COURSE DESCRIPTION:

Hack Warz® Cyber Attack: A Hands-On Lab for Network Defenders

LIFE CYCLE INSTITUTE

HACK WARZ®

As the Department of Defense, federal, state and local governments and commercial entities work to leverage the NIST standards to harden cyber defenses, hackers are innovating and deploying new exploits at an ever-increasing pace.

This one-day workshop combines the Hack Warz ethical hacking competition with the Risk Management Framework six-step Security Life Cycle to demonstrate how to think like a hacker when designing a systems hardening plan.

Participants will review the Risk Management Framework (RMF) six-step process (NIST 800-37) and use the RMF methodology to outline a defense-in-depth strategy. This includes correlating STIGs and IA controls to the new RMF controls. Participants will execute "white hat" attacks against typical IT systems in the hands-on, Hack Warz lab environment. Hack Warz is set up as a capture-the-flag event in which participants gain exposure to hacker tools and common exploits. After the lab, participants will debrief and use the RMF methodology to update their defense-in-depth strategies.

In the "not if you will be hacked, just when" world we live in, this iterative process of white hat ethical hacking establishes a best-practice and proactive approach to securing and verifying the security of IT assets.

Learn How to:

- Explain best practices using NIST Standards and the Risk Management Framework
- Outline an approach for a defense in-depth strategy
- Correlate STIGs and IA Controls to NIST
- Demonstrate proficiency with auditing tools
- Apply computer network defense using Hack Warz approach

What Our Students Are Saying:

"Learning activities kept the course energized and interactive. Facilitator practiced what she taught; very relevant."

- Training Specialist, US Marine Corps

"Truly amazed how [LCE] picked up on our requests for tying in our info into the curriculum. Very professional SMEs on the material and delivery."

- Kathleen Gebhard, SPAWAR

Who Should Attend:

Advanced IT Professionals responsible for cybersecurity. This includes people who administer, integrate and develop systems, including:

- IT Managers - CIO, DAA, CTO, CISO, ISSO, Head of Cybersecurity, Training Manager, Head of Innovation
- DoD Program Managers
- Technical Managers
- Technical Directors
- Requirements Officers

Course Information:

Each course includes a comprehensive, active learning manual, morning and afternoon refreshments and lunch. This is a one-day class. All students completing a class at the Life Cycle Institute will receive a certificate of completion awarding .8 CEUs.

Life Cycle Institute:

Life Cycle Institute is a recognized leader in learning, leadership and change management solutions. Be prepared to be an active learner. When you invest in training with the Life Cycle Institute, you will gain knowledge and learn skills that you will be able to apply immediately. Our courses are designed to teach by doing. Your training with the Life Cycle Institute is different because we offer:

- Facilitators who practice what they teach and teach what they practice.
- Course content that is constantly updated with the latest proven tools and methods.
- Adult learning methods that minimize lecture and emphasize learning by doing.
- Classrooms that are specifically designed to facilitate learning.

Registration:

Download our class schedule for the latest class dates and course costs or contact the Life Cycle Institute at: 800-556-9589 • education@LCE.com • www.LCE.com

Private Classes:

Your training needs are unique. Unique needs may require customized, on-site training. Learn from practicing cybersecurity professionals – on your site – at a time convenient for you – tailored for your environment. For more information please contact education at: 800-556-9589 • education@LCE.com • www.LCE.com