



# Become a Cyber Warrior for Free Courtesy of Uncle Sam

Open-source tools and resources for enhanced Training and Simulation

CERT® Cyber Workforce Development

Chris May  
18 Oct 2022

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

Copyright 2019 - 2022 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0578

# Agenda

## Introduction

## Overview and Demos of Open-source Training Tools

- TopoMojo
- Crucible
- TopGen/GreyBox
- GHOSTS
- WELLE-D
- SCADASim
- FinSim
- Foundry Virtual Appliance
- President's Cup Cybersecurity Competition



# Welcome and Logistics

## Introductions:

Chris May - CMU/SEI since 2001, IUP '92

## Purpose:

- Build awareness of CMU/SEI's open-source software developed to enhance cybersecurity training and simulations
- Encourage interaction and dialogue on emerging cybersecurity training and simulation requirements and best practices

## Challenge:

Try out some of the technical challenges we created for the President's Cup Cybersecurity Competition



# Cybersecurity Professionals Need Practice!

**Cyber Ranges (sandboxes) and Simulators let you:**





# TopoMojo

Simple Lab Builder and Player

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Motivation

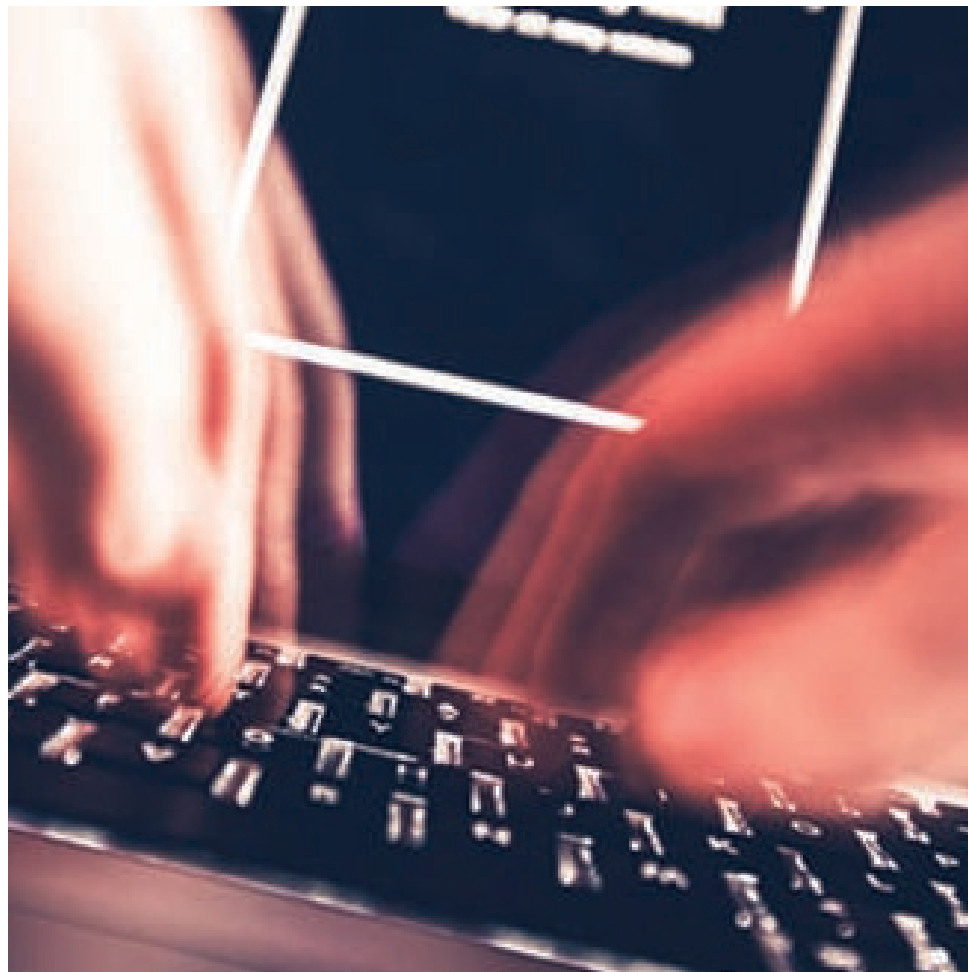
Make it easy and convenient for users to create, share, and consume hands-on training

- 100% browser-based

Essential for building real-world skills and experience – especially in the cyber domain

- Lots of Cyber Gurus out there, need tool to share their expertise with others

Enable large-scale cybersecurity competitions





# TopoMojo Features

Lab Builder

Lab Player

Competition Engine

Collaboration

File upload

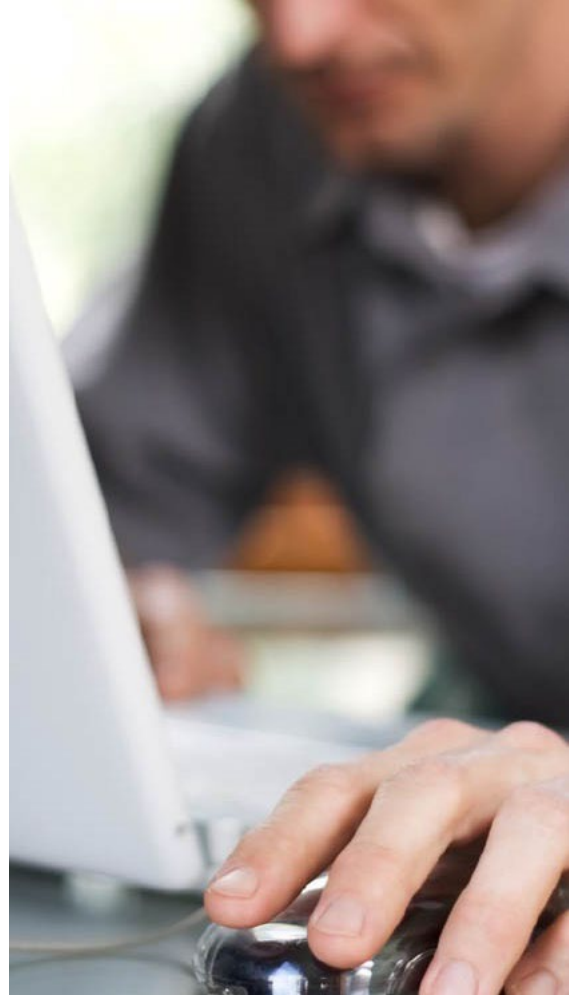
Document editor

Resource limits

Management Dashboard



TopoMojo  
**DEMO**



# Crucible

Cyber Range (sandbox)

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Crucible Simulation Framework (a.k.a. **Cyber Range**)



- Application framework for cyber modeling and simulation.
- Enterprise-grade tools to design, deploy, and manage training labs and exercises, both facilitated and on-demand.

# Crucible Core Components



Player



Caster



Steamfitter



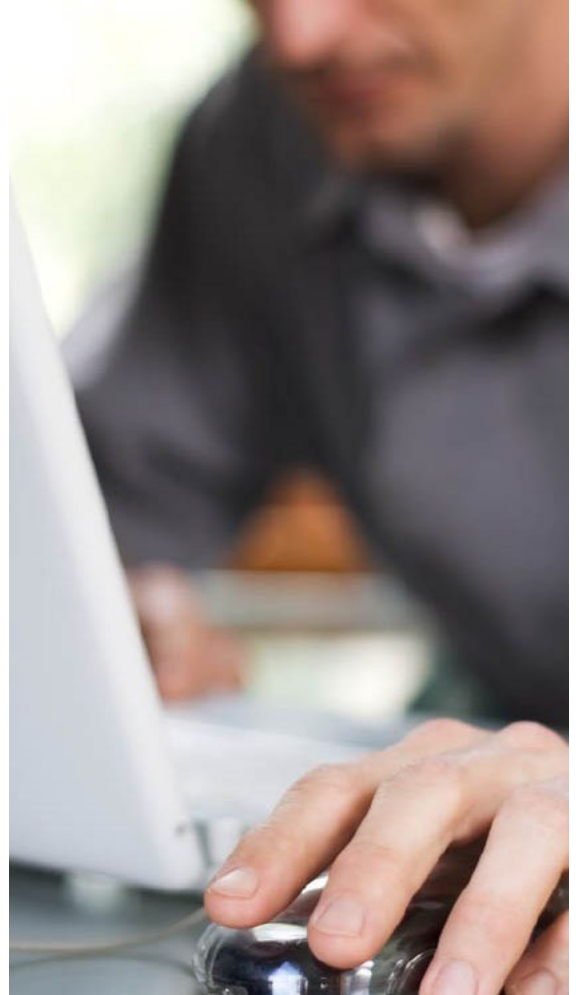
Alloy



SEER

Crucible

# DEMO





# TopGen and Greybox

Internet Simulation Tools

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

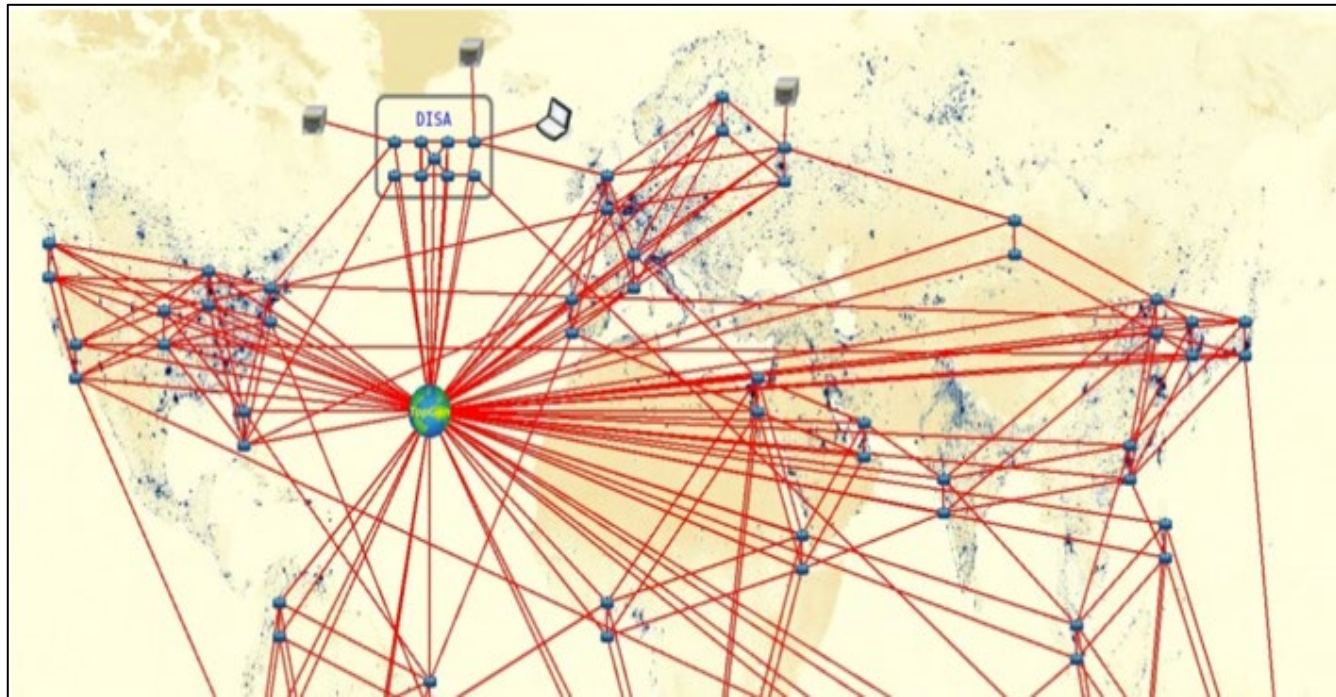


# TopGen & GreyBox

Designed to bring  
Internet Services  
to 'Air-Gapped'  
networks

Application  
Virtualization via  
containers

Portable and  
Extensible (1 VM)



# TopGen / Greybox Features

## TopGen

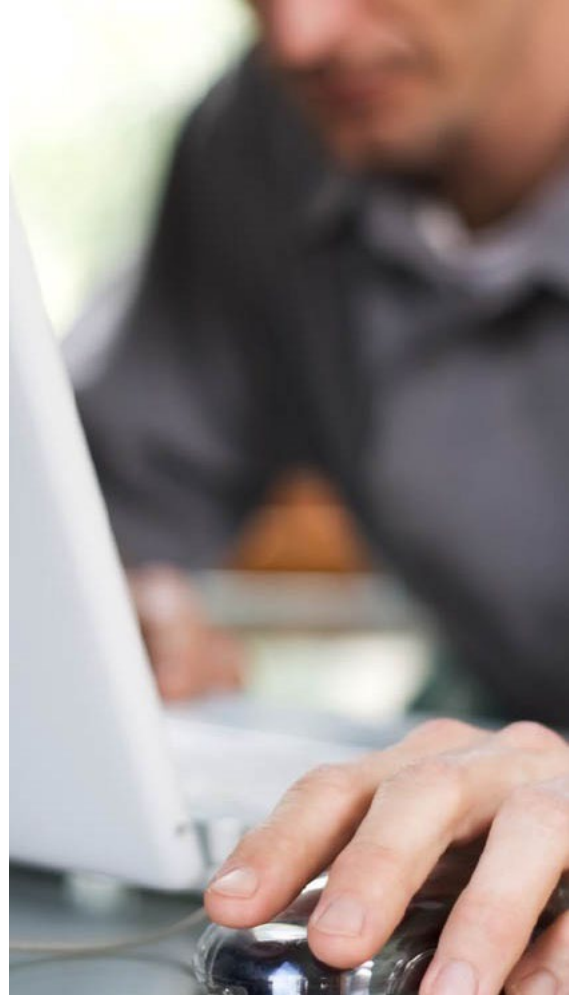
- WWW (http and https)
  - Scrape live sites with wget script
- DNS
- Email
- Tor
- Bitcoin

## Greybox (Internet in a box)

- Leverages the CORE open-source network simulator
- 70+ routers (containers) running BGP
- All TopGen services running

TopGen and Greybox

# DEMO





# GHOSTS in the Machine

Orchestrating Non-Player Characters (NPC)  
for a Realistic Cybersecurity Exercise Battlefield

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

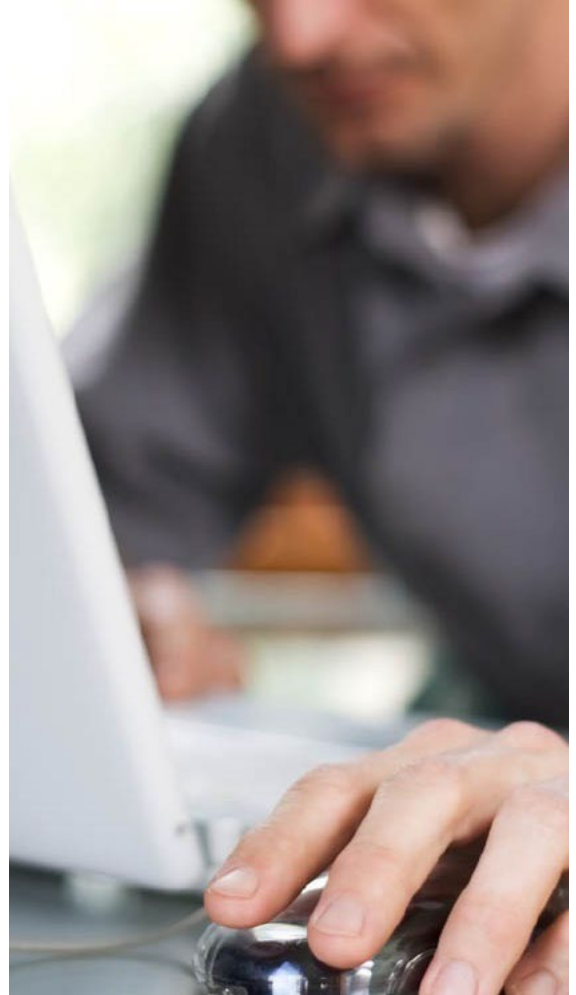
# GHOSTS orchestrates realistic NPCs that:

- Are behaviorally accurate, fully-autonomous & represent an infinite array of possible interactions (from harmless administrators to hostile nation-state attackers)
- Match training realism with high training value
- Prepare effective cyber warfare teams for success in real-world situations



GHOSTS NPC Orchestration

# DEMO







# WELLE-D

## Wireless Emulation Link-Layer Exchange Daemon

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# WELLE-D

## Wireless Emulation Link-Layer Exchange Daemon

Leverages frames from mac80211\_hwsim driver

Uses VSOCK to transfer frames

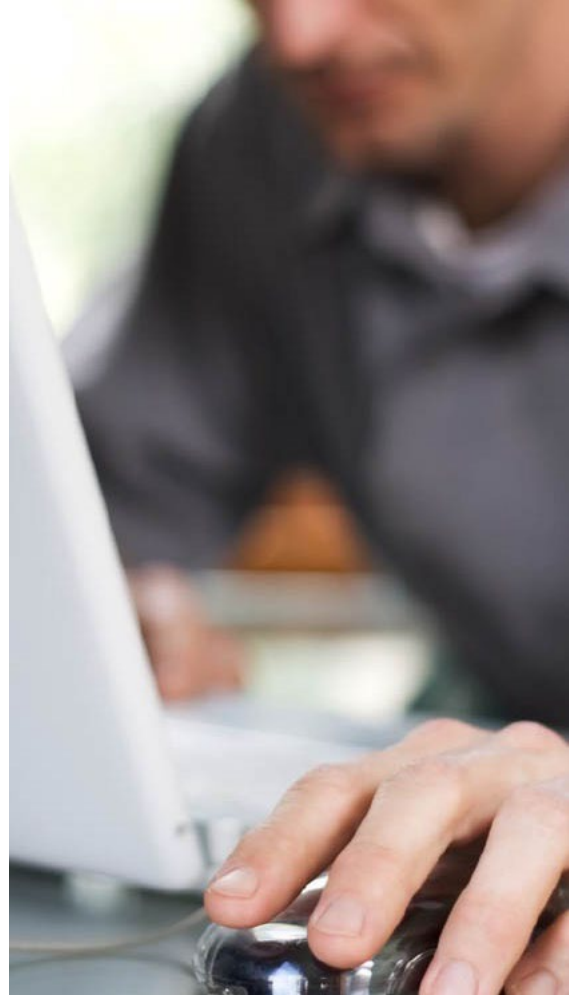
Simulates wireless medium

Provides GPS simulation

Enables high-fidelity use of full-featured operating systems



WELLE-D  
DEMO





# SCADASim & FinSim

Industrial Control System and Banking Simulators

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# SCADASim – Features

Configurable PLCs

Modbus communications with HMIs

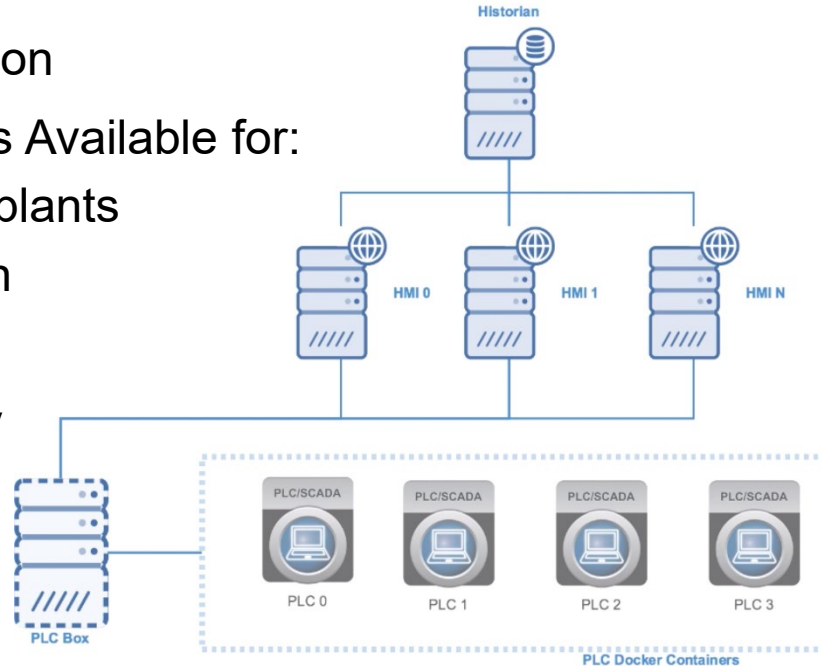
RapidSCADA integration

Sample Configurations Available for:

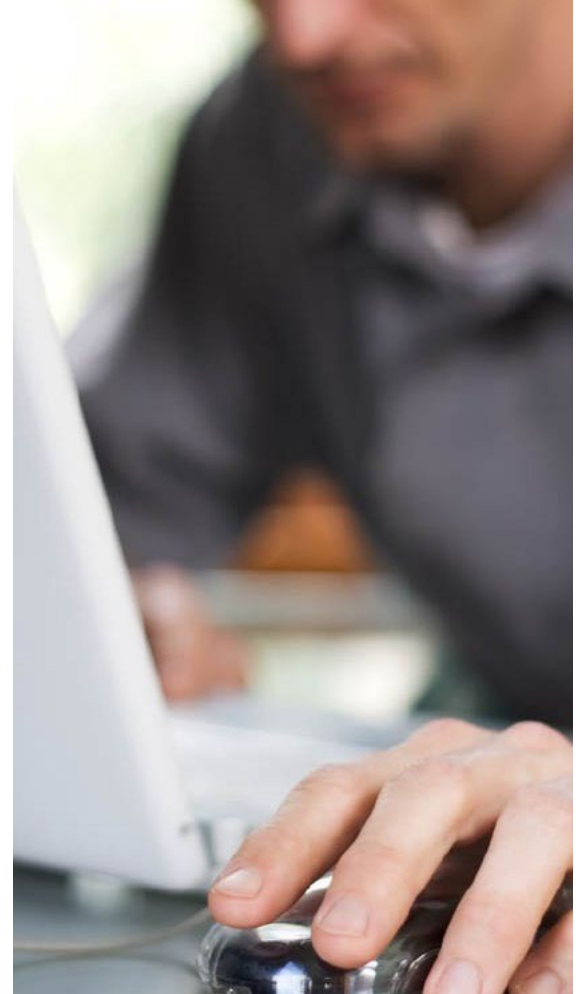
- Water treatment plants
- Power generation
- HVAC

Underlying technology

- Docker
- Postgres
- JSON



SCADASim  
**DEMO**





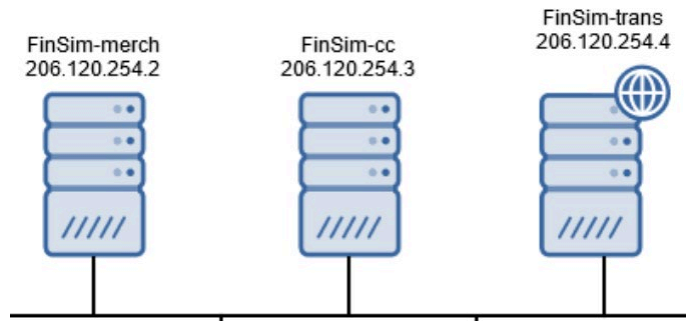
# FinSim – Features

Model financial system within a training environment

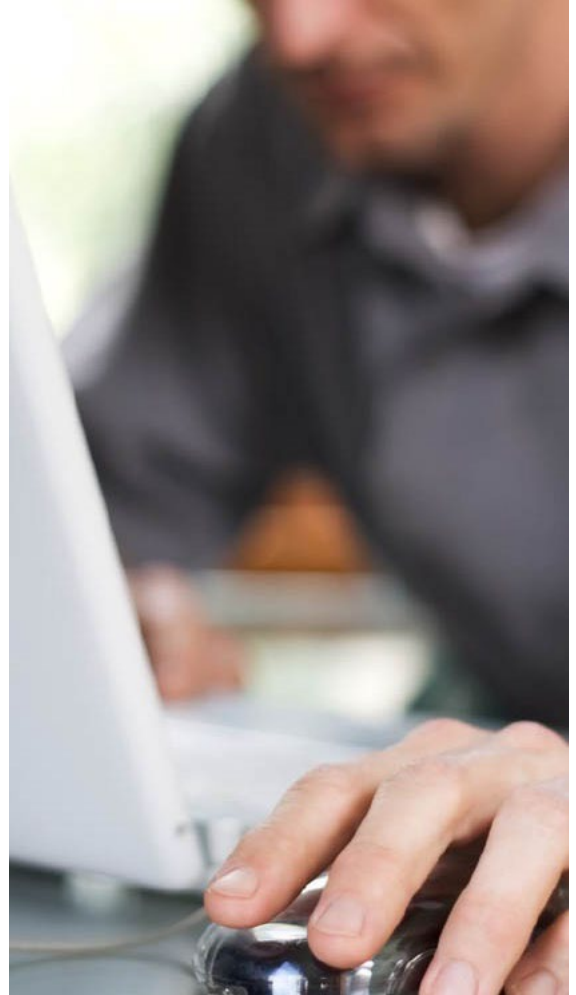
- Banks (accounts and web interface)
- Credit Card processors
- Merchants

Underlying technology

- Python
- Angular
- Flask
- MySQL
- JSON Web Tokens (JWT)

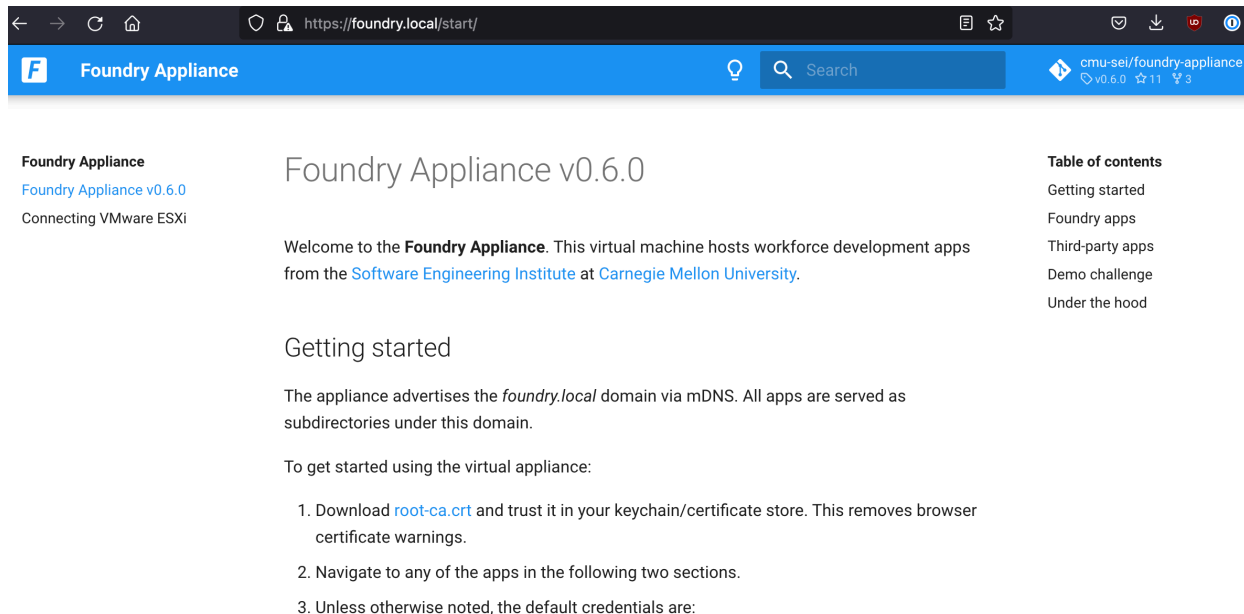


FinSim  
**DEMO**



# Foundry Virtual Appliance

Ubuntu virtual machine  
Docker and Kubernetes  
TopoMojo  
Gameboard  
PostgreSQL Database



The screenshot shows a web browser window with the address bar displaying `https://foundry.local/start/`. The page title is "Foundry Appliance". The main content area has a header "Foundry Appliance v0.6.0" and a welcome message: "Welcome to the **Foundry Appliance**. This virtual machine hosts workforce development apps from the [Software Engineering Institute](#) at [Carnegie Mellon University](#)." Below this is a section titled "Getting started" with the text: "The appliance advertises the *foundry.local* domain via mDNS. All apps are served as subdirectories under this domain." and "To get started using the virtual appliance:". A numbered list follows: 1. Download [root-ca.crt](#) and trust it in your keychain/certificate store. This removes browser certificate warnings. 2. Navigate to any of the apps in the following two sections. 3. Unless otherwise noted, the default credentials are:

On the left side of the page, there is a sidebar with the text: "Foundry Appliance", "Foundry Appliance v0.6.0", and "Connecting VMware ESXi". On the right side, there is a "Table of contents" section with links: "Getting started", "Foundry apps", "Third-party apps", "Demo challenge", and "Under the hood".

# Use Case: CISA President's Cup

- Presidential Executive Order 13870
- Cyber competition among DoD and federal executive workforce solving challenges
- 1,000s of individual and team participants
- Integrate immersive (gamified) experiences
- Platform and challenges released as open-source



<https://presidentcup.cisa.gov/>

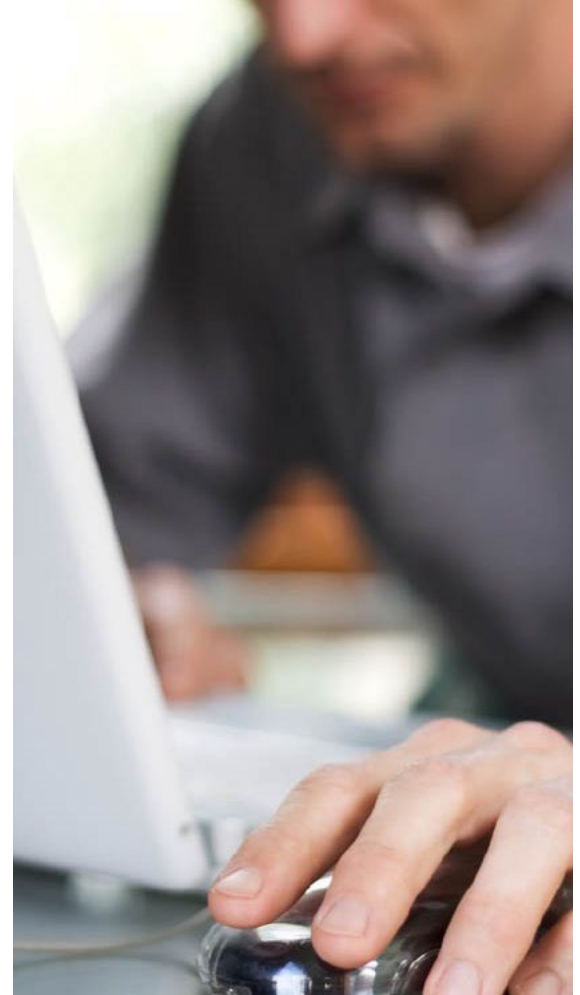
# Resources and Contact Info

<a href="https://sei.cmu.edu/go/cwd-tools">https://sei.cmu.edu/go/cwd-tools</a>	<a href="https://github.com/cmu-sei/vtunnel">https://github.com/cmu-sei/vtunnel</a>
<a href="https://github.com/cmu-sei/crucible">https://github.com/cmu-sei/crucible</a>	<a href="https://github.com/cmu-sei/welled">https://github.com/cmu-sei/welled</a>
<a href="https://github.com/cmu-sei/TopoMojo">https://github.com/cmu-sei/TopoMojo</a>	<a href="https://github.com/cmu-sei/SCADASim">https://github.com/cmu-sei/SCADASim</a>
<a href="https://github.com/cmu-sei/topgen">https://github.com/cmu-sei/topgen</a>	<a href="https://github.com/cmu-sei/finsim">https://github.com/cmu-sei/finsim</a>
<a href="https://github.com/cmu-sei/greybox">https://github.com/cmu-sei/greybox</a>	<a href="https://github.com/cmu-sei/foundry-appliance">https://github.com/cmu-sei/foundry-appliance</a>
<a href="https://github.com/cmu-sei/GHOSTS">https://github.com/cmu-sei/GHOSTS</a>	<a href="https://github.com/cmu-sei/Crucible.Appliance">https://github.com/cmu-sei/Crucible.Appliance</a>

Chris May: [cjm@cert.org](mailto:cjm@cert.org)  
[info@sei.cmu.edu](mailto:info@sei.cmu.edu)

# Challenge Time!

<https://iupsec.cmusei.dev/>







# Questions ?