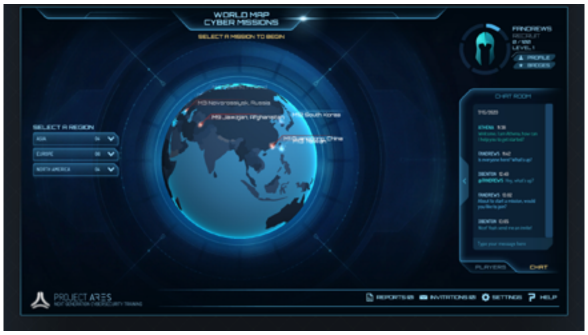
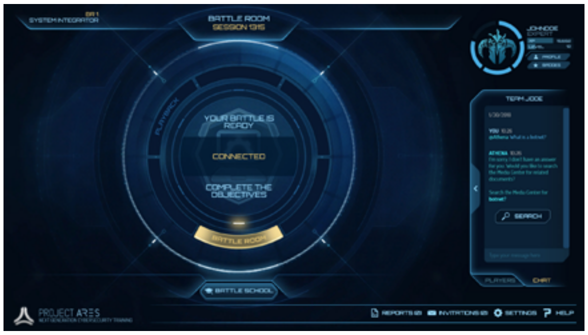
PROJECT ARES®
BY CIRCADENCE



Immersive learning with Project Ares cybersecurity labs

Project Ares is a cybersecurity education learning platform that delivers hands-on immersive labs. The lab exercises can be integrated into an existing syllubus or outline of a cybersecurity course or training program.

Project Ares Labs



- Deliver learning through virtual machines with open-source cyber tools.
- Create an immersive, true-to-life learning environment.
- Are available to learners and instructors anywhere and at any time through a browser interface.

LEARN MORE
ABOUT PROJECT ARES

Introductory Cyber Courses packaged with Project Ares Labs

Using Project Ares to deliver a purposeful learning experience to students takes preparation. For organizations with specific cyber learning objectives but limited resources to develop and teach classes, we offer ready-to-deliver, introductory cyber courses with lesson plans that incorporate Project Ares labs, classroom materials, and instructor time. Textbooks are available but optional to students.

You focus on scheduling and helping students on-board to Project Ares and we take it from there.

With our teaching partner, Phase2 Advantage, we offer packaged introductory courses for Incident Response and Cyber Forensics.

Introduction to Cyber Forensics

CYBER FORENSICS

Description: Introduces network forensics investigations with overview of network devices and services. Presents investigative principals and approaches to lead development in Windows system environments and web-based applications. Concludes with unit on the principles of static and dynamic malware triage.

Practical lab: Exercises utilize the Project Ares® cyber range, Battle Room 9 - Forensics, Autopsy, Ophcrack, Registry Editor, and Wireshark network traffic analyzer.

Pre-Requisites: None

Course Material Included: Syllabus, Lecture slides, Course lab guide with task assignments. A related textbook is optional. Project Ares subscriptions are priced separately.

Introduction to Incident Response

INCIDENT RESPONSE

Description: Introduces the Incident Response Life Cycle with overview of current threat landscape. Presents how to prepare for investigations through identifying network and system baselines. Discusses indicators of compromise, threat identification, incident containment and remediation, and includes principles of static and dynamic malware triage.

Practical lab: Exercises utilize the Project Ares® cyber range, Battle Room 11 - System Security Analysis with Kali Linux, PowerShell, and Microsoft command prompt.

Pre-Requisites: None

Course Material Included: Syllabus, Lecture slides, Course lab guide with task assignments. A related textbook is optional. Project Ares subscriptions are priced separately.

The online, instructor-led courses from Phase2 Advantage are designed to teach concepts plus offer practical skill experience for students. The courses are taught over 6 weeks for a total of 12 hours of instruction plus 6 hours of off-line student support through email or other tools.

Project-based learning is essential in cybersecurity. A student can enjoy a training experience and score well on an exam, but still not be able to apply their new knowledge. Even in introductory courses, hands on labs cement concepts that enable better advanced cyber learning.

The Instructor

Michael I Kaplan

Cyber Security Instructor
1.912.335.2217
michael.kaplan@phase2advantage.com
phase2advantage.com

PHASE2 ADVANTAGE

The Future of Immersive Cybersecurity Education.

Michael I. Kaplan is the Director of Operations for Phase2 Advantage, a cybersecurity training and publishing company based in Savannah, Georgia. He is also the Chairman of the Savannah Technical College Cybersecurity Advisory Committee and is heavily involved in curriculum design initiatives for several university systems.

Michael has written numerous courses and cybersecurity training programs for corporate, academic, and government personnel. And he has developed training programs for Law Enforcement and Fugitive Task Force investigators on the topics of Criminal Topology, Forensic Document Analysis, and Investigations.

Michael's technical areas of specialization are Incident Handling and Response, Network Forensics, Digital Forensics, and Information Technology Risk Management. He also provides consulting services for government, corporate, and academic organizations both domestically and internationally.