DEFENDING AGAINST AI-ENABLED THREATS

A Hands-On Playbook for Defenders

LEARN HOW AI IS BEING WEAPONISED AND HOW TO DEFEND AGAINST IT

One day. Hands-on. Walk out with a defensive playbook you can actually use.

March 20, 2026

Copenhagen, Denmark

Hosted at CodeNode, Nordhavn

Session 1: The New Threat Landscape

Understanding the Shift

Real-world cases where AI ran the attack - not just assisted it.
What changes when your adversary operates at machine speed.

Session 2: Threat Scenario Generation

Thinking Like the Adversary

Build realistic AI-powered attack scenarios
Share and stress-test scenarios with your group.

Session 3: Attack Surface Mapping

From Scenarios to Exposure

Use your scenarios to map where you're exposed.
Learn how to use vibe coding methods to identify blind spots.

Session 4: Building Your Defense Playbook

From Analysis to Action

Pull everything together into a playbook you can use on Monday.
Learn what others are building and defending against.

LEAD INSTRUCTOR

Christopher Spirito

Hacker, Teacher, Storyteller

Born to break things and explain how. With 30+ years in cyber defense, nuclear security, and unexpected places (from healthcare to beer analytics), Chris teaches across continents with stories that make hard concepts click. Brings global perspectives with technical precision.

chris@sanctumsec.com

WHAT YOU WILL TAKE HOME

The people who understand AI threats
are the ones companies need most right now.

The ability to identify and assess AI-enabled threats
Your own defensive playbook, built from real scenarios
Reusable threat patterns and templates that grow with your career

PREREQUISITES

What to Bring

Curiosity and a willingness to think like an adversary.
A laptop is welcome but not required.

Optional: Hands-on with AI Tools

Bring a laptop with your favorite LLM to follow along with live demos.

REGISTRATION & PRICING

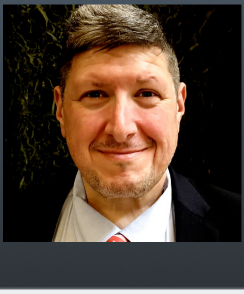
250 DKK / €35

Includes all materials, catering, and playbook development guide.

https://sanctumsec.com/ai-threats-workshop.html#register

CHRISTOPHER SPIRITO

Hacker, Teacher, Storyteller



ABOUT ME

My parents were teachers, so it only makes sense that I followed in their footsteps.
Over three decades ago my teaching journey started with classes on mathematics and emergency medicine, topics that perhaps seem distant, but overlap in both chaos and beauty. Through the decades I have delivered courses in hacking, cyber security and defense, information operations, nuclear security, insider threat analysis, and even improv comedy sketch writing and storytelling. I hope to bring to you an immersive learning experience, one which will help you feel empowered and ready for what's next.

SELECT COURSES AND EXERCISES

Defending Against AI-Enabled Threats

One-day hands-on workshop using coding agents to identify, assess, and defend against AI-powered attacks.

Hacking Handheld Radiation Detectors

3-day course on test and evaluation procedures from hardware hacking, firmware analysis, and exploit prototyping.

Insider Threat Chronicles

Data science course teaching defenders how to use Jupyter Notebooks for threat analysis.

Cyber Nucleus 2024

4-day event featuring a tabletop exercise bringing together reactor staff, regulators, and international cyber response teams.

SELECT PAPERS AND ARTICLES

Weaponising AI
The New Cyber Attack Surface
IISS Survival (2026)
How AI shifted from accelerating human hackers to running entire attack campaigns autonomously, and what that means for defence.

The Oxford Handbook of Nuclear Security
Cyber Security for Nuclear Facilities
Oxford University Press (2024)
A guide to securing digital assets at nuclear facilities, covering attack surfaces, threat actor capabilities, graded protection architectures, and defensive operations.

Unlearned Lessons behind Building a Shared Cyber Framework with your Geo-political Adversaries
The Cyber Defense Review (2022)
How geo-political competitors can build cyber stability using lessons from Cold War exchanges and the hacker community ethos.

Protecting and Defending against Autonomous Control Systems and Digital Twin Cyber Attacks
US Department of Energy (2023)
A response strategy for hyper-parameter attacks of Digital Twin Machine Learning Models in Nuclear Power Plants.

BACKGROUND

Sanctum Security | Idaho National Laboratory | The MITRE Corporation | University of Tartu - Faculty of Law

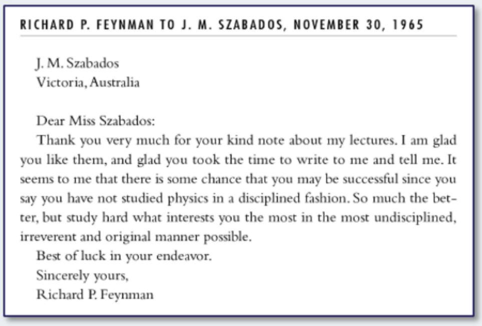
Worcester Polytechnic Institute | Harvard School of Public Health | Boston College | The Pingry School

WiRED International | Roundtable on Military Cyber Stability

Great workshops start with the people in the room.

This one is built around what you bring: your background, your curiosity, and the problems you're trying to solve.

To get the most out of the day, come ready to share, improvise, and surprise yourself with what you can build in a single day.



RICHARD P. FEYNMAN TO J. M. SZABADOS, NOVEMBER 30, 1965

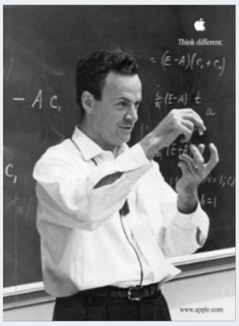
J. M. Szabados
Victoria, Australia

Dear Miss Szabados:

Thank you very much for your kind note about my lectures. I am glad you like them, and glad you took the time to write to me and tell me. It seems to me that there is some chance that you may be successful since you say you have not studied physics in a disciplined fashion. So much the better, but study hard what interests you the most in the most undisciplined, irreverent and original manner possible.

Best of luck in your endeavor.

Sincerely yours,
Richard P. Feynman



https://sanctumsec.com/ai-threats-workshop.html#register