CYBER DEFENSE EDUCATION & TRAINING

Meeting the Future Workforce Needs of Tomorrow

Strategy and Goals

CISA's Cyber Defense Education and Training (CDET) plays a critical role as a driver for thought leadership and building trusted partnerships in cyber education and training for the nation to enable the cyber-ready workforce of tomorrow. CDET leverages and accelerates cyber education and training to strengthen people, partnerships, and protect critical infrastructure.

People

Goal 1

Increase Access to Unrealized Cyber Talent

Partnerships

Goal 2

Accelerate Robust Collaborations and Alliances

Protecting Critical Infrastructure

Goal 3

Reduce Risk to Critical Infrastructure

Programs


Incident Response Training
PRESIDENT'S CUP
CYBERSECURITY COMPETITION
Industrial Control Systems
Zero Trust
PRESIDENT'S CUP
CYBERSECURITY COMPETITION
Practice Area
Federal Cyber Defense Skilling Academy
PISCES
CATER COI
FedVTE
DASHBOARD

President's Cup Cybersecurity Competition

Cyber threats across the globe have put into focus our country's need for cyber talent. CISA developed the President's Cup Cybersecurity Competition to identify, recognize, and reward the best cyber talent within the federal workforce who face these threats.

The President's Cup strengthens the federal cybersecurity workforce by providing a robust array of training materials designed around the NICE Framework, and by boosting the pipeline through increased recognition of the cybersecurity profession.

A Unique Training Experience

The competition's challenges are designed to stretch competitors' abilities and test their aptitudes through a fun, unique experience. By couching the competition in a video game setting, participants have a training activity that encourages fun and creativity while expanding their cybersecurity skill sets. To try your hand at past challenges, visit the President's Cup Practice Area!

1,400

Federal Employees

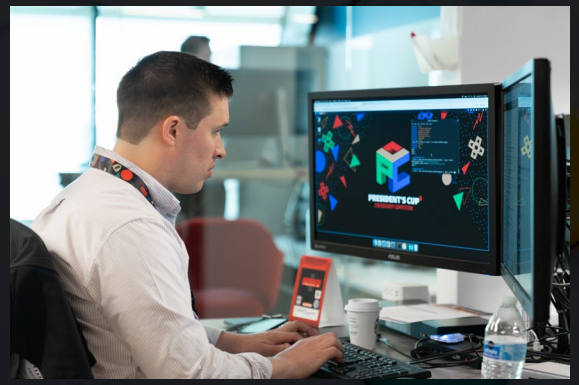
39

Government departments and agencies

The fifth annual President's Cup had over 1,400 federal employees compete in the competition. Participants came from at least 39 different federal government departments and agencies, including the Departments of Defense, Homeland Security, Justice, and many others.

President's Cup 5

PRESIDENT'S CUP
CYBERSECURITY COMPETITION



PCV Winners

Individuals Track A	Individuals Track B	Teams
nolax U.S. Army	mtu U.S. Marine Corps	Artificially Intelligent U.S. Army, U.S. Air Force, DoD

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Practice Area and Skilling Labs

- https://presidentscup.cisa.gov/gb/practice

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

President's Cup Platform

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

- Hosted within CISA owned AWS environment
- Accessible anywhere from a standard web browser
- Scalable to support potentially thousands of concurrent participants
- Open-Source Resources
  - TopoMojo – https://github.com/cmu-sei/TopoMojo
  - Gameboard - https://github.com/cmu-sei/Gameboard
  - GitHub - https://github.com/cisagov/prescup-challenges
  - YouTube - Highlights from the Fourth Annual President's Cup Cybersecurity Competition (youtube.com)

Cyber Defense Skilling Academy

The Federal Cyber Defense Skilling Academy helps students develop their cyber defense skills through training in the baseline knowledge, skills, and abilities of various cybersecurity work roles. Students will have the opportunity to temporarily step away from their current position to focus on professional growth through an intense, full-time, three-month accelerated training program. Full-time, federal employees in any job series and any grade or grade equivalent for non-GS employees are eligible to apply to the Skilling Academy.

Providing Lifelong Skills and Certifications

The course is mapped to the NICE Cybersecurity Workforce Framework and provides valuable opportunities to practice new cyber skills in a virtual lab environment.

900+
Applications

500+
Graduates

17
Departments and Agencies

Since its launch in 2021, CISA has received more than 900 applications from 17 Departments and Agencies, successfully graduating more than 500 students. The Skilling Academy will enter into its fourth year in FY25.

Cyber Defense Skilling Academy

Cyber Defense Analyst Pathway *Launched in FY22*

Goal: Develop skills required to utilize data gathered from diverse cyber defense tools and analyze events within their environment to mitigate potential cyber threats.

Eligible Certification: CompTIA's Security+ (Sec+)

Framework Alignment: Cyber Defense Analyst | NICCS (cisa.gov)

Cyber Defense Forensics Analyst Pathway *Launched in FY24

Goal: Develop the skills required to investigate and analyze digital evidence in support of vulnerability mitigation.

Eligible Certification: EC Council's Computer Hacking Forensic Investigator (CHFI)

Framework Alignment: Cyber Defense Forensics Analyst | NICCS (cisa.gov)

Cyber Defense Incident Responder Pathway *Launched in FY24

Goal: Develop the skills required to accurately identify, assess, and mitigate security incidents within a digital environment.

Eligible Certification: CompTIA's Cybersecurity Analyst (CySA+)

Framework Alignment: Cyber Defense Incident Responder | NICCS (cisa.gov)

Vulnerability Assessment Analyst Pathway *Launched in FY24

Goal: Develop skills required to engage in penetration testing and vulnerability management to prevent cyberattacks.

Eligible Certification: CompTIA's Penetration Testing (PenTest+)

Framework Alignment: Vulnerability Assessment Analyst | NICCS (cisa.gov)

Cyber Defense Skilling Academy

Objective: To ensure that the Skilling Academy remains at the forefront of cybersecurity education, exploration for new course offerings is an integral part of our commitment to provide industry relevant training in high impact cyber domains. The new topics anticipated to launch in FY25 are below:

Artificial Intelligence/Machine Learning

Goal: Develop skills required to design, develop, and modify AI applications, tools, and/or other solutions to enable successful accomplishment of mission objectives.

Framework Alignment: AI/ML Specialist – DoD Cyber Exchange

Systems Security Analyst

Goal: Develop skills required to conduct analysis and execute integrations, testing, operations, and maintenance of systems security.

Framework Alignment: Systems Security Analyst | NICCS (cisa.gov)

Cyber Defense Infrastructure Support Specialist

Goal: Develop skills required to deploy, implement, test, operate and maintain, review, and administer the infrastructure hardware and software that are required to effectively manage computer network defense service provider network and resources.

Framework Alignment: Cyber Defense Infrastructure Support Specialist | NICCS (cisa.gov)

Micro-course Topics

- ✓ IT Fundamentals
- ✓ Threat Analysis
- ✓ Incident Detection Response & Handling
- ✓ Digital Forensics
- ✓ Vulnerability Assessment/Pentesting
- ✓ AI Security Essentials

Industrial Control Systems

The security of industrial control systems (ICS) is among the most important aspects of CISA's collective effort to defend cyberspace. The ICS trainings are a symbol of CISA's commitment to working with the ICS community to address both urgent operational cyber events and long-term ICS risks.

The ICS Training avenues include:

- On Demand Training
  - Additional content added regularly
- Scheduled Online Training
  - Featuring the 301V and 401V courses, which run on a schedule
- Instructure-Led, In-Person Training
  - Featuring the 301L and 401L courses hosted by the Idaho National Laboratory (INL) in Idaho Falls, ID
- Regional Training
  - Virtual regional training events in support of the 10 CISA regions.

ICScape Rooms

The ICS training program is currently offering "ICScape rooms" that enable cyber teams to solve puzzles within a controlled system environment. Using a "game" type approach, the teams attempt to "escape" and beat the clock to achieve different goals, such as using reconnaissance, network discovery, and penetration testing tools.

Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) trainings optimize agencies' ability to utilize the CDM dashboard, which affords increased situational awareness across their networks.

The CDM trainings equip agencies with the skills that provide benefits such as:

- Increased **automation to identify assets**
- Improved **accuracy, reporting, risk management, decision making, and incident response**
- Enhanced **near-real-time monitoring and risk**
- **Streamlined compliance** with the Federal Information Security Modernization Act (FISMA) and other federal cybersecurity mandates and initiatives
- **Improved visibility and situational awareness** within agencies and across the federal government

A CDM training for everyone

The CDM trainings are available through multiple avenues to better accommodate student needs. These avenues include In-Person, Virtual In-Person and On-Demand using the Cyber Training Range, Micro Learn Videos, and Webinars.

Incident Response

The best offense is a good defense. To best protect and support the capacity of our nation's cyber enterprise, CISA offers free Incident Response (IR) training courses that address the defensive view. These courses provide not only the knowledge and tools needed to prepare an effective response if a cyber incident occurs, but also how to prevent incidents from happening in the first place.

Awareness Webinars

Awareness webinars, also referred to as 100-level courses, are one-hour, entry-level, virtual, and instructor-led classes with cybersecurity topic overviews for a general audience, including managers and business leaders. These courses provide core guidance and best practices to prevent incidents, and how to prepare an effective response if an incident occurs.

Cyber Range Training

Cyber range trainings, also referred to as 200-level courses, are four-hour, interactive, virtual, and instructor-led classes, with step-action labs in a realistic technical environment. Students participate in short lectures, followed by lab activities, to identify incidents and harden systems in the cyber range environment.

On Demand Training

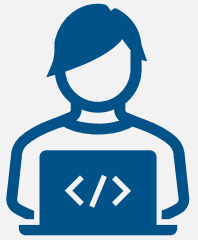
On-demand trainings are self-paced, available 24/7, and include two types of offerings: Step-By-Step Action Courses and Online Training Recordings.

Previously recorded training programs are available on the CISA YouTube Channel playlist and the Federal Virtual Training Environment (FedVTE)

Federal Virtual Training Environment (FedVTE)

The Federal Virtual Training Environment (FedVTE) provides cybersecurity education and training to federal employees.

- **Certification Prep**
  FedVTE offers certification prep courses on topics such as Ethical Hacking, Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP).
- **NICE Framework**
  All FedVTE courses are aligned with the NICE Cybersecurity Workforce Framework work roles, so you can find courses that are the most applicable to your role.



Training for everyone

FedVTE also provides various free public training courses ranging from beginner to advanced levels.

Zero Trust

Zero trust (ZT) is an approach where access to data, networks, and infrastructure is kept to what is minimally required, and the legitimacy of that access must be continuously verified. CISA seeks to further the federal government's progress toward a ZT approach to cybersecurity in support of the National Cybersecurity Strategy.

CISA's Zero Trust Community

In FY23, CDET stood up the first CISA sponsored federal-wide Community of Practice (CoP). This one-of-a-kind CoP is made up of ZT SMEs from various agencies and allows members to share best practices, discuss lessons learned, ask questions, and build peer to peer relationships across the FCEB. This results in interagency ZT collaboration and agency-specific expertise and implementation readiness.

In addition to the trainings currently offered, CDET is developing future trainings that will further support the needs of the ZT Community.

88%

Pass Rate

52

FCEB Agencies

*CDET was responsible for the management and execution of the **Forrester Zero Trust Certification Program.** It is a self-paced, practitioner focused, cohort-based program that includes six modules over 60 days.*

Three cohorts in FY23 and six cohorts in FY24 saw a certification/pass rate of 88% with 52 agencies represented.

For more information, email: zerotrust@cisa.dhs.gov

Cybersecurity Awareness, Training, Education, and Research Community of Interest

The Cybersecurity Awareness, Training, Education, and Research (CATER) Community of Interest (COI) promotes collaboration in cybersecurity training efforts throughout the federal government and shares information on federally developed training activities, thereby reducing costs and avoiding duplication of effort.

Discussion Topics

- Artificial Intelligence (AI)
- Escape Rooms
- Cybersecurity Awareness Month
- Phishing
- Supply Chain Management
- Election Security
- Competitions
- Cyber Training and Education Programs

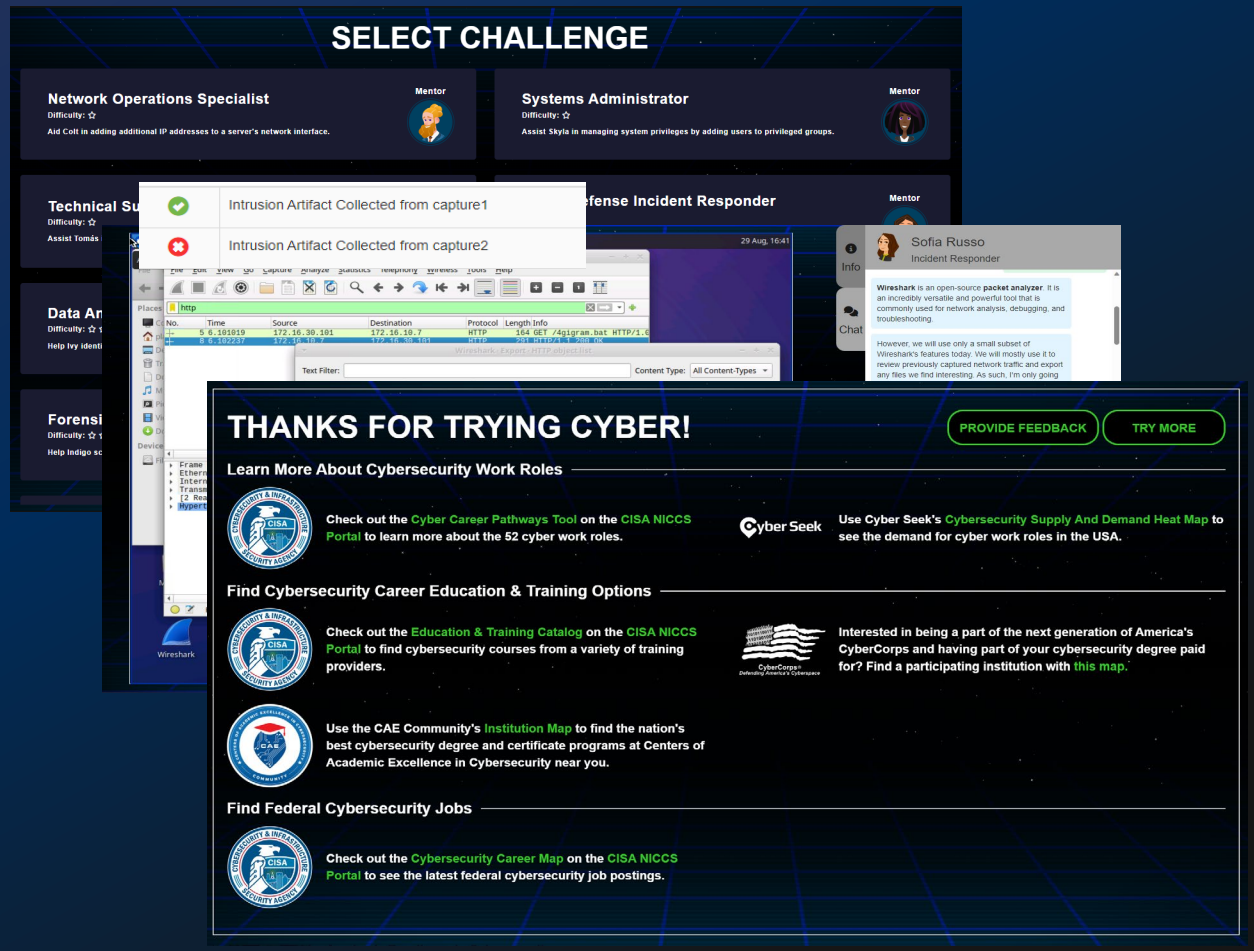
For questions about the CATER COI, send an email to catercoi@hq.dhs.gov.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Try Cyber

14 Micro-Challenges

Developed as resources for cybersecurity awareness and career exploration supporting the Cyber Careers Pathway Tool on the National Initiative for Cybersecurity Careers and Studies (NICCS®) website. The micro-challenges are quick, 15-minute, hands-on experiences that put users into cybersecurity workforce. **25,000+ user attempts since launch!**



15 Micro-Challenges (planned development)

Development will begin in 2025 to include both technical and non-technical cyber workforce roles.

TRY CYBER

https://trycyber.us/


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

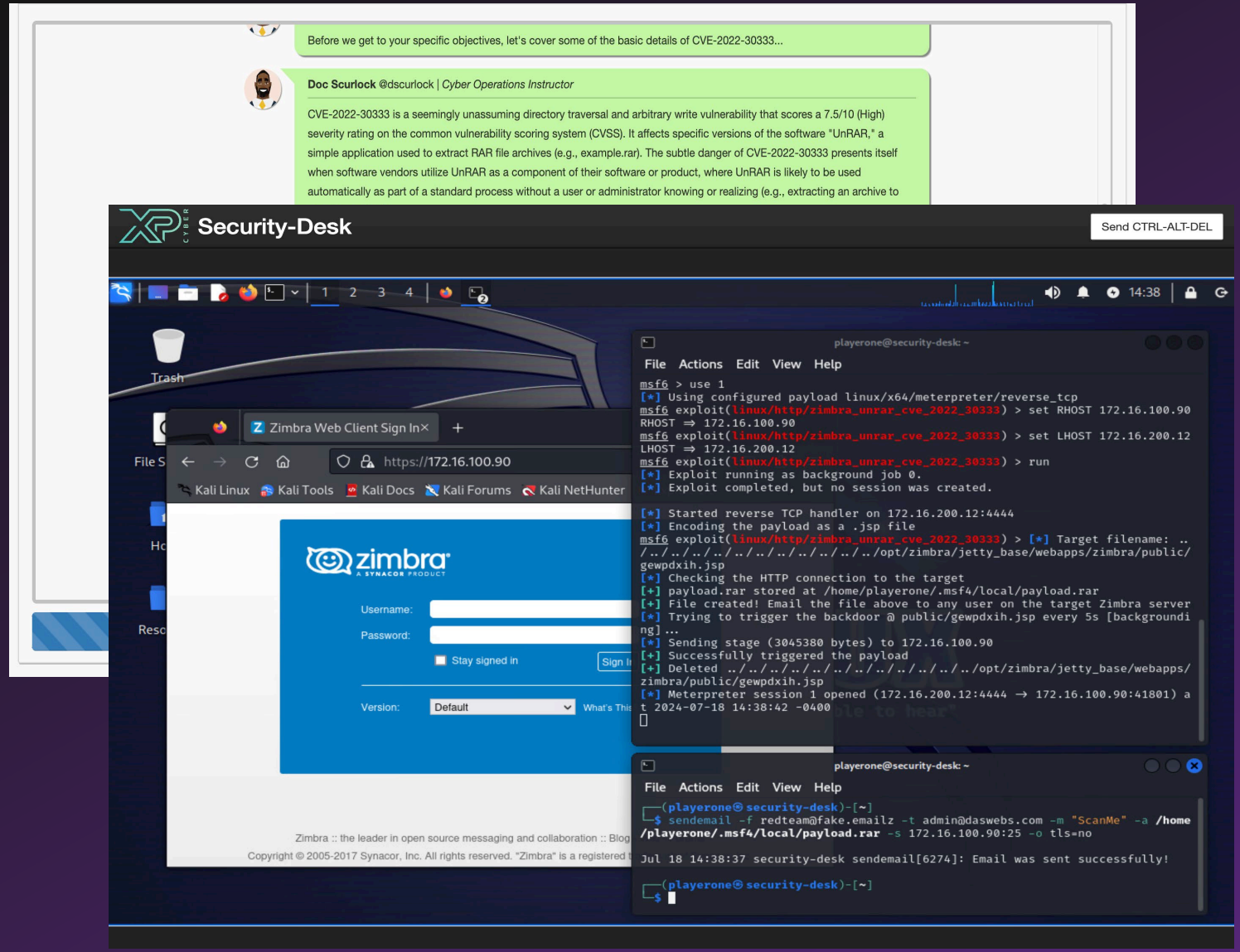
Experience Cyber

Threat Sandbox Challenges*

12 Threat Sandbox Challenges identified in the CISA Known Exploited Vulnerabilities (KEVs) Catalog. The Threat Sandbox Challenges will create an environment for students to learn the tools, techniques, and procedures (TTPs) involved in exploiting and mitigating critical and high vulnerabilities.

**Geared towards students pursuing cybersecurity degree programs.*

Launching September 2024



https://nice-challenge.com/

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

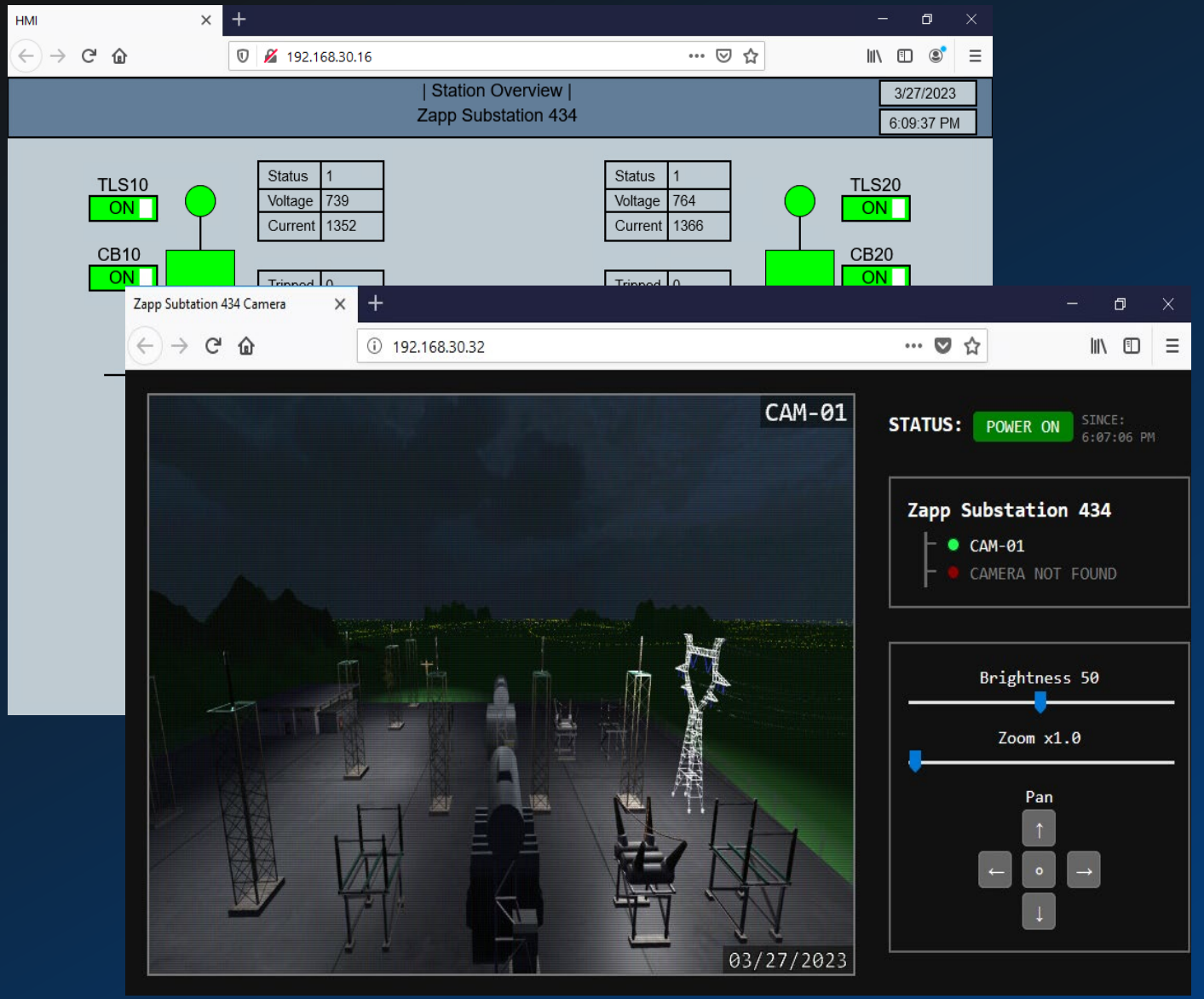
Experience Cyber

Industrial Control System Challenges*

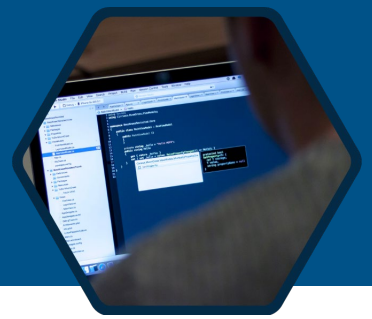
6 Industrial Control System Challenges focused on commonly seen security issues at an electrical substation. The challenges are used by NCAE-C students to assess their competency in addressing in operational technology and industrial control system virtual environments. Challenges increase in difficulty and include misconfigurations, credential stuffing, exposed and failing backups, and malware.

**Geared towards students pursuing cybersecurity degree programs.*

Over 800 user attempts since launch



https://nice-challenge.com/



CDET Training Offerings

Be sure to check out all the different CDET training and content!

- Additional CISA Training
- FedVTE Login Page (usalearning.gov)
- President's Cup Practice Site
- CISA's GitHub Page
- CISA's YouTube Channel
- ICS Training Range via the Virtual Learning Portal (VLP)
- CISA Cybersecurity Training & Exercises
- Cybersecurity Workforce Training Guide

*To learn more email **education@cisa.dhs.gov***