Wisconsin National Guard: Part of cyber defense exercise

Posted on Tuesday, Jun 21, 2022

NORTH LITTLE ROCK, Ark. — Always Ready, Always There includes cyberspace.

Members of Wisconsin's Cyber Response Team — the state's volunteer resource for cyber incidents — and eight Wisconsin National Guard members participated in Cyber Shield 22, the Defense Department's largest unclassified cyber defense exercise, which this year was held June 5-17 at the Army National Guard's Professional Educational Center in Camp Joseph T. Robinson in North Little Rock, Arkansas.

Various teams served roles in the exercise. The Blue Team was the defender of the network, and the focus of the exercise. The Red Team was the enemy force, or hackers, trying to compromise the network. The White Team was comprised of exercise observers and controllers, while the Gold Team was made of subject matter experts to provide instruction as needed. The Green Team operated and maintained the network used for the exercise, and the Black Team took care of exercise administrative functions such as lodging and meals.

"Our Blue Team consisted of four Wisconsin Army National Guard Soldiers, two Minnesota Air National Guard Airmen, one Naval Reserve Sailor and two civilians from the Wisconsin Cyber Response Team," said 1st Sgt. Michael David, an intelligence analyst with the Wisconsin Army National Guard. "Additionally, we had a Soldier on the Red Team, two on the White Team, and a Wisconsin Air National Guard [legal officer] and a state civilian CRT member acting as network owner for the Blue Team."

Wisconsin's cyber contingent included members of the Wisconsin detachment of the 176th Cyber Protection Team, which in late 2021 returned from a 14-month

deployment to Fort Meade, Maryland in support of U.S. Cyber Command.

David has now participated in five Cyber Shield exercises, and Wisconsin has sent blue teams to at least four of the exercises. He said that with many newer team members, this has been a building year.

“We used this exercise to verify our current standard operating procedures, and to build team cohesion,” David said.

Past exercises focused on attacks on critical infrastructure key networks owned by utilities or small companies. This year, Cyber Shield focused on the Defensive Cyber Operations Element (DCOE) response to the Department of Defense Information Network (DoDIN).

“This exercise will facilitate a jumping-off point for discussions going forward,” David said, “in the event that the DCOE has to respond to a major event on the DoDIN.”

According to the National Guard Bureau, the annual exercise is a concentrated effort to develop, train and exercise cyber forces in computer network internal defensive measures and cyber incident response.

“Cyber warfare is not just our future, it is our contemporary reality,” said Gen. Daniel Hokanson, National Guard Bureau chief, said during an April U.S. Cyber Command summit. “The National Guard is positioned to be leaders in the digital domain, and continues to enhance our nation’s cyber capabilities in combat and in the homeland.”

This is because, Hokanson explained, many of the 4,000 National Guard cyber operators from 40 states work for leading tech companies.

“The National Guard has the knowledge, skills and abilities to play a critical role in the DoD’s cyber enterprise,” Hokanson said.

George Battistelli, Cyber Shield 2022 exercise director, and the Army National Guard’s deputy chief information officer, said that the cyber skills many National Guard members bring to the fight are unique within the Defense Department, and can be brought to bear to defend the military’s own networks.

“We’re really trying to train the defensive cyber operations personnel,” Batistelli

said. “We will continue to evolve the exercise as the threat evolves.”

David said Wisconsin is one of the few states to have an active cyber response capability.

“To do this, we leverage our public and private partnerships,” he said. “When there is an incident, not only does the Guard respond, but we do so with employees from across state, local and tribal territory government workers, and some employees from private organizations.”

Wisconsin’s Cyber Response Team has around 200 volunteers, of whom 70 are trained and ready to respond to a cyber incident. CRT members include members of the Wisconsin National Guard and the U.S. Coast Guard, state IT professionals, school and municipal government employees and workers from private organizations.

“As we like to train as we fight, we bring these same people to participate with us in our cyber training as well,” David continued.

The first week of Cyber Shield involved training classes and hands-on exercises. Participants also had the opportunity to take information technology classes and earn industry-standard certifications which can be used in military and civilian careers.

The second week of the exercise had the Red Team take on the Blue Team. Blue Team members were required to identify intrusion into the computer network and counter the hacker’s actions.

“It is important for us to continue to train our Soldiers using real-world events, so they are able to cut down the noise and focus on the mission,” Battistelli said. “In the exercise, and in the real world, we strive to achieve and maintain information advantage over our adversaries.”

The exercise included a “Purple Day,” where Blue and Red Team members met to discuss the attacks and evaluate response efforts.

“We have to be right 100 percent of the time,” Battistelli said. “Our adversaries only need to be right once to get into our networks.”