

Capabilities Overview

13 JUL 2021

Cyber Workforce Development Directorate

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2021 Carnegie Mellon University.

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.

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

DM21-0629

Agenda

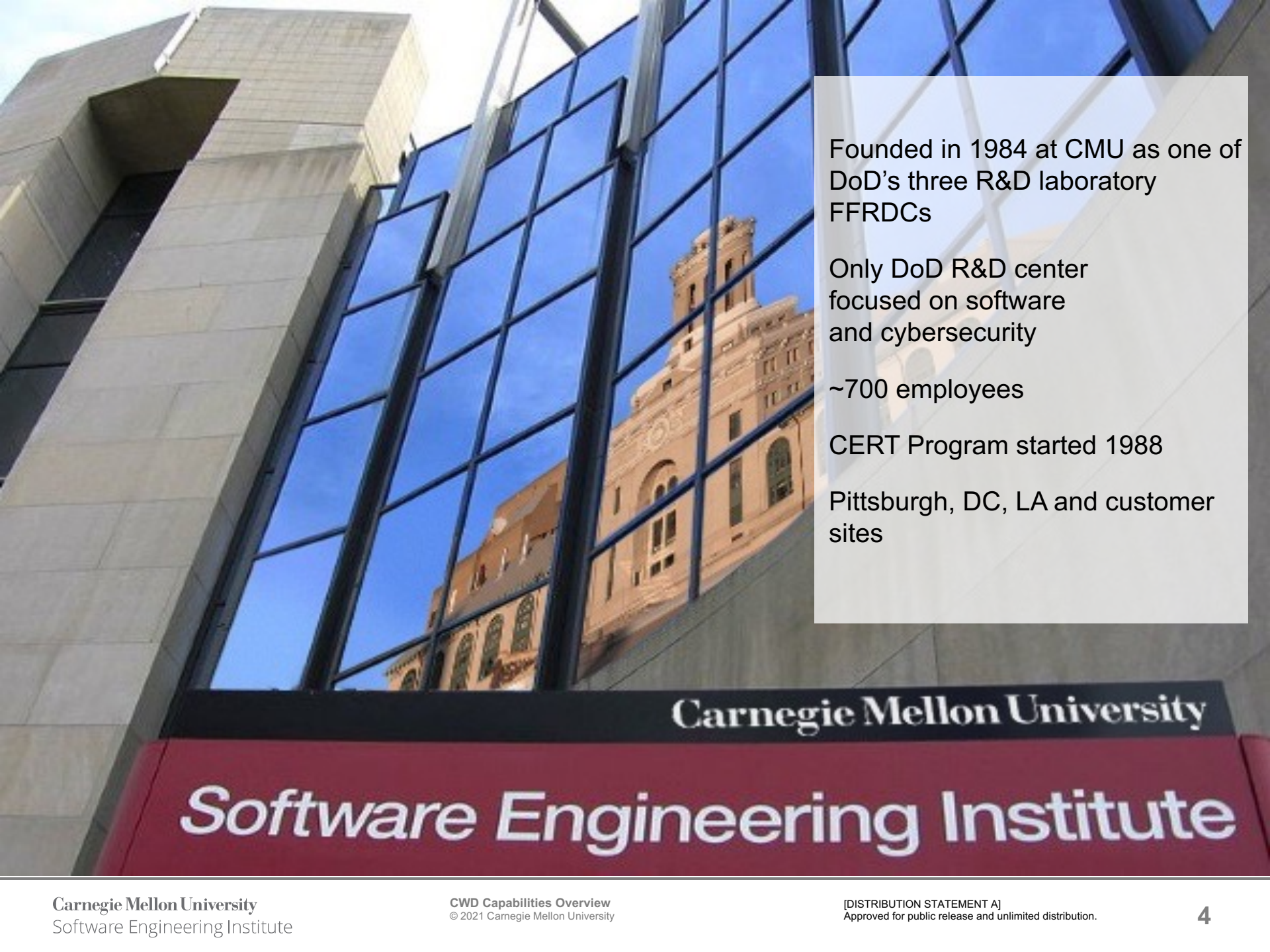
Meeting Objectives

SEI Overview

Sample Cybersecurity Workforce Development Programs

SEI Platforms

Next Steps



Founded in 1984 at CMU as one of
DoD's three R&D laboratory
FFRDCs

Only DoD R&D center
focused on software
and cybersecurity

~700 employees

CERT Program started 1988

Pittsburgh, DC, LA and customer
sites

Carnegie Mellon University

Software Engineering Institute

Cyber Workforce Development Directorate

Mission

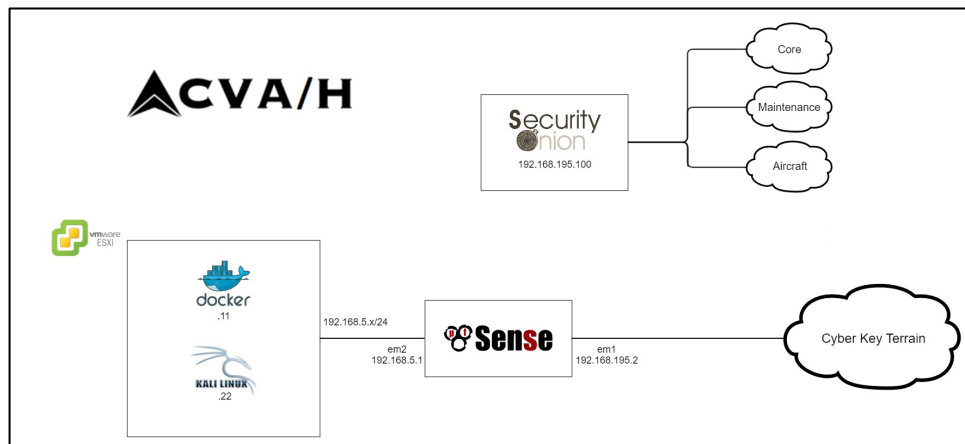
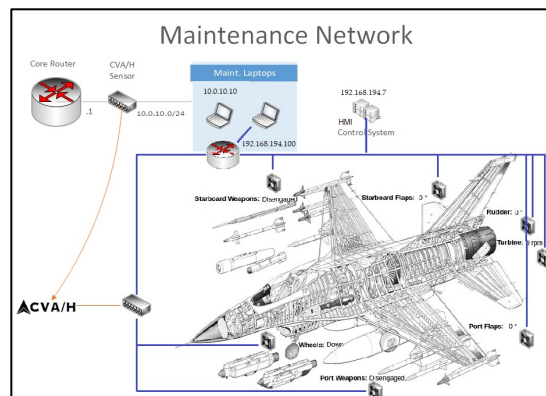
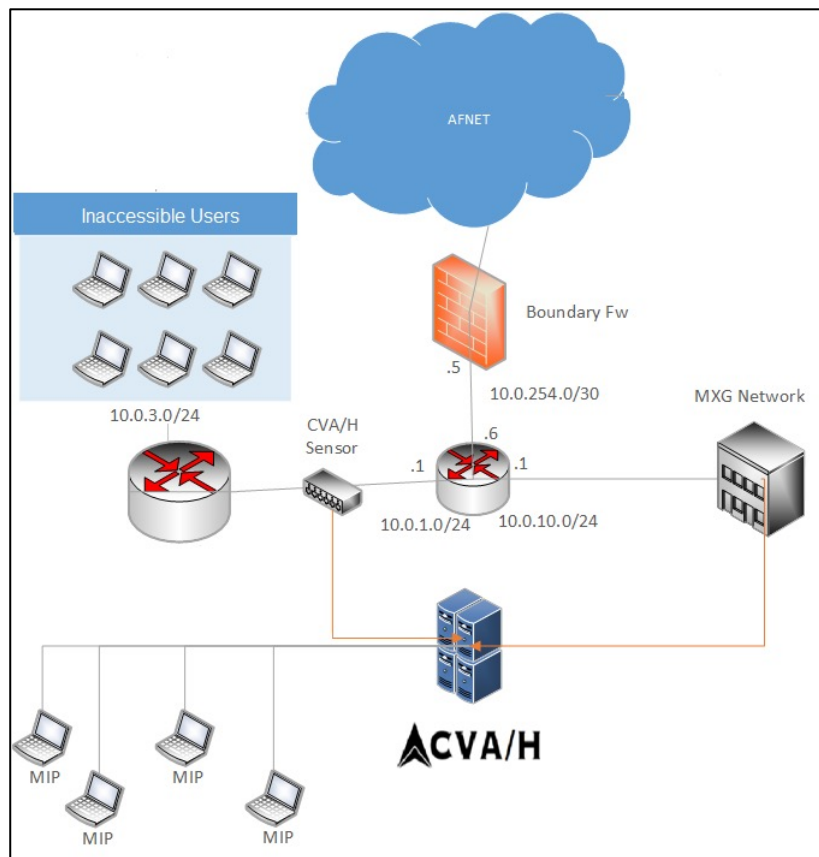
Provide force-multiplying solutions to rapidly grow and strengthen DoD's cybersecurity workforce--addressing the problems of **time**, **scale**, and **cost**

- We develop and transition cutting-edge **Prototypes and Content**
 - Training creation and delivery platforms
 - Joint Force level exercises
 - Modeling and simulation tools
 - Custom cybersecurity content





Network/System Modeling and Instrumentation



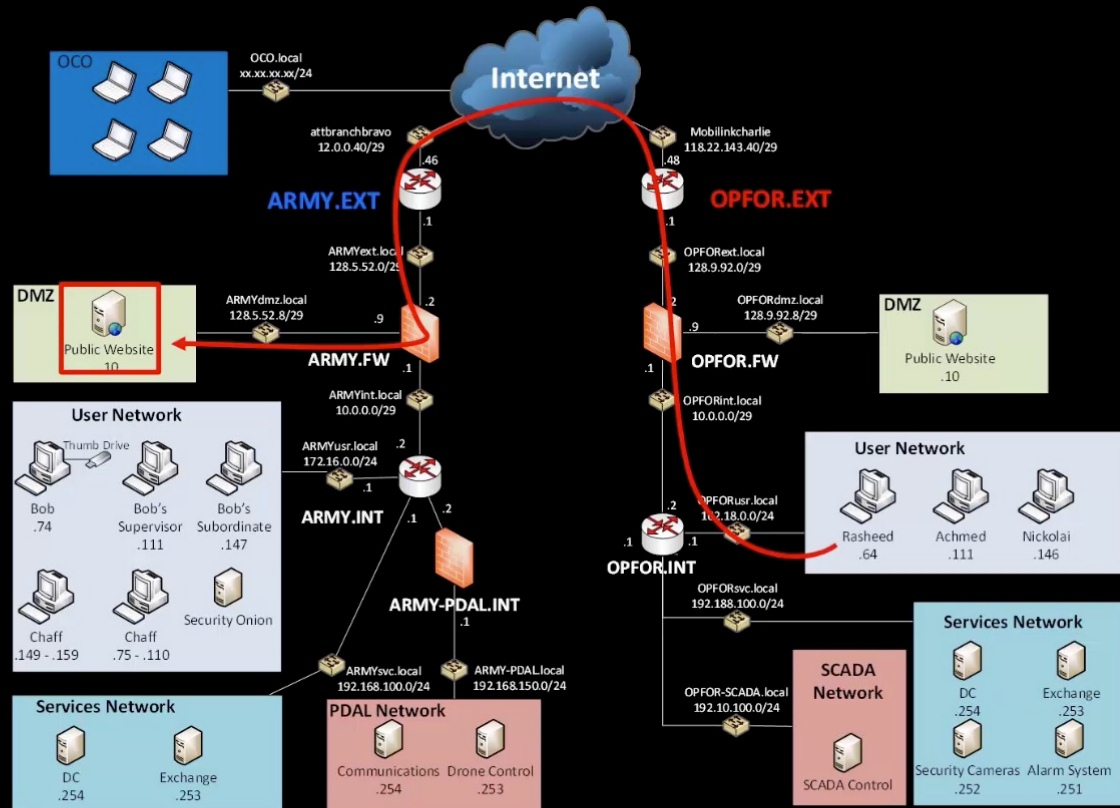
More than 39,000 hours of training delivered
to Air Force Mission Defense Teams since 2017

Cyber-Kinetic Effects Integration

Phase 1: Insertion



BLUE gains foothold on island..



..RED gains foothold in network

Critical Infrastructure Scenarios and Simulators



Chemical



Communications



Dams



DIB



Energy



Healthcare



Transportation



Water/Waste



Financial Services



Government Facilities

X-Games: ICS/SCADA DCO team exercises *on-demand, automated performance assessment*

The screenshot displays the Cyberforce portal interface. At the top, a red navigation bar contains the 'Cyberforce' logo, a menu of icons, a search bar with the text 'Content', and a user profile for 'YARGER.JOHN.W'. Below the navigation bar, the breadcrumb 'BROWSE CONTENT / X-GAMES: OPERATION COLT' is visible. The main content area features a large video player on the left showing soldiers in combat gear. To the right of the video, the title 'X-Games: Operation Colt' is displayed, followed by the date 'Added: July 12, 2021' and the author 'William.Reed'. A paragraph of text describes the exercise: 'The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. In this exercise, teams can choose from ten different sectors of critical infrastructure to defend against simulated cyber attacks.' Below the video player is a green 'Launch' button and three circular icons (list, settings, bookmark). At the bottom, a horizontal bar contains the labels 'EXERCISE', 'CRITICAL INFRASTRUCTURE', 'ICS/SCADA', and 'XGAMES', along with a 'Flag Content' link.

<https://portal.cyberforce.site/content/1746/x-games-operation-colt>

Platform Options

SEI built and hosted:

<https://cyberforce.site> (USCYBERCOM sponsored; CAC-only)

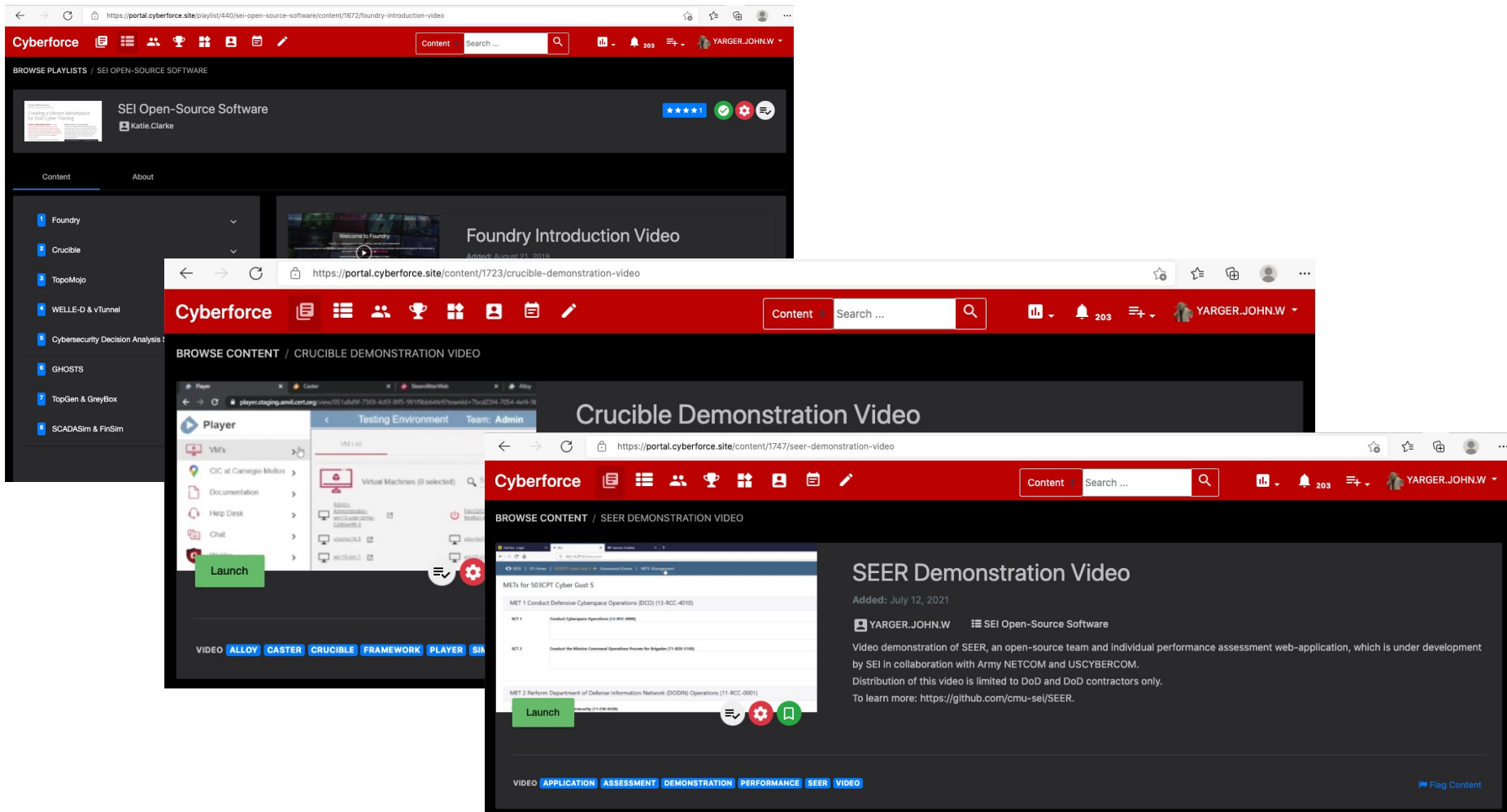
<https://gauntlet.sei.cmu.edu> (PIV, CAC, +; all-Azure; INDOPACOM)

SEI built, government owned/transitioned:

<https://hamilton.treasury.gov>

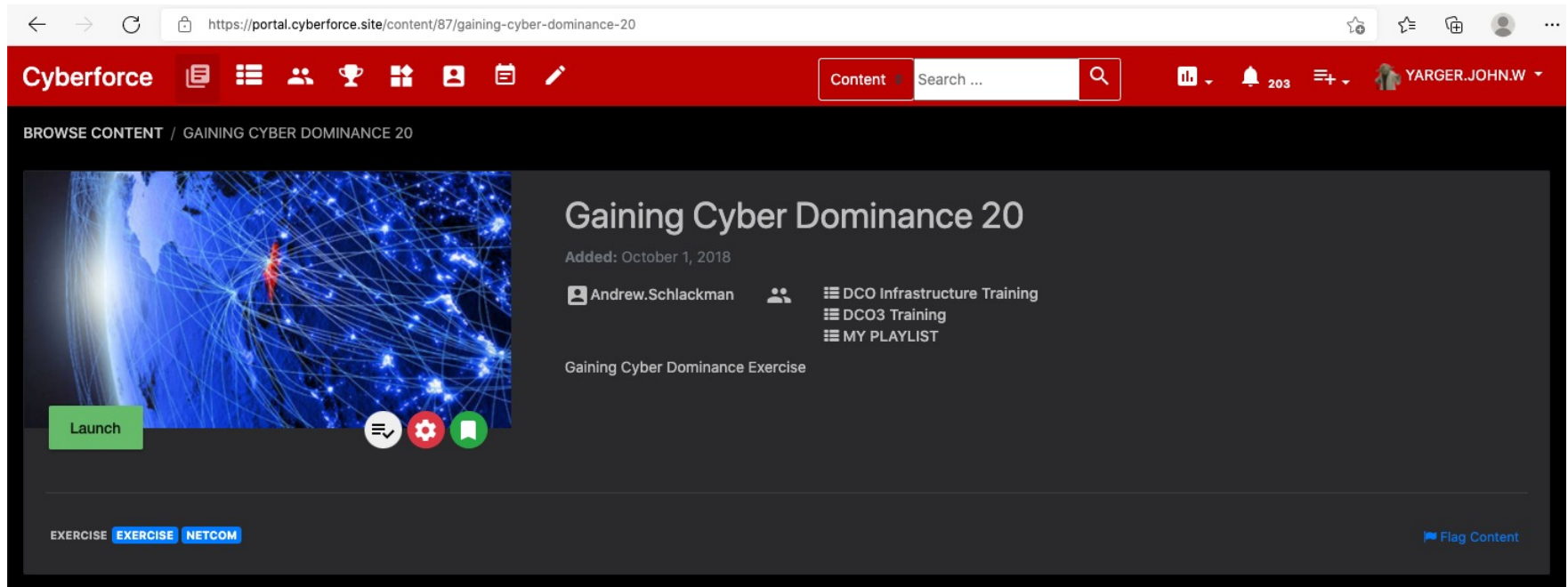
<https://presidentcup.cisa.gov/>

SEI Open-Source Software info playlist



<https://portal.cyberforce.site/playlist/440/sei-open-source-software/>

GCD: Regional Cyber Center exercise series *annual, persistent, facilitated*



The screenshot shows a web browser window with the URL <https://portal.cyberforce.site/content/87/gaining-cyber-dominance-20>. The page features a red header with the Cyberforce logo and navigation icons. Below the header, the breadcrumb trail reads "BROWSE CONTENT / GAINING CYBER DOMINANCE 20". The main content area displays a large image of a globe with network connections, a "Launch" button, and the title "Gaining Cyber Dominance 20". The page also shows the author "Andrew.Schlackman", the date "Added: October 1, 2018", and a list of related content including "DCO Infrastructure Training", "DCO3 Training", and "MY PLAYLIST". At the bottom, there are tags for "EXERCISE", "EXERCISE", and "NETCOM", and a "Flag Content" link.

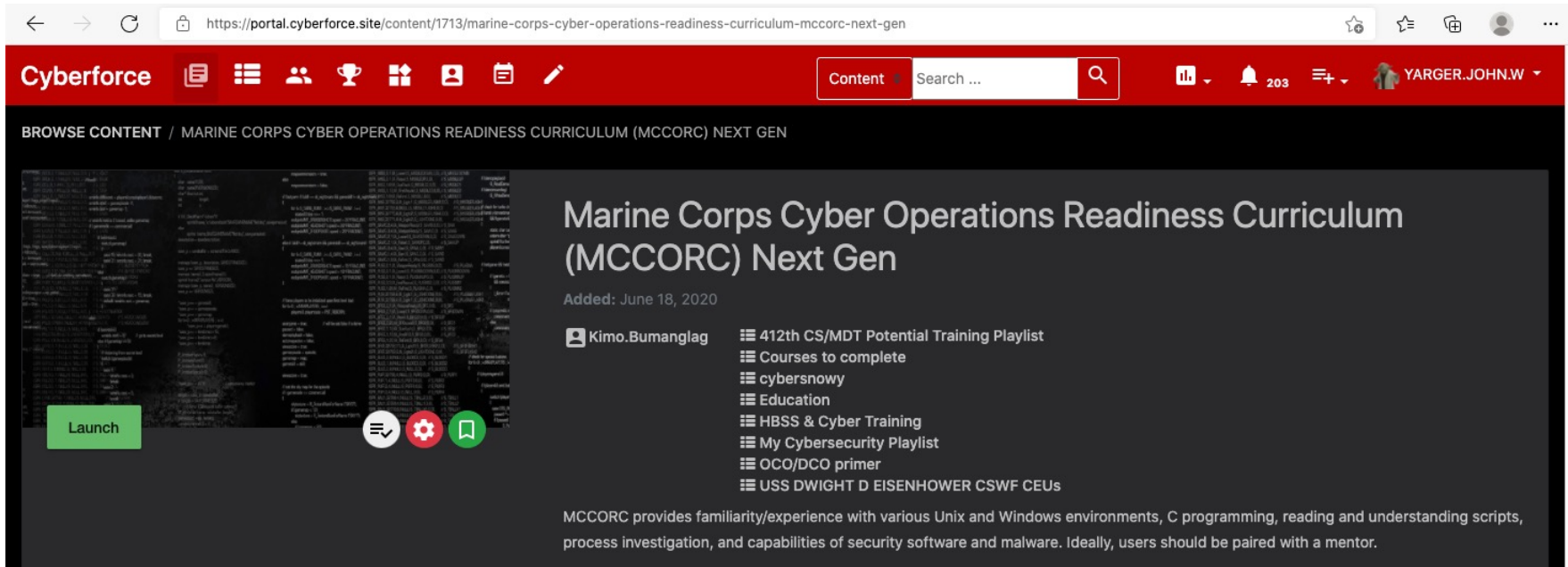


Army Network Enterprise Technology Command

<https://portal.cyberforce.site/content/87/gaining-cyber-dominance-20>

MCCORC: pre-RIOT ION training

5-wk, hand-on Linux/Windows content



The screenshot shows a web browser window with the URL <https://portal.cyberforce.site/content/1713/marine-corps-cyber-operations-readiness-curriculum-mccorc-next-gen>. The page header is red with the Cyberforce logo and navigation icons. The main content area is dark grey and features a large image of a terminal window on the left with a green 'Launch' button. To the right, the title 'Marine Corps Cyber Operations Readiness Curriculum (MCCORC) Next Gen' is displayed, followed by the date 'Added: June 18, 2020' and a list of tags including '412th CS/MDT Potential Training Playlist', 'Courses to complete', 'cybersnowy', 'Education', 'HBSS & Cyber Training', 'My Cybersecurity Playlist', 'OCO/DCO primer', and 'USS DWIGHT D EISENHOWER CSWF CEUs'. A paragraph at the bottom states: 'MCCORC provides familiarity/experience with various Unix and Windows environments, C programming, reading and understanding scripts, process investigation, and capabilities of security software and malware. Ideally, users should be paired with a mentor.'



Marine Corps Forces Cyberspace Command

<https://portal.cyberforce.site/content/1713/marine-corps-cyber-operations-readiness-curriculum-mccorc-next-gen>

Search workspace

workspace gamespace refresh

Moodle Test

PresCup R2 Individuals - PD 1000

PresCup R2 Individuals - PD 1000 3

President's Cup Season 2 - a01

President's Cup Season 2 - b01

President's Cup Season 2 - t01

Settings Templates Document Challenge Files Play

President's Cup Season 3 - t01

Settings Templates Document Challenge Files Play



975bec0f-e6ce-4498-9031-a1242f713a21

President's Cup Season 3 - t01

Settings Templates Document Challenge Files Play

Launch Count: 61
Last Activity: 2021-07-12T20:57:23.158652+00:00

Title

President's Cup Season 3 - t01

Description

Short description to display when browsing titles

Authorship

Christopher.Herr

text to indicate authorship of this resource

Audience

prescup cisa-playtest

space-delimited list of clients that can launch this as a gamespace

Foundry Appliance v0.1.0

Welcome to the Foundry Appliance. This virtual machine hosts workforce development apps from the [Software Engineering Institute](#) at [Carnegie Mellon University](#).

Getting Started

The appliance advertises the *foundry.local* domain via mDNS. All apps are served as directories under this domain.

To get started using the virtual appliance:

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:
`user: administrator@foundry.local`
`pass: foundry`
`code: 123456`

Foundry Apps

The following Foundry applications are loaded on this appliance:

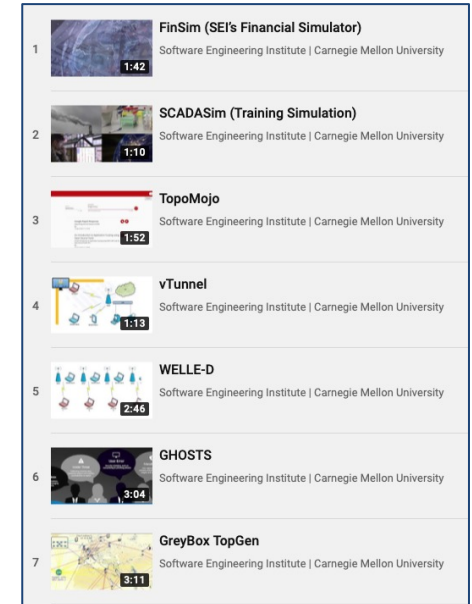
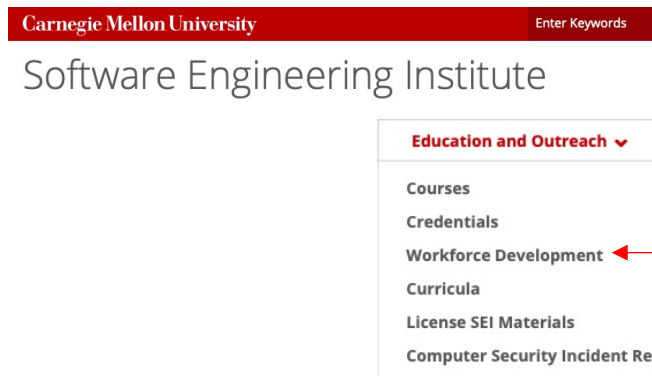
location	description
/identity	<i>Identity</i> manages logins/credentials across all of the apps. It can integrate with any

Next Steps

- SEI Software Prototypes, <https://code.sei.cmu.edu/bitbucket/projects/CWD>
- Cyberforce, <https://cyberforce.site>
- Project Work Plan (PWP)
 - Tech transition (e.g. CYBERCOM, MARFOR, 318th)
 - Crucible
 - Foundry Appliance for existing hardware?
 - Content?
 - Content Dev
 - Network/System Modeling
 - Threat emulation
 - Tool development and/or deployment guidelines
- Other Initiatives
 - Cloud transition
 - INDOPACOM
 - President's Cup transition to DHS managed Azure

More Info

- SEI YouTube, <https://www.youtube.com/user/TheSEICMU>
- SEI Open-Source Mod/Sim Tools Playlist, <https://portal.cyberforce.site/playlist/440/sei-open-source-mod-sim-tools/>
- SEI Website, <https://sei.cmu.edu>



Simulation Tools Playlist,
<https://www.youtube.com/playlist?list=PLSNIEg26NNpZr5mxy75HYitSQQFEex4Yc>