Table of Contents

General Overview

Welcome to the Department of Energy CyberForce Competition™. Your team is responsible for responding to the CyberForce Competition (CFC) Scenario and will be referred to as the Blue Team throughout this document. Read and review the scenario frequently to better understand the Blue Team mission in this competition. It is critical that you familiarize yourself with both the Rules document and Scoring document to ensure your team performs to the best of their abilities.

On November 12, 2018 all Blue teams will receive credentials for access to their own Azure cloud environment which hosts a mostly functional IT environment used to manage an Industrial Control System (ICS) and High Performance Computing (HPC) cluster. The credentials will be sent to all students. Each Blue team Azure environment for will contain several Virtual Machines (VMs) that the Blue team must manage and one VM managed by the CFC staff (White Team).

ICS Human Machine Interface (HMI) will be available through each Blue team's Azure environment from November 19 until November 29. You will have physical access to this cyber-physical device when you arrive on-site at your assigned national laboratory on November 30, 2018. During this setup period on November 30 you will also have an opportunity to acquaint yourself with the competition environment and gain hands-on assistance from laboratory volunteers, if needed. This will be a neutral competition period in which the red team will be allowed to perform passive scanning, but no active measures or attacks. Please notify a laboratory volunteer if you feel this is not the case.

Your Blue Team must submit documentation, similar to a cyber security plan, to the White Team that details your team's strategy for assessing the threats to their environment, hardening and monitoring their network, and responding to incidents. The White Team Security Strategy Documentation is due no later than 11:59 pm in your time zone on November 27, 2018.

During the attack phase of the competition on December 1, the Red Team will attempt to compromise your network. In addition, a Green Team will act as business users of the system by assessing its usability through a website that you make available to them. Finally, one member of your team will have two minutes to present the way your team has adopted an innovative and cutting-edge strategy to the Phish Tank (aka CISO Panel). A more comprehensive description of these teams follows this document.

Additional details for all scoring components are available in the Scoring guidelines.

CyberForce Competition™ December 2018 Scenario

You and your team have been working at Big Oil Logistics and Transportation Corporation (BOLT Corp.) for several years as dedicated system administrators and operations specialists. BOLT Corp. is a leading company in the petroleum discovery, exploration, and transportation field. BOLT Corp.'s use of high-performance computing (HPC) has provided much insight in terms of projections as to the locations of future excavations of raw materials, along with confidence in determining the most efficient route(s) for petroleum flow in the pipelines. HPC also helps in providing your team with a detailed view into current pipeline status and health.

At the beginning of each fiscal year, your team submits a report on the health of BOLT's Information Technology and Operational Technology (IT and OT) systems, including any cyber weaknesses. Because numerous cyber-attacks have been prevalent on the news within the last several weeks, you and your team have been granted permission to restructure a majority of the system to make it as cyber secure as possible, but with the caveats that no major purchases can be made, as well as no major upgrades to existing critical production systems, unless clearly stated otherwise.

Your team has already replaced a few non-critical systems with newer and more secure systems. However, it is imperative that once the restructure starts, you must be able to return the system to its full production state as quickly as possible. Your team has roughly three weeks to make the BOLT Corp. systems as secure as possible while remaining completely functional and user friendly.

Getting Started

Support Provided Prior to the Competition

Remote Setup

Student setup will be available remotely 24/7 after November 12, 2018 until the temporary Nov 29 offline period. White team support will be provided via webinars the week of November 12 and via email. Teams are encouraged to provide assistance to one another via the Slack Channel.

Students have been provided a registration link valid for 48 hours to the #cyberforcecomp-dec18 Slack channel available in the Slack app. If you need a new registration link, please email CyberForceCompetition@anl.gov. When registering in Slack, please be sure to include your Team # in your username (i.e., T23 – Janet; T45 – Bob).

VPN Install

The competition uses OpenVPN for access into the Azure environment. You will be provided an OVPN configuration file to connect to your network. Clients for each operating system can be found below:

- **Windows -** https://openvpn.net/index.php/download/community-downloads.html
  - Place the OVPN file into "C:\Program Files\Openvpn\config".
- **MacOS -** https://www.tunnelblick.net.
  - Double click the OVPN file to import it to Tunnelblick.
- **Linux** - sudo apt (or yum) install openvpn.
  - Run 'openvpn --config YOUR_OVPN_FILE.ovpn'

Azure Credentials

You should have received an email from CyberForceCompetition@anl.gov with your Azure credentials. If you did not, please contact CyberForceCompetition@anl.gov.

Blue teams are encouraged to seek help during the setup phase from one another and/or their mentors.

Key Dates

Opportunities for Q&A will be included in each of the educational webinars as outlined under Key Dates below:

Key Dates	Activity
Monday, November 12, 2018 Via email: CyberForceCompetition@anl.gov	Students are provided full rule set, guidance, and access to their Azure platform.
Monday, November 12, 2018 (3:30-5pm PT/4:30-6pm MT/5:30-7pm CT/6:30-8pm ET)	*Educational Interactive Webinar*: Introduction to CyberForce Competition™ and Industrial Control Systems (ICS) and Information Sharing
Tuesday, November 13, 2018 (3:30-5pm PT/4:30-6pm MT/5:30-7pm CT/6:30-8pm ET)	*Educational Interactive Webinar*: Introduction to Azure Environment, Scoring and Rules, Communication between Teams
Wednesday, November 14, 2018 (3:30-5pm PT/4:30-6 pm MT/5:30-7 pm CT/6:30-8 pm ET)	*Educational Interactive Webinar:* How to be Effective in the Phish Tank/CISO Panel Portion of the Competition and Review of Key Rules and Rules of Engagement
Thursday, November 15, 2018 (10am-1pm PT/11am-2pm MT/12-3pm CT/1-4pm ET)	*Education Interactive Question & Answer*: Azure Environment
Monday, November 19, 2018 Via Azure	Students are provided remote access to their industrial control systems.
Monday, November 19, 2018 (12-1:30pm PT/1-2:30pm MT/2-3:30pm CT/3-4:30pm ET)	*Educational Interactive Question & Answer*: Industrial Control System
Thursday, November 29, 2018 12pm Local Time of Hosting Site	Students temporarily lose remote access to their industrial control and high performance computing systems
Friday, November 30, 2018 See hosting laboratory's agenda	Students are provided physical access to their hosting laboratory* and their industrial control systems
Friday, November 30, 2018 5pm PT/6pm MT/7pm CT/8pm ET	Students are required to have all user information, including usernames and passwords, into the sCOARboard for Saturday morning.
Saturday, December 1, 2018	Competition Day*

See hosting laboratory's agenda	

* Please note some laboratories require arrival by certain times on Friday and Saturday.

Onsite Setup

Support Provided During the Competition

The following support may be provided during the competition but will be limited in scope:

- Image refresh
- Connectivity issues
- Industrial Control System issues

If your team needs support during the competition, please find a staff member (in white t-shirts) to assist you. It is imperative that you ensure your competition environment is set up properly the day before the competition (November 30). There will be staff present to assist and troubleshoot errors before they count against you in competition. Intervention not explicitly part of a competition setup error may incur point penalty at the discretion of the competition scoring team. Penalties are outlined in the scoring guidelines provided to each team prior to the competition start.

Competition Team Descriptions

Red Team - Volunteers

The Red team's goal is to evaluate the security of Blue team networks. This team is composed of volunteers with backgrounds in information security, computer security, computer science, and other related fields. Red team members rely on their backgrounds to identify and exploit vulnerabilities within Blue Team networks. Their knowledge of computer and industrial control system networks lead to cascading effects ranging from website defacement and lack of service uptime all the way to complete network control. At the conclusion of the competition, Red team volunteers will provide reports to the Blue teams to explain successful exploits and related mitigation techniques.

Green Team - Volunteers

The Green team members serve as models for real-life users of the system. This team is composed of volunteers that have a wide range of knowledge and skill sets that mirror a typical work environment. The Green team will represent a diverse set of user roles ranging from administrative assistants, to technical specialists, and everything in-between. The Green team will review and evaluate the Blue teams' work and submit points based on how easily they were able to do their "jobs" without unnecessary security obstacles.

White Team - National Laboratory Staff

The White team is the competition architecture team. They are available for assistance to any team in the event of network failures, hardware issues, documentation issues, rules questions, or industrial control system device failures. Some requests will cost Blue teams points (see the Scoring guidelines for details). This team will be wearing white CyberForce Competition T-shirts and will not use any information shared with them to assist the Red team.

CISO Panel/Phish Tank

The Phish Tank is a security pitch where you try and convince volunteers to give you competition points based on several criteria. Teams must demonstrate technical expertise, novelty, and creativity in order to persuade the Phish to give them full credit.