U.S. DEPARTMENT OF
ENERGY

Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

Veterans Health Administration uses FEMP Cyber Training Game to Enhance Cyber Awareness Among Energy Managers

VA Sierra Nevada Health Care System, Reno, NV. *Photo courtesy of Dept. of Veterans Affairs.*

The U.S. Department of Energy's FEMP developed an accredited, interactive, cybersecurity training game to help enhance the cybersecurity capabilities of the federal energy and water management community.

The Need for OT Cybersecurity

As advances in the connectedness and interoperability of facility related control systems grow, there is an increasing need to ensure that operational technologies (OT) are cybersecure. OT controls physical functions, such as those in an office building, hospital, or even a large manufacturing plant, and can be tempting targets for designated foreign terrorist organizations, persistent threat actors, or cyber criminals.

FEMP, working with the Pacific Northwest National Laboratory, has a suite of self-assessment tools to help facility staff assess their cybersecurity posture and communicate among stakeholders about cybersecurity risk. The tools help users across the five key cybersecurity functions laid out by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): identify, detect, protect, respond, and recover. FEMP's tools tailor the CSF for the facilities context called the Facility Cybersecurity Framework (FCF).

But tools alone will not secure federal facilities—the federal energy management community needs to be able to apply key OT cybersecurity concepts in the real-world as well.

Interactive Training

FEMP's Facility Cybersecurity Framework (FCF) Training Game aims to address that challenge. This accredited and interactive game helps players gain experience with and respond to cybersecurity events. Based on real-world experiences, the game asks users to apply the skills and self-assessment tools covered by the Facility Cybersecurity Framework to protect federal facilities from cybersecurity attacks.

The Veterans Health Administration (VHA) Energy Engineer's Working Group (VHA EEWG) recently used the Training Game to enhance their awareness of key OT cybersecurity concepts. The VHA has 170 medical centers across the country that serve to backup the public healthcare system in times of national emergencies. The VHA EEWG works to improve and enhance the overall U.S. Department of Veterans Health Administration's Energy Management Program.

"We were interested in FEMP's cybersecurity Training Game. We're greatly aware of the need for OT cybersecurity due to previous assessments and concern about potential cyber-attack surfaces based on our strategic engagement with the DOE CESER program office," said Allan Federman, Chairperson of the VHA EEWG. "We encourage cybersecurity exercises and training, like the Training Game, to help ensure this serious matter is getting the attention it requires."

The game can be an important first step for those who understand the need for OT cybersecurity training in real-world scenarios. "I think the information and lessons learned in the game would be good for any federal facility with the potential to be exploited," said Samuel Hirschman, Energy Manager for the VA St.

Louis, Columbia Health Care System after playing the Training Game. "Learning key cybersecurity terms and how systems were exploited and can be protected in different scenarios was insightful."

The Training Game currently offers five scenarios, with one—Centipede—offering continuing education units through the Whole Building Design Guide (see Figure 1).

In the "Centipede" scenario, the user is playing as a federal employee at the General Services Administration whose primary job duties involve energy and facility management. In the game, players are asked to take action in the face of cybersecurity crises, which could include choosing to develop a cybersecurity plan, enhancing protections, or mitigating cybersecurity gaps discovered in the facility. As in the real world, management insight and priorities are available to users to help choose among competing priorities.

At the end of the game, a report is generated showing the pathway the player took in response to requests for action, as well as the optimal pathway and control strategy to help understand where resources may be most effectively before, during, and after a cybersecurity attack or event.

Members of the VHA EWWG felt the Centipede scenario was very applicable to their duties and responsibilities. Given that it was based on a real-world scenario, they felt it was something that could be encountered by their engineers in the field. "The Federal Buildings Personnel Training Act requires a trained federal facility workforce," said Federman. "The Training Game helps give us some compressed training to give our staff experience with cybersecurity topics. We must continuously train our energy managers to make sure we maintain our cyber-readiness in order to protect our mission critical infrastructure and assets on behalf of the veterans we serve." ■

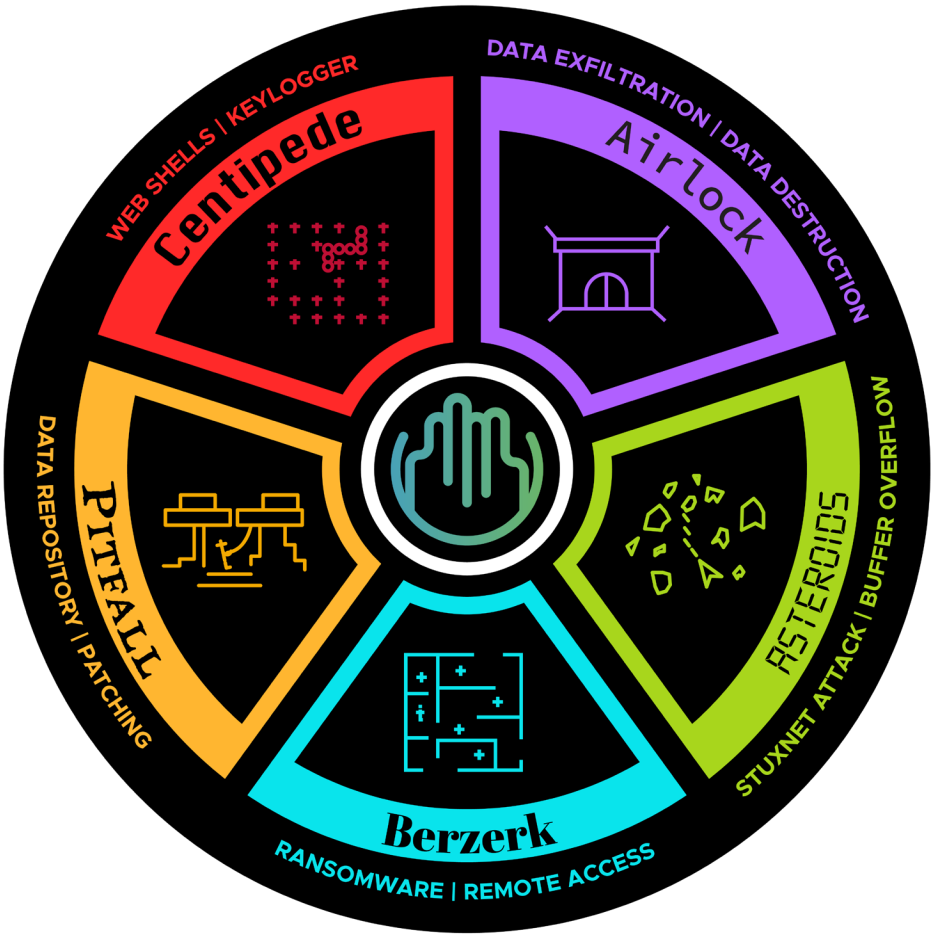

Figure 1: Training Game Scenarios. *Image courtesy of Pacific Northwest National Laboratory.*

Key Links:

FRCS Self-Assessment Toolsuite: https://facilitycyber.labworks.org/

Training Game: https://facilitycyber.labworks.org/training/trainingGame

Veterans Health Administration (VHA) Energy Engineer's Working Group: https://www.visn21.va.gov/vater.asp

WBDG FEMP Courses, search by "Cybersecurity": https://www.wbdg.org/continuing-education/femp-courses

U.S. DEPARTMENT OF ENERGY
Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

FEMP Federal Energy Management Program

For more information, visit:
energy.gov/eere/femp

DOE/EE-2363 · June 2021