receive a 50% refund.
**2.3.** No Refund: Cancellations made less than 7 days before the start date will not receive a refund.

gocyber
COLLECTIVE

gocybercollective.org